Міністерство освіти і науки України
Національний технічний університет
«Дніпровська політехніка»

Інститут електроенергетики
Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеня бакалавра

студента *Доленко Юлія Володимирівна*

академічної групи *125-17-2*

спеціальності *125 Кібербезпека*

спеціалізації[1]

за освітньо-професійною програмою *Кібербезпека*

на тему *Формування прихованого каналу передачі інформації з використанням комп'ютерної стеганографії*

Керівники	**Прізвище, ініціали**	**Оцінка за шкалою**		**Підпис**
		рейтинговою	**інституційною**	
кваліфікаційної роботи	к.т.н., доц. Герасіна О.В.			
розділів:				
спеціальний	ст. викл. Святошенко В.О.			
економічний	к.е.н., доц. Пілова Д.П.			
Рецензент				
Нормоконтролер	ст. викл. Мєшков В.І.			

Дніпро
2021

ЗАТВЕРДЖЕНО:
завідувач кафедри
безпеки інформації та телекомунікацій
_____ д.т.н., проф. Корнієнко В.І.

«_____»_____20___року

ЗАВДАННЯ
на кваліфікаційну роботу
ступеня бакалавра

студенту *Доленко Юлія Володимирівна* **академічної групи** *125-17-2*
(прізвище ім'я по-батькові) (шифр)

спеціальності *125 Кібербезпека*

за освітньо-професійною програмою *Кібербезпека*

на тему *Формування прихованого каналу передачі інформації з використанням комп'ютерної стеганографії*

затверджену наказом ректора НТУ «Дніпровська політехніка» від 07.06.2021 № 317-С

Розділ	Зміст	Термін виконання
Розділ 1	Аналіз принципів побудови стеганографічних методів захисту інформації і прихованої передачі даних, а також існуючих підходів до формування прихованого каналу передачі інформації.	25.02.2021 – 31.03.2021
Розділ 2	Розробка підходу до організації прихованої стеганографічної передачі інформації з маскуванням корисного сигналу та оцінка його ефективності.	01.04.2021 – 12.05.2021
Розділ 3	Розрахунки капітальних витрат, витрат на експлуатацію системи безпеки та термін окупності інвестицій застосування запропонованого підходу.	13.05.2021 – 09.06.2021

Завдання видано _____ Герасіна О.В.
(підпис керівника) (прізвище, ініціали)

Дата видачі: _____

Дата подання до екзаменаційної комісії: _____

Прийнято до виконання _____ Доленко Ю.В.
(підпис студента) (прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 73 с., 24 рис., 4 додатки, 35 джерел.

Об’єкт розробки – приховані канали передачі інформації.

Предмет розробки – підхід до формування прихованого каналу передачі інформації з використанням комп’ютерної стеганографії.

Мета кваліфікаційної роботи – збільшення скритності і точності відновлення приховуваного сигналу.

Наукова новизна результатів полягає у тому, що організація прихованої стеганографічної передачі інформації відбувається з маскуванням корисного сигналу, що дозволяє маскувати корисний сигнал в довільному шумовому сигналі при співвідношенні сигнал / шум менше 0,1 і відновлювати приймаючою стороною приховану інформацію у повному обсязі.

У першому розділі проаналізовано принципи побудови стеганографічних методів захисту інформації і прихованої передачі даних, а також існуючі підходи до формування прихованого каналу передачі інформації.

У спеціальній частині роботи запропоновано підхід до організації прихованої стеганографічної передачі інформації з маскуванням корисного сигналу та оцінено його ефективність. За наслідками досліджень зроблено висновки щодо рішення поставленої задачі.

У економічному розділі виконані розрахунки капітальних витрат, витрат на експлуатацію системи безпеки та термін окупності інвестицій застосування запропонованого підходу.

МАСКУЮЧИЙ СИГНАЛ, СКРИТНІСТЬ, ТОЧНІСТЬ ВІДНОВЛЕННЯ, КОМП’ЮТЕРНА СТЕГАНОГРАФІЯ, ПРИХОВАНА ПЕРЕДАЧА ДАНИХ, ПРОПУСКНА ЗДАТНІСТЬ, ІМІТАЦІЙНЕ МОДЕЛЮВАННЯ

РЕФЕРАТ

Пояснительная записка: 73 с., 24 рис., 4 приложения, 35 источников.

Объект разработки – скрытые каналы передачи информации.

Предмет разработки – подход к формированию скрытого канала передачи информации с использованием компьютерной стеганографии.

Цель квалификационной работы – увеличение скрытности и точности восстановления скрываемого сигнала.

Научная новизна заключается в том, что организация скрытой стеганографической передачи информации происходит с маскировкой полезного сигнала, что позволяет маскировать полезный сигнал в произвольном шумовом сигнале при соотношении сигнал/шум менее 0,1 и восстанавливать принимающей стороной скрытую информацию в полном объеме.

В первой главе проанализированы принципы построения стеганографических методов защиты информации и скрытой передачи данных, а также существующие подходы к формированию скрытого канала передачи информации.

В специальной части работы предложен подход к организации скрытой стеганографической передачи информации с маскировкой полезного сигнала и оценена его эффективность. По результатам исследований сделаны выводы относительно решения поставленной задачи.

В экономическом разделе выполнены расчеты капитальных затрат, затрат на эксплуатацию системы безопасности и срок окупаемости инвестиций применения предложенного подхода.

МАСКИРУЮЩИЙ СИГНАЛ, СКРЫТНОСТЬ, ТОЧНОСТЬ ВОССТАНОВЛЕНИЯ, КОМПЬЮТЕРНАЯ СТЕГАНОГРАФИЯ, СКРЫТАЯ ПЕРЕДАЧА ДАННЫХ, ПРОПУСКНАЯ СПОСОБНОСТЬ, ИМИТАЦИОННОЕ МОДЕЛИРОВАНИЕ

ABSTRACT

Explanatory note: p. 73, fig. 24, 4 additions, 35 sources.

The object of development is hidden channels of information transmission.

The subject of development is an approach to the formation of a hidden channel of information transmission using computer steganography.

The purpose of the qualification work is to increase the secrecy and accuracy of the recovery of the hidden signal.

The scientific novelty of the results is that the organization of latent steganographic transmission of information occurs with the masking of the useful signal, which allows you to mask the useful signal in an arbitrary noise signal at a signal-to-noise ratio of less than 0.1 and restore the hidden information in full.

The first section analyzes the principles of construction of steganographic methods of information protection and hidden data transmission, as well as existing approaches to the formation of a hidden information transmission channel.

In a special part of the work the approach to the organization of the hidden steganographic transfer of information with masking of a useful signal is offered and its efficiency is estimated. Based on the results of research, conclusions were made regarding the solution of the problem.

In the economic section, calculations of capital costs, costs of operating the security system and the payback period of the application of the proposed approach.

MASKING SIGNAL, SECRETIVENESS, RECOVERY ACCURACY, COMPUTER STEGANOGRAPHY, HIDDEN DATA TRANSMISSION, FLOW CAPACITY, SIMULATION MODELING

СПИСОК УМОВНИХ СКОРОЧЕНЬ

ЗДПФ – Зворотне дискретне перетворення Фур'є;

ДВП – Дискретне вейвлет перетворення;

ДКП – Дискретне косинусне перетворення;

КВЗ – Канал відкритого зв'язку;

КПЗ – Канал прихованого зв'язку;

КППД – Канал передачі приховуваних даних;

ПЗ – Пропускна здатність;

ППД – Прихована передача даних;

ППЗ – Прихована пропускна здатність;

СВЗ – Стеганографічний водяний знак;

ФСЧ – Фільтр середніх частот;

ФЩР – Функція щільності розподілу;

ЦВ – Цифровий відбиток;

ЦВЗ – Цифровий водяний знак;

ШПФ – Швидке перетворення Фур’є;

ЗМІСТ

ВСТУП

Наразі питання, пов'язані зі стеганографічними методами приховування інформації і їх виявленням, широко обговорюються в сфері інформаційної та кібербезпеки в силу того, що вони створюють дуже істотну і цілком реальну загрозу безпеці не тільки в державній, а й в комерційній сфері [1-4]. В останньому випадку мова йде, перш за все, про організацію витоків конфіденційної інформації і протидії їм. Інтенсивний розвиток інформаційно-обчислювальних мереж і технологій, включаючи сервіси, що базуються на мережевих протоколах реального часу, наприклад, в [5, 6], сприяє розвитку методів мережевої стеганографії, що дозволяють на базі телекомунікаційного каналу зв'язку організувати прихований інформаційний канал.

У загальному випадку мережева стеганографія реалізує ряд груп методів приховування інформації за допомогою модифікації даних в мережевих пакетах протоколів еталонної моделі OSI (Open Systems Interconnection basic reference model), модифікації структури передачі пакетів або гібридним підходом [7]. Методи мережевий стеганографії, засновані на модифікації даних в мережевих пакетах, здійснюють зміну полів службових даних [8, 9] або маніпулюють розміром пакетів [10], наприклад, за допомогою їх фрагментування. При цьому змістовна частина пакетів залишається без зміни, і основний комунікаційний канал не порушується. Методи мережевий стеганографії, засновані на модифікації структури передачі пакетів, не змінюють дані в пакетах, проте вносять зміни в структуру передачі пакетів таким чином, щоб «зашумлення» основного каналу передачі інформації було мінімальним. Для прихованої передачі можуть використовуватися часові затримки між пакетами [11], у тому числі і такі, які імітують звичайний мережевий трафік [12]. Гібридні методи використовують обидва підходи до організації прихованого каналу. Зауважимо, що перша група методів в сучасній стеганографії майже не застосовується через її низьку скритності [13].

Найбільш значущими параметрами методів мережевої стеганографії є пропускна здатність прихованого каналу передачі інформації, його вартісна оцінка (погіршення характеристик основного каналу), робастність (стійкість прихованого каналу в умовах природних шумів і протидії) і ймовірність виявлення [14]. Останній параметр є ключовим в силу самого призначення будь-якого стеганографічного методу. Як правило, пропускна здатність прихованого каналу знаходиться в прямій залежності від ймовірності його виявлення. Виходячи з цього, з точки зору розробки стеганографічного методу важливо знайти розумний баланс між усіма його значущими параметрами, перш за все, за показником скритності.

Наразі дуже популярними є різні сервіси та пристрої, що використовують протоколи потокової передачі даних. Це IP-камери, які використовуються для відеоспостереження, сервіси інтернет-телебачення, інтернет-радіо, тощо, які передають мультимедійні дані досить великого обсягу в режимі реального часу. Їх протоколи не гарантують доставку вмісту, є широкомовними та не мають жорстко заданих параметрів роботи [15]. Дані особливості дають можливості для організації прихованого каналу передачі інформації поверх основного.

Таким чином, вдосконалення підходів до організації прихованого каналу передачі інформації з використанням комп'ютерної стеганографії наразі є актуальною задачею.

Метою роботи є збільшення скритності і точності відновлення приховуваного сигналу.

Постановка задачі:

• проаналізувати принципи побудови стеганографічних методів захисту інформації, а також прихованої передачі даних;

• провести аналіз існуючих підходів до формування прихованого каналу передачі інформації;

• запропонувати підхід до організації прихованої стеганографічної передачі інформації з маскуванням корисного сигналу;

• оцінити ефективність запропонованого підходу.

1 СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ

1.1 Стеганографічні методи захисту інформації

1.1.1 Поняття стеганографії

Стеганографія (з грецької Στεγανός – прихований + γράφω – пишу; буквально «тайнопис») – міждисциплінарна наука і мистецтво про приховану передачу або зберігання інформації з урахуванням збереження в таємниці самого факту такої передачі (зберігання). На відміну від криптографії, яка приховує вміст таємного повідомлення, стеганографія приховує сам факт його існування. Включає сукупність методів, що ґрунтуються на різних принципах, які забезпечують приховання самого факту існування секретної інформації в тому або іншому середовищі, а також засобів реалізації цих методів [16-22].

Метою стеганографії є створення:

- прихованої передачі даних (ППД) – це «класична» мета стеганографії, відома з IV століття до Р.Х. Завдання – передати дані так, щоб супротивник не здогадався про сам факт появи повідомлення;

- цифрового відбитку (ЦВ) – різних стеганографічних міток-повідомлень для кожної копії контейнера;

- стеганографічного водяного знаку (СВЗ) – стеганографічної мітки, однакової для кожної копії контейнера.

Практичне застосування стеганографії:

І. Прихована передача даних:

1) непомітна передача інформації – на відміну від криптографічних методів (які таємниці, але не потайні), стеганографія застосовується як метод непомітної передачі інформації (це складає класичне практичне її застосування);

2) приховане зберігання інформації – стеганографія використовується для зберігання якої-небудь інформації, виявлення самого факту наявності якої

(нехай хоч навіть в зашифрованому виді) користувачеві небажано. Надмірність на багатьох носіях може бути неймовірна великою (наприклад, загальний об'єм даних, які можна записати на CD диск складають 1828 Мб даних – це величезна надмірність, яку можна використовувати для приховання даних);

3) зберігання інформації, яка не декларується – багато інформаційних ресурсів дозволяють зберігати дані тільки певного виду (наприклад портал YouTube дозволяє зберігати тільки відеоінформацію у форматах MOV, MPEG4, AVI, WMV, MPEG-PS, FLV, 3GPP, WebM). Проте можна використовувати стеганографію для зберігання даних в інших форматах. Наприклад, сайт hid.im дозволяє користувачам приховувати файли .torrent усередині зображень PNG;

4) прихована передача управляючого сигналу – стеганографія застосовується для доставки якого-небудь управляючого сигналу системі в таємниці від супротивника. Використання тільки криптографії, без стеганографії, може дати супротивникові інформацію про те, що щось змінилося і спровокувати його на небажані дії;

5) стеганографічні botnet-мережи – це застосування є часткою випадком прихованої передачі управляючого сигналу від органу управління бот-мережею на заражені комп'ютери з метою організації кібератаки;

6) Funkspiel («Радіогра») – стегоповідомлення містить дані (наприклад, яку-небудь хеш-функцію або наперед встановлену послідовність біт), повідомляючі про те, чи варто сприймати інформацію контейнера серйозно;

7) стеганографічне відвернення – задача – відвернути увагу супротивника. Для цього необхідно, щоб генерація стегоконтейнерів була істотно «дешевша» (з точки зору машинних і тимчасових ресурсів), ніж виявлення стеганографії супротивником. Стеганографічне відвернення чимось нагадує DoS і DDoS атаки. Відволікається увага супротивника від контейнерів, які дійсно містять щось цінне;

8) стеганографічне відстежування – тут мета стеганографії – піймати порушника, який «зливає» інформацію (аналог «мічених грошей», використовуваних правоохоронними органами, для того, щоб злочинець, що

отримав гроші за яку-небудь незаконну діяльність, не міг би потім заявити, що ці гроші були у нього до угоди).

II. Цифровий відбиток:

1) захист виняткового права – наприклад, в голографічних багатоцільових дисках (Holographic Versatile Disc, HVD), що містять до 200 Гб даних і використовуваних компаніями теле- і радіомовлення для зберігання відео- і аудіоінформації, наявність ЦВ усередині кодів цих дисків може використовуватися як засіб для захисту ліцензійного права; в Інтернет-продажи інформаційних ресурсів (книг, фільмів, музики і т.д.) кожна копія повинна містити спеціальну мітку для перевірки ліцензійна ця копія або не ліцензійна;

2) індивідуальний відбиток в системі електронного документообігу – використання індивідуального відбитку усередині *.docx та інших документів при роботі з ними користувачів дозволяє пізнати, хто працював з документом, а хто ні;

3) підтвердження достовірності переданої інформації – стегоповідомлення містить дані, такі, що підтверджують коректність передаваних даних в стегоконтейнері. Це може бути контрольна сума або хеш-функція (дайджест).

III. Стеганографічний водяний знак:

1) захист авторського права – одним знаком захищається кожна копія контенту. Наприклад, це може бути фотографія. У випадку якщо фотографію опублікують без дозволу фотографа, сказавши, що нібито не він автор цієї роботи, фотограф може спробувати довести своє авторство за допомогою стеганографії. В даному випадку в кожну фотографію необхідно вбудувати інформацію про серійний номер фотоапарата або інші дані, що дозволяють «прив'язати» фотографію до одного єдиного фотоапарата;

2) захист достовірності документів – стеганографія використовується не для підтвердження авторства, а для підтвердження достовірності документу (документ, що не містить СВЗ, вважається підробним);

3) водяний знак в системах запобігання витоку даних (Data Leak Prevention, DLP) – при створенні документу, що має конфіденційний характер, украплюється певна мітка, яка не змінюється незалежно від кількості копій і/або ревізій документу. Для витягання мітки потрібний стегоключ, який тримається в таємниці. DLP-система перед схваленням або відмовою видати документ зовні, перевіряє наявність або відсутність водяного знаку: якщо знак присутній, то система не дозволяє відправляти документ зовні системи.

4) невідчужуваність інформації – існує ряд документів, для яких важлива цілісність. Її можна здійснити резервуванням даних. Але що робити, якщо є необхідність мати документи у такому вигляді, щоб неможливо було одну інформацію відокремити від іншої інформації? Як приклад можна привести медичні знімки. Пропонується усередину знімків украплювати інформацію про ім'я, прізвище та інші дані пацієнта.

На рис. 1.1 представлені існуючі наразі напрями стеганографії.

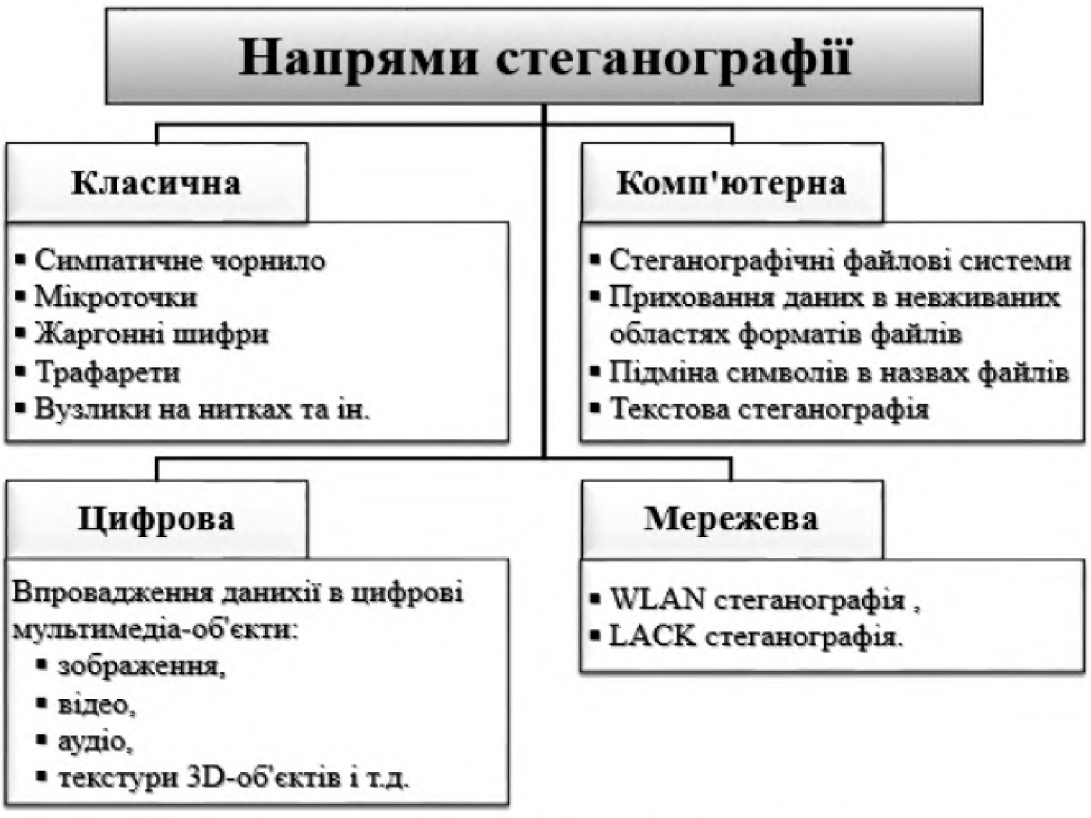

Рисунок 1.1 – Напрями стеганографії

1.1.2 Понятійний апарат стеганографії

У 1996 році на конференції Information Hiding: First Information Workshop була прийнята єдина термінологія у галузі стеганографії [16]:

1. Стеганографічна система (стегосистема) – об'єднання методів і засобів, використовуваних для створення прихованого каналу для передачі інформації. При побудові такої системи умовилися про те, що:

- порушник представляє роботу стегосистеми, однак невідомим для нього є ключ, за допомогою якого можна дізнатися про факт існування і зміст таємного повідомлення;

- при виявленні порушником наявності прихованого повідомлення він не повинен змогти витягнути повідомлення до тих пір, поки він не володітиме ключем;

- порушник не має технічних та інших переваг.

2. Стегоповідомлення – термін, використовуваний для загальної назви передаваної прихованої інформації, будь то лист з написами молоком, голова раба або цифровий файл.

3. Контейнер – будь-який фізичний або віртуальний об'єкт, використовуваний для приховання таємного повідомлення:

- порожній контейнер – контейнер, що не містить секретного послання;

- стегоконтейнер – заповнений контейнер, тобто контейнер, що містить секретне послання.

4. Стеганографічний канал (стегоканал) – канал передачі стегоконтейнера.

5. Стегоключ – секретний ключ, потрібний для приховання стегоконтейнера. Ключі в стегосистемах бувають двох типів:

- закриті (секретні) ключі (якщо стегосистема використовує закритий ключ, то він має бути створений або до початку обміну повідомленнями, або переданий по захищеному каналу);

- відкриті ключі (стегосистема, що використовує відкритий ключ, має бути влаштована так, щоб було неможливо отримати з нього закритий ключ. В цьому випадку відкритий ключ можна передавати незахищеним каналом).

На рис. 1.2 представлена узагальнена модель стегосистеми.

Рисунок 1.2 – Узагальнена модель стегосистеми

Будь-яка стегосистема повинна відповідати наступним вимогам:

1. Властивості контейнера мають бути модифіковані, щоб зміну неможливо було виявити при візуальному контролі. Ця вимога визначає якість приховання впроваджуваного повідомлення: для забезпечення безперешкодного проходження стегоповідомлення каналом зв'язку воно жодним чином не повинне притягнути увагу порушника.

2. Стегоповідомлення має бути стійке до спотворень, у тому числі і зловмисним. В процесі передачі зображення (звук або інший контейнер) може зазнавати різні трансформації: зменшуватися або збільшуватися, перетворюватися в інший формат і т.д. Крім того, воно може бути стисле, у тому числі і з використанням алгоритмів стискування з втратою даних.

3. Для збереження цілісності вбудованого повідомлення потрібне використання коду з виправленням помилки.

4. Для підвищення надійності вбудоване повідомлення має бути продубльовано.

Істотний вплив на надійність стегосистеми і можливість виявлення факту передачі прихованого повідомлення робить вибір контейнера.

За принципами побудови виділяють наступні типи стегосистем:

1. Безключові стегосистеми – не вимагають ніяких додаткових даних у вигляді стегоключа окрім алгоритму стеганографічного перетворення. Їх безпека заснована на секретності використовуваних стеганографічних перетворень, що суперечить основному принципу Керкхоффа для систем захисту інформації.

2. Стегосистеми з секретним ключем – безпека системи ґрунтується на секретному стегоключі, без знання якого не можна витягнути з контейнера секретну інформацію. Відправник, вбудовувавши секретне повідомлення у вибраний контейнер, використовує секретний стегоключ k в стеганографічним перетворенні. Якщо використовуваний стегоключ k відомий одержувачеві, то він зможе витягнути приховане повідомлення з контейнера. Без знання такого ключа будь-який інший користувач цього зробити не зможе.

Цей тип стегосистем припускає наявність безпечного каналу для обміну стегоключами.

Іноді стегоключ k обчислюють за допомогою секретної хеш-функції HASH, використовуючи деякі характерні особливості контейнера.

3. Стегосистеми з відкритим ключем не потребують додаткового каналу ключового обміну. Для їх функціонування необхідно мати два стегоключа: один секретний, який користувач повинен зберігати в таємниці, а другий – відкритий, який зберігається в доступному для усіх місці. При цьому відкритий ключ використовується в процесі приховання інформації, а секретний – для її витягання.

4. Змішані стегосистеми. У більшості застосувань прийнятними є безключові стегосистеми; хоча такі системи можуть бути відразу скомпрометовані у разі, якщо порушник дізнається про стеганографічне перетворення, що використовується. У зв'язку з цим в безключових

стегосистемах часто використовують особливості криптографічних систем з відкритим і (або) секретним ключем.

1.2 Системи прихованої передачі даних

Системи прихованої передачі даних застосовують для організації таємної комунікації. Вони відрізняються від усіх інших стеганографічних систем тим, що в цьому випадку оригінальний вміст контейнера не грає ніякої ролі ні для відправника, ні для одержувача, яких цікавить лише успішна передача повідомлення, вміщеного в ньому. Разом із тим потрібно обов'язково враховувати те, що факт відправлення контейнера від відправника до одержувача не повинен виглядати дивним, а також не повинно спостерігатись помітних відхилень контейнера від норми.

Основна мета таких систем – приховати наявність стеганоканалу, унеможливити розрізнення пустих і заповнених контейнерів без знання ключа. Для таких систем звичайно вважається, що контейнер не підлягає спотворенням в процесі його передачі по каналу зв'язку ($Y'=Y$), тому що таємна комунікація відбувається через відкритий канал цифрової мережі, наприклад, Інтернет, що забезпечує відсутність спотворень інформації при її передачі. В першу чергу для цих стеганосистем характерна наявність пасивного порушника, який намагається виявити факт експлуатації системи й прочитати таємну інформацію. Пропускна здатність стеганоканалу, під якою розуміють відношення розміру контейнера до розміру повідомлення, для систем прихованої передачі даних повинна бути суттєво вищою, ніж для інших видів систем.

Більшість методів розв'язування задач комп'ютерної стеганографії та відповідного їм програмного забезпечення використовують метод найменшого значущого біта, але аналіз їх якості показує низьку стеганостійкість і не може забезпечити потрібний рівень захисту інформації. Серед них більш стійкими є спектральні алгоритми, але більшість з них характеризується малою

пропускною здатністю створюваного стеганоканалу. Необхідність удосконалення існуючих стеганографічних методів та систем привела до створення нових методів та підходів, які були б вільні від цих недоліків.

В роботах [29], [30] запропоновані два підходи до побудови стійких стеганоконтейнерів, аналоги яких невідомі в світовій літературі.

1.2.1 Системи приховання інформації на рівні похибки заокруглення швидкого перетворення Фур'є

Перший підхід [29] базується на прихованні інформації в спектральній області зашумленого сигналу. Цей підхід дозволяє не тільки впроваджувати повідомлення в шумову компоненту сигналу, але й робити це таким чином, що при цьому величина зміни спектра стеганоконтейнера буде порівнянна з похибкою округлення стеганоалгорітма.

Якщо похибка обробки, викликана наявністю похибки округлення стеганоалгорітма, менше шуму сигналу, одержуємо подвійний стеганографічний захист секретного повідомлення: воно буде впроваджуватися в ті фрагменти контейнера, значення елементів яких не перевищує рівня шуму, точніше, на рівні похибки округлення стеганоалгорітма.

Ця ідея побудови стеганоалгорітма є оригінальною і на її основі побудований клас теоретично стійких стеганографічних алгоритмів (порушник не в змозі визначити факт використання стеганосистеми, оскільки не існує способу відрізнити порожній контейнер від заповненого) [11].

Одним з інструментів, широко використовуваних при розробці стеганосистем, є спектральний аналіз сигналів і зображень, дискретне перетворення Фур'є (ДПФ), дискретне косинусное перетворення (ДКП), дискретне вейвлет-перетворення (ДВП) і швидкі алгоритми їх реалізації.

Для одновимірного сигналу f(n), $n = \overline{0, N-1}$ ДПФ F(r) має вигляд:

$$F(r) = \sum_{n=0}^{N-1} f(n) W^{nr}, \quad W = e^{-i\frac{2\pi}{N}}, r = \overline{0, N-1}. \tag{1.1}$$

Для відновлення f(n) використовується зворотне дискретне перетворення Фур'є (ЗДПФ):

$$f(n) = \frac{1}{N}\sum_{r=0}^{N-1} F(r)W^{-nr}, \quad n = \overline{0, N-1}. \tag{1.2}$$

F(r) можна розділити на дійсну і уявну частини:

$$\mathrm{Re}(F(r)) = \sum_{n=0}^{N-1} f(n)\cos\left(2\pi\frac{rn}{N}\right), \tag{1.3}$$

$$\mathrm{Im}(F(r)) = \sum_{n=0}^{N-1} f(n)\sin\left(2\pi\frac{rn}{N}\right). \tag{1.4}$$

F(r) можна також представити у вигляді амплітудного і фазового спектрів:

$$|F(r)| = \sqrt{\mathrm{Re}^2(F(r)) + \mathrm{Im}^2(F(r))}, \tag{1.5}$$

$$\arg\left[F(r)\right] = arctg\frac{\mathrm{Im}(F(r))}{\mathrm{Re}(F(r))}, r = \overline{0, N-1}. \tag{1.6}$$

При роботі з зображеннями використовується двовимірне ДПФ.

Нехай f(k, m) – зображення розміром N×M. ДПФ даного зображення має вигляд

$$F(r,d) = \sum_{k=0}^{N-1}\sum_{m=0}^{M-1} f(k,m)\cdot e^{-2\pi i\left(\frac{rk}{N}+\frac{dm}{M}\right)}, \tag{1.7}$$

де $r = \overline{0, N-1}$, $d = \overline{0, M-1}$.

Відновлюється зображення за допомогою ЗДПФ

$$f(k,m) = \frac{1}{NM}\sum_{r=0}^{N-1}\sum_{d=0}^{M-1} F(r,d)\cdot e^{2\pi i\left(\frac{rk}{N}+\frac{dm}{M}\right)}, \tag{1.8}$$

де $k = \overline{0, N-1}$, $m = \overline{0, M-1}$.

Базовою операцією стеганоалгорітма є ДПФ, що використовується в одновимірному випадку тричі [29]: два рази відправником і один раз одержувачем. Загальна структура спектральних алгоритмів на базі оцінок похибки округлення представлена на рис. 1.3.

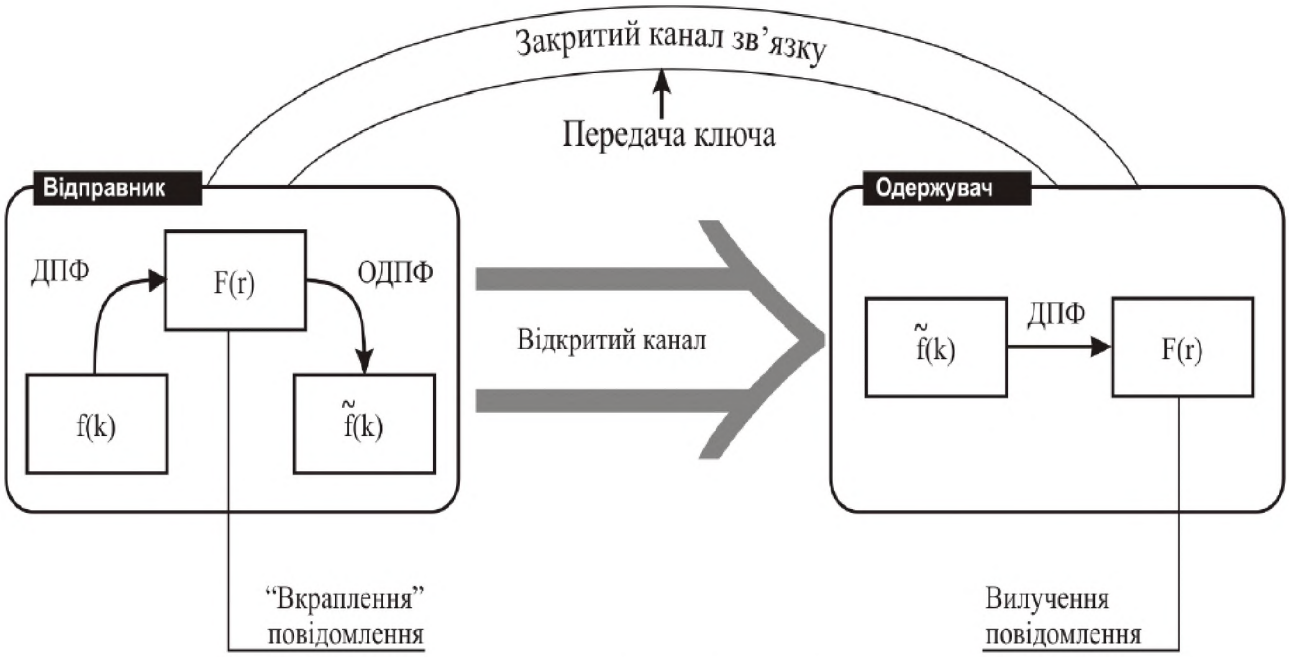

Рисунок 1.3 – Загальна структура підходів на основі оцінки похибки заокруглення ШПФ

Для зменшення оцінок складності стеганоалгорітма і оцінок похибки округлення для обчислення ДПФ автори пропонують використовувати ефективну обчислювальну процедуру швидкого перетворення Фур'є (ШПФ), яка замість $O(N^2)$ комплексних операцій додавання і множення для стандартного методу, вимагає $O(N \log_2 N)$ таких операцій.

Отже, у підході [29] використовується оригінальна модифікація алгоритму ШПФ, і похибка, яка при цьому вноситься, зіставлювана з похибкою заокруглення обчислення компонент спектра шуму

$$\left\|\varepsilon_з\right\|_E < \delta \cdot 1{,}06 \cdot \log_2 N \cdot \left\|\overset{)}{x}(t)\right\|_E \cdot 2^{-\tau}; \tag{1.9}$$

$$\sigma^2_{\varepsilon_з} = 0{,}21 \cdot \log_2 N \cdot \sigma^2_{\overset{)}{x}} \cdot 2^{-2\tau}, \tag{1.10}$$

де $\sigma^2_з$, $\sigma^2_{\overset{)}{x}}$ – відповідно дисперсії похибки заокруглення та ДПФ сигналу типу білого шуму. Оцінка (1.9) отримана для класичного правила заокруглення, а (1.10) – для рандомізованого.

При цьому відбувається не просто «занурення» інформації, яку треба приховати, в спектр шуму, а це «занурення» відбувається в ті розряди спектра шуму, які визначаються з оцінок похибки заокруглення алгоритму ШПФ. Враховується вся технологія обробки сигналу [11] і той факт, що в ній алгоритм ШПФ використовується тричі, цим гарантується незіпсованість інформації похибкою заокруглення. Це «найтонше» місце технології, і якість оцінки похибки заокруглення пов'язана зі стеганостійкістю підходу.

1.2.2 Системи приховання інформації у дискретній круговій згортці сигналів

Другий підхід до приховання інформації у дискретній круговій згортці сигналів [30] також базується на використанні ШПФ та на теоремі про дискретну згортку сигналів. Причому одним із сигналів, що згортається, є повідомлення, а другим – пустий контейнер. Стеганоконтейнером виступає результат згортки. Загальна структура підходів на базі теореми про згортку представлена на рис. 1.3.

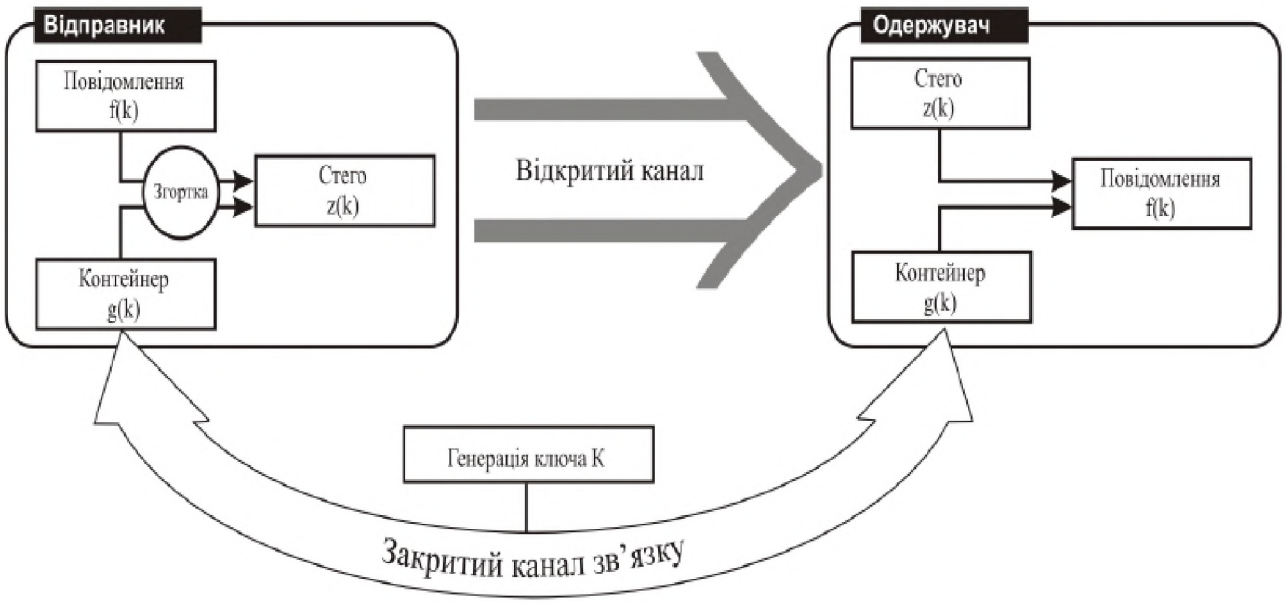

Рисунок 1.4 – Загальна структура підходів на базі теореми про згортку

Слід зазначити, що для підвищення стеганостійкості до приховання інформації у дискретній круговій згортці сигналів [30] треба зробити попередню обробку повідомлення.

1.3 Пропускна здатність каналів передачі приховуваних даних

1.3.1 Поняття пропускної здатності

Для розроблюваних або досліджуваних стеганографічних систем важливо визначити, наскільки великою може бути пропускна здатність (ПЗ) створюваних при цьому каналів передачі приховуваних даних (КППД) і як вона залежатиме від інших характеристик стеганосистем та умов їх використання. Під пропускною здатністю каналів передачі приховуваних даних або просто прихованою пропускною здатністю (ППЗ) розуміють максимальну кількість інформації, яка може бути вбудована до одного елементу (наприклад, пікселя чи відліку) контейнера. Обов’язковою умовою при цьому є безпомилковість передачі приховуваних даних одержувачеві, а також їх захищеність від таких атак порушника, як спроби виявлення факту наявності каналу прихованого зв’язку, одержання змісту приховуваних повідомлень, навмисне введення сфальсифікованих даних або ж руйнування вбудованої до контейнера інформації [1].

Канал прихованого зв'язку (КПЗ) утворюється всередині каналу відкритої зв'язку (КВЗ), для якого Шеннон (PЄ. Shannon) в своїх роботах по теорії інформації визначив пропускну здатність [21]. Пропускна здатність КВЗ визначається як кількість інформації, яку потенційно можна передати без похибок за одне використання каналу. При цьому не висувається жодної вимоги до захищеності від атак організованого порушника. Тому буде цілком логічно припустити, що прихована пропускна здатність КПЗ, в якому за одне використання каналу передається один елемент контейнера з вкладеною у

нього прихованою інформацією, ні в якому разі не може бути більше пропускної здатності КВЗ.

На сьогоднішній день намітилися різні, іноді діаметрально протилежні підходи до визначення кількості інформації, яка підлягає захисту від різноманітних атак порушника за допомогою стеганографічних методів. Ці розбіжності, обумовлені відмінностями в цілях захисту інформації, видами порушника, його можливостями та реалізованими ним атаками на стеганосистеми, видом використовуваних контейнерів і приховуваних повідомлень і багатьма іншими факторами.

Пропонується виконувати оцінку величини ПЗ КППД методами теорії інформації для різних стеганосистем. Теоретико-інформаційні методи дозволяють отримати строгі оцінки кількості інформації, що приховується, які абсолютно правомірно можуть бути використані як теоретично досяжні граничні швидкості передачі прихованої інформації для стеганосистем, не враховуючи принципи, закладені в основу їх побудови.

У [1] розглянуто два основні підходи до оцінки пропускної здатності КППД. Перший з них, орієнтований на стеганографічні системи, в яких повідомлення, що підлягають захисту, повинні бути безпомилково передані в умовах активної протидії порушника. Цей підхід описує сценарій приховування так званих безнадлишкових повідомлень в даних контейнера, і, що найголовніше, дозволяє враховувати той факт, що крім спотворень структури контейнера при встановленні в нього приховуваних даних, можливі його умисні спотворення з боку порушника. Крім того, існує ще і ймовірність спотворень випадкового характеру, викликаних ненавмисними завадами в каналі зв'язку.

Порушник, крім пасивних дій аналізу, може використовувати і активні дії (активний порушник). Метою активного порушника є руйнування прихованої інформації. Така постановка задачі інформаційного приховування є характерною, наприклад, для систем ЦВЗ.

Завдання інформаційного приховування часто формулюється як задача безпомилкової передачі приховуваної інформації при впливі випадкових і навмисних завад, а також визначається максимальна швидкість безпомилкової передачі при різних стратегіях дій відправника і атакуючого. Підходи такого типу визначають теоретично досяжну швидкість достовірної передачі приховуваних повідомлень, хоча в явному вигляді і не оцінюють захищеність останніх від виявлення факту їх існування. Однак для ряду стеганосистем не потрібно приховувати факт використання стеганографічного захисту: власник авторських або майнових прав на медіаконтейнер, який захищений ЦВЗ, як правило, відкрито повідомляє про застосування даної системи захисту. У подібних підходах досліджуються умови, при яких прихована інформація гарантовано передається в умовах довільних спроб порушника щодо її руйнування.

Знання параметрів стеганосистеми і можливих стратегій дій передавальної сторони, не повинно дозволити порушникові оптимізувати руйнівний вплив і оцінити його ефективність. Особливістю таких стеганосистем є, по-перше, те, що руйнівний вплив відбувається тільки в момент передачі прихованих даних і повинен здійснюватися в режимі реального часу. По-друге, існує завжди апріорна непоінформованість законного одержувача щодо приховано передаваної йому інформації. По-третє, порушник в переважній більшості випадків не здатний достовірно оцінити ефективність своїх дій.

Інша ситуація виникає при спробі активного порушника зруйнувати ЦВЗ з метою привласнити собі контейнер (права на нього). Порушник може як завгодно довго здійснювати руйнуючий вплив, вибираючи таку оптимальну стратегію, при якій, зруйнувавши ЦВЗ, він збереже необхідне йому якість контейнера. При цьому він заздалегідь знає про існування прихованої інформації, і, використовуючи загальновідомий детектор (рис. 3.3.), здатний оцінити ефективність своїх атак на ЦВЗ [1].

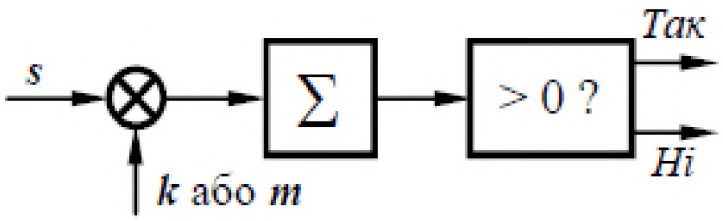

Рисунок 1.5 – Кореляційний детектор прихованих повідомлень

Другий підхід дає оцінку прихованої пропускної здатності безпосередньо в процесі вбудовування приховуваних повідомлень в надлишкові дані контейнера. Такий підхід враховує, що контейнери формуються реальними надлишковими джерелами з істотною пам'яттю, такими як джерела зображень або аудіосигналів. В цьому випадку оцінка ПЗ залежить від характеристик замаскованості прихованого каналу.

Цей підхід орієнтований на стеганосистеми, в яких реалізується прихована передача апріорно невідомої одержувачу інформації, причому пасивний порушник намагається в процесі спостереження за каналом відкритого зв'язку виявити факт наявності КПЗ і, в разі встановлення останнього, прагне розкрити зміст прихованого повідомлення у перехопленому контейнері.

Відома велика кількість робіт по синтезу стеганосистем, автори яких пропонують різноманітні способи вбудовування даних в надлишкові за своєю природою контейнери [1]. При цьому кількість інформації, вбудованість якої залишається непоміченою, оцінюється за допомогою додатково введених критеріїв рівня прихованості. Існуючі наразі оцінки ППЗ таких стеганоканалів, однак, не враховують можливі випадкові і навмисні спотворення контейнерів при їх передачі по каналу зв'язку.

1.3.2 Інформаційне приховування при активній протидії порушника

Розглянемо узагальнену структурну схему стеганографічної системи передачі прихованих повідомлень, представлену на рис. 1.6 [1].

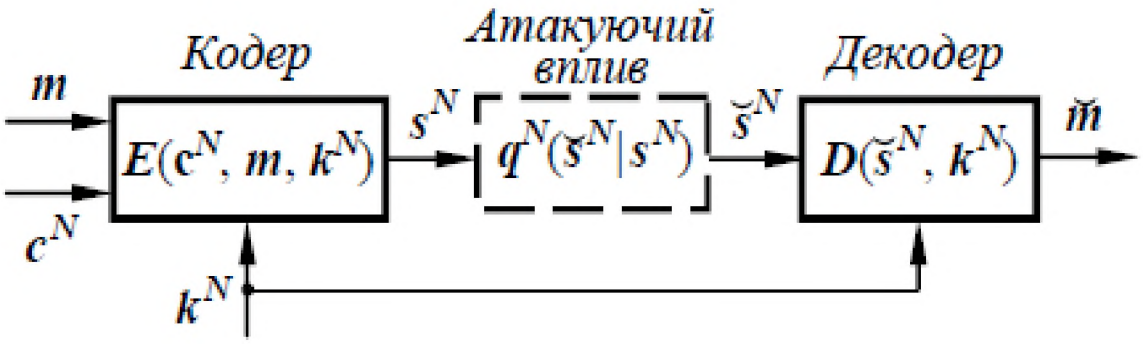

Рисунок 1.6 – Узагальнена структурна схема стеганосистеми при активній протидії порушника

У цій схемі приховувані повідомлення m рівномірно розподілені в безлічі повідомлень M і повинні бути безпомилково передані декодеру. Передавальна сторона подає порожній контейнер c^N (який являє собою послідовність з N незалежно і ідентично розподілених відліків відповідно до розподілу контейнера p(c)), секретний ключ k^n (кожен символ k_i (якого незалежно і рівномірно розподілений по функції p(k)), і повідомлення m на вхід кодера. Останній формує стеганограму s^N яка передається одержувачу по незахищеному каналу зв'язку.

Стеганограма s^N перехоплюється і обробляється порушником з метою руйнування або видалення повідомлення m. Перекручену порушником стеганограму відмітимо як $\tilde{s}^N$, а атакуючий вплив – умовною функцією розподілу

$$q^N\left(\tilde{s}^N \mid s^N\right) \tag{1.11}$$

Ця обробка включає, як окремий випадок формування спотвореної стеганограми у вигляді

$$\tilde{s}^N = q^N(s^N) \tag{1.12}$$

де q – детерміноване зображення

Основне припущення: порушник знає розподіл всіх змін в стеганосистемі і, власне, опис стеганосистеми, але не знає використовуваного секретного ключа (принцип Керхгофса для систем захисту інформації).

Нехай контейнер c, стеганограма s і модифікована порушником стеганограма $\tilde{s}$ належать одній множині $C\{c,s,\tilde{s}\in C\}$. Декодер одержувача обчислює оцінку $\tilde{m}$ первинного прихованого повідомлення m. Якщо $m\neq\tilde{m}$, то атакуючий зумів зруйнувати інформацію, яка захищалася стеганографічною системою.

Формально визначимо внесені спотворення в стратегіях передавальної сторони і порушника. Це завершує математичний опис стеганосистеми і дозволяє визначити швидкість безпомилкової передачі для схеми, представленої на рис. 1.6.

Функція спотворення, що вноситься відправником повідомлення, являє собою невід'ємну функцію

$$d_1 : C\times S\to\Re_+. \tag{1.13}$$

Функція спотворення внесеного атакуючої стороною, є ненегативною функцією

$$d_2 : S\times\tilde{S}\to\Re_+ \tag{1.14}$$

Функція спотворення d_1-обмежена:

$$d_{1,max}=\max_{(c,s)\in C\times S} d_1(c,s)\prec\infty \tag{1.15}$$

Крім того, дана міра спотворення симетрична $d_1(c,s)=d_1(s,c)$ для всіх $c,s\in C=S$. Виконання рівності $d_1(c,s)=0$ означає збіг: c=s. Якщо $d_1(c,s)=1$, то контейнер-результат не відповідає контейнеру-оригіналу.

Функції спотворення $d_i, i\in\{1;2\}$ поширюються на спотворення символьних послідовностей з довжиною блоків N:

$$d_i^N(x^N,y^N)=N^{-1}\cdot\sum_{j=1}^{N} d_i(x_j,y_j) \tag{1.16}$$

Назвемо спотворення контейнера *c*, викликане вбудовуванням в нього прихованого повідомлення m, спотворенням, викликаним кодуванням, а спотворення, викликане атакуючими діями порушника, – спотворенням, викликаним атакуючим впливом.

Стеганосистема з довжиною блоки N, яка веде до спотворення, викликаного кодуванням, рівень якого не перевищує A_1 є сукупністю множин приховуваних повідомлень M з кількістю елементів (потужністю) |M| контейнерів C, стеганограм $S \sim \widetilde{S} \sim C$ і ключів K, а також визначених на них функцій кодування E і декодування D. При цьому E – відображення контейнера c^N, повідомлення m і ключа k^N в стеганограму:

$$E : C \times M \times K \to C, s^N = E\left(c^N, m, k^N\right) \tag{1.17}$$

Це відображення обмежена величиною середнього спотворення A_1, викликаного кодуванням:

$$\sum_{c^N \in C} \sum_{m \in M} \sum_{k^N \in K} |M|^{-1} \cdot p\left(c^N, k^N\right) \cdot d_1^N\left[c^N, E(c^N, m, k^N)\right] \le A_1 \tag{1.18}$$

Відображення $D : C \times K \to \breve{M}$ – декодуюче відображення прийнятої стеганопослідовності $\widetilde{s}^N$ і ключа k^N в декодоване повідомлення $\breve{m} = D\left(\widetilde{s}^N, k^N\right)$.

Таким чином, величина A_1 характеризує максимально допустиму ступінь спотворення контейнера при встановленні в нього приховуваного повідомлення. Незважаючи на те, що дане визначення формально описує стеганосистеми блочного типу, на практиці воно може бути розширене і на стеганосистеми потокового типу, в яких вікно обробки описується ковзаючим блоком довжиною N. В цьому випадку параметр N стеганосистеми може бути названий довжиною кодового обмеження стеганосистеми (по аналогії з безперервними кодами).

У більшості випадків спотворення A_1 є малим, оскільки апріорно приймається, що результат вбудовування в контейнер повідомлення повинен бути непомітним для стороннього особи (в тому числі і порушника). У стеганосистемах, в яких контейнер являє собою корисний для одержувача інформаційний сигнал і якість якого необхідно зберегти, величина A_1

обмежується. У системах ЦВЗ вимога мінімізації A_1 формулюється як вимога прозорості водяного знака, що свідчить про належність контейнера [1].

Крім того, визначення обмеження (1.18) спотворення містить усереднення по відношенню до розподілу $p(c^N, k^N)$ і по відношенню до рівномірного розподілу повідомлень. Такий вибір зроблено для зручності, оскільки це дозволяє використовувати класичні положення теорії Шеннона [21].

Розподіл $p(c^N, k^N)$ і вибір відображення E визначають конкретний вид розподілу множин формованих стеганограм.

Атакуючий вплив (без пам'яті), що призводить до спотворення A_2, описується умовною функцією розподілу $q^N(\tilde{s}^N \mid s^N)$ з множини S до множини $\tilde{S}$, такою, що виконується умова

$$\sum_{s^N \in S} \sum_{\tilde{s}^N \in \tilde{S}} d_2^N(s^N, \tilde{s}^N) \cdot q^N(\tilde{s}^N \mid s^N) \cdot p(s^N) \le A_2 \qquad (1.19)$$

За визначенням, A_2 є максимальною величиною спотворення стеганограми, викликаного навмисними діями порушника. Фізичний сенс обмеження величини A_2 полягає в наступному. У системах ЦВЗ порушник, намагаючись видалити водяний знак з завіреного контейнера, змушений сам зменшувати величину A_2, щоб істотно не спотворити цінний для нього контейнер. В інших стеганосистемах величина A_2 обмежується наявним у атакуючого енергетичним потенціалом встановлення завад, виникаючими завадами для інших каналів зв'язку при використанні загального ресурсу і іншими причинами.

Логічно припустити, що для реальних стеганосистем зазвичай виконується співвідношення $A_2 \ge A_1$ [1].

Відповідно до (4.2), атакуючий вплив описується і обмежується усередненими спотвореннями між множинами S і $\tilde{S}$. В інших випадках, якщо атакуючий знає опис функції E, то атакуючий вплив описується і обмежується усередненим спотворенням між множинами C і $\tilde{S}$:

$$\sum_{\substack{c^N,m\\k^N,\tilde{s}^N}} d^N\left(c^N,\tilde{s}^N\right)\cdot q^N\left[\tilde{s}^N \mid E\left(c^N,m,k^N\right)\right]\cdot p\left(c^N,k^N\right)\le A_2 \qquad (1.20)$$

Визначення A_2 відповідно до вираження (4.3) допускає, що порушнику відомі точні ймовірнісні характеристики контейнерів. Ця обставина істотно ускладнює завдання забезпечення захищеності інформації, що приховується, тому в стійких стеганосистемах використовуються різні методи приховування від порушника характеристик використовуваних контейнерів. Наприклад, такі методи включають використання для вбудовування підмножини контейнерів з ймовірними характеристиками, відмінними від характеристик всієї множини відомих порушнику контейнерів, або рандомізовану компресію сигналу контейнера перед вбудовуванням в нього приховуваного повідомлення [1]. Тому обчислення спотворення A_2 відповідно до (4.2) є більш універсальним, оскільки порушник завжди має можливість вивчати ймовірні характеристики спостережуваних стеганограм.

Маючи опис стеганосистеми і атакуючого впливу $q^N\left(\tilde{s}^N \mid s^N\right)$, можна описати змагання (гру) проміжній атакуючої сторонами.

Інформаційно-приховуюче змагання, яке призводить до викривлення (A_1, A_2), описується взаємозв'язком використовуваної стеганосистеми, що викликає спотворення кодування A_1, до атакуючого впливу, що викликає спотворення A_2 Швидкість передачі прихованих повідомлень по стеганоканалу визначається у вигляді $R = N^{-1}\cdot\log|M|$. При цьому швидкість передачі R виражається через середню кількість біт приховуваного повідомлення, які безпомилково передаються (переносяться) одним символом (пікселем, відліком) стеганопослідовності s^N.

Це визначення співзвучно «класичному» визначенню швидкості передачі звичайних повідомлень по каналу відкритого зв'язку, яке виражається в середній кількості безпомилково переданих біт за одне використання каналу [1].

Ймовірність руйнування прихованого повідомлення (середню ймовірність похибки) в стеганопослідовності довжиною N визначають як

$$P_{br}^{N} = |M|^{-1} \cdot \sum_{m \in M} P\left[D\left(\tilde{S}, K\right) \neq m \mid M = m\right] \qquad (1.21)$$

де приховувані повідомлення m рівномірно вибираються з безлічі M. Ймовірність P_{br}^{N} є усередненою на множині всіх повідомлень ймовірністю того, що атакуючий успішно спотворить приховано передаване повідомлення. Атакуючий досягає успіху в інформаційному змаганні, якщо декодоване під час прийому повідомлення не збігається із вбудованим в контейнер прихованим повідомленням, або ж декодер нездатний прийняти однозначне рішення.

Теоретично досяжну швидкість безпомилкової передачі приховуваних повідомлень і приховану пропускну здатність при спотвореннях не більше, ніж (A_1, A_2), пропонується визначити наступним чином.

Швидкість R безпомилкової передачі приховуваних повідомлень є досяжною для спотворень не більше, ніж (A_1, A_2), якщо існує стеганосістема з довжиною блоку N, яка призводить до спотворення кодування не більше A_1 на швидкості $R_N > R$, така що $P_{br}^{N} \to 0$ при $N \to \infty$ будь-яких атаках порушника, що призводять до спотворень не більше A_2.

Прихована пропускна здатність B (A_1, A_2) є супремум (верхньою межею) всіх досяжних швидкостей безпомилкової передачі приховуваних повідомлень при спотвореннях не більше (A_1, A_2).

Таким чином, ППЗ є верхньою межею швидкості безпомилкової передачі приховуваних даних, при якій спотворення контейнера, викликані вбудовуванням в нього зазначених повідомлень (A_1) і діями порушника по руйнуванню цих повідомлень (A_2), не перевищують заданих величин.

Як і ПЗ каналів передачі відкритих повідомлень, ПЗ каналів передачі приховуваних повідомлень визначається в ідеалізованих умовах, при яких затримка кодування / декодування нескінченна (тобто), статистика контейнерів, приховуваних повідомлень, стеганограм і ключів точно відома, складність побудови стеганосистеми не обмежена.

Цілком очевидно, що така пропускна здатність каналу прихованого зв'язку має сенс теоретичної межі, що вказує області, в яких існують і, відповідно, не існують стеганосистеми при заданих величинах спотворень. Відомо, що швидкості реальних систем передачі відкритих повідомлень можуть тільки наближатися до величини ПЗ відкритих каналів, причому в міру наближення до неї обчислювальна складність реалізації систем передачі зростає спочатку приблизно по лінійній, а потім – по квадратичній і далі по експоненційній залежності від довжини блоку кодування N [1].

Цілком ймовірно, що аналогічні залежності зростання складності справедливі і для стеганосистем в міру наближення швидкості передачі приховуваних даних до величини СПС. Це припущення підтверджується наявним досвідом побудови стеганосистем [1]. Відомо, що спроби збільшити швидкість передачі приховуваних даних призводять до суттєвого ускладнення методів приховування інформації.

1.4 Існуючі підходи до формування прихованого каналу передачі інформації

Як аналог запропонованого підходу може бути розглянуто відомий підхід до захищеної передачі інформації з використанням імпульсного кодування [31], який включає формування інформаційного сигналу із закодованою інформацією, адитивне підсумовування інформаційного сигналу з хаотичним маскуючим сигналом, передачу сумарного сигналу по каналу зв'язку до приймального пристрою, детектування інформації. В якості інформаційного і маскуючого сигналів використовують послідовності одиночних імпульсів подібної форми. При цьому кодування інформації здійснюють відстанню між сусідніми імпульсами інформаційного сигналу, і в процесі детектування проводять розпізнавання форми імпульсів на основі нейромережевого методу і перетворюють інтервали часу між імпульсами інформаційного сигналу в інформацію.

На рис. 1.7 представлена схема для реалізації системи передачі інформації з використанням імпульсного кодування згідно відомого підходу [31].

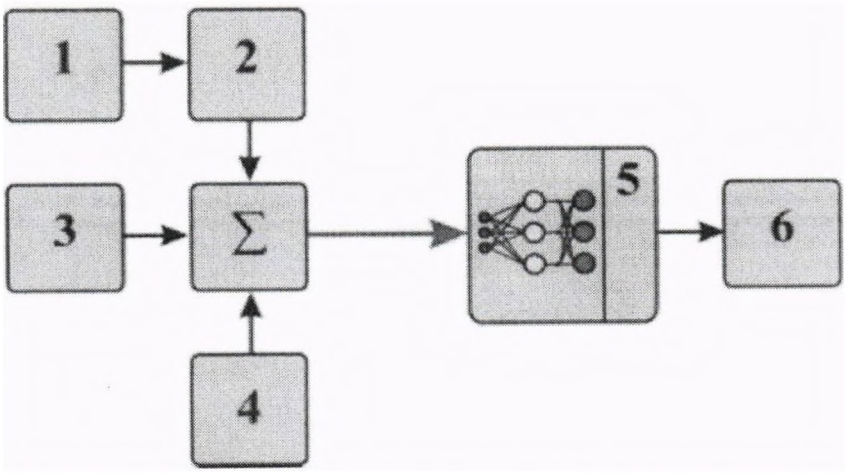

Рисунок 1.7 – Схема системи передачі інформації з використанням імпульсного кодування згідно відомого підходу [31]

На рис. 1.7 введено такі позначення:

1 – блок перетворення інформації в точковий процес;

2 – генератор одиночних імпульсів;

3 – генератор хаотичної послідовності маскуючих одиночних імпульсів;

4 – джерело шуму;

5 – блок розпізнавання форми одиночного імпульсу;

6 – перетворювач точкового процесу в інформацію.

Відомий підхід [31] полягає в наступному. Інформація за допомогою блоку 1 перетворюється в точковий процес, який кодує інформацію в інтервалах часу між моментами генерації одиночних імпульсів, форма яких задається генератором 2. Перетворення в точковий процес аналогового сигналу може проводитися в рамках моделі «накопичення-скидання», яка передбачає інтегрування сигналу і генерацію імпульсів при досягненні інтегралом заданого порогового рівня, після чого значення інтеграла обнуляється. Отриманий інформаційний сигнал підсумовується з хаотичною послідовністю маскуючих одиночних імпульсів форми, що незначно відрізняється, і яка генерується в

блоці 3. Для забезпечення захисту інформації, що передається додатково підмішується шум 4, що приводить до спотворень форми імпульсів і ускладнює їх розпізнавання. Інтенсивність шуму є досить великою для того, щоб ускладнити процедуру ідентифікації форми схожих імпульсів. Додатково дана процедура ускладнюється наявністю шумів в каналі зв'язку. У приймальному пристрої, що включає блоки 5 і 6, проводиться детектування інформаційного сигналу. В процесі детектування здійснюється розпізнавання зашумлених одиночних імпульсів за допомогою блоку 5, що містить мікропроцесор, запрограмований на реалізацію процедури нейромережевого методу. Використання мікропроцесора є простим і дешевим варіантом виконання, що дозволяє ефективно вирішувати завдання розпізнавання форми сигналу в умовах сильних завад. Виділена послідовність одиночних імпульсів інформаційного сигналу далі перетворюється в інформацію в блоці 6. За аналогією, даний підхід може бути реалізований для цифрових сигналів.

Процедура розпізнавання послідовності імпульсів, що кодує передане повідомлення у часових інтервалах між імпульсами, базується на стандартному методі розпізнавання сигналів на основі штучних нейронних мереж, що використовують перцептронну структуру із застосуванням моделі нейрона Маккалок-Пітса. Більш ефективні методи розпізнавання, як зазначається в підході [31], можуть ґрунтуватися на вейвлетних нейронних мережах, здатних знизити похибки ідентифікації форми зашумленного імпульсу. Вибір того чи іншого типу нейромережі не є принциповим для практичної реалізації відомого підходу до захищеної передачі інформації з використанням імпульсного кодування [31], і визначається технічними вимогами до характеристик каналу зв'язку. Зокрема, при високому рівні шумів в підході рекомендовано використання вейвлетних нейронних мереж, як кращого варіанту розпізнавання форм імпульсних сигналів

Недоліком відомого підходу до захищеної передачі інформації з використанням імпульсного кодування [31] є необхідність кодування інформації і складність її детектування.

Відомий підхід (прототип) до прихованої передачі інформації із розширенням спектра [2, 32, 33], заснований на додаванні вбудованого сигналу і сигналу, що є функцією вбудованого сигналу і маскуючого сигналу, а на приймальній стороні статистичним методом за допомогою порогового пристрою приймається рішення про наявність чи відсутність прихованої інформації. Відомий підхід-прототип застосовується для впровадження цифрових водяних знаків (ЦВЗ).

ЦВЗ впроваджується в аудіосигнали (послідовність 8- або 16-бітних відліків) шляхом незначної зміни амплітуди кожного відліку. Для виявлення ЦВЗ не вимагається вихідного аудіосигналу.

Для того, щоб визначити, чи дійсно певний ЦВЗ перебуває в сигналі, граничне значення ЦВЗ повинне бути вище 0,7. Якщо потрібна більша вірогідність у визначенні наявності ЦВЗ у сигналі, граничне значення необхідно збільшити. Робота кодера і декодера у відомому підході-прототипі представлені на рис. 1.8, де ГВЧ – генератор випадкових чисел.

На рис. 1.9 показана емпірична функція щільності ймовірності для аудіосигналу з ЦВЗ і без ЦВЗ. Емпірична функція щільності ймовірності аудіосигналу без ЦВЗ показана безперервною кривою, пунктирна крива описує емпіричну функцію щільності ймовірності аудіосигналу з вбудованим ЦВЗ. Обидва розподіли були обчислені з використанням 1 000 різних значень ЦВЗ при відношенні сигнал-шум 26 дБ.

Впровадження в один аудіосигнал великої кількості різних ЦВЗ приводить до збільшення чутності перекручувань. Максимальна кількість ЦВЗ обмежена енергією кожного з них. Декодер здатний правильно відновити кожний ЦВЗ за умови використання кодером унікальних ключів. На рис. 1.10 показаний приклад виявлення ЦВЗ із використанням 1 000 різних ключів, з яких тільки один – правильний [32].

В роботі [33] перевірялася стійкість розглянутого методу впровадження інформації до стиснення MPEG до швидкостей 80 кб/с і до 48 кб/с. Після відновлення при стиску до швидкості 80 кб/с можна спостерігати незначне

зменшення граничної величини виявлення в аудіосигналах зі ЦВЗ, що показано на рис. 1.11. При стисненні аудіосигналу до 48 кб/с з'являються звукові ефекти, відчутно знижують якість сигналів з ЦВЗ.

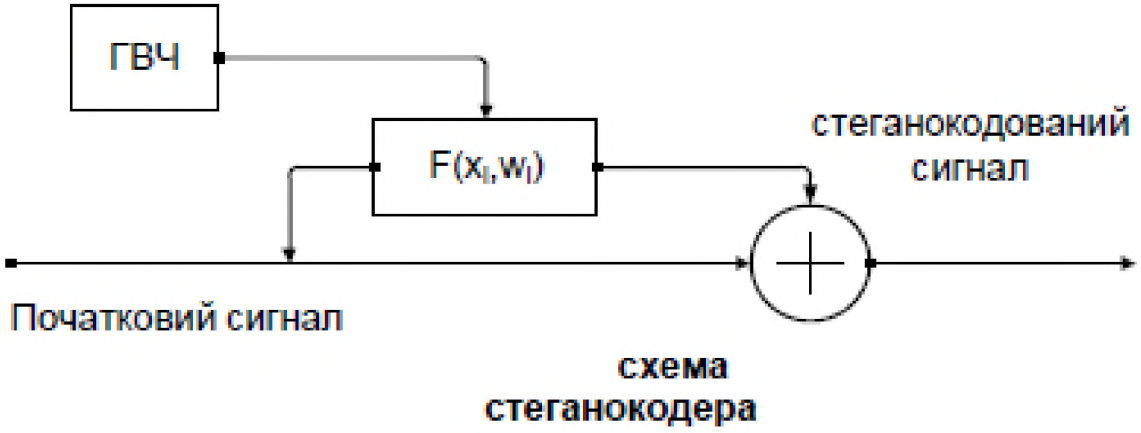

схема стеганокодера

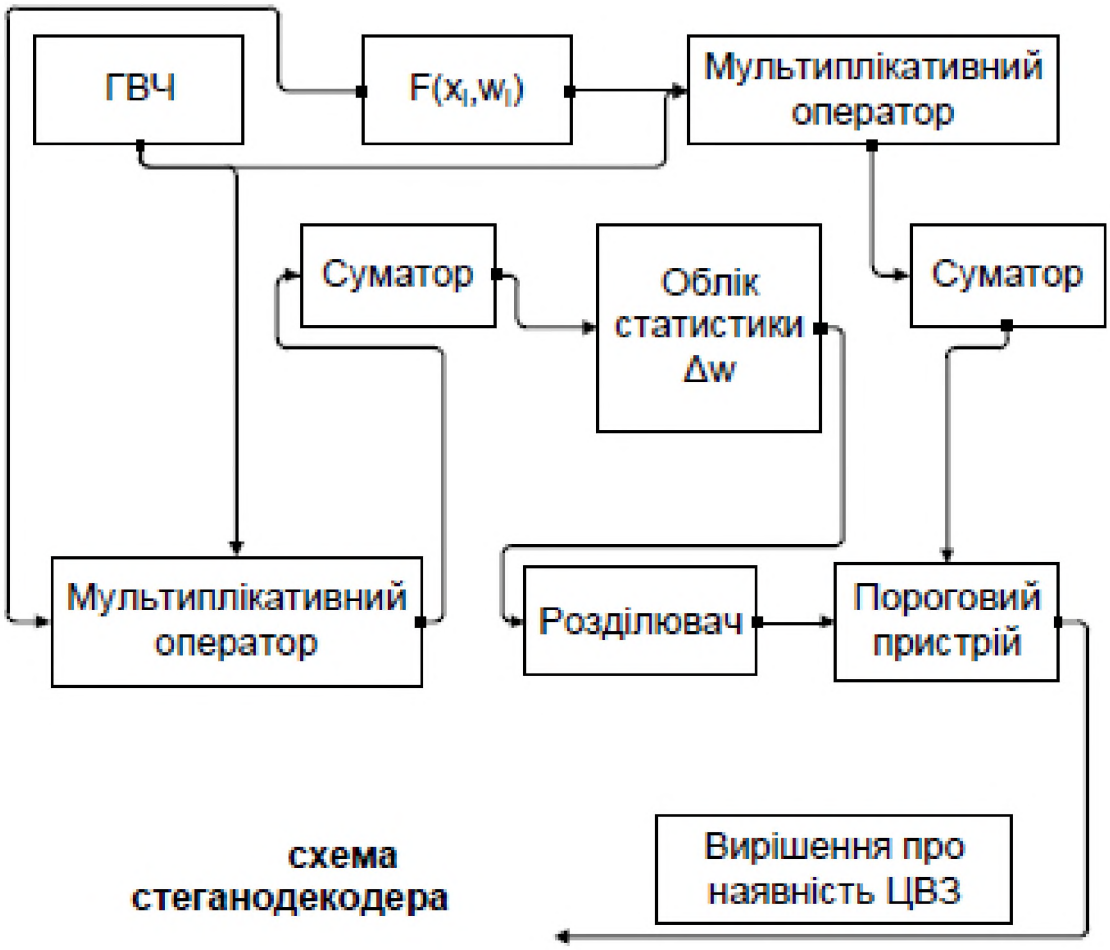

схема стеганодекодера

Рисунок 1.8 – Схеми стеганокодера і стеганодекодера згідно відомого підходу-прототипу [2, 32, 33]

Стійкість алгоритму вбудовування ЦВЗ до фільтрації перевірена застосуванням до нього ковзаючого фільтра середніх частот і фільтра нижніх частот. Аудіофайли із впровадженим ЦВЗ профільтровані ковзним фільтром середніх частот довжини 20, що вносить в аудіоінформацію значні перекручування.

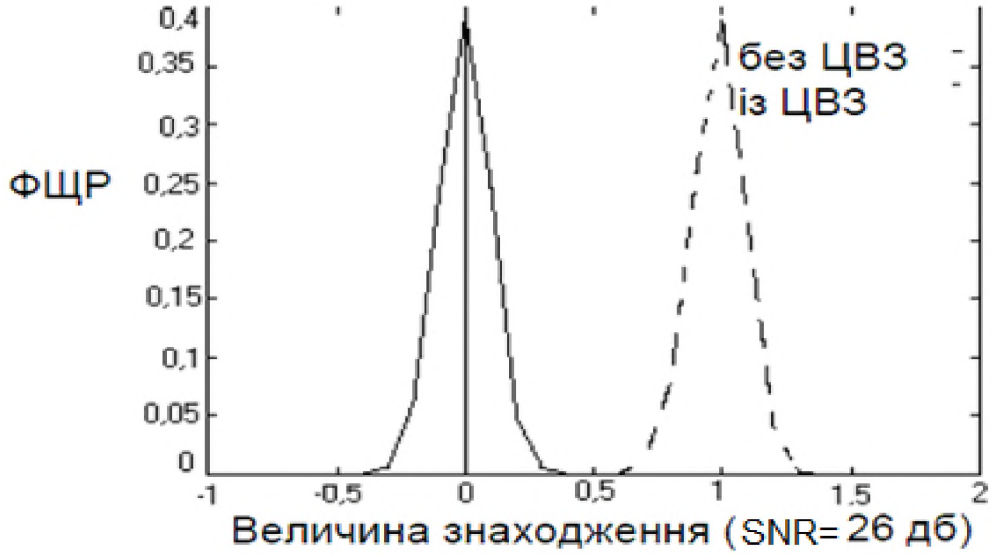

Рисунок 1.9 – Функція щільності розподілу (ФЩР) величини виявлення для сигналів з ЦВЗ і без ЦВЗ

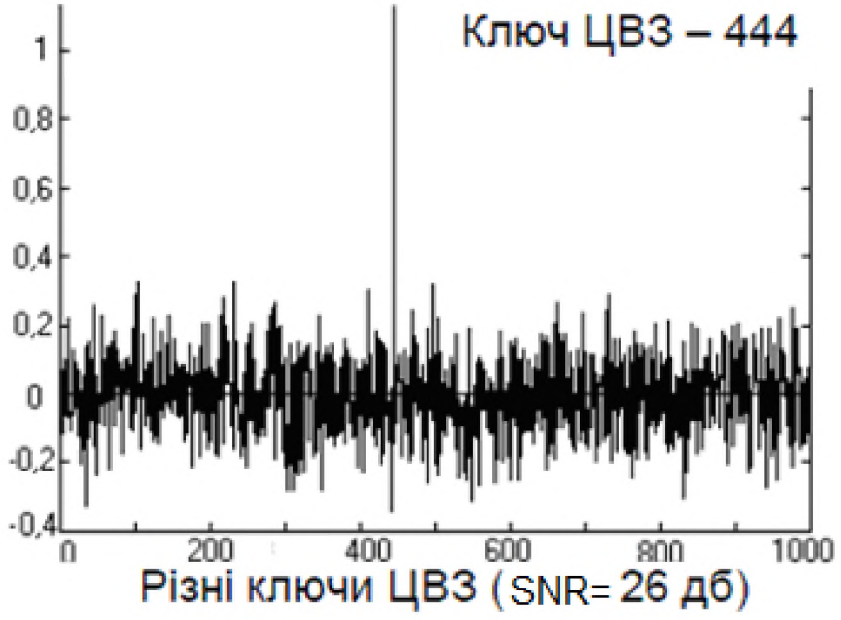

Рисунок 1.10 – Розпізнавання заданого ключа вбудованих ЦВЗ

На рис. 1.12 показано, як змінюється гранична величина виявлення при застосуванні описаного фільтра. Загалом, поріг виявлення збільшується у відфільтрованих сигналах. Це відбувається через те, що функція щільності розподілу сигналів після фільтрації зрушується вправо порівняно з відносною функцією розподілу сигналів, що не піддавалися фільтрації.

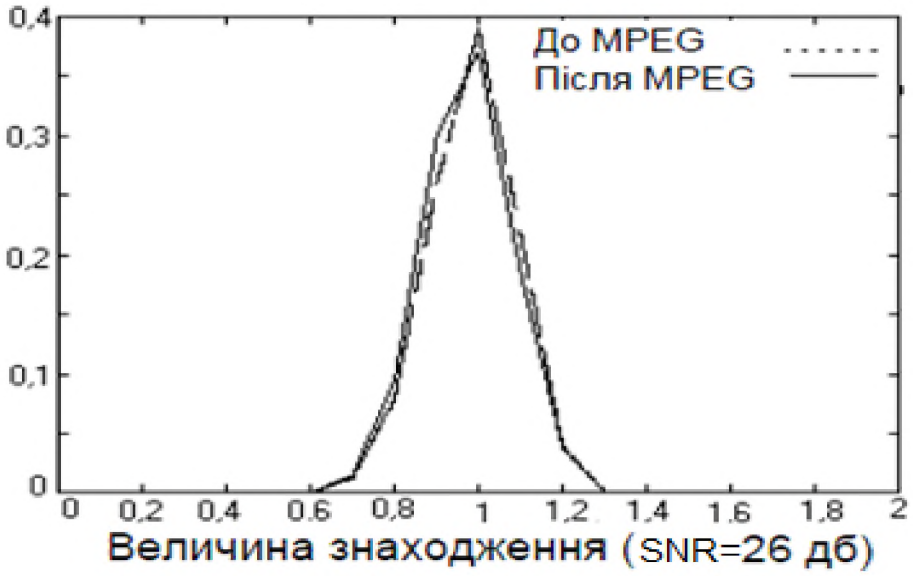

Рисунок 1.11 – Вплив стиску даних на ЦВЗ

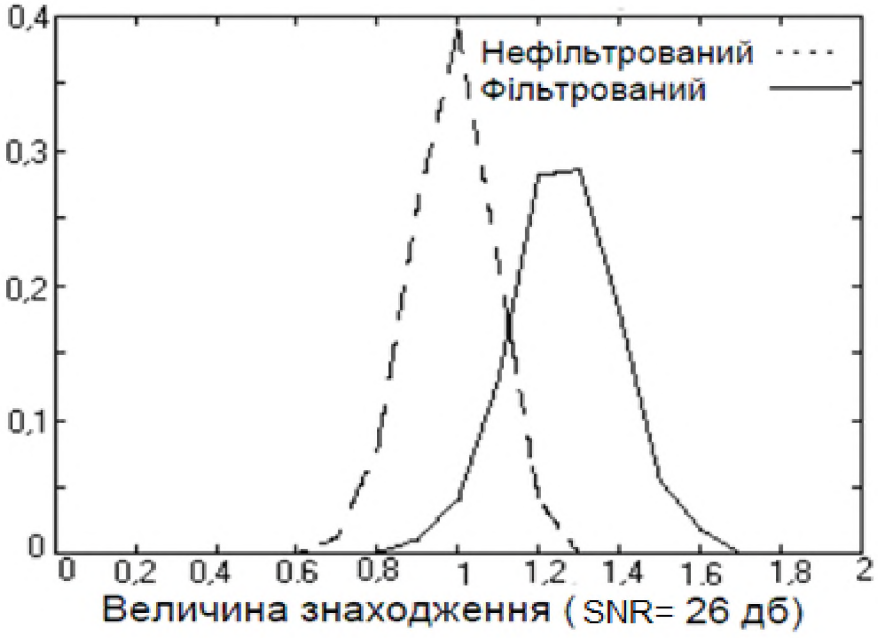

Рисунок 1.12 – Вплив на ЦВЗ застосування до аудіосигналу ковзного фільтра середніх частот (ФСЧ)

ЦВЗ зберігається й при застосуванні до аудіосигналу фільтра нижніх частот. Однак при фільтрації аудіосигналів зі ЦВЗ фільтром нижніх частот Хемінга 25-го порядку із частотою зрізу 2205 Гц мало місце зменшення ймовірності виявлення наявності ЦВЗ.

Для перевірки стійкості ЦВЗ до передискретизації Р. Бассіа й І. Пітасом аудіосигнали були передискретизовані на частоти 22050 Гц і 11025 Гц і назад на початкову частоту. ЦВЗ зберігався.

При переквантуванні аудіосигналу з 16-бітного в 8-бітний і назад впроваджений ЦВЗ зберігається, незважаючи на часткову втрату інформації. На рис. 1.13 показано наскільки добре ЦВЗ зберігається в 1000 аудіосигналах при їх переквантуванні в 8-бітові відліки і назад в 16-бітові.

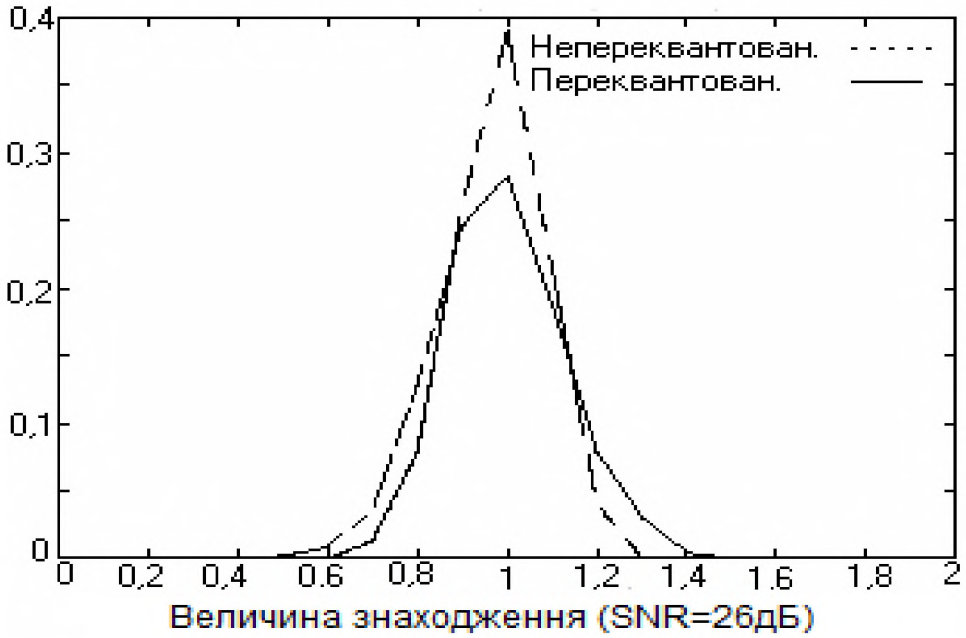

Рисунок 1.13 – Вплив переквантування сигналу на ЦВЗ

Девіація функції щільності розподілу переквантованого сигналу збільшується, як і в разі застосування фільтра нижніх частот, отже, має місце зменшення ефективності виявлення.

Слід зазначити, що недоліком відомого підходу-прототипу до прихованої передачі інформації із розширенням спектра [2, 32, 33] є необхідність

статистичної обробки прийнятої інформації і неможливість відновлення прихованої інформації в повному обсязі, оскільки результатом роботи пристрою, що реалізує підхід-прототип, є ухвалення рішення про наявність прихованої інформації.

1.5 Висновок. Постановка задачі

В розділі проаналізовано принципи побудови стеганографічних методів захисту інформації і прихованої передачі даних. Встановлено, що використання тільки криптографії, без стеганографії для прихованої передачі даних може дати супротивникові інформацію про те, що щось змінилося і спровокувати його на небажані дії.

В розділі проаналізовано існуючі підходи до формування прихованого каналу передачі інформації. Встановлено, що недоліком відомого підходу до захищеної передачі інформації з використанням імпульсного кодування [31] є необхідність кодування інформації і складність її детектування.

Встановлено, що недоліком відомого підходу-прототипу до прихованої передачі інформації із розширенням спектра [2, 32, 33] є необхідність статистичної обробки прийнятої інформації і неможливість відновлення прихованої інформації в повному обсязі, оскільки результатом роботи пристрою, що реалізує підхід-прототип, є ухвалення рішення про наявність прихованої інформації.

Таким чином, для усунення недоліків існуючих підходів необхідно:

• запропонувати підхід до організації прихованої стеганографічної передачі інформації з маскуванням корисного сигналу;

• оцінити ефективність запропонованого підходу.

2 СПЕЦІАЛЬНА ЧАСТИНА

2.1 Підхід до організації прихованої стеганографічної передачі інформації з маскуванням корисного сигналу

Запропонований підхід відноситься до комп'ютерної техніки, а саме до способу стеганографічного перетворення даних. Мета розробки запропонованого підходу – збільшення скритності і точності відновлення приховуваного сигналу. Підхід до організації прихованої стеганографічної передачі інформації з маскуванням корисного сигналу, заснований на додаванні приховуваного сигналу і сигналу, що є функцією приховуваного сигналу і маскуючого сигналу, який відрізняється тим, що, з метою збільшення скритності і точності відновлення приховуваного сигналу, формується стегоконтейнер, що містить дві компоненти, для цього виділяється перший сигнал, який дорівнює половині приховуваного сигналу, і другий сигнал, який дорівнює різниці значення першого ключа і першого сигналу. Перша компонента контейнера визначається першим сигналом, до якого додається добуток маскуючого сигналу на суму значення другого ключа і першого сигналу, друга компонента контейнера визначається другим сигналом, до якого додається добуток маскуючого сигналу на суму значення третього ключа і другого сигналу. Для відновлення прихованого сигналу визначаються чотири коефіцієнта, перший коефіцієнт дорівнює подвоєній сумі значень першого і третього ключів, другий коефіцієнт дорівнює подвоєному значенню другого ключа, третій коефіцієнт дорівнює подвоєному добутку значень першого і другого ключів, четвертий коефіцієнт дорівнює сумі значень другого і третього ключів. Відліки прихованого сигналу знаходять, складаючи третій коефіцієнт з добутком першої компоненти контейнера на перший коефіцієнт і віднімаючи добуток другої компоненти контейнера на другий коефіцієнт, отриманий результат ділять на суму першої та другої компоненти контейнера і четвертого коефіцієнта.

Запропонований підхід відноситься до електрозв'язку та обчислювальної техніки, до області способів і пристроїв стеганографічного перетворення даних і може бути використаний в зв'язкових, обчислювальних і інформаційних системах для стеганографічного приховування інформації при обміні даними урядовими, правоохоронними, оборонними, банківськими і промисловими установами, коли виникає необхідність зберігання та передачі конфіденційної інформації.

Технічними результатами, які були отримані в кваліфікаційній роботі, є підхід до організації прихованої стеганографічної передачі інформації з маскуванням корисного сигналу, що дозволяє маскувати корисний сигнал в довільному шумовому сигналі при співвідношенні сигнал / шум менше 0,1 і відновлювати приймаючою стороною приховану інформацію у повному обсязі.

На рис. 2.1 приведена структурна схема пристрою, що реалізує запропонований підхід до організації прихованої стеганографічної передачі інформації з маскуванням корисного сигналу.

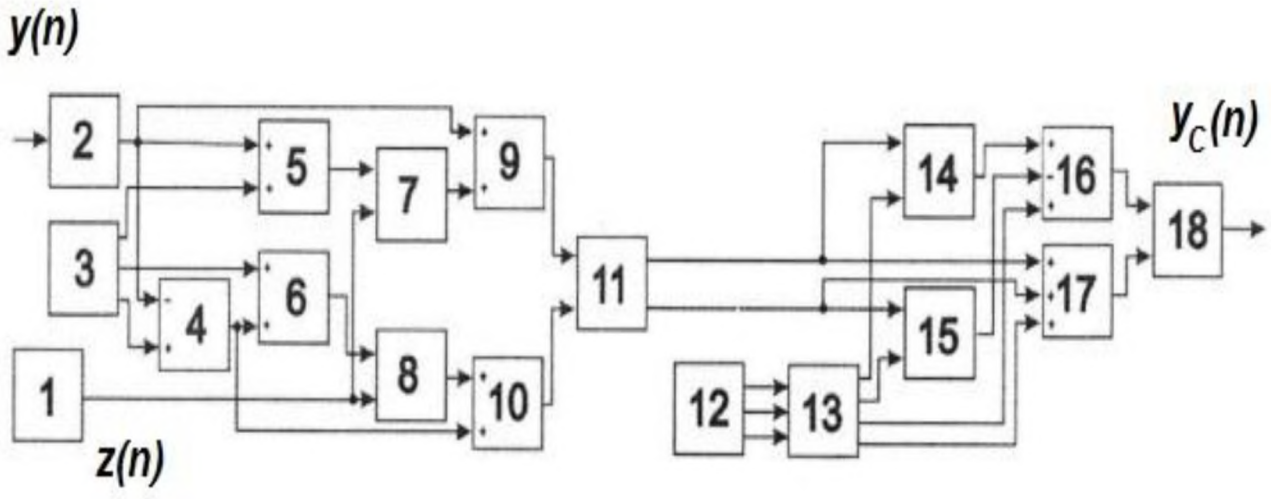

Рисунок 2.1 – Структурна схема пристрою, що реалізує запропонований підхід

На рис. 2.1 введено такі позначення:

1 – блок ослаблення сигналу;

2, 12 – перший і другий блоки пам'яті ключів, відповідно;

3 – блок формування маскуючого сигналу;

4 – блок віднімання;

5, 9, 6, 10, 17 і 16 – шість блоків підсумовування відповідно;

7, 8 , 14 і 15 – чотири блоки множення відповідно;

11 – блок пристрою передачі інформації;

13 – блок формування коефіцієнтів;

18 – блок розподілу.

Пристрій (рис. 2.1) містить блок ослаблення сигналу 1, до входу якого підключений вхід пристрою, вихід блоку ослаблення сигналу 1 підключений до першого входу блоку віднімання 4, до першого входу першого блоку підсумовування 5 і до першого входу другого блоку підсумовування 9. Перший вихід першого блоку пам'яті ключів 3 підключений до другого входу першого блоку підсумовування 5, другий вихід підключений до першого входу третього блоку підсумовування 6, третій вихід підключений до другого входу блоку віднімання 4. Вихід блоку формування маскуючого сигналу 3 підключений до другого входу першого блоку множення 7 і до другого входу другого блоку множення 8. Вихід блоку віднімання 4 підключений до другого входу третього блоку підсумовування 6 і до другого входу четвертого блоку підсумовування 10. Вихід першого блоку підсумовування 5 підключений до першого входу першого блоку множення 7. Вихід третього блоку підсумовування 6 підключений до першого входу другого блоку множення 8. Вихід першого блоку множення 7 підключений до другого входу другого блоку підсумовування 9, вихід другого блоку множення 8 підключений до першого входу четвертого блоку підсумовування 10. Вихід другого блоку підсумовування 9 підключений до першого входу блоку передачі інформації 11, вихід четвертого блоку підсумовування 10 підключений до другого входу блоку передачі інформації 11. Перший вихід блоку передачі інформації підключений до першого входу третього блоку множення 14 і до першого входу п'ятого блоку підсумовування 17, другий вихід блоку передачі інформації 11 підключений до першого входу четвертого блоку множення 15 і до другого входу п'ятого блоку підсумовування 17. Перший вихід другого блоку пам'яті

ключів 12 підключений до першого входу блоку формування коефіцієнтів 13, другий вихід підключений до другого входу блоку формування коефіцієнтів 13, третій вихід підключений до третього входу блоку формування коефіцієнтів 13. Перший вихід блоку формування коефіцієнтів 13 підключений до другого входу третього блоку множення 14, другий вихід підключений до другого входу четвертого блоку множення 15, третій вихід підключений до третього входу шостого блоку підсумовування 16, четвертий вихід підключений до третього входу п'ятого блоку підсумовування 17. Вихід третього блоку множення 14 підключений до першого входу шостого блоку підсумовування 16, вихід четвертого блоку множення 15 підключений до другого входу шостого блоку підсумовування 16. Вихід шостого блоку підсумовування 16 підключений до першого входу блоку розподілу 18, вихід п'ятого блоку підсумовування 17 підключений до другого входу блоку розподілу 18, вихід блоку розподілу 18 є виходом пристрою.

Відповідно до запропонованого підходу до організації прихованої стеганографічної передачі інформації з маскуванням корисного сигналу виконуються наступні операції. Формують відліки першого сигналу, значення яких в два рази менше значень відліків приховуваного сигналу. Формують відліки другого сигналу як різниця значень першого ключа і першого сигналу. Формують відліки першої компоненти стегоконтейнера, додаючи до першого сигналу добуток маскуючого сигналу на суму значень другого ключа і першого сигналу. Формують відліки другої компоненти стегоконтейнера, додаючи до другого сигналу добуток маскуючого сигналу на суму значень третього ключа і другого сигналу.

Стегоконтейнер передають по каналу зв'язку.

Для відновлення прихованого сигналу на приймальній стороні визначають чотири коефіцієнта. Перший коефіцієнт дорівнює подвоєній сумі значень першого і третього ключів. Другий коефіцієнт дорівнює подвоєному значенню другого ключа. Третій коефіцієнт дорівнює подвоєному добутку значень першого і другого ключів. Четвертий коефіцієнт дорівнює сумі значень

другого і третього ключів. Відлік прихованого сигналу знаходять, складаючи третій коефіцієнт з добутком першої компоненти контейнера на перший коефіцієнт і віднімаючи добуток другої компоненти контейнера на другий коефіцієнт, а отриманий результат ділять на суму першої та другої компоненти контейнера і четвертого коефіцієнта.

2.2 Оцінка ефективності запропонованого підходу до організації прихованої стеганографічної передачі інформації з маскуванням корисного сигналу

Оцінка ефективності запропонованого підходу до забезпечення конфіденційності при передачі інформації з маскуванням корисного сигналу проводилась в середовищі Matlab / Simulink за допомогою стандартних і розроблених програм.

Позначимо відліки приховуваного сигналу y(n), а відліки маскуючого сигналу z(n). Перший сигнал визначається виразом

$$y_1(n) = 0.5y(n), \tag{2.1}$$

а другий сигнал виразом

$$y_2(n) = K_1 - y_1(n), \tag{2.2}$$

де K_1 – значення першого ключа.

Загальний вигляд стеганографічного перетворення, що формує стегоконтейнер, описується системою рівнянь:

$$\begin{cases} u_1(n) = y_1(n) + \varphi_1[y_1(n), z(n)] \\ u_2(n) = y_2(n) + \varphi_2[y2(n), z(n)] \end{cases}, \tag{2.3}$$

де φ – функція стеганографічного перетворення.

Використання лінійної функції (2.3) стеганографічного перетворення дозволяє отримати просту математичну модель відновлення прихованої інформації на основі стискаючих відображень [34]. Використовуємо такі вирази для компонент стегоконтейнера:

$$\begin{cases} u_1(n) = y_1(n) + (K_2 + y_1(n))z(n) \\ u_2(n) = y_2(n) + (K_3 + y_2(n))z(n) \end{cases}, \quad (2.4)$$

де K_2 і K_3 – ключі стеганографічного перетворення.

На рис. 2.2 показані, як приклад, перший і другий сигнали, отримані за допомогою (2.1) і (2.2). Приховуваний сигнал є випадковим з рівномірним розподілом щільності ймовірності в інтервалі ±0,05.

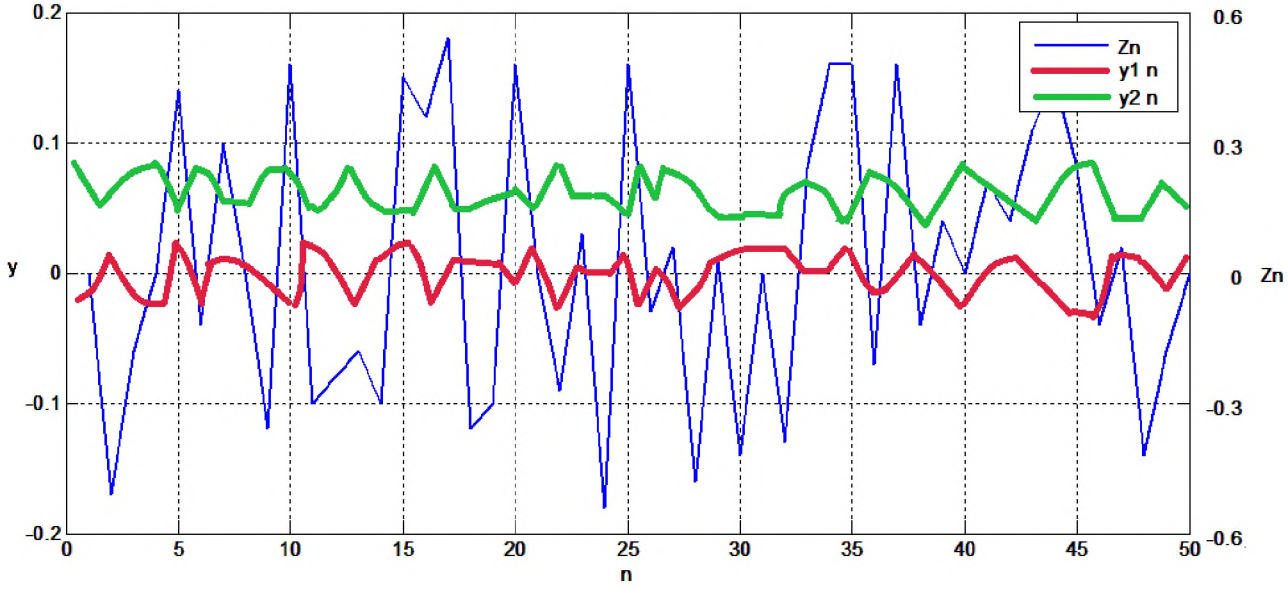

Рисунок 2.2 – Вибірка відліків маскуючого сигналу і першого і другого сигналів, отриманих при значенні першого ключа K_1=0,06

На рис. 2.3 показані обидві компоненти стегоконтейнера, отримані за допомогою (2.3). Маскуючий сигнал є випадковим з рівномірним розподілом щільності ймовірності в інтервалі ±1.

Закон розподілу щільності ймовірності у приховуваного і маскуючого сигналів може бути довільним.

На рис. 2.4 наведено фрагмент ковзаючого спектру 1024 відліків вбудовуваного сигналу.

На рис. 2.5 наведено фрагмент ковзаючого спектру 1024 відліків першої компоненти контейнера.

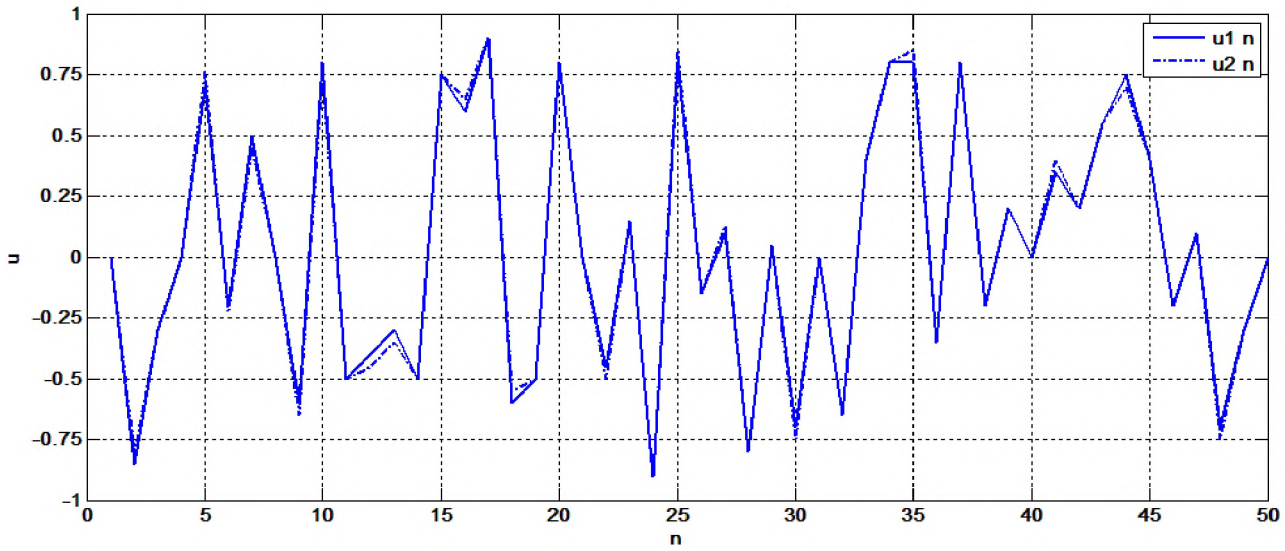

Рисунок 2.3 – Вибірка відліків першої і другої компоненти контейнера, отриманих при значеннях ключів K_2=1,9 і K_3=1,72

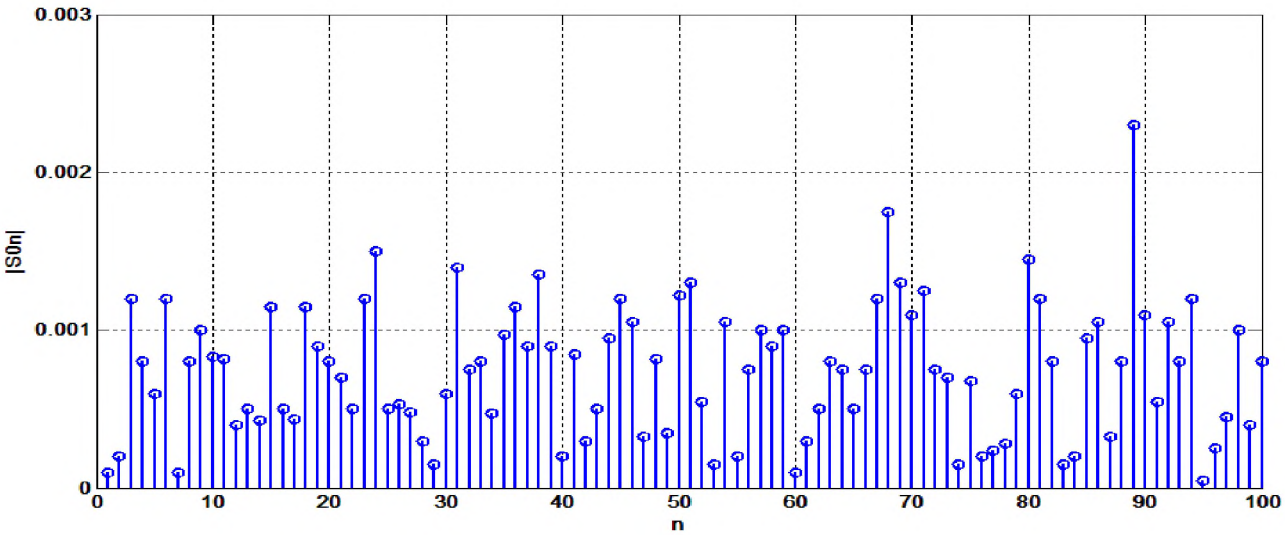

Рисунок 2.4 – Фрагмент ковзаючого спектру 1024 відліків вбудовуваного сигналу

На рис. 2.6 наведено фрагмент ковзаючого спектру 1024 відліків другої компоненти контейнера.

Аналіз спектрів приховуваного сигналу (рис. 2.4) і компонент стегоконтейнера (рис. 2.5 і 2.6) показує, що виділити приховуваний сигнал за допомогою фільтрації неможливо.

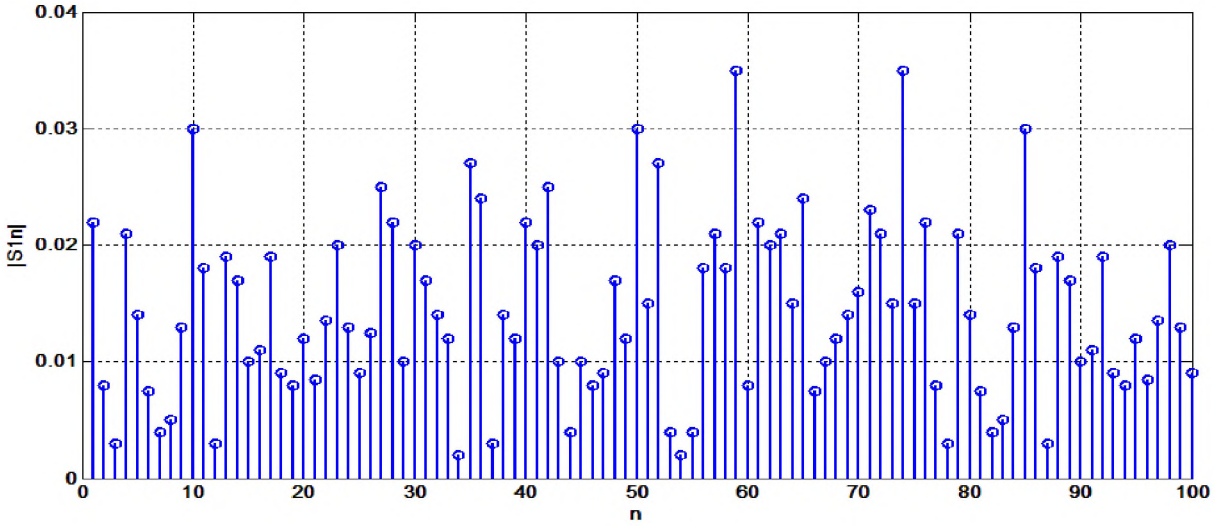

Рисунок 2.5 – Фрагмент ковзаючого спектру 1024 відліків першої компоненти контейнера

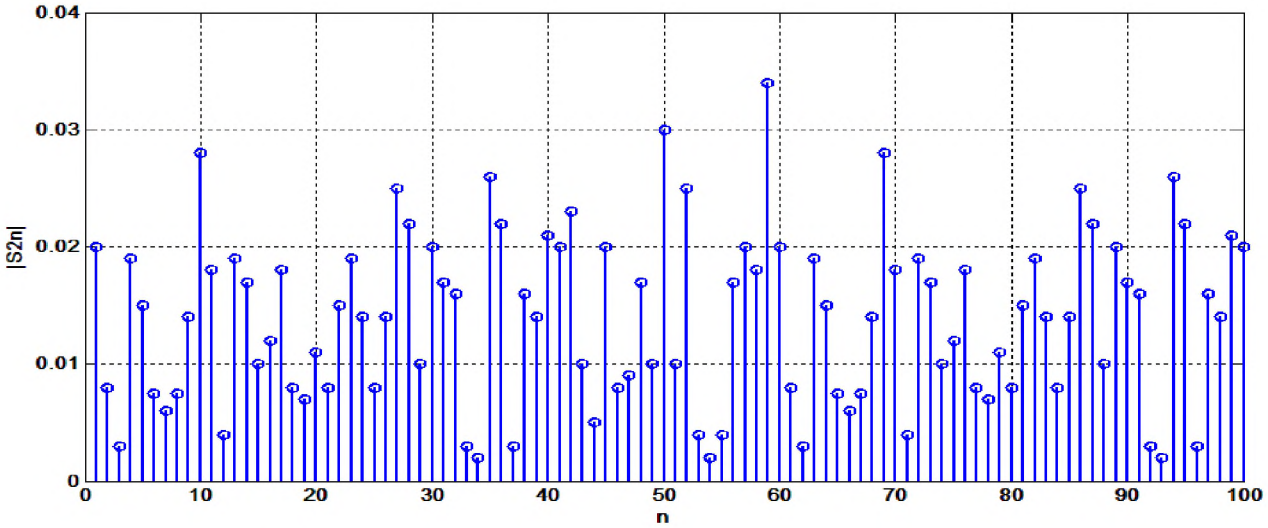

Рисунок 2.6 – Фрагмент ковзаючого спектру 1024 відліків другої компоненти контейнера

На рис. 2.7 наведено розподіл щільності ймовірності першої компоненти порожнього контейнера.

На рис. 2.8 наведено розподіл щільності ймовірності приховуваного сигналу.

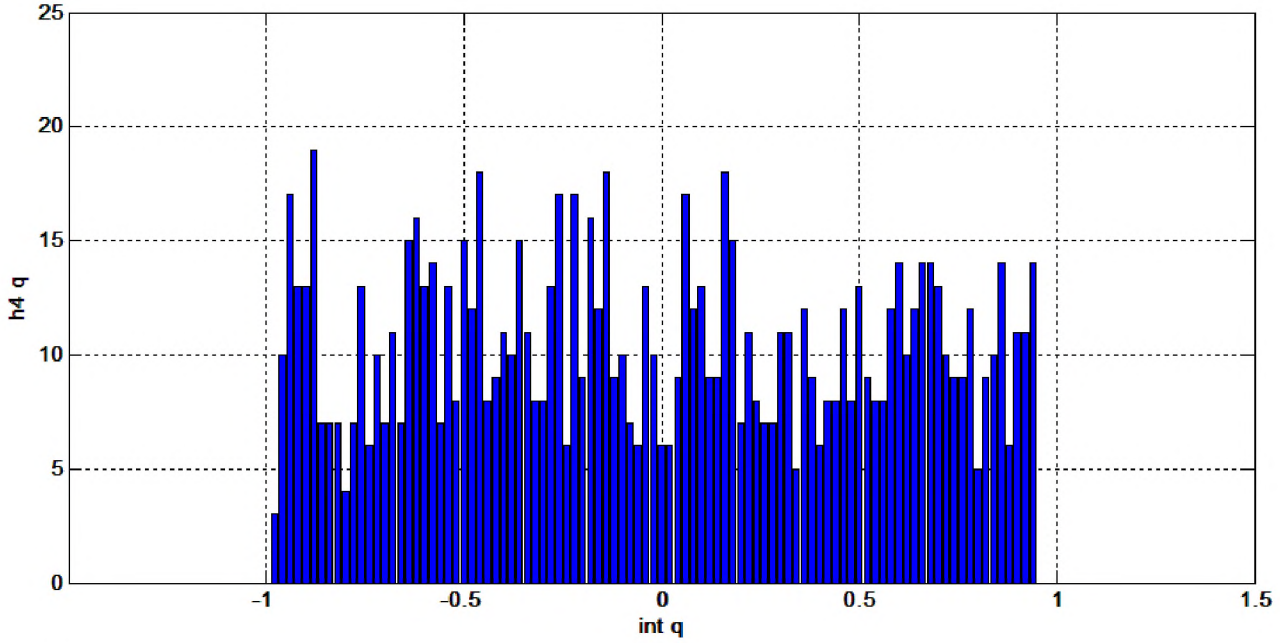

Рисунок 2.7 – Розподіл щільності ймовірності першої компоненти порожнього контейнера

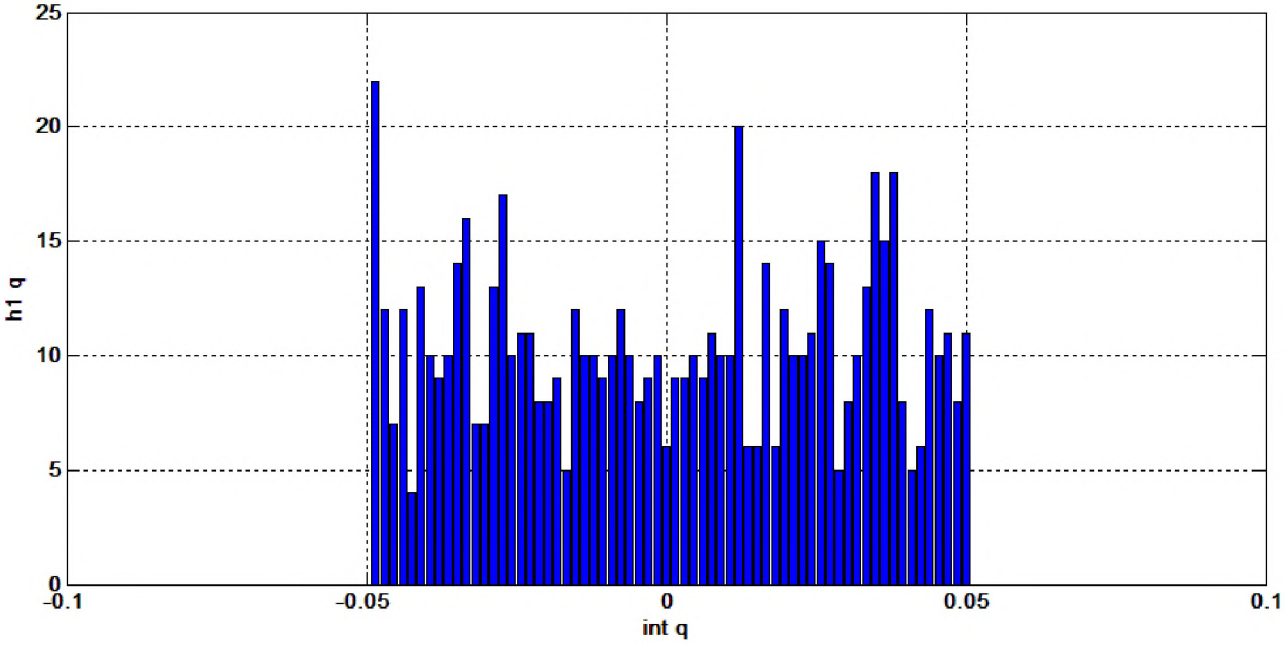

Рисунок 2.8 – Розподіл щільності ймовірності приховуваного сигналу

На рис. 2.9 наведено розподіл щільності ймовірності першої компоненти заповненого контейнера.

На рис. 2.10 наведено розподіл щільності ймовірності другої компоненти заповненого контейнера.

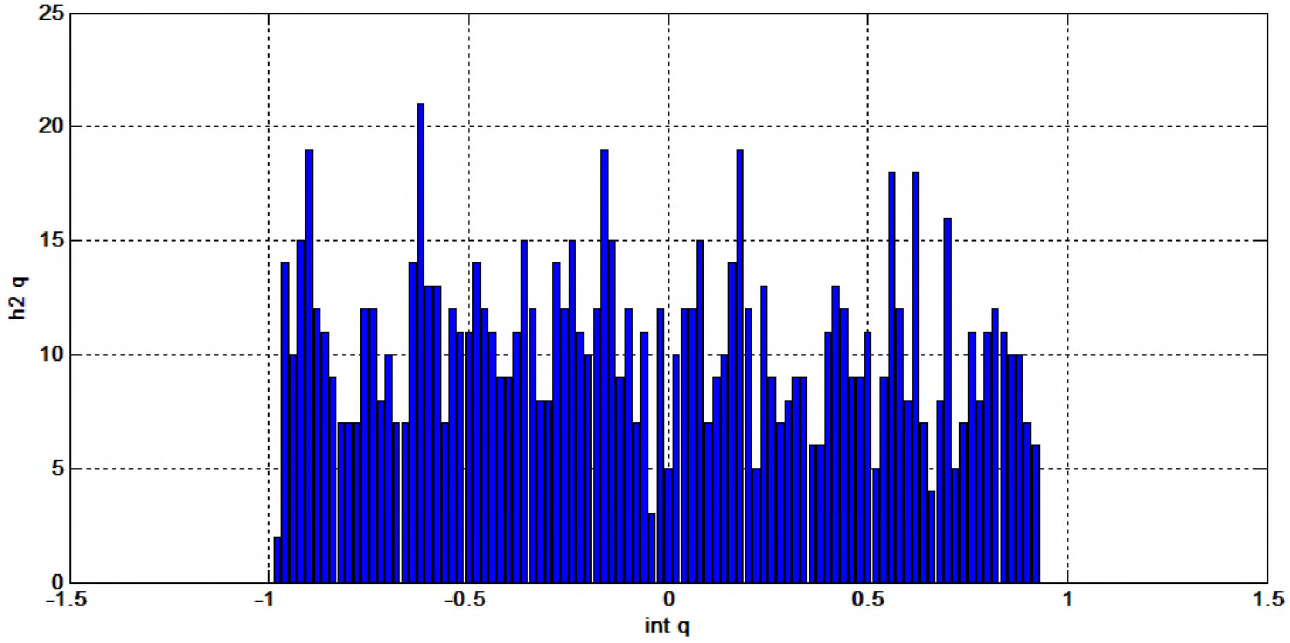

Рисунок 2.9 – Розподіл щільності ймовірності першої компоненти заповненого контейнера

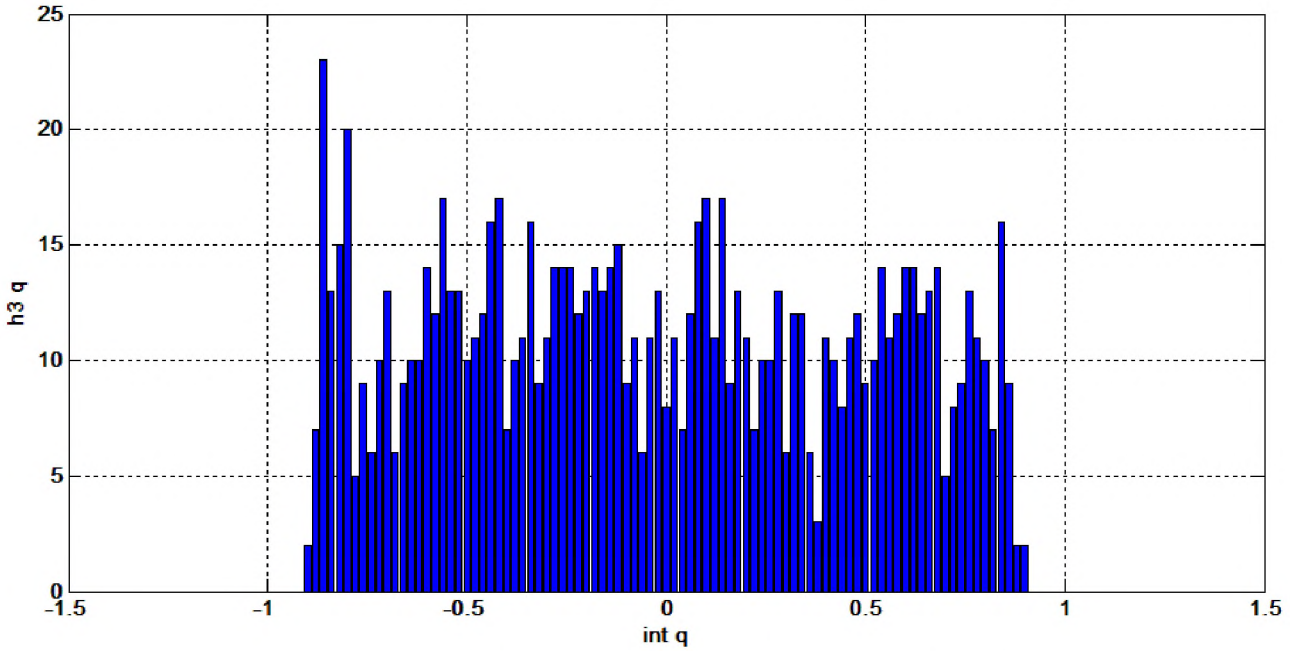

Рисунок 2.10 – Розподіл щільності ймовірності другої компоненти заповненого контейнера

Аналіз гістограм розподілу щільності ймовірності порожнього контейнера (рис. 2.7), приховуваного сигналу (рис. 2.8) і компонент

заповненого контейнера (рис. 2.9 і 2.10) показує, що розширення гістограми не відбувається.

Для виразів (2.4) відомі функціональні стискаючі відображення, що дозволяють виключити функції стеганографічного перетворення φ і виділити перший і другий сигнали [34]:

$$y_{1C}(n)=\frac{u_1(n)(K_3+K_1)+K_2(K_1-u_2(n))}{K_2+K_3+u_1(n)+u_2(n)}$$
$$y_{2C}(n)=\frac{u_2(n)(K_1+K_2)+K_2(K_1-u_1(n))}{K_2+K_3+u_1(n)+u_2(n)} \quad (2.5)$$

Приховуваний сигнал відновлюється наступним чином:

$$y_C(n)=y_{1C}(n)-y_{2C}(n)+K_1. \quad (2.6)$$

Після підстановки (2.5) в (2.6) отримаємо:

$$y_c(n)=\frac{u_{1c}(n)k_1-u_{2c}(n)k_2+k_3}{k_4+u_{1c}(n)+u_{2c}(n)}, \quad (2.7)$$

де коефіцієнти k визначаються за значеннями ключів K наступним чином:

$$k_1=2(K_1+K_3);\ \ k_2=2K_2;\ \ k_3=2K_1K_2;\ \ \ k_4=K_2+K_3. \quad (2.8)$$

На рис. 2.11 наведені відліки відновлених сигналів за допомогою виразів (2.5) і (2.7), а також похибка Δ відновлення приховуваного сигналу, яка порівнянна з похибкою роботи обчислювального процесора. Таким чином, операції відновлення приховуваного сигналу визначаються виразом (2.7).

Отже, пристрій, який реалізує запропонований підхід до організації прихованої стеганографічної передачі інформації з маскуванням корисного сигналу працює наступним чином.

Приховуваний сигнал надходить на блок ослаблення сигналу 1, де формується перший сигнал y_1 згідно (2.1).

Другий сигнал y_2 формується в блоці 4 з використанням першого ключа згідно (2.2).

Перша компонента стегоконтейнер u1 формується за допомогою блоків 5, 7, 9 згідно з першим рівнянням (2.4).

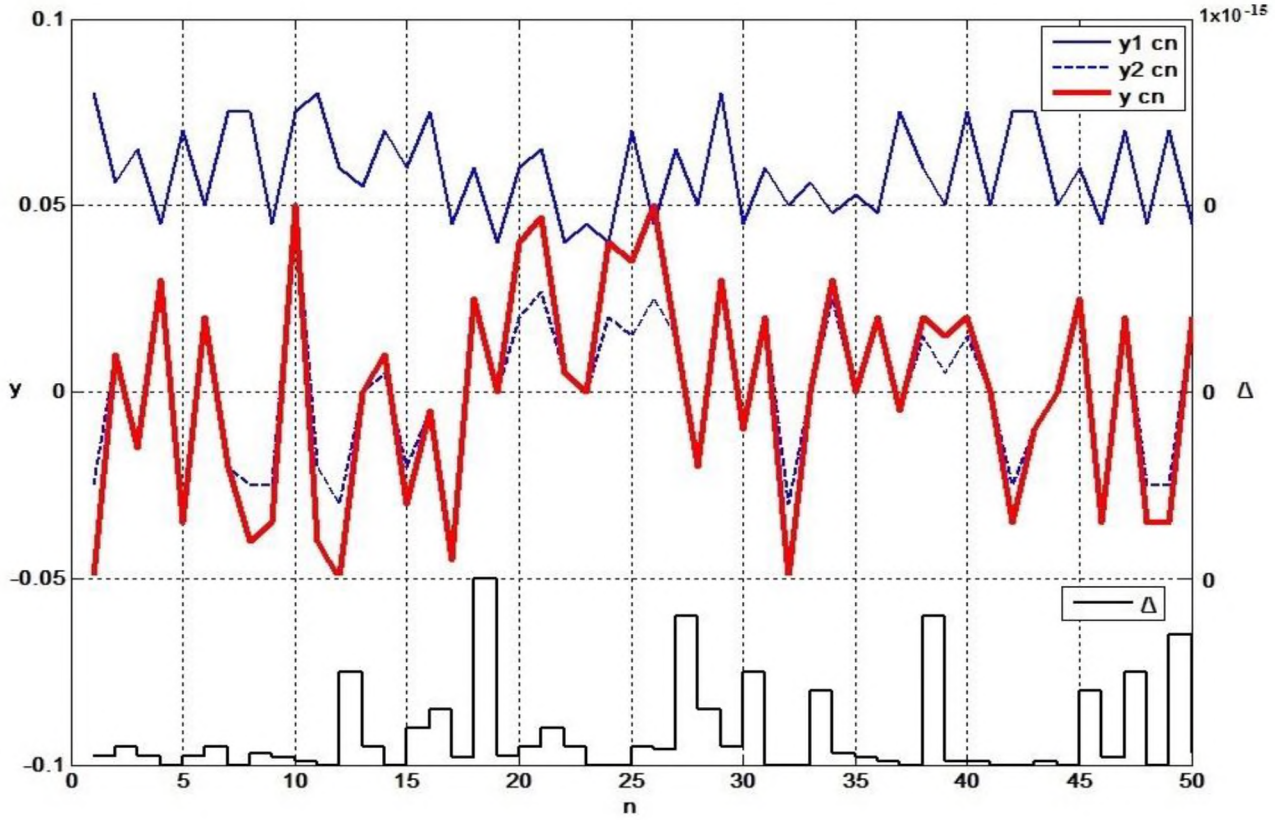

Рисунок 2.11 – Вибірка відліків, відновлених на приймальній стороні першого і другого сигналів, вбудованого сигналу і залежність похибки відновлення вбудованого сигналу

Другий компонент стегоконтейнер u_1 формується за допомогою блоків 6, 8, 10 згідно з другим рівнянням (2.4).

Обидві компоненти подаються на входи пристрою передачі інформації 11. Даний блок має на увазі пристрій передачі інформації, що включає в себе блоки модуляції сигналів, що передавальні і приймальні пристрої, і лінію передачі інформації. Прикладом пристрою передачі інформації, що реалізує одночасну передачу двох сигналів по одному каналу зв'язку є пристрій, що використовує квадратурну амплітудну модуляцію сигналу з подальшою демодуляцією [4]. Іншим прикладом є пристрій передачі стереофонічного аудіосигналу.

Виймання прихованої інформації на приймальному боці здійснюється відповідно до виразу (2.7). Коефіцієнти k рівняння (2.7) визначаються в блоці

13 за допомогою ключів K, які зберігаються в блоці 12. За допомогою блоків 14 і 16 визначається чисельник (2.7), за допомогою блоків 15 і 17 визначається знаменник (2.7), і з виходу дільника 18 знімається відновлена інформація.

Вихідний сигнал, при відсутності завад в блоці 11 і похибок квантування при виконанні обчислень, відповідає приховуваному сигналу з абсолютною точністю.

Таким чином, запропонований підхід до організації прихованої стеганографічної передачі інформації з маскуванням корисного сигналу дозволяє ефективно маскувати приховуваний сигнал в більш інтенсивному сигналі і передавати його по лінії зв'язку з подальшим відновленням.

2.3 Висновки

Запропонований підхід до організації прихованої стеганографічної передачі інформації з маскуванням корисного сигналу відноситься до комп'ютерної техніки, а саме до способу стеганографічного перетворення даних. Мета розробки запропонованого підходу – збільшення скритності і точності відновлення приховуваного сигналу.

Підхід заснований на додаванні приховуваного сигналу і сигналу, що є функцією приховуваного сигналу і маскуючого сигналу, який відрізняється тим, що, з метою збільшення скритності і точності відновлення приховуваного сигналу, формується стегоконтейнер, який містить дві компоненти: перший сигнал дорівнює половині приховуваного сигналу, і другий сигнал дорівнює різниці значення першого ключа і першого сигналу.

Для відновлення прихованого сигналу визначаються чотири коефіцієнта, перший коефіцієнт дорівнює подвоєній сумі значень першого і третього ключів, другий коефіцієнт дорівнює подвоєному значенню другого ключа, третій коефіцієнт дорівнює подвоєному добутку значень першого і другого ключів, четвертий коефіцієнт дорівнює сумі значень другого і третього ключів. Відліки прихованого сигналу знаходять, складаючи третій коефіцієнт з

добутком першої компоненти контейнера на перший коефіцієнт і віднімаючи добуток другої компоненти контейнера на другий коефіцієнт, отриманий результат ділять на суму першої та другої компоненти контейнера і четвертого коефіцієнта.

Запропонований підхід до організації прихованої стеганографічної передачі інформації з маскуванням корисного сигналу дозволяє маскувати корисний сигнал в довільному шумовому сигналі при співвідношенні сигнал / шум менше 0,1 і відновлювати приймаючою стороною приховану інформацію у повному обсязі.

Запропонований підхід відноситься області способів і пристроїв стеганографічного перетворення даних і може бути використаний в зв'язкових, обчислювальних і інформаційних системах для стеганографічного приховування інформації при обміні даними урядовими, правоохоронними, оборонними, банківськими і промисловими установами, коли виникає необхідність зберігання та передачі конфіденційної інформації.

Оцінка ефективності запропонованого підходу до організації прихованої стеганографічної передачі інформації з маскуванням корисного сигналу була проведена шляхом моделювання в середовищі Matlab / Simulink.

Встановлено, що запропонований підхід до організації прихованої стеганографічної передачі інформації з маскуванням корисного сигналу дозволяє ефективно маскувати приховуваний сигнал в більш інтенсивному сигналі і передавати його по лінії зв'язку з подальшим відновленням.

3 ЕКОНОМІЧНА ЧАСТИНА

Запропонований підхід до організації прихованої стеганографічної передачі інформації з маскуванням корисного сигналу відноситься до комп'ютерної техніки, а саме до способу стеганографічного перетворення даних. Збільшення скритності і точності відновлення приховуваного сигналу потребує економічного обґрунтування, що є метою даного розділу, досягнення якої потребує визначення величини капітальних витрат на розробку запропонованого підходу та експлуатаційних витрат на його реалізацію, економічного ефекту від впровадження запропонованого підходу та розрахунку показників економічної ефективності, зокрема коефіцієнту повернення інвестицій та періоду окупності.

3.1 Розрахунок (фіксованих) капітальних витрат

До капітальних витрат належать витрати на розробку заходів із забезпечення інформаційної безпеки, а також витрати на придбання матеріальних та нематеріальних активів.

Витрати на впровадження системи захисту інформації на підприємстві визначаються, виходячи з трудомісткості кожної операції, та належать до капітальних витрат.

Визначення трудомісткості розробки підходу щодо формування прихованого каналу передачі інформації з використанням комп'ютерної стеганографії

Трудомісткість розробки системи захисту інформації на підприємстві визначається тривалістю кожної робочої операції, до яких належать наступні :

де $t_{тз}$ – тривалість складання технічного завдання на розробку підходу щодо формування прихованого каналу передачі інформації з використанням комп'ютерної стеганографії, $t_{тз}=20$;

$t_в$ – тривалість аналізу існуючих інформаційних потоків організації, вивчення ТЗ, літературних джерел за темою тощо, $t_в=60$;

$t_а$ – тривалість аналізу існуючих загроз безпеки інформації, $t_а=68$;

$t_р$ – тривалість розробки підходу щодо забезпечення конфіденційності при передачі даних в волоконно-оптичній лінії зв'язку з використанням квантової криптографії, $t_м=80$;

$t_д$ – тривалість підготовки технічної документації, $t_д=18$.

Отже,

$$t = t_{тз}+ t_в+ t_а+ t_р+ t_д = 20+60+68+80+18= 246 \text{ години.}$$

Розрахунок витрат на розробку підходу щодо формування прихованого каналу передачі інформації з використанням комп'ютерної стеганографії

Витрати на розробку системи захисту інформації на підприємстві $К_{рп}$ складаються з витрат на заробітну плату спеціаліста з інформаційної безпеки $З_{зп}$ і вартості витрат машинного часу, що необхідний для розробки політики безпеки інформації $З_{мч}$.

$$К_{рп} = З_{зп} + З_{мч} .$$

$$К_{рп} = З_{зп} + З_{мч} = 42312+2204,16=44516,6 \text{ грн.}$$

$$З_{зп} = t\, З_{пр} = 246*172 = 42312 \text{ грн.}$$

де t – загальна тривалість розробки політики безпеки, годин;

$З_{іб}$ – средньогодинна заробітна плата спеціаліста з інформаційної безпеки з нарахуваннями, грн/годину.

Вартість машинного часу для розробки політики безпеки інформації на ПК визначається за формулою:

$$З_{мч}= t*С_{мч}=246*8,96=2204,16 \text{ грн.}$$

де $t_д$ – трудомісткість підготовки документації на ПК, годин;

$С_{мч}$ – вартість 1 години машинного часу ПК, грн./година.

Вартість 1 години машинного часу ПК визначається за формулою:

$$С_{мч} = 0,8 \cdot 5 \cdot 1,55 + \frac{6130 \cdot 0,4}{1920} + \frac{7100 \cdot 0,4}{1920} = 8,96 \text{ грн.}$$

Для реалізації запропонованого підходу може бути використано стандартне телекомунікаційне обладнання, яке вже наявне на підприємстві, тому капітальні витрати не виникають.

Оцінка ефективності запропонованого підходу до організації прихованої стеганографічної передачі інформації з маскуванням корисного сигналу була проведена шляхом моделювання в середовищі Matlab / Simulink. Зазначене програмне забезпечення вже використовується, тому в цьому випадку капітальні витрати не виникають.

Витрати на встановлення обладнання та налагодження системи інформаційної безпеки становитимуть 4000 грн.

Вирішення певних технічних завдань із збільшення скритності і точності відновлення приховуваного сигналу потребує залучення аутсорсингових організації, вартість послуг котрих складає 12000 грн.

Таким чином, капітальні (фіксовані) витрати на розробку засобів підвищення рівня інформаційної безпеки складуть:

$$К = К_{рп} + К_{зпз} + К_{пз} + К_{аз} + К_{навч} + К_{н} =$$

$$= 44516{,}6+12000+4000 = 60516{,}6 \text{ грн.}$$

де $К_{рп}$ – вартість розробки політики інформаційної безпеки та залучення для цього зовнішніх консультантів, тис. грн;

$К_{зпз}$ – вартість закупівель ліцензійного основного й додаткового програмного забезпечення (ПЗ), тис. грн;

$К_{пз}$ – вартість створення основного й додаткового програмного забезпечення, тис. грн;

$К_{аз}$ – вартість закупівлі апаратного забезпечення та допоміжних матеріалів, тис. грн;

$К_{навч}$ – витрати на навчання технічних фахівців і обслуговуючого персоналу,

$К_{н}$ – витрати на встановлення обладнання та налагодження системи інформаційної безпеки.

3.1.1 Розрахунок поточних витрат

Річні поточні витрати на функціонування системи інформаційної безпеки складають:

$$С = С_в + С_к + С_{ак}, \quad грн.$$

де $С_в$ - вартість відновлення й модернізації системи ($С_в = 0$);

$С_к$ - витрати на керування системою в цілому;

$С_{ак}$ - витрати, викликані активністю користувачів системи інформаційної безпеки ($С_{ак} = 0$ грн.).

Оскільки середовище Matlab/Simulink, яке застосовується для оцінки ефективності запропонованого підходу щодо прихованої стеганографічної передачі інформації з маскуванням корисного сигналу, вже використовується на підприємстві, тому додаткові витрати щодо відновлення й модернізації системи не виникають.

Витрати на керування системою інформаційної безпеки ($С_к$) складають:

$$С_к = С_н + С_а + С_з + С_{ел} + С_о + С_{тос}, \text{ грн.}$$

Витрати на навчання адміністративного персоналу й кінцевих користувачів визначаються сукупною величиною витрат на організаційні заходи, яка складає 6000 грн.

Річний фонд заробітної плати інженерно-технічного персоналу, що обслуговує систему інформаційної безпеки ($С_з$), складає:

$$С_з = З_{осн} + З_{дод}, \text{ грн.}$$

Основна заробітна плата визначається, виходячи з місячного посадового окладу, а додаткова заробітна плата – в розмірі 8-10% від основної заробітної плати.

Основна заробітна плата одного спеціаліста з інформаційної безпеки на місяць складає 16200 грн. Додаткова заробітна плата – 10% від основної заробітної плати. Виконання роботи щодо впровадження системи захисту інформації на підприємстві потребує залучення спеціаліста інформаційної безпеки на 0,2 ставки. Отже,

$С_з$ = (16200*12 + 16200*12*0,1)*0,2= 42768 грн.

Ставка ЄСВ для всіх категорій платників з 01.01.2021 р. складає 22%.

$С_{єв}$ = 42768*0,22 = 9408,96 грн.

Вартість електроенергії, що споживається апаратурою системою інформаційної безпеки протягом року ($С_{ел}$), визначається за формулою:

$$С_{ел} = Р \cdot F_р \cdot Ц_е, \text{ грн.},$$

де Р – встановлена потужність апаратури інформаційної безпеки, (Р=0,9 кВт);

$F_р$ – річний фонд робочого часу системи інформаційної безпеки ($F_р$ = 1920 год.);

$Ц_е$ – тариф на електроенергію, ($Ц_е$ = 1,55 грн./кВт за годину).

Вартість електроенергії, що споживається апаратурою системою інформаційної безпеки протягом року:

$С_{ел}$ = 0,8*5*1920*1,55 = 11904 грн.

Витрати на технічне й організаційне адміністрування та сервіс системи інформаційної безпеки визначаються у відсотках від вартості капітальних витрат – 1% ($С_{тос}$ = 60516,6*0,01=605,17 грн).

Витрати на керування системою інформаційної безпеки ($С_к$) визначаються:

$С_к$ = 6000+42768+9408,96+11904+605,17 = 70786,13 грн.

Таким чином, річні поточні витрати на функціонування системи інформаційної безпеки складають:

С =70786,13 грн.

3.2 Оцінка можливого збитку

Запропонований підхід відноситься області способів і пристроїв стеганографічного перетворення даних і може бути використаний в зв'язкових, обчислювальних і інформаційних системах для стеганографічного приховування інформації при обміні даними урядовими, правоохоронними,

оборонними, банківськими і промисловими установами, коли виникає необхідність зберігання та передачі конфіденційної інформації.

Оцінка величини можливого збитку визначатиметься для умовного підприємства, яке забезпечує відвернення певних загроз інформаційній безпеці шляхом збільшення скритності і точності відновлення приховуваного сигналу. Вартість інформації, яка підлягатиме збільшенню скритності і точності відновлення приховуваного сигналу, потенційно складає 800000 грн. Отже, можлива величина збитку (В) на рік від зазначених загроз інформаційній безпеці, становитиме:

$$B = 800000 \text{ грн.}$$

3.2.1 Загальний ефект від впровадження системи інформаційної безпеки

Загальний ефект від впровадження системи інформаційної безпеки визначається з урахуванням ризиків порушення інформаційної:

$$E = B \cdot R - C \text{ грн.},$$

де В – загальний збиток від атаки у разі перехоплення інформації, тис. грн.;

R – вірогідність успішної реалізації загрози (60%);

С – щорічні витрати на експлуатацію системи інформаційної безпеки.

Загальний ефект від впровадження системи інформаційної безпеки визначається з урахуванням ризиків порушення інформаційної безпеки:

$$E = 800000*0,6 - 70786,13 = 409213,9 \text{ грн.}$$

3.3 Визначення та аналіз показників економічної ефективності системи інформаційної безпеки

Для встановлення економічної ефективності визначають такі показники як: коефіцієнт повернення інвестицій (ROSI) та термін окупності капітальних інвестицій (T_o).

Коефіцієнт повернення інвестицій ROSI показує, скільки гривень додаткового прибутку приносить одна гривня капітальних інвестицій на впровадження системи інформаційної безпеки:

$$ROSI = \frac{E}{K}, \quad \text{частки одиниці,}$$

де E – загальний ефект від впровадження системи інформаційної безпеки грн.;

К – капітальні інвестиції за варіантами, що забезпечили цей ефект, грн.

Коефіцієнт повернення інвестицій ROSI:

$$ROSI = \frac{409213,9}{60516,6} = 6,76, \quad \text{частки одиниці,}$$

Проект визнається економічно доцільним, якщо розрахункове значення коефіцієнта повернення інвестицій перевищує величину річної депозитної ставки з урахуванням інфляції:

$$ROSI > (N_{деп} - N_{інф})/100),$$

де $N_{деп}$ – річна депозитна ставка, (5,5%);

$N_{інф}$ – річний рівень інфляції, (5%).

Розрахункове значення коефіцієнта повернення інвестицій:

$$6,76 > (5,5 - 5)/100 = 6,76 > 0,005.$$

Термін окупності капітальних інвестицій T_o показує, за скільки років капітальні інвестиції окупляться за рахунок загального ефекту від впровадження системи інформаційної безпеки:

$$T_O = \frac{K}{E} = \frac{1}{ROSI} = \frac{1}{6,76} = 0,15 \text{ років.}$$

3.4 Висновок

Виходячи із здійснених розрахунків, можна дійти висновку, що розробка підходу щодо формування прихованого каналу передачі інформації з використанням комп'ютерної стеганографії є економічно доцільною. При капітальних витратах, які складатимуть 60516,6 грн. підприємство може мати

економічний ефект величиною 409213,9 грн. Щорічні експлуатаційні витрати становлять 70786,13 грн. Коефіцієнт повернення інвестицій має значення 6,76 грн./грн., що означає 6,76 грн. економічного ефекту на 1 грн. капітальних витрат.

Величина економічного ефекту може бути значно більшою, якщо запропонований підхід буде використаний в зв'язкових, обчислювальних і інформаційних системах для стеганографічного приховування інформації при обміні даними урядовими, правоохоронними, оборонними, банківськими і промисловими установами, коли виникає необхідність зберігання та передачі конфіденційної інформації, вартість якої є дуже великою.

ВИСНОВКИ

1. В результаті аналізу принципів побудови стеганографічних методів захисту інформації, а також прихованої передачі даних встановлено, що використання тільки криптографії, без стеганографії для прихованої передачі даних може дати супротивникові інформацію про те, що щось змінилося і спровокувати його на небажані дії.

2. В результаті аналізу існуючих підходів до формування прихованого каналу передачі інформації встановлено їх недоліки. Недоліком відомого підходу до захищеної передачі інформації з використанням імпульсного кодування [31] є необхідність кодування інформації і складність її детектування. Недоліком відомого підходу-прототипу до прихованої передачі інформації із розширенням спектра [2, 32, 33] є необхідність статистичної обробки прийнятої інформації і неможливість відновлення прихованої інформації в повному обсязі, оскільки результатом роботи пристрою, що реалізує підхід-прототип, є ухвалення рішення про наявність прихованої інформації.

3. Запропоновано підхід до організації прихованої стеганографічної передачі інформації з маскуванням корисного сигналу з метою збільшення скритності і точності відновлення приховуваного сигналу. Це досягається шляхом формування стегоконтейнера, який містить дві компоненти: перший сигнал дорівнює половині приховуваного сигналу, і другий сигнал дорівнює різниці значення першого ключа і першого сигналу. Запропонований підхід дозволяє маскувати корисний сигнал в довільному шумовому сигналі при співвідношенні сигнал / шум менше 0,1 і відновлювати приймаючою стороною приховану інформацію у повному обсязі.

4. В результаті оцінки ефективності запропонованого підходу до організації прихованої стеганографічної передачі інформації з маскуванням корисного сигналу встановлено, що він дозволяє ефективно маскувати

приховуваний сигнал в більш інтенсивному сигналі і передавати його по лінії зв'язку з подальшим відновленням.

ПЕРЕЛІК ПОСИЛАНЬ

1. Конахович, Г.Ф. Компьютерная стеганография [Текст]: теория и практика / Г.Ф. Конахович, А.Ю. Пузыренко. – Киев : МК-Пресс, 2006. – 288 с.

2. Грибунин, В.Г. Цифровая стеганография [Текст] : монография / В.Г. Грибунин, И.Н. Оков, И.В. Туринцев. – М. : СОЛОН-Пресс, 2002. – 272 с.

3. Gutierrez-Cardenas J.M. Steganography and data loss prevention: an overlooked risk? // International Journal of Security and Its Applications. – 2017. – V. 11. – N 4. – P. 71-84.

4. Сергиенко, А.Б. Цифровая обработка сигналов / А.Б. Сергиенко //. - СПб.: Питер, 2005. - 604 с.

5. Karas M., Mazurczyk W., Szczypiorski K. SkyDe: a Skypebased steganographic method // International Journal of Computers, Communications & Control. – 2014. – V. 8. – N 3. – P. 432-443.

6. Janicki A., Karas M., Mazurczyk W., Szczypiorski K. YouSkyde: information hiding for Skype video traffic // Multimedia Tools and Applications. – 2016. – V. 75. – N 21. – P. 13521-13540.

7. Mazurczyk W., Wendzel S., Zander S., Houmansadr A., Szczypiorski K. Information Hiding in Communication Networks: Fundamentals, Mechanisms, Applications, and Countermeasures. – Wiley, 2016. – 296 p.

8. Dyatlov A., Castro S. Exploitation of data streams authorized by a network access control system for arbitrary data transfers: tunneling and covert channels over the http protocol. Technical Report. – Gray World, 2003. – 8 p.

9. Rowland C.H. Covert channels in the TCP/IP protocol suite // First Monday. – 1997. – V. 2. – N 5. – 15 p.

10. Lewis S., Murdoch S.J. Embedding covert channels into TCP/IP // Lecture Notes in Computer Science. – 2005. – V. 3727. – P. 247-261.

11. Berk V., Cybenko G., Giani A. Detection of covert channel encoding in network packet delays. Technical Report TR 2005-536. – Dartmouth College, 2005. – 11 p.

12. Gianvecchio S., Wang H., Wijesekera D., Jajodia S. Modelbased covert timing channels: automated modeling and evasion // Lecture Notes in Computer Science. – 2008. – V. 5230. – P. 211-230.

13. Wendzel S., Mazurczyk W., Caviglione L., Meier M. Hidden and uncontrolled – on the emergence of network steganographic threats // Proc. ISSE 2014 Securing Electronic Business Processes. – 2014. – P. 123-133.

14. Fridrich J. Applications of data hiding in digital images // Proc. 5th Int. Symposium on Signal Processing and its Applications. Brisbane, Australia, 1999. – V. 1. – 9 p.

15. Casner S., Frederick R., Jacobson V., Schulzrinne H. RFC 3550. RTP: A Transport Protocol for Real-Time Applications. Network Working Group, 2003. – 25 p.

16. Козюра В. Д., Хорошко В. О., Шелест М. Є., Ткач Ю. М., Балюнов О.О. Захист інформації в комп'ютерних системах: підручник. – Ніжин: ФОП Лук'яненко В.В., ТПК «Орхідея», 2020. – 236с.

17. Хорошко В.А. Введение в компьютерную стеганографию / В.А. Хорошко, М.Е. Шелест – К.: 2002. – 140 с.

18. Хорошко В.О. Комп'ютерна стеганографія / В.О. Хорошко, Ю.Є. Яремчук, В.В. Карпінець – Вінниця: ВНТУ, 2014. – 155 с.

19. Ленков С.В. Методы и средства защиты информации. В 2-х томах / С.В. Ленков, Д.А. Перегудов, В.А. Хорошко – К: Арий, 2008.

20. Хорошко В.О. Основи комп'ютерної стеганографії / В.О. Хорошко, О. Д. Азаров, М. Є. Шелест, Ю. Є. Яремчук – Вінниця: ВДТУ, 2003. – 143 с.

21. Шенон К. Теория связи в секретных системах. В «Работы по теории информации и кибернетике», с. 333 – 402. – М: Изд. ИЛ, 1963.

22. Перепелицын Е.Г. Нестандартные методы математической статистики и их применение к технической диагностике и анализу изображений / Е.Г. Перепелицын – М.: Омега – Л, 2006, – 312 с.

23. Основы компьютерной стеганографии / А.В. Аграновский, П.Н. Девянин, Р.А. Хади, А.В. Черемушкин. – М.: Радио и связь, 2003. – 152 с.

24. Пономарев К. И., Путилов Г. П. Стеганография: история и современные технологии. – М.: МИЭМ, 2009. – 70 с.

25. Цветков К.Ю., Ефимов С. Н., Осташов И. Т. Защита инфокоммуникационных систем и сетей специального назначения: учебное пособие. – СПб.: ВКА имени А.Ф. Можайского, 2010. – 160 с.

26. Ерунов А. А., Квасов М. Н. Распределение пропускной способности скрытого канала связи, организованного методом цифровой стеганографии // Сборник научных статей Всероссийской научно-практической конференции «Современное состояние и перспективы развития систем связи и радиотехнического обеспечения в управлении авиацией». – Воронеж: ВУНЦ ВВС «ВВА», 2015. – С. 4-5.

27. Коржик В. И., Небаева К. А. Основы стеганографии: учебно-методическое пособие по выполнению практических занятий. – СПб.: СПбГУТ, 2015. – 20 с.

28. Рябко Б.Я. Основы современной криптографии и стеганографии / Б.Я. Рябко, А.Н. Фионов. – М. : Горячая линия – Телеком, 2010. – 232 с.

29. Задірака В.К., Мельнікова С.С., Бородавка Н.В. Спектральні алгоритми комп'ютерної стенографії // Искусственный интеллект. – 2002. – № 3. – С. 532-541.

30. Бородавка Н.В., Задирака В.К. Стеганоалгоритмы на базе теоремы о свёртке // Кибернетика и системный анализ. – 2004. – № 1. – С. 139-144.

31. Патент РФ2493659. Способ защищенной передачи информации с использованием импульсного кодирования / А.И. Назимов, А.Н. Павлов. // заявл. 20.12.2011; опубл. 20.09.2013.

32. Arnold M., Kanka S. MP3 robust audio watermarking // International Watermarking Workshop. – 1999.

33. Bassia P., Pitas I., Robust audio watermarking in the time domain // Department of Informatics, University of Tressaloniki.

34. Шакурский, В.К. Алгоритм коррекции многофакторной дополнительной погрешности измерительных преобразователей / В.К. Шакурский // Приборы и системы управления. – 1996. – №7. – С. 20-23.

35. Методичні рекомендації до виконання кваліфікаційних робіт бакалаврів спеціальності 125 Кібербезпека/ Упоряд.: О.В. Герасіна, Д.С. Тимофєєв, О.В. Кручінін, Ю.А. Мілінчук – Дніпро: НТУ «ДП», 2020. – 47 с.

ДОДАТОК А. Відомість матеріалів кваліфікаційної роботи

№	**Формат**	**Найменування**	**Кількість листів**	**Примітки**
Документація				
1	А4	Реферат	3	
2	А4	Список умовних скорочень	1	
3	А4	Зміст	2	
4	А4	Вступ	2	
5	А4	Стан питання. Постановка задачі	31	
6	А4	Спеціальна частина	14	
7	А4	Економічний розділ	8	
8	А4	Висновки	2	
9	А4	Перелік посилань	4	
10	А4	Додаток А	1	
11	А4	Додаток Б	1	
12	А4	Додаток В	1	
13	А4	Додаток Г	1	

ДОДАТОК Б. Перелік документів на оптичному носії

1 Презентація Доленко.ppt

2 Диплом Доленко.doc

ДОДАТОК В. Відгук керівника економічного розділу

Керівник розділу _____ Пілова Д.П.

(підпис) (прізвище, ініціали)

ДОДАТОК Г. Відгук керівника кваліфікаційної роботи

В І Д Г У К

на кваліфікаційну роботу студента групи 125-17-2 Доленко Ю.В. на тему: «Формування прихованого каналу передачі інформації з використанням комп'ютерної стеганографії»

Пояснювальна записка складається зі вступу, трьох розділів і висновків, розташованих на 73 сторінках.

Мета роботи є актуальною, оскільки вона спрямована на збільшення скритності і точності відновлення приховуваного сигналу.

При виконанні роботи авторка продемонструвала добрий рівень теоретичних знань і практичних навичок. На основі аналізу принципів побудови стеганографічних методів захисту інформації і прихованої передачі даних, а також існуючих підходів до формування прихованого каналу передачі інформації в ній сформульовано задачі, вирішенню яких присвячений спеціальний розділ. У ньому було запропоновано підхід до організації прихованої стеганографічної передачі інформації з маскуванням корисного сигналу та оцінено його ефективність.

Практична цінність роботи полягає у тому, що запропонований підхід може бути використаний в зв'язкових, обчислювальних і інформаційних системах для стеганографічного приховування інформації.

До недоліків роботи слід віднести недостатню проробку окремих питань.

Рівень запозичень у кваліфікаційній роботі не перевищує вимог «Положення про систему виявлення та запобігання плагіату».

В цілому робота задовольняє усім вимогам, а її авторка Доленко Ю.В. заслуговує на оцінку « » та присвоєння кваліфікації «Бакалавр з кібербезпеки» за спеціальністю 125 Кібербезпека.

Керівник роботи,
к.т.н., доцент **О.В. Герасіна**