***Дячук О.Ю., ст. викладач***
***Іваницький Р.В., здобувач***
*Державний університет «Житомирська політехніка»*

# КОМПРОМЕТАЦІЯ ПРОТОКОЛІВ КВАНТОВИХ КОМУНІКАЦІЙ ТА ВПЛИВ НА БЕЗПЕКУ МЕРЕЖ МАЙБУТНЬОГО

З розвитком квантових технологій виникає необхідність дослідження потенційних загроз у протоколах квантових комунікацій та їхнього впливу на безпеку інформаційних мереж. Квантові комунікації пропонують революційні методи захисту даних, такі як квантовий розподіл ключів (QKD), однак вони також мають власні вразливості, що можуть бути експлуатовані зловмисниками.

Одним із головних принципів квантової криптографії є неможливість перехоплення інформації без її зміни, що базується на фундаментальних законах квантової механіки. Найпоширенішим протоколом є BB84, який дозволяє обмінюватися ключами без ризику перехоплення. Однак у практичних реалізаціях таких протоколів існують фізичні вразливості, що можуть бути використані для атак. Наприклад, лазерні атаки на детектори або атаки за допомогою маніпуляцій джерелом світла можуть дозволити зловмиснику зчитувати інформацію без порушення узгоджених правил передачі квантових даних .

Квантові комп'ютери також становлять серйозну загрозу для сучасних криптографічних методів, що базуються на складності обчислення, таких як RSA та алгоритми на основі еліптичних кривих. Завдяки алгоритму Шора квантові обчислювальні пристрої зможуть розкладати великі числа на множники в експоненційно коротший термін порівняно з класичними комп’ютерами. Це призведе до необхідності розробки квантово-стійкої криптографії, що базується на задачах, які складно вирішити навіть для квантових обчислень .

Окрім вразливостей на рівні криптографії, існують ризики, пов’язані із фізичною інфраструктурою квантових мереж. Наприклад, квантові повторювачі, що використовуються для збільшення дальності передачі квантових сигналів, можуть стати об’єктом атак. Вразливості можуть включати маніпуляції з квантовими станами або створення штучних заплутаних пар частинок для введення системи в оману. Також існує ризик атак на рівні синхронізації квантових сигналів, що може призвести до збільшення похибок у передачі даних [1].

Для мінімізації ризиків у квантових комунікаціях розглядаються кілька напрямків розвитку безпеки. По-перше, це вдосконалення механізмів виявлення атак, включаючи використання нових методів контролю параметрів переданих квантових частинок. По-друге, досліджується можливість створення гібридних криптографічних протоколів, що поєднують квантові та постквантові методи захисту. Крім того, тривають дослідження з розробки більш надійних квантових повторювачів та методів компенсації можливих атак на фізичному рівні [2].

Одним із перспективних напрямків є створення постквантових алгоритмів, що базуються на математичних задачах, які не піддаються ефективному вирішенню квантовими комп'ютерами. Прикладами таких алгоритмів є криптографія на основі решіток, хеш-функцій та ізогеній еліптичних кривих. Ці алгоритми вже активно досліджуються в рамках міжнародних стандартів, таких як ініціатива NIST щодо постквантової криптографії [3].

Ще одним важливим напрямком є застосування блокчейн-технологій для забезпечення цілісності квантових комунікацій. Розподілені реєстри можуть гарантувати достовірність переданих квантових ключів, унеможливлюючи їхню компрометацію з боку зловмисників.

Таким чином, дослідження вразливостей квантових комунікаційних систем та їхній вплив на безпеку майбутніх мереж є критично важливим завданням. Попри переваги квантової криптографії, залишається низка викликів, що потребують вирішення, включаючи як фізичні атаки, так і ризики, пов’язані з появою квантових обчислень. Розвиток нових захисних механізмів та адаптація криптографії до нових реалій є ключовими напрямками для забезпечення інформаційної безпеки у майбутньому.

**Список використаних джерел:**

1. Xu F., Ma X., Zhang Q., Lo H. K., Pan J. W. Secure quantum key distribution with realistic devices. Reviews of Modern Physics. 2020. Vol. 92, No. 2. P. 025002. URL: https://arxiv.org/abs/1903.09051 (дата звернення: 15.03.2025).
2. Pirandola S., Andersen U. L., Banchi L., Berta M., Bunandar D., Colbeck R., ... Wallden P. Advances in quantum cryptography. Advances in Optics and Photonics. 2020. Vol. 12, No. 4. P. 1012–1236. URL: https://arxiv.org/abs/1906.01645 (дата звернення: 15.03.2025).
3. Chen L., Jordan S., Liu Y. K., Moody D., Peralta R., Perlner R., Smith-Tone D. Report on post-quantum cryptography. National Institute of Standards and Technology, 2016. URL: https://www.scirp.org/reference/referencespapers?referenceid=3702424 (дата звернення: 15.03.2025).