ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет інформаційних технологій

Кафедра телекомунікацій, медійних та інтелектуальних технологій

ДИПЛОМНА РОБОТА

Другий (Магістерський)
Освітній рівень

Галузь знань 17 Електроніка та телекомунікації
Шифр і назва спеціальності

Спеціальність 172 Телекомунікації та радіотехніка
Шифр і назва спеціальності

на тему Система криптографічного захисту телефонних ліній

ДРМТР 202103.00.00

Виконав: студент 2 курсу, група $ТР_м$-20-1 _____ С.С. Гринь
підпис Ініціали, прізвище

Керівник: к. т. н. , доц. _____ А.А. Таранчук
підпис Ініціали, прізвище

До захисту допускаю:

Зав. кафедри: д-р техн. наук, доц. _____ С.К. Підченко
підпис Ініціали, прізвище

__3___ __грудня__2021 р.

Хмельницький, 2021

Хмельницький національний університет
Факультет *інформаційних технологій*
Кафедра *телекомунікацій, медійних та інтелектуальних технологій (ТМІТ)*
Освітній рівень *другий (магістерський)*
Галузь знань *17 – Електроніка та телекомунікації*
Спеціальність *172 – Телекомунікації та радіотехніка*
Освітня-професійна програма *Телекомунікації та радіотехніка*

ЗАТВЕРДЖУЮ
Зав. кафедрою ТМІТ
_____С.К. Підченко
«2» вересня 2021 р.

ЗАВДАННЯ
НА ДИПЛОМНУ РОБОТУ

Гриню Сергію Сергійовичу

1 Тема роботи: *Система криптографічного захисту телефонних ліній*

Керівник роботи Таранчук Алла Анатоліївна.
Затверджено наказом по університету від «25» серпня 2021р. № 102
2 Строк подання студентом роботи на кафедру:01.12.2021р.
3 Вихідні дані (характеристика об'єкта, умов дослідження та ін.)
Мета роботи: вдосконалення методів криптографічного захисту телефонних ліній на базі застосування сигналів детермінованого хаосу.
Об'єкт дослідження: процеси захисту від несанкціонованого доступу систем передачі сигналів.
Предмет дослідження: система криптографічного захисту телефонних ліній із застосуванням сигналів детермінованого хаосу.
4. Зміст пояснювальної записки (перелік питань, що їх належить розробити)
1. Аналіз існуючих систем криптографічного захисту та їх криптографічної стійкості. 2. Способи та методики використання сигналів детермінованого хаосу для підвищення безпеки передачі сигналів телефонними лініями. 3. Розробка системи із застосуванням сигналів детермінованого хаосу для передачі телефонних повідомлень цифровими сигналами. 4. Розробка системи із застосуванням сигналів детермінованого хаосу для передачі телефонних повідомлень аналоговими сигналамиу тональному спектрі.

Завдання отримав_____С.С. Гринь

Науковий керівник_____А.А. Таранчук

КАЛЕНДАРНИЙ ПЛАН

№ п/п	Назва етапів (розділів) дипломної роботи	Строк виконання етапів дипломної роботи	Примітка
1	*Вибір тематики роботи*	*до 25.08.21*	*обрано*
2	*Аналіз можливостей криптографічного захисту*	*до 5. 09. 21*	*проаналізовано*
3	*Написання 1 розділу (телефонний звязок)*	*до 15.09. 21*	*виконано*
4	*Оформлення 2 розділу (хаотична криптографія в телефонії)*	*до 25.09.21*	*виконано*
5	*Імітаційне моделювання в середовищі Matlab\Simulink*	*до14.10. 21*	*виконано*
6	*Оформлення 3 розділу (цифрова реалізація)*	*до24.10. 21*	*виконано*
7	*Подання публікації з тематики роботи*	*до 10.11.21*	*подано*
8	*Технічне оформлення тексту, плакатів, рисунків, додатків висновків, тощо*	*до 20.11. 21*	*оформлено*
9	*Врахування зауважень керівника, дооформлення*	*до 25.11. 21*	*враховано*
10	*Кінцеве оформлення роботи*	*до 30.11. 21*	*реалізовано*
11	*Подання готового проекту до ДЕК*	*1.12. 21*	*подано на каф.*

Студент _____ _____ С.С. Гринь
Підпис Ініціали, прізвище

Керівник роботи _____ А.А. Таранчук
Підпис Ініціали, прізвище

РЕФЕРАТ

Дипломна робота магістра на тему «Система криптографічного захисту телефонних ліній» виконана студентом 2-го курсу гр. ТРм-20-1 Гринь Сергієм Сергійовичем на кафедрі «Телекомунікацій, медійних та інтелектуальних технологій» Хмельницького національного університету у 2021р. Керівник роботи доц. каф. Таранчук Алла Анатоліївна.

Робота складається із вступу, 3 розділів, основних висновків по роботі, переліку джерел посилання (45 бібліографічних посилання, 5 сторінок) та 4 додатків (13 сторінок). Загальний обсяг роботи в якому викладено основний зміст складає 85 сторінок і містить 39 рисунків на 36 сторінках по тексту та 21 формулу. Повний обсяг роботи - 120 сторінок.

Дипломна робота присвячена розробці системи захисту телефонних ліній від несанкціонованого доступу через перетворення аналогових повідомлень за допомогою хаотичних методів обробки із використанням явищ хаотичної синхронізації та хаотичного синхронного відгуку. Запропоновано структурну схему системи, імітаційну модель та проведені необхідні дослідження для підтвердження функціонального призначення системи загалом.

Ключові слова: телефонний зв'язок, криптографія, генератор детермінованого хаосу, хаотична синхронізація.

ABSTRACT

Master's thesis proposal «An encrypted security system for telephone lines» written Gryn Serhii Serhiyovych, a 2nd year student of group ТРм-20-1 at the Department of Telecommunications, Media and Intellectual Technologies of Khmelnytsky National University, in 2021. Academic advisor – Taranchuk Alla Anatoliivna, Associate Professor.

The thesis proposal consists of an introduction, 3 sections, main scientific findings, a list of works cited (45 bibliographic references on 5 pages) and 4 items of additional materials (on 13 pages). The total volume of the thesis in which the main content is stated is 85 pages; it contains 39 figures on 36 pages of text and 213 formulas. The full volume of the thesis is 120 pages.

The thesis is concerned with the development of a system for securing telephone lines against unauthorized access through the conversion of analog messages using chaotic processing methods based on the phenomena of chaotic synchronization and chaotic synchronous response. The structural scheme of the system and the simulation model are proposed. The necessary research for confirmation of the functional purpose of the system as a whole is carried out.

Key words: telephone communication, cryptography, deterministic chaos generator, chaotic synchronization.

ЗМІСТ

СКОРОЧЕННЯ ТА УМОВНІ ПОЗНАКИ

АШ - алгоритм шифрування

БГШ – білий гаусівський шум

ВКФ – взаємна кореляційна функція

ГДХ – генератор детермінованого хаосу

ДА – дивний атрактор

КШ – ключ шифрування

НДС – нелінійна динамічна система

СДХ – сигнал детермінованого хаосу

СКВ – середньоквадратичне відхилення

ФНЧ – фільтр низьких частот

ОП – оптимальний приймач

РС - регулярний сигнал

ФПР – фазовий простір

ФТР – фазова траєкторія

ТЛ – телефонна лінія

ТК – телефонний канал

ТС – тональний спектр

ХГ –хаотичний генератор

SNR – відношення сигнал-шум

THD – коефіцієнт гармонік

RMS – ефективне значення сигналу

ВСТУП

Захист інформації в сучасному суспільстві одне із найважливіших завдань розвитку, без захисту інформації неможливе існування сучасної економіки в тому вигляді, що ми знаємо. Парадигма захисту інформації пов’язана із наданою природою можливістю людини мати та зберігати конфіденційні думки та наміри, що властиві тільки певній особі [1-3].

Із розширенням зони спілкування через появу потужних телекомунікаційних засобів, проблематика захисту інформації стає все більш гостріше. Доступ до «чужих» таємниць в мережі дозволяє зловмисникам не тільки проводити психологічну дискредитацію певної особи серед оточення, але заробляти на цьому чималі гроші, що є загалом кримінальними діями, які караються, і досить жорстко, сучасним законодавством [4-6].

Найкращим способом забезпечення проблематики захисту інформації є прихованість дії [7]. Прихованість дії забезпечує захист через неможливість виявлення навіть факту передачі сигналів. Природною прихованістю дії забезпечене функціонування мозку людини (поки читання думок недоступне), також прихованість дії в сучасних телекомунікаціях досягається через наявність величезної кількості інформаційних потоків (штучних та природник), що передаються різноманітними радіо та оптичними телекомунікаційними системами, в яких легко «загубитися» поодинокому телекомунікаційному каналу [4].

Для виділення інформації із цього потоку зловмиснику слід мати ряд апріорних даних (криптографічних ключів) [8-10], що дозволять йому здійснити перехоплення повідомлення, а також відповідну апаратуру. Часто це завдання настільки довготривале та складне, що підготовка до доступу в прихованому каналі з боку зловмисника надто довготривала. За цей тривалий час актуальність інформації буде втрачена, а всі зусилля зловмисника – марними.

Другий шлях захисту інформації – криптографічний [8-10], що передбачає застосування алгоритмів перетворення інформації, таким чином, щоб за умови можливості виявлення факту передачі, забезпечувалась неможливість виявлення її змісту. Під час такого процесу слід задовольняти ряд вимог узгодження із існуючою апаратурою, каналами зв’язку, застосованими сигналами, роботи в реальному часі, тощо.

Загалом проблематикою захисту інформації через різноманітні перетворення займається наука - криптологія (kryptos - таємний), що має дві частини протилежні за функціями: криптографію і криптоаналіз[11].

Часто під криптографією розуміють саме цифрові алгоритми, які прийнято називати шифруванням, хоча це не зовсім коректно. Великий розділ криптографії прийнято називати крипто аналізом, або дешифруванням, що охоплює алгоритми «зламу» коду та дослідження їх можливостей для роботи без втрати актуальності повідомлення (реальному часі) [12].

Основні зони використання криптографічних алгоритмів - це передача конфіденційних даних каналами зв'язку (наприклад, телефонія, SMS, Інтернет меседжери) та довготривале збереження даних в архівах та базах даних (бібліотеках) на електронних носіях у шифрованому вигляді [13-16].

Сучасна класична цифрова криптологія найбільш часто досліджує та розробляє такі напрямки [18-20]:

·А) симетричні цифрові кодеки шифрування (із секретним ключем);

Б) несиметричні цифрові кодеки шифрування (з відкритим ключем);

·В) системи додавання та фіксації авторизації користувача (електронного підпису);

Г) системи розподілу та управління ключами шифрування.

Діючі криптографічні системи захисту забезпечують високу криптографічну стійкість інформації в першу чергу за рахунок підтримки втаємничення ключів шифрування. Якщо в наявності певна апаратна підтримка, то будь-який ключ та алгоритми можуть бути підібрані. Вся

складність полягає у часі такого підбору та застосованих ресурсах, що визначається трудомісткістю криптоаналізу. Через це виникає необхідність вимірювання або оцінювання криптологічної стійкості шифрів, що власне є окремим завданням.

Застосування криптографії може бути не тільки для передавання даних та блокування їх перехоплення зловмисником, але і для: · аутентифікації; · забезпечення цілісності; досягнення · незаперечності.

Останніми десятиліттями з'явились вдалі спроби застосувати новітні методи забезпечення криптографічної стійкості на основі застосування методів, що лежать в основі нелінійних динамічних систем із використанням сигналів детермінованого хаосу [22-25]. Такі методи дозволяють вирішити як завдання прихованості дії, так і завдання забезпечення захисту від несанкціонованого доступу (криптології в широкому розумінні).

Застосування таких методів стало можливим через появу елементної бази із стабільними та точними параметрами та характеристиками. Одним із варіантів подібних систем забезпечення захисту від несанкціонованого доступу є квантові системи, що ґрунтуються на квантовій теорії поля та зчеплених квантових станах квантових носіїв [25].

Сигнали детермінованого хаосу за структурою є близькими до природних завад, наприклад, теплових шумів, тому можуть легко «загубитися» серед них у випадку застосування як носіїв в системах прихованого зв'язку. Також ці сигнали створюються в унікальних умовах генераторів детермінованого хаосу, що можливі лише за певних обставин, і для певних структур генеруючих схем. Ці обставини, разом із новітніми методами, точністю встановлення та різноманітністю структур генераторів детермінованого хаосу складають основу складного ключа криптографічного захисту як для цифрових так і для аналогових каналів передачі [26-27]. Розробка подібних систем має великі перспективи і є на даний час, особливо в умовах військової агресії, та є актуальним завданням для виконання в наукових роботах.

Мета роботи: вдосконалення методів криптографічного захисту телефонних ліній на базі застосування сигналів детермінованого хаосу.

Для досягнення вищевказаної мети в слід вирішити такі з***авдання***:

1. Провести аналіз можливостей застосування принципів, методів та методик захисту інформації від несанкціонованого доступу. Виділити перспективні напрямки, підходи та алгоритми щодо отримання високого рівня криптографічної стійкості.

2. Провести аналіз тактико-технічних характеристик телефонних каналів зв'язку та можливостей застосування методів та засобів захисту інформації для забезпечення високого рівня криптографічної стійкості за умови обмежень що накладаються з боку каналоутворюючої апаратури передачі тонального спектру.

3. Провести порівняльний аналіз застосування нелінійних динамічних систем із сигналами детермінованого хаосу для вирішення криптографічних завдань з точки зору еквівалентності перетворень повідомлень для забезпечення високого рівня прихованості дії та криптографічної стійкості.

4. Запропонувати структури схем передачі аналогових повідомлень із застосуванням методів обробки хаотичних сигналів на основі систем односпрямованої хаотичної синхронізації для одночасного підвищення прихованості дії та криптографічної стійкості захисту інформації аналогових повідомлень.

5. Провести імітаційне моделювання запропонованих методів шифрування та алгоритмів обробки зашифрованих повідомлень для підтвердження запропонованих методів захисту інформації аналогових повідомлень від несанкціонованого доступу.

Об`єктом дослідження є процеси захисту від несанкціонованого доступу систем передачі сигналів.

Предметом дослідження є система криптографічного захисту телефонних ліній із застосуванням сигналів детермінованого хаосу.

Наукова новизна одержаних результатів:

1. Запропоновано метод одночасного забезпечення прихованості дії та криптографічної стійкості аналогових телефонних повідомлень, що відрізняється застосуванням для передачі даних генераторів детермінованого хаосу із багатопараметричною модуляцією хаотичної піднесівної та детектуванням повідомлень на базі допоміжного хаотичного генератора із визначенням рівня сигналу за різницевою потужністю ведених генераторів, що дає можливість використати поле параметрів хаотичного генератора як ключі шифрування, а шумоподібний сигнал детермінованого хаосу для прихованості дії.

2. Запропоновано метод покращення криптографічної стійкості передачі аналогових повідомлень на основі застосування хаотичної піднесівної та параметричної модуляції інформаційним повідомленням веденого генератора, що відрізняється введенням інформації про траєкторію руху параметрів в багатовимірній площині параметрів під час модуляції інформаційного повідомлення. Збільшення параметрів для формування ключа шифрування різко збільшує криптографічну стійкість без порушення прихованості дії.

Практичне значення одержаних результатів:

1. Показано безпосередній еквівалентний діалектичний зв'язок між процесами та об’єктами криптографічного захисту та об’єктами та процесами нелінійної динаміки систем із сигналами детермінованого хаосу, що підтверджує можливість необхідність застосування хаотичних методів обробки в аналогових системах із захистом інформації на основі прихованості дії та впровадження криптографічних алгоритмів.

2. Запропоновано для забезпечення високого рівня криптографічного захисту застосувати методи хаотичної синхронізації та хаотичного синхронного відгуку під час взаємодії веденого та ведучого хаотичного генераторів, що дозволяє проводити детектування аналогових повідомлень за критерієм рівня синхронізму хаотичних генераторів в системі.

3. Запропонована методика використання лінійних ділянок залежностей рівня синхронізації на багато параметричній площині для формування ключів шифрування аналогових повідомлень в хаотичній системі передачі аналогових повідомлень по телефонним каналам передачі.

4. Запропоновано методики побудови імітаційних моделей та субмоделей каналів передачі аналогових повідомлень, що дозволяє проводити аналіз тактико-технічних характеристик каналів передачі аналогових повідомлень в обмеженому спектрі через багатопараметричну модуляцію біфуркаційних параметрів, за умови широкого діапазону відношень сигнал-завад, застосування різних типів та класів хаотичних генераторів, тощо.

Апробація результатів досліджень. Результати досліджень представлені в збірнику наукових праць молодих науковців і студентів «Актуальні проблеми комп'ютерних наук – 2021» м. Хмельницький та у тезах доповідей XVII міжнародної науково-практичної конференції «Військова освіта і наука: сьогодення і майбутнє» м. Київ 2021 (додаток Г).

1 КРИПТОГРАФІЧНІ СИСТЕМИ ТА ТЕЛЕФОННИЙ ЗВЯЗОК

1.1 Криптологія як наука

1.1.1 Основні криптологічні поняття

Із методологічної точки зору криптологія сформувалась як галузь науки і техніки про захист інформації від несанкціонованого доступу за допомогою перетворення форми її матеріальних носіїв, щоб ця форма була недоступна для зловмисника, ворога, конкурента (рис.1.1). Криптологія поєднує дві великих частини, кожна із яких займається власним завданням: криптоаналіз і криптографія. При цьому передбачається, що перетворене повідомлення доступно в однаковій якості як для абонента так і для зловмисника[4].

Криптографія та криптоаналіз сильно взаємно пов’язані між собою, прориви в одній галузі сприяють розвитку іншої. Однак їх можливо розглядати і як дві протилежні сутності, що ворогують між собою і в цій ворожбі і є їх сила з філософської точки зору [10].

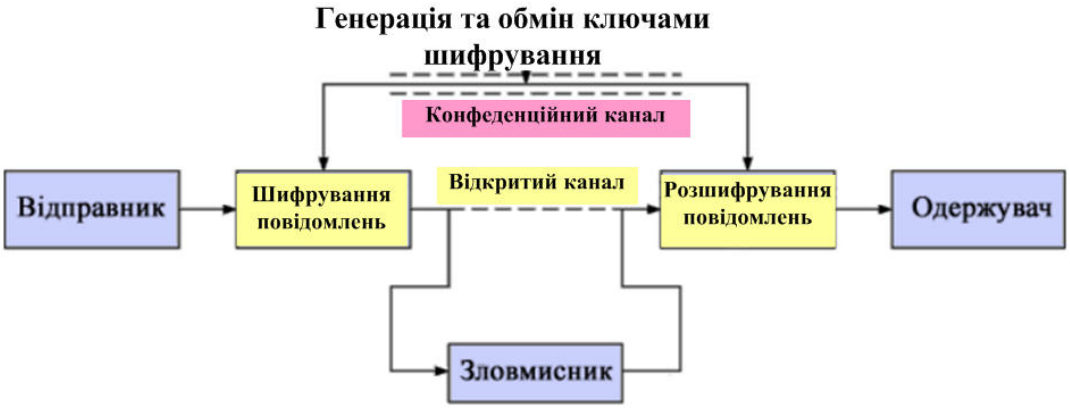


Рисунок 1.1 – Схема забезпечення шифрування повідомлень від несанкціонованого доступу

Криптографія (рис.1.2) займається пошуком і дослідженням методів та методик перетворення сигналів про повідомлення із метою приховування його змісту для «сторонніх очей». Основними напрямками діяльності криптографії є забезпечення конфіденційності каналів зв'язку, підтвердження не спотворення повідомлення у каналі, зберігання повідомлень на матеріальних носіях у зашифрованому вигляді.

Рисунок 1.2 – Структура понять криптології

На противагу криптографії, криптоаналіз пропонує та проводить аналіз дослідження можливостей доступу до конфіденційної інформації без апріорних відомостей про ключі шифрування [17]. У якості змісту повідомлень, що підлягають шифруванню й дешифровуванню часто розглядають, тексти, мову, відеосигнали, тощо, але в цифрових системах все це можливо представити у вигляді одного або декілька відео потоків, що підлягають шифрування та дешифруванню в реальних ділянках часу. В дискретних системах основою вхідних даних є алфавіт[1].

Алфавіт — це деяка кінцева множина використовуваних для шифрування повідомлень знаків, під знаком можливо також розуміти пакет бітів, що кодує його, або систему знаків національного алфавіту, ієрогліфів, тощо. Повідомлення різного характеру формуються із упорядкованого за правилами і протоколами набір з елементів знаків алфавіту, наприклад, текст, мова, кадри, пакети, тощо [14].

Захистом повідомлень від несанкціонованого доступу займається шифрування [20], що являє собою певний протокол дій за встановленим алгоритмом на основі ключа шифрування (рис.1.3), що призводить до незрозумілості повідомлення для конкурента. Дешифрування – процес зворотний шифруванню, що за наперед відомим ключем шифрування та алгоритмом однозначно відновлює первинне повідомлення для сприйняття коректним адресатом.

Рисунок 1.3 – Схема мережевого шифрування

Ключ шифрування – найважливіший елемент криптографії, і являє собою параметр або сукупність значень параметрів криптографічного алгоритму обробки повідомлення, що і забезпечує однозначний вибір тільки одного варіанту шифрування з усіх можливих для заданої методики виконання алгоритму. Часто зручно обирати ключем деяку послідовність символів використаного алфавіту. Набір можливих значень ключів шифрування називають простором ключів [20].

Усі криптографічні системи шифрування можливо поділити на симетричні й асиметричні (або із закритим та відкритим ключем). Якщо для процесу шифрування і дешифрування використовують один і той самий ключ, то таку систему називають симетричною. У асиметричні системи використовують 2 ключі: доступний для всіх один для шифрування, а інший, секретний, для дешифрування. Обидва ключі складним чином математично пов’язані один із одним, та забезпечення їх «зв’язку» часто і є завданням криптографії [17].

Багато телекомунікаційних систем потребують систем розподілу та обробки інформації на основі статичного та динамічного розподілу ключів та шифрів і це потребує додаткового секретного каналу обробки адміністративних ресурсів[19].

Кожна система шифрування характеризується криптологічною стійкістю до «зламу» без наявності точних відомостей про ключі шифрування, чим фактично і займається криптоаналіз. Основними показниками криптостійкості є: потужність поля незалежних величин для формування ключів шифрування та середній час проведення криптоаналитичної атаки за допомогою заданих методик та заданого устаткування, в тому числі і комп’ютерного.

Завданням криптографії є також забезпечення повідомлень абонентів механізмом достовірності переданого повідомлення, що робиться за допомогою електронного цифрового підпису - деякої ідентифікуючої інформації додатково введеної в первинне повідомлення в секретному місці і відоме лише автору повідомлення (або його комп’ютеру).

Криптологічною стійкістю називається характеристика шифру, що визначає його стійкість до розшифровування без знання ключа (тобто криптоаналізу). Є кілька показників криптостійкості, серед яких: кількість усіх можливих ключів; середній час, необхідний для успішної криптоаналитичної атаки того або іншого виду[20].

Таким чином рівень криптозахисту повідомлення телекомунікаційних систем, в тому числі і телефонних повідомлень забезпечується таємницею збереження шифру та криптостійкістю алгоритму шифрування.

1.1.2 Історія та різновиди криптологічних систем шифрування

Коли писемність тільки починала розвиватися і була відома обмеженій кількості грамотних людей, найчастіше релігійних представників високого рангу, то писемність сама виступала як крипто логічний шифр, невідомий багатьом. Але із поширенням алфавітів та писемності через наявність торгівлі, війн, дипломатичних відносин, що мають утаємничувати повідомлення, виникає потреба різко обмежувати кількість осіб, що мала доступ до конфіденційної інформації (осіб, які могли б зрозуміти шифрограму). Такі потреби сприяли появі перших крипто логічних винаходів - систем тайнопису. Процес розробки тайнопису відбувався паралельно в різних країнах світу в Єгипті, Месопотамії, Греції, Італії, Китаї, тощо [16-20].

Першими було розроблено та впроваджено в тайнопис перестановочні шифри, які змінюють порядок знаків в повідомленні за заданим алгоритмом і шифри, алгоритм дії яких полягає у заміні знаків або груп знаки іншими знаками або групами знаків із основного або додаткового алфавіту. Для шифрування навіть розроблялись механічні засоби, наприклад, про що сповіщає Плутарх у своїх літописах.

Перші досягнення із точки зору теорії ймовірностей в криптологія зробили араби, що визначили частоту повторення знаків в арабському алфавіті. Стрімке використання та розвиток криптографії відбувся в період пізнього середньовіччя Європі через ускладнення політичної ситуації, одночасно це потребувало більш надійного захисту від несанкціонованого доступу дипломатичних послань. У посольствах створювались шифрувальні відділи, де власне з’явилася професія шифрувальника та крипто аналітика

[20], які займались перехопленням листування. Першим друкованим твором (1513 р.) із криптологія вважається "Поліграфія" Дж. Тритеміуса. З цих пір фахівці - шифроаналітики відігравали в історичних подіях надзвичайно велику, хоча іноді не помітну роль.

Хоча історія криптоаналізу та шифрування нараховує вже більш як 4000 років, але криптологи вважають, що голландський вчений Керкхоф у своїй першій теоретичній роботі висунув головні правила (рис.1.4), з якими оперує криптологія і донині [19]:

1) Тайна збереження ключа і є стійкістю шифру.
2) Алгоритм шифрування та зашифроване повідомлення достовірно відоме криптоаналітику.

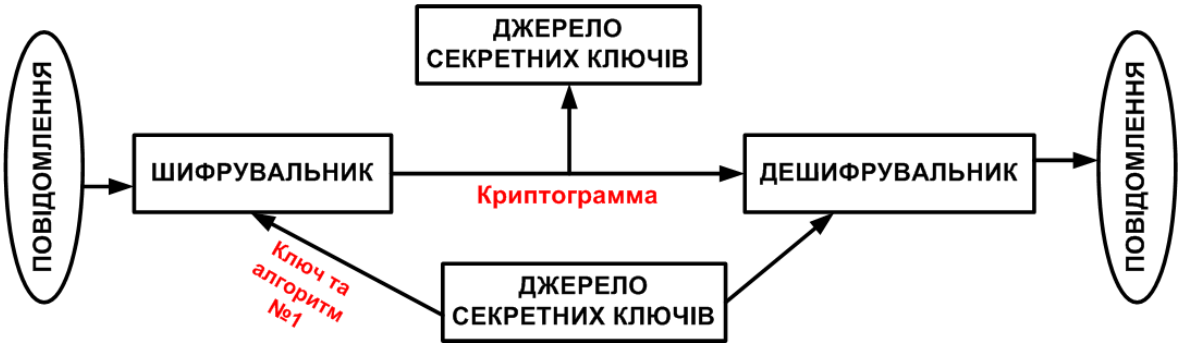


Рисунок 1.4 – Схема системи шифрування повідомлень

Один із ранніх алгоритмів шифрування вигадали римляни, для яких безпечний обмін повідомлення в військових кампаніях був життєво важливим. Шифр дістав назву шифру Цезаря, хоча сам Юлій Цезар навряд його вигадав. Суть алгоритму Цезаря полягає в тому, що кожен знак повідомлення замінювався літерою, що йшла в абетці через кілька знаків за даною літерою, наприклад через 3…5 позицій (для зручності).

На даний час більшість криптологів вважає, що криптологія саме як галузь науки і техніки виникла в 1949 році після появи статті основоположника теорії інформації К. Шенона - «Теорія зв'язку в секретних

системах» [16]. К. Шенон ввів поняття «секретна система» і зазначив можливі їх різновиди [19]:

1) Секретні системи маскування, що натепер називають системи забезпечення прихованості дії. Вони можуть застосовувати такі методи як, як наприклад, невидимі чорнила, де факт присутності секретної інформації в повідомленні прихований від конкурента (стеганографія).
2) Таємні засоби та системи шифрування (наприклад, написання мови ззаду наперед), що потребують для дешифрування секретної інформації в повідомленні потрібно спеціальних засобів (трафаретів, таблиць, машин, тощо).
3) Класичні системи шифрування, де інформаційний зміст повідомлення приховується за допомогою алгоритму шифрування та ключа шифрування, але сам фізичний сигнал повідомлене доступно для прийняття широкому колу адресатів, в тому числі і конкурентам або зловмисникам.

Предметом розгляду у цій роботі є криптологічні системи третього типу за Шеноном.

1.1.3 Класифікація та відмінності алгоритмів шифрування

Історичної точки зору алгоритми шифрування(рис.1.5) пройшли великий шлях [20], на якому можливо виділити три історичні епохи:

1) Донаукова криптологія(епоха до 1949 р.), в таку епоху алгоритми шифрування та дешифрування запропоновувались безсистемно (рис.1.6), «на вдачу», що продовжувалось до появи вже вищезгаданої праці Шенона із передавання секретної інформації.
2) Наукова дискретна та аналогова криптологія (епоха тривала із 1949 р. по сімдесяті роки 20 сторіччя), характеризувалась розробкою

основних алгоритмів та принципів математичного підтвердження якості їз роботи.

3) Наукова цифрова криптологія (із сімдесятих років 20 сторіччя дотепер), що характеризується широким використанням ЕОМ з використанням ЕОМ.
4) Квантова криптологія, що розвивається останнім десятиліттям, має надзвичайно великі потенційні можливості та використовує можливості якісно нових принципів побудови квантових комп'ютерів та їх підтримкою реалізації з боку технічних досягнень людства.

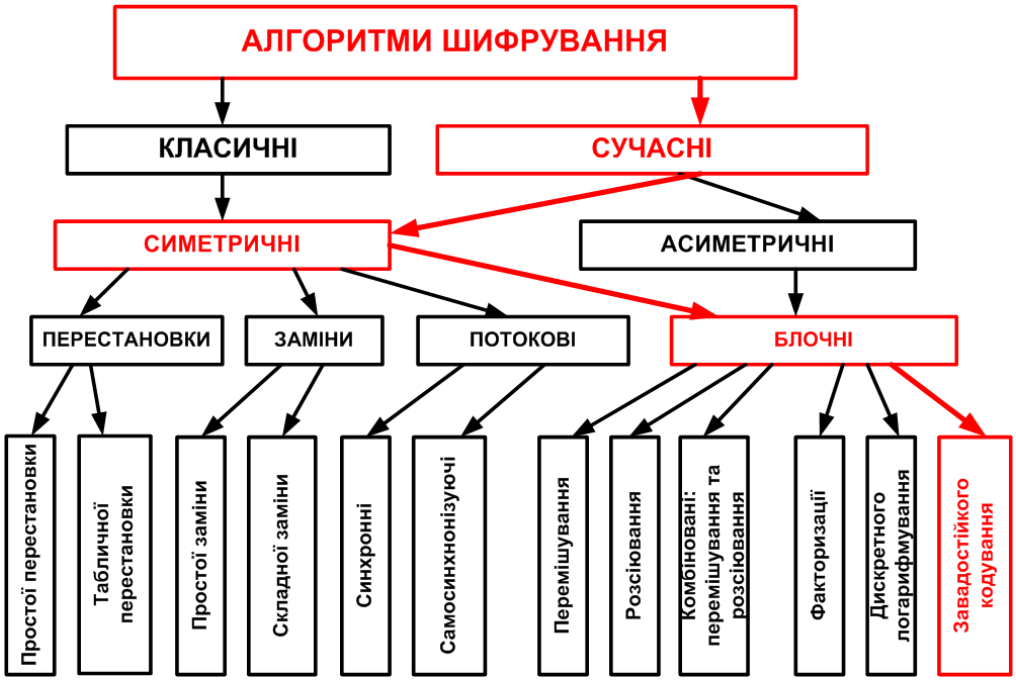


Рисунок 1.5 – Класифікація алгоритмів шифрування

Донаукова криптологія (класичні алгоритми) аж до початку 20-го століття, переважно застосовували лінгвістичні схеми шифрування, а натепер, зараз криптографія та крипто аналітика інтенсивно використовує такі математичні розділи як: теорія інформації (рис.1.5), теорія нечітких множин, теорія груп, математичної статистики, комбінаторики, тощо [14].

Слід пам’ятати, що на відміну від інших «логій» криптологія також включає в себе психологічні аспекти людського розуму та розумової діяльності і хоча часто криптологія вважають відгалуженням інженерії, слід пам’ятати, що крипто захист має також справу із винахідливим, хитрим та розумним конкурентом (ворогом, супротивником), а більшість інших видів природничих наук мають справу з діючими однаково на всіх абонентів природними завадами, впливами, навантаженнями, тощо.

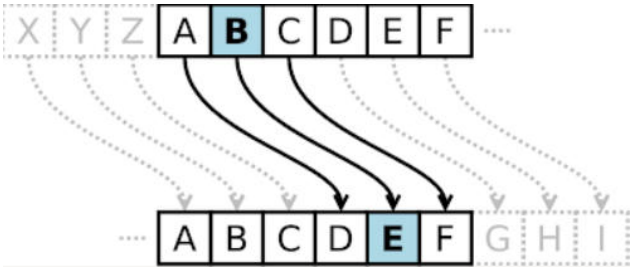


Рисунок 1.6 – Механізм шифрування за способом Цезаря

Розподіл на криптологічні епохи враховує основні події в науковій думці фахівці цієї галузі від мистецького підходу в класичну епоху, до чітких доведень в наукову епоху.

Суттєвий прорив у криптології здійснився із появою комп’ютерів, що дозволило пришвидшити криптоаналіз через прямий перебір ключів шифрування, але і можливості криптографії щодо генерації нових шифрів також зрости. Перші спроби застосувати комп’ютерні засоби були зроблені ще в 1942 у Великобританії А. Тюрінгом за допомогою ЕОМ "Колос" для дешифрування повідомлень німецько-фашистської шифрувальної машинки Энігма [9].

Класична епоха криптологія оперувала переважно із текстами за допомогою фактично тільки двох алгоритмів заміни й перестановки (рис.1.1). Перестановка це зміна позицій розташування знаків без зміни алфавіту за деяким правилом, а алгоритми заміни ґрунтуються на замінах знаків відкритого тексту знаками шифрованого тексту. Як правило класичні алгоритми шифрування мали власне ім’я.

Надалі, вже в наукову епоху, основними алгоритмами шифрування в криптографії стають алгоритми розсіювання й перемішування (рис 1.1)[14]. Із потребою формування бітових або блочних потоків під час цифрових телекомунікацій виділяються блокові і потокові алгоритми шифрування.

Суть блокових шифрів полягає у розбитті повідомлення на блоки із певною кількістю бітів, де кожний блок може бути зашифрований власним алгоритмом, але загальний алгоритм перемішування залишається однаковим для всієї послідовності блоків, наприклад, алгоритм DES.

Під час застосування потокових алгоритмів кожний знак неперервного повідомлення шифрується незалежно і головною проблемою створення потокового алгоритму є генерація допоміжних шифруючи послідовностей із дуже жорсткими вимогами щодо їх шумоподібності та синхронної генерації на приймальному та передавальному боці. Проблема синхронізації під час шифрування настільки важлива, що такі шифри поділяють на само синхронізуючі і з зовнішньою синхронізацією (синхронні).

Головною ідеєю під час створення асиметричних алгоритмів [18-20] є генерація відкритого та закритого ключа, перший призначений тільки для шифрування і поширюється по відкритих каналах зв'язку, другий (секретний ключ) призначений для дешифрування інформації. Математичною основою таких алгоритмів є математичні завдання із принципово тривалим та важким рішенням, наприклад, задачі пов’язані із завадостійким кодуванням, факторизацією (рис.1.5), розкладом на множники, пошуком простих чисел тощо, для яких існують жорсткі докази безпечності застосування в криптології.

В умовах сучасного розвитку систем захисту інформації розробникам алгоритмів шифрування також слід брати до уваги темпи удосконалення апаратної бази та технологій криптоаналізу. Наприклад, експоненційне зростання потужності комп’ютерів дозволяє сучасним смартфонам практично миттєво розшифровувати усі алгоритми донаукової епохи.

1.2 Телефонний зв’язок

1.2.1 Телефонні канали зв’язку

Для організації телефонного зв'язку між абонентами використовуються телефонні канали зв'язку, які мають смугу частот в діапазоні від 0,3 до 3,4 кГц. Канали передачі інформації з такою смугою прозорості називають каналами тональної частоти (ТЧ). Через надзвичайно велике поширення телефонного зв’язку характеристики цих каналів тональної частоти нормуються таким чином, щоб їх також можна було застосовувати для телеграфування, факсимільного зв’язку, передачі цифрових даних. Це можливе в усіх випадках, коли продуктивність повідомлень що передаються через такі канали не більше пропускної спроможності каналу тональної частоти [5].

Телефонні канали з боку абонента можуть використовуватися в одній із наступних схем включення:

1) двопровідну схема, що застосовується для проводових ліній дуплексного зв’язку;
2) чотирипроводова схема, що часто застосовується для радіоканалів.

Під час двопроводового режиму передача і прийом сигналів від апаратури вищих рівнів до абонента здійснюється почергово по колу із двох дротів, що складають абонентську лінію.

В чотирипроводній схемі включення тракти передачі і прийому телефонних сигналів розділені в просторі та практично не впливають один на одного завдяки тому, що ці сигнали передаються по фізично розділеним двом парам провідників [3].

Сучасна апаратура каналоутворення для багатоканальних телефонних аналогових систем передачі дозволяє також створити канали із більш

високою пропускною спроможністю через поєднання пропускних спроможностей декількох стандартних телефонних каналів із розширенням припустимої смуги частот. В наявній апаратурі систем телефонних телекомунікацій передбачається утворення каналів із наступними частотними ресурсами:

- 12...24 кГц (передгруповий канал);
- 60..108 кГц (первинний канал);
- 312...552 кГц (вторинний канал);
- 812...2044 кГц (третинний канал).

Широкосмугові групові телефонні канали застосовуються для транзиту груп стандартних телефонних каналів; сигналів радіо телемовлення, та цифрових даних по наявним каналам радіорелейних, супутникових та інших ліній передачі.

1.2.2 Загальні параметри телефонних каналів

Під час розробки, побудови і експлуатації телекомунікаційних систем зв'язку якість каналів ТЧ об'єктивно оцінюється за допомогою часткових або узагальнених кількісних електричних параметрів, які нормуються відповідно чинним стандартам. Такі параметри каналів тональної частоти мають певні діапазони числових значень, які залежать від структури телефонної системи, довжини лінії передачі, кількості транзитних ретрансляторів, тощо [3,5].

Параметри телефонних каналів встановлюються на простий та складений канали тональної частоти. Простим називають такий канал, який по всій довжині не має транзитних ліній в діапазоні частот 0,3...3,4 кГц. У цьому випадку телекомунікаційна апаратура, що організовує канал є тільки в в кінцевих пунктах, а в проміжних пунктах ретрансляції може застосовуватись транзит по високій частоті (ущільнення в групових трактах).

Складений канал складається з декількох простих каналів ТЧ поєднаних один із одним послідовно. Під словом «транзит» розуміють взаємний зв'язок простих каналів тональної частоти. Таким чином транзити в телефонному каналі різнять на транзити по тональній частоті або низькочастотні (НЧ) і транзити по груповим трактам або по високій частоті (ВЧ)). Транзити по ВЧ від по каналам від предгрупового тракту до третинного тракту [2].

Основними параметрами та характеристиками телефонних каналів є: залишкове затухання каналу; частотна характеристика залишкового затухання; фазочастотна характеристика каналу ; амплітудна характеристика каналу; коефіцієнт нелінійних спотворень каналу; девіація частоти сигналу, що перетворюється в групових трактах; захищеність та перехідні затухання між напрямками передачі і прийому; завадозахищеність від перехідних спотворень; завадозахищеність каналу від шумових та шумоподібних завад.

1.2.3 Частотна характеристика залишкового затухання

Залишковим називається затухання сигналу в телефонному каналі (1.1), яке виміряне для гармонічного сигналу на частоті 800Гц за умови навантаження каналу, що дорівнює 600 Ом [13]:

$$a_r = 10 \cdot \log_{10} \left(\frac{P_0}{P_H} \right) \Bigg|_{R_Г = R_H = 600 Ом} \qquad (1.1)$$

де P_0 – потужність, яку генератор стандартного сигналу із частотою 800Гц віддає навантаженню;

$P_н$ – потужність, яка виділяється у опорі навантаження (еквівалентному навантаженні) каналу.

Отже, залишкове затухання є різницею між доданком усіх затухань і доданком усіх підсилень в каналі телефонного зв’язку вираженому в

децибелах (1.2) за умови повністю узгодженого поєднання всіх його елементів:

$$a_r = \sum_i a_i - \sum_j S_j \,, \tag{1.2}$$

де, a_i - затухання і-го каскадного елементу каналу;

S_j - підсилення j - го підсилювача в сегментах каскадного каналу.

Виходячи із (1.2) якщо перша сума виразу більша за значенням за другу, то в телефонному каналі наявне залишкове затухання і значення затухання буде додатним. Якщо у (1.2) друга сума більше, то залишкове затухання буде набувати від'ємних значень, що говорить про сумарне підсилення в каналі тональної частоти. Залишкове затухання виражають як в децибелах так і в неперах, воно також визначається припустимими рівнями передачі та прийому.

Значення залишкового затухання залежить від складових частин каналу :фільтрів, перетворювачів, ліній передачі, підсилювачів, тощо. Залишкове затухання відповідальне за необхідну гучність передачі та стійкість до самозбудження. Залишкове затухання має бути в певному діапазоні, в протилежному випадку відбувається або погіршення зв'язку або неприпустиме самозбудження [5].

Для двопровідного закінчення каналу номінальне значення залишкового затухання нормується на частоті 800 Гц і складає 0,8 дБ. Для чотирипроводного каналу тональної частоти залишкове затухання має складати -17дБ. Крім цього потрібно, щоб в смузі частот 0,3кГц…3кГц різниця між двома значеннями затухання, виміряними на довільних двох частотах, що відрізняються одна від одної на 200Гц, не перевищує значення у 2 дБ.

Частотною характеристикою параметра «залишкове затухання» (рис.1.7) називається його залежність від частоти за умови постійного рівня тестового сигналу на вході. Частотна характеристика визначає амплітудно-частотні спотворення телефонних сигналів, що пов'язані в основному із

кількістю та якістю схем фільтрації в простих та складених транзитних трактах.

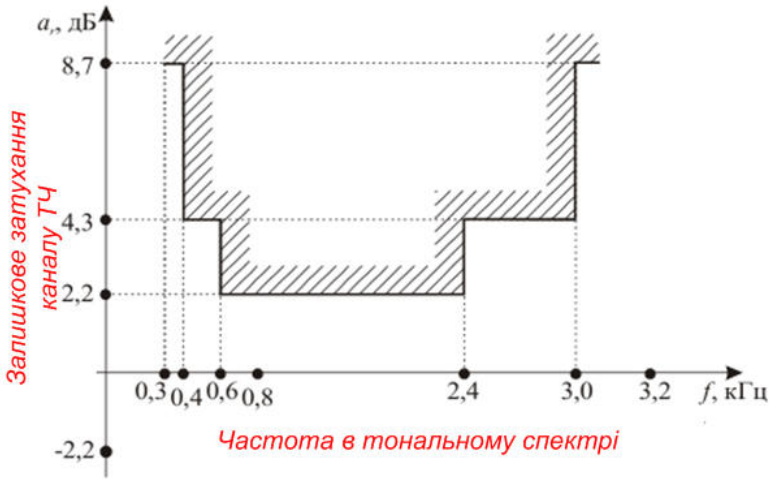


Рисунок 1.7 – Графік шаблон частотної характеристики залишкового затухання складеного каналу

Кожен транзит підвищує число послідовно фільтрових схем, що призводить до погіршення частотної характеристики залишкового затухання і, в кінцевому рахунку, збільшуються амплітудно-частотні спотворення сигналу, що неприпустимо, через погіршення розбірливості мови, та погіршення коефіцієнту помилок для інших різновидів повідомлень.

Частотна характеристика залишкового затухання як певна залежність нормується в деякій ефективній смузі частот сигналів. Ефективною смугою частот в телефонії називають частотний ресурс в межах якого на максимальній дальності зв'язку залишкове затухання не перевищує значення на частоті 800 Гц більш, ніж на 7,8 дБ або 1 Нп [3].

Норми на частотну характеристику встановлюють у вигляді відхилення між значенням залишкового затуханням на певній частоті і значенням залишкового затухання на частоті 800 Гц:

$$\Delta a_r = a_{rf} - a_{r0,8} \qquad (1.3)$$

Норми задаються для різного числа каскадно-з'єднаних простих каналів.

Для зручності визначення частотної характеристики залишкового затухання на вузлах та комутаційних станціях телефонного зв'язку будують графіки-шаблони (див. рис.1.7) для каналу ТЧ максимальної дальності і якщо виміряна частотна характеристика залишкового затухання не виходить за межі заштрихованої частини графіку, то канал за даною характеристикою (рис.1.8) припустимий для застосування під час передачі мовних повідомлень із заданою розбірливістю.

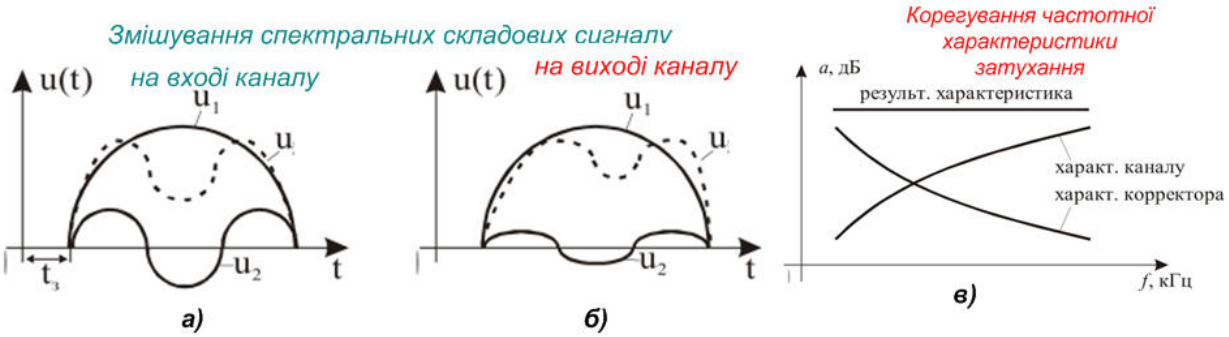


Рисунок 1.8 – Демонстрація результату частотних спотворень та можливостей корегування частотної характеристики затухання

Частотна характеристика затухання при цьому вимірюється на фіксованих частотах для пришвидшення процесу вимірювання.

1.2.4 Фазова та амплітудна характеристики

Фазовою або фазо-частотною характеристикою (ФЧХ) телефонного каналу називається залежність фазового зсуву гармонічного сигналу на виході відносно його фази на виході частоти. [11-12] Якщо ФЧХ лінійна (рис.1.1) у спектрі частот тонального або групового каналу, то сигнал

передається без лінійних спотворень і прийде на вихід каналу через інтервал часу що називають груповим часом затримки (ГЧЗ):

$$\tau_{ГР}(\omega) = \frac{d\phi(\omega)}{d\omega}, \tag{1.4}$$

де $\phi(\omega)$ - фазо-частотна характеристика каналу передачі.

ГЧЗ в телефонії визначають і інакше як інтервал часу від моменту подачі на вхід каналу сигналу до моменту появи на його виході максимуму енергії переданого сигналу.

При лінійній ФЧХ характеристика ГЧЗ постійна (1.4), значення якої чисельно дорівнює тангенсу кута нахилу прямої лінії ФЧХ:

$$tg(\alpha) = \tau_{ГР} = \frac{d\phi(\omega)}{d\omega} = \frac{d(\omega\tau_{ГР})}{d\omega}. \tag{1.5}$$

В реальних каналах тональної частоти ФЧХ далека від лінійної (1.5), що призводить до додаткових спотворень.

В ефективній смузі частот варто врахувати середнє значення групового часу затримки і відхилення його від середнього або заданого значення. За умови великих значень групового часу затримки, наприклад, викликаних віддаленістю абонента, ведення швидкої розмови стає утрудненим, порушується розуміння абонентами один одного [11].

Відхилення ГЧЗ від середнього значення не має суттєвого впливу на якість обміну мовною інформацією завдяки нечутливості вух людини до фази сигналу, але сильно впливає на якість транспортування по каналу ТЧ цифрових даних. На практиці фазочастотні спотворення оцінюються відхилень ГЧЗ від частоти у діапазоні частот стандартного телефонного каналу із складовою на частоті 1,9кГц (опосередненій частоті спектру телефонного сигналу) і нормується для ділянки довжиною у 2500км!

Якщо транзитних ділянок буде більше, то і відхилення зростатимуть в таку саму кількість разів (рис.1.9), крім того підлягає нормуванню ГЧЗ для наземних (100мс) та космічних (400мс) телефонних мереж.

Практично всі канали ТЧ не відповідають нормам ГЧЗ для кінцевої апаратури абонентів, але оскільки телефонні канали можуть використовуватись для передачі не тільки мовних сигналів, то вважається недоцільним в проміжних ланках каналоутворення встановлювати пристрої для корекції ФЧХ і подібна техніка розміщується наприкінці каналу зв'язку [5].

Рисунок 1.9 – Вплив неідеальності фазової характеристики на спотворення

Амплітудною характеристикою (1.6) телефонного каналу називають залежність залишкового затухання не від частоти а від рівня тестового гармонічного сигналу на вході каналу для частоти 800Гц:

$$a_r = \phi\left(p_{BX}\right) \ для \ f = 0{,}8кГц \qquad (1.6)$$

Перша точка всіх графіків амплітудної характеристики (рис.1.10) каналів тональної частоти фактично оцінює лінійність каналу, а наступні дві точки характеризують правильність роботи амплітудного обмеження, що застосовується завжди для запобігання перенавантажень транзисторів (активних нелінійних елементів), що встановлено в каскадах підсилення.

Ідеальна амплітудна характеристика (1.6) каналу ТЧ рівномірна, відхилення від рівномірності, або нелінійності погіршують якість мовних, телевізійних, і факсимільних повідомлень, погіршують ймовірність правильної передачі цифрових даних і телеграфних повідомлень.

Норми на АХ задаються для простого каналу ТЧ: під час підвищення рівня на вході каналу від номінального на 3,5 дБ залишкове затухання може підвищитися не більше за 0,3дБ. А за умови підвищення рівня вхідного сигналу на 10дБ, залишкове затухання має підвищитися не більше за 2 дБ (рис.1.1).

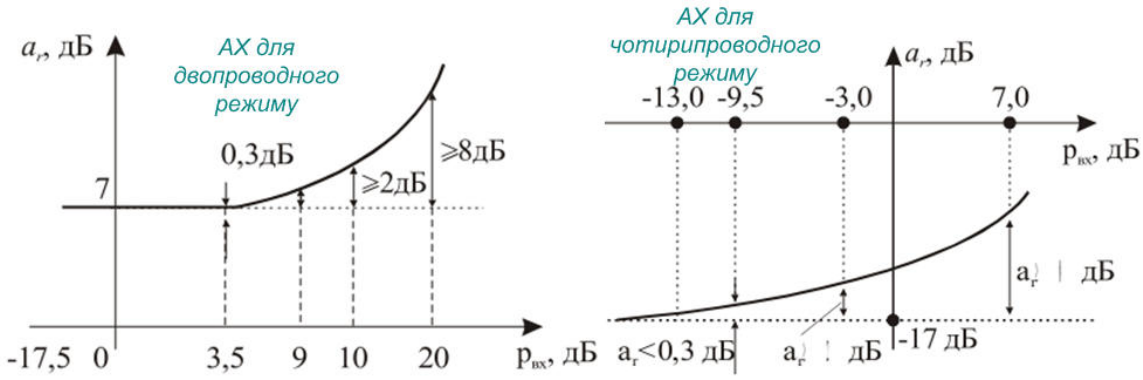


Рисунок 1.10 – Шаблони амплітудних характеристик телефонних каналів

Для каналу ТЧ без застосування примусового обмеження амплітуди сигналу нормується лише одне значення: під час підвищення рівня телефонного сигналу на вході каналу відносно номінального на 7дБ залишкове затухання може збільшитися не більше, за 3,0дБ. Для складених телефонних каналів каналу, який включає N простих каналів тональної частоти, норми на всі відхилення амплітудної характеристики від номінальних значень збільшуються в n разів [3].

Амплітудна характеристика (рис.1.10) не зовсім точно оцінює лінійність телефонного каналу загалом. Вона визначає лише поріг нелінійного перевантаження каналу, але не дає можливості провести вимірювання нелінійних спотворень на робочій ділянці. Для комплексного вимірювання таких спотворень використовують такий параметр як

коефіцієнт нелінійних спотворень або коефіцієнт гармонік (1.7), що вимірюється не під час перевищення рівнів сигналу на вході, а за умови номінальних рівнів за формулою:

$$K_Г = 100\% \frac{\sqrt{U_{2Г}^2 + U_{3Г}^2 + ... + U_{nГ}^2}}{U_{1Г}^2} \qquad (1.7)$$

де $U_{1Г}^2$ - квадрат амплітуди першої гармоніки сигналу;

$U_{nГ}^2$ - квадрат амплітуди *n-х* гармонік сигналу на виході телефонного тракту.

Особливістю вимірювання нелінійних спотворень в телефонії оцінюється не тільки коефіцієнт гармонік за, але і величина коефіцієнту третьої гармоніки за відношенням:

$$K_{3Г} = 100\% \frac{U_{3Г}}{U_{1Г}} \qquad (1.8)$$

Коефіцієнти гармонік (1.7,1.8) нормуються для частоти гармонічного тестового сигналу під час номінального рівня тональних сигналів на вході простого каналу як такі, що менше 1,5% по всім гармоніками і 1% по третій гармоніці. Для складеного каналу нормуючі значення простого каналу підвищується у корінь із кількості каналів.

1.3 Захищеність тонального каналу від завад та спотворень

1.3.1 Захищеність від сигналів по напрямку передачі

Захищеністю між напрямками передачі і прийому сигналів тональної частоти називається різниця логарифмічних рівнів сигналу і завади від сигналу протилежного напрямку на виході каналу [1]. Причинами дії одного

напрямку передачі каналу на інший часто є неідеальність монтажу та прокладання довгих ліній. Для мідних кабельних телефонних ліній основною причиною вказаних завад є перехідна завада на ближньому кінці підсилювачів в складі регенераторів сигналів.

За умови передачі телефонних сигналів по каналам тональної частоти перетікання енергії сигналів між каналами проявляється як так званий «місцевий ефект», але звичайно навіть сильна дія такого ефекту не погіршує якості обміну мовною інформацією. А от під час застосування телефонних каналів для інших повідомлень, подібний місцевий ефект розглядається як шумоподібні завада, що суттєво впливає на передачу повідомлень.

Захищеність між напрямами передачі тональних каналів стаціонарних 2-кабельних телекомунікаційних систем довжиною до 2500 км має бути для діючих систем не менше -52 дБ, а для систем телефонних комунікації, що тільки проектуються, не менше -55дБ. Якщо дальності L перевищують L_0=2500км, то норми вказаної захищеності розраховують за:

$$a_{3L} = a_{3L0} + 10 \times \lg\left(\frac{L_0}{L}\right)(\partial Б),$$
$$a_{3L} = a_{3L0} + \frac{1}{2} \times \ln\left(\frac{L_0}{L}\right)(Hn). \qquad (1.9)$$

Вимірювання захищеності (1.9) між напрямками реалізуються із використанням лабораторного вимірювального генератора і чутливого селективного вимірювача рівня [3].

1.3.2 Захищеність від завад подібних до сигналу

Одні із самих «важких» щодо завадостійкості завад в телекомунікаціях є завади подібні до сигналу. Що торкається телефонних каналів тональної частоти, то такими є розбірливі мовні завади, тобто голос іншої людини, що

«просочується» із іншого телефонного каналу. Розбірливі завади тональної частоти можуть бути між суміжними каналами однієї локальної телекомунікаційної системи або завадами, що виникають через нелінійність групового тракту каналоутворення.

Розбірливі завади проявляються як прослуховування чужих розмов на які налаштовується мовний апарат абонента і тим самим відвертають увагу від власної розмови свого співрозмовника, не кажучи про втрату таємничості телефонного зв’язку. Захищеність від розбірливих завад між каналами паралельно працюючих телефонних стаціонарних систем передачі на базі кабельних ліній зв’язку довжиною L_0 = 2500км має бути не менше 58 дБ для 90% комбінацій взаємних впливів каналів і не менше 52 дБ для всіх комбінацій взаємодії окремих каналів тональної частоти.

Для решти телефонних каналів норми захищеності розбірливих завад ще вищі.

1.3.3 Захищеність від шумових завад

Важливим показником якості тональних каналів зв'язку є рівень завад, що надходять разом із корисним сигналом і впливають на якість телефонних розмов. До того ж однакові за рівнем завади але із різною частотою чинять різний вплив на характеристики розбірливості мови через нерівномірну АЧХ вуха людини. Тому під час практичних досліджень впливу шумових завад, їх спектри формують відповідно чутливості вуха, пропускаючи через частото залежні кола – зважуючі фільтри. Потужність завад, яка вимірюється на вході подібного звужуючого фільтру називають псофометричною [3].

Якщо ж тональний канал передачі використовується не тільки для мовних повідомлень, але і для інших видів зв'язку, то застосовують поняття інтегральної напруги шуму. Під інтегральною шумовою напругою

розуміється ефективне значення напруги шуму в діапазоні частот стандартного каналу (рис.1.11).

Нормування шумових завад проводиться відповідно до міжнародних рекомендацій МККТТ для деякого гіпотетичного кабельного каналу довжиною 2500км. Під час телефонії по кабельній лінії і максимальній кількості регенераторів середня псофометрична потужність завад не має перевищувати 10 мкВт, що відповідає логарифмічному рівню у 50 дБ.

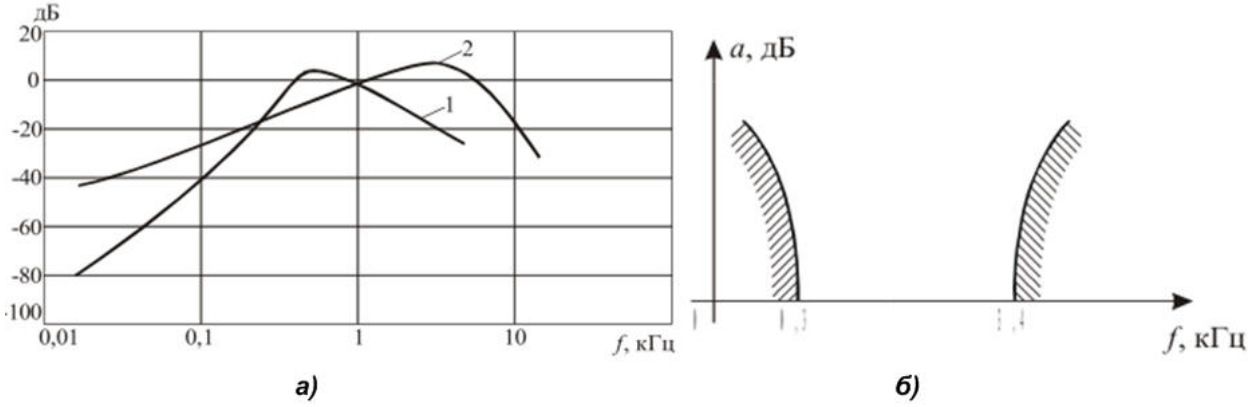


Рисунок 1.11 – Частотні характеристики псофометричних фільтрів

Приблизно 25% потужності шумів може вироблятися кінцевими і проміжними станціями транзиту, а до 75% вносить кабельна лінія зв'язку. За умови сумарної довжини у 2500 км потужність шумів не має перевищувати 7,5мкВт(псоф.). Якщо вважати розміщення регенеративних точок транзиту в лінійному тракті, то припускають, що на 1000м довжини каналу передачі потужність шумів, не має бути більшою за 2пВт (псоф).

Якщо для транзиту телефонного сигналу застосовуються повітряні лінії (на стовпах), які чутливі до зовнішніх впливів також і неелектричного характеру, специфікаціями МККТТ припускається і більша потужність завад. А саме для каналів повітряних ліній довжиною 2500 загальна псофометрична потужність шумів має бути не більше 20 мкВт, із яких 17,5мк Вт припадає на лінійний тракт кабельних ліній.

Якість передачі телефонних сигналів по радіорелейним лініям (РРЛ) прямої дії (рис.1.12а) не має відрізнятись від кабельних систем передачі, тобто з цієї точки зору вимоги однакові. Лінійний тракт РРЛ із довжиною 2500 км не має створювати завади не більше 7,5мкВт (псоф.) у будь який момент часу на протязі однієї хвилини, але допускається і підвищення середньо хвилинної потужності завад до 47мкВт але не більше ніж на годину щомісяця [3].

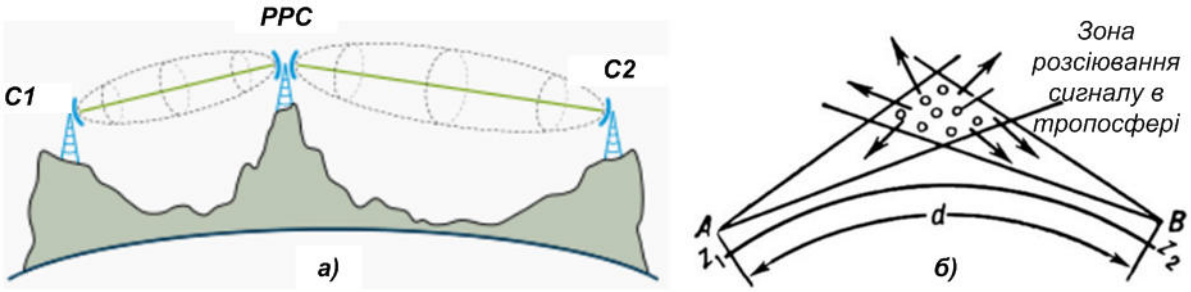


Рисунок 1.12 – Принцип роботи радіорелейної лінії (а) та тропосферної лінії зв’язку (б)

Для каналів тональної частоти тропосферних РРЛ (рис.1.12б), середня за годину потужність шумів може сягати до 25мкВТ (пВт/псоф). Така ж сама потужність але для космічних одностибкових ретрансляторів, діє норма у 10мкВт незалежно геодезичній відстані по поверхні землі між кінцевим устаткуванням.

2 ХАОТИЧНА КРИПТОГРАФІЯ

2.1 Процедурна еквівалентність захисту інформації

2.1.1 Детермінований хаос і криптографія

Такі повсякденні поняття як «детермінованість» і «хаос» для повсякденного користувача часто здаються антонімами. Перше асоціюється із цілковитою передбачуваністю та багаторазовою відтворюваністю, хаос – навпаки, із повною непередбачуваністю та неповторністю. Але вираз «детермінований хаос» (рис.2.1) для математика або фізика має глибокий сенс і коли вони говорять про детермінованість, то мають на увазі причинно-наслідковий зв'язок між подіями. Тобто коли наперед задано деякий стан системи в початковий момент часу, то він однозначно визначає стан такої системи у майбутньому [26-28].

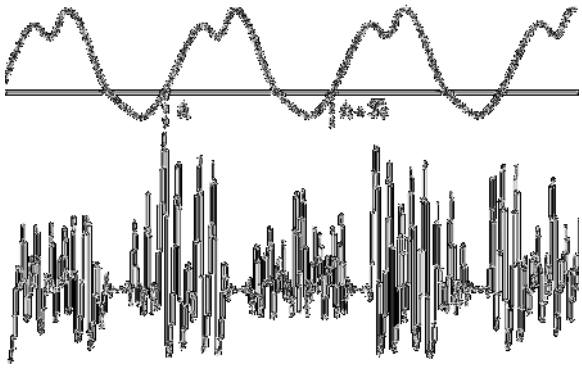


Рисунок 2.1 – Форма регулярного та хаотичного сигналів

Таким чином, у динамічній детермінованій системі стан, що характеризується значеннями внутрішніх незалежних змінних, змінюється за детермінованим законом. За цим законом динамічні системи можливо поділити на хаотичні та регулярні. Регулярні системи характеризуються стійкістю, де невеликі відхилення змінних із часом пригнічуються та

згасають, що приводить до повернення характеру поведінки системи до початкової.

А от, хаотична система має нестійкий характер поведінки де малі збурення посилюються та наростають у часі [24-25]. Хаотичні системи мають так звану експоненційну чутливістю де найменша зміна початкового стану призводить до суттєвої зміни всієї траєкторії руху внутрішніх змінних (рис.2.2), що посилюється із часом. Тому що в реальній фізичній системи не можливо виміряти початкові умови з абсолютною точністю, то помилка передбачення стану швидко зростає до неприйнятного рівня і реалізується хаотична динаміка.

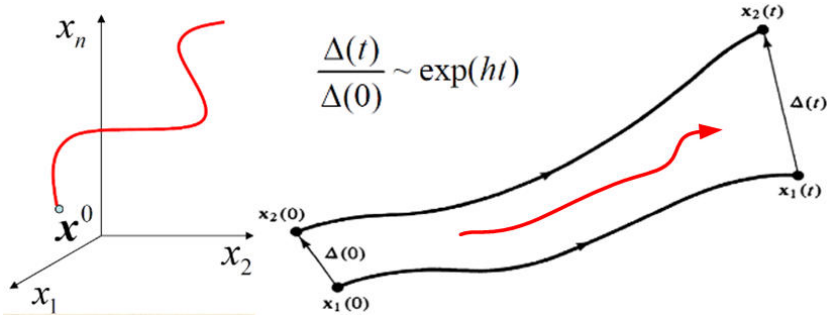


Рисунок 2.2 – Фазовий простір динамічної системи (ліворуч) та експоненційне зростання метрики розбігання (праворуч)

Отже, характер розвитку процесів в детермінованій хаотичній системі може бути передбачено тільки статистично, за допомогою деякої функції густини розподілу, що визначає асимптотичну ймовірність перебування багатомірної фазової траєкторії в кожній області фазового простору станів. Саме такими процесами займається теорія детермінованого хаосу [25].

Зусиллями багатьох вчених математична теорія детермінованого хаосу є фундаментальною базою сучасного природознавства [24]. Ними натепер переконливо доведено, що велика складність хаотичної поведінки прихована не у великій кількості незалежних змінних та ступенів їх свободи, а в експоненційний нестійкості поведінки та нелінійних характер взаємодії складових.

Типовими прикладами «детермінованого хаосу» є броунівська рух, погодні явища та процеси, девіації орбіт планет, економіка бірж; поширення кровотоку в судинах людини, тощо. Криптографічні системи в рамках такого підходу не є винятком, вони також можуть розглядатись за законами хаосу [28].

Криптографічні та хаотичні системи мають багато спільних рис навіть на концептуальному рівні. В першу чергу і в криптографії, і в «детермінованому хаосі» реалізується нелінійне перетворення інформації. А в реальних системах всі перетворення нелінійні і лише можуть вважатись в деякому діапазоні параметрів лінійними.

В криптографії, таке нелінійне перетворення - детерміновано, бо виконується детермінованим пристроєм - комп'ютером, але воно має бути практично непередбачуваним для спостерігача несанкціонованого доступу. Отже, термінологія «детермінований хаос» для криптографії теж підходить [28-29].

Крім загального взаємозв'язку на рівні нелінійностей, можна помітити, що на практиці хаотичні та криптографічні системи також подібні. Засновник статистичної теорії інформації. К.Шенон в явному вигляді згадував механізми хаотичної поведінки стосовно шифрування даних стискаючими та розтягуючи ми перетвореннями [13-14].

Усвідомлення надвеликої цінності знань стали причиною особливої актуальності криптографії сьогодні. Крім використання загальновідомих та практично відпрацьованих схем захисту інформації від несанкціонованого доступу, фахівцями спостерігається постійний пошук нових технологій криптографії. В переважній більшості це обумовлено не стільки бажанням збільшувати криптографічну стійкість традиційних засобів, а необхідністю бути автономним від існуючих засобів і стандартів, які, раптово можуть втратити свою актуальність.

2.1.2 Процедурна еквівалентність криптографії та хаосу

У широкому розумінні, криптографічна система це вся інфраструктура, що забезпечує захист інформації від несанкціонованого доступу засобами за допомогою комп'ютерів. Основними елементами криптографічної інфраструктури є: є сукупність засобів шифрування (рис.2.3), механізми та правила передачі ключів, забезпечення аутентифікації, тощо. У реальних застосуваннях криптосистема є досить складний та продуктивний апаратно-програмний комплекс, що взаємодіє з оператором [18].

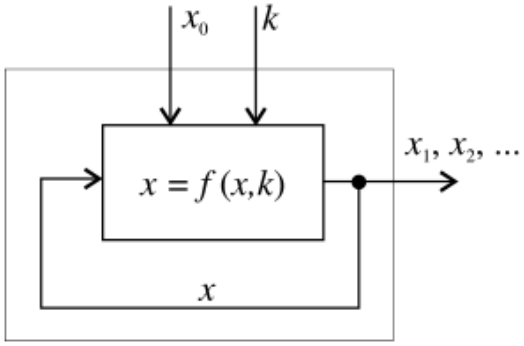


Рисунок 2.3 – Ітеративна процедура шифрування

Із математичної точки зору криптосистема є деяке перетворення інформації (рис.2.3), що визначається на базі початкових станів X, результатів Y та ключів шифрування K. Стан системи X кодує корисну інформацію, а функція перетворення f задається за допомогою алгоритму, який реалізується машиною Тюринга.

Подібне послідовне ітераційне перетворення станів системи в результаті дії деякої однотипної елементарної нелінійної функції f спостерігається під час блочного кодування, згорткового кодування, генераторах М-послідовностей, тощо.

В рамках порівняння криптографії та хаосу можливо виділити дві особливості [18,19,20,24]:

1) Шифрування за блочним алгоритмом здійснюється через *n*-кратне застосування деякої ітераційної функції *f* (рис.2.4). Тут кількість ітерацій n

досить невелике і зафіксовано (часто, n = 16). Кожна ітерація переводить криптосистему до наступного стану, тобто $x_{i+1} = f\left(x_i\right)$. Початковий стан – то інформація, що підлягає шифруванню (наприклад, відкритий текст), а кінцевий стан – зашифроване повідомлення стан приймається за шифротекст.

2) Згорткові схеми шифрування мають набагато більш різновидів. Їхньою відмінністю є те, що процес шифрування всього повідомлення відповідає одній траєкторії руху в просторі станів, тобто шифрування деякої порції відкритого повідомлення залежить від поточного стану криптосистеми в даний момент. В даному випадку кількість ітерацій не фіксована, а залежить від обсягу повідомлення, що підлягає шифруванню.

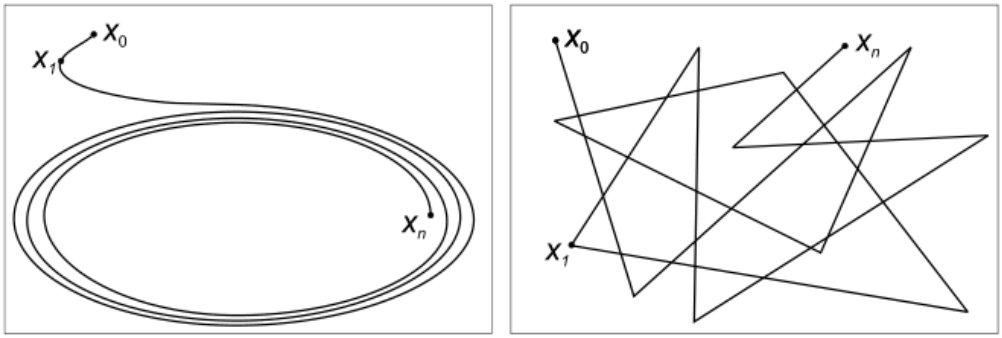


Рисунок.2.4 – Фазові портрети для хаотичної(ліворуч) та криптографічної систем (праворуч) в механізмі ітераційних алгоритмів

Ітераційна процедура також вимагає застосування генераторів псевдовипадкових чисел [21]. Наприклад, симетрична схема шифрування безумовно безпечна в тому випадку, якщо ключі k мають дійсно випадковий або рівномірний закон розподілу значень та її бітова довжина дорівнює довжині відкритого повідомлення, наприклад, шифрування за принципом одноразового блокноту.

Передавання ключів значної довжини стикається з проблемами, наприклад, перевантаження каналів і замість них і застосовують псевдовипадкові послідовності, що генеруються детермінованим генератором із детермінованою функцією із допомогою короткого ключа.

Псевдовипадкові генератори основний елемент сучасної криптографії де алгоритм криптографічного перетворення залишається незмінним під час передачі всього повідомлення, а змінюються тільки його параметри або ключі. Таким чином псевдовипадкова послідовність задає весь ланцюжок криптографічної процедури перетворень і вона є ітераційною [6,917].

Із математичної точки зору динамічні системи із хаотичною поведінкою можуть бути задані по різному, але якщо застосовуються неперервні змінні то переважно використовують диференційні рівняння:

$$\frac{dx}{dt} = f\left(x,k\right);\ x \in X \subseteq R^{d};\ x \in X \subseteq R^{dK} \qquad (2.1)$$

де $f : X \times K \to Y$ - гладка вектор-функція;

X – простір станів;

K – простір керуючих параметрів хаотичного генератора.

Для кожної початкової умови система (2.1) має одне рішення $x\left(t,x_0\right)$, *де* $x\left(0,x_0\right) = x_0$. Багатомірна крива лінія $\varphi_t\left(t,x_0\right)$, що відповідає такому рішенню є траєкторія, або фазова траєкторія динамічної системи.

Якщо динаміка системи представлена у дискретному часі, то її можливо записати у вигляді ітераційної функції:

$$x_{n+1} = f\left(x_n,k\right);\ x_n \in X \subseteq R^{d};\ x \in X \subseteq R^{dK};\ n = 0,1,2... \qquad (2.2)$$

де, x_n - ряд дискретних станів хаотичної системи.

Для такого представлення (2.2) фазова траєкторія є ряд точок. Вираз (2.3) схожий на операцію криптографічної функції, що застосовується у псевдовипадкових генераторах, під час блочного шифрування, тощо. Отже як в криптографічних системах так і у системах із детермінованим хаосом ми маємо справу із ітераційною процедурою перетворення інформації із використанням керуючих параметрів.

2.1.3 Ознаки хаотичної системи

Хаотична поведінка (рис.2.5) в нелінійній динамічній системі спостерігається не завжди, а за певних умов. Зокрема, необхідними умовами для появи хаосу в системі є топологічна транзитивність і експоненційна чутливість до початкових умов або збурень [22-24].

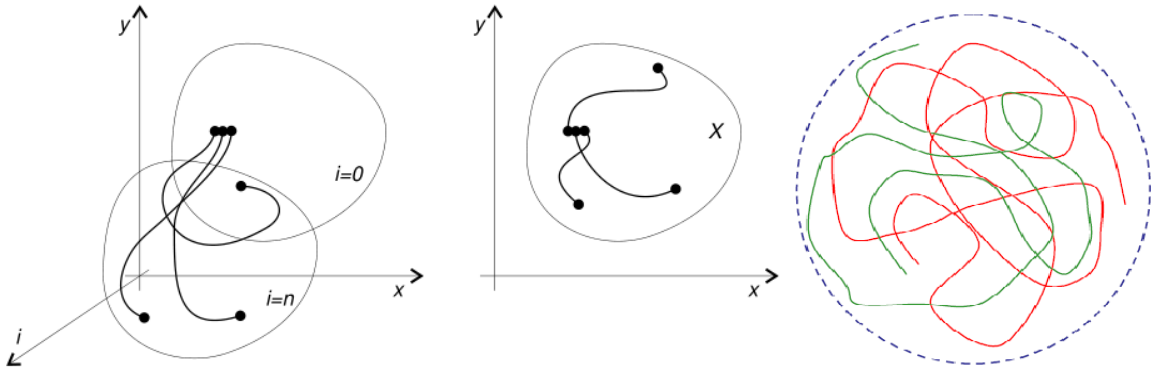


Рисунок 2.5 – Фазово-часові (ліворуч) та фазові (центр) та заплутування траєкторій руху динамічної системи із хаотичною поведінкою піж час експоненційного розбігання

Топологічна транзитивність означає обмеженість розташування траєкторій в певній ділянці фазового простору (рис.2.5), а експоненційна чутливість означає «розбігання» траєкторій або віддалення їх одна від одної в кожній точці фазового простору або простору станів системи.

Якщо проводити паралель між хаосом та криптографією, то топологічна транзитивність необхідна для використання заздалегідь виділеного обсягу пам’яті, а чутливість до початкових умов характеризує ступінь кореляції вихідного повідомлення та його зашифрованого вигляду.

Кількісною ознакою чутливості до початкових умов є показники Ляпунова, що для одномірної системи визначаються із рівняння [26-27]:

$$\left| f^n\left(x_0+\varepsilon\right) - f^n\left(x_0\right)\right| = \varepsilon \times \exp\left[n\lambda\left(x_0\right)\right] \tag{2.3}$$

де ε - невелика девіація початкового стану x_0,

n- кількість ітерацій або кроків дискретного стану.

В загальному випадку показники Ляпунова (2.3) залежать від початкового стану, тому часто визначають опосереднене їх значення, але для динамічних систем, що зберігають міру показники Ляпунова є сталими. Із практичної точки зору показники Ляпунова можливо обчислити за рівнянням:

$$\lambda\left(x_0\right) = \lim_{\substack{n\to\infty \\ \varepsilon\to 0}} \left[\frac{1}{n}\ln\left|\frac{f^n\left(x_0+\varepsilon\right) - f^n\left(x_0\right)}{\varepsilon}\right|\right] \tag{2.4}$$

Додатне значення показника Ляпунова (2.4) вказує на наявність хаотичної поведінки в системі (рис.2.6). Якщо система багатомірна, то ми отримаємо спектр показників Ляпунова і більш складу хаотичну поведінку, але всі її ознаки залишаються аналогічними як для одномірного випадку. Кількість показників Ляпунова в спектрі дорівнює розмірності системи.

З точки зору криптографії чим більше значення показника Ляпунова тим менше ітерацій необхідно для процедури шифрування що включає в себе розпорошення та змішування інформації псевдовипадкової послідовності і вихідного повідомлення.

Ознакою хаотичної поведінки системи є також біфуркація (рис.2.6), що характеризує процес якісного переходу від регулярної поведінки до хаотичної під час послідовної зміни керуючого параметра або параметрів. У точках біфуркацій відбувається подвоєння кількості стійких станів системи, якщо параметр змінювати далі, подвоєння відбуваються частіше, що і призводить до появи хаотичного режиму системи [28-30].

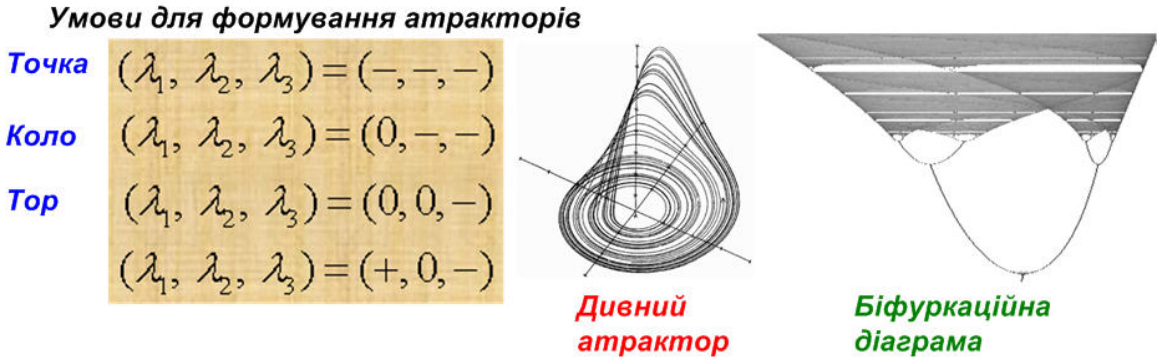


Рисунок 2.6 – Умови для асимптотичної поведінки за спектром показників Ляпунова для тривимірного простору

У криптографічних застосуваннях вибір значення керуючого параметру визначає глобальну непередбачуваність системи. Якщо цей параметр є ключем шифрування, то весь простір подібних ключів має відповідати хаотичному режиму роботи системи криптозахисту.

2.1.4 Хаотична генерація ключів шифрування

Криптоаналіз багатьох систем шифрування застосовує методи статистичного аналізу за частотою появи окремих символів, слів, комбінацій, тощо. В рамках такого криптоаналізу К.Шеноном запропоновано для ефективної криптографії два підходи: «розсіювання» та «перемішування», що потенційно забезпечують високу стійкість до дешифрування.

Підхід «розсіювання» аналогічний лавинному ефекту, що властивий також у хаосі через розбігання фазових траєкторій. Методика розсіювання передбачає що зміна одного біту потоку призводить до змін у решті бітів із імовірністю 0,5.

Підхід «перемішування» передбачає, що кожен наступний біт під час шифрування має бути корельованим із максимальною кількістю інших бітів забезпечуючи повноту шифру.

Вказані вище особливості хаотичних систем та їх способів модуляції та синхронізації припускають ефективне їх застосування для формування

потокових ключових послідовностей, що забезпечує ефективну підтримку підходів розсіювання та перемішування [17].

Наприклад, аперіодичність сигналу детермінованого хаосу вказує на можливість формування як завгодно тривали і неповторних ключів одноразового використання. Але з технічної точки зору такі можливості формування ключів обмежуються точністю цифрових обрахунків, наприклад, для генерації ключів на базі логістичного відображення точність відображення складала 10^{-9}, тобто за реальної техніки довжина ключа складає 9-10 десяткових цифр, що іноді замало для роботи професійних систем телекомунікацій [4].

Окремим класом систем шифрування інформації на базі хаотичних сигналів є такі методи та методики, що використовують фазові траєкторії сигналів детермінованого хаосу, наприклад, система Баптиста, основою якої є відображення, що задане співвідношенням (2.5):

$$x(n+1) = \phi\left[x(n)\right] \tag{2.5}$$

Особливістю відображення (2.5) є те, що зона припустимих значень складає [0;1], а будь-якому символу із первинного алфавіту ставиться у відповідність певна кількість ітерацій. Першим елементом ітерації є деяке початкове число x_0 . Множина значень цього числа та спосіб розбиття відрізка [0;1] на субінтервали є множиною усіх можливих ключів шифрування. Отже, генератори хаотичних сигналів можуть бути базою для створення окремого сімейства процедур отримання потокових ключів шифрування із високою стійкістю до статистичних методів криптоаналізу в першу чергу.

2.2 Генератори детермінованого хаосу

2.2.1 Застосування хаотичних генераторів в телекомунікаціях

Сучасний розвиток телекомунікаційних систем вимагає все більшого удосконалення засобів в напрямку забезпечення більшої продуктивності, менших помилок, підвищення прихованості дії та покращення способів криптографічного захисту. Комплексне виконання таких вимог можливе лише через застосування широкосмугових та надширокосмугових сигналів як допоміжних (несівних) сигналів для передачі і аналогових і цифрових повідомлень.

Розробка подібних систем проводиться повсякденно, особливо актуальні застосування таких систем із збільшенням частоти (рис.2.7), де можливо вільно розташувати розширений в сотні разів спектр, наприклад, подібні сигнали застосовуються в системах 5G, для стандартів радіозв'язку 802.16. В подібних системах розширення спектру відбувається через використання псевдовипадкових генераторів, що мають, як вже вказувалось, багато спільного із генераторами хаотичних сигналів.

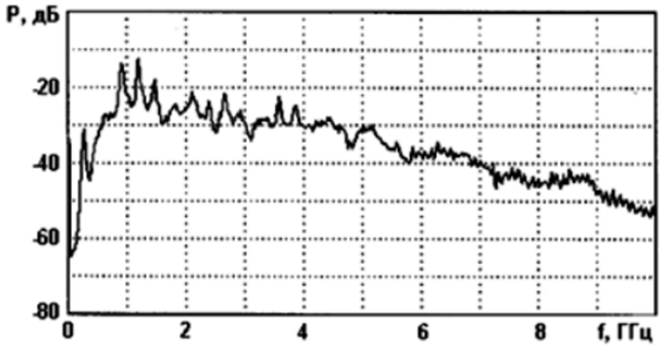


Рисунок 2.7 – Типовий спектр потужностей для НВЧ хаотичного широкосмугового генератора

Останніми роками сигналам псевдовипадкових генераторів знайдена потужна заміна в широкосмугових та надширокосмугових системах зв'язку, а

саме застосування генераторів динамічного хаосу. Через саму природу хаосу такі генератори створюють неперіодичні широкосмугові сигнали, але широкосмуговості ще замало[23]. Данні генератори мають мати властивості, які найбільш відповідають звичайним випадковим процесам, наприклад, спектр максимально близький до суцільного, а автокореляційна функція до ідеальної дельта-подібної, тощо. Особливо важлива непередбачуваність на великих інтервалах часу із можливістю точного відтворення на етапі моделювання через встановлення початкових параметрів та стартових змінних (початкових умов)[25].

Перші хаотичні детерміновані коливання, що описуються диференційними рівняннями були отримані в не радіотехнічних галузях, наприклад, для моделювання погоди (система Лоренца) або моделювання процесів під час хімічних перетворень (система Реслера), тощо. Аналіз поведінки перших генераторів хаосу показав саме необхідні властивості для створення хаотичної поведінки, а саме: чутливість до початкових умов та експоненційне розбігання фазових траєкторій.

Отже хаотичні коливання можуть і мають стати основою для створення широкосмугових несівних сучасних телекомунікацій за наступними ознаками:

1) Сигнали детермінованого хаосу можливо отримати на базі доволі простих динамічних схем, а математичне моделювання може бути здійснено на базі диференційних рівнянь наприклад, генератори Чуа, Чена, Піонтковського-Рабіновича, тощо.

2) На основі одного або декількох пов’язаних генераторів хаосу можливо створювати велику кількість каналів передачі, що характеризує високу інформаційну ємність хаотичних сигналів в такому аспекті.

3) Кількість методів введення інформаційного сигналу в хаотичну піднесівну набагато перевищує кількість класичних методів модуляції. Тому саме в техніці хаотичного зв’язку не прийнято застосовувати термін «модуляція».

4) Всі перших переваг було б не досить, якби не було здійснено відкриття явища хаотичної синхронізації, тобто вирівнювання динаміки руху генераторів різними способами на відстані. А також явища хаотичного синхронного відгуку, що теж можливо розглядати як один із варіантів синхронізації.

Саме ці особливості, дозволяють розглядати хаотичні системи натепер як конкуренти системам широкосмугових телекомунікацій із псевдовипадковими коливаннями та регулярними піднесівними.

2.2.2 Особливості та будова генераторів хаосу

В хаотичній телекомунікаційній схемі центральним елементом є генератор сигналу детермінованого хаосу або коротше – генератор хаосу, що створює хаотичну піднесівну для транспортування інформаційного повідомлення від передавача до приймача. Для телекомунікацій найбільш придатні генератори хаосу, спектр яких лежить в радіодіапазоні, синтезувати структуру якого не просто.

В рамках практичної реалізації генераторів хаосу радіодіапазону слід зважити на наступні зауваження [30]:

1) Генератор хаосу має генерувати сигнал в заданому діапазоні із заданими характеристиками і розподілом, що визначається структурою, тому синтез генераторів часто є емпіричним, а отримані структури або математичний опис називають іменем відкривача.
2) Генератор хаосу має бути складений на стандартних, відомих елементах, що застосовуються в класичних телекомунікаційних засобах.
3) НВЧ генератори хаосу застосовують елементи, що працюють на межі своїх параметрів, тому опис має бути багатогранним та

складним, а побудована математична модель важко асоціюється із реальним пристроєм.

4) До технології та конструкції виготовлення елементів, особливо в інтегральному виконанні можуть висуватись особливі вимоги.

Найбільш відомим, першим та популярним у застосуванні є генератор хаосу – Чуа, що складається всього із 5 елементів (рис.2.8).

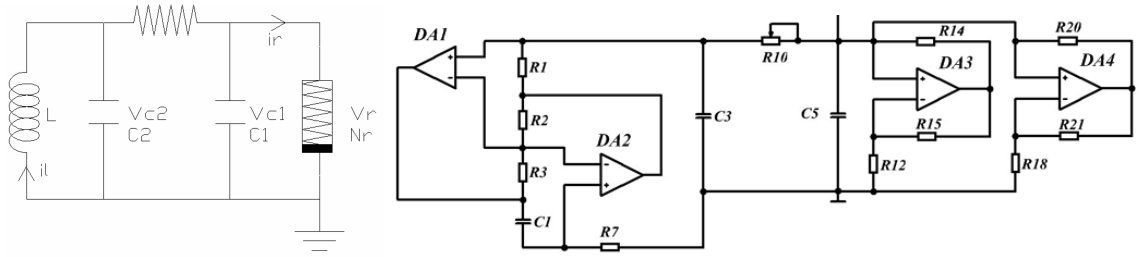


Рисунок 2.8 – Еквівалентна (ліворуч) та принципова схема (праворуч) генератора Чуа

Джерелом живлення в генераторі Чуа є резистор із нелінійним опором, що може бути заданий кусково-лінійною функцією, а резонансним елементом котушка індуктивності L разом із іншими елементами. Розсіювання енергії, або дисипацію реалізує активний опір, що ввімкнено між конденсаторами C1 та C2. Якщо елементи мають невеликі розміри, а частота генерації значна то для такої системи можливо скласти рівняння за правилами Кірхгофа [31]:

$$\begin{aligned} C_1 \frac{dV_{C_1}}{dt} &= \frac{1}{R}\left(V_{C_2} - V_{C_1}\right) - f\left(V_{C_1}\right); \\ C_2 \frac{dV_{C_2}}{dt} &= \frac{1}{R}\left(V_{C_1} - V_{C_2}\right) - i_L; \\ L \frac{di_L}{dt} &= -V_{C_2}. \end{aligned} \tag{2.6}$$

Перевагою генератора Чуа, є те, що для нього можливо побудувати рівняння у відносних параметрах де за відносними параметрами можливо

визначити абсолютні значення (2.6) резистору, індуктивності та конденсатору:

$$\begin{aligned} \frac{dx}{dt} &= \alpha\left(y - x - f\left(x\right)\right); \\ \frac{dy}{dt} &= y - x + z; \\ \frac{dz}{dt} &= -\beta y. \end{aligned} \tag{2.7}$$

Система Чуа має перевагу над іншими генераторами в тому, що вона спроможна генерувати сигнали детермінованого хаосу в досить широкому діапазоні параметрів (2.7), яких досить не багато, а нелінійну функцію (рис.2.9) легко реалізувати на операційних підсилювачах.

Таким чином, генератор Чуа може буди створений за допомогою простих елементів та через зміну їх номіналів може бути легко отриманий хаотичних режим в ньому.

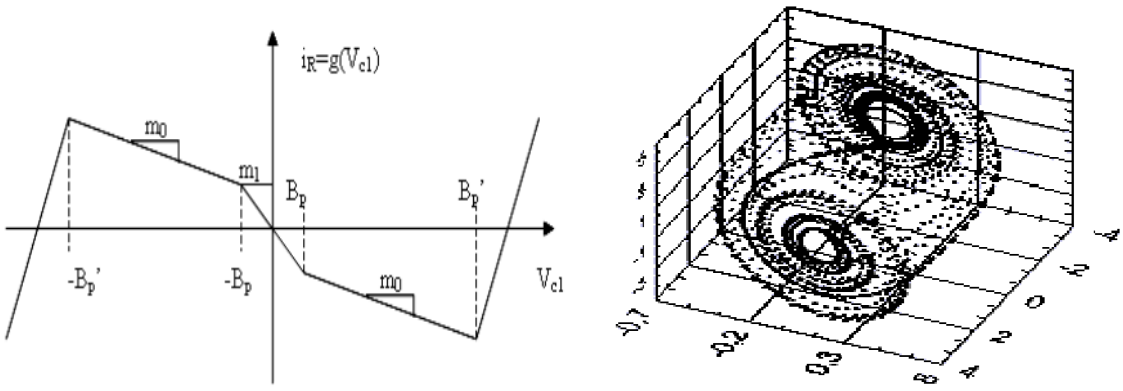


Рисунок 2.9 – Вольт-амперна характеристика (ліворуч) та форма дивного атрактора генератора Чуа (праворуч)

Хаотичні генератори також можуть бути створені на основі відомих схем у певних режимах роботи нелінійних елементів та значенні параметрів. Однією із таких схем є класичний синусоїдальний генератор зібраний за

схемою індуктивної або, частіше, ємнісної триточки (рис.2.10 - генератор Колпітца) [34-36].

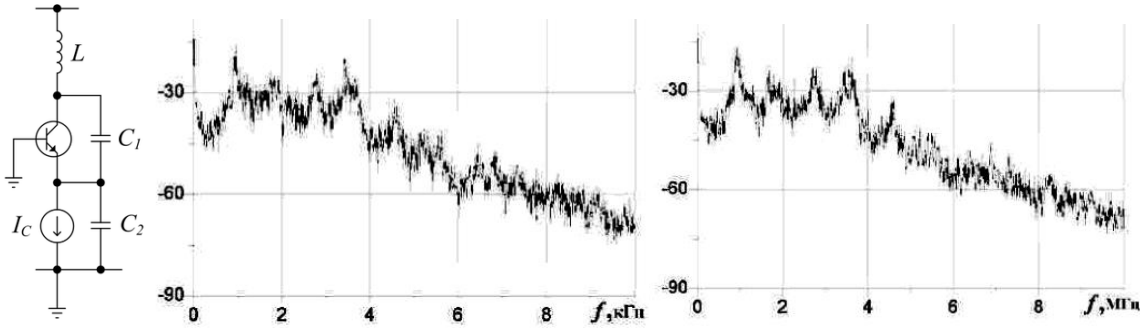


Рисунок 2.10 – Функціональна схема генератора Колпітца (ліворуч) та спектри еквівалентного перетворення (праворуч)

Генератор Колпітца в якості генератора шуму привабливий тим, що через зміну номіналів реактивних елементів(2.8) його легко пере налаштувати в різні діапазони частот, де структура спектру не змінюється. Під час підвищення діапазону частот структури генератора хаосу на основі генератора Колпітца використовується масштабування реактивностей в задану кількість раз:

$$C_1^1 = \frac{C_1^0}{\gamma};\ C_2^1 = \frac{C_2^0}{\gamma};\ L^1 = \frac{L^0}{\gamma}. \qquad (2.8)$$

Для демонстрації зміни частот, наприклад, застосуємо масштабування в 1000 разів, де реалізується перехід від кілогерцової зони до мегагерцевої зони (рис.2.10). Перехід до зони вищих частот зробити не так легко, завдяки суттєвому впливу паразитних параметрів елементів на таких високих частотах, але можливий через варіацію параметрів та підбір їх значень. Отже низькочастотні моделі хаотичних генераторів можуть бути із успіхом використані для побудови суттєво більш високочастотних генераторів детермінованого хаосу [30].

2.2.3 Декомпозиція та синхронізація хаотичних генераторів

Декомпозиція це можливість розділення схеми на окремі функціональні блоки або взаємопов’язані підсистеми. Для забезпечення процесу хаотичної синхронізації деякий зв'язок може бути розірвано для введення кола що забезпечує взаємодію між генераторами. Якщо хаотичну систему представити у вигляді системи диференційних рівнянь:

$$\frac{d\vec{U}}{dt} = \vec{f}\left(\vec{U}\right), \vec{U} \in R^n \tag{2.9}$$

і таку систему піддати декомпозиції, то її можливо представити у вигляді:

$$\begin{aligned} &\frac{d\vec{V}}{dt} = \vec{g}\left(\vec{V},\vec{W}\right),\ де\ \vec{V} = \left(U_1,...U_m\right);\ \vec{g} = \left[f_1\left(\vec{U}\right),...f_m\left(\vec{U}\right)\right]; \\ &\frac{d\vec{W}}{dt} = \vec{h}\left(\vec{V},\vec{W}\right),\ де\ \vec{W} = \left(U_{m+1},...U_n\right);\ \vec{h} = \left[f_{m+1}\left(\vec{U}\right),...f_n\left(\vec{U}\right)\right]. \end{aligned} \tag{2.10}$$

Якщо реалізувати подібну декомпозицію то сигнал або його частина може бути з одного генератора поданий на інший із такою ж декомпозицією (2.10), що і в першому. При чому перший генератора називають ведучим, а другий – веденим. Може бути і взаємний зв'язок між генераторами, де ведучого та веденого не має, але такий випадок відповідає одному складному генератору,а де процесу синхронізації [37-39].

Якщо параметри та структура веденого та ведучого генератора однакові (2.9), то навіть через різне установлення первинного стану в таких зв’язаних хаотичних генераторах спостерігається явище синхронної поведінки або хаотична синхронізація. Кількісно рівень синхронізації може бути визначений за різними критеріями, але найчастіше застосовується

відносне опосереднене відхилення, або величина, що називають «коефіцієнтом хаотичної синхронізації»:

$$\eta = \frac{\left\langle \Delta V^2 \right\rangle}{V_1^2} = \frac{\left\langle \left(V_2 - V_1\right)^2 \right\rangle}{V_1^2}; \quad \left|\vec{V}_1(t) - \vec{V}_2(t)\right| \xrightarrow[t\to\infty]{} 0 \tag{2.11}$$

Для того щоб синхронізація взагалі відбувалась необхідно виконання ряду умов:

1) В обох фазових площинах веденого та ведучого генераторів має існувати загальна фазова траєкторія.

2) Динаміка системи вздовж цієї траєкторії має бути стабільно стійкою стосовно трансверсального збурення.

Найпростіше генератор Чуа може бути підданий декомпозиції як на математичному, так і на фізичному рівні (рис.2.11) фізична декомпозиція реалізована за допомогою ідеальних операційних підсилювачів – інверторів. Якщо параметри веденої та ведучої систем обрати таким чином, щоб вони формували однакові фазові траєкторії (близькі параметри) у певній області керуючих параметрів буде спостерігатись повна або часткова хаотична синхронізація [38].

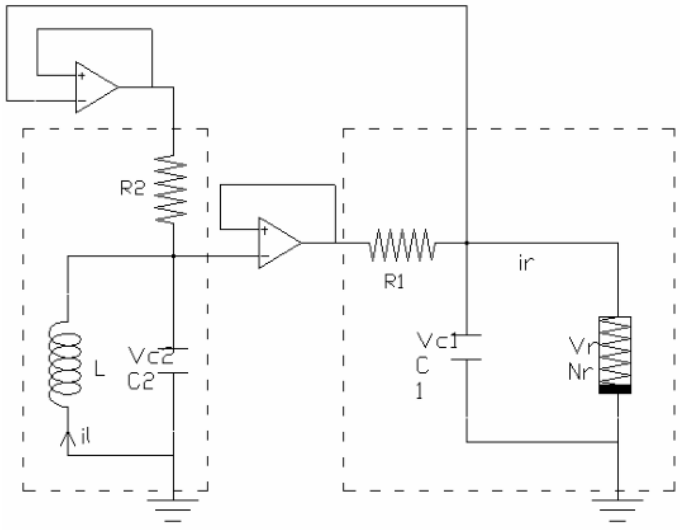


Рисунок 2.11 – Фізична декомпозиція генератора Чуа

Під час синхронізації загальна траєкторія – хаотичний атрактор, що виникає в спільному фазовому просторі, він має властивість стійкості до невеликих відхилень руху, що говорить про те, що синхронний відгук є стійким до дії адитивних шумоподібних завад.

2.2.4 Різновиди хаотичної синхронізації

Явище синхронізації до 90-х років розглядалось лише в аспекті регулярних сигналів, а синхронізація генераторів хаосу вважалася неможливою, через неможливість точного встановлення значень початкових умов та керуючих параметрів на передавальному та приймальному боці системи телекомунікацій. Проте роботи вчених Пекори і Керола [8] довели протилежність такої думки і навпаки вказано на можливість однакової еволюції двох пов’язаних генераторів хаосу по одним траєкторіям, саме це і обумовило можливість створення реальних фізичних телекомунікаційних систем із піднесівними сигналами у вигляді детермінованого хаосу.

Саме наявність синхронізації дозволило говорити про потенційну можливість зростання ТТХ телекомунікаційних системи, в тому числі прихованості дії та криптографічного захисту. На даний момент виділяють декілька різновидів синхронізації (рис.2.12), а застосовують на практиці лише одну – повну. Решта різновидів є предметом теоретичних досліджень.

Хаотичну синхронізацію поділяють на однобічну та двобічну (одно та двоспрямовану). Під час двобічної синхронізації розмірність та об’єм спільного фазового простору може бути відмінним від аналогічної однобічної синхронізації (рис.2.12), що виникає через взаємний вплив двох хаотичних генераторів та схем, що включено між ними для реалізації необхідного типу синхронізації.

Якщо між початковими налаштуваннями та параметрами керування в двох генераторах, що синхронізується існує істотна різниця, то з точки зору класичних поглядів такі генератори синхронізувати неможливо. Але така думка не відносить до хаотичних систем, можливий випадок, що доведено численними дослідженнями, що два генератора синхронізуються таким чином, що між траєкторіями їх синхронізованого руху існує певна детермінована функціональна залежність. Якщо синхронізуються таким чином ведений та ведучий генератор то подібний різновид синхронізації називають узагальненою[29].

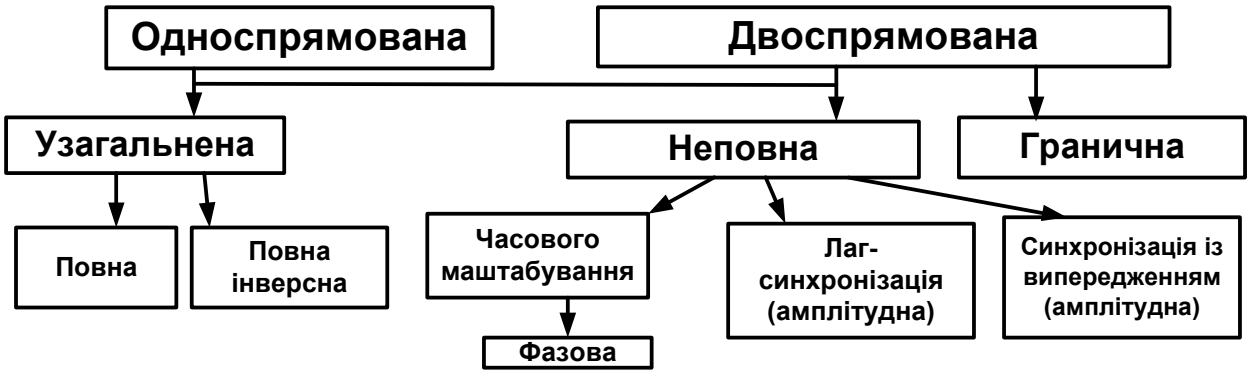


Рисунок 2.12 – Класифікація виділених вченими різновидів хаотичної синхронізації

Головним частинним випадком узагальненої хаотичної синхронізації є повна синхронізація (рис.2.12), де функція зв’язку між основним та допоміжним генераторами перетворюється у еквівалентність або тотожність. Отже за умови появи повної синхронізації реалізується максимально точний збіг фазових траєкторій ведучої та відомої хаотичної системи. Таким чином, критерієм ідеальної повної синхронізації є нульова різниця між однаковими фазовими змінними у векторі станів системи.

Набагато більш рідким різновидом узагальненої синхронізації є повна інверсна синхронізація де еквівалентність фазових траєкторій відбувається із точністю до протилежного знаку, що дивно для класичних різновидів синхронізації, але припустимо для нелінійних хаотичних систем. За певного

вибору параметрів протифазна синхронізація фіксується у взаємно пов’язаних системах Чуа.

Неповна хаотична синхронізація забезпечує неповне співпадіння вектору станів ведучої та відомої хаотичної системи лише із ненульовим значенням. Така похибка синхронізації в телекомунікаційних системах впливає на всі тактико-технічні характеристики і досягнення прогресу в їх покращенні є обмеженим, тому неповна синхронізація застосовується для практичної мети обмежено.

Різновидами неповної синхронізації є фазова синхронізація та синхронізація із запізненням (лаг-синхронізація) та синхронізація із випередженням (пре-синхронізація).

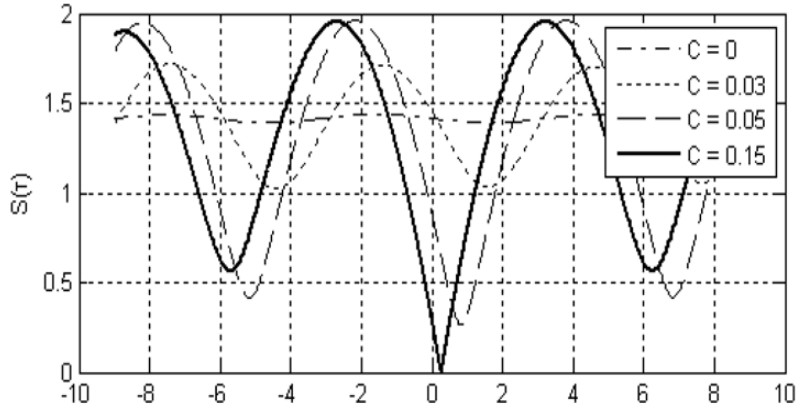


Рисунок 2.13 – Форма сигналів під час хаотичної синхронізації часового зсуву для хаотичної системи Чуа (С- сила зв’язку)

Фазова синхронізація є спробою накладання класичних ярликів на хаотичну синхронізацію у випадку наявності у спектрі хаотичної систему яскравого максимуму на деякій частоті. Таке доволі часто зустрічається, наприклад в системі Чуа для двозавиткового атрактора. Такі взаємодіючі під час синхронізації хаотичні генератори називають системами із репелерним атрактором, що можна описувати за допомогою поняття миттєвої фази $\varphi(t)$. Умова синхронізації – підтримання різниці миттєвих фаз у припустимих

межах відхилень, що є нестрогим правилом, а отже відповідна синхронізація вважається неповною [33,34].

Досить дивними також є інші різновиди неповної синхронізації, такі як лаг- та пре-синхронізація (рис.2.13), що проявляються як досягнення наближеної умови відповідності векторів стану ведучої та веденої системи але із деяким позитивним (для лаг-синхронізації) або навіть негативним часовим зсувом (пре-синхронізація). Ці дві синхронізації об'єднують під загальним ім'ям синхронізація часового зсуву.

Хаотична синхронізація часового зсуву між веденим та ведучим генераторами проявляється як певний зв'язок між амплітудами хаотичних сигналів на приймальному та передавальному боці де виникає ситуація однакової еволюції поведінки фазових змінних.

Хаотична синхронізація часового зсуву виникає в більшості випадків на межі між десинхронізацією та повною синхронізацію, тобто така синхронізація є перехідною з точки зору зміни параметру сили зв'язку між генераторами, що синхронізуються. Із збільшенням сили зв'язку часовий зсув наближається до нуля, а хаотична синхронізація часового зсуву переходить в повну синхронізацію.

Якщо збільшувати силу зв'язку між осциляторами то лаг синхронізація переходить в повну синхронізацію, а затримка наближається до нуля, наприклад, таке відбувається в хаотичних Реслера і Чуа (див. рис.2.9). Головним недоліком хаотичної синхронізації часового зсуву є те, що значення часового зсуву сильно залежить від значення керуючого параметра та встановити його наперед проблематично.

Цікавим та дуже рідким різновидом хаотичної синхронізації є гранична хаотична синхронізація. Під час такої синхронізації відбувається суттєва зміна атрактора веденої системи як за масштабом, де апертура атрактора може змінюватись в тисячі разів, або переміщуватись в іншу точку фазового простору. Так синхронізація спостерігалась за високого рівня зовнішнього шуму, в системі детектування із додатковим генератором Rucklidge.

Отже, для використання в аналогових телефонних системах телекомунікацій найбільш доцільним та практично реалізованим є режим повної хаотичної синхронізації. Така синхронізація може бути реалізована неперервно або імпульсно під час передачі тонального сигналу [40-44].

2.2.5 Детектування наявності синхронізації

Саме узагальнена синхронізація частіш за все реалізується між однотипними генераторами в формі повної синхронізації, де фазові траєкторії точно відтворюються на передавальному та приймальному кінці. В загальному випадку вираз для функції точки притягання обох синхронізованих генераторів знайти дуже складно, він може бути навіть фрактальним, але показати що існує синхронізація можливо одним із методів [26-27]:

1) Метод порівняння, де застосовується деякий критерій помилки фазової траєкторії веденого генератора відносно ведучого.

2) Метод умовних показників Ляпунова, чисто математичний метод і потребує відомих диференційних рівнянь для опису складної системи синхронізації.

3) Метод допоміжної хаотичної системи, що є найбільш доцільним для практичного використання.

В методі допоміжної хаотичної системи на приймальному боці розташовано не один, а два ведених генератора із однаковою структурою, що підключено до ведучого генератора ідентично, через розв’язку, що усуває взаємний вплив. Початкові умови та параметри керування основної хаотичної системи та додаткової хаотичної системи можуть бути різними, а оператори еволюції однаковими, в такому випадку характерна різка залежність рівня синхронізації від сили зв’язку між генераторами (рис.2.14).

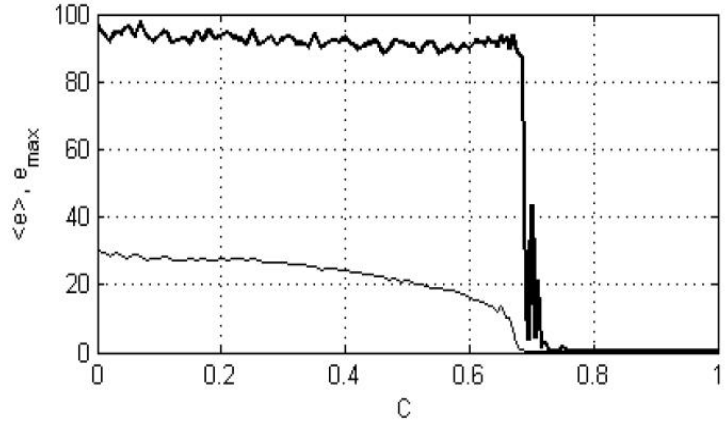


Рисунок 2.14 – Залежність інтегральної похибки синхронізації від сили односпрямованої взаємодії генераторів хаосу

Якщо початкові умови та параметри керування розташовуються в одній зоні притягання дивного атрактора оператора еволюції, то із часом обидва генератора синхронізуються та демонструють ідентичну поведінку із мінімальним значенням за обраним критерієм синхронізації. Якщо параметри керування та початкові умови знаходяться «далеко» то синхронна поведінка основного та допоміжного генератора не відбувається, що і може бути критерієм десинхронізації.

2.3 Аналогова хаотична модуляція

2.3.1 Модуляція хаотичним маскуванням

Хаотичне маскування корисного сигналу перший та найбільш технічно простий спосіб введення інформаційного сигналу в сигнал детермінованого хаосу (рис.2.15). Пристроєм модуляції в даному випадку є простий суматор. На передавальному боці аналоговий сигнал $x(t)$ підмішується в суматорі до несівного хаотичного сигналу $ch(t)$. Цей сигнал $ch(t)$ може бути одним із сигналів фазової змінної, або їх лінійною комбінацією. Така суміш

$u(t) = m \cdot x(t) + ch(t)$, де m - глибина модуляції в традиційному розумінні, в певній пропорції передається до приймача по лініям передачі [40,43].

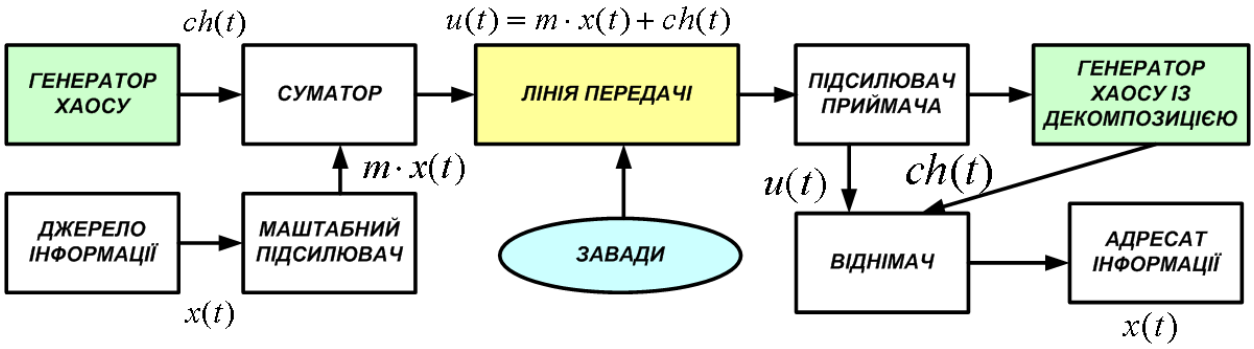


Рисунок 2.15 – Спрощена структура каналу зв’язку із хаотичним маскуванням

На приймальному боці такої системи реалізується всі механізми повної хаотичної синхронізації веденого та ведучого генератора. Якщо глибина модуляції невелика, то сигнал $x(t)$ розглядається як зашумлення веденого генератора в лінії передачі.

Під час процесу повної синхронізації на приймальному боці динаміка генератора хаосу приймача стає ідентичною генератору хаосу передавача без введеного інформаційного сигналу. Детектування інформаційного сигналу $x(t)$ просто отримати за допомогою лінійного віднімача між вхідним сигналом $u(t)$, що приймається і отриманим синхронним хаотичним відгуком хаотичного генератора в приймачі [28].

Схема передачі інформації на базі хаотичного маскування ефективно працює за умови низького рівня завад каналу зв'язку. За потужністю хаотичний сигнал має перевищувати потужність модулюючого сигналу на 35-55 дБ. Додавання шуму в лінії передачі хаотичного каналу зв’язку призводить до суттєвих втрат інформаційного повідомлення. Отже хаотичне маскування вимагає значних відношень сигнал-завада і ще його головний недолік.

Система хаотичного маскування вимагає, крім того, високого рівня підтримки ідентичності початкових умов та керуючих параметрів для веденого та ведучого генераторів. Це призводить до необхідності збільшення технологічної точності та здорожує апаратуру. Через застосування суматора як простого типу модулятора такай різновид слід віднести до аналогових, лінійних та зовнішніх, де структура хаотичного генератора на передавальному боці не підлягає ні впливу ззовні, ні декомпозиції.

2.3.2 Модуляція зміною параметрів керування

Принцип модуляції зміною параметрів полягає у зміні одного або декількох параметрів хаотичного генератора передавача таким чином, щоб забезпечувалась відповідна лінійна пропорційна зміна для синхронізованого хаотичного генератора на приймальному боці. Таким критерієм може бути рівень входження в синхронізм, або рівень десинхронізації основного та допоміжного хаотичного генераторів [39].

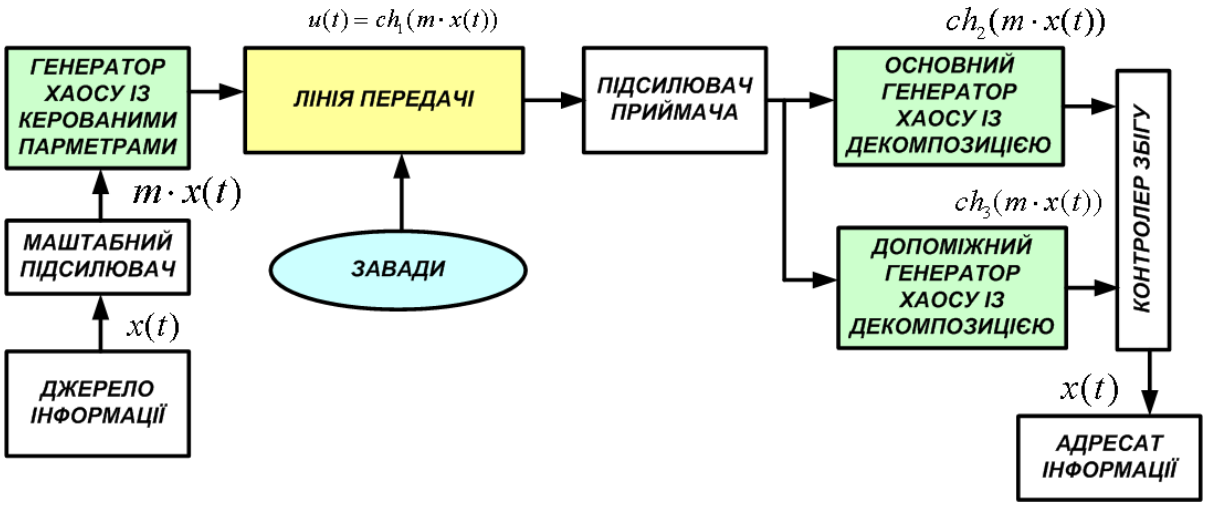


Рисунок 2.16 - Схема модуляції зміною параметрів керування

Модуляція зміною параметрів керування придатна (рис.2.16) також і для передавання цифрового сигналу. Під час такого процесу введення

інформаційний сигнал $x(t)$ змінює однин або декілька одночасно параметрів передаючого генератора $ch(t)$ таким чином, щоб після певного типу обробки та застосування критерію схожості фіксувалась наявність або відсутність синхронізації на приймальному боці.

Для можливості реалізації на практиці такої схеми модуляції керуючі параметри веденого та ведучого генераторів мають бути обрані ідентичними деяким наборам, що відповідають логічному нулю та логічній одиниці.

Більшість наукових робіт віддає перевагу використанню такої схеми для передавання цифрового сигналу, для передачі аналогових повідомлень застосування схеми досліджено слабко, що і є предметом досліджень.

Модуляція зміною параметру відноситься до внутрішніх, аналогових та в загальному випадку – нелінійних різновидів.

2.4 Криптостійкість повідомлень хаотичних каналів зв’язку

2.4.1 Хаотичні методи забезпечення криптостійкості

Якщо розглядати розвиток систем телекомунікацій із застосуванням сигналів детермінованого хаосу, то слід сказати, що на даний час вони не набули широкого поширення і розглядаються лише в спеціалізованих системах та як наукові доробки. В першу чергу цьому сприяють високі вимоги щодо ідентичності параметрів та характеристик засобів приймача та передавача, що на декілька порядків перевищують вимоги до традиційних систем обробки із класичними сигналами. Але із розвитком технологій та культури виробництва ці проблеми можуть бути подолані, от тоді і згодяться всі напрацювання «дослідників – хаосистів».

На початку спроб застосування сигналів детермінованого хаосу у радіотехніці була потреба генерації широкосмугових та широкосмугових сигналів простими технічними засобами. Широкосмугові сигнали мають ряд

переваг над вузькосмуговими, наприклад, збільшена база сигналу, ширші можливості багатоканальності, вища проникна здатність, захист від системних завад діючих вузькосмугових систем, тощо, і забезпечення прихованості дії в тому числі.

В результаті потреб широкосмуговості з’явились прямохаотичні системи зв’язку, де природна властивість неперервного спектру в широкому діапазоні частот і простій конфігурації власне генератора забезпечували ці потреби. Прихованість дії, як перший етап захисту інформації реалізовувалась на базі шумоподібності сигналів детермінованого хаосу та їх схожості на природні завади. Для роботи таких систем необхідно було застосування зовнішньої синхронізації, наприклад, через глобальну систему космічної навігації (GPS).

Рівень криптозахисту в даному випадку реалізовувався на основі апаратного вибору типу генератора, що недостатньо для потреб сучасних телекомунікацій, особливо у військовій галузі. Прямохаотична передача даних не використовує хаотичну синхронізацію як базовий принцип організації каналів зв’язку, для цього застосовуються деякі локальні та глобальні канали. Можна охарактеризувати прямохаотичні системи такі, які мають нульовий рівень крипто захисту.

Покращити рівень криптозахисту та сформувати дійсно хаотичні канали передачі цифрових та аналогових даних вдалось лише після відкриття явища хаотичної синхронізації та хаотичного синхронного відгуку. Першими та найпростішими системами із несівними коливаннями детермінованого хаосу запропоновані системи хаотичного маскування, де ведений хаотичний генератор виступає як високодобротний фільтр сигналу детермінованого хаосу із адитивної суміші із інформаційним сигналом повідомлення.

Криптографічний захист в даному випадку реалізований на базі вибору певної фазової траєкторії генераторів на приймальному та передавальному боці через встановлення параметрів хаотичного генератора певного типу. Однак застосування таких систем спряжене із високою чутливістю до

зовнішніх флуктуаційних завад , що вимагало надзвичайно «чистих» каналів передачі із відношенням сигнал- завада до 70..80дБ.

Рисунок 2.19 – Забезпечення рівня криптостійкості методами обробки хаотичних сигналів в каналах передачі

Крім того, в системах із хаотичним маскуванням рівень модулюючого сигналу має бути на 30..40 дБ нижчий за рівень несівного, що дає низьку енергетичну ефективність. Такі недоліки дають можливість охарактеризувати спосіб як низький рівень криптографічного захисту (див.рис.2.19).

Численними дослідниками пропонувалось різними шляхами обійти недоліки систем із хаотичним маскуванням в сенсі покращення прихованості дії дії. Такі шляхи можливо звести до двох основних нововведень: використання допоміжних сигналів різної форми та застосуванні переривчастої синхронізації. Найбільш часто зустрічають допоміжні сигнали у вигляді гармонічного коливання та лінійних допоміжних перетворень та імпульсна синхронізація веденого та ведучого генератора (див.рис.2.19).

Наступний крок підвищення захисту інформації в хаотичних каналах реалізовано на базі застосування допоміжного веденого хаотичного

генератора, що дозволило різко зменшити вимоги до якості аналогових каналів передачі в сенсі глобальної нелінійності та рівня завад на декілька порядків і об’єднати процес введення інформаційного повідомлення та хаотичної генерації через зміну параметрів керування хаотичного генератора (див.рис.2.19).

Модуляція параметрів керування відноситься до нелінійних способів і сам факт внутрішньої модуляції вже можливо розглядати як збільшення рівня криптографічного захисту до умовно середнього через вибір одного або декількох, або декількох разом параметрів для введення інформаційного сигналу в хаотичну піднесівну. При цьому фазові траєкторії суттєво змінюються, але залишаються в рамках атрактора даної хаотичної системи.

Для ще більшого рівня криптографічної стійкості (див. рис.2.19) на апаратному рівні пропонується застосувати екстраполяційну схему, що фактично відтворює модуляційну характеристику в просторі зміни параметрів керування за певним законом та зворотний зв'язок в системі детектування із декількома веденими генераторами, що можливо представити як високий рівень криптографічного захисту. При цьому рівень криптографічного захисту має зрости на декілька порядків в сенсі еквівалентної кількості ключів шифрування-дешифрування як в апаратному напрямку так і програмному.

2.4.2 Оцінювання кількості ключів шифрування

Рівень криптографічного захисту можливо оцінити через визначення кількості ключів шифрування через застосування діапазону можливих варіантів незалежних процедур та параметрів під час передачі та обробки сигналів хаотичними методами. В таких умовах загальна кількість варіантів є об’єднанням апаратних рішень щодо формування каналів передачі та

програмних рішень, що власне в класичних системах і розглядається як поле ключів шифрування.

В аспекті апаратного захисту кількість варіантів можливо оцінити як кількість схемотехнічних рішень, що застосовують хаотичні методи обробки. В таких рішеннях головним фактором є вибір схеми хаотичного генератора, яких на даний час винайдено більш як 1000, але придатними для застосування в багатоканальних широкосмугових телекомунікаційних системах, що мають високий рівень шумоподібності та найбільш оптимальні кореляційні та автокореляційні характеристики виділено близько 100.

Для оптимальних схем генераторів для телекомунікаційних потреб кількість їх біфуркаційних параметрів може сягати до 10Із урахуванням багатопараметричної модуляції фазових змінних та їх параметрів кількість незалежних схем модуляції може сягати до декількох десятків (рис.2.20).

Найбільш складним під час обробки хаотичних сигналів є побудова схеми хаотичної синхронізації та вибір динамічних змінних аналогового хаотичного генератора для використання як канального сигналу. В подавляючій більшості винайдених аналогових хаотичних генераторів, що можуть бути описані диференційними рівняннями та досліджені статистичними методами в сенсі формування хаотичних режимів а кількість розмірностей (кількість фазових змінних) складає 3 або 4. Використання більшої кількості розмірностей викликає різке зростання обчислювальних ресурсів для моделювання. Таким чином, застосування фазових змінних або їх комбінацій під час передачі інформації на базі хаотичного синхронного відгуку а також критеріїв синхронізації дає можливість оцінити нижню кількість варіантів апаратних криптографічних ключів до 10.

Отже нижню межу апаратних схем реалізації варіантів захисту інформації можливо оцінити як декілька тисяч, при цьому застосування іншої схеми для спроб дешифрування повідомлень автоматично призводить до некоректних результатів в апаратному сенсі.

Програмні ключі шифрування формуються на основі вибору значень деяких характеристик та параметрів введення інформаційного сигналу в хаотичну піднесівну таким чином, щоб за умови наявності певного варіанту апаратної реалізації у абонентів та зловмисника, у останнього виникла б потреба перебору великої кількості комбінацій для доступу до змісту зашифрованого повідомлення.

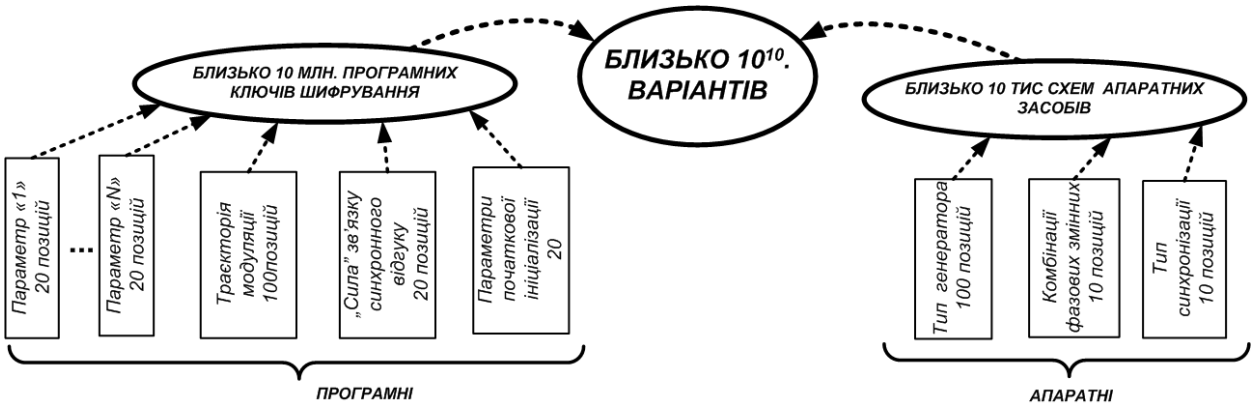


Рисунок 2.20 - Діаграма формування ключів шифрування в хаотичних системах захисту інформації

В першу чергу кількість ключів шифрування забезпечує вибір необхідних значень одного або декількох параметрів. В численних роботах [] показано, що зміна параметру на 5 відсотків забезпечує настільки суттєву зміну фазових траєкторій, що добування інформації без відомостей про поточне значення параметру стає неможливим, що дає близько 20 варіантів ключів по кожному параметру окремо. Для більшої кількості параметрів кількість ключів криптографічного захисту визначається як добуток кількості варіантів по кожному, через незалежність впливу параметрів на хаотичну поведінку в системі обраного хаотичного генератора.

Варіантів рухів хаотичних змінних в фазовому просторі є нескінченно багато, але на початковому етапі поведінка траєкторій залежить не тільки від біфуркаційних параметрів, але і від початкового стану системи, або значень фазових змінних в нульовий момент часу. Хоча поведінка хаотичної системи

надалі виходить на траєкторії атрактору, для систем реального часу початкові значення теж можливо вважати варіантами для формування ключів шифрування, кількість яких можливо оцінити до сотні (див. рис.2.20).

В нашому випадку розглядаються системи передачі аналогових телефонних повідомлень і для таких повідомлень важливе не тільки середні значення обраних параметрів але і параметри їх зміни під час введення аналогового сигналу в загальному просторі параметрів біфуркації. Це можливо розглядати, в деякому сенсі, як субалгоритм шифрування. Із зростанням кількості параметрів кількість таких субалгоритмів різко зростає, але для мінімальної кількості параметрів -2, кількість алгоритмів розумно встановити до сотні. Такий алгоритм «вкладається» як параметри екстраполятора на приймальному боці, та параметри зміни біфуркаційних параметрів параметричної модуляції на передавальному боці системи.

Окремо слід сказати про особливість синхронізації та вибору «глибини» рівня зв'язку між ведучим та веденими генераторами хаотичної системи захисту інформації, що в цьому випадку описується системою із збільшеною кількістю диференційних рівнянь. Рівень взаємодії опису ведучого та ведених генераторів також залежить від встановлення певного рівня глибини. Таким чином глибина зв'язку також розглядається як складова у варіантах комбінацій ключа шифрування, кількість яких оцінимо як до 20.

Об'єднана кількість варіантів із урахуванням зазначених змінних під час формування ключа шифрування в хаотичній системі із параметричною модуляцією та хаотичним синхронним відгуком визначається як добуток кількості та за попередніми оцінками складає до 10^{10} , що унеможливлює дешифрування в реальних ділянках часту аналогових повідомлень типу стандартний телефонний сигнал.

3 МОДЕЛЮВАННЯ СИСТЕМ ХАОТИЧНОЇ КРИПТОГРАФІЇ

3.1 Моделі взаємодії генераторів динамічного хаосу

3.1.1 Вибір опорного генератора та його модель

Отримання структури та дослідження генератора сигналів детермінованого хаосу є складним завданням, і натепер можливо виділити до сотні запропонованих схем генераторів в яких можливе явище детермінованого хаосу.

До вибору опорного генератора висувається ряд вимог, що надалі дозволить забезпечити більший рівень криптографічного захисту телефонного повідомлення, а саме:

1) Високий рівень неперервності та рівномірності спектру в заданому діапазоні частот, що необхідно для імітації найбільш ідеальної випадковості в умовах протидії конкурента.

2) Наближення кореляційних характеристик до ідеальних, що дозволяє генерувати багатоканальні схеми передачі телефонних повідомлень в системі криптографічного захисту із мінімальним рівнем системних завад.

3) Простота схеми та можливість практичної реалізації, особливо в аспекті відповідності нормованих параметрів математичного опису, номінальним значення компонент схеми.

4) Мінімальний рівень залежності опосередненої потужності, або енергії від зміни керуючого параметра хаотичних генераторів, що впливає на можливість дешифрування факту наявності повідомлення в хаотичному процесі, який діє в каналі зв’язку через аналіз структури енергетичного спектру.

За вказаними вище критеріями у [45] проведене впорядкування основних схем хаотичних генераторів, що придатні для застосування у

телекомунікаційних системах. Під порівняльного аналізу таких діаграм серед перших по якості завжди розташовується генератор Rucklidge, який надалі і будемо застосовувати як аргументований доцільний для використання в хаотичній системі телекомунікацій.

Нелінійна схема з хаотичним режимом запропонована дослідником А.К. Ракліджем ще у 1992р. під час аналізу поведінки магнітогідродинамічних явищ, що може бути представлена простою системою диференційних рівнянь першого порядку із трьох змінних (СДР) та [45]:

$$\left\{\frac{dx}{dt} = -kx + ay - yz;\quad \frac{dy}{dt} = x;\quad \frac{dz}{dt} = -z + y^2\right\}. \qquad (3.1)$$

Особливість такої структури хаотичного генератора полягає у квадратичній нелінійності «*y*» та наявності всього двох параметрів керування«*a*» та «*к*», що спрощує підбір режимів під час аналізу шляхом перебору. Наявність квадратичної нелінійності в генераторі Rucklidge (3.1) дозволяє в момент односпрямованої узагальненої синхронізації фазовій траєкторії швидко наблизитись у спільну зону притягання дивного атрактора. Спектр показників Ляпунова для схеми Rucklidge наступний: [0,193; 0; -3.193], що підтверджує наявність сигналу детермінованого хаосу на виході.

Для первинного імітаційного дослідження в середовищі Simulink розроблена схема генератора (рис.3.1) та проведено її симуляція з методою перевірки працездатності та виявлення кореляційних та спектральних характеристик. Дослідження проводились для основних фазових змінних, що подано у системі рівнянь (3.1), в результаті отримані часові діаграми роботи, які підтверджують хаотичний характер генерованого сигналу на усіх виходах.

Слід зазначити, що для використання у радіосистемах серед сигналів, що генеруються (рис.3.1), можуть використовуватись лише ті, в складі яких відсутня постійна складова. Тобто для передавання інформації по

радіоканалу зв'язку сигнал "Z» не є придатним. Цей факт підтверджується і подальшими дослідженнями.

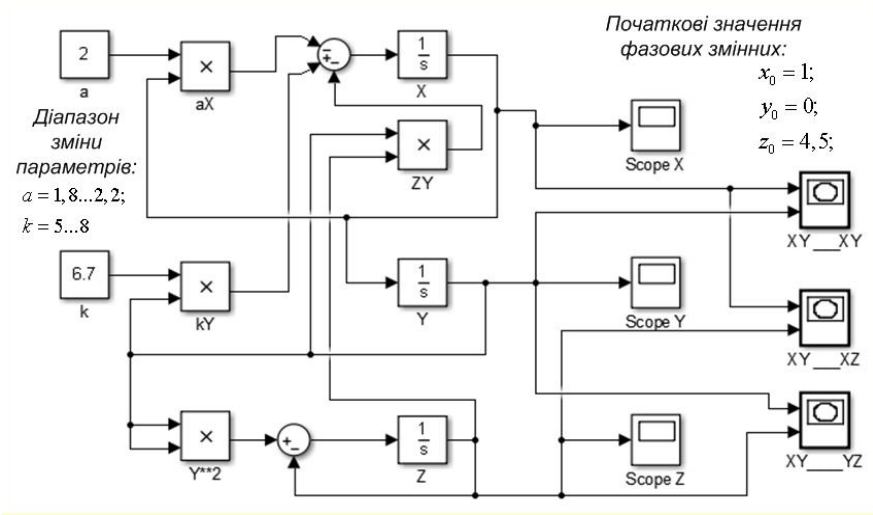


Рисунок 3.1 – Імітаційна модель хаотичного генератора Rucklidge в середовищі імітаційного моделювання MatLab/Simulink

Розмах сигналів детермінованого хаосу для хаотичного режиму роботи приблизно однаковий і не більше 20В по усім напрямкам двозавикового дивного атрактора, що досить рівномірно заповнено фазовими траєкторіями (рис.3.2).

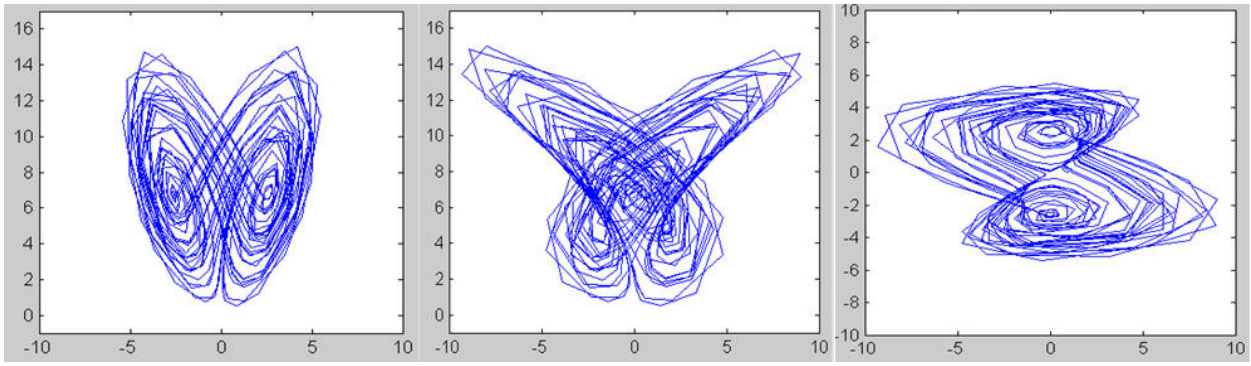


Рисунок 3.2 – Проекції дивного атрактора генератора Rucklidge на ортогональні площини за результатами моделювання

Такі особливості дозволяють стверджувати про наявність псевдо шумового характеру сигналу детермінованого хаосу, автоматичній отриманні широкосмуговості та кореляційних характеристик високої якості. Також це

підтверджує правильні висновки, щодо ранжування хаотичних генераторів у [45].

3.1.2 Синхронізація опорних хаотичних генераторів

В усіх телекомунікаційних схемах в тому числі і системах із криптографічним захистом слід в першу чергу подбати про синхронізацію, в даному випадку про забезпечення хаотичної синхронізації. Для більшості запропонованих схем із використанням генераторів хаосу застосовують зовнішню синхронізацію, тільки під час застосування допоміжного генератора факт синхронізації є інформаційним критерієм передачі бітових повідомлень [35].

Для забезпечення хаотичної синхронізації в генераторі Rucklidge можливо використати лише один сигнал змінної «y». Якщо синхронізація зовнішня, то окремий канал має використати сигнал саме із каналу інтеграції імітаційної моделі - «y». А інформаційний канал – «x», завдяки тому, що хаотична синхронізація по змінній «x» є нестабільною.

Блок синхронізації виконує функцію об’єднання двох коливань ведучого та веденого генератора в певній пропорції, щоб сумарний сигнал відповідав 100% дії фазової змінної. Односпрямоване об’єднання сигналів необхідно для можливості допуску відхилення фазових траєкторій по інформаційному каналу в деяких межах під час модуляції та взагалі можливості детектування аналогового сигналу за допомогою віднімача (рис.3.3).

Для виявлення режиму хаотичної синхронізації та визначення рівня синхронізації можуть бути застосовано багато критеріїв [39], але найбільшої популярності набув критерій мінімальної потужності (енергії) різницевого сигналу веденого та ведучого генераторів:

$$P_{\Delta} = \frac{1}{T}\int_{0}^{T} \left(\zeta_T - \zeta_R\right)^2 dt \qquad (3.2)$$

де, ζ_T, ζ_R - одна із фазових змінних, по яким проводиться аналіз ідентичності роботи ведучого та веденого генераторів відповідно;

T – час аналізу або характерний час в системі, виходячи із типу аналогового повідомлення.

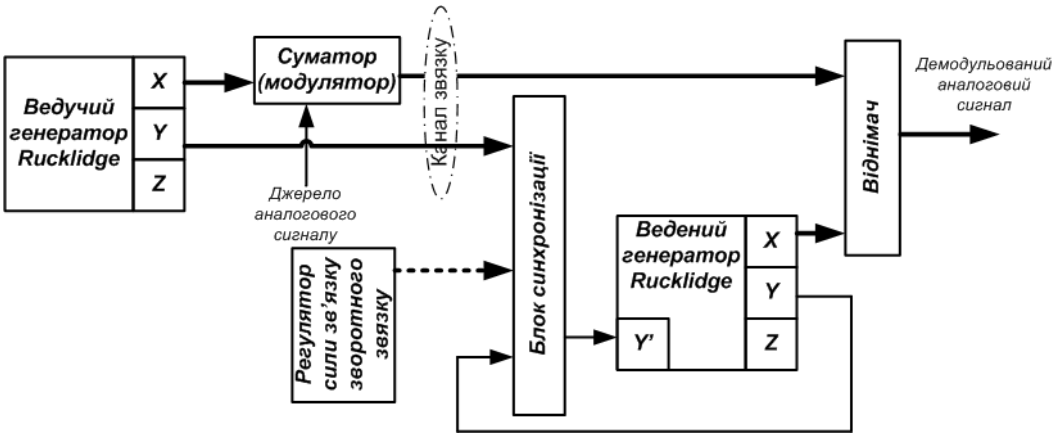


Рисунок 3.3 – Схема передачі аналогової інформації на основі хаотичного маскування та зовнішньої синхронізації

В ідеальному випадку після синхронізації потужність (3.2) P_{Δ}, прямує до нуля, а за наявності завад – до деякого мінімуму.

Візуальна ідентифікація може бути проведена за допомогою осцилографічного ортогонального методу фігур Лісажу, в випадку точного збігу сигналів веденого та ведучого генератора фігура Лісажу буде мати вигляд прямої нахильної лінії, а відмінності в сигналах «розмивають» лінію, та вона займає більшу площу. Площа фігур Лісажу отримана із веденого та ведучого генераторів може бути чисельним критерієм рівня синхронізації хаотичних генераторів в телекомунікаційній системі (рис.3.4).

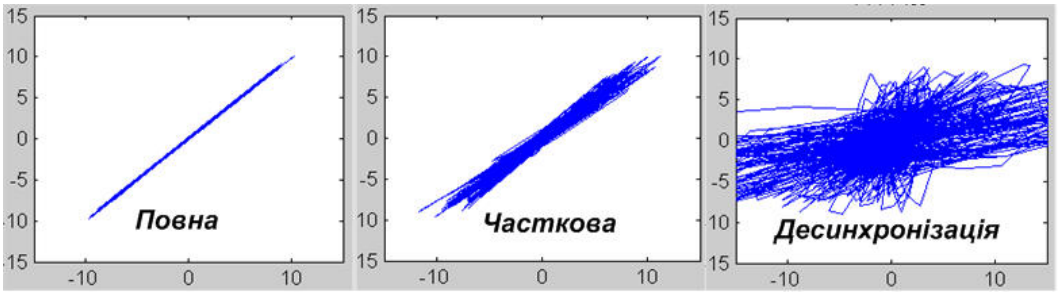


Рисунок 3.4 – Діаграми повної, часткової та відсутності синхронізації ведучого та веденого генераторів

Також критерієм наявності хаотичної синхронізації може бути визначення рівня взаємної кореляції двох однойменних сигналів за умови нульового часового зсуву вибірок між сигналами. Цей метод ґрунтується на шумоподібності хаотичних сигналів. На основі критеріїв можливо визначити діапазон параметрів та діапазон зовнішніх впливів під час яких хаотична синхронізація підтримується на заданому рівні.

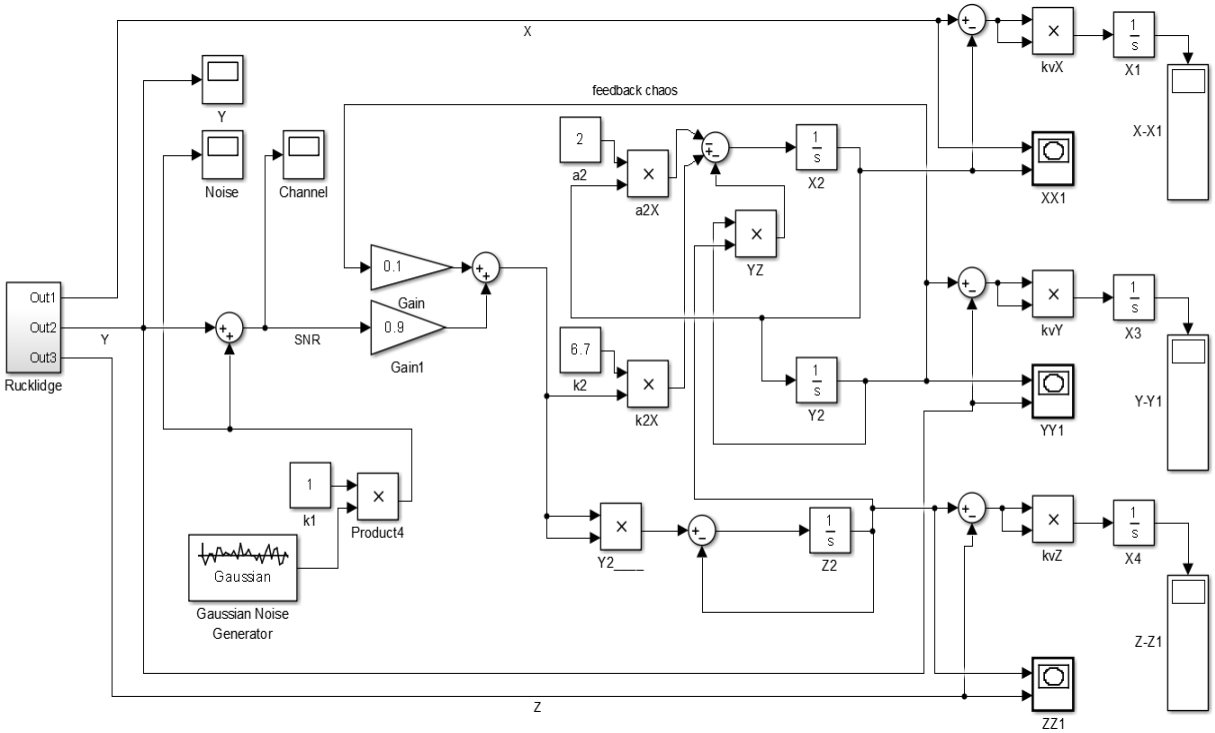


Рисунок 3.5 – Застосування критерію мінімальної потужності різницевого сигналу в імітаційній моделі синхронізації генераторів Rucklidge

Елементи обрахування індикації хаотичної синхронізації (рис.3.5) можуть бути підключено до усіх незалежних змінних генератора Rucklidge.

Діапазон коефіцієнтів зворотного зв’язку для веденого хаотичного генератора складає 0,05…0,2, що відповідає силі «нав’язаного» зв’язку для з боку ведучого хаотичного генератора 0,8…0,95, загалом це підтверджує необхідність «сильного» зв’язку для забезпечення режиму повної синхронізації за умови розлаштування параметрів веденого та ведучого генераторів.

Загалом відомо [44], що рівень збігу фазових траєкторій слабко залежить від потужності зв’язку, якщо зв'язок все ще сильний, тому для подальших досліджень в режимі сильного наведення встановимо його на рівні 90%.

3.1.3 Похибки синхронізації

Як і в будь-яких системах телекомунікацій, рівень кінцевих спотворень залежить від завад в каналі передачі. Завади в каналі, в переважній більшості представляють у вигляді білого гаусівського адитивного шуму.

Якщо застосувати критерій мінімуму різницевої потужності та представити залежності в логарифмічному масштабі, то яскраво видно наявність лінійної ділянки на графіках залежностей (рис.3.6). Цю залежність можливо застосувати для передачі інформаційного повідомлення за допомогою додаткового сигналу у вигляді гаусівського шуму.

Під час застосування хаотичного маскування в схемі із узагальненою синхронізацією (див. рис.3.3), де присутні два односпрямовані канали – синхронізації та передачі інформації, похибки різницевої потужності веденого генератора відносно ведучого досліджувались по кожному з них. Для кожного каналу графіки залежностей носять подібний характер із

яскраво вираженою лінійною ділянкою, якщо їх розглядати у логарифмічному масштабі.

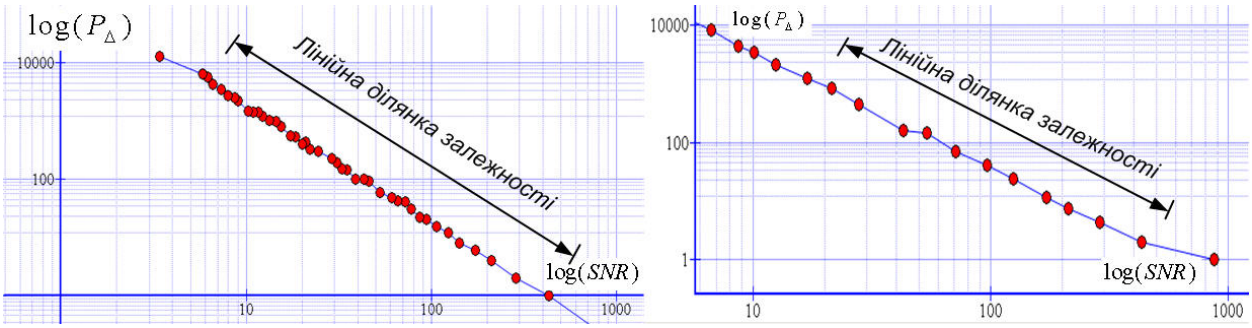


Рисунок 3.6 – Лінійні ділянки інформаційного каналу (ліворуч) та (каналу синхронізації) залежності похибки синхронізації від відношення сигнал-шум

Крім того, графіки залежностей різницевих потужностей по каналам за змінними X та Y дещо відрізняються хоча подібні функціонально. Контроль синхронізації по каналу «Y» реалізується із більшою чутливістю і за умови більших рівні шуму, що говорить доцільність застосування обраної хаотичної змінної як основи для формування сигналу детермінованого хаосу в системі.

Таку залежність можливо використати для передавання інформації в хаотичному каналі передачі із криптографічним захистом. Ідея полягає в тому, щоб застосувати додатковий шумовий сигнал як допоміжний, що обумовлює похибку синхронізації. В такому випадку структура буде мати вигляд (рис.3.7).

В такій хаотичній системі телекомунікацій потужність введеного в канал хаотичної синхронізації шуму, що генерується за допомогою генератора гаусівського шуму (або псевдо шуму) визначається миттєвими значеннями аналогового сигналу. Залежно від потужності шуму в каналі синхронізації ведений генератор в більшій або меншій мірі змінює потужність різницевого сигналу по інформаційному каналу, що і відбиває суть демодуляції аналогового сигналу за умови попереднього експоненціювання та обрахунку результату обчислень в логарифмічних одиницях.

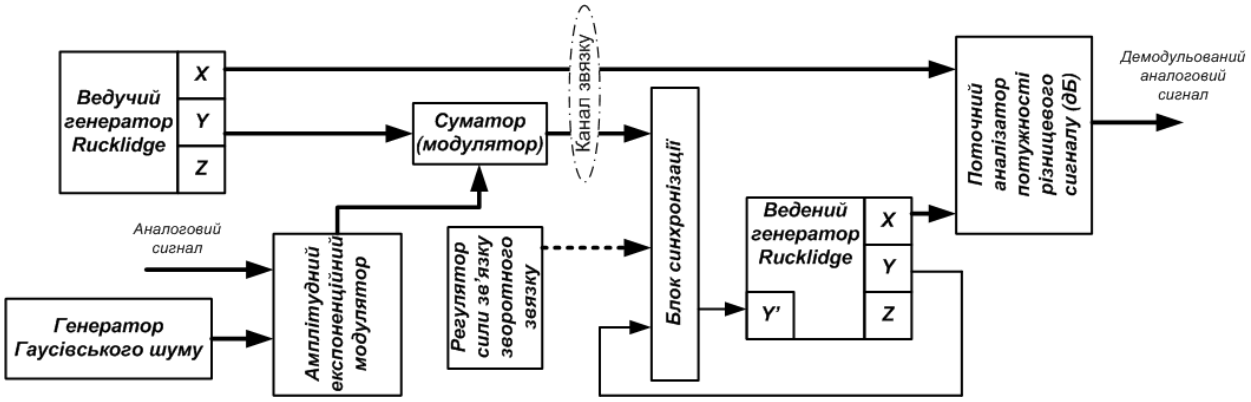


Рисунок 3.7 – Структура системи передачі із шумовою піднесівною на методі контролю синхронізації

Під час роботи такої системи передбачається що потужності штучних шумів в каналі значно переважають потужності шумів наведених ззовні. Тепловий шум в даному випадку буде впливати як деяка постійна підставка (постійний струм) де модульованого сигналу, що не є суттєвим для передачі телефонних повідомлень, що не мають постійної складової.

3.2 Модуляційні характеристики

3.2.1 Біфуркаційні параметри і синхронізація

Наступні досліди спрямовувались на встановлення загального характеру залежності рівня синхронізації від первинної неточності встановлення параметрів (рис.3.8) якщо рівень шумів мінімальний, стартові значення фазових змінних ідентичні, а сила зв’язку між генераторами – оптимальна близько 0,92.

Хаотичний генератор Rucklidge має лише два параметри, варіація яких впливає на хаотичний режим роботи. Зрозуміло, що для веденого та ведучого генераторів ідентичними ці параметри встановити неможливо і їх різниця є природною. За умови малої відмінності між параметрами веденого та

ведучого генераторів режим хаотичної синхронізації встановлюється більш швидко.

Для системи телекомунікацій із модуляцією через маскування час входу в синхронізм не суть важливий, але для схем із допоміжним генератором такий факт суттєво впливає на всі тактичні характеристики системи.

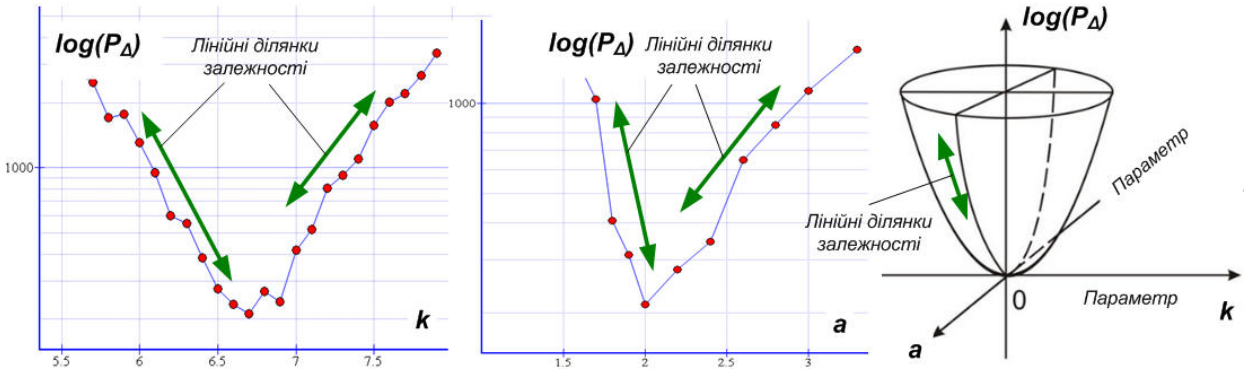


Рисунок 3.8 – Залежність похибки синхронізації від неточності хаотичного параметра – k,a, та тривимірна екстраполяція сукупного впливу параметрів

Під час досліджень входу в синхронізм генератора Rucklidge на основі детектування похибки синхронізації на базі додаткового генератора встановлено (див. рис.3.9), що загальний графік залежності похибки синхронізації від зміни параметрів *(a)* та *(k)* носить наближено парний характер відносно зони, де похибка мінімальна, тобто по центру хаотичного режиму (див.рис.3.8).

Крім того якщо застосувати для похибки (вимірюється як різницева потужність сигналу фазових змінних) логарифмічний масштаб то на залежності присутня значна лінійна ділянка, що може бути застосована як модуляційна характеристика в системі криптографічного захисту системи прихованого зв'язку. Розмір лінійної ділянки досить значний і сягає більш як 20% від оптимального значення параметрів керування генератора Rucklidge.

В такій системі передачі інформації сукупність пар значень параметрів хаотичного генератора, які визначають середину лінійної ділянки, задають

параметри криптографічного захисту, які впливають на сам характер сигналу детермінованого хаосу на виході.

Сукупну залежність похибки можливо представити у вигляді тривимірного конусу (рис.3.8 праворуч), де передавання аналогової інформації здійснюється через «пересування» значень його параметрів по поверхні в межах максимально лінійної ділянки і поточного фіксування різниці рівнів хаотичної синхронізації в лінійному масштабі.

Структурна схема, що використовує поданий вище принцип модуляції представлена на рис.3.9, в якій сумісний параметричний модулятор за допомогою ключів шифрування обирає траєкторію зміни параметрів під дією аналогового сигналу (тонального сигналу). Зміна параметрів відбувається відносно повільно від характерного часу змін у хаотичному сигналі, тому сигнал детермінованого хаосу не змінюючи хаотичного характеру виходить на іншу траєкторію, що подібна до попередньої. Таким чином зловмиснику або ворогу важко зрозуміти про початок передавання повідомлення та його наявність в даний момент часу. Фактично забезпечується прихованість дії крім криптографічної стійкості.

На приймальному боці такої телекомунікаційної криптографічної системи встановлено два структурно ідентичних неавтономних генератори Rucklidge із декомпозицією по змінній *“y”*. В канали цієї фазової змінної вводиться хаотичний сигнал із введеним аналоговим сигналом за принципом подвійної параметричної модуляції. В результаті ведені хаотичні генератори починають синхронізуватись із ведучим генератором тим краще, чим ближче значення їх параметрів до поточних параметрів ведучого генератора.

Якщо за допомогою блоків дешифрування обрати параметри ведених генераторів на різних боках лінійної ділянки (див. рис.3.8), то поточні значення похибки за критерієм різницевої потужності будуть змінюватись за законом аналогового повідомлення і таким чином реалізовуватиметься дешифрування. Дешифрування можливе лише за умови правильного вибору

значень параметрів, що забезпечується ключами шифрування на передавальному та приймальному боці.

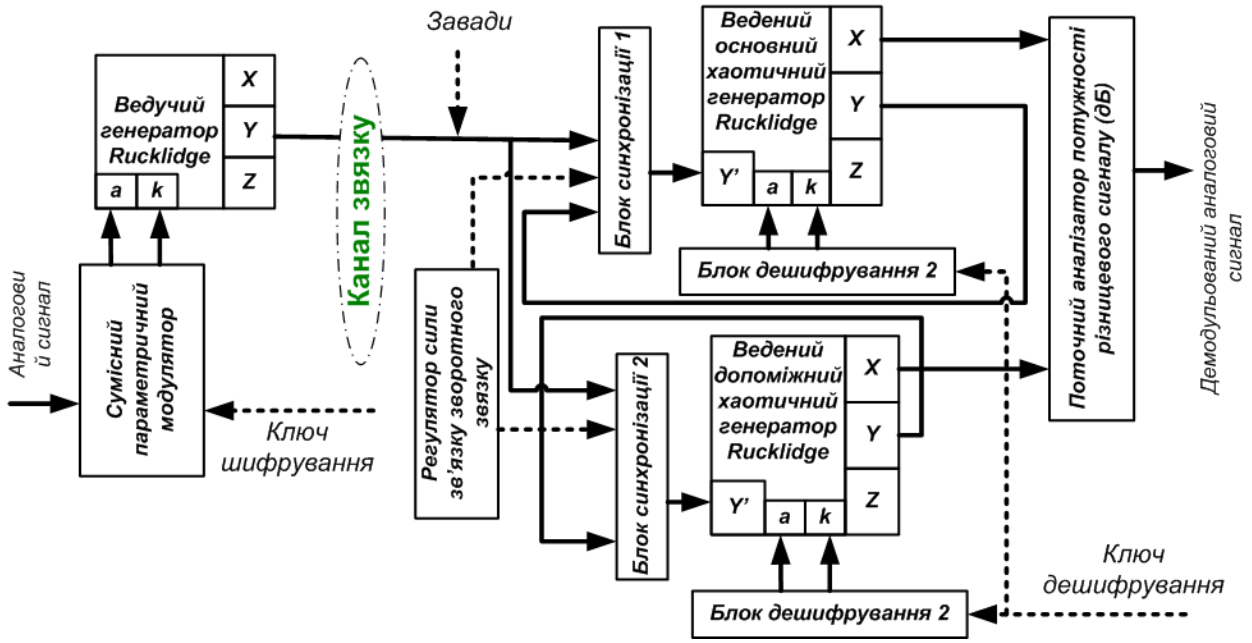


Рисунок 3.9 – Криптографічна система передачі інформації із параметричною модуляцією хаотичної підносівної та детектуванням на базі допоміжного хаотичного генератора

Шумоподібні завади, що діють в каналі зв’язку одночасно впливають на спроби узагальненої синхронізації як в основному, так і в додатковому веденому хаотичному генераторі, що говорить про високу потенційну стійкість до флуктуаційних завад такої схеми передачі.

Подібна схема передачі легко може бути перетворена для передавання цифрових повідомлень із попереднім суто цифровим криптографічним захистом, і, таким чином, загальний рівень криптографічної стійкості складатиметься із трьох складових: криптографічний цифровий код, код параметрів хаотичних генераторів та код обраної траєкторії руху по двовимірній характеристиці параметрів в хаотичній системі зв’язку на основі синхронізації допоміжного генератора.

3.2.2 Автоматична підстройка та екстраполяція

Криптографічний захист в схемі (див. рис.3.9) забезпечується за допомогою встановлення певної пари параметрів хаотичного генератора. Для збільшення рівня криптографічного захисту запропоновано в таку схеми ввести зворотний зв'язок на основі екстраполятора.

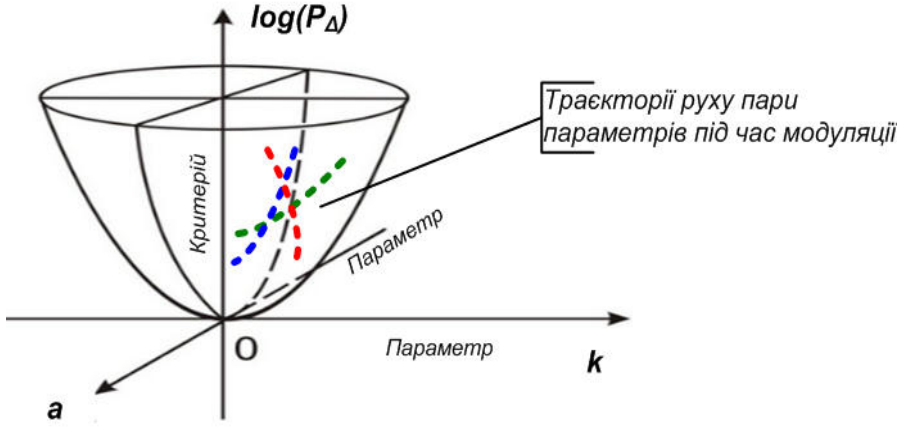


Рисунок 3.10 – Врахування траєкторій руху для збільшення криптографічного захисту

Зворотний зв'язок забезпечує рух значень параметрів не тільки по утворюючій для двовимірної поверхні (див. рис.3.10) але і задає траєкторію такого руху у тривимірному просторі, в результаті кількість незалежних параметрів керування зростає, зростає також складність ключа і загальна криптографічна стійкість без зменшення рівня прихованості дії.

Для забезпечення врахування траєкторії руху слід в схему рис.3.9 ввести зворотний зв'язок через екстраполятор, як показано на рис. 3.10. Саме в екстраполяторі через подання на нього певного ключа шифрування зберігається необхідна траєкторія руху (алгоритм зміни параметрів), що необхідний для правильної роботи системи автоматичного зворотного зв’язку.

Зрозуміло, що такий самий алгоритм введено і в схему сумісного параметричного модулятора на передавальному боці системи зв’язку, що

забезпечує принципову можливість дешифрування аналогових телефонних (або інших) повідомлень. Тобто криптографічний захист забезпечується не тільки власне вибором значень параметрів, але і вибором параметрів для встановлення характеру змін їх початкових значень.

Допоміжний генератор на приймальному боці, в схемі із покращеним криптографічним захистом (рис.3.11) може бути налаштований одноразово на центральні значення параметрів ведучого генератора, а підстроювання параметрів основного веденого генератора відбувається за допомогою екстраполятора значень, що керується поданням необхідних ключів шифрування.

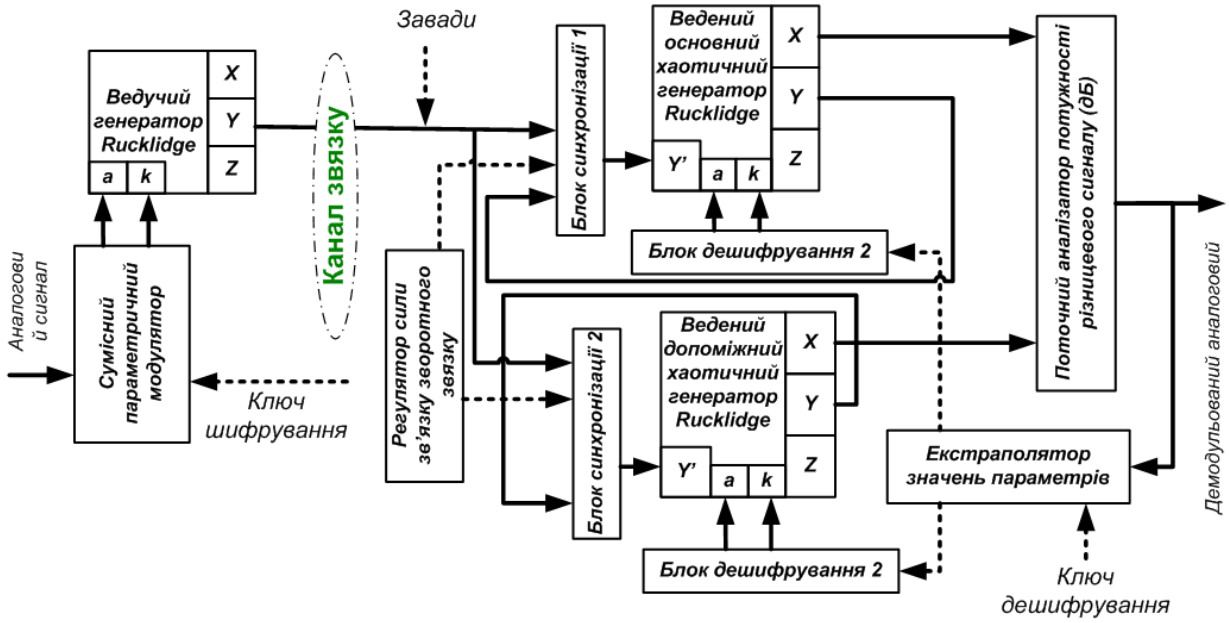


Рисунок 3.11 – Криптографічна система передачі інформації із підвищеним рівнем криптографічного захисту

Таким чином реалізується схема автоматичного підлаштування параметрів хаотичного генератора за критерієм мінімальної різниці різницевої потужності між сигналами основного та допоміжного ведених генераторів детермінованого хаосу. Сам сигнал зворотного зв’язку і є демодульованим аналоговим сигналом.

Слід відмітити, що існують генератори хаотичних сигналів, що мають кількість параметрів для керування більш як 2 і під час їх застосування в зазначеній схемі криптографічного хаотичного захисту можливо сягнути ще більшого рівня захисту через збільшену складність траєкторій руху параметрів в багатовимірному просторі.

3.2.3 Параметрична модуляція хаосу

Модуляція аналоговим інформаційним сигналом призводить до змін в структурі сигналу детермінованого хаосу та його спектрі і це є нормальним явищем. Якщо зміна параметрів не виходить за припустимий діапазон, то структура сигналу залишається шумоподібною, а ширина спектру практично не змінюється. Для дослідження впливу розроблена імітаційна модель (рис.3.12) , що дає можливість якісно порівняти вплив модуляції параметра хаотичного генератора Rucklidge на сигнали детермінованого хаосу, що надходять в канал зв'язку в умовах застосування системи криптографічного захисту.

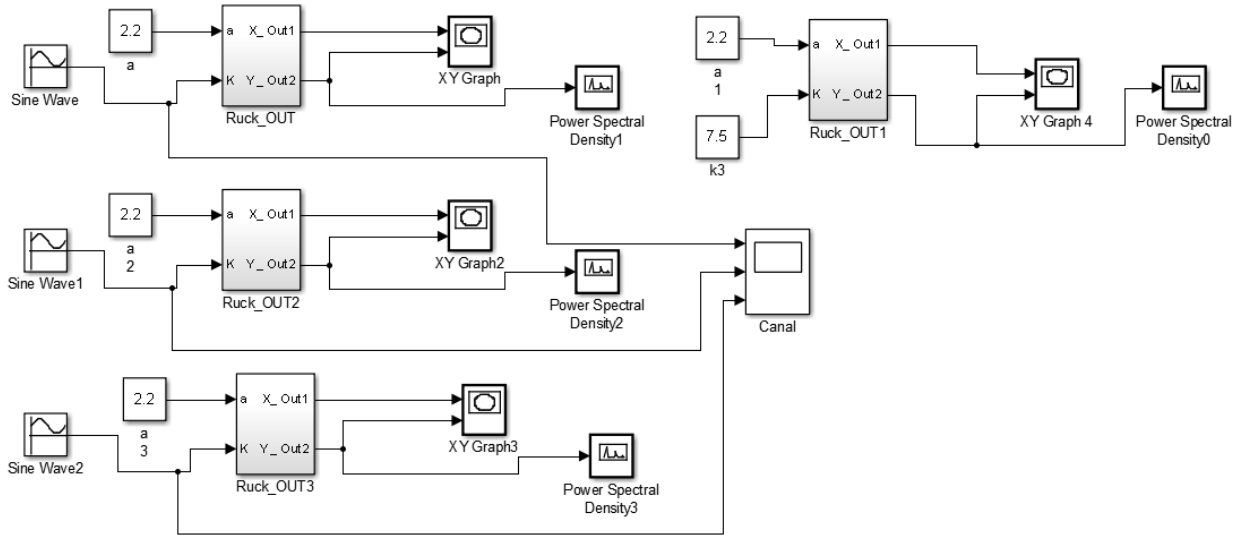


Рисунок 3.12 – Імітаційна модель дослідження впливу модуляції на форму та енергетичний спектр сигналу детермінованого хаосу

Імітаційна модель складається із двох автономних генераторів, один із яких модулюється з боку генератора синусоїдальних коливань, параметри якого встановлені таким чином, щоб їх діапазон значень розташовувався від 7 до 8, із середнім значенням 7,5 і амплітудою 0,5., що відповідає діапазону зміни параметра «*k*» хаотичного генератора, побудованого за схемою Rucklidge. Частота генератора синусоїдальних коливань обрана на порядок меншою за характерні частотні зміни в сигналі детермінованого хаосу (рис.3.13).

За результатами імітаційного моделювання форми та фазової діаграми можливо зробити такі висновки:

1) Структура форми сигналу детермінованого хаосу під час модуляції також залишається непередбачуваною як і без модуляції та є типовою для хаотичних коливань типу «спалахи».

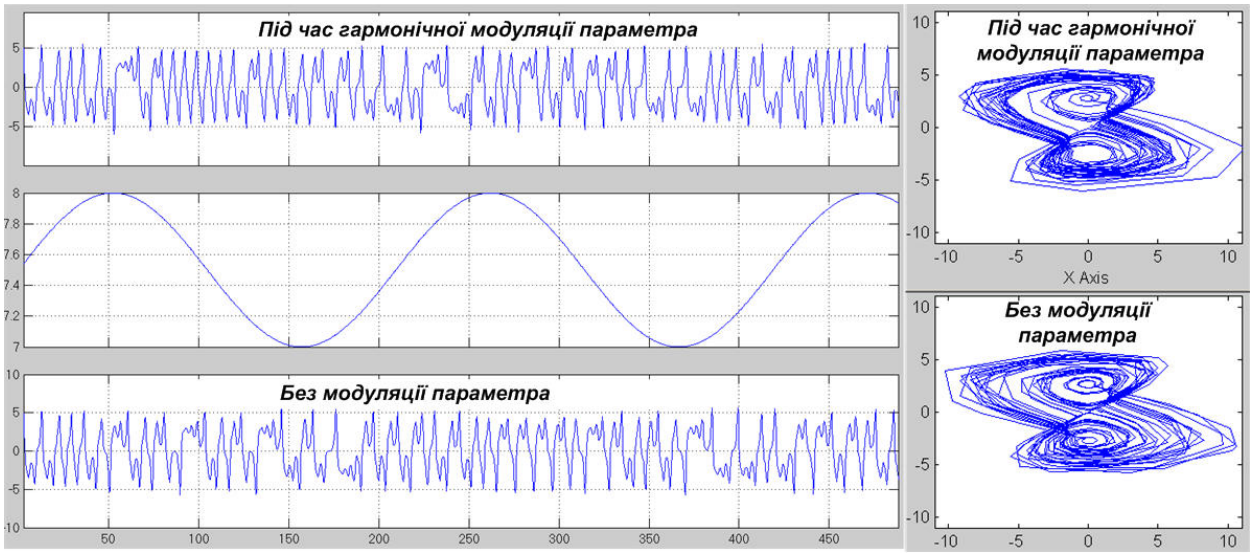


Рисунок 3.13 – Результати імітаційного моделювання впливу модуляції параметра генератора Rucklidge на форму сигналу (ліворуч) та фазову діаграму (праворуч)

2) Форма фазового портрету у вигляді подвійного завитка також залишається незмінною (досліджувалось за фазовими змінними X та

Y, що застосовуються в телекомунікаційній аналоговій системі із криптографічним захистом).

3) Апертура атрактора за фазовим портретом під час параметричної модуляції також залишилась практично незмінною , що говорить про неможливість ідентифікації факту введення інформаційного сигналу за змінною енергетикою хаотичних коливань на опорному виході Y хаотичного генератора Rucklidge.

За результатами імітаційного моделювання спектрів (рис.3.14) під час варіації частоти гармонічного сигналу, що модулює, можливо надати такі зауваження:

1) Структура спектру сигналу детермінованого хаосу із урахуванням модуляції різними частотами залишається незмінною в широкому розумінні.
2) Ширина спектру модульованого сигналу також практично не змінюється для різних значень модулюючих частот, що відрізняються більш як на дві декади.

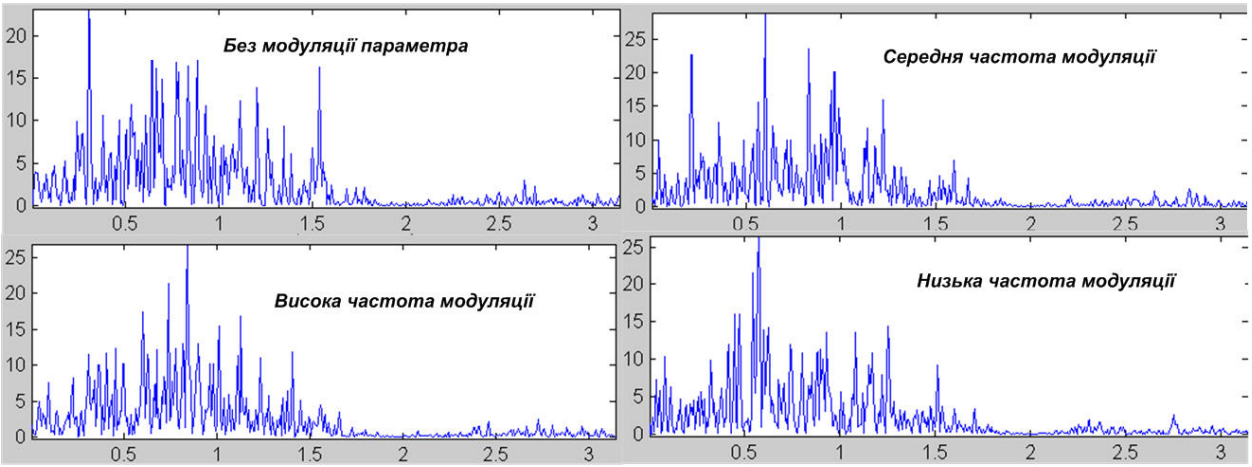


Рисунок 3.14 – Результати імітаційного моделювання впливу модуляції параметра генератора Rucklidge на спектр сигналу для різних частот модуляції

Відповідно проведеним дослідженням можливо зробити висновок про забезпечення високого ступеня прихованості дії через використання модуляції керуючого параметра генератора Rucklidge як за структурою сигналу так і за структурою і шириною спектру.

3.2.4 Сила зв’язку між генераторами

Синхронізацію між ведучим хаотичним генератором та веденими основним та допоміжним хаотичним генераторами забезпечує блок синхронізації (див. додаток Б), що об’єднує сигнали веденого і сигнал зворотного зв’язку хаотичних ведених генераторів із декомпозицією (див. додаток Б).

Завдяки блоку односпрямованої хаотичної синхронізації утворюється складна нелінійна динамічна хаотична система що включає передавальну та приймальну частини. Завдяки зворотному зв’язку ведені генератори мають можливість еволюціонувати за встановленими для них параметрами. Зазвичай для схеми передачі із допоміжним генератором застосовується «сильний» зв'язок, де більш як 90% складає сигнал веденого генератора.

Сила зв’язку під час хаотичної синхронізації носить суто нелінійний характер та залежить від багатьох факторів, в першу чергу від значень параметрів генераторів хаосу, що в нашому випадку і забезпечують криптографічну стійкість.

Дослідження впливу сили взаємодії проводилось на базі імітаційної моделі телекомунікаційної системи прихованого зв’язку (рис.3.15) із аналоговим модулюючим сигналом гармонічної форми. Для спрощення та пришвидшення розрахунків модуляція здійснювалась за одним параметром.

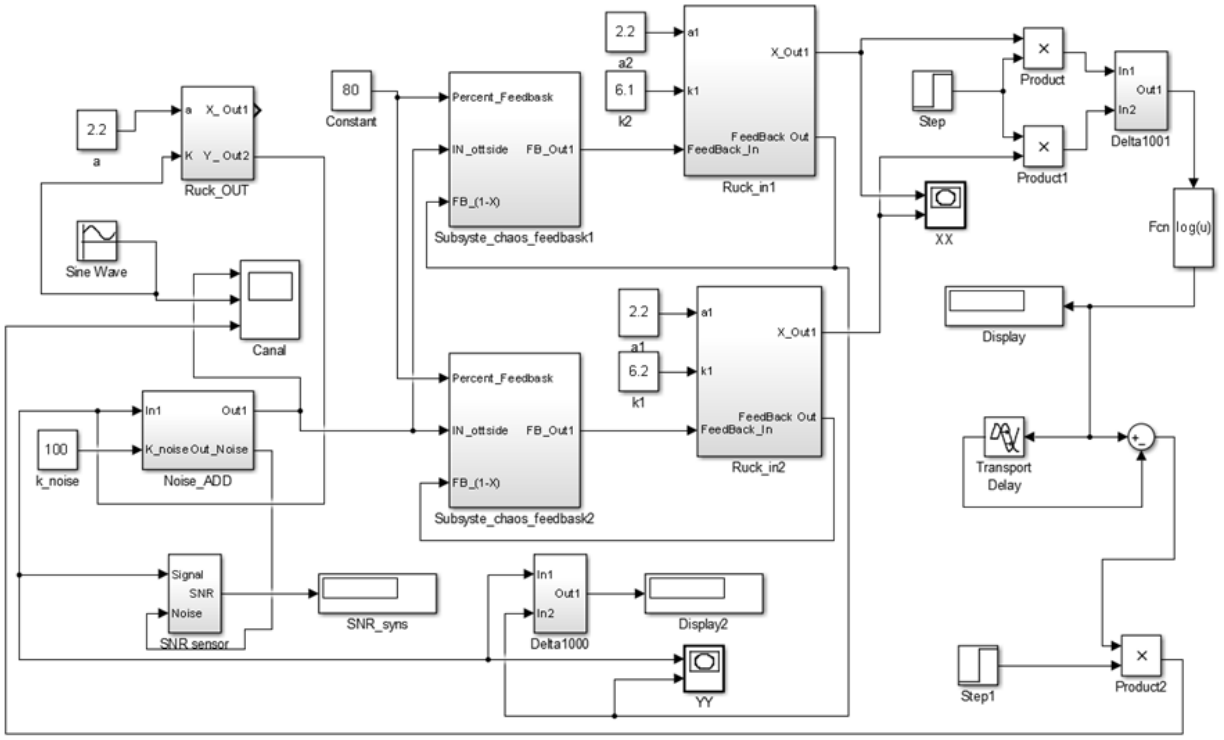


Рисунок 3.15 – Імітаційна модель дослідження впливу сили взаємодії на хаотичну синхронізацію в схемі із допоміжним хаотичним генератором

Модель (рис.3.15) має у складі основні елементи: хаотичні генератори, схеми синхронізації, та схему обчислення значень різницевої потужності за визначену кількість кроків моделювання, а також і додаткові блоки та субмодулі: обчислювачі SNR, плотери фазових діаграм, блоки встановлення часових інтервалів та затримок. Тобто модель має високий ступінь універсалізму та дозволяє застосовувати різні типи хаотичних генераторів та різні підходи критеріїв оцінки сигналів детермінованого хаосу в кінцевому рахунку.

За результатами моделювання (рис.3.16) робимо такі висновки:

1) Характер графіку залежності відповідає суто нелінійним властивостям сукупної динамічної системи із використанням хаотичних генераторів.
2) В діапазоні значень «середніх» рівнів зв’язку між ведучим та веденим генераторами 70-80% характер залежності практично лінійний, що говорить про правильність застосованого критерію.

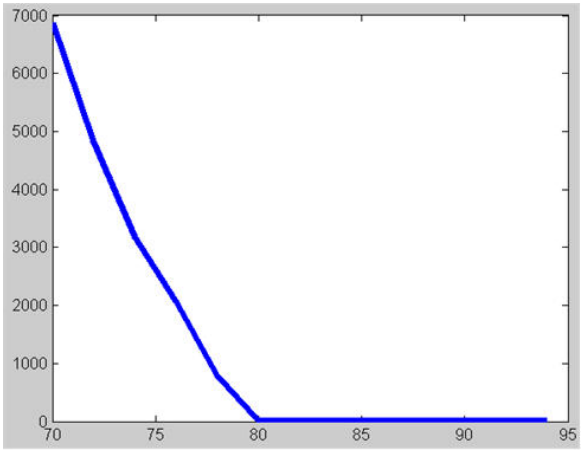


Рисунок 3.16 – Результати досліджень впливу відсоткового рівня синхронізації на значення ї сили зворотного зв’язку для параметрів імітаційної моделі *a1=a2=a3=2.2 k1=6.2 k2=6.1 k3=6.15 n=300*

3) В діапазоні значень більше 80% спостерігається явище захвату сигналу детермінованого хаосу веденого генератора – ведучим, що призводить до падіння рівня різницевої потужності між веденими генераторами практично до нуля (яскрава проява хаотичного синхронного відгуку ведених генераторів).

3.3 Моделювання каналів із криптографічним захистом

3.3.1 Система передачі із хаотичним маскуванням

Системи передачі із хаотичним маскуванням поділяють на системи із розділеними та суміщеним каналом синхронізації та передачі аналогових повідомлень. Більш практична з точки зору система із суміщеним каналом в імітаційній моделі якої (рис.3.17) застосовуються хаотичні генератори Rucklidge із двома параметрами керування та сильним рівнем зв’язку (90%) між веденим та ведучим генераторами.

Параметри ведених генераторів відрізняються на 0,05% для врахування можливості практичного втілення. В моделі каналу також введено керований генератор гаусівського шуму, сигнал якого вводиться в суміщений канал одночасно із інформаційним гармонічним коливанням (аналоговим сигналом повідомлення).

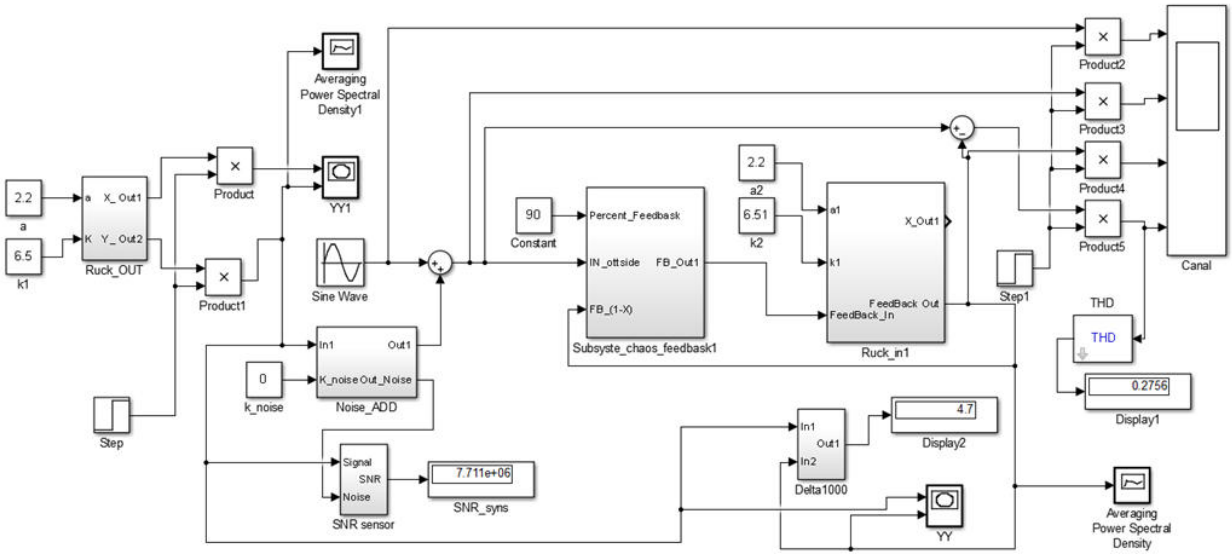


Рисунок 3.17 – Імітаційна модель хаотичного каналу із маскуванням аналогових повідомлень із суміщеним каналом синхронізації-даних

Під час імітаційного моделювання проводився аналіз форми сигналів, коефіцієнту гармонік після демодуляції та можливості підтримання хаотичних режимів для забезпечення одночасної прихованості дії.

Співвідношення між рівнями аналогового гармонічного сигналу та рівнями розмаху хаотичного сигналу близько -40дБ. За таких умов виділення модулюючого сигналу із адитивної суміші із хаотичною піднесівної у високій ступені утруднено (рис.3.20).

Працездатність системи та умови передачі сигналів оцінювались через визначення коефіцієнту гармонік(THD) вбудованими засобами Simulink. Через велику кількість встановлюваних параметрів аналіз проводився точковим випадковим методом встановлення значень.

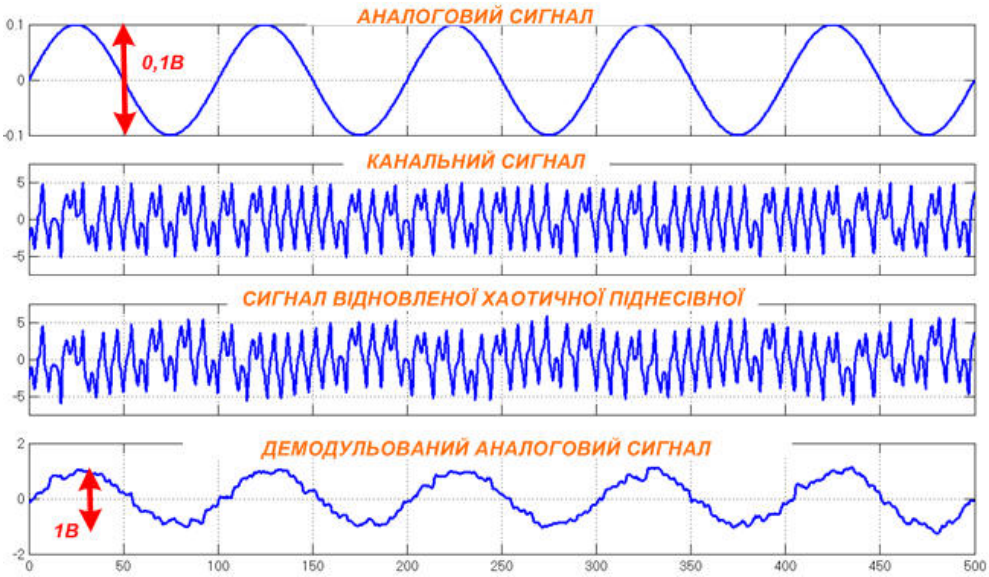


Рисунок 3.20 – Діаграми роботи системи зв'язку із хаотичним маскуванням

В результаті аналізу часових залежності можливо знобити наступні важливі висновки:

1) Працездатність системи передачі сигналів на рівні до 10% спотворень гармонічного сигналу забезпечувалась за умови відношення SNR в каналі відносно гаусівських шумів на рівні -70дБ, що говорить про високу чутливість системи до впливу стороніх завад та підтверджує необхідність застосування якісних каналів для передачі аналогових повідомлень.
2) Захват синхронізації та детектування аналогового повідомлення можливий за умови розузгодження параметрів веденого та ведучого генератора на рівні 5%, що підтверджує попередні оцінки щодо варіантів ключів шифрування хаотичними методами обробки.
3) Під час досліджень середній сигналу на виході веденого генератора змінюється за законом модулюючого сигналу, що є характерною проявою ефекту нелінійного синхронного детектування в системах із хаотичним маскуванням.
4) Під час передачі аналогового сигналу по ідеальному каналу виявлено ефект підсилення амплітуди (рис.3.21) модулюючого сигналу на виході приймача, що обумовлено нелінійними

властивостями обробки (потребує подальшого дослідження) і може бути використано для компенсації втрат у реальних каналах за умови мінімального рівня шумів.

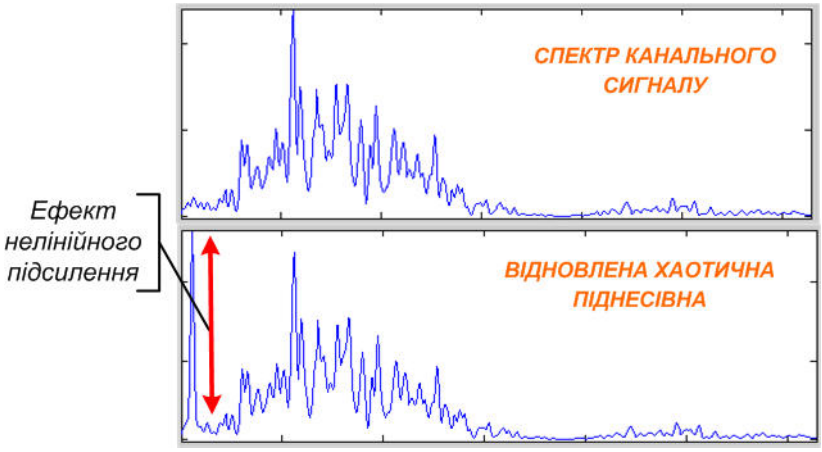


Рисунок 3.21 – Енергетичні спектри канального сигналу і сигналу на виході веденого хаотичного генератора

Дослідження спектрів канального сигналу та спектрів сигналу однойменної фазової змінної на виході веденого синхронізованого хаотичного генератора також підтверджує винайдений ефект нелінійного підсилення модулюючого сигналу у хаотичних генераторах, що взаємодіють.

Проведені дослідження підтверджують працездатність схеми, але для використання в діючих телефонних каналах використання схеми є проблематичним через високу чутливість до рівня зовнішніх завад.

3.3.2 Канал зв’язку із параметричною модуляцією

Імітаційна модель каналу із модуляцією біфуркаційних параметрів хаотичного генератора Rucklidge (рис.3.22) на відміну від моделі хаотичного маскування (рис. 3.19) має у складі два ведених генератора, за результатами поточної синхронізації яких визначається детектування аналогового повідомлення.

Принцип роботи системи полягає у зміні параметрів ведучого генератора таким чином, щоб ведені генератори в більшій або меншій мірі формували хаотичний синхронний відгук відповідно змінам параметра веденого генератора. Для пришвидшення моделювання застосовується зміна лише одного параметру генератора Rucklidge за гармонічним аналоговим модулюючим коливанням.

Для детектування рівня синхронних відгуків ведених генераторів запропоновано застосовувати наступний критерій, що ґрунтується на визначенні поточних дійсних значень хаотичних сигналів на виходах відмінних фазових змінних щодо сигналу в каналі передачі:

$$K_{\Delta} = \frac{\sqrt{\frac{1}{(T_2 - T_1)} \int_{T_1}^{T_2} \left(\zeta_1(t) - \zeta_2(t)\right)^2 dt}}{\sqrt{\frac{1}{(T_2 - T_1)} \int_{T_1}^{T_2} \left(\zeta_1(t)\right)^2 dt} + \sqrt{\frac{1}{(T_2 - T_1)} \int_{T_1}^{T_2} \left(\zeta_2(t)\right)^2 dt}} = \frac{RMS\left[\zeta_1(t) - \zeta_2(t)\right]}{RMS\left[\zeta_1(t)\right] + RMS\left[\zeta_1(t)\right]}, \quad (3.1)$$

де $(T_2 - T_1)$ - інтервал часу для поточного аналізу значення;

$\zeta_1(t), \zeta_2(t)$ - сигнали на виході однойменних фазових змінних ведених хаотичних генераторів.

Для детектування можливо застосування і інших критерії, але даний критерій, під час пробних досліджень забезпечує найменший рівень спотворень результату детектування інформаційного повідомлення.

На першому етапі проводилась перевірка працездатності схеми та аналіз різних критеріїв детектування аналогових повідомлень. В результаті проведених імітаційних моделювань зроблено наступні висновки:

1) Для виділення аналогового сигналу слід застосовувати «сильний зв'язок» між хаотичними генераторами на приймальному та передавальному боці (більше 80%). Використання слабкого зв’язку

спряжене із різким збільшенням рівня спотворень результату демодуляції.

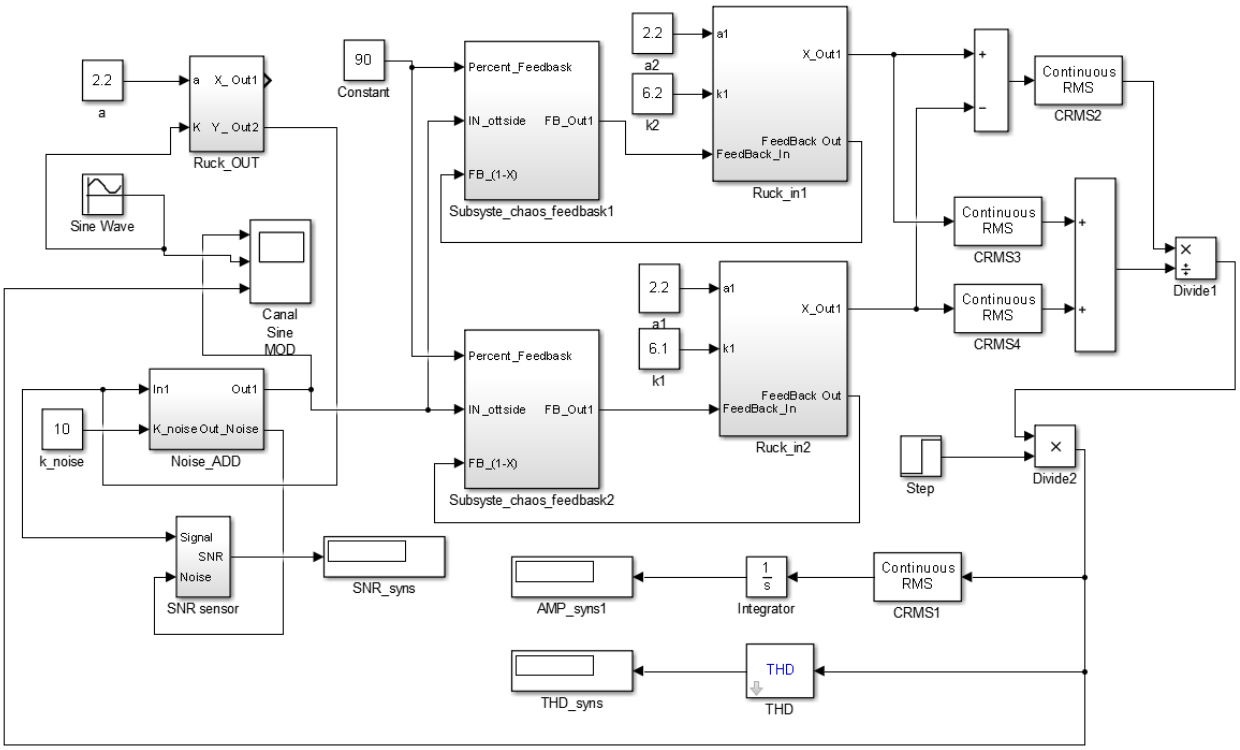


Рисунок 3.22 Імітаційна модель Matlab\Simulink хаотичної системи зв’язку із однопараметричною модуляцією та синхронним відгуком ведених генераторів

2) Більш якісні результати демодуляції за критерієм мінімуму коефіцієнту гармонік отримано у випадку розташування налаштувань ведених та ведучого генератора по обидва боки відносно оптимальних значень на залежності похибка-розузгодження (див. рис.3.8).
3) Підтверджено правильність застосування критерію (3.1) для схеми детектування аналогового повідомлення із мінімальними похибками.
4) Виявлена часова затримка реакції схеми детектування на дію модульованого сигналу.

5) Виявлено невеликий рівень субгармонік у складі де модульованого сигналу із частотою на порядок меншою за частоту модулюючого гармонічного коливання.

На другому етапі досліджень аналізувалась форма сигналу та амплітудно-частотна характеристика системи хаотичного детектування аналогового повідомлення в цілому (рис.3.22).

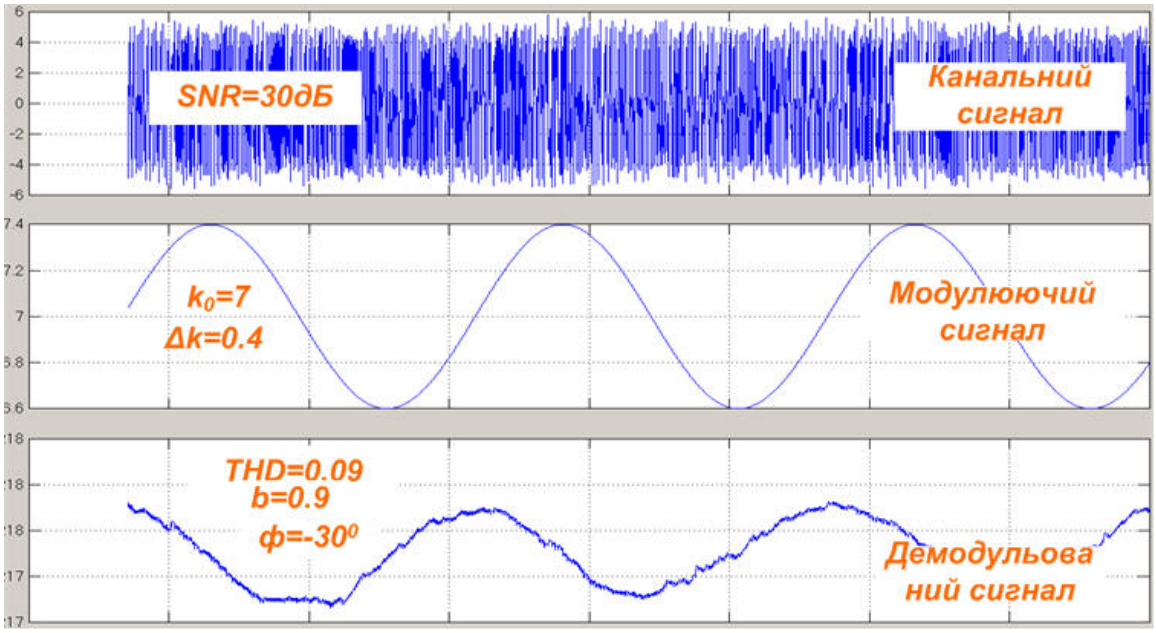


Рисунок 3.23 Діаграми хаотичної демодуляції в хаотичній системі захисту аналогової інформації

Другий етап досліджень показав наступні результати:

1) Працездатність системи на рівні THD менше 10% зберігається за умови відношення сигнал – завада в каналі більше 30%, що дає можливість застосувати дану схему для криптографічного захисту телефонних каналів.
2) Фазовий зсув між модулюючим сигналом на передавальному боці та сигналом після схеми хаотичного детектування складає близько 30..40 градусів із випередженням останнього, що говорить про необхідність більш ретельного дослідження фазо-частотної

характеристики такого хаотичного каналу передачі аналогових повідомлень.

3) Амплітудно - частотна характеристика каналу передачі в діапазоні дві декади залишалась рівномірною із відхиленнями менше 1%.

Третій етап досліджень імітаційної моделі рис.3.22 присвячений аналізу характеристик каналу із приведенням їх до потреб передачі тональних сигналів і телефонних каналів зв'язку (рис.3.24).

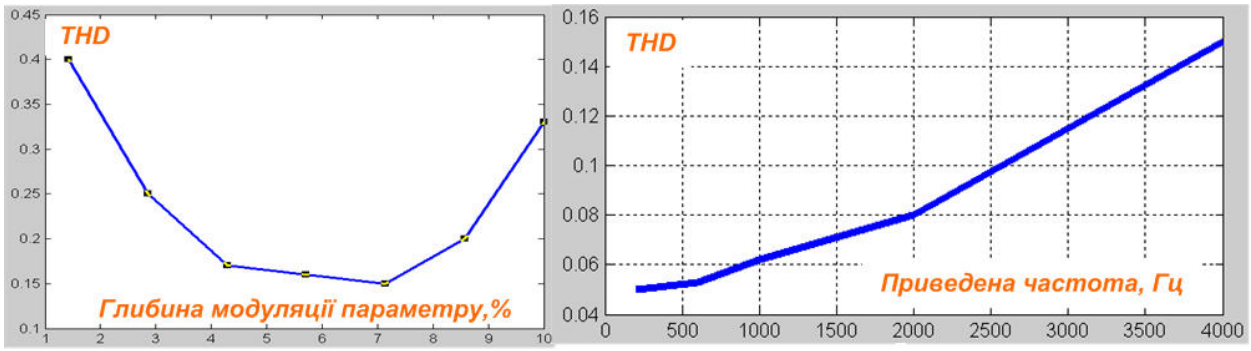


Рисунок 3.24 Діаграми хаотичної демодуляції в хаотичній системі захисту аналогової інформації

Під час досліджень третього етапу критерієм виступав коефіцієнт гармонік THD як критерій якості передачі сигналів. За результатами моделювання зроблено такі висновки:

1) Підтверджено оцінювання кількості ключів шифрування, що проведено вище із загального аналізу застосування хаотичних методів під час обробки сигналів із метою захисту інформації.
2) Встановлено, що глибина модуляції аналоговим сигналом керуючого параметру має оптимум приблизно у 6-7% (див.рис.3.24), відхилення від якого призводить до збільшення спотворень під час демодуляції аналогових повідомлень.
3) Спотворення демодульованого аналогового сигналу за умови встановлених параметрів та режимів мають досить високий рівень (10%) та наближено лінійно зростають із зростанням частоти

інформаційного повідомлення. Такий рівень спотворень призводить до суттєвого але не критичного зменшення якості телефонного сигналу.

4) Для забезпечення низького рівня спотворень для одного періоду аналогового синусоїдального сигналу необхідно використати до декількох десятків циклів хаотичного сигналу, що обґрунтовується статистичним характером обробки в нелінійному модуляторі на базі ведених генераторів.

Таким чином можливість високого рівня криптографічного захисту за умови середнього рівня спотворень аналогового телефонного повідомлення підтверджена імітаційним моделюванням.

За комплексними результатами проведених досліджень рекомендовано застосовувати запропоновану хаотичну схему захисту від несанкціонованого доступу для захисту аналогових телефонних ліній «останньої милі», що мають достатню ширину спектру для передачі широкосмугового хаотичного сигналу із прихованим аналоговим повідомленням.

ВИСНОВКИ

1. Проведено аналіз необхідності та доцільності застосування алгоритмів шифрування для забезпечення захисту інформації телекомунікаційних систем. Встановлено , що з точки зору криптоаналізу доцільне застосування новітніх програмно-апаратних засобів криптографії і одними із найбільш перспективних є системи передачі даних на базі хаотичних методів обробки сигналів детермінованого хаосу.

2. В рамках поставленого завдання застосування криптографії для аналогових сигналів тональних частот, що поширюються в телефонній лінії зв'язку, розглянуто основні принципи, параметри та характеристики телефонних каналів, що мають бути дотримано під час застосування хаотичних методів обробки із метою криптографічного захисту інформації.

3. На основі розгляду базових принципів побудови криптографічних алгоритмів показано процедурну еквівалентність криптографії і нелінійних динамічних систем із хаотичною поведінкою. Проведено паралелі між основними поняттями перемішування та розсіювання під час розробки цифрових алгоритмів шифрування та поведінкою динамічних змінних хаотичних систем у фазовому просторі. На основі паралелей зроблено висновок про доцільність використання хаотичної динаміки в криптологічних алгоритмах захисту аналогових повідомлень.

4. Розглянуто основні принципи побудови хаотичних систем телекомунікацій: хаотичну модуляцію, хаотичну синхронізацію, хаотичне детектування, тощо. Визначено параметри, що їх характеризують та їх вплив на забезпечення криптологічного захисту аналогових повідомлень. Проведено оцінювання кількості ключів під час застосування різних схем та алгоритмів обробки сигналів під час передачі аналогових телефонних повідомлень.

5. Запропоновано методи та методики застосування хаотичних принципів обробки в телекомунікаційних системах для забезпечення одночасної прихованості дії та криптографічного захисту в реальних телекомунікаційних каналах із завадами та спотвореннями.

6. Запропоновано використання ряду лінійних залежностей рівня синхронізації від різних параметрів телекомунікаційної системи, що застосовує в якості піднесівних коливань сигнали детермінованого хаосу, в якості модуляційних характеристик для передачі аналогових повідомлень в системах захисту інформації від несанкціонованого доступу.

7. Показано, що найвищий рівень захисту для реальних телефонних ліній останньої милі реалізується за допомогою багатопараметричної модуляції хаотичних генераторів високої розмірності, та детектування модулюючих сигналів за допомогою хаотичних синхронних відгуків ведених хаотичних генераторів із декомпозицією та екстраполяцією модуляційних характеристик.

8. Запропоновано критерій визначення ступеню розузгодження ведених генераторів приймального боку телекомунікаційної системи із ведучим генератором під час динамічної зміни параметрів біфуркації, що забезпечує детектуваня аналогових сигналів із мінімальним рівнем спотворень.

9. Проведено імітаційне моделювання окремих складових хаотичної системи, що підтвердило високий рівень прихованості дії та можливість їх застосування для реальних телефонних ліній передачі на основі дротяних кабелів. Також проведено імітаційне моделювання працездатності хаотичного каналу передачі даних на основі хаотичного маскування та параметричної модуляції. Визначено, що за умови коректного встановлення параметрів криптографічного захисту можливо досягти рівня спотворень передачі аналогового повідомлення менше 10%. Під час некоректного встановлення зловмисником параметрів шифрування рівень спотворень різко зростає, що призводить до фактичного блокування несанкціонованого доступу до переданого повідомлення.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Б.С. Гольдштейн, Н.А. Соколов, Г.Г. Яновский. Сети связи: Учебник для ВУЗов. СПб.: БХВ-Петербург, 20104. – 400 с., илл.

2. Конахович Г.Ф. Системи радіозв’язку. Навчальний посібник. – К.: НАУ, 2004 – 311с.

3. Конахович Г.Ф. Експлуатація телекомунікаційних систем / Г.Ф. Конахович, В.М. Чуприн, О.П. Ткаліч, І.О. Мачалін //Підручник – К.:НАУ, 2014 – 800 с.

4. Конахович Г.Ф. Захист інформації в телекомунікаційних системах /Г.Ф. Конахович, В.П. Климчук, С.М. Паук, В.Г. Потапов, В.М. Чуприн, О.О. Горбунов //Навчальний посібник.–К.: НАУ,2009. – 380с.

5. Телекомунікаційні мережі фіксованого телефонного зв’язку загального користування ТЕЛЕКОМУНІКАЦІЙНІ ПОСЛУГИ Показники якості. Методи випробування СОУ 64.2 – 00017584 – 002:2009.

6. Конахович Г.Ф. Мережі транспортування пакетних даних/ Г.Ф. Конахович, В.М. Чуприн //Навчальний посібник. – К.:НАУ, 2006 – 280 с.

7. Гусєв О.Ю. Теорія електричного зв’язку /О.Ю.Гусєв, Г.Ф.Конахович, В.І.Корнієнко, Г.В.Кузнецов, О.Ю.Пузиренко //Навчальний посібник.— Львів: Магнолія 2006, 2010. — 331 с.

8. Кузьмин И.В. Основы теории информации и кодирования. – Минск: Вышэйш. шк., 1986.

9. Хемминг Р.В. Теория информации и теория кодирования. - М.: Радио и связь, 1983.

10.Конахович Г. Ф., Пузиренко О.Ю. Комп’ютерна стеганографія. Теорія і практика. —К.: “МК-Пресс”,2006. — 288с.,іл.

11.Сапожков М.А., Михайлов В.Г. Вокодерная связь. –М.: Радио и связь, 1983.

12.Шелухин О.И., Лукьянцев Н.Ф. Цифровая обработка и передача речи. М.: Радио и связь, 2000.

13.Federal Standard 1016. Telecommunications: Analog to Digital Conversion of Radio Voice by 4,800 bit/second Code Excited Linear Prediction (CELP). February 14, 1991.

14. Шульгин В.И. Основы теории передачи информации. – Харьков «ХАИ», 2003.

15. ISO/IEC JTC1/SC29/WG11 NO803, MPEG, International Standard IS 13818-3 Information Technology – Generic Coding of Moving Pictures and Associated Audio: Audio, 11th November 1994.

16.Катунин, Г. П. Телекоммуникационные системы и сети. Учебное пособие для ВУЗов Том 2 / . Г. П. Катунин, Г. В. Мамчев, В. Н. Попантонопуло, В. П. Шувалов − М. Горячая линия – Телеком, 2004.

17.Венбо Мао. Современная криптография. Теория и практика. М: Вильямс, 2005. – 768 с.

18.Бернет С., Пэйн С., Криптография. Официальное руководство RSA Security. Изд. 2-е, стереотипное. – М.: ООО «Бином-Пресс», 2007. – 384 с.: ил.

19.Адаменко М.В. Основы классической криптологии: секреты шифров и кодов. – М.: ДМК Пресс, 2012. – 256 с.

20.Рябко Б.Я., Фионов А.Н. Криптографические методы защиты информации. М.: Горячая линия – Телеком, 2005. – 229с.

21.Залогин Н.Н., Кислов В.В. Широкополосные хаотические сигналы в радиотехнических и инфор-мационных системах. – М.: Радиотехника, 2006, с. 208.

22.Хармут Х. Ф. Несинусоидальные волны в радиолокации и радиосвязи: Пер. с англ. – М.: Радио и связь, 1985 г., -243с.

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

24.Дмитриев А.С. Динамический хаос: новые носители информации для систем связи / А.С. Дмитриев, А.И. Панас. – М. : Издательство Физико–математической литературы. – 2002. – 252 с.

25.Digital Communications Using Chaos and Nonlinear Dynamics / [Editors: Larson L.E., Liu J. – M., Tsimring L.S. – New York : Springer. – 2006. – 382 p.

26.Політанський Л. Система передачі інформації з використанням синхронного хаотичного відгуку / Л. Політанський, М. Кушнір, С. Галюк // Компютерні науки та інженерія : матеріали III міжн. конф. молодих вчених CSE-2009, 14–16 травня 2009 р. – 2009. – С. 319–320.

27.Політанський Л.Ф. Система передачі даних на основі динамічного хаосу / Л.Ф. Політанський, П.М. Шпатар, О.В. Гресь, Г.В. Косован // Сучасні інформаційні та електронні технології : тези допов. XI міжн. наук.-практ. конф., 24–28 травня 2010 р. / Одеса : Політтехперіодика. – 2010. – Т. 1. – С. 215.

28.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.

29.Короновский А. А. Скрытая передача информации на основе режима обобщенной синхронизации в присуствии шумов / А. А. Короновский, О. И. Москаленко, А.Е.Храмов // ЖТФ. – 2009. – т. 80. - № 4. – с. 1-8.

30.Е.В. Ефремова Генераторы хаотических колебаний радио- и СВЧ диапазонов / Успехи современной радиоэлектроники, №1, с.17-31, 2008.

31.Еліяшів О.М. Дослідження властивостей нелінійного елемента передавача хаотичної системи зв’язку / О.М. Еліяшів, В.Б. Русин, Л.Ф.Політанський, М.Я.Кушнір, Р.Л.Політанський // Радиоэлектроника и информатика. – 2011. – №2 (53). – С. 12 –16.

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

33.Андронов А.А. К математической теории захватывания / А.А. Андронов, А.А. Витт // Журнал прикладной физики. – 1930. – № 7. – С. 3–11.

34.Афраймович В.С. Стохастическая синхронизация колебаний в диссипативных системах / В.С. Афраймович, Н.Н. Веричев, М.И. Рабинович // Изв. вузов. Радиофизика. -1986. – Т. 29. – № 9. – С. 1050–1060.

35.Політанський Л.Ф. Багатокористувальницька система зв'язку з використанням хаотичної частотної модуляції / Л.Ф. Політанський, М.Я. Кушнір, Р.Л. Політанський та ін. // Східно-Європейський журнал передових технологій – 2010. – № 1/5(43). – С. 44-47.

36.Волковский А.Р., Рульков Н.Ф. Синхронный хаотический отклик нелинейной системы передачи информации с хаотической несущей // Письма в ЖТФ 19 (3) 71 (1993)

37.Блехман И.И. Синхронизация динамических систем / И.И. Блехман. – М. : Наука, 1971. – 896 с.

38.Анализ хаотической синхронизации динамических систем с плохо определенной фазой Короновский А.А., Храмов А.Е. Радиотехника и электроника 50 969 (2005)

39.Галюк С. Д. Дослідження узагальненої синхронізації модифікованого кільцевого генератора / С. Д. Галюк, М. Я. Кушнір, І. М. Годинюк // Матеріали І Всеукраїнської науково-практичної конференції “Фізико-технологічні проблеми радіотехнічних пристроїв, засобів телекомунікації, нано- та мікроелектроніки”, 13-15 жовтня 2011 р., Чернівці, Україна. – С. 97-100.

40.Вовчук Д.А. Адаптація методу хаотичного маскування для цифрового передавання інформації / Д.А. Вовчук, С.Д. Галюк, Л.Ф. Політанський // Східно-Європейський журнал передових технологій.- 2013. – №2/4 (62). - С.50-55.

41.Патент України на корисну модель UA97300U, МПК H04L 9/24 (2006.01) Спосіб прихованого передавання цифрової інформації з використанням хаотичного маскування / Д.А. Вовчук, С.Д. Галюк, Л.Ф. Політанський; Власник Чернівецький національний університет ім. Ю.Федьковича. - №u20140952; заявка 01.09.2014; опубл. 10.03.2015, Бюл. №5

42.О.М. Элияшив, Л.Ф. Политанський Безындуктивные генераторы хаотических колебаний по схеме Чуа / Технология и конструирование в электронной аппаратуре, №2, с. 12-15, 2012.

43.Вовчук Д.А. Моделювання системи передавання цифрової інформації з допомогою хаотичного маскування / Д.А. Вовчук // Технологічний аудит і резерви виробництва.- 2013. – №5/5(13). - С. 55-57.

44.Вовчук Д.А. Моделювання систем передавання цифрової інформації з хаотичною носійною / Д.А. Вовчук // Матеріали 17-го Міжнародного молодіжного форуму «Радиоэлектроника и молодежь в XXI веке». – Харків, 2013. – Т.7. – С. 106-107.

45.Голевич О. Б. Впорядкування ансамблів хаотичних сигналів та способи їх використання в надширокосмугових телекомунікаційних системах / О. Б. Голевич, О. С. Пивовар, І. В. Троцишин // Цифрові технології : зб. наук. пр. / Одес. нац. акад. зв'язку ім. О. С. Попова. – Одеса, 2015. – Вип. 17.– С. 181-191.

ДОДАТОК А
НЕЛІНІЙНІ ДИНАМІЧНІ СИСТЕМИ ТА ЇХ ЗАСТОСУВАННЯ

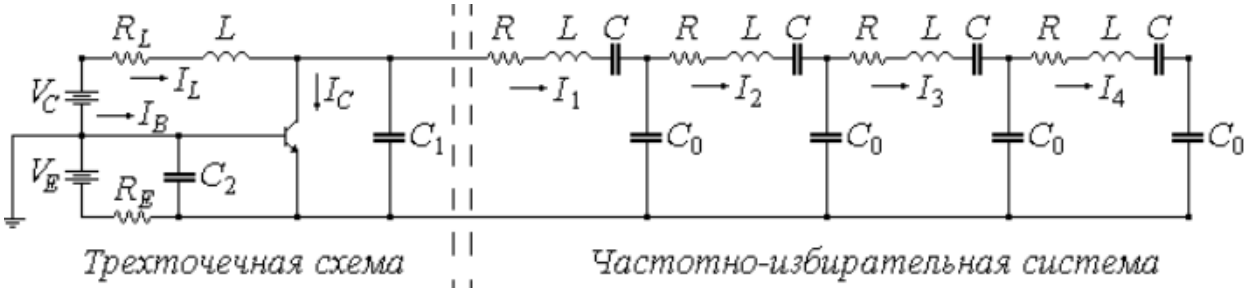


Рисунок А-1 Схема хаотичного генератора із багатьма ступенями свободи на базі ємнісної триточки

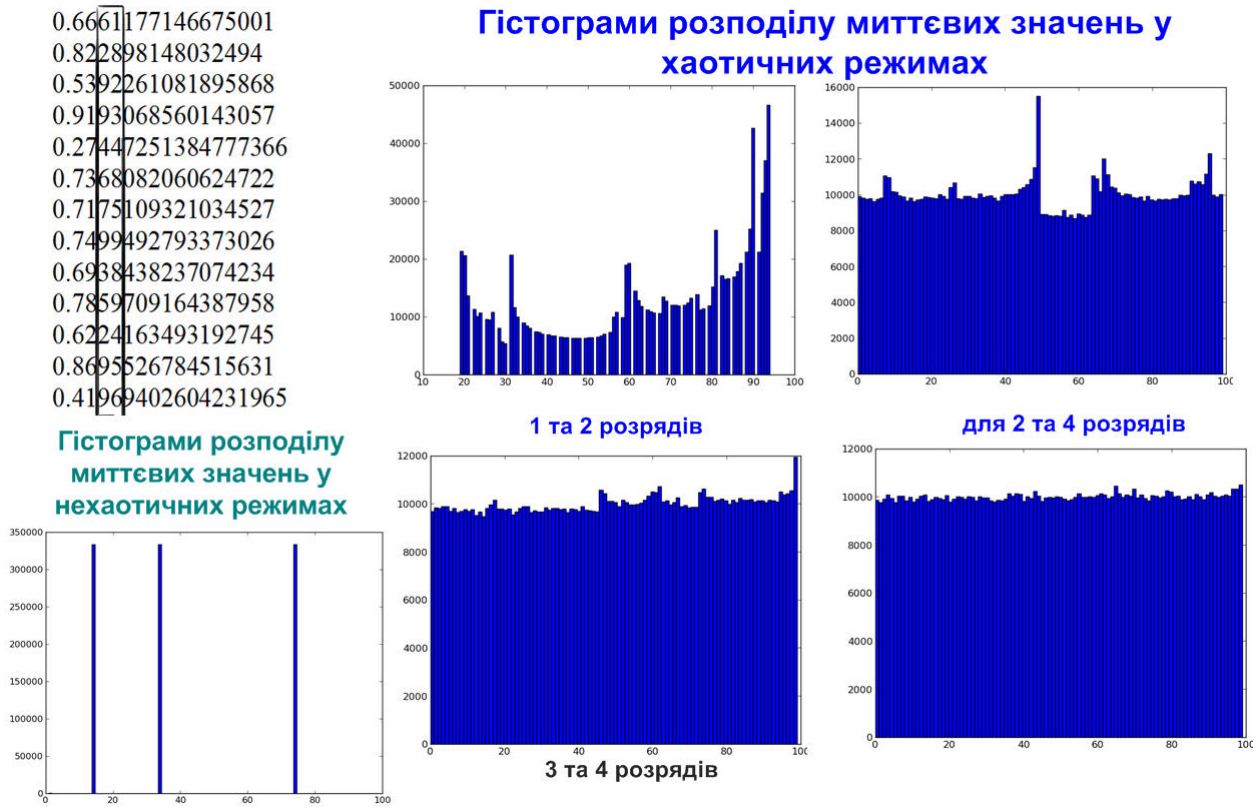


Рисунок А.2 – Утворення псевдовипадкової послідовності забезпечення криптостійкості відбором деяких розрядів логістичного дискретного хаотичного генератора

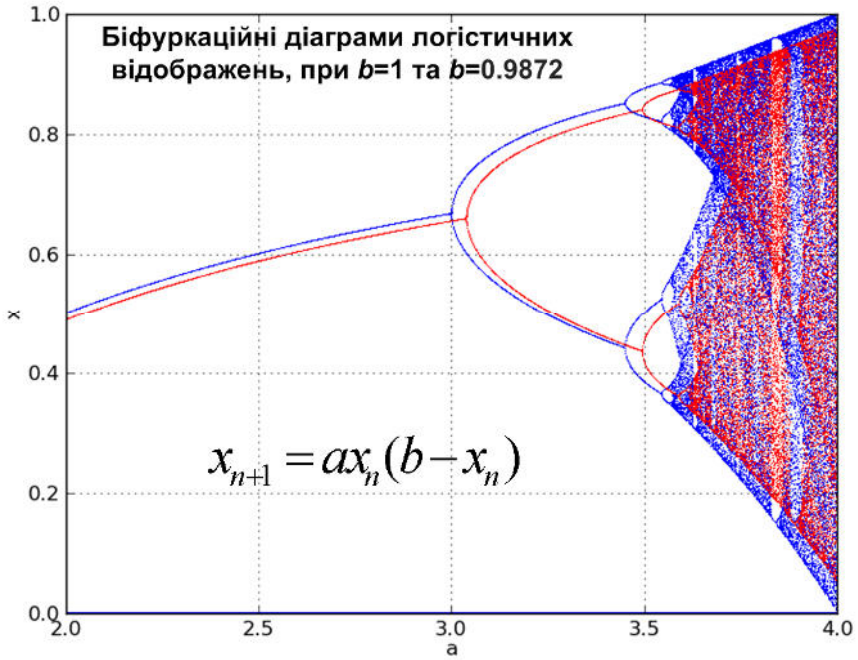


Рисунок А.3 - Суперпозиція біфуркаційних діаграм логістичного генератора з метою усування зон не хаотичності для формування рівномірного розподілу псевдовипадкових криптографічних послідовностей

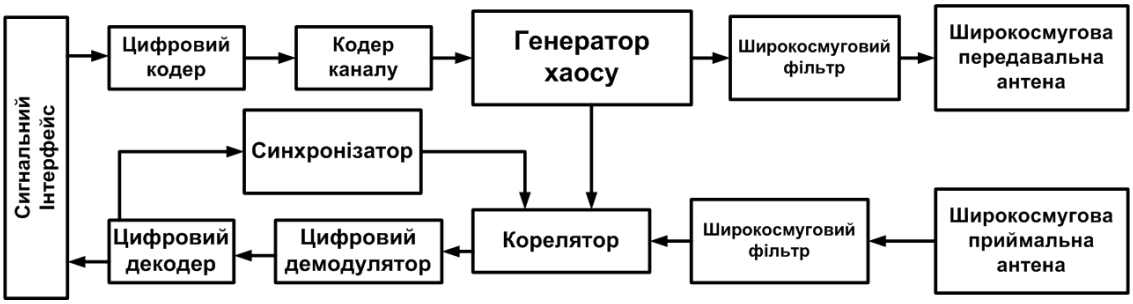


Рисунок А.4 – Система широкосмугової телекомунікації із застосуванням внутрішньої модуляції параметра хаотичного генератора

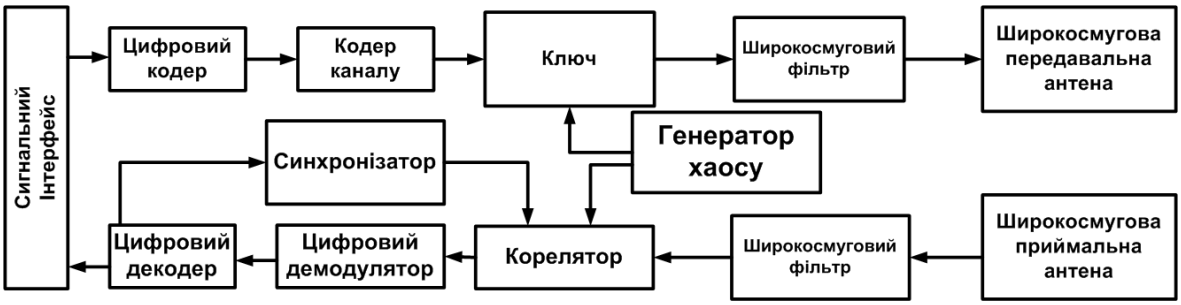


Рисунок А.5 – Прямохаотична імпульсна широкосмугова система зв’язку

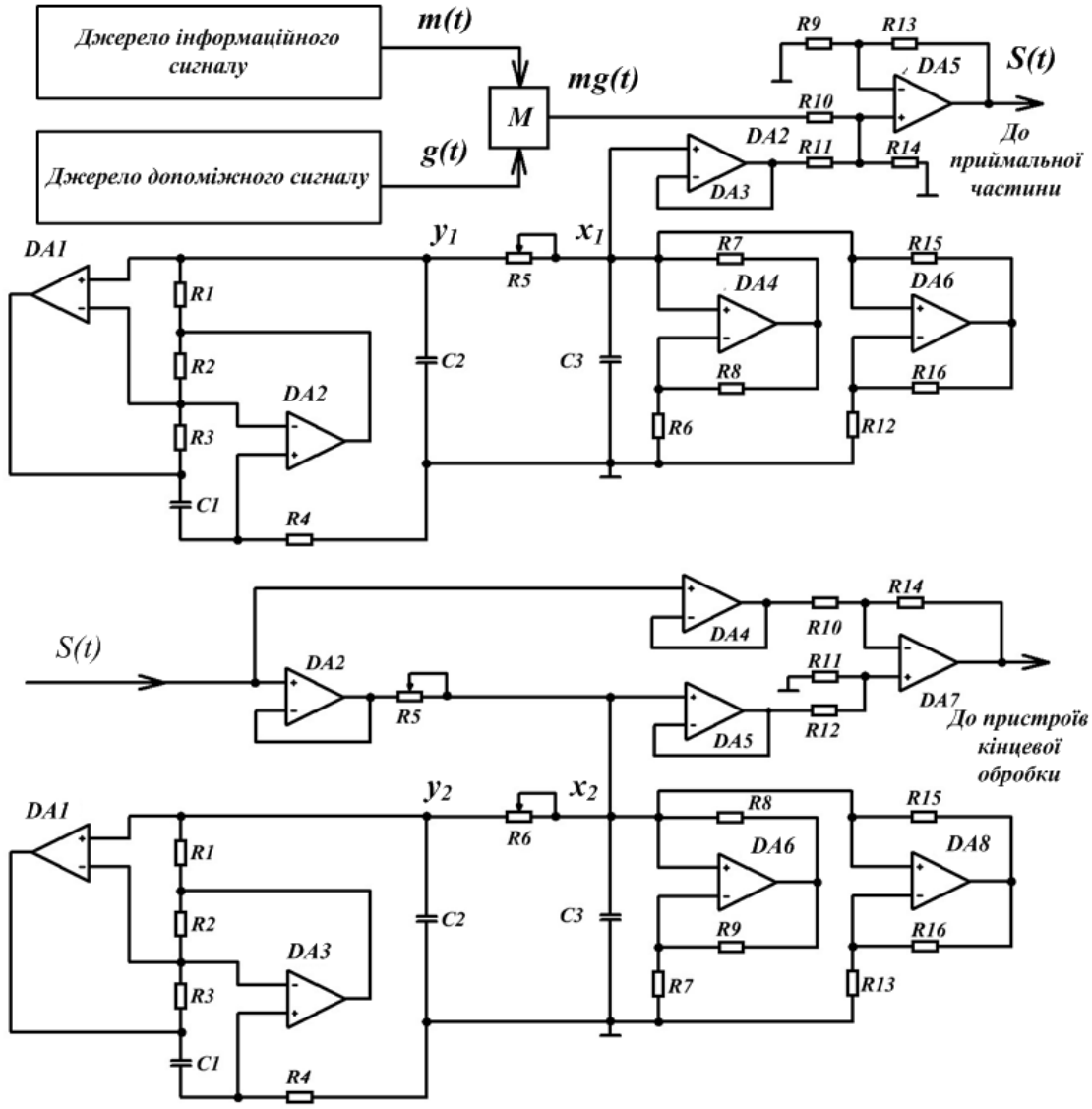


Рисунок А.6 – Схема хаотичної системи зв’язку на базі генератора Чуа із хаотичним маскуванням та застосуванням допоміжного сигналу

ДОДАТОК Б
ІМІТАЦІЙНІ СУБМОДЕЛІ MATLAB/SIMULINK

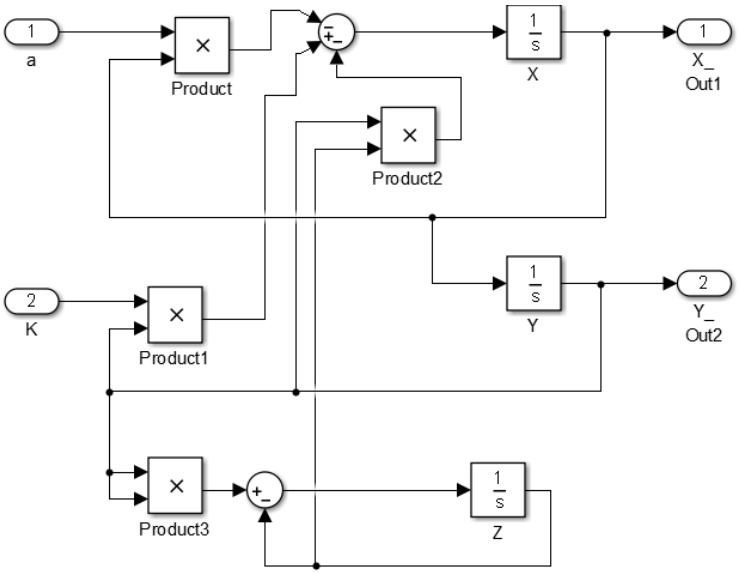


Рисунок Б.1 – Імітаційна субмодель хаотичного генератора Rucklidge із зовнішнім керуванням параметрами

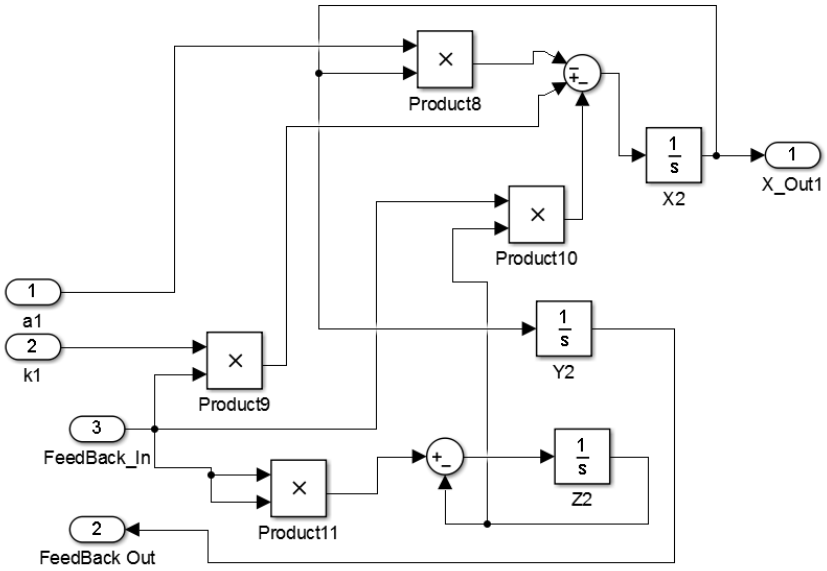


Рисунок Б.2 – Імітаційна субмодель хаотичного генератора Rucklidge із із декомпозицією по змінній «Y» зовнішнім керуванням параметрами

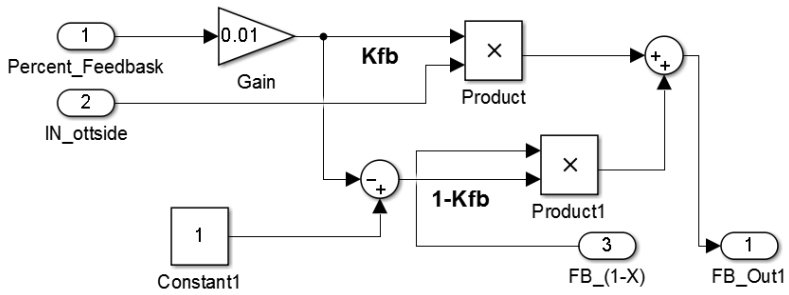


Рисунок Б.3 – Імітаційна субмодель хаотичного пропорційного синхронізатора

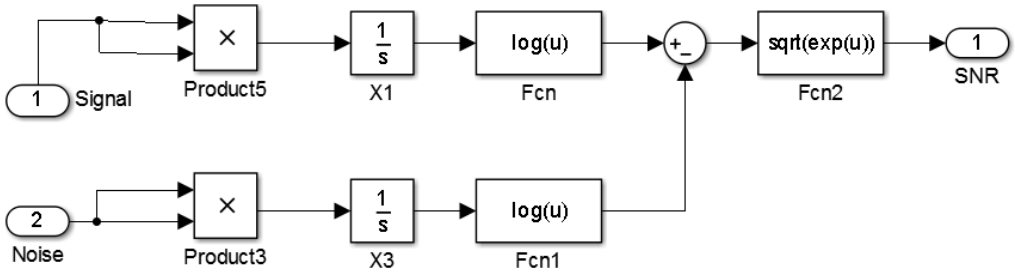


Рисунок Б.4 – Імітаційна субмодуль обчислювача відношення сигнал – завада (SNR – дБ)

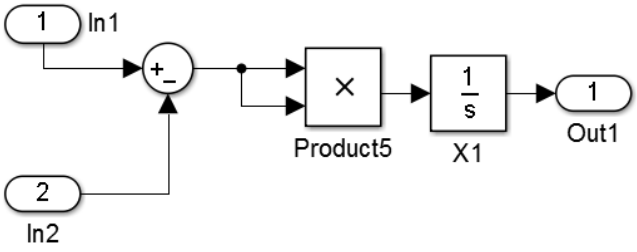


Рисунок Б.5 – Імітаційна субмодуль обчислювача значення різницевої потужності двох сигналів детермінованого хаосу

ДОДАТОК В

ПЛАКАТИ ДЛЯ ДОПОВІДІ

ДИПЛОМНА РОБОТА МАГІСТРА

зі спеціальності 172 "Телекомунікації та радіотехніка"

1

Тема: **Система криптографічного захисту телефонних ліній**

Студент гр. ТРм-20-1: **Гринь Сергій Сергійович**

Керівник: Таранчук Алла Анатоліївна, доц. каф. ТМІТ

Об'єкт дослідження: процеси захисту від несанкціонованого доступу систем передачі сигналів.

Предмет дослідження: система криптографічного захисту телефонних ліній із застосуванням сигналів детермінованого хаосу

Мета роботи: **вдосконалення методів криптографічного захисту телефонних ліній на базі застосування сигналів детермінованого хаосу**

Хмельницький національний університет, 2021

КРИПТОГРАФІЧНИЙ ЗАХИСТ

2

Рисунок 2.1 – Взаємозвязок технологій захисту інформації

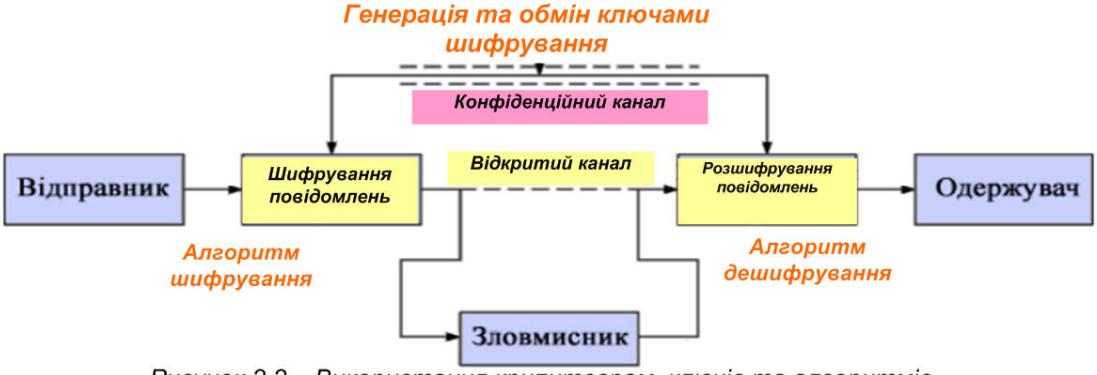


Рисунок 2.2 – Використання крипитограм, ключів та алгоритмів шифрування

Забезпечення захисту інформації – основа сучасної світової економіки людства!

КЛАСИФІКАЦІЯ АЛГОРИТМІВ ШИФРУВАННЯ

3

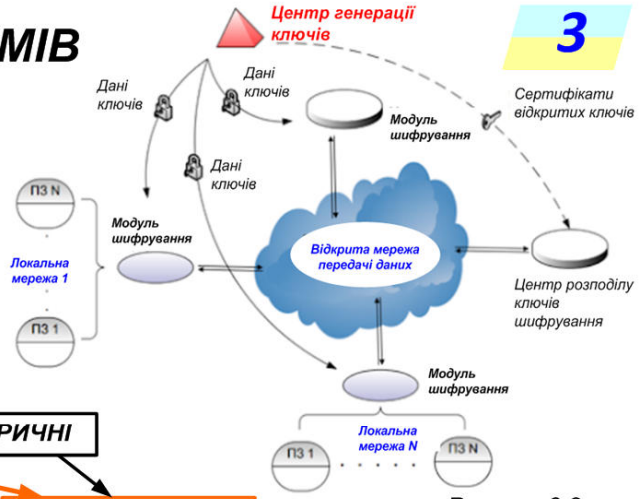


Рисунок 3.2 – Узагальнена схема мережевого криптографічного захисту

Рисунок 3.1 – Класифікація алгоритмів шифрування

ПРОЦЕДУРНА ЕКВІВАЛЕНТНІСТЬ ХАОСУ І КРИПТОГРАФІЇ

4

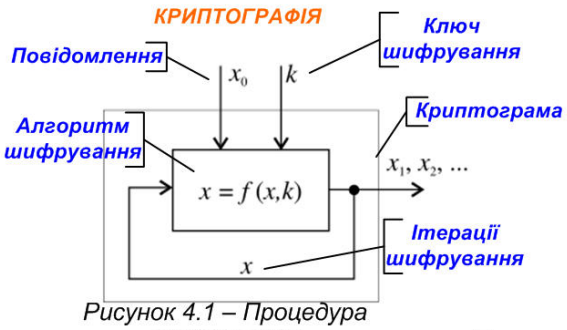


Рисунок 4.1 – Процедура шифрування

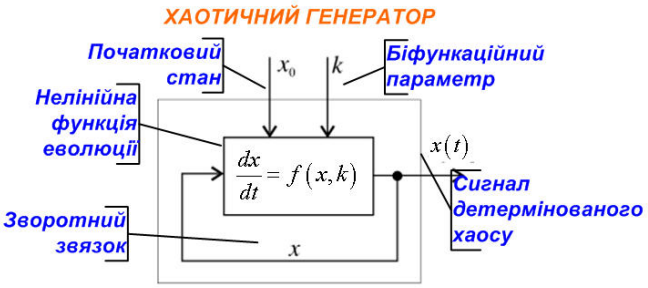


Рисунок 4.3 – Процедура отримання хаотичного сигналу

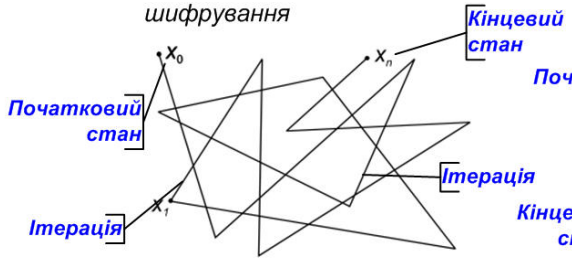


Рисунок 4.2 – Фазовий портрет станів під час шифрування

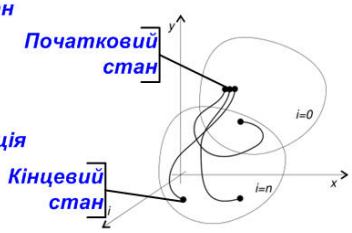
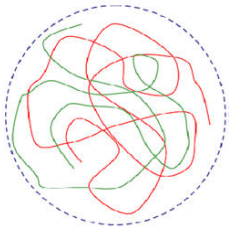


Рисунок 4.4 – Переплучування траєкторій



Рисунко 4.5 - Топологічна транзитивність хаосу

Розсіюванню та перемішуванню даних під час шифрування відповідає експонеційна чутливість та перемішування тараєкторій в хаотичній динаміці!

ХАОТИЧНІ ГЕНЕРАТОРИ ТА ЇХ ОПИС

5

МАТМОДЕЛЬ

$$\frac{dx}{dt} = \alpha\left(y - x - f(x)\right);$$
$$\frac{dy}{dt} = y - x + z;$$
$$\frac{dz}{dt} = -\beta y.$$

Рисунок 4.1

ЕКВІВАЛ. МОДЕЛЬ

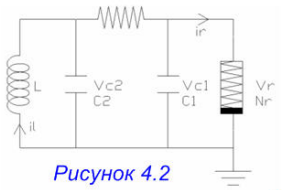


Рисунок 4.2

ПРИНЦИПОВА СХЕМА

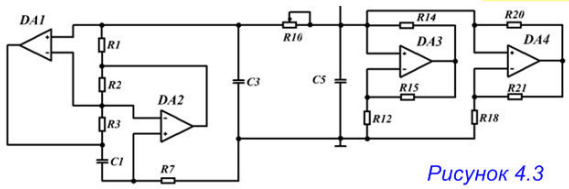


Рисунок 4.3

НЕЛІНІЙНІСТЬ

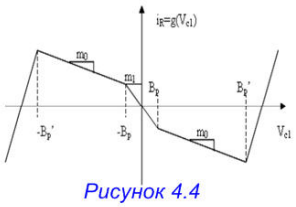


Рисунок 4.4

3D ФАЗОВИЙ ПОРТРЕТ

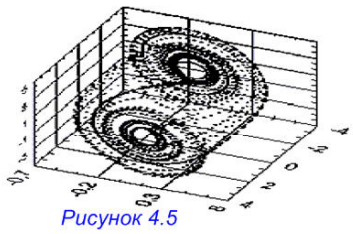


Рисунок 4.5

СПЕКТР

Рисунок 4.6

СИГНАЛ ДЕТЕРМІНОВАНОГО ХАОСУ

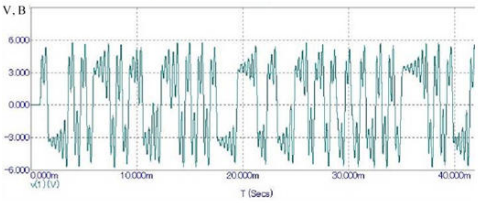


Рисунок 4.7

СПОСОБИ ХАОТИЧНОЇ СИНХРОНІЗАЦІЇ

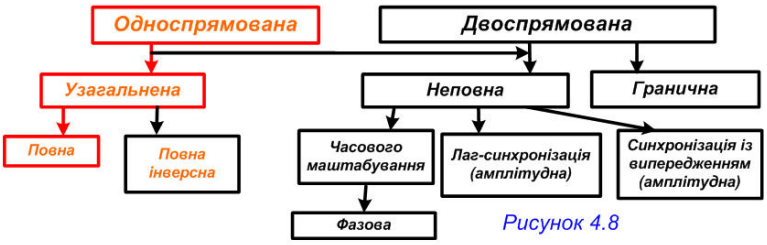


Рисунок 4.8

Сигнал детермінованого хаосу в класичній криптографії може бути використано для генерації ключів шифрування

ЗАХИСТ ІНФОРМАЦІЇ В ХАОТИЧНИХ КАНАЛАХ

6

Рисунок 6.1 – Хаотичні канали із хахистом інформації

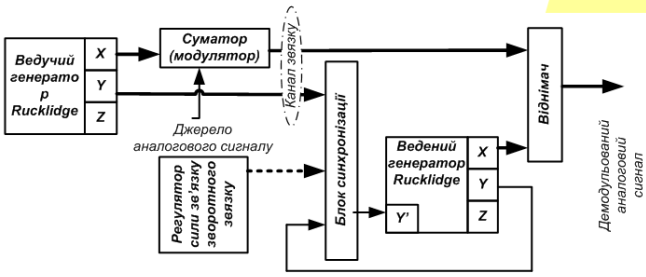


Рисунок 6.2 – Структурна схема каналу хаотичного маскування із розділеними каналами модуляції та синхронізації

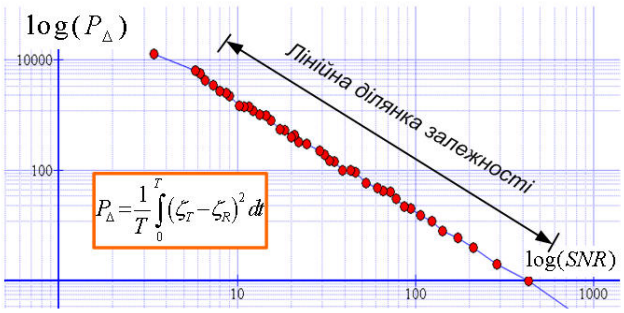


Рисунок 6.3 – Використання рівня десинхронізації як модуляційної характеристики

ЗАХИСТ ІНФОРМАЦІЇ В ХАОТИЧНИХ КАНАЛАХ ІЗ МАСКУВАННЯМ

7

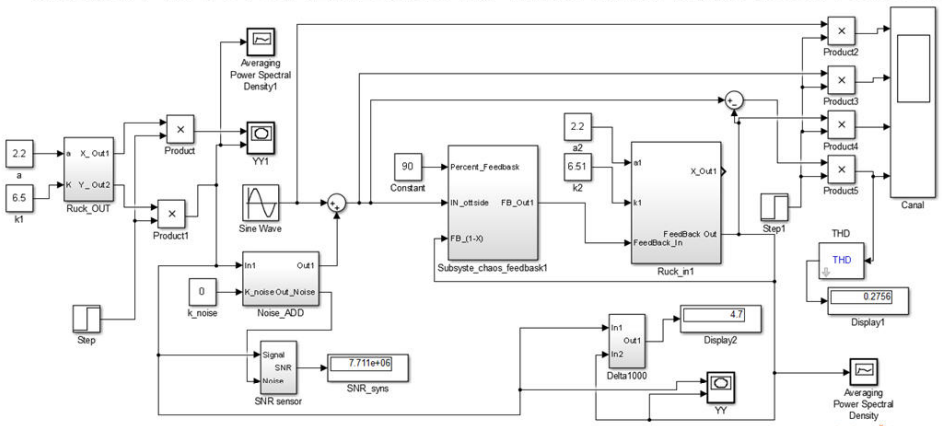


Рисунок 7.1 – Імітаційна модель хаотичного каналу із маскуванням аналогових повідомлень із суміщеним каналом синхронізації-даних

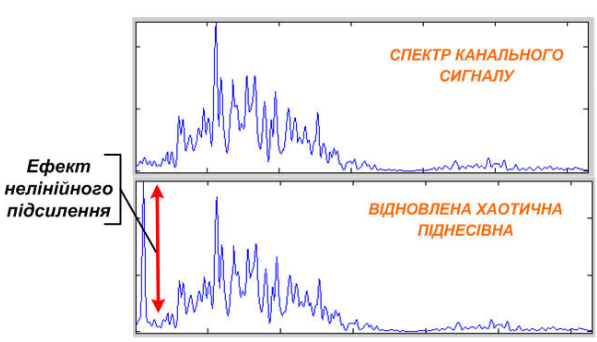


Рисунок 7.2 – Діаграми роботи системи зв'язку із хаотичним маскуванням

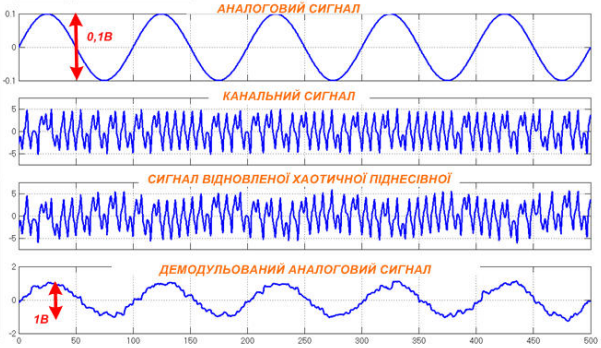


Рисунок 7.3 – Діаграми роботи системи зв'язку із хаотичним маскуванням

ОЦІНКА КІЛЬКОСТІ КЛЮЧІВ ШИФРУВАННЯ В КАНАЛАХ ІЗ ХАОТИЧНИМ СИНХРОННИМ ВІДГУКОМ ТА ПАРАМЕТРИЧНОЮ МОДУЛЯЦІЄЮ

8

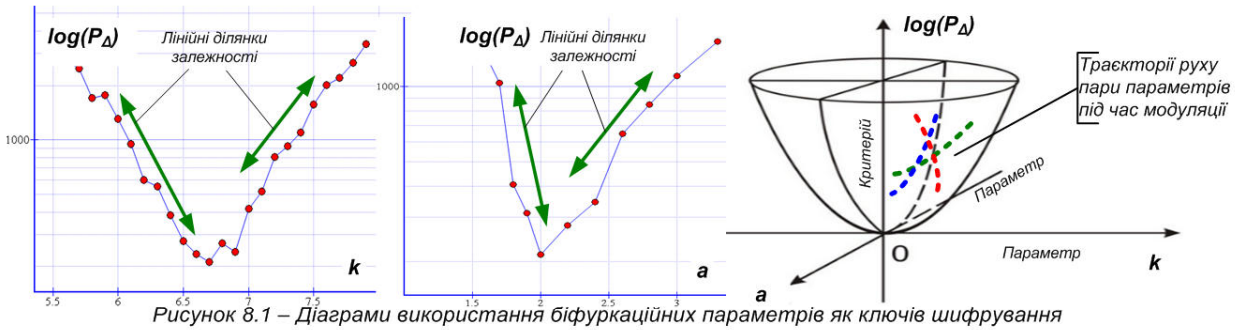


Рисунок 8.1 – Діаграми використання біфуркаційних параметрів як ключів шифрування

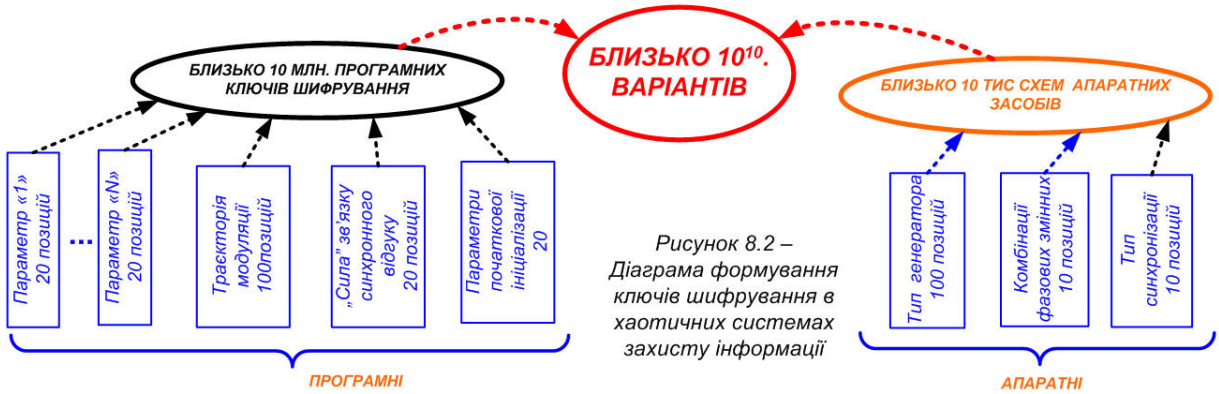


Рисунок 8.2 – Діаграма формування ключів шифрування в хаотичних системах захисту інформації

ВПЛИВ ПАРАМЕТРИЧНОЇ ХАОТИЧНОЇ МОДУЛЯЦІЇ НА КАНАЛЬНИЙ СИГНАЛ

9

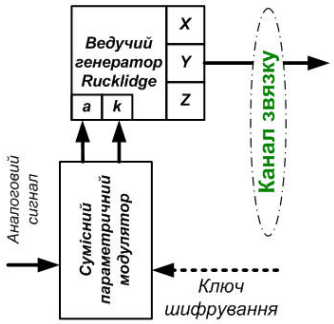


Рисунок 9.1 – Схема параметричної модуляції хаотичного генератора

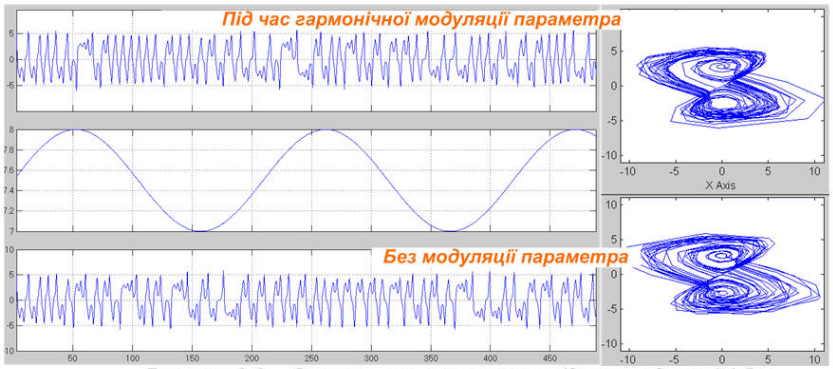


Рисунок 9.2 – Сигнали та атрактори під час модуляції і без

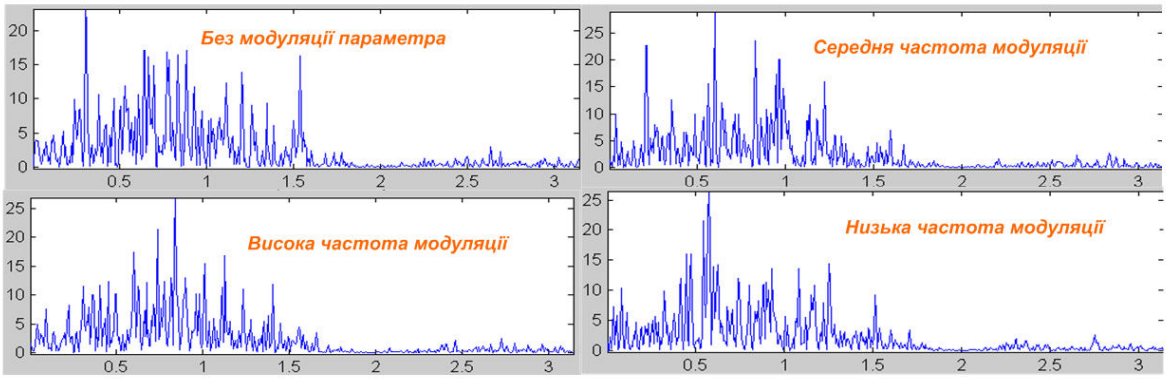
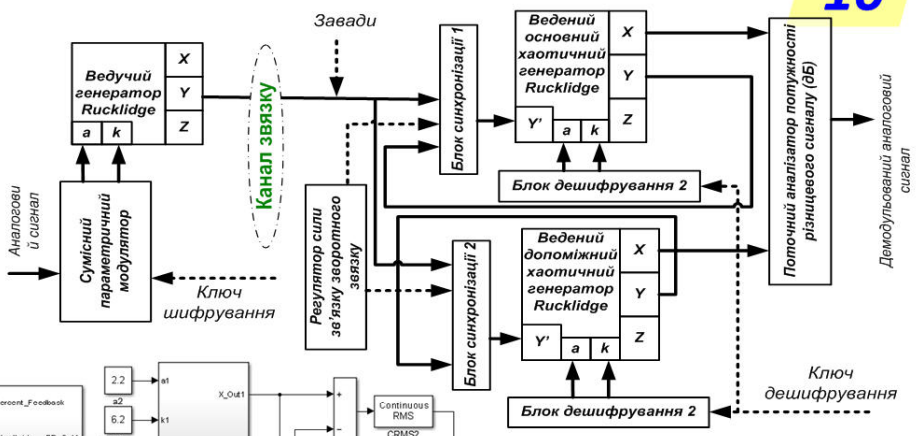


Рисунок 9.3 – Спектри канальних сигналів із модуляцією різними частотами

ІМІТАЦІЙНА МОДЕЛЬ КРИПТОГРАФІЧНОГО ЗАХИСТУ

10

Рисунок 10.1 – Схема криптографічного захисту із параметричною модуляцією



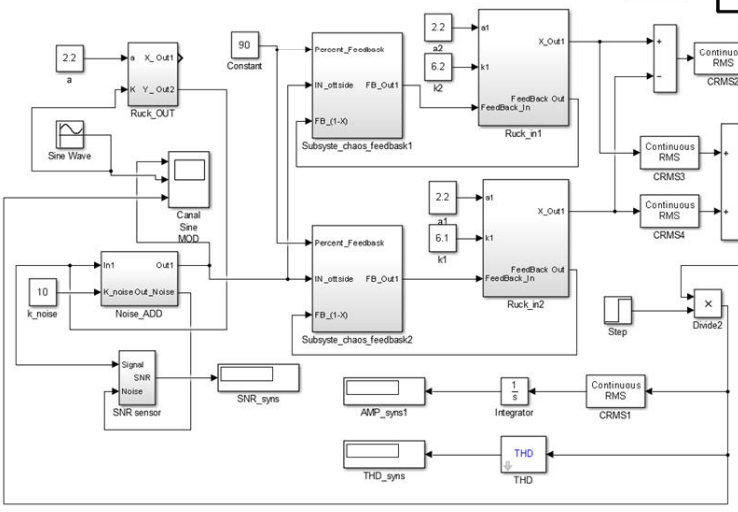


Рисунок 10.2 – Імітаційна модель Matlab\Simulink хаотичної системи зв'язку із однопараметричною модуляцією та синхронним відгуком ведених генераторів

Критерій демодуляції:

$$K_{\Delta}(t) = \frac{RMS\left[\zeta_1(t) - \zeta_2(t)\right]}{RMS\left[\zeta_1(t)\right] + RMS\left[\zeta_2(t)\right]}$$

РЕЗУЛЬТАТИ ІМІТАЦІЙНОГО МОДЕЛЮВАННЯ 11

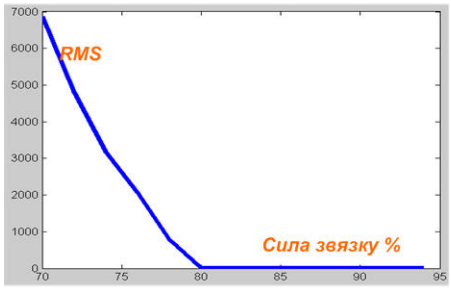


Рисунок 11.1 – Залежність рівня розугодження ведених генераторів від сили звязку

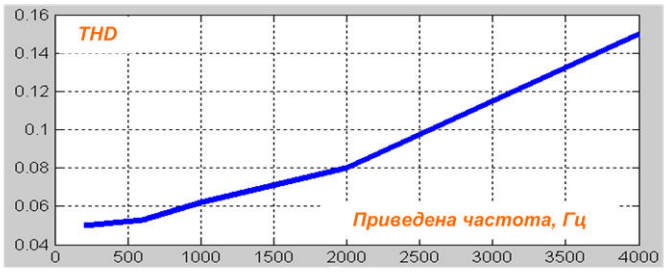


Рисунок 11.3 – Залежність коефіцієнту гармонік від діапазона частот, приведеного до стандартного телефонного каналу

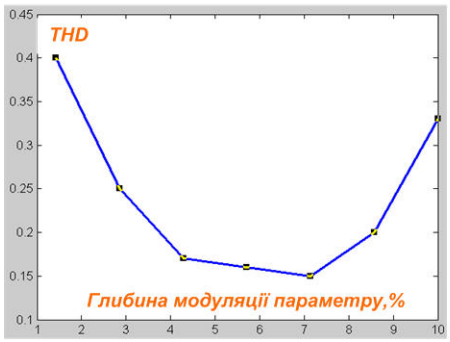


Рисунок 11.2 – Залежність коефіцієнту гармонік від глибини модуляції параметра

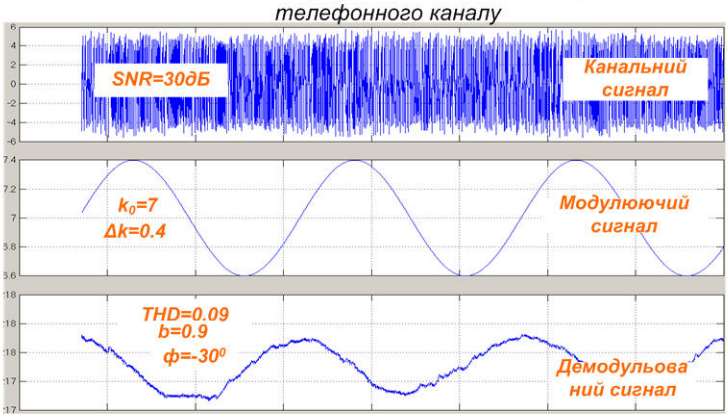


Рисунок 11.4– Діаграми хаотичної демодуляції в хаотичній системі захисту аналогової інформації

ВИСНОВКИ З ДИПЛОМНОЇ РОБОТИ МАГІСТРА 12

Наукова новизна:

1. *Запропоновано метод одночасного забезпечення прихованості дії та криптографічної стійкості аналогових телефонних повідомлень, що відрізняється застосуванням для передачі даних генераторів детермінованого хаосу із багатопараметричною модуляцією хаотичної піднесівної та детектуванням повідомлень на базі допоміжного хаотичного генератора із визначенням рівня сигналу за різницевою потужністю ведених генераторів, що дає можливість використати поле параметрів хаотичного генератора як ключі шифрування, а шумоподібний сигнал детермінованого хаосу для прихованості дії.*

2. *Запропоновано метод покращення криптографічної стійкості передачі аналогових повідомлень на основі застосування хаотичної піднесівної та параметричної модуляції інформаційним повідомленням веденого генератора, що відрізняється введенням інформації про траєкторію руху параметрів в багатовимірній площині параметрів під час модуляції інформаційного повідомлення. Збільшення параметрів для формування ключа шифрування різко збільшує криптографічну стійкість без порушення прихованості дії.*

Практичне значення:

1. *Показано безпосередній еквівалентний діалектичний зв'язок між процесами та об'єктами криптографічного захисту та об'єктами та процесами нелінійної динаміки систем із сигналами детермінованого хаосу, що підтверджує можливість необхідність застосування хаотичних методів обробки в аналогових системах із захистом інформації на основі прихованості дії та впровадження криптографічних алгоритмів.*

2. *Запропоновано для забезпечення високого рівня криптографічного захисту застосувати методи хаотичної синхронізації та хаотичного синхронного відгуку під час взаємодії веденого та ведучого хаотичного генераторів, що дозволяє проводити детектування аналогових повідомлень за критерієм рівня синхронізму хаотичних генераторів в системі.*

3. *Запропонована методика використання лінійних ділянок залежностей рівня синхронізації на багато параметричній площині для формування ключів шифрування аналогових повідомлень в хаотичній системі передачі аналогових повідомлень по телефонним каналам передачі.*

4. *Запропоновано методики побудови імітаційних моделей та субмоделей каналів передачі аналогових повідомлень, що дозволяє проводити аналіз тактико-технічних характеристик каналів передачі аналогових повідомлень в обмеженому спектрі через багатопараметричну модуляцію біфуркаційних параметрів, за умови широкого діапазону відношень сигнал-завад, застосування різних типів та класів хаотичних генераторів, тощо.*

ВІЙСЬКОВИЙ ІНСТИТУТ
КИЇВСЬКОГО НАЦІОНАЛЬНОГО УНІВЕРСИТЕТУ
ІМЕНІ ТАРАСА ШЕВЧЕНКА

ЗБІРНИК ТЕЗ ДОПОВІДЕЙ

XVII Міжнародної науково-практичної конференції

"Військова освіта і наука: сьогодення та майбутнє"

26 листопада 2021 року

ТОМ 1

(Технічні проблеми озброєння і військової техніки та технології подвійного призначення; Актуальні проблеми лінгвістичного забезпечення Збройних Сил України; Актуальні питання гуманітарного та соціального розвитку Збройних Сил України)

Київ – 2021

УДК 355(477)37
ББК 32.26.8-68.49

Т30 Збірник тез доповідей XVII Міжнародної науково-практичної конференції "Військова освіта і наука: сьогодення та майбутнє" 26 листопада 2021. – Том 1.– Київ : ВІКНУ, 2021. – 227 с.

Рекомендовано до друку Вченою радою Військового інституту Київського національного університету імені Тараса Шевченка
(протокол від 25.11.2021 № 7).

У збірнику тез доповідей друкуються матеріали виступів наукових і науково-педагогічних працівників, курсантів (студентів) Військового інституту Київського національного університету імені Тараса Шевченка та інших вищих військових та закладів вищої освіти України.

У публякаціях розглядаються: технічні проблеми озброєння і військової техніки та технології подвійного призначення; актуальні проблеми лінгвістичного забезпечення Збройних Сил України; актуальні питання гуманітарного та соціального розвитку Збройних Сил України; інформаційно-психологічна боротьба у воєнній сфері; сучасні інформаційно-комунікаційні технології сектору безпеки і оборони України; фінанси; актуальні проблеми військового права; актуальні проблеми геопросторової підтримки військ; наукові проблеми військової політології та морально-психологічного впливу; основні засади, принципів та технологій забезпечення кібербезпеки у воєнній сфері

Наукове видання

ТЕЗИ ДОПОВІДЕЙ

XVII Міжнародної науково-практичної конференції

"Військова освіта і наука: сьогодення та майбутнє"

ТОМ 1

Тексти тез представлено у авторській редакції. Автори несуть повну відповідальність за зміст, добір, точність наведених фактів, цитат, власних імен, дат та інших відомостей.

Збір, технічне редагування та комп'ютерна верстка – Бадрук О.О.
Оригінал-макет та обкладинка – Халіманенко С.М.

Підписано до друку 25.11.2021. Формат 60x84/16.
Гарнітура Times. Папір офсетний. Друк ризограф. Тираж 10.
Умов. друк. аркушів 18. Заказ № 41-16.

Надруковано в навчальному картографічному комплексі ВІКНУ
03189, Київ, вул. Ломоносова, 81
521-32-89

Гринь С.С. (ХмНУ)
к.т.н. Степаненко Є.О. (ГШ ЗСУ)
к.т.н. доц. Пивовар О.С. (ХмНУ)

Криптографічна хаотична система захисту тональних каналів зв`язку

Відкриття можливостей взаємодії хаотичних сигналів, що являють собою шумоподібні неперіодичні але детерміновані процеси суттєво змінює парадигму теорії передачі сигналів щодо використання допоміжних (несівних) коливань для вирішення завдань захисту інформації. Такі хаотичні коливання розглядають як сигнали із великою кількістю ступенів свободи (сигнали із великою базою), що обумовлює можливість застосування параметрів генераторів детермінованого хаосу як ключів шифрування криптографічної системи тонального зв'язку [1] в режимі прихованості дії системи загалом.

Нелінійні динамічні системи, найбільш придатні для генерації хаотичної підесівної під час реалізації завдань захисту каналів передачі, мають мати властивості консервативності, параметричності, декомпозиції та не автономності. Вони забезпечують можливості взаємодії генераторів хаосу на приймальному та передавальному боці каналу через хаотичну синхронізацію або хаотичний синхронний відгук, і таким чином, реалізують комплексні широкі можливості покращення характеристик систем тонального зв'язку особливо в аспектах конфіденційності.

Для введення тонального сигналу в хаотичну несівну застосовується принцип маскування інформаційного сигналу хаотичною піднесівною, що співмірні за шириною спектру та подібні за формою. Відновлення інформації на приймальному боці реалізується через забезпечення повної синхронізації веденого та ведучого хаотичних генераторів підесівних. Прихованість дії досягається малим рівнем інформаційного сигналу, а криптографічний захист – точністю встановлення параметрів обраної нелінійної динамічної системи для підтримання стійкої синхронізації.

Моделювання та дослідження умов роботи системи захисту через використання хаотичних сигналів проводилось в середовищі Mathlab[2] як для аналогових так і для цифрових інформаційних повідомлень, що дозволило встановити можливі параметри перетворень в каналі, що забезпечують максимізацію ключів шифрування за умови сталої прихованості дії.

1. Пивовар О.С. Варіант структурної будови широкосмугової аналогової системи прихованого зв'язку на основі застосування сигналів детермінованого хаосу/О.С. Пивовар//Вісник Хмельницького національного університету. Технічні науки.-2017.- № 6.- С.111-116.

2. Патрушев Е. М. Автоматическая симуляция в среде Matlab/Simulink на примере модели генератора Дуффинга-Холмса [Текст] / Т. В. Патрушева, Е. М. Патрушев, И. С. Наздрюхин // Ползуновский альманах. – Барнаул, 2016. – № 2. – С. 181-183.

УДК 004:37:001:62

Збірник наукових праць за матеріалами XIII Всеукраїнської науково-практичної конференції «Актуальні проблеми комп'ютерних наук АПКН-2021». Хмельницький – 2021. – 413с.

У збірнику наукових праць подані перспективні практичні розробки аспірантів, студентів та здобувачів в області сучасних інформаційних технологій. Розглянуто актуальні проблеми комп'ютерних наук, комп'ютерної інженерії, прикладної математики й інженерії програмного забезпечення, приведено ряд робіт по впровадженню інформаційних технологій у виробництво та управління. Висвітлено перспективні розробки сучасних систем пошуку, обробки й захисту інформації, медійних та комунікаційних системи.

УДК 004:37:001:62

Матеріали конференції відтворені з авторських оригіналів. При макетуванні можливі незначні зміни компоновки контенту авторських оригіналів.

Участь у конференції та складові всіх її етапів (розгляд праць, макетування, публікація збірника наукових праць та видача сертифікатів) є безкоштовними для всіх учасників. Оргкомітет конференції висловлює подяку учасникам конференції та сподівається на подальшу співпрацю.

З питань проведення конференції та подальшого обміну інформацією звертатись на e-mail конференції: *apkt.khnu@gmail.com*

Міністерство освіти і науки України
Хмельницький національний університет

ЗБІРНИК НАУКОВИХ ПРАЦЬ

за матеріалами XIII Всеукраїнської науково-практичної конференції «Актуальні проблеми комп'ютерних наук АПКН-2021»

15-16 жовтня 2021

Хмельницький 2021

АКТУАЛЬНІ ПРОБЛЕМИ КОМП'ЮТЕРНИХ НАУК - 2021

XIII Всеукраїнська науково-практична конференція

Метою конференції є висвітлення актуальних проблем комп'ютерних наук, інформатики та інформаційних технологій.

СЕКЦІЇ КОНФЕРЕНЦІЇ:

1. **Комп'ютерні науки та прикладні інформаційні технології.**
2. **Комп'ютерна інженерія та системи захисту інформації.**
3. **Математичне моделювання та інженерія програмного забезпечення**
4. **Телерадіокомунікації, медійні та комунікаційні системи.**
5. **Проблеми впровадження інформаційних технологій у виробництво та управління.**

Робочі мови конференції: українська, англійська

ОРГКОМІТЕТ:

СИНЮК О. М. голова оргкомітету, проректор Хмельницького національного університету з наукової роботи, доктор технічних наук, професор

САВЕНКО О. С. заступник голови оргкомітету, декан факультету Інформаційних технологій ХНУ, доктор технічних наук, професор

БАРМАК О. В. заступник голови оргкомітету, завідувач кафедри Комп'ютерних наук ХНУ, доктор технічних наук, професор

ГОВОРУЩЕНКО Т. О. завідувач кафедри Комп'ютерної інженерії та інформаційних систем ХНУ, доктор технічних наук, професор

ВИСОЦЬКА О. В. доктор технічних наук, завідувач кафедри Радіоелектронних та біомедичних комп'ютеризованих засобів і технологій Національного аерокосмічного університету ім. М. Є. Жуковського «Харківський авіаційний інститут», професор

ЛАВРОВ Є. А. доктор технічних наук, професор (Сумський державний університет)

ТІМОФЄЄВА Л. В. відповідальна за студентську науково-дослідну роботу ХНУ

МАЗУРЕЦЬ О. В. секретар конференції, к.т.н., доцент кафедри Комп'ютерних наук ХНУ

МОЛЧАНОВА М. О. секретар конференції, викладач кафедри Комп'ютерних наук ХНУ

КОНТАКТНА ІНФОРМАЦІЯ:

e-mail для листування: *apkt.khnu@gmail.com*

Для розробки системи передачі із хаотичним ЗІ запропоновано застосувати такі підходи: за умови малої відмінності між параметрами веденого та ведучого ХГ режим хаотичної синхронізації встановлюється більш швидко; для передачі аналогових повідомлень слід застосовувати «силу» зв'язку між веденим та ведучим генераторами менше критичної; для детектування аналогових повідомлень із підвищеним криптографічним захистом на приймальному боці слід використати екстраполятор із керованими параметрами.

Дослідження застосування вказаних підходів реалізовувалось на базі ХГ Rucklidge , який має два параметри керування (a,k).

Якщо для визначення похибки синхронізації застосувати різницеву потужність сигналу однойменних фазових змінних основного та допоміжного ведених генераторів та логарифмічний масштаб то на залежності (рис.1) присутня значна лінійна ділянка, що може бути застосована як модуляційна характеристика в системі криптографічного захисту, а дія шумоподібного хаотичного сигналу та власне схема передачі забезпечуватиме прихованість дії.

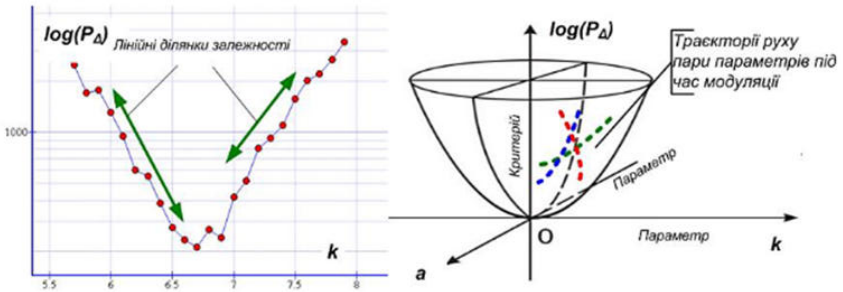


Рисунок 1 – Залежність похибки синхронізації від параметрів керування хаотичних веденого та ведучого генераторів

В такій системі прихованого зв'язку (рисунок 2) сукупність пар значень параметрів хаотичного генератора, які визначають середину лінійної ділянки, задають параметри криптографічного захисту, а характер їх функціональних – алгоритм шифрування (рисунок 1).

В схемі передачі (рис.2) за запропонованими принципами сумісний параметричний модулятор за допомогою ключів шифрування обирає траєкторію зміни параметрів під дією аналогового сигналу. На приймальному боці ведені ХГ починають синхронізуватись із ведучим генератором тим краще, чим ближче значення їх параметрів до поточних параметрів ведучого генератора встановлені екстраполятором. Дешифрування можливе лише за умови правильного вибору

УДК 623.519

Гринь С. С., Пивовар О. С., Таранчук А. А.

Хмельницький національний університет

ЗАБЕЗПЕЧЕННЯ ПРИХОВАНОСТІ ДІЇ ТА КРИПТОГРАФІЧНОГО ЗАХИСТУ АНАЛОГОВИХ СИГНАЛІВ В ХАОТИЧНІЙ СИСТЕМІ ЗВ'ЯЗКУ

Розглянуто можливості одночасного забезпечення прихованості дії та криптографічного захисту в телекомунікаційних системах із застосуванням сигналів детермінованого хаосу та хаотичних методів їх обробки.

Possibilities of simultaneous provision of stealth of action and cryptographic protection in telecommunication systems with application of signals of deterministic chaos and chaotic methods of their processing are considered.

Захист інформації (ЗІ) – одне із найважливіших завдань прогресивного розвитку людства. Без забезпечення конфіденційності даних неможливе існування світової економіки в тому вигляді, що ми знаємо. Найкращим способом забезпечення проблематики ЗІ є прихованість дії, що забезпечує захист через неможливість виявлення навіть факту передачі [1].

Інший спосіб ЗІ – криптографічний, що передбачає застосування алгоритмів перетворення повідомлень таким чином, щоб за умови можливості виявлення факту передачі, забезпечувалась неможливість виявлення її інформаційного змісту. Поєднання захисту прихованістю дії та криптографічними перетвореннями дає найліпші результати загалом [1].

Останніми десятиліттями з'явились вдалі спроби застосувати для захисту інформації методи хаотичної динаміки [2], що дозволяють одночасно вирішити як завдання прихованості дії, так і завдання криптографічного захисту.

Метою роботи є розробка концепції використання методів хаотичної динаміки для забезпечення захисту аналогових повідомлень від несанкціонованого доступу в телекомунікаційних каналах зв'язку.

Найбільш перспективним методом введення інформаційного сигналу в хаотичну піднесівну вважають метод параметричної модуляції хаотичного генератора (ХГ) [2], а найбільш завадостійким способом демодуляції є метод допоміжного ХГ на приймальному боці [3]. Основою роботи такої схеми передачі інформації є забезпечення односпрямованої хаотичної синхронізації та фіксація рівня її значення для через деякий критерій, який враховує відмінності між основним та допоміжним веденими ХГ [3].

АКТУАЛЬНІ ПРОБЛЕМИ КОМП'ЮТЕРНИХ НАУК 2021

ЗБІРНИК НАУКОВИХ ПРАЦЬ

Комп'ютерна верстка: **Мазурець О.В.**

Підписано до друку 14.10.2021.
Версія друку «APKN-2021 CorpusPaper v4mod3».

E-mail: *apkt.khnu@gmail.com*
ХНУ. м. Хмельницький, вул. Інститутська,11.

значень параметрів, що забезпечується ключами шифрування на передавальному та приймальному боці.

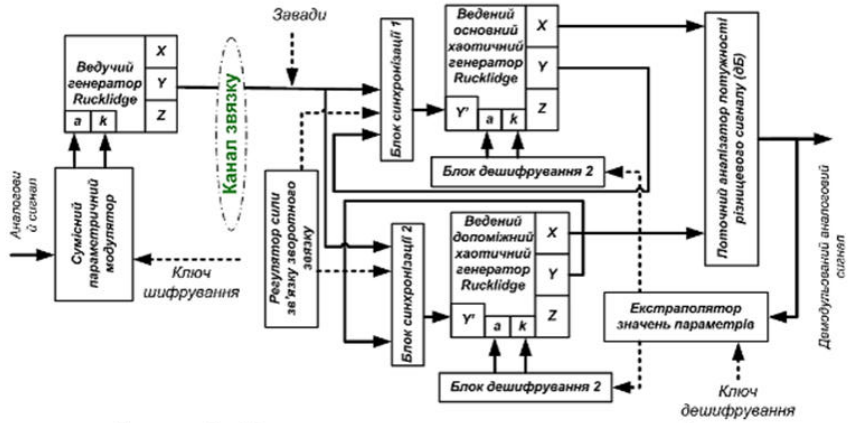


Рисунок 2 – Хаотична аналогова система прихованого зв'язку

Перевірка працездатності запропонованої схеми передачі реалізована в системі Mathlab/Simulink. Рівень нелінійних спотворень під час передавання повідомлень не перевищував 5% за умови відношення сигнал-шум 10дБ.

Перелік посилань

1. Конахович Г.Ф. Захист інформації в телекомунікаційних системах /Г.Ф. Конахович, В.П. Климчук, С.М. Паук, В.Г. Потапов, В.М. Чуприн, О.О. Горбунов //Навчальний посібник.– К.: НАУ,2009. – 380с.
2. Прикладне застосування теорії хаотичних систем у телекомунікаціях : монографія / Ю. Я. Бобало, С. Д. Галюк, М. М. Климащ, Р. Л. Політанський; Міністерство освіти і науки України, Національний університет "Львівська політехніка". – Львів; Дрогобич : Коло, 2015. – 184 с.
3. Golevych.O, Pyvovar. O. Dumenko.P "Synchronization of non-linear dynamic systems under the conditions of noise action in the channel", Latvian Journal of Physics and Technical Sciences Открытый доступ Volume 55, Issue 3, 1 June 2018, Pages 70-76 DOI: https://doi.org/10.2478/lpts-2018-0023

Tue Nov 30 12:26:54 EET 2021, Стецюк Віктор Іванович, Хмельницький національний університет, ХНУ

Anti-Plagiarism v-15.257

Максимальное совпадение с одним документом 1.0%

Словари проверки: en_US, ru_RU, ua_UA. **Ошибок в документах: 9%**

ID: 97575 Название: Система криптографічного захисту телефонних ліній Добавлено в БД: 2021-11-30 Авторы: Гринь Сергій Сергійович Руководители: Тарапчук Алла Анатоліївна Консультанты: Оппоненты:	Документ		Суммарное совпадение по Базе Данных	
	Символы	Лексемы	Символы	Лексемы
	114646	1779	1073 (1%)	22 (1%)

Источник плагиата

ID	Описание	Наличие плагиата в документе	
		Символы	Лексемы

UNICHECK

Ім'я користувача: Kafedra TMIT KhNU

ID перевірки: 1009442480

Дата перевірки: 30.11.2021 22:56:51 EET

Тип перевірки: Doc vs Internet

Дата звіту: 30.11.2021 23:19:19 EET

ID користувача: 100005657

Назва документа: Гринь_ТРм20-1

Кількість сторінок: 101 **Кількість слів:** 17383 **Кількість символів:** 140437 **Розмір файлу:** 1.53 MB **ID файлу:** 1009438376

218 слів позначені як "вилучені" та не враховуються у підрахунку слів

0.77% Схожість

Найбільша схожість: 0.26% з Інтернет-джерелом (http://diplomukr.com.ua/upload/21101.doc)

0.77% Джерела з Інтернету | 177 ..... Сторінка 103

Пошук збігів з Бібліотекою не проводився

0.03% Цитат

Цитати | 1 ..... Сторінка 104

Не знайдено жодних посилань

0% Вилучень

Немає вилучених джерел

Модифікації

Виявлено модифікації тексту. Детальна інформація доступна в онлайн-звіті.

Замінені символи | 7

РЕЦЕНЗІЯ

на магістерську дипломну роботу студента гр. ТРм-20-1
спеціальності 172 «Телекомунікації та радіотехніка»
Гринь Сергія Сергійовича
«Система криптографічного захисту телефонних ліній»

Магістерська робота виконана на актуальну на сьогоднішній день тему, оскільки застосування апаратно програмних засобів, що ґрунтуються на нових методах обробки сигналів сприяє розвитку економіки, забезпеченню обороноздатності країни та збереженню базових цінностей приватності особистостей.

Магістрантом оброблено велику кількість наукового та спеціального матеріалу, що не входить в основну програму навчання, на високому методологічному рівні проведено імітаційне моделювання, що підверджує результати впровадження запропонованих методів в аналогові системи захисту інформації.

Матеріал магістерської випускової роботи логічно структурований та написаний у науковому стилі. Робота складається із вступу, 3 розділів, основних висновків по роботі, переліку джерел посилання (45 бібліографічних посилання, 5 сторінок) та 4 додатків (13 сторінок). Загальний обсяг роботи в якому викладено основний зміст складає 85 сторінок і містить 39 рисунків на 36 сторінках по тексту та 21 формулу. Повний обсяг роботи - 120 сторінок.

У першому розділі автором проведений аналіз понять, параметрів та характеристик криптографічних методів захисту інформації та основних параметрів та характеристик систем передачі тональних сигналів телефонними каналами.

У другому розділі автор зупиняється аналізі процедурної еквівалентності захисту інформації діючими криптографічними алгоритмами та схемами генерації та обробки сигналів детермінованого хаосу. Розглянуто

можливості, запропоновано методи та методики застосування хаотичних методів обробки сигналів для досягнення високого рівня криптографічного захисту. Обґрунтована структура хаотичних апаратних засобів та проведена оцінка кількості ключів шифрування аналогових повідомлень..

Третій розділ магістрант присвятив розробці та імітаційним дослідженням моделей в середовищі Matlab\Simulink . За результатами імітаційного моделювання підтверджено припущення можливості застосування хаотичних каналів із параметричною модуляцією та хаотичним синхронним відгуком ведених хаотичних генераторів для забезпечення високого рівня криптографічного захисту. Розроблено ряд методик встановлення параметрів та характеристик, зазначено рекомендації що до практичного застосування запропонованих методів захисту інформації.

Магістрант показав уміння самостійно вирішувати завдання проектування у вказаній керівником тематиці. Сформульовані в роботі висновки достатньо обґрунтовані і можуть бути використані у практичній діяльності по захисту інформації в цивільній та військовій галузях.

Окремі огріхи у вигляді фразеологічних вивертів, орфографічних помилок та технічних помилок не зменшують наукової цінності роботи. Магістерська випускова робота є самостійною, цілісною та завершеною працею, виконана на високому науково-технічному рівні, відповідає вимогам оформлення. Автор магістерської дипломної роботи заслуговує на оцінку «відмінно».

__3_ грудня 2021 р.

Рецензент зав.каф. кібербезпеки ХНУ, к.т.н. , доц. 

Юрій КЛЬОЦ

Завідувачу кафедри
телекомунікацій, медійних та
інтелектуальних технологій (ТМІТ)
Підченко С.К.
здобувача вищої студента
2 курсу, гр. ТРм-20-1
Гриня Сергія Сергійовича

ЗАЯВА

З правилами чинного Положення «Про дотримання академічної доброчесності в Хмельницькому національному університеті» від 26.09.2020 (зі змінами від 26.11.2020), згідно з яким виявлення плагіату є підставою для відмови в допуску кваліфікаційної роботи до захисту та застосування заходів дисциплінарної та академічної відповідальності, ознайомлений. Про використання програмно-технічних засобів для перевірки кваліфікаційних робіт здобувачів вищої освіти на плагіат оповіщена та надаю свою згоду на обробку та збереження університетом моєї роботи в інституційному репозитарії університету.

Також надаю університету право на передачу моєї роботи для обробки та збереження в базах даних програмно-технічних засобів (Unicheck та Anti-Plagiarism) та використання роботи для виявлення плагіату в інших роботах, які перевіряються програмно-технічними засобами та користувачами, що мають доступ до цих програмно-технічних засобів, виключно в обмежених цілях для виявлення плагіату в текстах робіт.

Робота для перевірки університетом надається в друкованому та електронному варіанті. Електронна версія моєї роботи збігається (ідентична) з друкованою.

2.12.21  Гринь С.С.

дата підпис

РІШЕННЯ КАФЕДРИ

ТЕЛЕКОМУНІКАЦІЙ, МЕДІЙНИХ ТА ІНТЕЛЕКТУАЛЬНИХ ТЕХНОЛОГІЙ

ПРО ДОПУСК КВАЛІФІКАЦІЙНОЇ РОБОТИ ДО ЗАХИСТУ

Підтверджуємо ознайомлення з результатом звіту подібності щодо роботи, генерованого системою виявлення текстових збігів/ідентичності/схожості:

Назва: Система криптографічного захисту телефонних ліній

Автор**: Гринь Сергій Сергійович**

Спеціальність: **172 Телекомунікації та радіотехніка**

Освітня програма: Телекомунікації та радіотехніка

Науковий керівник: **к.т.н., доц. Таранчук Алла Анатоліївна**

Після аналізу звіту подібності зроблено такий висновок:

№	Висновок	Позначка про відповідність
1	Запозичення, виявлені в роботі, є законними і не є плагіатом (далі – зазначаються підстави віднесення запозичень до правомірних). Робота приймається до захисту.	**Відповідає**
2	Виявлені запозичення не є плагіатом, розміщені в розділах, які не описують безпосередньо авторське дослідження, але кількість цитат перевищує обсяг, виправданий поставленою метою роботи (далі – зазначаються детальні та аргументовані підстави віднесення запозичень до правомірних). Робота приймається до захисту, але має бути відкоригована. Відкоригований варіант має бути поданий на кафедру за 2 дні до захисту, разом із заявою щодо самостійності виконання письмової роботи та ідентичності друкованої та електронної версії роботи	
3	Виявлені запозичення не є плагіатом, але частково розміщені в розділах, які описують безпосередньо авторське дослідження, а кількість цитат перевищує обсяг, виправданий поставленою метою роботи. В зв'язку з цим мета роботи та поставлені завдання не були досягнені. Робота може бути допущена до захисту (наступного року) після того як буде відкоригована та допрацьована і успішно пройде повторну перевірку на академічний плагіат.	
4	Робота містить навмисні текстові спотворення, передбачувані спроби укриття запозичень або інші прояви академічного плагіату. Робота містить фабрикацію або фальсифікацію даних. Робота не допускається до захисту.	
5	Інше:	

Підтвердження: Запозичення у розмірі 0,77% є випадковими збігами та на рівень подібності не впливає.

3.12.2021р.

Відповідальний за контроль

плагіату за системою Unicheck: Олег ПИВОВАР

Зав. каф. ТМІТ Сергій ПІДЧЕНКО