УДК 004.056.55

Д. О. Пінчук
І. О. Бондаренко

ПЕРСПЕКТИВИ РОЗВИТКУ КВАНТОВИХ ТЕЛЕКОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ ДЛЯ ЗАХИЩЕНОЇ ПЕРЕДАЧІ ДАНИХ

Вінницький національний технічний університет

Анотація

У тезах розглянуто перспективи розвитку квантових телекомунікаційних технологій в Україні та світі для забезпечення захищеної передачі даних. Проаналізовано основні принципи квантової криптографії, стан розвитку технологій, їх переваги та виклики. Особлива увага приділяється використанню квантових систем для створення надійних каналів зв'язку, а також їх інтеграції у національну інфраструктуру кібербезпеки. Висвітлено перспективи участі України у глобальних проектах квантового інтернету та підвищення інформаційної безпеки державних і приватних установ.

Ключові слова: квантова криптографія, квантові телекомунікації, захищена передача даних, квантовий інтернет, кібербезпека, квантовий комп'ютер, квантовий розподіл ключів.

Abstract

The theses consider the prospects for the development of quantum telecommunication technologies in Ukraine and the world to ensure secure data transmission. The main principles of quantum cryptography, the state of technology development, their advantages and challenges are analyzed. Special attention is paid to the use of quantum systems to create reliable communication channels, as well as their integration into the national cyber security infrastructure. The prospects of Ukraine's participation in global quantum internet projects and improving the information security of state and private institutions are highlighted.

Keywords: quantum cryptography, quantum telecommunications, secure data transfer, quantum internet, cyber security, quantum computer, quantum key distribution.

Вступ

Квантові телекомунікаційні технології – один з ключових елементів у розвитку сучасної інформаційної безпеки. Вони пропонують унікальні можливості для захищеної передачі даних, використовуючи фундаментальні закони квантової фізики. Основою таких систем є квантова криптографія, яка забезпечує надійний захист завдяки неможливості перехоплення квантових ключів без їх пошкодження. Особливо актуальними ці технології є в умовах зростаючих кіберзагроз та можливого використання квантових комп'ютерів для зламу традиційних криптографічних систем.

В Україні розвиток квантових телекомунікацій перебуває на початковій стадії, проте вже з'являються освітні програми та наукові ініціативи. Наприклад, у Львівському національному університеті започатковано програму з квантового програмування, а вітчизняні науковці активно досліджують аспекти квантової криптографії та телекомунікацій. У міжнародному контексті Україна має потенціал для інтеграції у глобальні проекти, спрямовані на розбудову квантового інтернету та нових стандартів захищених мереж [1].

Результати дослідження

Для дослідження даної теми розглянемо основні поняття.

Квантова криптографія використовує принципи квантової механіки для створення безпечних методів зв'язку, які принципово відрізняються від традиційних криптографічних методів. Розуміння її основ є важливим для розуміння того, як квантова криптографія може підвищити безпеку мережі. Квантові комунікації передбачають використання квантових бітів або кубітів, які, на відміну від класичних бітів, можуть існувати в кількох станах одночасно (суперпозиція) і бути переплетеними з іншими кубітами. Система в суперпозиції може існувати в комбінації всіх можливих станів, доки вона не буде виміряна [2].

У квантових обчисленнях кубіти (квантові біти) використовують суперпозицію для виконання складних обчислень зі швидкістю, з якою класичні комп’ютери не можуть зрівнятися.

Крім того, у квантовій криптографії суперпозиція використовується для створення безпечних каналів зв’язку. Це гарантує, що будь-які спроби прослуховування порушать квантовий стан, сповіщаючи залучені сторони.

Квантові технології відкривають перед Україною нові можливості для розвитку науки, технологій та економіки. Завдяки активній участі українських вчених і стартапів, Україна має всі шанси стати одним з лідерів у цій перспективній галузі [3]. Українські вчені активно беруть участь у розробці квантових фотонних технологій, що підтверджується успіхами британського стартапу Aegiq, що подав патент га розроблену ним технологію [4].

Науковці Державної наукової установи «Київський академічний університет» зробили прорив у розробці нових матеріалів для квантових комп'ютерів. Їх проект «Багатозонність електронних станів: фізика та застосування», який отримав перемогу у конкурсі Національного фонду досліджень України «Підтримка провідних та молодих вчених», спрямований на вивчення багатозонності електронних станів, дозволив значно покращити характеристики надпровідних джозефсонівських контактів, що є ключовими елементами квантових комп'ютерів. Ці досягнення відкривають нові перспективи для створення стабільніших і ефективніших квантових обчислювальних систем [5].

Квантова криптографія стикається з численними практичними перешкодами, які заважають її впровадженню [2]:

1. Однією з головних проблем квантової криптографії є обмеження відстані. Передача квантових станів на великі відстані є складним завданням через крихку природу квантових станів. Квантові стани можуть бути легко зруйновані під впливом зовнішніх факторів, таких як втрати в оптичних волокнах, шум і взаємодія з навколишнім середовищем, що ускладнює підтримку когерентності квантового стану. Це ускладнює встановлення безпечного квантового каналу на великих відстанях. Тому, для передачі інформації на великі відстані необхідні квантові ретранслятори, які дозволяють відновити квантовий стан.

2. Квантова передача даних вимагає створення спеціалізованої інфраструктури, що включає високоточне обладнання для роботи з окремими фотонами та спеціальні оптичні волокна. Однак, така інфраструктура поки що є досить дорогою та складною у масштабуванні. Послідовна передача кожного фотона обмежує швидкість передачі даних, а для забезпечення безпеки кожному абоненту потрібен окремий канал зв'язку. Наприклад, для захисту транзакцій компанії, як-от Amazon, мали б прокладати окремі кабелі між своїми серверами та кожним клієнтським пристроєм, що потребувало б значних інвестицій у нову інфраструктуру [6].

3. Захист ключів, а не всієї інформації. Квантове шифрування не розв’язує всі проблеми безпеки — воно створює захищений канал для передачі ключів, але не шифрує самі дані. Після обміну ключами інформація шифрується традиційними методами (AES, ChaCha20 тощо), які досі можуть бути вразливими до квантових атак. Для повного захисту даних потрібні додаткові рішення, як-от постквантова криптографія, що забезпечує стійкість до майбутніх квантових загроз [2].

Постквантова криптографія – це частина криптографії, яка фокусується на розробці алгоритмів шифрування, стійких до атак з використанням квантових комп'ютерів. Тобто, це новий рівень захисту інформації, який дозволить зберігати конфіденційність даних навіть у світі, де квантові комп’ютери стануть потужними інструментами. Постквантові алгоритми засновані на математичних задачах, які вважаються складними як для класичних, так і для квантових комп’ютерів [2]. Постквантові криптоалгоритми впроваджують у державних системах США та інших організаціях, які потребують сертифікації FIPS (Federal Information Processing Standards).

Розробка та впровадження постквантових криптографічних алгоритмів вимагатиме ретельного планування та координації, щоб забезпечити плавний перехід. Організації повинні бути в курсі прогресу в цій галузі та бути готовими адаптувати свої криптографічні системи, коли це необхідно [6].

Впровадження PQC – це не просто підготовка до можливих загроз, а стратегічний крок на випередження. Навіть якщо квантові комп’ютери, здатні зламати сучасні алгоритми, поки що не створені, адаптація нових стандартів залишається критично важливою [2].

Таким чином, розробка та розгортання квантових телекомунікаційних інфраструктур є не лише науковим і технологічним заходом, а й стратегічним кроком для забезпечення національної безпеки України та підтримки конкурентної переваги на глобальній арені інформаційних технологій та кібербезпеки.

Висновки

Квантові телекомунікації є однією з найперспективніших сфер для розвитку сучасних технологій захисту інформації. Використання квантової криптографії забезпечує унікальну стійкість проти загроз перехоплення, зокрема від майбутніх квантових комп'ютерів. Україна, незважаючи на обмежені ресурси, демонструє потенціал у цій сфері завдяки освітнім ініціативам, науковим розробкам та участі в міжнародних дослідженнях.

Проте для впровадження квантових технологій необхідно вирішити низку проблем. Серед основних проблем є висока вартість розробки, потреба у спеціалізованій інфраструктурі та значні вимоги до технічного забезпечення. Також важливим аспектом є створення нормативної бази для регулювання використання квантових технологій у державних та приватних секторах.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. У Львівському університеті обговорили стан та перспективи квантових комп'ютерів. Львівський національний університет імені Івана Франка. URL: https://lnu.edu.ua/u-lvivskomu-universyteti-obhovoryly-stan-ta-perspektyvy-kvantovykh-komp-iuteriv/ (дата звернення: 14.11.2024).
2. Квантова криптографія: революція в кібербезпеці чи лише теорія?. robot_dreams - онлайн-курси для фахівців у сфері big data, machine learning, data science | Робот Дрімс. URL: https://robotdreams.cc/uk/blog/570-kvantova-kriptografiya (дата звернення: 14.11.2024).
3. Квантовий комп'ютер: нова ера на порозі – Газета "Світ". *Газета "Світ" – Науково-популярне періодичне видання*. URL: https://svit.kpi.ua/2021/09/13/1772/ (дата звернення: 17.11.2024).
4. Квантові технології: український стартап Aegiq прагне замінити цифровий зв'язок у всьому світі на квантовий. hubs. Новини, варті уваги. URL: https://hubs.ua/news/kvantovi-tehnologiyi-ukrayins-kij-startap-aegiq-pragne-zaminiti-tsifrovij-zv-yazok-u-vs-omu-sviti-na-kvantovij-268723.html (дата звернення: 19.11.2024).
5. Квантовий комп'ютер: нова ера на порозі – Національний фонд досліджень України. Національний фонд досліджень України – Віримо в нашу перемогу!. URL: https://nrfu.org.ua/news/kvantovyj-kompyuter-nova-era-na-porozi/ (дата звернення: 21.11.2024).
6. Новиков, Д. Технології постквантової криптографії / Д. Новиков, В. Полторак // Адаптивні системи автоматичного управління : міжвідомчий науково-технічний збірник. – 2023. – № 1 (42). – С. 171-183.

Пінчук Дар'я Олександрівна **–** студентка групи 1КІТС-22б, Факультет менеджменту та інформаційної безпеки, Вінницький національний технічний університет, м. Вінниця, e-mail: dashapinchukschool@gmail.com

Бондаренко Ірина Олексіївна **–** асистент кафедри менеджменту та безпеки інформаційних систем, Вінницький національний технічний університет, м. Вінниця, e-mail: bondarenko.i@vntu.edu.ua

Pinchuk Daria O. – student of group 1KITS-22b, Faculty of Management and Information Security, Vinnytsia National Technical University, Vinnytsia, e-mail: dashapinchukschool@gmail.com

Bondarenko Iryna O. **–** assistant of the Department of Management and Security of Information Systems Vinnytsia National Technical University, Vinnytsia, e-mail: bondarenko.i@vntu.edu.ua