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

Інститут електроенергетики
Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеня бакалавра

студента *Кроленко Владислав Миколайович*

академічної групи *125-17-1*

спеціальності *125 Кібербезпека*

спеціалізації[1]

за освітньо-професійною програмою *Кібербезпека*

на тему *Забезпечення конфіденційності при передачі інформації в системах зв'язку з використанням динамічного хаосу*

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
2021

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

«_____»_____20___року

ЗАВДАННЯ
на кваліфікаційну роботу
ступеня бакалавра

студенту ***Кроленко Владислав Миколайович*** **академічної групи** ***125-17-1***
(прізвище ім'я по-батькові) (шифр)

спеціальності ***125 Кібербезпека***

за освітньо-професійною програмою ***Кібербезпека***

на тему ***Забезпечення конфіденційності при передачі інформації в системах зв'язку з використанням динамічного хаосу***

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

Розділ	Зміст	Термін виконання
Розділ 1	Аналіз принципів застосування хаотичних широкосмугових сигналів у системах прихованої передачі інформації, а також існуючих підходів до прихованої інформації в таких системах.	25.02.2021 – 31.03.2021
Розділ 2	Розробка підходу до прихованої передачі інформації, заснованого на явищах узагальненої хаотичної синхронізації і синхронізації, індукованої шумом та оцінка його ефективності.	01.04.2021 – 12.05.2021
Розділ 3	Розрахунки капітальних витрат, витрат на експлуатацію системи безпеки та термін окупності інвестицій застосування запропонованого підходу.	13.05.2021 – 09.06.2021

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

Дата видачі: _____

Дата подання до екзаменаційної комісії: _____

Прийнято до виконання _____ Кроленко В.М.
(підпис студента) (прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 75 с., 14 рис., 4 додатки, 33 джерела.

Об’єкт розробки – детерміновані хаотичні сигнали.

Предмет розробки – підхід до прихованої передачі інформації в системах зв’язку з використанням динамічного хаосу.

Мета кваліфікаційної роботи – підвищення надійності і створення додаткової секретності.

Наукова новизна результатів полягає у тому, що шумовий сигнал, вироблений генератором шуму, забезпечує відсутність слідів модуляції керуючих параметрів, а отже, і додаткове маскування переданого по каналу зв'язку сигналу, тим самим перешкоджаючи третій стороні декодувати інформаційне повідомлення, що гарантує конфіденційність запропонованого підходу.

У першому розділі проаналізовано принципи застосування хаотичних широкосмугових сигналів у системах прихованої передачі інформації, а також існуючі підходи до прихованої передачі інформації в системах зв’язку з використанням динамічного хаосу.

У спеціальній частині роботи запропоновано підхід до прихованої передачі інформації, заснований на явищах узагальненої хаотичної синхронізації і синхронізації, індукованої шумом та оцінено його ефективність. За наслідками досліджень зроблено висновки щодо рішення поставленої задачі.

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

СИНХРОНІЗАЦІЯ, ІНДУКОВАНА ШУМОМ, СИСТЕМА РЕСЛЕРА, ДЕТЕРМІНОВАНІ ХАОТИЧНІ СИГНАЛИ, ПРИХОВАНА ПЕРЕДАЧА ІНФОРМАЦІЇ, УЗАГАЛЬНЕНА ХАОТИЧНА СИНХРОНІЗАЦІЯ, ІМІТАЦІЙНЕ МОДЕЛЮВАННЯ

РЕФЕРАТ

Пояснительная записка: 75 с., 14 рис., 4 приложения, 33 источника.

Объект разработки – детерминированные хаотические сигналы.

Предмет разработки – подход к скрытой передачи информации в системах связи с использованием динамического хаоса.

Цель квалификационной работы – повышение надежности и создание дополнительной секретности.

Научная новизна заключается в том, что шумовой сигнал, производимый генератором шума, обеспечивает отсутствие следов модуляции управляющих параметров, а следовательно, и дополнительную маскировку передаваемого по каналу связи сигнала, тем самым препятствуя третьей стороне декодировать информационное сообщение, что гарантирует конфиденциальность предложенного подхода.

В первой главе проанализированы принципы применения хаотических широкополосных сигналов в системах скрытой передачи информации, а также существующие подходы к скрытой передачи информации в системах связи с использованием динамического хаоса.

В специальной части работы предложен подход к скрытой передачи информации, основанный на явлениях обобщенной хаотической синхронизации и синхронизации, индуцированной шумом и оценена его эффективность. По результатам исследований сделаны выводы относительно решения поставленной задачи.

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

СИНХРОНИЗАЦИЯ, ИНДУЦИРОВАННАЯ ШУМОМ, СИСТЕМА РЕССЛЕРА, ДЕТЕРМИНИРОВАННЫЕ ХАОТИЧЕСКИЕ СИГНАЛЫ, СКРЫТАЯ ПЕРЕДАЧА ИНФОРМАЦИИ, ОБОБЩЕННАЯ ХАОТИЧЕСКАЯ СИНХРОНИЗАЦИЯ, ИМИТАЦИОННОЕ МОДЕЛИРОВАНИЕ

ABSTRACT

Explanatory note: p. 75, fig. 14, 4 additions, 33 sources.

The object of development is deterministic chaotic signals.

The subject of development is an approach to covert transmission of information in communication systems using dynamic chaos.

The purpose of the qualification work is to increase reliability and create additional secrecy.

The scientific novelty of the results is that the noise signal generated by the noise generator provides no traces of modulation of the control parameters, and hence additional masking of the signal transmitted over the communication channel, thereby preventing a third party from decoding the information message, ensuring confidentiality of the proposed approach .

The first section analyzes the principles of application of chaotic broadband signals in latent information transmission systems, as well as existing approaches to latent information transmission in communication systems using dynamic chaos.

The special part of the work proposes an approach to covert transmission of information, based on the phenomena of generalized chaotic synchronization and synchronization, induced by noise and evaluates its effectiveness. Based on the results of research, conclusions were made regarding the solution of the problem.

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

NOISE-INDUCED SYNCHRONIZATION, RESLER SYSTEM, DETERMINED CHAOTIC SIGNALS, HIDDEN TRANSMISSION OF INFORMATION, GENERALIZED GENERALIZATION, SIMULATION MODELING

СПИСОК УМОВНИХ СКОРОЧЕНЬ

ДС – Динамічна система;

НВЧ – Надвисокочастотний;

ППІ – Прихована передача інформації;

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

ЗМІСТ

ВСТУП

Відкриття детермінованого хаосу призвело до швидкого зростання фундаментальних і прикладних наукових досліджень, що дозволило описати поведінку цього нелінійного явища. Чутливість до початкових умов і можливість синхронізації хаотичних коливань дозволяють використовувати детермінований хаос в інформаційних системах.

Наразі, більшість робіт, пов'язаних з використанням хаосу в системах зв'язку, можна розділити на наступні чотири групи:

• загальні властивості хаотичних коливань — включають роботи, присвячені генераторам хаосу різних розмірностей і фундаментальні дослідження нових властивостей детермінованого хаосу;

• синхронізація і контроль хаосу — включають дослідження, що аналізують можливість синхронної хаотичної поведінки зв'язаних систем та керування ними;

• хаотична криптографія — включають дослідження з використанням хаотичної динаміки для створення криптосистем на основі хаосу: аналогового і цифрового;

• інформаційні системи з детермінованим хаосом — включають всі види хаотичних систем зв'язку для аналогової та цифрової передачі. Деякі з них включають хаотичні системи зв'язку на основі символічної динаміки.

Наразі відомо декілька різних типів хаотичної синхронізації: фазова синхронізація, узагальнена синхронізація, повна синхронізація, синхронізація із запізненням та синхронізація, індукована шумом. 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.

Режим узагальненої синхронізації має багато подібностей із режимом синхронізації, індукованої шумом, як по методам діагностики, так і за

механізмами виникнення синхронного режиму. Тому ці два типи синхронної поведінки іноді розглядає як єдиний тип синхронної хаотичної динаміки пов'язаних динамічних систем, причому це узагальнення стосується як систем з малим числом ступенів свободи, так і просторово-розподілених середовищ.

У той же самий час, в хаотичних системах синхронізація, індукована шумом, може спостерігатися далеко не завжди. Для цього хаотичні системи повинні мати певні властивості, такі, як сильне стиснення фазового обсягу в фазовому просторі, обмежена область фазового простору, де спостерігається збільшення фазового обсягу та інші. Отже, хаотичних систем, здатних демонструвати цей режим, виявляється досить багато. Більш того, якщо в системах, здатних демонструвати режим узагальненої синхронізації, замінити детерміноване вплив на випадковий, то в таких системах буде спостерігатися режим індукованої шумом синхронізації.

Таким чином, вдосконалення підходів до прихованої передачі інформації в системах зв’язку з використанням динамічного хаосу наразі є актуальною задачею.

Метою роботи є підвищення надійності і створення додаткової секретності.

Постановка задачі:

• проаналізувати принципи застосування хаотичних широкосмугових сигналів у системах прихованої передачі інформації;

• провести аналіз існуючих підходів до прихованої передачі інформації в системах зв’язку з використанням динамічного хаосу;

• запропонувати підхід до прихованої передачі інформації, заснований на явищах узагальненої хаотичної синхронізації і синхронізації, індукованої шумом;

• оцінити ефективність запропонованого підходу.

1 СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ

1.1 Застосування хаотичних широкосмугових сигналів у системах прихованої передачі інформації

1.1.1 Теоретичні засади моделювання телекомунікаційних систем передавання інформації з використанням динамічного хаосу

Однією із властивостей генераторів хаотичних коливань, що представляють інтерес і можуть бути використані у системах передавання інформації, є їх синхронізація [1-18].

Суть явища синхронізації систем полягає в тому, що фазові траєкторії двох або більше систем після закінчення перехідних процесів будуть однаковими.

Численні дослідження обумовили низку визначень поняття «синхронізація». Зокрема вважається, що повна синхронізація (complete, full, identique synchronization) з'єднаних ідентичних систем – це такий тип синхронізації, при якому має місце рівність усіх однотипних змінних стану систем. З точки зору теорії систем явище синхронізації передбачає принаймні дві системи, що задіяні в цьому процесі.

Синхронізовані системи розрізняють за способом передавання сигналу синхронізації між ними. Перший тип з'єднання полягає у тому що одна із систем не має на своєму вході сигналу з іншої, а конфігурація, що утворена при такому способі з'єднання систем називається однонаправленим з'єднанням або з'єднанням типу «головна-керована системи». Другий тип з'єднання, що називається двонаправленим, передбачає подачу сигналу із виходу однієї системи на вхід іншої і навпаки, тобто системи є рівноцінними за типом з'єднання.

Відкриття Каролем та Пекорою синхронізації систем із хаотичною динамікою відносять до 1990 р. Виникнення цього явища у електронних

пристроях та системах стало початком епохи розроблення систем передавання інформації із його використанням. Дослідженнями останніх десятиліть була показана можливість використання синхронізованих систем із псевдовипадковими коливаннями для кодування інформації, криптографічного захисту та використання псевдовипадковго сигналу в якості переносника [1-18].

До базових технологій синхронізації псевдовипадкових коливань необхідно віднести методи повного заміщення, адаптивної та імпульсної синхронізації.

Метод повного заміщення, що був винайдений і досліджений Каролем та Пекорою, базується на декомпозиції деякої системи на головну та керовану. На думку авторів при цьому вдається уникнути небажаної надзвичайної чутливості до початкових умов виникнення коливань, що можуть бути різними для різних систем.

Якщо обидві системи є частиною однієї, то умови виникнення коливань у них будуть майже однаковими. У даному випадку вихідні сигнали однієї з підсистем є вхідними сигналами для іншої. Отже, перша підсистема є головною, а друга – керованою. Зв'язок між системами є однонаправленим, тобто керована система не впливає на головну. Математична модель цього методу передбачає розділення змінних фазового простору на дві групи. Перша група описує головну, а друга – керовану системи.

Метод адаптивного контролю передбачає наявність головної та керованої систем (рис.1.1). Особливість цього методу полягає у тому, що керована система має коло оберненого зв'язку, а сигнал, що подається на вхід керованої системи є пропорційним різниці між сигналом на виході головної системи та сигналом оберненого зв’язку керованої системи. Якщо синхронізація має місце, то сигнал у колі зворотного зв'язку відсутній.

Як бачимо із приведеної схеми у методі адаптивного контролю рівень сигналу синхронізації залежить від ступеня синхронізованості головної та керованої систем, що забезпечує покращення синхронізації. Механізм роботи цієї схеми є подібним до механізму роботи схеми генератора, керованого

напругою (різниця між двома сигналами є коливанням збурення у системі, чим менше її значення, тим більше коливання наближені за формою до еталонного, і навпаки).

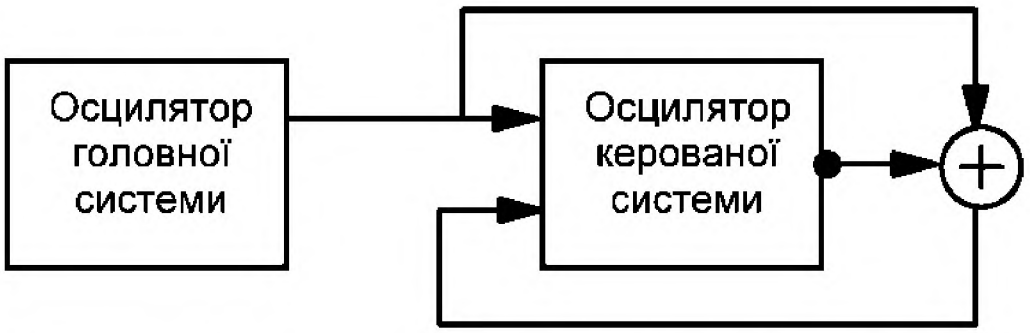


Рисунок 1.1 – Схема адаптивної синхронізації двох систем

Третім методом синхронізації є імпульсна синхронізація (рис.1.2).

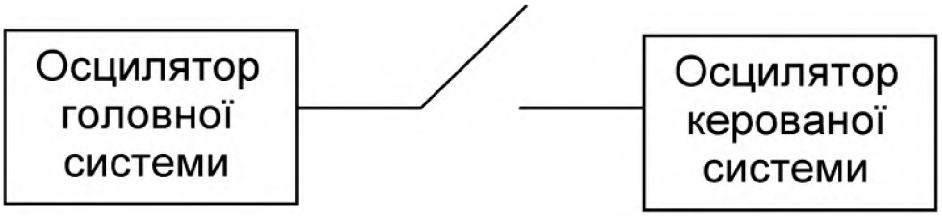


Рисунок 1.2 – Схема імпульсної синхронізації двох систем (Т1 – тривалість верхнього стану ключа, Т2 – тривалість нижнього стану ключа)

Метод імпульсної синхронізації характеризується додатковими параметрами – тривалістю та періодами імпульсів. За даними деяких авторів [1-18] імпульсна синхронізація є більш ефективною в умовах дії завад, що пояснюється ослабленням їх впливу за рахунок обмеженого часового інтервалу їх дії.

При розробленні телекомунікаційних систем, що використовують явище синхронізації псевдовипадкових коливань необхідно виконати наступні процедури:

- вибрати та сконструювати системи із псевдовипадковою динамікою, які необхідно синхронізувати;

- встановити граничні умови та швидкість синхронізації;

- дослідити стійкість синхронізації до впливу зовнішніх факторів (інтерференція, фільтрування, зовнішній шум);

- вивчити вплив параметрів систем на процес синхронізації;

- забезпечити унеможливлення відтворення системи передавання шляхом спостереження сигналу, що передається (секретність системи);

- встановити моменти початку та закінчення кодової посилки;

- визначити момент початку/закінчення прийнятого символа в межах кодового слова (кодової посилки)

Незважаючи на те, що дослідженню систем із псевдовипадковою динамікою присвяченна низка робіт провідних вчених, актуальним залишається питання дослідження псевдовипадкових траєкторій та атракторів для систем четвертого і вищого порядку із нелінійними членами. Про це свідчать відкриття нових та вдосконалення уже існуючих систем із псевдовипадковою динамікою, що знаходять своє практичне втілення у системах прихованого передавання інформації [1-18].

Найбільш узагальнена класифікація систем, що використовують хаотичні коливання для передавання інформації приведена на рис.1.3.

Практична реалізація широкосмугових сигналів стала можливою тільки після досягнення відповідного рівня розвитку базових технологій для надширокосмугової радіоелектроніки:

- технології стабільного генерування потужних надкоротких (тривалістю 1 нс і коротших) імпульсів з практично необмеженим ресурсом (набагато більшим 1010 імпульсів) та високою частотою повторення;

- технології випромінювання надкоротких імпульсів безпосередньо в ефір (надширокосмугова антенна техніка);

- технології формування надширокосмугових сигналів з будь-якою поляризаційною структурою;

- технології швидкісного цифрового оброблення великих масивів інформації (обчислювальна техніка).

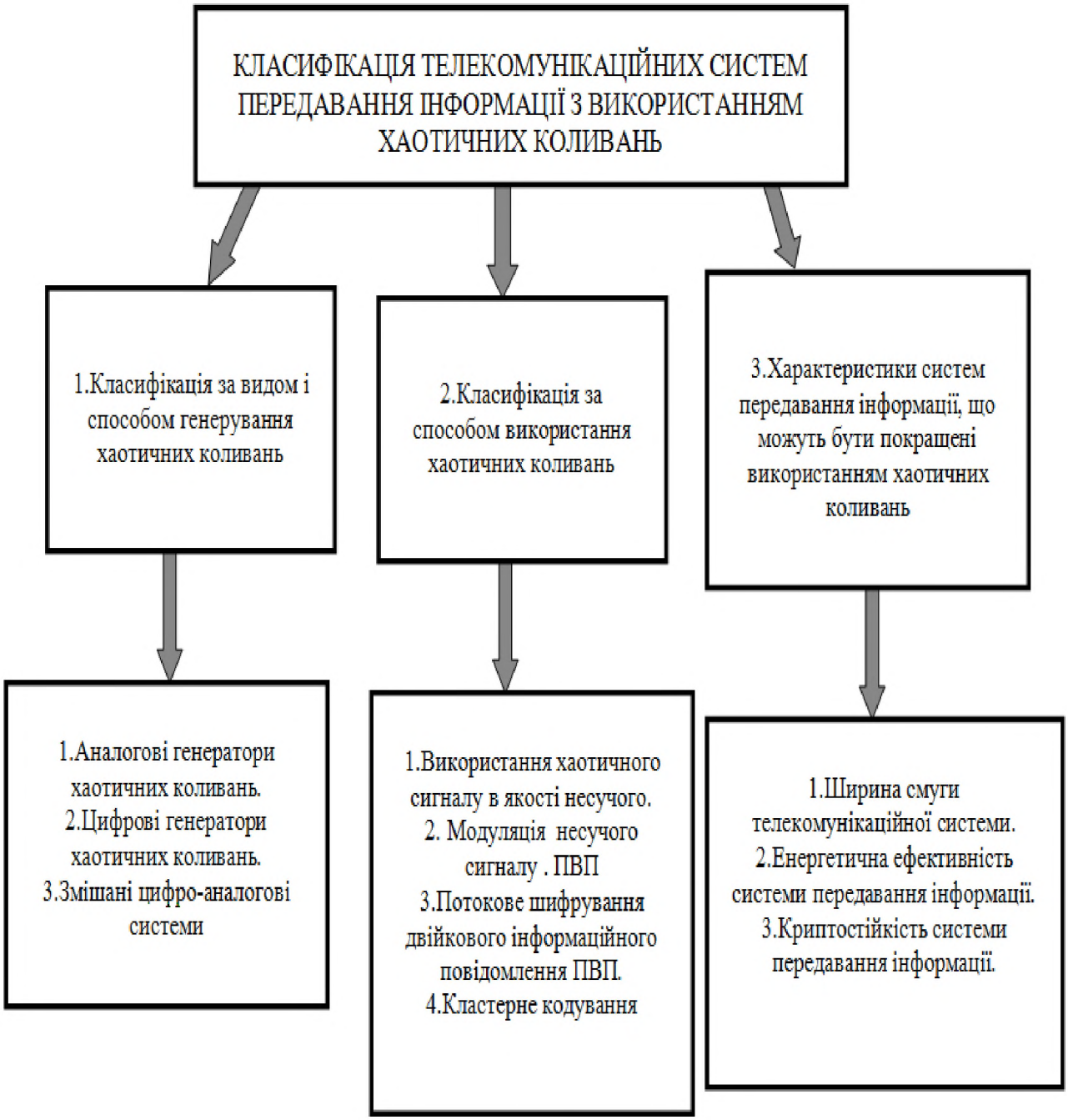


Рисунок 1.3 – Класифікація телекомунікаційних систем передавання інформації з використанням псевдовипадкових коливань

1.1.2 Передача інформації на основі явища детермінованого хаосу

Динамічний хаос є типовим коливальним режимом в багатьох нелінійних детермінованих системах, включаючи електронні [1-3]. Безліч різних

нетривіальних біфуркаційних явищ в системах з хаосом дозволяє сподіватися на можливість їх застосування в інформаційних технологіях. Хаотичні коливання можуть бути використані для передачі інформаційних повідомлень між нелінійною динамічною системою, що грає роль передавача, і нелінійною динамічною системою, яка виконує функцію приймача.

Структурна схема системи передачі і прийому інформації відображена на рис. 1.4. На схемі пунктиром обведені: передавач, який формує хаотичний сигнал, що несе інформацію, і приймач, який приймає сигнал, що передається і видобуває з нього інформацію. Передавач включає в себе модулятор і кільцевий генератор хаотичних коливань [1, 3], що складається з послідовно з'єднаних лінійного підсилювача – П, нелінійного елемента – НЕ, фільтра нижніх частот першого порядку $Ф^1$, фільтра нижніх частот другого порядку $Ф^2$. Формування інформаційного сигналу в передавачі здійснюється шляхом дискретного зміни одного з параметрів генератора. Вихідним сигналом передавача є коливання X_1 на виході фільтра $Ф^1$.

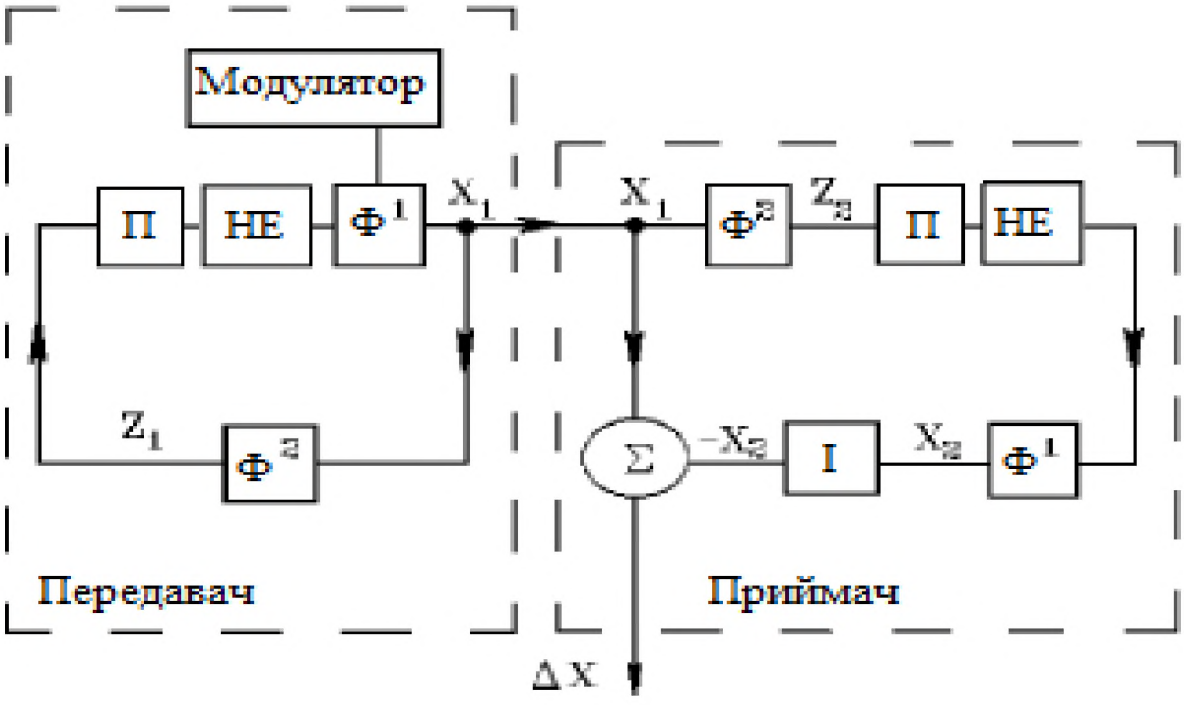


Рисунок 1.4 – Структурна схема системи передачі інформації

Основу приймача становить такий же генератор, але з розімкненим ланцюгом зворотного зв'язку.

Вихідний сигнал передавача подається на вхід фільтра $Ф^2$ приймача і далі проходить через підсилювач, нелінійний елемент, фільтр $Ф^1$ і інвертор І. Сигнал з виходу інвертора $(–X_2)$ підсумовується з сигналом X_1 в суматорі $\sum$. Передана інформація знімається з виходу цього суматора.

При співпадінні або близькості параметрів елементів $Ф^2$, У, НЕ, $Ф^1$, що входять в передавач і приймач, відбувається синхронізація сигналів X_1 і X_2, тобто після перехідного процесу вони стають однаковими. Якщо ж ці параметрі розрізняються, то синхронізація не відбувається.

У разі синхронізації сигналів X_1 і X_2, сигнал на виході суматора ΔX буде дорівнювати нулю, а в разі відсутності синхронізації на виході суматора буде мати місце хаотичний сигнал.

Під синхронізацією розуміють ситуацію, коли траєкторія однієї з систем сходиться до тих же самих значень, що й траєкторія іншої системи. Надалі ці траєкторії збігаються, і цей стан є стійким по відношенню до збурень. При такому розумінні явища синхронізації можна розглядати синхронізацію не тільки регулярних, але й хаотичних сигналів.

При побудові реальних комунікаційних каналів на основі хаосу, потрібно враховувати, що:

- хаотичні системи зв'язку будуть застосовуватися тільки там і тільки в тому випадку, коли вони будуть мати сукупність властивостей, які роблять їх конкуренто спроможними по відношенню до інших типів систем. У список цих властивостей можуть входити швидкість передачі інформації, простота і вартість системи, стійкість роботи в конкретних умовах, множинний доступ, можливість задоволення певними правилами частотного регулювання і т.д.;

- техніка передачі інформації за допомогою хаотичних сигналів знаходиться в початковій фазі, і ефективні інженерні рішення досить обмежені по елементній базі.

Основним елементом хаотичної системи зв'язку є генератор хаосу. В окремих випадках розглядаються схеми зв'язку, що використовують хаос як проміжний носій. У разі прямохаотичного зв'язку мова йде про генератори хаосу радіо- і надвисокочастотних (НВЧ) діапазонів.

Наразі відомий ряд динамічних систем, які демонструють хаотичну поведінку[3]. При цьому sз урахуванням можливостей сучасних технологій створити на їх основі генератор хаосу – завдання не настільки просте й тривіальна в силу наступних обставин:

1) необхідна не просто динамічна система, яка породжує хаос, а система, яка породжує хаос з певними, як мінімум спектральними властивостями; наприклад, система, яка породжує хаос з відносно рівномірною спектральною щільністю в заданому діапазоні частот;

2) це повинна бути система, що реалізується на більш-менш стандартних елементах, які використовуються в радіотехніці;

3) це повинна бути система, яка генерує хаос на високих або дуже високих частотах, можливо близьких до граничних характеристик використовуваної технології;

4) можуть бути додаткові обмеження з боку технології, наприклад, вимога, щоб системи була реалізована на CMOS (Complementary metal-oxide-semiconductor) технології.

Прямохаотичною схемою зв'язку називається [4] схема, в якій:

- джерело хаосу генерує хаотичні коливання безпосередньо в заданій смузі радіо- або НВЧ-діапазону;

- введення інформаційного сигналу в хаотичний здійснюється шляхом формування відповідного потоку хаотичних радіоімпульсів;

- вилучення інформації з НВЧ сигналу проводиться без проміжного перетворення частоти.

У прямохаотичних системах зв'язку можуть використовуватися різні види модуляції: наявність або відсутність хаотичного імпульсу на інформаційній позиції, відносна хаотична маніпуляція, модуляція позицій імпульсів і т.д.

Істотно, що для передачі інформації тут використовується не безперервний сигнал, а потік імпульсів. Тому, поряд з методом модуляції важливими характеристиками є довжина імпульсу і скважність. Варіація цих характеристик й визначає швидкісні властивості системи зв'язку і її стійкість для різних типів каналів зв'язку.

1.1.3 Інформація та динамічні системи

Дослідження систем з детермінованим хаосом також свідчить про тісний зв'язок між теорією динамічних систем і інформаційними процесами [3]. Ряд основних результатів динамічної теорії формулюється стосовно об'єктів, пов'язаних з інформацією. У теоремі А.Н. Шарковського мова йде про існування рахункового числа циклів з фіксованою структурою в динамічних системах типу одновимірного відображення.

Рахункові множини періодичних рухів виникають і в системах з безперервним часом. Для опису характеру поведінки таких систем використовується апарат символічної динаміки, основами якого є поняття складності та інформації. Прокаччі І. висловив ряд ідей, що вказують на зв'язок між хаосом, нестійкими періодичними орбітами і інформаційними властивостями динамічних систем.

Перша ідея полягає в тому, що хаотичні орбіти можуть бути організовані навколо скелета нестійких періодичних орбіт.

Друга ідея показує, що кожна періодична орбіта (точка) може бути універсально закодована. Апарат, який використовується для кодування, – символічна динаміка.

Третя ідея виходить з того, що існує граматика, яка визначає дозволені слова або періодичні орбіти. Показано, що граматика може бути універсальною. Поняття універсальності полягає у тому, що різні системи, що належать одному і тому ж універсального класу, у відповідних точках простору параметрів будуть мати один і той же розподіл періодичних орбіт.

Четверта ідея полягає в припущенні про існування зв'язку між періодичними точками і їх власними значеннями, з одного боку, і метричними властивостями дивного атрактора, – з іншого. Хаотичний рух розглядається автором як випадкове блукання між періодичними орбітами, кожна з яких вносить вклад у відповідні ймовірності відвідування. Чим більше нестійка періодична орбіта, тим менше її ймовірність.

П'ята ідея передбачає, що періодичні орбіти і їх власні значення можна витягти безпосередньо з експериментальних сигналів.

1.1.4 Способи побудови систем прихованої передачі інформації, заснованих на явищі хаотичної синхронізації

Розглянемо в якості основи для реалізації систем прихованої передачі інформації (ППІ) режим повної синхронізації, оскільки більшість відомих способів і пристроїв засноване саме на цьому типі синхронної поведінки [3].

Використання повної хаотичної синхронізації для прихованої передачі інформації має на увазі наявність, як мінімум, двох однонаправлено пов'язаних ідентичних хаотичних генераторів. Запропоновано досить багато таких способів прихованої передачі даних. Це, у першу чергу, хаотичне маскування [5], перемикання хаотичних режимів [6], нелінійне підмішування інформаційного сигналу до хаотичного [7], модулювання керуючих параметрів передавального генератора корисним цифровим сигналом [8] та ін. На основі цих методів було запропоновано безліч способів прихованої передачі даних. Тому розгляд основних принципів роботи таких схем є дуже важливим.

1.1.4.1. Хаотичне маскування.

Хаотична маскування – один з перших і найбільш простих способів прихованої передачі даних [2, 3, 5]. Принципова схема реалізації цього способу приведена на рис. 1.5.

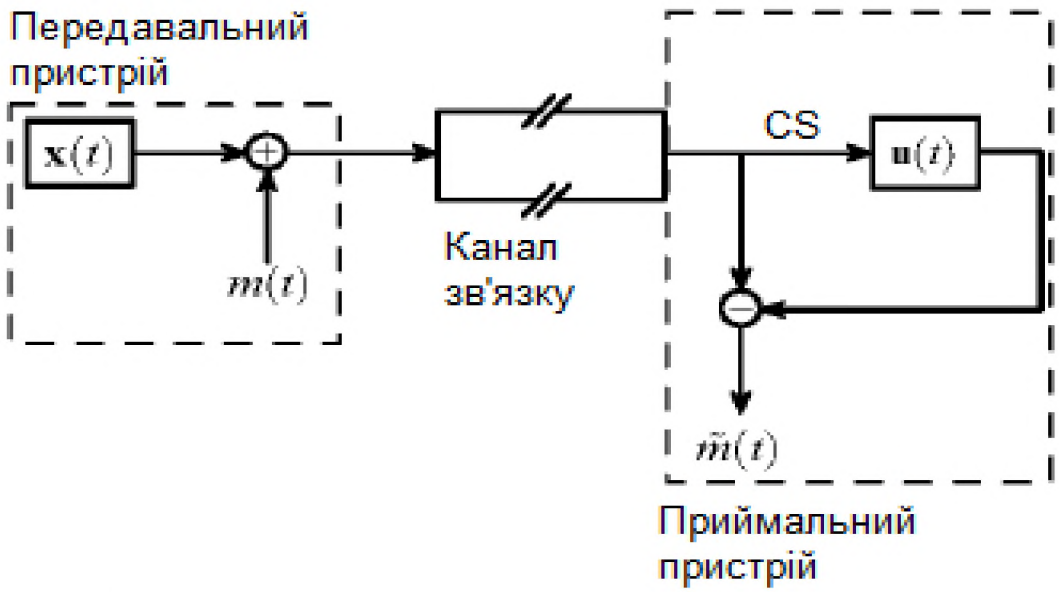


Рисунок 1.5 – Схема прихованої передачі інформації за допомогою хаотичного маскування (CS – повна хаотична синхронізація)

На передавальній стороні інформаційний сигнал m(t) підмішується в суматорі до несучого сигналу, що генерується передавальною хаотичною системою x(t), і далі передається по каналу зв'язку (рис. 1.2). У приймальному пристрої здійснюється повна хаотична синхронізація хаотичного генератора **u**(t), що знаходиться в ньому, за допомогою сигналу, в результаті чого динаміка приймального генератора стає ідентичною динаміці передавального. Детектувати сигнал $\tilde{m}$ виходить після проходження через віднімаючий пристрій як різниця між отриманим сигналом і синхронним відгуком генератора хаосу в приймальному пристрої.

Така схема прихованої передачі даних працює досить ефективно (тобто дозволяє якісно передавати інформацію та детектувати її на виході) в відсутності шумів в каналі зв'язку у тому випадку коли потужність сигналу, що генерується передавальної системою, перевищує потужність інформаційного сигналу на 35-65 дБ. Додавання шуму в канал зв'язку призводить до різкого погіршення якості переданої інформації і до високих відносин сигнал / шум, при яких схема залишається працездатною. Введення розладу керуючих параметрів між ідентичними хаотичними генераторами (що знаходяться на

різних сторонах каналу зв'язку) також призводить до появи на виході додаткових шумів десинхронізації і робить передачу інформації важко реалізовуваною. Існує також проблема конфіденційності передачі інформації. Незважаючи на низький рівень інформаційного сигналу у порівнянні з рівнем несучої, існують методи і підходи, що дозволяють відновити початковий хаотичний сигнал по сигналу, що передається по каналу зв'язку, і виділити корисну інформацію.

Слід зазначити, що всі вищевказані недоліки роблять схеми прихованої передачі інформації на основі хаотичного маскування маловживаними на практиці.

1.1.3.2. Перемикання хаотичних режимів.

Одна зі схем ППІ на основі перемикання хаотичних режимів приведена на рис. 1.6.

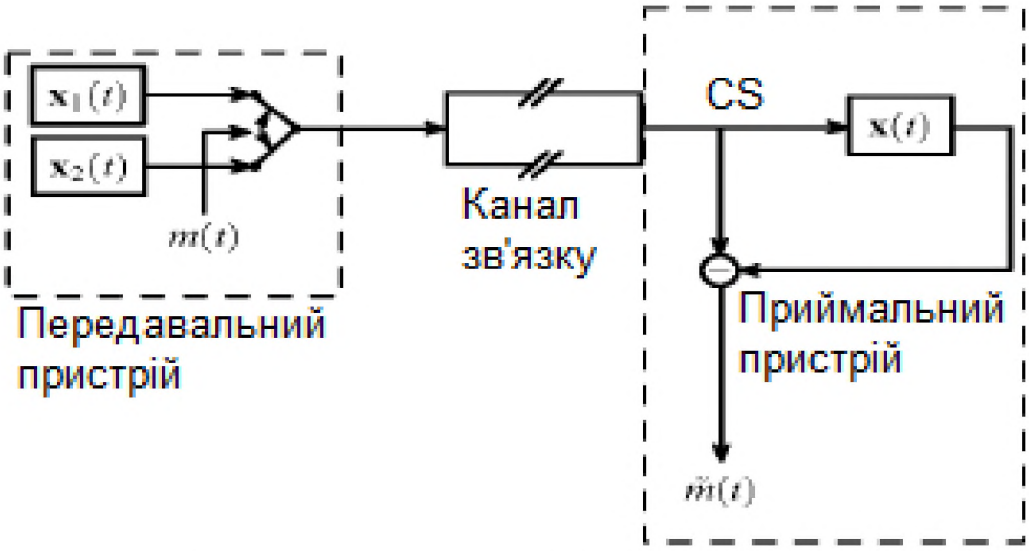


Рисунок 1.6 – Схема прихованої передачі інформації на основі перемикання хаотичних режимів

Передавальний пристрій містить два хаотичних генератора, $x_1(t)$ і $x_2(t)$, які можуть бути різними або однаковими, але з параметрами, які відрізняються, однак в інтересах конфіденційності передачі даних краще використовувати

останні; більш того, сигнали, які генеруються цими системами повинні мати подібні спектральні і статистичні властивості. Корисний цифровий сигнал m(t), представлений послідовністю бінарних бітів 0/1, використовується для перемикання сигналу, що передається, тобто сигнал, вироблений першим хаотичним генератором, кодує, наприклад, бінарний біт 0, а сигнал від другого генератора хаосу відповідно – бінарний біт 1. Отриманий таким чином сигнал передається по каналу зв'язку на приймаючий пристрій.

В залежності від числа генераторів, що знаходяться на приймальній стороні каналу зв'язку, розрізняють декілька схем прихованої передачі даних на основі перемикання хаотичних режимів. У схемі, представленій на рис. 1.6, приймальний пристрій містить один хаотичний генератор x(t), ідентичний будь-якому з передавальних, наприклад першому. Параметри генераторів повинні бути обрані таким чином, щоб сигнали, які генеруються ними, призводили до виникнення режиму повної хаотичної синхронізації лише у тому випадку, якщо передається тільки бінарний біт 0 (або тільки бінарний біт 1). Так само як і при хаотичному маскуванні, відновлений сигнал $\tilde{m}$ отримують після проходження через віднімаючий пристрій сигналу, що передається по каналу зв'язку, і синхронного відгуку хаотичного генератора пристрою отримувача.

Інші схеми прихованої передачі інформації з використанням перемикання хаотичних режимів, які засновані на тій же ідеї, відрізняються від описаної вище схеми тільки будовою і роботою пристрою отримувача. Наприклад, приймальний пристрій може містити два хаотичних генератора, ідентичних передавальним генераторам, і, отже, два віднімаючих пристроїв для детектування корисного сигналу. У цьому випадку корисний сигнал діагностується за наявністю або відсутністю хаотичних коливань в сигналах на виході приймального пристрою.

1.1.3.3. Нелінійне підмішування інформаційного сигналу до хаотичного.

Серед схем, в яких застосовуються різні операції («складання – віднімання», «ділення – множення», «складання по модулю з основою 2»,

«перетворення напруга - струм» і ін.), найбільшого поширення наразі отримали схеми, що використовують «складання – віднімання». В таких схемах інформаційний сигнал підмішується до хаотичного і бере участь у формуванні складної поведінки системи. Найбільш простим і технічно реалізованим способом забезпечення «нелінійного підмішування» є установка на передавальній стороні каналу зв'язку додаткового хаотичного генератора, ідентичного першому передавальному і взаємно пов'язаного з ним.

Принципова схема реалізації прихованої передачі інформації на основі нелінійного підмішування інформаційного сигналу до хаотичного наведена на рис. 1.7.

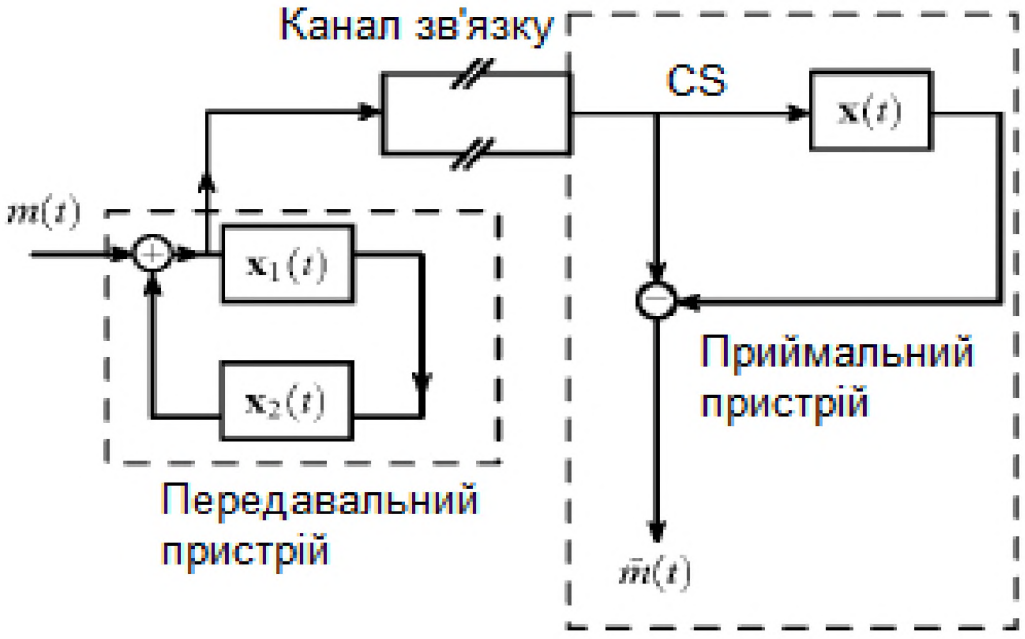


Рисунок 1.7 – Схема прихованої передачі інформації на основі нелінійного підмішування інформаційного сигналу до хаотичного

Отже, передавальна сторона містить два ідентичних по керуючим параметрам хаотичних генератора, $x_1(t)$ і $x_2(t)$. Інформаційний сигнал m(t) підмішується до сигналу, виробленому одним з генераторів передавального пристрою (або до обох сигналів одночасно). В результаті проходження по кільцю зворотного зв'язку (забезпечується взаємним зв'язком генераторів передавального пристрою) сигнал зазнає нелінійні зміни. Таким чином, по

каналу зв'язку буде передаватися сигнал, отриманий в результаті нелінійного підмішування інформаційного сигналу до хаотичного. Приймальний пристрій містить хаотичний генератор x(t), ідентичний по керуючим параметрам передавальним генераторам.

Сигнал, що надходить по каналу зв'язку на приймаючий пристрій, синхронізує приймальний генератор в разі передачі бінарного біта 0 (і не синхронізує при передачі бінарного біта 1).

Після проходження через віднімаючий пристрій сигналів від передавального і приймаючої генераторів детектується відновлений сигнал $\widetilde{m}$.

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 складновирішуєме технічне завдання 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.

1.1.3.4. Модулювання керуючих параметрів передавального генератора інформаційним сигналом.

Схеми на основі модулювання керуючих параметрів, або адаптивні методи, – природний етап при переході від дискретної модуляції керуючого параметра передавального генератора в схемі з перемиканням хаотичних

режимів до модуляції безперервним сигналом [2, 3]. При цьому роль модулюючого сигналу грає інформаційний сигнал.

Слід зазначити, що необхідною умовою реалізації схем на основі модулювання керуючих параметрів є попереднє визначення допустимого діапазону зміни параметра і нормування модулюючого інформаційного сигналу. Окремим випадком є використання бінарного цифрового сигналу в якості інформаційного та модулювання їм керуючого параметра передавального генератора.

Схема прихованої передачі інформації шляхом модулювання керуючих параметрів передавального генератора інформаційним сигналом наведена на рис. 1.8 [2, 3].

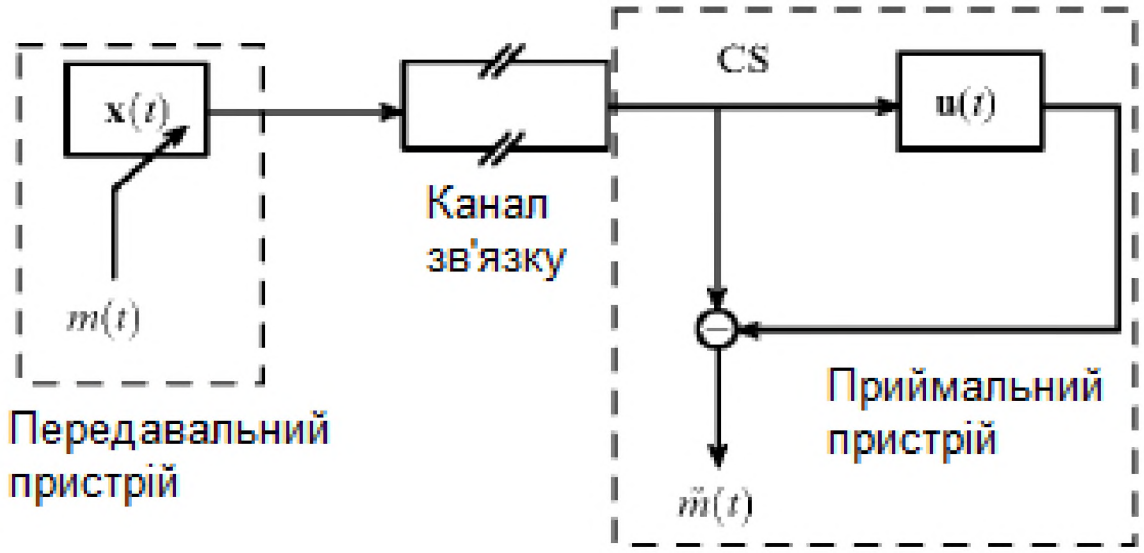


Рисунок 1.8 – Схема прихованої передачі інформації шляхом модулювання керуючого параметра передавального генератора інформаційним сигналом

Принцип її роботи аналогічний принципу роботи схеми на основі перемикання хаотичних режимів Корисний цифровий сигнал m(t) модулює один з параметрів передавального генератора x(t) таким чином, щоб в залежності від переданого бінарного біта 0 (1) між передавальним x(t) і приймальним u(t) генераторами існував (був відсутній) режим повної хаотичної синхронізації (рис. 1.8).

Тоді після проходження через віднімаючий пристрій сигналів передавального і приймального пристроїв детектується відновлений сигнал m(t). Для можливості реалізації режиму повної синхронізації керуючі параметри приймаючого генератора повинні бути обрані ідентичними керуючим параметрам передавального (точніше, одному з наборів параметрів передавального генератора, що відповідаю, наприклад, бінарним біту 0).

Особливості роботи, переваги і недоліки схем, заснованих на модуляції керуючих параметрів, 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.

1.2 Огляд математичних моделей, які є основою для побудови генераторів прихованої передачі інформації

Найбільш традиційними математичними моделями, що служать для обчислювальних експериментів з системами ППІ, є широко відомі моделі Ресслера Лоренца, Чуа та інші. Основними перевагами цих моделей є як математична простота, так і достатня вивченість хаотичної поведінки. Крім того, існує значна кількість робіт, присвячених апаратній реалізації хаотичних генераторів, побудованих на зазначених моделях.

У роботах [9-12] були розглянуті різні тривимірні автономні дисипативні системи звичайних диференціальних рівнянь. Деякі з розглянутих моделей були досліджені чисельним моделюванням на предмет їх використання в системах ППІ. Ці дослідження показали, що в моделях можуть бути реалізовані основні методи передачі інформації, апробовані на моделі Реслера [2], зокрема, метод модулювання керуючим параметром, метод нелінійного підмішування і інші. Застосування розроблених моделей в системах ППІ дозволяє ймовірно сподіватися на реалізацію численних хаотичних режимів, використовуючи одне й те ж обладнання (так звані мультиатракторні системи).

Теоретичною основою таких досліджень є теорія Фейгенбаума-Шарковського-Магницького (ФШМ), яка встановлює загальні закономірності сценаріїв переходу до динамічного хаосу в різних типах математичних систем [3, 13]. Ця теорія, зокрема, дозволяє дати відповідь на питання: до якої ділянки каскаду біфуркацій переходу до хаосу належить той чи інший хаотичний режим, який реалізується в системі ППІ.

Важливість відповіді на поставлене запитання полягає в наступних обставинах:

1) залежність ступеня складності сигналу і, таким чином, його конфіденційності, від місця режиму в каскаді;

2) ступінь впливу шуму на різні типи хаотичних режимів;

3) можливість отримання інформації третьою стороною з переданого сигналу і його стійкість по відношенню до процедур вилучення і т.д.

Виконаний огляд невеликого числа робіт з даної тематики показує, що необхідний значний обсяг досліджень, який дозволить вирішити основну проблему застосування динамічного хаосу в системах ППІ: практична реалізація за умови використання переваг широкополосності хаотичних режимів. Ці дослідження можуть бути спрямовані, зокрема, на розробку нових методів передачі інформації в більш високими швидкостями, більш надійного відновлення корисної інформації, зниження впливу шумів та інше.

1.2.1 Хаотична система Реслера

Система Реслера (R.Roessler) – одна із хаотичних систем, що може бути використана для захисту інформаційного носія, і яка описується трьома нелінійними диференціальними рівняннями:

$$\begin{aligned} dx/dt &= -y - z, \\ dy/dt &= x + ay, \\ dz/dt &= b - cz + xz, \end{aligned} \tag{1.1}$$

де x, y, z – початкові умови, a,b, c – параметри системи [14-17].

На рис. 1.6 наведено хаотичний атрактор Реслера при значеннях параметрів a=b=0,2; c=5,7.

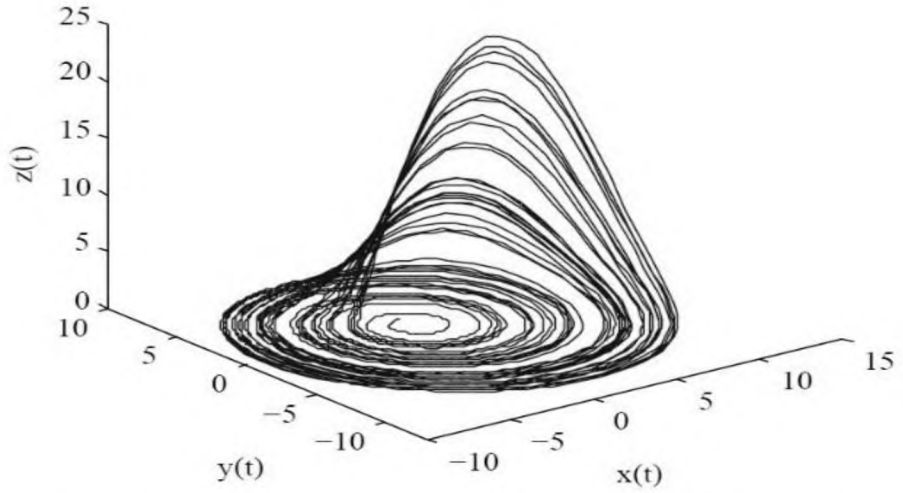


Рисунок 1.6 – Хаотичний атрактор системи Реслера

Система (1.1) є прикладом багатомірних систем, динаміку яких можна апроксимувати одномірним відображенням.

Хаотичний атрактор Реслера обертається навколо вісі Z, так що хороший вибір для січення Пуанкаре є площина, що проходить через вісь Z.

Послідовність таких січень Пуанкаре розміщена радіально на збільшення кутів по відношенню до вісі X, рис. 1.7, що ілюструє дію розділення і складання потоку Реслера.

Для орієнтування, було порівняно це з рис. 1.6, і звернуто увагу на різні масштаби Z-вісі. Видно, що рис. 1.7 збирає ці розділення в серію знімків потоку.

Слід підкреслити, що при значеннях параметрів a=0.15, b=0.2, c=10.0 система (1.1) характеризується режимом дивного атрактора [17].

Використаємо в якості одновимірного часового ряду a_i залежність в часі однієї з координат $y(i\Delta t)$, отриману чисельною інтеграцією рівнянь (1.1). Будемо вважати, що вид системи (1.1) і її розмірність нам невідомі. Спостережувана $a(t)=y(t)$, задана на кінцевому інтервалі часу $0\leq t\leq 100$, представлена на рис. 1.8,*а*.

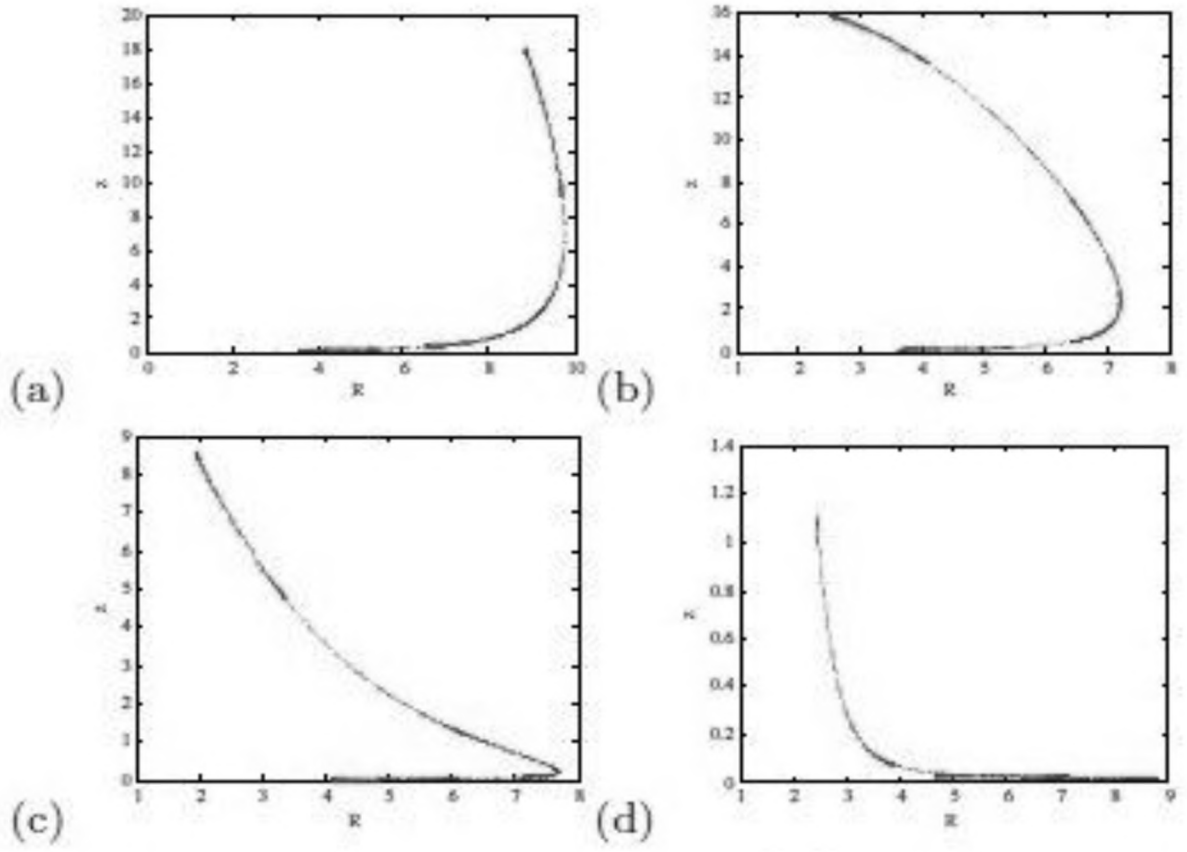


Рисунок 1.7 – Січення Пуанкаре потоку Реслера при 0^o, 45^o, 90^o і 135^o щодо X-вісі

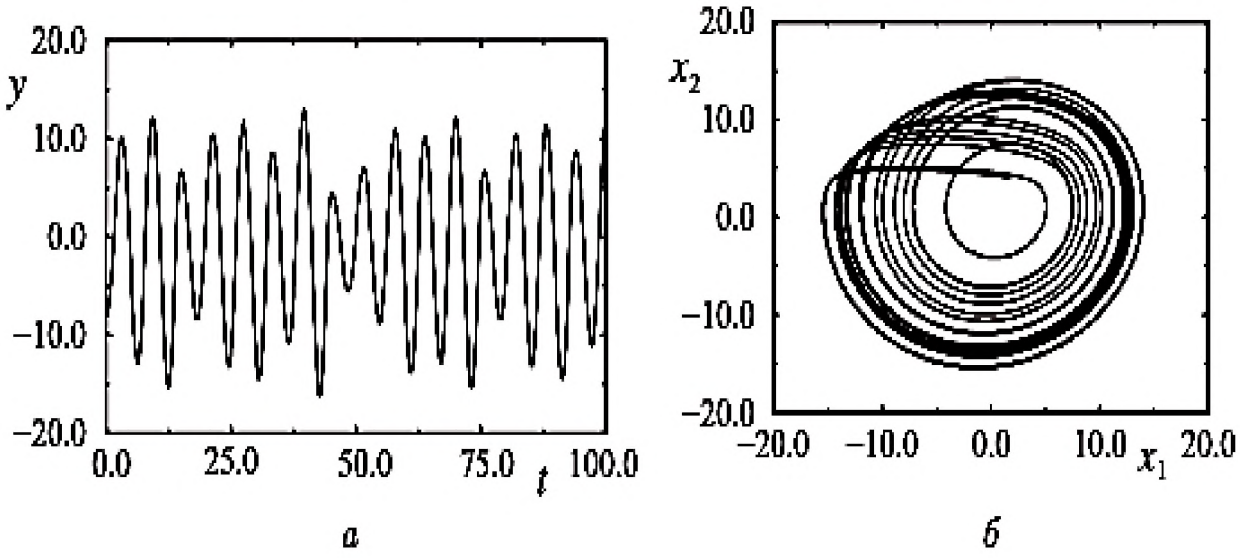


Рисунок 1.8 – Часова залежність координати $y(t)$ системи Реслера ($а$) та реконструйований атрактор в проекції на площину ($y(t)$, $y(t+\tau)$) ($б$)

Для завдання вектора стану реконструйованої системи скористаємося теоремою Такенса [17, 18].

У 1981 р. була доведена теорема Такенса, яка стверджує, що по одновимірній реалізації $a(t)$ динамічної системи (ДС), що має атрактор А, який належить гладкому d-мірному різноманіттю, методом затримки можна отримати n-мірну реконструкцію A_R вихідного атрактора як множину векторів $x(t)$ в R^n при $n \geq 2d+1$:

$$\boldsymbol{x}(t)=\Lambda_n(a(t))=\{a(t), a(t+\tau),..., a(t+(n-1)\tau)\}=\{x_1, x_2,..., x_n\}. \qquad (1.2)$$

Згідно з теоремою, відображення Λ_n: $A \rightarrow A_R$ є гладким і оборотним на A_R майже при довільній затримці τ (якщо $N \rightarrow \infty$).

Розраховуючи по спостережуваній $a(t)$ автокореляційну функцію, знаходимо час спадання її до нуля $\tau_0 \approx 1.6$ і використаємо цю величину в якості часу затримки в (1.2). На рис. 1.8,*б* представлена проекція реконструйованого атрактора на площину двох змінних:

$$x_1(t)=y(t) \text{ і } x_2(t)=y(t+\tau). \qquad (1.3)$$

Для визначення розмірності модельної системи потрібно розрахувати розмірність атрактора і розмірність простору вкладення. Для оцінки розмірності атрактора обчислимо його кореляційну розмірність D_c, використовуючи спеціальний алгоритм. Кореляційну розмірність D_C можна легше й швидше оцінити чисельно (в загальному випадку $D_C \leq D_0$):

$$D_c = \lim_{\varepsilon \to 0} \lim_{N \to \infty} \frac{\lg C(\varepsilon, N)}{\lg \varepsilon}, \qquad (1.4)$$

де $C(\varepsilon, N) = N^{-2} \sum_{i \neq j} v\left(\varepsilon - \left|x_i - x_j\right|\right)$ – кореляційний інтеграл, ε – розмір осередку розбивки фазового простору, N – число точок, використовуваних для оцінки розмірності, v – функція Хевісайда, $\boldsymbol{x}_i=\boldsymbol{x}(i\Delta t)$. Для визначення D_c будують залежність $\lg C(\varepsilon, N)$ від $\lg \varepsilon$ і шукають на ній лінійну ділянку, нахил якої і визначає шукане значення розмірності. Крім того, іноді аналізують залежність $D_c(n)$ і збільшують n до тих пір, поки D_c не досягне насичення.

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

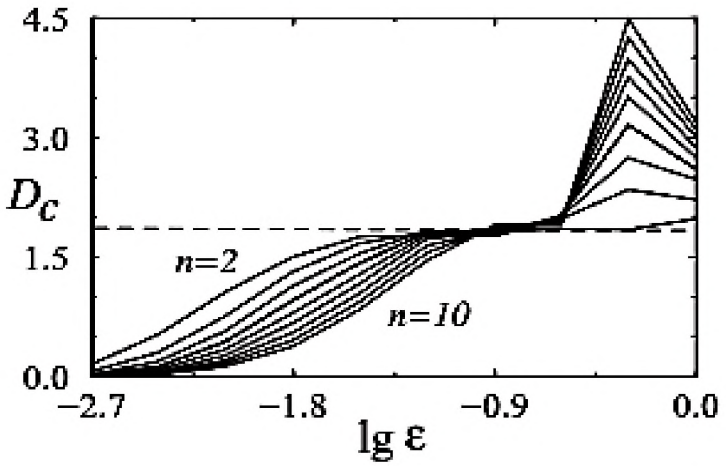


Рисунок 1.9 – Результати розрахунку кореляційної розмірності D_c при варіюванні розмірності простору вкладення n

Таким чином, реконструйований атрактор має розмірність $D \approx 2$ і може бути «вкладений» в тривимірний фазовий простір. Це означає, що ми можемо шукати модельну ДС у вигляді системи ЗДР третього порядку (n=3). Шукану систему рекомендовано записувати у формі Коші, використовуючи поліноміальну апроксимацію і обмежившись значенням n=3 і v=2 [17].

Результати інтегрування модельної ДС представлені на рис. 1.10 у вигляді залежності $x_1(t)$.

Порівняння даних рис. 1.10 з даними рис. 1.8,*а* показує якісну подібність реального і модельного коливальних процесів. Однак важливим, звичайно, є кількісні відповідності. Чи можливо за допомогою реконструйованої системи здійснювати прогноз еволюції системи в часі за межами інтервалу, на якому нам відома спостережувана? З цією метою проведемо наступний експеримент. Візьмемо в якості початкового значення координату останньої точки спостережуваної (рис. 1.8,*а*) в момент часу t_0=100. Далі інтегруємо як вихідну,

так і модельну системи з початковими умовами при $t=t_0$ і порівняємо результати для $t>t_0$.

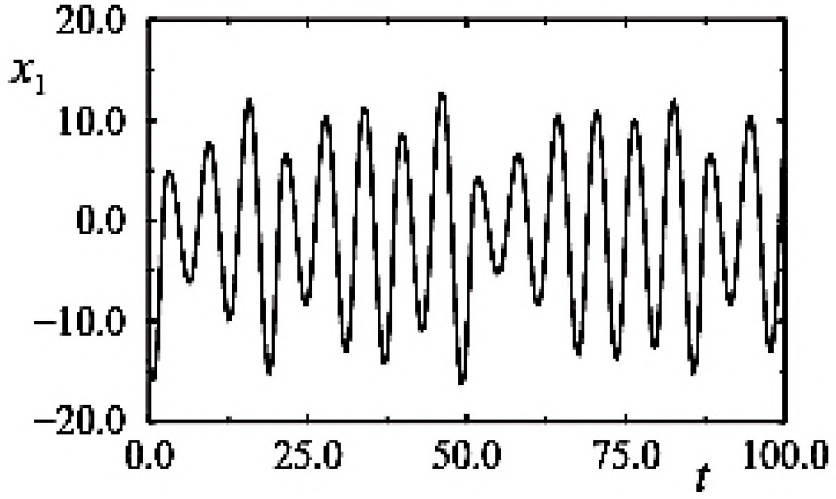


Рисунок 1.10 – Залежність $x_1(t)$, отримана чисельним інтегруванням реконструйованої системи

На рис. 1.11 наведені відповідні графіки залежностей $y(t)$ для тестової системи (1.1) і x_1(t) для реконструйованої ДС. Пунктирною лінією тут показано результат інтегрування системи (1.1), суцільною лінією – рішення реконструйованої модельної системи.

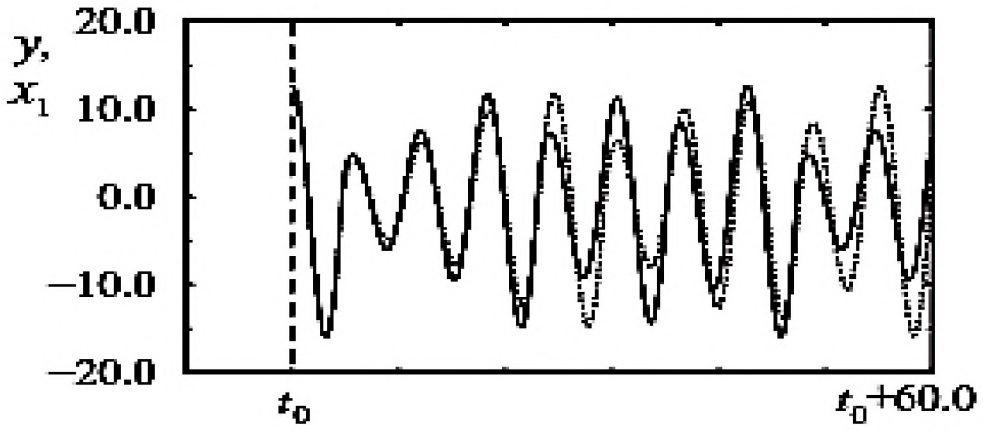


Рисунок 1.11 – Прогноз поведінки системи (1.1) після закінчення спостереження за сигналом, що генерується цією системою (час t_0)

Як випливає з рис. 1.11, прогноз еволюції системи в часі здійснюється з деякою похибкою, яка з часом наростає. Конкретний час прогнозу можна вказати, задавши точність передбачення. З результатів рис. 1.11 випливає, що якщо обмежитися похибкою ±5%, то час передбачення в нормованих одиницях становитиме приблизно T=12, тобто близько двох базових квазіперіодів коливань системи.

Обраний для ілюстрації приклад є далеко не простим, оскільки реконструюються хаотичні автоколивання. З цим пов'язані і похибки реконструкції, що обмежують час передбачення. Якщо в якості спостерігаючої ми маємо більш простий тип руху (наприклад, періодичні коливання), реконструкція призводить до зменшення похибок і збільшення часу прогнозу.

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

1.2.2 Проблеми моделювання систем з хаотичною поведінкою

Дослідження, проведені в останні роки, показують, що динамічний хаос володіє рядом властивостей, що роблять його привабливим для використання в системах зв’язку в якості несучих або модульованих коливань [15].

Безумовно, сучасна техніка зв’язку здатна вирішувати і вирішує значну частину виникаючих перед нею проблем традиційними методами, заснованими на регулярних сигналах і, при необхідності розширення спектра частот, на псевдошумових сигналах. Однак притягальним у використанні динамічного хаосу є те, що сукупність висунутих вимог до сучасних і перспективних систем зв’язку, природним чином може бути реалізована в рамках єдиного підходу. Це свідчить на користь потенційної ефективності застосування хаосу в системах зв’язку і налаштовує на наполегливе подолання наявних проблем.

А проблеми досить серйозні: відсутність вузлів і компонент, які використовують властивості хаотичної динаміки; необхідність створення

«прецизійних» елементів хаотичних систем і хаотичних систем у цілому, що забезпечують відтворюваність характеристик «від зразка до зразка»; висока чутливість схем передачі інформації на основі хаотичних сигналів до лінійних і нелінійних спотворень у вихідних ланках передавачів і вхідних ланках приймачів, а також безпосередньо в каналі зв'язку; відносно низька завадостійкість (по крайній мірі для більшості запропонованих схем); суттєва відмінність запропонованих рішень від рішень для традиційних систем зв'язку.

Слід зазначити, що більшість з перерахованих проблем виникають і при традиційних підходах, як тільки підвищуються вимоги до якості і швидкості передавання інформації. Дійсно, при необхідності передавання декількох біт замість одного за той самий інтервал часу потрібно або скоротити довжину імпульсів і тим самим розширити спектр переданого сигналу, або вводитидодаткове число градацій амплітуди імпульсів, що не змінює ширину смуги частот, але приводить до зниження стійкості сигналу стосовно шумів.

На сьогодні новою властивістю хаотичних сигналів як носіїв є те, що вони самі містять у собі визначену і, у середньому, фіксовану в одиницю часу інформацію. Наявність цієї інформації вимагає деякої додаткової пропускної здатності від каналу зв'язку. Разом з тим присутність інформаційної складової в хаотичному сигналі і керування нею можуть бути застосовані для додання схемі передачі деяких додаткових корисних властивостей.

Ідея використання хаосу в системах передавання інформації вже перейшла зі стадії сугубо фундаментальних досліджень у стадію аналізу і дослідження засобів зв'язку широких класів [15].

При створенні хаотичних передавачів виникає ряд проблем. Перша група проблем зв'язана зі створенням генераторів (джерел) хаосу. Джерела хаосу повинні задовольняти, як мінімум, наступним вимогам [15]:

- генерувати хаотичні коливання в необхідному діапазоні частот і мати можливо менше побічне випромінювання;

- забезпечувати в смузі частот генерації бажаний або близький до бажаного розподіл спектральної густини сигналу;

- бути керованими в тому розумінні, як цього вимагає використовувана схема введення інформації в хаотичний сигнал (схема модуляції);

- повинно бути забезпечене відтворення основних характеристик генераторів від зразка до зразка;

- для реалізації генератора у виді інтегральної мікросхеми повинна бути розроблена і досліджена досить точна еквівалентна схема, а також адекватна математична модель.

Друга група проблем зв'язана з введенням інформаційного сигналу в хаотичний сигнал. В ідеологічному плані тут не виникає ускладнень з методами введення, що використовують такі стандартні операції, як додавання сигналів, множення сигналів на ±1, перемножування хаотичного й інформаційного сигналів, модуляція інформаційним сигналом параметрів хаотичної системи і т. д.

Однак поряд із традиційними операціями для введення інформаційного сигналу в хаотичний сигнал запропоновано застосовувати і специфічні підходи, засновані на спеціальних властивостях хаотичних систем і, у силу цього, потенційно досить ефективні. Зокрема, таким перспективним підходом є введення інформації за рахунок малих збурень поточного стану хаотичної системи, для реалізації якого ведеться розробка відповідних пристроїв і вузлів.

Третя група проблем зв'язана з формуванням вигляду хаотичного передавача в цілому. Крім генератора і пристрою введення інформації в хаотичний сигнал, передавач може містити в собі цілий ряд елементів і вузлів, що забезпечують підсилення сигналів, фільтрацію позасмугових коливань, перенос частоти, модуляцію несучого періодичного коливання хаотичним коливанням і т. д. Багато цих вузлів добре відпрацьовані і широко застосовуються в стандартних радіотехнічних пристроях. Однак можливість їхнього застосування в передавачах з використанням хаосу може виявитися досить обмеженою. Причина полягає в різниці вимог, що пред'являються до таких елементів у двох типах систем. Наприклад, для багатьох традиційних систем передавання інформації фазові спотворення інформаційного сигналу не

грають істотної ролі. У той же час для систем зв'язку при наявності хаосу такі спотворення украй небажані.

Тепер представимо, що у відповідності зі структурою передавача виконується кілька послідовних операцій [15]. При кожній операції відбувається деяке спотворення сигналу. Якщо зафіксувати допустимі спотворення для передавача в цілому, то вимоги на допустимий рівень спотворень при окремих операціях будуть підсилюватися з ростом числа операцій.

Звідси випливає висновок: потрібно спробувати зменшити число перетворень над хаотичним сигналом і максимально спростити структуру передавача. Граничний випадок такого спрощення структури – прямо хаотичні передавачі. У них хаотичний сигнал формується безпосередньо в тому діапазоні частот, де виробляється його випромінювання, а введення інформаційного сигналу в хаотичний відбувається в результаті впливу на формувач хаотичного сигналу або вже на виході з нього. Таким чином, єдиним додатковим вузлом через який повинен пройти хаотичний сигнал, який містить корисну інформацію, є вихідний підсилювач. Він же служить узгоджувальним пристроєм між джерелом хаосу і каналом.

При створенні приймачів виникають наступні проблеми [15].

Задачами приймача є: сприйняття з каналу високочастотного або НВЧ-сигналу; перетворення цього сигналу до виду, придатного для виділення корисної інформації; безпосередній витяг інформації; приведення її до виду, який потрібен одержувачу. Звідси випливає, що дві групи проблем, зв'язаних з реалізацією приймачів, аналогічні тим, що виникають при реалізації передавачів і також приводять до висновку про бажаність спрощення структури системи. По-перше, та ланка вузлів, що стоїть в передавачі після введення інформаційного сигналу, має свій аналог у приймачі: підсилювачі, фільтри, пристрої, що забезпечують перенесення частоти (тепер уже зверху вниз), демодулятори і т.д. Тому й у приймачі існує проблема спотворення сигналу при послідовному виконанні операцій. По-друге, виникають проблеми з вузлом,

побудованим на елементах, що входять до складу хаотичного генератора передавача. Цей вузол відіграє роль нелінійного узгоджувального фільтра.

Питання, зв'язані з ефективним витягом інформаційного компонента, вимагає окремого обговорення. Справа в тому, що в силу специфічних інформаційних властивостей хаотичних сигналів схеми демодуляції й умови, при яких повинна вироблятися демодуляція, також досить незвичайні.

Нарешті, окрема група проблем зв'язана з проходженням сигналів, випромінюваних хаотичними передавачами через канал, під яким розуміється фізичне середовище поширення. Зокрема, це можуть бути радіо- і НВЧ-кабелі, радіорелейні лінії; поширення через вільний простір, пересічену місцевість, міську забудову і т. д.

Проходження через канал приводить до зміни характеристик сигналу, що позначається на роботі приймача. Оскільки успішний прийом сигналу і витяг з нього інформаційного компонента визначаються всією сукупністю спотворень, внесених у сигнал, вихідні вузли передавачів і вхідні блоки приймачів хаосу можна також віднести до елементів фізичного каналу.

Навіть якщо передавач і приймач хаосу виконані з необхідним ступенем точності і відтворюваності, що дозволяє у випадку «ідеального» каналу одержувати гарні характеристики, то наявність спотворень у каналі може приводити або до істотної деградації характеристик схеми зв'язку, або до її непрацездатності. Різні аспекти проблеми каналу і підходи до її вирішення вже обговорювалися в літературі [15]. Особливості цієї проблеми й аналіз шляхів її вирішення вимагають окремого детального розгляду.

1.3 Існуючі підходи до прихованої передачі інформації в системах зв'язку з використанням динамічного хаосу

У більшості запропонованих раніше підходів до прихованої передачі інформації використовується явище повної хаотичної синхронізації між ідентичними хаотичними генераторами, які перебувають на різних сторонах

каналу зв'язку. Це, в першу чергу, хаотичне маскування [19], перемикання хаотичних режимів [20], нелінійне підмішування інформаційного сигналу до хаотичного [21], модулювання керуючих параметрів хаотичного сигналу інформаційним [22] та інше. Існують також спроби використання узагальненої синхронізації для цих цілей [23] або обох вищезазначених типів синхронної поведінки одночасно [23, 24].

Принциповими недоліками всіх запропонованих в даний час схем [19-24] є наступні:

1. Вимога високого ступеня ідентичності хаотичних генераторів на різних сторонах каналу зв'язку, що є дуже серйозним і важкореалізовуваним завданням, особливо протягом тривалого часу експлуатації пристроїв. Малий розлад значень керуючих параметрів цих генераторів призводить до втрати значної частини переданої інформації.

2. Досить низька стійкість до шумів і флуктуацій в каналі зв'язку. При перевищенні інтенсивністю шуму і флуктуацій деякого порогового значення, який можна порівняти з природними шумами і спотвореннями, відомі системи передачі інформації стають непрацездатними.

3. Можливість реконструкції параметрів передавального генератора по сигналу, що передається по каналу зв'язку (особливо в разі використання повної хаотичної синхронізації для прихованої передачі інформації). Через наявність точної копії передавального генератора на іншій стороні каналу зв'язку третя сторона в деяких випадках може легко дешифрувати інформаційне повідомлення.

Всіх перерахованих вище недоліків позбавлений підхід до прихованої передачі інформації [25], який було обрано як прототип. Він заснований на явищі узагальненої хаотичної синхронізації і є найбільш близьким до запропонованого підходу до прихованої передачі інформації. Відповідно до цього відомого підходу корисний інформаційний сигнал кодується у вигляді бінарного коду. Один або декілька керуючих параметрів передавального хаотичного генератора модулюється корисним цифровим сигналом. Отриманий

таким чином сигнал передається по каналу зв'язку приймаючій стороні, що містить два ідентичних хаотичних генератора, здатних перебувати з передавальним генератором в режимі узагальненої хаотичної синхронізації. Сигнали, що знімаються з виходів генераторів приймаючої сторони, подаються на віднімаючий пристрій і по наявності / відсутності хаотичних коливань детектується корисний цифровий сигнал, представлений у вигляді двійкового коду.

Схема реалізації відомого підходу до прихованої передачі інформації з використанням узагальненої хаотичної синхронізації (прототипу) представлена на рис. 1.12.

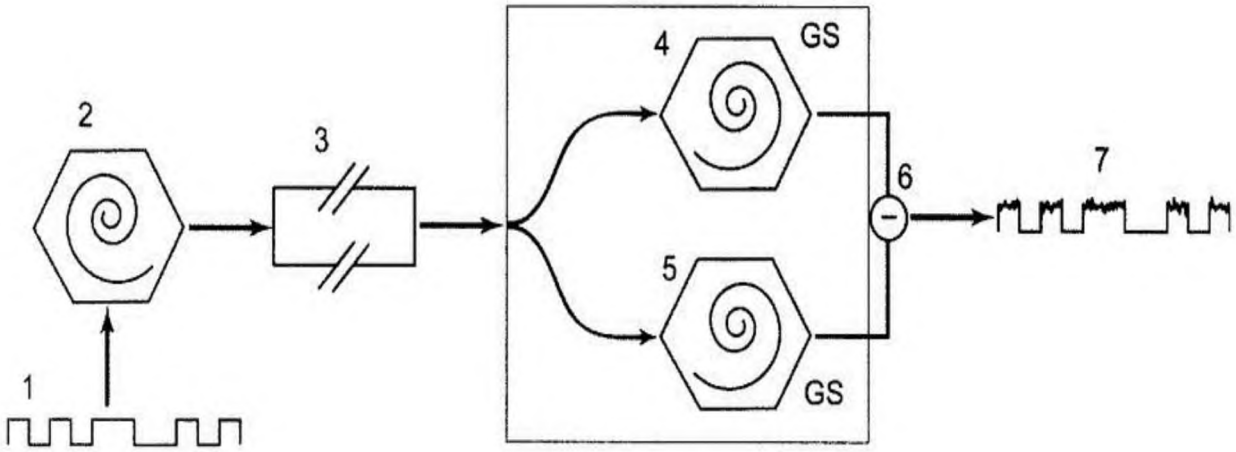


Рисунок 1.12 – Схема реалізації відомого підходу до прихованої передачі інформації з використанням узагальненої хаотичної синхронізації (прототипу)

На рис 1.12 введені такі позначення:

1 – корисний сигнал;

2 – передавальний генератор хаосу;

3 – канал зв'язку;

4 – приймаючий генератор хаосу;

5 – третій генератор, ідентичний приймаючому генератору 4 по керуючим параметрам;

6 – віднімаючий пристрій;

7 – дешифрований сигнал, що передається.

Даний тип синхронної поведінки (узагальнена синхронізація хаотичних осциляторів) вводиться для однонаправлено пов'язаних хаотичних генераторів. Наявність режиму узагальненої синхронізації означає, що між станами взаємодіючих ведучого $x_d(t)$ і веденого $x_r(t)$ хаотичних осциляторів існує деяка функціональна залежність $F[\bullet]$, така, що має місце функціональне співвідношення

$$x_r(t)=F[x_d(t)]. \qquad (1.5)$$

При цьому, сам вид цієї залежності $F[\bullet]$ може бути досить складним, в тому числі, і фрактальним, що є досить важливим при прихованій передачі інформації [25].

Відомий підхід до прихованої передачі інформації з використанням узагальненої хаотичної синхронізації (прототип), полягає в наступному: корисний сигнал кодується у вигляді двійкового коду. Один або декілька керуючих параметрів генератора хаотичних автоколивань 2 модулюються корисним двійковим сигналом 1. Це означає, що в залежності від переданого протягом заданого інтервалу часу двійкового біта («0» або «1») керуючі параметри генератора хаосу 2 змінюються якимось чином, наприклад, незначною зміною положення основної частоти в спектрі хаотичного сигналу передавального генератора. Сформований таким чином сигнал надходить в канал зв'язку 3 і з певною потужністю передається по каналу зв'язку приймаючій стороні. На приймаючому кінці каналу зв'язку знаходиться приймач.

Принцип роботи приймача заснований на детектуванні узагальненої хаотичної синхронізації за допомогою методу допоміжної системи. Для цього, на приймаючій стороні сигнал, знятий з каналу зв'язку, подають на два ідентичних генератора хаотичних автоколивань 4 і 5, здатних перебувати з передавальним генератором в режимі узагальненої хаотичної синхронізації.

Сигнали, що знімаються з виходів генераторів приймаючої сторони, подаються на віднімаючий пристрій 6.

Слід зауважити, що параметри модуляції керуючих параметрів передавального генератора необхідно обирати таким чином, щоб в залежності від переданого двійкового біта «0»/«1» між передавальним і приймаючими генераторами існував або був відсутній режим узагальненої хаотичної синхронізації.

Припустимо, при передачі двійкового бита «0» керуючі параметри передавача обираються таким чином, що між передавальним і приймальними генераторами реалізується режим узагальненої синхронізації. Тоді, в силу наявності функціональної залежності між станами хаотичних осциляторів, коливання, які генеруються двома ідентичними генераторами на приймальній стороні каналу зв'язку, будуть ідентичними і після проходження віднімаючого пристрою буде спостерігатися відсутність будь-яких коливань, тобто двійковий «0». Навпаки, при передачі двійкового бита «1» між передавальним і приймальним генераторами відсутній режим узагальненої синхронізації, і коливання ведених генераторів на приймаючій стороні будуть різними. Після проходження віднімаючого пристрою будуть спостерігатися хаотичні коливання з ненульовий амплітудою, тобто двійковий біт «1».

Слід відзначити, що саме цей відомий підхід-прототип з перерахованою сукупністю ознак володіє значною стійкістю до шумів і флуктуацій в каналі зв'язку.

Принциповим недоліком відомого підходу до прихованої передачі інформації з використанням узагальненої хаотичної синхронізації (прототипу) [25] є той факт, що сигнал, який передається по каналу зв'язку, несе на собі сліди модуляції керуючого параметра, що може дозволити третій стороні в деяких випадках декодувати інформаційне повідомлення. Таким чином, відомий підхід-прототип не забезпечує високу надійність передачі конфіденційної інформації.

1.4 Висновок. Постановка задачі

В розділі проаналізовано принципи застосування хаотичних широкосмугових сигналів у системах прихованої передачі інформації. 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 прихованої інформації. Встановлено, що режим узагальненої синхронізації має багато подібностей з режимом синхронізації, індукованої шумом, як по методам діагностики, так і за механізмами виникнення синхронного режиму, тому ці два типи синхронної поведінки іноді розглядає як єдиний тип синхронної хаотичної динаміки пов'язаних динамічних систем.

В розділі проаналізовано існуючі підходи до прихованої передачі інформації в системах зв’язку з використанням динамічного хаосу. У більшості з них використовується явище повної хаотичної синхронізації між ідентичними хаотичними генераторами, які перебувають на різних сторонах каналу зв'язку. Це, в першу чергу, хаотичне маскування [19], перемикання хаотичних режимів [20], нелінійне підмішування інформаційного сигналу до хаотичного [21], модулювання керуючих параметрів хаотичного сигналу інформаційним [22] та інше. Існують також спроби використання узагальненої синхронізації для цих цілей [23] або обох вищезазначених типів синхронної поведінки одночасно [23, 24].

Встановлено, що принциповими недоліками всіх запропонованих в даний час схем [19-24] є наступні:

1. Вимога високого ступеня ідентичності хаотичних генераторів на різних сторонах каналу зв'язку, що є дуже серйозним і важкореалізовуваним завданням, особливо протягом тривалого часу експлуатації пристроїв. Малий розлад значень керуючих параметрів цих генераторів призводить до втрати значної частини переданої інформації.

2. Досить низька стійкість до шумів і флуктуацій в каналі зв'язку. При перевищенні інтенсивністю шуму і флуктуацій деякого порогового значення, який можна порівняти з природними шумами і спотвореннями, відомі системи передачі інформації стають непрацездатними.

3. Можливість реконструкції параметрів передавального генератора по сигналу, що передається по каналу зв'язку (особливо в разі використання повної хаотичної синхронізації для прихованої передачі інформації). Через наявність точної копії передавального генератора на іншій стороні каналу зв'язку третя сторона в деяких випадках може легко дешифрувати інформаційне повідомлення.

Встановлено, що недоліком відомого підходу до прихованої передачі інформації з використанням узагальненої хаотичної синхронізації (прототипу) [25] є той факт, що сигнал, який передається по каналу зв'язку, несе на собі сліди модуляції керуючого параметра, що може дозволити третій стороні в деяких випадках декодувати інформаційне повідомлення. Таким чином, відомий підхід-прототип не забезпечує високу надійність передачі конфіденційної інформації.

Таким чином, для усунення недоліків існуючих підходів необхідно:

• запропонувати підхід до прихованої передачі інформації, заснований на явищах узагальненої хаотичної синхронізації і синхронізації, індукованої шумом;

• оцінити ефективність запропонованого підходу.

2 СПЕЦІАЛЬНА ЧАСТИНА

2.1 Підхід до прихованої передачі інформації, заснований на явищах узагальненої хаотичної синхронізації і синхронізації, індукованої шумом

Запропонований підхід відноситься до радіотехніки і передачі інформації і може знайти застосування в системах зв'язку для завадостійкої передачі цифрової інформації з певним ступенем конфіденційності. Технічний результат – підвищення надійності і створення додаткової секретності. Для цього корисний сигнал кодують в двійковий код, формують за допомогою першого хаотичного генератора початковий детермінований хаотичний сигнал шляхом модуляції параметрів хаотичного сигналу корисним цифровим сигналом, передають сформований таким чином сигнал по каналу зв'язку приймаючій стороні, де його ділять на два ідентичних сигнали, якими впливають на другий і третій хаотичні генератори. Другий і третій хаотичні генератори ідентичні один одному по керуючим параметрам і обрані з можливістю забезпечення режиму узагальненої синхронізації з першим хаотичним генератором. Зняті з виходів зазначених другого і третього генераторів сигнали подають на віднімаючий пристрій і при спостереженні або відсутності хаотичних коливань визначають наявність корисного цифрового сигналу, представленого у вигляді двійкового коду. Сформований першим хаотичним генератором детермінований хаотичний сигнал перед передачею по каналу зв'язку підсумовують з шумовим сигналом, виробленим генератором шуму, при цьому перший хаотичний генератор і генератор шуму налаштовують в режим, при якому відношення сигнал / шум (SNR – Signat to Noise Ratio) задовольняє наступній умові: SNR>-34.6 дБ.

Поставлена мета роботи вирішується тим, що в підході до прихованої передачі інформації, що містить корисний цифровий сигнал, що полягає в кодуванні корисного сигналу в двійковий код, формуванні за допомогою першого хаотичного генератора початкового детермінованого хаотичного

сигналу шляхом модуляції параметрів хаотичного сигналу корисним цифровим сигналом, передачі сформованого таким чином сигналу по каналу зв'язку приймаючій стороні, його розподілі на два ідентичних сигналу, вплив ними на другий і третій хаотичні генератори, ідентичні один одному по керуючим параметрам, вибрані з можливістю забезпечення режиму узагальненої синхронізації з першим хаотичним генератором, подачі знятих з виходів зазначених другого і третього генераторів сигналів на віднімаючий пристрій і визначенні при спостереженні або відсутності хаотичних коливань наявності корисного цифрового сигналу, представленого у вигляді двійкового коду. Відповідно до запропонованого підходу сформований першим генератором детермінований хаотичний сигнал перед передачею по каналу зв'язку підсумовують з шумовим сигналом, виробленим генератором шуму.

Крім того, перший хаотичний генератор і генератор шуму налаштовують в режим, при якому відношення сигнал / шум SNR задовольняє наступній умові: SNR> - 34.6 дБ.

В запропонованому підході шум грає конструктивну роль, у той час як у всіх аналогах роль шуму є деструктивною. Тому позитивний вплив шумів було використано з метою вдосконалення відомого підходу-прототипу до прихованої передачі інформації [25] і поліпшення його конфіденційності.

Технічний результат, який досягається в запропонованому підході до прихованої передачі інформації, полягає в тому, що шумовий сигнал, вироблений генератором шуму, забезпечує відсутність слідів модуляції керуючих параметрів, а отже, і додаткове маскування переданого по каналу зв'язку сигналу, тим самим перешкоджаючи третій стороні декодувати інформаційне повідомлення, що гарантує конфіденційність запропонованого підходу до прихованої передачі інформації.

На рис. 2.1 представлена схема для реалізації запропонованого підходу до прихованої передачі інформації, заснованого на явищах узагальненої хаотичної синхронізації і синхронізації, індукованої шумом.

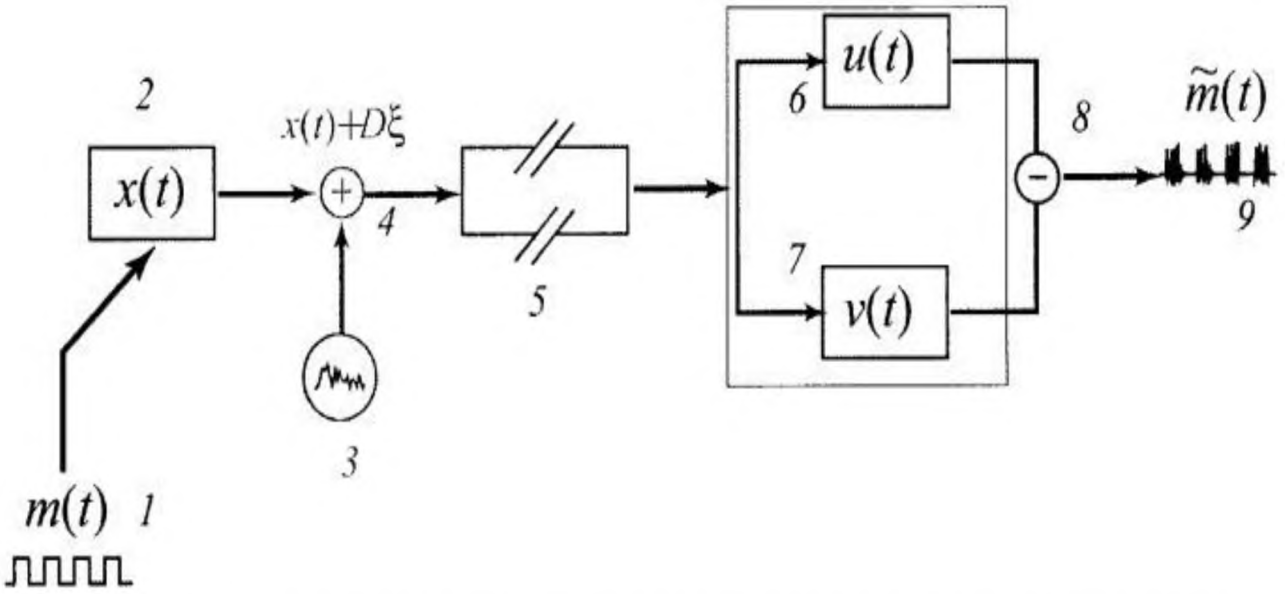


Рисунок 2.1 – Схема для реалізації запропонованого підходу до прихованої передачі інформації, заснованого на явищах узагальненої хаотичної синхронізації і синхронізації, індукованої шумом

На рис. 2.1 введено такі позначення:

1 – корисний бінарний сигнал;

2 – перший (передавальний) хаотичний генератор;

3 – генератор шуму;

4 – акумулятор;

5 – канал зв'язку;

6 – другий (приймальний) хаотичний генератор;

7 – третій генератор, ідентичний другому генератору 6 по керуючим параметрам;

8 – віднімаючий пристрій;

9 – відновлений корисний сигнал.

Запропонований підхід до прихованої передачі інформації заснований на явищах узагальненої хаотичної синхронізації [27] і синхронізації, індукованої шумом [28]. Узагальнена синхронізація може спостерігатися в системі двох однонаправлено пов'язаних хаотичних генераторів, ведучого і веденого (що і реалізується в запропонованому підході), і означає, що між їх станами x(t)

(ведучого) і u(t) (веденого) встановлюється деяке функціональне співвідношення F[·] таке, що u(t)=F[x(t)]. Найбільш простим і легко здійсненним на практиці (але при наявності копії веденого генератора) способом діагностики цього режиму є метод допоміжної системи [29]. У разі індукованої шумом синхронізації випадковий сигнал, який діє на два незалежних, але ідентичних хаотичних генератора, призводить до того, що їх коливання «повністю синхронізуються». По суті, ці два типи синхронної поведінки обумовлені однією і тією ж причиною і можуть бути розглянуті як єдиний тип синхронної поведінки пов'язаних хаотичних систем [30]. Відмінність між ними полягає лише в характері зовнішнього сигналу, випадковий він або детермінований. Тому можливо їх спільне використання для прихованої передачі інформації.

Запропонований підхід до прихованої передачі інформації, заснований на явищах узагальненої хаотичної синхронізації і синхронізації, індукованої шумом (рис. 2.1) полягає у наступному. Корисний інформаційний сигнал m(t) 1 кодується у вигляді бінарного коду. Один або декілька керуючих параметрів передавального (першого) хаотичного генератора 2 модулюється інформаційним сигналом таким чином, що характеристики переданого сигналу змінюються незначно. Для забезпечення додаткового маскування інформаційного сигналу і зміни характеристик сигналу, що передається використовується генератор шуму 3. Сигнал, що генерується передавальної системою, домішується в суматорі 4 до шумового сигналу і далі передається по каналу зв'язку 5. Тут він також підпадає під вплив шумів і флуктуації, неминуче присутніх в реальних пристроях. Приймальний пристрій знаходиться на іншій стороні каналу зв'язку. Він являє собою два ідентичних хаотичних генератора, другий 6 і третій 7, здатних перебувати в режимі узагальненої синхронізації з передавальним генератором 2. Принцип роботи пристрою одержувача заснований на діагностиці режиму узагальненої синхронізації за допомогою методу допоміжної системи [29]. Сигнал з каналу зв'язку надходить на генератори приймаючого пристрою. Отримані на виході сигнали проходять

через віднімаючий пристрій 8, і потім детектується відновлений корисний сигнал 9.

Параметри модуляції керуючих параметрів передавального (першого) генератора повинні бути обрані таким чином, щоб в залежності від переданого бінарного біта 0/1 між передавальним і приймальними генераторами за відсутністю шумів і флуктуації існував / був відсутній режим узагальненої хаотичної синхронізації. Тоді після проходження через віднімаючий пристрій буде детектуватися відновлений корисний сигнал, який представляє собою послідовність ділянок, що чергуються, з несинхронною (бінарний біт 1) і синхронною поведінкою (бінарний біт 0).

2.2 Оцінка ефективності запропонованого підходу до прихованої передачі інформації, заснованого на явищах узагальненої хаотичної синхронізації і синхронізації, індукованої шумом

Оцінка ефективності запропонованого підходу до прихованої передачі інформації, заснованого на явищах узагальненої хаотичної синхронізації і синхронізації, індукованої шумом була проведена шляхом моделювання в середовищі Matlab / Simulink за допомогою стандартного і розробленого програмного забезпечення.

Як приклад конкретної реалізації запропонованого підходу до прихованої передачі інформації, заснований на явищах узагальненої хаотичної синхронізації і синхронізації, індукованої шумом можна привести чисельне моделювання однонаправлено пов'язаних систем Реслера, обраних в якості передавального і приймального генераторів. Принципова схема генератора Реслера приведена в роботі [31].

Передавальний генератор описується наступною системою диференціальних рівнянь:

$$\begin{aligned} \dot{x}_1 &= -\omega_x x_2 - x_3, \\ \dot{x}_2 &= \omega_x x_1 + a x_2, \\ \dot{x}_3 &= p + x_3(x_1 - c), \end{aligned} \tag{2.1}$$

де $x(t)=(x_1,x_2,x_3)$ – вектор стану передавального генератора, що характеризує коливання напруги, що знімаються в різних ділянках ланцюга; a=0.15, p=0.2 і c=10 – керуючі параметри (що представляють собою композицію параметрів самої системи); ω_x – керуючий параметр, що характеризує власну частоту коливань системи.

Величина параметра ω_x модулюється корисним цифровим сигналом наступним чином. Якщо в заданий інтервал часу передається бінарний біт 1, тоді ω_x=0.95 протягом усього цього інтервалу. При передачі бінарного біта 0 ω_x=1 [32].

Приймальний пристрій містить два ідентичних хаотичних генератори, другий і третій, кожен з яких описується наступною системою рівнянь:

$$\begin{aligned} \dot{u}_1 &= -\omega_u u_2 - u_3 + \varepsilon(s(t) - u_1), \\ \dot{u}_2 &= \omega_u u_1 + a u_2, \\ \dot{u}_3 &= p + u_3(u_1 - c), \end{aligned} \tag{2.2}$$

Тут $u(t)=(u_1,u_2,u_3)$ – вектор стану другого генератора. Нехай $v(t)=(v_1,v_2,v_3)$, також задовольняє співвідношенню (2.2), буде вектором стану третього генератора (див. рис. 2.1). Керуючі параметри a, *p* і *c* виберемо ідентичними останнім для приймаючого генератора. Керуючий параметр ω_u, що характеризує власну частоту приймальних генераторів, виберемо рівним ω_u=0.95 протягом усього часу передачі сигналу.

Сигнал, що генерується передавальним пристроєм, підсумовується з сигналом, виробленим генератором шуму, і далі передається по каналу зв'язку. В імітаційній моделі це реалізується шляхом зв'язку приймальних генераторів з передавальним, тобто додаванням компоненти $\varepsilon(s(t)-u_1)$ в перше рівняння системи (2.2). Тут $s(t)=x_1+D\xi$ – це так званий сигнал в каналі зв'язку; доданок $D\xi$ – моделює шуми і флуктуації, вироблені генератором шуму; ξ – δ-

корельований білий шум, що характеризується наступним розподілом ймовірності:

$$p(\xi) = \frac{1}{\sqrt{2\pi\sigma}} \exp\left(-\frac{(\xi - \xi_0)^2}{2\sigma^2}\right), \tag{2.3}$$

де ξ_0=0 і σ=1 – середнє і дисперсія.

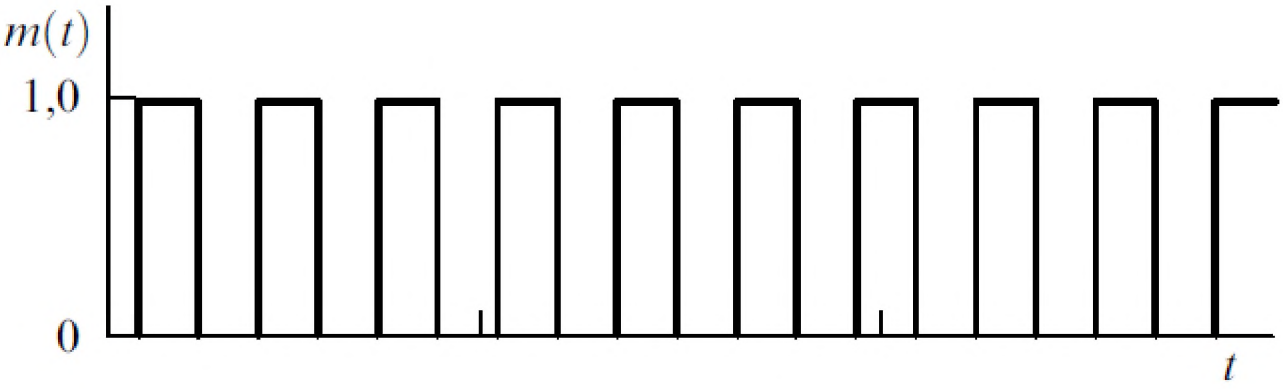
Важливо відзначити, що характер розподілу випадкової величини ξ не має особливого значення, і подібні результати можуть спостерігатися для інших типів розподілу ймовірності p(ξ), наприклад для рівномірного. Параметр D визначає сумарну інтенсивність шуму, що додається.

Сила зв'язку між передавальним і приймальними генераторами характеризується параметром ε. Він був обраний рівним ε=0.14. В цьому випадку, відомо, що під час відсутності шумів і флуктуації (D=0) режим узагальненої синхронізації в системі (2.1)-(2.2) має місце при ω_x=1, в той час як для ω_x=0.95 узагальнена синхронізація не спостерігається (більш детальніше див. [32]).

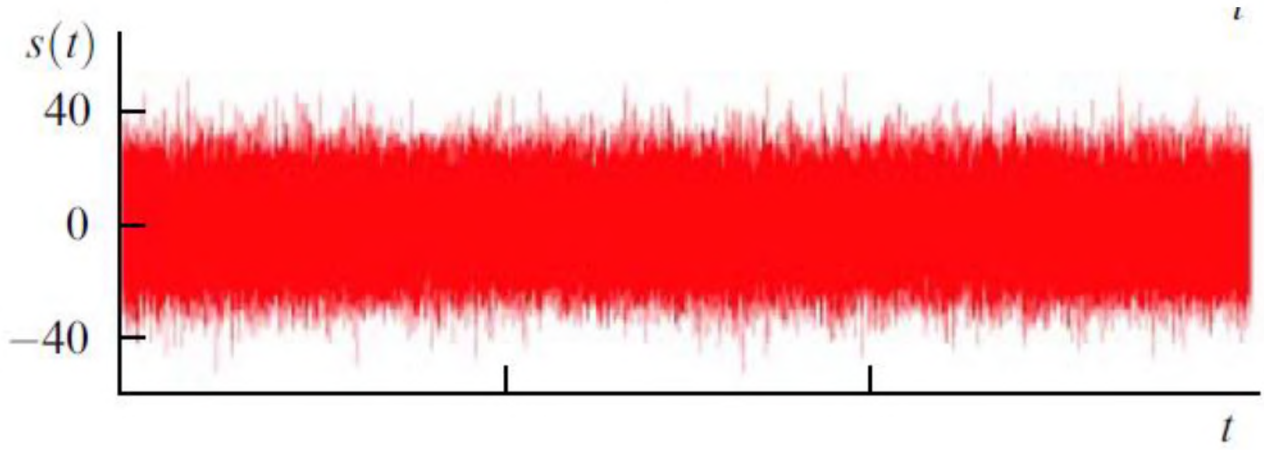
Віднімаючий пристрій виконує операцію $(u_1-v_1)^2$. Тоді після проходження через нього згідно з методом допоміжної системи повинно спостерігатися відсутність коливань для ω_x=1 і наявність хаотичних коливань для ω_x=0.95. відновлений сигнал $\widetilde{m}(t)$ буде являти собою послідовність областей з різними типами поведінки.

На рис. 2.2 представлені графіки, що характеризують процес передачі сигналу згідно запропонованого підходу. Причому на рис. 2.2,а представлено вихідний корисний цифровий сигнал; на рис. 2.2,б – сигнал, який передається по каналу зв'язку; на рис. 2.2,в – переданий корисний цифровий сигнал, відновлений в приймальнику хаотичних автоколивань.

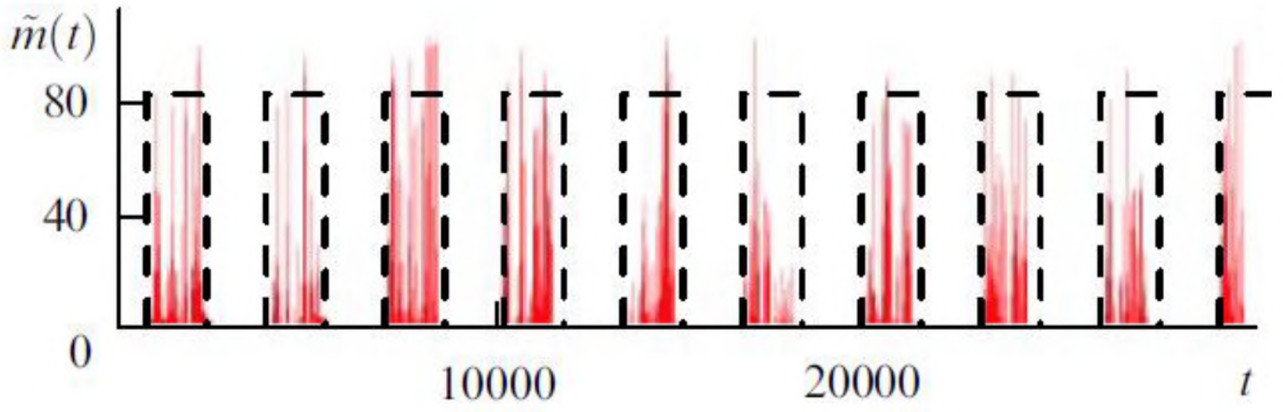
При здійсненні моделювання в якості інформаційного сигналу m(t) було обрано просту послідовність бінарних бітів 0/1, представлену на рис. 2.2,а. Для інтегрування стохастичного рівняння (2.2) було використано метод Ейлера з кроком дискретизації по часу h=0.0001.



а



б



в

Рисунок 2.2 – Графіки, що характеризують процес передачі сигналу згідно запропонованого підходу: *а* – вихідний корисний цифровий сигнал; *б* – сигнал, який передається по каналу зв'язку; *в* – переданий корисний цифровий сигнал, відновлений в приймальнику хаотичних автоколивань

Інтенсивність шуму була обрана досить великою, наприклад D=10, і було показано, як працює запропонований підхід до прихованої передачі інформації в цьому випадку.

На рис. 2.2,б наведено фрагмент сигналу s(t), що передається по каналу зв'язку. Видно, що зміна керуючого параметра ω_x сильно не змінює характеристики сигналу, що передається. Більш того, шум великої амплітуди ще більш спотворює сигнал, що передається, не залишаючи ніякої можливості третій стороні декодувати інформаційне повідомлення без повної інформації про характеристики приймальних генераторів.

Рис. 2.2,в ілюструє відновлений сигнал $\tilde{m}(t) = (u_1 - v_1)^2$. Неважко бачити, що за допомогою пропускання через фільтр нижніх частот і вибору порогових значень корисний цифровий сигнал може бути легко детектовано.

Слід зазначити, що аналогічні результати спостерігаються для різних значень інтенсивності шуму аж до D=400. У цьому випадку відношення сигнал / шум становить -34.6 дБ, що свідчить про значну стійкість запропонованого підходу до шумів і флуктуацій і про конструктивну роль шуму для передачі інформації.

Таким чином, позитивним ефектом запропонованого підходу до прихованої передачі інформації є забезпечення додаткового маскування переданого по каналу зв'язку сигналу і, отже, гарантія високого ступеня конфіденційності.

2.3 Висновки

Запропонований підхід відноситься до радіотехніки і передачі інформації і може знайти застосування в системах зв'язку для завадостійкої передачі цифрової інформації з певним ступенем конфіденційності. Технічний результат – підвищення надійності і створення додаткової секретності. Для цього корисний сигнал кодують в двійковий код, формують за допомогою першого хаотичного генератора початковий детермінований хаотичний сигнал шляхом

модуляції параметрів хаотичного сигналу корисним цифровим сигналом, передають сформований таким чином сигнал по каналу зв'язку приймаючій стороні, де його ділять на два ідентичних сигнали, якими впливають на другий і третій хаотичні генератори. Другий і третій хаотичні генератори ідентичні один одному по керуючим параметрам і обрані з можливістю забезпечення режиму узагальненої синхронізації з першим хаотичним генератором. Зняті з виходів зазначених другого і третього генераторів сигнали подають на віднімаючий пристрій і при спостереженні або відсутності хаотичних коливань визначають наявність корисного цифрового сигналу, представленого у вигляді двійкового коду. Сформований першим хаотичним генератором детермінований хаотичний сигнал перед передачею по каналу зв'язку підсумовують з шумовим сигналом, виробленим генератором шуму, при цьому перший хаотичний генератор і генератор шуму налаштовують в режим, при якому відношення SNR задовольняє наступній умові: SNR>-34.6 дБ.

В запропонованому підході до прихованої передачі інформації, заснованому на явищах узагальненої хаотичної синхронізації і синхронізації, індукованої шумом шум грає конструктивну роль, у той час як у всіх аналогах роль шуму є деструктивною. Тому позитивний вплив шумів було використано з метою вдосконалення відомого підходу-прототипу і поліпшення його конфіденційності.

Запропонований підхід заснований на явищах узагальненої хаотичної синхронізації і синхронізації, індукованої шумом. Узагальнена синхронізація може спостерігатися в системі двох однонаправлено пов'язаних хаотичних генераторів, ведучого і веденого, і означає, що між їх станами x(t) (ведучого) і u(t) (веденого) встановлюється деяке функціональне співвідношення F[·] таке, що u(t)=F[x(t)]. Найбільш простим і легко здійсненним на практиці (але при наявності копії веденого генератора) способом діагностики цього режиму є метод допоміжної системи. У разі індукованої шумом синхронізації випадковий сигнал, який діє на два незалежних, але ідентичних хаотичних генератора, призводить до того, що їх коливання «повністю синхронізуються». По суті, ці

два типи синхронної поведінки обумовлені однією і тією ж причиною і можуть бути розглянуті як єдиний тип синхронної поведінки пов'язаних хаотичних систем. Відмінність між ними полягає лише в характері зовнішнього сигналу, випадковий він або детермінований. Тому можливо їх спільне використання для прихованої передачі інформації.

Оцінка ефективності запропонованого підходу до прихованої передачі інформації, заснованого на явищах узагальненої хаотичної синхронізації і синхронізації, індукованої шумом була проведена шляхом моделювання в середовищі Matlab / Simulink.

Встановлено, що зміна керуючого параметра ω_x сильно не змінює характеристики сигналу, що передається. Більш того, шум великої амплітуди ще більш спотворює сигнал, що передається, не залишаючи ніякої можливості третій стороні декодувати інформаційне повідомлення без повної інформації про характеристики приймальних генераторів. Встановлено, що за допомогою пропускання через фільтр нижніх частот і вибору порогових значень корисний цифровий сигнал може бути легко детектовано. Такі результати спостерігаються для різних значень інтенсивності шуму аж до D=400. У цьому випадку відношення сигнал / шум становить -34.6 дБ, що свідчить про значну стійкість запропонованого підходу до шумів і флуктуацій і про конструктивну роль шуму для передачі інформації.

Таким чином, позитивним ефектом запропонованого підходу до прихованої передачі інформації, заснованого на явищах узагальненої хаотичної синхронізації і синхронізації, індукованої шумом є забезпечення додаткового маскування переданого по каналу зв'язку сигналу і, отже, гарантія високого ступеня конфіденційності.

3 ЕКОНОМІЧНА ЧАСТИНА

Метою даного розділу є встановлення економічної доцільності розробки підходу щодо забезпечення конфіденційності при передачі інформації в системах зв'язку з використанням динамічного хаосу. Досягнення цієї мети потребує виконання таких розрахунків, як:

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

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

– річний економічний ефект від впровадження запропонованих заходів;

– показники економічної ефективності впровадження системи захисту на підприємстві.

3.1 Розрахунок (фіксованих) капітальних витрат

Капітальні інвестиції – це кошти, призначені для створення і придбання основних фондів і нематеріальних активів, що підлягають амортизації.

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

Визначення трудомісткості розробки підходу щодо забезпечення конфіденційності при передачі інформації в системах зв'язку з використанням динамічного хаосу

Трудомісткість розробки підходу щодо забезпечення конфіденційності при передачі інформації в системах зв'язку з використанням динамічного хаосу визначається тривалістю кожної робочої операції, до яких належать наступні:

де $t_{тз}$ – тривалість складання технічного завдання на розробку підходу щодо забезпечення конфіденційності при передачі інформації в системах зв'язку з використанням динамічного хаосу, $t_{тз}=24$;

$t_в$ – тривалість аналізу існуючих інформаційних потоків організації, вивчення ТЗ, літературних джерел за темою тощо, $t_в=40$;

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

$t_р$ – тривалість розробки підходу щодо забезпечення конфіденційності при передачі інформації в системах зв'язку з використанням динамічного хаосу, $t_м=70$;

$t_а$ – тривалість апробації підходу щодо забезпечення конфіденційності при передачі інформації в системах зв'язку з використанням динамічного хаосу, $t_м=32$;

$t_д$ – тривалість підготовки технічної документації, $t_д=20$.

Отже,

$$t = t_{тз}+ t_в+ t_а+ t_р+t_р+t_д = 24+40+24+30+70+32+20 = 240 \text{ години.}$$

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

$$К_{рп} = З_{зп} + З_{мч}.$$

$$К_{рп} = З_{зп} + З_{мч} = 36480+2368,8 = 38848,8 \text{ грн.}$$

$$З_{зп} = t*З_{пр} = 240*152 = 36480 \text{ грн.}$$

де t – загальна тривалість розробки політики безпеки, годин;

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

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

$$З_{мч}= t*С_{мч}=240*9,87=2368,8 \text{ грн.}$$

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

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

Вартість 1 години машинного часу ПК визначається за формулою:

$$C_{мч} = 1{,}1 \cdot 4 \cdot 1{,}68 + \frac{10200 \cdot 0{,}3}{1920} + \frac{8500 \cdot 0{,}2}{1920} = 9{,}87 \text{ грн.}$$

Відповідно до запропонованого підходу щодо забезпечення конфіденційності при передачі інформації в системах зв'язку з використанням динамічного хаосу передбачене використання наступного апаратного забезпечення:

- хаотичний генератор (вартість – 26600 грн.), 3 од.;
- генератор шуму (вартість – 25100 грн.);
- віднімаючий пристрій (вартість – 342 грн.).

Оцінка ефективності запропонованого підходу до прихованої передачі інформації, заснованого на явищах узагальненої хаотичної синхронізації і синхронізації, індукованої шумом була проведена шляхом моделювання в середовищі Matlab / Simulink. Зазначене програмне забезпечення вже використовується, тому в цьому випадку капітальні витрати не виникають.

Витрати на встановлення обладнання та налагодження системи інформаційної безпеки становитимуть 5000 грн.

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

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

$$= 38848{,}8 + 3*26600 + 25100 + 342 + 5000 = 149090{,}8 \text{ грн.}$$

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

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

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

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

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

$К_н$ – витрати на встановлення обладнання та налагодження системи інформаційної безпеки.

3.1.1 Розрахунок поточних витрат

Річні поточні витрати на функціонування системи інформаційної безпеки складають:

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

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

$С_к$ - витрати на керування системою в цілому;

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

Середовище Matlab/Simulink, яке застосовується для оцінки ефективності запропонованого підходу до прихованої передачі інформації, заснованого на явищах узагальненої хаотичної синхронізації і синхронізації, індукованої шумом, вже використовується на підприємстві, тому додаткові витрати щодо відновлення й модернізації системи не виникають.

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

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

Розробки підходу щодо забезпечення конфіденційності при передачі інформації в системах зв'язку з використанням динамічного хаосу передбачає придбання апаратного забезпечення, яке підлягає амортизації, відповідно до чинних вимог законодавства України. Амортизаційні відрахування на визначатимуться прямолінійним методом. Строк корисного використання кожного з об'єктів встановлений у 8 років. Річні амортизаційні відрахування наведені в таблиці 3.1.

Таблиця 3.1 – Річні амортизаційні відрахування

№ п/п	Об'єкт основних засобів	Вартість, грн.	Строк корисного використання, років	Сума амортизаційних відрахувань на рік, грн.
1	Хаотичний генератор	79800	8	$С_{а1}$ = 79800/8 = 9975
2	Генератор шуму	25100	8	$С_{а2}$ = 25100/8 = 3137,5
Сукупні річні амортизаційні відрахування ($С_а$):				*13112,5*

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 18400 грн. Додаткова заробітна плата – 10% від основної заробітної плати. Виконання роботи щодо впровадження системи захисту інформації на підприємстві потребує залучення спеціаліста інформаційної безпеки на 0,25 ставки. Отже,

$$С_з = (18400*12 + 18400*12*0,1)*0,25= 60720 \text{ грн.}$$

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

$$С_{єв} = 60720*0,22 = 13358 \text{ грн.}$$

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=1,1 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:

$$С_{ел} = 1,1*4*1920*1,68 = 14192,64 \text{ грн.}$$

Витрати на технічне й організаційне адміністрування та сервіс системи інформаційної безпеки визначаються у відсотках від вартості капітальних витрат – 2% ($С_{тос}$ = 149090,8*0,02=2981,82 грн.).

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

$С_к$ = 13112,5+60720+13358+14192,64+2981,82 = 104365 грн.

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

С = 104365 грн.

3.2 Оцінка можливого збитку від атаки на вузол або сегмент мережі

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, 3 години;

$t_{ви}$ – час повторного введення загубленої інформації співробітниками атакованого вузла або сегмента корпоративної мережі, 2 години;

$З_о$ – заробітна плата обслуговуючого персоналу (адміністраторів та ін.), 20100 грн./міс.;

$З_с$ – заробітна плата співробітників атакованого вузла або сегмента корпоративної мережі, 18400 грн./міс.;

$Ч_о$ – чисельність обслуговуючого персоналу (адміністраторів та ін.), 1 особи;

$Ч_с$ – чисельність співробітників атакованого вузла або сегмента корпоративної мережі, 4 осіб.;

О – обсяг прибутку атакованого вузла або сегмента корпоративної мережі, 500 тис. грн. у рік;

$П_{зч}$ – вартість заміни встаткування або запасних частин, 5200 грн.;

I – число атакованих сегментів корпоративної мережі, 1;

N – середнє число атак на рік, 24.

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:

$$П_{П} = \frac{\sum Зс}{F} \cdot t_{п} = \frac{18400 \cdot 4}{176} \cdot 2 = 836{,}36 \text{ грн.},$$

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 $t_{ви}$:

$$П_{ви} = \frac{\sum Зс}{F} \cdot t_{ви} = \frac{18400 \cdot 4}{176} \cdot 2 = 836{,}36 \text{ грн.}$$

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

$$П_{пв} = \frac{\sum Зо}{F} \cdot t_в = \frac{20100 \cdot 1}{176} \cdot 3 = 342{,}61 \text{ грн.}$$

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

$$П_в = 836{,}36+342{,}61+5200 = 6378{,}97 \text{ грн.}$$

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:

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

$$V = \frac{500000}{2080} \cdot (2+3+2) = 1682{,}69 \text{ грн.}$$

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.

$$U = 836{,}36+6378{,}97+1682{,}69 = 8898{,}02 \text{ грн.}$$

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

$$B = \sum_i \sum_n U = \sum_1 \sum_{24} 8898{,}02 = 213552{,}5 \text{ грн.}$$

3.2.1 Загальний ефект від впровадження системи інформаційної безпеки

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

$$E = B \cdot R - C \text{ грн.,}$$

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

R – вірогідність успішної реалізації атаки на сегмент мережі, частки одиниці (80%);

С – щорічні витрати на експлуатацію системи інформаційної безпеки.

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

$$E = 213552,5*0,8 – 104365 = 66477 \text{ грн.}$$

3.3 Визначення та аналіз показників економічної ефективності системи інформаційної безпеки

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

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

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

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

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

Коефіцієнт повернення інвестицій ROSI:

$$ROSI = \frac{66477}{149090,8} = 0,45, \quad \text{частки одиниці,}$$

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, (7%);

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

Розрахункове значення коефіцієнта повернення інвестицій:

$$0,45 > (7 – 5)/100 = 0,45 > 0,02.$$

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

$$T_O = \frac{K}{E} = \frac{1}{ROSI} = \frac{1}{0,45} = 2,22 \text{ років.}$$

3.4 Висновок

Таким чином, відповідно до наведених розрахунків можна зробити висновок, що розробка підходу щодо забезпечення конфіденційності при передачі інформації в системах зв'язку з використанням динамічного хаосу може вважатися економічно доцільною. Про це свідчить отримане значення коефіцієнту повернення інвестицій (ROSI=0,45), що є вищим за дохідність альтернативного вкладення. Капітальні інвестицій на забезпечення конфіденційності при передачі інформації в системах зв'язку з використанням динамічного хаосу величиною 149090,8 грн. дозволяють отримати економічний ефект величиною 66477 грн. Експлуатаційні витрати складають 104365 грн. Термін окупності – 2,22 років.

ВИСНОВКИ

1. В результаті аналізу принципів застосування хаотичних широкосмугових сигналів у системах прихованої передачі інформації 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 прихованої інформації.

2. В результаті аналізу існуючих підходів до прихованої передачі інформації в системах зв'язку з використанням динамічного хаосу встановлено їх недоліки. Принциповими недоліками всіх запропонованих в даний час схем є: вимога високого ступеня ідентичності хаотичних генераторів на різних сторонах каналу зв'язку; досить низька стійкість до шумів і флуктуацій в каналі зв'язку; можливість реконструкції параметрів передавального генератора по сигналу, що передається по каналу зв'язку (особливо в разі використання повної хаотичної синхронізації для прихованої передачі інформації). Недоліком відомого підходу до прихованої передачі інформації з використанням узагальненої хаотичної синхронізації (прототипу) є той факт, що сигнал, який передається по каналу зв'язку, несе на собі сліди модуляції керуючого параметра, що може дозволити третій стороні в деяких випадках декодувати інформаційне повідомлення. Таким чином, відомий підхід-прототип не забезпечує високу надійність передачі конфіденційної інформації.

3. Запропоновано підхід до прихованої передачі інформації, заснованого на явищах узагальненої хаотичної синхронізації і синхронізації, індукованої шумом, який включає в себе кодування корисного сигналу в двійковий код; формування за допомогою першого хаотичного генератора початкового детермінованого хаотичного сигналу шляхом модуляції параметрів хаотичного сигналу корисним цифровим сигналом; передача сформованого таким чином сигналу по каналу зв'язку приймаючій стороні; ділення сигналу в приймачі на два ідентичних сигнали, якими впливають на другий і третій хаотичні

генератори; подачу знятих з виходів другого і третього генераторів сигналів на віднімаючий пристрій; визначення наявності корисного цифрового сигналу, шляхом спостереження або відсутності хаотичних коливань. При цьому, в запропонованому підході було використано позитивний вплив шумів для підвищення надійності і створення додаткової секретності.

4. Результат оцінки ефективності запропонованого підходу до прихованої передачі інформації, заснованого на явищах узагальненої хаотичної синхронізації і синхронізації, індукованої шумом у порівнянні із підходом-прототипом доводить ефективність запропонованого підходу, а саме – забезпечення додаткового маскування переданого по каналу зв'язку сигналу і, отже, гарантія високого ступеня конфіденційності.

ПЕРЕЛІК ПОСИЛАНЬ

1. Дмитриев А. С., Кислов В. Я. Стохастические колебания в радиофизике и электронике. – М.: Наука. – 1989.

2. Короновский А.А. О применении хаотической синхронизации для скрытой передачи информации / А.А. Короновский, О.И. Москаленко, А.Е. Храмов // Успехи физических наук. – 2009. – Т. 179. – № 12. – С.1281-1310.

3. Агуреев К.И. Применение детерминированного хаоса для передачи информации / К.И. Агуреев // Известия ТулГУ. Технические науки. – 2014. – Вып. 11. – Ч. 2. – С.197-212.

4. Dmitriev A. S., Panas A. I., Starkov S. O. Direct Chaotic Communication in Microwave Band – Electronic NonLinear Science Preprint. http://arxiv.org/abs/nlin.CD/0110047.

5. Cuomo K. M., Oppenheim A. V., Strogatz S. H. Synchronization of Lorenz-based chaotic circuits with application to communications // IEEE Trans. Circ. Syst. – 1993. – II. 40. 10. – P. 626-633.

6. Dedieu H., Kennedy M.P., Hasler M. Chaos shift keying: Modulation and demodulation of a chaotic carrier using self-synchronizing Chua's circuits // IEEE Trans. Circuits and Systems. – Oct. 1993. – V. CAS-40. – № 10. – P. 634.

7. Дмитриев А. С. Успехи современной радиоэлектроники (Зарубежная радиоэлектроника) // А.С. Дмитриев, А.И. Панас, С.О. Старков. Динамический хаос как парадигма современных систем связи. – 1997. – № 10. – С.4-26.

8. Короновский А. А., Храмов А. Е. Непрерывный вейвлетный анализ в приложениях к задачам нелинейной динамики. – Саратов: Изд-во ГосУНЦ «Колледж», 2002. – С. 216.

9. Агуреев И.Е., Борзенкова С.Ю., Чечуга О.В., Яковлев Б.С. Использование мультиаттракторных систем для скрытой передачи и хранения информации // Известия ТулГУ. – Технические науки. – Вып.6. – Ч.2. – Тула: Изд-во ТулГУ, 2011. – С.337-345.

10. Агуреев И.Е., Агуреев К.И. Численный анализ процессов скрытой передачи информации на основе мультиаттракторной системы // Известия ТулГУ. Технические науки. – Тула: Изд-во ТулГУ, 2013. – № 10. – С. 169-177.

11. Агуреев И.Е., Агуреев К.И., Пастухова Н.С. Закономерности каскадов бифуркаций сингулярных аттракторов в некоторых системах скрытой передачи информации // Известия ТулГУ. Технические науки. – Тула: Изд-во ТулГУ, 2013. – № 11. – С.153-160.

12. Агуреев И.Е., Агуреев К.И., Гладышев А.В. Последовательности сингулярных аттракторов в некоторых автономных диссипативных мультиаттракторных системах // Известия ТулГУ. Технические науки. – Тула: Изд-во ТулГУ, 2013. – № 11. – С.160-171.

13. Магницкий Н. А. Теория динамического хаоса. – М.: ЛЕНАНД, 2011. – 320 с.

14. 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.

15. Русин Володимир Богданович. Моделювання методів управління динамічним хаосом та їх практичне застосування : дис. ... к-та. техн. наук : 01.05.02 / Русин Володимир Богданович. – Чернівці, 2017. – 147 с.

16. Rossler O. E. An equation for continuous chaos / O. E. Rossler // Phys. Lett. A. – 1976. – Vol. 57. – № 5. – P. 397–398.

17. Інтелектуальне моделювання нелінійних динамічних процесів в системах керування, кібербезпеки, телекомунікацій: підручник / В.І. Корнієнко, О.Ю. Гусєв, О.В. Герасіна; за заг. ред. В.І. Корнієнка ; М-во освіти і науки України, Нац. техн. ун-т «Дніпровська політехніка». – Дніпро : НТУ «ДП», 2020. – 536 с. – ISBN 978-966-350-735-4.

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. Патент US № 5291555. Communication using synchronized chaotic systems / K. Cuomo, A. Oppenheim. – Application granted 14.12.1992, publication 01.03.1994.

20. Dedieu H. Chaos shift keying: modulation and demodulation of a chaotic carrier using delf-synchronizing Chua's circuits / H. Dedieu, M.P. Kennedy, M. Hosler // IEEE Trans. on Circ. Sys. – I. 40. – 1993. – P. 634.

21. Dmitriev A.S. Experiments on speach and music signals transmission using chaos / A.S. Dmitriev, A.I. Panas, S.O. Starkov. // Int. J. Bifurcations and Chaos. – Vol. 5 (4). – 1995. – P. 1249.

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

23. Terry J.R. Chaotic communication using generalized synchronization / J.R. Terry, G.D. VanWiggeren // Chaos, Solitons and Fractals. – Vol. 12. – 2001. – P. 145.

24. Murali K. Secure communication using a compound signal from generalized synchronizable chaotic systems / K. Murali, M. Lakshmanan // Phys. Lett. – Vol. 241. – 1998. – P. 303.

25. Патент РФ № 2295835. Способ секретной передачи информации / А.А. Короновский, О.И. Москаленко, П.В. Попов, А.Е. Храмов – заявл. 30.12.2006, опубл. 20.03.2007.

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

27. Rulkov N.F. Generalized synchronization of chaos in directionally coupled chaotic systems. / N.F. Rulkov, M.M. Sushchik, L.S. Tsimring, H.D.I. Abarbanel. // Physical Review. – Vol. 51. – 1995. – P. 980-989.

28. Fahy S. Transition from chaotic to nonchaotic behavior in randomly driven systems / S. Fahy, D.R. Hamman. // Physical Review Letters. – Vol. 69. – 1992. – P. 761.

29. Abarbanel H.D.I. Generalized synchronization of chaos: The auxiliary system approach / H.D.I. Abarbanel, N.F. Rulkov, M. Sushchik. // Physical Review. – 1996. – Vol. 53, № 5. – P. 4528-4535.

30. Hramov A.E. Are generalized synchronization and noise-induced synchronization identical types of synchronous behavior of chaotic oscillators? / A.E. Hramov, A.A. Koronovskii, O.I. Moskalenko // Phys. Lett. – Vol. 354. – 2006. – P. 423.

31. Rico-Martinez R. Adaptive Detection of Instabilities: An Experimental Feasibility Study. / R. Rico-Martinez, K. Krischer, G. Flätgen, J.S. Anderson, I.G. Kevrekidis // Physica D: Nonlinear Phenomena. – Vol. 176, Issues 1-18. – 2003. – P. 1-18.

32. Hramov A.E. Generalized synchronization onset / A.E. Hramov, A.A. Koronovskii, O.I. Moskalenko // Europhysics Letters. – Vol. 72 (6). – 2005. – P. 901.

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

ДОДАТОК А. Відомість матеріалів кваліфікаційної роботи

№	**Формат**	**Найменування**	**Кількість листів**	**Примітки**
Документація				
1	А4	Реферат	3	
2	А4	Список умовних скорочень	1	
3	А4	Зміст	2	
4	А4	Вступ	2	
5	А4	Стан питання. Постановка задачі	34	
6	А4	Спеціальна частина	11	
7	А4	Економічний розділ	10	
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 Кроленко.ppt

2 Диплом Кроленко.doc

ДОДАТОК В. Відгук керівника економічного розділу

Керівник розділу _____ Пілова Д.П.

(підпис) (прізвище, ініціали)

ДОДАТОК Г. Відгук керівника кваліфікаційної роботи

В І Д Г У К

на кваліфікаційну роботу студента групи 125-17-1 Кроленко В.М. на тему: «Забезпечення конфіденційності при передачі інформації в системах зв'язку з використанням динамічного хаосу»

Пояснювальна записка складається зі вступу, трьох розділів і висновків, розташованих на 75 сторінках.

Мета роботи є актуальною, оскільки вона спрямована на підвищення надійності і створення додаткової секретності.

При виконанні роботи автор продемонстрував добрий рівень теоретичних знань і практичних навичок. На основі аналізу принципів застосування хаотичних широкосмугових сигналів у системах прихованої передачі інформації, а також існуючих підходів до прихованої передачі інформації в системах зв'язку з використанням динамічного хаосу в ній сформульовано задачі, вирішенню яких присвячений спеціальний розділ. У ньому було запропоновано підхід до прихованої передачі інформації, заснований на явищах узагальненої хаотичної синхронізації і синхронізації, індукованої шумом та оцінено його ефективність.

Практична цінність роботи полягає у тому, що запропонований підхід може бути використаний в системах зв'язку для забезпечення конфіденційної передачі інформації.

До недоліків роботи слід віднести недостатню проробку окремих питань.

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

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

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