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 *Старостенко Андрій Олександрович*

академічної групи *125-17-2*

спеціальності *125 Кібербезпека*

спеціалізації[1]

за освітньо-професійною програмою *Кібербезпека*

на тему *Стеганографічне вбудовування цифрового водяного знака в завірене повідомлення*

Керівники	**Прізвище, ініціали**	**Оцінка за шкалою**		**Підпис**
		рейтинговою	**інституційною**	
кваліфікаційної роботи	к.т.н., доц. Герасіна О.В.			
розділів:				
спеціальний	ас. Мілінчук Ю.А.			
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 *Старостенко Андрій Олександрович* **академічної групи** *125-17-2*
(прізвище ім'я по-батькові) (шифр)

спеціальності *125 Кібербезпека*

за освітньо-професійною програмою *Кібербезпека*

на тему *Стеганографічне вбудовування цифрового водяного знака в завірене повідомлення*

затверджену наказом ректора НТУ «Дніпровська політехніка» від _____ № ____

Розділ	Зміст	Термін виконання
Розділ 1	Аналіз принципів вбудовування цифрових водяних знаків і атак на стеганосистеми, а також існуючих підходів до формування і перевірки завіреного цифровим водяним знаком повідомлення.	25.02.2021 – 31.03.2021
Розділ 2	Розробка підходу до формування і перевірки завіреного цифровим водяним знаком повідомлення із підвищеною захищеністю 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 _____ Старостенко А.О.
(підпис студента) (прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 77 с., 10 рис., 1 табл., 4 додатки, 36 джерел.

Об’єкт розробки – мультимедійні повідомлення.

Предмет розробки – підхід до формування і перевірки завіреного цифровим водяним знаком повідомлення.

Мета кваліфікаційної роботи – підвищення захищеності повідомлення, завіреного цифровим водяним знаком відправника, від навмисних дій зловмисника по зміні змісту повідомлення і його авторства.

Наукова новизна результатів полягає у використанні попередньо сформованої функції хешування, двійкове вихідне значення якої в рівній мірі залежить від кожного біта двійкових послідовностей чергових відліків повідомлення і кожного біта двійкової послідовності секретного ключа.

У першому розділі проаналізовано принципи вбудовування цифрових водяних знаків та атак на стеганосистеми, а також існуючі підходи до формування і перевірки завіреного цифровим водяним знаком повідомлення.

У спеціальній частині роботи запропоновано підхід до формування і перевірки завіреного цифровим водяним знаком повідомлення із підвищеною захищеністю 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.

ДВІЙКОВІ ПОСЛІДОВНОСТІ, СЕКРЕТНИЙ КЛЮЧ, КОМП’ЮТЕРНА СТЕГАНОГРАФІЯ, ФУНКЦІЯ ХЕШУВАННЯ, ЦИФРОВИЙ ВОДЯНИЙ ЗНАК, СПРАВЖНІСТЬ ПОВІДОМЛЕННЯ, ІМІТАЦІЙНЕ МОДЕЛЮВАННЯ

РЕФЕРАТ

Пояснительная записка: 77 с., 10 рис., 1 табл., 4 приложения, 36 источников.

Объект разработки – мультимедийные сообщения.

Предмет разработки – подход к формированию и проверки заверенного цифровым водяным знаком сообщение.

Цель квалификационной работы – повышение защищенности сообщения заверенного цифровым водяным знаком отправителя, от умышленных действий злоумышленника по изменению содержания сообщения и его авторства.

Научная новизна заключается в использовании предварительно сформированной функции хеширования, двоичное исходное значение которой в равной степени зависит от каждого бита двоичных последовательностей очередных отсчетов сообщения и каждого бита двоичной последовательности секретного ключа.

В первой главе проанализированы принципы встраивания цифровых водяных знаков и атак на стеганосистемы, а также существующие подходы к формированию и проверки заверенного цифровым водяным знаком сообщение.

В специальной части работы предложен подход к формированию и проверки заверенного цифровым водяным знаком сообщение с повышенной защищенностью 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.

ДВОИЧНЫЕ ПОСЛЕДОВАТЕЛЬНОСТИ, СЕКРЕТНЫЙ КЛЮЧ, КОМПЬЮТЕРНАЯ СТЕГАНОГРАФИЯ, ФУНКЦИЯ ХЕШИРОВАНИЯ, ЦИФРОВОЙ ВОДЯНОЙ ЗНАК, ПОДЛИННОСТЬ СООБЩЕНИЯ, ИМИТАЦИОННОЕ МОДЕЛИРОВАНИЕ

ABSTRACT

Explanatory note: p. 77, fig. 17, tab. 1, 4 additions, 35 sources.

The object of development is multimedia messages.

The subject of development - an approach to the formation and verification of a certified digital watermark message.

The purpose of the qualification work is to increase the security of the message, certified by the sender's digital watermark, from intentional actions of the attacker to change the content of the message and its authorship.

The scientific novelty of the results is the use of a pre-formed hashing function, the binary initial value of which depends equally on each bit of the binary sequences of the next message count and each bit of the binary sequence of the secret key.

The first section analyzes the principles of embedding digital watermarks and attacks on steganosystems, as well as existing approaches to the formation and verification of a digitally certified message.

In the special part of the work the approach to formation and check of the message certified by a digital watermark with the increased protection 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.

BINARY SEQUENCES, SECRET KEY, COMPUTER STEGANOGRAPHY, HASHING FUNCTION, DIGITAL WATERMARK, AUTHENTICITY OF MESSAGE, SIMULATION MODELING

СПИСОК УМОВНИХ СКОРОЧЕНЬ

ДКП – Дискретне косинусне перетворення;

ДП – Двійкова послідовність;

ЕЦП – Електронний цифровий підпис;

ІКМ – Імпульсно-кодова модуляція;

ПІН – Персональний ідентифікаційний номер;

ПВП – Псевдовипадкова послідовність;

СК – Секретний ключ;

ЦВЗ – Цифровий водяний знак;

DES – Data Encryption Standard – Алгоритм симетричного шифрування даних;

LSB – Least Significant Bit – Молодший значущий біт.

ЗМІСТ

ВСТУП

Наразі існує досить великий обсяг цифрових даних: фото, відео, документи, які використовуються в нашому житті, господарської діяльності, що вимагають негайного захисту від несанкціонованого копіювання та нелегального використання. Дуже актуальним є питання захисту авторських прав і інтелектуальної власності, яка представлена в цифровому вигляді і яка передається по каналах зв'язку. Зображення, відеофайли, будучи переданими по мережі, можуть зазнавати спотворення, піддаватися стиску і інший обробці.

Розділ стеганографії – цифрові водяні знаки (ЦВЗ), дають таку можливість щодо захисту інформації. Ідея технології ЦВЗ полягає в тому, щоб вбудувати невидимі «мітки» всередину файлу, що захищається, за умови збереження його високої якості, які стануть невід'ємною його частиною, стійкі до спроб видалення, і які зберігаються протягом усього життєвого циклу файлу. Реалізація цієї ідеї дозволяє вирішити широкий ряд проблем захисту інформації, переданої по мережах зв'язку [1-12].

Система ЦВЗ – система, яка за допомогою стеганографічних методів забезпечує безпечне зберігання та передачу цифрового об'єкта (сигнал, нерухоме зображення, відео, звук) в мережах зв'язку. Мультимедійне повідомлення при передачі по мережі може бути піддано стисненню (як зі втратами, так і без), можливе додавання шумів – такі спотворення (перетворення) зображення відносяться до природних. До них ЦВЗ повинен бути стійкий у першу чергу.

Перетворена відправником до цифрового вигляду мультимедійна інформація в процесі передачі і зберігання легко може бути змінена зловмисником і в зміненому вигляді передана одержувачу. Така стратегія дій зловмисника називається атакою підміни повідомлення. Також зловмисник, не чекаючи передачі законним відправником повідомлення, може заново сформувати неправдиве повідомлення і від імені відправника передати його одержувачу. Така стратегія дій зловмисника називається атакою імітації

повідомлення. Крім того, зловмисник може перехопити передане законним відправником повідомлення і замінити в ньому підпис відправника на свій, присвоївши собі право авторства даного повідомлення. Така стратегія дій зловмисника називається атакою підміни авторства повідомлення. Перераховані дії зловмисника легко реалізуються над цифровими мультимедійними повідомленнями, використовуючи загальнопоширені аудіо, відео, графічні і інші редактори. При цьому одержувач спотвореної інформації не може виявити факт спотворення її змісту і авторства. Тому для мовних, звукових, музичних, телевізійних, факсимільних і т.п. повідомлень, переданих по каналах зв'язку або записаних на різні носії (CD або DVD диски, дискети тощо) потрібно встановлювати відсутність в них навмисних спотворень і їх авторство.

Таким чином, вдосконалення підходів до формування і перевірки завірених цифровими водяними знаками повідомлень наразі є актуальною задачею.

Метою роботи є підвищення захищеності повідомлення, завіреного цифровим водяним знаком відправника, від навмисних дій зловмисника по зміні змісту повідомлення і його авторства.

Постановка задачі:

• проаналізувати принципи вбудовування цифрових водяних знаків, а також атаки на стеганосистеми;

• провести аналіз існуючих підходів до формування і перевірки завіреного цифровим водяним знаком повідомлення;

• запропонувати підхід до формування і перевірки завіреного цифровим водяним знаком повідомлення із підвищеною захищеністю;

• оцінити ефективність запропонованого підходу.

1 СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ

1.1 Цифрова стеганографія. Предмет, термінологія, області застосування

Цифрова стеганографія як наука народилася буквально в останні роки [1]. Вона включає в себе наступні напрямки:

1) вбудовування інформації з метою її прихованої передачі;

2) вбудовування цифрових водяних знаків (ЦВЗ) (watermarking);

3) вбудовування ідентифікаційних номерів (fingerprinting);

4) вбудовування заголовків (captioning).

ЦВЗ можуть застосовуватися, в основному, для захисту від копіювання та несанкціонованого використання. У зв'язку з бурхливим розвитком технологій мультимедіа гостро постало питання захисту авторських прав та інтелектуальної власності, представленої в цифровому вигляді. Прикладами можуть бути фотографії, аудіо і відеозаписи і так далі. Переваги, які дають представлення і передача повідомлень в цифровому вигляді, можуть виявитися зовсім не такими, оскільки досить легко можливо їх злодійство або модифікація. Тому розробляються різні заходи захисту інформації, організаційного і технічного характеру. Один з найбільш ефективних технічних засобів захисту мультимедійної інформації і полягає у встановленні в об'єкт, що захищається невидимих міток – ЦВЗ. Розробки в цій галузі ведуть найбільші фірми в усьому світі. Оскільки методи ЦВЗ почали розроблятися зовсім недавно (однією з першою була робота [2]), то тут є багато незрозумілих проблем, які вимагають свого вирішення.

Назву цей метод отримав від всім відомого способу захисту цінних паперів, у тому числі і грошей, від підробки. Термін «digital watermarking» був вперше застосований в роботі [3]. На відміну від звичайних водяних знаків ЦВЗ можуть бути не тільки видимими, але й (як правило) невидимими. Невидимі ЦВЗ аналізуються спеціальним декодером, який виносить рішення про їх коректності. ЦВЗ можуть містити деякий автентичний код, інформацію про

власника, або будь-яку керуючу інформацію. Найбільш придатними об'єктами захисту за допомогою ЦВЗ є нерухомі зображення, файли аудіо і відео даних.

Технологія вбудовування ідентифікаційних номерів виробників має багато спільного із технологією ЦВЗ. Відмінність полягає у тому, що в першому випадку кожна захищена копія має свій унікальний вбудований номер (звідси і назва – дослівно «відбитки пальців»). Цей ідентифікаційний номер дозволяє виробникові відстежувати подальшу долю свого дітища: чи не зайнявся хтось із покупців незаконним тиражуванням. Якщо так, то «відбитки пальців» швидко вкажуть на винного.

Вбудовування заголовків (невидиме) може застосовуватися, наприклад, для підпису медичних знімків, нанесення легенди на карту тощо. Метою є зберігання різнорідно представленої інформації в єдине ціле. Це, мабуть, єдиний додаток стеганографії, де в явному вигляді відсутній потенційний порушник.

Оскільки цифрова стеганографія є молодою наукою, то її термінологія не до кінця усталилась [1]. Основні поняття стеганографії були узгоджені на першій міжнародній конференції по прихованню даних [4]. Проте, навіть саме поняття «стеганографія» трактується по-різному. Так, деякі дослідники розуміють під стеганографією тільки приховану передачу інформації. Інші відносять до стеганографії такі додатки як, наприклад, метеорний радіозв'язок, радіозв'язок з псевдовипадковою перебудовою радіочастоти, широкосмуговий радіозв'язок. Але в більшості літератури є наступне визначення того, що таке цифрова стеганографія – це наука про непомітне і надійне приховування одних бітових послідовностей в інших, що мають аналогову природу. Під це визначення якраз підпадають всі чотири вищенаведених напрямки приховування даних, а додатки радіозв'язку – ні. Крім того, у визначенні міститься дві головні вимоги до стеганографічного перетворення: непомітність і надійність, або стійкість до різного роду спотворень. Згадка про аналогове природе цифрових даних підкреслює той факт, що вбудовування інформації виконується в оцифровані безперервні сигнали. Таким чином, в рамках

цифрової стеганографії не розглядаються питання впровадження даних в заголовки IP-пакетів і файлів різних форматів, в текстові повідомлення [1].

Найбільш істотна відмінність постановки завдання прихованої передачі даних від постановки завдання вбудовування ЦВЗ полягає у тому, що в першому випадку порушник повинен виявити приховане повідомлення, тоді як у другому випадку про його існування всі знають. Більш того, у порушника на законних підставах може бути пристрій виявлення ЦВЗ (наприклад, у складі DVD-програвача).

Слово «непомітному» передбачає обов'язкове включення людини в систему стеганографічної передачі даних. Людина тут може розглядатися як додатковий приймач даних, висуваючи до системи передачі досить важко формалізовані вимоги.

Задачу вбудовування та виділення повідомлень з іншої інформації виконує стегосистема. Стегосистема складається з наступних основних елементів, представлених на рис.1.1:

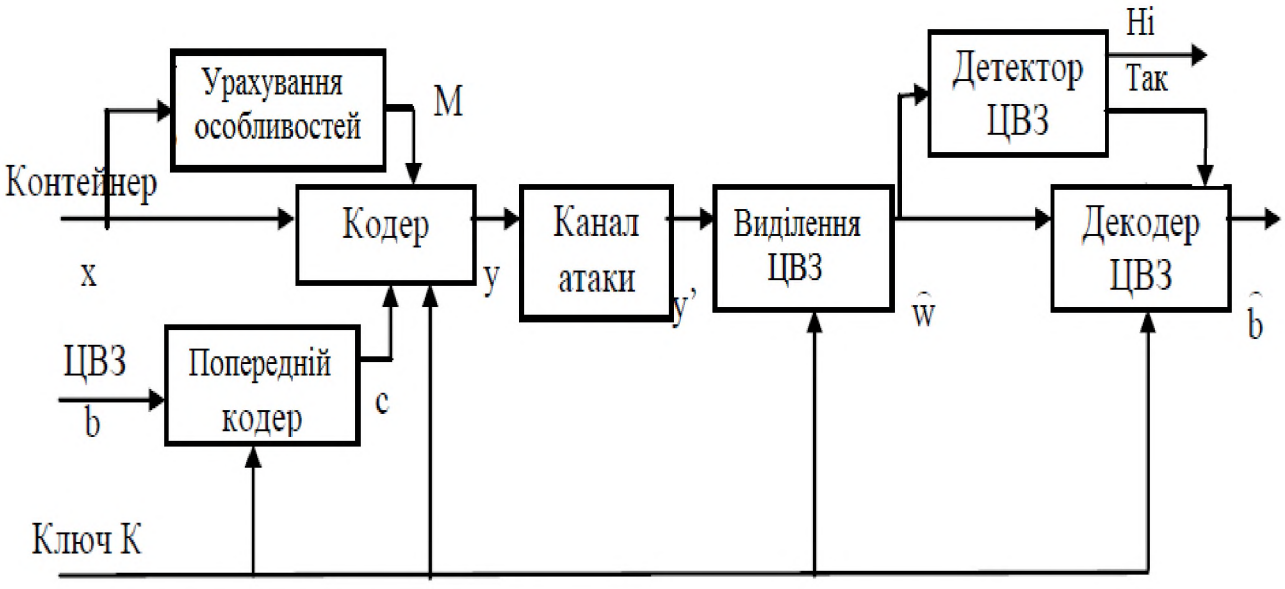

Рисунок 1.1 – Структурна схема типової стегосистеми ЦВЗ

- прекодер – пристрій, призначений для перетворення приховуваного повідомлення до вигляду, зручного для вбудовування в сигнал-контейнер

(контейнером називається інформаційна послідовність, в якій ховається повідомлення);

- стегокодер – пристрій, призначений для здійснення вкладення прихованого повідомлення в інші дані з урахуванням їх моделі;

- пристрій виділення вбудованого повідомлення;

- стегодетектор – пристрій, призначений для визначення наявності стегоповідомлення;

- декодер – пристрій, що відновлює приховане повідомлення, цей вузол може бути відсутнім.

Як показано на рис.1.1, в стегосистеми відбувається об'єднання двох типів інформації таким чином, щоб вони могли бути помітні двома принципово різними детекторами. В якості одного з детекторів виступає система виділення ЦВЗ, як іншого – людина.

Перш, ніж здійснити вкладення ЦВЗ в контейнер, ЦВЗ повинен бути перетворений до деякому відповідному вигляду. Наприклад, якщо в якості контейнера виступає зображення, то й послідовність ЦВЗ часто представляється як двовимірний масив біт. Для того, щоб підвищити стійкість ЦВЗ до спотворень нерідко виконують його завадостійке кодування, або застосовують широкосмугові сигнали. Первісну обробку прихованого повідомлення виконує показаний на рис.1.1 прекодер. Як найважливіша попередньа обробка ЦВЗ (а також і контейнера) є обчислення його узагальненого перетворення Фур'є. Це дозволяє здійснити вбудовування ЦВЗ в спектральної області, що значно підвищує його стійкість до спотворень. Попередня обробка часто виконується з використанням ключа K для підвищення секретності вбудовування. Далі ЦВЗ «вкладається» в контейнер, наприклад, шляхом модифікації молодших значущих біт коефіцієнтів. Цей процес можливий завдяки особливостям системи сприйняття людини. Добре відомо, що зображення мають велику псіховізуальну надмірність. Око людини подібне до низькочастотного фільтру, що пропускає дрібні деталі. Особливо непомітні спотворення в високочастотній області зображень. Ці особливості

людського зору використовуються, наприклад, при розробці алгоритмів стиснення зображень і відео.

Процес впровадження ЦВЗ також повинен враховувати властивості системи сприйняття людини. Стеганографія використовує наявну в сигналах психовізуальну надмірність, але іншим, ніж при стисканні даних чином. Так, розглянемо півтонування з 256 градаціями сірого, тобто з питомою швидкістю кодування 8 біт/піксель. Добре відомо, що око людини не здатне помітити зміну молодшого значущого біта. Ще в 1989 р. було отримано патент на спосіб прихованого вкладення інформації в зображення шляхом модифікації молодшого значущого біта. В даному випадку детектор стего аналізує тільки значення цього біта для кожного пікселя, а очі людини, навпаки, сприймають тільки старші 7 біт. Даний метод простий у реалізації і ефективний, але не задовольняє деяким важливим вимогам до ЦВЗ, як буде показано далі.

У більшості стегосистем для впровадження і виділення ЦВЗ використовується ключ. Ключ може бути призначений для вузького кола осіб або ж бути загальнодоступним. Наприклад, ключ повинен міститися у всіх DVD-плеєрах, щоб вони могли прочитати ЦВЗ, що містяться на дисках. Іноді за аналогією з криптографією стегосистеми ділять на два класи: з відкритим ключем і з секретним ключем. Ця аналогія не зовсім вірна, оскільки поняття відкритого ключа в даному випадку в корні різне. Правильним виразом було б «загальнодоступний ключ», причому ключ вбудовування збігається з ключем виділення. Взагалі не існує стегосистеми, в якій би при виділенні ЦВЗ була потрібна інша інформація, ніж при його вкладенні. Хоча й не доведена гіпотеза про неможливість існування подібної системи. В системі із загальнодоступним ключем досить складно протистояти можливим атакам з боку зловмисників. Справді, в даному випадку порушнику точно відомий ключ і розташування ЦВЗ, а також його значення.

У стегодетекторе відбувається виявлення ЦВЗ в (можливо зміненому) захищеному ЦВЗ зображенні. Ця зміна може бути обумовлена впливом похибок в каналі зв'язку, операцій обробки сигналу, навмисних атак

порушників. У багатьох моделях стегосистем сигнал-контейнер розглядається як адитивний шум [5]. Тоді задача виявлення і виділення стегоповідомлення є класичною для теорії зв'язку. Однак такий підхід не враховує двох факторів: невипадкового характеру сигналу контейнера і вимог по збереженню його якості. Ці моменти не зустрічаються в відомої теорії виявлення і виділення сигналів на фоні адитивного шуму. Їх облік дозволить побудувати більш ефективні стегосистеми.

Розрізняють стегодетектори, призначені для виявлення факту наявності ЦВЗ і пристрої, призначені для виділення цього ЦВЗ (стегодекодери). У першому випадку можливі детектори з жорсткими (так / ні) або м'якими рішеннями. Для винесення рішення про наявність або відсутність ЦВЗ зручно використовувати такі заходи, як відстань за Хемінгом, або взаємну кореляцію між наявними сигналами і оригіналом (при наявності останнього, зрозуміло). А що робити в ситуації, якщо немає вихідного сигналу? Тоді в справу вступають більш тонкі статистичні методи, які засновані на побудові моделей досліджуваного класу сигналів.

Залежно від того, яка інформація потрібна детектору для виявлення ЦВЗ, стегосистеми ЦВЗ діляться на три класи: відкриті, напівзакриті і закриті системи. Ця класифікація приведена в табл.1.1.

Таблиця 1.1 – Класифікація систем вбудовування ЦВЗ

		Що потрібно детектору		Вихід детектора	
Закриті	Тип I	+	+	+	-
	Тип II	+	-	-	+
Напівзакриті		-	+	+	-
Відкриті		-	-	-	+

Найбільше застосування можуть мати відкриті стегосистеми ЦВЗ, які аналогічні системам прихованої передачі даних. Найбільшу стійкість по відношенню до зовнішніх впливів мають закриті стегосистеми I типу.

Розглянемо докладніше поняття контейнера. До стегокодера – це порожній контейнер, після нього – заповнений контейнер, або стего. Стего повинен візуально не відрізнятися від порожнього контейнера. Розрізняють два основних типи контейнерів: потоковий і фіксований.

Потоковий контейнер являє собою безперервно наступну послідовність біт. Повідомлення вкладається в нього в реальному масштабі часу, так що в кодері невідомо заздалегідь, чи вистачить розмірів контейнера для передачі всього повідомлення. В один контейнер великого розміру може бути вбудовано й декілька повідомлень. Інтервали між вбудованими бітами визначаються генератором псевдовипадкової послідовності (ПВП) з рівномірним розподілом інтервалів між відліками. Основна складність полягає в здійсненні синхронізації, визначенні початку і кінця послідовності. Якщо в даних контейнера є біти синхронізації, заголовки пакетів і так далі, то прихована інформація може йти відразу після них. Труднощі забезпечення синхронізації перетворюються на переваги з точки зору забезпечення скритності передачі. Крім того, потоковий контейнер має велике практичне значення (наприклад, стегоприставка до звичайного телефону). Під прикриттям звичайного, незначущого телефонної розмови можна було б передавати іншу розмову, дані і тому подібне, і не знаючи секретного ключа не можна було б не тільки дізнатися зміст прихованої передачі, але й сам факт її існування. Не випадково, що робіт, присвячених розробці стегосистем з потоковим контейнером практично не зустрічається.

У фіксованого контейнера розміри і характеристики заздалегідь відомі. Це дозволяє здійснювати вкладення даних оптимальним в деякому сенсі чином.

Контейнер може бути обраним, випадковим або нав'язаним. Обраний контейнер залежить від вбудованого повідомлення, а в граничному випадку є його функцією. Цей тип контейнера більше характерний для стеганографії.

Нав'язаний контейнер може з'явитися в сценарії, коли особа, яка надає контейнер, підозрює про можливе приховане листування і бажає запобігти йому. На практиці ж найчастіше стикаються з випадковим контейнером.

Вбудовування повідомлення в контейнер може проводитися за допомогою ключа, одного або декількох. Ключ – ПВП біт, породжувана генератором, що задовольняє певним вимогам (криптографічно безпечний генератор). В якості основи генератора може використовуватися, наприклад, лінійний рекурентний регістр. Тоді адресатам для забезпечення зв'язку може повідомлятися початкове заповнення цього регістра. Числа, що породжуються генератором ПВП, можуть визначати позиції відліків, що модифікуються, в разі фіксованого контейнера або інтервали між ними в разі потокового контейнера. Треба відзначити, що метод випадкового вибору величини інтервалу між вбудованими бітами не дуже хороший. Причин цього дві. По-перше, приховані дані повинні бути розподілені по всьому зображенню. Тому, рівномірний розподіл довжин інтервалів (від найменшого до найбільшого) може бути досягнуто лише приблизно, оскільки необхідно бути впевненими в тому, що все повідомлення вбудовано, тобто «помістилося» в контейнер. По-друге, довжини інтервалів між відліками шуму розподілені не за рівномірним, а за експоненціальним законом. Генератор ж ПВП з експоненціально розподіленими інтервалами складний в реалізації.

Прихована інформація впроваджується відповідно до ключа в ті відліки, спотворення яких не призводить до суттєвих перекручень контейнера. Ці біти утворюють стегошлях. В залежності від програми, під істотним спотворенням можна розуміти спотворення, що призводить як до неприйнятності для людини-адресата заповненого контейнера, так і до можливості виявлення факту наявності прихованого повідомлення після стегоаналізу.

ЦВЗ можуть бути трьох типів: робасні, тендітні і напівкрихкі (semifragile). Під робастністю розуміється стійкість ЦВЗ до різного роду впливів на стего. Робастним ЦВЗ присвячено більшість досліджень.

Тендітні ЦВЗ руйнуються при незначній модифікації заповненого контейнера. Вони застосовуються для аутентифікації сигналів. Відмінність від засобів електронного цифрового підпису полягає у тому, що тендітні ЦВЗ все ж допускають деяку модифікацію контенту. Це важливо для захисту мультимедійної інформації, оскільки законний користувач може, наприклад, побажати стиснути зображення. Інша відмінність полягає у тому, що тендітні ЦВЗ повинні не тільки відобразити факт модифікації контейнера, але й також вид і місце розташування цієї зміни.

Напівкрихкі ЦВЗ стійкі по відношенню до одних впливів і нестійкі по відношенню до інших. Взагалі кажучи, всі ЦВЗ можуть бути віднесені до цього типу. Однак напівкрихкі ЦВЗ спеціально проектуються таким чином, щоб бути нестійкими по відношенню до певного роду операцій. Наприклад, вони можуть дозволяти виконувати стиснення зображення, але забороняти вирізку з нього або вставку в нього фрагмента.

На рис.1.2 представлена класифікація систем цифрової стеганографії.

Для того, щоб стегосистеми була надійною, необхідно виконання при її проектуванні ряду вимог [6-10].

1. Безпека системи повинна повністю визначатися секретністю ключа. Це означає, що порушник може повністю знати всі алгоритми роботи стегосистеми і статистичні характеристики множин повідомлень і контейнерів, і це не дасть йому ніякої додаткової інформації про наявність чи відсутність повідомлення в даному контейнері.

2. Знання порушником факту наявності повідомлення в будь-якому контейнері не повинно допомогти йому при виявленні повідомлень в інших контейнерах.

3. Заповнений контейнер повинен бути таким, що візуально не відрізняється від незаповненого. Для задоволення цієї вимоги треба, здавалося б, впроваджувати приховане повідомлення в візуально незначущі області сигналу. Однак, ці ж області використовують і алгоритми стиснення. Тому, якщо зображення буде надалі піддаватися стиску, то приховане повідомлення

може зруйнуватися. Отже, біти повинні вбудовуватися в візуально значущі області, а відносна непомітність може бути досягнута за рахунок використання спеціальних методів, наприклад, модуляції з розширенням спектра.

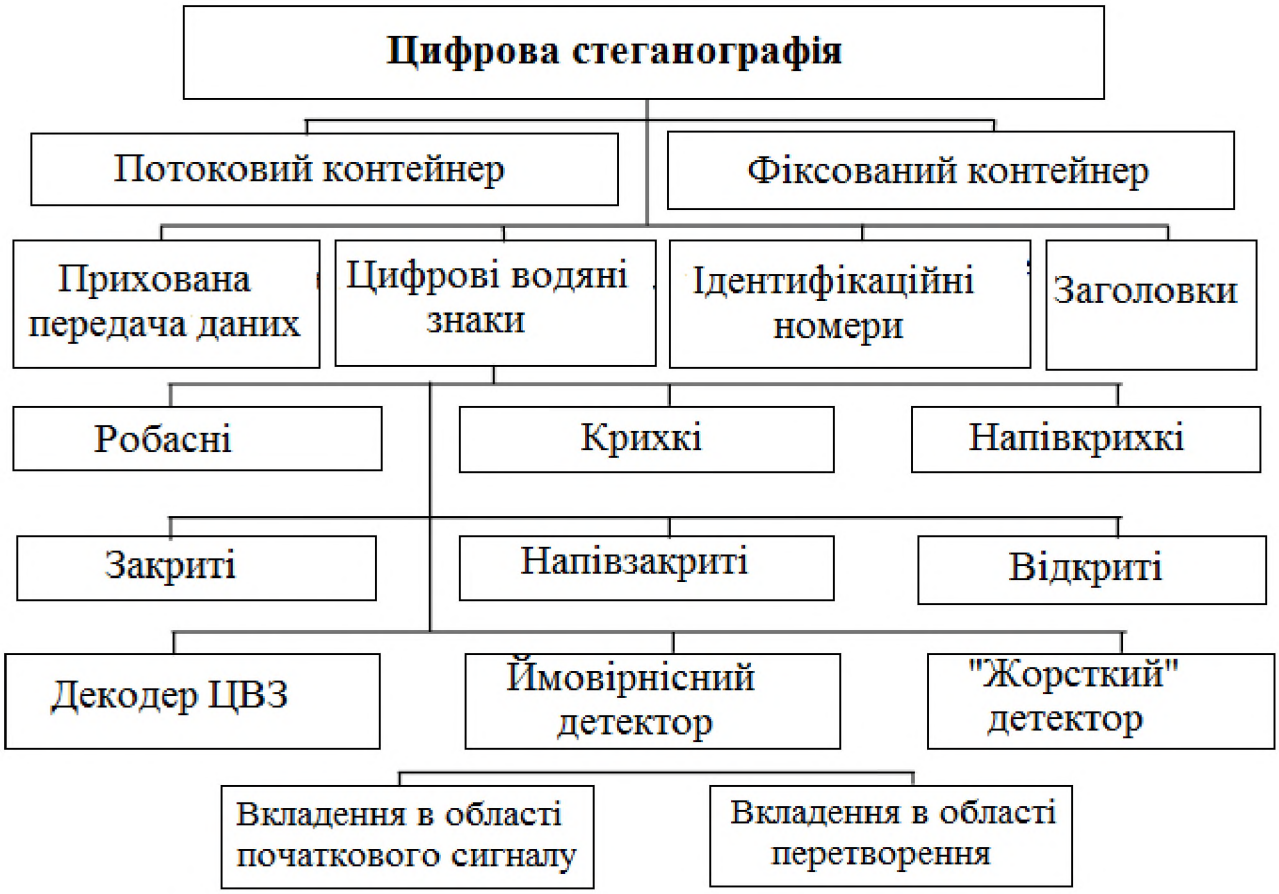

Рисунок 1.2 – Класифікація систем цифрової стеганографії

4. Стегосистеми ЦВЗ повинна мати низьку ймовірність помилкового виявлення прихованого повідомлення в сигналі, його що не містить. У деяких додатках таке виявлення може призвести до серйозних наслідків. Наприклад, помилкове виявлення ЦВЗ на DVD-диску може викликати відмову від його відтворення плеєром.

5. Повинна забезпечуватися необхідна пропускна здатність (ця вимога актуальна, в основному, для стегосистем прихованої передачі інформації).

6. Стегосистеми повинна мати прийнятну обчислювальну складність реалізації. При цьому можлива асиметрична за складністю реалізації система ЦВЗ, тобто складний стегокодер і простий стегодекодер.

До ЦВЗ ставляться наступні вимоги.

1. ЦВЗ повинен легко (обчислювально) вилучатись законним користувачем.

2. ЦВЗ повинен бути стійким або нестійким до навмисних і випадкових впливів. Якщо ЦВЗ використовується для підтвердження автентичності, то неприпустима зміна контейнера повинно призводити до руйнування ЦВЗ (крихкий ЦВЗ). Якщо ж ЦВЗ містить ідентифікаційний код, логотип фірми тощо, то він повинен зберегтися при максимальних викривленнях контейнера, звичайно, що не приводять до істотних спотворень початкового сигналу. Крім того ЦВЗ повинен бути робасним по відношенню до афінних перетворень зображення, тобто його поворотів, масштабування. При цьому треба розрізняти стійкість самого ЦВЗ і здатність декодера вірно його виявити. Скажімо, при повороті зображення ЦВЗ не зруйнується, а декодер може виявитися нездатним виділити його. Існують додатки, коли ЦВЗ повинен бути стійким по відношенню до одних перетворень і нестійким по відношенню до інших. Наприклад, може бути дозволено копіювання зображення (ксерокс, сканер), але накладена заборона на внесення в нього будь-яких змін.

3. Повинна бути можливість додавання до стего додаткових ЦВЗ. Наприклад, на DVD-диску є мітка про допустимість одноразового копіювання. Після здійснення такого копіювання необхідно додати мітку про заборону подальшого копіювання. Можна було б, звичайно, видалити перший ЦВЗ і записати на його місце другий. Однак, кращим виходом є додавання ще одного ЦВЗ, після якого перший не братиметься до уваги.

Важливою проблемою є визначення достовірності отриманої інформації, тобто її аутентифікація. Зазвичай для аутентифікації даних використовуються засоби цифрового підпису. Однак, ці засоби не зовсім підходять для забезпечення аутентифікації мультимедійної інформації. Справа у тому, що повідомлення, забезпечене електронним цифровим підписом (ЕЦП), має зберігатися і передаватися абсолютно точно, «біт в біт». Мультимедійна ж інформація може незначно спотворюватися як при зберіганні (за рахунок

стиснення), так і при передачі (вплив одиночних або пакетних похибок в каналі зв'язку). При цьому її якість залишається допустимим для користувача, але цифровий підпис працювати не буде. Одержувач не зможе відрізнити справжнє, хоча й трохи перекручене повідомлення, від помилкового. Крім того, мультимедійні дані можуть бути перетворені з одного формату в інший. При цьому традиційні засоби захисту цілісності працювати також не будуть. Можна сказати, що ЦВЗ здатні захистити саме зміст аудіо-, відеоповідомлення, а не його цифрове представлення у вигляді послідовності біт. Крім того, важливим недоліком цифрового підпису є те, що його легко видалити з завіреного ним повідомлення, після чого приробити до нього новий підпис. Видалення підпису дозволить порушнику відмовитися від авторства, або ввести в оману законного одержувача щодо авторства повідомлення. Система ЦВЗ проектується таким чином, щоб виключити можливість подібних порушень.

Як видно з рис.1.3, застосування ЦВЗ не обмежується додатками безпеки інформації. Основні галузі використання технології ЦВЗ можуть бути об'єднані в чотири групи: захист від копіювання (використання), прихована анотація документів, доказ автентичності інформації і прихований зв'язок.

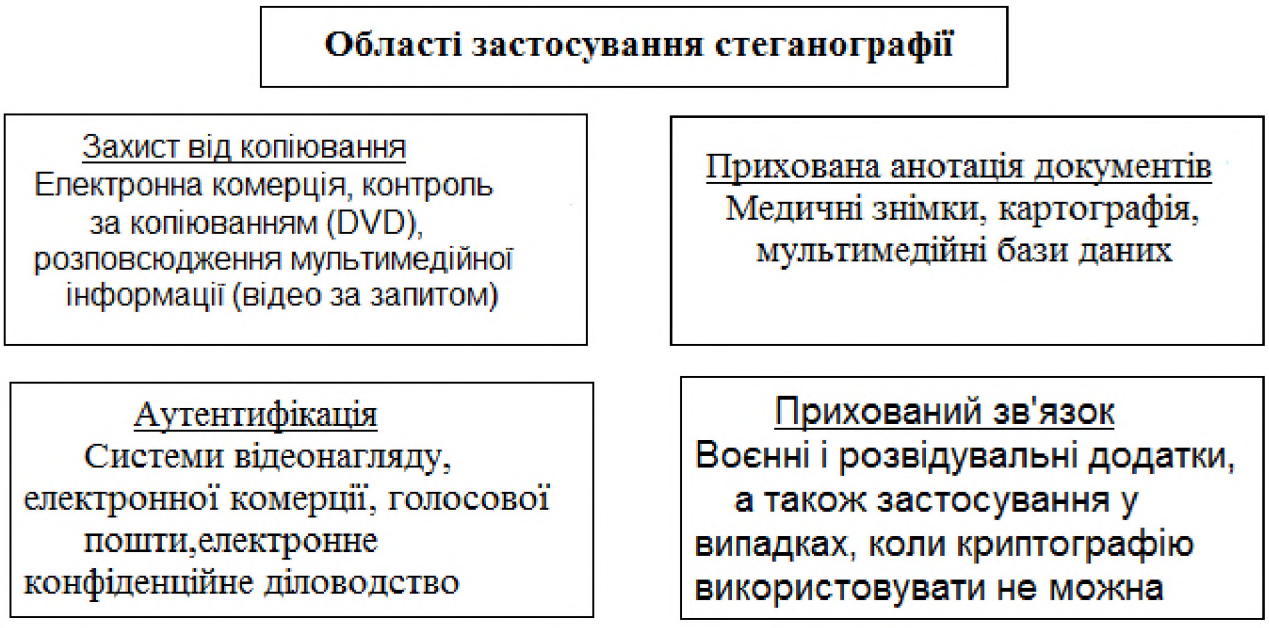

Рисунок 1.3 – Потенційні області застосування стеганографії

1.2 Вбудовування повідомлень в незначні елементи контейнера

Цифрові зображення являють собою матрицю пікселів. Піксель – це одиничний елемент зображення. Він має фіксовану розрядність двійкового представлення. Наприклад, пікселі півтонування кодуються 8 бітами (значення яскравості змінюються від 0 до 255).

Молодший значущий біт (Least Significant Bit, LSB) зображення несе в собі найменше інформації. Відомо, що людина зазвичай не здатна помітити зміну в цьому біті. Фактично, він є шумом. Тому його можна використовувати для вбудовування інформації. Таким чином, для напівтонового зображення обсяг вбудованих даних може становити 1/8 обсягу контейнера. Наприклад, в зображення розміром 512x512 можна вбудувати 32 кілобайт інформації. Якщо модифікувати два молодших біта (що також майже непомітно), то можна таємно передати вдвічі більший обсяг даних.

Переваги даного методу полягають в його простоті і порівняно великому обсязі вбудованих даних. Однак, він має серйозні недоліки. По-перше, приховане повідомлення легко зруйнувати. По-друге, не забезпечена таємність вбудовування інформації. Порушнику точно відомо місце розташування всього ЦВЗ. Для подолання останнього недоліку було запропоновано вбудовувати ЦВЗ не в усі пікселі зображення, а лише до деяких з них, що визначаються за псевдовипадковим законом відповідно до ключа, відомого тільки законному користувачеві. Пропускна здатність при цьому зменшується.

В роботі [11] відзначається невипадковий характер поведінки молодшого значущого біта зображень. Приховуване повідомлення не повинно змінювати статистики зображення. Для цього, в принципі можливо, маючи в своєму розпорядженні достатньо велику кількість незаповнених контейнерів, підшукати найбільш підходящий. Теоретично можливо знайти контейнер, що вже містить у собі наше повідомлення при цьому ключі. Тоді змінювати взагалі нічого не треба, і розкрити факт передачі буде неможливо. Цю ситуацію можна порівняти із застосуванням одноразового блокнота в криптографії. Метод

вибору підходящого контейнера вимагає виконання великої кількості обчислень і володіє малою пропускною здатністю.

Альтернативним підходом є моделювання характеристик поведінки LSB. Вбудоване повідомлення буде в цьому випадку частково або повністю залежати від контейнера. Процес моделювання є обчислювально трудомістким, крім того, його треба повторювати для кожного контейнера. Головним недоліком цього методу є те, що процес моделювання може бути повторений порушником, який можливо володіє великим обчислювальним ресурсом, що створює кращі моделі, що призведе до виявлення прихованого повідомлення. Це суперечить вимозі про незалежність безпеки стегосистеми від обчислювальної потужності сторін. Крім того, для забезпечення скритності, необхідно тримати використовувану модель шуму в таємниці. А порушнику невідомий повинен бути лише ключ.

В силу зазначених труднощів на практиці зазвичай обмежуються пошуком пікселів, модифікація яких не вносить помітних спотворень в зображення. Потім з цих пікселів відповідно до ключа вибираються ті, які будуть модифікуватися. Приховуване повідомлення шифрується із застосуванням іншого ключа. Цей етап може бути доповнений попередньою компресією для зменшення обсягу повідомлення.

1.3 Атаки на стеганосистеми

1.3.1 Атаки проти систем прихованої передачі повідомлень. Атаки на системи ЦВЗ

Зловмисник може бути пасивним, активним і злочинним. Залежно від цього він може створювати різні загрози [12-14].

Пасивний зловмисник може лише виявити факт наявності стегаканалу й, можливо, читати повідомлення. Діапазон дій активного зловмисника значно ширше. Сховане повідомлення може бути їм вилучено або зруйновано. Дії

злочинного зловмисника найнебезпечніші. Він здатний не тільки руйнувати, але й створювати помилкові стеги. Історія протистояння розвідки й контррозвідки знає чимало прикладів, коли реалізація цієї загрози приводила до катастрофічних наслідків. Ця загроза актуальна й стосовно систем ЦВЗ. Маючи здатність створювати водяні знаки, зловмисник може створювати копії контента, що захищається, створювати помилкові оригінали й т.д. У багатьох випадках зловмисник може створювати помилкові стеги без знання ключа.

Для здійснення тієї або іншої загрози зловмисник застосовує атаки.

Найбільш проста атака – суб'єктивна. Подібна атака може бути проведена лише проти зовсім незахищених стеганосистем. Проте вона найпоширеніша на практиці, принаймні, на початковому етапі розкриття стеганосистеми. Первинний аналіз також може містити в собі такі заходи [15-19]:

- первинне сортування стега за зовнішніми ознаками;
- виділення стега з відомим алгоритмом вбудовування;
- визначення використаних стегоалгоритмів;
- перевірка достатності обсягу матеріалу для стеганоаналізу;
- перевірка можливості проведення аналізу по окремих випадках;
- аналітична розробка стегоматеріалів, розробка методів розкриття стеганосистеми;
- виділення стега з відомими алгоритмами вбудовування, але невідомими ключами.

У стегоаналізі можна виділити такі типи атак [12, 20-21]:

- атака на основі відомого заповненого контейнера;
- атака на основі відомого збудованого повідомлення;
- атака на основі обраного прихованого повідомлення;
- адаптивна атака на основі обраного прихованого повідомлення;
- атака на основі обраного заповненого контейнера;
- атака на основі відомого порожнього контейнера;
- атака на основі обраного порожнього контейнера;

- атака на основі відомої математичної моделі контейнера або його частини.

1.3.2 Класифікація атак на стеганосистеми цифрових відеознаків

ЦВЗ повинні задовольняти суперечливим вимогам візуальної (аудіо) непомітності й працездатності до основних операцій обробки сигналів. Надалі без втрати спільності будемо припускати, що як контейнер використовується зображення.

Звернемося знову до системи вбудовування повідомлень шляхом модифікації молодшого значущого біта (LSB) пікселів, розглянутої в розділі 1.2. Практично будь-який спосіб обробки зображень може привести до руйнування значної частини убудованого повідомлення. Наприклад, розглянемо операцію обчислення ковзного середнього по двох сусіднім пік селам (a+b)/2, що є найпростішим прикладом низькочастотної фільтрації. Нехай значення пікселів a і b можуть бути парними або непарними з ймовірністю p=1/2. Тоді й значення молодшого значущого біта зміниться після усереднення в половині випадків. До того ж ефекту може привести й зміна шкали квантування, скажемо, з 8 до 7 бітів. Аналогічний вплив робить і стиск зображень із втратами. Більше того, застосування методів очищення сигналів від шумів, що використовують оцінювання й вирахування шуму, приведе до перекручування переважної більшості бітів прихованого повідомлення.

Існують також і набагато більш згубні для цифрових відеознаків (ЦВДЗ) операції обробки зображень, наприклад, масштабування, повороти, усікання, перестановка пікселів. Ситуація збільшується ще й тим, що перетворення стегоповідомлення можуть здійснюватися не тільки зловмисником, але й законним користувачем, або бути наслідком помилок при передачі по каналу зв'язку.

Зрушення на трохи пікселів може привести до невиявлення ЦВДЗ у детекторі. У детекторі маємо

$$S_{W_S} \cdot W = (S_{0S} + W_S) \cdot W = S_{0S} \cdot W + W_S \cdot W, \quad (1.1)$$

де індексом S позначені зміщені версії відповідних сигналів.

Добуток $S_{W_S} \cdot W$, як і колись, близький до нуля. Однак, якщо знаки у W вибиралися випадково й незалежно, то й $W_S \cdot W$ буде близьким до нуля, і стегоповідомлення не буде виявлено.

Можлива різна класифікація атак на стеганосистеми. Виділяють наступні атаки, специфічні для систем ЦВДЗ [12, 22-25]:

1. Атаки проти збудованого повідомлення – спрямовані на видалення або псування ЦВДЗ шляхом маніпулювання стега. Вхідні в цю категорію методи атак не намагаються оцінити й виділити водяний знак. Прикладами таких атак можуть бути лінійна фільтрація, стиск зображень, додавання шуму, вирівнювання гістограми, зміна контрастності тощо.

2. Атаки проти стегадетектора – спрямовані на те, щоб утруднити або унеможливити правильну роботу детектора. При цьому водяний знак у зображенні залишається, але губиться можливість його прийому. У цю категорію входять такі атаки, як афінні перетворення (тобто масштабування, зсуви, повороти), усікання зображення, перестановка пікселів тощо.

3. Атаки проти протоколу використання ЦВДЗ – в основному пов'язані зі створенням помилкових ЦВДЗ, помилкових стегів, інверсією ЦВДЗ, додаванням декількох ЦВДЗ.

4. Атаки проти самого ЦВДЗ – спрямовані на оцінювання й витягнення ЦВДЗ зі стегаповідомлення, по можливості без перекручування контейнера. У цю групу входять такі атаки, як атаки змови, статистичного усереднення, методи очищення сигналів від шумів, деякі види нелінійної фільтрації та інші.

Треба відмітити, що розглянута класифікація атак не є єдино можливою й повною. Крім того, деякі атаки (наприклад, видалення шуму) можуть бути віднесені до декількох категорій.

Відповідно до цієї класифікації всі атаки на системи вбудовування ЦВДЗ можуть бути розділені на чотири групи:

1) атаки, спрямовані на видалення ЦВДЗ;

2) геометричні атаки, спрямовані на перекручування контейнера;

3) криптографічні атаки;

4) атаки проти використовуваного протоколу вбудовування й перевірки ЦВДЗ.

1.4 Існуючі підходи до формування і перевірки завіреного цифровим водяним знаком повідомлення

Відомі способи встановлення справжності мультимедійних повідомлень, записаних на аудіо- або відеокасети, CD диски та дискети. Ці способи використовують унікальні технологічні ознаки носіїв. Наприклад, справжність повідомлення встановлюється, якщо пристрій зчитування виявляє на диску-носії повідомлень, що захищаються, в необхідному місці мітку у вигляді збійного сектора. Відомі способи встановлення автентичності мультимедійних повідомлень, записаних на аудіо- або відеокасети, CD диски та дискети [26]. Однак встановлення автентичності повідомлень на основі використання унікальних технологічних ознак носіїв цих повідомлень принципово не здатне встановити відсутність в цих повідомленнях навмисних спотворень і їх авторство при їх перезапису з носіїв, що володіють унікальними технологічними ознаками, на носії, які цих ознак не мають.

Тому способи встановлення справжності мультимедійних повідомлень доцільно будувати на основі вбудовування в самі повідомлення інформації їх аутентифікації, не використовуючи будь-яку прив'язку до унікальних технологічних або інших ознак носіїв цих повідомлень. Такі способи в останні роки розробляються в рамках стеганографічних методів захисту інформації і отримали назву способів формування і перевірки завіреного цифровим водяним знаком повідомлення. Ці способи описані, наприклад, в [1]. Основна ідея цих способів полягає у вбудовуванні в мультимедійне повідомлення спеціальної ЦВЗ відправника (автора) повідомлення з використанням секретного ключа. Даний ЦВЗ є унікальним ідентифікатором відправника і однозначно

ідентифікує відправника повідомлення при добуванні одержувачем цього ЦВЗ з отриманого повідомлення із використанням секретного ключа. Факт вилучення цього ЦВЗ з отриманого повідомлення із використанням секретного ключа також дозволяє одержувачеві переконатися, що зміст завіреного даним водяним знаком повідомлення не змінено і не сформовано в результаті злочинних дій. ЦВЗ повідомлень можуть бути такими, що візуально сприймаються, наприклад, зображення зареєстрованого товарного знака фірми-виробника або зображення особи відправника, і такими, що візуально не сприймаються, наприклад, двійкова послідовність (ДП), зареєстрована як персональний ідентифікаційний номер (ПІН) відправника мультимедійних повідомлень.

Вбудовування в мультимедійне повідомлення, що завіряється, ЦВЗ відправника можливо при використанні секретного ключа, невідомого потенційному зловмиснику. На етапі перевірки з прийнятого мультимедійного повідомлення з використанням цього ж секретного ключа витягується цифровий водяний знак, який звіряється з цифровим водяним знаком відправника повідомлень, і при їх збізі виноситься рішення про авторство даного повідомлення і відсутності в ньому спотворень. Зловмисник, якому відомий ЦВЗ відправника повідомлення, але невідомий його секретний ключ, не здатний сформувати мультимедійне повідомлення, завірене ЦВЗ даного відправника, яке при перевірці одержувач визнає справжнім.

Відомий підхід до стегоаналізу зображень, створених за допомогою сучасного стеганографічного програмного забезпечення [27]. Він полягає в попередньому формуванні для відправника і одержувача ДП ЦВЗ довжиною 64 біта. Двійкова послідовність ЦВЗ є однією і тією ж для будь-яких мультимедійних повідомлень, що завіряються відправником. Для завірення у відправника повідомлення, починаючи з першого відліку, чергові відліки повідомлення зчитують в черговий блок відліків довжиною 64 відліки. Черговий блок відліків перетворюють способом дискретного косинусного перетворення (ДКП) в 64 коефіцієнта дискретного косинусного перетворення. Значення коефіцієнтів округлюють до цілих значень. Починаючи з першого і до

останнього біта, зчитують і-ий біт, де і=1,2,...,64, ДП ЦВЗ. Починаючи з першого і до останнього коефіцієнта ДКП зчитують черговий коефіцієнт, в якому його найменш значущий біт замінюють на і-й біт ДП ЦВЗ, перетворене значення чергового коефіцієнта ДКП зчитують в черговий вихідний блок коефіцієнтів довжиною 64 коефіцієнта. При заповненні чергового вихідного блоку коефіцієнтів його перетворюють способом зворотного ДКП в 64 відліки чергового блоку завіреного повідомлення, який передають одержувачу. Зчитують чергові 64 відліки повідомлення і повторно зчитують ДП ЦВЗ і виконують наступні за ним дії до тих пір, поки надходять чергові відліки повідомлення.

Для перевірки справжності прийнятого одержувачем повідомлення, починаючи з першого відліку, прийняті чергові відліки повідомлення зчитують в черговий блок прийнятих відліків довжиною 64 відліки. Черговий блок прийнятих відліків перетворюють способом ДКП в 64 прийнятих коефіцієнта ДКП. Значення прийнятих коефіцієнтів округлюють до цілих значень. Починаючи з першого і до останнього біта, зчитують і-ий біт, де і=1,2,...,64, ДП ЦВЗ і, з першого і до останнього, прийнятий черговий коефіцієнт ДКП, в якому його найменш значущий біт порівнюють з і-им бітом ДП ЦВЗ. Якщо все найменш значущі біти прийнятих чергових коефіцієнтів збіглися з відповідними і-ми бітами ДП ЦВЗ, то черговий блок прийнятих відліків вважають справжнім. Потім такі прийняті відліки повідомлення зчитують в черговий блок прийнятих відліків довжиною 64 відліки, після чого повторюють дії по перевірці чергового блоку прийнятих відліків до тих пір, поки надходять прийняті чергові відліки повідомлення.

У відомому підході до стегоаналізу зображень, створених за допомогою сучасного стеганографічного програмного забезпечення [27] заміна найменш значущого біта чергових коефіцієнтів ДКП чергового блоку відліків на і-ті біти ДП ЦВЗ призводить до невеликої зміни значення чергових відліків повідомлення даного блоку. Якщо, наприклад, завірене ЦВЗ повідомлення є напівтоновим зображенням, то застосування відомого підходу до стегоаналізу

зображень, створених за допомогою сучасного стеганографічного програмного забезпечення [27] призводить до порівняно невеликих змін яскравості кожного з 64 пікселів чергового блоку зображення, що візуально малопомітно і практично не знижує якість зображення (рис. 1.4).

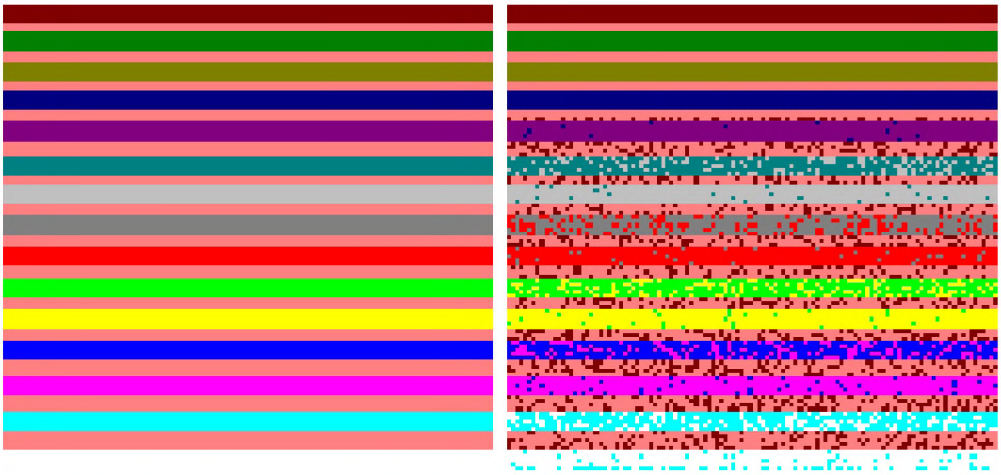

Рисунок 1.4 – Оригінальне 8-бітове зображення обкладинки (ліворуч) та 8-бітове стегозображення (праворуч), створене за згідно відомого підходу [27]

У відомому підході до стегоаналізу зображень, створених за допомогою сучасного стеганографічного програмного забезпечення [27] було визначено характеристики сучасного програмного забезпечення для стеганографії, яке здійснює стеганаліз на існування прихованого повідомлення та було представлено результати роботи S-Tools – інструменту для автоматичного виявлення прихованих повідомлень на зображеннях (рис. 1.5).

Недоліком відомого підходу до стегоаналізу зображень, створених за допомогою сучасного стеганографічного програмного забезпечення [27] є низька захищеність повідомлення, завіреного цифровим водяним знаком відправника, від навмисних дій зловмисника по зміні змісту повідомлення і його авторства.

Найбільш близьким за своєю технічною суттю до запропонованого підходу є підхід «Стеганографічний метод та пристрій» [28]. Підхід-прототип формування та перевірки завіреного цифровим водяним знаком повідомлення

полягає в попередньому формуванні для відправника і одержувача ДП мітки ЦВЗ довжиною m біт, ДП ЦВЗ довжиною k біт і ДП секретного ключа довжиною k біт. Попередньо встановлюють число збігів бітів ДП мітки ЦВЗ і число збігів бітів ДП ЦВЗ в нульове значення. Для завірення у відправника повідомлення, починаючи з першого і до m-го символу, зчитують черговий біт ДП мітки ЦВЗ і ДП чергового відліку повідомлення. У ДП чергового відліку повідомлення молодший біт замінюють на черговий біт ДП мітки ЦВЗ і перетворену ДП чергового відліку повідомлення передають одержувачу в якості завіреної. Після чого послідовно зчитують і-ий (i=1,2,...,k) біт ДП секретного ключа, і-й біт ДП ЦВЗ і ДП чергового відліку повідомлення.

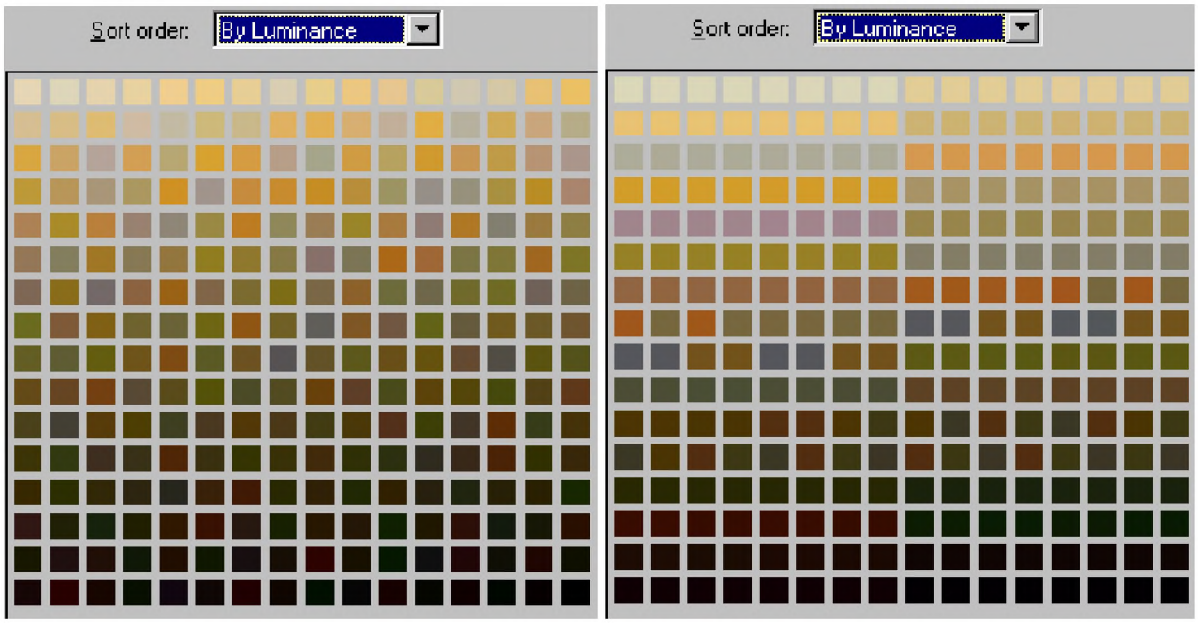

Рисунок 1.5 – Обкладинка (ліворуч) та палітра стегозображень (праворуч) після S-Tools [27]

Якщо і-й біт ДП секретного ключа приймає одиничне значення, то молодший біт ДП чергового відліку повідомлення замінюють на і-й біт ДП ЦВЗ і перетворену ДП чергового відліку повідомлення передають одержувачу в якості завіреної. Якщо і-й біт ДП секретного ключа приймає нульове значення, ДП чергового відліку повідомлення без зміни передають одержувачу в якості завіреної. Далі повторно, починаючи з першого і до m-го символу, зчитують

черговий біт ДП мітки ЦВЗ і ДП чергового відліку повідомлення і виконують наступні за ним дії до тих пір, доки надходять виконавчі послідовності чергових відліків повідомлення.

Для перевірки справжності прийнятого одержувачем повідомлення зчитують прийняту ДП чергового відліку повідомлення і, починаючи з першого і до m-го символу, черговий біт ДП мітки ЦВЗ. Молодший біт прийнятої ДП чергового відліку повідомлення порівнюють із черговим бітом ДП мітки ЦВЗ і при їх збізі число збігів бітів ДП мітки ЦВЗ збільшують на середнє арифметичне значення, інакше це число встановлюють в нульове значення і зчитують прийняту ДП чергового відліку повідомлення і повторно зчитують, починаючи з першого і до m-го символу, черговий біт ДП мітки ЦВЗ і виконують наступні за ним дії. Якщо число збігів бітів ДП мітки ЦВЗ досягло значення m, то зчитують прийняту ДП чергового відліку повідомлення, і-й біт ДП секретного ключа та і-й біт ДП ЦВЗ. Якщо і-й біт ДП секретного ключа дорівнює одиничному значенню, то молодший біт прийнятої ДП чергового відліку повідомлення порівнюють з і-м бітом ДП ЦВЗ і при їх збізі число збігів бітів ДП ЦВЗ збільшують на середнє арифметичне значення, після зчитування k-го біта ДП ЦВЗ число збігів бітів ДП ЦВЗ порівнюють з числом одиничних значень бітів ДП секретного ключа і при їх рівності прийняті виконавчі послідовності m+k чергових відліків повідомлення вважають справжніми, після чого повторюють дії по перевірці справжності чергової групи з m+k прийнятих чергових відліків повідомлення до завершення прийому всіх відліків повідомлення.

Недоліком відомого підходу «Стеганографічний метод та пристрій» (прототипу) [28] є низька захищеність повідомлення, завіреного ЦВЗ відправника, від навмисних дій зловмисника по зміні змісту повідомлення і його авторства. При навмисному зміні змісту повідомлення, завіреного ЦВЗ відправника, зловмисник може змінити будь-які біти, крім молодших бітів, довільного числа чергових відліків завіреного повідомлення. Оскільки молодші біти чергових відліків зміненого повідомлення не змінюються зловмисником,

то одержувач зміненого повідомлення, виконуючи описані дії перевірки, помилково визнає прийняте повідомлення справжнім. Тим самим зловмисник має можливість переробити повідомлення, завірене ЦВЗ відправника, в неправдиве повідомлення. Отже, відомий способ-прототип не забезпечує захищеність повідомлення, завіреного цифровим водяним знаком відправника, до атаки підміни повідомлення.

При іншій стратегії дій зловмисник, якому відома ДП ЦВЗ відправника, може сформувати неправдиве повідомлення, що складається з чергових відліків, і молодші біти ДП чергових відліків неправдивого повідомлення замінити на молодші біти ДП чергових відліків повідомлення, завіреного ЦВЗ відправника. Одержувач такого помилкового повідомлення, виконуючи описані дії перевірки, помилково визнає прийняте повідомлення справжнім. Тим самим зловмисник має можливість від імені відправника успішно нав'язувати одержувачу довільні неправдиві повідомлення. Отже, відомий способ-прототип не забезпечує захищеність повідомлення, завіреного цифровим водяним знаком відправника, до атаки імітації повідомлення.

При третій стратегії дій зловмисник може замінити молодші біти ДП чергових відліків повідомлення, завіреного ЦВЗ відправника, на чергові біти ДП своєї мітки ЦВЗ і чергові біти ДП свого ЦВЗ. При цьому зловмисник зберігає незмінними інші біти ДП чергових відліків повідомлення, тобто зміст повідомлення не змінюється. Зловмисник, як і законний відправник, може бути таким же потенційним автором повідомлень в інформаційно-телекомунікаційній системі та відповідно відомого способу попередньо для зловмисника формують унікальні ДП мітки ЦВЗ довжиною m біт, ДП ЦВЗ довжиною k біт і ДП секретного ключа довжиною k біт. Одержувач повідомлення зі зміненим авторством, виконуючи описані в у відомому способі-прототипі дії перевірки з використанням ДП мітки ЦВЗ довжиною m біт, ДП ЦВЗ довжиною k біт і ДП секретного ключа довжиною k біт зловмисника, помилково визнає автором прийнятого повідомлення зловмисника. Тим самим зловмисник здатний залишити за собою авторство

довільного повідомлення законного відправника. Отже, відомий способ-прототип не забезпечує захищеність повідомлення, завіреного ЦВЗ відправника, до атаки підміни авторства.

При всіх описаних навмисних діях зловмисника йому не потрібне знання ДП секретного ключа довжиною k біт.

Зазначений недолік відомого підходу «Стеганографічний метод та пристрій» (прототипу) [28] виник через те, що вбудована в повідомлення двійкова послідовність ЦВЗ не залежить від самого повідомлення, яке завіряється, і двійкової послідовності секретного ключа.

1.5 Висновок. Постановка задачі

В розділі проаналізовано принципи вбудовування цифрових водяних знаків, а також атаки на стеганосистеми. Встановлено, що встановлення справжності повідомлень на основі використання унікальних технологічних ознак носіїв цих повідомлень принципово не здатне встановити відсутність в цих повідомленнях навмисних спотворень і їх авторство при їх перезапису з носіїв, що володіють унікальними технологічними ознаками, на носії, які цих ознак не мають.

Тому способи встановлення справжності мультимедійних повідомлень доцільно будувати на основі вбудовування в самі повідомлення спеціального ЦВЗ відправника (автора) повідомлення з використанням секретного ключа. Даний ЦВЗ є унікальним ідентифікатором відправника і однозначно ідентифікує відправника повідомлення при добуванні одержувачем цього ЦВЗ з отриманого повідомлення із використанням секретного ключа. Факт вилучення цього ЦВЗ з отриманого повідомлення із використанням секретного ключа також дозволяє одержувачеві переконатися, що зміст завіреного даним водяним знаком повідомлення не змінено і не сформовано в результаті злочинних дій. ЦВЗ повідомлень можуть бути такими, що візуально сприймаються, наприклад, зображення зареєстрованого товарного знака фірми-виробника або зображення

особи відправника, і такими, що візуально не сприймаються, наприклад, двійкова послідовність (ДП), зареєстрована як персональний ідентифікаційний номер (ПІН) відправника мультимедійних повідомлень.

В розділі проаналізовано існуючі підходи до формування і перевірки завіреного цифровим водяним знаком повідомлення. Встановлено, що недоліком відомого підходу до стегоаналізу зображень, створених за допомогою сучасного стеганографічного програмного забезпечення [27] є низька захищеність повідомлення, завіреного цифровим водяним знаком відправника, від навмисних дій зловмисника по зміні змісту повідомлення і його авторства.

Встановлено, що недоліком відомого підходу «Стеганографічний метод та пристрій» (прототипу) [28] є низька захищеність повідомлення, завіреного ЦВЗ відправника, від навмисних дій зловмисника по зміні змісту повідомлення і його авторства. Відомий підхід-прототип не забезпечує захищеність повідомлення, завіреного цифровим водяним знаком відправника, до атаки підміни повідомлення, атаки імітації повідомлення та атаки підміни авторства.

Зазначений недолік відомого підходу «Стеганографічний метод та пристрій» (прототипу) [28] виник через те, що вбудована в повідомлення двійкова послідовність ЦВЗ не залежить від самого повідомлення, яке завіряється, і двійкової послідовності секретного ключа.

Таким чином, для усунення недоліків існуючих підходів необхідно:

• запропонувати підхід до формування і перевірки завіреного цифровим водяним знаком повідомлення із підвищеною захищеністю;

• оцінити ефективність запропонованого підходу.

2 СПЕЦІАЛЬНА ЧАСТИНА

2.1 Підхід до формування і перевірки завіреного цифровим водяним знаком повідомлення із підвищеною захищеністю

Запропонований підхід відноситься до області електрозв'язку і інформаційних технологій, а саме до техніки захисту справжності повідомлень, таких як перетворені до цифрового вигляду мовні, звукові, музичні, телевізійні, факсимільні і подібні повідомлення. Під справжнім повідомленням розуміється таке повідомлення, в якому відсутні неавторизовані зміни його змісту і ідентифікований його відправник (автор). Неавторизовані зміни змісту і авторства повідомлення може здійснювати зловмисник в процесі передачі і зберігання сформованого відправником повідомлення. Завданням одержувача повідомлення є встановлення факту, що зміст прийнятого повідомлення відповідає змісту переданого відправником повідомлення і що автором прийнятого повідомлення є саме цей відправник. Технічним результатом, що досягається при реалізації запропонованого рішення, є розробка підходу до формування і перевірки завіреного ЦВЗ повідомлення, що забезпечує підвищення захищеності повідомлення, завіреного ЦВЗ відправника, від навмисних дій зловмисника по зміні змісту повідомлення і його авторства. Технічний результат досягається тим, що попередньо для відправника і одержувача формують двійкову послідовність (ДП) цифрового водяного знаку довжиною k біт і ДП секретного ключа, завіряють у відправника повідомлення із використанням ДП ЦВЗ і секретного ключа, передають завірене повідомлення одержувачу, де перевіряють справжність прийнятого повідомлення із використанням ДП ЦВЗ і секретного ключа.

Запропонований підхід до формування і перевірки завіреного цифровим водяним знаком повідомлення із підвищеною захищеністю може бути використаний для встановлення справжності мовних, звукових, музичних,

телевізійних, факсимільних і інших мультимедійних повідомлень, переданих і збережених в сучасних інформаційно-телекомунікаційних системах.

Поставлена мета досягається тим, що у відомому підході до формування і перевірки завіреного цифровим водяним знаком повідомлення із підвищеною захищеністю, що полягає в попередньому формуванні для відправника і одержувача ДП ЦВЗ довжиною k біт і ДП секретного ключа, завіряють у відправника повідомлення із використанням ДП ЦВЗ і секретного ключа. Передають завірене повідомлення одержувачу, де перевіряють справжність прийнятого повідомлення з використанням ДП ЦВЗ і секретного ключа. Додатково попередньо для відправника і одержувача формують функцію хешування з двійковим вихідним значенням і встановлюють мінімально допустиму кількість K_{min} справжніх відліків повідомлення в групі з k послідовно прийнятих. Мінімально допустима кількість K_{min} справжніх відліків повідомлення в групі з k послідовно прийнятих встановлюють з умови

$$2^{k-K_{\min}} \geq 2^k P_{доп}, \qquad (2.1)$$

де $P_{доп}$ – допустима ймовірність прийняття справжньої групи з k чергових відліків повідомлення, яка є не справжньою.

Для завірення у відправника повідомлення послідовно зчитують і-й біт ДП ЦВЗ (i=1,2,...,k) і ДП чергового відліку повідомлення, яку хешують з використанням ДП секретного ключа за попередньо сформованою функцією хешування. Після чого порівнюють хешоване значення з і-м бітом ДП ЦВЗ і при їх збізі ДП чергового відліку повідомлення передають одержувачу в якості завіреної, а при розбіжності ДП чергового відліку повідомлення послідовно перетворюють шляхом зміни її молодших бітів. Для перетворення ДП чергового відліку повідомлення шляхом зміни її молодших бітів послідовно змінюють її один, два, три і так далі найменш значущі біти. Далі після кожного перетворення перетворену ДП чергового відліку повідомлення хешують з використанням ДП секретного ключа за попередньо сформованою функцією хешування, порівнюють хешоване значення за і-м бітом ДП ЦВЗ, причому перетворення ДП чергового відліку повідомлення виконують до збігу

хешованого значення перетвореної ДП чергового відліку повідомлення з і-м бітом ДП ЦВЗ, після чого останню перетворену ДП чергового відліку повідомлення передають одержувачу в якості завіреної. Після завірення ДП чергового відліку повідомлення з використанням k-го біта ДП ЦВЗ повторно, починаючи з першого і до k-го, зчитують і-й біт ДП ЦВЗ, і ДП чергового відліку повідомлення і виконують наступні за ним дії до тих пір, поки надходять виконавчі послідовності чергових відліків повідомлення.

У одержувача повідомлення попередньо з числа прийнятих ДП чергових відліків повідомлення виділяють відлік, що відповідає першому біту ДП ЦВЗ у відправника повідомлення. Для виділення чергового відліку повідомлення, відповідного першому біту ДП ЦВЗ у відправника повідомлення, попередньо встановлюють максимально допустиме значення ймовірності $P_{пом}$ помилкового виділення цього відліку, прийняті одержувачем ДП чергових відліків повідомлення хешують з використанням ДП секретного ключа за попередньо сформованою функцією хешування, хешовані значення порівнюють послідовно з відповідними, починаючи з першого, значеннями бітів ДП ЦВЗ до досягнення m їх збігів поспіль, де

$$m=\lfloor -\log_2 P_{пом} \rfloor, \qquad (2.2)$$

а дія $\lfloor -\log_2 P_{пом} \rfloor$ означає округлення значення $-\log_2 P_{пом}$ до найближчого цілого, причому відповідним першому біту ДП ЦВЗ у відправника повідомлення приймають перший відлік з k послідовно прийнятих ДП чергових відліків повідомлення.

Після чого для перевірки справжності прийнятого одержувачем повідомлення послідовно приймають k ДП чергових відліків повідомлення, хешують їх з використанням ДП секретного ключа за попередньо сформованою функцією хешування і кожне і-е хешоване значення порівнюють з і-м бітом ДП ЦВЗ. Обчислюють число K_c хешованих ДП чергових відліків повідомлення з k прийнятих відліків, що збіглися зі значеннями відповідних їм бітів ДП ЦВЗ, і при $K_c \geq K_{min}$ прийняті k ДП чергових відліків повідомлення вважають справжніми, після чого повторюють дії по перевірці справжності чергової

групи з k ДП чергових відліків повідомлення і так до завершення прийому всіх ДП чергових відліків повідомлення.

Зазначена нова сукупність виконуваних дій за рахунок непередбачуваної для зловмисника залежності всіх бітів ДП чергових відліків завіреного ЦВЗ повідомлення від відповідних бітів ДП ЦВЗ довжиною k біт і ДП секретного ключа дозволяє підвищити захищеність повідомлення, завіреного ЦВЗ відправника, до навмисних дій зловмисника по зміні змісту повідомлення і його авторства. Дана непередбачуваність при невідомої для зловмисника ДП секретного ключа забезпечується хешуванням ДП чергового відліку повідомлення з використанням ДП секретного ключа за попередньо сформованою функцією хешування з двійковим вихідним значенням. Попередньо сформована функція хешування з двійковим вихідним значенням для зловмисника не відрізняється від випадкової функції, тобто ймовірність правильного визначення її вихідного значення при невідомій для зловмисника ДП секретного ключа дорівнює ½, тобто дорівнює ймовірності випадкового вгадування.

Попередньо сформована функція хешування з двійковим вихідним значенням повинна відповідати наступним вимогам:

1) двійкове вихідне значення функції хешування в рівній мірі залежить від кожного біта ДП чергових відліків повідомлення і кожного біта ДП секретного ключа;

2) знаючи опис функції хешування і ДП чергових відліків завіреного повідомлення, зловмисник не здатний обчислити ДП секретного ключа;

3) знаючи опис функції хешування, зловмисник не здатний правильно сформувати вихідне значення функції хешування з ймовірністю істотно більшою ½ для ДП чергових відліків обраного повідомлення, не знаючи ДП секретного ключа.

При невідомої зловмисникові ДП секретного ключа він не може в завіреному відправником ЦВЗ повідомленні змінити чергові відліки повідомлення так, щоб одержувач зміненого повідомлення, виконуючи описані

дії перевірки, помилково визнав прийняте повідомлення справжнім. При зміні зловмисником одного чергового відліку завіреного повідомлення ймовірність того, що хешоване значення ДП зміненого зловмисником одного чергового відліку повідомлення співпаде з відповідним бітом ДП ЦВЗ, дорівнює ½. У групі з k послідовно прийнятих відліків повідомлення для визнання їх справжніми має співпасти не менше K_{min} хешованих значень ДП змінених зловмисником чергових відліків повідомлення з відповідними бітами ДП ЦВЗ. Отже, ймовірність прийняття справжньої групи з k чергових відліків повідомлення, що є не справжньою, дорівнює (2.1).

Вибором відповідного значення K_{min} можна забезпечити як завгодно малу допустиму ймовірність $P_{доп}$ при даній атаці підміни повідомлення. Наприклад, при $K_{min}=20$ ймовірність успішної атаки підміни повідомлення не перевищує однієї мільйонної: $P_{доп}\leq 2^{-20}$. Тому зазначена нова сукупність виконуваних дій дозволяє підвищити захищеність повідомлення, завіреного ЦВЗ відправника, до атаки підміни повідомлення.

Також при невідомій зловмисникові ДП секретного ключа і відомих одному або декількох повідомленнях, завірених ЦВЗ відправника, зловмисник не може заново сформувати несправжнє повідомлення, що складається з ДП чергових відліків таким чином, щоб одержувач несправжнього повідомлення, виконуючи описані дії перевірки, помилково визнав прийняте повідомлення справжнім. При формуванні зловмисником неправдивого повідомлення довжиною k чергових відліків ймовірність того, що не менше K_{min} хешованих значень ДП чергових відліків не справжнього повідомлення співпадуть з відповідними бітами ДП ЦВЗ, дорівнює $2^{-K_{min}}$. Отже, ймовірність прийняття справжньої групи з k чергових відліків повідомлення, що є не справжньою, дорівнює $2^{-K_{min}}$. Вибором відповідного значення K_{min} можна забезпечити як завгодно малу ймовірність $P_{доп}$ при розглянутій атаці імітації повідомлення. Наприклад, при $K_{min}=30$ ймовірність успішної атаки імітації повідомлення не перевищує однієї мільярдної. Тому зазначена нова сукупність виконуваних дій

дозволяє підвищити захищеність повідомлення, завіреного ЦВЗ відправника, до атаки імітації повідомлення.

Також при невідомої зловмисникові ДП секретного ключа і відомому повідомленні, завіреному ЦВЗ відправника, зловмисник не може змінити авторство цього повідомлення на своє. Нехай зловмисник, як і відправник, є таким же потенційним автором повідомлень і відповідно до запропонованого підходу попередньо для зловмисника можуть формуватися унікальні ДП ЦВЗ довжиною k біт і ДП секретного ключа. При зміні авторства повідомлення зловмисник в кожній ДП чергового відліку повідомлення, завіреного ЦВЗ відправника, повинен декілька найменш значущих бітів, за якими одержувач перевіряє ЦВЗ відправника, замінити на відповідне число найменш значущих бітів, в які вбудовується ЦВЗ зловмисника. При цьому завірене повідомлення спотворюється в декількох найменш значущих бітах ДП кожного чергового відліку повідомлення. При цьому якість мовного, звукового, музичного, телевізійного, факсимільного і т.п. повідомлення, переданого по каналу зв'язку або записаного на носії (аудіо- або відеокасети, CD або DVD диски, дискети тощо) стає істотно гірше. Метою зловмисника в атаці підміни авторства є присвоєння собі авторських і майнових прав на повідомлення за умови збереження необхідної якості повідомлення. Тому зазначена нова сукупність виконуваних дій дозволяє підвищити захищеність повідомлення, завіреного цифровим водяним знаком відправника, до атаки підміни авторства.

Реалізація запропонованого підходу до формування і перевірки завіреного цифровим водяним знаком повідомлення із підвищеною захищеністю полягає в наступному (рис. 2.1).

На рис. 2.1,а показаний вид ДП секретного ключа (СК). Одиничні значення бітів на фігурах показані у вигляді заштрихованих імпульсів, нульові значення – не заштрихованих імпульсів. До ДП СК пред'являються вимога неможливості його обчислення зловмисниками, яким можуть бути відомі завірені з його використанням повідомлення.

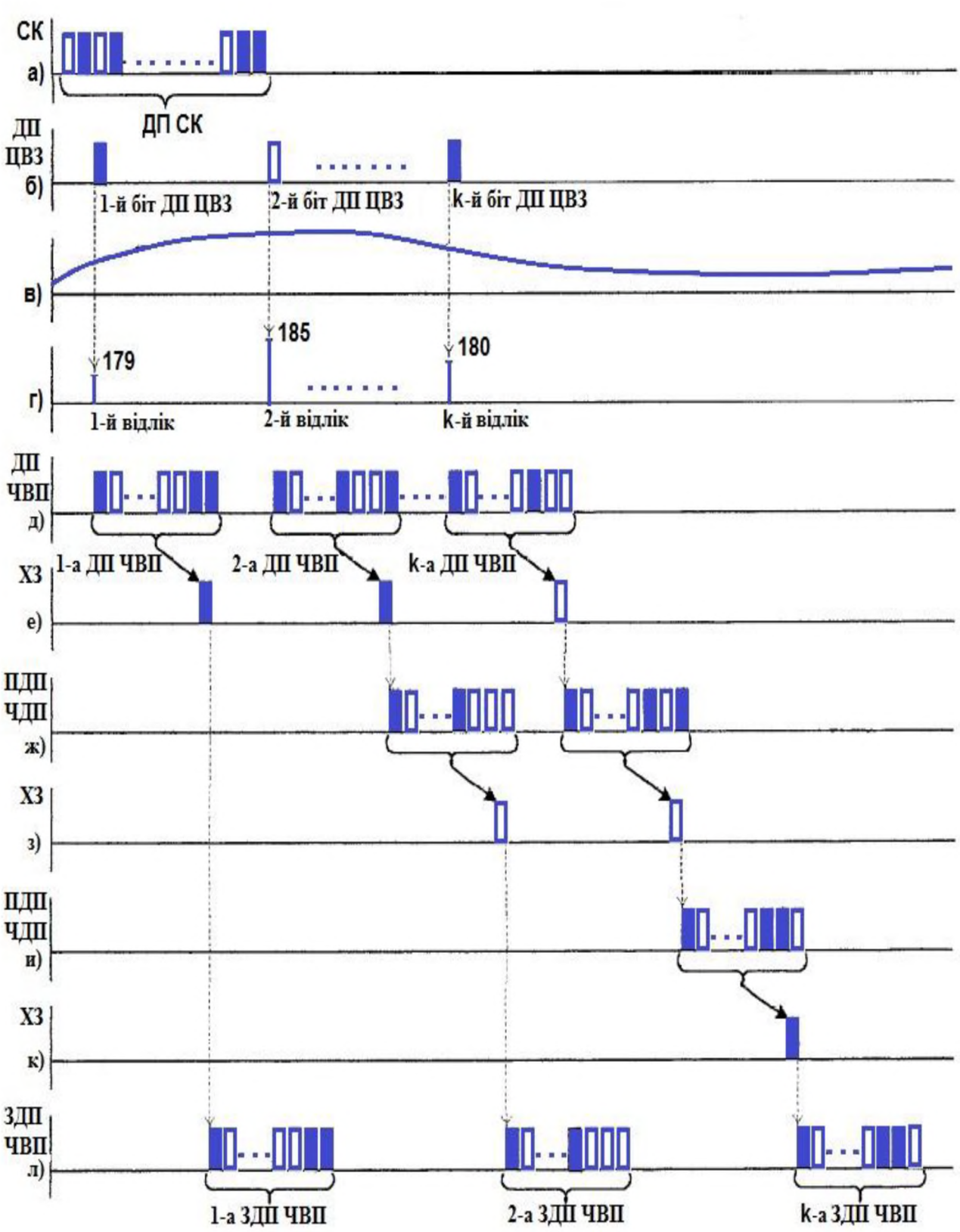

Рисунок 2.1 – Часові діаграми формування завіреного цифровим водяним знаком повідомлення згідно запропонованого підходу

Вид двійковій послідовності цифрового водяного знаку (ДП ЦВЗ) довжиною k біт показаний на рис. 2.1,б. ДП ЦВЗ відправника повідомлення реєструється як унікальний ідентифікатор відправника повідомлень і факт її виявлення в прийнятому повідомленні з використанням СК відправника в прийнятому повідомленні однозначно свідчить про авторство відправника повідомлень, якому належить даний ЦВЗ, і відсутності спотворень в прийнятому повідомленні. ДП ЦВЗ відправника (автора) повідомлень може бути загальновідомою.

Початкові повідомлення, такі як мовні, звукові, відео, факсимільні і т.п., вид яких показаний на рис.2.1,в, до їх завірення ЦВЗ заздалегідь перетворюють до цифрового вигляду, наприклад, методом імпульсно-кодової модуляції (ІКМ) [33]. Відомі способи перетворення можуть виконувати в два етапи: спочатку виконують дискретизацію і квантування, а потім дискретизований і квантований сигнал перетворюють в ДП чергових відліків повідомлення.

Вид цифрових мовних, звукових, відео, факсимільних і подібних до них повідомлень, дискретизованих з частотою дискретизації F=1/T, де T – інтервал часу між черговими відліками, і квантованих на q рівнів (q=256) показаний на рис. 2.1,г . Перший відлік має значення, рівне 179, другий відлік – 185, k-ий відлік – 180 і так далі. Вид ДП чергових відліків повідомлення (ДП ЧВП) показаний на рис. 2.1,д. При q=256 виконавчі послідовності чергових відліків повідомлення складаються з 8 бітів. Старший біт послідовності записують першим (зліва на рис. 2.1,д), найменший значущий біт записують останнім в послідовності (праворуч на рис. 2.1,д).

Як вже зазначалось у розділі 1, відомі підходи до формування і перевірки завіреного ЦВЗ повідомлення побітно вбудовують ДП ЦВЗ в найменші значущі біти послідовності відліків повідомлення [29]. Вбудовування ДП ЦВЗ в найменші значущі біти послідовності відліків мовних, звукових, відео, факсимільних і подібних до них мультимедійних повідомлень практично не погіршує якість повідомлень, що завіряються.

Зловмисники можуть намагатися зруйнувати вбудовані в завірені мультимедійні повідомлення ЦВЗ або зробити їх такими, що не виявляються при перевірці. Якщо зловмисник зумів зруйнувати вбудований ЦВЗ або зробити його не що виявляється, то він може видати себе за законного автора такого мультимедійного повідомлення.

Для визначення номера відліку повідомлення, починаючи з якого при перевірці ЦВЗ необхідно почати вилучення ДП ЦВЗ, в відомих підходах до вбудовування власне ЦВЗ в повідомлення вбудовується ДП мітки ЦВЗ. Якщо при перевірці ЦВЗ в повідомленні ідентифікована ДП мітки ЦВЗ, то однозначно визначено початок вбудованої в повідомлення ДП ЦВЗ.

Отже, якщо зловмисником будуть спотворені відліки завіреного повідомлення, в які вбудована ДП мітки ЦВЗ, то при перевірці ЦВЗ мітку не буде виявлено і внаслідок цього ЦВЗ не буде зчитано. ДП мітки ЦВЗ зазвичай є загальновідомою, тому легко може бути знайдена і спотворена зловмисником в завіреному повідомленні. Підвищення стійкості до навмисних дій зловмисника може бути досягнуто, якщо не використовувати спеціальну ДП мітки ЦВЗ і визначати початок вбудованої в повідомлення ДП ЦВЗ по самій ДП ЦВЗ із використанням відомої одержувачу ДП секретного ключа.

Якщо будуть спотворені відліки завіреного повідомлення, в які вбудована ДП ЦВЗ, то в відомих підходах при перевірці вилучена з завіреного повідомлення ДП ЦВЗ не буде ідентифікована з ДП ЦВЗ автора (відправника) повідомлення, оскільки вони вимагають їх збігу з точністю до біта. Тому підвищення стійкості до навмисних дій зловмисника може бути досягнуто, якщо використовувати ЦВЗ, який можна ідентифікувати з ЦВЗ автора (відправника) повідомлення при наявності спотворень в одному або декількох відліках завіреного повідомлення.

У запропонованому підході для забезпечення формування та перевірки завіреного ЦВЗ повідомлення, що підвищує захищеність повідомлення, завіреного ЦВЗ законного відправника, до навмисних дій зловмисника по зміні змісту повідомлення і його авторства, реалізується наступна послідовність дій.

Попереднє формування для відправника і одержувача ДП ЦВЗ довжиною k біт полягає в наступному. Обирається унікальний ЦВЗ відправника. Унікальну ДП ЦВЗ довжиною k біт відправника формують випадковим вибором послідовності двійкових символів [30]. При випадковому виборі ДП ЦВЗ відправника довжиною 32 біта ймовірність її збігу з ДП ЦВЗ іншого відправника дорівнює $2^{-32} \approx 10^{-9}$, що практично достатньо для забезпечення неповторюваності ЦВЗ великого числа відправників.

Попереднє формування для відправника і одержувача ДП секретного ключа полягає у наступному. ДП секретного ключа формують випадковим вибором послідовності двійкових символів, описаним, наприклад, в [30]. Довжина ДП секретного ключа повинна бути не менше 64 біт, як описано, наприклад, в [34].

Попереднє формування для відправника і одержувача функції хешування з двійковим вихідним значенням полягає в наступному. Відомі способи попереднього формування функції хешування [34], які полягають в формуванні функції хешування по секретному ключу, використовуючи алгоритм шифрування даних DES в режимі зворотного зв'язку по шифртексту або в режимі зворотного зв'язку по виходу. Однак ці методи попереднього формування функції хешування формують функції хешування з вихідним значенням довжиною 64 біта. Тому для попереднього формування функції хешування з двійковим вихідним значенням пропонується вихідне значення довжиною 64 біта функції хешування, сформованої в відомих способах, перетворити обчисленням за модулем 2 [32]. У результаті цього перетворення парні вихідні значення довжиною 64 біта приймуть нульові значення, а непарні вихідні значення довжиною 64 біта приймуть одиничні значення.

Попереднє встановлення для відправника і одержувача мінімально допустимого числа K_{min} справжніх відліків повідомлення в групі з k послідовно прийнятих полягає в наступному. Мінімально допустима кількість K_{min} справжніх відліків повідомлення в групі з k послідовно прийнятих встановлюють рівним $2^{k-K_{\min}} \geq 2^k P_{доп}$, де $P_{доп}$ – допустима ймовірність

прийняття справжньої групи з k чергових відліків повідомлення, що є не справжньою. Наприклад, величину допустимої ймовірності прийняття справжньої групи з k чергових відліків повідомлення, що є не справжньою, встановлюють рівній $P_{доп}=2^{-32}$, як рекомендується в [31]. Отже, величину K_{min} доцільно встановити не менше 32.

Для завірення у відправника повідомлення з використанням ДП ЦВЗ довжиною k біт і секретного ключа послідовно зчитують і-й (i=1,2,...,k) біт ДП ЦВЗ і ДП чергового відліку повідомлення відомими способами [32].

Зчитану ДП чергового відліку повідомлення хешують з використанням ДП секретного ключа за попередньо сформованою функцією хешування. Для цього ДП чергового відліку повідомлення шифрують за алгоритмом шифрування даних DES в режимі зворотного зв'язку по шифртексту з використанням ДП секретного ключа [34]. Далі вихідне значення довжиною 64 біта функції хешування перетворюють обчисленням за модулем 2 [32]. В результаті цього перетворення хешоване значення прийме нульове значення при парних вихідних значеннях довжиною 64 біта, і прийме середнє арифметичне значення при непарних вихідних значеннях довжиною 64 біта.

На рис. 2.2 показаний типовий приклад результатів хешування ДП чергових відліків повідомлення з використанням ДП секретного ключа за попередньо сформованою функцією хешування. ДП чергових відліків повідомлення, а також перетворені виконавчі послідовності чергових відліків повідомлення відповідають значенням чергових відліків повідомлення від 0 до 255. Хешоване значення ДП чергових відліків повідомлення приймають нульове або середнє арифметичне значення з ймовірністю, близькою до 1/2.

Далі порівнюють хешоване значення ДП чергового відліку повідомлення з і-м бітом ДП ЦВЗ [35]. Результатом порівняння може бути їх збіг або розбіжність. При збізі хешованого значення з і-м бітом ДП ЦВЗ двійкову послідовність чергового відліку повідомлення передають одержувачу в якості завіреної [33].

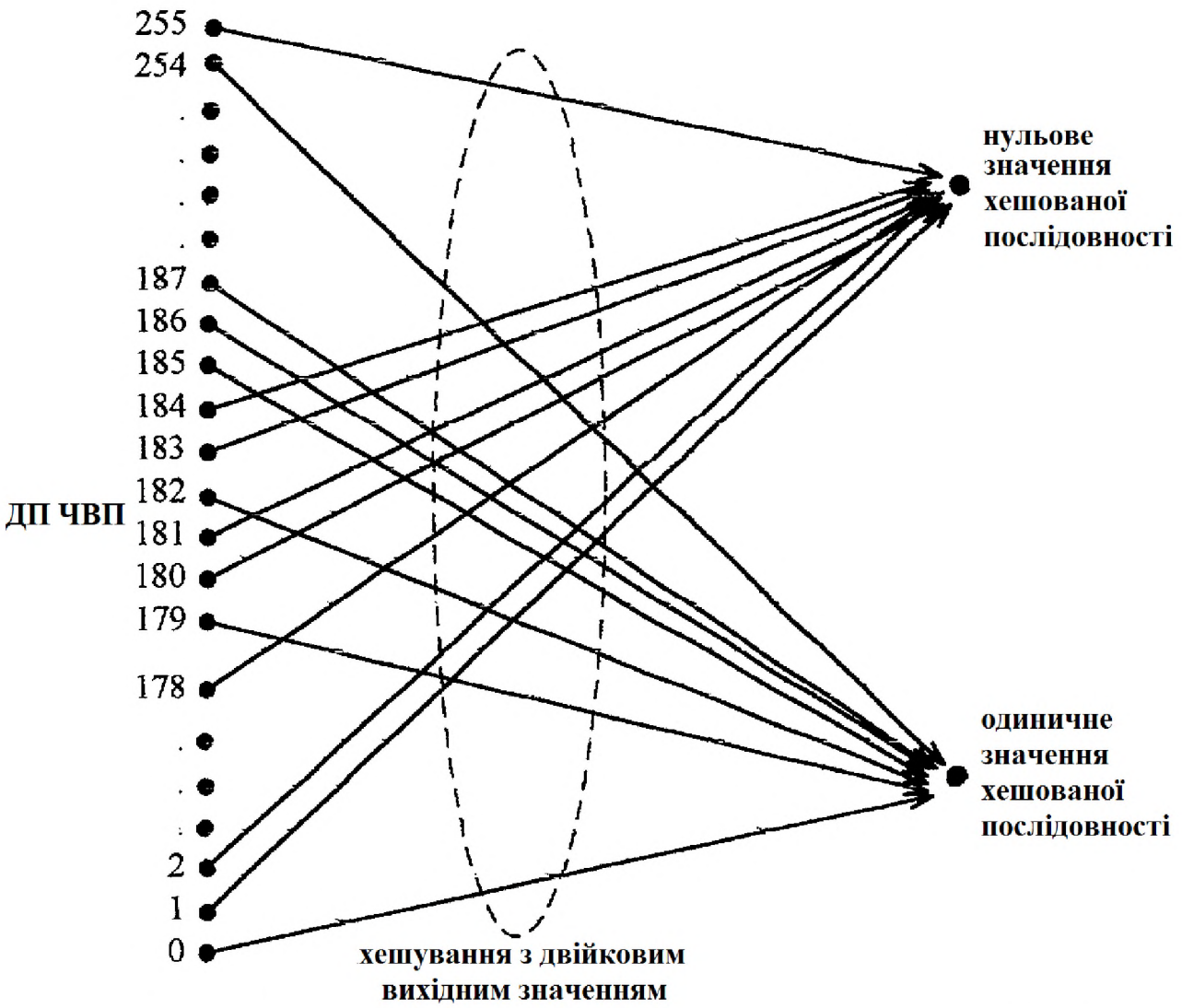

Рисунок 2.2 – Приклад результатів хешування ДП чергових відліків повідомлення з використанням ДП секретного ключа за попередньо сформованою функцією хешування

Приклад отриманих хешованих значень (ХЗ) показаний на рис. 2.1,е. Нехай при хешуванні ДП першого відліку повідомлення сформовано одиничне хешоване значення. Воно порівнюється зі значенням першого біта ДП ЦВЗ і при їх збізі ДП першого відліку повідомлення передають одержувачу в якості завіреної ДП першого відліку повідомлення. Приклад завірених ДП чергових відліків повідомлення (ЗДП ЧВП) показаний на рис. 2.1,л.

При розбіжності ДП чергового відліку повідомлення послідовно перетворюють шляхом зміни її молодших бітів. Для перетворення ДП

чергового відліку повідомлення шляхом зміни її молодших бітів послідовно змінюють її один, два, три і так далі найменш значущі біти. Ця зміна може бути виконана послідовним інвертуванням одного, двох, трьох і так далі найменш значущих бітів даної ДП [32].

Після кожного перетворення перетворену ДП чергового відліку повідомлення хешують із використанням ДП секретного ключа за попередньо сформованою функцією хешування, порівнюють хешоване значення за і-м бітом ДП ЦВЗ, причому перетворення ДП чергового відліку повідомлення виконують до збігу хешованого значення перетвореної ДП чергового відліку повідомлення з і-м бітом ДП ЦВЗ, після чого останню перетворену ДП чергового відліку повідомлення передають одержувачу в якості завіреної.

Для хешування з використанням ДП секретного ключа за попередньо сформованою функцією хешування перетворену ДП чергового відліку повідомлення шифрують за алгоритмом шифрування даних DES в режимі зворотного зв'язку по шифротексту із використанням ДП секретного ключа [34]. Далі вихідне значення довжиною 64 біта функції хешування перетворюють обчисленням за модулем 2. У результаті цього перетворення хешоване значення прийме нульове значення при парних вихідних значеннях довжиною 64 біта, і середнє арифметичне значення – при непарних.

Потім порівнюють хешоване значення перетвореної ДП чергового відліку повідомлення з і-м бітом ДП ЦВЗ [35]. При збізі хешованого значення з і-м бітом ДП ЦВЗ останню перетворену ДП чергового відліку повідомлення передають одержувачу в якості завіреної, інакше продовжують перетворення ДП чергового відліку повідомлення [33].

Приклад отриманих хешованих значень показаний на рис. 2.1,е. Нехай, як показано на рис. 2.1,е, при хешуванні ДП другого відліку повідомлення сформовано одиничне хешоване значення. Воно не співпадає з значенням другого біта ДП ЦВЗ. Тому ДП другого відліку повідомлення послідовно перетворюють. Для цього середнє арифметичне значення найменш значущого біта ДП другого відліку повідомлення змінюють на нульове значення, як

показано на рис. 2.1,ж. Хешоване значення перетвореної двійковій послідовності (ПДП) другого відліку повідомлення є нульовим, тобто збігається з другим бітом ДП ЦВЗ. Далі перетворену ДП другого відліку повідомлення передають одержувачу в якості завіреної перетвореної ДП другого відліку повідомлення

Нехай, як показано на рис. 2.1,е, при хешуванні ДП k-го відліку повідомлення сформовано нульове хешоване. Воно не співпадає зі значенням k-го біта ДП ЦВЗ. Тому ДП k-го відліку повідомлення послідовно перетворюють. Для цього нульове значення найменш значущого біта ДП k-го відліку повідомлення змінюють на середнє арифметичне значення, як показано на рис. 2.1,ж. Хешоване значення перетвореної ДП k-го відліку повідомлення є нульовим, тобто знову не збігається з k-м бітом ДП ЦВЗ. Далі нульове значення передостаннього (по рис. 2.1,д) значущого біта ДП k-го відліку повідомлення змінюють на середнє арифметичне значення, як показано на рис. 2.1,и. Хешоване значення перетвореної таким чином ДП k-го відліку повідомлення є одиничним, тобто збігається з k-м бітом ДП ЦВЗ. Далі останню перетворену ДП k-го відліку повідомлення передають одержувачу в якості завіреної.

Ймовірність розбіжності хешованого значення ДП чергового відліку повідомлення з і-м бітом ДП ЦВЗ дорівнює ½. Після перетворення ДП чергового відліку повідомлення зміною її одного найменш значущого біта ймовірність розбіжності хешованого значення перетвореної ДП чергового відліку повідомлення з і-м бітом ДП ЦВЗ дорівнює 1/4. Після послідовної зміни одного, двох, трьох і так далі найменш значущих біт ДП чергового відліку повідомлення перетворення ДП чергового відліку повідомлення ймовірність розбіжності хешованого значення перетвореної ДП чергового відліку повідомлення з і-м бітом ДП ЦВЗ дорівнює $2^{-\eta-1}$, де η - число послідовно змінених найменш значущих біт ДП чергового відліку повідомлення. Вибираючи відповідне значення числа η, можна практично гарантувати збіг хешованого значення перетвореної ДП чергового відліку повідомлення з і-м бітом ДП ЦВЗ.

Після завірення ДП чергового відліку повідомлення з використанням k-го біта ДП ЦВЗ повторно, починаючи з першого і до k-го, зчитують і-й біт ДП ЦВЗ, і ДП чергового відліку повідомлення та виконують наступні за ним дії до тих пір, поки надходять ДП чергових відліків повідомлення. Число ДП чергових відліків повідомлення може бути досить великим. З ростом її довжини пропорційно зростає і число чергових груп з k ДП чергових відліків повідомлення, в кожній з яких одержувачем проводиться перевірка справжності прийнятого повідомлення. Отже, чим довше повідомлення, тим складніше зловмисникові змінити його зміст або авторство. Якщо зловмисник розділить завірене повідомлення на декілька частин, то завдяки завіренню відправником кожної чергової групи з k ДП чергових відліків повідомлення одержувач будь-якій частині завіреного повідомлення довжиною не менше k ДП чергових відліків здатний виконати перевірку її достовірності. Оскільки величина k становить не більше десятків ДП, то зловмисник практично не здатний розділити завірене повідомлення на частини, довжиною менш k ДП чергових відліків, через те, що такі короткі фрагменти мовних, звукових, музичних, телевізійних, факсимільних і т.п. повідомлень не несуть значимої інформації для їх потенційних одержувачів.

У одержувача повідомлення попередньо з числа прийнятих ДП чергових відліків повідомлення виділяють відлік, що відповідає першому біту ДП ЦВЗ у відправника повідомлення. Для виділення чергового відліку повідомлення, відповідного першому біту ДП ЦВЗ у відправника повідомлення, попередньо встановлюють максимально допустиме значення ймовірності $P_{пом}$ помилкового виділення цього відліку. Значення ймовірності $P_{пом}$ може бути встановлено, наприклад, порядку $10^{-1}...10^{-2}$. Якщо в результаті похибок каналу передачі або навмисних спотворень завіреного повідомлення зловмисником одержувач не зможе виділити відлік, що відповідає першому біту ДП ЦВЗ у відправника повідомлення в черговій групі з k ДП чергових відліків повідомлення, то одержувач буде шукати необхідний відлік в наступній групі з k ДП чергових відліків повідомлення і так до тих пір, доки необхідний відлік не буде виділено.

Ймовірність невиділення необхідного відліку в β послідовних групах з k ДП чергових відліків повідомлення дорівнює $P^{\beta}_{пом}$. Оскільки з ростом числа β ймовірність $P^{\beta}_{пом}$ дуже швидко наближається до нуля, то забезпечується гарантоване виділення одержувачем чергового відліку повідомлення, відповідного першому біту ДП ЦВЗ у відправника повідомлення на довжині не більше β декількох послідовних груп з k ДП чергових відліків повідомлення.

Прийняті одержувачем ДП чергових відліків повідомлення хешують з використанням ДП секретного ключа за попередньо сформованою функцією хешування. Для хешування із використанням ДП секретного ключа за попередньо сформованою функцією хешування прийняту ДП чергового відліку повідомлення шифрують за алгоритмом шифрування даних DES в режимі зворотного зв'язку за шифротекстом з використанням ДП секретного ключа [34]. Далі вихідне значення довжиною 64 біта функції хешування перетворюють обчисленням за модулем 2.

Хешовані значення прийнятих ДП чергових відліків повідомлення порівнюють послідовно з відповідними, начиняючи з першого, значеннями бітів ДП ЦВЗ до досягнення m їх збігів поспіль, де $m=\lfloor -\log_2 P_{пом} \rfloor$, а дія $\lfloor -\log_2 P_{пом} \rfloor$ означає округлення значення $-\log_2 P_{пом}$ до найближчого цілого, причому відповідним першому біту ДП ЦВЗ у відправника повідомлення, приймають перший відлік з m послідовно прийнятих ДП чергових відліків повідомлення [35].

Потім для перевірки справжності прийнятого одержувачем повідомлення послідовно приймають k ДП чергових відліків повідомлення [35].

Прийняті ДП чергових відліків повідомлення хешують з використанням ДП секретного ключа за попередньо сформованою функцією хешування. Для хешування з використанням ДП секретного ключа за попередньо сформованою функцією хешування прийняту ДП чергового відліку повідомлення шифрують за алгоритмом шифрування даних DES в режимі зворотного зв'язку за шифротекстом з використанням ДП секретного ключа [34]. Потім вихідне

значення довжиною 64 біта функції хешування перетворюють обчисленням за модулем 2.

Кожне і-е хешоване значення прийнятої ДП чергового відліку повідомлення порівнюють з і-м бітом ДП ЦВЗ [35]. Результатом порівняння значень може бути їх збіг або розбіжність.

Обчислюють число $К_с$ хешованих ДП чергових відліків повідомлення з k прийнятих відліків, що збіглися зі значеннями відповідних їм бітів ДП ЦВЗ. Число $К_с$ обчислюють як арифметичну суму випадків збігу хешованих ДП чергових відліків повідомлення з k прийнятих відліків зі значеннями відповідних їм бітів ДП ЦВЗ. Обчислення значення $К_с$ може перебувати в межах від нульового значення до k включно.

При виконанні умови $К_с \geq К_{min}$ прийняті k ДП чергових відліків повідомлення вважають справжніми. При невиконанні цієї нерівності справжність прийнятих k ДП не підтверджується.

На рис. 2.3 представлені часові діаграми перевірки отриманого повідомлення, зсунутого щодо завіреного ЦВЗ повідомлення (Пр ДП ЧВП – перетворена двійкова послідовність чергових відліків повідомлення).

На рис. 2.4 представлено часові діаграми перевірки отриманого повідомлення, засинхронізованого щодо завіреного ЦВЗ повідомлення.

Нехай, як показано на рис. 2.4,е, перевіряється справжність прийнятих k ДП чергових відліків повідомлення. Хешоване значення прийнятої ДП першого відліку повідомлення, показане на рис. 2.4,ж, збігається зі значенням першого біта ДП ЦВЗ, тому число $К_с$ встановлюється в середнє арифметичне значення: $К_с=1$, як показано на рис. 2.4,з.

Аналогічно обробляються наступні k-1 прийняті ДП чергових відліків повідомлення. Нехай, як показано на рис. 2.4,з, після прийому k ДП чергових відліків повідомлення виконується умова $К_с \geq К_{min}$. Тому прийняті k ДП чергових відліків повідомлення вважають справжніми, як показано на рис. 2.4,и.

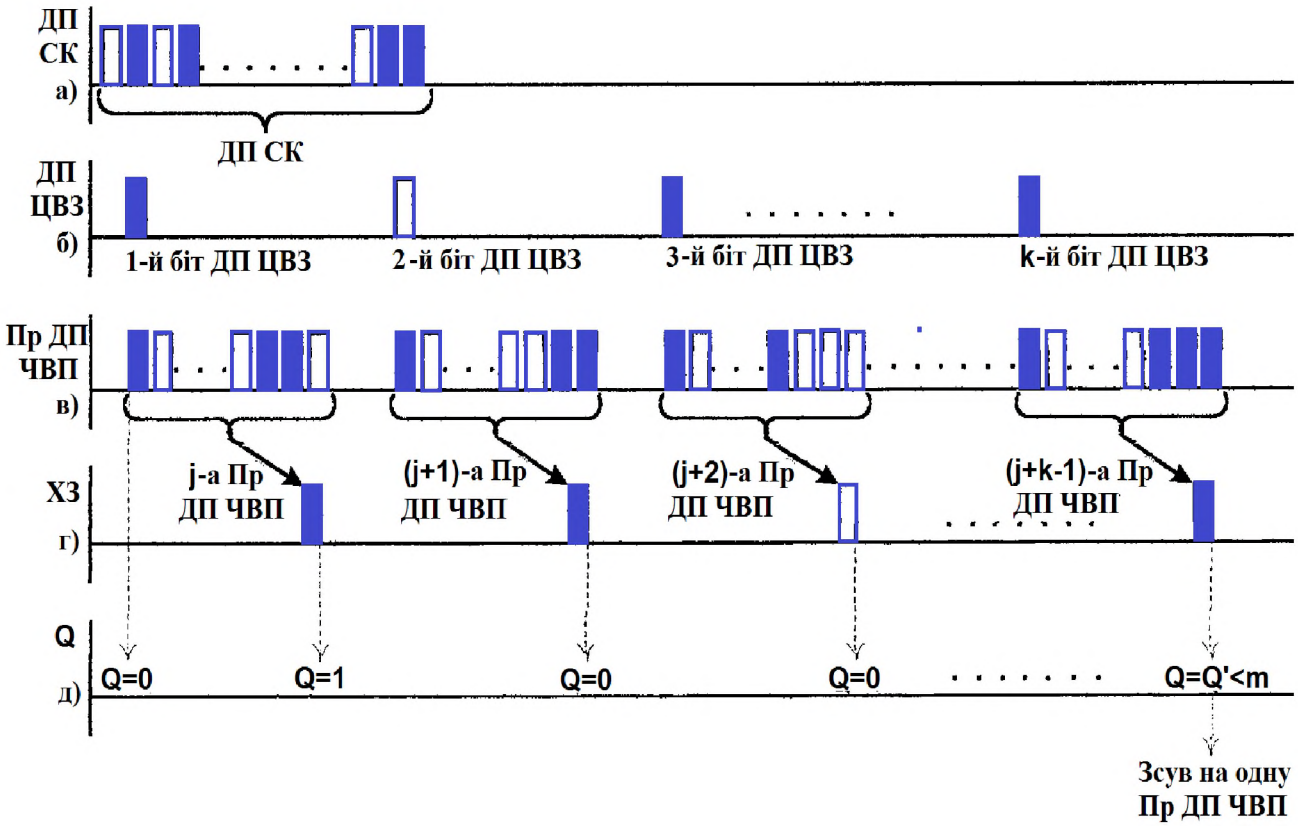

Рисунок 2.3 – Часові діаграми перевірки отриманого повідомлення, зсунутого щодо завіреного ЦВЗ повідомлення

Далі повторюють дії по перевірці справжності чергової групи з k ДП чергових відліків повідомлення і так до завершення прийому всіх ДП чергових відліків повідомлення. Якщо при перевірці справжності все прийняті k ДП чергових відліків повідомлення визнані справжніми, то все отримане повідомлення вважають справжнім.

2.2 Оцінка ефективності запропонованого підходу до формування і перевірки завіреного цифровим водяним знаком повідомлення із підвищеною захищеністю

Перевірка теоретичних передумов запропонованого підходу до формування і перевірки завіреного цифровим водяним знаком повідомлення із підвищеною захищеністю перевірялася шляхом його аналітичних досліджень.

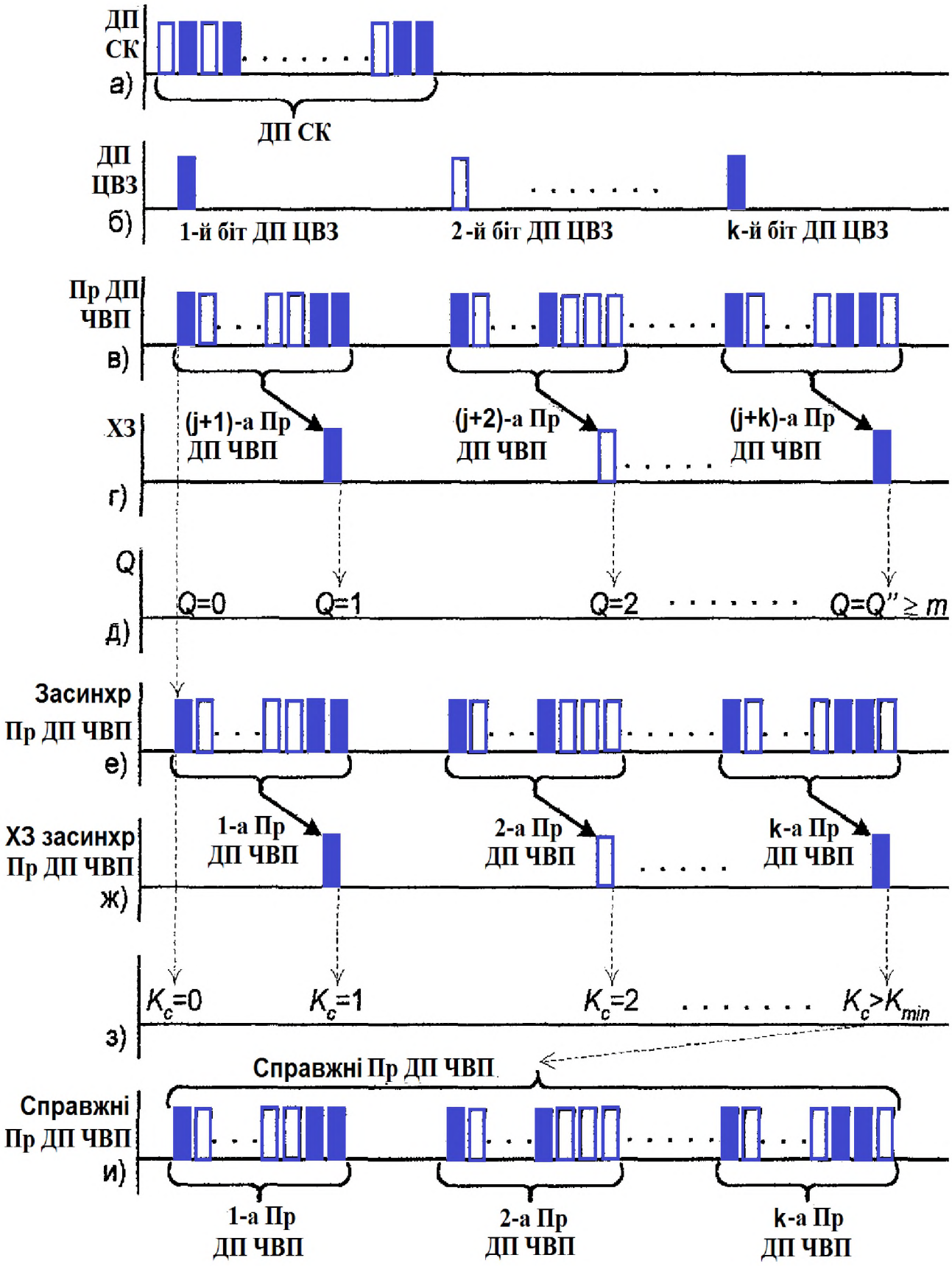

Рисунок 2.4 – Часові діаграми перевірки отриманого повідомлення, засинхронізованого щодо завіреного ЦВЗ повідомлення

Ймовірність прийняття справжньої групи з k чергових відліків повідомлення, які є справжньою, дорівнює $P_{несправж} = 2^{-K_{\min}}$. На рис. 2.5 показана залежність $P_{несправж}$ від значення K_{min}. З рис. 2.5 видно, що мінімально допустиме число K_{min} має бути встановлено таким, щоб виконувалося співвідношення $P_{несправж} \leq P_{доп}$.

Проведені дослідження підтверджують, що при використанні запропонованого підходу до формування і перевірки завіреного цифровим водяним знаком повідомлення із підвищеною захищеністю забезпечується підвищення його захищеності до навмисних дій зловмисників зі зміни змісту повідомлення і його авторства.

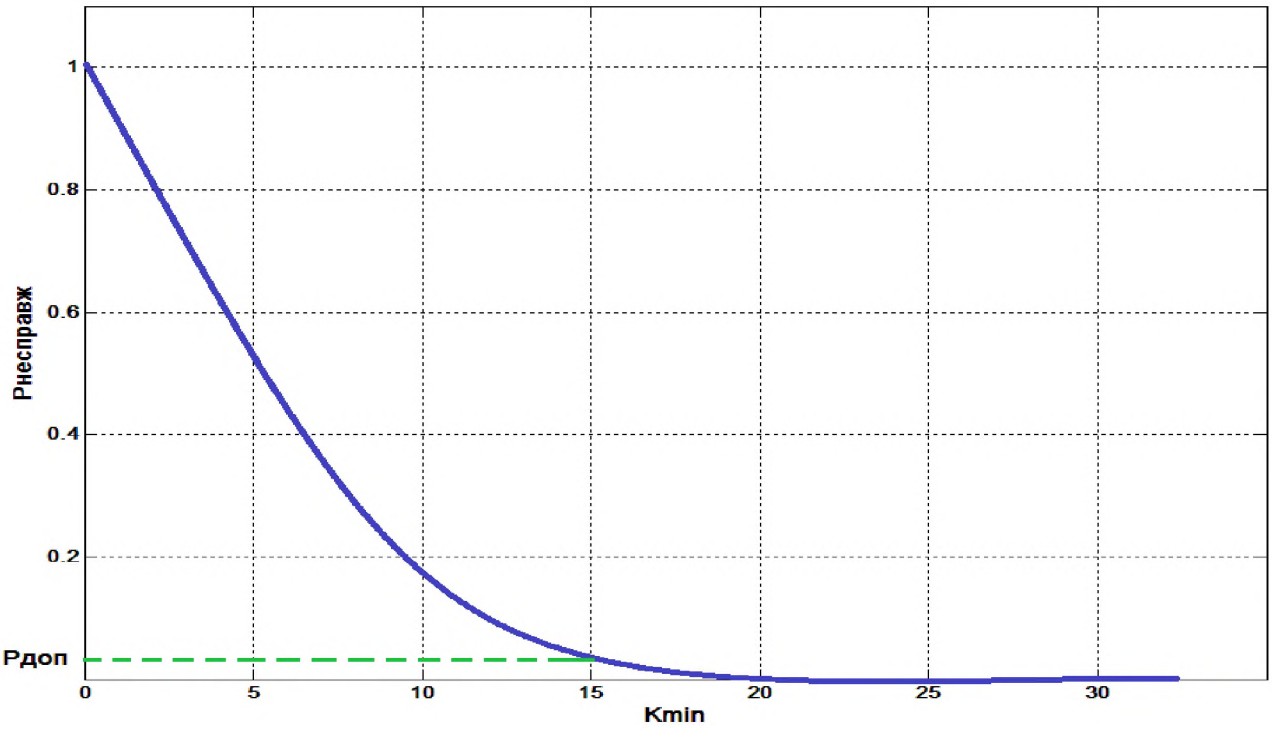

Рисунок 2.5 – Графіки, що показують ефект запропонованого підходу

2.3 Висновки

Запропонований підхід до формування і перевірки завіреного цифровим водяним знаком повідомлення із підвищеною захищеністю відноситься до

області електрозв'язку і інформаційних технологій, а саме до техніки захисту справжності повідомлень, таких як перетворені до цифрового вигляду мовні, звукові, музичні, телевізійні, факсимільні і подібні повідомлення. Технічним результатом, що досягається при реалізації запропонованого рішення, є розробка підходу до формування і перевірки завіреного ЦВЗ повідомлення, що забезпечує підвищення захищеності повідомлення, завіреного ЦВЗ відправника, від навмисних дій зловмисника по зміні змісту повідомлення і його авторства. Технічний результат досягається тим, що попередньо для відправника і одержувача формують двійкову послідовність (ДП) цифрового водяного знаку довжиною k біт і ДП секретного ключа, завіряють у відправника повідомлення із використанням ДП ЦВЗ і секретного ключа, передають завірене повідомлення одержувачу, де перевіряють справжність прийнятого повідомлення із використанням ДП ЦВЗ і секретного ключа.

Поставлена мета досягається шляхом використання попередньо сформованої функції хешування, двійкове вихідне значення якої в рівній мірі залежить від кожного біта двійкових послідовностей чергових відліків повідомлення і кожного біта двійкової послідовності секретного ключа.

Зазначена нова сукупність виконуваних дій за рахунок непередбачуваної для зловмисника залежності всіх бітів ДП чергових відліків завіреного ЦВЗ повідомлення від відповідних бітів ДП ЦВЗ довжиною k біт і ДП секретного ключа дозволяє підвищити захищеність повідомлення, завіреного ЦВЗ відправника, до навмисних дій зловмисника по зміні змісту повідомлення і його авторства. Дана непередбачуваність при невідомої для зловмисника ДП секретного ключа забезпечується хешуванням ДП чергового відліку повідомлення з використанням ДП секретного ключа за попередньо сформованою функцією хешування з двійковим вихідним значенням. Попередньо сформована функція хешування з двійковим вихідним значенням для зловмисника не відрізняється від випадкової функції, тобто ймовірність правильного визначення її вихідного значення при невідомій для зловмисника

ДП секретного ключа дорівнює ½, тобто дорівнює ймовірності випадкового вгадування.

Попередньо сформована функція хешування з двійковим вихідним значенням повинна відповідати наступним вимогам:

1) двійкове вихідне значення функції хешування в рівній мірі залежить від кожного біта ДП чергових відліків повідомлення і кожного біта ДП секретного ключа;

2) знаючи опис функції хешування і ДП чергових відліків завіреного повідомлення, зловмисник не здатний обчислити ДП секретного ключа;

3) знаючи опис функції хешування, зловмисник не здатний правильно сформувати вихідне значення функції хешування з ймовірністю істотно більшою ½ для ДП чергових відліків обраного повідомлення, не знаючи ДП секретного ключа.

В результаті оцінки ефективності запропонованого підходу до формування і перевірки завіреного цифровим водяним знаком повідомлення із підвищеною захищеністю було встановлено, що при його використанні забезпечується підвищення захищеності повідомлення до навмисних дій зловмисників зі зміни змісту повідомлення і його авторства.

Запропонований підхід до формування і перевірки завіреного цифровим водяним знаком повідомлення із підвищеною захищеністю може бути використаний для встановлення справжності мовних, звукових, музичних, телевізійних, факсимільних і інших мультимедійних повідомлень, переданих і збережених в сучасних інформаційно-телекомунікаційних системах.

3 ЕКОНОМІЧНА ЧАСТИНА

Метою даного розділу є обґрунтування економічної доцільності запропонованого підходу до стеганографічного вбудовування цифрового водяного знака в завірене повідомлення. Досягнення цієї мети потребує визначення таких показників, як:

– капітальні витрати на придбання і налагодження складових системи інформаційної безпеки або витрат, що пов’язані з виготовленням апаратури, приладів, програмного забезпечення;

– річні експлуатаційні витрати на утримання і обслуговування об'єкта проектування;

– річний економічний ефект від впровадження запропонованих заходів;

– показники економічної ефективності впровадження системи захисту на підприємстві.

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 стеганографічного вбудовування цифрового водяного знака в завірене повідомлення

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 стеганографічного вбудовування цифрового водяного знака в завірене повідомлення, $t_{тз}=18$;

$t_в$ – тривалість аналізу існуючих інформаційних потоків організації, вивчення ТЗ, літературних джерел за темою тощо, $t_в=41$;

$t_а$ – тривалість аналізу існуючих загроз безпеки інформації, $t_а=70$;

$t_р$ – тривалість розробки підходу щодо стеганографічного вбудовування цифрового водяного знака в завірене повідомлення, $t_м=52$;

$t_д$ – тривалість підготовки технічної документації, $t_д=10$.

Отже,

$$t = t_{тз}+ t_в+ t_а+ t_р+ t_д = 18+41+70+52+10= 191 \text{ години.}$$

Розрахунок витрат на розробку підходу щодо стеганографічного вбудовування цифрового водяного знака в завірене повідомлення

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 $З_{мч}$.

$$К_{рп} = З_{зп} + З_{мч}\ .$$

$$К_{рп} = З_{зп} + З_{мч} = 42312+1944,38 =44256,38 \text{ грн.}$$

$$З_{зп} = t\ З_{пр} = 191*164 = 31324 \text{ грн.}$$

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:

$$З_{мч}= t*С_{мч}=191*10,18=1944,38 \text{ грн.}$$

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:

$$Смч = 0,9 \cdot 4 \cdot 1,55 + \frac{4600 \cdot 0,6}{1920} + \frac{8500 \cdot 0,2}{1920} = 10,18 \text{ грн.}$$

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

Оцінка ефективності запропонованого підходу щодо стеганографічного вбудовування цифрового водяного знака в завірене повідомлення 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 3000 грн.

Вирішення певних технічних завдань із збільшення скритності і точності відновлення приховуваного сигналу потребує залучення аутсорсингових організації, вартість послуг котрих складає 15000 грн.

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

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

$$= 44256{,}38+15000+3000 = 62256{,}38 \text{ грн.}$$

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.).

Середовище Matlab/Simulink, яке застосовується для оцінки ефективності запропонованого підходу щодо стеганографічного вбудовування цифрового водяного знака в завірене повідомлення, 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 8000 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 15400 грн. Додаткова заробітна плата – 9% від основної заробітної плати.

Виконання роботи щодо впровадження системи захисту інформації на підприємстві потребує залучення спеціаліста інформаційної безпеки на 0,2 ставки. Отже,

$$С_з = (15400*12 + 15400*12*0,09)*0,2= 40286,4 \text{ грн.}$$

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

$$С_{єв} = 40286,4*0,22 = 8863 \text{ грн.}$$

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:

$$С_{ел} = 0,9*4*1920*1,55 = 10713,6 \text{ грн.}$$

Витрати на технічне й організаційне адміністрування та сервіс системи інформаційної безпеки визначаються у відсотках від вартості капітальних витрат – 1% ($С_{тос}$ = 62256,38*0,01=622,56 грн).

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

$$С_к = 8000+40286,4+8863+10713,6+622,56= 68485,56 \text{ грн.}$$

Витрати, викликані активністю користувачів системи інформаційної безпеки ($С_{ак}$) можна орієнтовно визначити, виходячи з величини капітальних витрат та середньостатистичних даних щодо активності користувачів. За статистичними даними активність користувачів складає 20%. Тому:

$$С_{ак}= 62256,38*0,2=12451,28 \text{ грн.}$$

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

$$С =68485,56+12451,28=80936,84 \text{ грн.}$$

3.2 Оцінка можливого збитку

Запропонований підхід до формування і перевірки завіреного цифровим водяним знаком повідомлення із підвищеною захищеністю відноситься до техніки захисту справжності повідомлень, таких як перетворені до цифрового вигляду мовні, звукові, музичні, телевізійні, факсимільні і подібні повідомлення. Технічним результатом, що досягається при реалізації запропонованого рішення, є розробка підходу до формування і перевірки завіреного ЦВЗ повідомлення, що забезпечує підвищення захищеності повідомлення, завіреного ЦВЗ відправника, від навмисних дій зловмисника по зміні змісту повідомлення і його авторства.

Формування і перевірку завіреного цифровим водяним знаком повідомлення із підвищеною захищеністю може бути використано для встановлення справжності мовних, звукових, музичних, телевізійних, факсимільних і інших мультимедійних повідомлень, переданих і збережених в сучасних інформаційно-телекомунікаційних системах.

Для розрахунку вартості такого збитку можна застосувати наступну спрощену модель оцінки.

При порушенні прав інтелектуальної власності на мовні, звукові, музичні, телевізійні, факсимільні і інших мультимедійні повідомлення, передані і збережені в сучасних інформаційно-телекомунікаційних системах, величина можливого збитку може бути визначена відповідно до розміру відшкодування завданих збитків, що визначається правом інтелектуальної власності, зокрема Цивільним кодексом України, Кримінальним кодексом України, ВСУ від 31.03.95 р. №4 «Про судову практику у справах про відшкодування морального (немайнового) збитку» тощо. У разі встановлення величини компенсації за завдану шкоду підприємству, яка виникла внаслідок недостатнього рівня захищеності його об’єктів інтелектуальної власності, а саме мовних, звукових,

музичних, телевізійних, факсимільних і інших мультимедійних повідомлень, величину можливого збитку можна встановити наступним чином:

$$B = n * R * F$$

де n – кількість мовних, звукових, музичних, телевізійних, факсимільних і інших мультимедійних повідомлень, що потребує захисту;

R – середнє значення можливості реалізації ризику порушень прав інтелектуальної власності;

F – середнє значення можливого штрафу за законодавством України (ВСУ від 31.03.95 р. № 4 «Про судову практику у справах про відшкодування морального (немайнового) збитку»).

При кількості зображень мовних, звукових, музичних, телевізійних, факсимільних і інших мультимедійних повідомлень, що потребує захисту, 120 одиниць, вірогідності реалізації ризику, яка дорівнює 25% (R=0,25) та величині штрафу за порушення прав інтелектуальної власності, який дорівнюватиме 22000 грн., величина можливого збитку складе:

$$B=120*0,25*22000=66000 \text{ грн.}$$

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

R – вірогідність успішної реалізації загрози (25%);

C – щорічні витрати на експлуатацію системи інформаційної безпеки.

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

$$E = 660000 – 80936,84 = 579063,16 \text{ грн.}$$

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 (То).

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:

$$ROSI = \frac{579063,16}{62256,38} = 9,3, \quad \text{частки одиниці,}$$

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, (6%);

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

Розрахункове значення коефіцієнта повернення інвестицій:

$$9,3 > (6 - 5)/100 = 9,3 > 0,01.$$

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

$$T_O = \frac{K}{E} = \frac{1}{ROSI} = \frac{1}{9,3} = 0,11 \text{ років.}$$

3.4 Висновок

Таким чином, відповідно до проведених розрахунків можна дійти висновку, що розробка підходу щодо стеганографічного вбудовування цифрового водяного знака в завірене повідомлення є економічно доцільною. Капітальні витрати, які складають 62256,38 грн. можливо отримати ефект величиною 579063,16 грн. Щорічні експлуатаційні витрати становлять 80936,84 грн. Коефіцієнт повернення інвестицій (ROSI=9,3) свідчить про отримання 9,3 грн. економічного ефекту на 1 грн. капітальних витрат.

Величина економічного ефекту визначатиметься також розміром компанії, величиною вартості нематеріальних активів (об'єктів прав інтелектуальної власності) та кількістю об'єктів прав інтелектуальної власності (як то: мовні, звукові, музичні, телевізійні, факсимільні і інших мультимедійні повідомлення, передані і збережені в сучасних інформаційно-телекомунікаційних системах), право на авторство яких може бути порушеним.

ВИСНОВКИ

1. В результаті аналізу принципів вбудовування цифрових водяних знаків, а також атаки на стеганосистеми встановлено, що встановлення справжності повідомлень на основі використання унікальних технологічних ознак носіїв цих повідомлень принципово не здатне встановити відсутність в цих повідомленнях навмисних спотворень і їх авторство при їх перезапису з носіїв, що володіють унікальними технологічними ознаками, на носії, які цих ознак не мають. Тому підходи до встановлення справжності мультимедійних повідомлень доцільно будувати на основі вбудовування в самі повідомлення спеціального ЦВЗ відправника (автора) повідомлення з використанням секретного ключа.

2. В результаті аналізу існуючих підходів до формування і перевірки завіреного цифровим водяним знаком повідомлення встановлено їх недоліки. Недоліком відомого підходу до стегоаналізу зображень, створених за допомогою сучасного стеганографічного програмного забезпечення [27] є низька захищеність повідомлення, завіреного цифровим водяним знаком відправника, від навмисних дій зловмисника по зміні змісту повідомлення і його авторства. Недоліком відомого підходу «Стеганографічний метод та пристрій» (прототипу) [28] є низька захищеність повідомлення, завіреного ЦВЗ відправника, від навмисних дій зловмисника по зміні змісту повідомлення і його авторства. Відомий підхід-прототип не забезпечує захищеність повідомлення, завіреного цифровим водяним знаком відправника, до атаки підміни повідомлення, атаки імітації повідомлення та атаки підміни авторства. Зазначений недолік відомого підходу «Стеганографічний метод та пристрій» (прототипу) [28] виник через те, що вбудована в повідомлення двійкова послідовність ЦВЗ не залежить від самого повідомлення, яке завіряється, і двійкової послідовності секретного ключа.

3. Запропоновано підхід до формування і перевірки завіреного цифровим водяним знаком повідомлення із підвищеною захищеністю, згідно з яким попередньо для відправника і одержувача формують двійкову послідовність

(ДП) цифрового водяного знаку довжиною k біт і ДП секретного ключа, завіряють у відправника повідомлення із використанням ДП ЦВЗ і секретного ключа, передають завірене повідомлення одержувачу, де перевіряють справжність прийнятого повідомлення із використанням ДП ЦВЗ і секретного ключа. При цьому, використовується попередньо сформована функція хешування, двійкове вихідне значення якої в рівній мірі залежить від кожного біта двійкових послідовностей чергових відліків повідомлення і кожного біта двійкової послідовності секретного ключа.

4. Результат оцінки ефективності запропонованого підходу до формування і перевірки завіреного цифровим водяним знаком повідомлення у порівнянні із підходом-прототипом доводить ефективність запропонованого підходу, а саме – підвищення захищеності повідомлення, завіреного ЦВЗ відправника, від навмисних дій зловмисника по зміні змісту повідомлення і його авторства. Зазначена нова сукупність виконуваних дій за рахунок непередбачуваної для зловмисника залежності всіх бітів ДП чергових відліків завіреного ЦВЗ повідомлення від відповідних бітів ДП ЦВЗ довжиною k біт і ДП секретного ключа дозволяє підвищити захищеність повідомлення, завіреного ЦВЗ відправника, до навмисних дій зловмисника по зміні змісту повідомлення і його авторства. Дана непередбачуваність при невідомої для зловмисника ДП секретного ключа забезпечується хешуванням ДП чергового відліку повідомлення з використанням ДП секретного ключа за попередньо сформованою функцією хешування з двійковим вихідним значенням. Попередньо сформована функція хешування з двійковим вихідним значенням для зловмисника не відрізняється від випадкової функції, тобто ймовірність правильного визначення її вихідного значення при невідомій для зловмисника ДП секретного ключа дорівнює ½, тобто дорівнює ймовірності випадкового вгадування.

ПЕРЕЛІК ПОСИЛАНЬ

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

2. Matsui K., Tanaka K., and Nakamura Y. Digital signature on a facsimile document by recursive MH coding // Symposium On Cryptography and In-formation Security, 1989.

3. Osborne C., van Schyndel R., Tirkel A. A Digital Watermark // IEEE Intern. Conf. on Image Processing, 1994. – P. 86-90.

4. Anderson R., editor. // Proc. Int. Workshop on Information Hiding: Lecture Notes in Computer Science. – Springer-Verlag, Cambridge. – 1996.

5. Ramkumar M. Data Hiding in Multimedia. PhD Thesis. – New Jersey Institute of Technology, 1999. – 72 p.

6. Simmons G. The prisoner`s problem and the subliminal channel // Proc. Workshop on Communications Security (Crypto`83), 1984. P. 51-67.

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

8. Хорошко, В.А. Методы и средства защиты информации : научное издание / В.А. Хорошко, А.А. Чекатков; Ред. Ю.С. Ковтанюк. – К. : ЮНИОР, 2003. – 505 с.

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

10. Кобозєва, А.А. Аналіз захищеності інформаційних систем / А.А. Кобозєва, І.О. Мачалін, В.О. Хорошко. – К. : Вид. ДУІКТ, 2010. – 316 с.

11. Fridrich J., Du R., Long M. Steganalysis of LSB encoding in color images // ICME, 2000.

12. Voloshynovskiy S., Pereira S., Iquise V., Pun T. Attack Modelling: Towards a Second Generation Watermarking Benchmark // Preprint. – University of Geneva, 2001. – 58p.

13. Стеганографія : навчальний посібник / О.О. Кузнецов, С.П. Євсеєв, О.Г. Король. – Х. : Вид. ХНЕУ, 2011. – 232 с.

14. Гонсалес Р. Цифровая обработка изображений (перевод с английского) / Р. Гонсалес, Р. Вудс, под ред. П.А. Чочиа – М.: Техносфера, 2005. – 1072 с.

15. Основи комп'ютерної стеганографії : навч. посібн. для студентів і аспірантів / В. О. Хорошко, О. Д. Азаров, М. В. Шелест та ін. – Вінниця : ВДТУ, 2003. – 143 с.

16. Анин Б. Ю. Защита компьютерной информации / Б. Ю. Анин. – СПб. : BHV-Санкт-Петербург, 2000. – 284 с.

17. Грибунин В. Г. Стеганографическая защита речевых сигналов в каналах открытой телефонной связи / В. Г. Грибунин, И. Н. Оков, И. В. Туринцев // Сборник тезисов Российской НТК "Методы и технические средства обеспечения безопасности информации". – СПб. : ГТУ, 2001. – С. 83–84.

18. Стасєв Ю. В. Основи теорії побудови сигналів / Ю. В. Стасєв. – Х. : ХВУ, 1999. – 87 с.

19. Термінологічний довідник з питань технічного захисту інформації / В. О. Хорошко, І. М. Огаркова, Д. В. Чирков та ін. ; за ред. проф. Хорошка В. О. – 3-тє вид., доп. і перероб. – К. : ТОВ "ПоліграфКонсалтинг", 2003. – 286 с.

20. A secure, robust watermark for multimedia / I. J. Cox, J. Kilian, T. Leighton, T. G. Shamoon // Information hiding: first international workshop. Lecture Notes in Comp. Science. – 1996. – Vol. 1174. – P. 183–206.

21. Chae J. J. A robust embedded data from wavelet coeffcients / J. J. Chae, D. Mukherjee, B. S. Manjunath // Proceedings of SPIE, Electronic Imaging, Storage and Retrieval for Image and Video Database. – 1998. – Vol. 3312. – P. 308–317.

22. Collberg C. On the limits of software watermarking / C. Collberg, C. Thomborson // Technical report, University of Auckland, New Zealand, 1998.

23. Corvi M. Wavelet-based image watermarking for copyright protection / M. Corvi, G. Nicchiotti // Scandinavian Conference on Image Analysis. – 1997.

24. Lu C.-S. Oblivious watermarking using generalized gaussian / C.-S.Lu, H.-Y. M. Liao // Proceedings of the 7th International Conference on Fuzzy Theory and Technology.– 2000. – P. 260–263.

25. Secure spread spectrum watermarking for images, audio and video / I. J. Cox, J. Kilian, T. Leighton, T. G. Shamoon // Proceedings of the IEEE International Conference on Image Processing. – 1996. – P. 243–246.

26. Жельников В. Криптография от папируса до компьютера. М.: ABF, 1996. – 335 с.

27. Johnson N., Jajodia S. Steganalysis of Images Created Using Current Steganographic Software // Proceeding of the Workshop on Information Hiding, 1998.

28. Patent US 5613004. Steganographic method and device / Marc Cooperman, Scott A. Moskowitz – 1997.

29. Романцев А.П. Статистический метод выявления стеганографического скрытия информации в звуковых файлах: Материалы Международного форума информатизации МФИ-2000. – М.: ЗАО "Информсвязьиздат". – 2000. – с.203-204.

30. Кнут Д. Искусство программирования на ЭВМ. Т.2: Получисленные алгоритмы. – М.: Мир. – 1977.

31. Симмонс Г. Дж. Обзор методов аутентификации информации. // ТИИЭР. – 1988. – Т. 76, № 5. – С. 105-125.

32. Калабеков Б.А. Микропроцессоры и их применение в системах передачи и обработки сигналов / Б.А. Калабеков – М.: Радио и связь, 1988. – 368 с.

33. Зюко А.Г. Теория передачи сигналов / А.Г. Зюко, Д.Д. Кловский, М.В. Назаров, Л.М. Финк. – Москва: Радио и связь, 1986. – 304 с.

34. Смид М.Э. Стандарт шифрования данных: Прошлое и будущее / М.Э. Смид, Д.К. Бранстед // ТИИЭР. – 1988. – Т. 76, №5. – С. 43-54.

35. Питерсон У., Уэлдон Э. Коды, исправляющие ошибки. – М.: Мир, 1976. – 352 с.

36. 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	26	
6	А4	Спеціальна частина	22	
7	А4	Економічний розділ	9	
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 Старостенко.ppt

2 Диплом Старостенко.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 Старостенко А.О. на тему: «Стеганографічне вбудовування цифрового водяного знака в завірене повідомлення»

Пояснювальна записка складається зі вступу, трьох розділів і висновків, розташованих на 77 сторінках.

Мета роботи є актуальною, оскільки вона спрямована на підвищення захищеності повідомлення, завіреного цифровим водяним знаком відправника, від навмисних дій зловмисника по зміні змісту повідомлення і його авторства.

При виконанні роботи автор продемонстрував добрий рівень теоретичних знань і практичних навичок. На основі аналізу принципів вбудовування цифрових водяних знаків і атак на стеганосистеми, а також існуючих підходів до формування і перевірки завіреного цифровим водяним знаком повідомлення в ній сформульовано задачі, вирішенню яких присвячений спеціальний розділ. У ньому було запропоновано підхід до формування і перевірки завіреного цифровим водяним знаком повідомлення із підвищеною захищеністю та оцінено його ефективність.

Практична цінність роботи полягає у тому, що запропонований підхід може бути використаний для встановлення справжності повідомлень переданих і збережених в сучасних інформаційно-телекомунікаційних системах.

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 автор Старостенко А.О. заслуговує на оцінку « » та присвоєння кваліфікації «Бакалавр з кібербезпеки» за спеціальністю 125 Кібербезпека.

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