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 *Ахмєдова Ахмеда Анара огли*

академічної групи *125м-20-2*

спеціальності *125 Кібербезпека*

спеціалізації[1]

за освітньо-професійною програмою *Кібербезпека*

на тему *Забезпечення конфіденційності в системах передачі інформації з використанням хаотичних коливань*

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 *Ахмєдову Ахмеду Анару огли* **академічної групи** *125м-20-2*
(прізвище ім'я по-батькові) (шифр)

спеціальності *125 Кібербезпека*

за освітньо-професійною програмою *Кібербезпека*

на тему *Забезпечення конфіденційності в системах передачі інформації з використанням хаотичних коливань*

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

Розділ	Зміст	Термін виконання
Розділ 1	Аналіз шляхів передачі інформації в системах зв'язку з використанням хаотичних коливань, а також існуючих схем і підходів до прихованої передачі з використанням хаотичних сигналів.	03.09.2021 – 10.10.2021
Розділ 2	Обґрунтування і дослідження підходу до прихованої передачі з підвищеною стійкістю до шумів на основі узагальненої хаотичної синхронізації, а також 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 _____ Ахмєдов А.А.
(підпис студента) (прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 87 с., 17 рис., 4 додатки, 38 джерел.

Об’єкт дослідження – детерміновані хаотичні сигнали.

Предмет дослідження – підходи до прихованої передачі інформації в системах зв’язку з використанням хаотичних коливань.

Мета кваліфікаційної роботи – забезпечення більш високого ступеня захисту інформації при її передачі в системах передачі інформації з використанням хаотичних коливань.

Наукова новизна результатів полягає у тому, що досліджений підхід до прихованої передачі з підвищеною стійкістю до шумів на основі узагальненої хаотичної синхронізації, реалізований на основі моделі Реслера має перевагу у стійкості до шумів і до нелінійних спотворень каналу зв'язку.

У першому розділі проаналізовано шляхи передачі інформації в системах зв’язку з використанням хаотичних коливань, а також існуючі схеми і підходи до прихованої передачі з використанням хаотичних сигналів.

У спеціальній частині роботи обґрунтовано структурну стійкість режиму узагальненої синхронізації до шумів, досліджено підхід до прихованої передачі з підвищеною стійкістю до шумів на основі узагальненої хаотичної синхронізації, оцінено ефективність відомих схем і підходів до прихованої передачі інформації. 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, ХАОТИЧНА СИНХРОНІЗАЦІЯ, ПРИХОВАНА ПЕРЕДАЧА ІНФОРМАЦІЇ, ДЕТЕРМІНОВАНІ СИГНАЛИ, КАНАЛ ЗВ’ЯЗКУ, ФАЗОВИЙ ПОРТРЕТ, ІМІТАЦІЙНЕ МОДЕЛЮВАННЯ

РЕФЕРАТ

Пояснительная записка 87 с., 17 рис., 4 приложения, 38 источников.

Объект исследования – детерминированные хаотические сигналы.

Предмет исследования – подходы к скрытой передаче информации в системах связи с использованием хаотических колебаний.

Цель квалификационной работы – обеспечение более высокой степени защиты информации при ее передаче в системах передачи информации с использованием хаотических колебаний.

Научная новизна результатов заключается в том, что исследованный подход к скрытой передаче с повышенной стойкостью к шумам на основе обобщенной хаотической синхронизации, реализованный на основе модели Реслера, имеет преимущество в устойчивости к шумам и нелинейным искажениям канала связи.

В первой главе проанализированы пути передачи информации в системах связи с использованием хаотических колебаний, а также существующие схемы и подходы к скрытой передаче с использованием хаотических сигналов.

В специальной части работы обоснована структурная устойчивость режима обобщенной синхронизации к шумам, исследован подход к скрытой передаче с повышенной устойчивостью к шумам на основе обобщенной хаотической синхронизации, оценена эффективность известных схем и подходов к скрытой передаче информации. По результатам исследований сделаны выводы о решении поставленной задачи.

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

ЦИФРОВАЯ ОБРАБОТКА СИГНАЛОВ, ХАОТИЧЕСКАЯ СИНХРОНИЗАЦИЯ, СКРЫТАЯ ПЕРЕДАЧА ИНФОРМАЦИИ, ДЕТЕРМИНИРОВАННЫЕ СИГНАЛЫ, КАНАЛ СВЯЗИ, ФАЗОВЫЙ ПОРТРЕТ, ИМИТАЦИОННОЕ МОДЕЛИРОВАНИЕ

ABSTRACT

Explanatory note: p. 87, fig. 27, 4 additions, 38 sources.

The object of study is deterministic chaotic signals.

The subject of research is approaches to covert transmission of information in communication systems using chaotic oscillations.

The purpose of the qualification work is to provide a higher degree of protection of information during its transmission in information transmission systems using chaotic oscillations.

The scientific novelty of the results is that the investigated approach to latent transmission with increased noise resistance based on generalized chaotic synchronization, implemented on the basis of the Rössler model has an advantage in noise resistance and nonlinear distortion of the communication channel.

The first section analyzes the ways of information transmission in communication systems using chaotic oscillations, as well as existing schemes and approaches to covert transmission using chaotic signals.

In the special part of the work the structural stability of the generalized synchronization mode to noise is substantiated, the approach to latent transmission with increased noise resistance based on generalized chaotic synchronization is investigated, the efficiency of known schemes and approaches to latent transmission of information is evaluated. 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, CHAOTIC SYNCHRONIZATION, HIDDEN TRANSMISSION OF INFORMATION, DETERMINED SIGNALS, COMMUNICATION CHANNEL, PHASE PORTRAIT, SIMULATION MODELING

СПИСОК УМОВНИХ СКОРОЧЕНЬ

ВАХ – Вольт-амперна характеристика;

ОП – Операційний підсилювач;

ДС – Динамічна система;

НВЧ – Надвисокочастотний;

BER – Bit Error Rate – Коефіцієнт бітових похибок, відношення кількості помилкових біт до їх загального переданого числа;

SNR – Signal to Noise Ratio – Відношення сигнал / шум.

ЗМІСТ

с.

ВСТУП

Динамічний (детермінований) хаос – це неперіодичні коливання в нелінійних детермінованих системах, що демонструють високу чутливість до початкових умов. Ці коливання мають ряд спільних рис із випадковими процесами, зокрема, суцільний спектр потужності, але їх природа пов'язана не з випадковістю, а з нелінійними властивостями, що породжують нерегулярні коливання в динамічних системах [1-6].

Відкриття Лоренцем динамічного хаосу у 1961 р. та його подальші дослідження стало справжньої наукової революцією, яка привернула пильну увагу фахівців з різних галузей знань своєю поширеністю як у природних, так і штучних системах, простотою математичних моделей, на яких його можна дослідити, універсальністю шляхів виникнення з регулярної динаміки та біфуркаційних механізмів. Вивчення динамічного хаосу та пов'язаних із ним явищ зажадало, по суті, створення нового розділу математики – математика нелінійних динамічних систем зі складною поведінкою.

Крім загальнонаукового та світоглядного інтересу, динамічний хаос представляє великий інтерес і має великі потенційні можливості у сфері прикладних досліджень і розробок, насамперед у радіофізиці, електроніці, системах передачі та захисту інформації.

Отже, останні десятиліття характеризуються великим інтересом до використання хаотичних коливань як несучих передачі інформації. Виниклий інтерес був пов'язаний з відкриттям явищ хаотичної синхронізації і хаотичного синхронного відгуку. Наразі відомо декілька різних типів хаотичної синхронізації: фазова синхронізація, узагальнена синхронізація, повна синхронізація та синхронізація із запізненням. Відомо також, що ці типи синхронної поведінки можуть розглядатися як різні прояви одного і того ж режиму, відомого як синхронізація часових масштабів. Як правило, в системах такого типу для досягнення синхронізму необхідно забезпечувати високу ступінь ідентичності параметрів передавача і приймача. Структура і параметри

передавача, у загальному випадку, не відомі третім особам, що забезпечує конфіденційність інформації, яка передається.

Розроблені підходи та моделі передачі інформації з використанням хаотичної синхронізації та їх експериментальна перевірка заклали основу для подальшого розвитку хаотичних комунікацій. Інтерес до хаотичних комунікаційних систем обумовлений тим, що хаотичні системи мають широкосмуговий спектр потужності, дозволяють забезпечити високу швидкість передачі інформації і залишаються працездатні при малих відношеннях сигнал-шум. Крім того, вони допускають можливість простої апаратної реалізації з великим вибором різних коливальних режимів.

Проте, не дивлячись на наявність досить великого числа робіт, присвячених даній тематиці, ряд питань, залишається досі відкритим.

Таким чином, дослідження та вдосконалення підходів до прихованої передачі інформації в інформаційно-телекомунікаційних системах з використанням хаотичних коливань наразі є актуальною задачею.

Метою роботи є забезпечення більш високого ступеня захисту інформації при її передачі в системах передачі інформації з використанням хаотичних коливань.

Постановка задачі:

• проаналізовати шляхи передачі інформації в системах зв'язку з використанням хаотичних коливань;

• провести аналіз схем і підходів до прихованої передачі з використанням хаотичних сигналів;

• обґрунтувати структурну стійкість режиму узагальненої синхронізації до шумів;

• дослідити підходу до прихованої передачі з підвищеною стійкістю до шумів на основі узагальненої хаотичної синхронізації;

• оцінити ефективність відомих схем і підходів до прихованої передачі інформації на основі хаотичної синхронізації у середовищі Matlab за допомогою стандартних і розроблених програм.

1 СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ

1.1 Застосування хаотичної синхронізації для прихованої передачі інформації

1.1.1 Введення в предметну область

Синхронізація автоколивальних процесів є одним з фундаментальних нелінійних явищ, яке вже кілька століть з часів Гюйгенса (який вперше описав це явище з прикладу пов'язаних механічних систем (маятниковых годин)) привертає пильну увагу дослідників [1-7]. В останні десятиліття центр досліджень у цій галузі зміщується до дослідження синхронізації хаотичних автоколивань, що обумовлено великим інтересом у нелінійній фізиці до проблеми детермінованого хаосу та різних додатків теорії хаосу [8-13]. Тому вивчення хаотичної синхронізації стало природним розвитком теорії динамічного хаосу, що обумовлено як великим фундаментальним значенням дослідження хаотичної синхронізації, так і її широкими практичними додатками, наприклад, при прихованій передачі інформації [14-16], у біологічних, фізіологічних та хімічних завданнях, при керуванні хаосом, у тому числі, у системах надвисокочастотної (НВЧ) електроніки тощо.

Останнім часом увагу дослідників дедалі більше привертають не тільки радіофізичні моделі і системи, для яких було отримано основні результати у цій галузі [8], а й системи живої природи. Одним із цікавих, важливих напрямків є застосування хаотичної синхронізації в телекомунікаційних завданнях, у першу чергу, при створенні систем прихованої передачі інформації. Водночас оглядових робіт із застосування хаотичної синхронізації в інформаційно-телекомунікаційних системах не дуже багато. Так, лише за останні десять років, за даними ISI Web of Knowledge, кількість публікацій з цієї тематики зросла більш ніж у 100 разів. У цьому індекс цитування робіт у зазначеній області зростає практично експоненційно (рис. 1.1).

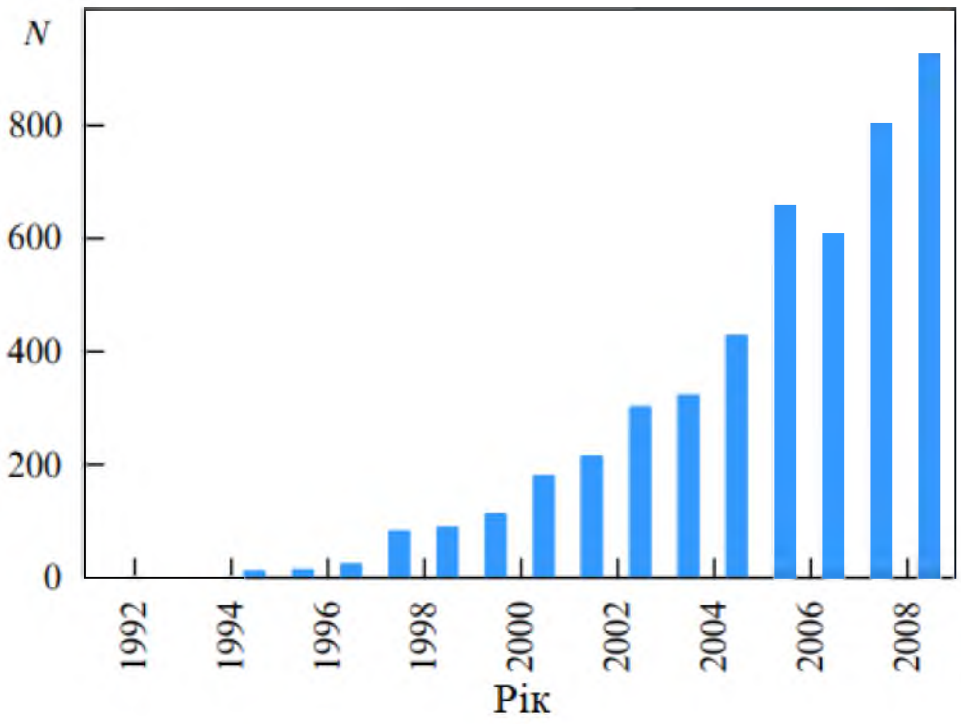

Рисунок 1.1 – Кількість цитувань у наукових журналах публікацій, присвячених використанню хаотичної синхронізації в інформаційно-телекомунікаційних системах, за роками

Нарешті, важливо відзначити, що останніми роками відбувся перехід від теоретичного розгляду проблеми до створення практичних зразків, що дозволили здійснити передачу інформації на основі хаотичної синхронізації на кілька десятків кілометрів із використанням раніше створених систем телекомунікації. Все вищесказане свідчить про важливість та актуальність даного напряму [17-21].

Більшість способів прихованої передачі з використанням синхронізації хаосу засновано, у першу чергу, на режимі повної хаотичної синхронізації [5], що тягне за собою вимогу до високого ступеня ідентичності генераторів, які розташовуються на різних сторонах каналу зв'язку. У зв'язку з відкриттям та інтенсивним вивченням інших типів синхронної поведінки пов'язаних хаотичних систем, таких як фазова синхронізація, узагальнена синхронізація, синхронізація із запізненням, синхронізація, індукована шумом, удосконалення

методів прихованої передачі даних на їх основі стало одним із важливих завдань досліджень у галузі створення інформаційно-телекомунікаційних систем на основі динамічного хаосу.

Слід зазначити, що частина способів прихованої передачі придатна передачі як аналогових, і цифрових сигналів. Однак частина методів може бути використана тільки для передачі цифрових сигналів. З метою досягнення можливості зіставлення всіх розглянутих підходів в рамках кваліфікаційної роботи було вирішено використовувати як інформаційні лише цифрові сигнали.

Принциповою перевагою методів на основі хаотичної синхронізації у порівнянні з традиційними методами (методом LSB (Least Significant Bit), exo-методами, методами розширеного спектру та іншими) є значне підвищення стійкості до шумів та спотворень у каналі зв'язку, а також збільшення швидкості передачі інформації [5]. Крім того, використання саме хаотичної синхронізації є надзвичайно важливим для підвищення конфіденційності передачі даних. Відомі й інші підходи до створення способів прихованої передачі з використанням динамічного хаосу, розгляду яких багато в чому присвячена монографія [12], що стала вже класичною і активно цитованою. Це насамперед прямохаотичні системи зв'язку, принцип роботи яких полягає у безпосередній генерації несучих інформацію хаотичних коливань, у тому числі у НВЧ-діапазоні, та модуляції цих коливань інформаційним сигналом. Такі методи порівняно легко реалізуються і дозволяють досягти швидкості передачі даних до 200 Мб/с. Однак конфіденційність схем на основі хаотичної синхронізації є значно вищою.

Незважаючи на різноманітність робіт, присвячених використанню хаотичної синхронізації в інформаційно-телекомунікаційних системах, слід зазначити, що в основі більшості способів передачі інформації лежать найперші, досить добре відомі способи прихованої передачі, що використовують явище повної хаотичної синхронізації. Ці методи лягли основою наступних, досконаліших методів, які, тим не менш, зберігають ряд недоліків, властивих і їх попередникам.

Однією з важливих проблем, з погляду передачі, є вплив шумів і спотворень сигналів на працездатність схем передачі. Відомо, що шуми практично завжди впливають на динаміку систем, причому цей вплив може призводити до істотних змін у поведінці систем [1-10], що стосовно схем передачі інформації, заснованих на явищі хаотичної синхронізації, може негативно позначатися на їх працездатності. Нелінійні спотворення можуть призводити до зниження працездатності таких схем [12]. Між тим, розгляд схем передачі інформації, заснованих на використанні режимів явища хаотичної синхронізації, у переважній більшості випадків проводиться у припущенні відсутності шумів та спотворень, що залишає низку найважливіших питань про можливість практичного застосування цих схем та їх ефективність відкритими.

1.1.2 Основні типи хаотичної синхронізації динамічних систем

Як вже зазначалось у розділі 1.1.1, основними типами хаотичної синхронізації, які лежать в основі сучасних систем зв'язку, є режими повної, фазової та узагальненої синхронізації [1-6, 8-13].

Режим повної синхронізації означає точний збіг векторів стану взаємодіючих (односпрямовано або взаємно пов'язаних) систем $\mathbf{x}(t)\equiv\mathbf{u}(t)$, і, отже, цей режим можливий лише у разі їх ідентичності за керуючими параметрами. Якщо керуючі параметри злегка різняться, можливе виникнення режиму синхронізації із запізненням, в якому взаємодіючі системи демонструють близькі до ідентичних, але зрушені на деякий інтервал часу τ коливання, тобто $\mathbf{x}(t)\approx\mathbf{u}(t+\tau)$. Зі збільшенням сили зв'язку між злегка розлаштованими осциляторами, часовий зсув τ прагне до нуля, а режим синхронізації із запізненням – до режиму повної хаотичної синхронізації.

Для діагностики режиму повної синхронізації досить часто проводять безпосереднє порівняння векторів станів взаємодіючих систем $\mathbf{x}(t)$ та $\mathbf{u}(t)$, розраховуючи похибку синхронізації:

$$\langle e \rangle = \int_0^\infty \|\mathbf{x}(t) - \mathbf{u}(t)\| \, \mathrm{d}t \,. \tag{1.1}$$

Слід зазначити, що в літературі досить часто, поряд з повною хаотичною синхронізацією, розглядають синхронізацію хаотичних систем, отриманих в результаті декомпозиції автоколивальної системи, або «хаотичний синхронний відгук». В результаті декомпозиції автоколивальна система набуває вигляду кільцевої структури, в якій підсистеми утворюють єдине кільце зворотного зв'язку. На наступному кроці використовуються дві ідентичні системи, отримані в результаті однакової декомпозиції, одну з яких залишають у первісному вигляді (ведуча автоколивальна, або активна система), а в іншій кільце зворотного зв'язку розривають (ведена, або пасивна система). Якщо сигнал з виходу однієї з підсистем ведучої системи подати на вхід іншої підсистеми веденої системи, то за певних умов різниця між вхідним і вихідним сигналами веденої системи буде прагнути до нуля, тобто виникне повна синхронізація між станами ведучої та веденої систем.

Узагальнена синхронізація, яка вводиться для системи двох односпрямовано пов'язаних хаотичних осциляторів – ведучого $\mathbf{x}(t)$ та веденого $\mathbf{u}(t)$, означає, що після завершення перехідного процесу встановлюється функціональна залежність між їхніми станами, тобто

$$\mathbf{u}(t)=F[\mathbf{x}(t)]. \tag{1.2}$$

При цьому вид залежності $F[\cdot]$ може бути досить складним, а процедура її знаходження дуже нетривіальною.

Наразі запропоновано декілька методів для діагностування режиму узагальненої синхронізації між хаотичними осциляторами, такі як метод найближчих сусідів, метод розрахунку умовних ляпуновських експонент і метод допоміжної системи. Останній досить часто використовується і є таким, що відносно легко здійснюється на практиці.

Суть методу допоміжної системи полягає у наступному. Поряд із веденою системою $\mathbf{u}(t)$ розглядається ідентична їй допоміжна система $\mathbf{v}(t)$. Початкові умови для допоміжної системи $\mathbf{v}(t_0)$ вибираються відмінними від початкових

умов веденої системи $\mathbf{u}(t_0)$, однак такі, що лежать у басейні тяжіння того ж атрактора (на практиці це означає невелике розлаштування початкових умов, що реалізується автоматично через наявність флуктуації). За відсутності режиму узагальненої синхронізації між взаємодіючими системами вектори стану веденої $\mathbf{u}(t)$ і допоміжної $\mathbf{v}(t)$ систем належать одному й тому хаотичному атрактору, але є різними. У тому випадку, коли має місце режим узагальненої синхронізації, після завершення перехідного процесу стани веденої та допоміжної систем повинні стати ідентичними, $\mathbf{u}(t)\equiv\mathbf{v}(t)$, в силу виконання співвідношень $\mathbf{u}(t)=F[\mathbf{x}(t)]$ і $\mathbf{v}(t)=F[\mathbf{x}(t)]$. Таким чином, еквівалентність станів веденої та допоміжної систем після перехідного процесу є критерієм наявності узагальненої синхронізації між ведучим та веденим осциляторами.

Аналіз режиму узагальненої синхронізації може бути проведений також за допомогою обчислення умовних ляпуновських експонент. Якщо розмірності фазових просторів відомої (drive system) і веденої (response system) систем відповідно дорівнюють N_d і N_r то поведінка односпрямовано пов'язаних хаотичних осциляторів може бути охарактеризовано за допомогою спектра ляпуновських показників $\lambda_1\geq\lambda_2\geq\ \geq\lambda_{Nd+Nr}$.

Взагалі, зважаючи на незалежність поведінки ведучої системи від стану веденого осцилятора спектр ляпуновських показників може бути розділений на дві частини: ляпуновські показники відомої системи $\lambda^d_1\geq\ldots\geq\lambda^d_{Nd}$ і умовні ляпуновські показники $\lambda^r_1\geq\ldots\geq\lambda^r_{Nr}$. Критерієм існування узагальненої синхронізації в односпрямовано пов'язаних динамічних системах є негативність старшого умовного ляпуновського показника λ^r_1. Слід підкреслити, що для односпрямовано пов'язаних хаотичних осциляторів режими повної синхронізації та синхронізації із запізненням є окремими випадками режиму узагальненої синхронізації.

Фазова синхронізація означає, що відбувається захоплення фаз хаотичних сигналів, тоді як амплітуди цих сигналів залишаються незв'язаними між собою і виглядають хаотичними. В основі концепції хаотичної фазової синхронізації лежить поняття миттєвої фази $\phi(t)$ хаотичного сигналу.

Слід зазначити, що немає універсального способу введення фази хаотичного сигналу, який би давав коректні результати будь-яких динамічних систем. Так, існує кілька способів введення фази, що підходять для систем з досить простою топологією хаотичного атрактора, які в літературі називають «системами з добре визначеною фазою» або «системами з фазово-когерентним атрактором». Хаотичний атрактор таких систем повинен бути таким, щоб проекція фазової траєкторії на деяку площину станів (x, y) постійно оберталася навколо деякого центру, не перетинаючи і не огинаючи його. Тоді миттєва фаза $\phi(t)$ хаотичного сигналу може бути введена в розгляд одним із наступних способів: як кут у полярній системі координат, за допомогою перетворення Гілберта часової реалізації сигналу або з використанням поверхні перерізу Пуанкаре. Однак для систем із погано визначеною фазою ці методи не працюють [5, 16]. Проте у ряді випадків фазова синхронізація подібних систем може бути виявлена за допомогою непрямих спостережень та вимірювань.

Фазова синхронізація виникає у тому випадку, коли різниця миттєвих фаз хаотичних сигналів $\mathbf{x}_{1,2}(t)$ введена одним з вищеперерахованих способів, є обмеженою в часі:

$$\left|\phi_1(t) - \phi_2(t)\right| < \text{const}. \tag{1.3}$$

Слід зазначити, що поняття «фазова синхронізація» може бути узагальнено введенням у розгляд множини часових масштабів s та асоційованих з ними фаз $\phi_s(t)$ хаотичного сигналу за допомогою безперервного вейвлетного перетворення з комплексним базисом.

Якщо існує діапазон (або набір діапазонів) часових масштабів $s_m<s<s_b$, для кожного з яких виконується умова захоплення фаз, аналогічна (1.3), і частка енергії вейвлетного спектра, що припадає на цей діапазон, відрізняється від нуля, то часові масштаби s виявляються синхронізованими, а хаотичні осцилятори знаходяться в режимі синхронізації часових масштабів. Якщо хоча б один часовий масштаб виявляється синхронізованим, то в деяких випадках можна говорити про наявність фазової синхронізації. Однак у разі систем з фазово-некогерентним атрактором, у яких фазову синхронізацію діагностувати

традиційними методами неможливо, говорять про виникнення синхронізації часових масштабів.

Слід зазначити, що синхронізація часових масштабів дозволяє розглядати з єдиних позицій усі вищеописані типи хаотичної синхронізації. Характер синхронного режиму при цьому визначається лише діапазоном синхронізованих часових масштабів.

1.1.3 Схеми прихованої передачі інформації

Можливість синхронізації хаотичних систем спонукала до пошуку способів використання даного явища для передавання інформації. В останні роки з'явилася велика кількість робіт, в яких запропоновані різні схеми передавання інформації, що базуються на повній синхронізації хаосу: хаотичне маскування, перемикання хаотичних режимів, нелінійне підмішування, адаптивні методи [5].

1.1.3.1. Хаотичне маскування.

Хаотичне маскування – один з перших і найбільш простих способів прихованої передачі даних. При хаотичному маскуванні інформаційний сигнал s(t) адитивно підмішується до хаотичного c(t) на виході ведучої системи [13].

Сумарний сигнал r(t)=s(t)+c(t), що передається через канал зв'язку до приймача, відновлюється завдяки синхронній роботі хаотичних систем передавача і приймача (рис. 1.2). Переданий корисний сигнал s(t) відновлюється як різниця між прийнятим сигналом та сигналом синхронного відгуку генератора приймача:

$$s'(t)=r'(t)-c'(t). \qquad (1.4)$$

Даний спосіб передавання інформації вимагає високого ступеню ідентичності ведучої та веденої хаотичних систем і необхідності перевищення потужності хаотичного сигналу над інформаційним на 35-65дБ.

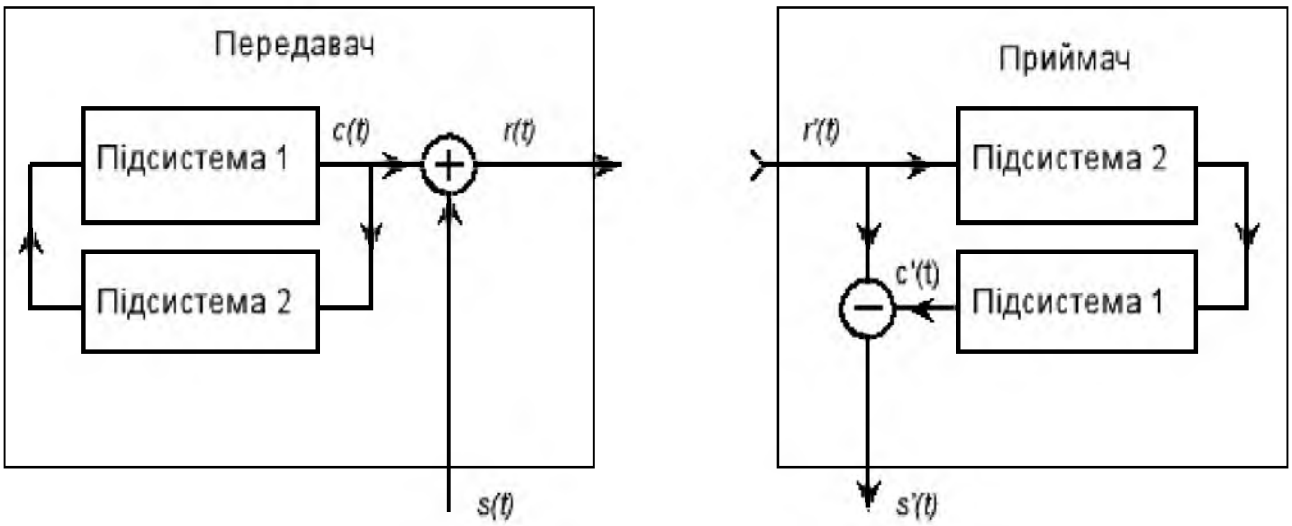

Рисунок 1.2 – Схема хаотичного маскування інформаційного повідомлення

При невиконанні цих умов спостерігаються сильні шуми десинхронізації, що унеможливлює передавання інформації. Шуми в каналі зв'язку призводить до різкого погіршення якості передавання інформації. Система залишається працездатною при співвідношенні сигнал/шум (SNR – Signal to Noise Ratio) більше 40-60дБ.

Крім того, існує проблема забезпечення конфіденційності передавання інформації. Незважаючи на низький рівень інформаційного сигналу в порівнянні з несучим хаотичним, існують методи, що дозволяють відновити початковий хаотичний сигнал за допомогою сигналу, що передається в каналі зв'язку, і відповідно, відновити передане повідомлення [13]. Внаслідок цього схема хаотичного маскування є малопридатною для прихованого передавання інформації.

1.1.3.2. Перемикання хаотичних режимів.

На початку 90-х років XX ст. було запропоновано, крім хаотичного маскування ще декілька способів прихованої передачі даних, об'єднаних загальною назвою «перемикання хаотичних режимів».

При перемиканні хаотичних режимів [23] різні інформаційні біти передаються за допомогою фрагментів хаотичного сигналу з генераторів, що структурно або параметрично відрізняються між собою (рис. 1.3).

Інформаційний сигнал, представлений послідовністю бінарних бітів «0» і «1», використовується для перемикання між генераторами при формуванні вихідного сигналу r(t).

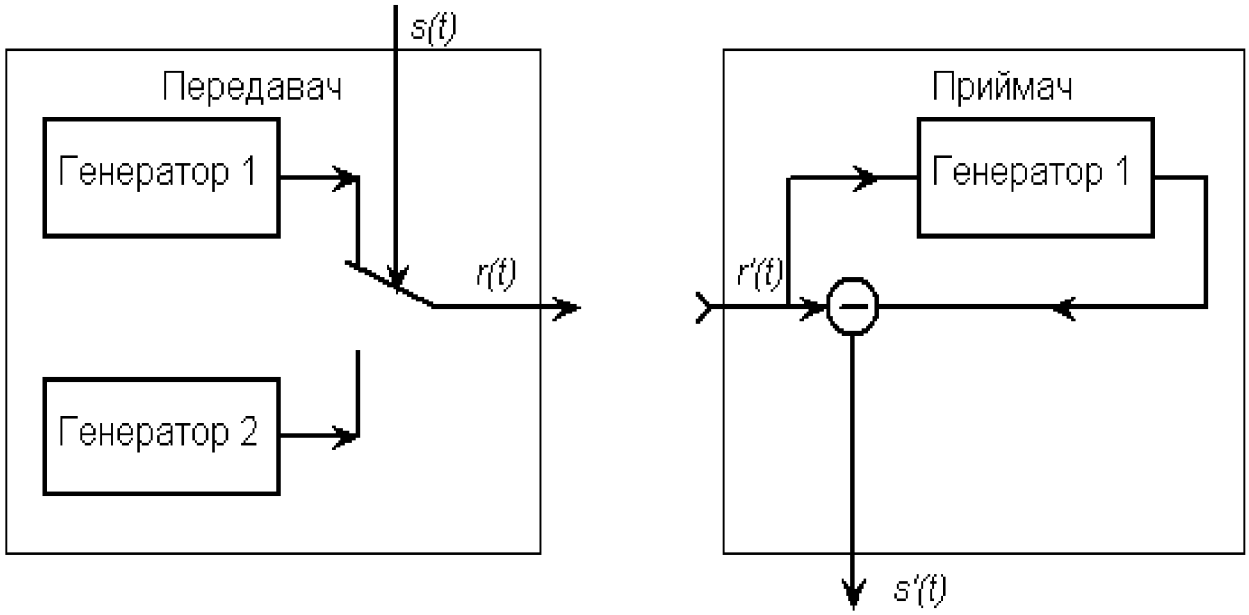

Рисунок 1.3 – Кодування інформації за схемою перемикання хаотичних режимів

В залежності від кількості генераторів на приймальній стороні розрізняють декілька способів прихованого (замаскованого) передавання даних на основі перемикання хаотичних режимів. В схемі на рис. 1.3 приймач містить один генератор, що є ідентичним одному з генераторів передавача. Параметри генераторів передавача вибираються таким чином, щоб генеровані ними сигнали забезпечували встановлення режиму повної синхронізації з генератором приймача тільки у випадку передавання одного з бітів «0» чи «1», і до десинхронізації в протилежному випадку. Відновлення переданого сигналу здійснюється шляхом віднімання прийнятого сигналу та вихідного сигналу генератора приймача.

Інші схеми прихованої передачі з використанням перемикання хаотичних режимів, засновані на тієї ж ідеї, та відрізняються від описаної вище схеми тільки будовою і роботою приймаючого пристрою. Так, приймаючий пристрій

може містити два хаотичних генератора, ідентичних передавальним генераторам, і, отже, два віднімаючих пристрої для детектування корисного сигналу. У цьому випадку корисний сигнал діагностується за наявністю або відсутністю хаотичних коливань сигналів на виході приймаючого пристрою.

Схеми з перемиканням хаотичних режимів є більш стійкими до дії на них шумів і флуктуацій в каналі зв'язку, але стійкість їх роботи залишається обмеженою. У випадку, якщо у жорстких обмеженнях на розлаштування параметрів генераторів передавача немає необхідності, то забезпечення конфіденційності можливе при виборі їх значень таким чином, щоб генеровані сигнали мали якомога близькі статистичні характеристики. Недоліками схеми є виникнення перехідних процесів при перемиканні, що зменшує швидкодію системи.

Ступінь конфіденційності таких схем є низькою, а також існує ймовірність енергетичного виявлення передавання інформації при використанні в передавачі структурно однакових генераторів, що відрізняються значеннями параметрів.

1.1.3.3. Нелінійне підмішування.

Удосконалення методу хаотичного маскування були спрямовані на підвищення секретності та конфіденційності передачі інформації. В результаті було запропоновано декілька способів, які можна поєднати загальною назвою «нелінійне підмішування інформаційного сигналу до хаотичного».

Особливістю роботи таких схем є безпосереднє введення інформаційного сигналу в передавальну систему та його участь у формуванні вихідного сигналу передавача [24-25]. Найчастіше інформаційний сигнал вводиться за допомогою операції додавання з носійним сигналом і відновлюється на приймальній стороні за допомогою операції віднімання від прийнятого сигналу сигналу, що генерований приймальною стороною. У схемі з нелінійним підмішуванням немає обмежень відносно рівня потужності інформаційного сигналу, але при його виборі необхідно забезпечити незначну зміну динамічного режиму

хаотичної системи під впливом інформаційного сигналу. За рахунок циркуляції по колу оберненого зв’язку над вхідним інформаційним сигналом здійснюється нелінійне перетворення., Прийнятий з каналу зв’язку сигнал r'(t) синхронізує генератор приймача при передаванні бінарного біта «0». У випадку передавання біта «1» синхронізація генераторів приймальної та передавальної сторін відсутня. Відновлений сигнал s'(t) є різницею між прийнятим сигналом та відгуком системи на цей сигнал (рис. 1.4).

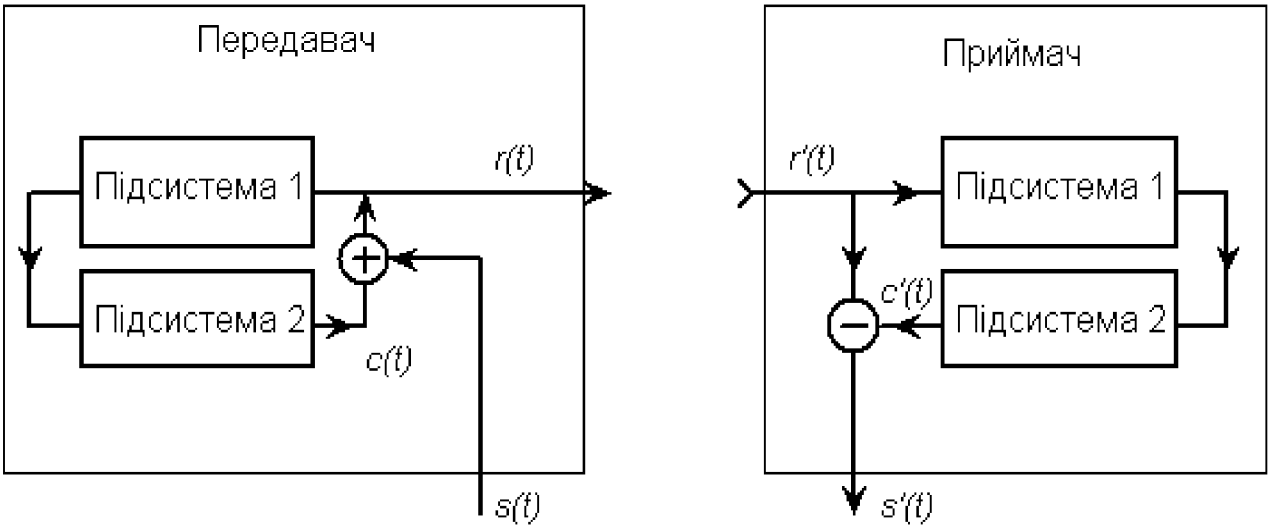

Рисунок 1.4 – Нелінійне підмішування інформаційного сигналу до хаотичного з використанням операцій додавання-віднімання

Важливою перевагою таких схем перед схемами заснованими на хаотичному маскуванні, є можливість варіювання рівня інформаційного повідомлення, що вводиться. Це дозволяє управляти якістю передачі інформації. У той же час, збільшення якості передачі інформації тягне за собою, як відомо, втрату її конфіденційності, що є істотним недоліком. Крім того, такі схеми характеризуються досить низькою стійкістю до шумів в каналі зв'язку і до розладу керуючих параметрів спочатку ідентичних хаотичних генераторів. Необхідність забезпечення ідентичності трьох генераторів хаосу, два з яких знаходяться на різних сторонах каналу зв'язку, являє собою технічне завдання, яке складно вирішується, і є ще одним недоліком такої схеми.

Залежність сигналу, що передається від інформаційного, оскільки передавальний генератор по суті є неавтономною системою, що не гарантує формування їм саме хаотичного сигналу при зміні тих чи інших параметрів схеми, може призводити до втрати конфіденційності.

Отже, схеми з нелінійним підмішуванням характеризуються низькою стійкістю до шумів і високою чутливістю до розлаштування параметрів керування генераторів хаосу. Підвищення якості системи знижує конфіденційність передавання, що є суттєвим недоліком схеми.

1.1.3.4. Адаптивні методи.

Схеми на основі адаптивних методів (або модулювання керуючих параметрів) – природний етап при переході від дискретної модуляції керуючого параметра передавального генератора в схемі з перемиканням хаотичних режимів до модуляції безперервним сигналом [26-27]. При цьому роль модулюючого сигналу грає інформаційний сигнал.

В адаптивних методах здійснюється модуляція параметра ведучої системи аналоговим інформаційним сигналом s(t) [26-27]. Слід зазначити, що необхідною умовою реалізації таких схем є необхідним попереднє встановлення допустимого діапазону зміни параметра і нормування інформаційного сигналу. Окремим випадком є використання бінарного цифрового сигналу в якості інформаційного та модулювання їм керуючого параметра передавального генератора.

Умовою модуляції є стійкість хаотичного режиму генератора приймача. На відміну від нелінійного підмішування, в адаптивних методах приймач містить систему керування, що забезпечує синхронність роботи ведучої та веденої систем шляхом зміни модульованого параметра ведучої системи (рис. 1.5).

Особливості роботи, переваги і недоліки схем, заснованих на адаптивних методах, є тими ж, що і в разі схем з перемиканнями. Однак для даної схеми

технічна реалізація дещо спрощується завдяки наявності на передавальній стороні каналу зв'язку тільки одного генератора.

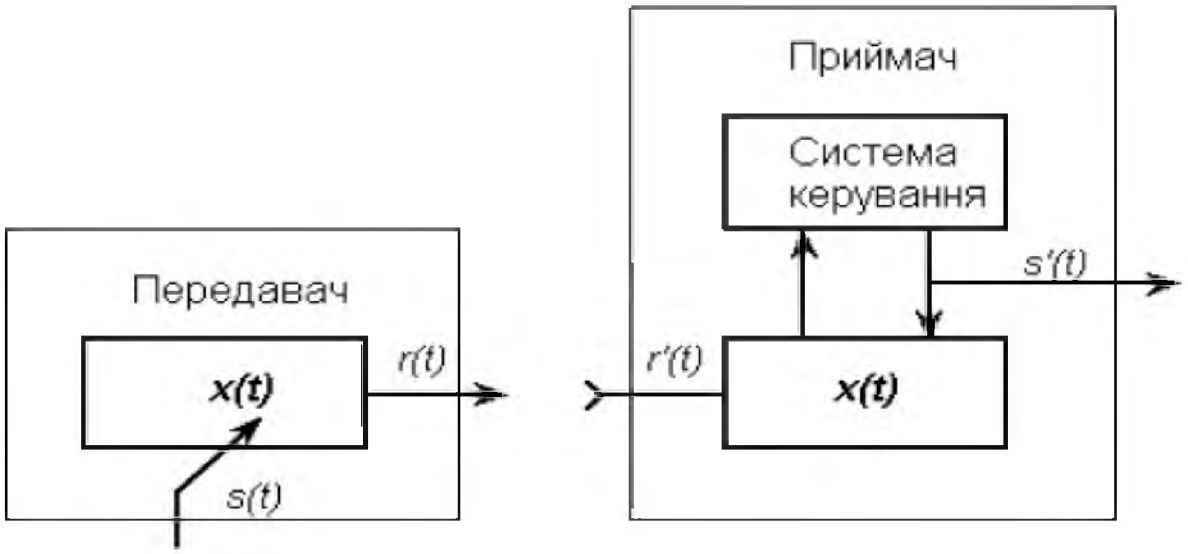

Рисунок 1.5 – Адаптивна система передавання інформації

Недоліком адаптивних методів передавання інформації з використанням хаотичних коливань у порівнянні з попередніми є мала швидкість передавання інформації.

1.1.4 Математичні моделі неперервних динамічних систем

Найбільш традиційними математичними моделями, що служать для обчислювальних експериментів з системами прихованої передачі інформації, є широко відомі моделі Ресслера Лоренца, Чуа та інші. Основними перевагами цих моделей є як математична простота, так і достатня вивченість хаотичної поведінки.

1.1.4.1. Визначення динамічної системи.

Під динамічною системою (ДС) розуміють будь-який об'єкт або процес, для якого однозначно визначено поняття стану як сукупності деяких величин або функцій в даний момент часу, і заданий закон, який описує зміну

(еволюцію) початкового стану з плином часу. Цей закон дозволяє за початковим станом прогнозувати майбутній стан ДС, і його називають законом еволюції.

Розглянемо ДС, що моделюються кінцевим числом звичайних диференціальних рівнянь. Опис стану задамо величинами x_1, x_2, . . . , x_N в деякий момент часу $t=t_0$. Тоді закон еволюції ДС має вигляд

$$\frac{dx_i}{dt} = \dot{x}_i = f_i\left(x_i, x_2, ..., x_N\right), \quad i = 1,2,...,N. \tag{1.5}$$

Якщо розглядати величини x_1, x_2, . . . ,x_N як координати точки x в N-вимірному просторі, то виходить наочне геометричне уявлення стану ДС у вигляді цієї точки. Останню називають зображуючою, а частіше – фазовою точкою, а простір станів – фазовим простором ДС. Зміні стану системи у часі відповідає рух фазової точки вздовж деякої лінії, яка називається фазовою траєкторією.

Необхідно уточнити взаємозв'язок понять числа ступенів свободи і розмірності фазового простору ДС. Під числом ступенів свободи розуміється найменше число незалежних координат, необхідних для однозначного визначення стану системи. Під координатами спочатку розумілись саме просторові змінні, що характеризують взаємне розташування тіл і об'єктів. У той же час для однозначного рішення відповідних рівнянь руху необхідно, окрім координат, задати відповідні початкові значення імпульсів або швидкостей. У зв'язку з цим система з n ступенями свободи характеризується фазовим простором розмірністю в два рази більшою ($N=2n$).

ДС формально визначена, якщо задані:

1) множина станів X, яке утворює повний метричний простір (фазовий простір);

2) множина моментів часу Θ;

3) оператор еволюції $T_{t_0}^{T}$ – деяке відображення $T_{t_0}^{T} : X \to X$, яке кожному стану $x_0 \in X$ в початковий момент часу $t_0 \in \Theta$ однозначно ставить у відповідність

деякий стан $x_t \in X$ в будь-який інший момент часу $t = t_0 + \tau \in \Theta$. Таким чином, можна записати:

$$\boldsymbol{x}_t = T_{t_0}^{T} \boldsymbol{x}_0,\ t = t_0 + \tau, \tag{1.6}$$

де τ – інтервал (зсув) часу.

Способи завдання оператора еволюції можуть бути різними: у вигляді інтегрального перетворення, у вигляді матриці або таблиці, у вигляді графіка або функції тощо.

Важливу групу ДС представляють системи, в яких можливі коливання. Коливальні системи з точки зору їх математичних моделей поділяють на певні класи. Розрізняють лінійні і нелінійні коливальні системи, зосереджені і розподілені, консервативні і дисипативні, автономні і неавтономні. Особливий клас представляють так звані автоколивальні системи.

Коливальна система називається лінійною або нелінійною залежно від того, лінійна або нелінійна система диференціальних рівнянь, яка її описує.

Коливальні системи, що моделюються кінцевим числом звичайних диференціальних рівнянь, називають зосередженими або точковими системами. Вони описуються за допомогою кінцеве вимірного фазового простору і характеризуються кінцевим числом ступенів свободи. Одна й та ж система в різних умовах може розглядатися як зосереджена або як розподілена. Математичні моделі розподілених систем – це диференціальні рівняння в часткових похідних, інтегральні рівняння або звичайні рівняння з аргументом, який запізнюється. Число ступенів свободи розподіленої системи нескінченно, і потрібно нескінченне число даних для визначення її стану.

За енергетичною ознакою ДС діляться на консервативні і неконсервативні. Консервативні системи характеризуються незмінним у часі запасом енергії. У механіці їх називають гамільтоновими.

ДС із змінним в часі запасом енергії називаються відповідно неконсервативними. Системи, в яких енергія зменшується в часі через тертя або розсіювання, є дисипативними. Відповідно до цього системи, енергія яких у

часі наростає, називаються системами з негативним тертям або негативною дисипацією. Такі системи можна розглядати як дисипативні при зміні напрямку відліку часу на протилежний. Принциповою особливістю дисипативних систем є залежність елемента фазового обсягу від часу. У системах з поглинанням енергії фазовий обсяг в часі зменшується, в системах з негативним тертям – збільшується.

Коливальні системи називаються автономними, якщо вони не схильні до дії зовнішніх сил, змінних у часі. Рівняння автономних систем явної залежності від часу не містять.

Більшість реальних коливальних систем у фізиці, радіофізиці, біології, хімії та інших галузях знань неконсервативні. Серед них виділяється особливий клас так званих автоколивальних систем, які принципово неконсервативні і нелінійні. Автоколивальною називають ДС, яка перетворює енергію джерела в енергію незатухаючих коливань, причому основні характеристики коливань (амплітуда, частота, форма коливань тощо) визначаються параметрами системи і в певних межах не залежать від вибору початкового стану.

1.1.4.2. Система Лоренца.

Система Лоренца є першою динамічною системою, при чисельному дослідженні якої було отримано нетривіальні розв'язки для її змінних і виявлено нетипову поведінку та високу чутливість до початкових умов. Система Лоренца є фізичною моделлю конвекції потоків газів та рідин під час їхнього нагрівання [5].

Аналітично система описується наступними диференційними рівняннями:

$$\begin{cases} \dot{x} = \sigma \cdot (y - x) \\ \dot{y} = r \cdot x - y - x \cdot z \\ \dot{z} = x \cdot y - b \cdot z \end{cases} \tag{1.7}$$

де σ, r, b – параметри системи.

Найчастіше систему (1.7) досліджують при значенні параметрів σ=10 , r=28 , b=8/3. Хаотичний атрактор, отриманий [11] при вказаних значеннях параметрів, наведений на рис. 1.6.

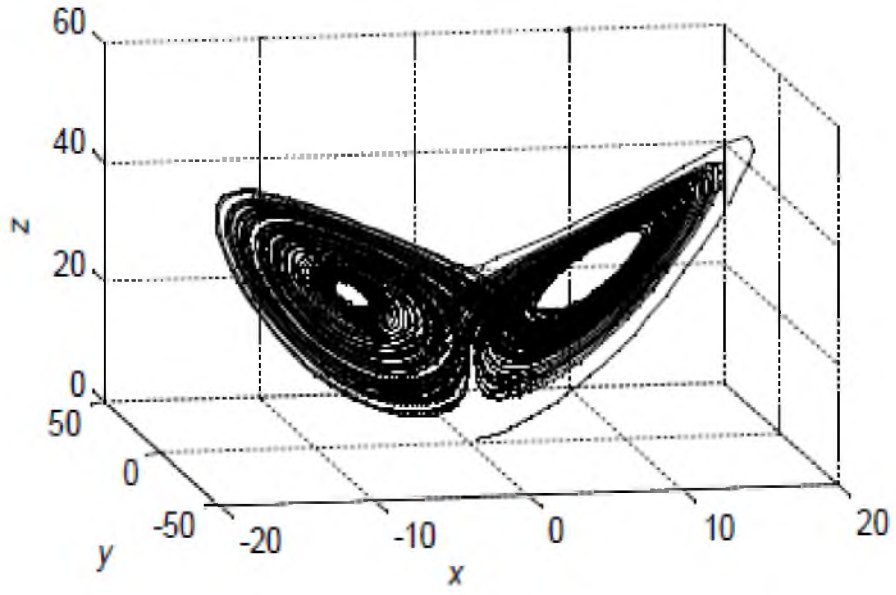

Рисунок 1.6 – Хаотичний атрактор системи Лоренца

Система Лоренца – це хронологічно перший приклад системи звичайних диференційних рівнянь, розв'язки якої є чутливими до початкових значень змінних. Система (1.7) містить дві квадратичні нелінійності в другому та третьому рівнянні і має три точки рівноваги:

$$x_0^1 = (0,0,0)$$
$$x_0^2 = \left(\sqrt{b\cdot(r-1)}, \sqrt{b\cdot(r-1)}, r-1\right) \quad . \tag{1.8}$$
$$x_0^3 = \left(-\sqrt{b\cdot(r-1)}, -\sqrt{b\cdot(r-1)}, r-1\right)$$

1.1.4.3. Система Реслера.

Система Реслера є моделлю динаміки хімічних реакцій, що відбуваються в деякій суміші з перемішуванням [1, 10] і аналітично описується наступними диференційними рівняннями:

$$\begin{cases} \dot{x} = -y - z \\ \dot{y} = x + a \cdot y \\ \dot{z} = b + z \cdot (x - c) \end{cases} \quad (1.9)$$

де a,b,c – параметри системи.

Система Реслера має одну квадратичну нелінійність в третьому рівнянні та дві точки рівноваги:

$$d_{1,2} = \frac{c}{2 \cdot a} \pm \sqrt{\frac{c^2}{4 \cdot a^2} - \frac{b}{a}} \quad (1.10)$$

що в залежності від значення параметрів a,b,c є стійкими або нестійкими.

Система (1.9) є прикладом багатомірних систем, динаміку яких можна апроксимувати одномірним відображенням. Якщо провести переріз Пуанкаре при y=0 і побудувати одномірне відображення точок x_n, тобто залежність $x_{n+1}=f(x_n)$, то отримана крива буде подібною до параболи (рис. 1.7).

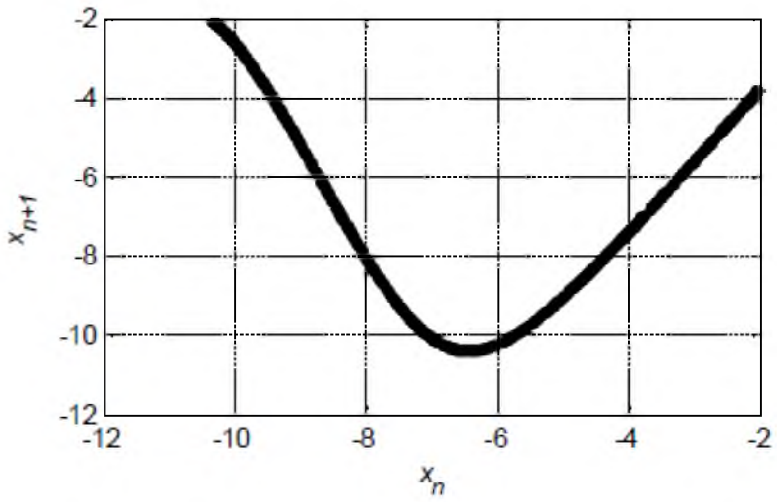

Рисунок 1.7 – Залежність між послідовністю точок перетину площини y=0 $x_{n+1}=f(x_n)$ для системи Реслера

В хаотичному режимі траєкторії системи Реслера при значенні її параметрів a=0,2; b=0,2; c=6,5 залежно від початкових умов повертаються навколо однієї з точок рівноваги (рис. 1.8). Часова залежність змінних x, y нагадує зашумлені коливання. Система Реслера при вибраних значеннях параметрів відноситься до фазокогерентних.

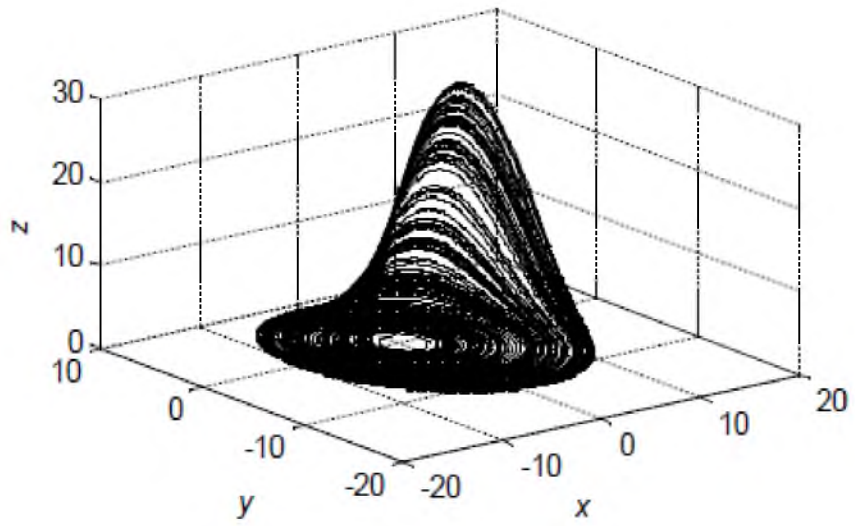

Рисунок 1.8 – Хаотичний атрактор системи Реслера

Часто в літературі при дослідженні явищ синхронізації використовують математичну модель системи Реслера з параметром w , що задає основну частоту коливань в системі [5]:

$$\begin{cases} \dot{x} = -(wy + z) \\ \dot{y} = wx + ay \\ \dot{z} = b + z(x - c) \end{cases} \quad (1.11)$$

де a,b,c , w – параметри системи.

Параметр системи (1.11) w чисельно дорівнює значенню основної частоти коливань сигналів, що генеруються нею.

Системи Лоренца і Реслера є класичним прикладом систем з хаотичною поведінкою, що демонструють велику кількість динамічних режимів та послідовність їх зміни при зміні параметрів систем.

1.2 Існуючі підходи до прихованої передачі інформації на основі хаотичної синхронізації

У розділі 1.1.3 було розглянуто основні типи схем прихованої передачі на основі повної хаотичної синхронізації. Існують й інші схеми, але вони є

різновидами вже відомих схем і не становлять принципового інтересу, відбиваючи швидше ті чи інші особливості технічної реалізації. Схеми, розглянуті в розділі 1.1.3, є найпростішими системами, які є основою для використання хаотичної синхронізації для прихованої передачі даних. Як вже зазначалось, жодна з них не позбавлена недоліків. Подальші дослідження йдуть у напрямку створення нових схем, у яких робляться спроби усунути зазначені недоліки, підвищуючи в деяких випадках конфіденційність схем, у деяких – стійкість до шумів, в деяких – позбавляючись необхідності ідентичності генераторів і забезпечуючи тим самим можливість більш простої технічної реалізації схем. Природним шляхом у разі є перехід від повної хаотичної синхронізації до інших типів синхронної поведінки. Слід зазначити, що опис таких спроб, хоч і не часто, зустрічається в літературі.

Так, у роботі [28] запропоновано схему захищеного зв'язку, яка заснована на фазовій синхронізації хаотичних систем.

Принципова схема реалізації такого підходу наведена на рис. 1.9. На передавальній стороні каналу зв'язку знаходяться два ідентичних взаємопов'язаних хаотичних генератора з 1,5 ступенями свободи, що характеризуються векторами станів $\mathbf{x}_{1,2}(t)=(x_{1,2}, y_{1,2}, z_{1,2})$. Зв'язок між генераторами є дисипативним, що дозволяє забезпечити фазову синхронізацію при досить малому параметрі зв'язку ε. Один з керуючих параметрів цих генераторів (один і той же в обох системах) модулюється корисним цифровим сигналом m(t). Як сигнал, що передається, використовується миттєва фаза $\phi_m(t)$ сигналу $x_m(t)=(x_m,y_m,z_m)$, яка представляє собою середнє значення сигналів $\mathbf{x}_{1,2}(t)$, що генеруються цими системами (фаза вводиться в розгляд на площині (x_m,y_m), де $x_m=(x_1+x_2)/2$, $y_m=(y_1+y_2)/2$). Отриманий таким чином сигнал $\phi_m(t)$, що містить корисну інформацію, передається по каналу зв'язку (в якому він піддається впливу шумів) на пристрій, що містить хаотичний генератор $x_3(t)=(x_3,y_3,z_3)$, ідентичний генераторам передавального пристрою, що забезпечує виникнення режиму фазової синхронізації між ними. Як сигнал, що безпосередньо впливає на приймаючий генератор хаосу, використовується

сигнал $s(t)=\eta(r_3 \cos \phi_m - x_3)$, де $r_3=(x_3+y_3)^{1/2}$, η – амплітуда сигналу. Відновлений сигнал $\tilde{m}(t)$ отримують в результаті аналізу поведінки різниці фаз $\Delta\phi=\phi_m-\phi_3$ відповідних сигналів.

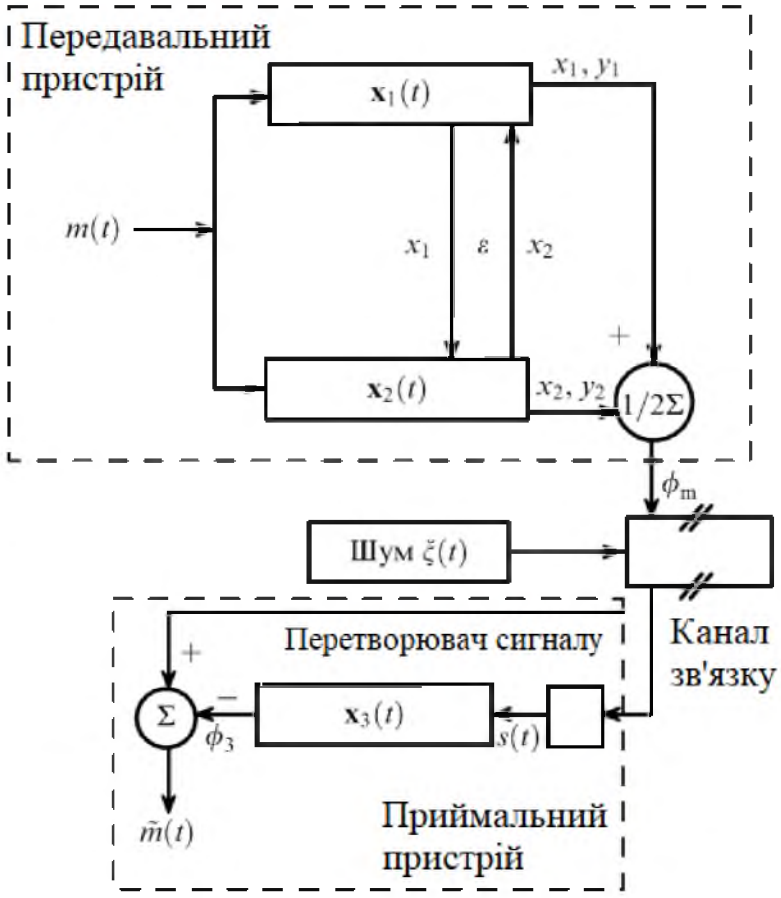

Рисунок 1.9 – Схема прихованої передачі на основі фазової хаотичної синхронізації з роботи [28]

Як видно з наведеного опису схеми прихованої передачі інформації на основі фазової синхронізації, принцип її роботи суттєво відрізняється від принципу роботи схем, розглянутих у розділі 1.1.3. Проте більшість недоліків, властивих схемам з урахуванням повної хаотичної синхронізації, тут залишається. Крім того, цей підхід [28] має суттєві додаткові складнощі з точки зору технічної реалізації (наприклад, експериментальне визначення фази хаотичних сигналів, створення сигналу s(t), наявність додаткових ідентичних генераторів на різних сторонах каналу зв'язку).

Є також спроби використовувати для прихованої передачі даних, поряд з фазовою синхронізацією, узагальнену синхронізацію [29]. Використання цього типу синхронної поведінки відкриває ряд нових можливостей, нехарактерних, наприклад, для повної та фазової синхронізації. По-перше, узагальнена синхронізація, на відміну від повної хаотичної синхронізації, може спостерігатися в різних взаємодіючих динамічних системах [30], що говорить про можливість спрощення технічної реалізації підходів до прихованої передачі даних, заснованих на цьому типі синхронного поведінки. По-друге, вид функціональної залежності, що встановлюється між станами взаємодіючих систем при реалізації узагальненої синхронізації, може бути дуже складним, у тому числі фрактальним, що значно зменшує можливість отримання третьою стороною інформації про характеристики генератора на приймаючій стороні каналу зв'язку по часовій реалізації переданого сигналу, тобто. підвищує конфіденційність. По-третє, поведінка кордону узагальненої синхронізації, що розташовується на площині параметрів «частота розлаштування – інтенсивність зв'язку», є аномальною, що істотно відрізняється від поведінки кордонів усіх відомих типів синхронної поведінки. Зокрема, для низки систем поріг виникнення режиму узагальненої синхронізації в області відносно слабких значень розлаштування частот перевищує аналогічне значення за параметром зв'язку в області великих значень частотного розладу приблизно в два рази [31]. Ця особливість дозволяє забезпечити виникнення або руйнування синхронного режиму при дуже слабкій модуляції керуючого параметра, що гарантує ефективну модуляцію керуючого параметра для передачі інформації по каналах зв'язку. Нарешті шум мало впливає поріг виникнення режиму узагальненої синхронізації, тобто синхронний режим виникає в односпрямовано пов'язаних динамічних системах за відсутності та за наявності шуму при близьких значеннях сили зв'язку між системами. Тому можна очікувати високої стійкості схем на основі режиму узагальненої синхронізації до шумів у каналах зв'язку. Більш того, додатковий шум може бути використаний для створення додаткового маскування сигналу, що передається по каналу зв'язку.

Тим не менш необхідно відзначити, що більшість відомих способів прихованої передачі інформації на основі режиму узагальненої синхронізації не використовують повною мірою всіх переваг цього режиму.

Однією з небагатьох робіт, у яких використовується режим узагальненої синхронізації для прихованої передачі інформації є робота [32]. Принципова схема реалізації такого підходу до прихованої передачі даних наведена на рис. 1.10.

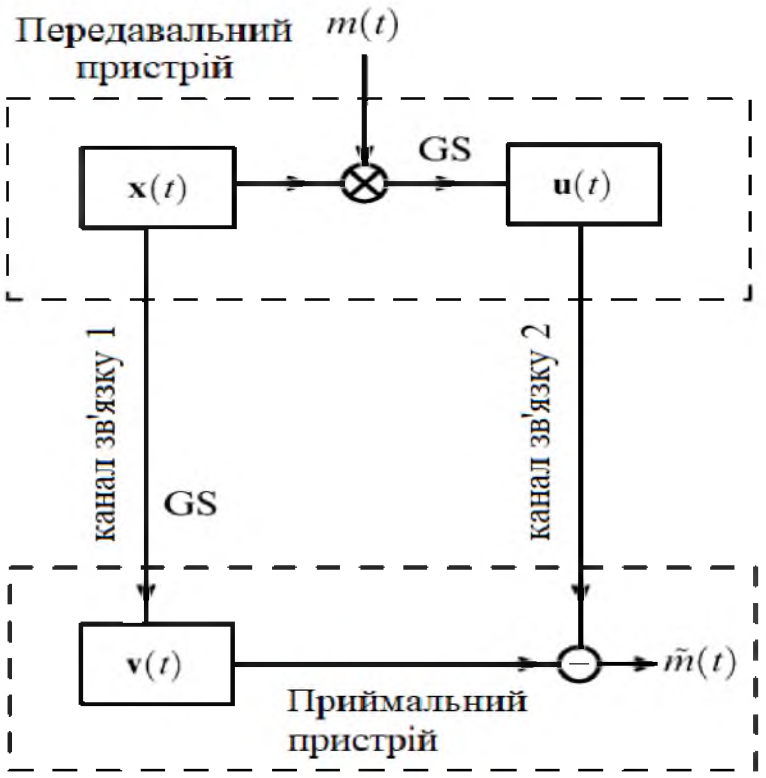

Рисунок 1.10 – Схема прихованої передачі на основі узагальненої синхронізації з роботи [32]

Передавальна сторона містить два хаотичні генератори, відомий **x**(t) і ведений **u**(t), які можуть бути неідентичними (рис. 1.10). Сигнал з відомого генератора передається на ведений, причому його інтенсивність модулюється корисним цифровим сигналом m(t) таким чином: якщо передається бінарний біт 0, то між відомим та веденим генераторами встановлюється режим

узагальненої синхронізації, а якщо передається бінарний біт 1, то режим узагальненої синхронізації між ними руйнується.

На приймальній стороні каналу зв'язку знаходиться так званий допоміжний хаотичний генератор **v**(t), ідентичний веденому за керуючими параметрами. Сигнал з відомого генератора по каналу зв'язку передається на допоміжний, що забезпечує виникнення режиму узагальненої синхронізації між ними, причому інтенсивність сигналу, що передається по каналу зв'язку повинна збігатися з інтенсивністю сигналу, що надходить до веденої системи при передачі бінарного біта 0. Сигнал з веденого генератора по іншому каналу зв'язку передається приймаючій стороні.

Так само як і в способах прихованої передачі даних, заснованих на режимі повної хаотичної синхронізації, приймаюча сторона має у своєму розпорядженні як хаотичний сигнал, що містить корисну інформацію, так і сигнал без неї. Тому можна легко виділити корисний цифровий сигнал $\tilde{m}(t)$ простим відніманням одного сигналу з іншого.

Неважко бачити, що у такій схемі прихованої передачі інформації активно використовується метод допоміжної системи, що потребує наявності двох ідентичних за керуючими параметрами хаотичних генераторів. Так само як і в схемах, заснованих на режимі повної хаотичної синхронізації, ці генератори розташовуються на різних сторонах каналу зв'язку, що є суттєвою проблемою з погляду технічної реалізації даного підходу. Невеликий розлад значень керуючих параметрів у цих системах призводить до появи шумів десинхронізації, роблячи таку схему непрацездатною. Крім того, реалізація двох каналів зв'язку є істотним недоліком не тільки через додаткові витрати при реалізації, але і внаслідок того, що наявність двох каналів сприяє появі додаткових шумів у каналі зв'язку (можливо, навіть зовсім іншої природи), що спотворюють сигнал, що передається. Тому така схема прихованої передачі характеризується досить низькою стійкістю до шумів у каналі зв'язку і є такою, що складно реалізується на практиці.

Виникають також проблеми з конфіденційністю передачі інформації. Зрозуміло, що використання іншого типу синхронної поведінки, а також наявність додаткового каналу зв'язку, з цього погляду, грають позитивну роль. Однак, так само як і в стандартних схемах на основі нелінійного підмішування інформаційного сигналу до хаотичного, підвищення якості інформації, що передається, тягне за собою втрату конфіденційності. Але ця проблема тут є менш істотною порівняно з аналогічною проблемою для схем, що ґрунтуються на режимі повної хаотичної синхронізації.

Підвищити конфіденційність передачі інформації можна за допомогою використання кількох типів синхронної поведінки одночасно. Наприклад, в роботах [32, 33] запропоновані підходи до прихованої передачі даних, що використовують одночасно режими узагальненої та повної хаотичної синхронізації.

Схема, запропонована в роботі [32] (рис. 1.11), є модифікацією схеми, представленої на рис. 1.10. Принцип роботи передавального пристрою аналогічний принцип роботи передавального пристрою схеми, представленої на рис. 1.10. Модифікація полягає в тому, що на стороні каналів зв'язку знаходиться додатковий хаотичний генератор $x_2(t)$, ідентичний відомому $x_1(t)$ за керуючими параметрами (далі – другий відомий генератор). Сигнал, що генерується відомою системою, передається по першому каналу зв'язку, переводячи другий відомий генератор в повний режим синхронізації. Конфіденційність можна підвищити за рахунок того, що сигнали, що надходять на ведений і другий відомий генератори, можуть бути різними (наприклад, веденій системі передається сигнал, що представляє собою x-координату відомої системи, а другій ведучій – сигнал, що є y-координатою). На приймаючій стороні каналу зв'язку сигнал від другого відомого генератора, впливаючи на допоміжний, забезпечує виникнення режиму узагальненої синхронізації між ними. Сигнал з веденого генератора надходить по другому каналу зв'язку на приймаючу сторону. Внаслідок ідентичності сигналів, що впливають на ведений і допоміжний генератори, як і в попередньому випадку,

приймаюча сторона має у своєму розпорядженні як сигнал, що містить корисну інформацію, так і сигнал без неї. Після проходження через віднімаючий пристрій корисний сигнал може бути легко детектований.

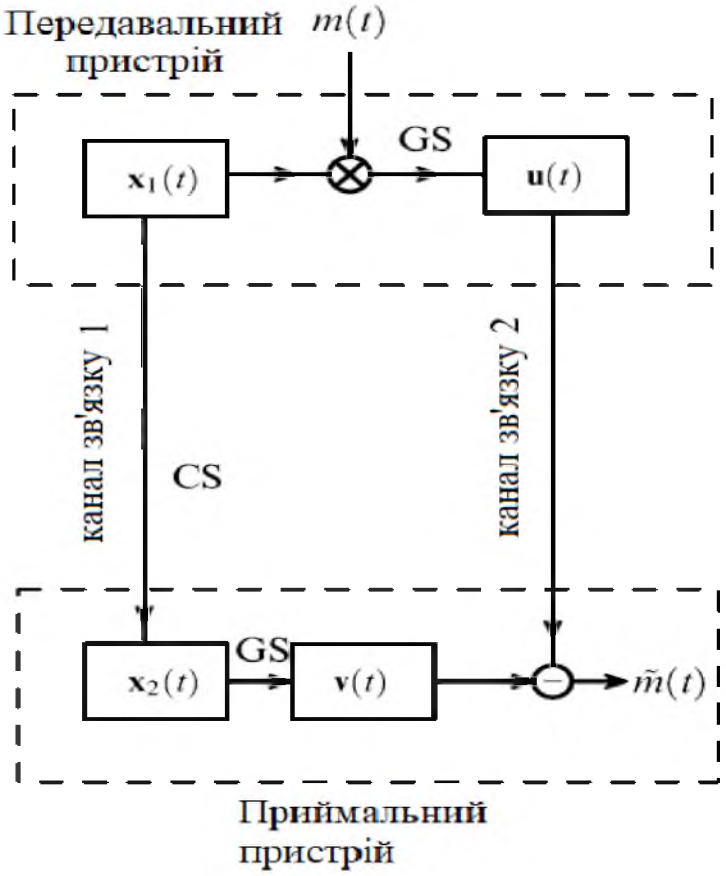

Рисунок 1.11 – Схема прихованої передачі за допомогою узагальненої і повної хаотичної синхронізації з роботи [32]

Зрозуміло, що така модифікована схема з роботи [32] є ефективнішою з погляду конфіденційності, тобто знижується ймовірність детектування інформаційного повідомлення третьою стороною. Проте низка інших проблем залишається невирішеною. Наявність ідентичних генераторів у передавальному та приймальному пристроях (тепер це вже дві пари ідентичних генераторів), реалізація двох каналів зв'язку, низька стійкість до шумів у каналі зв'язку, яка стає ще нижчою внаслідок руйнування повної хаотичної синхронізації, – всі ці недоліки роблять подібні схеми прихованої передачі даних малозастосовними практично.

У роботі [33] було запропоновано інший спосіб прихованої передачі інформації, в якому також використовуються два типи синхронної поведінки - узагальнена та повна хаотична синхронізація, але схема [33] є модифікацією однієї із схем для прихованої передачі даних, заснованих на нелінійному підмішуванні інформаційного сигналу до хаотичного.

Принципова схема реалізації такого підходу до прихованої передачі даних наведено на рис. 1.12.

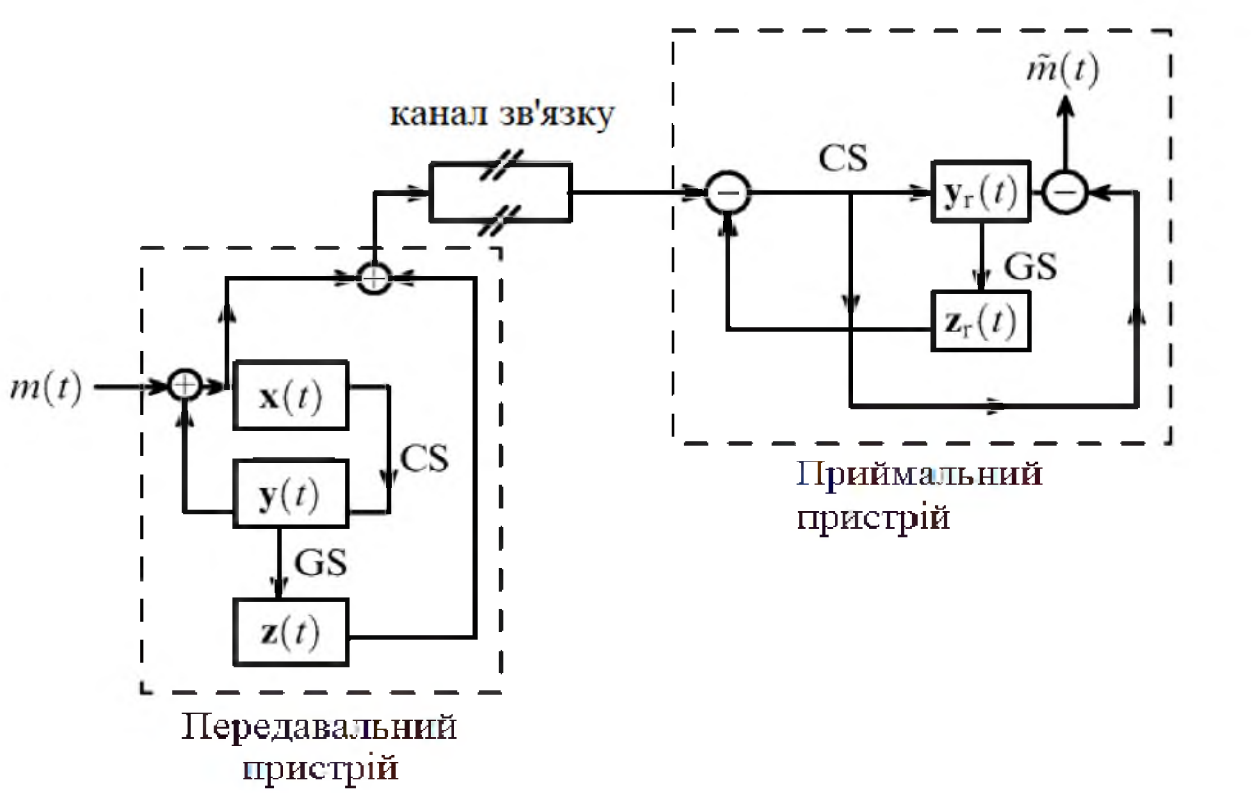

Рисунок 1.12 – Схема прихованої передачі з використанням комбінованого хаотичного сигналу з роботи [33]

Передавальний пристрій, так само як і в схемі на основі нелінійного підмішування інформаційного сигналу до хаотичного, містить два взаємопов'язані ідентичні хаотичні генератори **x**(t) і **y**(t) (далі – перший і другий) (рис. 1.12). Інформаційний сигнал *m*(t) підмішується до сигналів, що виробляються цими генераторами, і тим самим зазнає нелінійних змін. Крім того, на передавальній стороні каналу зв'язку знаходиться ще один генератор **z**(t) (названий третім), неідентичний першому та другому за керуючими

параметрами і односпрямовано пов'язаний з другим. Значення керуючих параметрів генераторів передавального пристрою повинні бути обрані таким чином, щоб другий і третій генератори знаходилися в режимі узагальненої хаотичної синхронізації, у той час як перший і другий були повністю синхронізованими, тобто знаходились режим повної синхронізації. Третій генератор використовується для підвищення конфіденційності: він формує сигнал, який у найпростішому випадку просто додається до сигналу, що містить корисну інформацію, що формує вже комбінований сигнал, створюючи тим самим додаткове маскування.

Такий спосіб передачі інформації авторами [161] був названий «прихована передача інформації з використанням комбінованого сигналу хаотичних систем в режимі узагальненої синхронізації». Комбінований сигнал по каналу зв'язку передається на пристрій, що містить два генератори: четвертий – $y_r(t)$, ідентичний першому і другому за керуючими параметрами, і п'ятий – $z_r(t)$, ідентичний у тому ж самому сенсі третьому. Четвертий і п'ятий генератори повинні бути у режимі узагальненої синхронізації. Тоді згідно методу допоміжної системи, внаслідок ідентичності четвертої і другої систем, третій і п'ятий генератори будуть здійснювати ідентичні коливання. Сигнали з каналу зв'язку і п'ятого генератора надходять на віднімаючий пристрій. На четвертий генератор і другий віднімаючий пристрій, будуть вже надходити сигнали, вільні від додаткових складових. У разі дії на четвертий генератор цей сигнал синхронізує його при передачі бінарного біта 0 і не синхронізує при передачі бінарного біта 1. На виході буде отримано відновлений сигнал $\tilde{m}(t)$, що є послідовністю ділянок із синхронною (бінарний біт 0) і несинхронною (бінарний біт 1) поведінкою.

З наведеного вище розгляду випливає, що така схема є досить конфіденційною: по комбінованому сигналу, що передається по каналу зв'язку, в більшості випадків навіть без шумів, діагностувати інформаційне повідомлення третьою стороною неможливо. Однак, як і у схемах на основі нелінійного підмішування, якість передачі інформації (а отже, і можливість

відновлення якісної інформації) сильно залежить від конфіденційності, а саме: чим вища конфіденційність, тим нижча якість. У той же час зрозуміло, що за рахунок створення комбінованого сигналу ця залежність буде не настільки різкою, що є певною перевагою цієї схеми перед іншими. Однак одна перевага не закриває ряду недоліків. Створення п'яти генераторів, три та два з яких повинні бути ідентичні між собою, є практично нерозв'язним технічним завданням, особливо якщо генератори розташовуються на різних сторони каналу зв'язку. Введення досить малого розладу керуючих параметрів цих генераторів відразу робить схему непрацездатною. Крім того, шуми в каналі зв'язку, безсумнівно, призведуть до спотворення сигналу, що передається, а отже, до руйнування режимів повної синхронізації між другим і четвертим генераторами і узагальненої синхронізації між четвертим і п'ятим. Сигнали на різних сторонах каналу зв'язку стануть неідентичними, і детектування інформаційного повідомлення на приймальній стороні каналу зв'язку виявиться неможливим.

Таким чином, часткова ліквідація одних недоліків у більшій кількості випадків призводить до посилення інших. З огляду на низьку стійкість до шумів і розлад керуючих параметрів технічна реалізація таких схем, що мають досить високу конфіденційність, є дуже складною. Тому «екстенсивний» шлях удосконалення способів прихованої передачі даних – використання кількох типів синхронної поведінки для передачі інформації – мабуть, є неоптимальним.

1.3 Висновок. Постановка задачі

В розділі проаналізовано шляхи передачі інформації в системах зв’язку з використанням хаотичних коливань. Встановлено, що хаотичні комунікаційні системи мають широкосмуговий спектр потужності, дозволяють забезпечити високу швидкість передачі інформації і залишаються працездатні при малих

відношеннях сигнал-шум та є ефективними для передавання конфіденційної інформації.

В розділі проведено розгляд типових схем прихованої передачі інформації: хаотичне маскування; перемикання хаотичних режимів нелінійне підмішування, адаптивні методи. Встановлено їх переваги і недоліки.

В розділі проведено розгляд підходів до прихованої передачі з використанням хаотичних сигналів, основу яких лежать різні типи синхронної поведінки хаотичних систем: повна хаотична синхронізація, фазова синхронізація, узагальнена хаотична синхронізація, а також декілька типів синхронної поведінки одночасно (наприклад, узагальнена та повна синхронізації). Кожна зі схем характеризується своїми особливостями та принципами роботи і має властиві тільки їй переваги та недоліки.

В результаті аналізу існуючих схем та підходів до передачі інформації, розглянутих у розділах 1.1.3 та 1.2, встановлено, що, незважаючи на використання різних типів синхронної поведінки для прихованої передачі, специфічні особливості цих методів, їх характерні відмінності, переваги і недоліки у тій чи іншій мірі притаманні всім відомим зараз схемам. Це насамперед:

• вимога високого ступеня ідентичності до хаотичних генераторів, що розташовуються на різних сторонах каналу зв'язку;

• низька стійкість до шумів у каналі зв'язку;

• низька конфіденційність, тобто можливість у ряді випадків реконструкції параметрів передавального генератора по сигналу, що передається по каналу зв'язку (особливо для схем на основі повної хаотичної синхронізації), з подальшим відновленням інформаційного сигналу.

Таким чином, для усунення недоліків існуючих підходів необхідно:

• обґрунтувати структурну стійкість режиму узагальненої синхронізації до шумів;

• дослідити підхід до прихованої передачі з підвищеною стійкістю до шумів на основі узагальненої хаотичної синхронізації;

• оцінити ефективність відомих схем і підходів до прихованої передачі інформації на основі хаотичної синхронізації у середовищі Matlab за допомогою стандартних і розроблених програм.

2 СПЕЦІАЛЬНА ЧАСТИНА

2.1 Підхід до прихованої передачі з підвищеною стійкістю до шумів на основі узагальненої хаотичної синхронізації

Як вже зазначалось у висновках до першого розділу, аналіз схем та підходів до прихованої передачі інформації, розглянутих у розділах 1.1.3 та 1.2, показує, що, незважаючи на використання різних типів синхронної поведінки їх характерні відмінності, переваги і недоліки у тій чи іншій мірі притаманні всім відомим зараз схемам. Це насамперед: вимога високого ступеня ідентичності до хаотичних генераторів, що розташовуються на різних сторонах каналу зв'язку; низька стійкість до шумів у каналі зв'язку; низька конфіденційність.

У цьому розділі буде розглянуто підхід прихованої до передачі інформації, який багато в чому позбавлений вищезгаданих недоліків. Більш того, він має значну стійкість до шумів і, як наслідок, характеризується досить високим ступенем конфіденційності. Підхід заснований на узагальненій синхронізації, проте на відміну від способу, розглянутого в [32] (див. рис. 1.11), він враховує всі особливості режиму узагальненої синхронізації, й тому має принципові переваги у порівнянні з відомими аналогами.

Перш, ніж перейти до опису самого підходу, розглянемо причини структурної стійкості режиму узагальненої синхронізації до шумів.

2.1.1 Стійкість режиму узагальненої синхронізації до шумів

Відомо, що режим узагальненої синхронізації може спостерігатися у системах з дисипативним та недисипативним типами зв'язку [30]. Для систем з дисипативним зв'язком рівняння, що описують динаміку взаємодіючих систем у присутності шуму, можуть бути представлені у вигляді

$$\dot{\mathbf{x}}(t) = \mathbf{G}\left(\mathbf{x}(t), \mathbf{g}_{\mathrm{d}}\right), \tag{2.1}$$

$$\dot{\mathbf{u}}(t) = \mathbf{H}\left(\mathbf{u}(t), \mathbf{g}_r\right) + \varepsilon A\left(\mathbf{x}(t) - \mathbf{u}(t) + D\xi(t)\right), \tag{2.2}$$

де **x**(t) і **u**(t) – вектори стану відомої та веденої систем відповідно; ξ(t) – шумовий сигнал; **G** і **H** – векторні поля взаємодіючих систем; g_d і g_r – вектори керуючих параметрів; $A=\{\delta_{ij}\}$ – матриця зв'язку; $\delta_{ii}=0$ або $\delta_{ii}=1$, $\delta_{ij}=0$ $(i\neq j)$, ε – параметр зв'язку; D – інтенсивність шуму.

Механізми виникнення режиму узагальненої синхронізації може бути виявлено з допомогою методу модифікованої системи [164, 165]. Згідно з цим методом, ведена система **u**(t) може бути розглянута як деяка модифікована система:

$$\dot{\mathbf{u}}_m(t) = \mathbf{H}'\left(\mathbf{u}_m(t), \mathbf{g}_r, \varepsilon\right), \tag{2.3}$$

що знаходиться під зовнішнім впливом $\varepsilon\left(A\mathbf{x}(t)+D\xi(t)\right)$,

$$\dot{\mathbf{u}}_m(t) = \mathbf{H}'\left(\mathbf{u}_m(t), \mathbf{g}_r, \varepsilon\right) + \varepsilon\left(A\mathbf{x}(t) + D\xi(t)\right), \tag{2.4}$$

де $\mathbf{H}'\left(\mathbf{u}(t)\right) = \mathbf{H}\left(\mathbf{u}(t)\right) - \varepsilon A\mathbf{u}(t)$ Складане $-\varepsilon A\mathbf{u}(t)$ вносить додаткову дисипацію в модифіковану систему (2.3).

Режим узагальненої синхронізації, що виникає в системі (2.2), може бути розглянутий як наслідок двох взаємопов'язаних процесів, що протікають одночасно: збільшення дисипації в модифікованій системі (2.3) та зростання амплітуди зовнішнього (хаотичного та шумового) сигналу. Обидва процеси пов'язані між собою за допомогою параметра ε і не можуть бути реалізовані у веденій системі (2.2) окремо. Однак збільшення дисипації в модифікованій системі (2.3) призводить до спрощення її поведінки та переходу від хаотичних коливань до періодичних (або до стаціонарного стану). Зовнішній вплив, навпаки, прагне ускладнити поведінку модифікованої системи та нав'язати їй свою динаміку. Очевидно, що виникнення режиму узагальненої синхронізації можливе лише тоді, коли власна хаотична динаміка у веденій системі виявляється пригніченою внаслідок дисипації.

Таким чином, стійкість режиму узагальненої синхронізації визначається насамперед властивостями самої модифікованої системи. Тому поріг виникнення режиму узагальненої синхронізації не повинен сильно залежати від

інтенсивності шуму Dξ(t), що впливає на односпрямовано пов'язані хаотичні системи. Якщо шум не змінює характеристики модифікованої системи (2.3), він не повинен впливати на поріг виникнення режиму узагальненої синхронізації.

Дійсно, як вже зазначалось у розділі 1.1, діагностування режиму узагальненої синхронізації можливе як за допомогою методу допоміжної системи, так і шляхом розрахунку умовних ляпуновських експонент. Зрозуміло, що ведена і допоміжна системи можуть бути розглянуті як дві ідентичні системи з близькими початковими умовами. Обчислення похідної від різниці їх станів $\mathbf{\Delta}(t)=\mathbf{v}(t)-\mathbf{u}(t)$ за наявності (D>0) та відсутності шуму (D=0), внаслідок ідентичності детермінованих і стохастичних сигналів, що впливають на ці системи, призводить до одного і того ж рівняння:

$$\dot{\mathbf{\Delta}}(t) = \left(\mathbf{JH}(\mathbf{u}(t)) - \varepsilon A\right)\mathbf{\Delta}(t) = \mathbf{JH}'(\mathbf{u}(t))\,\mathbf{\Delta}(t)\,, \qquad (2.5)$$

де J – матриця Якобі. Так як рівняння (2.5) може бути розглянуто як рівняння в варіаціях при обчисленні умовних ляпуновських експонент, можна зробити висновок, що старші умовні ляпуновські показники (визначають поріг виникнення режиму узагальненої синхронізації) будуть поводитися подібним чином як за відсутності, так і за наявності шуму. Тому поріг виникнення режиму узагальненої синхронізації не повинен залежати від інтенсивності шуму, а сам тип синхронної поведінки повинен мати значну стійкість до шумів.

Справедливість теоретичних міркувань підтверджується результатами моделювання [34]. Як показують результати досліджень, режим узагальненої синхронізації має структурну стійкість до шумів як у системах з малим числом ступенів свободи, так і в просторово розподілених середовищах.

2.1.2 Опис підходу до прихованої передачі з підвищеною стійкістю до шумів на основі узагальненої хаотичної синхронізації

Принципова схема реалізації підходу до прихованої передачі інформації з підвищеною стійкістю до шумів наведена на рис. 2.1.

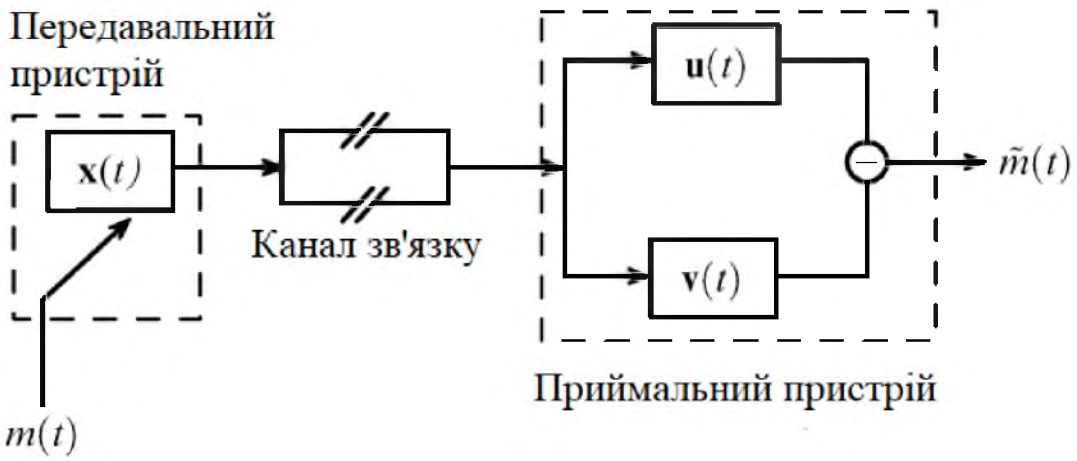

Рисунок 2.1 – Схема реалізації підходу до прихованої передачі з підвищеною стійкістю до шумів на основі узагальненої хаотичної синхронізації

Підхід до прихованої передачі інформації з підвищеною стійкістю до шумів полягає в наступному. Інформаційний сигнал m(t) кодується у вигляді бінарного коду. Один або декілька керуючих параметрів передавального генератора **x**(t) модулюються бінарним сигналом таким чином, щоб характеристики сигналу, що передається, змінювалися незначно. Отриманий таким чином сигнал передається по каналу зв'язку. Тут він піддається спотворенню під впливом шумів. Приймач, який знаходиться на іншій стороні каналу зв'язку, являє собою два ідентичні генератори **u**(t) і **v**(t), здатних перебувати в режимі узагальненої синхронізації з передавальним генератором. Принцип роботи приймача заснований на діагностиці режиму узагальненої синхронізації за допомогою методу допоміжної системи (див. розділ 1.1.1). Сигнал з каналу зв'язку надходить на генератори приймача. Отримані на виході сигнали проходять через віднімаючий пристрій, і потім детектується відновлений корисний сигнал $\tilde{m}(t)$.

Модуляція керуючих параметрів передавального генератора повинна бути здійснена таким чином, щоб в залежності від передавального бінарного біта 0(1) між передавальним і приймальним генераторами існував (був відсутній) режим узагальненої синхронізації. Наприклад, якщо режим узагальненої синхронізації спостерігається в тому випадку, якщо передається

бінарний біт 0, тоді обидва приймаючі генератори демонструватимуть ідентичні коливання, а після проходження через віднімаючий пристрій буде спостерігатися відсутність хаотичних коливань, тобто бінарний біт 0. Навпаки, при передачі бінарного біта 1 узагальнена синхронізація не спостерігається, а коливання приймаючих генераторів є неідентичними. Тоді після проходження через віднімаючий пристрій спостерігатиметься ненульова амплітуда хаотичних коливань, тобто бінарний біт 1.

Важливою перевагою аналізованого підходу до прихованої передачі даних є відсутність вимоги ідентичності генераторів на різних сторонах каналу зв'язку Два ідентичні генератори розташовуються на приймальній стороні. Слід зазначити, що наявність ідентичних генераторів на одній стороні каналу зв'язку дозволяє легко здійснити їх юстування, що знижує вимогу до ступеня ідентичності генераторів, а отже, спрощує технічну реалізацію схеми.

Крім того, сигнали, що надходять на генератори приймального пристрою завжди будуть однаковими, навіть за наявності шуму в каналі зв'язку. Отже, як вже зазначалось у розділі 2.1.1, при дисипативному зв'язку між генераторами передавального та приймального пристроїв шум не повинен сильно впливати на поріг виникнення режиму узагальненої синхронізації. Ця особливість дозволяє говорити про можливість створення стійких до шумів підходів до прихованої передачі на основі режиму узагальненої синхронізації.

2.2 Оцінка ефективності відомих схем і підходів до прихованої передачі інформації на основі хаотичної синхронізації

Було проведено порівняльний аналіз працездатності підходів до прихованої передачі за допомогою хаотичної синхронізації. Для перевірки ефективності цих підходів за наявності шуму було використане імітаційне моделювання в середовищі Matlab та оцінено деякі кількісні характеристики працездатності схем. Як генератори передавального та приймального пристроїв у всіх випадках обрано односпрямовано пов'язані системи Реслера (див. розділ

1.1.4.3) з близькими значеннями керуючих параметрів, а як інформаційні сигнали – прості послідовності бінарних біт. Вибір саме цих моделей радіотехнічних генераторів пов'язаний з тим, що:

1) система Реслера досить добре досліджена, у тому числі, і з погляду хаотичної синхронізації;

2) у односпрямовано пов'язаних системах Реслера можливе встановлення всіх типів синхронної поведінки, на основі яких побудовані схеми прихованої передачі даних, що досліджуються;

3) розташування межі узагальненої синхронізації на площині параметрів «частота розлаштування – інтенсивність зв'язку» задовольняє вимогам, зазначеним у розділі 1.2.

2.2.1 Оцінка ефективності підходу до прихованої передачі з підвищеною стійкістю до шумів на основі узагальненої хаотичної синхронізації

Як вже зазначалось раніше, підхід до прихованої передачі з підвищеною стійкістю до шумів на основі узагальненої хаотичної синхронізації володіє надстійкістю до шумів і не вимагає наявності ідентичних генераторів на різних сторонах каналу зв'язку (див. розділ 2.1.2, рис. 2.1). У цьому випадку передавальний генератор описується наступною системою диференціальних рівнянь:

$$\begin{aligned} \dot{x}_1 &= -\omega_x x_2 - x_3, \\ \dot{x}_2 &= \omega_x x_1 + a x_2, \\ \dot{x}_3 &= p + x_3(x_1 - c), \end{aligned} \tag{2.6}$$

де $\mathbf{x}(t)=(x_1, x_2, x_3)$ – вектор стану передавального генератора, керуючі параметри a=0,15, p=0,2 і c=10, ω_x – керуючий параметр, що характеризує власну частоту коливань системи.

Розмір параметра ω_x модулюється корисним цифровим сигналом наступним чином. Якщо заданий інтервал часу передається бінарний біт 1, то ω_x=0,95 протягом усього цього інтервалу. При передачі бінарного біта 0 ω_x=1.

Слід зазначити, що такий вибір значень параметра ω_x продиктований виключно демонстраційними цілями та обумовлений характером розташування кордону узагальненої синхронізації. Насправді параметр ω_x може приймати досить довільні значення (наприклад, результати, аналогічні описаним нижче, були отримані для ω_x=0,91 при передачі бінарного біта 1 і $\omega_x \in$[0,9, 0,91] при передачі бінарного біта 0). Необхідною умовою є лише чергування областей з асинхронною динамікою та режимом узагальненої синхронізації.

Приймальний пристрій містить два ідентичні хаотичні генератори , кожен з яких описується наступною системою рівняння:

$$\begin{aligned} \dot{u}_1 &= -\omega_u u_2 - u_3 + \varepsilon\big(s(t) - u_1\big)\,, \\ \dot{u}_2 &= \omega_u u_1 + a u_2\,, \\ \dot{u}_3 &= p + u_3(u_1 - c)\,. \end{aligned} \tag{2.7}$$

Тут $\mathbf{u}(t)=(u_1, u_2, u_3)$ – вектор стану першого приймального генератора. Нехай $\mathbf{v}(t)=(v_1, v_2, v_3)$, також задовольняє (2.7), є вектором стану другого приймального генератора (див. рис. 2.1). Керуючі параметри a, p, c було обрано ідентичними відповідним параметрам передавального генератора. Керуючий параметр ω_u, що характеризує власну частоту приймальних генераторів, обрано рівним ω_u=0,95 протягом усього часу передачі сигналу.

Сигнал, що генерується передавальним пристроєм, передається по каналу зв'язку. В досліджуваній моделі (2.6), (2.7) це реалізується у вигляді зв'язку приймального генератора з передавальними, тобто додаванням компоненти $\varepsilon(s(t)-u_1)$ в перше рівняння системи (2.7). Тут $s(t)=x_1+D\xi$ – це сигнал у каналі зв'язку. Доданок $D\xi$ моделює шуми в каналі зв'язку, ξ – стохастичний гаусів процес, що характеризується наступним розподілом ймовірності:

$$p(\xi) = \frac{1}{\sqrt{2\pi}\sigma} \exp\left[-\frac{(\xi - \xi_0)^2}{2\sigma^2}\right], \tag{2.8}$$

де ξ_0=0, σ=1 – середнє і дисперсія, відповідно. Параметр D визначає інтенсивність шуму, що додається.

Інтенсивність зв'язку між передавальним та приймальним генераторами характеризується параметром ε. Він був обраний рівним ε=0,14. У цьому випадку відомо, що при відсутності шумів і флуктуації в каналі зв'язку (D=0) режим узагальненої синхронізації в системі (2.6), (2.7) має місце при ω_x=1, у той час як при ω_x=0,95 узагальнена синхронізація не спостерігається.

Віднімальний пристрій виконує операцію $(u_1-v_1)^2$. Тоді після проходження через нього, згідно з методом допоміжної системи, має спостерігатися відсутність коливань для ω_x=1 та наявність хаотичних коливань для ω_x=0,95. Відновлений сигнал буде послідовністю областей з різними типами поведінки.

Проста послідовність бінарних бітів 0 / 1, обрана як початкове інформаційне повідомлення, наведена на рис. 2.2,а. Для інтегрування стохастичного рівняння (2.7) використовувався метод Ейлера з кроком дискретизації за часом h=0,0001.

Моделювання було розпочато з ідеалізованої ситуації, коли шуми в каналі зв'язку відсутні (тобто амплітуда шуму D=0). Зрозуміло, що такий випадок фактично нереалізований на практиці, оскільки шуми завжди присутні у реальних пристроях. У той самий час саме з урахуванням розгляду схем з ідеальними («безшумовими») каналами зв'язку було запропоновано і протестовано практично всі способи прихованої передачі, а вплив шуму на працездатність таких схем, аналізувався далеко не завжди. Тому розгляд ідеалізованої ситуації важливий як для перевірки працездатності схеми, так і для її зіставлення з відомими раніше схемами прихованої передачі.

Працездатність схеми без шумів ілюструє рис. 2.2,б-в. Сигнал x(t), що генерується передавальної системою для передачі по каналу зв'язку, наведено на рис. 2.2,б. Характеристики цього сигналу практично не змінюються в залежності від бінарного біта 0 / 1, який передається, (зміни параметра ω_x), що виразно видно по відсутності слідів амплітудної і частотної модуляції у сигналі x(t).

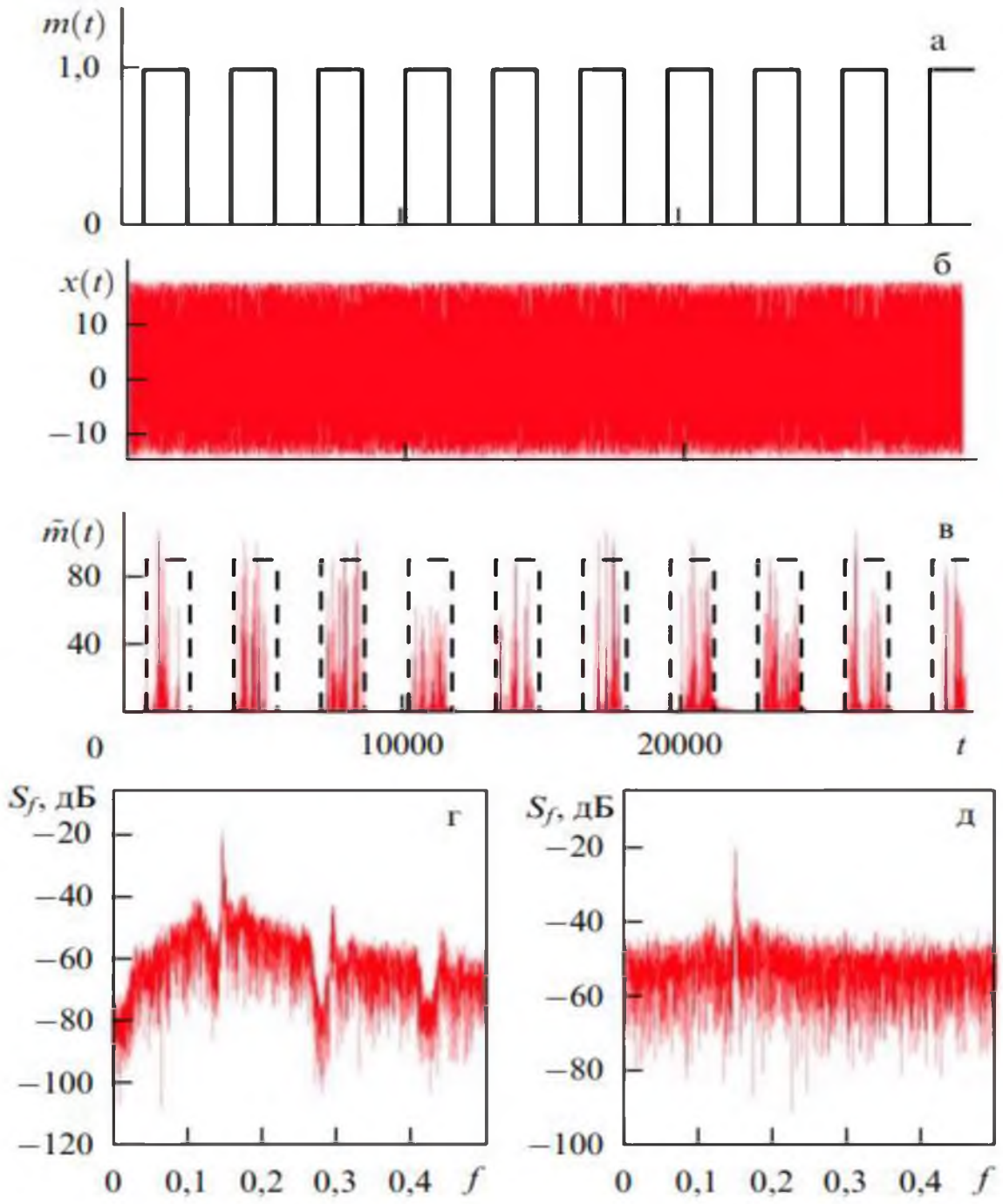

Рисунок 2.2 – Результати моделювання підходу до прихованої передачі з підвищеною стійкістю до шумів при відсутність шумів і флуктуації в каналі зв'язку (D=0): а – інформаційний сигнал m(t); б – сигнал x(t), вироблений передавальним генератором для подальшої передачі по каналу зв'язку; в – відновлений сигнал $\tilde{m}(t)$ і детектований інформаційний сигнал (штрихова лінія); г – спектр потужності сигналу в каналі зв'язку без шуму; д – спектр потужності сигналу в каналі зв'язку при шумі інтенсивністю D=10

У спектрі потужності такого сигналу завдяки відносно малому частотному розладу міститься лише одна чітко виражена спектральна компонента (рис. 2.2,г), що унеможливлює дешифрацію інформаційного повідомлення третьою стороною. На рис. 2.2,в показаний відновлений у приймаючому пристрої сигнал $\tilde{m}(t)$ після пропускання якого через фільтр нижніх частот і правильного вибору порогових значень може бути легко детектований початковий інформаційний сигнал.

Розглянемо тепер, який вплив надає шум, який неминуче присутній у каналах зв'язку реальних пристроїв, на ефективність досліджуваного підходу до прихованої передачі з підвищеною стійкістю до шумів на основі узагальненої синхронізації. Зрозуміло , що шум різко спотворює сигнал, який передається, що може серйозно позначитися на якості передачі інформації або, більше того, зробити її зовсім неможливою. Однак, як зазначалося у розділі 2.1.1, шум практично не впливає на поріг виникнення режиму узагальненої синхронізації в дисипативно пов'язаних хаотичних системах, тобто синхронний режим і за наявності, і за відсутності шуму виникає в таких системах при приблизно однакових значеннях параметра зв'язку ε. У той самий час аналіз стійкості аналізованої схеми до шуму показує , що при досить великих амплітудах шуму можлива ситуація, коли шум не тільки не руйнує режим узагальненої синхронізації, а й, навпаки, призводить до його виникнення при менших значеннях інтенсивності зв'язку, при яких без шуму режим узагальненої синхронізації не спостерігається. Це може негативно позначитись на якості передачі, тобто привести до можливості детектування лише бінарного біта 0. Однак лише шум з дуже великою амплітудою здатний «підсилити» узагальнену синхронізацію. Як випливає з результатів проведених досліджень, для системи (2.6), (2.7) із зазначеними значеннями керуючих параметрів така ситуація виникає при амплітудах шуму $D>400$.

Працездатність аналізованого підходу до прихованої передачі з підвищеною стійкістю до шумів за наявності досить сильних шумів у каналі зв'язку (D=10) показує рис. 2.3.

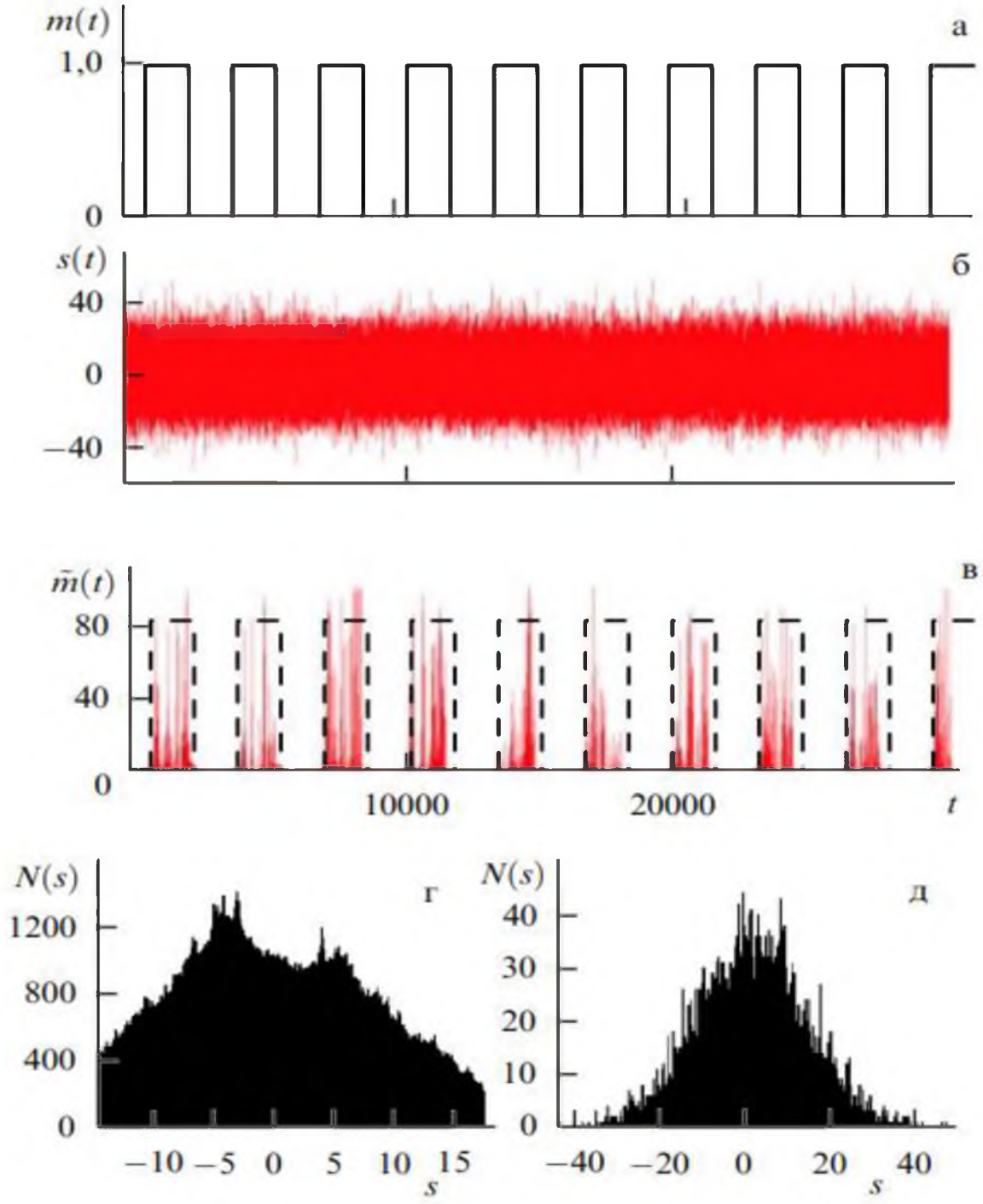

Рисунок 2.3 – Результати моделювання підходу до прихованої передачі з підвищеною стійкістю до шумів за наявності сильних шумів каналу зв'язку (D=10): а – інформаційний сигнал m(t); б – сигнал, що передається по каналу зв'язку; в – відновлений сигнал $\tilde{m}(t)$ і детектований інформаційний сигнал (штрихова лінія); г – розподіл амплітуд сигналу в каналі зв'язку без шуму; д – за наявності шуму інтенсивністю D=10 в каналі зв'язку

На рис 2.3, як і на рис. 2.2, представлені інформаційний сигнал m(t) (рис. 2.3,а), сигнал s(t) (рис. 2.3,б), що передається по каналу зв'язку (тобто сигнал, що генерується передавальної системою плюс шуми каналу зв'язку) і відновлений сигнал $\tilde{m}(t)$ до (суцільна лінія) та після (штрихова лінія) пропускання через фільтр нижніх частот та вибору порогових значень. За рахунок додавання шуму з досить великою амплітудою сигнал, який передається по каналу зв'язку, стає таким, що практично не відрізняється від стохастичного, що виразно видно як за характером часової реалізації сигналу, так і за характером розподілу його амплітуд (що є близьким до гаусового (рис. 2.3,г-д, на яких наведені подібні розподіли при відсутності і за наявності шуму). В спектрі потужності такого сигналу (рис. 2.2,д), так само як і за відсутності шуму в каналі зв'язку, міститься одна чітко виражена спектральна компонента, а додавання шуму призводить лише до збільшення інтенсивності п'єдесталу шуму, присутнього в ньому. У цьому випадку детектування інформаційного повідомлення третьою стороною є практично неможливим. Водночас якість інформації, відновленої в приймальному пристрої, залишається такою ж високою, як і при відсутності шумів у каналі зв'язку (див. рис. 2.2,в і рис. 2.3,в). Аналогічна ситуація має місце при будь-яких значеннях інтенсивності шуму D в діапазоні 0-400, що ще раз підтверджує значну стійкість досліджуваного підходу до прихованої передачі на основі узагальненої синхронізації до шуму в каналі зв'язку, а також свідчить про конструктивну роль шуму у збільшенні конфіденційності передачі інформації згідно цього підходу без втрати якості.

2.2.2 Оцінка ефективності інших відомих підходів до прихованої передачі інформації на основі хаотичної синхронізації

Перейдемо до імітаційного моделювання інших підходів до прихованої передачі на основі хаотичної синхронізації, розглянутих в розділах 1.1.3 та 1.2. Насамперед слід зазначити, що чисельна реалізація схем на основі хаотичного

маскування (див. розділ 1.1.3.1), перемикання хаотичних режимів (див. розділ 1.1.3.2), модулювання керуючих параметрів (див. розділ 1.1.3.4), а також двох запропонованих у роботі [32] схем, розглянутих у розділі 1.2 (рис. 1.10 та 1.11), не призводить до істотних змін рівнянь для передавальних і приймальних генераторів. Тому, якщо не обговорюється особливо, вважатимемо, що вони описуються системами диференціальних рівнянь (2.6)-(2.7) відповідно з керуючими параметрами a=0,15, p=0,2, c=10, ω_x=0,95. Значення інших керуючих параметрів сильно залежать від типу синхронної поведінки, яка використовується в даному підході, та специфіки її реалізації, тому вони вибиратимуться для кожної схеми різними. Крім того, від схеми до схеми змінюється характер сигналу в каналі зв'язку. Однак у всіх випадках було використано цифровий сигнал, представлений простою послідовністю бінарних бітів 0 / 1, як інформаційний і припускати, що шуми в каналі зв'язку підпорядковуються розподілу (2.8).

Для реалізації способу прихованої передачі на основі хаотичного маскування (див. розділ 1.1.3.1, рис. 1.2) необхідна наявність двох ідентичних генераторів, передавального і приймального, на різних сторонах каналу зв'язку. Тому виберемо ω_x=0,95 протягом усього часу передачі сигналу. Хаотичне маскування здійснюється безпосереднім домішуванням інформаційного сигналу до хаотичного, тобто сигнал у каналі зв'язку матиме вигляд $s(t)=x_1+m(t)+D\xi$. Крім того, для можливості реалізації режиму повної хаотичної синхронізації необхідно збільшити інтенсивність зв'язку між системами, тому виберемо ε=0,25.

У схемі на основі перемикання хаотичних режимів (див. розділ 1.1.3.2, рис. 1.3) передавальний пристрій містить два генератори, один з яких знаходиться в режимі повної хаотичної синхронізації з приймальним генератором, тобто є його точною копією (ω_x=0,95) та кодує бінарний біт 0. Другий передавальний генератор, який не ідентичний приймаючому і не синхронізований з ним (виберемо ω_x=1 у цьому випадку), кодує бінарний біт 1. Сигнал у каналі зв'язку тоді матиме вигляд $s(t)=x_1+D\xi$, а інтенсивність зв'язку

між системами, за аналогією зі схемою на основі хаотичного маскування, виберемо рівною ε=0,25.

Для схеми на основі модулювання керуючих параметрів (див. розділ 1.1.3.4, рис. 1.5) доцільно вибрати ті ж значення керуючих параметрів, що і для схеми на основі перемикання хаотичних режимів, оскільки чисельна реалізація цих двох схем прихованої передачі даних (при виборі якості передавальних генераторів двох ідентичних систем з параметрами, що злегка розрізняються в схемі на основі перемикання хаотичних режимів) є однаковою. Тому виберемо $s(t)=x_1+D\xi$, ε=0,25, $\omega_x = \begin{cases} 0{,}95, & m(t)=0, \\ 1{,}00, & m(t)=1. \end{cases}$

Схема на основі режиму узагальненої хаотичної синхронізації [32] (див. розділ 1.2, рис. 1.10) вимагає наявності додаткового хаотичного генератора, ідентичного приймальному, на передавальній стороні каналу зв'язку. Як і в роботі [32], називатимемо генератори передавального пристрою відомим і веденим, а ідентичний веденому генератор на приймальній стороні каналу зв'язку – допоміжним. В цьому випадку відомий генератор описується системою рівнянь (2.6) з вищевказаними значеннями керуючих параметрів і $\omega_x=1$ (з метою забезпечення неідентичності з іншими генераторами), а ведений і допоміжний генератори – системою (2.7), але сигнали s(t), що впливають на них будуть різними: $s(t)=n(t)x_1$, де $n(t) = \begin{cases} 0{,}9, & m(t)=1, \\ 1{,}0, & m(t)=0, \end{cases}$ у разі впливу на генератор передавального пристрою, і $s(t)=x_1+D\xi$ при передачі сигналу каналом зв'язку на приймальний генератор. З метою забезпечення можливості виникнення режиму узагальненої синхронізації між неідентичними генераторами виберемо параметр зв'язку ε=0,14.

У схемі на основі узагальненої та повної хаотичної синхронізації [32] (див. розділ 1.2, рис. 1.11), на приймальній стороні каналу зв'язку з'являється додатковий генератор, ідентичний першому передавальному по керуючих параметрах і односпрямовано пов'язаний з ним (далі – другий відомий генератор). Це генератор описується системою рівнянь (2.6) із додаванням додаткового доданку, тобто:

$$\dot{y}_1 = -\omega_x y_2 - y_3 + \varepsilon_2 (g(t) - y_1),$$
$$\dot{y}_2 = \omega_x y_1 + a y_2,$$
$$\dot{y}_3 = p + y_3 (y_1 - c), \qquad (2.9)$$

де **y**(t)=(y_1, y_2, y_3) – вектор стану цього генератора, ε_2=0,2 – параметр, що характеризує силу зв'язку між «відомими» генераторами, g(t)=x_1+$D\xi$ – сигнал, що передається по першому каналу зв'язку. Сигнал s(t) у цьому випадку також зазнає деяких змін: тепер на допоміжний генератор впливатиме сигнал s(t)=y_1.

При моделюванні обох схем, запропонованих у роботі [32] (рис. 1.10, 1.11), необхідно враховувати наявність другого каналу зв'язку, тобто при передачі сигналу від веденого генератора на пристрій до нього також домішуються шуми. Тому на віднімаючий пристрій надходитимуть не тільки детерміновані сигнали, вироблені веденим і допоміжним генераторами, а й стохастичний сигнал з другого каналу зв'язку. Відновлений сигнал тоді матиме вигляд $\tilde{m}(t)$=(u_1+$D\xi$-v_1)^2, якщо не брати до уваги, що шуми у двох каналах зв'язку є різними (облік цього значно погіршує можливість детектування корисного сигналу).

При моделюванні схем на основі нелінійного підмішування інформаційного сигналу до хаотичного (див. розділ 3.3, рис. 4) передавальний пристрій описується такими системами диференціальних рівнянь:

$$\dot{x}_1 = -\omega_x x_2 - x_3 + \varepsilon (y_1 + m(t) - x_1),$$
$$\dot{x}_2 = \omega_x x_1 + a x_2,$$
$$\dot{x}_3 = p + x_3 (x_1 - c), \qquad (2.10)$$
$$\dot{y}_1 = -\omega_x y_2 - y_3 + \varepsilon (x_1 + m(t) - y_1),$$
$$\dot{y}_2 = \omega_x y_1 + a y_2,$$
$$\dot{y}_3 = p + y_3 (y_1 - c). \qquad (2.11)$$

Тобто представляє собою два ідентичних взаємно пов'язаних хаотичних генератора. Тут **x**(t)=(x_1, x_2, x_3) і **y**(t)=(y_1, y_2, y_3) – вектори станів першого і другого передавальних генераторів відповідно, m(t) – інформаційний сигнал, ω_x=1, ε=0,25. Приймальний генератор описується системою рівнянь (2.7), ω_u=1.

Сигнал у каналі зв'язку в цьому випадку є просто сумою сигналу, що генерується однією з передавальних хаотичних систем, і шумів каналу зв'язку, тобто $s(t)=x_1+D\xi$.

Реалізація підходу до прихованої передачі інформації, запропонованого в роботі [33] (див. розділ 1.2, рис. 1.12), є деяким родом ускладненням схеми на основі нелінійного підмішування інформаційного сигналу до хаотичного, що полягає в появі ще двох ідентичних генераторів на різних сторонах каналу зв'язку. Тому рівняння та параметри трьох генераторів, присутніх в обох схемах, залишимо тими самими. Додатковий генератор на передавальній стороні каналу зв'язку описується наступною системою рівнянь:

$$\begin{aligned} \dot{z}_1 &= -\omega_z z_2 - z_3 + \varepsilon(y_1 - z_1), \\ \dot{z}_2 &= \omega_z z_1 + a z_2, \\ \dot{z}_3 &= p + z_3(z_1 - c), \end{aligned} \qquad (2.12)$$

де $\mathbf{z}(t)=(z_1, z_2, z_3)$ – вектор стану цього генератора, $\omega_z=0{,}95$. Аналогічний генератор на приймальній стороні каналу зв'язку, що характеризується вектором стану $\mathbf{v}(t)=(v_1, v_2, v_3)$, також задовольняє системі рівнянь (2.12) з точністю до заміни $\mathbf{z}(t)\to\mathbf{v}(t)$, $\mathbf{y}(t)\to\mathbf{u}(t)$, де $\mathbf{u}(t)=(u_1, u_2, u_3)$ – вектор стану приймального генератора, що задовольняє системі рівнянь (2.7), але в цьому випадку $s(t)=y_1+z_1-v_1+D\xi$. Сигнал $-v_1$ не передається по каналу зв'язку, а додається після проходження через нього, але до надходження на приймаючий генератор.

Реалізація підходу до прихованої передачі на основі фазової хаотичної синхронізації (див. розділ 1.2, рис. 1.9) на прикладі систем Реслера з близькими значеннями керуючих параметрів була здійснена в роботі [28]. У цьому випадку генератори передавального та приймального пристроїв описуються такими системами рівнянь:

$$\begin{aligned} \dot{x}_{1,2} &= -(\omega_x + \Delta\omega) y_{1,2} - z_{1,2} + \varepsilon(x_{2,1} - x_{1,2}), \\ \dot{y}_{1,2} &= (\omega_x + \Delta\omega) x_{1,2} + a y_{1,2}, \\ \dot{z}_{1,2} &= p + z_{1,2}(x_{1,2} - c), \end{aligned} \qquad (2.13)$$

$$\dot{x}_3 = -\omega_u y_3 - z_3 + \eta(r_3 \cos\phi_m - x_3),$$
$$\dot{y}_3 = \omega_u x_3 + a y_3,$$
$$\dot{z}_3 = p + z_3(x_3 - c), \qquad (2.14)$$

де $\mathbf{x}_{1,2}=(x_{1,2}, y_{1,2}, z_{1,2})$, $\mathbf{x}_3=(x_3, y_3, z_3)$ – вектори станів генераторів передавального та приймального пристроїв відповідно, $\omega_x=\omega_u=1$, $\varepsilon=5\text{x}10^{-3}$, $\eta=5{,}3$ – параметри зв'язку, $\Delta\omega=\pm 0{,}01$ – розлад параметра ω_x, що модулюється корисним цифровим сигналом (знак плюс відповідає передачі бінарного біта 1, знак мінус – 0), $r_3 = (x_3^2 + y_3^2)^{1/2}$ – амплітуда сигналу, що генерується приймальною системою.

Чисельна реалізація всіх інших розглянутих підходів до прихованої передачі інформації з вище зазначеними значеннями керуючих параметрів ще раз підтверджує, що усі вони мають дуже обмежену стійкість до шумів. Більш того, незважаючи на використання в них різних типів синхронної поведінки і різні принципи їх роботи, якісно шум впливає на них абсолютно однаково.

Найбільш наочно вплив шуму на працездатність підходу до прихованої передачі з допомогою узагальненої хаотичної синхронізації, запропонованого у роботі [32], ілюструє рис. 2.4, на якому поряд з інформаційним сигналом m(t), представленим простою послідовністю бінарних бітів 0/1 (рис. 2.4,а), наведено відновлені сигнали $\tilde{m}(t)$ (суцільні лінії) при різних значеннях амплітуди шуму (рис. 2.4,б-г). У відсутність шумів у каналі зв'язку (рис. 2.4,б) такий підхід працює досить ефективно. Інформаційний сигнал може бути легко детектований по відсутності/наявності хаотичних коливань в сигналі $\tilde{m}(t)$. Відновлений таким чином сигнал показаний штриховою лінією. Неважко помітити, що якість передачі інформації є досить високою, хоча в деяких випадках через наявність перехідних процесів помилкове діагностування бінарного біта 1 залишається можливим.

Поява шумів у каналі зв'язку призводить до шумів десинхронізації. Якщо інтенсивність шуму досить мала, ще залишається можливість декодувати інформаційне повідомлення m(t) по відновленому сигналу $\tilde{m}(t)$. Як видно з рис. 2.4,в, відповідного випадку D=1,5, незважаючи на наявність шумів

десинхронізації у всьому сигналі $\tilde{m}(t)$, ділянки, що відповідають бінарному біту 0, характеризуються нижчою амплітудою. Тому за правильного вибору порогового значення інформаційний сигнал можна буде детектувати; відновлений сигнал показаний штриховою лінією.

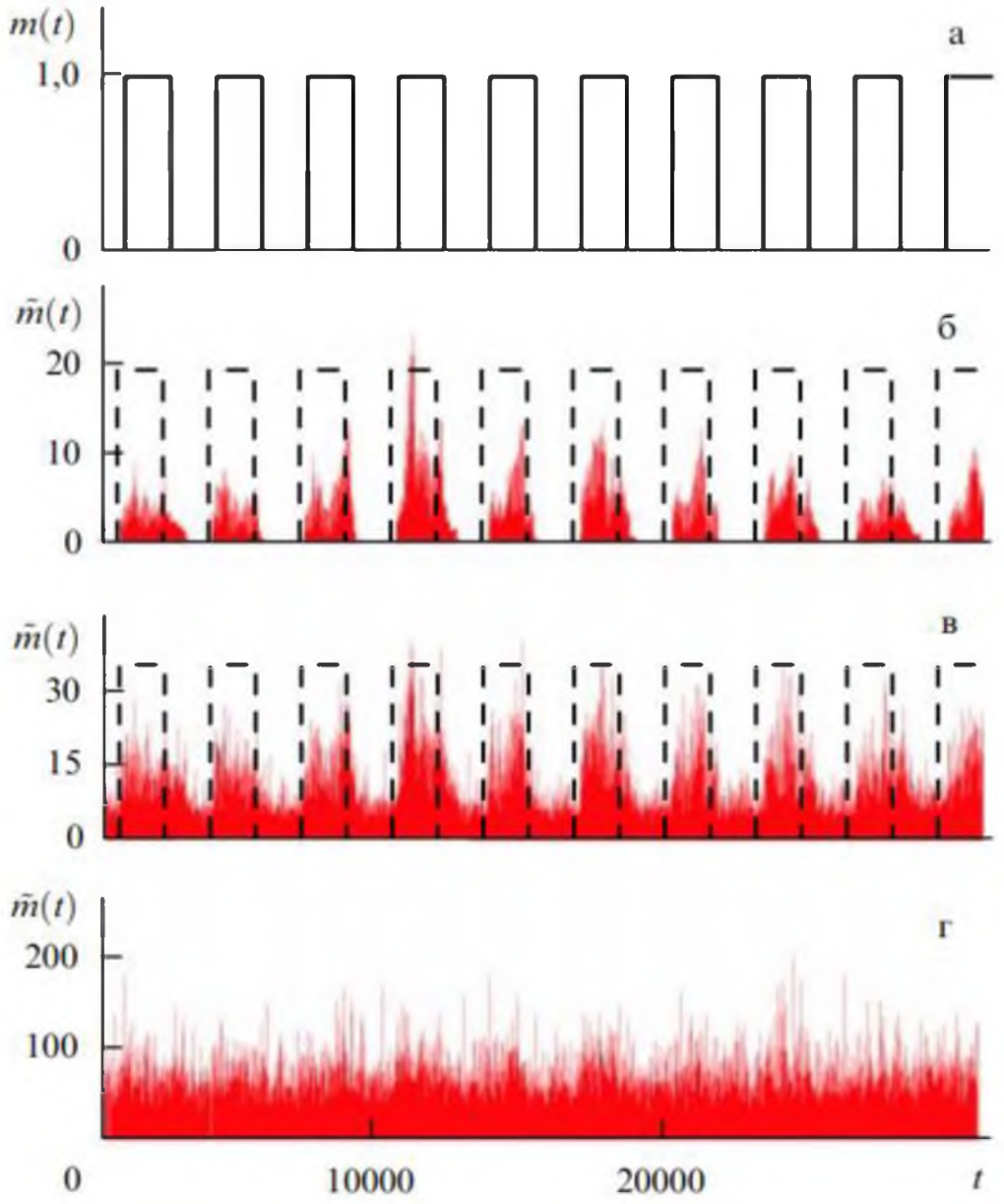

Рисунок 2.4 – Вплив шуму в каналі зв'язку на ефективність підходу [32]: а – інформаційний сигнал m(t); б – відновлений сигнал $\tilde{m}(t)$ при значенні амплітуди шуму D=0 (відсутності шумів та флуктуації в каналі зв'язку); в – D=1,5 (шуми з досить слабкою інтенсивністю); г – D=3 (шуми з сильнішою інтенсивністю)

Подальше збільшення амплітуди шуму призводить до «вирівнюванню» інтенсивності амплітуд коливань на ділянках, що відповідають бінарним бітам 0 та 1 (див., наприклад, рис. 2.4,г, де показаний сигнал $\tilde{m}(t)$ при D=3). Неважко помітити, що в даному випадку немає ніякої можливості декодувати інформаційне повідомлення.

Отже, з рис. 2.4 видно, що у випадках (б) та (в) інформаційний сигнал може бути детектований (штрихова лінія), у той час як у випадку (г) діагностувати інформаційний сигнал неможливо.

Якісно аналогічна ситуація спостерігається для всіх підходів до прихованої передачі інформації, розглянутих у розділах 1.1.3 та 1.2. Таким чином, проведені дослідження встановили, що на переважну більшість відомих підходів до прихованої передачі інформації шум впливає деструктивно. Однак, для того, щоб кількісно зіставити схеми одну з одною, необхідно оцінити деякі інші характеристики їх працездатності.

2.2.3 Оцінка кількісних характеристик працездатності схем і підходів до прихованої передачі інформації

Основними кількісними характеристиками працездатності схем прихованої передачі інформації є:

1. Критичне значення SNR_C відношення енергії на біт до спектральної щільності потужності шуму (SNR), при якому схема передачі стає непрацездатною, тобто виявляється неможливим відновлення початкового корисного цифрового сигналу m(t) по сигналу $\tilde{m}(t)$, що отримується на виході. Відношення енергії на біт до спектральної щільності шуму, яке вводиться в розгляд для цифрових систем зв'язку, є аналогом відношення сигнал/шум аналогового зв'язку:

$$\mathrm{SNR} = 10 \lg \frac{E_b}{N_0} \ [\text{дБ}], \tag{2.15}$$

де E_b – енергія сигналу, що припадає на один біт інформації, яка передається, N_0 – спектральна щільність потужності шуму. При цьому енергія, що припадає на один біт, описується як

$$E_b=P_{sign}\,T, \tag{2.16}$$

де P_{sign} – потужність переданого сигналу без шуму, T – час передачі одного біта, а спектральна потужність шуму визначається як

$$N_0=\frac{P_{noise}}{\Delta f}, \tag{2.17}$$

де P_{noise} – потужність шуму в каналі зв'язку, Δf – ширина смуги пропускання каналу. Оскільки шуми неминуче присутні в каналах зв'язку реальних пристроїв, оцінка працездатності схем передачі інформації при наявності шумів є актуальним завданням.

Розрахунок потужності як детермінованого, так і стохастичного сигналів здійснювався по їх часовій реалізації. При проведенні чисельних розрахунків передбачалося, що ширина смуги пропускання $\Delta f=f_2-f_1=0{,}2$, де $f_1=0{,}05$, $f_2=0{,}25$ – межі смуги пропускання каналу у разі використання генераторів Реслера.

Для характеристики ступеня стійкості схем прихованої передачі по відношенню до зовнішніх шумів у цифрових системах зв'язку досить часто використовують, поряд з характеристикою, описаною вище, залежність ймовірності похибки на біт (BER – Bit Error Rate) від відношення енергії на біт до спектральної щільності потужності шуму. Ймовірність помилки на біт характеризує якість передачі інформації і є кількістю похибок, віднесене до числа переданих бітів. Припустимо, що схема коректно передає бінарний біт 0 з ймовірністю P_{00} та бінарний біт 1 з ймовірністю P_{11}. Тоді помилкове діагностування бінарного біта 1 при передачі бінарного біта 0 характеризується ймовірністю $P_{01}=1-P_{00}$, а ймовірність $P_{10}=1-P_{11}$ характеризує помилкове діагностування бінарного біта 0 при передачі бінарного біта 1. Якщо символи з'являються в переданій послідовності з ймовірностями P_{00} і P_{11} відповідно, то ймовірність помилки на біт обчислюється таким чином:

$$BER=2(P_{01}P_0+P_{10}P_1), \tag{2.18}$$

причому ймовірності P_{01} і P_{10} залежить від типу і параметрів системи зв'язку.

2. Максимальне значення PM_C розладу керуючих параметрів (PM, %) генераторів, які спочатку повинні бути ідентичними. Як вже зазначалось, у більшості випадків такі генератори повинні розташовуватися на різних сторонах каналу зв'язку. Зважаючи на складність технічної реалізації таких пристроїв вплив розладу їх керуючих параметрів на ефективність роботи підходів до передачі інформації є дуже актуальною проблемою.

3. Максимальний рівень ND_C нелінійних спотворень у каналі зв'язку, при якому схема працює:

$$\mathrm{ND} = 10 \lg \frac{P_x}{P_y} \quad [\text{дБ}]. \tag{2.19}$$

Тут P_x – потужність сигналу $x(t)$ на виході передавального генератора, P_y – потужність сигналу $y(t)$ на вході приймаючого пристрою. Традиційно в чисельних розрахунках використовуються нелінійні спотворення у вигляді кубічної нелінійності $y=x(1-\alpha x^2)$, де α – малий параметр [12], тому далі вважатимемо, що при проходженні через канали зв'язку всіх схем та пристроїв сигнал зазнає спотворення такого роду.

Для того, щоб кількісно порівняти підходи до прихованої передачі інформації, описані в цьому огляді, оцінимо вищезгадані характеристики для всіх розглянутих схем. Слід зазначити, що в роботі [12] була введена інша характеристика працездатності схеми передачі даних, заснована на оцінці ступеня близькості сигналів, яка визначається як

$$\eta = \frac{\Delta P}{P}, \tag{2.20}$$

де ΔP – потужність шуму десинхронізації, P – потужність шуму на вході генератора. Але слід зазначити, що дана характеристика має сенс тільки для схем, заснованих на повній хаотичній синхронізації, тому з метою досягнення спільності та можливості порівняння різних методів вона не розглядалась.

Результати розрахунку кількісних характеристик працездатності схем представлені у табл. 2.1.

Таблиця 2.1 – Кількісні характеристики працездатності схем

№	Назва схеми / підходу	SNR_C, дБ	PM_C, %	ND_C, дБ
1.	Хаотичне маскування (рис. 1.2)	56,48	0,30	1,03
2.	Перемикання хаотичних режимів (рис. 1.3)	30,76	2,00	23,3
3.	Нелінійне підмішування (рис. 1.4)	64,99	0,30	0,26
4.	Адаптивні методи (рис. 1.5)	30,76	2,00	23,3
5.	Підхід на основі режиму фазової синхронізації (рис. 1.9)	32,40	0,80	10,7
6.	Підхід на основі режиму узагальненої синхронізації (рис. 1.10)	39,52	1,00	7,75
7.	Підхід на основі узагальненої та повної синхронізації (рис. 1.11)	39,24	0,50	4,83
8.	Підхід зі «складним сигналом» (рис. 1.12)	61,47	0,20	2,63
9.	Підхід з підвищеною стійкістю до шумів (рис. 2.1)	-10,01	2,00	27,2

Як видно з табл. 2.1, схема 9, стає непрацездатною при SNR_C=-10,01 дБ, у той час як для інших розглянутих нами схем SNR_C виявляється позитивним. Тобто за наявності в каналі зв'язку шумів певного рівня (навіть якщо потужність шумів менша за потужність переданого сигналу) більшість схем стає непрацездатними. Зрозуміло, що значення таких характеристик змінюватимуться від схеми до схеми. Зі схем 1-8 найкращими в цьому відношенні є схеми на основі перемикання хаотичних режимів і адаптивні методи (модулювання керуючих параметрів) (схеми 2 і 4, SNR_C=30,76 дБ). Але позитивне значення відношення енергії на біт до спектральної щільності шуму свідчить про обмежену стійкість до шумів та деструктивну роль шуму при передачі інформації.

Схема 9, детально розглянута в розділі 2.1.2, має значну стійкість до шумів в каналі зв'язку. При цьому, ще більше спотворюючи сигнал, що передається, шум перешкоджає третій стороні декодувати інформаційне повідомлення. У цьому випадку можна говорити про конструктивну роль шуму у підвищенні конфіденційності передачі інформації, тоді як у інших випадках роль шуму є деструктивною.

Справедливість вищенаведених міркувань підтверджується також залежністю ймовірності похибки на біт від спектральної щільності потужності шуму для різних схем прихованої передачі. Зазначені залежності представлені на рис. 2.5.

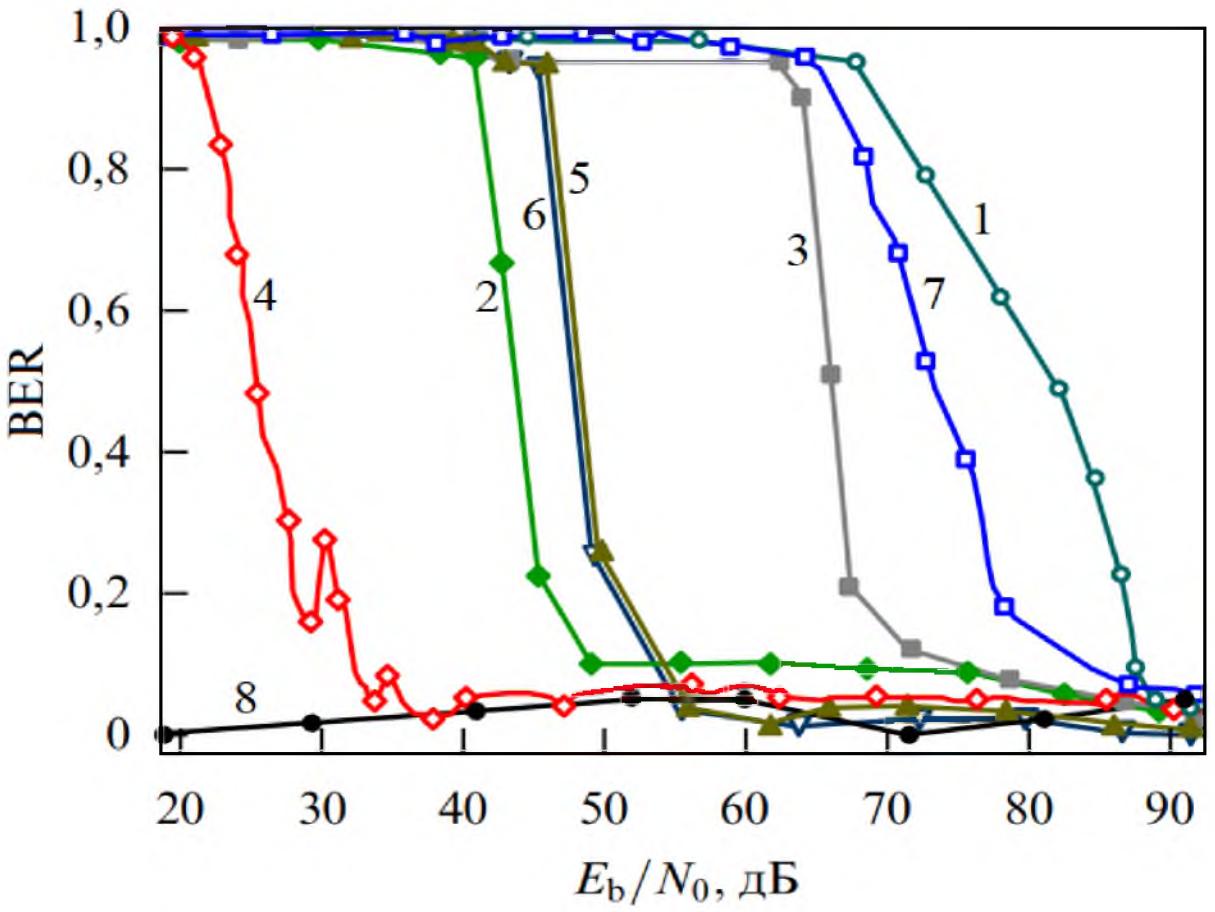

Рисунок 2.5 – Залежність BER від відношення енергії на біт до спектральної щільності потужності шуму(E_b/N_0) для різних схем прихованої передачі: 1 – хаотичне маскування; 2 –перемикання хаотичних режимів (модулювання керуючих параметрів); 3 – нелінійне підмішування; 4 – підхід на основі режиму фазової синхронізації, 5 – підхід на основі режиму узагальненої синхронізації; 6 – підхід на основі узагальненої та повної синхронізації; 7 – підхід з «складним сигналом», 8 – підхід з підвищеною стійкістю до шумів

При розрахунку ймовірності похибки на біт граничне значення, що дозволяє відновити початкову послідовність бінарних бітів по сигналу $\tilde{m}(t)$, вибиралось фіксованим незалежно від інтенсивності шуму, що впливає на

систему, тоді як при визначенні показників, представлених у табл. 2.1, воно змінювалося. У той же час, як видно з рис. 2.5 для різних підходів прихованої передачі інформації (схеми 1-8 табл. 2.1) ймовірність похибки на біт досить швидко стає рівною 1, тоді як для підходу з підвищеною стійкістю (схема 9) вона виявляється близькою до 0, незалежно від інтенсивності шуму, який впливає на систему, що досить добре узгоджується з результатами, наведеними вище.

Оцінимо тепер вплив розладу керуючих параметрів на ефективність роботи розглянутих підходів до прихованої передачі даних. Для цього введемо розлад у параметр ω_u однієї з двох спочатку ідентичних систем. Тоді параметр ω однієї з систем заміниться параметром $\omega(1\pm\eta)$, де η – розлад по ω (РМ). Для певності у всіх випадках братимемо знак «плюс» (аналогічні результати отримані при виборі знаку «мінус»).

Подібні оцінки дозволяють зробити висновок, що схема підходу з підвищеною стійкістю до шумів (схема 9 у табл. 2.1) залишатиметься працездатною до тих пір, поки генератори приймального пристрою, не будуть розладжені більш ніж до 2% за параметром ω_u. Звичайно, це не настільки велика величина, і в цьому відношенні розглянута схема 9 має конкурентів, якими знову є схеми передачі інформації на основі перемикання хаотичних режимів і модулювання керуючих параметрів (схеми 2 та 4 у табл. 2.1 відповідно). Однак схема 9 і з цієї точки зору має принципову перевагу перед схемами 2 і 4. Спочатку ідентичні хаотичні генератори в схемах 2 і 4 табл. 2.1 (так само як і у всіх інших, крім схеми 9) повинні розташовуватися на різних сторонах каналу зв'язку (для можливості реалізації режиму повної синхронізації між ними). У схемі 9 ідентичні генератори розташовуються тільки на приймальній стороні каналу зв'язку, що дозволяє легко здійснити при необхідності їх юстування.

Що стосується стійкості до нелінійних спотворень у каналі зв'язку, то і за цією характеристикою схема підходу з підвищеною стійкістю до шумів (схема 9 у табл. 2.1) перевершує всі відомі аналоги. Зрозуміло , що чим більше вплив

нелінійних спотворень на сигнал, тим вище має бути максимально допустимий рівень нелінійних спотворень, при якому підхід до прихованої передачі буде залишатися ще працездатним. Як видно з табл. 2.1, максимальний рівень нелінійних спотворень для схеми 9 ND_C=27,2 дБ. Найбільш близькими показниками знову володіють способи прихованої передачі інформації на основі перемикання хаотичних режимів і модулювання керуючих параметрів (схеми 2 і 4), проте стійкість схеми 9 до нелінійних спотворень виявляється трохи вище. Крім того, схеми 2 і 4 мають обмежену стійкість до шумів, у той час як стійкість схеми 9 є практично необмеженою в реальних межах.

Зрозуміло, що зміна значень керуючих параметрів і рівнянь генераторів (наприклад, у всіх випадках в передавальному і приймальному пристроях можна використовувати генератори Чуа [35], кільцеві генератори хаосу із запізненням [36], генератори хаосу на основі систем фазового автопідстроювання [37], генератори хаосу з 2,5 ступенями свободи [22] ті інші моделі), а також зміна характеру розподілу випадкової величини ξ може призвести до зміни кількісних значень аналізованих характеристик. У той самий час порядки цих величин і співвідношення з-поміж них завжди залишатимуться приблизно однаковими (див., наприклад, [38]).

2.3 Висновки

Обґрунтовано і розглянуто підхід до прихованої передачі з підвищеною стійкістю до шумів за допомогою узагальненої хаотичної синхронізації, позбавлений вищезгаданих недоліків. За допомогою імітаційного моделювання в середовищі Matlab/Simulink односпрямовано пов'язаних систем Реслера, обраних як генератори передавального та приймального пристроїв, проведено порівняння між собою усіх схем і підходів, розглянутих в роботі.

Розрахунок кількісних характеристик працездатності схем і підходів до прихованої передачі даних показав, що розглянутий підхід до прихованої передачі з підвищеною стійкістю до шумів за допомогою узагальненої

хаотичної синхронізації має значну, практично необмежену в реальних межах стійкість до шумів у каналі зв'язку, у той час як стійкість інших розглянутих схем і підходів є обмеженою. Крім того, цей метод досить стійкий до розладу керуючих параметрів спочатку ідентичних хаотичних генераторів (які розташовуються на одній стороні каналу зв'язку, що також є важливою перевагою) і до нелінійних спотворень каналу зв'язку.

Досліджений підхід до прихованої передачі з підвищеною стійкістю до шумів за допомогою узагальненої хаотичної синхронізації відкриває ряд нових можливостей для експериментальної реалізації прихованої передачі на основі хаотичної синхронізації. Відсутність низки недоліків, властивих більшості схем прихованої передачі, робить це завдання актуальним і перспективним.

Подальші дослідження мають бути спрямовані на імітаційному моделюванні в середовищі Matlab/Simulink всіх розглянутих підходів і схем на основі інших математичних моделей (Лоренца, Чуа тощо) та розрахунків кількісних характеристик їх працездатності.

3 ЕКОНОМІЧНИЙ РОЗДІЛ

Метою розділу є обґрунтування економічної доцільності забезпечення конфіденційності в системах передачі інформації з використанням хаотичних коливань. За для того необхідно встановити величини капітальних витрат на розробку запропонованого підходу та експлуатаційних витрат на його реалізацію, економічний ефект від впровадження запропонованого підходу та розрахувати показники економічної ефективності, зокрема коефіцієнт повернення інвестицій та період окупності.

3.1 Розрахунок (фіксованих) капітальних витрат

Фіксованими витрати називаються тому, що робляться, як правило, один раз, на початкових етапах створення ІС. До фіксованих належать 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 забезпечення конфіденційності в системах передачі інформації з використанням хаотичних коливань визначаються, виходячи з трудомісткості кожної операції, та належать до капітальних витрат.

Визначення трудомісткості розробки підходу із забезпечення конфіденційності в системах передачі інформації з використанням хаотичних коливань

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

– тривалість складання технічного завдання забезпечення конфіденційності в системах передачі інформації з використанням хаотичних коливань, $t_{тз}$=15 годин;

– аналіз можливих загроз безпеки інформації, $t_{аз}$=20 годин;

– технічна експертиза забезпечення конфіденційності в системах передачі інформації з використанням хаотичних коливань, $t_{нд}$=16 годин;

– тривалість визначення вимог до заходів, методів та засобів захисту, $t_{вз}$=24 години;

– тривалість апробації результатів із реалізації підходу щодо забезпечення конфіденційності в системах передачі інформації з використанням хаотичних коливань, $t_{озб}$=46 години;

$t_{овр}$ – тривалість організації виконання відновлювальних робіт і забезпечення неперервного функціонування організації, $t_{овр}$=20 годин;

$t_{э}$ – тривалість документального оформлення запропонованого підходу із забезпечення конфіденційності в системах передачі інформації з використанням хаотичних коливань, $t_{д}$=16 годин.

Отже,

$t = t_{тз}+ t_{аз}+ t_{нд}+ t_{вз}+ t_{озб}+ t_{овр}+ t_{д}$=15+20+16+24+46+20+16 = 157 години.

Розрахунок витрат на розробку підходу із забезпечення конфіденційності в системах передачі інформації з використанням хаотичних коливань

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 запропонованого підходу $З_{мч}$.

$$К_{рп} = З_{зп} + З_{мч}\ .$$

$$К_{рп} = З_{зп} + З_{мч} = 35325 + 985,96 = 36310,96 \text{ грн.}$$

$$З_{зп} = t\ З_{пр} = 157*225 = 35325 \text{ грн.}$$

де t – загальна тривалість розробки політики безпеки, годин;

$Зіб$ – средньогодинна заробітна плата спеціаліста з інформаційної безпеки з нарахуваннями, грн/годину.

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

$$З_{мч}= t*С_{мч}=157*6,28=985,96 \text{ грн.}$$

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:

$$\text{Смч} = 0{,}7 \cdot 4 \cdot 1{,}68 + \frac{6700 \cdot 0{,}3}{1920} + \frac{3400 \cdot 0{,}3}{1920} = 6{,}28 \text{ грн.}$$

Реалізація запропонованого із забезпечення конфіденційності в системах передачі інформації з використанням хаотичних коливань здійснюється із використанням універсального генератору шуму, вартість якого складає 13759 грн.

Оцінка ефективності запропонованого підходу до забезпечення конфіденційності в системах передачі інформації з використанням хаотичних коливань проводилась в середовищі Matlab/Simulink за допомогою стандартних і розроблених програм. Отже, додаткових витрат немає.

Витрати на встановлення обладнання та налагодження системи інформаційної безпеки заплановані величиною 800 грн.

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

$К=К_{рп}+К_{зпз}+К_{пз}+К_{аз}+К_{навч}+К_{н}$ =36310,96 +13759+800= 50869,96 грн.

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

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

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

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

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

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

3.1.1 Розрахунок поточних витрат

Річні поточні витрати на функціонування системи інформаційної безпеки складають:

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

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

$С_к$ - витрати на керування системою в цілому;

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

Витрати на відновлення й модернізації системи інформаційної безпеки заплановані в розмірі 2200 грн.

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

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

Річні амортизаційні відрахування матеріальних активів, які відповідно до чинного законодавства України підлягають амортизації, визначатимуться, виходячи зі строку корисного використання 5 років. Сума амортизаційних відрахувань визначається за прямолінійним методом нарахування амортизації. Таким чином, річні амортизаційні відрахування за апаратним забезпеченням, а саме, універсальним генератором шуму, складуть:

$$С_а = 13759/5 = 2751{,}8 \text{ грн.}$$

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 22000 грн. Додаткова заробітна плата – 10% від основної заробітної плати. Виконання роботи щодо впровадження системи захисту

інформації на підприємстві потребує залучення спеціаліста інформаційної безпеки на 0,5 ставки. Отже,

$$С_з = (22000*12 + 22000*12*0,1)*0,5= 145200 \text{ грн.}$$

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

$$С_{єв} = 145200*0,22 = 31944 \text{ грн.}$$

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:

$$С_{ел} = 0,9*1920*1,68 = 2903,04 \text{ грн.}$$

Витрати на технічне й організаційне адміністрування та сервіс системи інформаційної безпеки визначаються у відсотках від вартості капітальних витрат – 2% ($С_{тос}$ = 50869,96*0,02=1017,4 грн).

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

$$С_к = 2200+2751,8+ = 123681,6 \text{ грн.}$$

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

$$С = 2000+123681,6+145200+31944+2903,04+1017,4+123681,6 = 430427,64 \text{ грн.}$$

3.2 Оцінка можливого збитку

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

Необхідні *вихідні дані* для розрахунку:

$t_п$ – час простою вузла або сегмента корпоративної мережі внаслідок атаки, 2 години;

$t_в$ – час відновлення після атаки персоналом, що обслуговує корпоративну мережу, 4 години;

$t_{ви}$ – час повторного введення загубленої інформації співробітниками атакованого вузла або сегмента корпоративної мережі, 3 годин;

$З_о$ – заробітна плата обслуговуючого персоналу (адміністраторів та ін.), 18000 грн./міс.;

$З_с$ – заробітна плата співробітників атакованого вузла або сегмента корпоративної мережі, 16000 грн./міс.;

$Ч_о$ – чисельність обслуговуючого персоналу (адміністраторів та ін.), 2 особи;

$Ч_с$ – чисельність співробітників атакованого вузла або сегмента корпоративної мережі, 6 осіб.;

О – обсяг прибутку атакованого вузла або сегмента корпоративної мережі, 700 тис. грн. у рік;

$П_{зч}$ – вартість заміни встаткування або запасних частин, 2000 грн;

I – число атакованих сегментів корпоративної мережі, 1;

N – середнє число атак на рік, 200.

Упущена вигода від простою атакованого сегмента корпоративної мережі становить:

$$U = П_п + П_в + V,$$

де $П_п$ – оплачувані втрати робочого часу та простої співробітників атакованого вузла або сегмента корпоративної мережі, грн;

$П_в$ – вартість відновлення працездатності вузла або сегмента корпоративної мережі (переустановлення системи, зміна конфігурації та ін.), грн;

V – втрати від зниження обсягу продажів за час простою атакованого вузла або сегмента корпоративної мережі, грн.

Втрати від зниження продуктивності співробітників атакованого вузла або сегмента корпоративної мережі являють собою втрати їхньої заробітної плати (оплата непродуктивної праці) за час простою внаслідок атаки:

$$П_п = \frac{\sum З_с}{F} t_п = \frac{16000 * 6}{176} * 2 = 1090{,}91 \text{ грн},$$

де F – місячний фонд робочого часу (при 40-а годинному робочому тижні становить 176 ч).

Витрати на відновлення працездатності вузла або сегмента корпоративної мережі включають кілька складових:

$$П_в = П_{ви} + П_{пв} + П_{зч},$$

де $П_{ви}$ – витрати на повторне уведення інформації, грн.;

$П_{пв}$ – витрати на відновлення вузла або сегмента корпоративної мережі, грн;

$П_{зч}$ – вартість заміни устаткування або запасних частин, грн.

Витрати на повторне введення інформації $П_{ви}$ розраховуються виходячи з розміру заробітної плати співробітників атакованого вузла або сегмента корпоративної мережі $З_с$, які зайняті повторним введенням втраченої інформації, з урахуванням необхідного для цього часу $t_{ви}$:

$$П_{ви} = \frac{\sum З_с}{F} t_п = \frac{16000 * 6}{176} * 3 = 1636{,}36 \text{ грн.}$$

Витрати на відновлення сегмента корпоративної мережі $П_{пв}$ визначаються часом відновлення після атаки $t_в$ і розміром середньогодинної заробітної плати обслуговуючого персоналу (адміністраторів):

$$П_{пв} = \frac{\sum З_с}{F} t_п = \frac{18000 * 1}{176} * 4 = 409{,}09 \text{ грн.}$$

Тоді витрати на відновлення працездатності вузла або сегмента корпоративної мережі складуть:

$$П_в = 1636{,}36+409{,}09+2000 = 4045{,}45 \text{ грн.}$$

Втрати від зниження очікуваного обсягу прибутків за час простою атакованого вузла або сегмента корпоративної мережі визначаються виходячи із средньогодинного обсягу прибутку і сумарного часу простою сегмента корпоративної мережі:

$$V = \frac{О}{Fг} \cdot (t_п + t_в + t_{ви})$$

$$V = \frac{700000}{2080} \cdot (2 + 3 + 4) = 3028{,}85 \text{ грн.}$$

де $F_г$ – річний фонд часу роботи філії (52 робочих тижні, 5-ти денний робочий тиждень, 8-ми годинний робочий день) становить близько 2080 год.

U = 1090,91+4045,45 +3028,85=8165,21 грн.

Таким чином, загальний збиток від атаки на сегмент корпоративної мережі організації складе:

$$B = \sum_i \sum_n U = \sum_1 \sum_{200} 3028{,}85 = 605770 \text{ грн.}$$

3.2.1 Загальний ефект від впровадження системи інформаційної безпеки

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

$$E = B * R - C \text{ грн.},$$

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

R – вірогідність успішної реалізації атаки на сегмент мережі, частки одиниці (90%);

C – щорічні витрати на експлуатацію системи інформаційної безпеки.

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

E = 605770*0,9 - 430427,64=114765,36 грн.

3.3 Визначення та аналіз показників економічної ефективності системи інформаційної безпеки

За методикою сукупної вартості володіння (ТСО) визначають такі показники економічної ефективності системи інформаційної безпеки 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:

$$ROSI = \frac{114765,36}{50869,96} = 2,26, \quad \text{частки одиниці,}$$

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

$$ROSI > (N_{деп} - N_{інф})/100),$$

де $N_{деп}$ – річна депозитна ставка, (6%); $N_{інф}$ – річний рівень інфляції, (5%).

Розрахункове значення коефіцієнта повернення інвестицій:

$$2,26 > (6 - 5)/100 = 2,26 > 0,01.$$

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

$$T_o = \frac{K}{E} = \frac{1}{ROSI} = \frac{1}{2,26} = 0,44, \quad \text{років.}$$

3.4 Висновок

Розробка підходу із забезпечення конфіденційності в системах передачі інформації з використанням хаотичних коливань може вважатися економічно доцільною, тому що значення коефіцієнту повернення інвестицій ROSI складає 2,24 грн./грн., що означає, що на 1 гривню капітальних витрат припадає 2,24 грн. економічного ефекту. Величина економічного ефекту складає 114765,36 грн. Капітальні витрати складають 50869,96 грн. Отримане значення коефіцієнта ROSI перевищує дохідність альтернативного вкладення коштів. Термін окупності при цьому складає 0,44 років.

ВИСНОВКИ

Основні результати кваліфікаційної роботи полягають у наступному:

В роботі проведено розгляд схем і підходів до прихованої передачі з використанням хаотичних сигналів, основу яких лежать різні типи синхронної поведінки хаотичних систем: повна хаотична синхронізація, фазова синхронізація, узагальнена хаотична синхронізація, а також декілька типів синхронної поведінки одночасно (наприклад, узагальнена та повна синхронізації). Кожна зі схем характеризується своїми особливостями та принципами роботи і має властиві тільки їй переваги та недоліки. У той же час більшість недоліків та труднощів технічної реалізації характерно для низки схем та пристроїв подібного призначення. Це насамперед: 1) вимога високого ступеня ідентичності генераторів на різних сторонах каналу зв'язку; 2) низька стійкість до шумів у каналі зв'язку; 3) досить низька конфіденційність.

Обґрунтовано і розглянуто підхід до прихованої передачі з підвищеною стійкістю до шумів за допомогою узагальненої хаотичної синхронізації, позбавлений вищезгаданих недоліків. За допомогою імітаційного моделювання в середовищі Matlab/Simulink односпрямовано пов'язаних систем Реслера, обраних як генератори передавального та приймального пристроїв, проведено порівняння між собою усіх схем і підходів, розглянутих в роботі.

Розрахунок кількісних характеристик працездатності схем і підходів до прихованої передачі даних показав, що розглянутий підхід до прихованої передачі з підвищеною стійкістю до шумів за допомогою узагальненої хаотичної синхронізації має значну, практично необмежену в реальних межах стійкість до шумів у каналі зв'язку, у той час як стійкість інших розглянутих схем і підходів є обмеженою. Крім того, цей метод досить стійкий до розладу керуючих параметрів спочатку ідентичних хаотичних генераторів (які розташовуються на одній стороні каналу зв'язку, що також є важливою перевагою) і до нелінійних спотворень каналу зв'язку.

Досліджений підхід до прихованої передачі з підвищеною стійкістю до шумів за допомогою узагальненої хаотичної синхронізації відкриває ряд нових можливостей для експериментальної реалізації прихованої передачі на основі хаотичної синхронізації. Відсутність низки недоліків, властивих більшості схем прихованої передачі, робить це завдання актуальним і перспективним.

Подальші дослідження мають бути спрямовані на імітаційному моделюванні в середовищі Matlab/Simulink всіх розглянутих підходів і схем на основі інших математичних моделей (Лоренца, Чуа тощо) та розрахунків кількісних характеристик їх працездатності.

ПЕРЕЛІК ПОСИЛАНЬ

1. Шустер Г. Детерминированный хаос: Введение / Г. Шустер; пер. с англ. под ред. Ф. М. Израйлева. – М. : Мир, 1988. – 240 с.

2. Варакин Л.Е. Системы связи с шумоподобными сигналами / Л.Е. Варакин. – М. : Радио и связь, 1985. – 384 с.

3. Кислов В.Я. Новый класс сигналов для передачи информации. Широкополосные хаотические сигналы / В.Я. Кислов, В.В. Кислов // Радиотехника и электроника. – 1997. – Т. 42, № 8. – С. 962-973.

4. Дмитриев А.С. Динамический хаос как парадигма современных средств связи / А.С. Дмитриев, А.И. Панас, С. О. Старков // Зарубежная радиоэлектрон. Успехи современной радиоэлектрон. – 1997. – № 10. – С. 4–26.

5. 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.

6. Галюк С.Д. Особливості синхронізації хаотичних систем // С.Д. Галюк., Л.Ф. Політанський, М.Я. Кушнір, Р.Л. Політанський // Складні системи і процеси. – 2011. – №2. – С. 3–29.

7. Ван-дер-Поль Б. Нелинейная теория электрических колебаний / Б. Ван-дер-Поль. – М.: Связьтехиздат, 1935. – 384 с.

8. Блехман И.И. Синхронизация в природе и технике / И.И. Блехман. – М.: Наука, 1981. – 274 с.

9. Анищенко В.С. Нелинейная динамика хаотических и стохастических систем. Фундаментальные основы и избранные проблемы / В.С. Анищенко, Т.Е. Вадивасова, В.В. Астахов. – Саратов: Изд-во Сарат. ун-та, 1999. – 288 с.

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

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

12. Дмитриев А.С. Динамический хаос: новые носители информации для систем связи. / А.С. Дмитриев, А.И. Панас. – М.: Физматлит, 2002. – 252 с.

13. Галюк С.Д. Адаптивна синхронізація кільцевих генераторів хаосу / С. Галюк, М. Кушнір, В. Русин // Комп'ютерні науки та інженерія: матеріали IV міжн. конф. молодих вчених CSE–2010. 25–27 жовтня 2010. – Львів. – С. 319-320.

14. Cuomo M.K. Synchronization of Lorenz-based chaotic circuits with application to communications. / M.K. Cuomo, A.V. Oppenheim, S.H. Strogatz. // IEEE Trans. Circuits and Syst., 1993. – Vol.40, №10. – P. 626.

15. Kocarev L. Experimental demonstration of secure communications via chaotic synchronization. / L. Kocarev, K.S. Halle, K. Eckert, L. Chua, U. Parlitz. // Int. J. Bifurcation and Chaos. 1992. – Vol.2, №3. – P.709-713.

16. Parlitz U. Transmission of digital signal by chaotic synchronization. / U. Parlitz, L.O. Chua, Lj. Kocarev, K.S. Halle, A. Shang. // Int. J. Bifurcation and Chaos. 1992. – Vol.2, №4. – P.973-977.

17. Hramov A.E. Generalized synchronization: A modified system approach. / A.E. Hramov, A.A. Koronovskii. // Physical Review. – 2005. – Vol. 71, № 6. – P. 201.

18. Boccaletti S. Adaptive synchronization of chaos for secure communication / S. Boccaletti, B. Farini, F.T. Arecchi // Phys. Rev. E. 1997. – V. 55. – № 5. – P. 4979– 4981.

19. Mossayebi F. Adaptive estimation and synchronization of chaotic systems / F. Mossayebi, H.K. Qammar , T.T. Hartley // Phys. Lett. A. – 1991. – V. 161. – P. 255–262.

20. Hayes S. Communication with chaos. / S. Hayes, C. Grebogy, E. Ott. // Physical Review. Lett. 1993. – Vol.70, №20. – P. 3031-3034.

21. 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. Oct. 1993. – V. CAS-40. – № 10. – P. 634.

22. Бельский Ю.Л. Передача информации с помощью детерминированного хаоса / Ю.Л. Бельский, А.С. Дмитриев // Радиотехника и электроника. – 1993. – Т. 38. – № 7. – С. 1310–1315.

23. Волковский А.Р. Синхронный хаотический отклик нелинейной системы передачи информации с хаотической несущей. / А.Р. Волковский, Н.В. Рульков // Письма в ЖТФ. – 1993.– Т. 19. – №. 3. – С. 71–75.

24. Дмитриев А.С. Эксперименты по передаче информации с использованием хаоса через радиоканал / А.С. Дмитриев, Л.В. Кузьмин, А.И. Панас, С.О. Старков // Радиотехника и электроника. – 1998. – Т. 43. – № 9. – С. 1115-1128.

25. Дмитриев А.С. Детерминированный хаос и информационные технологии / А.С. Дмитриев // Компьютерра. – 1998. – № 47(275). – С. 27–30.

26. Boccaletti S. Adaptive synchronization of chaos for secure communication / S. Boccaletti, B. Farini, F.T. Arecchi // Phys. Rev. E. 1997. – V. 55. – № 5. – P. 4979– 4981.

27. Mossayebi F. Adaptive estimation and synchronization of chaotic systems / F. Mossayebi, H.K. Qammar , T.T. Hartley // Phys. Lett. A. – 1991. – V. 161. – P. 255–262.

28. Chen J.Y. A secure communication scheme based on the phase synchronization of chaotic systems / J.Y. Chen, K.W. Wong, L.M. Cheng // Chaos: An Interdisciplinary Journal of Nonlinear Science. – 2003 – Volume 13, Issue 2.

29. Rosenblum Michael G. From Phase to Lag Synchronization in Coupled Chaotic Oscillators / Michael G. Rosenblum, Arkady S. Pikovsky, Jürgen Kurths // Phys. Rev. Lett. – 1997. – Vol. 78, num. 22. – P. 4193-4196.

30. Pyragas K. Weak and strong synchronization of chaos / K. Pyragas // Phys. Rev. – 1996 – Vol. 54(5). – P. 4508-4511.

31. Hramov A.E. Generalized synchronization onset / A.E. Hramov, A.A. Koronovskii, O.I. Moskalenko // Europhys. Lett., 2005. – 72 (6). – P. 901-907.

32. Terry J.R. Chaotic communication using generalized synchronization / John R Terry, Gregory D VanWiggeren // Chaos, Solitons & Fractals, 2001. – Vol. 12, Iss. 1. – P. 145-152.

33. Murali K. Secure communication using a compound signal from generalized synchronizable chaotic systems / K. Murali, M. Lakshmanan // Physics Letters A, 1998. – Volume 241, Iss. 6. – P. 303-310.

34. Koronovskii A.A. On the use of chaotic synchronization for secure communication / A.A. Koronovskii, O.I. Moskalenko, A.E. Hramov // Uspekhi Fizicheskikh Nauk, Physics-Uspekhi. – 2009. – Volume 52, Number 12.

35. Chua L.O. The Double Scroll Family / L.O. Chua, M. Komuro, T. Matsumoto // IEEE Transactions on Circuits & Systems, 1986. – Vol. CAS-33, no. 11. – P. 1073-1118.

36. Кузнецов С.П. Сложная динамика генераторов с запаздывающей обратной связью (обзор) / С.П. Кузнецов // Известия вузов. Радиофизика. – 1982. – Т. 25, № 12. – С. 1410-1428.

37. Шалфеев В.Д. Динамический хаос в ансамблях связанных фазовых систем / В.Д. Шалфеев, В.В. Матросов, М.В. Корзинова // Зарубежная радиоэлектроника. Успехи современной радиоэлектроники. – 1998. – № 11. – С. 44-56.

38. Yang T. Secure communication via chaotic parameter modulation / T. Yang, L.O. Chua // IEEE Trans. on Circ. Sys. – I. 43. – 1996. – P. 817.

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	3	
4	А4	Вступ	2	
5	А4	Стан питання. Постановка задачі	32	
6	А4	Спеціальна частина	26	
7	А4	Економічний розділ	9	
8	А4	Висновки	2	
9	А4	Перелік посилань	4	
10	А4	Додаток А	1	
11	А4	Додаток Б	1	
12	А4	Додаток В	1	
13	А4	Додаток Г	1	

ДОДАТОК Б. Перелік документів на оптичному носії

1 Презентація Ахмєдов.ppt

2 Диплом Ахмєдов.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-20-2 Ахмєдова Ахмеда Анара огли

на тему: «Забезпечення конфіденційності в системах передачі інформації з використанням хаотичних коливань»

Пояснювальна записка складається зі вступу, трьох розділів і висновків, розташованих на 87 сторінках.

Мета роботи є актуальною, оскільки вона спрямована на забезпечення більш високого ступеня захисту інформації при її передачі в системах передачі інформації з використанням хаотичних коливань.

При виконанні роботи автор продемонстрував добрий рівень теоретичних знань і практичних навичок. На основі аналізу шляхів передачі інформації в системах зв'язку з використанням хаотичних коливань, а також існуючих схем і підходів в ній сформульовані задачі, вирішенню яких присвячений спеціальний розділ. У ньому було обґрунтовано і досліджено підхід до прихованої передачі з підвищеною стійкістю до шумів на основі узагальненої хаотичної синхронізації, а також оцінено його ефективність у середовищі Matlab за допомогою стандартних і розроблених програм.

Практична цінність роботи полягає в тому, що досліджений підхід може бути використаний в системах передачі інформації для підвищення стійкості до шумів і нелінійних спотворень каналу зв'язку.

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

В цілому робота задовольняє усім вимогам, а її автор Ахмєдов Ахмед Анар огли заслуговує на оцінку « » та присвоєння кваліфікації «Магістр з кібербезпеки» за спеціальністю 125 Кібербезпека.

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