

СТЕГАНОГРАФІЯ ТА СТЕГОАНАЛІЗ / STEGANOGRAPHY & STEGANALYSIS

DOI: [10.18372/2225-5036.25.13958](https://doi.org/10.18372/2225-5036.25.13958)

ЗАБЕЗПЕЧЕННЯ НАДІЙНОСТІ ФУНКЦІОНУВАННЯ КОМП'ЮТЕРНИХ ЛІНГВІСТИЧНИХ СТЕГОСИСТЕМ В УМОВАХ ПРОТИДІЇ ІНФОРМАЦІЙНІЙ ПРОПАГАНДИ

Ярослав Тарасенко

Черкаський державний технологічний університет



ТАРАСЕНКО Ярослав Володимирович, к.т.н.

Рік та місце народження: 1993 рік, м. Черкаси, Україна.

Освіта: Черкаський державний технологічний університет, 2015 рік,
Черкаський державний технологічний університет, 2016 рік.

Посада: асистент кафедри інформаційних технологій проектування.

Наукові інтереси: комп'ютерна лінгвістична стеганографія, математична та прикладна лінгвістика, інформаційна безпека держави.

Публікації: більше 20 наукових публікацій (у тому числі статті, тези доповідей на конференціях, розділ у колективній монографії).

E-mail: yaroslav.tarasenko93@gmail.com.

Orcid ID: 0000-0002-5902-8628.

Анотація. В статті проводиться огляд існуючих методів підвищення надійності функціонування комп'ютерних лінгвістичних стегосистем. Оскільки, в ході дослідження виявлено, що перспективним напрямком, особливо в умовах протидії інформаційній пропаганді є квантова стеганографія, тому розглядаються саме ці підходи для вирішення поставленої задачі. Аналіз існуючих розробок доводить відсутність повноцінної практичної реалізації подібного підходу в стеганографії. В роботі висувається припущення, що причина у відсутності єдності корпускулярно-хвильових характеристик в процесі приховування стегоповідомлення. В статті доводиться, що на даний момент подібний підхід можливо реалізувати лише в комп'ютерній лінгвістичній стеганографії шляхом її поєднання з квантовою стеганографією. Аналіз виявив, що текстова стеганографія на основі квантових законів знаходиться на початковому етапі розвитку, а дослідження проводяться лише в області методів довільного інтервалу. Для вирішення поставленої в роботі задачі вводиться поняття квантово-семантичної лінгвістичної стеганографії. Існуючі недоліки методів квантової стеганографії, а саме неможливість практичного відтворення множинності світів чи вразливість тексту до систем автоматичної семантичної модифікації пропонується виправити шляхом використання методики лінгво-комбінаторного моделювання важкоформалізованих систем та засад кібернетичної герменевтики для взаємодії з квантовими станами, а інтенціональної логіки для вирішення проблеми квантової заплутаності з метою збереження квантового дуалізму для формалізації та впровадження ідеї квантово-семантичної стеганографії на практиці. В свою чергу реалізація афінних перетворень стосовно функції, що описує суб'єктивну семантичну лінію тексту забезпечить процес протидії інформаційній пропаганді. Використання ж методів ЦВЗ для розшифровки зміни семантичних станів при формуванні тексту за суб'єктивною семантичною лінією допomoже зменшити імовірність виявлення факту передачі стегоповідомлення.

Ключові слова: квантово-семантична лінгвістична стеганографія, квантова лінгвістика, квантова стеганографія, протидія пропаганді, комп'ютерна лінгвістична стегосистема, надійність комп'ютерної лінгвістичної стегосистеми, корпускулярно-хвильові характеристики тексту.

Вступ

На поточний період, все більше розширюється область застосування комп'ютерної стеганографії. Таким чином, крім класичної задачі організації секретного каналу зв'язку та прихованої передачі повідомлення, з'являються нові задачі, продиктовані сучасними умовами міграції інформації та постійної інформаційної війни як в сфері комерції так і у державній сфері. Оскільки, відомо, що один із напрямків стеганографії, який полягає у вбудовуванні цифрових водяних знаків (ЦВЗ)

використовується для запобігання викрадення чи модифікації даних [1], тому новою задачею використання ЦВЗ може стати протидія інформаційній пропаганді, що полягає у запобіганні модифікації інформації з метою здійснення інформаційного впливу на свідомість громадян.

Виходячи з [2], для проведення впливу на свідомість громадян використовується саме текстова інформація, що розміщується у загальнодоступних джерелах. Виходячи з [3], текстова інформація забез-

печує процес навчання, в процесі якого забезпечується процес формування навичок на основі тексту. Враховуючи прагнення громадян до навчання в мережі та до вивчення англійської мови, це робить англійський текст цільовим інформаційним носієм для здійснення впливу.

Крім того, стеганографічні методи можуть допомогти у процесі виявлення наявності пропаганди шляхом пошуку факту втручання в стегосистему. Отже, актуальною є і проблема забезпечення надійності функціонування комп'ютерних стегосистем в умовах протидії інформаційній пропаганді та, відповідно, підвищення ефективності таких комп'ютерних лінгвістичних стегосистем.

Факт втручання зловмисником в канал зв'язку можливо виявити застосовуючи підходи квантової криптографії, що описані в [4], при цьому адаптувавши їх до використання в стегосистемі. Крім того, методи квантової стеганографії можуть також бути використані для підвищення надійності стегосистеми.

Оскільки в ролі цільового стегоконтейнеру розглядається текст, при тому не власне комп'ютерний текстовий файл, а його семантична складова, тому слід ввести поняття квантово-семантичної лінгвістичної стеганографії. А, отже, квантово-семантична стеганографія по аналогії з квантовою стеганографією може виявляти факт втручання в канал зв'язку, що означає можливість попередження контрмір, які полягають у протидії здійсненню зворотного впливу на пропагандиста.

Аналіз досліджень та постановка завдання

На даний момент, в забезпеченні захисту інформації, в тому числі інформаційної безпеки держави, використовуються квантові технології [5]. На ряду з такими квантовими технологіями, як розподіл ключів, цифровий підпис, розподілення секрету стоїть і квантова стеганографія [5]. Базові підходи, на яких вона ґрунтується описані в [6-7]. Звідси можна зробити висновок, що ведуться роботи по підвищенню надійності комп'ютерних стегосистем на основі квантових явищ.

Основні сучасні методи квантової стеганографії описуються в [8]. Це ж джерело і трактує квантову стеганографію, як таку, що підвищує рівень секретності за рахунок приховування факту передачі даних за аналогією з класичною стеганографією. Однак в [8] зазначається відсутність практичної реалізації квантової стеганографії.

Зокрема, існують роботи [9-12], в яких робляться спроби формалізації процесу приховування стегоповідомлення на основі квантових явищ. Так, в [9] застосовується особливість квантової інформації. В роботі [10] приховування базується на квантовому надщільному кодуванні. Робота [11] звертає більшу увагу на квантовий зв'язок, а робота [12] присвячена дослідженню станів Бела з метою кодування стегоповідомлення.

Однак, описані процеси не стосуються лінгвістичної стеганографії. В згаданих роботах не враховується особливість текстової інформації, а це означає, що і кодування стегоповідомлення та приховування його в семантичній складовій текстового контейнеру за допомогою описаних методів на даний момент неможлива. А отже, постає задача розробки підходів, що

могли б реалізувати на практиці засади квантової стеганографії та застосувати їх до комп'ютерної лінгвістичної стеганографії, зокрема в контексті семантики текстових даних, особливо англійською мовою. Така задача спричинена відкритим питанням щодо більшої практичної ефективності квантових стегосистем в порівнянні з класичними [5]. Однак, висувається гіпотеза щодо підвищеної ефективності таких систем. Це зумовлено тим фактом, що на даний момент, хоч і не існує практично реалізованих квантових стегосистем, однак лінгвістичні особливості тексту, зокрема доведені квантові властивості мислення, що реалізують квантову механіку мозку [13] дозволяють зробити припущення, що на сьогоднішній день лінгвістична стеганографія єдина може дозволити на практиці реалізувати більшість властивостей квантової стеганографії і таким чином підвищити ефективність роботи комп'ютерних лінгвістичних стегосистем. Це означає, що пошук кардинально нових підходів до підвищення ефективності стегосистем, які могли б значно вплинути на розвиток стегосистем в умовах вкрай недостатньо дослідженої квантової стеганографії, особливо для подальшої практичної реалізації цих підходів, на сьогоднішній день є вкрай актуальною задачею, зумовленою постійною інформаційною війною в державі та потребою протидіяти ворожій інформаційній пропаганді. Протидія пропаганді досягається шляхом використання квантової лінгвістики в інформаційному протиборстві, що описується в роботі [14]. Крім того, в статті зазначається необхідність застосування методу опитування інформанта для визначення психолінгвістичних особливостей тексту та формування психолінгвістичного портрету пропагандиста, що вимагає привернення уваги до тексту. В той же час, приховування інформації, що несе в собі ознаки впливу на підсвідомість пропагандиста, шляхом застосування стеганографічних методів, адаптованих до цієї задачі завдяки використанню квантово-семантичного лінгвістичного дослідження дозволить уникнути спротиву та підвищити ефективність зворотного впливу на пропагандиста. Крім того, це може допомогти у формуванні психолінгвістичного портрету пропагандиста з використанням методу опитування інформанта, та підвищити ефективність цього процесу.

Отже, метою статті є огляд існуючих методів та підходів квантової стеганографії та пошук можливості їх застосування саме в контексті їх подальшої формалізації та практичної реалізації інформаційних систем квантово-семантичної стеганографії для забезпечення надійності функціонування комп'ютерних лінгвістичних стегосистем в умовах протидії інформаційній пропаганді.

Основна частина дослідження

Перш за все, для огляду переваг та недоліків існуючих методів та підходів квантової стеганографії, слід розглянути основні квантові принципи, які беруться за основу в квантових стегосистемах, після чого дослідити які саме принципи впливають на можливість реалізації таких підходів. Це дасть змогу чітко уявити, як саме можливо застосувати подібні властивості в контексті лінгвістики.

Отже, в системах [9-11] розглядається безпосередня можливість утворення квантового каналу стеганографічного зв'язку для передачі інформації на рівні квантових часток світла. Процес подібний за своєю структурою з квантовими криптографічними системами [4], які також базуються на використанні квантового каналу передачі даних. Однак, в цьому і полягає складність практичної реалізації подібних систем. Використання суто фізичних явищ, при тому які на даний момент недостатньо вивчені та практично відтворені з урахуванням усіх властивостей квантової заплутаності зумовлює складність, якщо не неможливість (принаймні на даний час) реалізації подібних систем. Квантова заплутаність надзвичайно складна система для практичної реалізації з огляду на те, що веде до поняття множинності світів. Однак, якщо розглядати це поняття з точки зору лінгвістики, то їх існування в контексті семантики не є новиною. В [15] описано дослідження тексту за допомогою формальної семантики, що має назву інтенціональна логіка. Звідси слідує, що наявність формальних підходів до опису та дослідження множинних світів семантики тексту відкриває шляхи дослідження та маніпуляції з квантовою заплутаністю, пов'язаною з існуванням цих світів.

В контексті протидії пропаганді можна сказати, що існує безліч світів сприйняття одного і того ж поняття, основане на психолінгвістичному портреті кожної конкретної людини (в даному випадку зловмисника). Таким чином, якщо назвати N людям один термін, одночасно утвориться N світів сприйняття цього поняття. При цьому, якщо попросити будь-яку з N осіб описати поняття, жодне з них не повториться, оскільки не існує двох однакових психолінгвістичних портретів. І це стосується навіть найменших семантичних понять як терміни, не кажучи про складні семантичні структури. При цьому приховування стегоповідомлення можливо на основі поняття квантової зв'язності. Таким чином, при конкретизації терміна для окремої людини, будь-який інший світ в той же час може виступати як біт стегоповідомлення.

Оскільки стеганографія має на меті приховування самого факту передачі даних, якість приховування інформації в семантиці тексту впливає на ефективність стегосистеми. Іншими словами зловмисник не повинен здогадатися про існування секретного повідомлення, а отже на основі його психолінгвістичних вподобань воно повинно бути якнайбільш нейтральним.

Не варто забувати про існування комп'ютерних систем протидії використанню методів лінгвістичної стеганографії, як метод семантичного стиснення текстової інформації [16]. Їх використання впливає на надійність функціонування стегосистем. Це стосується виключно лінгвістичного аспекту формування стегосистеми. Однак, існують атаки, що можуть бути застосовані до лінгвістичної стегосистеми, походючи з атаки на квантові системи передачі даних [5].

Квантові властивості мови можуть допомогти у виявленні факту втручання в канал зв'язку чи безпосередньо у контейнер зі стегоповідомленням [5]. І хоча квантові властивості реалізуються на різних рівнях, в статті йде мова про семантичну квантовість, в

[5] йде мова про виключно фізичні явища, однак вразливість до описаної атаки за допомогою «троянських фотонів» та атаки з використанням «фальшивих станів» може бути використана і в квантово-самантичній лінгвістичній стегосистемі. Для її запобігання пропонується використання корпускулярно-хвильового дуалізму в контексті семантики тексту. Таким чином, при зміні станів семантичної частки чи додаванні додаткових часток вони випадатимуть за межі функції, що описує суб'єктивну семантичну лінію тексту, утворену за психолінгвістичним портретом зловмисника.

Можна зробити висновок, що вищезазначені методи квантової стеганографії використовують корпускулярні фізичні властивості, оскільки базуються на властивостях квантових станів [8]. Однак існують методи, що ґрунтуються на квантовій телепортації, як в [17], хоча і використовується при цьому класична модель утворення каналу передачі стегоповідомлення.

Стосовно лінгвістичних властивостей тексту, можна сказати, що засади квантової телепортації виконуються в повній мірі, оскільки приховування стегоповідомлення відбувається не на основі зміни початкової інформації, а на зміні її сприйняття, після чого стан семантичної частинки руйнується при прочитанні тексту нецільовою особою. Світ сприйняття семантичної частинки переноситься і інтерпретується вірним чином лише при прочитанні тексту цільовою особою чи засобами інтерпретації стегоповідомлення, налаштованими потрібним чином. Звідси слідує важливість вірного утворення квантового ключа, що допомагає розшифрувати стегоповідомлення.

Згідно з [5], квантовий розподіл ключів включає в себе такі протоколи, як протоколи з використанням одиничних поляризованих фотонів, з використанням фазового кодування, з використанням переплутаних станів та зі станами «приманки». Звідси слідує, що основні властивості квантового розподілу ключів відбувається на основі корпускулярних фізичних властивостей фотону. Якщо ж розглянути принцип приховування інформації в класичній стеганографії на прикладі цифрового водяного знаку (ЦВЗ) [1], приховування може відбуватися на основі зіставної функції.

Висувається допущення, що генерація ключа для застосування до квантової лінгвістичної стегосистеми можлива з використанням як квантових так і класичних властивостей. Стегоключем в інтерпретації лінгвістики може стати хвильова характеристика суб'єктивного сприйняття тексту будь-якою особою.

Таким чином, криптостійкість ключа, а, відповідно, і загальна робастність стегосистеми підвищується на основі двох принципів, по-перше, невідомо яка саме особа була взята за основу для побудови суб'єктивної семантичної лінії. Це може бути абсолютно будь-яка людина, що зараз живе чи жила колись за умови наявності інформації про її психолінгвістичний портрет, або тексту, написаного цією особою для виокремлення її психолінгвістичного портрету. І, по-друге, який саме текст був еталоном для суб'єктивного сприйняття семантики тексту обраною особою. За умови приховування факту передачі такого повідомлення, зловмисник не матиме змогу ні виявити факт його передачі, ні вплинути на стегоконтейнер

програмно-апаратними засобами. При цьому за аналогією із квантовими криптосистемами [4], можливо виявити факт втручання в стегоконтейнер, що хоч і не вплине на передачу стегоповідомлення, однак дасть можливість зрозуміти, що зловмисник міг запідозрити наявність стегоповідомлення у тексті та застосував відповідні засоби його модифікації. Однак, властивості згаданої вище квантово-семантичної телепортації забезпечать максимальну робастність системи. Відмінність переваги використання підходу виявлення факту втручання в передачу криптоповідомлення і стегоповідомлення полягає у тому, що в першому варіанті на основі квантових властивостей виявляється факт втручання в канал зв'язку, а в другому випадку – власне у стегоконтейнер.

Одна з вдалих спроб створити квантовий стеганографічний протокол для приховування стегоповідомлення у тексті була описана у роботі [18]. Описаний протокол володіє важливими перевагами в умовах протидії інформаційній пропаганді, а саме можливість використання будь-якого звичайного тексту в якості контейнеру. Крім того, одним із важливих досягнень стала можливість залишати сам текст у незміненому стані при вбудовуванні стегоповідомлення, а також той факт, що вбудоване повідомлення не включається у відкриту інформацію, а представлене як фази квантових станів. Отже, це підвищує робастність системи та покращує надійність її функціонування. Однак є істотний недолік подібних систем, що полягає у приховуванні стегоповідомлення шляхом включення даних текстового контейнеру у дані стегоповідомлення. Таким чином, відкривається вразливість, що полягає у можливості відшарування усієї другорядної інформації шляхом семантичної компресії, що приведе до спотворення чи знищення стегоповідомлення. Крім того, може порушитися смислова лінія тексту, що тягне за собою можливість викликання підозри у конкретного зловмисника щодо наявності у тексті стегоповідомлення. В умовах протидії інформаційній пропаганді такий стан речей недопустимий, оскільки знижує надійність функціонування комп'ютерної лінгвістичної стегосистеми.

Однак, вищеописані переваги слід використати і в плані квантово-семантичної лінгвістичної стеганографії. По-перше, приховування стегоповідомлення без зміни контейнеру з огляду на використання квантової лінгвістики рекомендується проводити на основі зміни семантичних станів сприйняття семантичної частинки конкретної людиною. По-друге, побудова тексту за загальною семантичною лінією з урахуванням суб'єктивної семантичної лінії сприйняття цього тексту конкретною особою зумовить зниження імовірності розкриття факту наявності стегоповідомлення. По-третє, засоби модифікації контейнеру не матимуть можливості знищити стегоповідомлення, основане на сприйнятті квантової семантичної частинки конкретною особою. І нарешті, це відкриває можливість до приховування стегоповідомлення не лише в інформаційному шумі, який можна видалити, а в головних семантичних категоріях тексту, що підвищує робастність системи в цілому.

Що ж до протоколів квантової стеганографії як в зашумлених каналах [19], так і в незашумлених [20],

то тут постає розглянута раніше проблема використання суто фізичних квантових властивостей при організації каналу зв'язку. Подібні системи, на відміну від попередньої важко адаптувати під потреби текстової стеганографії, а отже і ускладнюється їх використання в рамках протидії інформаційній пропаганді. В квантовій лінгвістичній стеганографії передача даних повинна залишатися класичною, а приховування інформації слід проводити на рівні сприйняття, основується на квантовій природі процесу мислення.

Якщо говорити саме про текстову стеганографію, можна відзначити і інші спроби використання квантових явищ у процесі приховування стегоповідомлення саме у текстовій інформації. Так, в [21] використовують властивості квантової заплутаності та виділяють такі переваги описаного підходу, як об'єднання квантових кодів корекції помилок із заплутаністю, що тягне за собою підвищення робастності та стійкості стегосистеми, оскільки помилки в стегоконтейнері не впливають на відновлення стегоповідомлення. Крім того, існує можливість створювати стегоповідомлення та його контейнер окремо. Ці властивості частково підходять для задачі протидії інформаційній пропаганді, при тому що відбувається підвищення надійності функціонування текстової стегосистеми, оскільки зменшується імовірність видалення стегоповідомлення внаслідок модифікації контейнеру. Однак, можливість окремого створення стегоповідомлення та його контейнеру є основним недоліком запропонованої розробки в контексті розглядуваної проблематики для застосування в лінгвістичній стегосистемі, оскільки основна хвилева квантова характеристика контейнеру може бути порушена у зв'язку з відсутністю врахування особливостей основної та суб'єктивних семантичних ліній тексту, а це може впливати на виникнення підозри у зловмисника щодо наявності стегоповідомлення у тексті. І все ж, не дивлячись на те, що внутрішня форма контейнеру не змінюється при вбудовуванні стегоповідомлення, що певним чином знижує вірогідність виникнення підозри у зловмисника, однак при значній модифікації контейнеру все ж існує імовірність втратити велику кількість даних, необхідних для його відновлення. Це зумовлено відсутністю врахування підходів квантової лінгвістики при застосуванні квантової стеганографії до текстової інформації.

Робота [22] також присвячена вирішенню проблеми забезпечення надійності функціонування лінгвістичної стегосистеми. В роботі пропонується використання квантового підходу, що базується на використанні інвертованих лапок в бенгальській мові при застосуванні таблиць істинності для квантового підходу. Однак в рамках протидії інформаційній пропаганді такий підхід використовувати неможливо, оскільки його можна вважати однотипним із методами довільного інтервалу в класичній лінгвістичній стеганографії, а це означає відсутність врахування семантичних особливостей тексту.

Системи, що використовують квантові явища для маніпуляції з ASCII кодами [23] взагалі не підходять для забезпечення надійності лінгвістичних стегосистем в умовах протидії інформаційній пропаганді, оскільки враховують лише технічні характерис-

тики символів і не зважають на семантичні особливості контейнеру. Це може спричинити виявлення факту наявності стегоповідомлення у тексті.

Вирішення згаданих недоліків пропонується шляхом врахування не лише семантики тексту, але і особливостей її сприйняття конкретним зловмисником чи групою людей завдяки побудови тексту згідно з цими особливостями, а квантові явища застосовувати вже конкретно до процесу сприйняття. Це забезпечить одночасно як стійкість до модифікації контейнеру, так і знизить імовірність виявлення факту передачі стегоповідомлення. Це може забезпечити одночасно використання усіх переваг підходу [21], однак єдність стегоповідомлення, контейнеру та необхідна інтерпретація його семантичного навантаження дозволить ефективно домогтися вирішення задачі підвищення робастності системи в боротьбі з інформаційною пропагандою.

Іще однією спробою підвищення рівня безпеки вбудованого стегоповідомлення у текст стала робота [24]. Її відмінною характеристикою стало спрямування на опрацювання текстів, що передаються у будь-яких публічних ЗМІ. Це робить підхід цікавим в плані протидії інформаційній пропаганді. Він заснований на використанні секретного стеганографічного коду для вбудовування стегоповідомлення на основі зміни квантових станів двох специфічних та двох спеціальних символів регіональної індійської мови гуджараті. Підхід схожий за своєю природою та методикою із підходом, описаним у [22], де також використовуються таблиці істинності. Головний недолік підходу, як і [22] полягає у використанні особливостей мови не широкого вжитку. Якщо ж у вигляді цільової мови розглядати англійську, постає проблема знаходження аналогічної пунктуації, до якої можливо було б застосувати квантовий підхід зміни станів, а у випадку знаходження аналогу, неможливо гарантувати криптостійкість системи, оскільки зміна станів непристосованого для цієї мети пунктуаційного знаку може спричинити виявлення факту наявності стегоповідомлення у тексті.

Отже, опираючись на аналізі сучасного стану використання квантового підходу у лінгвістичній стеганографії, можна стверджувати що квантова лінгвістична стеганографія знаходиться на першому рівні за аналогією із класичною лінгвістичною стеганографією (від методів довільних інтервалів до більш ускладненого рівня синтаксичних методів стеганографії та найбільш складного рівня семантичної стеганографії), хоча і поточні здобутки доводять підвищення надійності функціонування лінгвістичної стегосистеми шляхом використання підходу зміни квантових станів. Отже, звідси випливає неймовірна актуальність застосування квантового підходу до найбільш складного рівня лінгвістичної стеганографії, що базується на використанні особливостей зміни семантики. Можна допустити, що квантово-семантична лінгвістична стеганографія зможе забезпечити максимальну робастність стегосистеми по аналогії із класичною стеганографією. Підтвердження цієї гіпотези потребує подальших досліджень та практичної реалізації. Однак, напевно можна сказати, що та-

кий підхід забезпечить надійну протидію інформаційній пропаганді, що проводиться у відкритих джерелах ЗМІ.

При цьому, всі підходи використовують лише квантові стани без урахування дуалізму в квантовій фізиці, що означає відсутність врахування хвильової характеристики кванту, що тягне за собою неповне розкриття потенціалу квантової стеганографії та неможливість її ефективного впровадження у зв'язку з лише частковим та відокремленим застосуванням дуалістичних законів фізики.

Згідно з [25], стеганографію взагалі поділяють на класичну, цифрову, в яку входить і комп'ютерна, лінгвістичну та квантову. Оскільки, сучасні реалії комп'ютерної обробки даних потребують об'єднання певних окремих класів стеганографії, як це відбулось із комп'ютерною та лінгвістичною стеганографією, тому, квантова та комп'ютерна лінгвістична стеганографія також потребує об'єднання для вирішення задачі підвищення надійності функціонування стегосистем, а задача протидії інформаційній пропаганді потребує використання нових підходів для реалізації квантових явищ в стеганографії. Таким чином, вирішення пропонується шляхом зміни квантових семантичних станів при впровадженні лише ЦВЗ, що вказує на ключ, тобто на функцію, за допомогою якої відбуватиметься розшифровка. Функція в свою чергу буде реалізацією хвильової квантової характеристики і може зміщатися з головної семантичної лінії тексту на будь-яку суб'єктивну. Отже, реалізація афінних перетворень у квантово-семантичній стеганографії дозволить повною мірою використати потенціал квантових явищ для вирішення актуальної задачі протидії інформаційній пропаганді.

У [26] зазначається, що для усіх стеганографічних методів справедлива залежність, при якій збільшення обсягу вбудованих даних знижує надійність системи. При відсутності будь-яких слідів модифікації контейнеру, який побудований на основі психофізіологічних особливостей зловмисника і націлений на суб'єктивне сприйняття ним текстової інформації дозволить поєднати переваги використання ЦВЗ для приховування стегоповідомлення будь-якого об'єму. Таким чином квантово-семантичний підхід до комп'ютерної лінгвістичної стеганографії дозволить змінити таку залежність, і цим самим забезпечить надійність функціонування комп'ютерних лінгвістичних стегосистем, а хвильова квантова характеристика, налаштована на сприйняття тексту зловмисником забезпечить протидію інформаційній пропаганді.

Таким чином, вищесказане доводить, що потребують подальшого вдосконалення підходи квантової лінгвістики з метою вбудовування стегоповідомлення у текст на основі квантової природи мислення та сприйняття текстової інформації для зменшення кількості маніпуляцій з текстом. В свою чергу, відсутність в сучасних дослідженнях спрямованості на квантову семантику і використання лише зовнішніх механічних властивостей тексту для приховування стегоповідомлення, використовуючи зміну квантових станів доводить необхідність роботи в цьому напрямку. Допускається, що у вирішенні цієї задачі може допомогти методика лінгво-комбінаторного моделю-

вання важко формалізованих систем [27] та засади кібернетичної герменевтики [28, 29]. Ці підходи дозволяють взаємодіяти із квантовими станами, а інтенціональна логіка [15] допоможе вирішити проблеми квантової заплутаності та квантової зв'язності, що в свою чергу допоможе в розкритті потенціалу хвильової функції, і таким чином, збереже квантовий дуалізм для формалізації та впровадження ідеї квантово-семантичної стеганографії на практиці.

Незважаючи на те, що спроби об'єднати квантову механіку та лінгвістику проводилися вже в 2012 році, однак в роботі [30] лінгвістика в більшій мірі розглядається як аспект квантової механіки, а це, відповідно лише філософське уявлення. Натомість ідею використання квантових властивостей як аспекту проведення лінгвістичних досліджень можливо формалізувати та реалізувати на практиці за допомогою вищезгаданих методів і, таким чином забезпечити надійне функціонування комп'ютерних лінгвістичних стегосистем, зокрема в контексті протидії інформаційній пропаганді в текстових ЗМІ.

Висновок

В статті доводиться, що в світлі вимог сучасної кібербезпеки та в рамках протидії інформаційній пропаганді, для забезпечення надійності функціонування комп'ютерних стегосистем слід використовувати принципи квантової фізики. На основі цього, проведено огляд існуючих методів та підходів квантової стеганографії для здійснення пошуку можливості їх застосування саме в контексті практичної реалізації інформаційних систем квантової стеганографії та їх адаптації до лінгвістичної стеганографії. Оскільки в ролі цільового стегоконтейнера розглядається текст з його семантичною складовою, тому було введено поняття квантово-семантичної лінгвістичної стеганографії.

Було сформовано другу частину протиріччя, яке полягає в одночасному приверненні уваги до тексту та приховуванні інформації з ознаками зворотного впливу на пропагандиста для того, щоб знайшовши баланс між приверненням уваги та втаємниченням підвищити ефективність урівноваження впливу інформаційної пропаганди.

В результаті дослідження існуючих методів квантової стеганографії, виявлено, що багато джерел використовує для реалізації на практиці лише одну із дуалістичних складових, а саме зміну квантових станів у процесі приховування стегоповідомлення. Ігнорування дуалізму корпускулярно-хвильових властивостей унеможливило ефективну реалізацію подібних систем.

Висувається припущення, що застосування законів квантової фізики в контексті використання в лінгвістичній стеганографії може сприяти повноцінній подальшій практичній реалізації квантової стеганографії. Іншими словами, пропонується об'єднати квантову та комп'ютерну лінгвістичну стеганографію шляхом застосування афінних перетворень у головній (об'єктивній) та суб'єктивній семантичній лінії тексту, що є відображенням квантової природи мислення та сприйняття текстової інформації для змінення кількості маніпуляцій з текстом. Ключ, що вказує на функцію розшифровки стегоповідомлення

пропонується приховувати за допомогою методів ЦВЗ, що дозволяє знизити до мінімуму маніпуляції з текстом при одночасній можливості приховування повідомлення будь-якої довжини у текст, створений за суб'єктивною семантичною лінією, притаманною зловмиснику, що дозволяє змінити класичне уявлення про залежність зниження надійності стегосистеми від збільшення вбудованого стегоповідомлення, що вкрай важливо при використанні в протидії пропаганді через невеликі за об'ємом тексти, використані у ЗМІ. Крім того, розглянуті сучасні дослідження, що застосовують підходи квантової фізики для приховування стегоповідомлення у текст не розглядають семантику, як можливий компонент зміни квантових станів, а спрямовані лише на зовнішні механічні властивості тексту. Допускається, що підходи лінгво-комбінаторного моделювання важко формалізованих систем та кібернетичної герменевтики дозволяють взаємодіяти із квантовими станами на рівні семантики, а інтенціональна логіка допоможе вирішити проблеми квантової заплутаності та квантової зв'язності, що в свою чергу допоможе в розкритті потенціалу хвильової функції, і таким чином, збереже квантовий дуалізм для формалізації та впровадження ідеї квантово-семантичної стеганографії на практиці з метою протидії інформаційній пропаганді.

Відзначається необхідність проведення подальших досліджень для автоматизації процесу приховування стегоповідомлення у семантичній складовій тексту шляхом використання корпускулярно-хвильових квантових особливостей сприйняття текстової інформації зловмисником, що дозволить знизити імовірність виявлення факту наявності стегоповідомлення і забезпечить надійність функціонування комп'ютерних лінгвістичних стегосистем завдяки впровадженню квантово-семантичної лінгвістичної стеганографії для боротьби з інформаційною пропагандою.

Подальших досліджень потребує процес визначення координат семантичних часток при реалізації корпускулярно-хвильових властивостей для здійснення афінних перетворень семантики тексту відповідно до суб'єктивної семантичної лінії його сприйняття потенційним зловмисником.

В перспективі, подібний підхід може вплинути на розвиток квантового розподілу ключів в лінгвістичній стеганографії та квантового цифрового підпису на основі реалізації та впровадження квантової заплутаності станів сприйняття семантичних значень в текстовій інформації, що дозволить ідентифікувати особистість за написаним нею текстом, а це в свою чергу вплине на підвищення інформаційної безпеки як держави так і окремих громадян.

Література

- [1]. В. Грибунин, И. Оков, И. Туринцев, *Цифровая стеганография*, М.: СОЛОН-ПРЕСС, 2009, 263 с.
- [2]. М. Кононенко, "Патогенні тексти на шпальтах місцевих газет", *Медіапростір*, Спецвип. № 8, С. 144-147, 2015.
- [3]. Л. Васюкович, "Текстовая компетенция в контексте современного лингвистического образования", *Преподаватель XXI век*, № 1, С. 185-193, 2015.

- [4]. І. Лімарь, Є. Васіліу, О. Рябуха, Т. Жмурко, "Класифікація атак на квантові системи передавання конфіденційних даних", *Безпека інформації*, Том 23, № 3, С. 181-189, 2017.
- [5]. О. Корченко, Є. Васіліу, С. Гнатюк, "Сучасні квантові технології захисту інформації", *Захист інформації*, Том 12, № 1(46), С. 77-89, 2010.
- [6]. А. Башаров, В. Горбачев, А. Трубило, "Один протокол квантовой стеганографии на основе перепутанных состояний W-класса", *Оптика и спектроскопия*, Т. 112, № 3, С. 361-364, 2012.
- [7]. В. А. Shaw, Т. А. Brun, *Quantum Steganography*, 2010. [Електронний ресурс]. Режим доступу: <https://arxiv.org/abs/1006.1934> (дата звернення: 27.05.2019).
- [8]. Г. Коханович, О. Шевченко, В. Кінзерявий, Ю. Хохлачова, "Сучасні методи квантової стеганографії", *Захист інформації*, Том 13, № 2(51), С. 82-86, 2011.
- [9]. М. Curty, D.J. Santos, "Quantum steganography", *2nd Bielefeld Workshop on Quantum Information and Complexity*, Bielefeld, Germany, October 12-14, pp. 12-14, 2000.
- [10]. S. Natori, "Why Quantum Steganography Can Be Stronger Than Classical Steganography", In: Imai H., Hayashi M. (eds) *Quantum Computation and Information. Topics in Applied Physics*, Vol. 102, Springer, Berlin, Heidelberg, pp. 235-240, 2006.
- [11]. К. Martin, "Steganographic communication with quantum information", *Lecture Notes in Computer Science*, V. 4567, pp. 32-49, 2007.
- [12]. В. Terhal, D. DiVincenzo, D. Leung, "Hiding bits in Bell states", *Physical review letters*, Vol. 86, Issue 25, pp. 5807-5810, 2001.
- [13]. В. Маслова, "Основные тенденции современной лингвистики", *Вестник РУДН. Серия: Русский и иностранные языки и методика их преподавания*, Т. 16, № 2, С. 172-190, 2018.
- [14]. Я. Тарасенко, "Використання принципів квантової лінгвістики в інформаційному протиборстві", *Безпека інформації*, Том 25, № 2, С. 96-103, 2019.
- [15]. Г. Осипов *Методы искусственного интеллекта*, М.: ФИЗМАТЛИТ, 2011, 296 с.
- [16]. Я. Тарасенко, О. Півень, І. Федотова-Півень, "Метод семантичного стиснення текстової інформації для протидії комп'ютерній лінгвістичній стеганографії", *Наука і техніка Повітряних Сил Збройних Сил України*, № 3 (32), С. 68-78, 2018.
- [17]. С.Н. Bennett, G. Brassard, C. Crepeau, "Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels", *Physical Review Letters*, Vol. 70, Issue 13, pp. 1895-1899, 1993.
- [18]. Т. Mihara, "Quantum Steganography Embedded any Secret Text without Changing the Content of Cover Data", *Journal of Quantum Information Science*, Vol. 2, № 1, pp. 10-14, 2012.
- [19]. С. Sutherland, Т. Brun, *Quantum Steganography over Noisy Channels: Achievability and Bounds*, 2018. [Електронний ресурс]. Режим доступу: <https://arxiv.org/abs/1808.03183> (дата звернення: 02.06.2019).
- [20]. С. Sutherland, Т. Brun, *Quantum Steganography over Noiseless Channels: Achievability and Bounds*, 2018. [Електронний ресурс]. Режим доступу: <https://arxiv.org/abs/1805.01599> (дата звернення: 02.06.2019).
- [21]. Т. Mihara, "Quantum steganography using prior entanglement", *Physics Letters A*, Vol. 379, Issue 12-13, pp. 952-955, 2015.
- [22]. I. Banerjee, S. Bhattacharyya, G. Sanyal, "Text Steganography through Quantum Approach", *Proceedings of 6th International Conference on Information Processing «Wireless Networks and Computational Intelligence»*, Bangalore, India, August 10-12, Vol. 292, pp. 632-643, 2012.
- [23]. R.-G. Zhou, J. Luo, A Novel, *Quantum Steganography Scheme Based on ASCII*, 2019. [Електронний ресурс]. Режим доступу: <https://www.intechopen.com/online-first/a-novel-quantum-steganography-scheme-based-on-ascii> (дата звернення: 10.06.2019).
- [24]. I. Banerjee, S. Bhattacharyya, G. Sanyal, "Text Steganography Using Quantum Approach in Regional Language with Revised SSCE", *International Journal of Computer Network and Information Security*, № 12, pp. 73-81, 2012.
- [25]. О. Стасюк, С. Гнатюк, Н. Довгич, М. Літош, "Сучасні стеганографічні методи захисту інформації", *Захист інформації*, Том 13, № 1(50), С. 56-63, 2011.
- [26]. А. Горпенюк, А. Стороженко, "Дослідження та порівняльний аналіз стеганографічних методів для впровадження даних у цифрові файли", *Вісник Національного університету «Львівська політехніка» Серія: Автоматика, вимірювання та керування*, Вип. 741, С. 176-179, 2012.
- [27]. М. Игнатъев, "Лингво-комбинаторное моделирование плохо формализованных систем", *Информационно-управляющие системы*, № 6, С. 34-37, 2003.
- [28]. М. Игнатъев, *Просто кибернетика*, СПб.: Страта, 2016, 248 с.
- [29]. R. Kozma, C. Alippi, Y. Choe, F. Morabito, *Artificial Intelligence in the Age of Neural Networks and Brain Computing*, London, San Diego: Academic Press, 2018, 352 p.
- [30]. S. Ishikawa, "Quantum Mechanics and the Philosophy of Language: Reconsideration of Traditional Philosophies", *Journal of Quantum Information Science*, Vol. 2, № 1, pp. 2-9, 2012.

УДК 004.056

Тарасенко Я. В. Обеспечение надежности функционирования компьютерных лингвистических стегосистем в условиях противодействия информационной пропаганде

Аннотация. В статье проводится обзор существующих методов повышения надежности функционирования компьютерных лингвистических стегосистем. Поскольку в ходе исследования выявлено, что перспективным направлением, особенно в условиях противодействия информационной пропаганде является квантовая стеганография, поэтому рассматриваются именно эти подходы для решения поставленной задачи. Анализ существующих разработок доказывает отсутствие полноценной практической реализации подобного под-

хода в стеганографии. В работе выдвигается предположение, что причина в отсутствии единства корпускулярно-волновых характеристик в процессе сокрытия стегосообщения. В статье доказывается, что на данный момент, подобный подход возможно реализовать только в компьютерной лингвистической стеганографии путем ее сочетания с квантовой стеганографией. Анализ выявил, что текстовая стеганография на основе квантовых законов находится на начальном этапе развития, а исследования проводятся только в области методов произвольного интервала. Для решения поставленной в работе задачи вводится понятие квантово-семантической лингвистической стеганографии. Существующие недостатки методов квантовой стеганографии, а именно невозможность практического воспроизведения множественности миров или уязвимость текста к системам автоматической семантической модификации предлагается исправить путем использования методики лингво-комбинаторного моделирования сложноформализованных систем и принципов кибернетической герменевтики для взаимодействия с квантовыми состояниями, а интенциональной логики для решения проблемы квантовой запутанности с целью сохранения квантового дуализма для формализации и внедрения идеи квантово-семантической стеганографии на практике. В свою очередь, реализация аффинных преобразований относительно функции, описывающей субъективную семантическую линию текста обеспечит процесс противодействия информационной пропаганде. Использование же методов ЦВЗ для расшифровки изменения семантических состояний при формировании текста согласно субъективной семантической линии поможет уменьшить вероятность обнаружения факта передачи стегосообщения.

Ключевые слова: квантово-семантическая лингвистическая стеганография, квантовая лингвистика, квантовая стеганография, противодействие пропаганде, компьютерная лингвистическая стегосистема, надежность компьютерной лингвистической стегосистемы, корпускулярно-волновые характеристики текста.

Tarasenko Ya. Ensuring the functional reliability of computer linguistic stegosystems in context of countering the information propaganda

Abstract. The article reviews the existing methods for improving the functional reliability of computer linguistic stegosystems. Since it was found during the study that quantum steganography is promising direction, especially in the context of countering the information propaganda, therefore these approaches are the ones that are considered for solving the problem. The analysis of existing developments proves the lack of a full-fledged practical implementation of such an approach in steganography. An assumption is put forward in the work that the reason is in absence of unity of the corpuscular-wave characteristics in the process of hiding the stegomessage. It is being proved in the article that at the moment such an approach can only be realized in computer linguistic steganography, by combining it with quantum steganography. The analysis found that textual steganography basing on quantum laws is at the initial stage of development, and studies are conducted only in the field of random interval methods. The concept of quantum-semantic linguistic steganography is introduced to solve the problem in the work. Existing disadvantages of quantum steganography methods, namely, the inability to reproduce the plurality of worlds or the text's vulnerability to systems of automatic semantic modification, are proposed to be corrected by using the method of linguistic-combinatorial modeling of difficult-formalized systems and the principles of cybernetic hermeneutics for interaction with quantum states, and intensional logic to solve the problem of quantum entanglement to save quantum dualism for the formalization and implementation of the idea of the quantum-semantic steganography in practice. In turn, the implementation of affine transformations in relation to the function describing the subjective semantic line of the text will provide a process of countering the information propaganda. The use of the digital watermarking methods for decryption the change of semantic states in formation of the text by subjective semantic line will help to reduce the probability of detecting the fact of the stegomessage transmission.

Keywords: quantum-semantic linguistic steganography, quantum linguistics, quantum steganography, counter propaganda, computer linguistic stegosystem, reliability of computer linguistic stegosystem, corpuscular-wave characteristics of the text.

Отримано 10 жовтня 2019 року, затверджено редколегією 13 листопада 2019 року
