Супруненко К. О., здобувач,
Шелуха О. О., к.т.н., доцент
Державний університет «Житомирська політехніка»

ПЕРСПЕКТИВИ ТА ПРОБЛЕМИ ІНТЕГРАЦІЇ КВАНТОВИХ ТЕХНОЛОГІЙ У СУЧАСНІ СИСТЕМИ КІБЕРЗАХИСТУ

Захист від кібератак та збереження цілісності інформації стають все більш важливими у світі, де діджиталізація переповнює наші повсякденність і бізнес-процеси.

Квантові технології є перспективним напрямком розвитку заходів з захисту інформації. Однією з головних областей є квантова криптографія, яка базується на принципах квантової механіки для створення безпечних криптографічних систем. Наприклад, протоколи квантової криптографії використовують принципи невизначеності та заплутаності для забезпечення абсолютної безпеки комунікаційних каналів. Квантовий розподіл ключів, найбільш вивчений і життєздатний метод квантової криптографії, використовує серію фотонів для передачі секретної випадкової послідовності, відомої як ключ. Порівнюючи вимірювання, зроблені на обох кінцях передачі, користувачі дізнаються, чи був ключ зламаний. Якщо хтось прослуховував телефон, він міг перехопити секретний код, не знаючи абонентів. Навпаки, немає способу «прослухати» або спостерігати квантовий зашифрований ключ, не порушуючи фотони та не змінюючи результати вимірювань на кожному кінці [1].

Крім того, квантові технології використовуються у квантових обчисленнях, де кубіти замінюють класичні біти, що дозволяє вирішувати складні задачі швидше, ніж традиційні комп'ютери. Це може мати важливий вплив на розвиток алгоритмів шифрування та розшифрування, зміцнюючи безпеку інформаційних систем [2, 3].

Тобто, ці технології використовують принцип квантової обчислювальної переваги, де вони можуть вирішувати певні обчислювальні завдання швидше, ніж класичні комп'ютери. Використання квантової криптографії є ще однією ключовою складовою, забезпечуючи безпеку обміну інформацією. Ці принципи становлять основу для новаторських застосувань у сфері обчислень, комунікацій та кібербезпеки.

Квантові алгоритми в кіберзахисті використовують потужність квантових обчислень для шифрування та розшифрування інформації, що може революціонізувати кібербезпеку: використання квантових властивостей для створення абсолютно безпечних криптографічних протоколів. З іншого боку квантовий алгоритм Шора може швидко розкладати числа на прості множники, що може порушити основи криптографії на основі факторизації; зловмисники можуть використовувати квантові комп'ютери для швидкого зламування стандартних шифрів і захисту; квантові комп'ютери можуть швидко аналізувати великі мережі та застосовувати методи симуляції для виявлення уразливостей.

Також викликами інтеграції квантових технологій у сучасні системи є необхідність вирішення складних технічних завдань, включаючи створення стабільних квантових бітів, адекватних алгоритмів корекції помилок та забезпечення ефективної взаємодії між квантовими та класичними системами. Але з іншого боку, інтеграція квантових технологій відкриває перспективи революційних досягнень у криптографії. Зокрема, квантова криптографія може забезпечити абсолютну безпеку обміну ключами, уникнувши загроз з боку потенційних квантових обчислювальників. Однак інтеграція квантових технологій також вимагає вирішення етичних та правових питань, таких як забезпечення приватності та контроль за потенційно небезпечними застосуваннями. Додатково, важливо враховувати ефекти національної та глобальної безпеки при розвитку квантових технологій [4].

Список використаних джерел

1. How Will Quantum Technologies Change Cryptography? Quantum Cryptography and Quantum Encryption Explained. Caltech Science Exchange. California Institute of Technology. URL: https://scienceexchange.caltech.edu/topics/quantum-science-explained/quantum-cryptography

2. Основи кібербезпеки та кібероборони: підручник / Ю.Г. Даник, П.П. Воробієнко, В.М. Чернега. – [Видання друге, перероб. та доп.]. – Одеса.: ОНАЗ ім. О.С. Попова, 2019. − 320 с. URL: https://metod.suitt.edu.ua/download/686

3. Корченко О.Г Василіу Є.В, Gnatyuk S. (2010). Сучасні квантові технології захисту інформації. Ukrainian Information Security Research Journal. 12. С.77-89. URL: https://doi.org/10.18372/2410-7840.12.1937

4. Лісовська Ю.П. Сучасні перспективи розвитку квантової безпеки як дифузійно якісна цифрова модель у міжнародній інформації знань. Інформація і право. №4 (35). 2020 р. С. 92-97. – URL: https://doi.org/