УДК 004.056.5:004.7 **Стасюк О.І., Гнатюк С.О., Довгич Н.І., Літош М.С. (НАУ)**

СУЧАСНІ СТЕГАНОГРАФІЧНІ МЕТОДИ ЗАХИСТУ ІНФОРМАЦІЇ

У роботі представлена систематизація та класифікація сучасних напрямів стеганографії, наведені переваги та недоліки конкретних стеганографічних методів. Виконане дослідження спрямоване на полегшення пошуку існуючих стеганографічних методів та засобів в науковій літературі з метою розробки нових ефективних систем захисту інформації.

Вступ. Проблема захисту інформації (ЗІ) від несанкціонованого доступу існувала в усі часи протягом існування людства. Для її вирішення уже в Древньому світі виділилося два основних шляхи, що існують і до сьогодні – криптографія і стеганографія. Слово "стеганографія" має грецьке коріння і буквально перекладається як "тайнопис". На відміну від криптографії, яка приховує вміст секретного повідомлення, стеганографія приховує саме його існування. Тайнопис зазвичай використовується спільно з методами криптографії, таким чином, доповнюючи її.

Аналіз останніх досліджень та постановка проблеми. *Актуальність* дослідження методів стеганографії невпинно росте, адже з поширенням персональних комп'ютерів, і особливо Інтернету, можливість конфіденційно передавати інформацію привертає увагу значної кількісті людей. Переважна більшість теоретичних та практичних досліджень у галузі стеганографії присвячена саме розробці нових та вдосконаленню існуючих методів приховування даних. Кількість останніх з часом невпинно зростає, однак в сучасній науковій літературі [1–8] відсутня чітка класифікація таких методів, що ускладнює пошук і не дає змоги у повній мірі оцінити рівень існуючих досягнень для їх подальшого ефективного використання. ***Метою*** даної роботи є класифікація стеганографії та таксономія (систематизація) сучасних стеганографічних методів ЗІ, якісний аналіз переваг та недоліків останніх, перспектив та труднощів їх практичного впровадження.

Основна частина. Провівши аналіз сучасної наукової літератури, можна виділити чотири напрями стеганографії – це класична, цифрова, лінгвістична та квантова стеганографія. ***Класична (традиційна) стеганографія*** – спосіб приховування даних, що здійснюється за допомогою технічних засобів ЗІ. Перша згадка [2] про класичні стеганографічні методи у літературі приписується Геродоту, що описав випадок передачі повідомлення Демартом, який зіскоблював віск з дощечок, писав листа прямо на дереві, а потім заново покривав дощечки воском. Сучасна класична стеганографія (рис.1) включає в себе хімічні та фізичні методи.

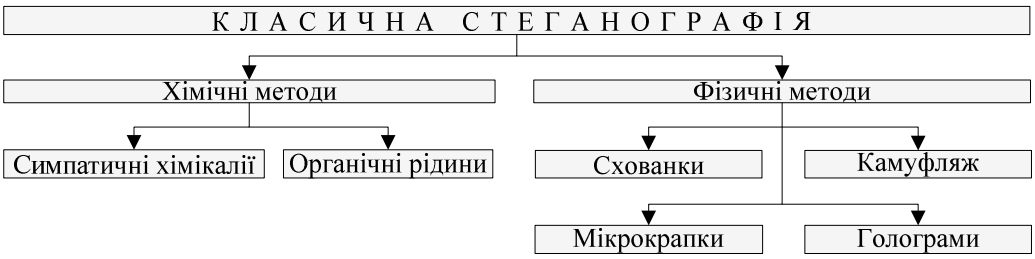
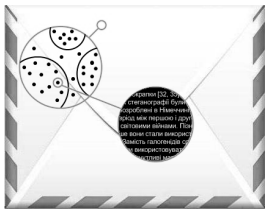


Рис.1. Методи класичної (традиційної) стеганографії

Загалом, ***хімічні методи*** стеганографії зводяться до застосування невидимого чорнила. До цих методів відносяться симпатичні хімікалії і органічні рідини. *Симпатичні хімікалії* [3, 4] є одним з найбільш поширених методів класичної стеганографії. Зазвичай, процес запису здійснюється наступним чином: перший шар – наноситься важливий запис невидимим чорнилом, другий шар – нічого не значущий запис видимим чорнилом. Текст записаний таким чином, що проявляється тільки при певних умовах (нагрівання, освітлення, хімічний проявник тощо)**.** *Органічні рідини* [4] мають схожі властивості з симпатичними хімікаліями: при нагріванні вони темніють (в них міститься велика кількість вуглецю).

До ***фізичних методів*** можна віднести різного виду схованки, методи камуфляжу та мікрокрапки. У даний час фізичні методи представляють інтерес в галузі дослідження різних носіїв інформації з метою запису на них даних, які б не виявлялися звичайними методами зчитування. Особливий інтерес присутній до стандартних носіїв інформації, засобів обчислювальної, аудіо- та відеотехніки. Крім цього, з'явився цілий ряд нових технологій [9], які, базуючись на традиційній стеганографії, використовують останні досягнення мікроелектроніки (голограми). *Схованки* для таємних послань використовувалися з часів Стародавньої Греції, замасковані в осях возів, сандалях і підкладках плащів [4, 5]. Схованки для послання можуть приймати найрізноманітніші форми. Для прикладу, персів, що облягали одне із грецьких міст, спритно обдурив один грек Гістіей, зумівши таємно передати послання Мілетському правителю Арістагору. Гістіей оголив наголо свого раба, наніс послання йому на голову і почекав поки волосся відросте. Природно, що обшук гінця на виїзді з міста не дав результатів, і послання знайшло адресата. У наш час Інтернет став сучасною версією подібної схованки. *Мікрокрапки* [6, 7] для стеганографії були розроблені в Німеччині у період між світовими війнами. Пізніше вони стали використовуватися багатьма країнами для передачі секретних повідомлень звичайною поштою. Замість галогенідів срібла стали використовуватися світлочутливі матеріали на основі аніліну, що значно ускладнило пошук мікрокрапок. Після зведення Берлінської стіни для виготовлення мікрокрапок використовувалися спеціальні фотокамери. З того часу мікрокрапки прикріплювалися до непримітного листа і пересилалися поштою. Мікрокрапки, зважаючи на малий розмір, як правило, залишалися непоміченими. Адресат отримував листа (рис.2 а) і читав послання у мікрокрапці за допомогою мікроскопа (рис.2 б).



а

б

Рис.2. Приклад застосування мікрокрапок у стеганографії: а) конверт з мікрокрапкою; б) спеціальний кишеньковий мікроскоп для читання мікрокрапок

Метод на голографічній основі [8] полягає в тому, що у зображення-контейнер вбудовуються не безпосередньо конфіденційні дані, а їх *голограма*. Цей метод має найвищий рівень стійкості до злому. Застосування голографічного підходу, дозволяє здійснювати вбудовування конфіденційних даних у звичайні фотографії на паперовій або пластиковій основі. Основний недолік даного методу пов'язаний з обмеженим обсягом вбудовуваних даних. Найбільш доцільно застосовувати голографічний підхід для приховування невеликих зображень, відновлення яких допускає незначну втрату якості: зразки підписів, відбитків пальців і т.п. На рис.3 а представлений контейнер із вбудованим факсимільним зразком підпису, а на рис.3 б показаний результат відновлення. Метод *камуфляжу* [4] полягає у тому, що конфіденційне повідомлення маскується таким чином, щоб "зливатися" із забарвленням предмету, який виконує роль контейнера.

а

б

Рис.3. Використання голограм в стеганографії: а) контейнер із вбудованим факсимільним зразком підпису; б) результат відновлення

Таким чином, проаналізувавши методи класичної стеганографії, можна підбити певні підсумки та виділити їх переваги й недоліки. До переваг класичної стеганографії можна віднести доступність засобів реалізації, а основними недоліками є складність практичної реалізації та можливість випадкового вияву таємного послання.

Цифрова стеганографія [2,9] (рис.4) – заснована на приховуванні або вбудовуванні додаткової інформації в цифрові об'єкти, викликаючи при цьому деякі їх спотворення. Як правило, дані об'єкти є мультимедійними і внесення спотворень, які знаходяться нижче порога чутливості середньостатистичної людини, не призводить до їх помітних змін.

Рис.4. Методи цифрової стеганографії

Приховування даних у просторовій області [10] може здійснюватися за допомогою наступних методів**:** *1) метод заміни найменш значущого біта (НЗБ)*, що полягає в заміні останніх значущих бітів в контейнері на біти приховуваного повідомлення; *2) метод псевдовипадкового інтервалу* – полягає у довільному розподілі бітів секретного повідомлення по контейнеру, в результаті відстань між вбудовуваними бітами визначається псевдовипадково; *3) метод псевдовипадкової перестановки* заснований на тому, що генератор псевдовипадкових чисел (ПВЧ) утворює послідовність індексів $j_1, j_2, ..., j_{lM}$ та зберігає k-й біт повідомлення в пікселі з індексом j_k. Таким чином, секретні біти будуть рівномірно розподілені по всьому бітовому просторі контейнера; *4) метод блокового приховування* полягає в тому, що зображення-оригінал розбивається на l_M неперетинних блоків $\Delta_i (1 \le i \le l_m)$ довільної конфігурації, для кожного з яких обчислюється біт парності $b(\Delta_i) : b(\Delta_i) = \sum_{J=\Delta i}^{\mathrm{mod}\,2} LSB(C_J)$. У кожному блоці виконується приховування одного секретного біта M_i. Якщо біт парності $b(\Delta_i \ne M_i)$ то відбувається інвертування одного з НЗБ блоку $\Delta_i d$ в результаті чого $b(\Delta_i = M_i)$*; 5) метод заміни палітри* полягає в наступному: палітра з N кольорів визначається як список пар індексів (i, Δ_i), що визначає відповідність між індексом і його вектором забарвлення Δ_i. Кожному пікселю зображення ставиться у відповідність певний індекс у таблиці. Оскільки порядок кольорів у палітрі не важливий для відновлення загального зображення, конфіденційна інформація може бути прихована шляхом перестановки кольорів у палітрі; *6) метод квантування зображення* [3] відбувається таким чином, що інформація приховується за рахунок коригування різницевого сигналу Δ_i. Стеганоключ представляє собою таблицю, яка кожному можливому значенню Δ_i ставить у відповідність визначений біт*; 7) метод Куттера-Джордана-Боссена* – це алгоритм вбудовування в канал синього кольору зображення, яке має {R,G,B} кодування, оскільки до синього кольору зорова система людини є найменш чуттєвою; *8) метод Дармстедтера-Делейгла-Квісквотера-Макка* базується на елементарному перцепційному (відчуттєвому)

сприйнятті і дозволяє пристосовувати вбудовування до вмісту блоків контейнера. Перед вбудовуванням конфіденційна інформація перетворюється у вектор двійкових даних, а кожен біт вбудовується в окремий блок.

Приховування даних в частотній області зображення [9] можливе при використанні таких методів: 1) *метод відносної заміни величин коефіцієнтів дискретно косинусного перетворення (ДКП) (метод Коха і Жао)* – один із найпоширеніших на сьогодні методів приховування секретної інформації в частотній області зображення. Даний метод базується на відносній заміні величин коефіцієнтів ДКП. На початковому етапі зображення розбивається на блоки розміром 8×8 пікселів і, в результаті певних перетворень, ДКП застосовується до кожного блоку, потім отримуємо матрицю 8×8 коефіцієнтів ДКП. Кожен блок при цьому призначений для приховування 1 біта даних; *2) метод Бенгама-Мемона-Ео-Юнга* є оптимізованою версією попереднього методу, причому, оптимізація проведена за двома напрямами: а) для вбудовування використовуються не всі блоки, а лише ті, які найбільш підходять для цього; б) в частотній області вибирається не 2 а 3 коефіцієнти ДКП; *3) метод Хсу і Ву* полягає у вбудовуванні цифрового водяного знака у масив коефіцієнтів ДКП блоків зображення-контейнера; *4) метод Фрідріха* є комбінацією двох алгоритмів – відповідно до одного з них, приховувані дані вбудовуються в низькочастотні, у іншому – в середньочастотні ДКП коефіцієнти.

До методів розширення спектру [2, 10] можна віднести: *метод розширення спектру за допомогою прямої псевдовипадкової послідовності (РСПП*) полягає в тому, що інформаційний сигнал, при розширенні спектру прямою послідовністю, модулюється функцією, яка приймає псевдовипадкові значення у встановлених межах і множиться на тимчасову константу – частоту (швидкість) проходження елементів сигналу. Даний псевдовипадковий сигнал містить складові на всіх частотах, які, при їх розширенні, модулюють енергію сигналу в широкому діапазоні; *метод розширення спектру за допомогою стрибкоподібного перебудовування частот* – передавач миттєво змінює одну частоту несучого сигналу на іншу, секретним ключем при цьому є псевдовипадковий закон зміни частот; *метод розширення спектру за допомогою компресії з використанням лінійної частотної модуляції (ЛЧМ)* заснований на тому, що при компресії з використанням ЛЧМ сигнал модулюється функцією, частота якої змінюється в часі.

Приховування даних в аудіосигналах [10] можливе при використанні наступних методів: *1) кодування найменш значущих біт (тимчасова область)* відбувається шляхом використання звукового сигналу із заміною НЗБ кожної точки здійснення вибірки, представленої двійковою послідовністю; *2) фазового кодування (частотна область)* полягає в заміні фази вихідного звукового сегмента на опорну фазу, характер зміни якої відображає собою дані, які необхідно приховати; *3) розширення спектру (тимчасова область)* використовує технологію РСПП, яка розширює сигнал даних (повідомлення), множачи його на сигнал несучої та псевдовипадкову шумову послідовність, що характеризується широким частотним спектром; 4) *приховування даних з використанням ехо-сигналу* полягає у вбудовуванні даних в аудіосигнал-контейнер шляхом введення в нього ехо-сигналу. Дані приховуються зміною трьох параметрів ехо-сигналу: початкової амплітуди, швидкості загасання і зсуву.

До методів приховування даних в тексті [10, 11] належать: *1) синтаксичні та семантичні методи.* До синтаксичних методів [12] відносять методи зміни пунктуації та методи зміни структури і стилю тексту. Семантичні методи подібні до синтаксичних, вони визначають два синоніми котрі відповідають значенням приховуваних біт. Для використання семантичних методів потрібна таблиця синонімів; *2*) *методи довільного інтервалу* ґрунтуються на трьох методах (заміни інтервалу між реченнями, заміни кількості пробілів у кінці текстових рядків, зміни кількості пропусків між словами вирівняного за шириною

тексту). Для приховування даних вони використовують вільне місце в тексті. У деяких джерелах [5, 11] описані вище методи відносять до лінгвістичної стеганографії.

Проаналізувавши методи цифрової стеганографії, можна виділити їх переваги та недоліки. До переваг можна віднести: 1) простоту реалізації методів; 2) високу стійкість до атак; 3) візуальну незмінність між модифікованим і первинним повідомленнями; 4) наявність вільного програмного забезпечення для реалізації методів. До недоліків цифрової стеганографії можна віднести: 1) високу чутливість до найменших спотворень контейнера; 2) ймовірність виникнення помилок при детектуванні; 3) складність вбудовування інформації в контейнер (у випадку великого об'єму таємного послання).

Лінгвістична стеганографія [5; 10] – напрям, який вивчає методи приховування конфіденційної інформації в непримітний текст, застосовуючи мовні властивості та лінгвістичні ресурси. Лінгвістичні методи стеганографії (рис.5) поділяються на дві основні категорії: умовне письмо і семаграми.

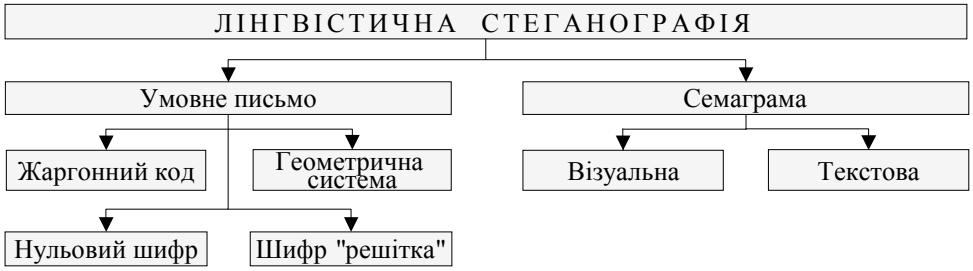


Рис.5. Методи лінгвістичної стеганографії

До ***умовного письма*** відносять: жаргонний код, геометричну систему, нульовий шифр і шифр "решітка". *Жаргонний код* передбачає використання не привертаючих увагу слів, які мають зовсім інше реальне значення, а текст складається так, щоб виглядати максимально непримітно і правдоподібно. Жаргонні коди включають в себе нанесення піктограм, таємну термінологію або типову розмову, яка передає особливий зміст внаслідок того, що ключ відомий тільки певним особам. При застосуванні *геометричної системи* мають значення слова, розташовані на сторінці в певних місцях або в точках перетину геометричної фігури заданого розміру. *Нульовий шифр* приховує повідомлення відповідно до певного, заздалегідь підготовленого, набору правил (наприклад, "прочитайте кожне п'яте слово" або "подивіться на третю букву в кожному слові"). *Шифр "решітка"* застосовує шаблон, який використовується для приховування повідомлення-контейнера. Слова, які з'являються в отворах шаблону, є прихованим повідомленням.

Іншу категорію лінгвістичних методів становлять ***семаграми*** – таємні повідомлення, в яких значеннями шифру є будь-які символи (крім літер і цифр). Наприклад, ці повідомлення можуть бути передані в малюнку, що містить крапки і тире для читання за кодом Морзе. *Візуальна семаграма* використовує, на перший погляд, нешкідливі звичайні фізичні об'єкти для передачі повідомлення. Наприклад, умовний знак рукою, розміщення предметів на столі в певній послідовності, характерні зміни в дизайні веб-сайту – все це семаграми. *Текстова семаграма* приховує повідомлення, змінюючи зовнішній вигляд тексту-контейнера (наприклад, ледь помітні зміни в розмірі або типі шрифту, додавання додаткових пробілів, різних завитків у буквах рукописного тексту).

Основною перевагою методів лінгвістичної стеганографії є можливість передавання повідомлення великої довжини, а головними недоліками – можливість випадкового вияву кодуючого алгоритму (здатність людини відчути суттєву різницю між модифікованим і первинним повідомленнями) та складність процесу кодування повідомлення.

Квантова стеганографія [14] аналогічно традиційним аналогам має за мету приховування самого факту передачі інформації. Квантова стеганографія ще не набула масовості, але у деяких працях [13, 15] пропонуються моделі систем ЗІ, що використовують

квантові властивості. Даний напрям є синтезом класичної і квантової інформатик [17] та заснований на злитті понять квантової фізики та класичної теорії інформації. Запропонована класифікація методів квантової стеганографії зображена на рис.6:

Рис.6. Методи квантової стеганографії

Хуліо Джі-Бенаклач у своїй роботі [18] запропонував ідею приховування таємних повідомлень у формі синдрому помилки при застосуванні квантових коригуючих кодів. Однак, протокол, що він запропонував, не дає можливості непримітно приховувати конфіденційну інформацію в квантовому каналі. Пізніше, Керті у праці [17] запропонував три стеганографічні системи, які використовують квантові інформаційні характеристики. Перша система приховує один класичний біт $E \in \{0;1\}$ в шумоподібний кубіт [19] (наприклад, молодший біт квантових значень), заміною кубіта з $|+\rangle = (1/\sqrt{2})(|0\rangle + |1\rangle)$ (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 щільним кодуванням. Безпека цієї системи залежить від ідентичності між квантовим шумом та справжнім білим шумом (матриці щільності). У третій системі кубіт передається через класичний стеганографічний канал за допомогою квантової телепортації [20]. Безпека цієї системи аналогічна тій, що лежить в основі класичної стеганографічної системи. Однак, жоден з цих протоколів не вирішує питання про передачу непримітних повідомлень через відкритий класичний канал або загальний квантовий канал в умовах секретності. Наторі у своїй роботі [21] трактує елементарні поняття квантової стеганографії, яка є модифікацією надщільного кодування. Мартіном в роботі [22] було введено поняття квантового стеганографічного зв'язку, а запропонований ним протокол квантового розподілу ключів (КРК) є варіантом протоколу Беннета і Брассара (BB84) [14, 16], в якому він приховує стеганографічний канал (контейнер). Виділяючи переваги та недоліки квантової стеганографії, можна сказати, що вона є значно стійкішою за традиційну, насамперед тим, що перехопити і декодувати конфіденційну інформацію, закодовану у квантові стани, теоретично неможливо (теоретико-інформаційна стійкість).

Висновки. У даній роботі проведено систематизацію та класифікацію сучасних стеганографічних напрямів. Встановлено, що на даному етапі є чотири напрями стеганографії: класична, цифрова, лінгвістична та квантова. Кожен напрям представлений конкретними методами приховування конфіденційної інформації. Систематизація стеганографічних методів ЗІ значно полегшує пошук і дозволяє у повній мірі оцінити рівень існуючих досягнень для їх подальшого ефективного використання. Виконана робота залишає широке поле для подальших фундаментальних досліджень, а також дозволяє підвищити ефективність створення нових стеганографічні системи ЗІ (стійких до різного роду атак).

Література

1. Хорошко В.А. Методы и средства защиты информации / В.А. Хорошко, А.А. Чекатков. – К. : Юниор, 2003. – 464 с.

2. Грибунин В.Г. Цифровая стеганография / В.Г. Грибунин, И.Н. Оков, И.В. Туринцев; – М : СОЛОН-Пресс, 2002. – 261 с.

3. Генне О.В. Основные положения стеганографии // Защита информации. Конфидент – 2000. №3 – 56 с.

4. Жельников В. Криптография от папируса до компьютера / В. Жельников. – М. : ABF, 1997. – С.12-15.

5. Conway M. Steganography, Signals Intelligence, and Terrorism // Knowledge, Technology and Policy. – 2003. – V.16, №2. – P. 45-47.

6. Шелков В.А. История "Микроточки" // Журнал "Специальная Техника". – №4/5 – 1999.

7. Buckland M., Goldberg E. Emanuel Goldberg and His Knowledge Machine. – Libraries Unlimited. – 2006. – 70 p.

8. Смирнов М. Скрытая передача и хранение конфиденциальной информации в Интернете и сотовой связи [Ел. ресурс]. – Режим доступу: http://www.infocity.kiev.ua/hack/content/hack264.phtml.

9. Барсуков В.С. Компьютерная стеганография вчера, сегодня, завтра. Технологии информационной безопасности 21 века / В.С. Барсуков, А.П. Романцов ; – М : "Специальная Техника", 2007. – 225 с.

10. Конахович Г.Ф. Компьютерная стеганография. Теория и практика / Г.Ф. Конахович, А.Ю Пузыренко – К.: МК-Пресс, 2006. – 249 с.

11. An Overview of Steganography for the Computer Forensics Examiner. 2004. [Електронний ресурс]. – Режим доступу: http://www.garykessler.net/library/fsc_stego.html.

12. The Third International Conference on Vailability, Reliability and Security A Statistical Algorithm for Linguistic Steganography Detection Based on Distribution of Words. [Електронний ресурс]. – Режим доступу: http://www.giac.unibel.by/sm_full.aspx?guid=7933.

13. Imai H. Quantum Computation and Information. From Theory to Experiment / H. Imai, M. Hayashi – Springer-Verlag: Berlin, Heidelberg. – 2006. – P. 235.

14. Корченко О.Г., Василіу Є.В., Гнатюк С.О. Сучасні квантові технології захисту інформації // Науково-технічний журнал "Захист інформації". – 2010, № 1. – С. 77-89.

15. Bilal A. Shaw. Quantum steganography and quantum error-correction // University of Southern California. – 2010. – P.137.

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

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

18. Ben-Aroya A., Ta-Shma A. On the complexity of approximating the diamond norm – 2009. – V.3. – P. 51-58.

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

20. Teleporting an unknown quantum state via dual classical and Einstein-Podolsky Rosen channels / Bennett C.H., Brassard G., Crepeau C., Jozsa R., Peres A., Wootters W.K. – 1993. – 128 p.

21. Bennett C., Wiesner S. Communication via one- and two-particle operators on Einstein-Podolsky-Rosen states. – 1992. – V. 69. – P. 2881-2884.

22. Martin K. Steganographic communication with quantum information / Lecture Notes in Computer Science, – 2008. – 130 p.

Надійшла: 26.02.11

Рецензент: д.т.н., проф. Конахович Г.Ф.