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 магістра

студента *Зубова Дмитра Сергійовича*

академічної групи *125м-20-1*

спеціальності *125 Кібербезпека*

спеціалізації[1]

за освітньо-професійною програмою *Кібербезпека*

на тему *Забезпечення конфіденційності при передачі інформації з використанням вейвлет-перетворення сигналів*

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

Дніпро
20__

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

«_____»_____20___року

ЗАВДАННЯ
на кваліфікаційну роботу
ступеня магістра

студенту *Зубову Дмитру Сергійовичу* **академічної групи** *125м-20-1*
(прізвище ім'я по-батькові) (шифр)

спеціальності *125 Кібербезпека*

за освітньо-професійною програмою *Кібербезпека*

на тему *Забезпечення конфіденційності при передачі інформації з використанням вейвлет-перетворення сигналів*

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

Розділ	Зміст	Термін виконання
Розділ 1	Аналіз основ теорії вейвлет-аналізу і принципів передачі інформації в системах зв'язку з використанням теорії хаосу, а також існуючих підходів до виділення інформаційних повідомлень із хаотичного несучого сигналу на основі реконструкції динамічних систем.	03.09.2021 – 10.10.2021
Розділ 2	Дослідження підходу, заснованого на поєднанні техніки глобальної реконструкції і дискретного вейвлет-перетворення та оцінка його ефективності.	11.10.2021 – 24.11.2021
Розділ 3	Розрахунки капітальних витрат, економічного ефекту та терміну окупності капітальних інвестицій застосування запропонованих рішень.	25.11.2021 – 04.12.2021

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

Дата видачі: _____

Дата подання до екзаменаційної комісії: _____

Прийнято до виконання _____ Зубов Д.С.
(підпис студента) (прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 82 с., 27 рис., 4 додатки, 55 джерел.

Об’єкт дослідження – детерміновані хаотичні сигнали.

Предмет дослідження – підхід до забезпечення конфіденційності при передачі інформації з використанням техніки реконструкції динамічних систем та дискретного вейвлет-перетворення.

Мета кваліфікаційної роботи – підвищення завадостійкості при передачі інформації з використанням динамічного хаосу та дискретного вейвлет-перетворення сигналів.

Наукова новизна результатів полягає у тому, що дискретні вейвлети допомагають звести систему звичайних диференціальних рівнянь до системи рівнянь алгебри для визначення параметрів передавального генератора.

У першому розділі проаналізовано основи теорії вейвлетів і принципи передачі інформації в системах зв’язку з використанням теорії хаосу, а також існуючі підходи до виділення інформаційних повідомлень із хаотичного несучого сигналу на основі реконструкції динамічних систем.

У спеціальній частині роботи розглянуто і досліджено підхід, заснований на поєднанні техніки глобальної реконструкції та дискретного вейвлет-перетворення та оцінено його ефективність. За наслідками досліджень зроблено висновки щодо рішення поставленої задачі.

У економічному розділі виконані розрахунки капітальних витрат, економічного ефекту та терміну окупності капітальних інвестицій застосування запропонованих рішень.

ЦИФРОВА ОБРОБКА СИГНАЛІВ, КОНФІДЕНЦІЙНІСТЬ, КАНАЛ ЗВ’ЯЗКУ, ДЕТЕКТУВАННЯ, ХАОТИЧНІ СИГНАЛИ, РЕКОНСТРУКЦІЯ ДИНАМІЧНИХ СИСТЕМ, СИНХРОНІЗАЦІЯ, ВЕЙВЛЕТ-ПЕРЕТВОРЕННЯ, ІМІТАЦІЙНЕ МОДЕЛЮВАННЯ

РЕФЕРАТ

Пояснительная записка 82 с., 27 рис., 4 приложения, 55 источников.

Объект исследования – детерминированные хаотические сигналы.

Предмет исследования – подход к обеспечению конфиденциальности при передаче информации с использованием техники реконструкции динамических систем и дискретного вейвлет-преобразования.

Цель квалификационной работы – повышение помехоустойчивости при передаче информации с использованием динамического хаоса и дискретного вейвлет-преобразования сигналов.

Научная новизна результатов состоит в том, что дискретные вейвлеты помогают свести систему обычных дифференциальных уравнений к системе алгебраических уравнений для определения параметров передающего генератора.

В первой главе проанализированы основы теории вейвлетов и принципы передачи информации в системах связи с использованием теории хаоса, а также существующие подходы к выделению информационных сообщений из несущего хаотического сигнала на основе реконструкции динамических систем.

В специальной части работы рассмотрен и исследован подход, основанный на сочетании техники глобальной реконструкции и дискретного вейвлет-преобразования и оценена его эффективность. По результатам исследований сделаны выводы относительно решения поставленной задачи.

В экономическом разделе выполнены расчеты капитальных затрат, экономического эффекта и срока окупаемости капитальных инвестиций по применению предложенных решений.

ЦИФРОВАЯ ОБРАБОТКА СИГНАЛОВ, КОНФИДЕНЦИАЛЬНОСТЬ, КАНАЛ СВЯЗИ, ДЕТЕКТИРОВАНИЕ, ХАОТИЧЕСКИЕ СИГНАЛЫ, РЕКОНСТРУКЦИЯ ДИНАМИЧЕСКИХ СИСТЕМ, СИНХРОНИЗАЦИЯ, ВЕЙВЛЕТ-ПРЕОБРАЗОВАНИЕ, ИМИТАЦИОННОЕ МОДЕЛИРОВАНИЕ

ABSTRACT

Explanatory note: p. 82, fig. 27, 4 additions, 55 sources.

The object of study is deterministic chaotic signals.

The subject of research is the approach to ensuring confidentiality in the transmission of information using the technique of reconstruction of dynamic systems and discrete wavelet transform.

The purpose of the qualification work is to increase noise immunity in the transmission of information using dynamic chaos and discrete wavelet signal conversion.

The scientific novelty of the results is that discrete wavelets help to reduce the system of ordinary differential equations to a system of equations of algebra to determine the parameters of the transmitting generator.

The first section analyzes the basics of wavelet theory and the principles of information transmission in communication systems using chaos theory, as well as existing approaches to the extraction of information messages from a chaotic carrier signal based on the reconstruction of dynamic systems.

In a special part of the work the approach based on a combination of global reconstruction technique and discrete wavelet transform is considered and investigated 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, economic effect and payback period of capital investments are performed using the proposed solutions.

DIGITAL SIGNAL PROCESSING, CONFIDENTIALITY, COMMUNICATION CHANNEL, DETECTION, CHAOTIC SIGNALS, RECONSTRUCTION OF DYNAMIC SYSTEMS, SYNCHRONIZATION, WAVELET CONVERSION, SIMULATION MODELING

СПИСОК УМОВНИХ СКОРОЧЕНЬ

ВА – Вейвлет-аналіз;

ВП – Вейвлет-перетворення;

ВАХ – Вольт-амперна характеристика;

ВЧХ– Вейвлет-частотна характеристика;

ГІН – Генератор з інерційною нелінійністю;

ДС – Динамічна система;

ЛХП – Ляпуновські характеристичні показники;

СПІ – Системи передачі інформації;

CWT – Continuous Wavelet Transform – Безперервне вейвлет-перетворення;

DWT – Discrete Wavelet Transform – Дискретне вейвлет-перетворення.

ЗМІСТ

с.

ВСТУП ... 9

1 СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ ... 12

1.1 Передача інформації в системах зв'язку з використанням теорії хаосу ... 12

1.1.1 Розвиток теорії нелінійних процесів в системах зв'язку ... 12

1.1.2 Атрактори типу Лоренца ... 15

1.1.3 Приклад реконструкції динамічної системи Реслера ... 18

1.1.4 Схема Чуа ... 21

1.1.5 Схема кільцевого генератора ... 23

1.2 Основи теорії вейвлет-аналізу ... 24

1.2.1 Базисні функції ... 25

1.2.2 Безперервне вейвлет-перетворення ... 27

1.2.3 Дискретне вейвлет-перетворення ... 30

1.2.3.1. Дискретизація масштабу ... 30

1.2.3.2. Приклади вейвлетів для дискретного перетворення ... 32

1.3 Підходи до виділення інформаційних повідомлень із хаотичного несучого сигналу на основі реконструкції динамічних систем ... 35

1.4 Висновок. Постановка задачі ... 43

2 СПЕЦІАЛЬНА ЧАСТИНА ... 45

2.1 Детектування інформаційних сигналів на основі реконструкції динамічних систем і ДВП ... 45

2.1.1 Диференціювання сигналів із застосуванням дискретних вейвлетів ... 45

2.1.2 Детектування інформаційних сигналів з використанням дискретних вейвлетів ... 50

2.1.3 Визначення оптимального вейвлет-базису ... 55

2.2 Висновок ... 60

3 ЕКОНОМІЧНИЙ РОЗДІЛ ... 63

3.1 Розрахунок (фіксованих) капітальних витрат ... 63

3.1.1 Визначення трудомісткості розробки підходу щодо

забезпечення конфіденційності при передачі інформації
з використанням вейвлет-перетворення сигналів 63
3.1.2 Розрахунок витрат на розробку підходу щодо
забезпечення конфіденційності при передачі інформації
з використанням вейвлет-перетворення сигналів 64
3.1.3 Розрахунок поточних витрат 66
3.2 Оцінка можливого збитку 68
3.2.1 Оцінка величини збитку 68
3.2.2 Загальний ефект від впровадження системи інформаційної безпеки 68
3.3 Визначення та аналіз показників економічної ефективності
системи інформаційної безпеки 69
3.4 Висновок 70
ВИСНОВКИ 71
ПЕРЕЛІК ПОСИЛАНЬ 73
ДОДАТОК А. Відомість матеріалів кваліфікаційної роботи 79
ДОДАТОК Б. Перелік документів на оптичному носії 80
ДОДАТОК В. Відгук керівника економічного розділу 81
ДОДАТОК Г. Відгук керівника кваліфікаційної роботи 82

ВСТУП

Вейвлет-перетворення (ВП) – це напрямок в області цифрової обробки сигналів, який наразі успішно розвивається. Він виник в кінці минулого століття, що спричинило за собою зростання наукового інтересу до теорії і техніки обробки сигналів, зображень та часових рядів. Відомо [1], що ВП добре пристосоване для вирішення сформованих задач і абсолютно виправдано при вивченні структури неоднорідних сигналів.

Вейвлет перетворення є потужним інструментом аналізу, застосовним до коротких, зашумлених і нестаціонарних випадкових процесів. Незважаючи на значні успіхи теорії вейвлетів та її численні застосування у вирішенні великої кількості завдань, нині активно використовується лише частина її потенційних можливостей.

Наразі значний інтерес викликають комбіновані підходи, що базуються на поєднанні вейвлетів з іншими методами аналізу структури сигналів. Подібне поєднання дозволяє вирішувати різні завдання – від розпізнавання образів та кількісного опису складних нестаціонарних процесів до покращення характеристик систем зв'язку.

Одним із напрямків у сучасній нелінійній динаміці є завдання реконструкції динамічних систем (ДС). Інтерес до цього завдання був викликаний появою робіт [2-3]. У першій з них було показано, що фазовий портрет атрактора ДС може бути відновлений за скалярним часовим рядом $a_i=a(i\Delta t)$, якщо як відсутні координати вектора стану використовується той же самий ряд a_i, взятий з деяким запізненням. У [3] можливість реконструкції фазового портрета атрактора по одновимірній реалізації одержала теоретичне обґрунтування у вигляді теореми Такенса.

Слід зазначити, що поява широкого кола прикладних завдань у сучасній нелінійній динаміці (у тому числі завдання захищеної передачі інформації) в останні роки зумовлено розвитком уявлень про динамічний хаос, зокрема явище хаотичної синхронізації. Саме ефект хаотичної синхронізації

використовували автори перших робіт щодо здійснення конфіденційності переданої інформації, що застосовували широкополосні коливання генератора хаосу як маскуючого [4] або несучого сигналу [5-6]. Але методи, що ґрунтуються на явищі синхронізації, не позбавлені низки недоліків.

Отже, вейвлет перетворення має низку корисних властивостей. Одним із них є можливість проводити чисельне диференціювання зашумлених сигналів шляхом переходу в простір вейвлет-коефіцієнтів. Особливістю таких підходів є те, що похідна сигналу може бути замінена похідною базисної функції, заданої в аналітичній формі. Ця властивість дозволяє ефективно вирішувати завдання синтезу. Спільне використання вейвлетів та техніки реконструкції динамічних систем є новим напрямом, що дозволяє розробляти ефективні методи оцінок параметрів автоколивальних режимів, що відкриває широкі перспективи вирішення завдань прихованої передачі інформації із застосуванням хаотичних несучих сигналів.

Таким чином, дослідження і вдосконалення підходів до забезпечення конфіденційності при передачі інформації зі спільним використанням динамічного хаосу та вейвлет-перетворення сигналів, наразі є актуальною задачею.

Метою роботи є підвищення завадостійкості при передачі інформації з використанням динамічного хаосу та дискретного вейвлет-перетворення сигналів.

Постановка задачі:

• проаналізувати основи теорії вейвлет-аналізу, а також принципи прихованої передачі інформації в системах зв’язку з використанням теорії хаосу;

• провести аналіз існуючих підходів до виділення інформаційних повідомлень із хаотичного несучого сигналу на основі реконструкції динамічних систем;

• розглянути і дослідити підхід до прихованої передачі інформації, заснований на поєднанні техніки глобальної реконструкції та дискретного вейвлет-перетворення;

• оцінити ефективність дослідженого підходу.

1 СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ

1.1 Передача інформації в системах зв'язку з використанням теорії хаосу

1.1.1 Розвиток теорії нелінійних процесів в системах зв'язку

Основою впровадження досягнень фундаментальних досліджень теорії нелінійних коливань та хаотичних процесів є три видатні наукові досягнення: винайдення відносно нескладних електронних схем, що здатні генерувати хаотичні коливання, відкриття явища синхронізації систем із хаотичною динамікою та існування атрактора траєкторій системи у фазовому просторі (рис. 1.1) [7].

Рисунок 1.1 – Фундаментальні віхи у галузі хаотичної динаміки

У 1975 році явище виникнення хаотичних коливань було встановлено Т. Лі та Д. Йорком. Ними у роботі «Period three implies chaos» [8], було вперше

показано, що відносно нескладне відображення може генерувати складну динаміку та запропонований термін «хаос» для одновимірного відображення, що описується узагальненим логістичним відображенням:

$$x_{n+1} = x_n \cdot (1 - x_n / K), \quad (1.1)$$

де x_n, x_{n+1} – поточне та наступне значення.

Винайдення електронних схем, що генерують хаотичні коливання, відноситься до початку 80-х рр. XX ст. [9-11]. Їх розробленню передували численні електричні схеми генерування періодичних коливань із загальною назвою – мультивібратори. До найбільш ранніх із них відносяться схеми, основою функціонування яких були напівпровідникові транзистори та електронні лампи.

Майже одночасно і практично незалежно один від одного ряд інженерів-електроніків прийшли до загального висновку що генерування хаотичних коливань електронними схемами можливе при наявності в них електронних компонентів з нелінійними характеристиками. Серед перших винахідників генераторів хаотичних коливань були: Леон Чуа, Т. Лі, Ван дер Поль, Колпітц. Винайдення таких схем дозволило перенести абстрактні математичні моделі у галузь електронної інженерії [13].

Другим фундаментальним відкриттям є відкрите Каролем та Пекорою у 1990 р. явище синхронізації двох хаотичних систем, при певних співвідношеннях між значеннями їх параметрів [12]. За результатами досліджень, що активно проводяться впродовж декількох десятків років можна здійснити класифікацію основних видів синхронізації (рис. 1.2).

Режим повної синхронізації хаосу означає точне співпадання векторів стану систем, що взаємодіють між собою, за умови повної ідентичності їх параметрів. Явище повної синхронізації має місце для неперервних та дискретних хаотичних систем [13].

Під фазовою синхронізацією розуміють захоплення фаз та середніх частот хаотичних коливань. Недосконалу фазову синхронізацію можна розглядати як захоплення середніх частот. В останньому випадку розрізняють

синхронні режими, при яких частоти взаємодіючих систем співвідносяться як деякі цілі числа (m:n синхронізація) [7, 14].

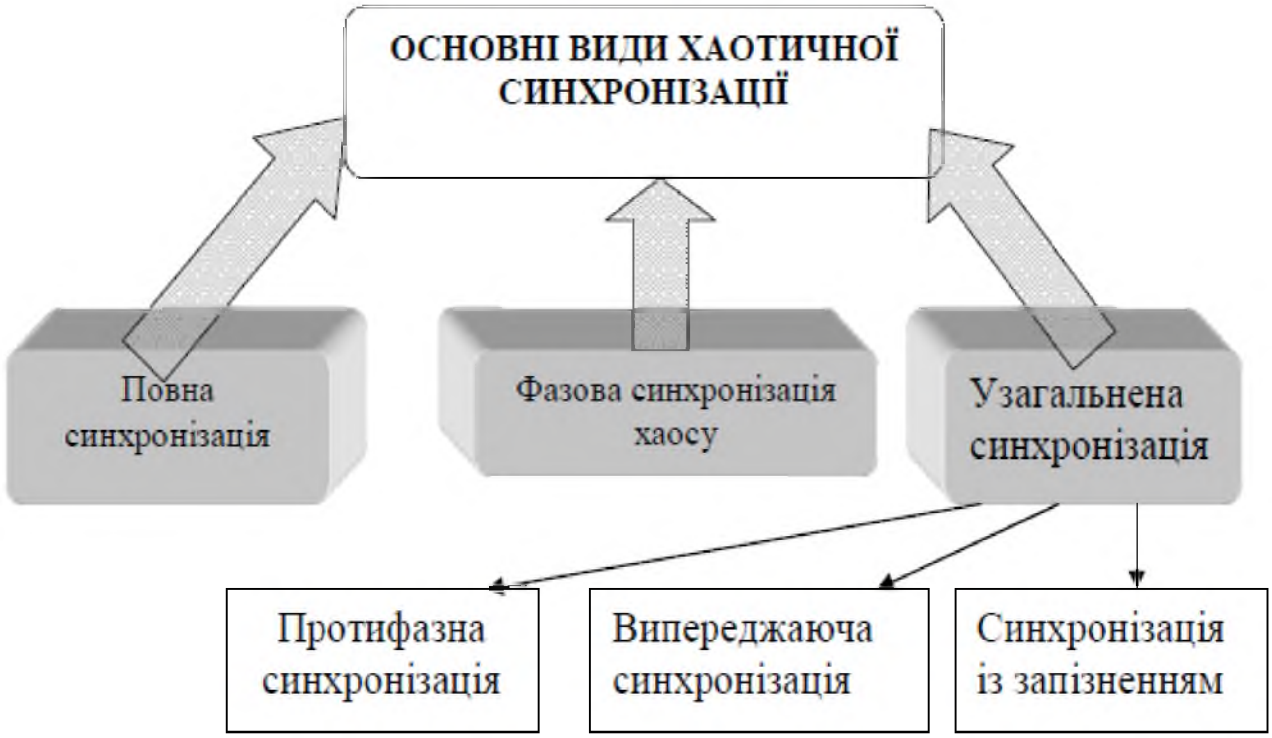


Рисунок 1.2 – Основні види хаотичної синхронізації

Узагальнена синхронізація хаосу означає, що після закінчення перехідних процесів між станами двох (чи більше) хаотичних систем встановлюється функціональна залежність [7].

Як і у випадку повної синхронізації, поняття узагальненої синхронізації еквівалентне асимптотичній стійкості веденої системи. Критерієм існування узагальненої синхронізації є від'ємний старший показник Ляпунова веденої системи. Для виявлення можливості узагальненої синхронізації існує декілька методів: аналіз умовних показників Ляпунова, «найменшої взаємної похибки найближчих траєкторій» та «середньої умовної дисперсії» допоміжної системи.

Узагальнена синхронізація є найбільш перспективною для використання в системах прихованого передавання даних за рахунок складної та неявної залежності між станами ведучої – веденої систем і високої стійкості до шумів. Недавно узагальнену синхронізацію експериментально спостерігали між

високочастотними хаотичними генераторами мікрохвильового діапазону, що є додатковим аргументом для проведення досліджень, оскільки такі системи передачі інформації (СПІ) можна буде використовувати для високошвидкісного передавання інформації [7].

Третім фундаментальним відкриттям у галузі моделювання систем із хаотичною динамікою було встановлення існування атрактора у вигляді фрактальної множини точок фазового простору, до якої прямують фазові траєкторії системи з розвитком у часі [14]. Закономірності, що пов'язані з цим явищем є основою багатьох базових технологій, що використовують явище синхронізації.

До зазначених закономірностей відносяться: надзвичайна чутливість до початкових умов системи та властивість перемішування. Перша властивість була помічена і названа «ефектом метелика» ще Е. Лоренцом (за його словами, якщо на півночі метелик змахне крилами, то на півдні виникне буря) [15].

Будь-які достатньо сильні нерегулярності, що зустрічаються у природі з плином часу отримують фрактальну структуру. Тому виявляється, що реально існуючі нелінійні динамічні системи мають фрактальні атрактори (наприклад, атрактори Лоренца та Реслера). Це означає, що надзвичайно нестійкі фазові траєкторії таких систем протягом часу перетворюються на фрактали. Дослідження самоподібності процесів у природі висвітлено у ряді літературних джерел [16].

Ці новаторські на той час результати теоретичних досліджень були використані у моделюванні систем передавання інформації з використанням детермінованого хаосу. Прикладом таких систем є прямохаотичні широкосмугові системи зв'язку [17-18].

1.1.2 Атрактори типу Лоренца

Найбільш традиційними математичними моделями, що служать для обчислювальних експериментів з системами ППІ, є широко відомі моделі

Ресслера Лоренца, Чуа та інші. Основними перевагами цих моделей є як математична простота, так і достатня вивченість хаотичної поведінки. Крім того, існує значна кількість робіт, присвячених апаратній реалізації хаотичних генераторів, побудованих на зазначених моделях.

Слід зазначити, що математичні моделі радіотехнічних схем дозволяють спростити та зменшити час, необхідний для їх дослідження. Найпростіші хаотичні системи (схема Чуа, кільцевий генератор, генератор з інерційним нелінійним елементом) є низькочастотними, а їх спектр знаходиться в діапазоні звукових частот. З розвитком засобів інформаційних технологій встановилася стійка тенденція підвищення та розширення спектру несучих частот до 10 ГГц.

При розробленні математичних моделей систем зв'язку в безрозмірних змінних їх доцільно описувати якомога меншою кількістю параметрів. Безрозмірні змінні отримуються нормуванням розмірних величин до величин однакової розмірності. Нормування змінних можна здійснювати на значення, що характеризують поведінку систем, залишаючись при цьому постійними в часі. Прикладом величин, на які можуть бути нормовані змінні, є напруга живлення, максимальне чи мінімальне значення сигналів системи, для хаотичних систем – точки зміни нахилу нелінійних характеристик їх елементів. Масштабування часу доцільно здійснювати відносно резонансних частот коливальних контурів (або основної частоти коливань) та частоти зрізу фільтрів.

Рівняння Лоренца були отримані з рівнянь Нав'є-Стокса в задачі про теплову конвекцію і мають вигляд [19]:

$$\begin{aligned} \dot{x} &= -\sigma(x - y), \\ \dot{y} &= rx - y - xz, \\ \dot{z} &= xy - bz, \end{aligned} \tag{1.2}$$

де σ, b і r – керуючі параметри.

Відзначимо, що в системі (1.2) режим квазігіперболічного хаосу реалізується в кінцевій області значень її керуючих параметрів. На рис. 1.3

представлена біфуркаційна діаграма системи. Існуванню атрактора Лоренца відповідає заштрихована область в параметричному просторі.

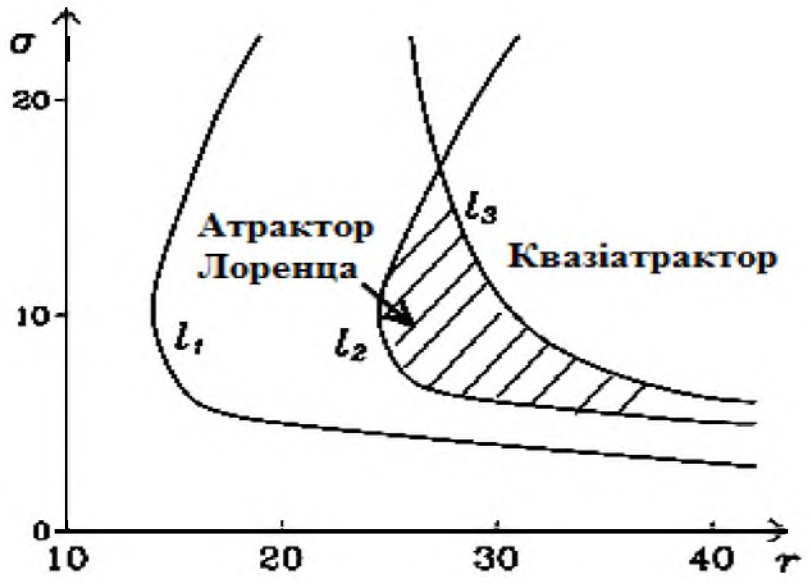


Рисунок 1.3 – Біфуркаційна діаграма системи Лоренца на площині параметрів r і σ для b=8/3

Фазовий портрет атрактора Лоренца представлений на рис. 1.4,*а*. Поза зазначеної області властивості хаотичного атрактора будуть іншими: атрактор Лоренца трансформується в квазіатрактор.

Назвемо типові властивості атрактора Лоренца. Спектр ляпуновських характеристичних показників (ЛХП) не змінюється при варіації початкових умов, оскільки атрактор Лоренца є єдиним, басейном тяжіння якого служить весь фазовий простір; спектр ЛХП практично не змінюється, якщо варіювати керуючі параметри системи в області існування атрактора Лоренца.

Ці властивості наочно ілюструють грубість атрактора Лоренца з точки зору експерименту: структура атрактора зберігається при варіації параметрів і початкових умов, біфуркації атрактора відсутні. Наслідком хаотичної динаміки є характерний вид автокореляційної функції, яка експоненційно спадає зі збільшенням часу практично монотонно, що ілюструє рис. 1.4,*б*.

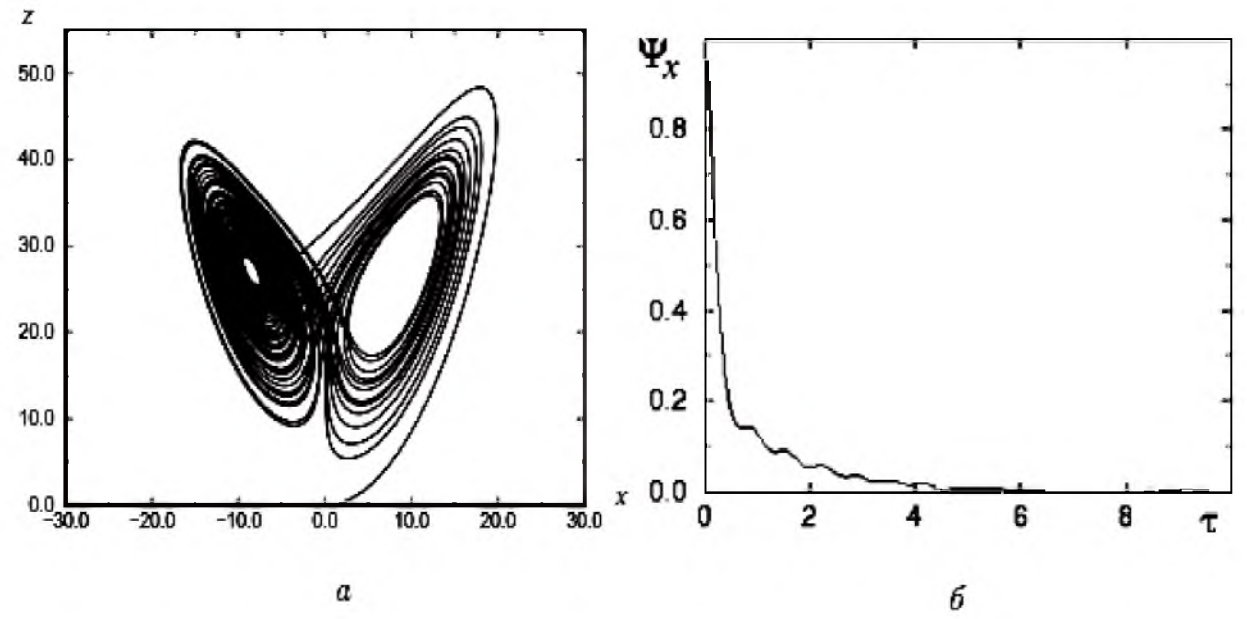


Рис. 1.4 – Фазовий портрет (*а*) і автокореляційна функція (*б*) атрактора Лоренца (при $\sigma = 10$, $r = 28$ і $b = 8/3$)

1.1.3 Приклад реконструкції динамічної системи Реслера

Розглянемо конкретний приклад застосування описаного алгоритму. З цією метою виберемо відому динамічну систему Реслера (R.Roessler) [19]:

$$\begin{aligned} dx/dt &= -y - z, \\ dy/dt &= x + ay, \\ dz/dt &= b - cz + xz, \end{aligned} \qquad (1.3)$$

яка описує режим неперіодичних коливань. При значеннях параметрів a=0.15, b=0.2, c=10.0 система (1.3) характеризується режимом дивного атрактора

Використаємо в якості одновимірного часового ряду a_i залежність в часі однієї з координат $y(i\Delta t)$, отриману чисельною інтеграцією рівнянь (1.3). Будемо вважати, що вид системи (1.3) і її розмірність нам невідомі. Спостережувана $a(t)=y(t)$, задана на кінцевому інтервалі часу $0 \le t \le 100$, представлена на рис. 1.5,*а*.

Для завдання вектора стану реконструйованої системи скористаємося теоремою Такенса. Розраховуючи по спостережуваній $a(t)$ автокореляційну функцію, знаходимо час спадання її до нуля $\tau_0 \approx 1.6$ і використаємо цю величину

в якості часу затримки. На рис. 1.5,*б* представлена проекція реконструйованого атрактора на площину двох змінних: $x_1(t)=y(t)$ і $x_2(t)=y(t+\tau)$.

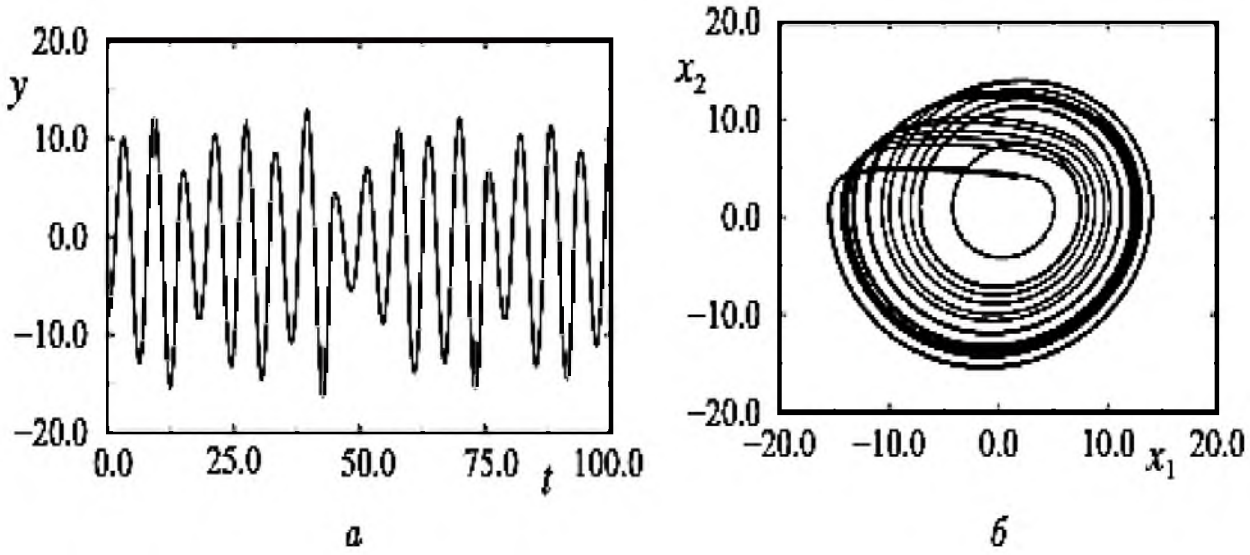


Рисунок 1.5 – Часова залежність координати $y(t)$ системи Реслера (*а*) та реконструйований атрактор в проекції на площину $(y(t), y(t+\tau))$ (*б*)

Для визначення розмірності модельної системи потрібно розрахувати розмірність атрактора і розмірність простору вкладення. Для оцінки розмірності атрактора обчислимо його кореляційну розмірність D_c, використовуючи спеціальний алгоритм.

На рис. 1.6 наведені результати розрахунку залежності D_c від $\lg \varepsilon$, де ε – розмір осередку розбивки фазового простору. Як видно з графіків, незалежно від розмірності простору вкладення n, є «поличка» на рівні $D_c \approx 1.9$, який і приймаємо за значення шуканої розмірності.

Таким чином, реконструйований атрактор має розмірність $D \approx 2$ і може бути «вкладений» в тривимірний фазовий простір. Це означає, що ми можемо шукати модельну ДС у вигляді системи звичайного диференціального рівняння третього порядку ($n=3$).

Шукану систему запишемо у формі Коші, використовуючи поліноміальну апроксимацію і обмежившись значенням $n=3$ і $v=2$.

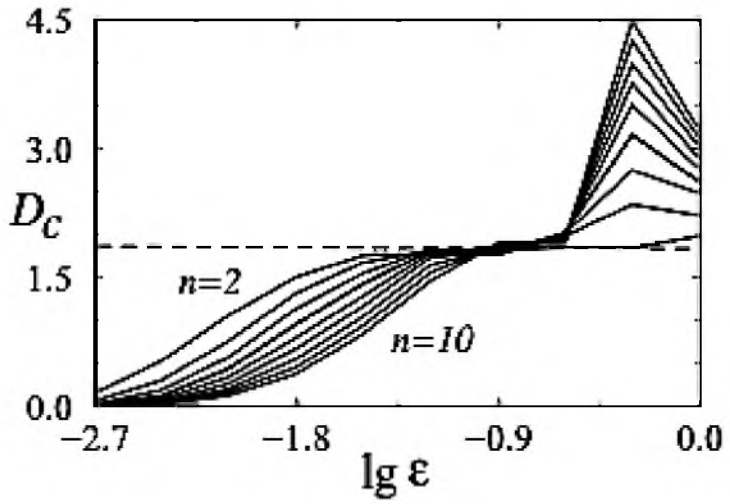


Рисунок 1.6 – Результати розрахунку кореляційної розмірності D_c при варіюванні розмірності простору вкладення n

Результати інтегрування модельної ДС представлені на рис. 1.7 у вигляді залежності $x_1(t)$.

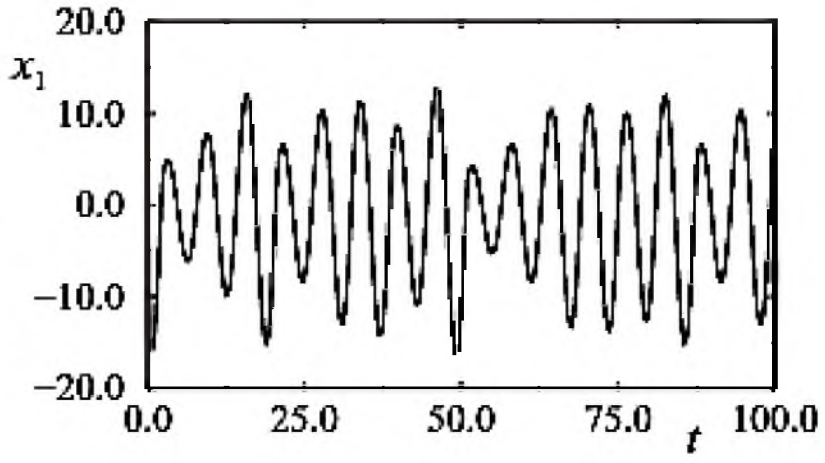


Рисунок 1.7 – Залежність $x_1(t)$, отримана чисельним інтегруванням реконструйованої системи

Слід визначити чи можливо за допомогою реконструйованої системи здійснювати прогноз еволюції системи в часі за межами інтервалу, на якому нам відома спостережувана.

З цією метою було проведено наступний експеримент. Було взято в якості початкового значення координату останньої точки спостережуваної (рис. 1.5,*а*) в момент часу t_0=100. Далі було проінтегровано як вихідну, так і модельну системи з початковими умовами при $t=t_0$ і порівняно результати для $t>t_0$.

На рис. 1.8 наведені відповідні графіки залежностей $y(t)$ для тестової системи і x_1(t) для реконструйованої ДС. Пунктирною лінією тут показано результат інтегрування системи, суцільною лінією – рішення реконструйованої модельної системи.

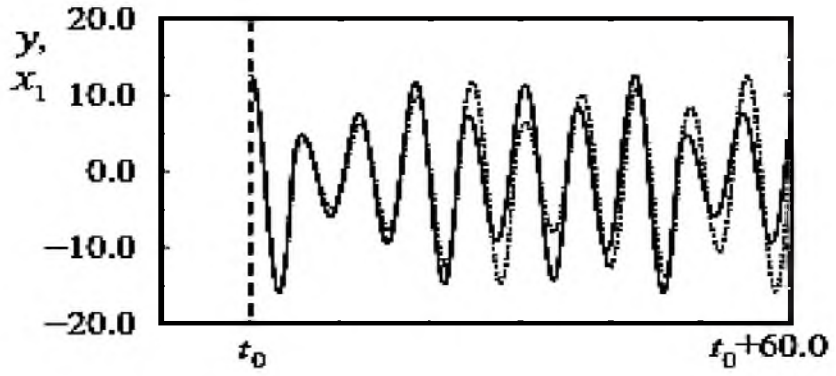


Рисунок 1.8 – Прогноз поведінки системи (5.62) після закінчення спостереження за сигналом, що генерується цією системою (час t_0)

Як випливає з рис. 1.8, прогноз еволюції системи в часі здійснюється з деякою похибкою, яка з часом наростає. Конкретний час прогнозу можна вказати, задавши точність передбачення.

З результатів рис. 1.8 також випливає те, що якщо обмежитися похибкою ±5%, то час передбачення в нормованих одиницях становитиме приблизно T=12, тобто близько двох базових квазіперіодів коливань системи.

1.1.4 Схема Чуа

Схема Чуа (рис. 1.9) складається з резонансного LC-контуру, інерційної RC-ланки та нелінійного елемента, вольт-амперна характеристика (ВАХ) якого

є нелінійною. Нелінійний елемент може бути реалізованим на двох операційних підсилювачах (ОП), на двох діодах і ОП та у вигляді кубічної нелінійності.

Описавши схему Чуа (рис. 1.9) за допомогою законів Кірхгофа, отримаємо наступну систему диференційних рівнянь:

$$\begin{cases} C_1 \cdot \dfrac{dU_{C1}}{dt} = \dfrac{U_{C2} - U_{C1}}{R} + \dfrac{U - U_{C1}}{R} - i(U_{C1}) \\ C_2 \cdot \dfrac{dU_{C1}}{dt} = i_L - \dfrac{U_{C2} - U_{C1}}{R} \\ L \cdot \dfrac{di_L}{dt} = -U_{C2} - i_L \cdot R \end{cases} \quad (1.4)$$

де U_{C1}, U_{C2} – напруги на конденсаторах C_1 та C_2, відповідно; i_L – струм, що протікає через котушку індуктивності; $i(U_{C1})$ – струм, що протікає через нелінійний елемент:

$$i(U_{C1})=K_0U_{C1}+1/2(K_1-K_0)[|U_{C1}+1|+|U_{C1}-1|], \quad (1.5)$$

де K_0, K_1 – коефіцієнти.

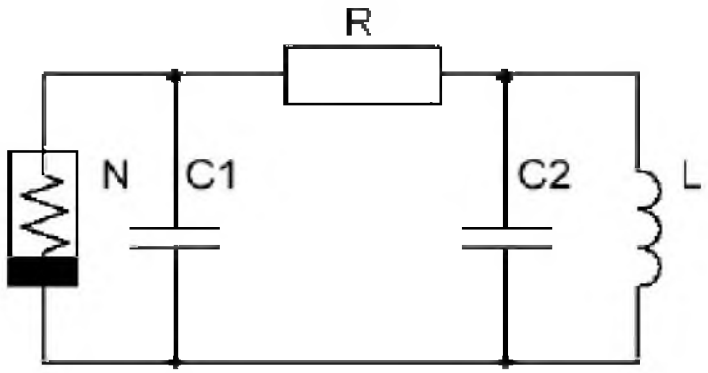


Рисунок 1.9 – Схема Чуа

Вольт-амперна характеристика нелінійного елемента, що наведена на рис. 1.10, є кусково-лінійною функцією.

Схема Чуа має три точки рівноваги зі значеннями напруги $U_{C1}=\pm B$ та $U_{C1}=0$, де B – значення напруги в точці перегину ВАХ нелінійного елемента (рис. 1.10).

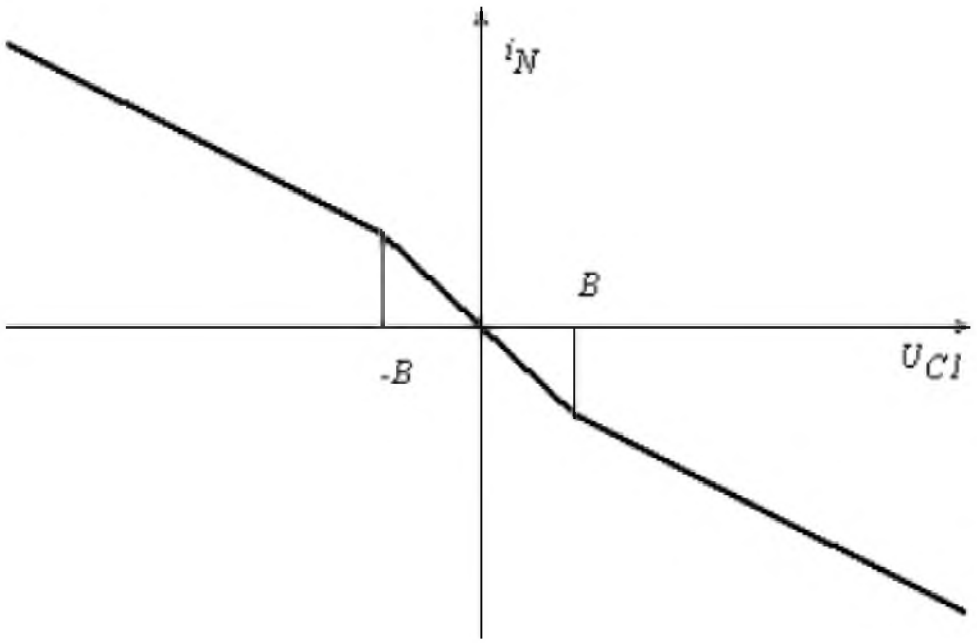


Рисунок 1.10 – Вольт-амперна характеристика нелінійного елемента схеми Чуа

1.1.5 Схема кільцевого генератора

Розглянемо схему кільцевого генератора, що складається із послідовно з'єднаних і замкнених в коло оберненим зв'язком двох фільтрів низьких частот (ФНЧ) та нелінійного елемента (рис. 1.11) [1]. Записавши закони Кірхгофа для схеми кільцевого генератора отримаємо наступну систему диференційних рівнянь:

$$\begin{cases} C_1 \cdot \dfrac{dU_{C1}}{dt} = \dfrac{F\left(U_{C_2}\right) - U_{C_1}}{R_1} \\ C_2 \cdot \dfrac{dU_{C1}}{dt} = i_L \\ L \cdot \dfrac{di_L}{dt} = U_{C1} - i_L \cdot R_2 - U_{C2} \end{cases} \tag{1.6}$$

Вольт-вольтна характеристика нелінійного елемента описується наступним рівнянням:

$$F(U) = M \cdot \left(\left|U_{C2} + B_1\right| - \left|U_{C2} - B_1\right| + \left|U_{C2} - B_2\right| - \left|U_{C2} + B_2\right|\right). \tag{1.7}$$

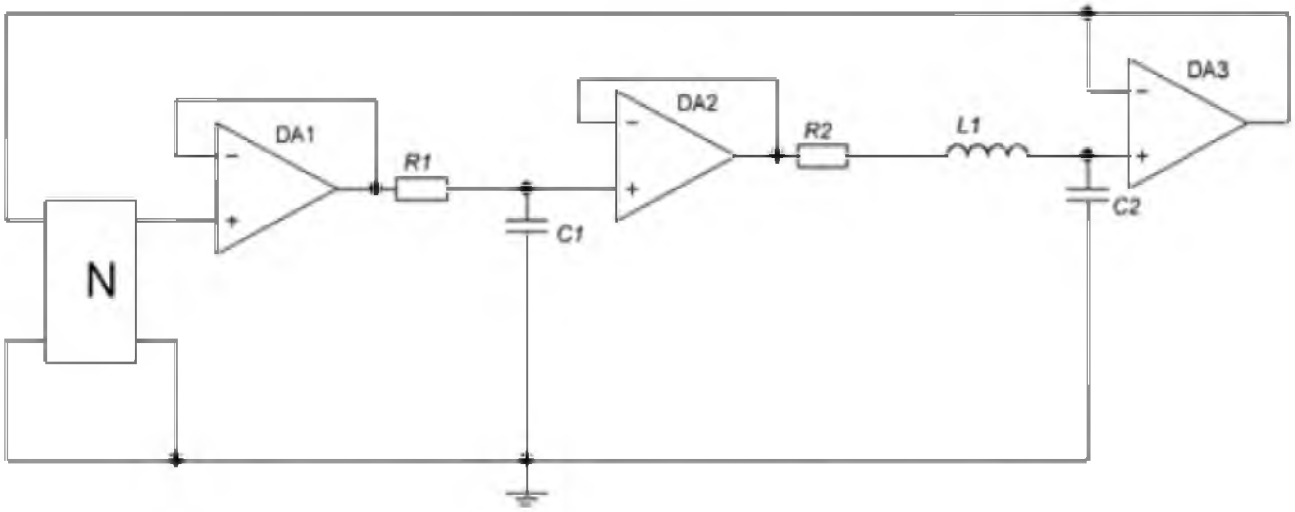


Рисунок 1.11 – Схема кільцевого генератора хаосу

Вольт-вольтна характеристика нелінійного елемента, представлена на рис. 1.12.

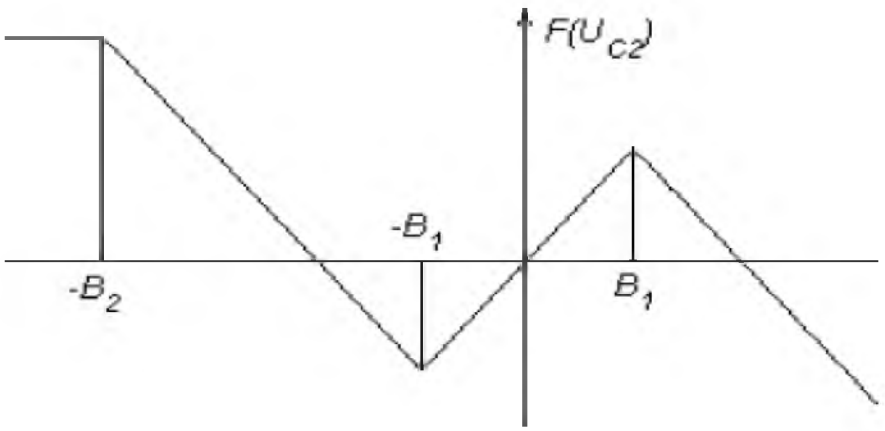


Рисунок 1.12 – Вольт-вольтна характеристика нелінійного елемента кільцевого генератора хаосу

1.2 Основи теорії вейвлет-аналізу

Вейвлет-аналіз став фактично стандартним інструментом для дослідження частотно-часової поведінки сигналів. На відміну від класичних методів аналізу Фур'є, які являють собою сигнали у вигляді комплексного гармонічного спектра, вейвлет-аналіз дає опосередковану інформацію про частотний склад сигналу та його зміну в часі. Це досягається через розклад

сигналу на сукупність складових з компактним носієм, кожна з яких є розтягнутою або стиснутою копією єдиної материнської вейвлет функції [1, 19-26].

ВП необхідне для аналізу структури і поведінки сигналів, які містять у собі ділянки різної тривалості з коливаннями різної швидкості або різної частотної наповненості. Часто в літературі такі сигнали називають «нестаціонарними», маючи на увазі, що їх спектральні характеристики досить істотно змінюються з часом, причому ці зміни можуть відбуватися протягом різного періоду. Для такого випадку, коли в сигналі є локалізовані в часі ділянки різних частотних властивостей, використовується розклад у набір вейвлет-функцій, які самі є також локалізованими в часі і мають різний спектральний склад.

Такий розклад гарантує проведення локального аналізу сигналу: якщо певний коефіцієнт розкладу сигналу є великим, то можна визначити ту ділянку часу, якій він відповідає, а отже, проаналізувати її більш детально і визначити, яким є частотний склад тієї ділянки сигналу та її тривалість. Скрізь, де треба дослідити нерегулярності в сигналах, альтернативи ВП майже немає. Внаслідок названих унікальних можливостей, поряд із плідним розвитком математичної теорії вейвлетів, різноманітні модифікації вейвлет-аналізу набули бурхливого розвитку.

1.2.1 Базисні функції

Взагалі частотно-часовий аналіз призначений для виявлення локальних частотно-часових збурень сигналу [19]. Унаслідок короткочасності таких збурень, сам сигнал може розглядатися як заданий в просторі L_2, тобто для одновимірних сигналів – на всій дійсній вісі $R(-\infty, \infty)$ з нормою $\|f(t)\|^2 < \infty$.

Отже, базисні функції (які отримали назву вейвлетів), також повинні належати L_2 і швидко спадати при $t \to \infty$. Тоді, щоб перекрити такими базисними функціями усі можливі часові положення сигналу, необхідно, щоб базисні

функції являли собою набір зміщених у часі функцій. Зручніше за все, якщо цей набір утворюється з однієї і тієї ж «материнської» функції $\psi(t)$ (прототипу), зсунутої по вісі t, тобто $\{\psi(t-b)\}$.

Щоб забезпечити частотний аналіз, базисна функція повинна мати ще один аргумент – масштабний коефіцієнт, який є аналогом частоти в Фур'є-аналізі. Тоді базисні функції для частотно-часового аналізу матимуть наступний вигляд

$$\psi\left(\frac{t}{a}-\frac{b}{a}\right)=\psi\left(\frac{t-b}{a}\right); \quad a,b,\in R, \tag{1.8}$$

де масштабний коефіцієнт a введений як дільник t, причому масштабуванню піддається також і зсув b.

Це дозволяє зберегти відносну «щільність» розташування базисних функцій по вісі t при розширенні або стисненні самої функції і при $a/b=\Delta=const$ (рис. 1.13).

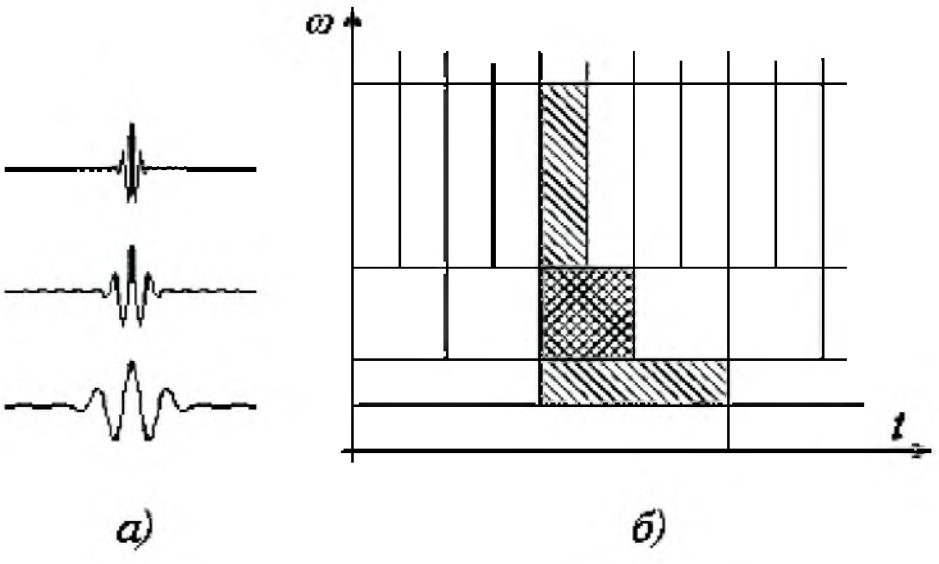


Рисунок 1.13 – Базисні функції вейвлет при масштабах $a - 2k$, $k = 0,1, 2$ ($а$) і їх зображення в площині час-частота ($б$)

Таким чином, базисні функції для частотно-часового аналізу повинні мати наступні властивості.

Обмеженість, тобто належність L_2

$$\int_{-\infty}^{\infty} |\psi(t)|^2 \, dt < \infty. \tag{1.9}$$

Локалізація. Базисні функції вейвлет-аналізу (ВА), на відміну від перетворення Фур'є, повинні бути локалізовані, тобто визначені на кінцевому інтервалі як в часовій, так і в частотній областях. Для цього достатньо, щоб виконувались умови:

$$|\psi(t)| \le C\left(1+|t|\right)^{-1-\varepsilon}; \quad |\psi(\omega)| \le C\left(1+|\omega|\right)^{-1-\varepsilon} \tag{1.10}$$

при $\varepsilon > 0$.

Нульове середнє. Рівність нулю нульового моменту

$$\int_{-\infty}^{\infty} \psi(t) = 0 \tag{1.11}$$

або, що іноді необхідно – рівність нулю моменту m-го порядку

$$\int_{-\infty}^{\infty} t^m \psi(t) = 0. \tag{1.12}$$

Це вейвлети m-го порядку, що дозволяють аналізувати більш тонку структуру сигналу, пригнічуючи його складові, які повільно змінюються.

1.2.2 Безперервне вейвлет–перетворення

Введемо базис, який відповідає наведеним вище умовам [19]:

$$\psi_{a,b}(t) = \frac{1}{\sqrt{|a|}} \psi\left(\frac{t-b}{a}\right), \tag{1.13}$$

де множник $\frac{1}{\sqrt{|a|}}$ необхідний для збереження норми $\left\|\psi_{a,b}(t)\right\| = \left\|\psi(t)\right\|$.

Нехай a, $b \in R$, тобто приймають довільні речові значення, тоді пара перетворень, що носить назву безперервного вейвлет перетворення (CWT – Continuous Wavelet Transform), буде мати вигляд:

$$CWT_f(a,b)=\left\langle f(t),\psi_{a,b}(t)\right\rangle=\frac{1}{\sqrt{|a|}}\int_{-\infty}^{\infty}f(t)\psi\left(\frac{t-b}{a}\right)dt, \qquad (1.14)$$

$$f(t)=C_\psi^{-1}\int_{-\infty}^{\infty}\frac{da}{a^2}\int_{-\infty}^{\infty}CWT_f(a,b)\psi\left(\frac{t-b}{a}\right)db, \qquad (1.15)$$

де нормалізуючий коефіцієнт

$$C_\psi=\int_{-\infty}^{\infty}\frac{|\Psi(\omega)|^2}{|\omega|}d\omega<\infty. \qquad (1.16)$$

Інтегруванням (1.16) за частинами можна переконатися у тому, що ця умова завжди виконується, якщо $\Psi(\omega)=0$ при $\omega=0$ і, отже, дорівнює нулю принаймні, нульовий момент функції $\psi(t)$.

Наведемо приклади материнських вейвлетів, які формують базис (1.13). Найбільшою популярністю наразі користуються функції на основі похідних функції Гауса:

$$\psi_m(t)=(-1)^m\frac{d^m}{dt^m}\exp\left\{-\frac{t^2}{2}\right\}. \qquad (1.17)$$

Це викликано тією обставиною, що функція Гауса має найкращі показники локалізації як в часовій, так і в частотній областях.

При m=1 отримуємо вейвлет (рис. 1.14,*а*), який називають WAVE-вейвлет з рівним нулю нульовим моментом.

При m=2 отримуємо вейвлет (рис. 1.14,*б*), званий як «мексиканський капелюх» – MHAT-вейвлет:

$$\psi(t)=\frac{2}{\sqrt{3}}\pi^{1/4}\left(1-t^2\right)e^{t^2/2}, \qquad (1.18)$$

у якого нульовий і перший моменти дорівнюють нулю. Спектр Фур'є цього вейвлета більш вузький, тому він має кращу роздільність.

Функція Гауса утворює також DOG-вейвлет – різницю двох Гаусіан:

$$\psi(t)=\exp\left\{-\frac{t^2}{2}\right\}-0{,}5\left\{-\frac{t^2}{8}\right\}. \qquad (1.19)$$

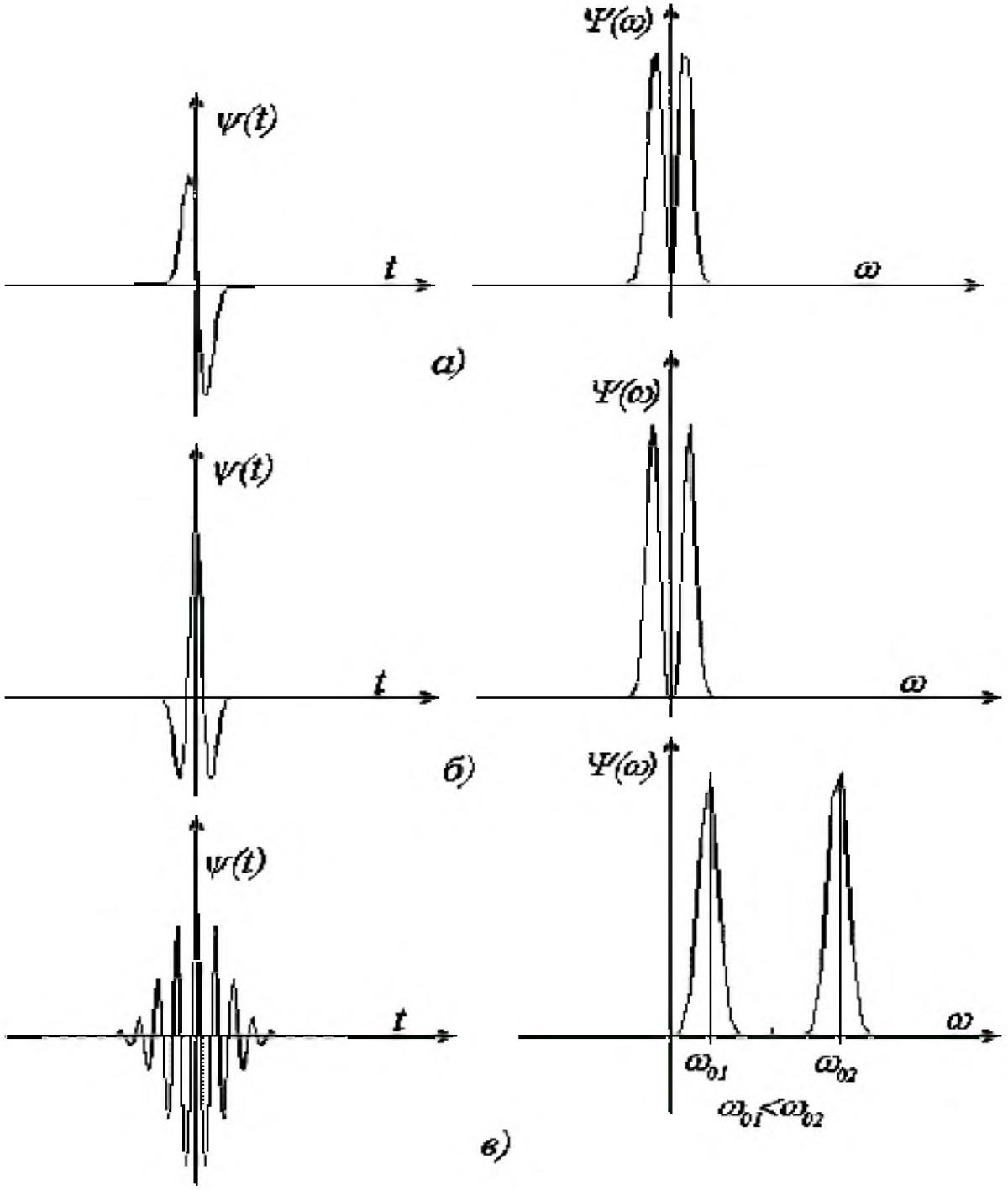


Рисунок 1.14 – Приклади базисних функцій WAVE-вейвлета (*а*), MHAT-вейвлета (мексиканський капелюх) (*б*) і вейвлета Морле (*в*)

Широке поширення отримав також вейвлет Морле (Morlet) (рис. 1.14,*в*),

$$\psi(t) = \exp\left\{j\omega_0 t\right\}\exp\left\{\frac{t^2}{2}\right\}. \qquad (1.20)$$

де ω_0 – домінантна частота, що дозволяє варіювати вибірковістю базису.

Вейвлет Морле відрізняється від інших, перш за все тим, що він є комплексною функцією, у якій дійсні і уявні частини – модульовані гаусіаном гармоніки.

1.2.3 Дискретне вейвлет-перетворення

Представлення функції $f(t)$ через її безперервне ВП є надмірним. В задачах обробки інформації, що зустрічаються на практиці, сигнал, по-перше, має обмежену смугу частот і, по-друге, допускаються ті чи інші похибки в одержуваних результатах. Тому використовують дискретне представлення безперервних сигналів, при яких параметри перетворення, в даному випадку a і b, набувають дискретні значення.

Вейвлет-перетворення, при якому значення a і b дискретні, називають дискретним ВП (DWT – Discrete Wavelet Transform).

1.2.3.1. Дискретизація масштабу.

Розглянемо спочатку випадок дискретного масштабу a і покладемо $a = a_m = a_0^m \quad \left(a_0 > 1\right)$. Це рівноцінно розбиттю частотної вісі на піддіапазони (частотні смуги). Припустимо, що $\omega_0 = \left(a_0 + 1\right)\Delta_\omega$. Тоді частотне вікно дорівнюватиме

$$\left[\frac{\omega_0}{a_m} - \frac{\Delta_\omega}{a_m}, \frac{\omega_0}{a_m} + \frac{\Delta_\omega}{a_m}\right] = \left(a_0^{-m+1}\Delta_\omega, a_0^{-m+2}\Delta_\omega\right), \qquad (1.21)$$

а центральна частота m-го вейвлета:

$$\frac{\omega_0}{a_m} = \left(a_0 + 1\right)a_0^{-m}\Delta_\omega. \qquad (1.22)$$

Базисом для DWT є функція, яка отримана з (1.9) при $a = a_0^m$:

$$\psi_{m,b}(t) = a_0^{\frac{m}{2}} \psi\left(a_0^{-m}(t-b)\right). \tag{1.23}$$

Якщо справедливо (1.12) і якщо $\psi(t)$ досить швидко згасає, то будь-яка функція з L_2 може бути представлена у вигляді дискретної послідовності

$$DWT_f(m,b) = \left\langle f, \psi_{m,b} \right\rangle = a_0^{\frac{m}{2}} \int_{-\infty}^{\infty} f(t)\psi\left(a_0^{-m}t - b\right)dt. \tag{1.24}$$

Для відновлення $f(t)$ по дискретним значенням на базис $\psi_{m,b}(t)$ накладаються додаткові обмеження, а саме: Фур'є-образ вейвлета $\psi_{m,b}(t)$ повинен задовольняти співвідношенню

$$A \le \sum_{m \in Z} \left|\Psi\left(a_0^m \omega\right)\right|^2 \le B, \tag{1.25}$$

де константи A і B такі, що $0<A\le B<\infty$.

Умова (1.25) в термінах радіотехніки має досить прозоре тлумачення. Дійсно, оскільки при кожному значенні масштабу a_0^m вейвлет є смуговим фільтром, то набір (сума) цих фільтрів є деяким пристроєм з нерівномірною частотною характеристикою, яка визначається константами A і B (рис. 1.15).

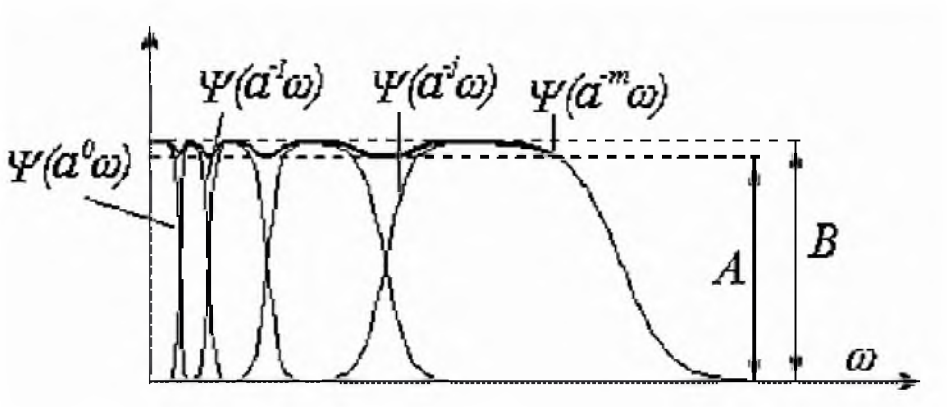


Рисунок 1.15 – Частотна характеристика смугових фільтрів, утворених вейвлетами $\Psi\left(a^m\omega\right)$ з різним масштабом при m = 0,–1,–2,–3,–4

Сигнал, наприклад звуковий, на виході такого пристрою при сильній нерівномірності частотної характеристики зазнає суттєвих спотворень. Тому для його відновлення приймають спеціальні заходи, зокрема, встановлюють фільтр, що компенсує спотворення частотної характеристики.

У ВП таким фільтром є дуальний (подвійний) вейвлет $\tilde{\psi}(t)$, Фур'є-образ якого має вигляд:

$$\tilde{\Psi}(\omega)=\frac{\Psi(\omega)}{\sum_n\left|\Psi\left(a_0^n\omega\right)\right|^2}. \tag{1.26}$$

За допомогою такого вейвлета за коефіцієнтами DWT сигнал повністю відновлюється.

1.2.3.2. Приклади вейвлетів для дискретного перетворення.

Як було зазначено вище, функції вейвлет мають властивість частотно-часової локалізації, тобто вони обмежені як в частотній, так і в часовій областях. Нижче розглянемо два приклади: перший – спектр вейвлетів в частотній області є ідеальним смуговим фільтром, другий – самі функції вейвлет є прямокутниками. Усі вейвлети, з точки зору частотно-часових властивостей, займають проміжне положення між цими крайніми випадками.

Sinc-базис. Розіб'ємо вісь частот на інтервали (піддіапазони), як показано на рис. 1.16 при a_0=2. Таке розбиття називають логарифмічним, оскільки відношення верхньої і нижньої меж діапазонів постійне і дорівнює 2.

Таке розбиття є ще й ідеальним, оскільки воно реалізується ідеальними смуговими фільтрами. Така ідеалізація потрібна для дослідження властивостей частотного розкладу за допомогою ідеалізованих вейвлетів, що дозволить у подальшому перейти до більш складних розкладань.

Будь-який сигнал $f(t)\in L_2$ зі спектром $F(\omega)$ може займати смугу частот, що охоплює кілька таких піддіапазонів. Тоді $F(\omega)=\sum_m F_m(\omega)$ і $f(t)=\sum_m f_m(t)$, тобто сигнал є сумою деякого числа елементарних сигналів. В даному

ідеальному випадку частотні канали не перекриваються, тому має місце ортогональність цих елементарних сигналів, тобто

$$\int f_i(t) f_k(t) dt = \frac{1}{2\pi} \int F_i(\omega) F_k(\omega) d\omega = \delta(i-k). \qquad (1.27)$$

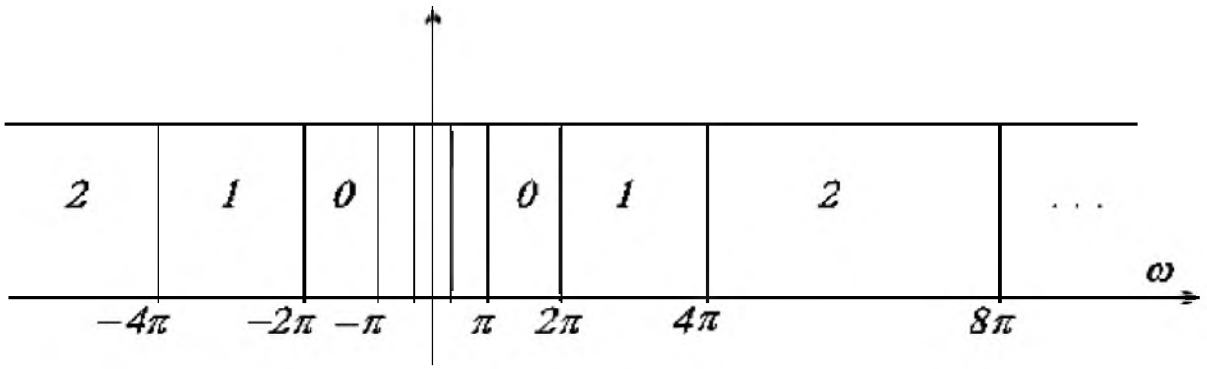


Рисунок 1.16 – Розбиття вісі частот в логарифмічному масштабі при a_0=2

Виберемо з усієї множини сигналів такі, які обмежені смугою частот 2^I, тобто такі, які мають спектр $F_I(\omega)$.

Розглянемо періодичну функцію $\Phi_I(\omega)$ таку, що

$$\Phi_I(\omega) = \sum_{k=-\infty}^{\infty} F_I\left(\omega - 2\pi 2^I k\right), \qquad (1.28)$$

тобто отриману періодизацією $F_I(\omega)$ (рис. 1.17).

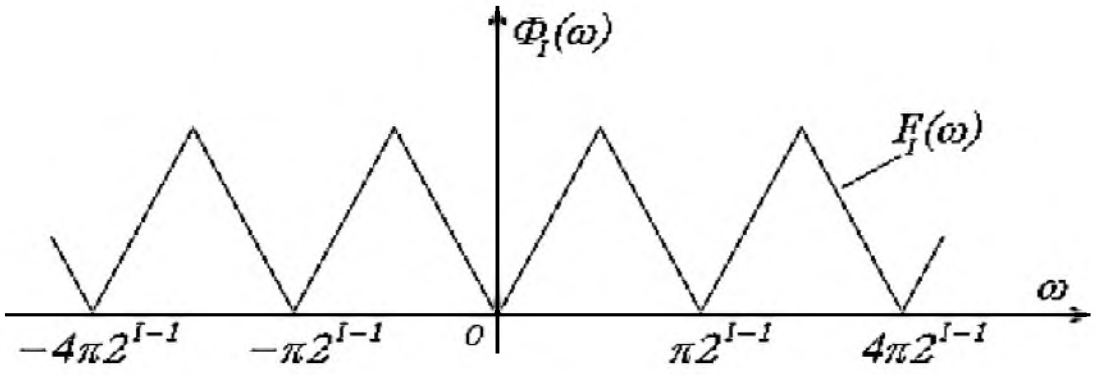


Рисунок 1.17 – Періодизація функції $F_I(\omega)$

Тоді спектр функції $F_I(\omega)$ при довільному I можна представити у вигляді

$$F_2(\omega) = \hat{O}_2(\omega)\left(\prod\left(\frac{\omega}{\pi 2^{2}+1}\right) - \prod\left(\frac{\omega}{\pi 2^{2}}\right)\right), \tag{1.29}$$

де $\prod(x)$ – функція вікна така, що

$$\prod(x) = \begin{cases} 1, & -1/2 \le x \le 1/2; \\ 0, & \textit{інакше.} \end{cases} \tag{1.30}$$

Представлення функції $f(t)$ в часовій області.

$$f(t) = \sum_{i=0}^{M-1} f_i(t) = \sum_{i,k} a_i[k]\psi_{ik}(t), \quad a_i[k] = 2^{i/2} b_i[k], \tag{1.31}$$

де вейвлет

$$\psi_{ik}(t) = 2^{i/2}\psi\left(2^i t - k\right) \tag{1.32}$$

має вигляд:

$$\psi(x) = 2\varphi(2x) - \varphi(x). \tag{1.33}$$

Вираз (1.31) є представленням функції $f(t)$ в базисі вейвлет. В даному випадку вейвлетом є функція (1.32), утворена з материнської функції $\psi(x)$ за (1.33) з урахуванням (1.31). Такий вейвлет – sinc-вейвлет (рис. 1.18).

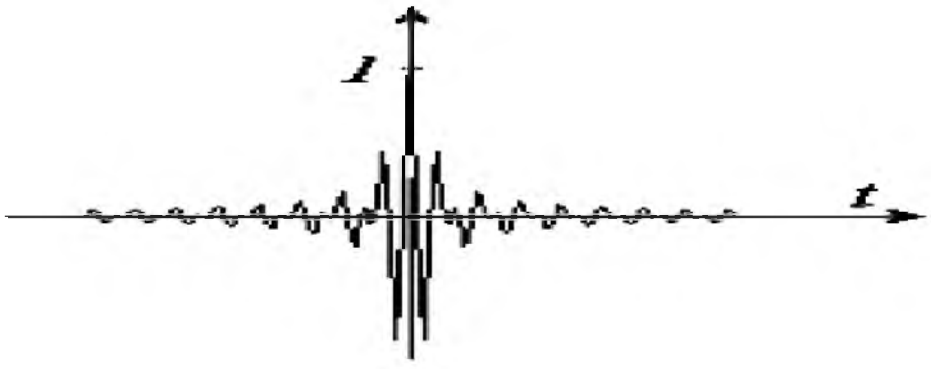
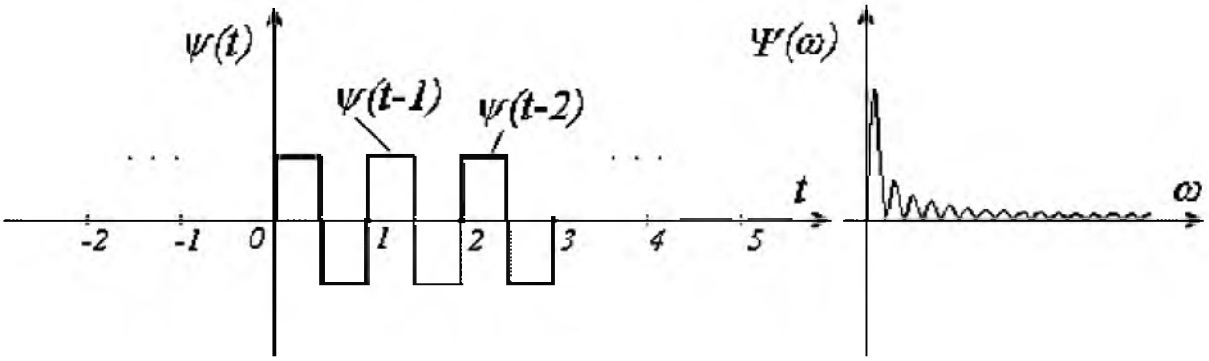


Рисунок 1.18 – Sinc-вейвлет

Вейвлет Хаара. Розіб'ємо тепер часову вісь на інтервали (рис. 1.19) і визначимо на одиничному інтервалі функцію

$$\psi(t)=\begin{cases}1, & 0<t<1/2;\\ -1, & 1/2\le t<1;\\ 0, & \textit{інакше.}\end{cases} \tag{1.34}$$



а *б*

Рисунок 1.19 – Вейвлет Хаара $\psi(t)$ (*а*) і спектр Фур'є його амплітуди (*б*)

1.3 Підходи до виділення інформаційних повідомлень із хаотичного несучого сигналу на основі реконструкції динамічних систем

Як вже зазначалось у вступі, захист інформації при її передачі каналом зв'язку є однією з проблем, особливо актуальних у період активного розвитку сучасних інформаційних технологій. Забезпечення захисту повідомлень, що передаються, є важливим, зокрема, при проведенні банківських операцій, передачі паролів та ідентифікаційних кодів (у тому числі, через інтернет) і т.д. Одним з нових способів вирішення цієї проблеми є застосування для передачі повідомлень широкосмугових хаотичних сигналів. Інтенсивні дослідження у цьому напрямі ведуться з початку 1990-х р. XX ст. У перших роботах було запропоновано використовувати явище хаотичної синхронізації для виділення інформаційного сигналу з хаотичного несучого. Пропонувалися два конкретні способи вирішення проблеми, заснованих на використанні ідентичних генераторів хаосу в передавальному та приймальному пристроях: адитивне

додавання інформаційного повідомлення до несучого сигналу [4, 27-28] та модуляція параметрів генератора хаосу [5-6, 29].

Пізніше було розглянуто завдання багатоканальної захищеної передачі на основі так званого феномена «автосинхронізації», тобто використання систем з автоматичним підстроюванням параметрів [30-31]. Перші серйозні успіхи були пов'язані з тим, що для низки модельних схем було продемонстровано можливість передачі цифрових та аналогових повідомлень з використанням хаотичних сигналів. У схемі з нелінійним підмішуванням інформаційного сигналу в хаотичний, передача мовних та музичних сигналів у низькочастотному та в радіодіапазонах була продемонстрована в роботі [32].

Встановлено, що підходи, які ґрунтуються на явищі синхронізації, мають ряд недоліків, найбільш істотною з яких є вимога ідентичності генераторів хаотичних коливань у приймачі та передавачі. Якщо параметри відповідних генераторів відрізнятимуться більш ніж на 1–2%, то ці методи стають неефективними [33]. Головні принципи, що лежать в основі інших існуючих розробок, які базуються на використанні хаотичних коливань як несучі сигнали, полягають у наступному [32-35].

1. Використання генератора хаотичних сигналів у передавальному пристрої дозволяє забезпечити одночасну передачу декількох незалежних повідомлень по одному каналу зв'язку, наприклад, шляхом модуляції параметрів даного генератора. На відміну від класичних методів (амплітудна, частотна модуляція), інформаційні повідомлення можуть передаватися шляхом модуляції параметрів, що характеризують різні деталі складної форми несучого хаотичного сигналу. Зокрема, у роботах [36-37] було продемонстровано можливість одночасної передачі 3-х незалежних повідомлень в одному несучому та їх достовірного виділення при проведенні демодуляції.

2. Процедура виділення інформаційних повідомлень з хаотичного несучого сигналу неможлива без точного знання хаотичних характеристик генератора коливань у передавальному пристрої, що забезпечує високий ступінь захищеності інформації, що передається. Наразі існує декілька базових

моделей генераторів хаосу, проте для проведення демодуляції необхідно знати не тільки яка саме базова модель використовується, але і точний вид характеристики нелінійного елемента, яка може бути задана індивідуально для кожного генератора, і визначити її шляхом простого перебору різних варіантів у загальному випадку неможливо.

Використання реконструкції для детектування повідомлень вперше обговорювалося у роботі [38], в якій продемонстровано можливість виділення одного адитивного впливу на генератор хаотичних коливань за наявності апріорної інформації про структуру математичної моделі генератора та про те, яким чином подається зовнішній вплив (тобто як воно вводиться в рівняння, що описують динаміку генератора).

У роботі [39] було запропоновано більш універсальний спосіб, який дозволяє здійснювати детектування інформаційних сигналів, що здійснюють модуляцію параметрів ДС.

Розвиток ідей реконструкції неавтономних систем було здійснено в роботі [40].

Розглянемо можливість детектування інформаційних повідомлень на прикладі генератора хаотичних коливань, що моделюється системою звичайних диференціальних рівнянь

$$\frac{d\vec{x}}{dt} = \vec{F}(\vec{x},\ \vec{\mu}^0), \quad \vec{x} \in R^n, \quad \vec{\mu}^0 \in R^l, \tag{1.35}$$

у якій $\vec{x}$ – вектор стану; $\vec{F}$ – вектор правих частин модельної системи; $\vec{\mu}^0$ – вектор постійних значень параметрів.

Здійснюватимемо відносно повільну модуляцію довільного числа параметрів інформаційними сигналами $\mu_i(t)$, тобто введемо до розгляду змінні величини

$$\mu_i^* = \mu_i^0 + \mu_i(t), \tag{1.36}$$

що дозволить реалізувати одночасну передачу кількох повідомлень. У цьому випадку сигнал, що передається по каналу зв'язку, являє собою одномірну

реалізацію коливального процесу генератора хаосу, що породжується неавтономною динамічною системою виду

$$\frac{d\vec{x}}{dt} = \vec{F}(\vec{x},\ \vec{\mu}^0 + \vec{\mu}(t)). \tag{1.37}$$

Для вирішення задачі синтезу ДС щодо одномірної реалізації система (1.31) повинна бути зведена до виду

$$\begin{aligned} \frac{dx_1}{dt} &= x_2, \\ \frac{dx_2}{dt} &= x_3, \\ &\cdots\cdots \\ \frac{dx_n}{dt} &= f(x_1,\ x_2, \ldots,\ x_n,\ \vec{\mu}). \end{aligned} \tag{1.38}$$

Це означає, що шляхом замін змінних необхідно перетворити праві частини таким чином, щоб замість вектора-функції $\vec{F}$ залишилася тільки одна скалярна нелінійна функція *f*.

Багато базових моделей динамічного хаосу (системи Лоренца, Реслера, модифікований генератор з інерційною нелінійністю та інші) задовольняють цій вимозі. Оскільки інформаційні сигнали зазвичай є повільними порівняно з несучим, можна ввести в розгляд інтервал часу t^*, протягом якого значення параметрів можна вважати практично постійними: для часів порядку t^* можна не враховувати неавтономність системи (1.37). Це дає можливість відновлення поточних значень параметрів системи за короткими ділянками її одновимірної реалізації, тобто відтворення інформаційних сигналів $\mu_i(t)$, які здійснюють параметричну модуляцію хаосу.

Застосовуючи техніку реконструкції до одновимірної реалізації генератора хаосу $x_1(t)$, яку можна виміряти на виході передавального пристрою, одержувач інформації, що знає загальний вигляд математичної моделі (1.35), виділяє корисні сигнали $\mu_i(t)$. З цією метою йому необхідно *n* раз продиференціювати реалізацію $x_1(t)$, що дозволить визначити ліві частини модельної системи (1.34). У результаті завдання визначення значень параметрів

в даний момент часу зводиться до необхідності розв'язування рівнянь алгебри з деякою кількістю невідомих.

Оскільки при комп'ютерній обробці доводиться мати справу не з аналоговим сигналом, а з дискретизованою часовою залежністю $x_1(i\Delta t)$, похідні визначаються в моменти часу $i\Delta t$ за наближеними формулами чисельного диференціювання. Записуючи систему K алгебраїчних рівнянь ($K=[t^*/\Delta t]$) для L невідомих ($L<<K$) і вирішуючи її методом найменших квадратів, можна здійснити апроксимацію невідомих коефіцієнтів.

Виберемо як модельну систему (1.35) модифікований генератор з інерційною нелінійністю (ГІН) [41]

$$\begin{aligned}\frac{dx}{dt} &= m_0 x + y - xz,\\ \frac{dy}{dt} &= -x,\\ \frac{dz}{dt} &= -g_0 z + 0.5 g_0 (x + \mid x \mid) x.\end{aligned} \tag{1.39}$$

Вважаючи, що випромінюваним сигналом генератора є одновимірна реалізація y(t), здійснимо перетворення системи рівнянь (1.39) до виду (1.38) шляхом замін змінних

$$Y = y, \quad Z = -x, \quad X = -m_0 x - y + xz, \tag{1.40}$$

в результаті яких рівняння генератора набувають вигляду

$$\begin{aligned}\frac{dY}{dt} &= Z,\\ \frac{dZ}{dt} &= X,\\ \frac{dX}{dt} &= f(X, Y, Z, \vec{\mu}), \quad \vec{\mu} = (m_0, g_0),\end{aligned}$$

$$f = \frac{X(X+Y)}{Z} + (m_0 g_0 - 1)Z - g_0(X+Y) + 0.5 g_0(\mid Z \mid - Z)Z^2. \tag{1.41}$$

Проілюструємо за допомогою моделі генератора з інерційною нелінійністю можливість одночасної передачі двох незалежних інформаційних сигналів по одному каналу зв'язку шляхом моделювання в середовищі

Matlab/Simulink. З цією метою параметр m_0 модулювався широкосмуговим хаотичним сигналом, а параметр g_0 – гармонійним сигналом.

У системі, що описана формулою (1.39) було обрано наступні значення постійних величин: g_0=0.2, m_0=1.5. Для перевірки ефективності цього підходу з точки зору його завадостійкості здійснювалося додавання нормально розподіленої випадкової величини з дисперсією 10^{-3} до інформаційних сигналів, що здійснюють параметричну модуляцію, і 10^{-4} – адитивно до несучого хаотичного сигналу.

Залежність у часі параметрів m_0 та g_0 даної системи проілюстровано на рис. 1.16,а-б. Одержувач інформації, який знає вид нелінійної функції f в системі (1.37), приймаючи сигнал (рис. 1.16,в) відновить сигнали модуляції (рис. 1.16,г-д).

Подальші дослідження проводилися моделі Реслера:

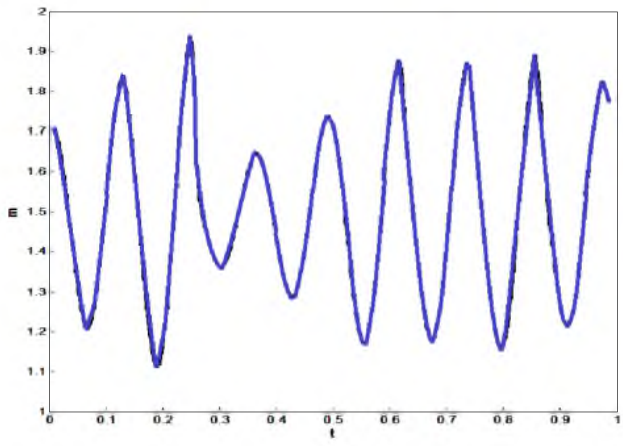
$$\begin{aligned} \frac{dx}{dt} &= -(y+z), \\ \frac{dy}{dt} &= x + ay, \\ \frac{dz}{dt} &= b + z(x-c). \end{aligned} \tag{1.42}$$

Вибравши як несучий сигнал координату y(t) даної моделі, шляхом замін змінних

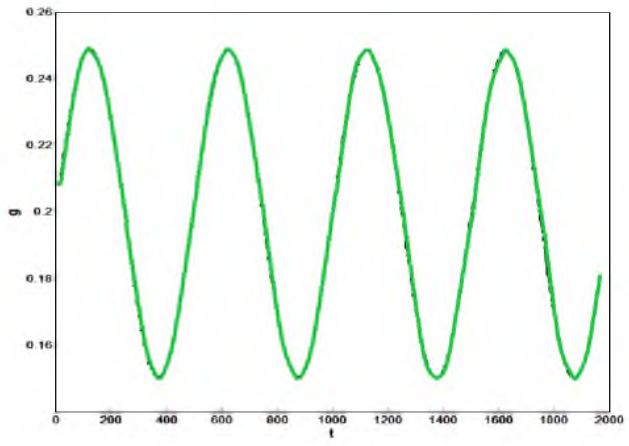
$$Y = y, \quad Z = x + ay, \quad X = ax + (a^2 - 1)y - z \tag{1.43}$$

перетворюємо систему рівнянь (1.38) до виду

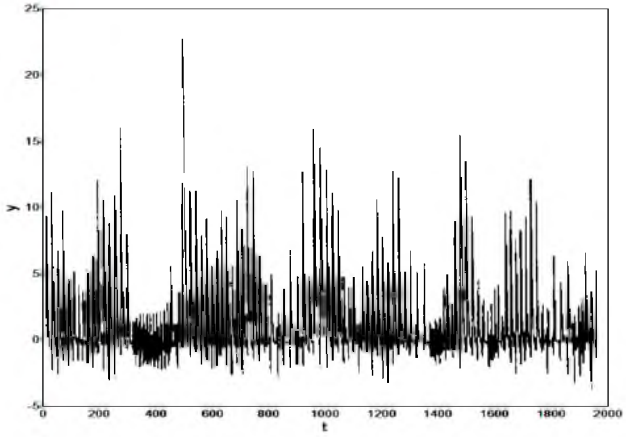
$$\begin{aligned} \frac{dY}{dt} &= Z, \\ \frac{dZ}{dt} &= X, \\ \frac{dX}{dt} &= -b + (a-c)X - cY + (ac-1)Z - aY^2 - \\ &\quad -aZ^2 - aXY + XZ + (a^2+1)YZ. \end{aligned} \tag{1.44}$$



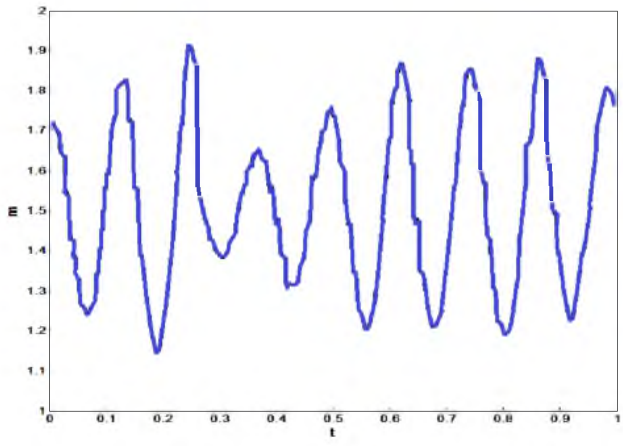
а



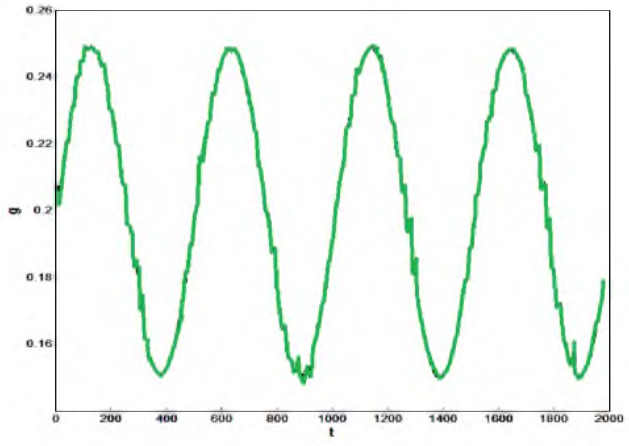
б



в



г



д

Рисунок 1.16 – Приклад детектування на основі техніки реконструкції: *а*, *б* – сигнали, що передаються; *в* – сигнал в каналі зв'язку; *г*, *д* – сигнали, виділені з хаотичного несучого

Як було показано в [42], існує можливість передавати одночасно принаймні три інформаційні сигнали в одному несучому. Теоретично метод детектування на основі реконструкції ДС не накладає обмежень на кількість одночасно змінюваних параметрів. Насправді такі обмеження виникають у з кінцевою точністю обчислення μ_i^*.

До переваг розглянутого підходу детектування належать такі.

1. Наявність тільки одного генератора хаотичних сигналів, розташованого в приймальному пристрої, і відсутність проблеми ідентичності генераторів приймача і передавача, що є однією з ключових для систем, які використовують принцип синхронізації коливань.

2. Широка смуга частот передачі інформаційних повідомлень. За цим параметром аналізований підхід до детектування, як мінімум, не поступається принципам детектування в системах, що ґрунтуються на ефекті синхронізації хаосу (у разі передачі інформаційних сигналів шляхом модуляції керуючих параметрів). Реконструкція ДС дозволяє проводити оцінку параметрів за дуже короткими ділянками перехідних процесів, що становлять, наприклад, 1/5 частину базового періоду несучого сигналу або навіть менше. Через наявність дуже великої кількості варіантів схем передачі інформації, що базуються на використанні хаотичних несучих сигналів, детальне зіставлення технічних характеристик кожної з них є окремим і дуже трудомістким завданням (яке виходить за рамки кваліфікаційної роботи). Але слід зазначити, що для розглянутих прикладів підхід, заснований на техніці реконструкції, забезпечує майже в 2 рази ширшу смугу частот передачі інформації. Зрозуміло, у цьому випадку йдеться про просте спостереження, і для того, щоб проводити більш детальне зіставлення технічних характеристик, необхідні спеціальні порівняльні дослідження.

Головним недоліком розглянутого підходу до детектування, що базується на реконструкції ДС, є необхідність диференціювання сигналів, які на практиці завжди є зашумленими. Обчислення похідних за наявності адитивного шуму

призводить до суттєвих помилок. Для їх зменшення спочатку було запропоновано використовувати триступеневу фільтрацію: фільтрація несучого сигналу в припущенні, що сигнал і шум розділені в частотній області (1-й етап), застосування методу найменших квадратів для отримання усереднених значень параметрів у межах малого часового вікна (2-й етап), згладжування виділених сигналів модуляції з урахуванням повільної зміни параметрів порівняно з хаотичним сигналом (3- й етап).

Тим не менш, наявність шуму у початковому процесі залишається найбільш серйозною проблемою з точки зору практичної реалізації підходу до демодуляції, заснованого на техніці реконструкції ДС.

1.4 Висновок. Постановка задачі

Захист інформації при її передачі каналом зв'язку є однією з проблем, особливо актуальних у період активного розвитку сучасних інформаційних технологій. Одним з нових способів вирішення цієї проблеми є застосування для передачі повідомлень широкосмугових хаотичних сигналів.

Вейвлет перетворення є потужним інструментом аналізу, застосовним до коротких, зашумлених і нестаціонарних випадкових процесів. До переваг теорії вейвлетів належить можливість усунення некоректності операції диференціювання зашумлених часових рядів шляхом переходу в простір вейвлет-коефіцієнтів. Наразі значний інтерес викликають комбіновані підходи, що базуються на поєднанні вейвлетів з іншими методами аналізу структури сигналів.

Проаналізовано існуючі підходи до виділення інформаційних повідомлень із хаотичного несучого сигналу на основі реконструкції динамічних систем. Встановлено, що підходи, які ґрунтуються на явищі синхронізації, мають ряд недоліків, найбільш істотною з яких є вимога ідентичності генераторів хаотичних коливань у приймачі та передавачі. Якщо параметри відповідних генераторів відрізнятимуться більш ніж на 1–2%, то ці

методи стають неефективними. Головним же недоліком підходу до детектування, що базується на реконструкції ДС, є необхідність диференціювання сигналів, які на практиці завжди є зашумленими. Обчислення похідних за наявності адитивного шуму призводить до суттєвих помилок.

Таким чином, для усунення недоліків існуючих підходів необхідно:

• розглянути і дослідити підхід, заснований на поєднанні техніки глобальної реконструкції та дискретного вейвлет-перетворення;

• оцінити ефективність дослідженого підходу.

2 СПЕЦІАЛЬНА ЧАСТИНА

2.1 Детектування інформаційних сигналів на основі реконструкції динамічних систем і ДВП

Як вже зазначалось у розділі 1.3, наявність шуму у початковому процесі залишається найбільш серйозною проблемою з точки зору практичної реалізації підходу до демодуляції, заснованого на техніці реконструкції ДС. У цьому розділі розглянуто і досліджено підхід до вирішення цієї проблеми шляхом поєднання техніки глобальної реконструкції та дискретного ВП. До переваг теорії вейвлетів належить можливість усунення некоректності операції диференціювання зашумлених часових рядів шляхом переходу в простір вейвлет-коефіцієнтів.

2.1.1 Диференціювання сигналів із застосуванням дискретних вейвлетів

Властивість диференціювання ВП можна записати наступним чином [43]:

$$W\left[\partial_t^p f\right] = (-1)^p \int_{-\infty}^{\infty} f(t)\partial_t^p \left[(\psi_{ab}^*(t))\right] dt. \tag{2.1}$$

Формула (2.1) означає, що замість того, щоб диференціювати p раз сигнал f(t), можна продиференціювати p раз аналізуючий вейвлет. Це дуже корисна властивість при роботі з експериментальними даними, оскільки функція f(t) є рядом чисел (і містить шум), а аналізуючий вейвлет заданий формулою (у разі CWT).

З точки зору безпосередньо процедури обчислення похідних функції $\psi_{ab}^*(t)$ простіше користуватися безперервними вейвлет-базисами, що дозволяють отримувати аналітичні вирази для $\partial_t^p \left[(\psi_{ab}^*(t))\right]$, що очевидно, наприклад, для базисів, сконструйованих на основі похідних функції Гауса:

$$\psi_p(t) = (-1)^p \, \partial_t^p \left[\exp\left(-\frac{t^2}{2}\right)\right]. \tag{2.2}$$

У той самий час CWT має низку недоліків у разі його використання під час вирішення завдання визначення параметрів ДС. Справа в тому, що базиси на основі безперервних вейвлетів, строго кажучи, не є ортонормованими [1, 44], тоді як дискретні вейвлети призводять до більш точного зворотного відновлення сигналу, наприклад, після процедури стиснення даних. Для дискретних вейвлетів легше обчислити зворотне перетворення, попри те, що вони не можуть бути записані в аналітичній формі (за винятком вейвлета Хаара). Дискретні вейвлети забезпечують суттєвий виграш у швидкості проведення обчислень у рамках процедури швидкого перетворення, що є однією з важливих переваг при їх використанні для передачі інформації.

При DWT сигналу f(t) розглядаються скейлінг-функція (або масштабна функція) $\varphi(t)$ і базисний вейвлет $\psi(t)$, що визначаються наступним чином [45]:

$$\begin{aligned} \varphi(t) &= \sqrt{2}\sum_{k=0}^{2M-1} h_k \varphi(2t-k), \\ \psi(t) &= \sqrt{2}\sum_{k=0}^{2M-1} g_k \varphi(2t-k), \\ g_k &= (-1)^k h_{2M-k-1}, \end{aligned} \tag{2.3}$$

де h_k – коефіцієнти. Масштабування та зміщення зазначених функцій задаються виразами

$$\begin{aligned} \varphi_{j,k} &= 2^{j/2}\varphi(2^j t-k), \\ \psi_{j,k} &= 2^{j/2}\psi(2^j t-k). \end{aligned} \tag{2.4}$$

В рамках багатомасштабного аналізу функції $\varphi_{j,k}$ і $\psi_{j,k}$ служать високочастотними і низькочастотними фільтрами, відповідно. Із загальних властивостей скейлінг-функцій та вейвлетів однозначно визначаються коефіцієнти h_k.

Застосування вейвлетів спрощує вивчення багатьох математичних операторів, що дозволяє вирішувати з їх допомогою диференціальні рівняння. Розглянемо як ілюстрацію оператор диференціювання 1-го порядку. Ґрунтуючись на матричному поданні [45], запишемо наступний вираз для матричного елемента оператора:

$$\tau_l = \int_{-\infty}^{\infty} \varphi(t) \frac{d}{d\tau} \varphi(t-l) dt. \tag{2.5}$$

З урахуванням (2.3) отримаємо

$$\begin{aligned} \tau_l &= \int_{-\infty}^{\infty} \sum_{j=0}^{2M-1} h_j \varphi(2t+j) \frac{d}{d\tau} \left[\sum_{k=0}^{2M-1} h_k \varphi(2t-2l+k) \right] dt = \\ &= \sum_{j=0}^{2M-1} \sum_{k=0}^{2M-1} h_j h_k \int_{-\infty}^{\infty} \varphi(2t+j) \frac{d}{d\tau} \varphi(2t-2l+k) dt = \\ &= \sum_{j=0}^{2M-1} \sum_{k=0}^{2M-1} h_j h_k \tau_{2l-k+j}. \end{aligned} \tag{2.6}$$

Це рівняння пов'язує матричні елементи на сусідніх рівнях. Для вейвлетів Добеші (D4) отримаємо наступне матричне рівняння:

$$\begin{bmatrix} \tau_{-3} & \tau_{-2} & \tau_{-1} & \tau_0 & \tau_1 & \tau_2 & \tau_3 \end{bmatrix}^T = \tag{2.7}$$

$$= \begin{bmatrix} \sum h_i h_{i+3} & 0 & 0 & 0 & 0 & 0 & 0 \\ \sum h_i h_{i+1} & \sum h_i h_{i+2} & \sum h_i h_{i+3} & 0 & 0 & 0 & 0 \\ \sum h_i h_{i-1} & \sum h_i h_i & \sum h_i h_{i+1} & \sum h_i h_{i+2} & \sum h_i h_{i+3} & 0 & 0 \\ \sum h_i h_{i-3} & \sum h_i h_{i-2} & \sum h_i h_{i-1} & \sum h_i h_i & \sum h_i h_{i+1} & \sum h_i h_{i+2} & \sum h_i h_{i+3} \\ 0 & 0 & \sum h_i h_{i-3} & \sum h_i h_{i-2} & \sum h_i h_{i-1} & \sum h_i h_i & \sum h_i h_{i+1} \\ 0 & 0 & 0 & 0 & \sum h_i h_{i-3} & \sum h_i h_{i-2} & \sum h_i h_{i-1} \\ 0 & 0 & 0 & 0 & 0 & 0 & \sum h_i h_{i-3} \end{bmatrix} \begin{bmatrix} \tau_{-3} \\ \tau_{-2} \\ \tau_{-1} \\ \tau_0 \\ \tau_1 \\ \tau_2 \\ \tau_3 \end{bmatrix}.$$

При обчисленні першої похідної $\tau_{-j}=-\tau_j$. Рішення матричного рівняння дозволяє обчислити елементи оператора диференціювання. За аналогією можна визначити матричні елементи диференціальних операторів вищих порядків. Приклад обчислень для базису вейвлетів Добеші (D8) – див. табл. 2.1 [45].

Взагалі вейвлети Добеші названі на честь математика з США, яка першою побудувала дане сімейство, Інгрід Добеші (Ingrid Daubechies). Вона ввела вейвлет ψ і функцію шкали (будівельний блок) φ наступним чином. Одна вимога полягала в тому, щоб функція шкали φ мала компактний носій. Вона повинна дорівнювати нулю поза кінцевого відрізка. Добеші вибрала в якості носія відрізок [0, 3]. Вона довела, що цю функцію не можна виразити через відомі елементарні функції: многочлени, тригонометричні або ступеневі функції. Вона також показала, що φ можна побудувати рекурсивно, за

допомогою деякого початкового завдання і рекурсивного правила. Вона вибрала наступні початкові значення:

$$\varphi(0)=0,\quad \varphi(1)=\frac{1+\sqrt{3}}{2},\quad \varphi(2)=\frac{1-\sqrt{3}}{2},\quad \varphi(3)=0, \tag{2.8}$$

і задала рекурсивне співвідношення

$$\varphi(r)=\frac{1+\sqrt{3}}{4}\varphi(2r)+\frac{3+\sqrt{3}}{4}\varphi(2r-1)+\frac{3-\sqrt{3}}{4}\varphi(2r-2)+\frac{1-\sqrt{3}}{4}\varphi(2r-3)=$$

$$=h_0\varphi(2r)+h_1\varphi(2r-1)+h_2\varphi(2r-2)+h_3\varphi(2r-3)=$$

$$=(h_0,h_1,h_2,h_3)\cdot(\varphi(2r),\varphi(2r-1),\varphi(2r-2),\varphi(2r-3)) \tag{2.9}$$

Подальше обчислення значень функції φ відбувається по шагам. Функція φ служить будівельним блоком для побудови вейвлета Добеші ψ, який задається також рекурсивно.

Таблиця 2.1 – Приклад обчислень для базису вейвлетів Добеші (D8)

k	h_k	τ_k
−6	0	0.00000084
−5	0	−0.00017220
−4	0	−0.00222404
−3	0	0.03358020
−2	−0.07576571	−0.19199897
−1	−0.02963552	0.79300950
0	0.49761866	0
1	0.80373875	−0.79300950
2	0.29785779	0.19199897
3	−0.09921954	−0.03358020
4	−0.01260396	0.00222404
5	0.03222310	0.00017220
6	0	−0.00000084

На рис. 2.1 представлені скейлінг φ(t) і вейвлет ψ(t) функції Добеші другого, третього и четвертого порядку. Очевидно, що вейвлети більш високого порядку (третього, четвертого) більш гладкі порівняно з вейвлетами другого порядку; всі функції φ_n і ψ_n несиметричні. Порядок вейвлета визначає число нульових моментів. Слід зазначити, що чим більше число нульових моментів

містить вейвлет (тобто чим вище його порядок), тим більш тонку структуру сигналу він дозволяє аналізувати.

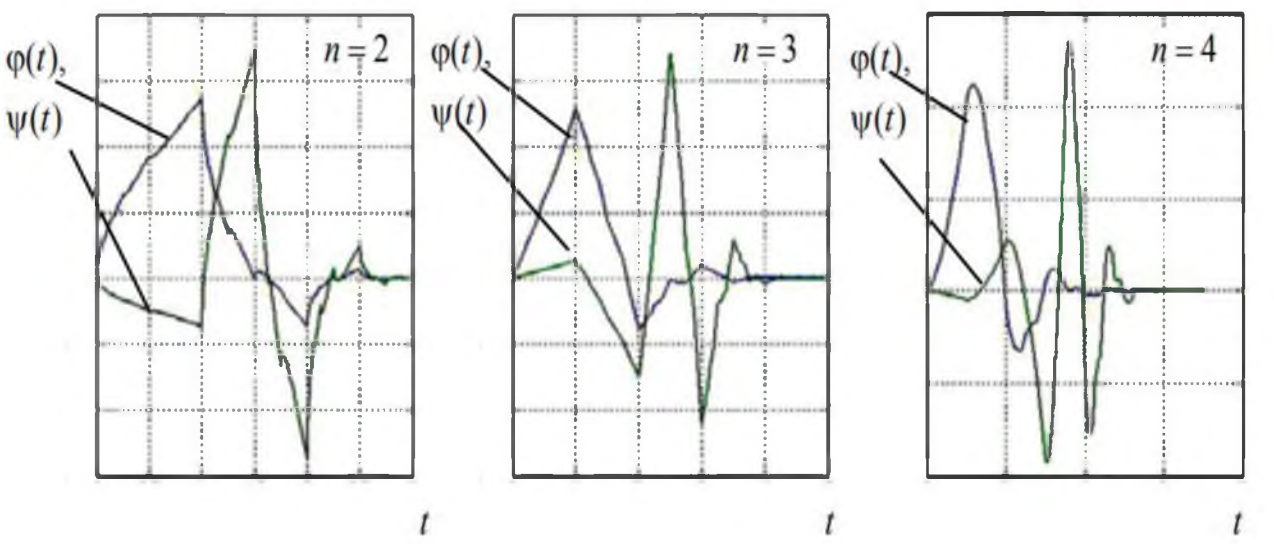


Рисунок 2.1 – Скейлінг φ(t) і вейвлет ψ(t) функції Добеші другого, третього и четвертого порядку

Частотно-часова характеристика фільтрів Добеші (рис. 2.2) дає можливість з найбільшою ймовірністю виявити локальний сигнал, ґрунтуючись на частотному діапазоні самого локального сигналу і діапазоні на який налаштований фільтр (при наявності базових апріорних знань про вхідний сигнал). Виробляючи вибір відповідного кроку дискретизації сигналу можна забезпечити максимальний відгук вейвлет коефіцієнтів при перетворенні.

Основні властивості вейвлетів сімейства Добеші:

- мають хороший локалізований спектр в частотної області, характеризуються двома функціями: вейвлет функцією ψ і масштабуючою функцією φ;

- є вейвлетами ортогонального типу, зосереджені на кінцевому інтервалі часу і мають кінцеве кількість фільтруючих коефіцієнтів;

- здатні повністю відновити довільний локальний сигнал на нульовому рівні реконструкції;

- мають можливість виконувати дискретні перетворення з застосуванням алгоритмів швидкого вейвлет перетворення.

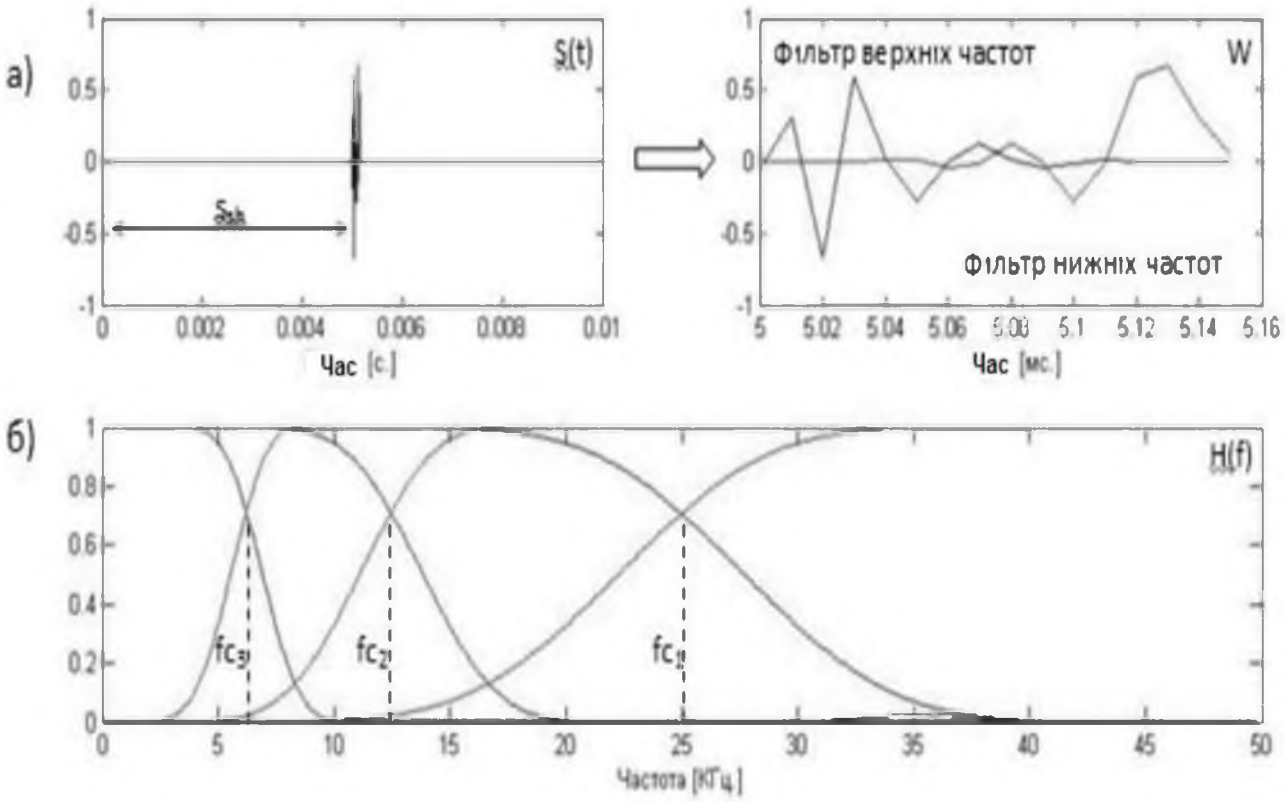


Рисунок 2.2 – Зображення часової (*а*) і частотної (*б*) характеристик вейвлет фільтрів Добеші

2.1.2 Детектування інформаційних сигналів з використанням дискретних вейвлетів

Повернімося до системи рівнянь (1.44), отриманої шляхом замін змінних у моделі Реслера (R.Roessler), і вирішуватимемо завдання визначення поточних значень параметрів a, b і c, використовуючи можливості, які надає вейвлет-аналіз.

Існує декілька варіантів вирішення цього завдання. Один з них полягає в тому, що замість обчислення похідної функції y(t), тобто несучого хаотичного сигналу, здійснюється перехід у простір коефіцієнтів прямого ВП з

використанням матричних елементів диференціального оператора першого порядку k. Потім за допомогою зворотного ВП (з використанням коефіцієнтів h_k) отримується часова залежність функції dy(t)/dt.

Зазначений розглянутий підхід, який передбачає пряме та зворотне вейвлет-перетворення із різними коефіцієнтами, має безперечну перевагу у порівнянні з чисельним диференціюванням сигналу y(t) за наближеними математичними формулами.

Оцінемо ефективність розглянутого підходу, що передбачає пряме та зворотне ВП з різними коефіцієнтами, шляхом моделювання в середовищі Matlab/Simulink за допомогою стандартних і розроблених програм.

Результат моделювання зображено на рис. 2.3. Якщо до аналізованого сигналу (рис. 2.3,а) додається нормально розподілений випадковий процес з дисперсією 0.05, то формальне застосування формул чисельного диференціювання, заснованих на інтерполяційних багаточленах Ньютона, призведе до великих похибок оцінки похідних (рис. 2.3,б). Даний підхід на основі вейвлетів забезпечує, як мінімум, на порядок меншу величину похибки (рис. 2.3,в), і ця похибка може бути зменшена ще сильніше шляхом вибору відповідного вейвлет-базису.

Аналогічні результати для іншого рівня шуму (з дисперсією 0.1) наведено на рис. 2.4. Обчислення похідних $d^2y(t)/dt^2$ та $d^3y(t)/dt^3$ буде призводити до значно суттєвіших помилок для звичайного чисельного диференціювання у порівнянні з вейвлетами. Замість багаторазового застосування формул диференціального оператора 1-го порядку можна обчислити елементи диференціальних операторів 2-го та 3-го порядків, що дозволить проводити одночасне обчислення всіх необхідних похідних.

Рис. 2.5 ілюструє, як похибка обчислення (детектування) залежить від інтенсивності шуму, що додається адитивно до одного з параметрів (рис. 2.5,*а*), до несучого сигналу (рис. 2.5,*б*) і вводиться в праві частини рівнянь моделі (рис. 2.5,*в*).

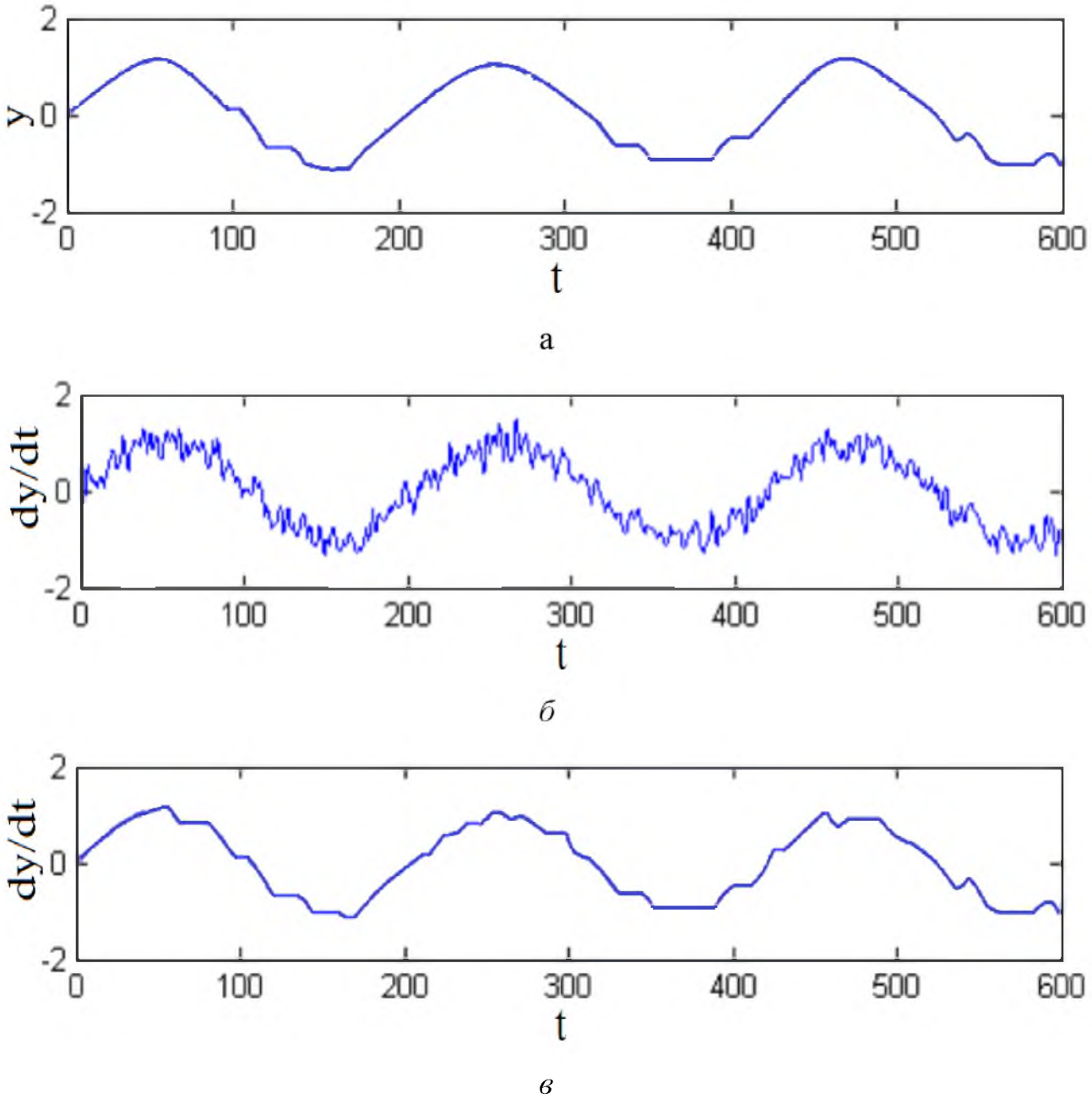
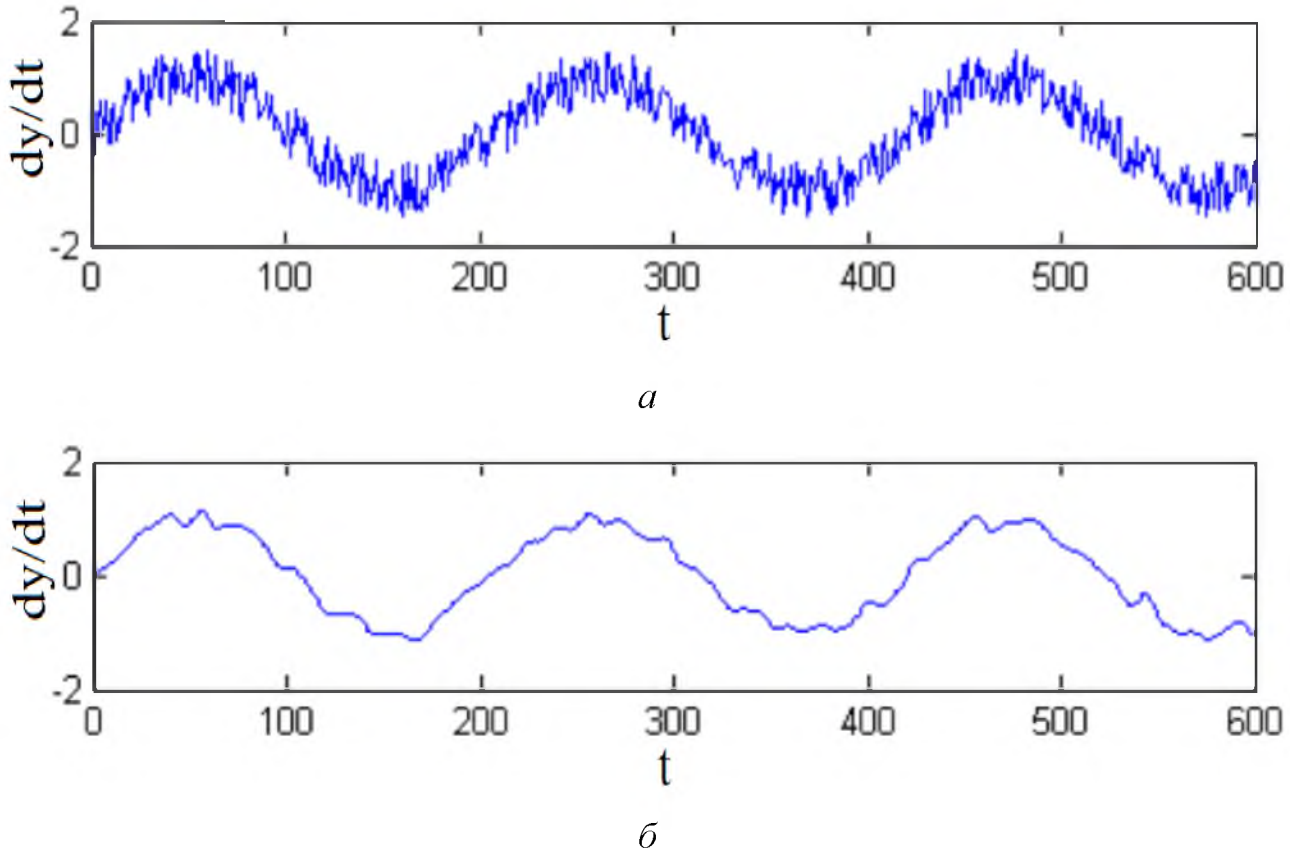


Рисунок 2.3 – Початковий сигнал системи Реслера (*а*), до якого додається шум з дисперсією 0.05; результати обчислення першої похідної зашумленого процесу за наближеними формулами чисельного диференціювання (*б*) та за допомогою вейвлет-аналізу (*в*)

Для підвищення швидкості обчислень можна змінити підхід до визначення поточних значень параметрів. Замість проведення прямого та зворотного вейвлет-перетворень можна перейти у простір вейвлет-коефіцієнтів і у цьому просторі вирішувати завдання визначення параметрів шляхом

розв'язання алгебраїчних рівнянь. Цей підхід не буде мати принципових відмінностей від дослідженого вище, і є альтернативним варіантом технічної сторони процедури детектування. Подальші дослідження мають бути спрямовані на моделювання альтернативного варіанту.

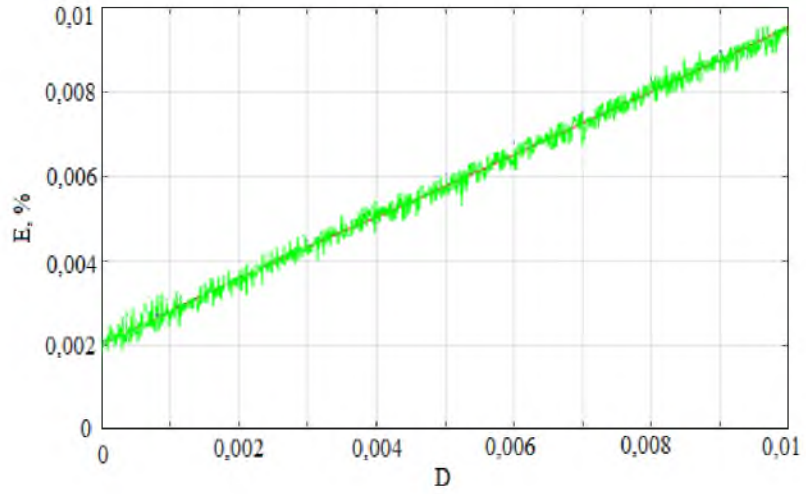


а

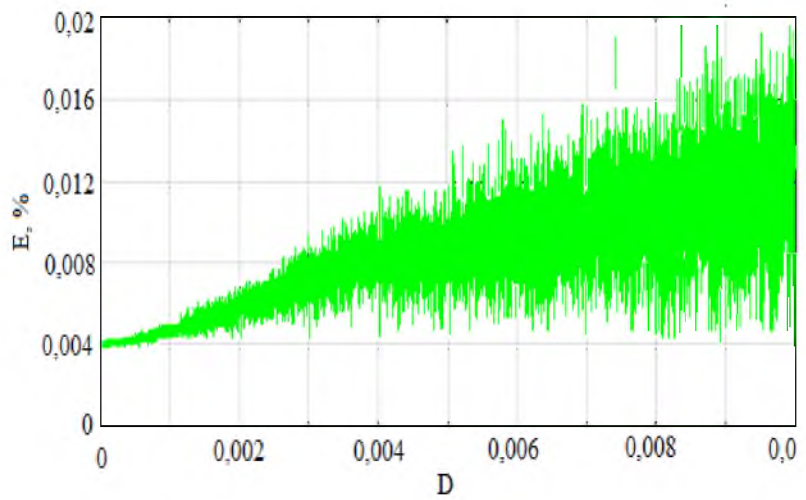
б

Рисунок 2.4 – Результати обчислення першої похідної сигналу, зображеного на рис. 2.1, при додаванні шуму з дисперсією 0.1:
а – за наближеними формулами чисельного диференціювання;
б – за допомогою вейвлет-аналізу

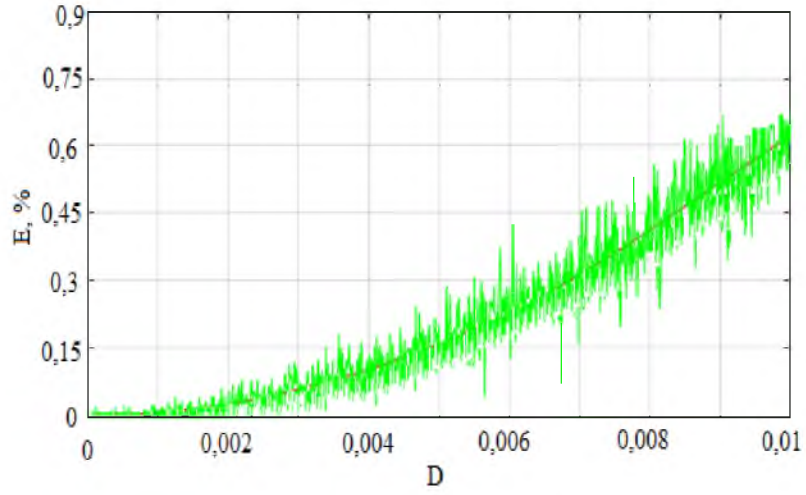
Таким чином, важливою обставиною подальшого прогресу у сфері використання динамічного хаосу в комунікаціях є формулювання інших принципів модуляції та детектування інформаційних повідомлень – чим різноманітнішими є підходи до вирішення даної проблеми, тим вищий рівень захисту переданих повідомлень може бути забезпечений.



а



б



в

Рисунок 2.5 – Залежність похибки детектування від дисперсії шуму, що додається адитивно до одного з параметрів (*а*), до несучого сигналу (*б*), в рівняння (*в*)

У розділі розглянуто і досліджено підхід до виділення повідомлень, що передаються з хаотичного несучого сигналу, заснований на поєднанні техніки реконструкції динамічних систем та дискретних вейвлетів. Безперечною перевагою ВП є можливість усунення некоректності операції диференціювання зашумлених часових рядів шляхом переходу у простір коефіцієнтів.

Помилки, що виникають під час використання наближених формул чисельного диференціювання, заснованих на інтерполяційних багаточленах Ньютона, можуть бути зменшені за рахунок використання спеціальних прийомів, наприклад, попередньої цифрової фільтрації та подальшого застосування сплайнів, що забезпечують безперервність кількох похідних. Такий прийом також має недоліки, наприклад, якщо не забезпечується якісна фільтрація, то застосування сплайнів до зашумлених даних призводитиме до похибок інтерполяції. Цей прийом досить тісно пов'язаний зі скейлінг-функціями DWT, але перевага вейвлетів полягає у можливості прискорити процедуру обчислень за рахунок застосування швидких (пірамідальних) алгоритмів, що забезпечують суттєвий виграш у швидкості (за аналогією з швидким перетворенням Фур'є). Це один із важливих моментів з погляду комунікацій.

Порівняно з використанням підходу до детектування, який базується на реконструкції динамічної системи у тому варіанті, який був представлений в розділі 1.3, підхід, розглянутий у даному розділі, забезпечує не тільки суттєвий виграш у швидкості обчислень, але й значно більш високу стійкість до завад (при проведеному імітаційному моделюванні похибку визначення поточних значень параметрів вдавалося зменшити на 1 порядок).

2.1.3 Визначення оптимального вейвлет-базису

Визначення оптимального вейвлет-базису є важливим етапом в вейвлет-аналізі, тому що саме по цьому базису будуть проходити процеси розкладання-складання сигналу. На практиці часто вибір материнського вейвлету носить

суб'єктивний характер і ґрунтується на досвіді самого дослідника. Одним з підходів є використання вейвлет-частотної характеристики (ВЧХ) як основи для вибору вейвлет-базису.

Для визначення оптимального вейвлету з заданого вейвлет-сімейства використовувались наступні параметри ВЧХ [46-55]:

• ширина смуги пропускання (L_p) головної пелюстки ВЧХ (на рівні -3 дБ);

• площа бічних пелюсток (S_b);

• близькість центральної частоти головної пелюстки до частоти досліджуваного сигналу (F_{cs}).

Тоді оптимальним вейвлет-базисом називають такий вейвлет $W_{opt}=W_i$, якому відповідає $\min(Lp^H, Sb^H, Fcs^H)$, де:

1. $Lp_i^H = \frac{Lp_i - \overline{Lp}}{\Delta Lp}$ $(\overline{Lp} = \frac{1}{N}\sum_{i=1}^{N} Lp_i,\ \Delta Lp = Lp_{\max} - Lp_{\min})$.

2. $Sb_i^H = \frac{Sb_i - \overline{Sb}}{\Delta Sb}$ $(\overline{Sb} = \frac{1}{N}\sum_{i=1}^{N} Sb_i,\ \Delta Sb = Sb_{\max} - Sb_{\min})$.

3. $Fcs_i^H = \frac{Fcs_i - \overline{Fcs}}{\Delta Fcs}$ $(\overline{Fcs} = \frac{1}{N}\sum_{i=1}^{N} Fcs_i,\ \Delta Fcs = Fcs_{\max} - Fcs_{\min})$.

Були проаналізовані сімейства Добеші, сімлетів, койфлетів, Гаусових вейвлетів, Біортогональних вейвлетів, а також вейвлетів Хаара, Мейера, Морле і «мексиканський капелюх» відповідно до описаних вище параметрів ВЧХ. Результати аналізу наведені в таблицях 2.1-2.6.

Таблиця 2.1 – Результати аналізу сімейства койфлетів

Вейвлет	L_p, Гц	S_b, $*10^5$ Гц	F_{cs}, Гц
coif1	25	2.4901	3
coif2	23	2.4837	1
coif3	23	2.4888	0
coif4	22	2.2719	1
coif5	23	2.3252	1

Таблиця 2.2 – Результати аналізу сімейства Добеші

Вейвлет	L_p, Гц	S_b, $*10^5$ Гц	F_{cs}, Гц
db1	25	2.5513	8
db2	29	2.5313	2
db3	22	2.4972	3
db4	24	2.4672	0
db5	24	2.4786	2
db6	22	2.4885	0
db7	23	2.4543	0
db8	23	2.4034	1
db9	21	2.2912	0
db10	21	2.0156	0

Таблиця 2.3 – Результати аналізу сімейства сімлетів

Вейвлет	L_p, Гц	S_b, $*10^5$ Гц	F_{cs}, Гц
sym2	29	2.5440	2
sym3	22	2.4956	3
sym4	24	2.4434	0
sym5	24	2.4750	2
sym6	22	2.4796	1
sym7	23	2.4547	0
sym8	23	2.4212	2
sym9	22	2.4019	0
sym10	22	2.4202	1

Згідно з отриманими результатами кращими базисами в кожному вейвлет-сімействі можна вважати: вейвлет «db10» з сімейства Добеші; вейвлет «sym9» з сімейства сімлетів; вейвлет «coif4» з сімейства койфлетів; вейвлет

«gaus3» з сімейства Гаусових вейвлетів; вейвлет «bior3.9» з сімейства біортогональних вейвлетів.

Таблиця 2.4 – Результати аналізу сімейства біортогональних вейвлетів

Вейвлет	L_p, Гц	S_b, $*10^5$ Гц	F_{cs}, Гц
bior1.1	25	2.5312	8
bior1.3	26	2.4821	3
bior1.5	24	2.4716	0
bior2.2	18	1.9766	3
bior2.4	19	2.4449	1
bior2.6	16	2.5008	1
bior2.8	16	2.5189	0
bior3.1	16	2.5020	1
bior3.3	15	2.9987	0
bior3.5	14	2.6446	1
bior3.7	14	2.5891	0
bior3.9	15	2.4684	0
bior4.4	22	2.3215	1
bior5.5	20	2.2738	2
bior6.8	21	2.1269	1

Таблиця 2.5 – Результати аналізу вейвлетів Мейера, «мексиканський капелюх», Морле, Хаара

Вейвлет	L_p, Гц	S_b, $*10^5$ Гц	F_{cs}, Гц
Meyr	21	1.6666	0
Mexh	23	1.9361	3
Morl	10	1.7105	1
Haar	25	2.5513	8

Таблиця 2.6 – Результати аналізу сімейства Гаусових вейвлетів

Вейвлет	L_p, Гц	S_b, $*10^5$ Гц	F_{cs}, Гц
gaus1	39	1.9826	2
gaus2	27	2.0414	2
gaus3	21	1.9105	0
gaus4	16	1.9653	3
gaus5	16	1.9764	0
gaus6	14	2.0835	2
gaus7	14	1.9675	0
gaus8	14	1.9446	2

Результат ВЧХ для вейвлета «db10» представлено на рис. 2.6, вейвлета «db2» - на рис. 2.7.

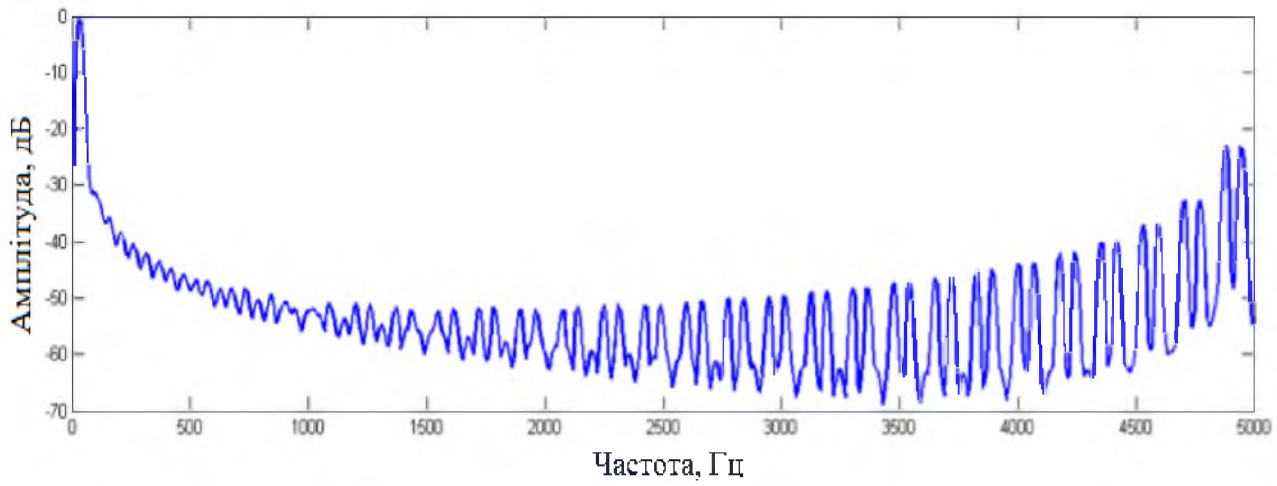


Рисунок 2.6 – ВЧХ вейвлету «db10»

Аналізуючи вейвлет-частотні характеристики вейвлет-сімейств, можна зробити висновок, що зі збільшенням порядку вейвлета в його сімействі зменшується смуга пропускання головної пелюстки і площа, зайнята бічними пелюстками. В середньому смуга пропускання склала близько 20 Гц.

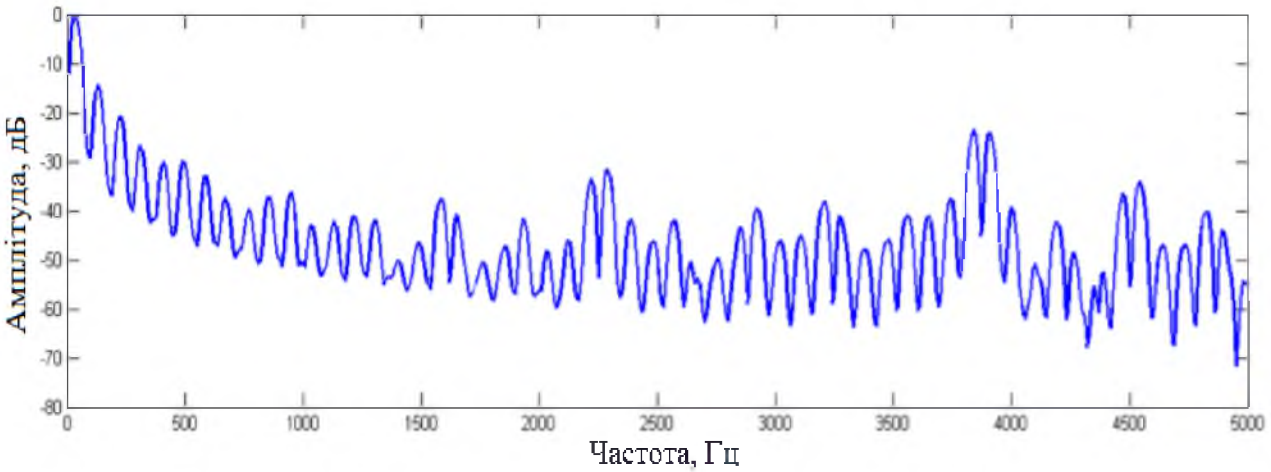


Рисунок 2.7 – ВЧХ вейвлету «db2»

У сімействі Добеші, сімлети й койфлети бічні пелюстки мало виражені або практично відсутні. У сімействі Гауссових вейвлетів є велика кількість бічних пелюсток і вузька смуга пропускання. У вейвлетів Меєра та Морле є кілька яскраво виражених бічних пелюсток на частотах 2300-2400 Гц і 2900-3000 Гц. Найменшу смугу пропускання мають вейвлети Морле, Гаусові вейвлети «gaus6» - «gaus8», біортогональні вейвлети «bior3.3» - «bior3.9».

2.2 Висновки

У цьому розділі розглянуто і досліджено підхід до забезпечення конфіденційності при передачі інформації заснований на техніці глобальної реконструкції динамічних систем та дискретного вейвлет-перетворення. Додаткове використання ВП дозволяє усунути некоректності операції диференціювання зашумлених часових рядів шляхом переходу в простір вейвлет-коефіцієнтів. Помилки, що виникають під час використання наближених формул чисельного диференціювання, заснованих на інтерполяційних багаточленах Ньютона, можуть бути зменшені за рахунок використання спеціальних прийомів, наприклад, попередньої цифрової фільтрації та подальшого застосування сплайнів, що забезпечують безперервність кількох похідних.

Слід зазначити, що цей прийом досить тісно пов'язаний зі скейлінг-функціями дискретного вейвлет-перетворення, але перевага вейвлетів полягає у можливості прискорити процедуру обчислень за рахунок застосування швидких (пірамідальних) алгоритмів, що забезпечують суттєвий виграш у швидкості (за аналогією зі швидким перетворенням Фур'є). Це один із важливих моментів з погляду комунікацій.

Отже, використання техніки реконструкції динамічних систем спільно з дискретним вейвлет-перетворенням в системі захищеної передачі інформації, що використовує принцип модуляції параметрів генератора хаотичних коливань і хаотичні несучі сигнали, дозволяє здійснювати детектування декількох інформаційних повідомлень, що одночасно передаються в одному несучому сигналі. Наявність тільки одного генератора хаотичних коливань, розташованого в передавальному пристрої, усуває проблему неідентичності генераторів приймача і передавача, що є однією з ключових для систем захищеної передачі інформації, які реалізують процедуру детектування на основі ефекту синхронізації коливань.

Дискретні вейвлети допомагають звести систему звичайних диференціальних рівнянь до системи рівнянь алгебри для визначення параметрів передавального генератора (вирішуючи при цьому одну з технічних проблем, пов'язаних з необхідністю диференціювання зашумлених сигналів). Однією з переваг теорії вейвлетів є можливість усунення некоректності операції диференціювання зашумлених часових рядів шляхом переходу в простір вейвлет-коефіцієнтів та заміни похідної від сигналу на похідну від вейвлета. Це дозволяє суттєво знизити похибки детектування.

Слід також зазначити, що порівняно з використанням підходу до детектування, який базується на реконструкції ДС у тому варіанті, який був представлений в розділі 1.3, підхід до забезпечення конфіденційності при передачі інформації заснований на техніці глобальної реконструкції динамічних систем та дискретного вейвлет-перетворення, розглянутий у даному розділі, забезпечує не тільки суттєвий виграш у швидкості обчислень,

але й значно більш високу стійкість до завад (при проведеному моделюванні похибку визначення поточних значень параметрів вдавалося зменшити на 1 порядок).

Для вирішення завдання вибору материнського вейвлету при застосуванні математичного апарату вейвлет-перетворення запропоновано використовувати вейвлет-частотну характеристику як основу для вибору вейвлет-базису. ВЧХ визначається як чутливість вейвлет-коефіцієнтів розкладання від частоти сигналу і дозволяє аналізувати будь-який вейвлет як базис, не вимагаючи наявності скейлинг-функції й реконструкції сигналу. Оптимальний вейвлет-базис визначається як вейвлет, який має такі мінімальні значення параметрів ВЧХ: ширина смуги пропускання головної пелюстки, площа бічних пелюсток, близькість центральної частоти головної пелюстки до частоти вхідного сигналу.

3 ЕКОНОМІЧНИЙ РОЗДІЛ

Метою даного розділу є обґрунтування економічної доцільності забезпечення конфіденційності при передачі інформації з використанням вейвлет-перетворення сигналів. Досягнення цієї мети потребує здійснення визначення величини капітальних витрат на придбання і налагодження складових системи інформаційної безпеки або витрат, що пов'язані з виготовленням апаратури, приладів, програмного забезпечення; річних експлуатаційних витрат на утримання і обслуговування об'єкта проектування; річного економічного ефекту від впровадження запропонованих заходів; показників економічної ефективності впровадження системи захисту на підприємстві.

3.1 Розрахунок (фіксованих) капітальних витрат

Капітальними витрати називаються тому, що робляться, як правило, один раз, на початкових етапах створення ІС. До капітальних слід відносити наступні витрати: вартість розробки і впровадження проекту; залучення зовнішніх консультантів; первинні закупівлі основного ПЗ; первинні закупівлі додаткового ПЗ; первинні закупівлі апаратного забезпечення тощо.

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

3.1.1 Визначення трудомісткості розробки підходу щодо забезпечення конфіденційності при передачі інформації з використанням вейвлет-перетворення сигналів

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 забезпечення конфіденційності при передачі інформації з використанням вейвлет-перетворення сигналів, $t_{тз}$=20;

$t_в$ – тривалість аналізу існуючих інформаційних потоків організації, вивчення ТЗ, літературних джерел за темою тощо, $t_в$=42;

$t_а$ – тривалість аналізу існуючих загроз безпеки інформації, $t_а$=30;

$t_р$ – тривалість розробки підходу щодо стеганографічного вбудовування інформації в цифрове зображення із використанням вейвлет-фільтрів, $t_м$=50;

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

Отже,

$$t = t_{тз} + t_в + t_а + t_р + t_д = 20+42+30+50+10 = 152 \text{ години.}$$

3.1.2 Розрахунок витрат на розробку підходу щодо забезпечення конфіденційності при передачі інформації з використанням вейвлет-перетворення сигналів

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 $З_{мч}$.

$$К_{рп} = З_{зп} + З_{мч} .$$

$$К_{рп} = З_{зп} + З_{мч} = 34200+1173,44 = 35373,44 \text{ грн.}$$

$$З_{зп} = t\, З_{пр} = 152*225 = 34200 \text{ грн.}$$

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:

$$З_{мч} = t*С_{мч}=152*7,72=1173,44 \text{ грн.}$$

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

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

Вартість 1 години машинного часу ПК визначається за формулою:

$$C_{мч} = 0,9 \cdot 2 \cdot 1,68 + \frac{6800 \cdot 0,3}{1920} + \frac{1125 \cdot 0,2}{1920} = 7,72 \text{ грн.}$$

Оцінка ефективності запропонованого підходу до забезпечення конфіденційності при передачі інформації з використанням вейвлет-перетворення сигналів проведена шляхом моделювання в середовищі Matlab/Simulink за допомогою стандартних і розроблених програм. Зазначене програмне забезпечення вже використовується, тому в цьому випадку капітальні витрати не виникають.

Додаткові витрати, які складають 9400 грн., виникають у разі залучення зовнішніх консультантів.

Витрати на встановлення обладнання та налагодження системи інформаційної безпеки становитимуть 4200 грн.

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

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

$$=36296,08+9400+4200= 49896,08 \text{ грн.}$$

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.

3.1.3 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.

Оскільки середовище Matlab/Simulink, яке використовується для оцінки ефективності запропонованого підходу до забезпечення конфіденційності при передачі інформації з використанням вейвлет-перетворення сигналів вже використовується, 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 10000 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 21000 грн. Додаткова заробітна плата – 5% від основної заробітної плати. Виконання роботи щодо впровадження системи захисту інформації на підприємстві потребує залучення спеціаліста інформаційної безпеки на 0,1 ставки.

Отже,

$$С_з = (21000*12 + 21000*12*0,05)*0,1= 26460 \text{ грн.}$$

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

$$С_{єв} = 26460*0,22 = 5821,2 \text{ грн.}$$

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, ($Ц_е$ = 1,68 грн./кВт за годину).

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

$$С_{ел} = 0,9*2*1920*1,68 = 5806,08 \text{ грн.}$$

Витрати на технічне й організаційне адміністрування та сервіс системи інформаційної безпеки визначаються у відсотках від вартості капітальних витрат – 1% ($С_{тос}$ = 49896,08*0,01=498,96 грн).

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

$$С_к = 10000+26460+5821,2 +5806,08 +498,96 = 48586,24 \text{ грн.}$$

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 15%. Тому:

$$С_{ак} = 49896,08*0,15=7484,41 \text{ грн.}$$

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

$$С = 48586,24 + 7484,41 = 56070,75 \text{ грн.}$$

3.2 Оцінка можливого збитку

3.2.1 Оцінка величини збитку

Запропонований підхід до забезпечення конфіденційності при передачі інформації з використанням вейвлет-перетворення сигналів може бути використаний для організації прихованого зберігання і передачі конфіденційної інформації по відкритих каналах зв'язку.

Оцінка величини можливого збитку визначатиметься для умовного підприємства, яке може передавати інформацію по відкритих каналах зв'язку, вартість якої потенційно складає 600000 грн.

Вірогідність реалізації загроз (R) при передачі інформації, складає 65%.

Отже, можлива величина збитку (В) на рік від загроз щодо при передачі інформації, які можуть порушити цілісність інформації, становитиме:

$$B = 600000*0,65 = 390000 \text{ грн.}$$

3.2.2 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 (65%);

С – щорічні витрати на експлуатацію системи інформаційної безпеки.

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

$$E = 390000 - 56070,75 = 333929,25 \text{ грн.}$$

3.3 Визначення та аналіз показників економічної ефективності системи інформаційної безпеки

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

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

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

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

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

Коефіцієнт повернення інвестицій ROSI:

$$ROSI = \frac{333929,25}{49896.08} = 6,69 \text{ частки одиниці,}$$

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, (6,5%);

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

Розрахункове значення коефіцієнта повернення інвестицій:

$$6,69 > (6,5 - 5,5)/100 = 6,69 > 0,01.$$

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

$$T_o = \frac{K}{E} = \frac{1}{ROSI} = \frac{1}{6.69} = 0,15 \text{ років .}$$

3.4 Висновок

Таким чином, забезпечення конфіденційності при передачі інформації з використанням вейвлет-перетворення сигналів можна вважати економічно доцільним, виходячи з отриманих значень показників економічної ефективності. Коефіцієнт повернення інвестицій ROSI свідчить про отримання 6,69 грн. економічного ефекту на 1 грн. капітальних витрат. При цьому період окупності складатиме 0,15 років. Капітальні витрати складатимуть 49896,08 грн.

ВИСНОВКИ

Основні результати кваліфікаційної роботи полягають у наступному:

1. Захист інформації при її передачі каналом зв'язку є однією з проблем, особливо актуальних у період активного розвитку сучасних інформаційних технологій. Одним з нових способів вирішення цієї проблеми є застосування для передачі повідомлень широкосмугових хаотичних сигналів. Вейвлет перетворення є потужним інструментом аналізу, застосовним до коротких, зашумлених і нестаціонарних випадкових процесів. До переваг теорії вейвлетів належить можливість усунення некоректності операції диференціювання зашумлених часових рядів шляхом переходу в простір вейвлет-коефіцієнтів. Наразі значний інтерес викликають комбіновані підходи, що базуються на поєднанні вейвлетів з іншими методами аналізу структури сигналів.

2. Проаналізовано існуючі підходи до виділення інформаційних повідомлень із хаотичного несучого сигналу на основі реконструкції динамічних систем. Встановлено, що підходи, які ґрунтуються на явищі синхронізації, мають ряд недоліків, найбільш істотною з яких є вимога ідентичності генераторів хаотичних коливань у приймачі та передавачі. Якщо параметри відповідних генераторів відрізнятимуться більш ніж на 1–2%, то ці методи стають неефективними. Головним же недоліком підходу до детектування, що базується на реконструкції ДС, є необхідність диференціювання сигналів, які на практиці завжди є зашумленими. Обчислення похідних за наявності адитивного шуму призводить до суттєвих помилок.

3. Використання техніки реконструкції динамічних систем спільно з дискретним вейвлет-перетворенням в системі захищеної передачі інформації, що використовує принцип модуляції параметрів генератора хаотичних коливань і хаотичні несучі сигнали, дозволяє здійснювати детектування декількох інформаційних повідомлень, що одночасно передаються в одному несучому сигналі. Наявність тільки одного генератора хаотичних коливань, розташованого в передавальному пристрої, усуває проблему неідентичності

генераторів приймача і передавача, що є однією з ключових для систем захищеної передачі інформації, які реалізують процедуру детектування на основі ефекту синхронізації коливань. Дискретні вейвлети допомагають звести систему звичайних диференціальних рівнянь до системи рівнянь алгебри для визначення параметрів передавального генератора (вирішуючи при цьому одну з технічних проблем, пов'язаних з необхідністю диференціювання зашумлених сигналів). Однією з переваг теорії вейвлетів є можливість усунення некоректності операції диференціювання зашумлених часових рядів шляхом переходу в простір вейвлет-коефіцієнтів та заміни похідної від сигналу на похідну від вейвлета. Це дозволяє суттєво знизити похибки детектування.

4. Порівняно з використанням підходу до детектування, який базується на реконструкції ДС у тому варіанті, який був представлений в розділі 1.3, підхід до забезпечення конфіденційності при передачі інформації заснований на техніці глобальної реконструкції динамічних систем та дискретного вейвлет-перетворення, розглянутий у даному розділі, забезпечує не тільки суттєвий виграш у швидкості обчислень, але й значно більш високу стійкість до завад. Для вирішення завдання вибору материнського вейвлету при застосуванні математичного апарату вейвлет-перетворення запропоновано використовувати вейвлет-частотну характеристику як основу для вибору вейвлет-базису. ВЧХ визначається як чутливість вейвлет-коефіцієнтів розкладання від частоти сигналу і дозволяє аналізувати будь-який вейвлет як базис, не вимагаючи наявності скейлинг-функції й реконструкції сигналу. Оптимальний вейвлет-базис визначається як вейвлет, який має такі мінімальні значення параметрів ВЧХ: ширина смуги пропускання головної пелюстки, площа бічних пелюсток, близькість центральної частоти головної пелюстки до частоти вхідного сигналу.

ПЕРЕЛІК ПОСИЛАНЬ

1. Добеши И. Десять лекций по вейвлетам. / И. Добеши. И: НИЦ «Регулярная и хаотическая динамика», 2001. – 464 с.

2. Packard N.H., Crutchfield J.P., Farmer J.D., Shaw R.S. Geometry from a Time Series // Phys. Rev. Lett. –1980. –Vol. 45. –P. 712-715.

3. Takens F. Lecture Notes in Mathematics / F. Takens // Ed. by D.A. Rang, L.S. Young. Berlin: Springer, 1981. – Vol. 898. – P. 366-381.

4. Cuomo K. Circuit Implementation of Synchronized Chaos with Application to Communications / K. Cuomo, A. Oppenheim // Phys. Rev. Lett. – 1993. – Vol. 71. – P. 65–68.

5. Transmission of digital signals by chaotic synchronization / U. Parlitz, L. Chua, L. Kosarev et al. // Int. J. Bifurcation and Chaos. – 1992. – 2, N 4. – P. 973–977.

6. Dedieu H. Chaos Shift Keying Modulation and Demodulation of a Chaotic Carrier Using Self-synchronizing Chua's Circuits / H. Dedieu, M. P. Kennedy, M. Hasler // IEEE Trans. Circuits and Systems. – 1993. – 40, N 10. – P. 634–642.

7. Прикладне застосування теорії хаотичних систем у телекомунікаціях : монографія / Ю.Я. Бобало, С.Д. Галюк, М.М. Климаш, Р.Л. Політанський; Міністерство освіти і науки України, Національний університет "Львівська політехніка". – Львів ; Дрогобич : Коло, 2015. – 184 с.

8. Li T.Y. Period three implies chaos / T.Y. Li, J.A. Yorke // The American mathematical monthly. – 1975. – Vol. 82. – № 10. – P. 985-992.

9. Gonzalez, J.A. Chaos-induced true randomness / J.A. Gonzalez, L.I. Reyes, J.J. Suarez, L.E. Guerrero, G. Gutierez // Physica A. – 2002. – V. 316. – P. 259-288.

10. Chen, G. A symmetric image encryption scheme based on 3D chaotic cat maps / G. Chen, Y. Mao., C.K. Chui // Chaos, Solitons and Fractals. – 2004. – V. 21. – P. 749-761.

11. Kocarev, L. Public-key encryption with chaos / L. Kocarev, M. Sterjev // Chaos. – 2004. – V. 14 – № 4. – P. 1078-1082.

12. Pecora L.M. Driving system switch chaotic signals / L. M. Pecora, T. L. Carroll // Phys. Rev. A. – 1991. – Vol. 44. – № 4. – P. 2374-2383.

13. Пиковский А. С. Синхронизация. Фундаментальное нелинейное явление / А.С. Пиковский, М.Г. Розеблюм, Ю. Куртс. – Москва : Техносфера. – 2003. – 496 с.

14. Кузнецов С. П. Динамический хаос (курс лекций) / С. П. Кузнецов. – М.: Физматлит, 2006. – 356 с.

15. Lorenz E.N. Deterministic nonperiodic flow / E. N. Lorenz // J. Atmos. Sci. – Vol. 20. – № 2. – P. 130-141.

16. Кроновер, Р. М. Фракталы и хаос в динамических системах. Основы теории: пер. с англ. – L.: Jones and Bartlett Publishers Inc.; М.: Постмаркет, 1999. – 352с.

17. Дмитриев А.С. Прямохаотические системы связи / А.С. Дмитриев, Л.В. Кузьмин, А.И. Панас, Д.Ю. Пузиков, С.О. Старков // Успехи современной радиоэлектроники. –2003. –№ 9. – С.40-55.

18. Дмитриев, А. С. Сверхширокополосная беспроводная связь на основе динамического хаоса / А. С. Дмитриев, А. В. Клецов, А. М. Лактюшкин, А. И. Панас, С. О. Старков // Радиотехника и Электроника. –2006. – Т.51, № 10. – С.1193-1209.

19. Корнієнко В.І. Інтелектуальне моделювання нелінійних динамічних процесів в системах керування, кібербезпеки, телекомунікацій: підручник / В.І. Корнієнко, О.Ю. Гусєв, О.В. Герасіна; за заг. ред. В.І. Корнієнка ; М-во освіти і науки України, Нац. техн. ун-т «Дніпровська політехніка». – Дніпро : НТУ «ДП», 2020. – 536 с.

20. Munoz A. Continuous wavelet transform with arbitrary scales and O(N) complexity / A. Munoz, R. Ertlé, M. Unser // Signal Processing. – 2002. – Vol. 82. – P. 749-757.

21. Малла С. Вейвлеты в обработке сигналов. / С. Малла– М.: Мир, 2005. – 672 с.

22. Чуи К. Введение в вейвлеты. / К. Чуи – М.: Мир, 2001. – 412 с.

23. Блаттер К. Вейвлет-анализ. Основы теории. / К. Блаттер – М.: Техносфера, 2004. – 280 с.

24. Переберин А.В. О систематизации вейвлет-преобразований / А.В. Переберин // Вычисл. математика и программирование. – 2001. – № 2. – С. 15-40.

25. Mallat S.G. A theory for multiresolution signal decomposition: the wavelet representation // IEEE Transactions on pattern analysis and machine intelligence. – 1989. – Vol. 11, N 7. – P. 674-693.

26. Daubechies I. Factoring wavelet transforms into lifting steps / I. Daubechies, W. Sweldens // J. of Fourier Analysis and Applications. – 1998. – Vol. 4, N 3. – P. 247-269.

27. Kocarev L., Halle K.S., Eckert K., Chua L.O., Parlitz U. Experimental demonstration of secure communications via chaotic synchronization // Int. J. Bifurcation Chaos. – 1992. – Vol. 2. – P. 709.

28. Wu C.W., Chua L.O. A simple way to synchronize chaotic systems with applications to secure communication systems // Int. J. Bifurcation Chaos. – 1993. – Vol. 3. – P. 1619.

29. Cuomo K.M., Oppenheim A.V., Strogatz S.H. Synchronization of Lorenz-based chaotic circuits with application to communications // IEEE Trans. Circuits Syst. – 1993. – Vol. 40. – P. 626.

30. Parlitz U. Estimating model parameters from time series by autosynchronization / U. Parlitz // Phys. Rev. Lett. – 1996. – Vol. 76. – P. 1232.

31. Parlitz U. Multichannel communication using autosynchronization / U. Parlitz, L. Kocarev // Int. J. Bifurcation Chaos. – 1996. – Vol. 6. – P. 581.

32. Дмитриев А.С. Динамический хаос. Новые носители информации для систем связи. / А.С. Дмитриев, А.И. Панас. – М: Физматлит, 2002.

33. Starkov S.O. Digital communication systems, using chaos / S.O. Starkov, S.V. Yemetz // Proc. Int. Conf. Control of Oscillations and Chaos. St.Peterburg, 1997. – Vol. 2. – P. 207.

34. Dmitriev A.S., Kyarginsky B.Ye., Panas A.I., Starkov S.O. Experiments on ultra wideband direct chaotic information transmission in microwave band // Int. J. Bifurcation and Chaos. – 2003. – Vol. 13. – P. 1495.

35. Короновский А.А., Москаленко О.И., Попов П.В., Храмов А.Е. Способ скрытой передачи информации, основанный на явлении обобщенной синхронизации // Известия РАН. Серия физическая. – 2008. – Т. 72, № 1. – С. 143.

36. Anishchenko V.S. Global reconstruction in the presence of a priori information / V.S. Anishchenko, A.N. Pavlov, N.B. Janson // Chaos, Solitons and Fractals. – 1998. – Vol. 9. – P. 1267.

37. Janson N.B., Pavlov A.N., Anishchenko V.S. // Chaos and its reconstruction / Edited by G. Gouesbet, S. Meunier-Guttin-Cluzel. – New York: Novascience publishers, 2003. – P. 287.

38. Gribkov D.A., Gribkova V.V, Kuznetsov Yu.I., Rzhanov A.G. Global dynamical modeling of time series and application to restoration of broadband signal characteristics // Chaotic, fractal and nonlinear signal processing. – Edited R.A. Katz. Mystic, Juli, 1995. – P. 181.

39. Анищенко В.С., Павлов А.Н., Янсон Н.Б. Реконструкция динамических систем в приложении к решению задачи защиты информации // Журнал технической физики. – 1998. – № 12. – С. 1.

40. Bezruchko B.P., Dikanev T.V., Smirnov D.A. Role of transient processes for reconstruction of model equations from time series // Phys. Rev. E. – 2001. – Vol. 64. – P. 036210.

41. Anishchenko V.S., Astakhov V.V., Neiman A.B., Vadivasova T.E., Schimansky-Geier L. Nonlinear Dynamics of Chaotic and Stochastic Systems. Tutorial and Modern Development. – Berlin, Heidelberg: Springer, 2007.

42. Janson N.B. Chaos and its reconstruction / N.B. Janson, A.N. Pavlov, V.S. Anishchenko // Edited by G. Gouesbet, S. Meunier-Guttin-Cluzel. – New York: Novascience publishers, 2003. – P. 287.

43. Астафьева Н.М. Вейвлет-анализ: основы теории и примеры применения / Н.М. Астафьева // Успехи физических наук. – 1996. – Т. 166. – С. 1145.

44. Meyer Y. Wavelets: Algorithms and Applications. / Y. Meyer– Philadelphie: S.I.A.M., 1993.

45. Дремин И.М. Вейвлеты и их применение / И.М. Дремин, О.В. Иванов, В.А. Нечитайло // Успехи физических наук. 2001. – Т. 171. – С. 465.

46. Сергиенко А.Б. Цифровая обработка сигналов / А.Б. Сергиенко. – 2-е издание. – СПб.: Питер, 2006. – 752 с.

47. Сато Юкио. Обработка сигналов. Первое знакомство / Юкио Сато. – М.: Додэка-XXI, 2008. – 176 с.

48. Оппенгейм А. Цифровая обработка сигналов / А. Оппенгейм, Р. Шафер. – Изд. 2-е, испр. – М.: Техносфера, 2007. – 856 с.

49. Ососков, Г. Применение вейвлет-анализа для обработки дискретных сигналов гауссовой формы. / Г. Ососков, А. Шитов. — Сообщение ОИЯИ Р11-97-347. – Дубна, 1997.

50. Ososkov, G. Gaussian Wavelet Features and their Applications for Analysis of Discretized Signals. / G. Ososkov, F. Shitov. — Computer Physics Communications, 2000. – Vol. 126. – P. 149-157.

51. Barclay, V.J. Application of Wavelet Transforms to Experimental Spectra: Smoothing, Denoising and Data Set Compression / V.J. Barclay, R.F. Bonner, I.P. Hamilton //Anal.Chem.1997. – Vol. 69, No.l. – P. 78-90.

52. Pen W. Application of Wavelets to Filtering of Noisy Data. / W. Pen. In Wavelets: the Key to Intermittent Information? – Oxford University Press, 2000. – 255 p.

53. Штарк Г. Г. Применение вейвлетов для ЦОС // Перевод с англ. Н. И. Смирновой / Под ред. А.Г. Кюркчана. -М.: Техносфера, 2007. - 192 с.

54. Айфичер Эммануил С. Цифровая обработка сигналов: практический подход / Эммануил С. Айфичер, Барри У. Джервис. – М.: Вильямс, 2004. – 992 с.

55. Короновский А.А. Анализ фазовой хаотической синхронизации с помощью непрерывного вейвлетного преобразования / А.А. Короновский, А.Е. Храмов // Письма в ЖТФ, 2004. - Т. 30, № 14. - С. 29-36.

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	3	
5	А4	Стан питання. Постановка задачі	33	
6	А4	Спеціальна частина	18	
7	А4	Економічний розділ	8	
8	А4	Висновки	2	
9	А4	Перелік посилань	6	
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 Зубова.ppt

2 Диплом Зубов.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 125м-20-1 Зубова Д.С.

на тему: «Забезпечення конфіденційності при передачі інформації з використанням вейвлет-перетворення сигналів»

Пояснювальна записка складається зі вступу, трьох розділів і висновків, розташованих на 82 сторінках.

Мета роботи є актуальною, оскільки вона спрямована на підвищення завадостійкості при передачі інформації з використанням динамічного хаосу та дискретного вейвлет-перетворення сигналів.

При виконанні роботи автор продемонстрував добрий рівень теоретичних знань і практичних навичок. На основі аналізу теорії вейвлетів і принципів передачі інформації в системах зв'язку з використанням теорії хаосу, а також існуючих підходів до виділення інформаційних повідомлень із хаотичного несучого сигналу на основі реконструкції динамічних систем в ній сформульовані задачі, вирішенню яких присвячений спеціальний розділ. У ньому розглянуто і досліджено підхід, заснований на поєднанні техніки глобальної реконструкції та дискретного вейвлет-перетворення та оцінено його ефективність.

Практична цінність роботи полягає в тому, що впровадження дослідженого підходу дозволить прискорити процедуру обчислень за рахунок застосування швидких (пірамідальних) алгоритмів ВП.

Рівень запозичень у кваліфікаційній роботі відповідає вимогам «Положення про систему виявлення та запобігання плагіату».

В цілому робота задовольняє усім вимогам, а її автор Зубов Д.С. заслуговує на оцінку « » та присвоєння кваліфікації «Магістр з кібербезпеки» за спеціальністю 125 Кібербезпека.

Керівник роботи,

к.т.н., доцент **О.В. Герасіна**