УДК 004.7:621.39

**Конахович Г.Ф. (НАУ), Шевченко О.В. (ДЕТУТ),
Кінзерявий В.М. (НАУ), Хохлачова Ю.Є. (НАУ)**

СУЧАСНІ МЕТОДИ КВАНТОВОЇ СТЕГАНОГРАФІЇ

У даній статті проведено дослідження існуючих методів квантової стеганографії. Запропоновано класифікацію сучасних квантово-стеганографічних методів з точки зору застосовуваних стегоконтейнерів, а також проведено якісний аналіз їх переваг та недоліків з позицій ефективності та можливості практичної реалізації.

Ключові слова: квантова стеганографія, стеганографічний протокол, стегосистема, стегоканал, контейнер, теоретико-інформаційна стійкість, однокубітова операція.

Вступ. Першочерговим чинником, що впливає на складові національної безпеки, є ступінь захищеності кіберпростору [1]. Питання кібербезпеки набуває актуальності як у процесі стрімкого розвитку комп'ютерних технологій, так і у контексті різкого збільшення терористичних актів, злочинів та інших протиправних дій, що спрямовані на порушення конфіденційності, цілісності та доступності інформації [2]. Основна роль у забезпеченні інформаційної безпеки в інформаційних та телекомунікаційних системах відводиться криптографії. Зазвичай використовуються методи традиційної симетричної та асиметричної криптографії, проте в останні роки значний інтерес викликає квантова криптографія [3-5].

Аналіз існуючих досліджень та постановка проблеми. Переважна більшість теоретичних та практичних досліджень у галузі квантової криптографії присвячена розробці та вдосконаленню протоколів квантового розподілу ключів (КРК), які поряд з іншими квантовими криптографічними протоколами становлять сукупність квантових методів захисту інформації (методів на основі квантових технологій) [3]. Кількість таких методів з часом невпинно зростає, проте в сучасній науковій літературі відсутня чітка їх класифікація, що ускладнює пошук і не дає змоги у повній мірі оцінити рівень існуючих досягнень для їх подальшого ефективного використання. До складу квантових методів захисту інформації входять [3]: КРК, квантовий прямий безпечний зв'язок, квантове розділення секрету, квантовий потоковий шифр, квантовий цифровий підпис та квантова стеганографія. Останній метод є найменш досліджуваним, проте, з огляду на можливості традиційного аналога, квантова стеганографія становить інтерес для світової наукової спільноти. Таким чином, **метою даної статті** є пошук ефективних методів квантової стеганографії, якісний аналіз переваг та недоліків, перспектив та труднощів їх практичного впровадження.

Основна частина дослідження. Проводячи паралель між криптографією та стеганографією, варто відмітити, що основним завданням останньої є приховування самого факту передачі (існування) певного повідомлення, тоді як криптографія приховує лише його зміст. Проте, на сучасному етапі, є доцільним застосування даних методів у комплексі, що дозволяє забезпечити вищий рівень захищеності. Існує багато підходів до класифікації сучасних стеганографічних методів захисту інформації, але на думку авторів найбільш повною є класифікація, представлена у роботі [6], відповідно до якої стеганографія поділяється на класичну, цифрову, лінгвістичну та квантову. *Класична стеганографія* реалізується за допомогою технічних засобів захисту інформації і включає у себе хімічні (симпатичні хімікалії, органічні рідини) та фізичні методи (схованки, камуфляж, мікрокрапки та голограми). *Цифрова стеганографія* базується на вбудовуванні додаткової інформації в цифрові об'єкти і поділяється на методи приховування даних в нерухомих зображеннях (приховування даних у просторовій чи частотній областях, розширення спектру тощо), приховування даних в аудиосигналах (кодування найменш значущих біт, фазове кодування, використання ехо-сигналу та ін.) та приховування даних у тексті (синтаксичні та семантичні методи, методи довільного інтервалу). *Лінгвістична стеганографія* приховує конфіденційну інформацію у текст, використовуючи мовні властивості та лінгвістичні ресурси, і включає у себе умовне письмо (жаргонний код, нульовий шифр, шифр "решітка"

тощо) та семаграми (візуальні та текстові). Виходячи з мети та проблематики даного дослідження, переважна його частина буде присвячена саме *квантовій стеганографії.*

Квантова стеганографія аналогічно традиційним методам має за мету підвищення рівня секретності шляхом приховування самого факту передачі інформації. Подібно до класичної цифрової стеганографії, у квантовій інформація приховується через вкладення повідомлення у надлишкову частину середовища покриття (контейнер). Квантова стеганографія ще не вийшла на рівень практичної реалізації, але в декількох працях [7-15] пропонуються теоретичні моделі стегосистем, що використовують властивості квантових станів. Даний напрям є синтезом класичної та квантової інформатик [16] та ґрунтується на спільному використанні законів квантової фізики та класичної теорії інформації.

Керті у праці [7] запропонував три стегосистеми, які використовують характеристики квантової інформації. Перша система приховує один класичний біт $E \in \{0;1\}$ в шумоподібний кубіт (подібно тому, як в класичних системах цифрової стеганографії інформація приховується в найменш значущому) заміною кубіта на $|+\rangle = (1/\sqrt{2})(|0\rangle + |1\rangle)$ (якщо $E = 1$) або $|-\rangle = (1/\sqrt{2})(|0\rangle - |1\rangle)$ (якщо $E = 0$). Друга система приховує два класичних біта в один шумоподібний кубіт шляхом заміни кубіта із використанням квантового надщільного кодування. Безпека цієї системи залежить від того, наскільки шумоподібний кубіт подібний до справжнього білого шуму, тобто повністю змішаного стану. У третій системі кубіт передається через класичний стегоканал за допомогою квантової телепортації [17]. Безпека цієї системи визначається безпекою класичної стегосистеми, що лежить в її основі.

У роботі [9] розглядаються елементарні поняття методу квантової стеганографії, який є модифікацією квантового надщільного кодування. У роботі [10] було введено поняття квантового стеганографічного зв'язку, а запропонований там протокол КРК є варіантом протоколу ВВ84, в якому й приховується стегоканал.

Простий квантовий стеганографічний протокол з використанням чотирьох двокубітових переплутаних станів Бела:

$$|\varphi^+\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle_1|0\rangle_2 + |1\rangle_1|1\rangle_2\right); \qquad |\varphi^-\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle_1|0\rangle_2 - |1\rangle_1|1\rangle_2\right);$$

$$|\psi^+\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle_1|1\rangle_2 + |1\rangle_1|0\rangle_2\right); \qquad |\psi^-\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle_1|1\rangle_2 - |1\rangle_1|0\rangle_2\right), \qquad (1)$$

запропонований в [18]. У цьому протоколі *n* станів Бела, серед яких є всі чотири стани (1) з однаковою ймовірністю, розділяються між двома легітимними сторонами, Алісою (відправник) та Бобом (отримувач), деякою третьою стороною, Трентом. Для кожного стану перший кубіт прямує до Аліси, а другий – до Боба. Секретний біт закодований у кількості *m* синглетних станів $|\psi^-\rangle$ в послідовності із *n* станів: парне *m* представляє "0", непарне – "1". Аліса та Боб виконують локальні вимірювання, кожний над своїм кубітом, і підраховують кількість синглетних станів $|\psi^-\rangle$. Таким чином, в цьому протоколі Трент може таємно передати інформацію відразу двом абонентам.

У роботі [12] протокол, запропонований у [11], був вдосконалений та реалізований практично, стани Бела генерувались шляхом спонтанного параметричного розсіювання світла. Подальше удосконалення та узагальнення схеми даного протоколу виконано у роботах [13, 14]. У роботі [15] запропоновано квантовий стеганографічний протокол, в якому інформаційний кубіт ховається в середину квантового завадостійкого коду. Таким чином, для зловмисника передавання кубітів квантовим каналом виглядає, як звичайне передавання квантової інформації в шумному каналі. Для виявлення інформаційного кубіту отримувач

повинен мати спільний секретний ключ з відправником, який повинен бути розподілений до початку стеганографічного протоколу.

На рис. 1 показано схему протоколу, запропонованого в [15]. Аліса приховує інформаційний кубіт, міняючи його містами з кубітом в її квантовому кодовому слові. Вона використовує свій секретний ключ для визначення того, який кубіт в кодовому слові повинен бути замінений. Далі, Аліса знову використовує ключ, щоб обертати інформаційний кубіт. Обертання означає, що Аліса застосовує одну з чотирьох однокубітових операцій (гейтів) I, σ_x, σ_y або σ_z до цього кубіта, визначаючи конкретну операцію за допомогою двох поточних бітів ключа.

Для зловмисника, який не має ключа, цей кубіт виглядає як такий, що знаходиться у максимально змішаному стані (обертання може трактуватися як квантовий шифр Вернама). Далі Аліса застосовує випадкові помилки деполяризації (з використанням тих же однокубітових операцій σ_x, σ_y або σ_z) до деякої частини інших кубітів кодового слова, імітуючи тим самим деякий рівень шуму в деполяризуючому каналі, а потім посилає кодове слово Бобові. Він використовує спільний з Алісою секретний ключ, щоб правильно застосувати операцію по зворотному обертанню, а потім знову використовує ключ для знаходження інформаційного кубіту.

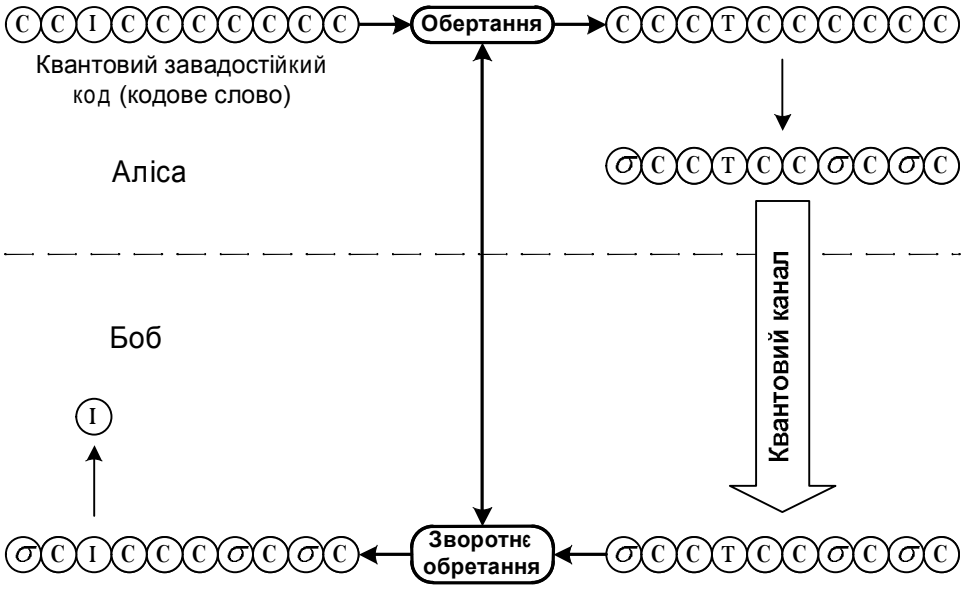

Рис.1. Схема квантового стеганографічного протоколу: C – кубіт кодового слова, I – інформаційний кубіт, T – інформаційний кубіт після обертання, σ – кубіт, на який Аліса діє оператором Паулі (кубіт, що імітує шум)

Стійкість цього протоколу залежить від стійкості попередньої процедури розподілу ключа. За рахунок використання обертання інформаційного кубіту, що еквівалентно використанню квантового шифру Вернама, може бути досягнута теоретико-інформаційна стійкість, якщо ключ розподілений з таким рівнем стійкості. Як відомо, теоретико-інформаційну стійкість розподілу ключа забезпечують відповідні протоколи КРК [3, 16]. Але, якщо зловмисник постійно моніторить канал тривалий період часу й якщо в нього є точне знання властивостей каналу, тоді він в остаточному підсумку виявить, що Аліса передає інформацію Бобові за допомогою квантового стеганографічного протоколу. Крім того, постійно виконуючи квантові вимірювання станів кубітів, що передаються, зловмисник може запобігти передаванню інформації, ефективно затопляючи квантовий канал шумом (атака "відмова в обслуговуванні").

Таким чином, на даний час пропонуються три основних методи квантової стеганографії:

1) приховування у квантовому шумі;

2) приховування із застосуванням квантових завадостійких кодів;

3) приховування у форматах даних, протоколах тощо.

Вкладення повідомлень на рівні форматів даних та протоколів вважається найбільш перспективним напрямком квантової стеганографії у майбутньому, також перспективним є метод приховування із застосуванням квантових завадостійких кодів.

Запропонована класифікація методів квантової стеганографії зображена на рис.2:

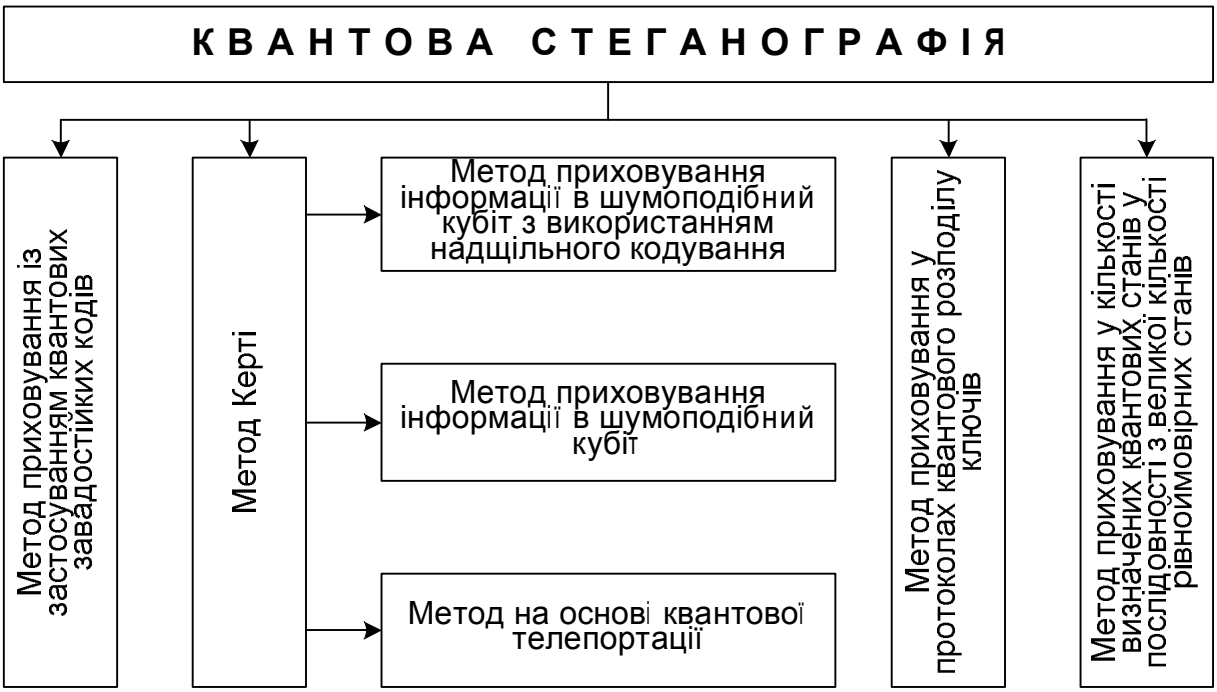

Рис.2. Методи квантової стеганографії

Взагалі, квантова стеганографія може бути значно стійкішою за традиційну внаслідок використання властивостей квантових систем, притаманних тільки квантовим системам [16], проте для практичного використання квантової стеганографії в системах захисту інформації необхідно вирішити ще ряд завдань як теоретичного, так і особливо практичного характеру.

Висновки. Таким чином, у даній роботі проведено пошук та систематизацію існуючих методів квантової стеганографії. У результаті аналізу встановлено, що базовими напрямками розвитку квантової стеганографії на даний момент є приховування даних у квантовому шумі, приховування із застосуванням квантових завадостійких кодів та приховування даних у форматах даних і протоколах. Запропоновано класифікацію квантових методів стеганографічного захисту даних з точки зору використовуваних стегоконтейнерів. Крім того, було проаналізовано переваги та недоліки кожного методу, а також проведена оцінка можливості їх практичної реалізації. Отримані результати дозволяють підвищити ефективність вибору певних квантових стеганографічних методів для побудови систем захисту інформації. Подальші дослідження можуть бути пов’язані з оцінкою стійкості досліджуваних методів до різного роду кібератак.

Література:

1. Харченко В.П. Кибертерроризм на авиационном транспорте / Харченко В.П., Чеботаренко Ю.Б., Корченко О.Г., Паціра Є.В., Гнатюк С.О. // Проблеми інформатизації та управління: збірник наукових праць: Випуск 4(28). — К.: НАУ, 2009. — С. 131-140.

2. Корченко А.Г. Построение систем защиты информации на нечетких множествах. Теория и практические решения / А.Г. Корченко. — К. : НАУ, 2005. — 336 с.

3. Корченко О.Г. Сучасні квантові технології захисту інформації / О.Г. Корченко, Є.В. Василіу, С.О. Гнатюк // Захист інформації. — 2010. — № 1. — С. 77–89.

4. Килин С.Я. Квантовая криптография : Идеи и практика : Монография / С.Я. Килин, Д.Б. Хорошко, А.П. Низовцев. — Мінськ, 2008. — 398 с.

5. Румянцев К.Е. Квантовая связь и криптография: Учебное пособие / К.Е. Румянцев, Д.М. Голубчиков — Таганрог: Изд-во ТТИ ЮФУ, 2009. — 122 с.

6. Стасюк О.І. Сучасні стеганографічні методи захисту інформації / Стасюк О.І., Гнатюк С.О., Довгич Н.І., Літош М.С. // Захист інформації. — 2011. — №1 (50). — С. 56–63.

7. Curty M., Santos D.J. Quantum steganography // In 2nd Bielefeld Workshop on Quantum Information and Complexity. — 2000. — P. 12-14.

8. Mogos G. Stego Quantum Algorithm / G. Mogos // International Symposium on Computer Science and its Applications. — 2008. — P. 187-190.

9. Natori S. Why Quantum Steganography Can Be Stronger Than Classical Steganography / S. Natori // Quantum Computation and Information, Topics Appl. Phys. — 2006. — V. 102. — P. 235-240.

10. Martin K. Steganographic communication with quantum information / K. Martin // Lecture Notes in Computer Science. — 2007. — V. 4567. — P. 32-49.

11. Terhal B.M. Hiding bits in Bell states / B.M. Terhal, D.P. DiVincenzo, D.W. Leung // Physical review letters. — 2001. — V. 86, issue 25. — P. 5807-5810.

12. Guo G.-C. Quantum data hiding with spontaneous parameter down-conversion / G.-C. Guo, G.-P. Guo // Physical review A. — 2003. — V. 68, issue 4. — 044303.

13. DiVincenzo D.P. Quantum data hiding / D.P. DiVincenzo, D.W. Leung, B.M. Terhal // IEEE Trans. Inf. Theory. — 2002. — V. 48, number 3. — P. 580–599.

14. DiVincenzo D.P. Hiding quantum data / D.P. DiVincenzo, P. Hayden, B.M. Terhal // [Електронний препринт] http://arxiv.org/abs/quant-ph/0207147.

15. Shaw B.A. Quantum steganography / B.A. Shaw, T.A. Brun // [Електронний препринт] http://arxiv.org/abs/1006.1934v1.

16. Гомонай О.В. Лекції з квантової інформатики: Навчальний посібник / Гомонай О.В. – Вінниця : О.Власюк. — 2006. — 146 с.

17. Bennett C.H. Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels / Bennett C.H., Brassard G., Crepeau C. [et al.]. — Physical Review Letters. — 1993. — V. 70, number 13. — P. 1895-1899.

Надійшла: 06.06.2011 р.

Рецензент: д.т.н., проф. Шелест М.Є.