ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
Факультет програмування та комп'ютерних і телекомунікаційних систем
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 «Конфіденційна система зв'язку з використанням пристроїв із хаотичною динамікою»

ДРТР. 2015005.01.02 ПЗ

Виконав: студент 2 курсу, група $ТР_м$-19-1 _____ М.О. Лівчук
підпис Ініціали, прізвище

Керівник: докт. техн. наук, доц. _____ С.К. Підченко
підпис Ініціали, прізвище

До захисту допускаю:

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

10 12 2020 р.

Хмельницький, 2020

Хмельницький національний університет

Факультет *програмування та комп'ютерних і телекомунікаційних систем*
Кафедра *телекомунікацій, медійних та інтелектуальних технологійта*
Освітній рівень *другий (магістерський)*
Галузь знань *17 – Електроніка та телекомунікації*
Спеціальність 172 – *Телекомунікації та радіотехніка*
Освітня-професійна програма *Телекомунікації та радіотехніка*

ЗАТВЕРДЖУЮ
Зав. кафедрою_____
_____
«_3_»_____09_____ 2020 р.

ЗАВДАННЯ
НА ДИПЛОМНУ РОБОТУ

Лівчуку Максиму Олександровичу

1 Тема роботи: *Конфіденційна система зв'язку з використанням пристроїв із хаотичною динамікою*
керівник роботи Підченко Сергій Костянтинович, д.т.н, доцент
Затверджено наказом по університету від «1» вересня 2020 р. № 118
2 Строк подання студентом роботи на кафедру: 25.11.2020 р.
3 Вихідні дані (характеристика об'єкта, умов дослідження та ін.)
Метою роботи є підвищення рівня конфіденційності та ефективності передачі інформації в телекомунікаційних системах.
Об'єкт дослідження – процес конфіденційної передачі інформаційних сигналів каналами зв'язку в телекомунікаційних системах.
Предмет дослідження – методи та засоби конфіденційної передачі інформаційних сигналів за допомогою пристроїв із хаотичною динамікою.
4 Зміст пояснювальної записки (перелік питань, що їх належить розробити)
1 АНАЛІЗ МЕТОДІВ ТА ЗАСОБІВ ЗАХИСТУ ІНФОРМАЦІЇ В ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ.
2 МАТЕМАТИЧНІ МОДЕЛІ ДИНАМІЧНИХ СИСТЕМ ІЗ ХАОТИЧНОЮ ПОВЕДІНКОЮ
3 АНАЛІЗ ТА МАТЕМАТИЧНЕ МОДЕЛЮВАННЯ ДИНАМІЧНОЇ СИСТЕМИ ЛОРЕНЦА
4 МЕТОДИ ПЕРЕДАЧІ ТА ЗАХИСТУ ІНФОРМАЦІЇ ЗА ДОПОМОГОЮ ДЕТЕРМІНОВАНО ХАОСУ НА БАЗІ СИСТЕМИ ЛОРЕНЦА

Завдання отримав_____

Науковий керівник_____

КАЛЕНДАРНИЙ ПЛАН

№ п/п	Назва етапів (розділів) дипломної роботи	Строк виконання етапів дипломної роботи	Примітка
1	Аналіз літературних джерел	10.09.2020 р.	виконано
2	Написання 1 розділу ДР	22.09.2020 р.	виконано
3	Визначення проблеми дослідження	29.09.2020 р.	виконано
4	Написання 2 розділу	20.10.2020 р.	виконано
5	Розробка моделі	27.10.2020 р.	виконано
6	Написання тез конференції	2.11.2020 р.	виконано
7	Написання 3 розділу ДР	7.11.2020 р.	виконано
8	Теоретичне та практичне моделювання	15.11.2020 р.	виконано
9	Написання 4 розділу	24.11.2020 р.	виконано
10	Оформлення пояснювальної записки до ДР	26.11.2020 р.	виконано
11	Оформлення презентаційних матеріалів	30.11.2020 р.	виконано

Студент _____ Лівчук М.О.
Підпис Ініціали, прізвище

Керівник роботи _____ Підченко С.К.
Підпис Ініціали, прізвище

ЗМІСТ

ВСТУП

Впровадження ідей та методів щодо використання теорії нелінійних процесів із хаотичною поведінкою в сучасних радіотехнічних пристроях та засобах телекомунікацій за останні декілька десятиліть набуто великої популярності серед науковців та інженерів-дослідників у суміжних галузях. Розвиток теорії нелінійних процесів динамічних систем забезпечує підґрунтя для практичного застосування хаосу в прикладних задачах, що пов’язані із розробкою пристроїв та засобів телекомунікацій. Явище детермінованого динамічного хаосу представляє собою складні неперіодичні коливання, які генеруються деякою нелінійною динамічною системою. Такі коливання не залежать від впливу зовнішніх шумів та повністю визначаються параметрами динамічної системи, що їх породжує.

Актуальність теми дослідження. Актуальність теми магістерського дослідження обумовлена проблемою захисту інформації, яка передається каналами зв’язку в телекомунікаційних системах. Сьогодні з метою забезпечення конфіденційності повідомлень, що передаються відкритими каналами зв’язку, використовуються криптографічні методи для шифрування. За допомогою методів стеганографії здійснюється приховання самого факт передачі інформації. Також корисними з точки зору захисту інформації можуть бути хаотичні сигнали, зокрема, вони можуть бути використані для прихованої передачі інформації на основі методу хаотичного маскування. Іншим прикладом застосування хаосу є генерування дискретними динамічними системами псевдовипадкових числових послідовностей для використання в алгоритмах шифрування.

Мета і задачі дослідження. Метою дослідження є підвищення рівня конфіденційності та ефективності передачі інформації в телекомунікаційних системах.

Для досягнення поставленої мети в роботі сформульовані та вирішені наступні задачі:

- аналіз методів та існуючих рішень щодо використання детермінованого хаосу для передачі інформації;
- аналіз математичних моделей динамічних систем, які можуть генерувати хаос;
- вибір засобів та алгоритмів для чисельного розрахунку та моделювання нелінійних систем;
- моделювання синхронно зв’язаних хаотичних систем
- моделювання процесу передачі сигналів за допомогою хаотичних систем
- розробка алгоритму та програмна реалізація шифрування даних дискретними хаотичними послідовностями.

Об’єкт дослідження: процес конфіденційної передачі інформаційних сигналів каналами зв’язку в телекомунікаційних системах.

Предмет дослідження: методи та засоби конфіденційної передачі інформаційних сигналів за допомогою пристроїв із хаотичною динамікою.

Методи дослідження: Для вирішення поставлених задач були використані методи математичного аналізу, нелінійної динаміки, математичного моделювання, алгоритмізації і програмування, теорії електричних кіл та сигналів.

Наукова новизна отриманих результатів: отримав розвиток метод шифрування даних на основі дискретних хаотичних послідовностей. На базі дискретно-часової динамічної моделі Лоренца було розроблено алгоритм шифрування вихідного масиву байтів.

Практичне значення отриманих результатів:

- розроблена імітаційна модель генератора хаотичних коливань на основі моделі Лоренца;
- розроблена імітаційна модель хаотичного маскування аналогових сигналів на базі системи Лоренца;

- розроблена імітаційна модель передачі цифрових сигналів шляхом маніпуляції хаотичних режимів генератора передавача;
- розроблено алгоритм та запропонована програмна реалізація процедури шифрування байтового масиву дискретними хаотичними послідовностями.

Апробація результатів дослідження. За результатами магістерської роботи були підготовлені тези, що були опубліковані в збірнику тез доповідей IX Міжнародної науково-технічної конференції молодих учених та студентів «Актуальні задачі сучасних технологій», яка проходила в Тернополі 20-26 листопада 2020 року.

1 АНАЛІЗ МЕТОДІВ ТА ЗАСОБІВ ЗАХИСТУ ІНФОРМАЦІЇ В ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ

1.1 Передумови для використання хаосу для передачі інформації

В основі теорії використання хаотичних пристроїв в телекомунікаційних системах лежать такі наукові досягнення (рисунок 1.1):

- відкриття та розробка теорії нелінійних процесів, пов’язаних із поняттям «дивного атрактора»;
- винайдення простих електронних схем, які за певних умов можуть генерувати складні хаотичні коливання;
- відкриття явища синхронізації систем із хаосом та розвиток теорії щодо його застосування в системах передачі інформації;
- розробка методів кількісної оцінки ступеня хаотичності систем.

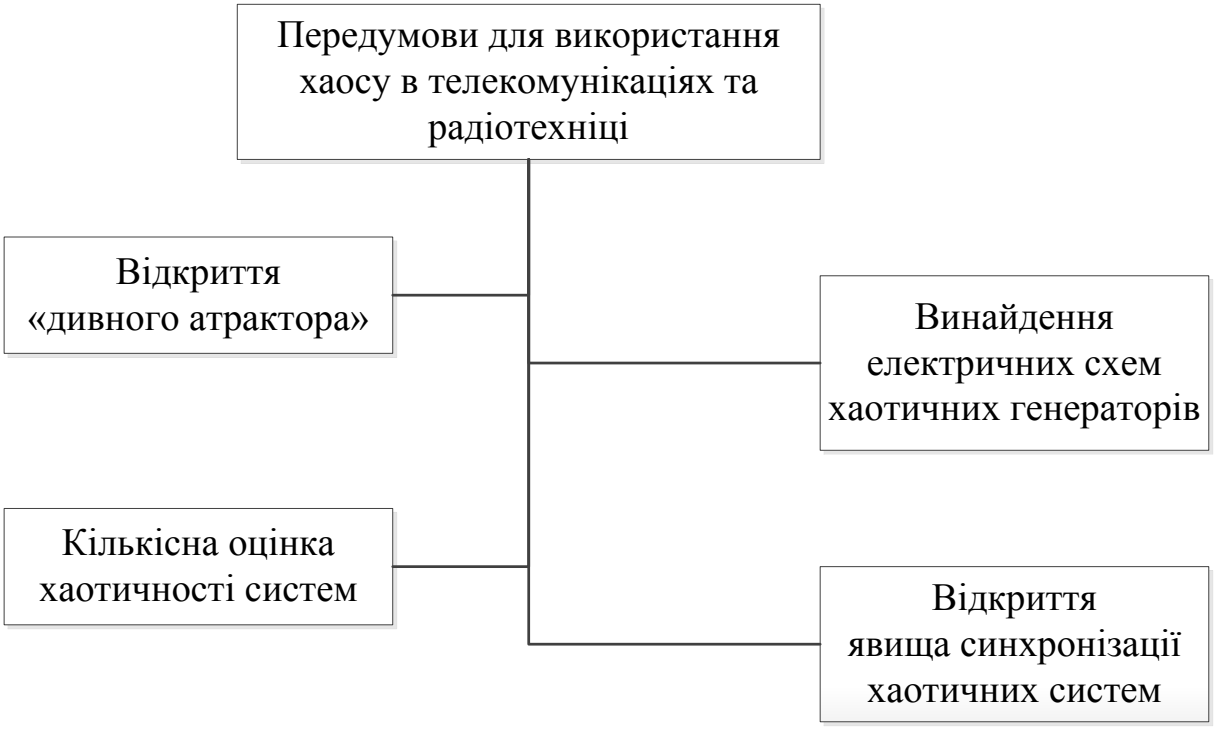


Рисунок 1.1 – Передумови використання хаосу в радіотехніці

Класичним прикладом нелінійної системи, яка демонструє хаотичну поведінку є система Лоренца, яка була відкрита в 1963 як модель конвекції потоків рідини та газу під час нагрівання [1].

Термін «хаос» було запропоновано у 1975 році у роботі Т. Лі [2] для описання поведінки логістичного відображення:

$$x_{n+1} = r x_n \left(1 - x_n\right), \tag{1.1}$$

де x_n – n-й відлік послідовності; r – параметр системи.

Рівняння (1.1) задає відображення деякого значення з проміжку [0; 1] у цей самій проміжок та, за деяких значень параметру k, може генерувати хаотичні послідовності із властивостями, подібними до випадкових величин.

Поведінку логістичного відображення залежно від параметру r ілюструє біфуркаційна діаграма, зображена на рисунку 1.2.

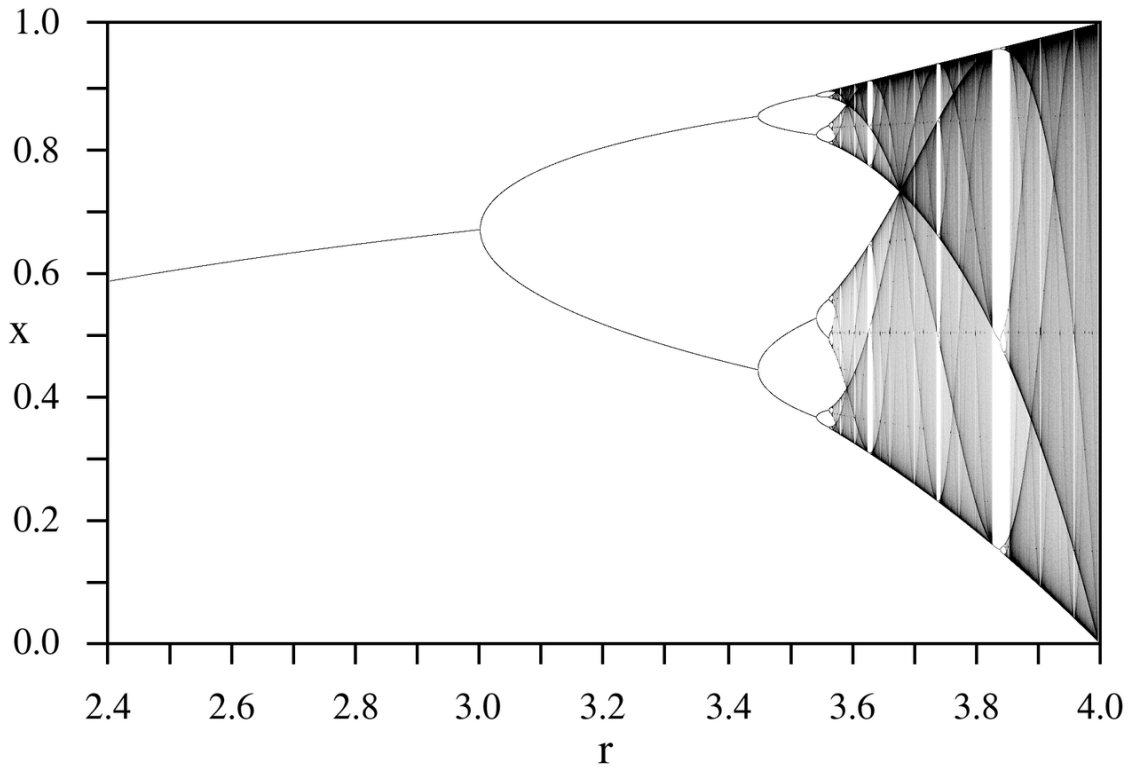


Рисунок 1.2 – Біфуркаційна діаграма для логістичного відображення

З рисунку 1.2 видно, що хаотична поведінка логістичного відображення (1.1) починається зі значення $r \approx 3{,}57$.

Також з рисунку 1.2 видно, що структура діаграми є самоподібною. Наприклад, якщо збільшити масштаб діаграми в околі одного з розгалужень, то ми побачимо повторення структури усієї діаграми. Цей ефект наглядно демонструє тісний зв'язок хаосу та фракталів [1].

Хаотичні генератори у вигляді електричних схем є розвитком теорії та практики розробки мультивібраторних схем генераторів періодичних коливань, що була розроблена та детально вивчена в другій половині XX ст [1]. В основі роботи таких пристроїв завжди лежить використання нелінійного елементу.

Електронні схеми генераторів хаотичних коливань можуть бути побудовані на базі радіоелементів з нелінійною або кусково-лінійною вольт-амперною характеристикою (ВАХ) [1]. Одними з перших електронних генераторів хаосу були схеми Чуа, Лі, Ван дер Поля, Колпітца [1, 3].

«Дивним атрактором» прийнято називати фрактальну множину точок фазового простору, до якої прямують фазові траєкторії системи з плином часу. Існування хаотичних атракторів динамічних систем дає можливість синхронізувати хаотичні системи.

Хаотична поведінка системи супроводжується такими базовими ознаками [1, 4, 5]:

- сильна чутливість до початкових умов;
- фрактальна розмірність атрактора у фазовому просторі;
- неперервний спектр часових реалізацій компонентів системи

Таким чином реальні динамічні системи, які зустрічаються у природі, наприклад, системи Лоренца та Реслера [1, 2] мають фрактальну структуру. Математичні моделі таких систем знайшли застосування в теорії передачі інформації [3].

1.2 Методи синхронізації хаотичних систем

Фундаментальним відкриттям в теорії нелінійних процесів є явища синхронізації двох хаотичних систем.

Вперше синхронізацію двох хаотичних систем для деякого співвідношення параметрів дослідили Т. Карол та Л. Пекора у 1990 в своїй роботі [6].

У літературі прийнято виділяти наступні типи хаотичної синхронізації (рисунок 1.3), які отримали найбільшого поширення і бути детально вивчені [1, 3]:

- повна синхронізація
- фазова синхронізація
- узагальнена синхронізація.

Узагальнена синхронізація в свою чергу поділяється на протифазну, синхронізацію з випередженням, синхронізацію із запізненням.

Повна синхронізація двох неперервних або дискретних хаотичних систем полягає у досягненні режиму їх роботи, коли спостерігається точне співпадіння фазових векторів стану цих систем [1, 6, 8].

Фазова синхронізація полягає у захопленні фаз та середніх частот генераторів хаосу.

Узагальнена синхронізація полягає у становленні з часом деякої функціональної залежності між двома хаотичними системами.

Метод узагальненої синхронізації вважається найбільш придатним для використання у системах прихованої передачі інформації. Це обумовлено стійкістю функціональної залежності між синхронними системами до шумів каналу зв’язку [1].

В результаті синхронізації двох систем спостерігається основні спектральні компоненти відповідних часових реалізацій співпадають. Для режиму повної синхронізації, коли зв’язок між системами максимальний, кількість ідентичних спектральних компонент максимальна [10].

Очевидно, що саме можливість синхронізація хаотичних генераторів дозволяє використовувати їх в якості бази для побудови системи передачі інформації.

В літературі запропоновано чимало підходів щодо способу передачі інформації за допомогою хаосу [1, 9].

Рисунок 1.3 – Види синхронізації хаотичних систем

1.3 Методи передачі інформації на основі детермінованого хаосу

З теорії інформації відомо, що стохастичні сигнали, які отримані на основі випадкових процесі, мають високу інформаційну ємність. Основна проблема при розробці носіїв інформації в цифрових телекомунікаційних каналах – складність генерації випадкових числових послідовностей з використанням короткого набору ключів. Математичні алгоритми, які для заданого ключа здатні генерувати псевдовипадкові послідовності з ключа, повинні мати наступні властивості:

- якомога велика довжина періоду псевдовипадкової послідовності;

- статистична подібність отриманої послідовності чисел властивостями з суто випадкової вибірки;

- можливість програмно-апаратної реалізації генератора випадкових чисел з для застосування в телекомунікаційних пристроях з метою передачі каналом зв’язку з потрібною швидкістю.

Використання хаотичних коливань для передачі інформації є перспективним напрямком сучасної радіотехніки в силу таких особливостей:

- широкосмуговість: хаотичні сигнали не є періодичними і мають неперервний спектр. Для багатьох хаотичних сигналів цей спектр займає широку смугу частот. Вони використовуються для уникнення ослаблення сигналу в певній смузі частот.

- складність форми: хаотичні сигнали мають складну структуру. Хаотичний генератор може генерувати різні коливання при невеликих змінах початкових умов. Це ускладнює визначення внутрішньої структури генератора і прогнозування сигналу, який давно використовується в криптографії.

- ортогональность: функція автокореляції хаотичного сигналу швидко спадає. Отже, сигнали від декількох генераторів можна розглядати як некорельовані, тобто ортогональні, як це використовується в багатьох системах зв'язку.

Передача інформації з низькою ймовірністю помилки може здійснюватися, якщо швидкість генерації інформації хаотичною системою, а отже, і топологічна ентропія системи, не менше швидкості інформації від її джерела, без врахування обмежень в каналі зв'язку, наприклад, обумовленими наявністю завад.

Відомо декілька основних методів побудови систем з хаотичною динамікою для передачі інформації, серед яких можна виділити:

- хаотичне маскування (Chaotic Masking) [12, 25];

- перемикання хаотичних режимів (Chaos Shift Keying, CSK) [12-15];

- нелінійне підмішування (Nonlinear Mixing) [3, 16-17];

- пряма хаотична модуляція (Inverse Systems) [18];

- випереджене керуванням перерізом Пуанкаре (Predictive Poincare Control Modulation) [19];

- хаос в системах з фазовим автопідстроюванням частоти [20];

- частотна модуляція хаотичним сигналом [21].

За способом вилучення інформаційного повідомлення з прийнятого сигналу розрізняють системи з когерентним і некогерентного прийомом. В основі роботи систем, що реалізують когерентний метод прийому, лежить явище хаотичної синхронізації [6], що використовується для демодуляції хаотичних коливань. Як правило, в системах такого типу для досягнення режиму синхронізації необхідно забезпечувати високий ступінь ідентичності параметрів передавача і приймача. Структура і параметри передавача, в загальному випадку, не відомі третім особам, що забезпечує конфіденційність передається інформації. До недоліків систем з хаотичною синхронізацією відносяться необхідність строго витримувати ідентичність параметрів передавача і приймача, а також обмеження, пов'язані з підвищеними вимогами до якості каналу зв'язку, і низька стійкість до адитивних шумів в каналі зв’язку.

До систем, що не використовують явище хаотичної синхронізації, можна віднести:

- системи з відносним прийомом (Differential Chaos Shift Keying, DCSK) [22];
- системи з енергетичний прийом [23];
- інверсні систему без хаотичної синхронізації [14].

У DCSK-системах і системах з оцінкою енергетичних параметрів для вилучення інформації з сигналу використовуються його статистичні властивості і застосовуються традиційні методи обробки сигналів. Таким чином, може бути забезпечена висока завадостійкість, що притаманна системам, які реалізують оптимальний прийом сигналу.

1.2 Огляд методів захисту передачі інформації в телекомунікаційних системах

1.2.1 Криптографічні методи

Криптографічні методи та засоби захисту інформації використовують математичні алгоритми для взаємо однозначного перетворення відкритого тексту в шифротекст (шифр) на основі ключа шифрування.

Власне криптографія – наука, яка вивчає методи забезпечення конфіденційності та цілісності даних на основі алгоритмів шифрування.

На даний час прийнято розділяти криптографічні алгоритми на дві основні категорії:

- алгоритми шифрування з секретним ключем (симетричні): блокові шифри та потокові шифри;
- алгоритми шифрування з відкритим ключем (асиметричні).

Більшості ітераційних блокових шифрів полягають у побудові криптостійких системи шляхом послідовного застосування відносно простих криптографічних перетворень. Принцип багаторазового шифрування за допомогою простих криптографічних перетворень був вперше запропонований Шеноном [36]: він

використовував з цією метою перетворення перестановки і підстановки. Перше з цих перетворень переставляє окремі символи перетворюваного інформаційного блоку, а друге – замінює кожен символ (або групу символів) іншим символом з того ж алфавіту (відповідно групою символів того ж розміру і з того ж алфавіту). Вузли, що реалізують ці перетворення, називаються, відповідно, P-блоками (P-box, permutation box) і S-блоками (S-box, substitution box).

З 2001 року для шифрування даних використовується Advanced Encryption Standard (AES), який прийшов на заміну стандартам Data Encryption Standard (DES) та Tripple DES. Шифр AES оснований на алгоритмі, розробленому бельгійцями Д. Дейменом і В. Райменом. Він швидкий, простий, захищений, універсальний і добре підходить для реалізації на смарт-картах. В основі алгоритму лежить ітераційний блоковий шифр, що має архітектуру «Квадрат». Шифр має змінну довжин блоків і різні довжини ключів. Довжина ключа і довжина блоку можуть бути рівні незалежно один від одного 128, 192 або 256 бітів. Стандарт AES визначає довжину блоку рівною 128 бітів.

Основна ідея потокового шифрування полягає в тому, що кожен з послідовних знаків відкритого тексту підлягає окремому перетворенню. Різні знаки відкритого тексту піддаються різним перетворенням, таким чином перетворення, якому піддаються знаки відкритого тексту, змінюватимуться з кожним наступним моментом часу. Можлива реалізація такого підходу в наступний спосіб: деяким чином генерується послідовність знаків k_1 k_2, ... k_n, що називається ключовим потоком (keystream) або біжучим ключем (running key, RK), потім кожен знак x_i відкритого тексту підлягає оборотному перетворенню залежно від елементу k_i послідовності ключа.

Потокові шифри зазвичай працюють швидше і потребують для своєї реалізації набагато менше програмного коду, ніж блокові шифри. Найбільш відомий потоковий шифр був розроблений Р. Ривестом – це шифр RC4, який характеризується змінним розміром ключа і байт-орієнтованими операціями. На

один байт потрібно від 8 до 16 операцій, програмна реалізація шифру виконується досить швидко. Шифр RC4 використовується для шифрування файлів в таких пристроях, як RSA SecurPC. Він також застосовується для захисту комунікацій, наприклад, для шифрування потоку даних в Інтернет-з'єднаннях, що використовують протокол SSL.

У випадку асиметричної криптографії, для шифрування і розшифрування використовуються різні функції. Асиметричні алгоритми основуються на ряді математичних задач, на яких і базується їх стійкість. Поки не буде знайдений поліноміальний алгоритм рішення цих задач, дані алгоритми будуть стійки. У цьому полягає ще одна відмінність симетричного і асиметричного шифрування: стійкість першого є доведеним фактом, стійкість другого – імовірною.

Найбільш відомі криптосистеми з відкритим ключем:

- рюкзачна криптосистема (Knapsack Cryptosystem);
- криптосистема RSA;
- криптосистема Ель-Гамаля – EGCS (El Gamal Cryptosystem);
- криптосистема, основана на властивостях еліптичних кривих – ECCS (Elliptic Curve Cryptosystems).

Застосування алгоритмів шифрування з відкритим ключем дозволяє позбутися необхідності використання секретних каналів зв'язку для попереднього обміну ключами, а також звести проблему злому шифру до вирішення алгоритмічно складної математичної задачі.

Все більшого поширення в якості альтернативи RSA отримують криптосистеми на основі еліптичної кривої отримують все більше поширення. Вони володіють деякими перевагими, особливо при використанні в пристроях з малопотужними процесорами та обмеженим обсягом оперативної пам'яті. Типовими галузями застосування таких криптосистем є застосування: m-commerce - мобільна торгівля (WAP, стільникові телефони, кишенькові комп'ютери); смарт-

карти (наприклад, EMV); e-commerce - електронна торгівля і банківські операції (наприклад, SET); Інтернет-додатки (наприклад, в протоколі SSL) тощо.

1.2.2 Стеганографічні методи

В той час коли метою криптографії є збереження в таємниці семантики переданих повідомлень, методи стеганографії спрямовані на збереження в таємниці самого факту передачі такого повідомлення [25].

На сьогодні умовно виділяють наступні напрямки стеганографії:

- класична стеганографія, яка включає в себе «некомп'ютерні методи» приховування повідомлень неелектричної природи;

- комп'ютерна стеганографія, що передбачає використання властивостей форматів даних, які обробляються і передаються в інфокомунікаційних мережах;

- цифрова стеганографія, що основується на введенні надлишковості в передані мультимедійні дані, які представлені в цифровому вигляді, але по суті своїй мають аналогову природу (зображення, відео, звук).

Прихованої, або стеганографічною, передачею інформації називають процеси, що реалізують методи передачі інформації, при яких можлива передача додаткових даних, представлених в цифровому вигляді, що використовуються як контейнер, переважно за рахунок введення надлишковості.

Під контейнером, в який упаковується деякий об'єктом даних, розуміють такі цифрові дані, використання надлишковості в яких дозволяє передавати додаткову інформацію, не виявляючи факту передачі. Контейнер, що не містить додаткової інформації, називають порожнім, в іншому випадку – заповненим стегоконтейнером.

Методи та засоби вбудовування та вилучення додаткової інформації без порушення цілісності контейнера споживачем дозволяє говорити про формування прихованого стеганографічного каналу передачі інформації.

Стеганографічною системою, або стегосистемою, називають сукупність засобів і методів передачі і прийому порожнього контейнера, які функціонують взаємопов’язано із засобами для створення прихованого каналу передачі інформації.

Рівень приховання, або стеганографічна стійкістю, визначається можливими діями (атаками) порушника щодо стегосистеми. Залежно від цілей організації стегосистеми під скритністю розуміється стійкість такого до факту виявлення, або стійкість спробі видалення або руйнування стегоповідомлення, коли факт його існування не є таємницею для порушника. При цьому в першому випадку атаки, що здійснюється умовним порушником, матимуть пасивний характер, і можуть виражатися в проведенні наступних дій:

- візуальний контроль з метою суб’єктивної оцінки якості відеоданих;
- об’єктивний контроль відеоданих за одним або декількома обраними параметрами оцінки якості зображень.

У другому випадку очікуються геометричні атаки стегоповідомленнь: поворот, масштабування, стиснення тощо.

1.2.3 Захист програм і даних

Актуальність завдання аналізу програмних реалізацій алгоритмів захисту обумовлюється наступними факторами:

- комп’ютеризація всіх галузей діяльності: в даний час комп’ютерні технології активно застосовуються практично у всіх нових сферах нашого життя. Автоматизовані засоби обробки інформації використовуються як у державних установах управління, так і в численних підприємствах і організаціях, банках тощо. Практично кожна організаціям має у своєму розпорядженні конфіденційну інформацію, яка потребує захисту;

- різноманіття програмних засобів обробки інформації та засобів захисту, що в них використовуються. Засоби захисту вбудовуються в велику кількість програмних продуктів різного призначення (операційні системи, системи управління бази даних, системи електронного документообігу, різноманітні утиліти тощо). Тому часто детальний технічний опис, а також дані незалежних експертиз якості системи захисту, яка використовується, далеко не завжди доступні користувачеві;

- регулярна поява нових версій програмних продуктів, які можуть відрізнятися і засобами захисту. Сучасні засоби обробки інформації – сфера діяльності, що надзвичайно швидко розвивається, тому перевірка надійності засобів захисту інформаційної системи не може розглядатися як короткочасний епізод в житті організації. До цього питання доводиться повертатися неодноразово, в зв'язку з чим варто задача розробки ефективних засобів аналізу, максимальної автоматизації найбільш трудомістких його етапів.

Аналіз програмного забезпечення включає в себе три основні етапи.

- первинне знайомство з аналізованою програмою;
- вивчення доступної документації;
- планування та огранізація роботи щодо подальшого дослідження;
- відновлення алгоритмів функціонування програми;
- написання тестових програм та перевірка отриманих результатів.

В даний час сформувалися такі підходи до відновлення алгоритмів, що реалізуються програмою:

- метод експериментів;
- статичний метод;
- динамічний метод.

Експериментальний метод аналізу програм передбачає розгляд програми, що аналізується як «чорний ящик», який здійснює певні перетворення в залежності від вхідних даних. Проводяться багаторазові експерименти із маніпуляцією вхідними

даними, аналізуються і порівнюються отримані результати. На основі цих експериментів відновлюється алгоритми перетворень.

Статичний метод полягає у відновленні основних елементів програмного забезпечення на основі файлів програм з метою подальшого аналізу та отримання алгоритму захисту. Основним інструментом статичного методу є програми дизасемблера, що відновлюють вихідний код виконуваних файлів.

У випадку динамічного методу аналізу, програма, або сценарій виконується під контролем інших спеціалізованих програмних засобів. Завдяки чому можливе виконання програм у покроковому режимі та зупинка роботи внаслідок тих чи інших подій, що значно полегшує пошук і аналіз фрагментів програми, які реалізують перетворення, пов’язані із захистом інформації. Основним інструментом динамічного методу є так звані програми-дебагери. Разом з тим можуть використовуватися і інші програмні засоби.

Вищезазначені методи мають свої переваги і недоліки і багато в чому доповнюють один одного та використовуються в комплексі. Так, при реалізації динамічного методу нерідко проводиться вивчення окремих функцій аналізованої програми, як і в методі експериментів з «чорним ящиком». Деякі методи автоматизації статичного методу допускають емуляцію виконання окремих процедур процесором в режимі інтерпретатора з метою ідентифікації алгоритмів за результатами їх реалізації.

Щодо застосування методів нелінійної динаміки та теорії хаосу в засобах захисту програмного забезпечення та серверів баз даних від кібератак, варта відзначити перспективність використання моделей хаотичних систем в алгоритмах шифрування з метою криптозахисту.

Насамперед на базі шифрування даних хаосом можна організувати захищені канали зв’язку, наприклад такі, що можуть бути використані для побудови приватних конфіденційних локальних обчислювальних мереж із розмежуванням прав доступу користувачів.

1.4 Висновки до першого розділу та постановка задачі дослідження

В першому розділі магістерської роботи було проведено огляд існуючих методів та підходів щодо застосування теорії хаосу в системах телекомунікації.

Актуальність теми магістерського дослідження обумовлена проблемою захисту інформації, яка передається каналами зв’язку в телекомунікаційних системах.

Аналіз літературних джерел наукових періодичних видань показав, що хаотичні системи можуть бути ефективно використані для конфіденційної передачі аналогових та цифрових систем.

Сьогодні з метою забезпечення конфіденційності повідомлень, що передаються відкритими каналами зв’язку, використовуються криптографічні методи для шифрування. За допомогою методів стеганографії здійснюється приховання самого факт передачі інформації. Також корисними з точки зору захисту інформації можуть бути хаотичні сигнали, зокрема, вони можуть бути використані для прихованої передачі інформації на основі методу хаотичного маскування. Іншим прикладом застосування хаосу є генерування дискретними динамічними системами псевдовипадкових числових послідовностей для використання в алгоритмах шифрування.

Постановка задачі дослідження полягає у вирішення таких проблем:

- аналіз методів та існуючих рішень щодо використання детермінованого хаосу для передачі інформації;
- аналіз математичних моделей динамічних систем, які можуть генерувати хаос;
- вибір засобів та алгоритмів для чисельного розрахунку та моделювання нелінійних систем;
- моделювання синхронно зв’язаних хаотичних систем

- моделювання процесу передачі сигналів за допомогою хаотичних систем
- розробка алгоритму та програмна реалізація шифрування даних дискретними хаотичними послідовностями.

В якості математичної моделі було обрано систему Лоренца [1, 3].

Для вирішення поставлених задач передбачається використання методів дослідження: математичного аналізу, нелінійної динаміки, математичного моделювання, алгоритмізації і програмування, теорії електричних кіл та сигналів.

2 МАТЕМАТИЧНІ МОДЕЛІ ДИНАМІЧНИХ СИСТЕМ ІЗ ХАОТИЧНОЮ ПОВЕДІНКОЮ

2.1 Системи Лоренца та Реслера

Першою динамічною системою, при чисельному дослідженні якої були отримано нетривіальні розв'язки для її змінних і виявлено нетипову поведінку та високу чутливість до початкових умов, є фізична модель конвекції потоків газів та рідин під час їхнього нагрівання [4]. Дана система вперше була досліджена Е. Лоренцом в 1963 р.

Аналітично система Лоренца описується наступними диференційними рівняннями:

$$\begin{cases} \dfrac{dx}{dt} = \sigma\left(y - x\right) \\ \dfrac{dy}{dt} = rx - y - xz \\ \dfrac{dz}{dt} = xy - bz \end{cases} \tag{2.1}$$

де σ, r, b – параметри системи.

Класичним набором параметрів, для яких проводиться дослідження системи Лоренца є: $\sigma = 10$, $r = 28$, $b = 8/3$. На рисунку 2.1 зображено хаотичний атрактор системи Лоренца та часову діаграму сигналу $x(t)$.

Іншим класичним прикладом системи з хаосом, яка описує динаміки хімічних реакцій, що відбуваються в деякій суміші з перемішуванням, є система Реслера. Дана аналітична модель була запропонована німецьким вченим і дослідником

О. Реслером в 1976 році як проста система з хаотичною поведінкою, що могла б описати деякі хімічні процеси.

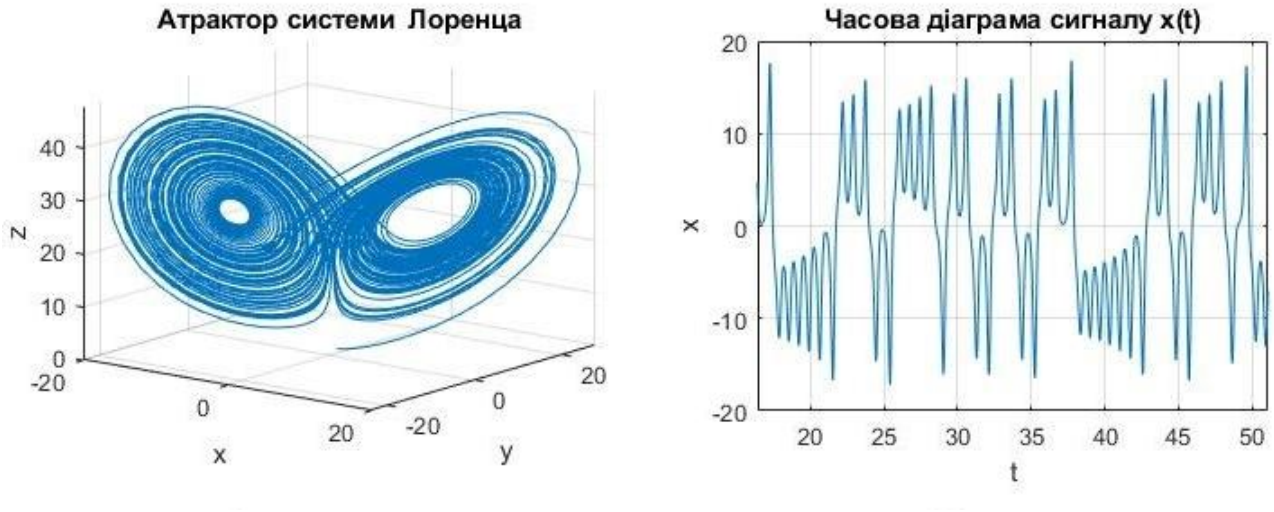


Рисунок 2.1 – Атрактор системи Лоренца та часова діаграма сигналу $x(t)$

Система Реслера описується наступними диференційними рівняннями:

$$\begin{cases} \dfrac{dx}{dt} = -y - x \\ \dfrac{dy}{dt} = x + ay \\ \dfrac{dz}{dt} = b + z(x - c) \end{cases} \tag{2.2}$$

де a, b, c – параметри системи.

Відомо [1], що для значень параметрів системи $a = 0{,}2$; $b = 0{,}2$ та $2{,}6 \leq c \leq 4{,}2$ система демонструє граничний цикл з каскадом подвоєння періодів. При $c > 4.2$ виникає хаотичний атрактор системи.

В хаотичному режимі часова залежність змінних *x*, *y* мають шумоподібну форму коливання.

На рисунку 2.2 зображено хаотичний атрактор та часову діаграму сигналу координати *x*(*t*). системи Реслера, отримані для значень параметрів $a = 0{,}2$; $b = 0{,}2$ та $c = 6{,}5$.

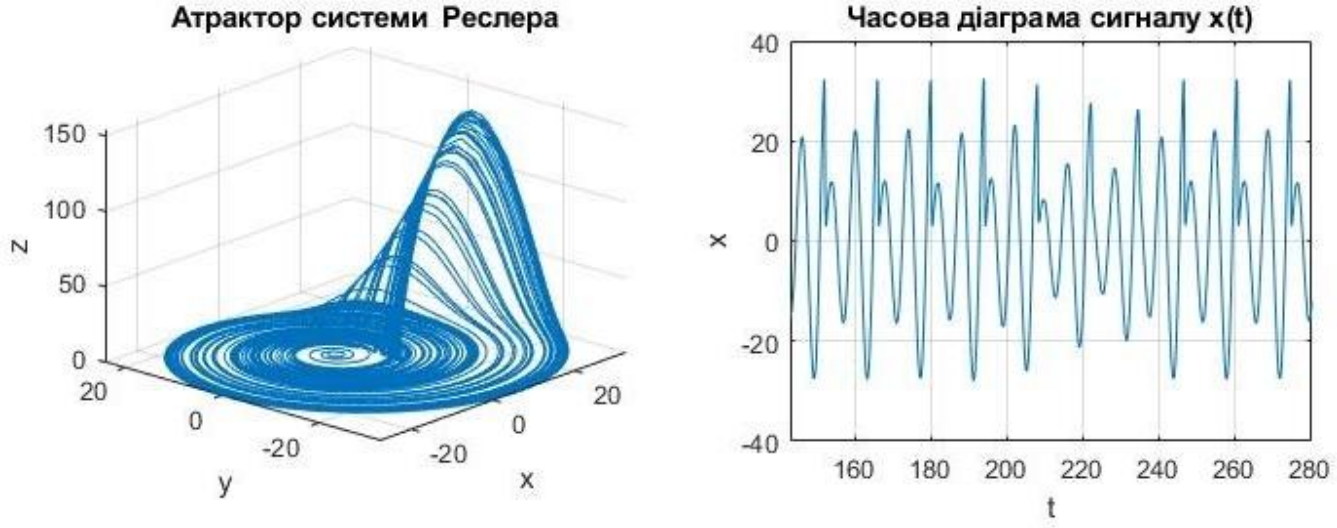


Рисунок 2.2 – Атрактор системи Реслера та часова діаграма сигналу *x*(*t*)

Системи Лоренца та Реслера є класичними прикладами моделей з хаотичною динамікою, що демонструють велику кількість динамічних режимів та сильну залежність від початкових умов. Існує багато варіантів схемотехнічної реалізації систем Реслера та Лоренца, що побудовані на основі рівнянь (2.1) та (2.2) відповідно [1-5].

2.2 Генератор Дуффінга-Холмса

Рівняння Дуффінга-Холмса описує квазіперіодичну коливальну систему з кубічним типом нелінійності, яка при деяких значеннях параметрів системи демонструє хаотичну поведінку.

Вигляд рівняння Дуффінга-Холмса наступний:

$$\frac{d^2x}{dt^2} + \delta\frac{dx}{dt} + x\left(x^2 - 1\right) = \lambda\cos\omega t \tag{2.3}$$

де δ, λ, ω – параметри системи.

Ввівши заміну $y = dx/dt$, диференціальне рівняння другого порядку (2.3) можна представити у вигляді системи рівнянь першого порядку:

$$\begin{cases} \dfrac{dx}{dt} = y \\ \dfrac{dy}{dt} = x\left(1 - x^2\right) - \delta y + \lambda\cos\omega t \end{cases} \tag{2.4}$$

На рисунку 2.3 зображено хаотичний атрактор та часову діаграму сигналу координати $x(t)$. системи Дуффінга-Холмса, отримані для значень параметрів $\delta = 0{,}08$, $\lambda = 0{,}1$ та $\omega = 0{,}8$.

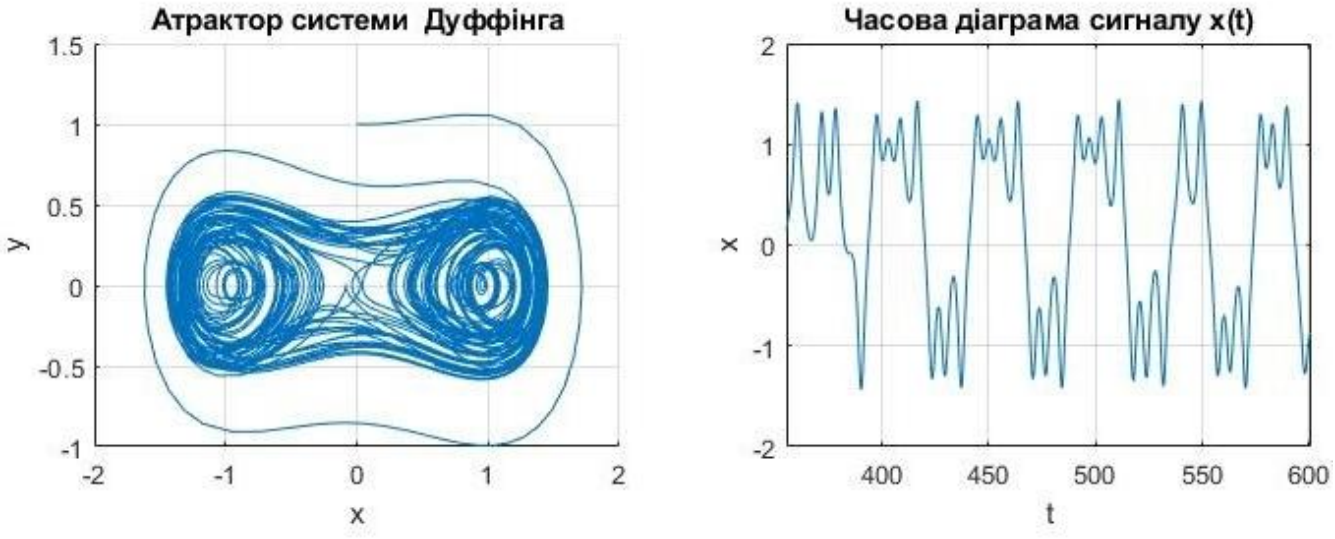


Рисунок 2.3 – Атрактор системи Дуффінга-Холмса та часова діаграма сигналу $x(t)$

2.3 Схема Чуа

На рисунку 2.3 зображена схема Чуа, яка складається з двох конденсаторів, однієї котушки індуктивності, лінійного резистора та нелінійного єлементу, який ще називають діодом Чуа. Схема була запропонована Леоном Чуа в 1983 році.

Вольт-амперна характеристика (ВАХ) нелінійного елементу схеми Чуа має вигляд кусково-неперервної функції, вид якої показано на рисунку 2.5.

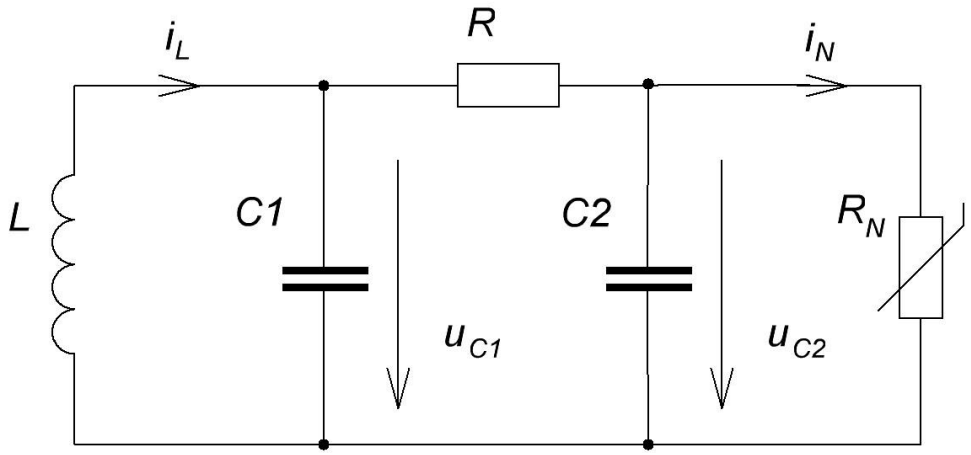


Рисунок 2.4 – Електрична схема генератора Чуа

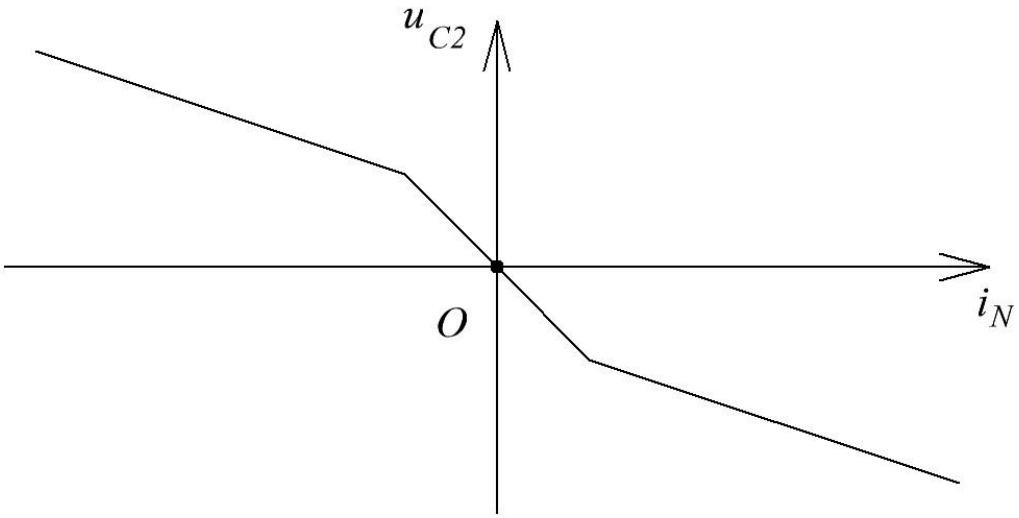


Рисунок 2.5 – Вольт-амперна характеристика нелінійного елемента схеми Чуа

Описавши схему Чуа (рисунок 2.3, а) за допомогою законів Кірхгофа, отримаємо наступну систему диференційних рівнянь:

$$\begin{cases} C_1 \dfrac{du_{C1}}{dt} = \dfrac{u_{C2} - u_{C1}}{R} + i_L \\ C_2 \dfrac{du_{C1}}{dt} = \dfrac{u_{C1} - u_{C2}}{R} - i_N \\ L \dfrac{di_L}{dt} = -u_{C2} \end{cases} \tag{2.5}$$

де u_{C1} та u_{C2} – напруги на конденсаторах C_1 та C_2 відповідно;

i_L – струм, що протікає через котушку індуктивності L,

$i_N = f(u_{C2})$ – струм, що протікає через нелінійний елемент R_N.

Для системи (2.5) можна виконати масштабування за часом RC_1, RC_2 або $\sqrt{LC_2}$ шляхом замін $t' = t/(RC_1)$, $t' = t/RC_2$, і $t' = t/\sqrt{LC}$ відповідно.

В результаті нормування часу на RC_1 та RC_2 отримаємо систему диференційних рівнянь в безрозмірних змінних з трьома параметрами, а за нормування на $\sqrt{LC_2}$ система описуватиметься чотирма параметрами.

Система Чуа для безрозмірних коефіцієнтів має вигляд:

$$\begin{cases} \dot{x} = \alpha(y - x - f(x)) \\ \dot{y} = x - y + z \\ \dot{z} = -\beta y - \gamma z \end{cases} \tag{2.6}$$

де α, β, γ – параметри системи.

Функція $f(x)$ є аналітичним переставленням ВАХ нелінійного елементу діода Чуа (з урахуванням введених коефіцієнтів масштабування):

$$f(x) = m_0 x + \frac{1}{2}(m_1 - m_0)\left(|x+1| + |x-1|\right) \qquad (2.6)$$

де k_0 та k_1 – деякі масштабні коефіцієнти.

На рисунку 2.4 зображено хаотичний атрактор системи Чуа, отриманий при вказаних значеннях параметрів, а також часову діаграму, спектр, та автокореляційну функцію для сигналу $x(t)$.

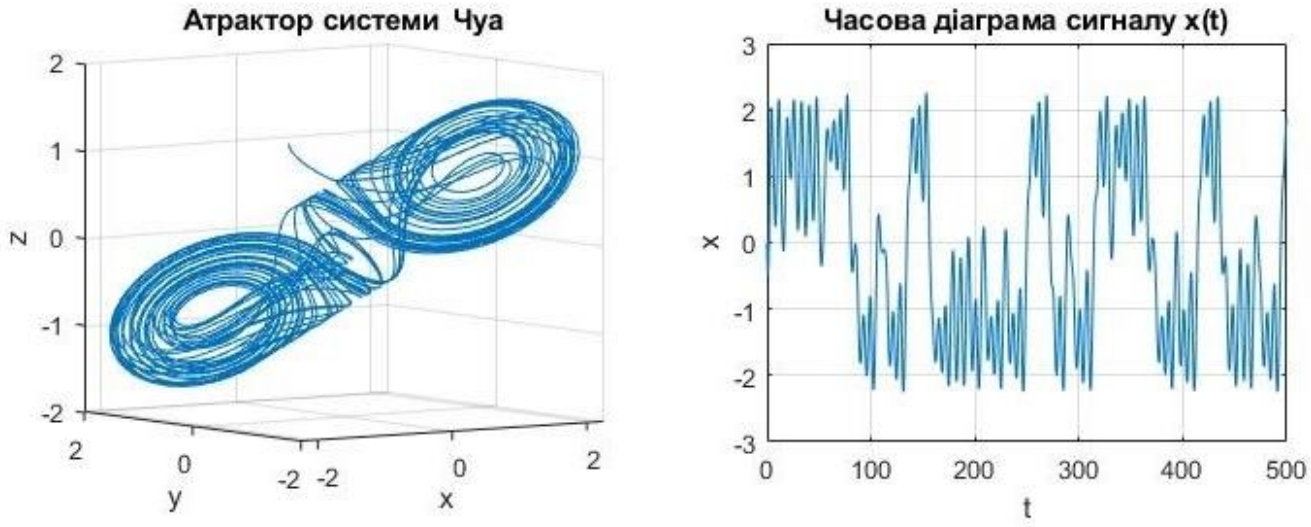


Рисунок 2.8 – Атрактор системи Чуа та часова діаграма сигналу $x(t)$

Генератор Чуа демонструє хаотичку поведінку в досить вузькій області значень його параметрів. Із наближенням до хаотичного режимом, система показує цикл подвоєнь періоду аж до утворення хаотичного аттрактора.

Оскільки діод Чуа реалізується на операційних підсилювачах, він має обмежений динамічний діапазон і тому в системі існує також великий за розмірами стійкий граничний цикл, що охоплює всі ділянки ВАХ діода Чуа.

2.4 Висновки до другого розділу

В другому розділі магістерської роботи було проведено огляд найвідоміших динамічних систем, які за деяких умов можуть показувати хаотичну поведінку.

Класичними прикладами систем із хаосом є системи Лоренца та Реслера. Вони відіграють важливу роль в історії розвитку теорії хаосу як науки та в процесі вивчення відповідних навчальних дисциплін оскільки наглядно показують, що реальні фізичні процеси бувають хаотичними.

З іншого боку – рівняння Дуффінга-Холмса є суто математичною моделлю із нестійкістю розв’язки. Однак на його базі можуть бути побудовані реальні фізичні пристрої та системи, пов’язані із генерацією та обробкою хаотичних сигналів. Схема Чуа є прикладом практичної реалізації хаотичної системи у вигляді електричного кола.

Усі представлені в другому розділі математичні моделі нелінійних систем володіють наступними ключовими властивостями (що притаманні усім системам з хаосом):

- часові реалізації сигналів є шумуродібними;

- спектр, усіх досліджених хаотичних сигналів займає достатньо широку область частот, тобто дані сигнали є широкосмуговими;

- автокореляційна функція (АКФ) хаотичних сигналів має яскраво виражений максимум, що дозволяє виявляти сигнали з однаковою хаотичною поведінкою.

Системи рівнянь (2.1) – (2.6) такі, що не можуть бути розв’язані аналітично в явному вигляді, тому для їх дослідження необхідно використовувати обчислювальні методи.

Одними із таких методів є метод розв’язування диференціальних рівнянь та їх систем Рунге-Кутти [37]. Даний метод може бути реалізований за допомогою

імперативних алгоритмічних мов програмування, наприклад, вбудованій мові програмної системи MATLAB.

В якості математичної моделі нелінійної системи із хаосом, яка буде використана для дослідження явища синхронізації та передачі інформаційних сигналів, було обрано систему Лоренца (2.1).

3 АНАЛІЗ ТА МАТЕМАТИЧНЕ МОДЕЛЮВАННЯ ДИНАМІЧНОЇ СИСТЕМИ ЛОРЕНЦА

3.1 Обчислювальні методи розв’язування диференціальних рівнянь та їх систем засобами MATLAB/Simulink

3.1.1 Метод Рунге-Кутти

Для чисельного розв’язку систем диференціальних рівнянь із заданими початковими умовами (розв’язку задачі Коші) скористаємось методом Рунге-Кутти четвертого порядку.

Нехай задана деяка система диференціальних рівнянь у векторній формі:

$$\frac{d\bar{Y}}{dt} = \bar{F}\left(t, \bar{Y}\right), \tag{3.1}$$

та вектор початкових умов:

$$\bar{Y}\left(0\right) = \bar{Y}_0 \tag{3.2}$$

Тоді наближене значення вектору $\bar{Y}$ в точках обчислюється згідно наступної ітеративної формули:

$$\bar{Y}_{n+1} = \bar{Y}_n + \frac{h}{6}\left(\bar{k}_1 + 2\bar{k}_2 + 2\bar{k}_3 + \bar{k}_4\right), \tag{3.3}$$

де h – розмір кроку за часом t,

$\bar{k}_1 \cdots \bar{k}_4$ – проміжні значення.

Значення коефіцієнтів $\bar{k}_1 \cdots \bar{k}_4$ розраховуються за формулами:

$$\begin{gathered} \bar{k}_1 = \bar{F}\left(t_n, \bar{Y}_n\right) \\ \bar{k}_2 = \bar{F}\left(t_n + \frac{h}{2}, \bar{Y}_n + \frac{h}{2}\bar{k}_1\right) \\ \bar{k}_3 = \bar{F}\left(t_n + \frac{h}{2}, \bar{Y}_n + \frac{h}{2}\bar{k}_2\right) \\ \bar{k}_4 = \bar{F}\left(t_n + h, \bar{Y}_n + h\bar{k}_3\right) \end{gathered} \tag{3.4}$$

Для розв'язку задачі Коші для одновимірних систем, які описуються одним диференціальним рівнянням $\frac{dx}{dt} = f\left(t, x\right)$ з початковими умовами $x\left(0\right) = x_0$ використовуються скалярні аналоги формул (3.3) та (3.4):

$$x_{n+1} = x_n + \frac{h}{6}\left(k_1 + 2k_2 + 2k_3 + k_4\right) \tag{3.5}$$

$$\begin{gathered} k_1 = f\left(t_n, x_n\right) \\ k_2 = f\left(t_n + \frac{h}{2}, x_n + \frac{h}{2}k_1\right) \\ k_3 = f\left(t_n + \frac{h}{2}, x_n + \frac{h}{2}k_2\right) \\ k_4 = f\left(t_n + h, x_n + hk_3\right) \end{gathered} \tag{3.6}$$

В системі MATLAB метод Рунге-Кутти представлений у вигляді функції ode45 з ключем «runge».

Блок-схема алгоритму Рунге-Кутти для розв'язку одновимірної системи, що складається з одного диференціального рівняння зображена на рисунку 3.1.

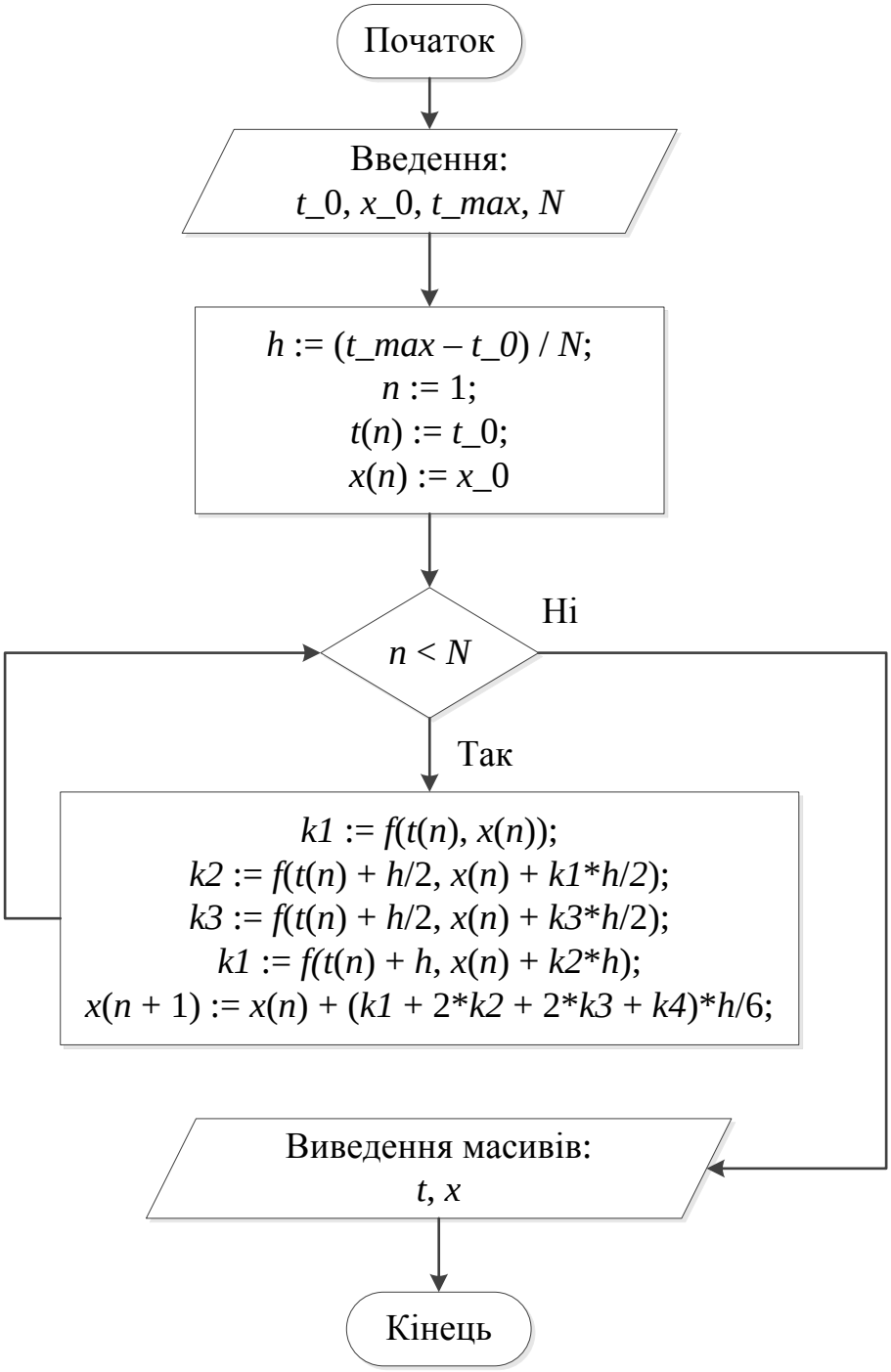


Рисунок 3.1 – Блок-схема алгоритму Рунге-Кутти

Розглянемо в якості прикладу диференціальне рівняння з заданими початковими умовами:

$$\frac{dx}{dt} = x \cdot t\,,\ x(0) = 1 \qquad (3.7)$$

Нижче наведений MATLAB-код, що реалізує алгоритм, який заданий виразами (3.5) і (3.6) та зображений на рисунку 3.1, на прикладі розв’язку диференціального рівняння (3.7).

```
f=@(t,x)t*x;
N = 10000;                          % кількість ітерацій
h = 1.0/(N - 1);                    % крок сітки
x(1) = 1; t(1) = 0;                 % початкові умови
for n = 1:(N - 1)                   % наближений розв’язок диф. рівняння
        k1 = f(t(n), x(n));
        k2 = f(t(n) + 0.5*h, x(n) + 0.5*h*k1);
        k3 = f(t(n) + 0.5*h, x(n) + 0.5*h*k2);
        k4 = f(t(n) + h, x(n) + h*k3);
        x(n + 1) = x(n) + (h/6)*(k1 + 2*k2 + 2*k3 +k4);
        t(n + 1) = n*h;
end
plot(t,x);grid on; xlabel('t, s'); ylabel('x(t)');          % побудова графіка розв’язку
```

Результат виконання програми показано на рисунку 3.2.

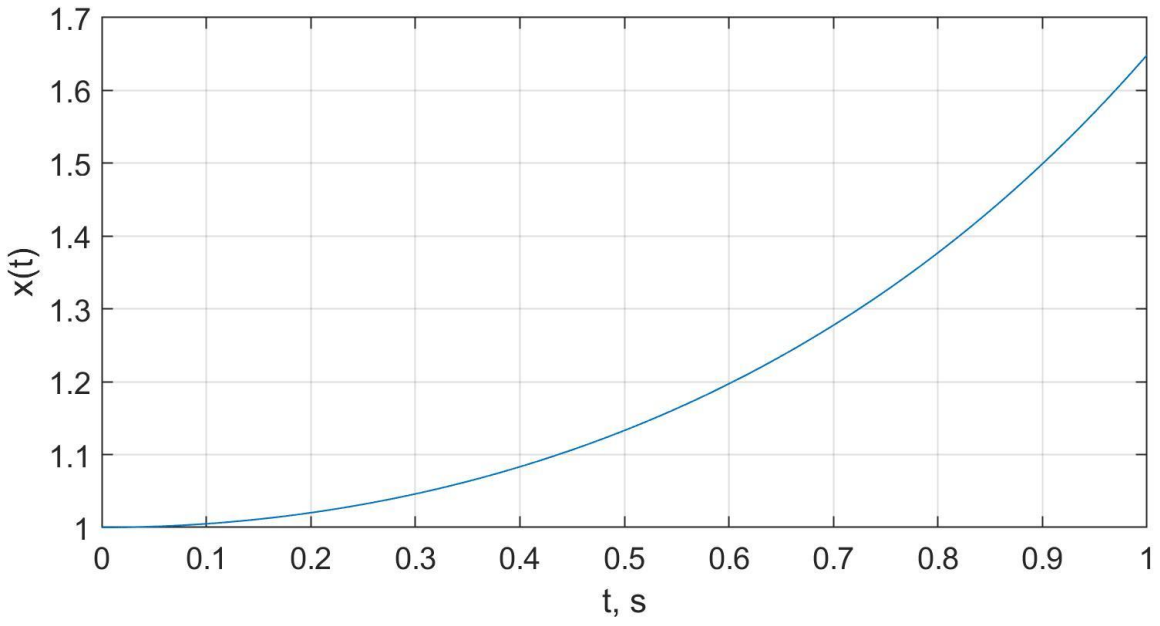


Рисунок 3.2 – Результат виконання алгоритму Рунге-Кутти на прикладі розв’язку диференціального рівняння (3.7)

3.1.2 Розв’язок диференціальних рівнянь динамічних систем в середовищі візуального моделювання Simulink

Програма Simulink, яка входить по пакету програм системи MATLAB, надає можливості візуального інтегрування диференціальних рівнянь та їх систем, а також здійснювати імітаційне моделювання динамічних систем в реальному часі.

На рисунку 3.3 показаний приклад розв’язування рівняння (3.7) за допомогою програми Simulink.

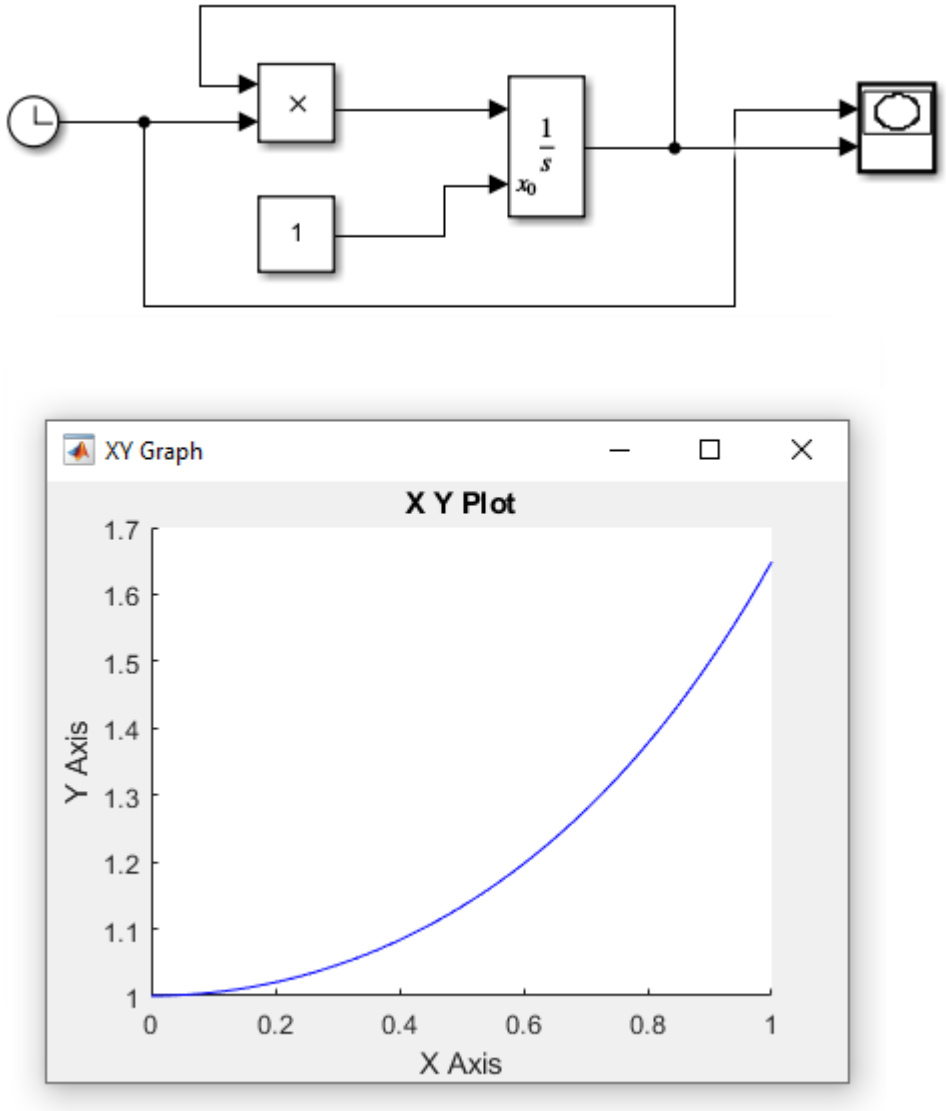


Рисунок 3.3 – Розв’язування диференціального рівняння (3.7) в програмі Simulink

Схема на рисунку 3.3 складається з наступних елементів:

- елемент Clock для явного задання часового вектору при моделюванні;

- модель Product, що використовується для перемноження двох вхідних сигналів;

- блок Constant, який представляє константу для вказання початкових умов для інтегратора;

- чисельний інтегратор – елемент Integrator. Виконує інтегрування за часом вхідного сигналу з урахуванням початкових умов;

- блок XY Graph – елемент для побудови двовимірних графіків.

Вибір чисельного алгоритму розв'язку, а також налаштування його параметрів здійснюються у відповідному вікні (рисунок 3.4).

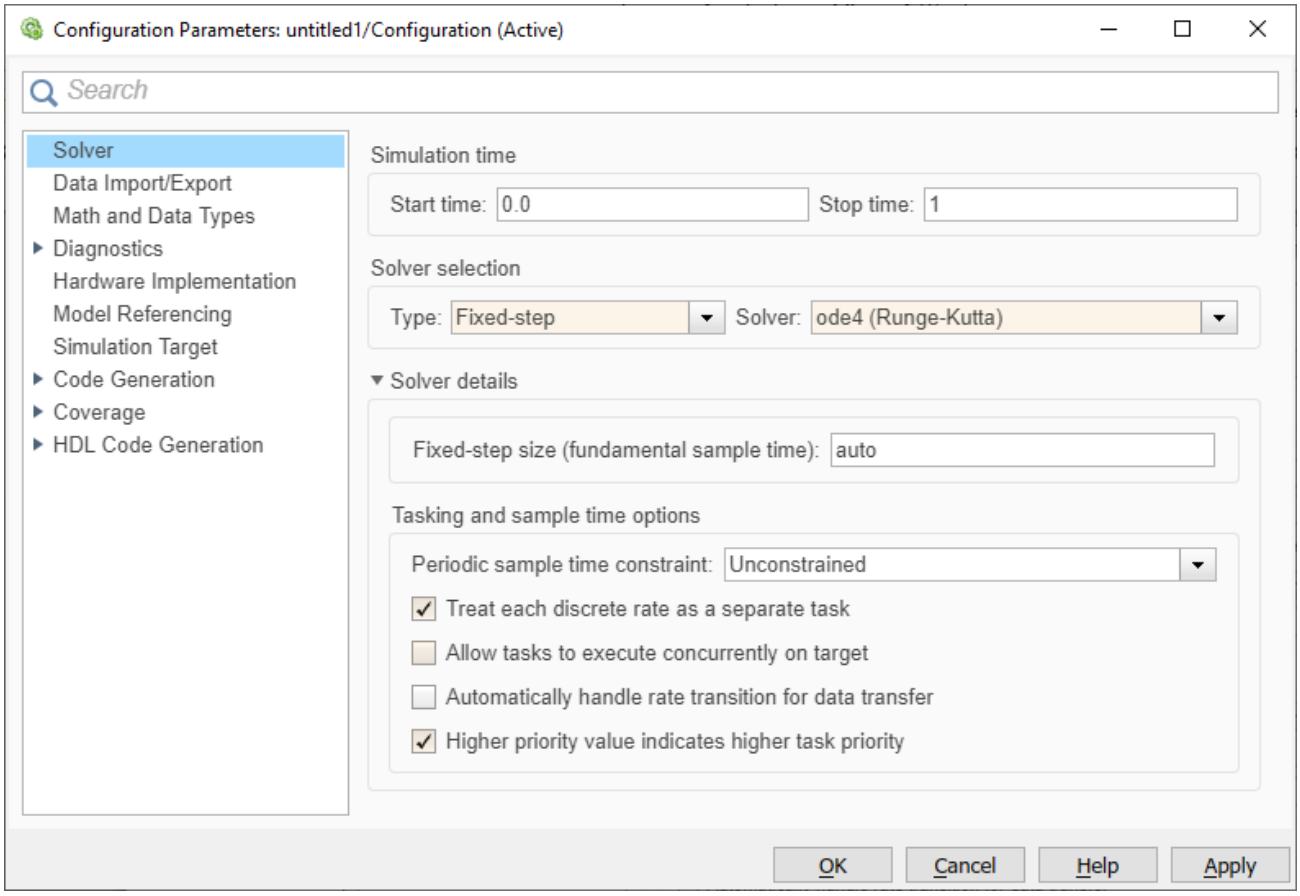


Рисунок 3.4 – Вікно налаштування параметрів чисельного алгоритму

3.1.3 Оцінка точності чисельного розв’язку диференціальних рівнянь

Використання обчислювальних методів, які базуються на ітеративних процедурах, завжди супроводжується похибками результатів обчислення. Для методу Рунге-Кутти, алгоритм якого був описаний в п.3.1.1, точність обчислення залежить від розміру кроку часової сітки, що також визначає кількість ітерацій головного циклу, а отже і обчислювальну складність відповідної процедури.

З метою оцінки точності обчислювального алгоритму було проведено багаторазове інтегрування диференціального рівняння (3.7) методом Рунге-Кутти з різним значенням кроку сітки.

Оцінка точності обчислень здійснюється згідно співвідношення:

$$\left|x\left(t_{end}\right)-u\left(t_{end}\right)\right| \le \mu \cdot h^4, \tag{3.8}$$

де $u\left(t_{end}\right)=e^{0,5t_{end}^2}$ – точне значення функції в момент $t=t_{end}$.

Значення μ в (3.8) не повинно залежати від кроку h. Залежність параметра μ від величини h зображений в логарифмічному масштабі на рисунку 3.5.

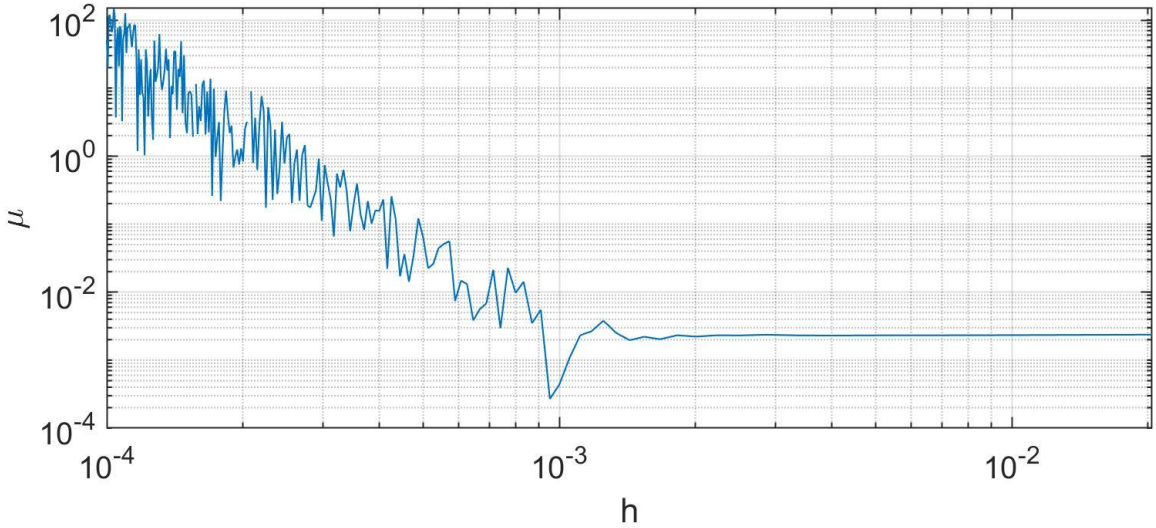


Рисунок 3.5 – Залежність параметру μ від величини кроку сітки h

3.2 Імітаційне моделювання та чисельний розв’язок системи Лоренца

3.2.1 Simulink-модель динамічної системи Лоренца

Simulink-модель системи Лоренца, побудована з математичних елементів відповідно до системи рівнянь (2.1), зображена на рисунку 3.6.

Схема на рисунку 3.3 складається з наступних елементів:

- базових математичних операторів алгебраїчної суми – Sum/Subtract та множення – Product;
- двох блоків підсилення сигналу Gain, за допомогою яких задається масштабування відповідних сигналів згідно значень параметрів системи (2.1);
- трьох чисельних інтеграторів, які призначені для інтегрування за часом відповідних рівнянь системи (2.1) з урахуванням початкових умов.

Для імітаційного моделювання динамічної системи Лоренца зі зміною параметра *r*, модель, що зображена на рисунку 3.6, була поміщена всередину модуля Sybsystem та доповнена елементами для відображення результатів моделювання (рисунок 3.7).

Simulink-модель, представлена у вигляді підсистеми, складається з таких елементів:

- блоки XY Graph – елементи для відображення атрактора системи на фазових площинах;
- елементу Scope для виведення часових діаграм результату моделювання;
- елементу Constant, який задає початкове значення керуючого параметру *r*.

Крім того, для задання параметрів моделі та початкових умов елемент Sybsystem був доповнений маскою, яка представляє собою вікно, що призначене для вводу налаштувань моделі.

Вікно налаштування параметрів системи Лоренца зображено на рисунку 3.8.

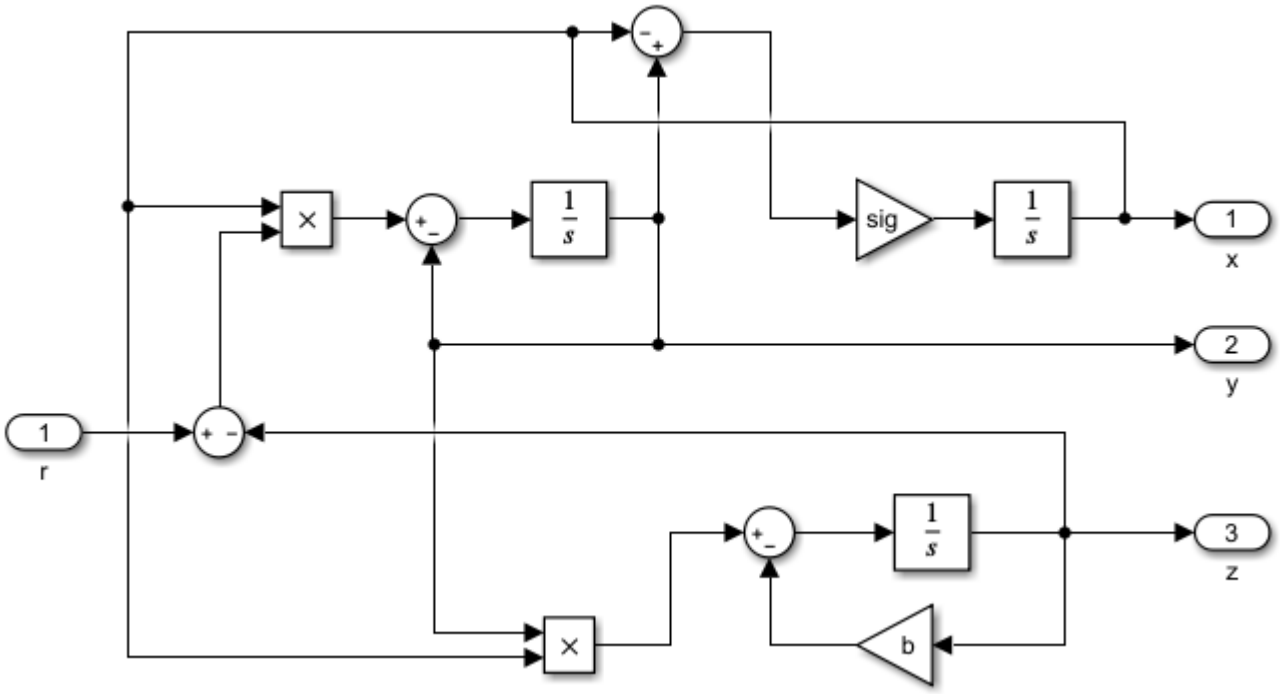


Рисунок 3.6 – Simulink-модель системи Лоренца

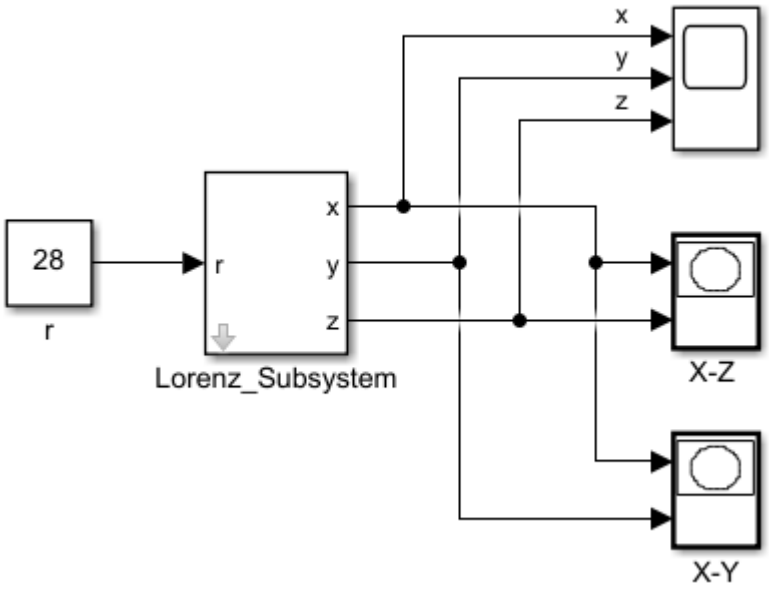


Рисунок 3.7 – Simulink-модель системи Лоренца, представленої у вигляді підсистеми (Subsystem) з керуючим елементом *r*

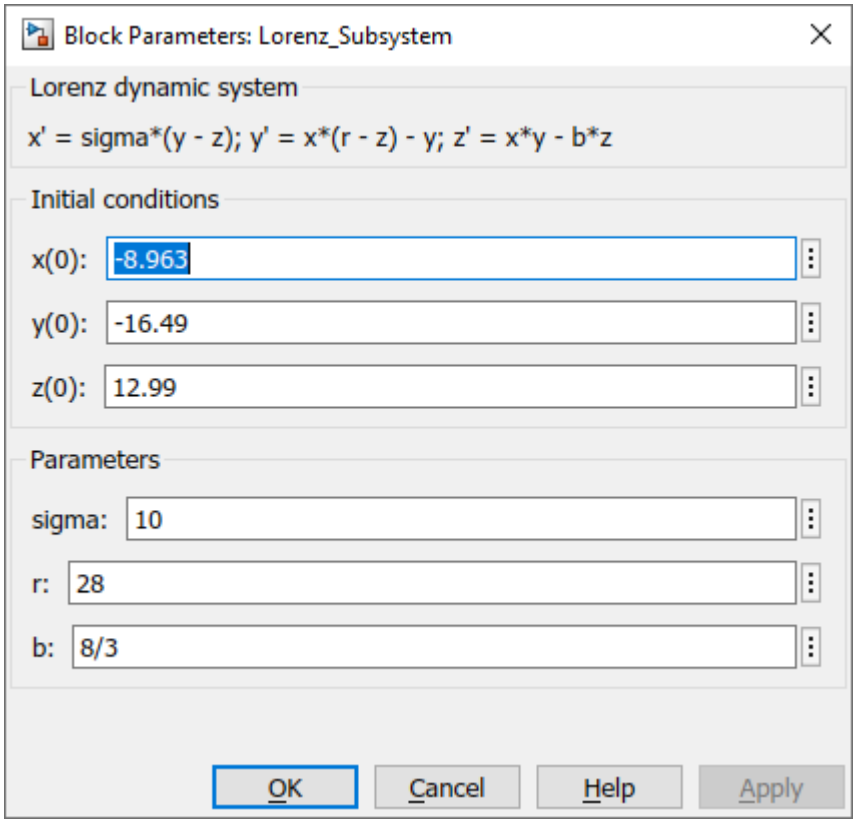


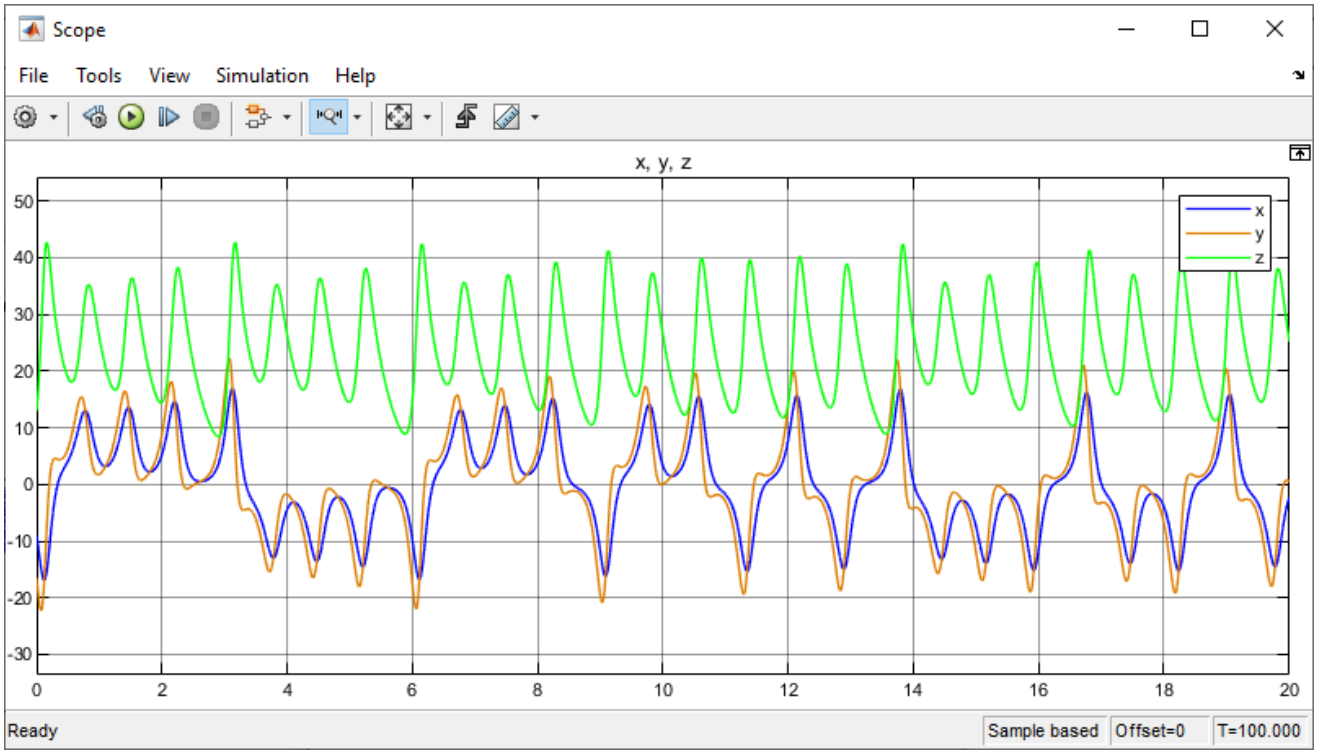
Рисунок 3.8 – Вікно налаштування параметрів моделі

Вікно налаштування параметрів, яке зображено на рисунку 3.8, дозволяє вказувати наступні параметри системи Лоренца:

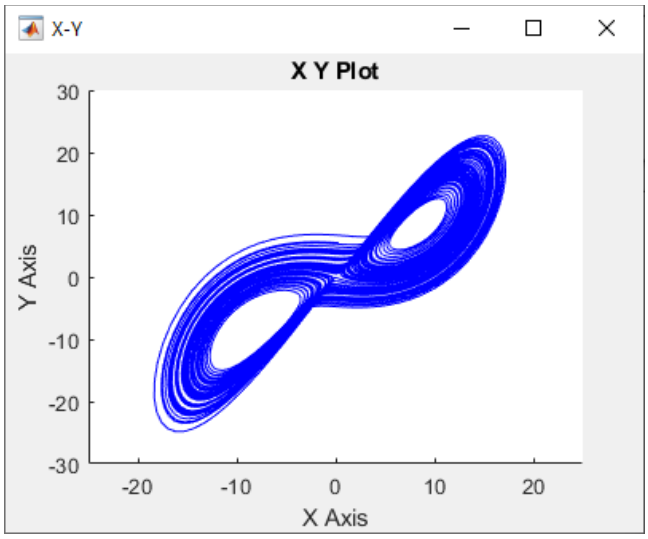
- початкове значення координати x в момент $t = 0$;
- початкове значення координати y в момент $t = 0$;
- початкове значення координати z в момент $t = 0$;
- значення параметру σ;
- значення параметру r;
- значення параметру b.

Результати моделювання системи Лоренца, схема якої зображена на рисунку 3.9, представлені на рисунку 3.9.

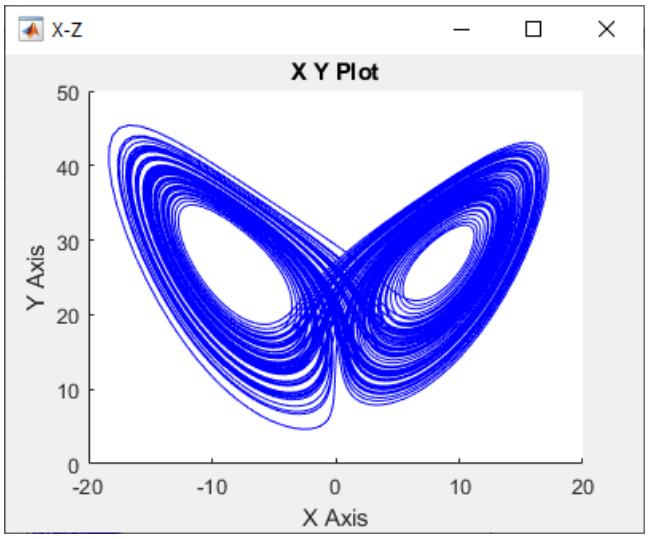
Блок Scope моделі призначений для графічного відображення часових залежностей вхідних сигналів.



а)



б)



в)

Рисунок 3.9 – Результати моделювання системи Лоренца в програмі Simulink:
часові діаграми сигналів *x*, *y*, *z* - а)
фазовий портрет атрактора на площині *x*-*y* – б),
портрет атрактора на площині *x*-*z* – в)

3.2.2 Чисельний розв’язок системи Лоренца

Даний розділ присвячений чисельному моделюванню динамічної системи Лоренца шляхом розв’язку її системи диференціальних рівнянь (2.1). Приводяться результати дослідження поведінки системи в залежності від значення керуючого параметра [38].

Система Лоренца має такі точки рівноваги: P_0 (0; 0; 0) – для довільних значень параметрів; $P_1\left(\sqrt{b(r-1)};\sqrt{b(r-1)};r-1\right)$ та $P_2\left(-\sqrt{b(r-1)};-\sqrt{b(r-1)};r-1\right)$ для значення $r > 1$.

Для $0 < r < 1$ точка P_0 – єдина точка рівноваги. Подальше збільшення значення параметра r призводить до наступних змін динаміки системи:

- вилкоподібна біфуркація після досягнення значення $r = 1$, що супроводжується втратою стійкості точки P_0 для $r \geq 1$ та появою пари стійких положень рівноваги P_1 та P_1;
- збільшення амплітуди фазових коливань відносно положень рівноваги із зростанням параметру r;
- перестроювання атрактора у фазовому просторі у разі $r \approx 13{,}927$ – за нульових початкових умов, здійснивши оберт навколо однієї з точок рівноваги, траєкторія повернеться у початок координат;
- руйнування гомоклінічних траєкторій та поява граничних циклів для $r > 13{,}927$, розмах коливань зменшується зі зростанням r, траєкторія приходить в одну з точок P_1, P_2;
- перестроювання атрактора після досягнення r ≈ 24,06, що супроводжується появою у фазовому просторі хаотичного атрактора;
- втрата стійкості точок P_1 або P_1 після досягнення значення r ≈ 24,74.

Фазові портрети часові діаграми $x(t)$ для різних значень параметра r, що відповідають характерним динамічним режимам показані на рисунках 3.10 – 3.17.

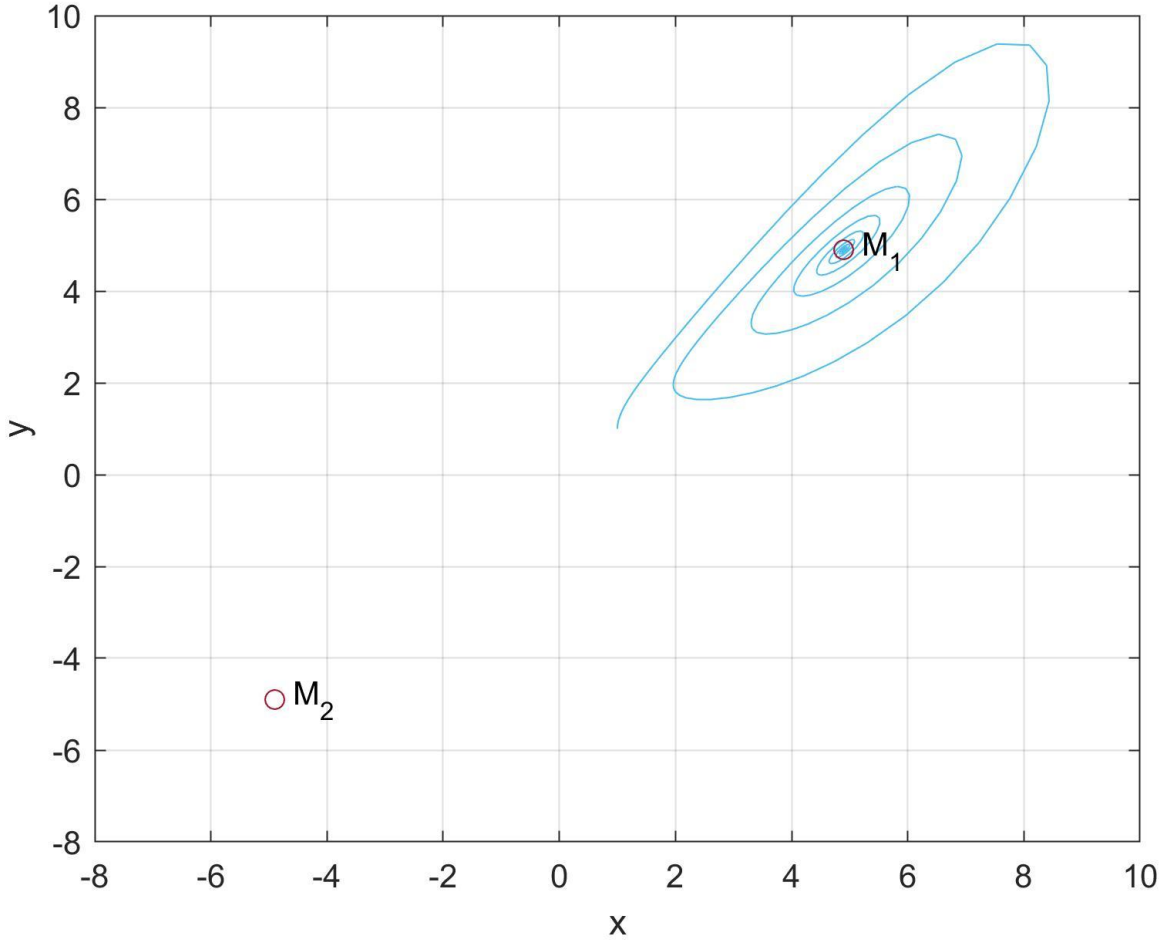


Рисунок 3.10 – Фазовий портрет атрактора системи Лоренца для значення r = 10

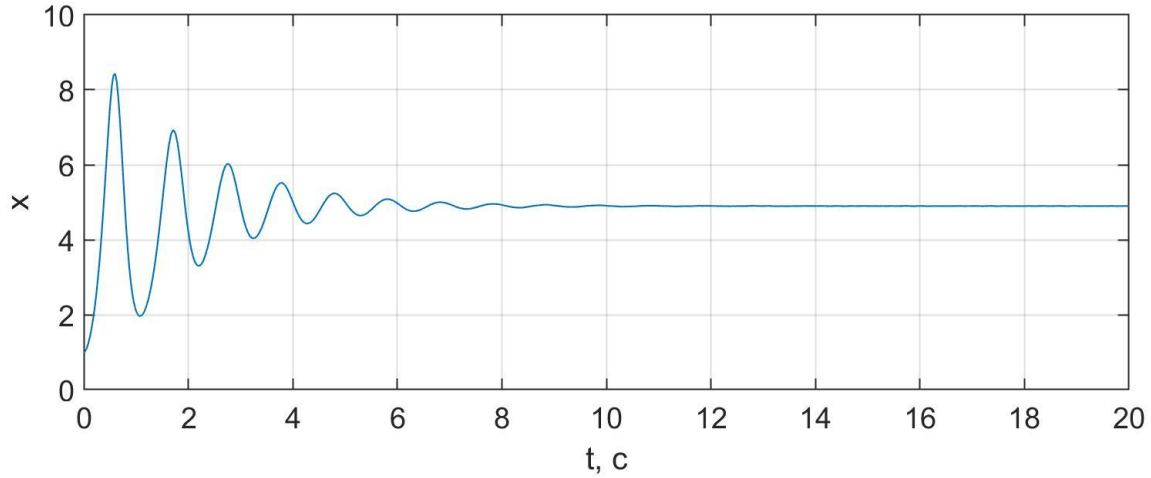


Рисунок 3.11 – Часовий графік сигналу $x(t)$ системи Лоренца для значення r = 10

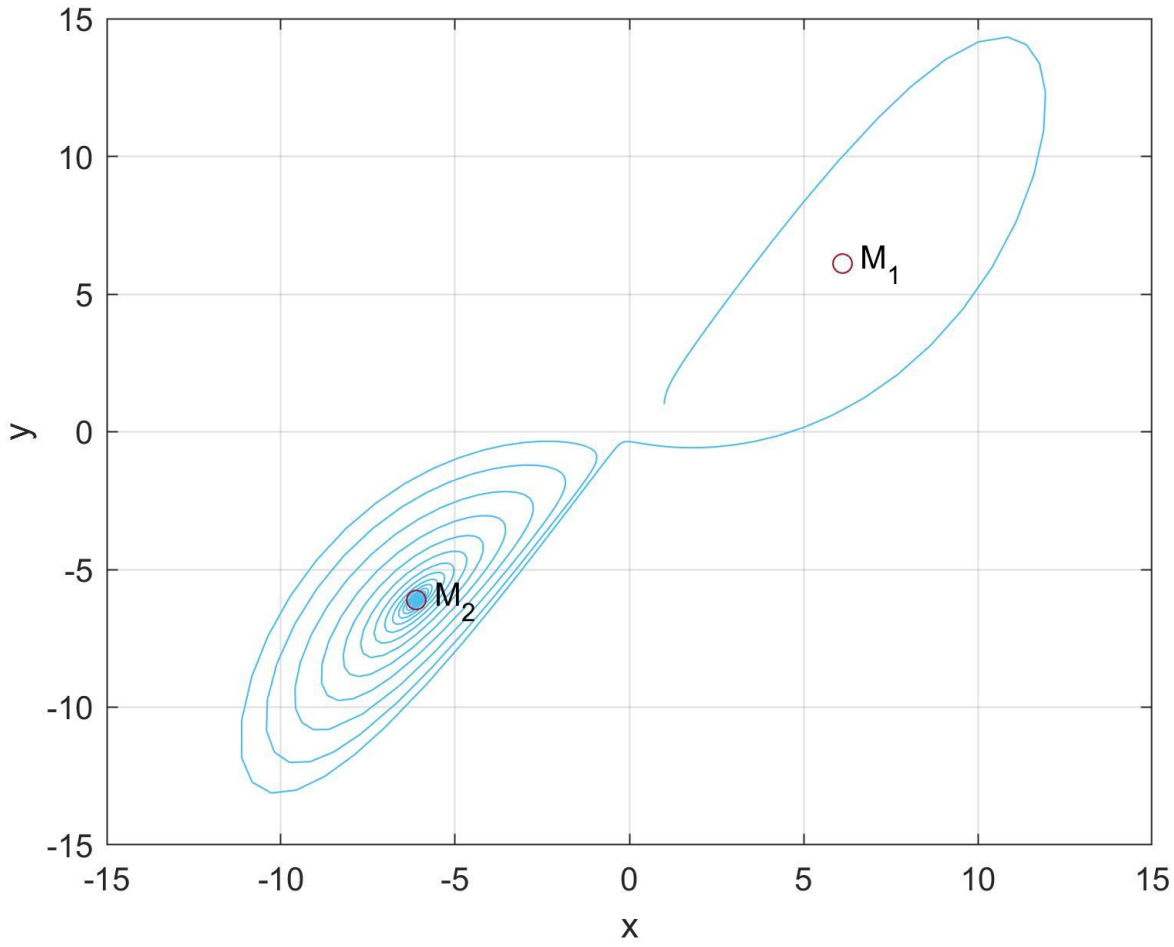


Рисунок 3.12 – Фазовий портрет атрактора системи Лоренца для значення r = 15

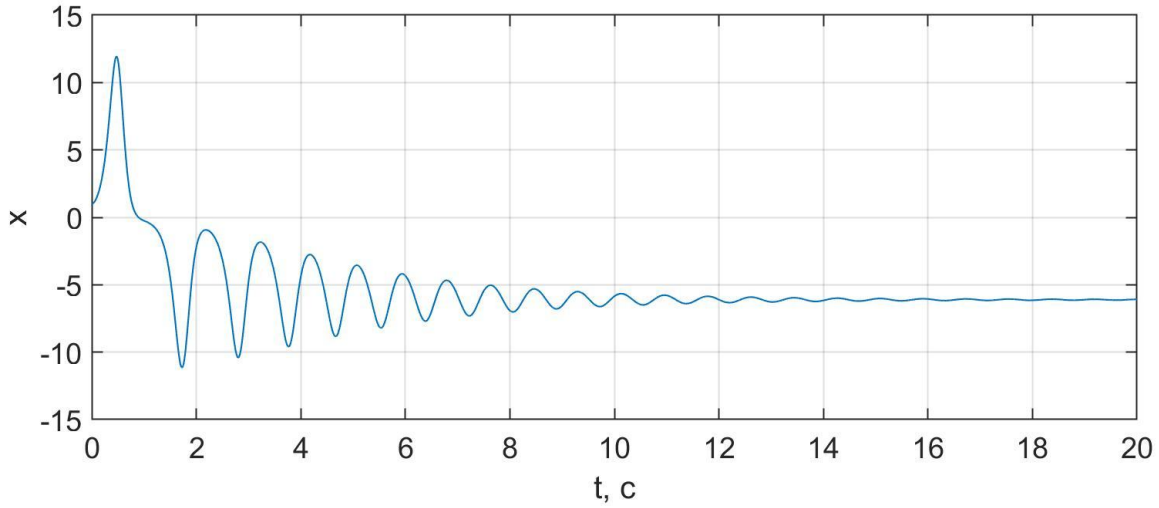


Рисунок 3.13 – Часовий графік сигналу $x(t)$ системи Лоренца для значення r = 15

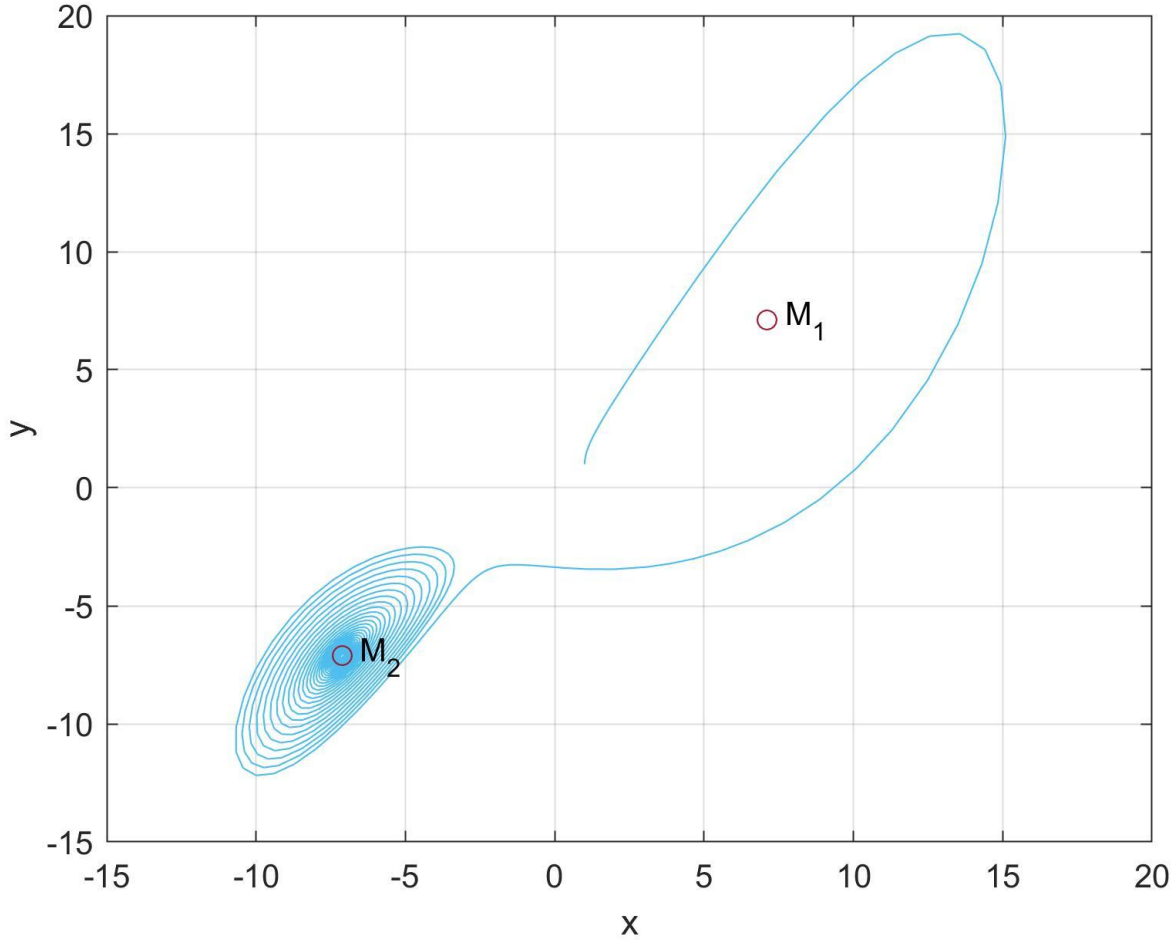


Рисунок 3.14 – Фазовий портрет атрактора системи Лоренца для значення r = 20

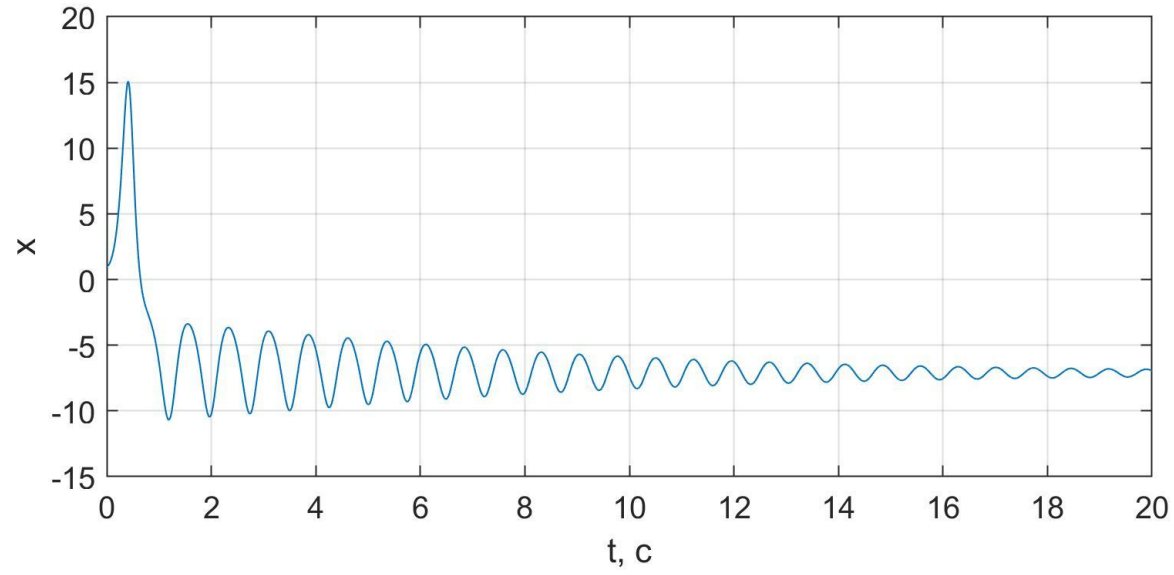


Рисунок 3.15 – Часовий графік сигналу $x(t)$ системи Лоренца для значення r = 20

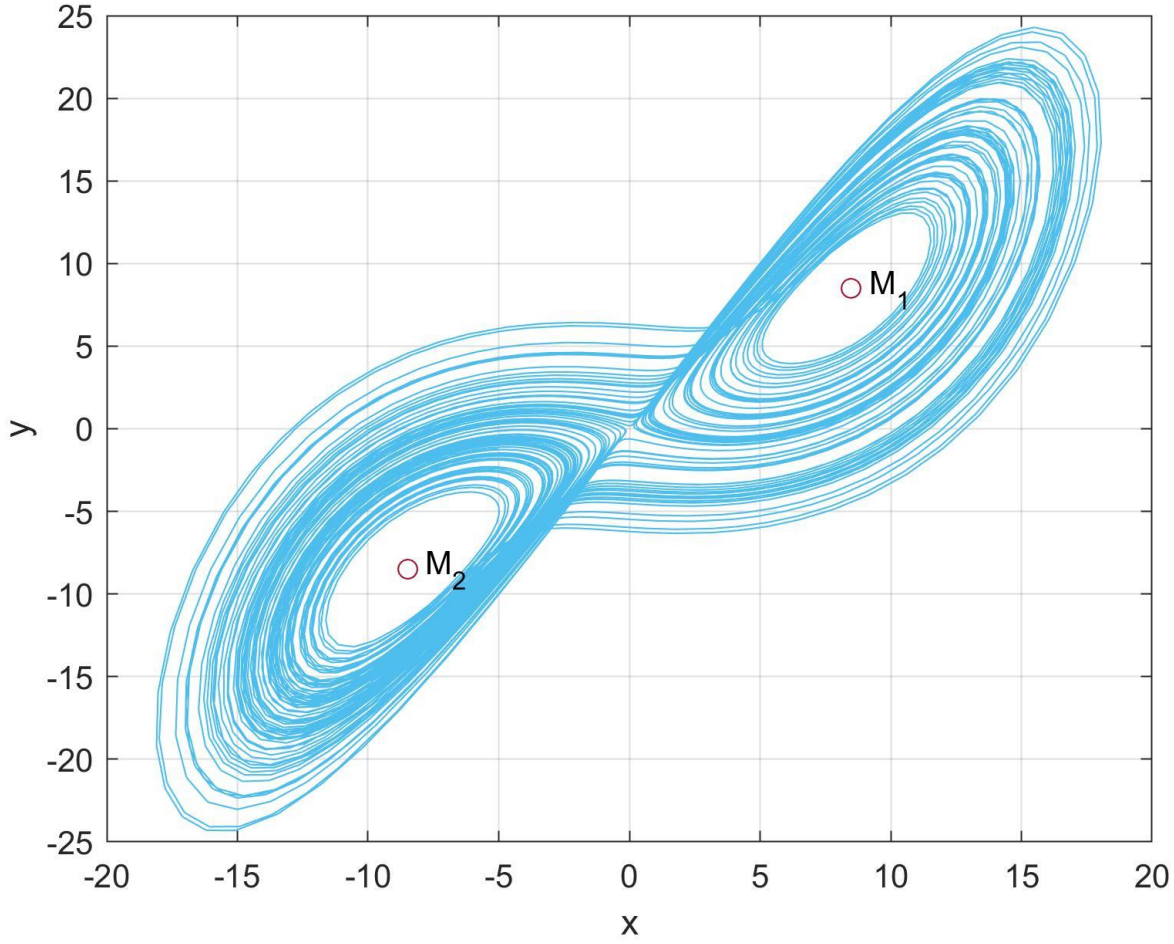


Рисунок 3.16 – Фазовий портрет атрактора системи Лоренца для значення r = 28

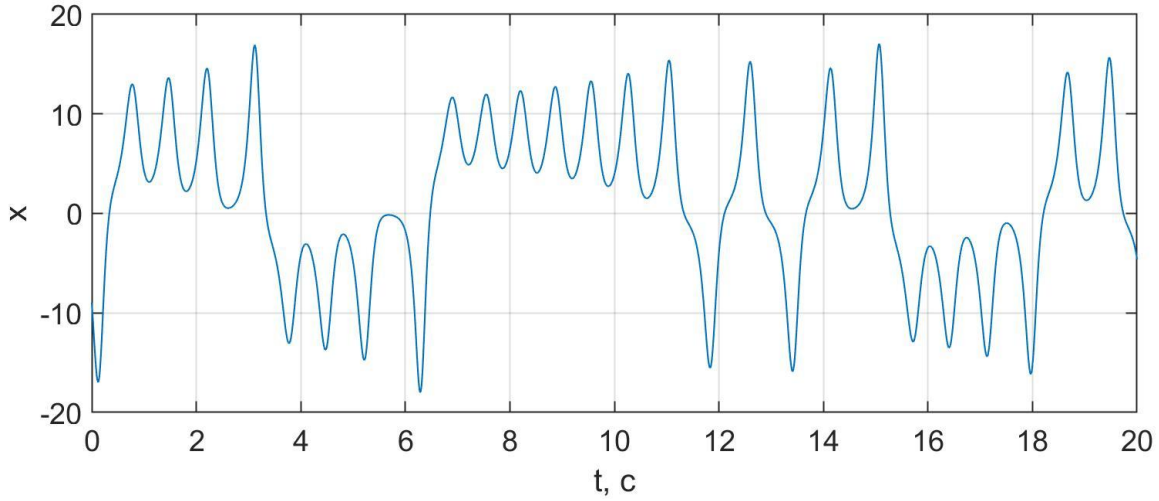


Рисунок 3.17 – Часовий графік сигналу $x(t)$ системи Лоренца для значення r = 28

3.3 Розрахунок показників Ляпунова

Досліджуючи різні режими роботи динамічних систем важливо чітко розрізняти тип коливання, яке породжено даною системою, що в свою чергу може бути періодичним, квазіперіодичним, випадковим або хаотичним. Візуальний аналіз фазових портретів дозволяє якісно оціни форму траєкторій, які описує система у фазовому просторі. Однак однозначно ідентифікувати хаотичний сигнал серед набору квазіперіодичних або суто випадкових сигналів таким чином неможна.

Відмінною особливістю хаотичних коливань є сильна залежність від початкових умов. Оцінка швидкості розходження фазових траєкторій дозволяє визначити чи знаходиться система в хаотичному режимі. Кількісно це можна зробити шляхом обчислення показників Ляпунова [1-3].

Для деякої неперервної в часі N-вимірної системи суть методу полягає в наступному: набору початкових умов ставиться у відповідність деяка нескінченно мала сфера, яка з часом еволюціонує в еліпсоїд. Таким чином i-й показник Ляпунова може бути виражений через довжини відповідних осей даного еліпсоїду:

$$\lambda_i = \lim_{t\to\infty}\left[\frac{1}{t}\ln\left(\frac{p_i(t)}{p_i(0)}\right)\right], \tag{3.9}$$

де p_i – довжина i-ї осі еліпсоїда.

Про хаотичну поведінку системи та наявність у фазовому просторі «дивного атрактора» свідчить додатній знак старшого показника Ляпунова. Для періодичного чи квазіперіодичного коливання показник Ляпунова дорівнює нулю.

Для системи з розмірністю $N = 3$, спектр показників Ляпунова λ_i ($i = 1\ldots3$) може мати такі комбінації знаків:

$\lambda_1 < 0;\ \lambda_2 < 0;\ \lambda_3 < 0$ – фокус;

$\lambda_1 = 0;\ \lambda_2 < 0;\ \lambda_3 < 0$ – граничний цикл;

$\lambda_1 < 0;\ \lambda_2 = 0;\ \lambda_3 < 0$ – двовимірний тор;

$\lambda_1 > 0;\ \lambda_2 = 0;\ \lambda_3 < 0$ – хаотичний атрактор.

Для системи Лоренца залежності показників Ляпунова від параметрів системи були розраховані в середовищі MATLAB за допомогою відповідної алгоритмічної процедури, що була розроблена згідно (3.9).

Залежності показників Ляпунова від параметрів системи Лоренца:

- від параметру σ (0 < σ <12). та сталих для r = 28, b = 8/3 (рисунок 3.18);
- від параметру r (0 < r < 30) та сталих для σ = 10, b = 8/3 (рисунок 3.19);
- від параметру b (0 < b < 10). та сталих для σ = 10, r = 28 (рисунок 3.20).

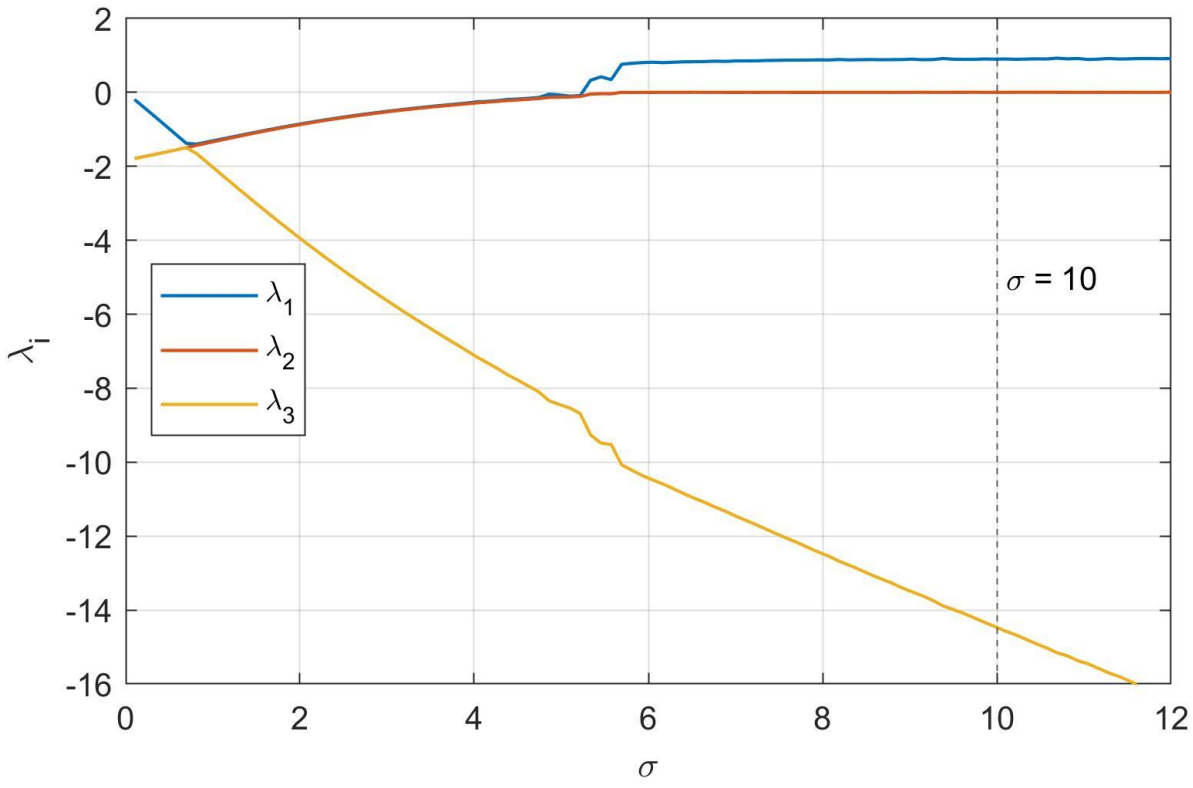


Рисунок 3.18 – Залежність показників Ляпунова від параметру σ (для r = 28, b = 8/3)

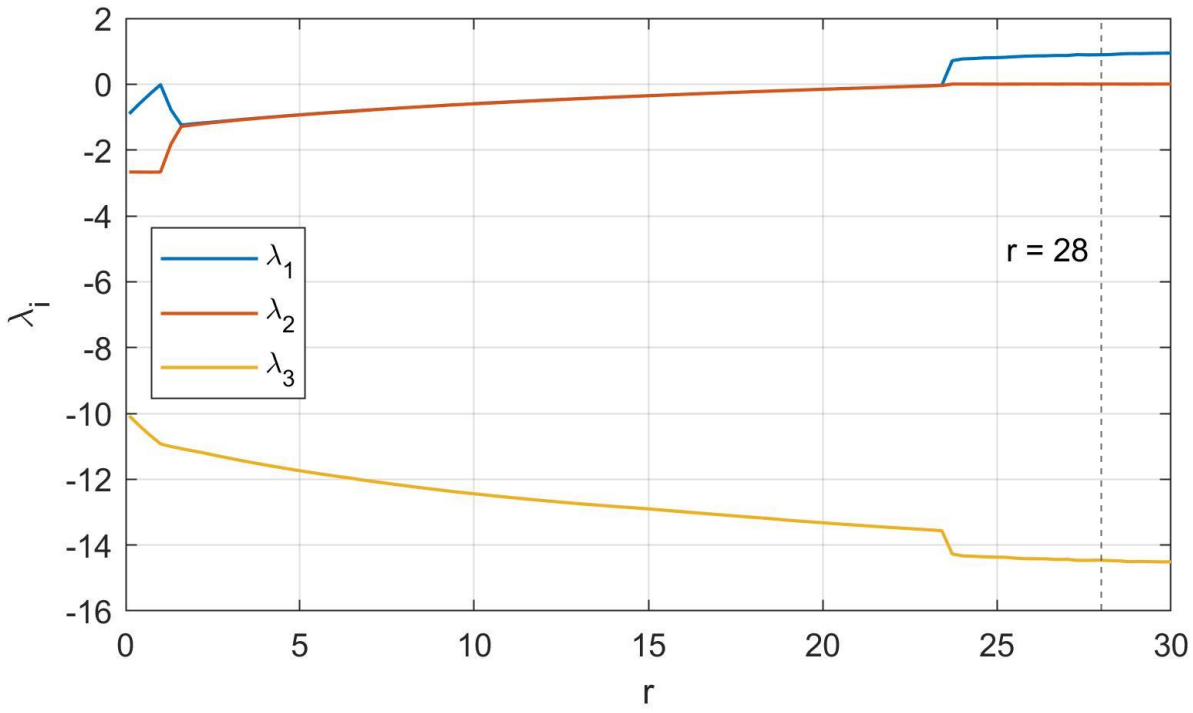


Рисунок 3.19 – Залежність показників Ляпунова від параметру r (для $\sigma = 10$, $b = 8/3$)

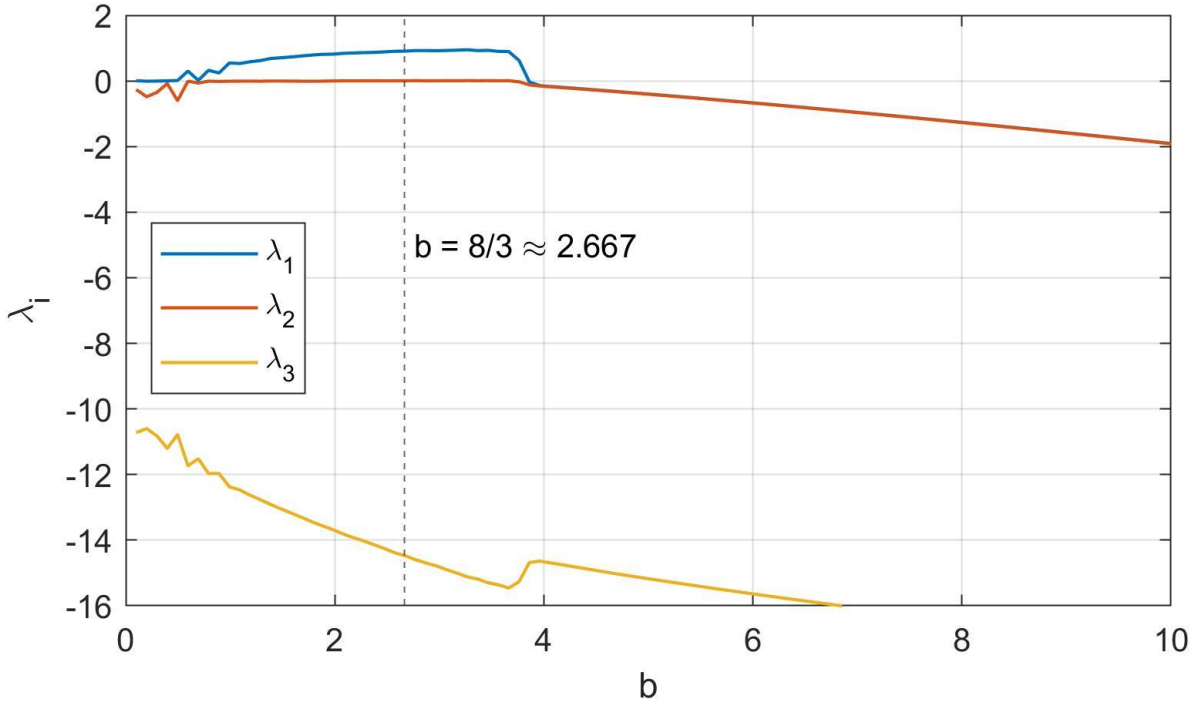


Рисунок 3.20 – Залежність показників Ляпунова від параметру b (для $\sigma = 10$ $r = 28$)

3.4 Висновки до третього розділу

В третьому розділі магістерської роботи було зроблено наступне:

- розглянуто методи та засоби математичного моделювання та чисельного розв’язку систем нелінійних диференціальних рівнянь;
- описано алгоритм Рунге-Кутти та його реалізацію в системі MATLAB;
- розглянуто можливості візуального моделювання та розвязку диференціальних рівнянь програмі Simulink;
- розроблена імітаційна модель системи Лоренца в програмі Simulink;
- проведено чисельний розрахунок в системі MATLAB динамічної системи Лоренца для різних значень керуючого параметру;
- розраховано спектр показників Ляпунова з метою дослідження режимів роботи системи для різних значень параметрів.

4 МЕТОДИ ПЕРЕДАЧІ ТА ЗАХИСТУ ІНФОРМАЦІЇ ЗА ДОПОМОГОЮ ДЕТЕРМІНОВАНО ХАОСУ НА БАЗІ СИСТЕМИ ЛОРЕНЦА

4.1 Синхронізація двох зв’язаних систем Лоренца

Для можливості передачі інформації за допомогою хаотичних коливань необхідно забезпечити режим синхронізації хаотичних генераторів на передавальній та приймальній сторонах [3].

Розглянемо пару, яка складається з ведучої та веденої систем Лоренца. Ведена система відповідає системі (2.1) та аналогічна Simulink-моделі (3.6). Ведена система відрізняється від ведучої наявністю вхідного сигналу для синхронізації.

Така пара однонаправлено зв’язаних систем може бути описана наступної системою диференціальних рівнянь:

$$\begin{cases} \dot{x}_1 = \sigma_1\left(y_1 - x_1\right) \\ \dot{y}_1 = x_1\left(r_1 - z_1\right) - y_1 \\ \dot{z}_1 = x_1 y_1 - b_1 z_1 \\ \dot{x}_2 = \sigma_2\left(y_2 - x_2\right) \\ \dot{y}_2 = x_2\left(r_2 - z_2\right) - y_2 \\ \dot{z}_2 = x_2 y_2 - b_2 z_2 \end{cases}, \tag{4.1}$$

де x_1, y_1, z_1 та x_2, y_2, z_2 –координати ведучою та веденої систем відповідно;

σ_1, r_1 b_1 та σ_2, r_2 b_2 – параметри ведучою та веденої систем відповідно.

Режим синхронізація для системи (4.1) досягається за умови $y_1 = y_2$. Передбачається, що ведуча система пов’язана із стороною передачі, а ведена – відповідно зі стороною прийому.

Моделі ведучої (Lorenz_1) та веденої (Lorenz_2) систем Лоренца, побудовані в середовищі Simulink, зображено на рисунках 4.1 та 4.2 відповідно.

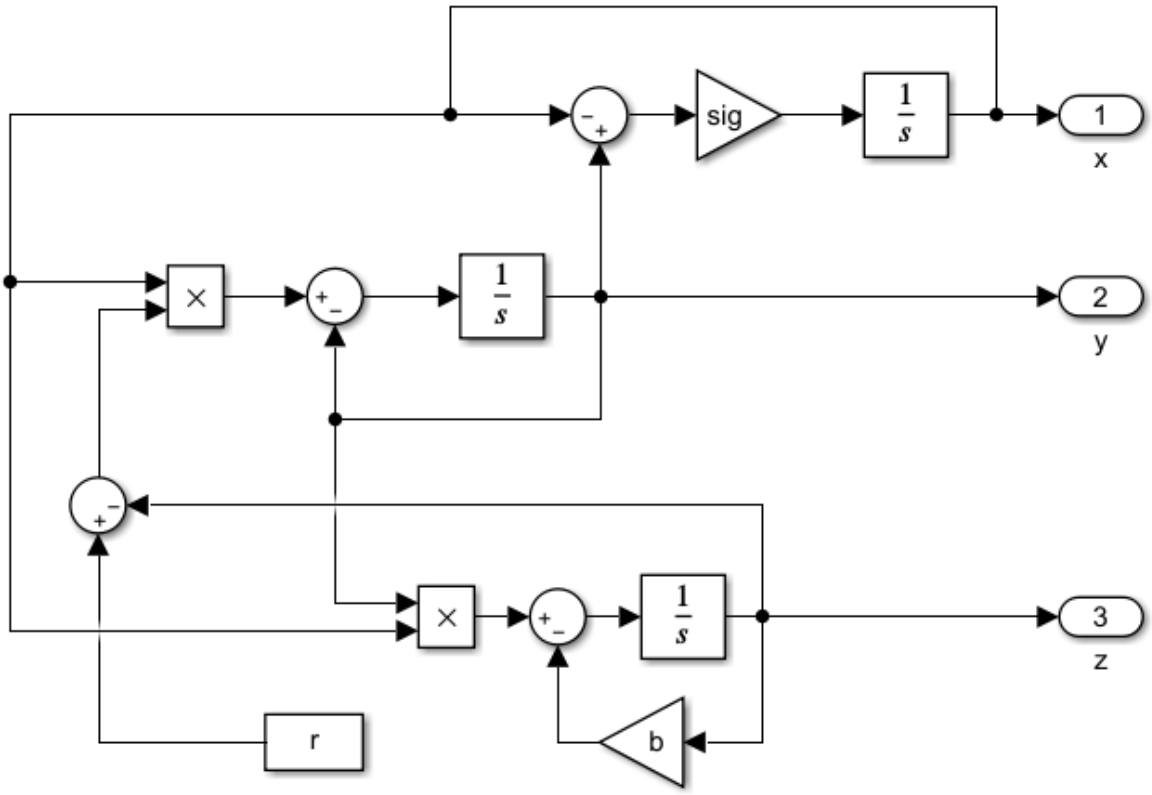


Рисунок 4.1 – Структурна схема ведучої системи Lorenz_1

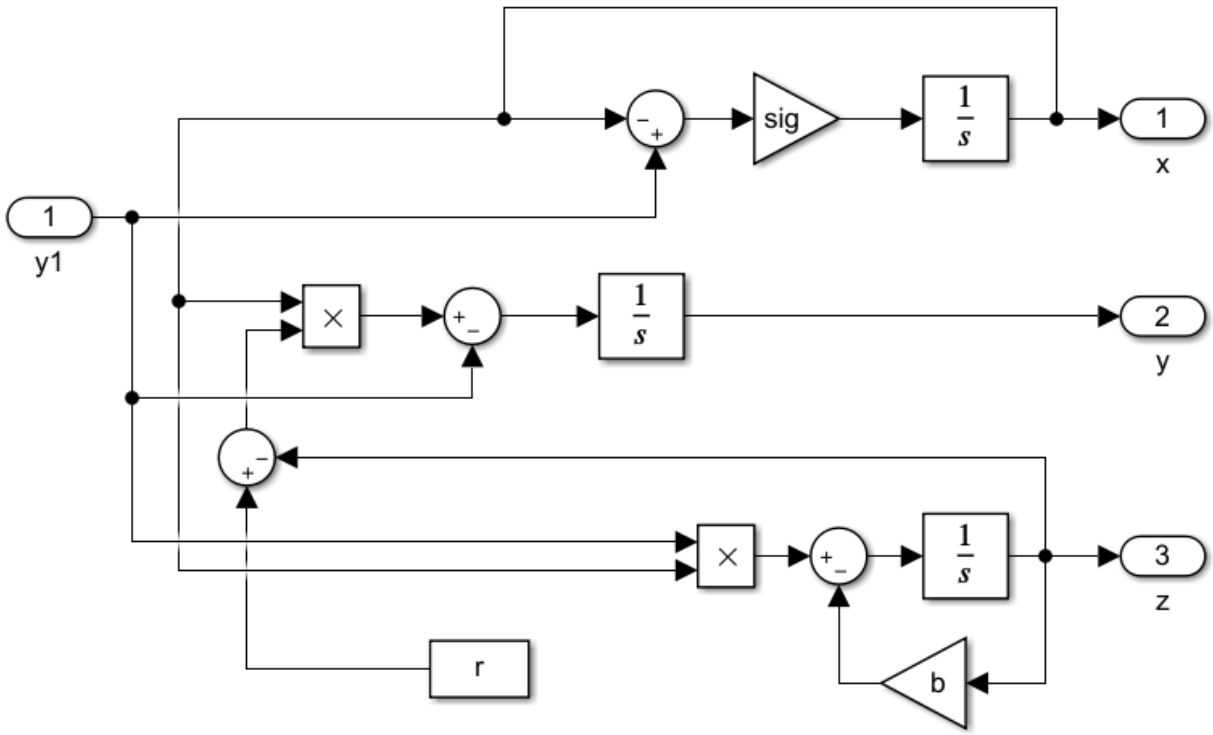


Рисунок 4.2 – Структурна схема веденої системи Lorenz_2

Модель пари однонаправлено зв’язаних систем Лоренца, побудована в системі Simulink, показана на рисунку 4.3 (параметри систем є ідентичними).

Перехідний процес синхронізації на прикладі координат $x_1(t)$ та $x_2(t)$ показаний на рисунку 4.4.

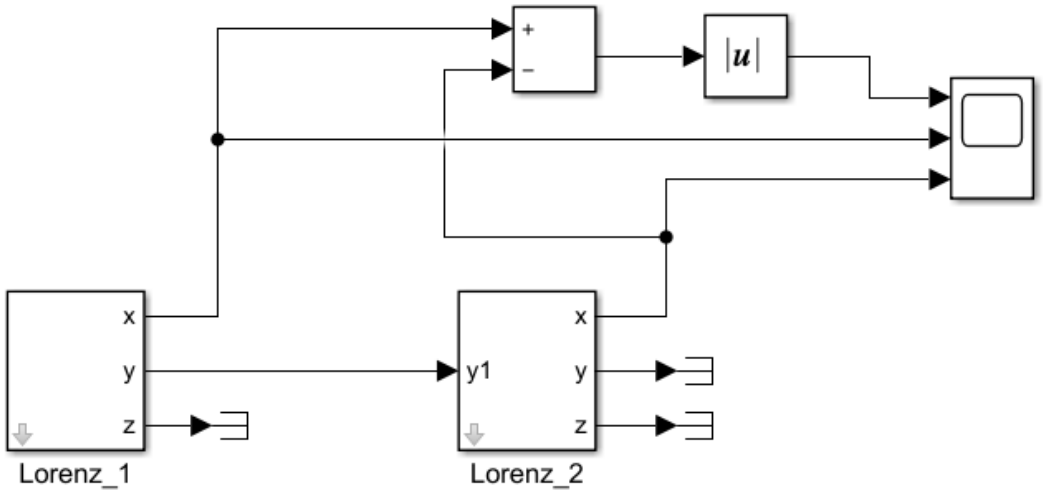


Рисунок 4.3 – Simulink-модель пари однонаправлено зв’язаних систем Лоренца

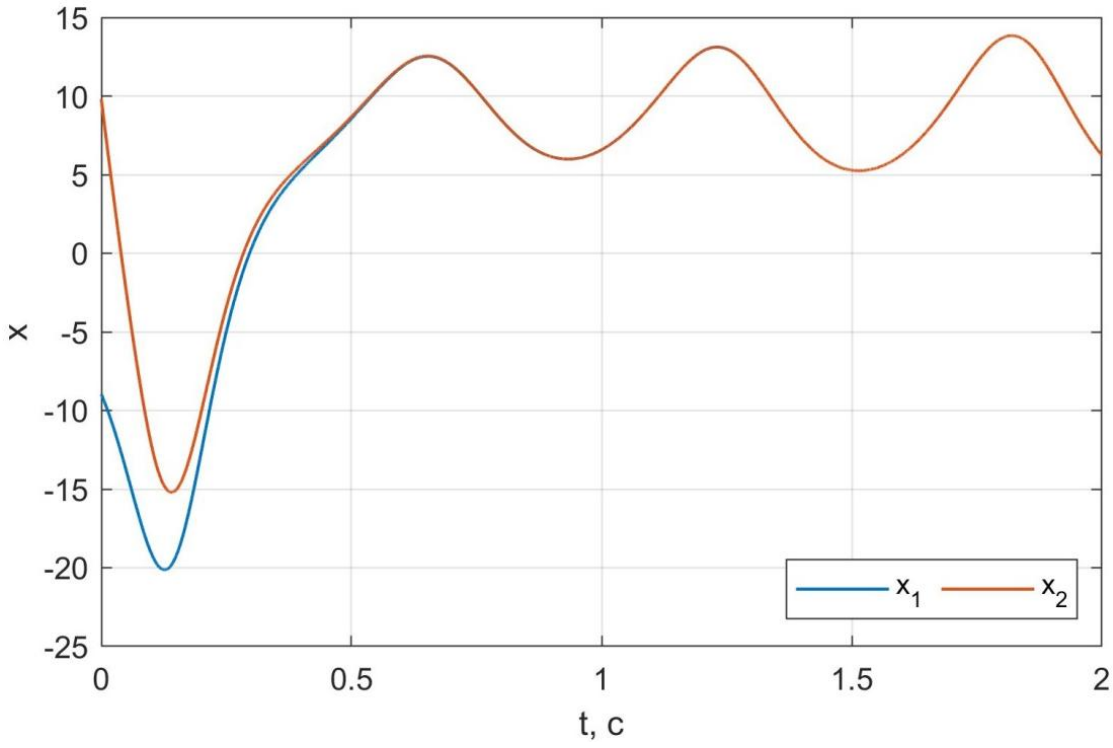


Рисунок 4.4 – Перехідний процес синхронізації на прикладі координат $x_1(t)$ та $x_2(t)$

4.2 Хаотичне маскування вузькосмугових сигналів

Метод передачі інформації на основі хаотичного маскування полягає в наступному:

- інформаційний сигнал $s(t)$ смутується з хаотичним сигналом $x_1(t)$ генератора ведучої системи та передається каналом зв'язку;
- після встановлення режиму синхронізації вихідний сигнал $x_2(t)$ веденої системи приймача та хаотичний складова $x_1(t)$ переданого сигналу є ідентичними;
- демодуляцій здійснюється шляхом віднімання від прийнятого сигналу хаотичного сигналу $x_2(t)$ генератора веденої системи.

Модель системи передачі з хаотичним маскуванням, що була розроблена в середовищі Simulink, зображена на рисунку 4.5. Вона є модифікацією системи синхронізації, яка була показана на рисунку 4.3, з доповненнями у вигляді блоку MATLAB-функції для аналітичного задання інформаційного сигналу $s(t)$ та елементів додавання/віднімання сигналів.

Синхронізація систем Lorenz_1 та Lorenz_2, що зображені на рисунку 4.5, здійснюється за допомогою координати $y(t)$. Параметри систем також вважаються ідентичними, а канал зв'язку такий, що не містить завад.

Метод передачі, що оснований на хаотичному маскуванні, може володіти деякими конфіденційними властивостями за умови дотримання певних умов. Зокрема, маскуючий хаотичний сигнал повинен переважати інформаційний сигнал за спектральною потужністю та шириною робочої смуги частот [3]. Отже, хаотичне маскування можна розглядати як додатковий ступінь захисту при передачі інформації в телекомунікаційних системах.

Розглянемо хаотичне маскування на прикладі гармонічного сигналу та вузькосмугових сигналів з частотною модуляцією (ЧМ) та амплітудною модуляцією (АМ).

Результати моделювання показані на рисунках 4.6 – 4.11.

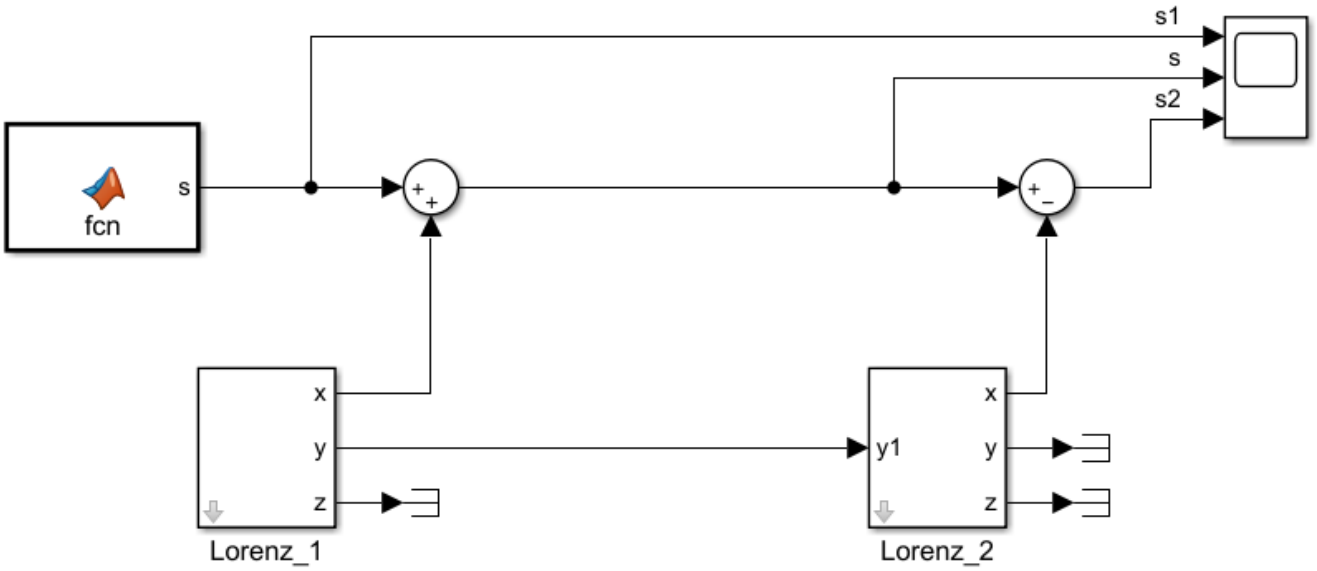


Рисунок 4.5 – Simulink-модель передачі шляхом хаотичного маскування

Аналітично гармонічний сигнал задається виразом:

$$s(t) = S_0 \sin(\omega_0 t + \varphi_0), \tag{4.2}$$

де S_0, ω_0, φ_0 – амплітуда кутова частота та початкова фаза сигналу.

Сигнал з частотною модуляцією:

$$s_{ЧМ}(\lambda, t) = S_0 \sin\left(\omega_0 t + m_{ЧМ} \int_0^t \lambda(t)\, dt + \varphi_0\right), \tag{4.3}$$

де $m_{ЧМ}$ – коефіцієнт частотної модуляції, $\lambda(t)$ – інформаційний сигнал

Сигнал з амплітудною модуляцією:

$$s_{AM}(\lambda, t) = S_0 \left[1 + m_{AM} \cdot \lambda(t)\right] \sin(\omega_0 t + \varphi_0), \tag{4.4}$$

де m_{AM} – індекс амплітудної модуляції, $\lambda(t)$ – інформаційний сигнал.

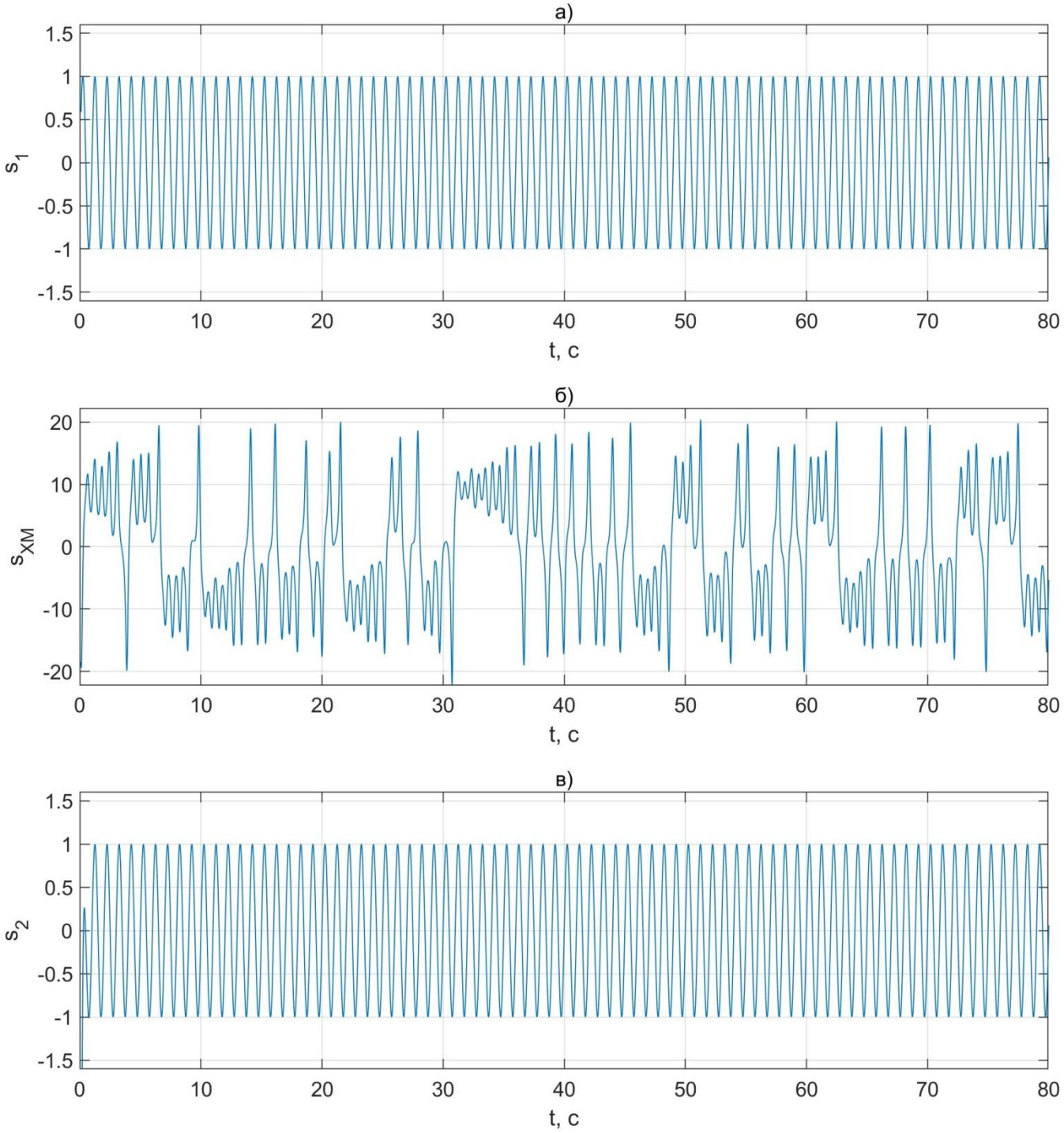


Рисунок 4.6 – Хаотичне маскування гармонічного сигналу (в часовій області):
сигнал на вході системи Lorenz_1 (передавача) – а)
сигнал на виході системи Lorenz_1 (в каналі зв’язку) – б)
сигнал після демодуляції прийнятого сигналу системою Lorenz_2 – в)

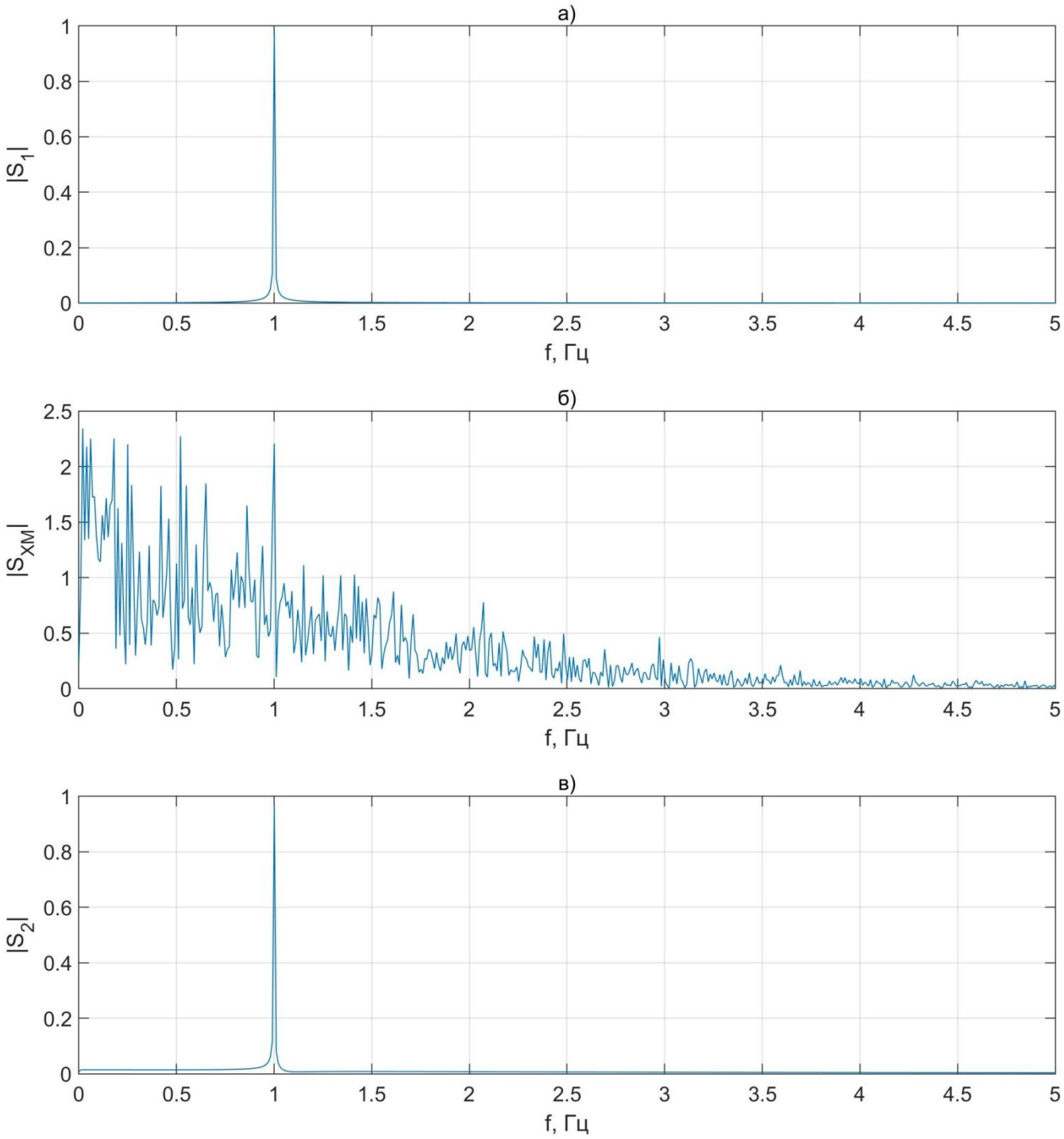


Рисунок 4.7 – Хаотичне маскування гармонічного сигналу (в частотній області):
сигнал на вході системи Lorenz_1 (передавача) – а)
сигнал на виході системи Lorenz_1 (в каналі зв’язку) – б)
сигнал після демодуляції прийнятого сигналу системою Lorenz_2 – в)

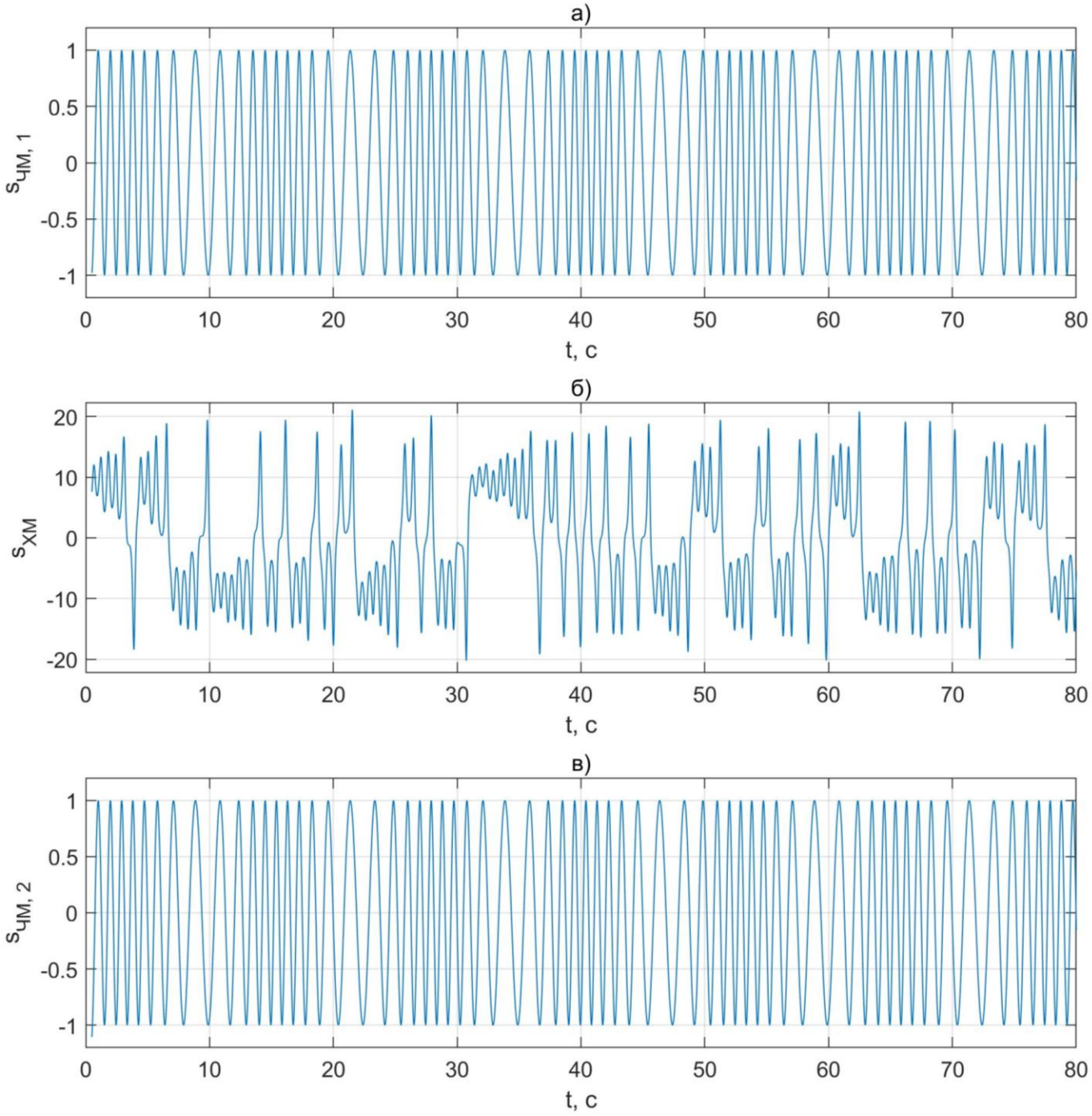


Рисунок 4.8 – Хаотичне маскування ЧМ-сигналу (в часовій області):
сигнал на вході системи Lorenz_1 (передавача) – а)
сигнал на виході системи Lorenz_1 (в каналі зв’язку) – б)
сигнал після демодуляції прийнятого сигналу системою Lorenz_2 – в)

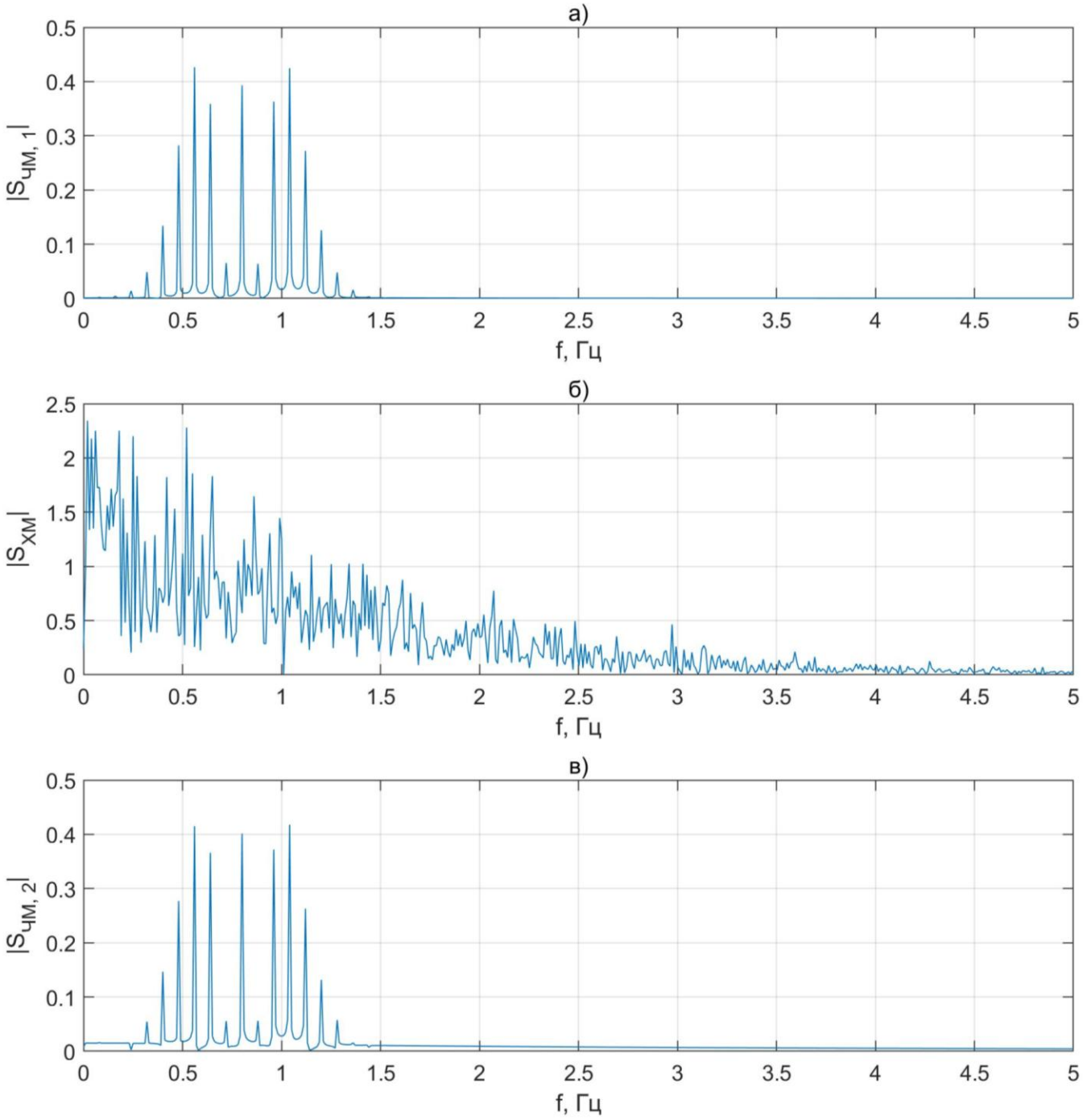


Рисунок 4.9 – Хаотичне маскування ЧМ-сигналу (в частотній області):
сигнал на вході системи Lorenz_1 (передавача) – а)
сигнал на виході системи Lorenz_1 (в каналі зв’язку) – б)
сигнал після демодуляції прийнятого сигналу системою Lorenz_2 – в)

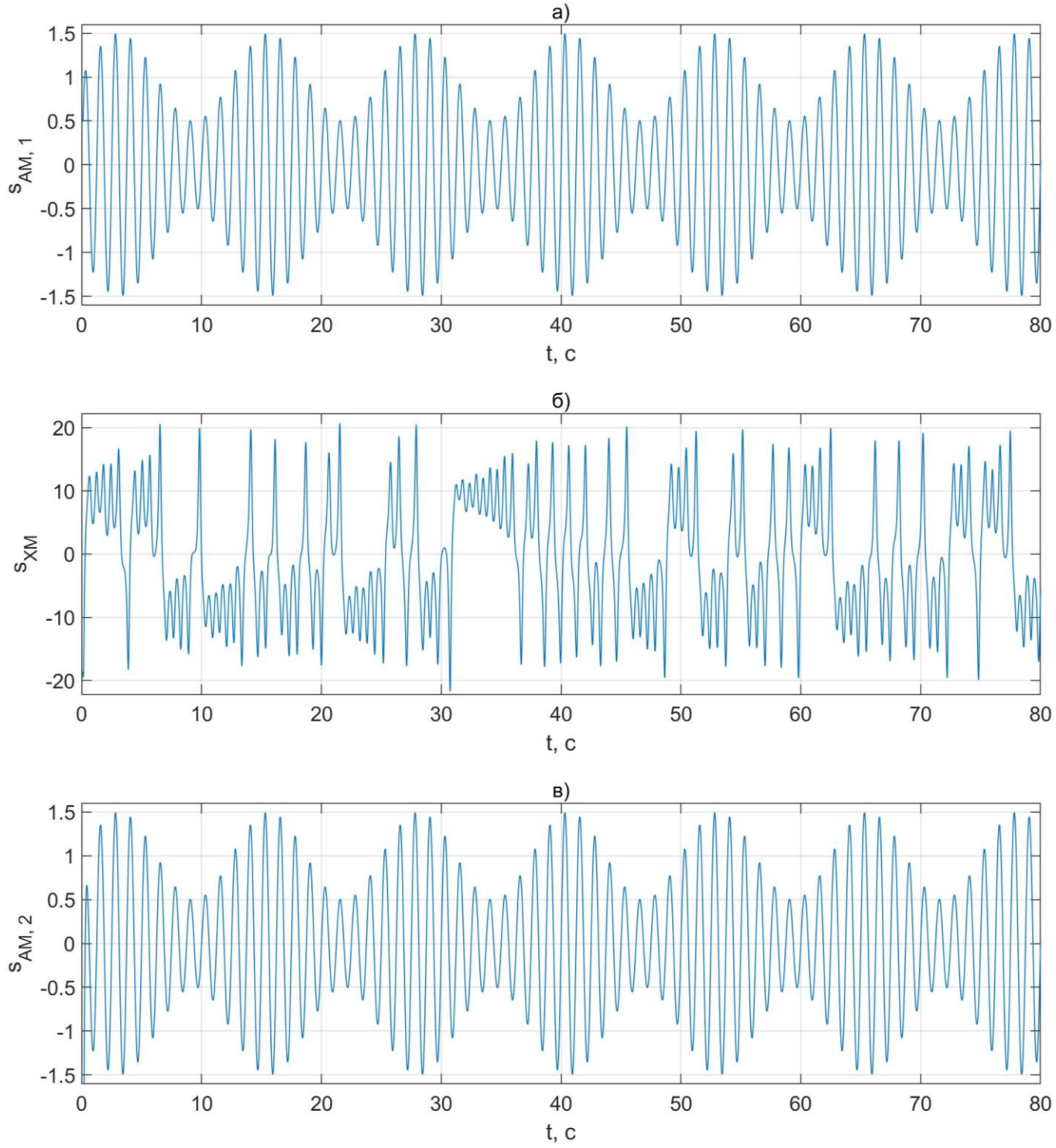


Рисунок 4.10 – Хаотичне маскування АМ-сигналу (в часовій області):
сигнал на вході системи Lorenz_1 (передавача) – а)
сигнал на виході системи Lorenz_1 (в каналі зв’язку) – б)
сигнал після демодуляції прийнятого сигналу системою Lorenz_2 – в)

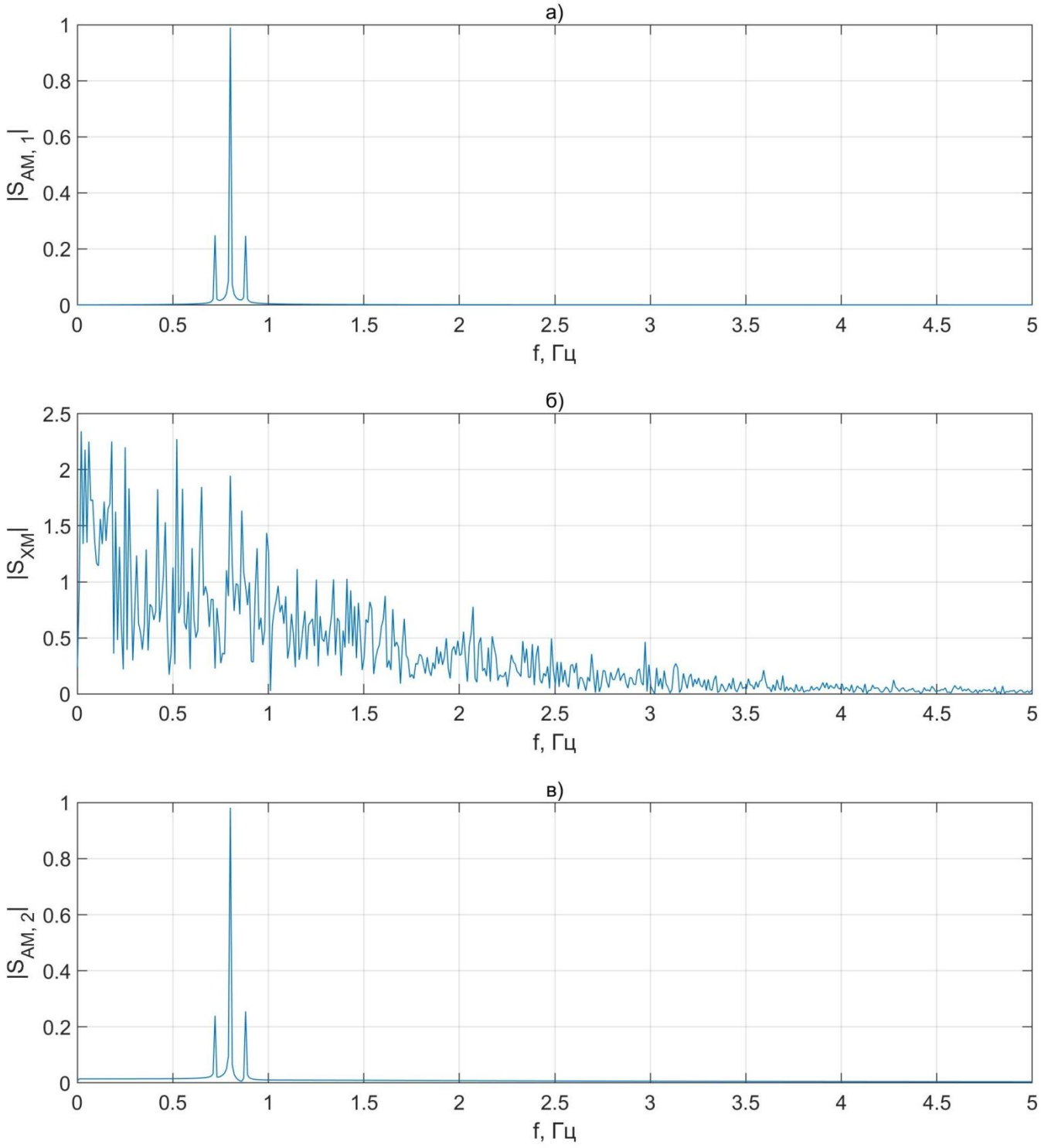


Рисунок 4.11 – Хаотичне маскування АМ-сигналу (в частотній області):
сигнал на вході системи Lorenz_1 (передавача) – а)
сигнал на виході системи Lorenz_1 (в каналі зв’язку) – б)
сигнал після демодуляції прийнятого сигналу системою Lorenz_2 – в)

4.3 Передача бітових послідовностей шляхом перемикання хаотичних режимів генератора

Передачу цифрових сигналів за допомогою детермінованого хаосу можливо організувати шляхом перемикання хаотичних сигналів, отриманих від генераторів із різним набором параметрів. Схема Simulink-моделі, яка реалізує даний підхід показана на рисунку 4.12.

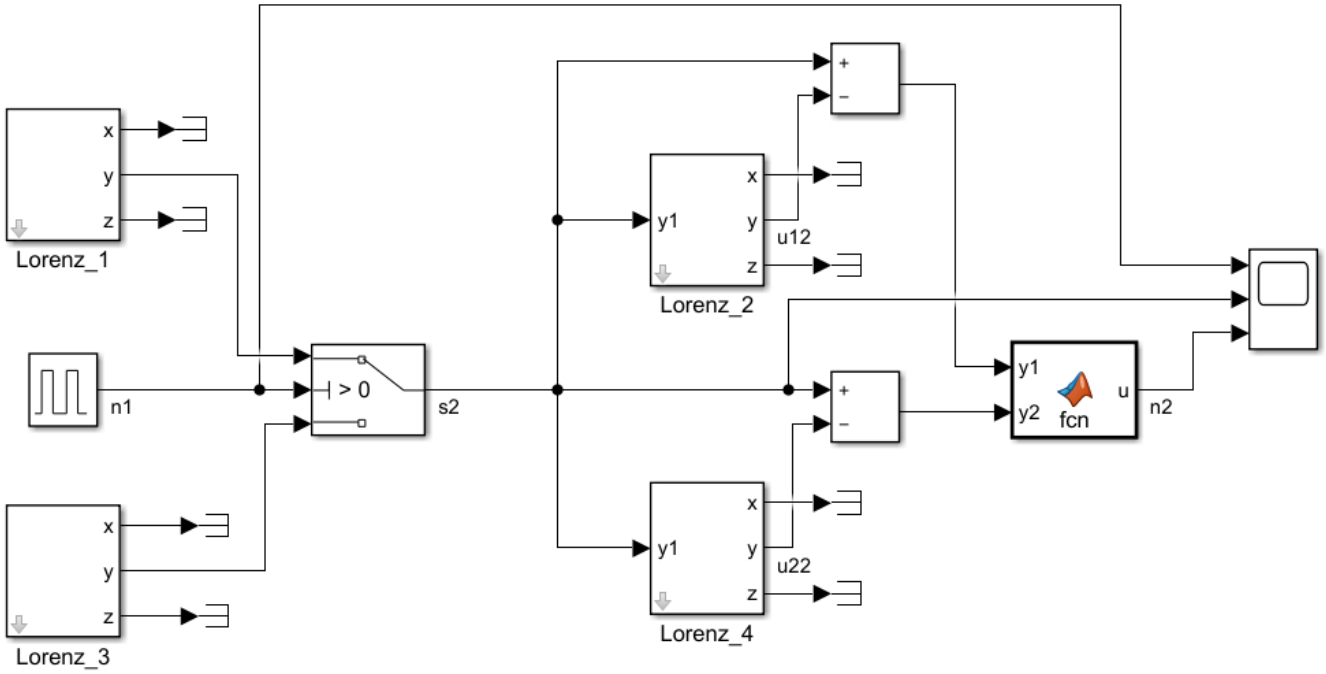


Рисунок 4.12 – Simulink-модель передачі цифрового сигналу шляхом перемикання хаотичних режимів

Схема, зображена ра рисунку 4.12, складається з двох пар однонаправлено з'єднаних хаотичних генераторів – Lorenz_1, Lorenz_2 та Lorenz_3, Lorenz_4 відповідно. Для систем Lorenz_1 і Lorenz_2 параметр $r = 25$, а для систем Lorenz_3 і Lorenz_4 – $r = 30$. Інші два параметри однакові для усіх систем ($\sigma = 10$, $b = 8/3$).

Вихідна бітова послідовність n_1 керує ключем *Sn1*, який перемикає подачу в канал зв'язку сигналів одного з двох ведучих хаотичних генераторів, що відповідають умовно логічному «0» чи «1».

Таким чином, синхронізація на приймальній стороні відбувається також почергово – в залежності від того, сигнал якого з двох хаотичних генераторів передавача приймається в даний момент часу.

Демодуляція цифрового сигналу здійснюється шляхом порівняння сигналу на вході ведених систем приймача із вихідним сигналом ведених систем:

$$n_2 = \begin{cases} 0, & якщо \quad s_x - y_{12} = 0 \\ 1, & якщо \quad s_x - y_{22} = 0 \end{cases}, \tag{4.5}$$

де S_x – сигнал в каналі зв'язку;

y_{12}, y_{22}– сигнали на виходах ведених систем Lorenz_2 та Lorenz_4 відповідно

Процедура порівняння різниць абсолютної похибки згідно (4.5) для моделі, зображеної на рисунку 4.12, реалізована у вигляді MATLAB-функції.

Спектр хаотичного сигналу в каналі зв'язку зображений на рисунку 4.13; часові залежності переданої та прийнятої бітової послідовності та сигналу в каналі зв'язку зображені на рисунку 4.14.

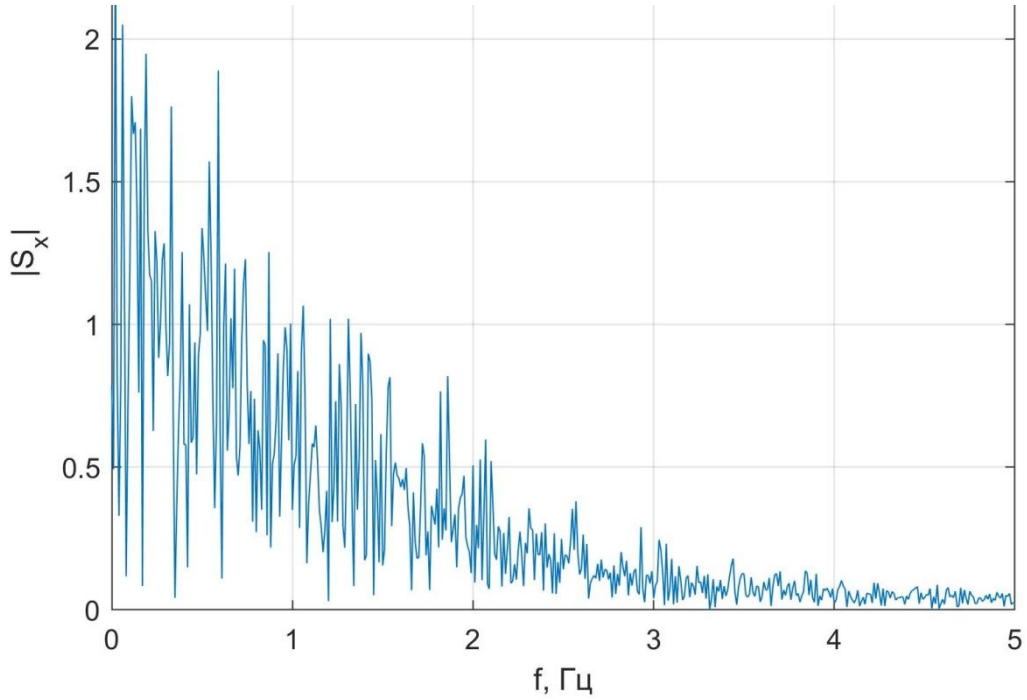


Рисунок 4.13 – Спектр сигналу з перемиканням хаотичних режимів

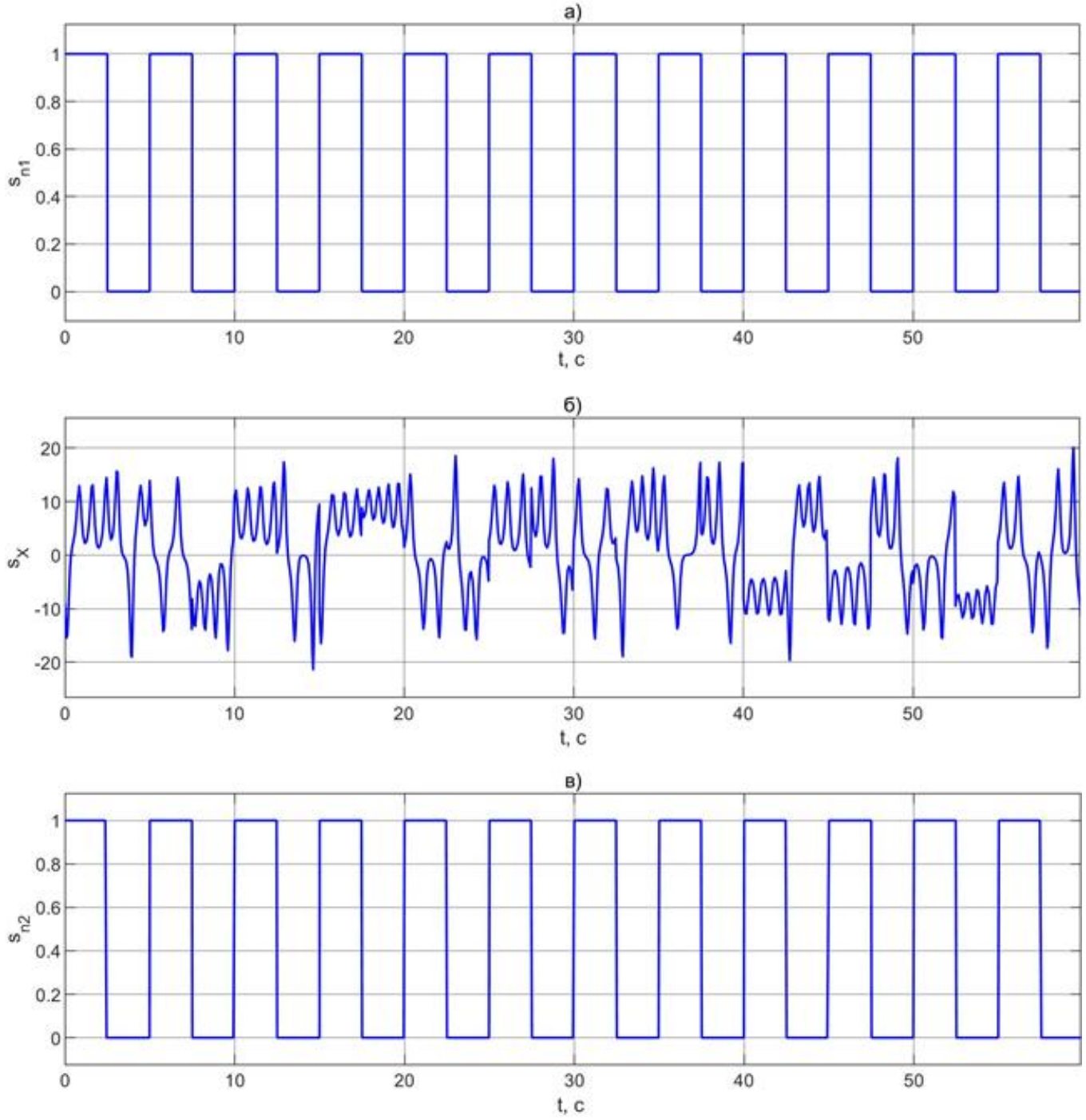


Рисунок 4.14 – Передача цифрового сигналу шляхом перемикання хаотичних режимів генератора передавача: вихідна бітова послідовність – а)
сигнал в каналі зв’язку – б)
прийнятий сигнал після демодуляції – в)

4.4 Шифрування даних за допомогою дискретних хаотичних послідовностей

Математичні моделі нелінійних систем із хаотичною динамікою можуть бути ефективно використані в якості генераторів послідовностей псевдовипадкових чисел в алгоритмах шифрування. Сильна чутливість до початкових умов забезпечує високу криптостійкість систем, побудованих на їх основі.

Для генерування цифрових хаотичних послідовностей використовується ітеративні функція, значення яких за певних початкових умов рівномірно розподілені на обмеженому відрізку.

Дискретно-часова система Лоренца може бути задана у вигляді системи нелінійних дискретних відображень:

$$\begin{cases} x(n+1) = \sigma\big(y(n) - x(n)\big)\Delta t + x(n) \\ y(n+1) = \big(x(n)\big(r - z(n)\big) - y(n)\big)\Delta t + y(n), \\ z(n+1) = \big(x(n)y(n) - bz(n)\big)\Delta t + z(n) \end{cases} \tag{4.6}$$

де σ, r, b – параметри системи, Δt – період дискретизації.

Для вказаних значень параметрів система (4.6) демонструє нестійкість фазових траєкторій та сильною залежністю від початкових умов, про що свідчить додатне значення старшого показника Ляпунова $\lambda_0 > 0$ [1, 2].

Отримані в результаті ітеративної процедури псевдовипадкові числові послідовності перетворюються в цілі двійкові числа згідно виразу:

$$w(n) = \left\lfloor \big(x(n) - l\big) / \big(h - l\big) \cdot \big(2^k - 1\big) \right\rfloor, \tag{4.7}$$

де k – розрядність двійкового представлення цілого числа,

h, l – відповідно максимальне та мінімальне значення послідовності x.

Фазовий портрет дискретної системи Лоренца зображено на рисунку 4.15, а псевдовипадкові хаотичні послідовності показані на діаграмі, що зображена на рисунку 4.16.

Вихідний байтовий масив b, що представляє собою інформаційне повідомлення, побітово сумується за модулем 2 з хаотичною послідовністю w. Отриманий в результаті шифрування код передається захищеним або відкритим каналом зв'язку та дешифрується на приймальній стороні аналогічним чином. Ключем шифру є дійсний вектор початкових значень $K = \left[x(0), y(0), z(0) \right]$. Криптографічна стійкість системи залежить від кількості можливих ключів шифрування [3]. Наприклад, дійсні числа, представлені у форматі з плаваючою комою подвійної точності мають 15 значущих цифр [4], тоді кількість ключів становитиме приблизно:

$$N_K \approx \left(10^{15}\right)^3 = 10^{45} \tag{4.8}$$

Операції шифрування та дешифрування виконуються однією процедурою, блок-схема алгоритму якої зображена на рисунку 4.17.

Алгоритм шифрування, що зображений на рисунку 4.17, був реалізований на мові програмування MATLAB.

На рисунку 4.18 показано результат роботи програми на прикладі шифрування та дешифрування растрового зображення у форматі .jpeg розміром 1000×1000 пікселів.

Описаний алгоритм шифрування даних за допомогою дискретних хаотичних послідовностей, згенерованих на основі динамічної системи Лоренца, дозволяє здійснювати шифрування і дешифрування довільних байтових послідовностей та може бути застосований в конфіденційних системах зв'язку, в тому числі телемедичних.

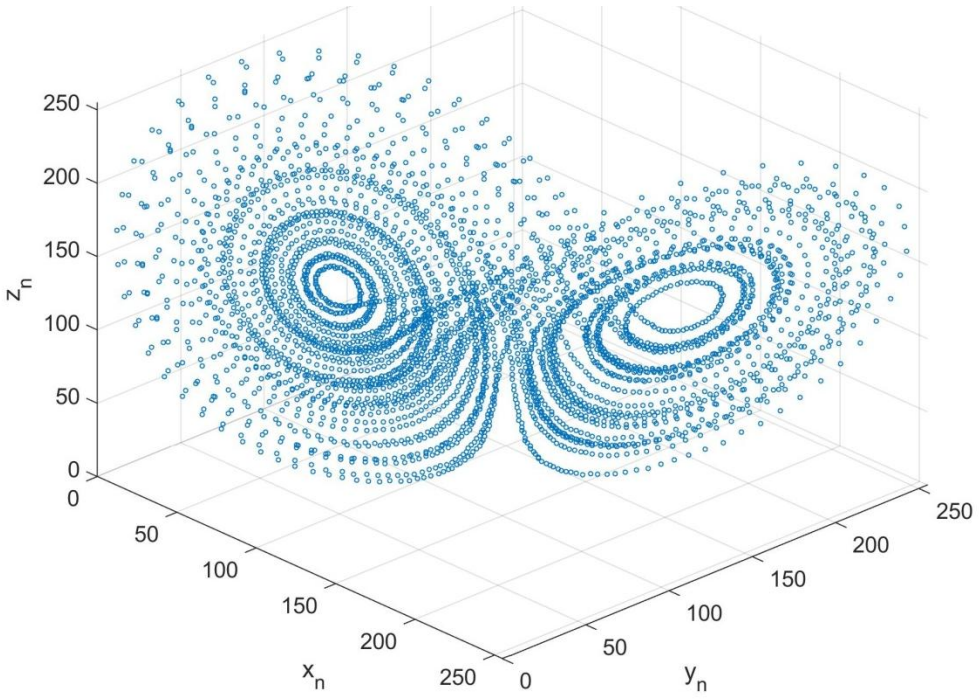


Рисунок 4.15 – Фазовий портрет дискретної системи Лоренца

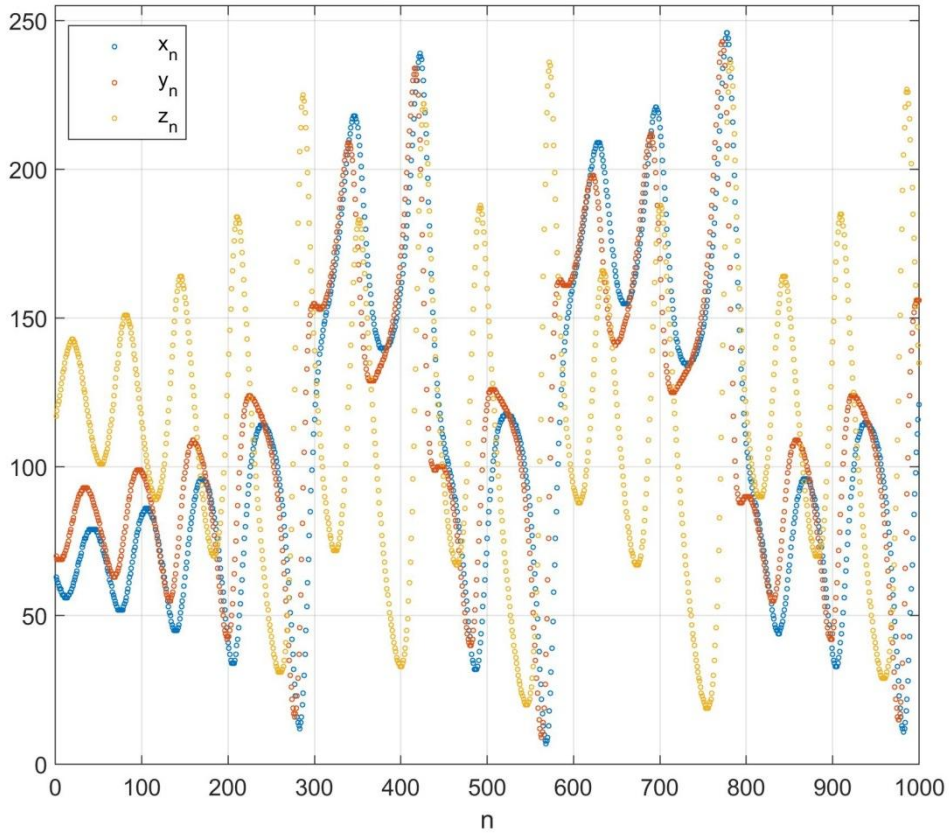


Рисунок 4.16 – Діаграми хаотичних псевдовипадкових послідовностей

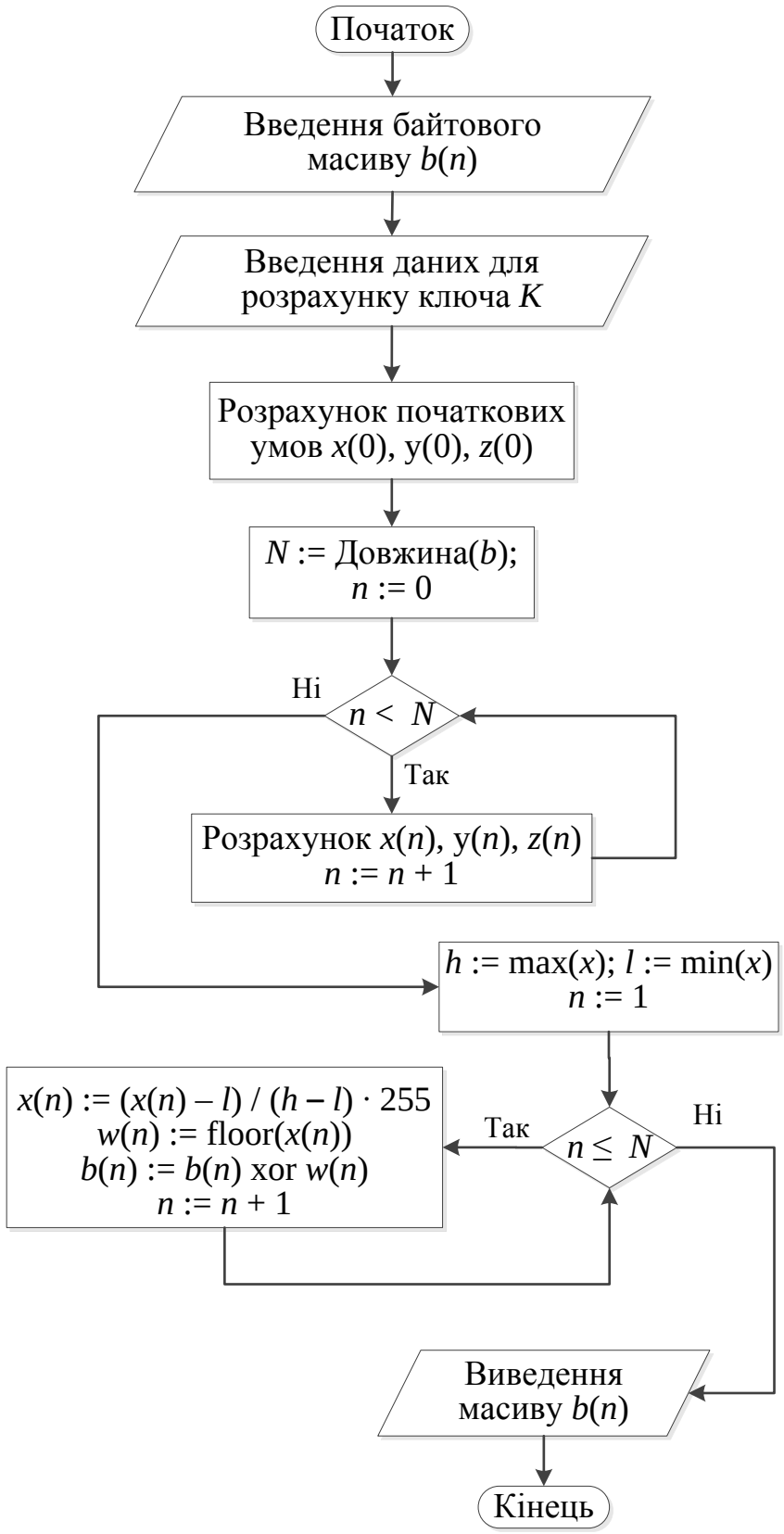
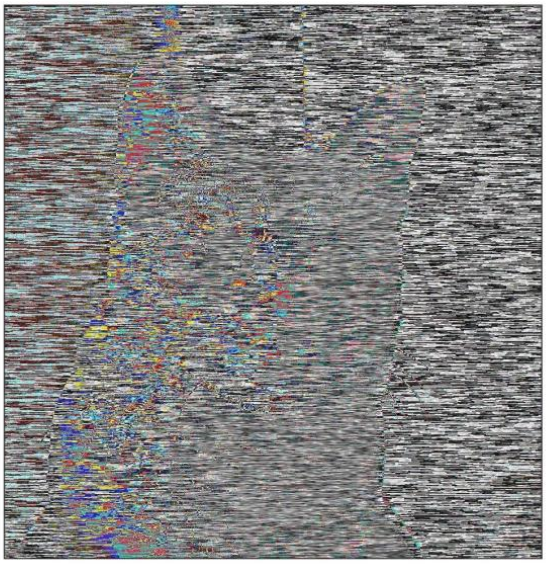


Рисунок 4.17 – Алгоритм шифрування/дешифрування вихідного байтового масиву

а)



б)

в)

Рисунок 4.18 – Результат роботи програми шифрування:
вихідне .jpeg зображення – а)
зображення .jpeg після шифрування – б)
зображення .jpeg після дешифрування – в)

4.4 Висновки до четвертого розділу

В четвертому розділі магістерської роботи було зроблено наступне:

- розроблена імітаційна модель в середовищі Simulink для дослідження синхронізації однонаправлено з’єднаних хаотичних ситсем Лоренца;
- на основі побудованої системи синхронізації було побудовано модель хаотичного маскування вузькосмугових сигналів;
- розроблена модель передачі цифрових сигналів за допомогою перемикання хаотичних режимів, які передаються каналом зв’язку, на база двох пар однонаправлено з’єднаних систем Лоренца із різним набором керуючих параметрів;
- на базі дискретно-часової системи Лоренца розроблено алгоритм шифрування байтових масивів.
- протестовано алгоритм шифрування дискретними хаотичними послідовностями на прикладі шифрування растрового зображення у форматі .jpeg.

Використання описаних методів дозволить підвищити ефективність та конфіденційність передачі інформації при розробці захищених систем зв’язку.

Загальні висновки до роботи

В роботі представлено ряд методів, що основані на теорії детермінованого хаосу, за допомогою яких можливо підвищити ефективність та конфіденційність передачі інформації в телекомунікаційних система.

На базі динамічної системи Лоренца було розроблено комплекс імітаційних моделей хаотичних генераторів, систем синхронізації та передачі дискретних та аналогових сигналів за допомогою хаосу. Крім того запропоновано алгоритм шифрування даних за допомогою дискретних хаотичних відображень.

В ході виконання роботи були поставлені та вирішені таки дослідницькі задачі:

- аналіз методів та існуючих рішень щодо використання детермінованого хаосу для передачі інформації;
- аналіз математичних моделей динамічних систем, які можуть генерувати хаос;
- вибір засобів та алгоритмів для чисельного розрахунку та моделювання нелінійних систем (MATLAB/Simulink);
- моделювання синхронно зв’язаних хаотичних систем;
- моделювання процесу передачі сигналів за допомогою хаотичних систем
- розробка алгоритму та програмна реалізація шифрування даних дискретними хаотичними послідовностями.

Описані методи можуть бути застосовані для розробки та впровадження захищених конфіденційних систем зв’язку різного роду призначення.

За результатами дослідження були підготовлені тези доповіді для IX Міжнародної науково-технічної конференції молодих учених та студентів «Актуальні задачі сучасних технологій», яка проходила в Тернополі 20-26 листопада 2020 року.

Перелік джерел посилання

1. Прикладне застосування теорії хаотичних систем у телекомунікаціях: монографія / [Ю.Я. Бобало, С.Д. Галюк, М.М. Климаш, Р.Л. Політанський]; Нац. ун-т «Львів. політехніка». – Львів: Коло, 2015. – 178 с.

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

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

4. Lorenz E.N. Deterministic nonperiodic flow / E. N. Lorenz // J. Atmos. Sci. – 1962 – Vol. 20. – № 2. – P. 130–141.

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

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

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

8. 7. Boccaletti S. The synchronization of chaotic systems / S. Boccaletti, J. Kurths, G.Osipov, D. L. Valladares, and C. S. Zhou // Physics Report. – 2002. – Vol. 366. – № 1–2. – P. 1–101.

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

10. Москаленко О.М. Хаотическая синхронизация (Различные механизмы и применение для передачи информации) / О.М. Москаленко // Диссертация на соискание ученой степени кандидата физико–математических наук , Саратов. – 2008. – 215с

11. Земляный О.В. Передача информации на основе манипуляции спектром широкополосного хаотического сигнала / О. В. Земляный // Радиофизика и электроника. – 2015. – Т. 6(20), № 3. – С. 72–78.

12. Cuomo K. Circuit Implementation of Synchronized Chaos with Application to Communications / K. Cuomo, A. Oppenheim // Phys. Rev. Lett. – 1993. – 71, N 1. – P. 65–68.

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

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

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

16. Волковский А. Р. Синхронный хаотический отклик нелинейной системы передачи информации с хаотической несущей / А. Р. Волковский, Н. В. Рульков // Письма в журн. техн. физики. – 1993. – 19, вып. 3. – С. 71–75.

17. Dmitriev A. S. Experiments on speech and music signals transmission using chaos / A. S. Dmitriev, A. I. Panas, S. O. Starkov // Int. J. of Bifurcation and chaos. – 1995. – 5, N 4. – P. 1249–1254.

18. Information transmission by chaotizing / F. Bohme, U. Feldman, W. Schwarz, A. Bauer // Proc. 2nd Int. Workshop on Nonlinear Dynamics of Electronic Systems (NDES'94). – Krakov, 1994. – P. 163–168.

19. Schweizer J. Predictive Poincare Control: a Control Theory for Chaotic Systems / J. Schweizer, M. P. Kennedy // Phys. Rev. E. – 1995. – 52, Iss. 5. – P. 4865–4876.

20. Козлов А. К. Управление хаотическими колебаниями в генераторах с запаздывающей петлей фазовой автоподстройки / А. К. Козлов, В. Д. Шалфеев // Прикладная нелинейная динамика. – 1994. – № 2. – С. 36–47.

21. Multi-User Communication using Chaotic Frequency Modulation / A. R. Volkovskii, S. C. Young, L. S. Tsimring, N. F. Rulkov // Proc. Int. Symp. Nonlinear Theory and Its Applications (NOLTA'01). – Miyagi, 2001. – P. 561–564.

22. Kennedy M. P. Chaotic Modulation for Robust Digital Communications over Multipath Channels / M. P. Kennedy, G. Columban // Int. J. Bifurcation Chaos. – 2000. – 10, N 4. – P. 695–719.

23. Перпективы создания прямо хаотических систем связи в радио- и СВЧ-диапазонах / А. С. Дмитриев, Б. Е. Кяргинский, Н. А. Максимов и др. // Радиотехника. – 2000. – № 3. – С. 9–20.

24. Ryabov V. B. Chaotic masking without synchronization / V. B. Ryabov, P.V. Usik, D. M. Vavriv // Радиофизика и радиоастрономия. - 1997. - 2, № 4. - С. 473-479.

25. Абазина Е.С. Цифровая стеганография: состояние и перспективы / Е.С. Абазина, А.А. Ерунов // Системы управления, связи и безопасности. – 2016. – № 2. – С. 182–201.

26. Иванюк П.В. Хаотическое маскирование информационных сигналов с использованием генератора на базе системы Лю / П.В. Иванюк, Л.Ф. Политанский, Р.Л. Политанский, О.М. Элияшив // Технология и конструирование в электронной аппаратуре. – 2012. – № 3. – С. 11–17.

27. Пятін І.С. Конфіденційна система зв’язку / І.С. Пятін, В.І. Лужанський, Л.В. Карпова // Вісник Хмельницького національного університету. Технічні науки. –2015. – № 1. – С. 207–212.

28. Колесов В.В. Применение дискретных хаотических алгоритмов в широкополосных телекоммуникационных системах / В.В. Колесов, А.И. Полубехин, Е.П. Чигин, А.Д. Юрин // Вестник СибГУТИ. – 2016. – № 3. – С. 77–92.

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

30. Передерий Ю.А. Метод оценки спектра ляпуновских показателей по временной реализации / Ю.А. Передерий // Известия вузов. ПНД. – 2012. – Т. 20, вып. 1. – С. 99–104.

31. M.-F. Danca. Matlab code for Lyapunov exponents of fractional order systems / Marius-F. Danca, N.V. Kuznetsov // International Journal of Bifurcation and Chaos. – 2018. – Vol. 28, No. 05, 1850067, – 14 p.

32. Kehui Sun. Bifurcations of fractional-order diffusionless Lorenz system / Kehui Sun, Xia Wang, J.C. Sprott // International Journal of Bifurcation and Chaos. – 2010. – Vol. 20, No. 04, – P. 1209–1219.

33. Taranchuk A.A. Construction of measuring piezoresonance mechanotrons and their practical implementation for telemedicine diagnostic systems // Telecommunications and Radio Engineering. – 2018. – Volume 77, Issue 3, – PP. 269-281.

34. Политанский Р.Л. Система передачи данных с шифрованием хаотическими последовательностями / Р.Л. Политанский, М.П. Шпатарь, А.В. Гресь, А.Д. Верига // Технология и конструирование в электронной аппаратуре. – 2014. – № 2-3. – С. 28–32.

35. Генри С. Уоррен. Числа с плавающей точкой // Алгоритмические трюки для программистов = Hacker’s Delight. — М.: Вильямс, 2007. – С. 288.

36. Шеннон К. Работы по теории информации и кибернетике. — М.: Изд. иностр. лит., 1963. – 830 с.

37. Арушанян О. Б. Решение систем обыкновенных дифференциальных уравнений методами Рунге–Кутта // О. Б. Арушанян, С. Ф. Залеткин, 2014, 58с

38. Слободян М.О. Генерування широкосмугових хаотичних сигналів для прихованої передачі даних в телекомунікаційних системах / М.О. Слободян, А.А. Таранчук, В.Є. Гавронський // Вісник Хмельницького національного університету. Технічні науки. –2020. – № 4. – С. 192–198.

ДОДАТОК А

(обов’язковий)

ПРОГРАМНА РЕАЛІЗАЦІЯ АЛГОРИТМУ ШИФРУВАННЯ РАСТРОВОГО ЗОБРАЖЕННЯ ДИСКРЕТНИМИ ХАОТИЧНИМИ ПОСЛІДОВНОСТЯМИ НА МОВІ MATLAB

```
clear;
sigma = 10;
r = 28;
b = 8/3;
dt = 0.01;
I = [-9.0472,-10.3329,25.9613];

P = imread('cat.jpg');
N = size(P,1);
M = size(P,2);

[x,y,z] = mylorenz(sigma,r,b,dt,dt*N*M*3*1.1,I);

w = uint8((x - min(x)) ./ (max(x)-min(x)) .* 255);
% w = uint8((y - min(y)) ./ (max(y)-min(y)) .* 255);
% w = uint8((z - min(z)) ./ (max(z)-min(z)) .* 255);

P1 = uint8(zeros(N,M,3));
q = 1;
n = 1;
while n <= N
   m = 1;
   while m <= M
      k = 1;
      while k <= 3
         P1(n,m,k) = bitxor(P(n,m,k),w(q));
         q = q + 1;
```

```
            k = k + 1;
        end
        m = m + 1;
    end
    n = n + 1;
end

% I = [-9.0473,-10.3328,25.9612];
I = [-9.0472,-10.3329,25.9613];
[x] = mylorenz(sigma,r,b,dt,dt*N*M*3*1.1,I);
w = uint8((x - min(x)) ./ (max(x)-min(x)) .* 255);
% w = uint8((y - min(y)) ./ (max(y)-min(y)) .* 255);
% w = uint8((z - min(z)) ./ (max(z)-min(z)) .* 255);

P2 = uint8(zeros(N,M,3));
q = 1;
n = 1;
while n <= N
    m = 1;
    while m <= M
        k = 1;
        while k <= 3
            P2(n,m,k) = bitxor(P1(n,m,k),w(q));
            q = q + 1;
            k = k + 1;
        end
        m = m + 1;
    end
    n = n + 1;
end

figure('Position', [50 25 1000 260]);
subplot(1,3,1);
image(P);
xticks([]);
yticks([]);
```

```
subplot(1,3,2);
image(P1);
xticks([]);
yticks([]);
subplot(1,3,3);
image(P2);
xticks([]);
yticks([]);

function [x,y,z,t,M] = mylorenz(sigma,r,b,dt,tmax,I)
   M(1,1) = sqrt(b*(r-1));
   M(1,2) = sqrt(b*(r-1));
   M(1,3) = r-1;
   M(2,1) = -sqrt(b*(r-1));
   M(2,2) = -sqrt(b*(r-1));
   M(2,3) = r-1;

   t = 0:dt:tmax;
   N = length(t);
   x = zeros(N,1);
   y = zeros(N,1);
   z = zeros(N,1);
   x(1) = I(1);
   y(1) = I(2);
   z(1) = I(3);

   for k = 2:N
      dx = sigma.*(y(k-1) - x(k-1)).*dt;
      dy = (x(k-1).*(r - z(k-1)) - y(k-1)).*dt;
      dz = (x(k-1).*y(k-1) - b.*z(k-1)).*dt;

      x(k) = x(k-1) + dx;
      y(k) = y(k-1) + dy;
      z(k) = z(k-1) + dz;
   end
end
```

ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет програмування та комп’ютерних і телекомунікаційних систем

Кафедра телекомунікацій, медійних та інтелектуальних технологій

ДИПЛОМНА РОБОТА

«*Конфіденційна система зв'язку з використанням пристроїв із хаотичною динамікою*»

Спеціальність 172 – «Телекомунікації та радіотехніка»

Виконав: студент 2 курсу, група ТРм-19-1 М.О. Лівчук

Керівник: д-р. техн. наук, доц. С.К. Підченко

Хмельницький, 2020

Метою роботи є підвищення рівня конфіденційності та ефективності передачі інформації в телекомунікаційних системах.

Завдання, які вирішуються в роботі:

- аналіз методів та існуючих рішень щодо використання детермінованого хаосу для передачі інформації;
- аналіз математичних моделей динамічних систем, які можуть генерувати хаос;
- вибір засобів та алгоритмів для чисельного розрахунку та моделювання нелінійних систем;
- моделювання синхронно зв’язаних хаотичних систем
- моделювання процесу передачі сигналів за допомогою хаотичних систем
- розробка алгоритму та програмна реалізація шифрування даних дискретними хаотичними послідовностями.

Об’єкт дослідження – процес конфіденційної передачі інформаційних сигналів каналами зв’язку в телекомунікаційних системах.

Предмет дослідження – методи та засоби конфіденційної передачі інформаційних сигналів за допомогою пристроїв із хаотичною динамікою.

Науково-практична новизна роботи:

1. Отримав розвиток метод шифрування даних на основі дискретних хаотичних послідовностей. На базі дискретно-часової динамічної моделі Лоренца було розроблено алгоритм шифрування вихідного масиву байтів.

2. Представлено ряд методів, що основані на теорії детермінованого хаосу, за допомогою яких можливо підвищити ефективність та конфіденційність передачі інформації в телекомунікаційних система. На базі динамічної системи Лоренца було розроблено комплекс імітаційних моделей хаотичних генераторів, систем синхронізації та передачі дискретних та аналогових сигналів за допомогою хаосу.

За результатами дослідження були підготовлені тези доповіді для IX Міжнародної науково-технічної конференції молодих учених та студентів «Актуальні задачі сучасних технологій», яка проходила в Тернополі 20-26 листопада 2020 року.

Структура і обсяг дипломної роботи. Дипломна робота складається із вступу, чотирьох розділів, висновків до кожного розділу, загального висновку до роботи, списку використаних джерел, додатків. Загальний обсяг роботи складає 81 сторінку комп'ютерного тексту, у тому числі: 47 рисунків, список використаних джерел вміщує 38 найменувань.

1 АНАЛІЗ МЕТОДІВ ТА ЗАСОБІВ ЗАХИСТУ ІНФОРМАЦІЇ В ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ

Передумови для використання хаосу для передачі інформації

В основі теорії використання хаотичних пристроїв в телекомунікаційних системах лежать такі наукові досягнення (рисунок 1.1):

- відкриття та розробка теорії нелінійних процесів, пов'язаних із поняттям «дивного атрактора»;
- винайдення простих електронних схем, які за певних умов можуть генерувати складні хаотичні коливання;
- відкриття явища синхронізації систем із хаосом та розвиток теорії щодо його застосування в системах передачі інформації;
- розробка методів кількісної оцінки ступеня хаотичності систем.

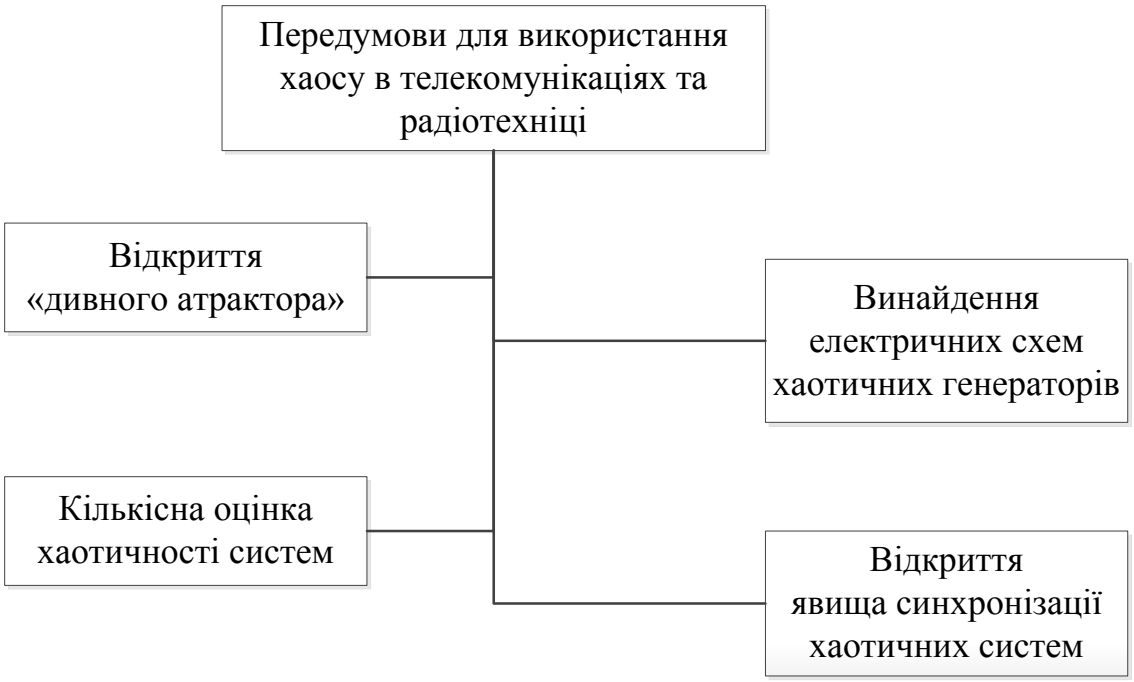


Рисунок 1.1 – Передумови використання хаосу в радіотехніці

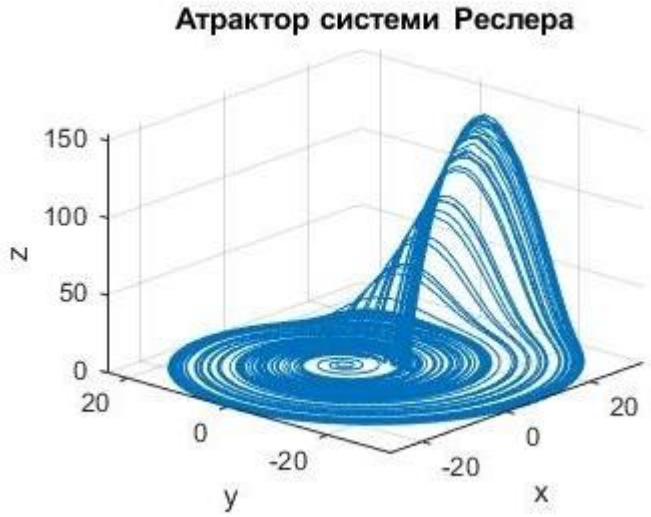
Властивості хаотичних атракторів

«Дивним атрактором» прийнято називати фрактальну множину точок фазового простору, до якої прямують фазові траєкторії системи з плином часу. Існування хаотичних атракторів динамічних систем дає можливість синхронізувати хаотичні системи.

Хаотична поведінка системи супроводжується такими базовими ознаками [1, 4, 5]:

- сильна чутливість до початкових умов;
- фрактальна розмірність атрактора у фазовому просторі;
- неперервний спектр часових реалізацій компонентів системи

Таким чином реальні динамічні системи, які зустрічаються у природі, наприклад, системи Лоренца та Реслера [1, 2] мають фрактальну структуру. Математичні моделі таких систем знайшли застосування в теорії передачі інформації [3].



2 МАТЕМАТИЧНІ МОДЕЛІ ДИНАМІЧНИХ СИСТЕМ ІЗ ХАОТИЧНОЮ ПОВЕДІНКОЮ

Система Лоренца

Першою динамічною системою, при чисельному дослідженні якої були отримано нетривіальні розв'язки для її змінних і виявлено нетипову поведінку та високу чутливість до початкових умов, є фізична модель конвекції потоків газів та рідин під час їхнього нагрівання [4]. Дана система вперше була досліджена Е. Лоренцом в 1963 р.

Аналітично ***система Лоренца*** описується наступними диференційними рівняннями:

$$\begin{cases} \dfrac{dx}{dt} = \sigma(y - x) \\ \dfrac{dy}{dt} = rx - y - xz \\ \dfrac{dz}{dt} = xy - bz \end{cases} \qquad (2.1)$$

де σ, r, b – параметри системи.

Класичним набором параметрів, для яких проводиться дослідження системи Лоренца є: $\sigma = 10$, $r = 28$, $b = 8/3$. На рисунку 2.1 зображено хаотичний атрактор системи Лоренца та часову діаграму сигналу $x(t)$.

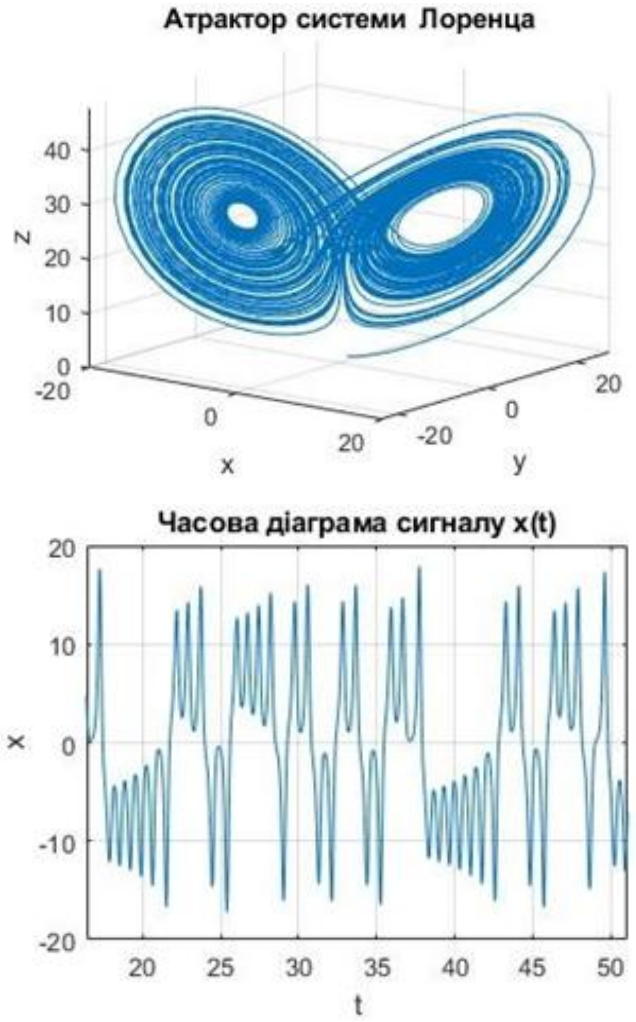


Рисунок 2.1 – Атрактор системи Лоренца та часова діаграма сигналу $x(t)$

3 АНАЛІЗ ТА МАТЕМАТИЧНЕ МОДЕЛЮВАННЯ ДИНАМІЧНОЇ СИСТЕМИ ЛОРЕНЦА

Чисельний розв'язок системи Лоренца

Фазові портрети та часові діаграми $x(t)$ для деяких значень параметра r (σ=10, b = 8/3), що відповідають характерним динамічним режимам показані на рисунках 3.10 – 3.17. M_1 та M_2 – точки рівноваги системи

r = 10

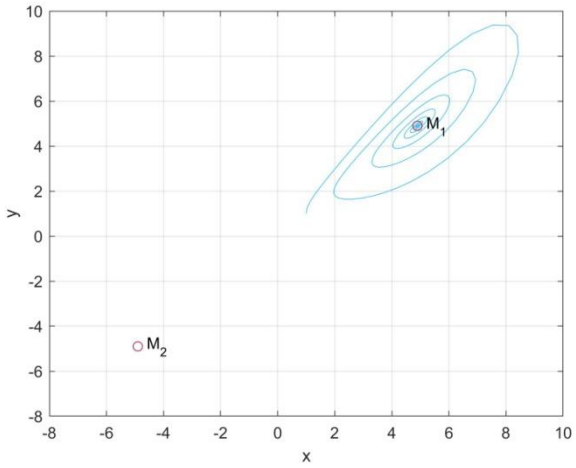


Рисунок 3.10

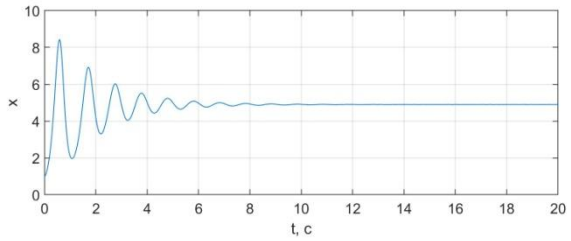


Рисунок 3.11

r = 20

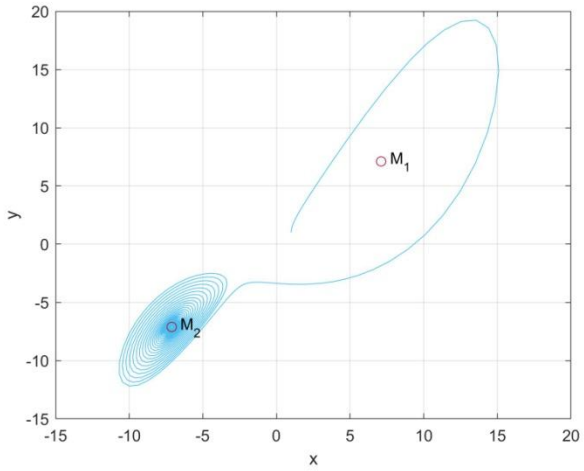


Рисунок 3.14

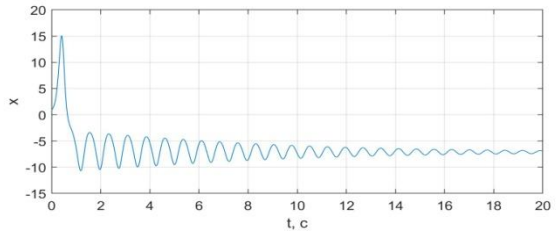


Рисунок 3.15

r = 28 (хаос)

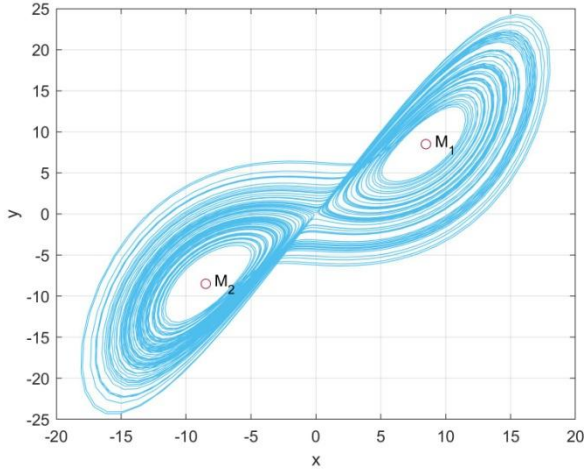


Рисунок 3.16

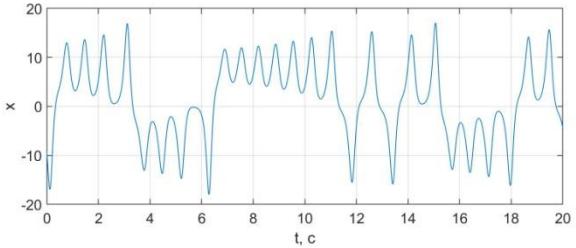


Рисунок 3.17

4 МЕТОДИ ПЕРЕДАЧІ ТА ЗАХИСТУ ІНФОРМАЦІЇ ЗА ДОПОМОГОЮ ДЕТЕРМІНОВАНО ХАОСУ НА БАЗІ СИСТЕМИ ЛОРЕНЦА

Синхронізація двох зв'язаних систем Лоренца

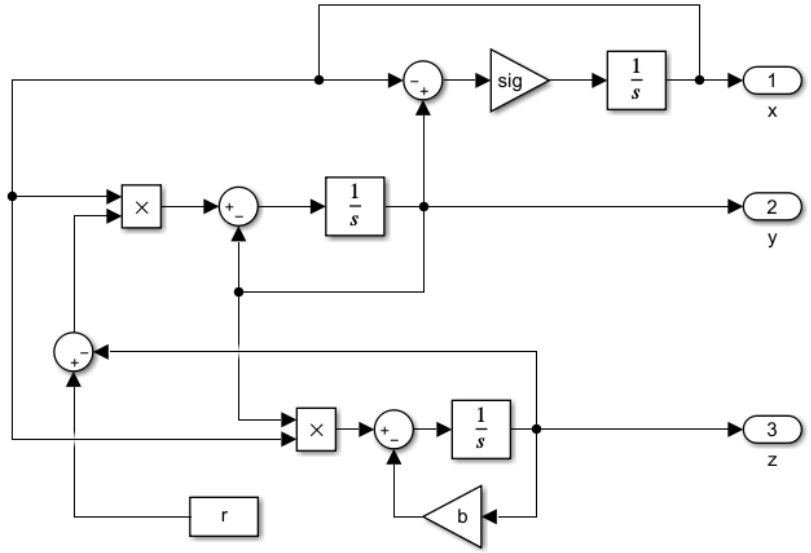


Рисунок 4.1 – Структурна схема ведучої системи Lorenz_1

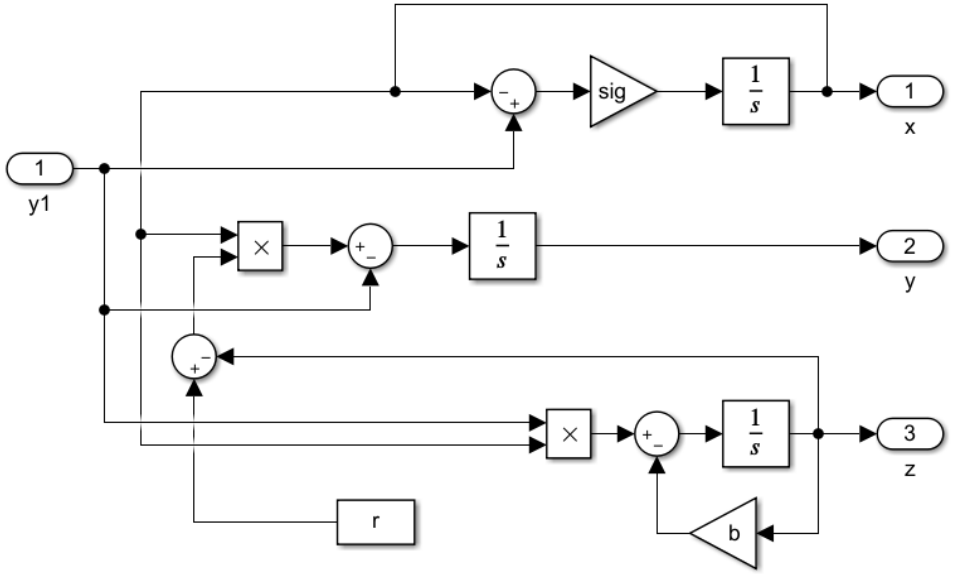


Рисунок 4.2 – Структурна схема веденої системи Lorenz_2

Для можливості передачі інформації за допомогою хаотичних коливань необхідно забезпечити режим синхронізації хаотичних генераторів.

Розглянемо пару, яка складається з ведучої та веденої систем Лоренца (рисунок 4.1 та 4.2). Ведена система відповідає системі (2.1) та аналогічна Simulink-моделі (3.6). Ведена система відрізняється від ведучої наявністю вхідного сигналу для синхронізації.

Режим синхронізація для системи (4.1) досягається за умови $y_1 = y_2$. Передбачається, що ведуча система пов'язана із стороною передачі, а ведена – відповідно зі стороною прийому.

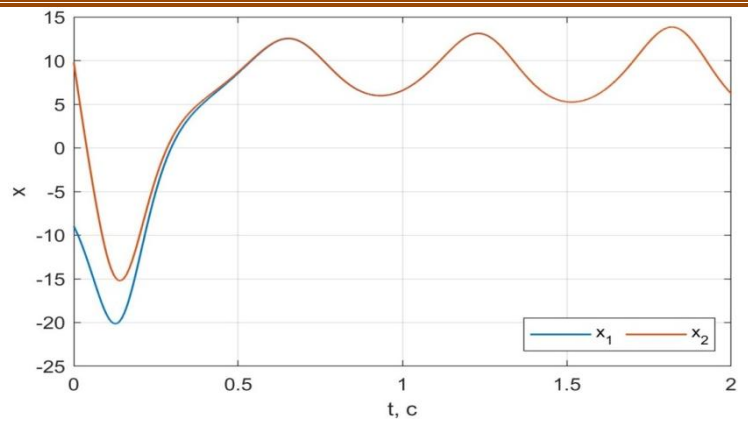


Рисунок 4.4 – Перехідний процес синхронізації на прикладі координат $x_1(t)$ та $x_2(t)$

Хаотичне маскування

Метод передачі інформації на основі ***хаотичного маскування*** полягає в наступному:

- інформаційний сигнал $s(t)$ смутується з хаотичним сигналом $x_1(t)$ генератора ведучої системи та передається каналом зв'язку;
- після встановлення режиму синхронізації вихідний сигнал $x_2(t)$ веденої системи приймача та хаотичний складова $x_1(t)$ переданого сигналу є ідентичними;
- демодуляцій здійснюється шляхом віднімання від прийнятого сигналу хаотичного сигналу $x_2(t)$ генератора веденої системи.

Синхронізація систем Lorenz_1 та Lorenz_2, що зображені на рисунку 4.5, здійснюється за допомогою координати $y(t)$. Параметри систем також вважаються ідентичними, а канал зв'язку такий, що не містить завад.

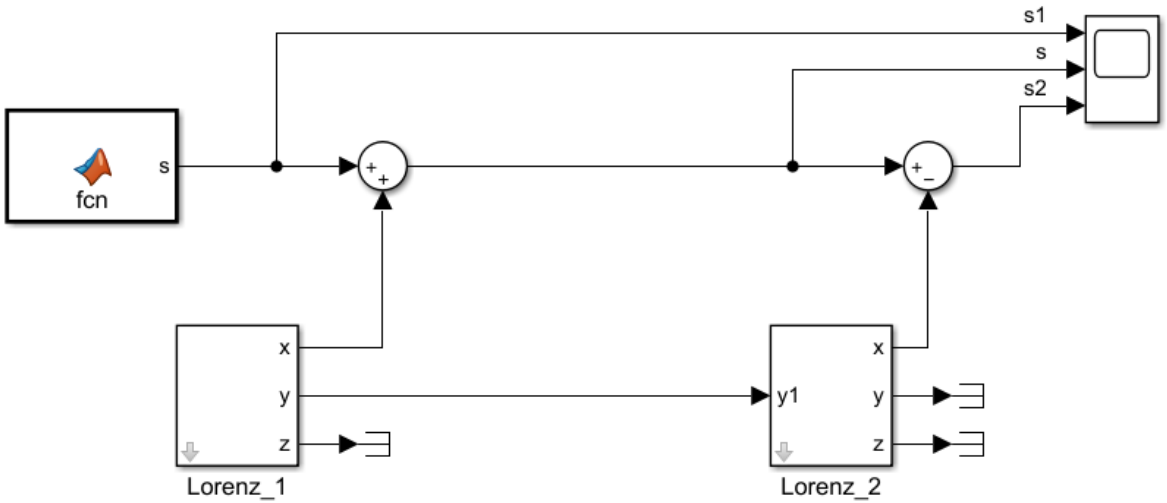
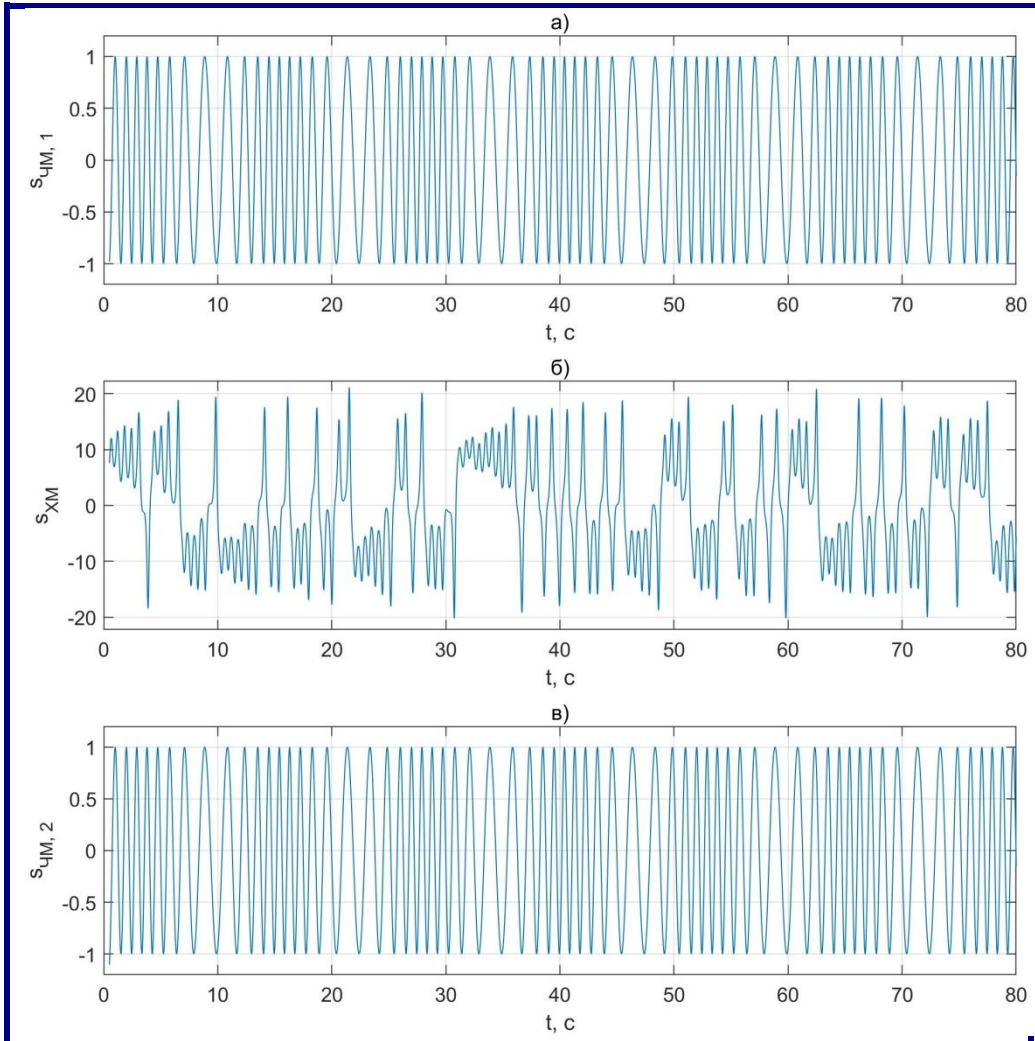


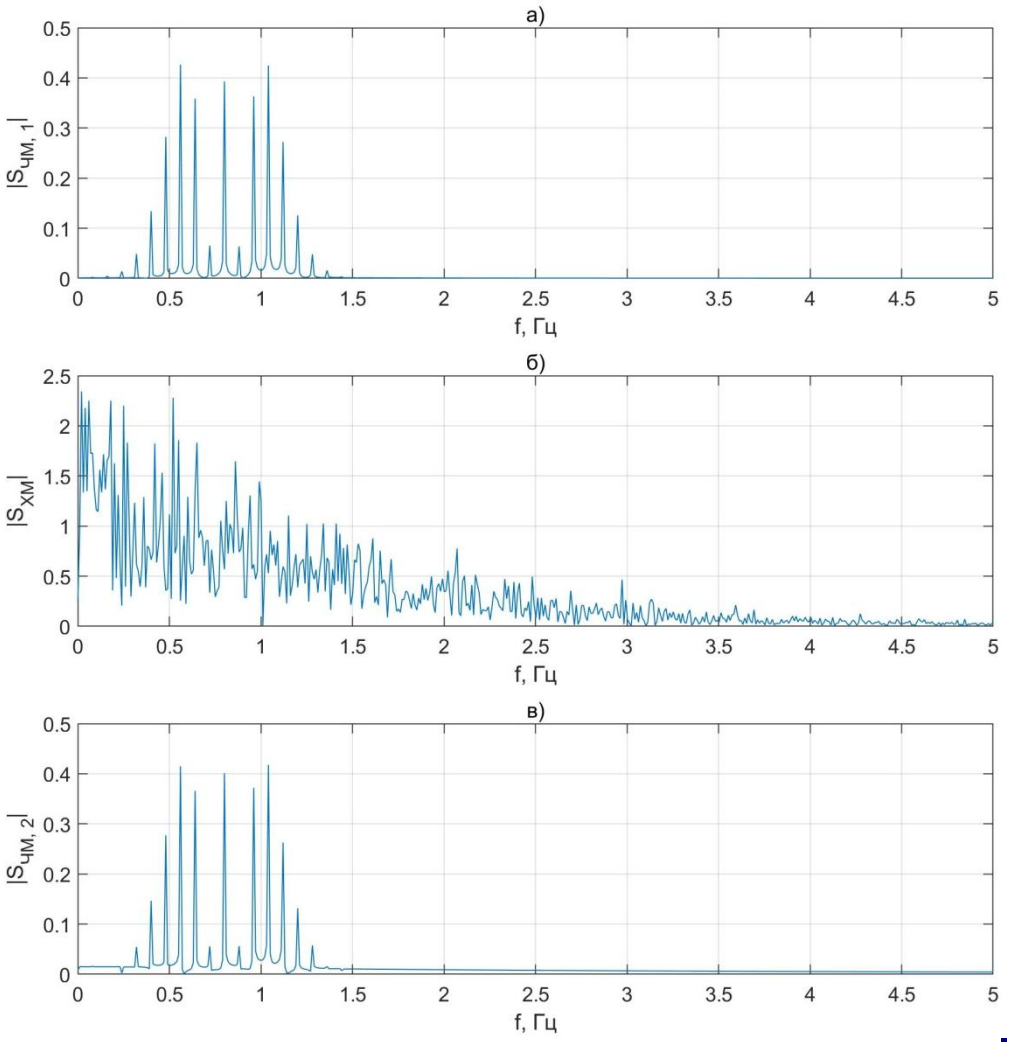
Рисунок 4.5 – Simulink-модель хаотичного маскування

Метод передачі, що оснований на хаотичному маскуванні, може володіти деякими ***конфіденційними властивостями*** за умови дотримання певних умов. Зокрема, маскуючий хаотичний сигнал повинен переважати інформаційний сигнал за спектральною потужністю та шириною робочої смуги частот [3]. Отже, хаотичне маскування можна розглядати як додатковий ступінь захисту при передачі інформації в телекомунікаційних системах.

Приклад хаотичного маскування ЧМ-сигналу



Сигнали в часовій області:
на вході системи Lorenz_1 (передавача) – а)
на виході системи Lorenz_1 (в каналі зв’язку) – б)
після демодуляції прийнятого сигналу системою Lorenz_2 – в)



Спектри сигналів:
на вході системи Lorenz_1 (передавача) – а)
на виході системи Lorenz_1 (в каналі зв’язку) – б)
після демодуляції прийнятого сигналу системою Lorenz_2 – в)

Передача бітових послідовностей шляхом перемикання хаотичних режимів генератора

Передачу цифрових сигналів за допомогою детермінованого хаосу можливо організувати шляхом ***перемикання хаотичних сигналів***, отриманих від генераторів із різним набором параметрів.

Схема, зображена ра рисунку 4.12, складається з двох пар однонаправлено з'єднаних хаотичних генераторів – Lorenz_1, Lorenz_2 та Lorenz_3, Lorenz_4 відповідно. Для систем Lorenz_1 і Lorenz_2 параметр $r = 25$, а для систем Lorenz_3 і Lorenz_4 – $r = 30$. Інші два параметри однакові для усіх систем ($\sigma = 10$, $b = 8/3$).

Вихідна бітова послідовність n_1 керує ключем S_{n1}, який перемикає подачу в канал зв'язку сигналів одного з двох ведучих хаотичних генераторів, що відповідають умовно логічному «0» чи «1».

Таким чином, синхронізація на приймальній стороні відбувається також почергово – в залежності від того, сигнал якого з двох хаотичних генераторів передавача приймається в даний момент часу.

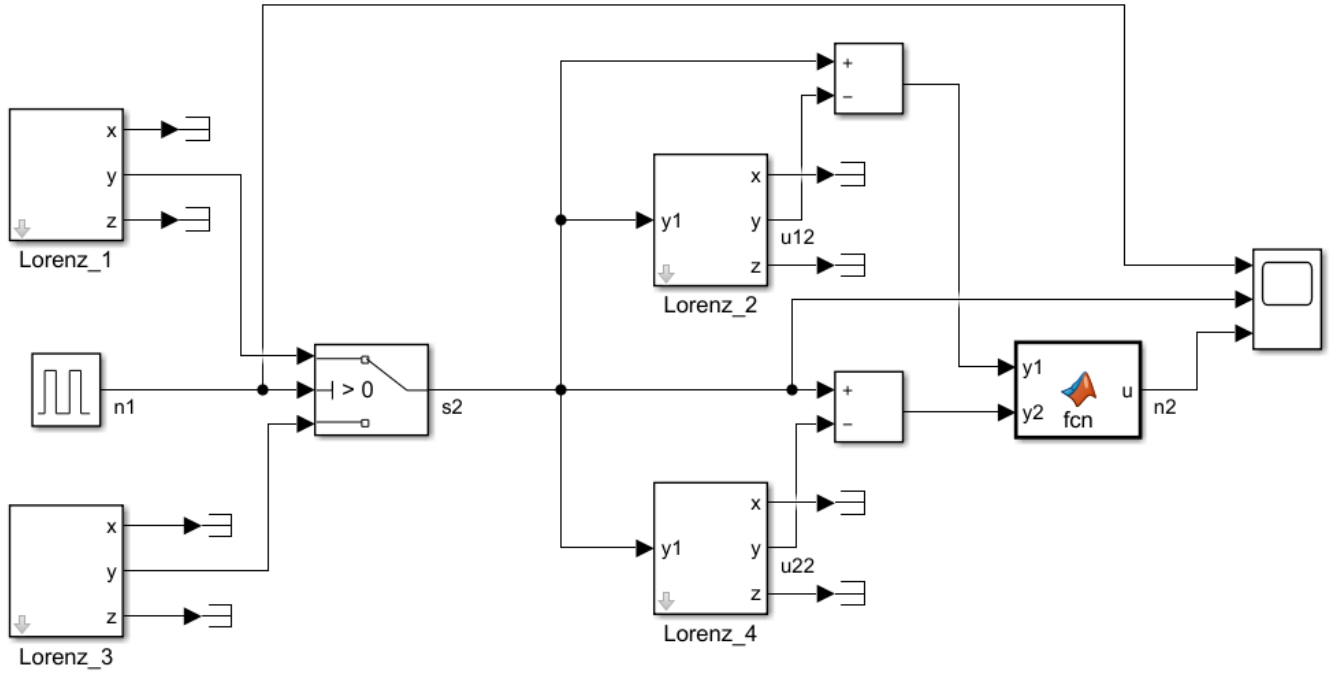


Рисунок 4.12 – Simulink-модель передачі цифрового сигналу шляхом перемикання хаотичних режимів

Демодуляція цифрового сигналу здійснюється шляхом порівняння сигналу на вході ведених систем приймача із вихідним сигналом ведених систем:

$$n_2 = \begin{cases} 0, & якщо \quad s_x - y_{12} = 0 \\ 1, & якщо \quad s_x - y_{22} = 0 \end{cases}, \qquad (4.5)$$

де S_x – сигнал в каналі зв'язку;

y_{12}, y_{22}– сигнали на виходах ведених систем Lorenz_2 та Lorenz_4 відповідно

Передача бітових послідовностей шляхом перемикання хаотичних режимів генератора

Спектр хаотичного сигналу в каналі зв’язку зображений на рисунку 4.13; часові залежності переданої та прийнятої бітової послідовності та сигналу в каналі зв’язку зображені на рисунку 4.14.

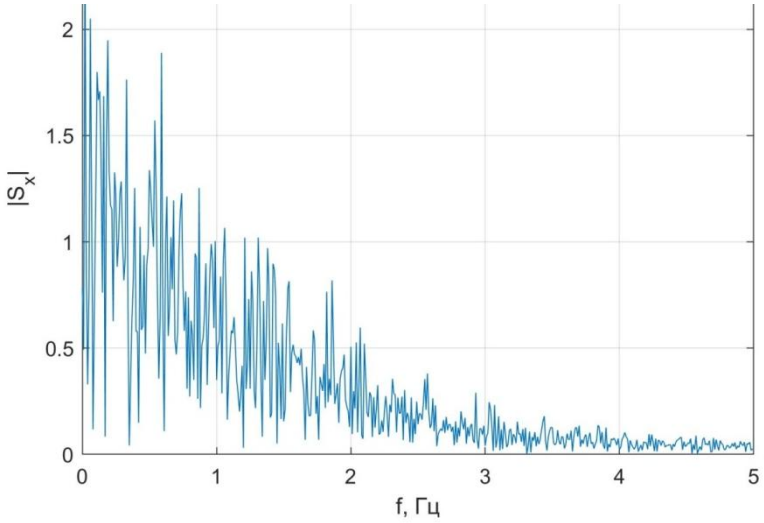


Рисунок 4.13 – Спектр сигналу з перемиканням хаотичних режимів

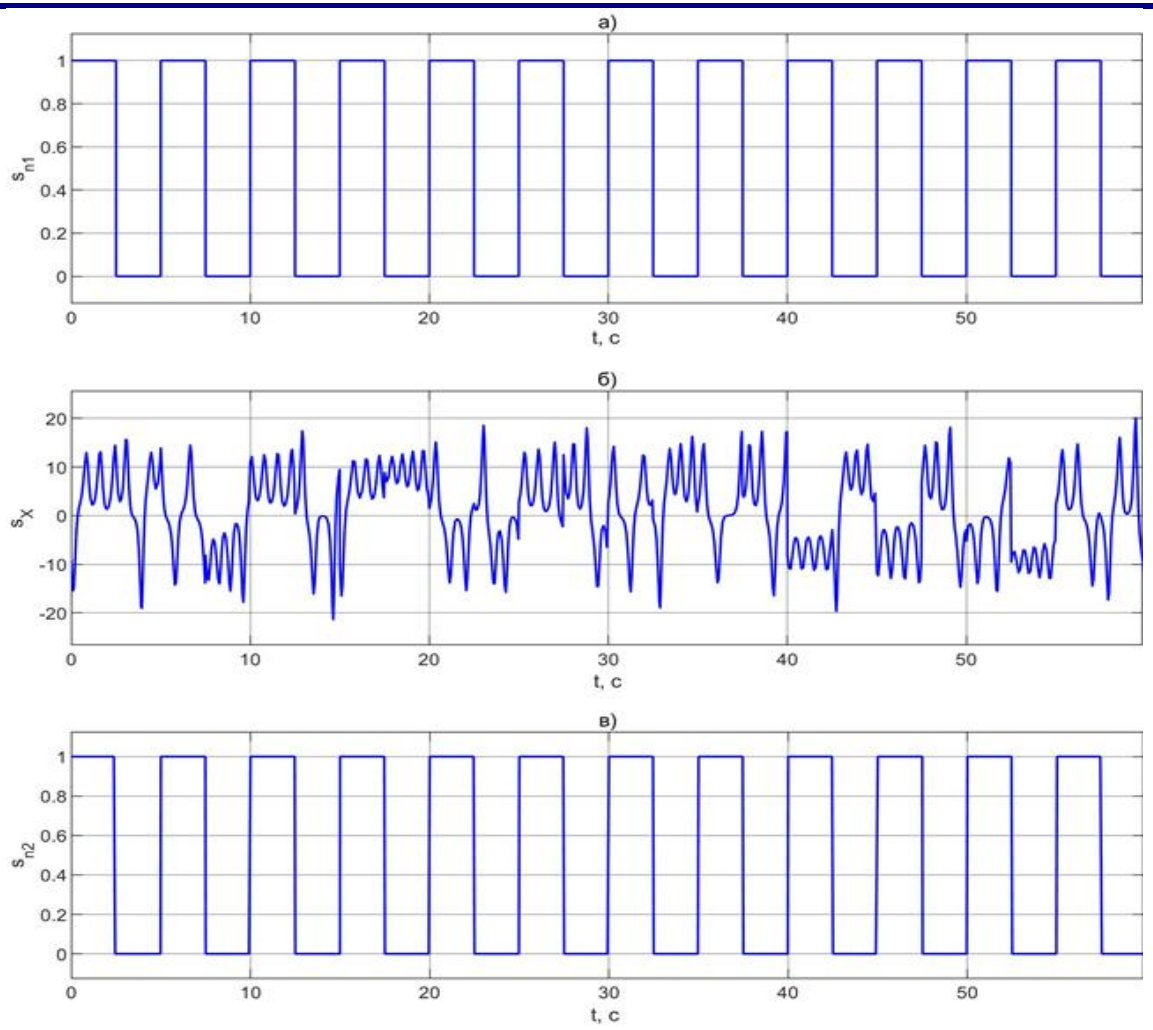


Рисунок 4.14 – Передача цифрового сигналу шляхом перемикання хаотичних режимів генератора передавача: вихідна бітова послідовність – а)
сигнал в каналі зв’язку – б)
прийнятий сигнал після демодуляції – в)

Шифрування даних за допомогою дискретних хаотичних послідовностей

Дискретно-часова система Лоренца може бути задана у вигляді системи нелінійних дискретних відображень:

$$\begin{cases} x(n+1) = \sigma\big(y(n) - x(n)\big)\Delta t + x(n) \\ y(n+1) = \big(x(n)\big(r - z(n)\big) - y(n)\big)\Delta t + y(n), \\ z(n+1) = \big(x(n)y(n) - bz(n)\big)\Delta t + z(n) \end{cases} \quad (4.6)$$

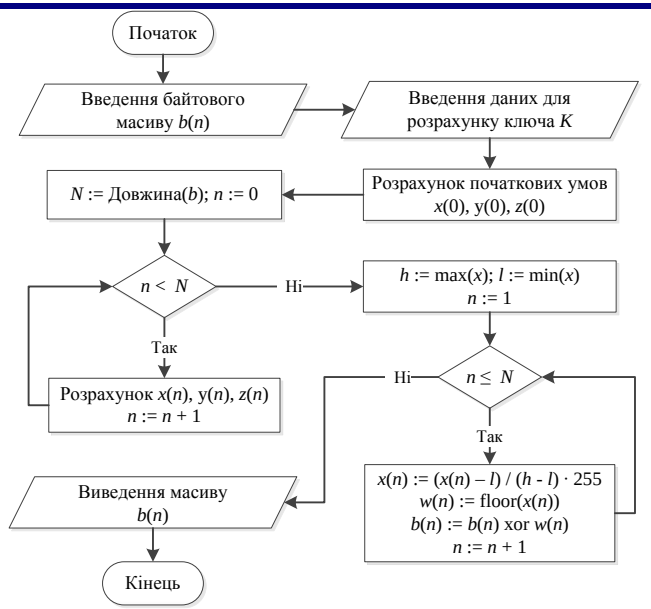
де σ, r, b – параметри системи, Δt – період дискретизації.

Отримані в результаті ітеративної процедури псевдовипадкові числові послідовності перетворюються в цілі двійкові числа згідно виразу:

$$w(n) = \left\lfloor \big(x(n) - l\big) / \big(h - l\big) \cdot \big(2^k - 1\big) \right\rfloor, \quad (4.7)$$

де k – розрядність двійкового представлення цілого числа,

h, l – відповідно максимальне та мінімальне значення послідовності x.



Алгоритм шифрування/дешифрування вихідного байтового масиву

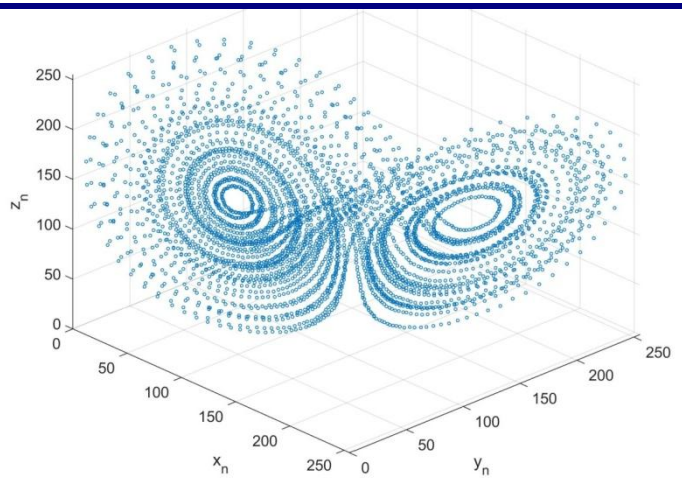


Рисунок 4.15 – Фазовий портрет дискретної системи Лоренца

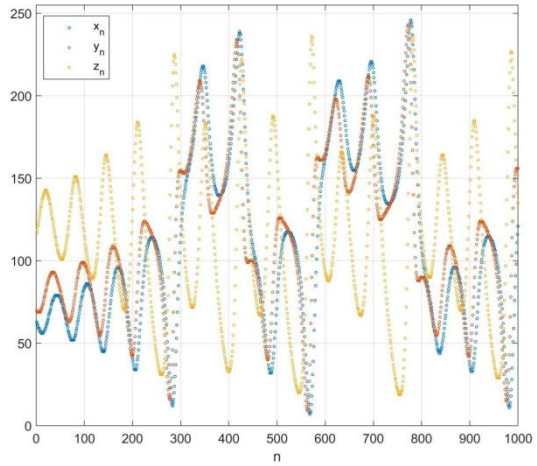
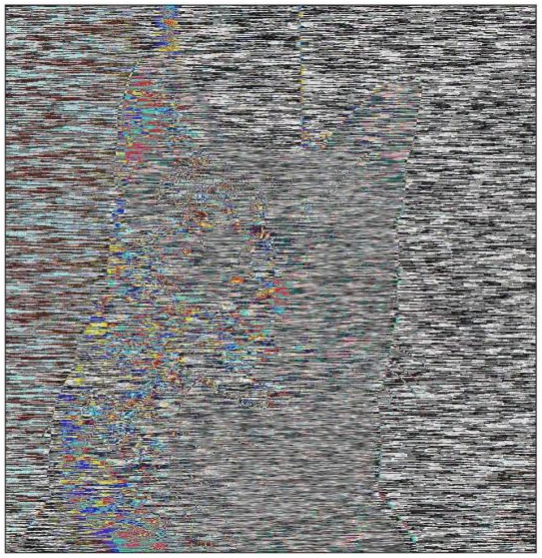


Рисунок 4.16 – Діаграми хаотичних псевдовипадкових послідовностей

а)



б)

в)

Рисунок 4.18 – Результат роботи програми шифрування:

вихідне .jpeg зображення – а)

зображення .jpeg після шифрування – б)

зображення .jpeg після дешифрування – в)

ВИСНОВКИ

В роботі представлено ряд методів, що основані на теорії детермінованого хаосу, за допомогою яких можливо підвищити ефективність та конфіденційність передачі інформації в телекомунікаційних система.

На базі динамічної системи Лоренца було розроблено комплекс імітаційних моделей хаотичних генераторів, систем синхронізації та передачі дискретних та аналогових сигналів за допомогою хаосу. Крім того запропоновано алгоритм шифрування даних за допомогою дискретних хаотичних відображень.

В ході виконання роботи були поставлені та вирішені таки дослідницькі задачі:

-аналіз методів та існуючих рішень щодо використання детермінованого хаосу для передачі інформації;

-аналіз математичних моделей динамічних систем, які можуть генерувати хаос;

-вибір засобів та алгоритмів для чисельного розрахунку та моделювання нелінійних систем (MATLAB/Simulink);

-моделювання синхронно зв’язаних хаотичних систем;

-моделювання процесу передачі сигналів за допомогою хаотичних систем

-розробка алгоритму та програмна реалізація шифрування даних дискретними хаотичними послідовностями.

Описані методи можуть бути застосовані для розробки та впровадження захищених конфіденційних систем зв’язку різного роду призначення.

За результатами дослідження були підготовлені тези доповіді для IX Міжнародної науково-технічної конференції молодих учених та студентів «Актуальні задачі сучасних технологій», яка проходила в Тернополі 20-26 листопада 2020 року.

ДЯКУЮ ЗА УВАГУ!

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Тернопільський національний технічний університет імені Івана Пулюя (Україна)
Національна академія наук України
Університет імені П'єра і Марії Кюрі (Франція)
Маріборский університет (Словения)
Технічний університет у Кошице (Словаччина)
Вільнюський технічний університет ім. Гедимінаса (Литва)
Шяуляйська державна колегія (Литва)
Жешувський політехнічний університет ім. Лукасевича (Польща)
Білоруський національний технічний університет (Республіка Білорусь)
Міжнародний університет цивільної авіації (Марокко)
Національний університет біоресурсів і природокористування України (Україна)
Наукове товариство ім. Шевченка
ГО «Асоціація випускників Тернопільського національного технічного університету імені Івана Пулюя»

АКТУАЛЬНІ ЗАДАЧІ СУЧАСНИХ ТЕХНОЛОГІЙ

Збірник

тез доповідей

Том ІІ

ІХ Міжнародної науково-технічної конференції молодих учених та студентів

25-26 листопада 2020 року

УКРАЇНА
ТЕРНОПІЛЬ – 2020

Матеріали IX Міжнародної науково-технічної конференції молодих учених та студентів.
Актуальні задачі сучасних технологій – Тернопіль 25-26 листопада 2020.

УДК 621.391

М.О. Слободян, М.О. Лівчук, С.К. Підченко, докт. техн. наук, проф.
Хмельницький національний університет, Україна

АЛГОРИТМ ШИФРУВАННЯ ДАНИХ ЗА ДОПОМОГОЮ ДИСКРЕТНИХ ХАОТИЧНИХ ПОСЛІДОВНОСТЕЙ

M.O. Slobodian, M.O. Livchuk, S.K. Pidchenko, Dr., Prof.

DATA ENCRYPTION ALGORITHM USING DISCRETE CHAOTIC SEQUENCES

Важливими аспектами проектування та розробки телекомунікаційних систем є захист та конфіденційність інформації. В роботі запропоновано алгоритм шифрування вихідного байтового масиву хаотичними числовими послідовностями, отриманими за допомогою дискретної моделі динамічної системи Лоренца [1, 2].

Дискретно-часова система Лоренца може бути задана у вигляді системи нелінійних дискретних відображень:

$$\begin{cases} x(n+1) = \sigma\big(y(n) - x(n)\big)\Delta t + x(n) \\ y(n+1) = \big(x(n)\big(r - z(n)\big) - y(n)\big)\Delta t + y(n), \\ z(n+1) = \big(x(n)y(n) - bz(n)\big)\Delta t + z(n) \end{cases} \quad (1)$$

де $\sigma = 10$, $r = 28$, $b = 8/3$ – параметри системи, Δt – час дискретизації.

Для вказаних значень параметрів система (1) демонструє нестійкість фазових траєкторій та сильною залежністю від початкових умов, про що свідчить додатне значення старшого показника Ляпунова $\lambda_0 > 0$ [1, 2].

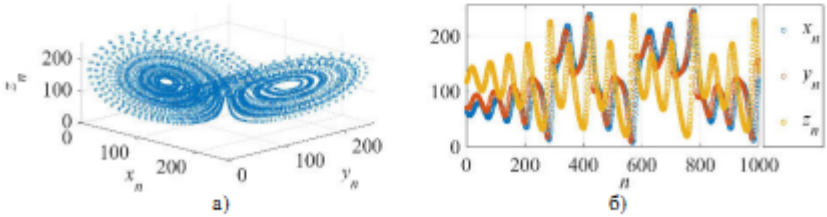
Отримані в результаті ітеративної процедури псевдовипадкові числові послідовності перетворюються в цілі двійкові числа згідно виразу:

$$w(n) = \left\lfloor \big(x(n) - l\big) \Big/ \big(h - l\big) \cdot \big(2^k - 1\big) \right\rfloor, \quad (2)$$

де k – розрядність двійкового представлення цілого числа,

h, l – відповідно максимальне та мінімальне значення послідовності x.

Фазовий портрет системи та діаграма хаотичних послідовностей показані на рис. 1.



а) б)

Рисунок 1. Фазовий портрет атрактора (а), та діаграми хаотичних послідовностей (б)

Вихідний байтовий масив b, що представляє собою інформаційне повідомлення, побітово сумується за модулем 2 з хаотичною послідовністю w. Отриманий в результаті шифрування код передається захищеним або відкритим каналом зв'язку та дешифрується на приймальній стороні аналогічним чином. Ключем шифру є дійсний вектор початкових значень $K = \big[x(0), y(0), z(0)\big]$. Криптографічна стійкість системи залежить від кількості можливих ключів шифрування [3]. Наприклад, дійсні числа,

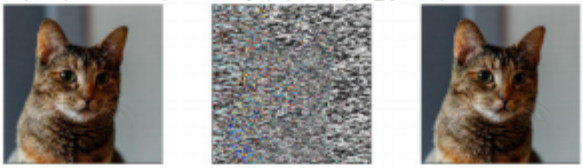
представлені у форматі з плаваючою комою подвійної точності мають 15 значущих цифр [4], тоді кількість ключів становитиме приблизно:

$$N_K \approx \left(10^{15}\right)^3 = 10^{45} \qquad (3)$$

Операції шифрування та дешифрування виконуються однією процедурою, блок-схема алгоритму якої зображена на рис. 2.

Рисунок 2. Алгоритм шифрування/дешифрування вихідного байтового масиву *b*

Описаний алгоритм шифрування (рис. 2) був реалізований на мові програмування Python 3. На рис.3 показано результат роботи програми на прикладі шифрування та дешифрування растрового зображення у форматі .jpeg розміром 1000×1000 пікселів.



а) б) в)

Рисунок 3. Результат роботи програми шифрування:
вихідне зображення (а), після шифрування (б), після дешифрування (в)

В результаті науково-практичного дослідження можна зробити наступні висновки:

1. Математичні моделі нелінійних систем із хаотичною динамікою можуть бути ефективно використані в якості генераторів послідовностей псевдовипадкових чисел в алгоритмах шифрування. Сильна чутливість до початкових умов забезпечує високу криптостійкість систем, побудованих на їх основі.

2. Описаний алгоритм шифрування даних за допомогою дискретних хаотичних послідовностей, згенерованих на основі динамічної системи Лоренца, дозволяє здійснювати шифрування і дешифрування довільних байтових послідовностей та може бути застосований в конфіденційних системах зв'язку, в тому числі телемедичних.

Література

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

2. Прикладне застосування теорії хаотичних систем у телекомунікаціях: монографія / [Ю.Я. Бобало, С.Д. Галюк, М.М. Климаш, Р.Л. Політанський]; Нац. ун-т «Львів. політехніка». – Львів: Коло, 2015. – 178 с.

3. Политанский Р.Л. Система передачи данных с шифрованием хаотическими последовательностями / Р.Л. Политанский, М.П. Шпатарь, А.В. Гресь, А.Д. Верига // Технология и конструирование в электронной аппаратуре. – 2014. – № 2-3. – С. 28–32.

4. Генри С. Уоррен. Числа с плавающей точкой // Алгоритмические трюки для программистов = Hacker's Delight. — М.: Вильямс, 2007. – С. 288.

Anti-Plagiarism v-15.257

Максимальное совпадение с одним документом 1.0%

Словари проверки: en_US, ru_RU, ua_UA. **Ошибок в документах: 10%**

	Документ		Суммарное совпадение по Базе Данных	
ID: 82576 Название: Конфіденційна система зв'язку з використанням пристроїв із хаотичною динамікою Добавлено в БД: 2020-12-06 Авторы: Лівчук Максим Олександрович Руководители: Підченко Сергій Костянтинович Консультанты: Опоненты:	Символы	Лексемы	Символы	Лексемы
	52796	762	1136 (2%)	15 (2%)

Источник плагиата

ID	Описание	Наличие плагиата в документе	
		Символы	Лексемы

UNICHECK

Имя пользователя:
Kafedra TMIT KhNU

ID проверки:
1005386794

Дата проверки:
07.12.2020 12:35:48 EET

Тип проверки:
Doc vs Internet + Library

Дата отчета:
07.12.2020 16:48:33 EET

ID пользователя:
100005657

Название файла: Лівчук_ТРм-19-1

Количество страниц: 76 Количество слов: 9497 Количество символов: 74307 Размер файла: 4.42 MB ID файла: 1005672066

1436 слов помечены как "исключенные" и не учитываются в подсчете слов

Обнаружены модификации текста (могут влиять на процент совпадений)

2.82%
Совпадения

Наибольшее совпадение: 0.84% с Интернет-источником (http://elar.khnu.km.ua/jspui/bitstream/123456789/4078/1/%D0.

2.43% Источники из Интернета	189	Страница 78
0.81% Источники из Библиотеки	6	Страница 79

5.5% Цитат

Цитаты	1	Страница 80

Не найдено ни одной ссылки

0% Исключений

Нет исключенных источников

Модификации

Обнаружены модификации текста. Подробная информация доступна в онлайн-отчете.

Замененные символы	4
Подозрительное форматирование	20 страниц

ВІДЗИВ

на дипломну роботу другого (магістерського) рівня студента групи ТРм-19-1
Лівчука Максима Олександровича

«Конфіденційна система зв'язку з використанням пристроїв із хаотичною динамікою»

Актуальність теми магістерського дослідження обумовлена проблемою захисту інформації, яка передається каналами зв'язку в телекомунікаційних системах. За допомогою методів стеганографії здійснюється приховання самого факт передачі інформації. Вільми корисними з точки зору захисту інформації можуть бути хаотичні сигнали, зокрема, вони можуть бути використані для прихованої передачі інформації на основі методу хаотичного маскування, де генерування дискретними динамічними системами псевдовипадкових числових послідовностей для використання в алгоритмах шифрування.

Метою дослідження є підвищення рівня конфіденційності та ефективності передачі інформації в телекомунікаційних системах.

Для досягнення поставленої мети в магістерській роботі виконується ряд задач, а саме:

- аналіз методів та існуючих рішень щодо використання детермінованого хаосу для передачі інформації;
- моделювання синхронно зв'язаних хаотичних систем;
- моделювання процесу передачі сигналів за допомогою хаотичних систем
- розробка алгоритму та програмна реалізація шифрування даних дискретними хаотичними послідовностями.

Дипломна робота представлена пояснювальною запискою обсягом 84 сторінки, складається з чотирьох основних розділів та додатку. Оформлення пояснювальної записки знаходиться на належному рівні.

За змістом робота є завершеною працею та містить достатньо посилань на літературу. Викладення матеріалу є послідовним та логічно правильним. Висновки добре обґрунтовані. Мова викладення роботи є технічно грамотною, зрозумілою.

Перевагою даної роботи є розроблення імітаційної моделі передачі цифрових сигналів шляхом маніпуляції хаотичних режимів генератора передавача та

розроблення алгоритмічно-програмного забезпечення процедури шифрування байтового масиву дискретними хаотичними послідовностями.

Серйозних недоліків робота не містить. Присутні незначні неточності, орфографічні та стилістичні помилки, які не впливають на суть роботи.

Вважаю, що дана робота відповідає загальним вимогам щодо дипломних робіт другого (магістерського) рівня, і заслуговує оцінки "добре", а Лівчук Максим Олександрович – присвоєння кваліфікації магістра зі спеціальності 172 – "Телекомунікації та радіотехніка".

Рецензент:

Зав. каф. АКІТТ
д.т.н., професор  Мартинюк В.В.

Завідувачу кафедри ТМІТ
Підченко С.К.
здобувача вищої освіти
Лівчук Максим
Олександрович

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 (а). Про використання програмно-технічних засобів для перевірки кваліфікаційних робіт здобувачів вищої освіти на плагіат оповіщений (а) 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.

08.12.2020
дата

підпис

РІШЕННЯ ЕКСПЕРНОЇ КОМІСІЇ ПО КАФЕДРИ
Телекомунікацій, медійних та інтелектуальних технологій (ТМІТ)
ПРО ДОПУСК КВАЛІФІКАЦІЙНОЇ РОБОТИ ДО ЗАХИСТУ

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

Назва: «Технологія побудови ефективної безпроводової мережі з використанням протоколу LoRaWAN»

Автор: Лівчук Максим Олександрович

Спеціальність: 172 Телекомунікації та радіотехніка

Освітня програма: Телекомунікації та радіотехніка

Науковий керівник: Підченко Сергій Костянтинович, д.т.н, доцент

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 досягненні. 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:

Виявлені в роботі збіги складають 2,82%, що виявленні в роботі є випадковими та не являються плагіатом. Дипломна робота допускається до захисту.

7.12.2020 р.

Відповідальний за перевірку на плагіат
к.т.н., доц. Пивовар О.С.

Зав. каф. ТМІТ
д.т.н., доц. Підченко С.К.