Міністерство освіти і науки України
Національний університет
«Львівська політехніка»

На правах рукопису

ПОЛІТАНСЬКИЙ РУСЛАН ЛЕОНІДОВИЧ

УДК: 621.391; 621.391.8

РОЗРОБЛЕННЯ ЗАВАДОЗАХИЩЕНИХ СИСТЕМ ПЕРЕДАВАННЯ ІНФОРМАЦІЇ НА ОСНОВІ ПСЕВДОВИПАДКОВИХ КОЛИВАНЬ ТА ФРАКТАЛЬНИХ СИГНАЛІВ

Спеціальність:
05.12.02 – телекомунікаційні системи та мережі

Дисертація
на здобуття наукового ступеня
доктора технічних наук

Науковий консультант
Ю.Я. Бобало
доктор технічних наук, професор

Ідентичність усіх екземплярів дисертації
ЗАСВІДЧУЮ

Вчений секретар спеціалізованої
вченої ради Д 35.052.10 Бондарєв А.П.

Львів – 2015

ЗМІСТ

СПИСОК УМОВНИХ ПОЗНАЧЕНЬ І СКОРОЧЕНЬ

СПІ – система передавання інформації;

ХС – хаотичні сигнали;

ХК – хаотичні коливання;

ФГШ – фрактальний гаусовий шум;

ФСГС – фрактальний сигнал гребінкової структури;

СМО – система масового обслуговування;

ПВП – псевдовипакові послідовності;

AWGN – адитивний білий гаусовий шум;

CRC-32 – циклічний надлишковий код;

ASCII – американський стандарт кодування інформації;

ЛКГ – лінійний конгруетний генератор.

ВСТУП

Актуальність теми. Сучасні тенденції розвитку алгоритмів кодування, шифрування та передавання інформації характеризуються використанням складних сигналів із базою, що сягає сотень, а іноді тисяч одиниць. Це обумовлено складністю структури таких сигналів, що забезпечує більшу ширину смуги сигналу при однаковій тривалості імпульсів у порівнянні із простими сигналами з невеликим значенням бази сигналу. Можливість використання таких сигналів обумовлена розвитком технологій генерування та розроблення наносекундних, а іноді й пікосекундних імпульсів.

Значні успіхи у створенні систем передавання інформації на основі імпульсів короткої тривалості були досягнуті завдяки використанню теоретичних напрацювань: В. Котельникова, В. Тіхонова, К. Шеннона, тощо. Практичне впровадження систем з використанням послідовності імпульсів невеликої тривалості, що формують широкосмугові сигнали, ґрунтувалося на проведені В. Болотовим, Л.Чуа та А. Потаповим експериментальних досліджень як окремих функціональних блоків так і повнофункціональних систем передачі інформації.

Використання широкосмугових сигналів в умовах дії завад забезпечує покращення показників енергетичної прихованості, завадостійкості та швидкості передавання інформації.

Особливістю сучасних телекомунікаційних систем є інтеграція методів і способів шифрування та кодування інформації.

Інтерес до використання генераторів хаотичних коливань у сучасних технологіях передавання інформації обумовлений можливостями генерування складних неперіодичних коливань відносно нескладними електронними схемами; керування параметрами хаотичних сигналів за допомогою незначних змін параметрів системи що їх генерує та отримання сигнального простору високої розмірності, а також нетрадиційним підходом до способів мультиплексування і демультиплексування, що ґрунтується на явищі синхронізації хаотичних коливань та ін.

При цьому актуальною залишається проблема зменшення значення відношення сигнал/шум, при якому можливе якісне та безпомилкове передавання інформації нескладними високопродуктивними системами.

Перспективним напрямком у вирішенні цього питання є використання у сучасному телекомунікаційному зв’язку широкосмугових сигналів.

Важливим завданням у даному напрямку є побудова фізичних моделей систем, що уможливлюють встановлення компромісу між допустимим значенням сигнал/шум, швидкістю передавання інформації та складністю їх реалізації.

При цьому є перспективним розроблення нових методів кодування/декодування інформації у телекомунікаційних системах з використанням псевдовипадкових та фрактальних сигналів. Потребує подальших досліджень моделювання процесу синхронізації генераторів псевдовипадкових коливань приймальної та передавальної сторін телекомунікаційних систем.

Залишаються недостатньо дослідженими властивості окремого виду псевдовипадкових сигналів типу фрактальний гаусовий шум. Існуюча дискретна модель фрактального гаусового шуму характеризується значенням показника Херста та коефіцієнту масштабування у часі, вплив якого на властивості ФГШ є недостатньо дослідженими.

Актуальним є питання синтезу нових видів фрактальних широкосмугових сигналів складної конструкції, що можуть бути використані у завадостійких телекомунікаційних системах.

Науково-прикладною проблемою, вирішенню якої присвячена дисертаційна робота, є розробка методів і моделей програмно-апаратної реалізації функціональних вузлів завадостійких телекомунікаційних систем та мереж із кодуванням інформації хаотичними коливаннями та фрактальними сигналами.

Зв’язок роботи з науковими програмами, планами, темами.

Робота виконувалася у відповідності до наукового напряму кафедри

телекомунікацій Національного університету «Львівська політехніка» - «Інфокомунікаційні системи та мережі», в рамках держбюджетної науково-дослідної теми «Дослідження та розроблення телекомунікаційних мережних систем для застосувань телематики та телеметрії» (ДБ/КОМ), (2011-2012 рр.), № держреєстрації 0111U001223, у якій автор був задіяний як відповідальний виконавець.

Мета та задачі дослідження – метою дисертаційної роботи є програмно-апаратна реалізація моделей телекомунікаційних систем та мереж із підвищеною завадостійкістю шляхом використання хаотичних та фрактальних сигналів.

Для досягнення мети необхідно було вирішити наступні задачі:

1. Розробити модель системи передавання шифрованих ПВП текстових повідомлень із забезпеченням синхронної роботи великої кількості користувачів.

2. Розробити модель канального кодування та дослідити його вплив на тривалість встановлення синхронізації приймальної та передавальної сторін телекомунікаційної системи передавання шифрованої ПВП цифрової інформації.

3. Розробити моделі та структурні схеми прихованого передавання інформації із використанням генераторів хаотичних коливань, що описуються неперервною функцією відображення та дослідити процеси проходження інформації у таких системах.

4. На основі математичної моделі ФГШ дослідити вплив коефіцієнту часового масштабування на статистичні, кореляційні та енергетичні властивості сигналів типу фрактальний гаусовий шум.

5. Змоделювати процеси проходження самоподібного трафіку у телекомунікаційних системах.

6. Розробити алгоритм та запропонувати метод розпізнавання інформаційних бітів закодованих сигналами ФГШ з різними показниками Херста за їх фазовими портретами.

7. Розробити структурну схему телекомунікаційної системи приймання/передавання інформації, що базується на розпізнаванні інформаційних бітів закодованих дискретними сигналами ФГШ за їх фазовими портретами.

8. Запропонувати структуру та розробити математичну модель фрактальних сигналів гребінкової структури, що складаються із елементарних прямокутних імпульсів однакової тривалості та амплітудами, значення яких залежать від формованого ними рівня фракталу.

9. Розробити та реалізувати кодер/декодер фрактальних сигналів гребінкової структури на основі мікроконтролера, згенерувати та дослідити їх властивості.

Об'єктом дослідження є процеси передавання та оброблення інформації в завадозахищених телекомунікаційних системах з використанням псевдовипадкових та фрактальних сигналів.

Предметом дослідження є хаотичні коливання і фрактальні сигнали та методи їх використання у телекомунікаційних системах.

Методи дослідження. Дослідження виконані з використанням теорії інформації та кодування, теорії сигналів і процесів, теорії ймовірності, числових методів розв'язування диференційних рівнянь, теорії фракталів, статистичних методів, математичного та комп'ютерного моделювання випадкових процесів, їх експериментальне дослідження.

Наукова новизна роботи:

1. Розвинута модель системи передавання текстових повідомлень на основі клієнт-серверної архітектури із використанням стандартного алгоритму CRC-32, ключами якого є псевдовипадкові послідовності, що генеровані дискретним логістичним відображенням із забезпеченням синхронного обміну інформацією між багатьма користувачами шляхом передавання значень контрольної суми, розрахованої за алгоритмом CRC-32. Конфіденційність процесу передавання інформації забезпечується потужністю простору ключів, що визначається точністю представлення

початкового значення хаотичного коливання та параметру керування логістичного відображення і становить 2^{29}.

2. Розвинуто метод оцінки впливу канального кодування на перебіг процесу встановлення синхронізації між генераторами хаотичних коливань приймальної та передавальної сторін телекомунікаційної системи. Показано, що використання відносно нескладних схем лінійного блокового кодування забезпечує зменшення часу встановлення синхронізації приймальної та передавальної сторін системи на 100…200 нс.

3. Набули подальшого розвитку методи синхронізації автоколивальних систем генерування хаотичних коливань із використанням функції подібності між сигналами головної та керованої систем. Вперше встановлено, що синхронізація генераторів псевдовипадкових коливань приймальної та передавальної сторін системи передавання інформації можлива при значеннях коефіцієнта зв'язку між ними e>2 та частоті зрізу фільтру низьких частот, що моделює канал зв'язку, u=6. Встановлені значення параметрів системи Лоренца, що описує генератор хаотичних сигналів σ, r, b, використовуваних для кодування цифрової інформації, при яких має місце стійка синхронізація та якісне передавання інформації в телекомунікаційних системах.

4. Вперше методом усереднення за реалізаціями отримані залежності енергетичних, кореляційних та статистичних властивостей сигналів типу фрактальний гаусів шум, що можуть використовуватися для кодування інформаційних бітів, від коефіцієнту часового масштабування. Виявлено, що для сигналів з показником Херста 0,1 має місце зростання їхньої дисперсії від 0,8 до 1,2 в діапазоні значень параметру часового масштабування n=1…50, а для сигналів із показниками Херста 0,5 (білий шум) та 0,9 (сірий шум) залежність дисперсії від параметру часового масштабування носить коливний характер. Встановлено, що в спектрі сигналу з показником Херста 0,1 (рожевий шум) при збільшенні коефіцієнта часового масштабування від 1 до 50, значення спектральної густини потужності зростає в два та три рази

при нормованих частотах 0,1 і 0,4 відповідно.

5. Набула подальшого розвитку теорія проходження трафіку через телекомунікаційні системи. У наближенні самоподібних потоків показано, що при значенні інтенсивності $0.9 \cdot 10^5$ запитів/годину та сумарній пропускній здатності вузлів мережі на рівні 180 запитів/с, пікові навантаження збільшують середній час перебування запитів у мережі на 6…25%, що обумовлено неможливістю компенсації черги у системі з часовими проміжками з інтенсивністю потоку меншою за пропускну здатність вузла.

6. Вперше розроблено метод декодування інформаційних бітів, кодованих сигналами типу фрактальний гаусів шум, що базується на порівнянні кількісних характеристик кластерів (корінь квадратний із суми квадратів відстаней від точок кластера до його центру), утворених у фазовому просторі прийнятих сигналів. При цьому розпізнавання інформаційних бітів закодованих ФГШ із показниками Херста 0,1 та 0,9 можливе при співвідношенні сигнал/шум у каналі рівному -7,5 дБ та при значенні похибки синхронізації рівному 80% від тривалості маркерного сигналу.

7. Вперше розроблено метод декодування інформаційних повідомлень представлених манчестерським цифровим форматом та закодованих псевдовипадковими сигналами типу ФГШ (250 відліків дискретних ФГШ із показниками Херста 0,9 та 0,1 для нижнього та високого рівнів відповідно). Метод базується на оцінюванні та порівнянні значень розпізнавальних параметрів кластерів сусідніх сигналів, є стійким до дії зовнішніх електромагнітних факторів та уможливлює процес декодування без визначення рівня шуму в каналі.

8. Набув подальшого розвитку метод синтезу широкосмугових сигналів типу «фрактальний сплайн» із використанням послідовності елементарних прямокутних імпульсів однакової тривалості з розподілом значень їх

амплітуди згідно заданому алгоритму. Це забезпечує формування самоподібної структури, що визначається коефіцієнтом утворення та кількістю твірних елементів. Показано, що такі сигнали є складними зі значеннями бази біля 200 для сигналів формованих імпульсами із п’ятьма твірними елементами. Їхні кореляційні та спектральні властивості подібні до шумоподібних сигналів і забезпечують значення коефіцієнту завадостійкості близьке до одиниці, що уможливлює їх розпізнавання в телекомунікаційних системах при дії значних зовнішніх завад.

Практичне значення одержаних результатів полягає у тому, що:

1. Запропонований метод декодування цифрової інформації, що базується на порівнянні кластерів отриманих сигналів сформованих у фазовому просторі (Пат. 106856 Україна, МПК H04L 9/00) не потребує визначення рівня шуму на приймальній стороні СПІ та забезпечує стійку роботу ТКС у складних електромагнітних обставинах.

2. Розроблено програмне забезпечення для моделювання процесу проходження самоподібного трафіку у телекомунікаційних системах.

3. Запропоновано метод оцінювання гранично можливого відношення сигнал/шум в умовах дії завад типу AWGN для моделювання процесів передавання інформації в телекомунікаційних системах.

4. Розроблена модель багатокористувацької системи шифрованого обміну текстовими повідомленнями, що підтримує: ідентифікацію користувачів за **IP**-адресою та унікальним ключем, що генерований логістичним відображенням, синхронізацію клієнтської та серверної частин за стандартним алгоритмом **CRC-32**; потокове шифрування повідомлень засобом ПВП, генерованих пороговим методом за логістичним відображенням.

5. Розроблений з використанням мікроконтролерів PIC18F2550 кодер/декодер фрактальних сигналів гребінкової структури можуть бути використанні в завадостійких системах передавання інформації.

Одержані в роботі наукові результати знайшли практичне

впровадження на підприємствах ПАТ «Укртелеком», Чернівецькій філії для прогнозування інтенсивності трафіку, що проходить через телекомунікаційні мережі підприємства; на підприємстві ПАТ «ТК Энергия», м. Харків для дослідження проходження трафіку із самоподібним розподілом; на підприємстві «Кодек-Фактор» при вимірюваннях інтенсивності трафіку та встановлення часу пікових навантажень; на підприємстві ПАТ «Utel», Чернівецькій філії рекомендовано для аналізу можливості інженерного проектування радіотехнічних систем, що використовують виділення інформаційного сигналу в умовах сильно зашумлених каналів методом синхронізації генераторів хаосу; в Чернівецькому національному університеті ім. Ю.Федьковича у навчальному курсі «Теорія інформації та кодування».

Публікації. За результатами дослідження опубліковано 53 наукові праці. Серед них опублікована 1 монографія у співавторстві, 29 статей, із яких – 24 статті у наукових журналах та збірниках наукових праць, що включені до Переліку наукових фахових видань України, 4 статті опубліковані у провідних закордонних журналах, одна стаття у електронному фаховому виданні та 25 тези та матеріали доповідей на конференціях. 23 статті індексовані у міжнародних науково-метричних базах. Отримані два патенти України на винахід та один патент на корисну модель.

Особистий внесок здобувача. Основні результати дисертаційної роботи, що висвітлені у пунктах наукової новизни та висновках, отримані здобувачем особисто. У публікаціях, опублікованих у співавторстві здобувачеві належать:

[1] – автору належать розробка та дослідження методу кластерного кодування, розроблення методу генерування та математичної моделі само подібних фрактальних сигналів, розвиток методу шифрування на основі алгоритму узагальненого відображення Пекаря; [2] – постановка задачі та розроблення програмного забезпечення для дослідження проходження трафіку через багатоканальну СМО із різними статистичними властивостями;

[3, 6, 35, 38] – розроблена математична модель і метод генерування ФСГС, отриманий аналітичний вираз спектральної густини їх потужності та досліджені спектри генерованих на основі отриманої моделі сигналів; [4, 39] – аналіз процесів проходження звукового сигналу через систему передавання інформації, і аналіз результатів; [5, 36] – розроблення цифрового генератора хаосу на основі мікроконтролера PIC18F2550; [7] – написання програми, що реалізує алгоритм шифрування зображень на основі тривимірного дискретизованого перетворення Пекаря та підбір оптимальних параметрів для шифрування зображень; [8] – дослідження процесів синхронізації із використанням алгоритму CRC-32 та його застосування у моделі багатокористувацького чату; [9] – дослідження роботи схеми і порівняння з іншими методами; [10, 42, 43] – розробка методики дослідження хаотичних сигналів типу дискретний ФГШ методом усереднення за реалізаціями сигналу, дослідження їх спектральних та статистичних властивостей; [11, 40] – аналіз властивостей ФГШ та впливу на них параметру часового масштабування; [12, 18, 44, 46] – аналіз криптостійкості методу шифрування, проведення досліджень роботи програми, аналіз результатів; [13] – розроблена математична модель та досліджено на її основі вплив кількості надлишкових бітів на тривалість процесу синхронізації; [14] – математичний аналіз системи із кубічною нелінійністю; [16, 21, 50] – аналіз областей хаосу та порівняння розрахункових і експериментальних результатів моделювання системи Лю ; [51] – дослідження алгоритмів оцінювання властивостей самоподібності хаотичних процесів; [15] – аналіз моделей систем генерування ПВП на регістрах зсуву з нелінійною функцією оброблення, написання програмного коду, що реалізує метод шифрування; [17, 31, 37, 45] – розроблення методу кластерного кодування з використанням ФГШ, розроблення методики дослідження залежності сигнал/шум від тривалості самого сигналу; [19] – участь у систематизації теоретичних поглядів на явище синхронізації у електронних схемах на основі аналізу літературних джерел; [22] – моделювання функціонування кільцевого автогенератора в

середовищі Multisim 11, аналіз математичних моделей кільцевого автогенератора; [23] – постановка задачі визначення оптимальних параметрів співвідношення потужностей інформаційного сигналу та псевдовипадкового переносника у процесах проходження синусоїдних та ЧМ коливань через кільцевий автогенератор, аналіз результатів; [24, 52] – аналіз літературних джерел та моделювання СПІ з використанням генераторів ПВК, що описані системою рівнянь Лоренца, знаходження областей хаосу методом математичного моделювання; [25-27, 30, 53] – розроблення комп'ютерних програм на мові С++ для генерування бінарних ПВП та дослідження їх властивостей; [28, 29] – дослідження процесів генерування ПВК генераторами Чуа, кільцевими автогенераторами та їх синхронізації, [31] – розробка методу декодування, що не потребує визначення рівню шуму в каналі зв'язку, оцінювання можливостей функціонування системи в умовах складних електромагнітних обставин, оформлення документів на патент; [32] – розроблення методу криптографічного стиснення із підвищеною швидкістю оброблення інформації на основі відомого прототипу; [33] – постановка задачі та схемо-технічне моделювання, оформлення документації на патент пристрою для вивчення загорткового коду, [49] – розроблення методів генерування ПВП.

Апробація результатів дисертації. Результати досліджень, що приведені в дисертації, були представлені на 15 наукових, науково-практичних конференціях, форумах, симпозіумах та школах-семінарах: 4-а Міжнародна конференція «Проблеми телекомунікацій – 2010» (ПТ-10), 2-а Студентська науково-технічна конференція (СК-12) «Проблеми телекомунікацій» (Київ, НДІТ НТУУ, 2010), 4-а Міжнародна науково-технічна конференція молодих вчених «Computer Science and Engineering 2010 (CSE-2010)» (Львів, НУ «Львівська Політехніка», 2010), 1-а Всеукраїнська науково-практична конференція «Фізико-технологічні проблеми радіотехнічних пристроїв, засобів телекомунікацій, нано- та мікроелектроніки» (Чернівці, ЧНУ ім. Ю. Федьковича, 2011), XII

Міжнародна науково-практична конференція «Сучасні інформаційні та електронні технології» (Одеса, Травень, 2011), 8-а Міжнародна науково-технічна конференція «Сучасні інформаційно-комунікаційні технології» (Крим, 2012), 11-а та 13-а Міжнародна IEEE конференція «Modern Problems of Radio Engineering, Telecommunications, and Computer Science (TCSET)» (Львів-Славське, НУ «Львівська Політехніка», 2012, 2014), 2-а, 3-я та 4-а Міжнародна науково-практична конференція «Фізико-технологічні проблеми радіотехнічних пристроїв, засобів телекомунікацій, нано- та мікроелектроніки (PREDT)» (Чернівці, ЧНУ ім. Ю. Федьковича, 2012, 2013, 2014), 6-ий Міждународний науково-технічний симпозіум «Новые технологии в телекоммуникациях» (Київ-Вишків, ДУІКТ, 2013), 12-а Міжнародна IEEE коференція «The Experience of Designing and Application of CAD Systems in Microelectronics » (CADSM) (Поляна-Свалява, НУ «Львівська Політехніка», 2013), 4-а Міжнародна науково-практична конференція «Обробка сигналів і негауссівських процесів» (Черкаси, ЧДТУ, 2013), 2-а Міжнародна науково-технічна конференція «Інформаційні проблеми теорії акустичних, радіоелектронних і телекомунікаційних систем» (IPST) (Алушта, НТУ «Харківський Політехнічний Університет», 2013).

Структура та обсяг дисертації

Дисертаційна робота складається із вступу, 6 розділів, висновків, списку літератури, що налічує 221 найменування на 24 сторінках, 3 додатки на 9 сторінках, 161 рисунок, 10 таблиць, загальний обсяг роботи становить 300 сторінок.

РОЗДІЛ 1. СУЧАСНИЙ СТАН ПРОБЛЕМИ ГЕНЕРУВАННЯ ТА ЗАСТОСУВАННЯ ХАОТИЧНИХ ШИРОКОСМУГОВИХ СИГНАЛІВ У ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ

1.1. Теоретичні засади моделювання телекомунікаційних систем передавання інформації з використанням псевдовипадкових коливань

Традиційно сигнали розділяються на два великі класи: стохастичні та детерміновані [54, 55]. Стохастичні сигнали – це сума випадкових процесів, кожен із яких визначається відповідною густиною імовірності, тоді як детерміновані сигнали генеруються детермінованими динамічними системами, що можуть перебувати у одному із множини можливих станів: нерухомі точки, періодичні, квазіперіодичні та псевдовипадкові коливання. Ці режими відрізняються один від одного складністю динаміки траєкторій системи у фазовому просторі, та обумовлені різною кількістю показників Ляпунова, що мають додатній знак. Детерміновані сигнали можна описати математично за допомогою диференційних або різницевих рівнянь, в залежності від того, є процес, що розглядається, неперервним чи дискретним.

Нерухома точка та періодичні коливання є найбільш простим прикладом стану і осциляцій у стабільній системі відповідно.

Найбільш загальною моделлю систем, що генерують псевдовипадкові коливання, є система звичайних нелінійних диференційних рівнянь, які у більшості випадків не мають аналітичного розв’язання:

$$\begin{cases} \dot{x}_1 = f_1\left(x_1,\ldots,x_i,\ldots x_n\right) \\ \ldots \\ \dot{x}_i = f_i\left(x_1,\ldots,x_i,\ldots x_n\right) \\ \ldots \\ \dot{x}_n = f_n\left(x_1,\ldots,x_i,\ldots x_n\right) \end{cases} \qquad (1.1)$$

Використання псевдовипадкових коливань у телекомунікаційні системи здійснювалось на основі трьох значних наукових досягнень.

На початку 1980-х років були розроблені електронні схеми генерування псевдовипадкових коливань з живленням від джерела постійного струму [56-58], що дозволило перенести абстрактні математичні моделі у галузь електронної інженерії.

Другим фундаментальним відкриттям, що уможливило використання систем із псевдовипадковими коливаннями в телекомунікаціях, є відкриття у 1990 році Каролем та Пекорою явища синхронізації двох генераторів псевдовипадкових коливань [59] за умови певних співвідношень між параметрами систем та способу передавання енергії коливань від однієї системи до іншої. Це явище наштовхнуло на думку, що шумоподібний спектр псевдовипадкових коливань може покращити завадостійкість та стеганографічні властивості телекомунікаційних систем.

Третьою фундаментальною особливістю систем із псевдовипадковими коливаннями є існування атрактора у вигляді фрактальної множини точок фазового простору, до якої прямують фазові траєкторії системи з розвитком у часі [60]. Будь-які достатньо сильні нерегулярності, що зустрічаються у природі з плином часу, отримують фрактальну структуру, внаслідок чого реально існуючі нелінійні динамічні системи мають фрактальні атрактори (наприклад, атрактори Лоренца та Реслера). Це означає, що надзвичайно нестійкі фазові траєкторії таких систем протягом часу перетворюються на фрактали. Результати дослідження самоподібності процесів у природі висвітлено у літературних джерелах [61, 62]. На даний час регулярно друкується журнал “Fractals”, метою якого є висвітлення результатів досліджень властивостей фракталів [63].

Вище зазначені відкриття були використані у моделюванні систем передавання інформації з використанням псевдовипадкових коливань. Прикладом таких систем є прямохаотичні широкосмугові системи зв’язку [64, 65].

Явище виникнення псевдовипадкових коливань було досліджене Лоренцом у 1968 році. Розв’язки системи диференційних рівнянь, що названа

його іменем, виявилися надзвичайно чутливими до початкових умов. Тьєном Лі та Джеймсом Йорком у 1975 році у роботі “Period three implies chaos” [66] вперше був використаний термін «хаос» для одновимірного відображення, математична модель якого має наступний вигляд:

$$x_{n+1} = x_n \cdot \left(1 - x_n / K\right) \qquad (1.2),$$

де x_n, x_{n+1} – текуче та наступне значення, K – дійсне число.

Саме вони вперше показали, що відносно нескладне відображення може генерувати складну динаміку.

Дослідження систем із псевдовипадковими коливаннями дозволили висунути гіпотези, що описують механізми переходу до псевдовипадкових коливань шляхом подвоєння періоду (біфуркації) [60, 67] та перемішування [57].

Український вчений О. М. Шарковський довів теорему про зародження псевдовипадкових коливань шляхом біфуркації подвоєння періоду, що уможливлює встановлення перехідних зон від періодичних коливань до псевдовипадкових [68], та теорему про нерухому точку відображення, що трансформує одиничний відрізок у самого себе [69, 70]. Вище зазначені теореми описують поведінку будь-якого дискретного відображення. Перехід до псевдовипадкових коливань через біфуркації подвоєння періоду є можливим кількість нерухомих точок дорівнює 2^k, де k – ціле додатне число. Результати моделювання режиму генерування псевдовипадкових коливань системою, що має 16 нерухомих точок для логістичного відображення наступного вигляду [70]:

$$x_{n+1} \equiv \lambda \cdot x_n \cdot \left(1 - x_n\right) \qquad (1.3)$$

З подальшим збільшенням періоду біфуркацій виникають коливання з періодом, що дорівнює трьом. У цьому випадку за теоремою Шарковського система має як завгодно багато періодичних точок з періодами більшими трьох. Біфуркаційна діаграма розвитку псевдовипадкових коливань у випадку одновимірних дискретних відображень приведена на рис.1.1.

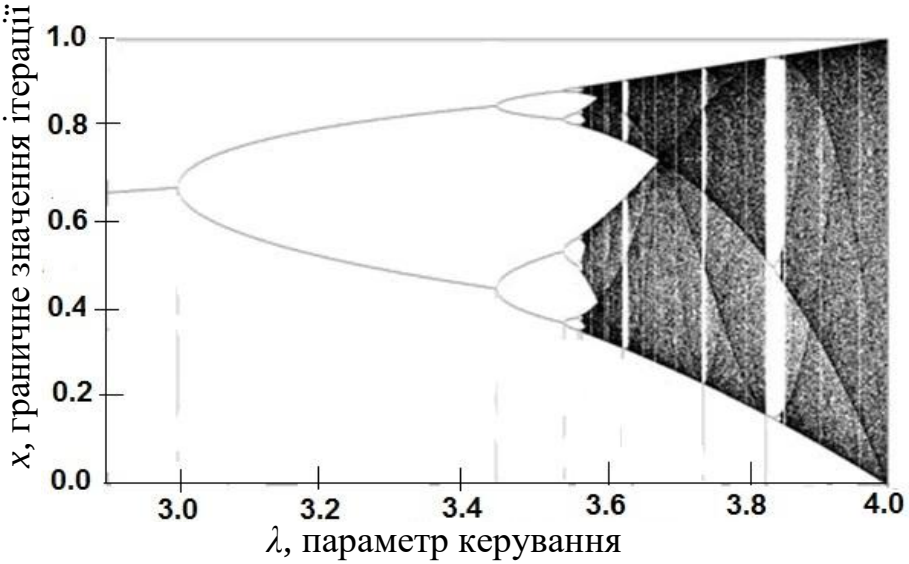


Рис.1.1. Діаграма біфуркацій для
логістичного відображення $x_{n+1} = \lambda \cdot x_n \cdot (1 - x_n)$ [74]

Використовуючи властивості масштабування Фейгенбаум [71, 72] розвинув теорію псевдовипадкових коливань та застосував метод ренормування груп для дослідження їх особливостей.

Помо та Манневіллем [73] був досліджений механізм переходу до псевдовипадкових коливань шляхом чергування у часі псевдовипакових та періодичних коливань, що є розв'язками диференційних рівнянь системи Лоренца:

$$\begin{cases} \dot{x} = \sigma \cdot (y - x) \\ \dot{y} = r \cdot x - y - x \cdot z \\ \dot{z} = -b \cdot z + x \cdot y \end{cases} \qquad (1.4)$$

Зупинимось детальніше на системі Лоренца [74], що надзвичайно широко використовується у наукових дослідженнях, результатом яких була отримана узагальнена система рівнянь Лоренца [75]:

$$\dot{x} = A \times x + c \times x \times B \cdot x, \quad (1.5)$$

де $x=\left[x_1,x_2,x_3\right]^{\mathrm{T}}$, $A=\begin{bmatrix} a_{11} & a_{12} & 0 \\ a_{21} & a_{22} & 0 \\ 0 & 0 & \lambda_3 \end{bmatrix}$, λ_3, a_{11}, a_{12}, a_{21}, a_{22} – дійсні числа,

$$c=\left[c_1,c_2,c_3\right]^{T},\ B=\begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & -1 & 0 \end{bmatrix}.$$

До правої частини узагальненої системи рівнянь Лоренца входить лінійний оператор A та нелінійний член, що заданий вектором c і матрицею B. При цьому власні значення матриці А повинні задовільняти наступному співвідношенню:

$$-\lambda_2>\lambda_1>-\lambda_3>0 \qquad (1.6)$$

Іншими відомими системами із псевдовипадковою динамікою, що були розроблені на основі систем звичайних диференційних рівнянь, є так звані системи третього порядку Чена [75], Реслера [76, 77] та Спротта [78] і система четвертого порядку Лю [79, 80], що описуються системами диференційних рівнянь (1.10), (1.11), (1.12) та (1.13) відповідно.

$$\begin{cases} \dot{x}=a\cdot\left(y-x\right) \\ \dot{y}=\left(c-a\right)\cdot x-x\cdot z+c\cdot y, \\ \dot{z}=x\cdot y-b\cdot z \end{cases} \qquad (1.10)$$

$$\begin{cases} \dot{x}=-y-z \\ \dot{y}=x+a\cdot y \\ \dot{z}=b+\left(x-r\right)\cdot z \end{cases} \qquad (1.11)$$

$$\begin{cases} \dot{x}=y \\ \dot{y}=-x+y\cdot z \\ \dot{z}=1-y^2 \end{cases} \qquad (1.12)$$

$$\begin{cases} \dot{x}=a\cdot\left(x-y\right) \\ \dot{y}=b\cdot x-h\cdot x\cdot z+\lambda\cdot w \\ \dot{z}=c\cdot x^2-d\cdot z \\ \dot{w}=-n\cdot y \end{cases} \qquad (1.13),$$

де x, y, z та w – змінні, що описують стан систем, a, b, c, d, r, λ, n — їх параметри.

Система (1.12) що налічує біля тридцяти модифікацій, праві частини, яких є поліномами другого або вищого степеню, була досліджена шляхом комп'ютерного моделювання американським вченим Дж. Спроттом у 1999 році [61].

Системи із псевдовипадковою динамікою характеризують наступні властивості [57, 60]:

– Суттєва залежність від початкових умов. Якщо початкові точки траєкторій системи у фазовому просторі знаходяться на як завгодно малій відстані, то протягом певного проміжку часу різниця між цими траєкторіями стає значною. Таку властивість іноді також називають «ефектом метелика» — за історичною метафорою, присвоєною їй Лоренцом, який вперше спостерігав цю особливість для названої його іменем системи рівнянь.

– Властивість щільності суть якої полягає у тому, що якщо у довільному околі будь-якої точки існує принаймі одна, а значить і безмежна кількість періодичних точок. Наслідком даної властивості є існування атрактора системи.

– Властивість транзитивності, що полягає в існуванні такого проміжку часу, протягом якого траєкторії множин, що не мали спільних точок в початковий момент часу, починають перетинатись.

Наслідком третьої властивості є дивний атрактор – об'єкт, що притягує до себе траєкторії системи у фазовому просторі. Назва «дивний» атрактор пов'язана із незвичайною його структурою, що обумовлена транзитивністю, тобто за будь-якого масштабу через виділену область атрактора завжди проходитимуть траєкторії системи.

Чисельними мірами псевдовипадкових коливань прийнято вважати показники Ляпунова та кореляційну розмірність [57, 60].

Показники Ляпунова характеризують середню швидкість сходження

або розбігання траєкторій системи у фазовому просторі. Якщо дійсна частина хоча б одного показника Ляпунова є додатною, то траєкторії системи у фазовому просторі розбігаються; для того, щоб траєкторії збігались, усі дійсні частини показників Ляпунова мають бути від'ємними [57].

У випадку додатнього показника Ляпунова у динамічній системі спостерігаються псевдовипадкові коливання, часовий масштаб яких тим менший, чим більше значення показника. Тому особливо важливою задачею є визначення найбільшого (або старшого показника Ляпунова) [81]. У фазовому просторі неперервної у часі динамічної системи має місце видовження у напрямку додатніх показників Ляпунова та стиснення у напрямку від'ємних – перетворення сфери на еліпсоїд [57] (рис.1.2).

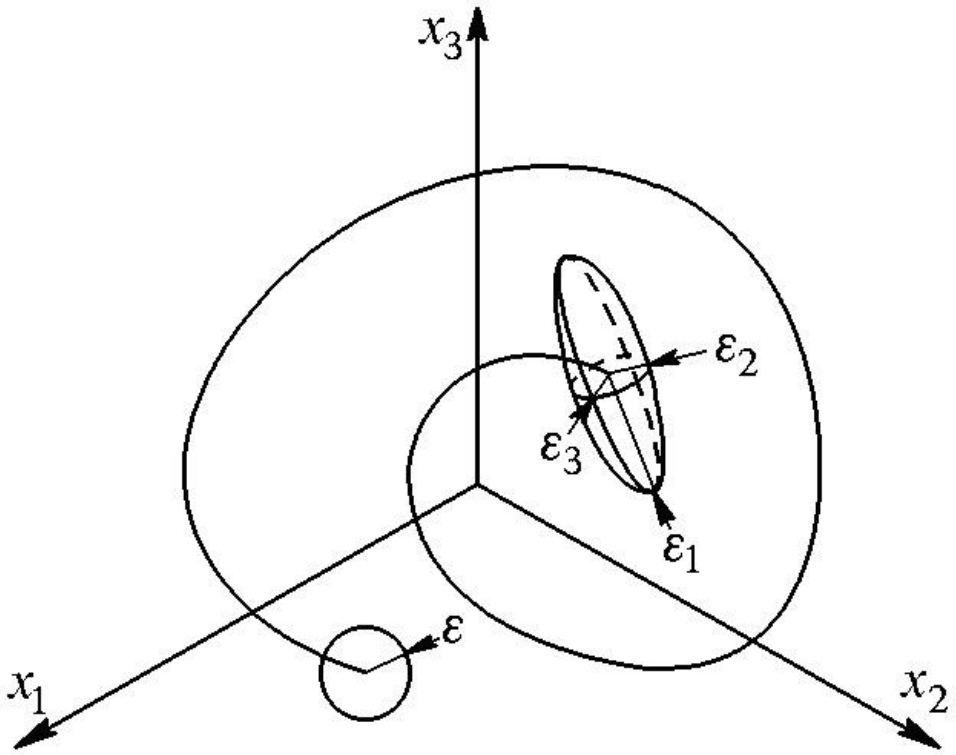


Рис.1.2. Геометрична інтерпретація спектру показників Ляпунова. Кожен із показників характеризує зміну масштабу вздовж головних осей еліпсоїда ε_1, ε_2, ε_3 , у який перетворюється нескінченно мала кулька із центром на досліджуваній траєкторії за деякий час T [57]

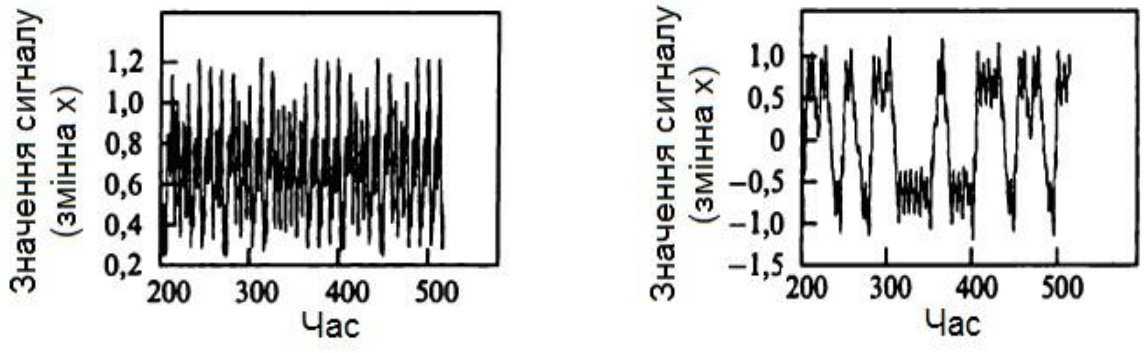
Для систем із точно визначеною динамікою, що описується системою диференційних рівнянь спектр показників Ляпунова визначається за так званим алгоритмом Бенеттіна [81, 83].

Однією із найбільш досліджених систем, що генерують хаос є так званий кільцевий генератор, математична модель якого описує систему рівнянь:

$$\begin{cases} \dfrac{dx}{dt} = \dfrac{F(z) - x}{T} \\ \dfrac{dy}{dt} = \omega^2 \cdot (x - z), \\ \dfrac{dz}{dt} = y - \alpha \cdot z \end{cases} \quad (1.14)$$

де α, ω, T, M, E_1, E_2 – параметри системи; $F(z)$ – значення функції, що є характеристикою нелінійного елемента в точці z.

Дослідження роботи кільцевих генераторів при різних значеннях параметрів системи α, ω, T, M, E_1, E_2 здійснювалися чисельним моделюванням методом Рунге-Кутта [84]. Результати моделюваня приведені на рис.1.3; 1.4; 1.5; 1.6.



а) б)

Рис. 1.3. Форма сигналу на виході підсистеми 2 ($x(t) \equiv U_{c1}$) при фіксованих значеннях коефіцієнтів $\alpha = 0{,}22$, $T = 3$, $\omega = 1$, $E_1 = 0{,}5$, $E_2 = 2$ та значеннях коефіцієнтів підсилення: $м$ =2,8 (а); $м$ =5 (б) [84]

а) б)

Рис. 1.4. Фазовий портрет в площині x - z ($z \equiv U_{c2}$) при фіксованих значеннях коефіцієнтів $\alpha = 0{,}22$, $T = 3$, $\omega = 1$, $E_1 = 0{,}5$, $E_2 = 2$ та значеннях коефіцієнтів підсилення: M =2,8 (а); M =5 (б) [84]

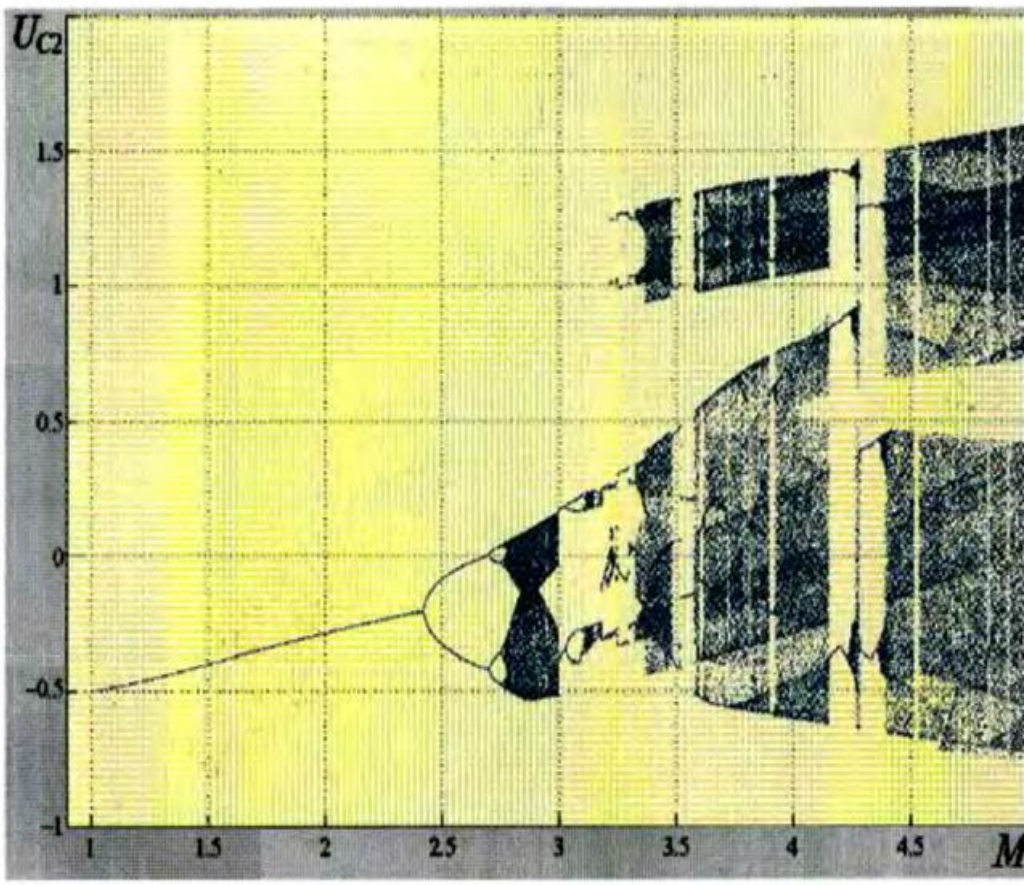
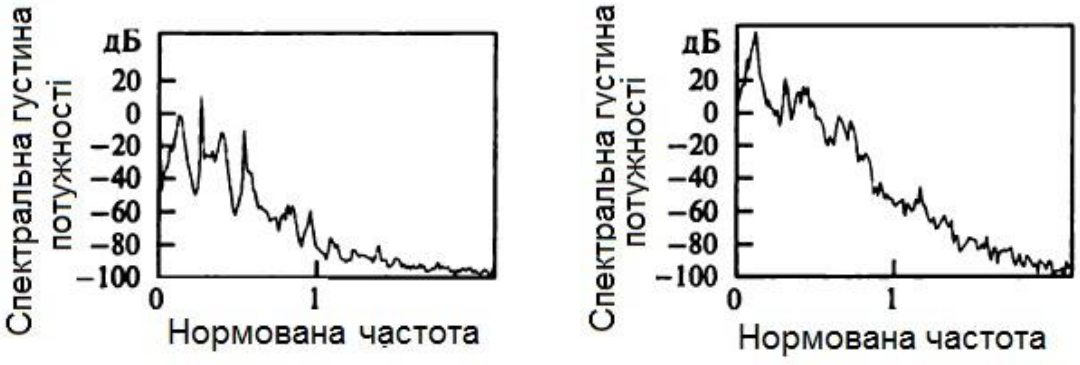


Рис. 1.5. Біфуркаційна діаграма змінної z (напруга U_{c2}) в околиці нерухомої точки $z = 0$ в залежності від значення коефіцієнта підсилення M [84]



а) б)

Рис. 1.6. Спектр сигналу на виході підсистеми 2 ($x(t) \equiv U_{c1}$) при фіксованих значеннях коефіцієнтів $\alpha = 0{,}22$, $T = 3$, $\omega = 1$, $E_1 = 0{,}5$, $E_2 = 2$ та значеннях коефіцієнтів підсилення: M =2,8 (а); M =5 (б) [84]

Із аналізу часових діаграм (рис.1.3) та спектрів (рис.1.6) генерованих сигналів можна зробити висновок, що генеровані сигнали є квазіперіодичними при значеннях коефіцієнтів підсилення $M = 2{,}8$ і $M = 5$ із спадаючим з частотою псевдошумовим спектром. Із рис. 1.5 випливає, що нерухома точка у початку координат втрачає стійкість при $M > 2{,}5$, а псевдовипадкові коливання у системі виникають за рахунок біфуркацій подвоєння періоду.

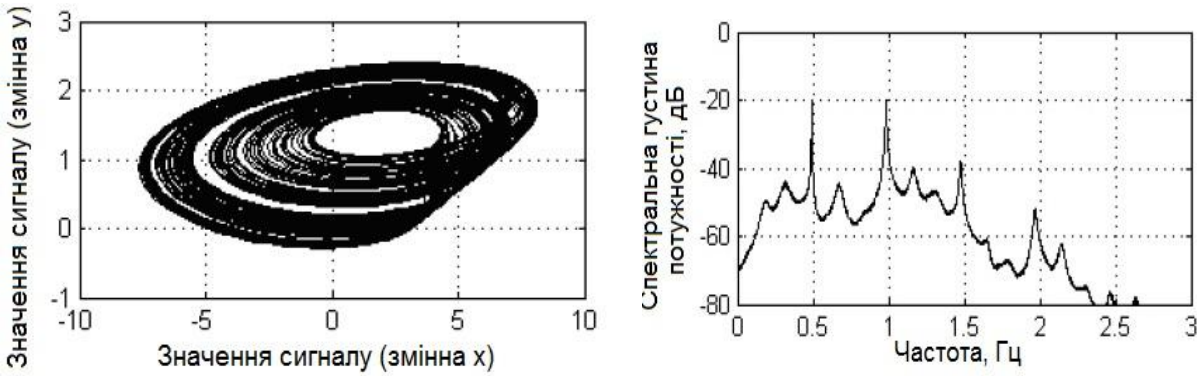
При $M < 2{,}5$ нульове положення є стійким (при невеликих збуреннях, що викликають відхилення від положення рівноваги має місце експоненційне затухання розв'язків системи, а якщо напрям збурення співпадає із напрямком першого показника Ляпунова, мають місце стійкі еліптичні орбіти). Друге і третє положення рівноваги, що має місце при $M > 1$ є нестійкими, оскільки розв'язок системи містить прямо пропорційний часу доданок, що зростає при як завгодно малому збуренні.

При проходженні параметру M через біфуркаційне значення $M \approx 2{,}5$ нульове положення втрачає стійкість. Два ненульових положення знаходяться на значній відстані від початку координат і є нестійкими. Поряд із виникненням коливань навколо положення рівноваги виникають стійкі межі циклів кінцевих розмірів, а відповідні їм автоколивання мають частоту

близьку до резонансної частоти фільтра другого порядку [84].

Інваріантність приймальної та передавальної частин системи до інверсії полярності сигналу та можливість визначення його спектральних характеристик обумовлює використання таких генераторів у системах зв'язку [84]. При забезпеченні інваріантності до інверсії полярності сигналу на виході приймальної системи матиме місце синхронізований сигнал незалежно від того, буде сигнал передавальної частини інвертованим чи ні. Дослідження спектральних характеристик дозволяє зазначити, що спектр є суцільним та рівномірним у певній смузі частот.

При вибраних параметрах атрактор системи (1.5) є фазокогерентним, тобто зміна у часі фазових змінних відбувається когерентно за певним гладким законом, і має вигляд листка Мебіуса (рис. 1.7а). Середнє значення частоти генератора знайдене шляхом моделювання становить $f \approx 1$ Гц (рис.1.7б). Також у спектрі наявні субгармоніки на частотах, кратних $f/2$ [85].



а) б)

Рис. 1.7. Проекція атрактора у площині x-y (а) та нормований спектр потужності псевдовипадкових коливань, генерованих кільцевим автогенератором (б) [85]

Однією із властивостей генераторів хаотичних коливань, що представляють інтерес і можуть бути використані у системах передавання

інформації, є їх синхроннізація.

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

Явище класичної синхронізації осциляторів було відкрито Крістіаном Гюйгенсом у 17-му столітті при вивченні з'єднаних механічним способом настінних годинників [86]. Резонансна взаємодія природних систем є також проявом синхронізації, суть якої полягає у виникненні значних за енергією коливних процесів у системах різного фізичного походження під дією зусиль, що їх спричиняють.

Фундаментальне явище синхронізації проявляє себе у системах найрізноманітнішого походження: біологічних системах (циркадні ритми [87], синхронне світіння світлячків [88], в ритмах серця [89] та мозку людини [90]), неживих природних системах (хіміча реакція Білоусова − Жаботинського [91]), економічних та соціальних системах [92, 93, 94]. Приклади синхронізації систем різного походження приведені в монографіях [84, 95].

У перших наукових працях, присвячених дослідженню явища синхронізації, вважалося, що вона виникає лише у випадку періодичних траєкторій. Згодом у 1963 році Е. Лоренцом було відкрито явище синхронізації псевдовипадкових коливань [73]. Отримані ним результати знайшли своє підтвердження у роботах [96-98]. Результати фундаментальних досліджень інших учених, присвячені синхронізації псевдовипадкових коливань, були опубліковані у 1990 році [59], після чого теоретичні та експериментальні дослідження явищ синхронізації систем стали одним з основних напрямів у галузі нелінійної динаміки.

Численні дослідження обумовили низку визначень поняття «синхронізація». Зокрема вважається, що повна синхронізація (complete, full, identique synchronization) з'єднаних ідентичних систем — це такий тип синхронізації, при якому має місце рівність усіх однотипних змінних стану

систем. З точки зору теорії систем явище синхронізації передбачає принаймні дві системи, що задіяні в цьому процесі.

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

Відкриття Каролем та Пекорою синхронізації систем із хаотичною динамікою відносять до 1990 року [99]. Виникнення цього явища у електронних пристроях та системах стало початком епохи розроблення систем передавання інформації із його використанням. Дослідженнями останніх десятиліть була показана можливість використання синхронізованих систем із псевдовипадковими коливаннями для кодування інформації [100, 101], криптографічного захисту [102-104] та використання псевдовипадковго сигналу в якості переносника [105-108].

До базових технологій синхронізації псевдовипадкових коливань необхідно віднести методи повного заміщення [109], адаптивної синхронізації [110] та імпульсної синхронізації [111].

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

Якщо обидві системи є частиною однієї, то умови виникнення коливань у них будуть майже однаковими. У даному випадку вихідні сигнали однієї з підсистем є вхідними сигналами для іншої. Отже, перша підсистема є головною, а друга – керованою. Зв'язок між системами є однонаправленим,

тобто керована система не впливає на головну. Математична модель цього методу передбачає розділення змінних фазового простору на дві групи. Перша група описує головну, а друга – керовану системи.

Метод адаптивного контролю передбачає наявність головної та керованої систем (рис.1.8). Особливість цього методу полягає у тому, що керована система має коло оберненого зв'язку, а сигнал, що подається на вхід керованої системи є пропорційним різниці між сигналом на виході головної системи та сигналом оберненого зв’язку керованої системи. Якщо синхронізація має місце, то сигнал у колі зворотнього зв'язку відсутній.

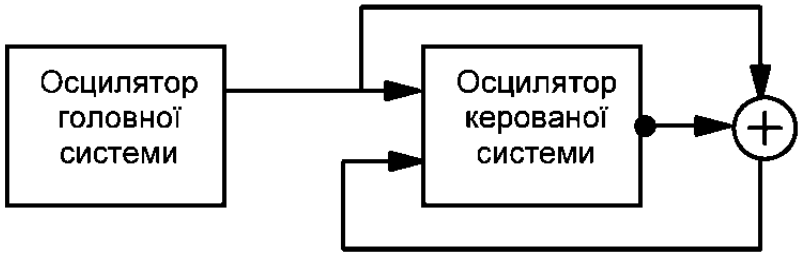


Рис. 1.8. Схема адаптивної синхронізації двох систем [110]

Як бачимо із приведеної схеми у методі адаптивного контролю рівень сигналу синхронізації залежить від ступеня синхронізованості головної та керованої систем, що забезпечує покращення синхронізації. Механізм роботи цієї схеми є подібним до механізму роботи схеми генератора, керованого напругою (різниця між двома сигналами є коливанням збурення у системі, чим менше її значення, тим більше коливання наближені за формою до еталонного, і навпаки).

Третім методом синхронізації є імпульсна синхронізація (рис.1.9).

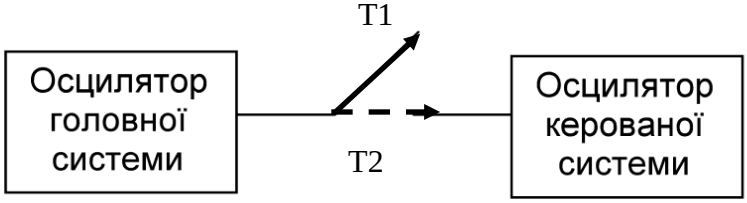


Рис.1.9. Схема імпульсної синхронізації двох систем (T1 – тривалість верхнього стану ключа, T2 – тривалість нижнього стану ключа) [110]

Метод імрульсної синхронізації характеризується додатковими параметрами – тривалістю та періодами імпульсів. За даними деяких авторів [111] імпульсна синхронізація є більш ефективною в умовах дії завад, що пояснюється ослабленням їх впливу за рахунок обмеженого часового інтервалу їх дії.

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

- вибрати та сконструювати системи із псевдовипадковою динамікою, які необхідно синхронізувати;
- встановити граничні умови та швидкість синхронізації;
- дослідити стійкість синхронізації до впливу зовнішніх факторів (інтерференція, фільтрування, зовнішній шум);
- вивчити вплив параметрів систем на процес синхронізації;
- забезпечити унеможливлення відтворення системи передавання шляхом спостереження сигналу, що передається (секретність системи);
- встановити моменти початку та закінчення кодової посилки;
- визначити момент початку/закінчення прийнятого символа в межах кодового слова (кодової посилки).

Незважаючи на те, що дослідженню систем із псевдовипадковою динамікою присвяченна низка робіт провідних вчених, актуальним залишається питання дослідження псевдовипадкових траєкторій та атракторів для систем четвертого і вищого порядку із нелінійними членами. Про це свідчать відкриття нових та вдосконалення уже існуючих систем із псевдовипадковою динамікою, що знаходять своє практичне втілення у системах передавання інформації [80].

Зауважимо що існує декілька наукових шкіл, що активно досліджують це явище та по різному класифікують методи синхронізації

псевдовипадкових коливань у електронних колах [57, 109-116].

Більшість авторів вважають що синхронізація зв'язаних осциляторів може бути використана для передавання інформації у тому або іншому вигляді. На сьогоднішній день в численних наукових працях недостатньо уваги приділено питанню встановлення конкретних значень числових параметрів систем диференційних рівнянь, при яких можливі синхронні псевдвоипадкові коливання. Складність цього явища та чутливість псевдовипадкових систем до початкових умов обумовлює необхідність проведення досліджень в умовах розбалансування параметрів компонентів елементної бази, що використовуються для виготовлення генераторів псевдовипадкових коливань.

Імпульсна синхронізація [112] є менш чутливою до розкиду параметрів генераторів та може забезпечувати високу завадостійкість системи при меншій надлишковості кодових слів внаслідок менших проміжків часу дії шумів каналу на сигнали у порівнянні з неперервною синхронізацією.

Слід зауважити, що дослідження процесу неперервної синхронізації генераторів псевдовипадкових коливань залишаються актуальним, оскільки проводяться розробки нових видів генераторів зі складними за своєю структурою басейнами значень параметрів та початкових умов необхідних для генерування складних коливань. Крім того, за своєю реалізацією пристрої імпульсної синхронізації є значно складнішими.

1.2. Системи передавання інформації, що базуються на базі ПВП

Псевдовипадкові бінарні послідовності використовуються в телекомунікаційних системах [117-119] для побудови блокових та поточних шифрів, а також генерування широкосмугових сигналів [120-123].

Методи генерування ПВП, що використовуються в телекомунікаційних системах поділяються на структурні та математичні (рис.1.10):

- Структурні методи — лінійний зсувовий регістр із оберненими

зв’язками (LSFR), або так звані М-послідовності, нелінійний зсуводвоий регістр із оберненими зв’язками (CNFSR).

– Математичні методи — лінійні конгруентні методи (або методи модулярного перетворення): алгоритми Рівеста-Шаміра-Аделмана (RSA), Мікалі-Шнора (MS), Блюм-Блюм-Шаба (BBS), та Бокса-Міллера); нестійкі розв’язки системи диференційних рівнянь; одно- або багатовимірні рекурентні відображення, що зв’язують два послідовних члени числової послідовності (метод неперіодичної коливної функції з обмеженою множиною можливих значень); фрактальні часові ряди (фрактальний кольоровий шум, фрактальне вейвлет-перетворення, дробовий шум.

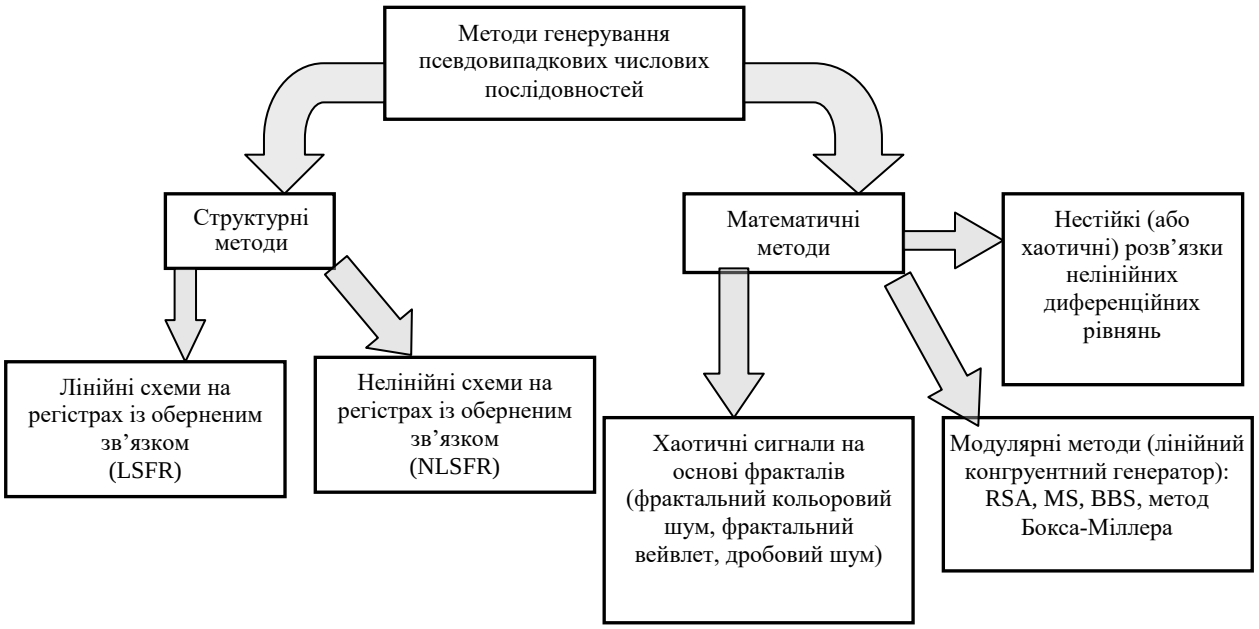


Рис. 1.10. Класифікація методів генерування ПВП

Лінійний конгруентний генератор [124] генерує послідовності цілих чисел, що підпорядковані рівномірному розподілу і описується рекурентною формулою:

$$x_{n+1} = (a \cdot x_n + b) \mod m \qquad (1.15),$$

де x_n та x_{n+1} n-ий та n+1-ий члени послідовності, a, b та m – цілі великі за модулем та взаємно прості числа.

Необхідно зауважити, що простори ключів, генерованих медулярними

методами є малопотужними, оскільки їм притаманний детермінований характер та мала тривалість періоду формованих послідовностей (декілька десятків символів).

У багатьох схемах шифрування генерування псевдовипадкової послідовності бітів може здійснюватися апаратними засобами з використанням лінійних регістрів зсуву з оберненим зв’язком.

Аналіз таких схем [120] показує, що вони є вразливими до дії зовнішніх атак. На рис. 1.11 приведена схема потокового шифрування, що базується на 4-розрядному лінійному регістрі зі зворотнім зв’язком.

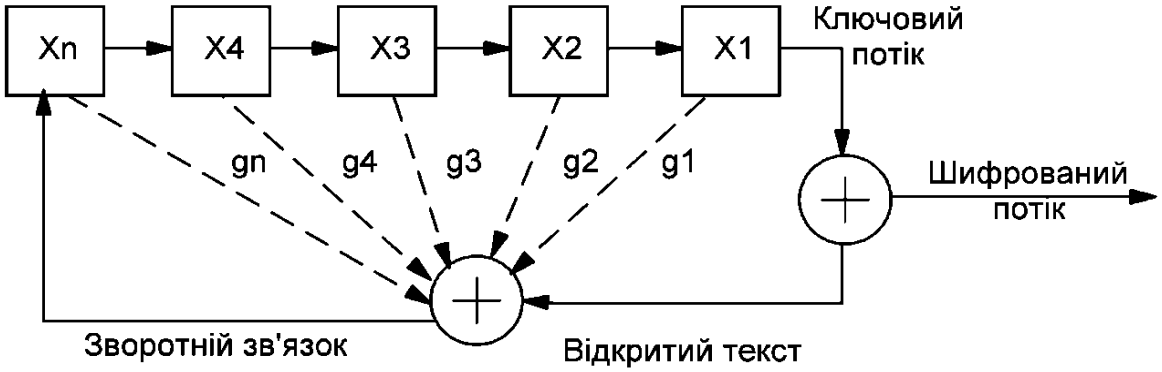


Рис. 1.11. Схема потокового шифрування з використанням n-розрядного лінійного регістра з оберненим зв’язком (X_1, X_2, X_3, X_4, X_n – комірки пам’яті регістра зсуву, g_1, g_2, g_3, g_4, g_n – гілки оберненого зв’язку) [120].

Для визначення схеми зворотнього зв’язку, початкового стану регістра та ключової послідовності, криптоаналітику потрібно лише $2 \cdot n$ біт відкритого тексту і відповідний йому зашифрований текст, де n — число розрядів регістру. Ключова послідовність при цьому є сумою послідовностей, що відповідають відкритому та зашифрованому тексту по модулю 2.

Потік бітів, що поступають на вхід регістра через зворотній зв’язок можна описати рівнянням у матричній формі [120]:

$$|x| = \|X\| \times \|G\| \qquad (1.16),$$

де

$$|x| = \begin{bmatrix} x_{n+1} \\ x_{n+2} \\ \vdots \\ x_{2\cdot n} \end{bmatrix}, \quad \|X\| = \begin{bmatrix} x_1 & x_2 & \cdots & x_n \\ x_2 & x_3 & \cdots & x_{n+1} \\ \vdots & \vdots & \cdots & \vdots \\ x_n & x_{n+1} & \cdots & x_{2\cdot n-1} \end{bmatrix}, \quad \|G\| = \begin{bmatrix} g_1 \\ g_2 \\ \vdots \\ g_n \end{bmatrix}$$

У приведених рівняннях послідовність $\{x_1; x_2; x_3; \ldots; x_{n+1}; x_{n+2}; \ldots x_{2\cdot n-1}; x_{2\cdot n}\}$ є послідовністю ключових бітів, а послідовність $\{g_1; g_2; \ldots g_{n-1}; g_n\}$ відображає зв'язки регістра ($g_i = 0$, при відсутності зв'язку , $g_i = 1$, при його наявності). Для визначення $\{g_1; g_2; g_3; .. g_{n-1}; g_n\}$ необхідно знайти обернену матрицю *n*-го порядку. За умови, що *n=100* для обчислення зв'язків регістра необхідно затратити біля однієї секунди машинного часу.

Нелінійна схема на зсувових регістрах із оберненим зв'язком відрізняється від попередньої тим, що замість додавання за модулем 2 використовується деяка, взагалі кажучи нелінійна функція, аргументами якої є числа, значення яких дорівнюють вмісту регістрів зсуву (рис.1.12).

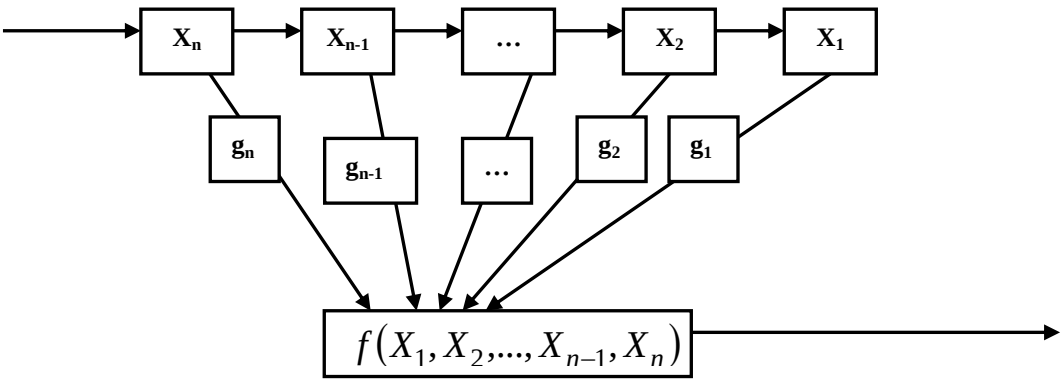


Рис.1.12. Схема потокового шифрування з використанням n-канального нелінійного регістра з оберненим зв'язком (X_n, X_{n-1}, X_2, X_1 – комірки пам'яті регістра зсуву, g_n, g_{n-1}, g_2, g_1 – гілки оберненого зв'язку, f – нелінійна функція оберненого зв'язку)

Однією із найбільш поширених систем, що використовуються для генерування псевдовипадкових послідовностей, є система з наступною функцією відображення:

$$x_n = P\left(\theta \cdot z^n\right) \qquad (1.17),$$

де $P(t)$ – періодична функція, θ, z – параметри, що є дійсними числами. Логістичне відображення (1.3) з параметром $\lambda = 4$ є окремим випадком цього класу відображень при умові, що: $P(t) = \sin^2(t)$, $\theta = \arcsin\left(\sqrt{x_0}\right)$, $z = 2$.

Початкове значення x_0 належить відрізку $[0;1]$. Динаміка такої системи визначається значенням параметру λ:

- При значенні параметра $\lambda \in (0;1)$ послідовність має одне асимптотичне значення, що дорівнює 0;

- При значенні параметра $\lambda \in (1;3)$ послідовність має одне асимптотичне значення, величина якого залежить від початкового значення;

- При значеннях параметра $\lambda \in (3;3.5699)$ послідовність має два асимптотичні значення, що залежать від початкового значення, а члени послідовності періодично наближаються до однієї з двох границь;

- При значеннях параметра $\lambda \in (3.5699;3.6)$: послідовність проявляє властивість, що називається «біфуркацією подвоєння періоду»;

- При значеннях параметра $\lambda \in (3.6;4.0)$ система проявляє генерує псевдовипадкові коливання.

Логістичному відображенню з параметром $\lambda = 4$ притаманні рекурентний (1.18) та аналітичний (1.19) способи відображення:

$$x_{n+1} = 4 \cdot x_n \cdot (1 - x_n), \qquad (1.18)$$

$$x_n = \sin^2\left[2^n \cdot \arcsin\left(\sqrt{x_0}\right)\right] \qquad (1.18)$$

Взаємозв’язок між виразами (1.18) та (1.19) легко встановити, здійснивши нескладні математичні операції, використовуючи метод

математичної індукції.

Іншим відомим відображенням є відображення Пекаря (відображення Бейкера), що описується наступними аналітичними виразами:

$$x_{n+1} = \begin{cases} 2 \cdot x_n, & 0 \le x_n < 1/2 \\ 2 \cdot (1 - x_n), & 1/2 \le x_n < 1 \end{cases} \quad (1.20)$$

$$x_n = \frac{1}{\pi} \cdot \arccos\left(\cos\left(2^n \cdot \pi \cdot x_0\right)\right) \quad (1.21)$$

Криптографічні методи на основі ПВП ввійшли у практику побудови систем передавання інформації протягом двох останніх десятиріч [122, 125, 126]. Їх подальший розвиток обумовлений зростанням обчислювальних потужностей ЕОМ та алгоритмів зламу криптографічних систем [127-132].

Класифікація методів шифрування інформації в телекомунікаційних системах приведена на рис.1.13.

Одним із способів шифрування інформації, що використовує псевдовипадкові послідовності є метод потокового шифрування [133-135]. Ключем такого методу є ПВП, членами якої є двійкові числа – «0» або «1». Узагальнена схема методу базується на додаванні по модулю 2 нескінченного ключового потоку та елементів інформаційного повідомлення.

Одним із методів криптоаналізу багатьох систем шифрування є статистичний аналіз, що використовує частоту виникнення окремих символів та їх комбінацій [127]. Шенон [136] розробив дві концепції шифрування, названі ним методом «розсіювання» (diffusion) та «перемішування» (confusion). У розробленій Шеноном концепції метод «розсіювання», або як його інакше називають методом «лавинного ефекту» (avalanche), є перетворенням, в якому зміна значення одного біту з імовірністю ½ призводить до зміни значень усіх інших бітів, задіяних у перетворенні.

Внаслідок цього забезпечується стійкість шифру до статистичного аналізу, що полягає у простому підрахунку частот або використання імовірнісних моделей тексту. Найбільш продуктивними методами криптографічних перетворень є запропоновані Хорстом Файстелем методи

[137], що отримали назву мережі Файстеля, архітектура якої приведена на рис. 1.14 [127].

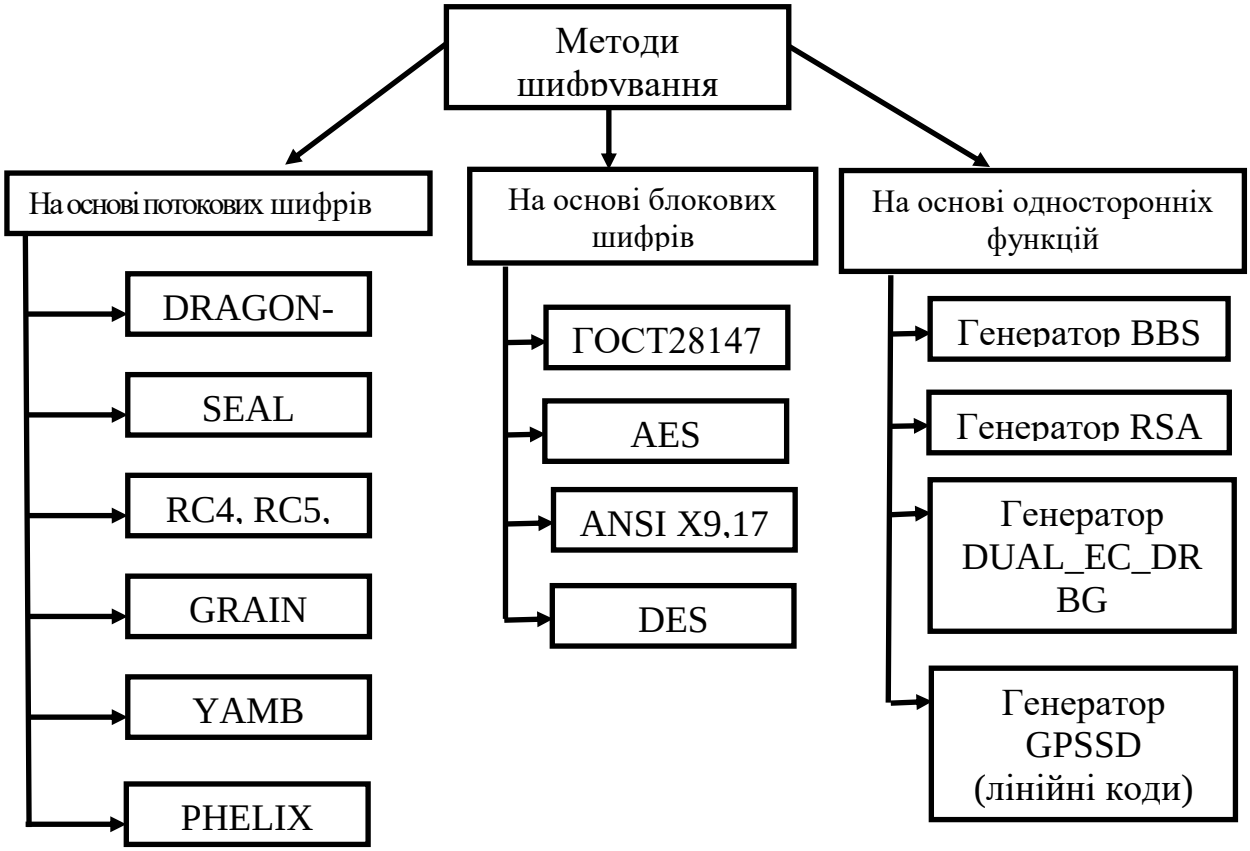


Рис.1.13. Класифікація традиційних методів шифрування інформації в телекомунікаційних системах

На рис.1.9 буквами *Li* та *Ri* позначені ліва і права половини початкових даних на *i*-му кроці послідовного перетворення. Кожен такий крок називають раундом шифрування. На кожному раунді може бути використана своя функція гамування *Fi*. У приведеній схемі генерована за допомогою функції гамування гама-послідовність залежить від ітераційного ключа k_i і правої половини даних. Після цього ліва половина сумується із отриманою гамою по модулю 2. В подальшому після обміну місцями правої та лівої половин процес генерування повторюється. Поскільки за один раунд обробляється тільки одна половина даних, бажано, щоб число раундів було кратним 2.

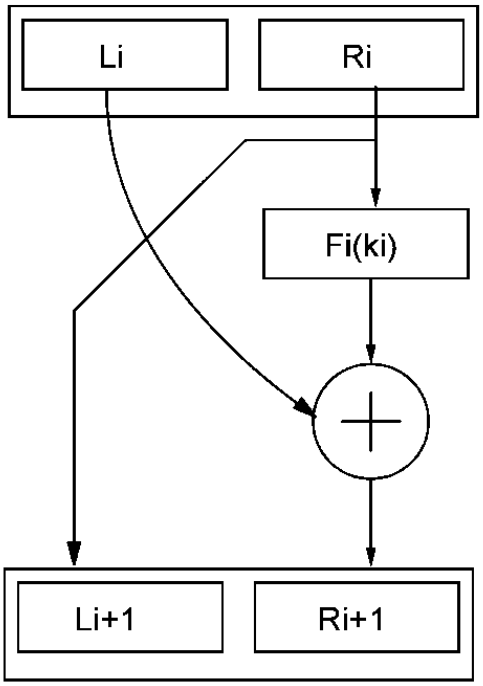


Рис.1.14. Архітектура мережі Файстеля (*Li*, *Ri* – ліва і права половина початкових даних на *i*-му кроці послідовного перетворення, *Fi* – функція гамування, k_i – ключ цієї функції) [127]

Суть властивості перемішування (властивість повноти шифру) полягає в тому що, що кожен новий біт криптографічного перетворення повинен бути залежним від якомога більшої кількості попередніх бітів. Такі перетворення забезпечують повну залежність шифрованого тексту від ключа та відкритого тексту.

Раніше зазначені особливості систем із псевдовипадковою динамікою уможливлюють їх використання у криптографії для генерування потокових ключових послідовностей [138, 139], що забезпечують виконання вимог Шеннона. Їх аперіодичність вказує на можливість генерування як завгодно великих унікальних ключів, придатних для одноразового використання у потокових системах шифрування [119, 123, 140]. Внаслідок кінцевої точності представлення чисел в будь-якій системі відліку, що може бути використана у реальних системах криптографічного захисту, генеровані ключі при певній їх довжині проявлятимуть властивість періодичності [141]. Тому однією із

задач, що вирішувалася в процесі виконання дисертаційної роботи, було дослідження залежності максимальної довжини ПВП, при якій вона не проявляє властивості періодичності, від точності представлення параметрів логістичного відображення та відображення Пекаря.

Одним із класів криптосистем є системи, що використовують фазові траєкторії із псевдовипадковою динамікою. Однією із найбільш поширених криптосистем такого класу є система Баптіста [103, 142], основою якої є дискретне відображення, що задане співвідношенням:

$$x[n+1]=\phi(x[n]) \quad (1.22)$$

Відображення φ відображає символьний алфавіт $A=\{M_i\}$ потужністю k у набір відрізків $\{I_k\}$ із довжинами 10^{-k}. При цьому всі отримані в результаті ітерацій значення знаходяться на відрізку $(0;1)$. Шифруванння за даним методом базується на тому, що будь-якому символу із алфавіту A ставиться у відповідність таке ціле число, що дорівнює кількості ітерацій N_i, причому:

$$x[N_i]\in I_i \quad (1.23)$$

Першим елементом ітерації є деяке початкове число x_0. Множина значень цього числа та спосіб розбиття відрізка $(0;1)$ на підінтервали є множиною ключів описуваного способу відображення.

Зауважимо, що крім шифрування та кодування інформації [143, 145] системи із псевдовипадковою динамікою можна використати для моделювання пам'яті живих організмів, зокрема такий підхід описаний у [146].

1.3. Системи передавання інформації, що базуються на властивостях псевдовипадкових коливань

Практичне використання псевдовипадкових сигналів у системах зв'язку

викликає велику зацікавленість вчених, конструкторів та інженерів і є одним із головних напрямків досліджень у галузі телекомунікацій та теорії передавання інформації.

Теоретичні основи та практичне використання систем із псевдовипадковою динамікою є самостійним науковим напрямком, що виник на стику теорії диференційних рівнянь, математичної та статистичної фізики, термодинаміки, гідродинаміки, радіоелектроніки та інше.

У багатьох випадках радіотехнічні пристрої з нелінійними елементами, володіють властивостями що притаманні динамічним системам із псевдовипадковою динамікою. Моделювання таких пристроїв здійснюється на основі відповідних математичних моделей.

Властивості систем із псевдовипадковою динамікою обумовили розвиток нових підходів для вирішення проблем передавання інформації [147, 148, 150-153]. Існує декілька напрямків використання псевдовипадкових сигналів у системах зв’язку, до яких зокрема відносяться алгоритми канального кодування цифрової інформації, що одночасно забезпечують підвищення їх завадостійкості та криптостійкості [128, 154, 155]. Зауважимо, що псевдовипадкова динаміка використовується поряд із традиційними методами блокового канального кодування [101, 156, 157].

До методів кодування інформації в телекомунікаційних системах відноситься кодування бітової інформації наявністю чи відсутністю синхронного відгуку у передавачеві (до таких систем слід віднести також системи із CSK (chaos shift keying)) або перемикання режимів генерування псевдовипадкових коливань [158]); модуляція псевдовипадкового носійного сигналу інформаційним сигналом, в тому числі нелінійне підмішування інформаційної складової до псевдовипадкового сигналу з метою маскування процесу передавання інформації (стеганографія) [159-164] та використання нелінійного фільтрування псевдовипадкового сигналу [165].

Особливою рисою методу нелінійного підмішування, що базується на взаємооберненому перетворенні сигналів, є можливість зміни у широких

межах рівня вхідного сигналу на приймальній стороні системи по відношенню до значення псевдовипадкового сигналу. При цьому амплітуда інформаційного сигналу може бути такого ж порядку, меншою або перевищувати рівень псевдовипадкового носійного сигналу. Система зв’язку, що використовує модулі генерування псевдовипадкових сигналів з нелінійним підмішуванням інформаційного сигналу підтвердила свою дієздатність у фізичних експериментах.

По мірі розвитку елементної бази, що може бути використана у системах передавання інформації, набули розвитку прямохаотичні або широкосмугові системи передавання [64, 65]. Тому необхідно зазначити роботи, пов'язані з розробленням нових генераторів псевдовипадкових коливань та дослідженнями процесів, що у них відбуваються. Одним із способів генерування широкосмугового сигналу є використання систем із псевдовипадковою динамікою для генерування послідовностей, що розширюють спектр сигналу [166].

Розглянемо коротко типи систем, що використовують псевдовипадкові сигнали для передавання інформації. Найбільш узагальнена класифікація систем, що використовують псевдовипадкові сигнали та псевдовипадкові послідовності для передавання інформації приведена на рис.1.15.

Практична реалізація широкосмугових сигналів стала можливою тільки після досягнення відповідного рівня розвитку базових технологій для надширокосмугової радіоелектроніки (середина 1990-х років):

- технології стабільного генерування потужних надкоротких (тривалістю 1 нс і коротших) імпульсів з практично необмеженим ресурсом (набагато більшим 10^{10} імпульсів) та високою частотою повторення;
- технології випромінювання надкоротких імпульсів безпосередньо в ефір (надширокосмугова антенна техніка);
- технології формування надширокосмугових сигналів з будь-якою поляризаційною структурою;

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

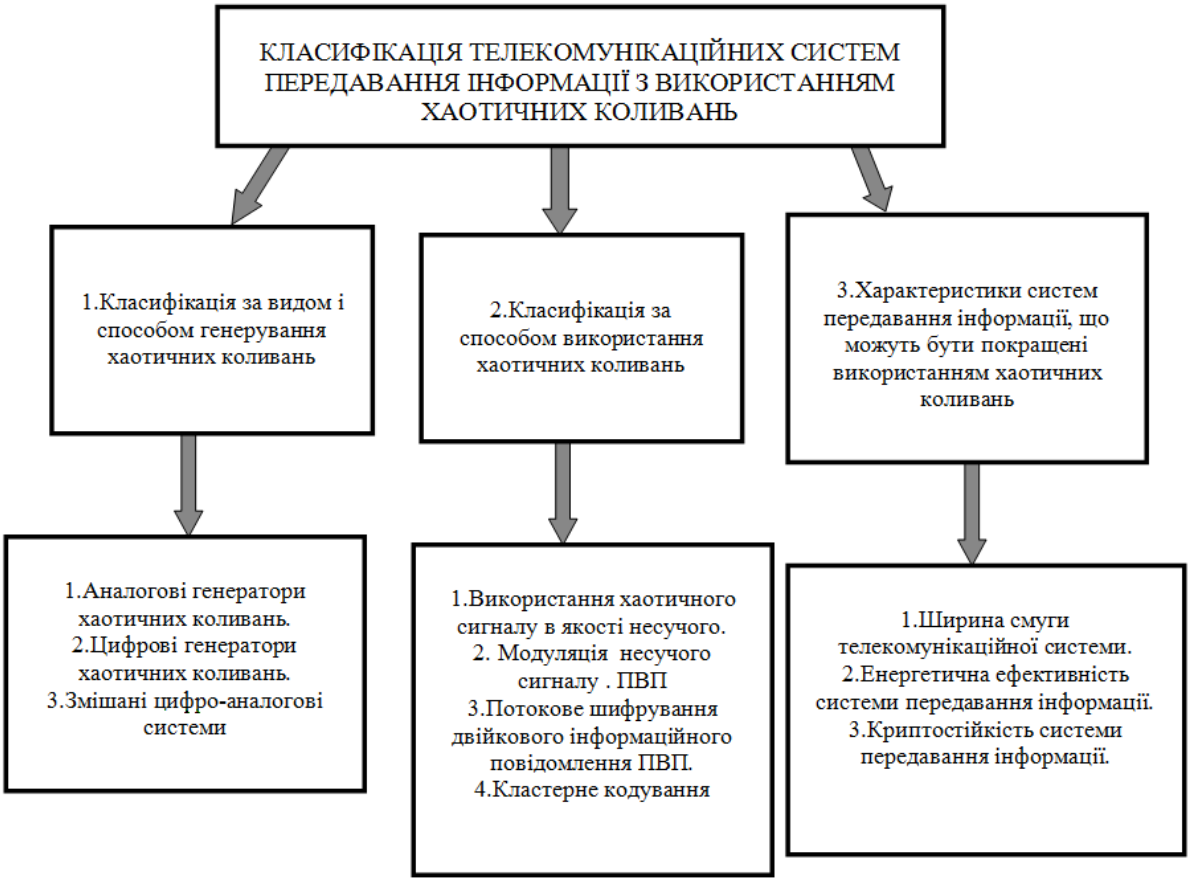


Рис.1.15. Класифікація телекомунікаційних систем передавання інформації з використанням псевдовипадкових коливань

Для розділення сигналів в умовах складних електромагнітних обставин (багатопроменеве поширення, багатокористувальницька система у широкій смузі частот) потрібно, щоб виконувалась умова ортогональності на при будь-яких величинах часового зсуву τ між сигналами $s_1(t)$ та $s_2(t)$ [55]:

$$\int_{t}^{t+T} s_1(t)\cdot s_2(t-\tau)dt = 0, \quad (1.24)$$

де T – тривалість імпульсу кодової послідовності, $0 \le \tau \le T$.

Виконання (1.24) є можливим лише за умови, що кореляційна функція сигналів є дельта-функцією, а тривалість імпульсу кодової послідовності

$T = 0$ [55, 167]. При цьому смуга частот носійних сигналів повинна бути безмежною, тобто сигналам $s_1(t)$ та $s_2(t)$ притаманні властивості білого шуму. Практична реалізація таких сигналів є неможливою. Можлива реалізація сигналів, взаємна енергія яких є набагато меншою за енергію одного із сигналів:

$$\int_{t}^{t+T} s_1(t) \cdot s_2(t-\tau)dt << \left\| s_{i,2} \right\|^2 . \quad (1.25)$$

Такі сигнали є майже ортогональними і за своїми властивостями подібними до білого шуму, внаслідок чого їх називають шумоподібними.

У технологіях детектування широкосмугових сигналів характерним є те, що використання добре розвинутих методів перетворення Гільберта є неможливим. Тому особливого значення набувають теоретичні дослідження процесів у широкосмугових системах, що є вивченими набагато менше, ніж вузькосмугові сигнали (основані на перетворенні Гільберта).

Теоретичною основою конструювання телекомунікаційних систем з розширеним спектром є теорема Клода Шенона стосовно залежності пропускної здатності гаусового каналу C (біт/с) від ширини смуги та співвідношення потужностей сигнал/шум [168].

Конструюванню систем передавання інформації на базі псевдовипадкових коливань передувало дослідження властивостей систем із псевдовипадковою динамікою, що тривають і по даний час [112].

Статистичні, спектральні та кореляційні характеристики, генерованих системами з псевдовипадковою динамікою сигналів, є близькими до характеристик білого шуму. Тому такі сигнали, що називаються шумоподібними, володіють низкою переваг:

- можливістю роботи у сильно зашумлених каналах;
- стійкістю до ефектів (федінг, інтерференція), що мають місце в умовах багатопроменевого поширення сигналів;
- можливістю відтворення інформації при частковій втраті або спотворенні прийнятого сигналу;

- можливістю маскування процесу передавання інформації (стеганографія) завдяки кореляційним та спектральним властивостям таких сигналів.

Однією зі сфер використання надширокосмугового зв'язку є створення систем передавання через акустичні канали, в тому числі ультразвукового діапазону, що є актуальним для забезпечення підводного зв’язку.

Найбільш значущі результати використання широкосмугових сигналів були отримані у радіолокаційних системах. У 1989 році відбулися випробування потенціально перспективної надширокосмугової радіолокаційної станції, що детально описані у роботі Осипова М. [169]. В ході випробувань літак з ефективною площею розсіювання порядка 1 $м^2$ можна було детектувати на фоні острова на відстанях порядку 100 км. При цьому роздільна здатність визначення відстані до об'єкта становила 1 м. В якості формувача сигналів зондування використовувався генератор радіоімпульсів з несучою частотою 10 ГГц та тривалістю 5 нс.

Іншим важливим аспектом практичного застосування НШСС є виявлення та спостереження об'єктів на коротких дистанціях (1-10 м, 1-10 км) як у щільних середовищах (грунт, лід), так і у повітрі [170].

За допомогою НШС радіолокаційних станцій є можливим виявлення на місцевості різних прихованих або замаскованих об'єктів та отримання їх деталізованого зображення.

Діапазон частот широкосмугових сигналів становить 1…10 ГГц. Верхня границя смуги є значно нижчою від частоти електромагнітних коливань, при якій спостерігається резонансне поглинання молекулами води [171], тому є можливим поширення таких радіохвиль в умовах туману. Це дає можливість використовувати широкосмугові сигнали у так званих всепогодних радіолокаторах. Іншою спорідненою сферою використання сигналів із таким частотним діапазоном є підводний радіозв'язок [170]. Використання широкосмугових сигналів дає можливість уникнути ефекту маскування літаків, обумовленого випромінюванням сигналу, що є

протифазним до сигналу радіолокації. У випадку використання широкосмугового сигналу зондування метод маскування, що базується на випромінюванні протифазного сигналу, є неефективним внаслідок складності сигналу зондування.

Розроблена у 1998 році японською фірмою ARIB система WCDMA (Wideband Code Division Multiply Access) є узгодженою більшістю операторів системою, здатних працювати у новому спектрі частот. Для кодового розділення каналів система WCDMA використовує коди Голда.

Система TD-WCDMA (Time Division – Wideband Code Division Multiple Access) забезпечує часове розділення та широкосмуговий багатокористувацький доступ із кодовим розділенням. Ця система поєднує властивості систем розділення каналів TDMA та CDMA (частота та канальний інтервал системи) [172].

Найбільш поширеною математичною моделлю генерування псевдовипадковх сигналів є системи диференційних рівнянь. На основі аналізу численних публікацій, присвячених аналізу математичних моделей, можна зробити висновок, що для генерування псевдовипадкових розв’зків необхідно, щоб система містила нелінійні відносно її змінних доданки. Це є очевидним, оскільки розв’язком лінійної систем є лінійна комбінація експоненційних та тригонометричних функцій [173], внаслідок чого генерування псевдовипадкових коливань унеможливлене.

Розвиток телекомунікаційних систем, що використовують псевдовипадкові сигнали та ПВП розпочався у 1990-х [57]. Першим поколінням таких систем є системи з додаванням псевдовипадкового маскувального сигналу до інформаційного , системи із перемиканням (або csk – chaotic shift keying) між генераторами псевдовипадкових сигналів [110] та системи із імпульсною синхронізацією [111]. Ці системи грунтувалися на перших експериментах результатах синхронізації електронних кіл [99].

Система з додаванням псевдовипадкового маскувального сигналу (рис. 1.17) має два ідентичні синхронно працюючі генератори

псевдовипадкових коливань на приймальній та передавальній сторонах системи. Відновлення інформаційного сигналу відбувається шляхом віднімання від прийнятого сигналу s(t) псевдовипадкового c(t), що генерований на приймальній стороні системи передавання інформації.

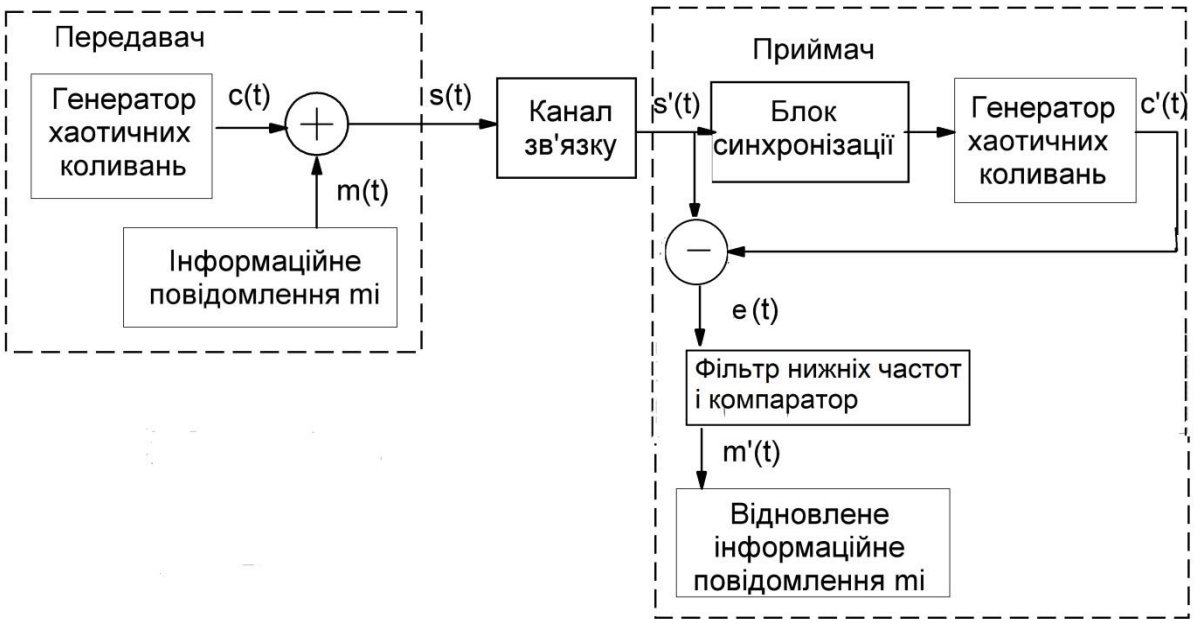


Рис.1.17. Структурна схема системи з додаванням псевдовипадкового маскувального сигналу до інформаційного, де: c(t) – псевдовипадковий сигнал, m(t) – інформаційний сигнал, s(t) – псевдовипадковий сигнал, що передається у канал зв’язку s'(t) – прийнятий сигнал, c' (t) – синхронізований псевдовипадковий сигнал, e(t) – помилка синхронізації, m'(t) – прийнятий інформаційний сигнал [112]

Слід зауважити, що псевдовипадкові сигнали можуть бути використані в якості ключа у потоковому шифруванні. Крім того, можливе комбіноване застосування оскільки у таких схемах неможливо розділити передавання даних від шифрування сигналів. Одним із їх узагальнень є схема кодування інформації з нелінійним підмішуванням інформаційного сигналу. Схема такого процесу приведена на рис. 1.18.

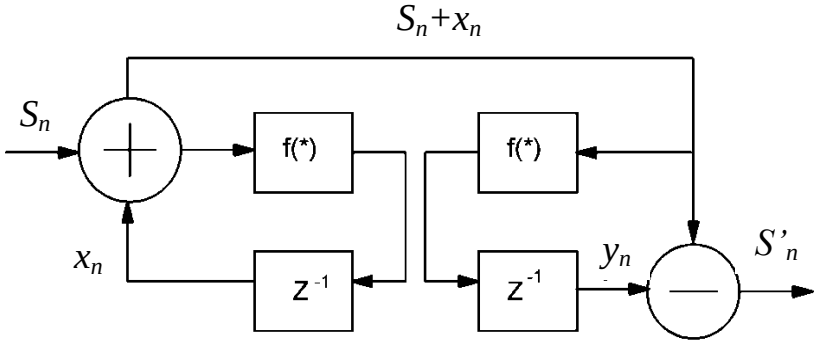


Рис. 1.18. Схема кодування із нелінійним підмішуванням інформаційного сигналу, де: S_n — інформаційний сигнал, x_n — псевдовипадковий сигнал, f(*) – функція нелінійної обробки, z^{-1} – затримка на час, що відповідає інтервалу дискретизації, S_n+x_n – сигнал, що передається у канал зв'язку, y_n – прийнятий сигнал, S'_n – розшифрований інформаційний сигнал

Аналіз літературних джерел [110, 112] показує, що процеси синхронізації досліджені лише для нескладних генераторів, а вплив значень їх параметрів на процес синхронізації потребує детального дослідження. Також недостатньо висвітленим у літературних джерелах є питання вибору оптимального співвідношення потужностей інформаційного та псевдовипадкового сигналу. Покращення енергетичних показників систем передавання інформації потребує зменшення потужності інформаційного сигналу, але завади та шуми в каналі накладають обмеження на її мінімальне значення.

У системі з перемиканням генераторів псевдовипадкових коливань (рис. 1.19). Інформаційне повідомлення, що є цифровим сигналом, використовуються для керування ключем між двома статистично незалежними генераторами псевдовипадкових сигналів із різними параметрами, що використовуються для кодування логічної «1» та логічного «0».

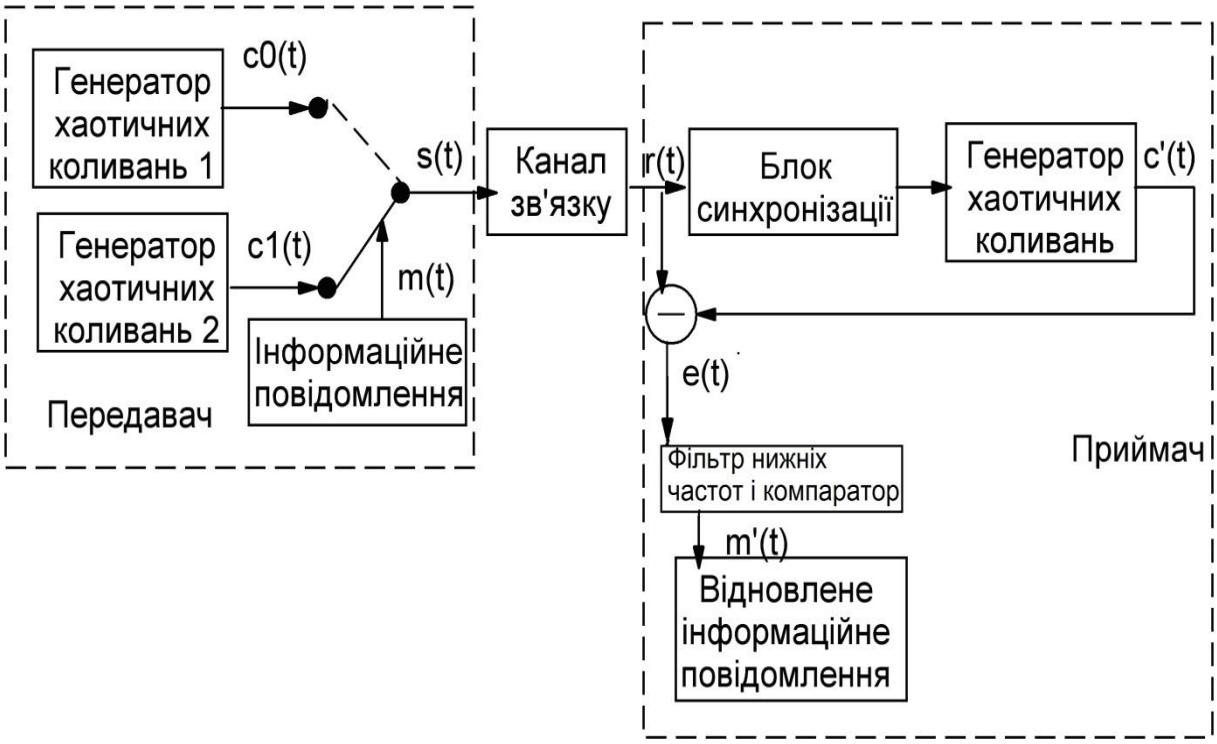


Рис.1.19. Система із перемиканням генераторів псевдовипадкових коливань, (chaos shift keying – csk), де: c0(t), c1(t) – псевдовипадкові сигнали, m(t) – інформаційний сигнал, s(t) – псевдовипадковий сигнал, що передається у канал зв’язку, r(t) – прийнятий сигнал, c' (t) – псевдовипадковий сигнал, e(t) – помилка синхронізації, m'(t) – прийнятий інформаційний сигнал) [112]

Інформаційний сигнал відновлюється шляхом проходження через фільтр нижніх частот, що відфільтровує високочастотні коливання, обумовлені процесом встановлення синхронізації, з наступною подачею на вхід компаратора, що оцифровує прийнятий сигнал.

Іншою базовою технологією синхронізації, що є ефективною у системах захищеного передавання інформації є імпульсна синхронізація. Додатковими параметрами у такій схемі є частота та тривалість імпульсів синхронізації (рис. 1.20) [112].

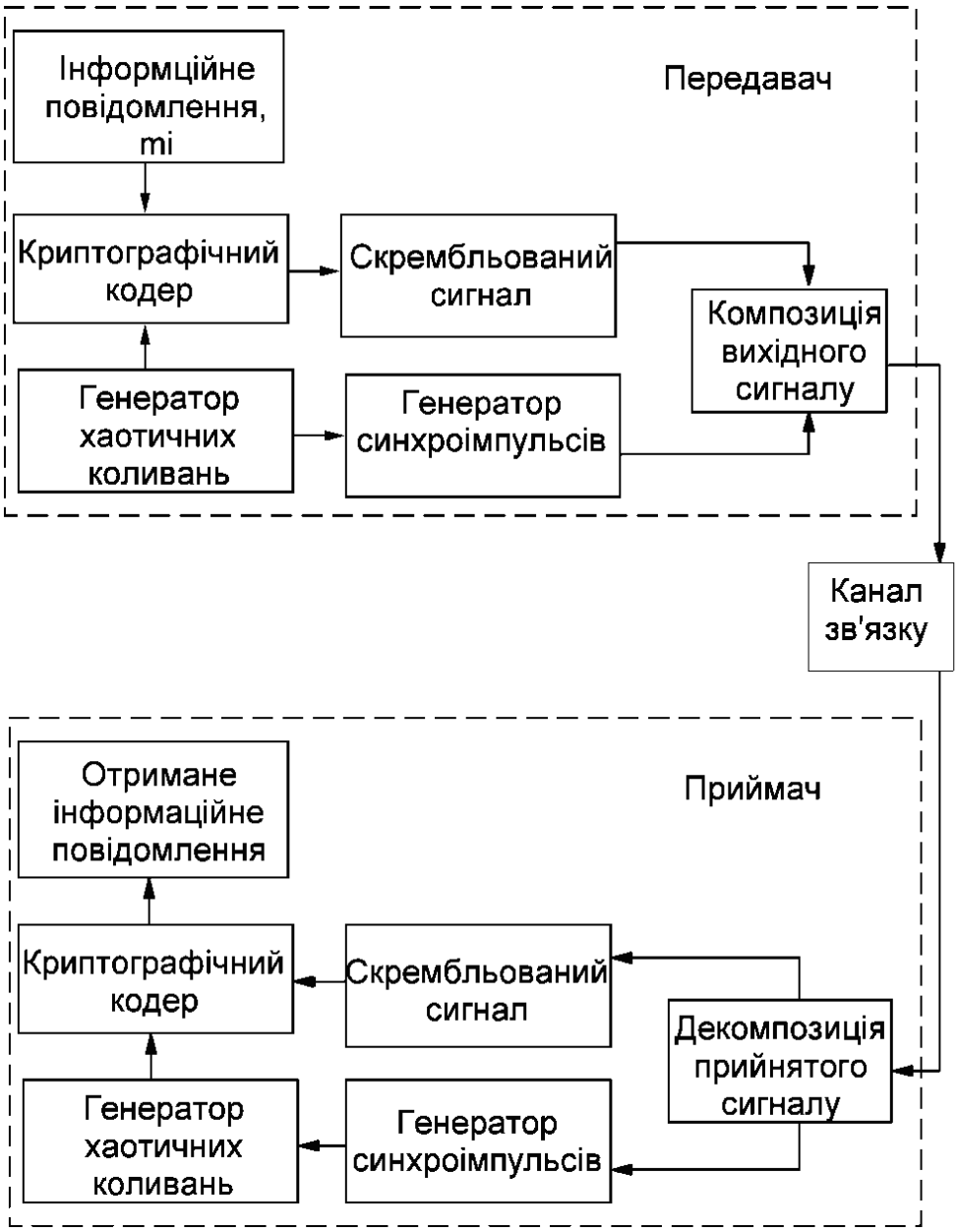


Рис.1.20. Структурна схема системи цифрового зв’язку з імпульсною синхронізацією [112]

Передавальна та приймальна сторони системи містять ідентичні генератори псевдовипадкових коливань, кодер та декодер, що використовують одноковий криптографічний алгоритм, пристрій додавання та пристрій відділення зашифрованого сигналу та імпульсу синхронізації. Сигнал, що передається у канал зв’язку, складається із двох частин – синхроімпульсу та зашифрованого методами традиційної криптографії інформаційного сигналу (рис. 1.21).

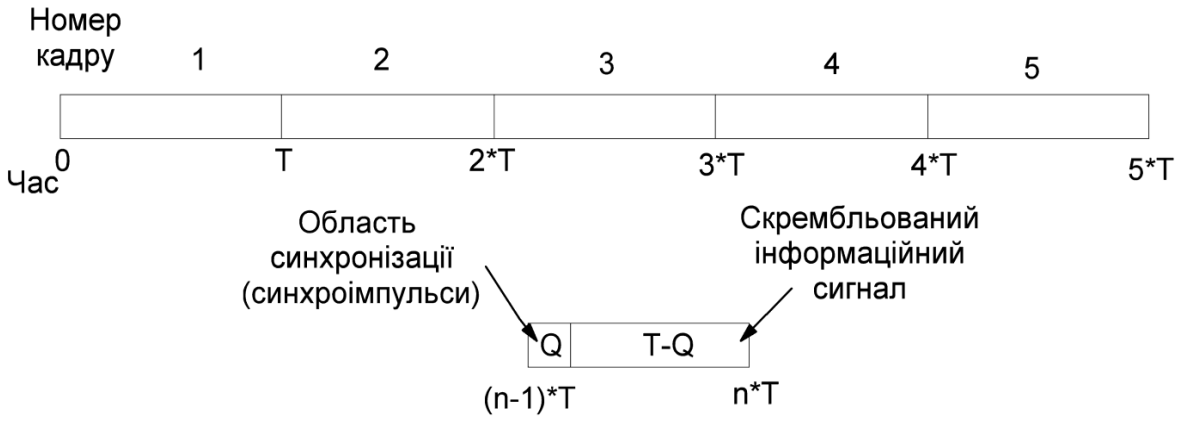


Рис.1.21. Структура переданого сигналу у випадку імпульсної синхронізації , де: n – номер інформаційного кадру, Q – тривалість синхроімпульсу, T – тривалість кадру, T-Q – тривалість зашифрованого інформаційного сигналу) [112]

Кожен кадр передавання інформації (рис. 1.21) тривалістю T поділяється на дві частини: синхронізуючу (час синхронізації Q) та зашифрований інформаційний сигнал (T-Q). У цьому випадку використаний найменш складний спосіб композиції – суміщення інформаційних сигналів та сигналів синхронізації заданої тривалості.

Зростання потужності цифрових засобів оброблення сигналів розширює потенційні можливості розробників телекомунікаційних систем в напрямку зменшення співвідношення сигнал/шум при незмінній швидкодії системи, що згідно з теоремою Шенона про пропускну здатність каналу, можливо встановленням компромісу у будь-якій системі зв'язку.

Проблема синтезу різноманітних фрактальних сигналів і методів фрактальної модуляції має важливе наукове та прикладне значення. Зокрема фрактальна модуляція може бути використана у сучасній радіофізиці та радіоелектроніці [174]:

- фрактальні антени та їх конструювання;
- фрактальні і текстурні сигнатури;
- розсіювання електромагнітних хвиль фрактальною поверхнею;

– динамічні моделі розсіювання радіохвиль на основі псевдовипадкової динаміки;

– виявлення малоконтрастних об’єктів;

– фрактальна модуляція і сигнали;

– фрактальні вибірково поглинаючі матеріали;

– радіоелементи із фрактальним імпедансом;

Результати дослідження властивостей фрактальних антен та можливостей їх використання описані у роботі українських науковців [175].

Методи фрактальної модуляції та формування фрактальних сигналів є перспективними для застосування у телекомунікаційних системах. У таких системах робочими сигналами є фрактальні імпульси, що утворені елементарними сигналами довільної форми, значення яких підпорядковані певним функціональним закономірностям, що мають властивості самоподібності.

Аналізуючи публікації [175-179] можна зробити висновок про те, що системи передавання інформації з використанням фрактальних сигналів мають однакову схему кодування, але відрізняються типом використовуваних несучих сигналів та способом декодування.

На рис.1.22 приведена блок-схема системи передавання інформації з використанням фрактальних сигналів [176].

Сигнал, з виходу комп’ютера 1 надходить з конвертора 2, що генерує аналоговий сигнал заданої форми, на вхід вейвлет-генератора 3. Вихід генератора керується імпульсами прямокутної форми, що надходять з виходу конвертора. Цифровий блок вейвлет генератора використовує програмовані логічні інтегральні схеми (ПЛІС), завдяки чому можна генерувати більше 20 типів сигналів з максимальним значенням амплітуди 2В (у тому числі ортогональних).

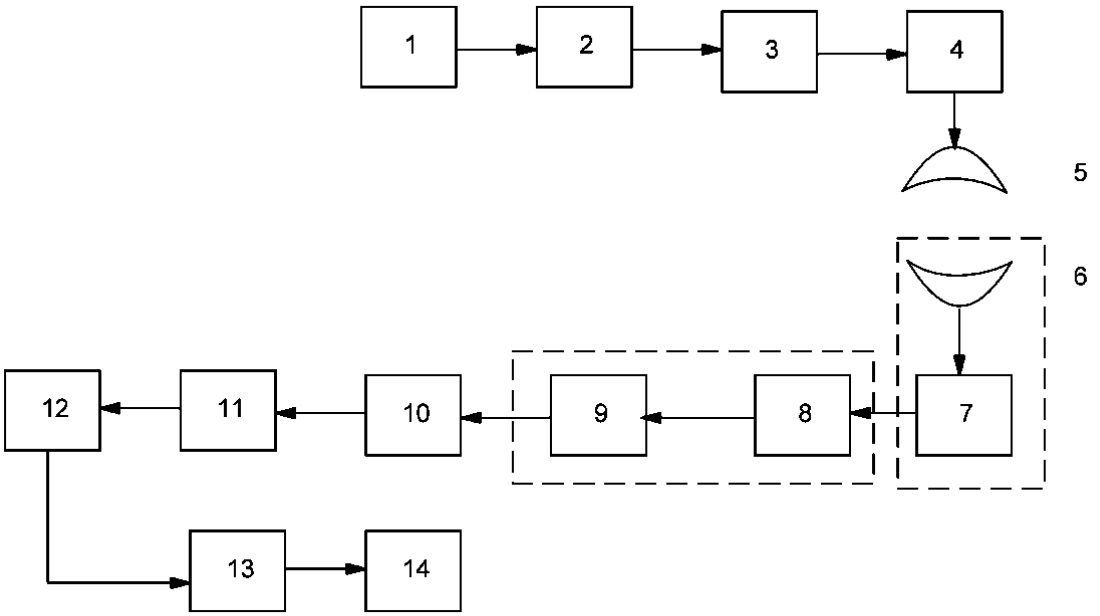


Рис.1.22. Блок-схема системи передавання інформації за допомогою фрактальних сигналів між двома комп'ютерами, де: 1 – комп'ютер-передавач; 2 – конвертор; 3 – генератор фрактального вейвлету; 4 – фрактальний модулятор; 5 – передавальна широкосмугова антена; 6 – приймаюча фрактальна антена; 7 – фрактальний фільтр високих частот; 8 – фрактальний приймач; 9 – смуговий низькочастотний фільтр; 10 – детектор; 11 – компаратор; 12 – генератор прямокутних імпульсів; 13 – конвертер; 14 – комп'ютер-одержувач [176]

Сформовані сигнали надходять із виходу генератора на фрактальний модулятор 4, що здійснює модуляцію та підсилення сигналу перед його передачею у ефір за допомогою широкосмугової антени 5. Центр смуги сигналу знаходиться на частоті 2 Ггц. Модулятор оперує в частотному діапазоні від 1,8 до 2,15 Ггц. Прийнятий широкосмуговою антеною 6 сигнал, проходить через фрактальний фільтр високих частот 7 і подається на вхід фрактального приймача 8. Приймач здійснює підсилення та відновлення сигналу моделювання із прийнятого радіочастотного сигналу. Автори зазначають, що покращити характеристики описаної системи можна шляхом використання засобів кореляційного детектування фрактального сигналу, але

це значно збільшує вартість приладу.

Для боротьби з інтерференцією система оснащена широкосмуговим фільтром. Аналоговий сигнал, що позбавлений шумової складової за допомогою такого фільтра, надходить у коло формування послідовності прямокутних імпульсів 10-12, на виході якого утворюється цифровий сигнал. Призначенням цього кола є формування бітової інформаційної послідовності та старт-стопових бітів інформаційного пакету у загальному інформаційному потоці. На вході генератора прямокутних імпульсів 12 встановлений компаратор, на виході якого формується прямокутний імпульс, що відповідає одному інформаційному біту. В якості компаратора використовують високошвидкісну лінійку мікросхем, що формують додатні імпульси напругою TTL-логіки кожного пікового імпульсу відеосигналу із шириною не меншою ніж 0,75 нс. Із виходу компаратора сигнал надходить на конвертор 13. Після цього оцифровані дані надходять на USB-порт приймального персонального комп'ютера 14 з наступним перетворенням у прийнятну для операційної системи форму шляхом застосування спеціального програмного забезпечення.

Конвертори, що перетворюють дані із формату USB у формат RS-485, і навпаки використовуються як для узгодження швидкостей передавання даних з порту USB (12 Мбіт/сек) з робочими фрактальними сигналами (0,9216 Мбіт/сек), так і для формування трігерних сигналів, що надходять до вейвлетного генератора.

Розглянемо більш детально характеристики робочого сигналу. Інформаційним сигналом що модулює високочастотний несучий сигнал є послідовність наносекундних імпульсів, спектральна густина потужності якої приведена на рис. 1.23.

Модульований та підсилений сигнал передавався у радіоефір, дальність зв'язку становила 100 м при швидкості передавання порядка 0.9 Мбіт/сек. Очевидним є те, що передавання широкосмугових сигналів на великі відстані через радіоефір є неможливим, проте системи подібного класу можуть

використовуватися для оперативного керування. Зауважимо що сучасні системи мобільного та супутникового зв'язку використовують носійні сигнали надвисокої частоти, ширина смуги яких є відносно невисокою.

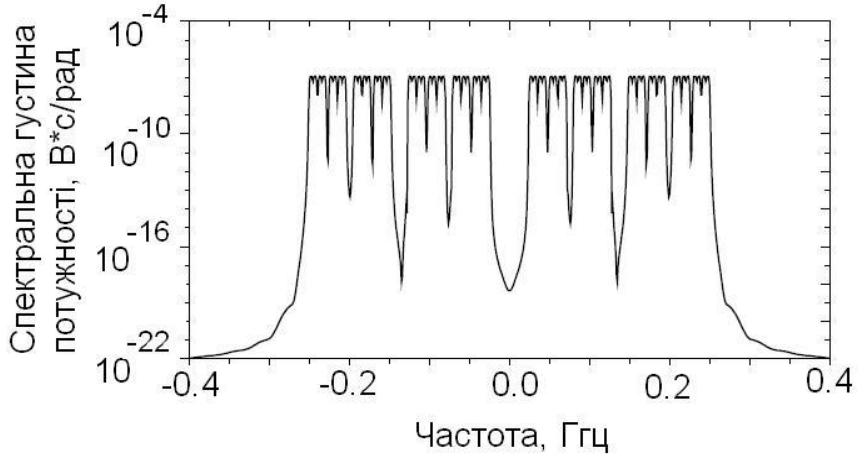


Рис. 1.23. Спектральна густина потужності фрактального вейвлету [176]

Розглянемо інший тип систем, в яких для кодування бітів логічного нуля та одиниці використовуються різні випадкові процеси. Узагальнена структурна схема кодування у цих системах приведена рис. 1.24.

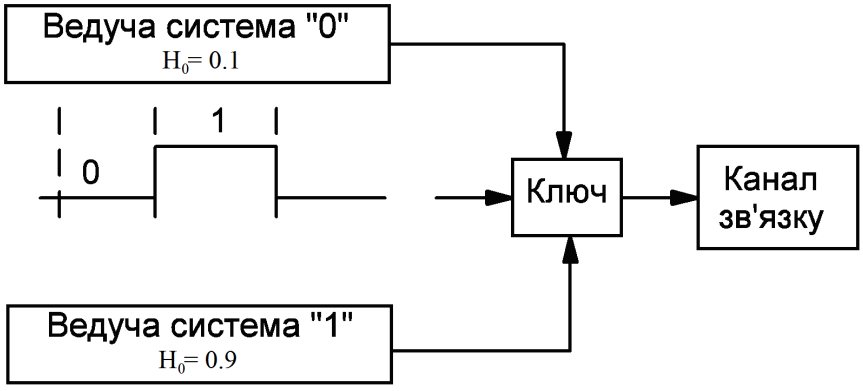


Рис.1.24. Структурна схема кодування бінарного повідомлення з використанням в якості елементів коду випадкових процесів з різними законами розподілу, де: H_0, H_1 – показники Херста випадкового сигналу типу фрактальний гаусовий шум [178]

Система передавання цифрової інформації, що використовує в якості

псевдовипадкового переносника випадковий процес, яким є фрактальний гаусовий шум із різними показниками Херста (кольоровий шум) описана у статті К. Васюти [177]. Кодування цифрової інформації досягається шляхом маніпуляції параметром Херста фрактального гаусового шуму (H_0=0.1, H_1=0.9). На рис.1.25 приведені бінарна інформаційна послідовність, закодована інформаційна послідовність, що сформована маніпулюванням параметра Херста H та її фазовий портрет.

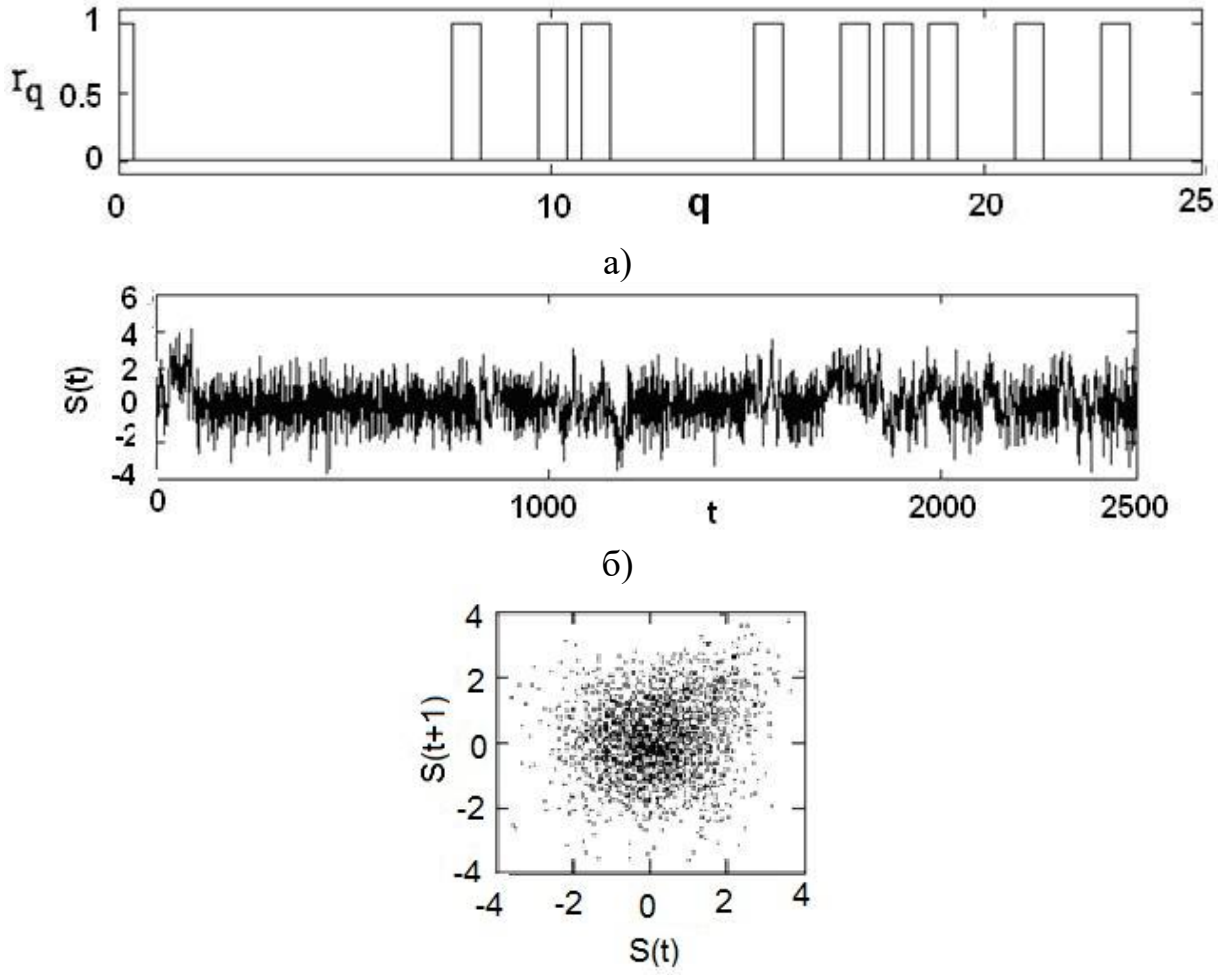


Рис. 1.25. Бінарне інформаційне повідомлення (а), де: r_q – значення відліку інформаційного повідомлення: «0» або «1», q – порядковий номер біту інформаційного повідомлення; закодована інформаційна послідовність – (б), де: S(t) – випадковий сигнал, t – час; фазовий портрет випадкового сигналу – (в), де: S(t+1), S(t) – сусідні відліки дискретизованого випадкового сигналу[177]

Поскільки в якості робочого сигналу у даній системі використовуються сигнали, що породжені випадковим процесом, то генерування його копії на приймальній стороні системи є неможливим.

Тому декодування в даній системі здійснюється шляхом обчислення функції правдоподібності:

$$G\left(H,\sigma_s^2\right)=\ln p\left(\tilde{y}(\omega)\,|\,H,\sigma_s^2\right)=-T\cdot\frac{1}{2\cdot\pi}\cdot\int_{-\infty}^{\infty}\left[\frac{\left|\tilde{y}(\omega)\right|^2}{\tilde{R}_y\left(\omega,H,\sigma_s^2\right)}+\ln\tilde{R}_y\left(\omega,H,\sigma_s^2\right)\right]d\omega, \quad (1.26)$$

$$R_y(\tau,\varepsilon)=\frac{\sigma_s^2\cdot\varepsilon^{2\cdot H-2}}{2}\cdot\left[\left(\frac{\tau}{\varepsilon}+1\right)^{2\cdot H}+\left(\frac{\tau}{\varepsilon}-1\right)^{2\cdot H}-2\cdot\left(\frac{\tau}{\varepsilon}\right)^{2\cdot H}\right]+\sigma_n^2\cdot R_n(\tau), \quad (1.27)$$

де H – показник Херста генерованого сигналу;

σ_s^2 – його дисперсія;

ε – період дискретизація вибірки прийнятого сигналу;

σ_n^2 – дисперсія шуму в каналі зв'язку;

$R_n(\tau)$ – функція автокореляції шумового сигналу.

Таким чином, визначення значення переданого біта інформації зводиться до визначення найбільш вірогідної оцінки його параметра Херста H. При цьому оптимізація відбувається за обома параметрами. На рис. 1.26 приведений вигляд функції правдоподібності в залежності від показника Херста сигналу для співвідношення сигнал/шум, що становить $\sigma_s^2/\sigma_n^2=5$.

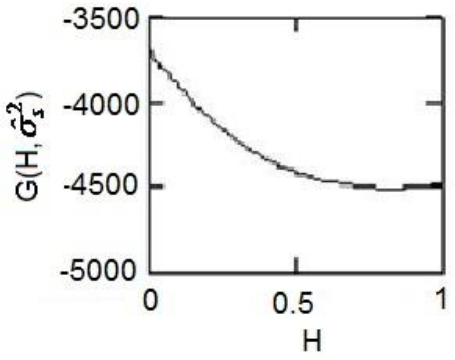


Рис.1.26. Функція максимальної правдоподібності G (H – показник Херста випадкового сигналу типу ФГШ, $\hat{\sigma}_s^2$ – його потужність) [177]

Зауважимо, що процеси кодування у розглянутих системах є різними. У першій системі використовується модуляція високочастотного коливання фрактальним сигналом, за рахунок чого відбувається додатково розширення його спектру, а у другій системі – використовуються випадкові процеси із різними показниками Херста в залежності від значення інформаційного біту.

Недоліком обох описаних систем є складність реалізації. У першій системі це пов'язано із методом генерування сигналу типу фрактальний вейвлет, оскільки для цього потрібно запам'ятовувати велику кількість відліків, або ж потрібно виконувати операцію перетворення Фур'є над досить складним за своєю формою сигналом. У другій системі складним є ускладненою оптимізація функції правдоподібності за двома параметрами.

Описані вище системи використовують досить специфічні методи генерування фрактальних сигналів – сигнал типу фрактальний вейвлет, що передбачає перетворення Фур’є, та кольоровий фрактальний шум.

Зростання обчислювальної потужності сучасної комп’ютерної техніки значно розширює можливості розробників систем передавання інформації. Зокрема поряд із традиційними характеристиками сигналів (дисперсія, математичне сподівання тощо), варіація котрих дає можливість кодувати цифрову інформацію, можна використовувати інші, більш складні характеристики, що враховують тонку структуру сигналу.

ВИСНОВКИ

1. Проведений аналіз існуючих генераторів псевдовипадкових коливань дає можливість розділити їх дві групи – радіотехнічні пристрої, з відомими схемотехнічними рішеннями та пристрої, робота яких грунтується на аналізі математичних моделей, що пов’язано з необхідністю розроблення схемотехнічних рішень.

2. Оснований на теоретичних досягенннях математики аналіз математичних об’єктів, до яких належать системи диференційних рівнянь, різницевих рівнянь, дискретних відображень, , дає можливість знаходити області існування псевдовипадкових розв’язків у таких системах. До найбільш поширених та ефективних методів слід віднести дослідження спектру показників Ляпунова системи, значення модуля яких дає можливість однозначо встановити умови виникнення псевдовипадкових коливань. Ці умови відносно нескладно можна переносити на електричні схеми, що можуть бути описані відповідними математичними об’єктами. Іншим важливим досягненням теорії є твердження щодо необхідних умов для виникнення псевдовипадкових розв'язків – існування нелінійних членів у системі рівнянь та порядок системи не нижчий двох.

2. Із аналізу літературних джерел останніх двох десятиліть присвячених дослідженню процесів передавання інформації, випливає, що подальше підвищення завадостійкості можливе шляхом використання широкосмугових фрактальних сигналів. Теорія завадостійкого передавання інформації розвивається у напрямку пошуку нових класів сигналів, використання яких уможливлює розробку завадостійких телекомунікаційних систем. Поширення набули декілька базових технологій основаних на синхронізації псевдовипадкових коливань та модуляції псевдовипадкового переносника інформаційним сигналом.

3. Для якісної роботи систем передавання інформації, що використовує псевдовипадкові коливання необхідно забезпечити синхронну роботу

генераторів псевдовипадкових коливань передавальної та приймальної сторін, що є ускладненим із-за впливу багатьох факторів – розбалансу параметрів генераторів передавача та приймача, дисперсії, затухання та міжсимвольної інтерференції в каналі зв'язку.

4. Використання модуляції інформаційним сигналом псевдовипадкового переносника вимагає дослідження впливу глибини модуляції, співвідношення амплітуд і частотних характеристик інформаційного сигналу та псевдовипадкового переносника на якість відтворення інформаційного сигналу. Вигляд функції взаємної кореляції між вхідним та вихідним сигналами генератора вказує на необхідність використання кореляторів на приймальній стороні системи.

5. Більша кількість розроблених на даний час генераторів псевдовипадкових коливань не може використовуватися для генерування псевдовипадкового переносника, оскільки генеровані коливання мають спектри потужності, що є сильно сегментованими, тоді як для вирішення прикладних завдань передавання інформації необхідна рівномірна спектральна щільність у смузі генерації. Для синхронізації коливань у приймачеві та передавачеві необхідна розробка прецизійних генераторів зі стабільними характеристиками, що мають малий розкид, або розробка генераторів з практично допустимою чутливістю до розкиду параметрів. У порівнянні зі звичайними генераторами псевдовипадкових коливань прецизійні генератори володіють високою стійкістю та якістю синхронного відгуку.

6. За сучасними стандартами передавання інформації будь-яка система потребує криптографічного захисту. До сучасних методів крптографічного захисту інформації з високою швидкодією можна віднести потокове шифрування інформаційного повідомлення псевдовипадковими послідовностями. При цьому псевдовипадкові послідовності повинні відповідати вимогам тестів. Дослідження таких властивостей є окремим етапом розроблення телекомунікаційних систем.

7. Однією із задач криптографії є захист мультимедійної інформації (відеофайлів, графічної та аудіо- інформації). При цьому важливим завданням є вирішення проблеми синхронізації передавальної та приймальної сторін системи у так званих системах реального часу, до яких відносяться системи передавання аудіоінформації.

8. Поряд із псевдовипадковими сигналами, базові технології яких вже стали традиційними (перемикання між генераторами псевдовипадкових коливань, модуляція псевдовипадковим переносником, імпульсна синхронізація), розвивається ряд методів, що використовують фрактальні робочі сигнали, у тому числі самоподібні сигнали, зокрема фрактальний гаусовий шум.

9. Теорія самоподібних сигналів, яким притаманні властивості псевдовипадкових сигналів, є досить складною і вимагає розвитку та удосконалення методів математичного моделювання їх спектральних і імовірнісних властивостей.

РОЗДІЛ 2. МОДЕЛІ ЦИФРОВИХ СИСТЕМ ЗВ'ЯЗКУ З ШИФРУВАННЯМ ІНФОРМАЦІЇ ПСЕВДОВИПАДКОВИМИ БІНАРНИМИ ПОСЛІДОВНОСТЯМИ, ФОРМОВАНИМИ ХАОТИЧНИМИ КОЛИВАННЯМИ З ДИСКРЕТНОЮ ФУНКЦІЄЮ ВІДОБРАЖЕННЯ

У сучасних системах передавання інформації поряд із традиційними алгоритмами шифрування (рис. 1.8) набув поширення метод шифрування, що отримав назву потокового (його історична назва – гамування [127]).

У даному розділі приведені результати досліджень властивостей ПВП із характерними для криптографії довжинами (64, 128, 256, 512, 1024 біти), що використовуються в якості ключів в стандартних алгоритмах оброблення інформації у телекомунікаційних системах; розроблені моделі систем передавання цифрової інформації з використанням хаотичних коливань, генерованих логістичним відображенням та узагальненим відображенням Пекаря. Досліджені алгоритми шифрування текстової інформації, зображень та мовних сигналів, та вплив канального кодування на тривалість процесу синхронізації генераторів хаотичних коливань передавальної та приймальної сторін системи передавання інформації.

2.1. Моделювання системи передавання текстової інформації з шифруванням псевдовипадковими послідовностями генерованими за логістичним відображенням

Розроблена [1, 9] програмна реалізація системи передавання даних, що зашифровані послідовностями, формованими на основі одновимірних дискретних відображень. Однією із основних проблем, що виникають при побудові таких систем є забезпечення синхронізації між передавальною та приймальною сторонами системи зв'язку. Більшість способів прихованого передавання інформації, що використовують явище синхронізації хаотичних

коливань (ХК) вимагає забезпечення високого ступеня ідентичності генераторів [22], що є важкою технологічною та технічною задачею.

Потокове шифрування текстової інформації здійснювалось з використанням бінарних ПВП, генерованих за логістичним відображенням:

$$x_{n+1} = \lambda \cdot x_n \cdot (1 - x_n), \qquad (2.1)$$

Генеровані за логістичним відображенням послідовності є псевдовипадковими при значеннях параметру λ, що належить діапазону $3,65 \cdots 3,95$.

Структурні схеми кодера і декодер приведені на рис.2.1 та рис. 2.2 відповідно.

Згідно структурній схемі кодера (рис.2.1) початкові дані (текст) від джерела інформації поступають на вхід кодера системи з подальшим перетворенням у 8-бітові символи у відповідності з таблицею американського стандарту кодування інформації (далі – ASCII).

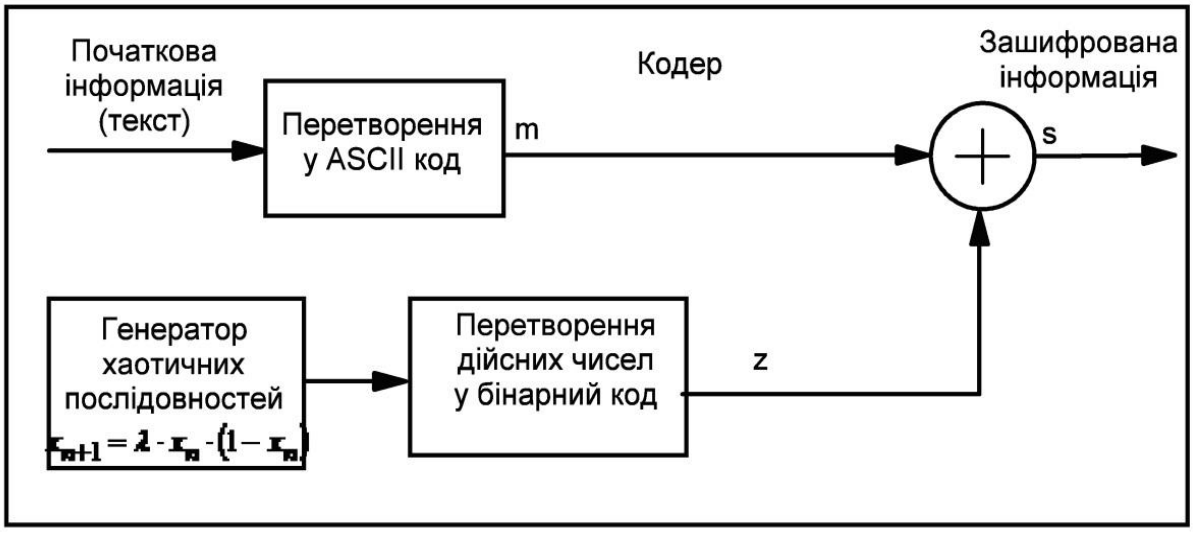


Рис.2.1. Структурна схеми кодера СПІ, що використовує логістичне відображення, де λ, x_n, x_{n+1} параметр та значення динамічних змінних, dt – період синхронізації, m – інформаційне повідомлення, z – ПВП, s – отримана зашифрована інформація

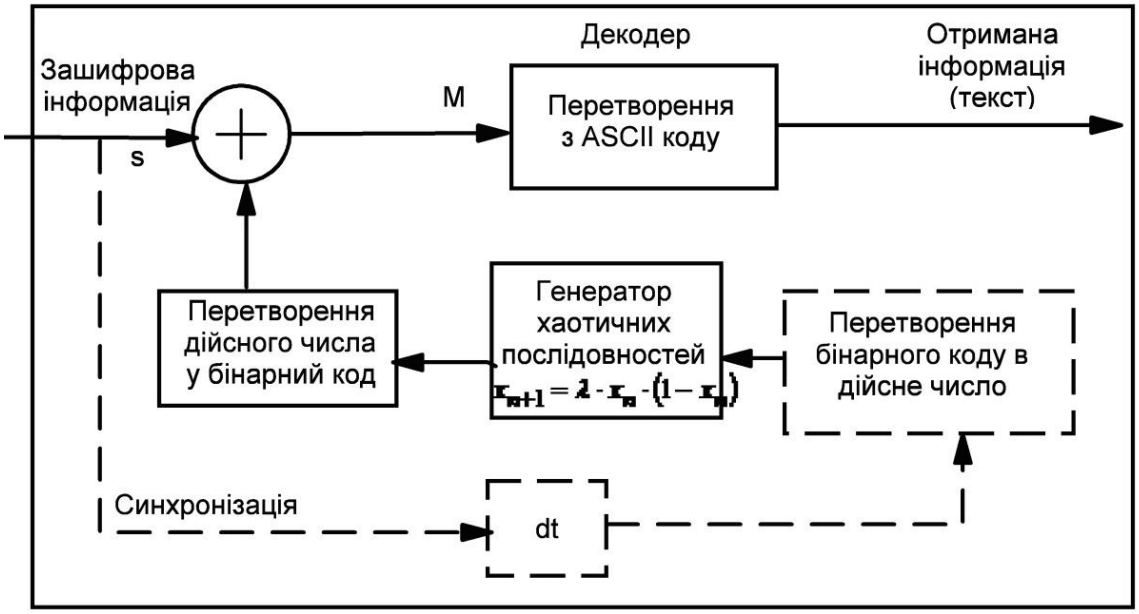


Рис.2.2. Структурна схема декодера СПІ, що викоистовує логістичне відображення, де λ, x_n, x_{n+1} параметр та значення динамічних змінних, dt – період синхронізації, m – інформаційне повідомлення, z – ПВП, s – отримана зашифрована інформація

Генерована за логістичним відображенням послідовність чисел трансформується у двійкові 8-бітні символи у відповідності із поліномним представленням:

$$z_n = 2^{-1} \cdot b_{n1} + 2^{-2} \cdot b_{n2} + \cdots + 2^{-8} \cdot b_{n8}. \quad (2.2)$$

Інформаційне повідомлення m_i сумується по модулю 2 з елементами ПВП:

$$s_i = m_i \oplus z_i. \qquad (2.3)$$

Процес розшифровування інформації здійснюється шляхом додавання по модулю 2 отриманої зашифрованої послідовності генерованою приймальною стороною декодером ПВП при тому ж початковому значенні динамічної змінної елемента x_0 та параметру керування λ.

Ключем шифрування слугує параметр керування λ та початкове значення динамічної змінної x_0, тому кількість можливих реалізацій ключів, що визначає крипостійкість системи дорівнює:

$$N = \left(10^n\right)^2. \quad (2.4)$$

У нашому випадку точність задання початкових умов на програмному рівні дорівнює 10. Тобто потужність простору ключів системи дорівнює 10^{20}, що є хорошим результатом для двопараметричної системи. Псевдовипадковий характер генерованих біполярних ПВП підтверджується результатами їх тестування за тестами NIST STS (табл. 2.1).

Таблиця 2.1.

Результати проходження тестів NIST (National Institute of Standards and Technology) STS (StatisticalTest Suit)

Назва тесту	Значення p-value	Проходження, %
Частотний побітовий тест	0,345	99
Частотний блочний тест	0,297	96
Тест на послідовність однакових бітів	0,654	97,2
Тест на найдовшу послідовність одиниць у блоці	0,612	99
Тест рангів бінарних матриць	0,732	98
Спектральний тест	0,512	98
Тест на співпадання неперетинних шаблонів	0,432	98,5
Тест на співпадання перетинних шаблонів	0,371	97,5
Універсальний статистичний тест Мауера	0,052	98
Тест на основі стискування Лемпела-Зіва	0,299	97
Тест на лінійну складність	0,377	97,3
Тест приблизної ентропії	0,342	98,1
Тест кумулятивних сум	0,099	96
Тест на довільні відхилення	0,645	99
Інший тест на довільні відхилення	0,034	99
Тест на періодичність	0,087	97

Синхронізація генераторів ппиймальної та передавальної сторні системи здійснювалася шляхом чергування часових проміжків передавання

послідовності синхронізації та інформаційної зашифрованої послідовності (рис.2.3).

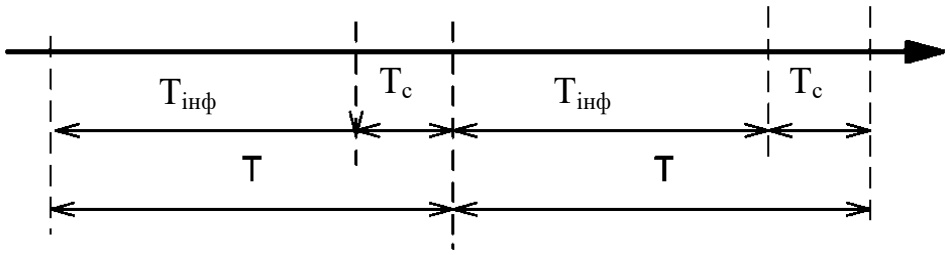


Рис.2.3. Часова діаграма передавання послідовності синхронізації та інформаційного повідомлення ($T_{інф}$ – тривалість інформаційного сигналу, $T_с$ – тривалість послідовності синхронізації)

В якості послідовності синхронізації використовувалася бінарна послідовність, сформована представленням потокового значення хаотичного коливання в двійковому коді. Період передавання послідовності синхронізації залежить від швидкодії комп'ютера та відстані між комп'ютерами приймальної та передавальної сторін системи.

Для реалізації системи на програмно-апаратному рівні були використані сучасні програмні засоби, а саме мова програмування Delphi 7.0. Система працює у реальному часі та повно дуплексному режимі за умови наявності довільного апаратного засобу доступу до мережі Інтернет. Користувачам системи достатньо лише вказати IP-адреси для їх ідентифікації.

Робота програми була протестована шляхом передавання текстів з різною довжиною. Було встановлено, що при передаванні текстових повідомлень довжиною до 10000 символів на різних мовах в on-line режимі мала місце стійка синхронізація та безпомилкове передавання інформації. Підбір періоду синхронізації виконувався на програмному рівні. При передаванні інформації між комп'ютерами Intel P-IV 2,4 ГГц розташованих на відстані 100 м максимальне значення періоду становило 27,8 мкс, тобто при значеннях періоду менших 27,8 мкс мала місце стабільна синхронізація.

2.2. Шифрування інформації з використанням псевдовипадкових гаусових послідовностей

Перспективним напрямком розвитку засобів телекомунікацій є використання у СПІ нових методів кодування, шифрування та передавання інформації, що базуються на складних шумоподібних сигналах. Швидкий розвиток електронних засобів телекомунікацій сприяв розробленню методів, що ґрунтуються на теорії динамічних систем, використовуваних для генерування хаотичних коливань.

Більшість із таких методів та алгоритмів шифрування, особливо потокові шифри, використовують генератори ключових послідовностей у вигляді потоку бітів, що можуть бути точно відтвореними на приймальній стороні, в той час як для стороннього спостерігача він видається випадковим.

Генерування ключового потоку в свою чергу можна здійснити на основі випадкової множини чисел із заданим розподілом. З теорії випадкових величин добре відомо, що будь-який розподіл густини імовірності можна отримати із рівномірного розподілу шляхом функціонального перетворення випадкових величин [181]:

$$p(y)=\sum_{i=1}^{n} p_0\left[h_i(y)\right]\cdot\left|h_i'(y)\right|, \qquad (2.5)$$

де $p_0\left[h_i(x)\right]$ — випадкова величина (у нашому випадку — це нормальний розподіл), n — кількість гілок оберненої функції $y=h(x)$.

Найбільш поширеними методами генерування випадкових величин із заданою функцією розподілу є перетворення рівномірно розподілених на відрізку $[0;1]$ чисел. Найбільш відомомим на сьогодні генератором випадкових чисел із рівномірним розподілом є схема Лемера [182], що була запропонована у 1948 році. Послідовність псевдовипадкових чисел $\{x_n\}$ може бути отримана із лінійного рекурентного рівняння:

$$x_{n+1}=a\cdot x_n+b(\mathrm{mod}\, m),\ n=0,1,\ldots \qquad (2.6)$$

де $x_0 \geq 0$ — початкове значення (ключ); $a \geq 0$, $b \geq 0$, $m \geq 0$ – достатньо великі по модулю взаємно прості числа; $mod\,(m)$ – залишок від ділення на m.

Очевидно, що послідовність генерована за рівнянням (2.6) матиме період значення якого є меншим ніж m. Тому для отримання довгих послідовностей необхідно вибирати досить великі значення модуля m. Для створення лінійного конгруентного генератора (далі – ЛКГ) були вибрані наступні значення параметрів:

$$m = 2^{24},\ a = 75,\ b = 7,\ x_0 = 1 \quad (2.7)$$

Генерування ПВП із заданою функцією розподілу можна здійснити шляхом перетворення (2.6) рівномірно розподілених чисел на відрізку $[0;1]$. Рівномірно розподілені числа отримують використанням лінійного конгруентного генератора [182], що утворює періодичну послідовність цілих чисел з рівномірним розподілом на відрізку $\{0, N-1\}$. Сформована генератором послідовність цілих чисел перетворюється за допомогою алгоритму Бокса-Мюллера [183] у послідовність псевдовипадкових дійсних чисел, що належать інтервалу $[0;1]$, значення яких підпорядковане розподілу Гауса.

Щоб детальніше проаналізувати роботу алгоритму, розглянемо перетворення чисел за алгоритмом Бокса-Міллера. У нашій схемі цей алгоритм використовує два різні лінійні конгруентні генератори:

$$x_{1,n+1} = \left(a_1 \cdot x_{1,n} + d_1\right) \bmod N, \quad (2.8)$$

$$x_{2,n+1} = \left(a_2 \cdot x_{2,n} + d_2\right) \bmod N, \quad (2.9)$$

Послідовності дійсних чисел, що сформовані такими генераторами, перетворюють згідно наступних співвідношень:

$$\nu = x_{1,n}^2 + x_{2,n}^2, \quad (2.10)$$

$$y_{1,n} = x_{1,n} \cdot \sqrt{\frac{-2 \cdot \log(\nu)}{\nu}}, \quad (2.11)$$

$$y_{2,n} = x_{2,n} \cdot \sqrt{\frac{-2 \cdot \log(\nu)}{\nu}}, \qquad (2.12)$$

де $x_{1,n}$, $x_{2,n}$ – псевдовипадкові числа з рівномірним розподілом; $y_{1,n}$, $y_{2,n}$ – псевдовипадкові числа з Гаусовим розподілом.

Якщо сума квадратів чисел $x_{1,n}$ та $x_{2,n}$ є більшою за одиницю, то обчислення за (2.8) і (2.9) не виконується, а здійснюється вибір наступних чисел.

Розглянемо алгоритм шифрування кольорового зображення на прикладі растрового [184] формату у трикольоровому стандарті подання кольору RGB, в якому кожне зображення представлене набором пікселів, що утворюють двовимірний масив. Кожен піксель є кольоровою крапкою з певними координатами. Колір пікселя кодується трьома дійсними числами із значеннями від 0 до 255, що означають яскравість однієї базової палітри: червоний, зелений або синій колір.

У процесі шифрування зображення використовуємо бінарне представлення цілих чисел: восьми-бітовим двійковим числом:

$$z_{r,n} = 0, b_{r,n1}, b_{r,n2} \ldots b_{r,n1} = 2^{-1} \cdot b_{r,n1} + 2^{-2} \cdot b_{r,n2} + \ldots + 2^{-8} \cdot b_{r,n8}, \qquad (2.13)$$

де $r = 1,2,3$ – індекси, що позначають один із трьох кольорів RGB (червоний, зелений або синій).

Ключова послідовність шифрування утворюється шляхом восьмираундового виконання алгоритму Бокса-Міллера, причому на кожному кроці здійснюється порівняння значення одного із випадкових дійсних чисел $y_{1,n}$ або $y_{2,n}$ з 0.5. Якщо це число має значення менше 0.5 ,то вважатимемо, що генерується біт зі значенням «0»; у іншому випадку — генерується біт зі значенням «1». Таким чином формується 8-бітова послідовність $m_8 = \{m_1, m_2, m_3, m_4, m_5, m_6, m_7, m_8\}$. Для шифрування трьох базових кольорів, необхідно сформувати три відповідні їм послідовності: m_8^r,

m_8^g, m_8^b. Отже на шифрування одного пікселя кольорового зображення потрібно 24 двійкові числа, що генеровані за алгоритмом Бокса-Міллера. Оскільки перетворенню підлягають два дійсні числа, то вони можуть бути представлені дванадцяти-розрядним двійковим числом. Таким чином визначені за виразами 2.14 та 2.15 дійсні числа матимуть у двійковому форматі наступне представлення:

$$y_{1,n} = 2^{-1} \cdot b_{y1,n1} + 2^{-2} \cdot b_{y1,n2} + \cdots + 2^{-11} \cdot b_{y1,n11} + 2^{-12} \cdot b_{y1,n12} \qquad (2.14)$$

$$y_{2,n} = 2^{-1} \cdot b_{y2,n1} + 2^{-2} \cdot b_{y2,n2} + \cdots + 2^{-11} \cdot b_{y2,n11} + 2^{-12} \cdot b_{y2,n12} \qquad (2.15)$$

Зашифрована послідовність, що представляє градацію одного із базових кольорів, утворюється шляхом додавання по модулю 2 (операція XOR) елементів ПВП та бітів із 8 бітного представлення кожного цілого числа, що представляє даний колір (формула 2.13). Описаний алгоритм шифрування приведений на рис.2.4. Операція шифрування може бути представлена наступною формулою:

$$s_i = m_i \oplus z_i, \qquad (2.16)$$

де s_i – зашифрована послідовність, m_i – ключова послідовність шифрування, $\oplus$ – символ дії XOR, z_i – біти незашифрованого зображення.

Таким чином була отримана система шифрування, що використовує ПВП із гаусовим розподілом [12, 15].

У розробленій нами [15, 12] системі передавання двійкових даних для шифрування використовуються ПВП генеровані за логістичним та ЛКГ.

Першим етапом у СПІ є перетворення символьного потоку даних до двійкового вигляду у нотації ASCII. Далі кожному байту утвореної бітової послідовності ставимо у відповідність восьмибітове двійкове представлення дійсного числа, що генероване за логістичним відображенням. З метою шифрування інформації додаємо до одного байту повідомлення (код символу інформаційного потоку в коді ASCII) додається один байт двійкового представлення десяткового дробу, значення якого із відповідною точністю

представлення числа із плаваючою крапкою знаходимо за логістичним відображенням.

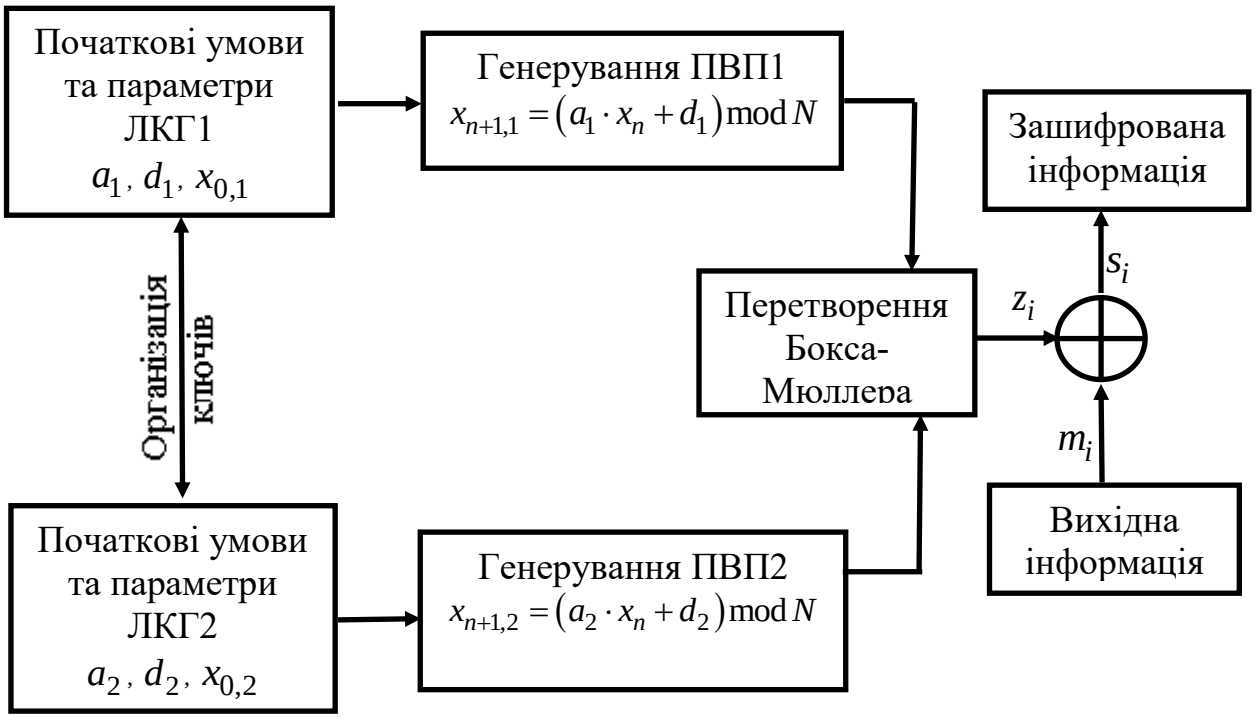


Рис. 2.4. Алгоритм схеми шифрування зображень (a_1, d_1, a_2, d_2 , N – параметри ЛКГ, $x_{0,1}$, $x_{0,2}$ – початкові значення ЛКГ, x_n, $x_{n+1,1}$, $x_{n+1,2}$ – значення динамічних змінних ЛКГ; z_i – бінарна ПВП, m_i – двійкова інформаційна послідовність, s_i – зашифрована інформаційна послідовність)

Даний алгоритм може бути використаним для шифрування текстової та графічної інформації. Лабораторний макет даного алгоритму був реалізований у середовищі програмування Borland Delphi.

На рис.2.5 зображено вікно програмного додатку, що розроблений у середовищі Borland Delphi 7.0. У полі адресатат повідомлення вказано IP-адресу комп’ютера, що з’єднаний у мережу із комп’ютером передавача (у полі «Ім’я (адреса) одержувача» вказана його адреса 10.105.10.83). Ключі шифрування повідомлення залежать від початкового значення динамічної змінної x_0 та параметру логістичного відображення λ, для введення яких передбачені спеціальні поля у вікні програми.

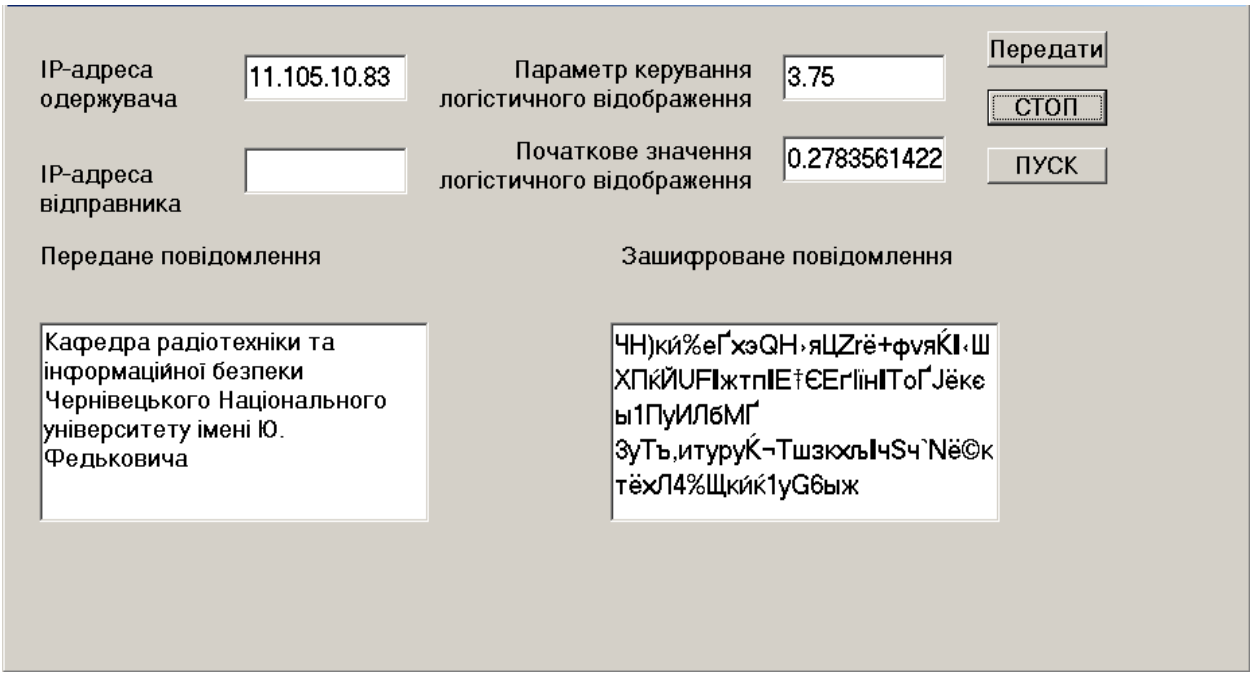


Рис.2.5. Інтерфейс програми для обміну текстовими повідомленнями

Розглянемо детальніше процес шифрування текстової інформації. Вихідні дані (текст) надходять із джерела інформації на вхід кодера системи і перетворюються у восьмибітові символи у відповідності з таблицею ASCII символів. Для шифрування інформаційного потоку використовують псевдовипадкову послідовність чисел з гаусовим розподілом формованими алгоритмом Бокса-Мюллера з використанням генерованих за логістичним та конгруентним відображеннями псевдовипадкових послідовностей (рис. 2.6).

Кожне із чисел утвореної послідовності перетворюється до двійкової форми за допомогою поліноміального представлення:

$$x_n = \left(b_{-1}b_{-2}b_{-3}b_{-4}b_{-5}b_{-6}b_{-7}b_{-8}\right)_n = \sum_{i=1}^{8} b_{-i}^{(n)} \cdot 2^{-i}. \quad (2.17)$$

Черговий восьмибітовий символ ASCII інформаційного повідомлення сумується по модулю 2 (дія XOR) із бітами ПВП.

$$s_i = m_i \oplus b_i^{(n)} \qquad (2.18)$$

Блок-схема дешифрування вказаним методом приведена на рис. 2.7.

Дешифрування інформації здійснюється за допомогою тієї ж операції XOR. При цьому поточні значення x_n ПВП генерованої передавальною

стороною періодично передаються приймальній стороні, що забезпечує синхронну роботу приймача та передавача телекомунікаційної системи.

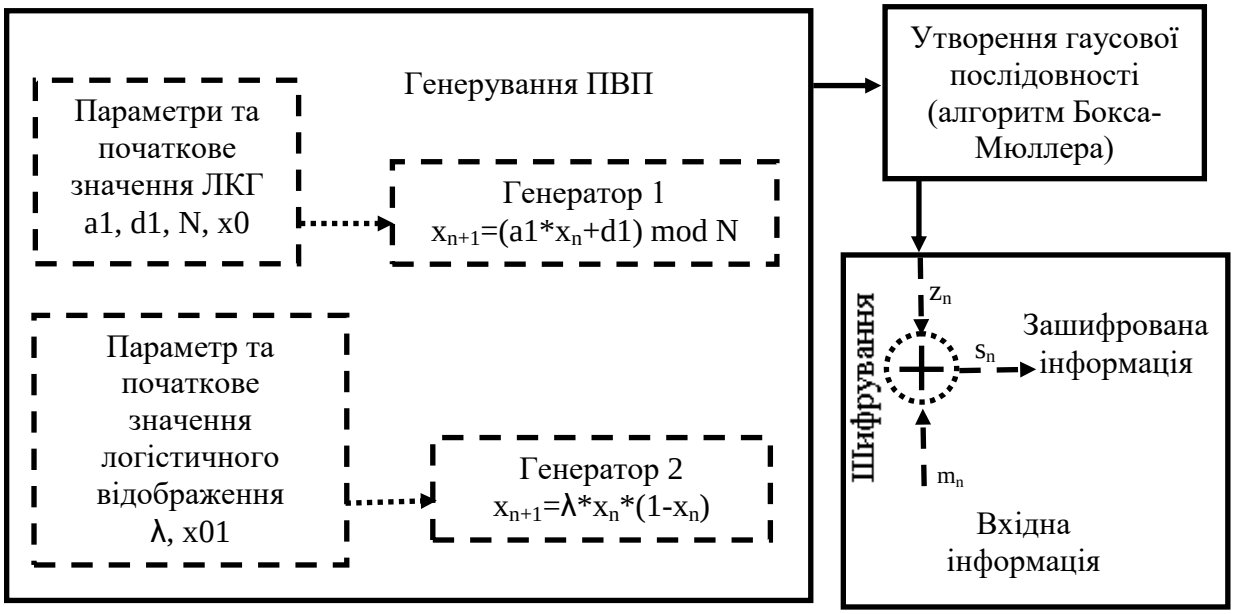


Рис.2.6. Блок-схема методу шифрування інформації із сумісним використанням ПВП, генерованих за логістичним відображенням та алгоритмом Бокса-Мюллера, де: a1, d1, x0 – параметри лінійного конгруентного генератора та його поаткове значення; λ , x01 – парметр та початкове значення логістичного відображення; z_n – бінарна псевдовипадкова послідовність, m_n – двійкова інформаційна послідовність, s_n – зашифрована інформаційна послідовність

Необхідність використання вищеприведеного методу синхронізації [9] обумовлена можливістю передавання інформації без спотворень на протязі обмеженого часового інтервалу, після якого виникає потреба підтримання синхронної роботи системи.

Для шифрування зображень з використанням розробленого методу додатково використовувався механізм дифузії [185], що описується наступною формулою:

$$C(k)=\phi(k)\oplus\{[I(k)+\phi(k)]\bmod N\}\oplus C(k-1), \qquad (2.19)$$

де $C(k-1)$ та $C(k)$ — попередній та наступний байти зашифрованої послідовності, $I(k)$ — байт інформаційної послідовності; $\phi(k)$ — коливна неперіодична функція, в якості якої вибрано логістичне відображення.

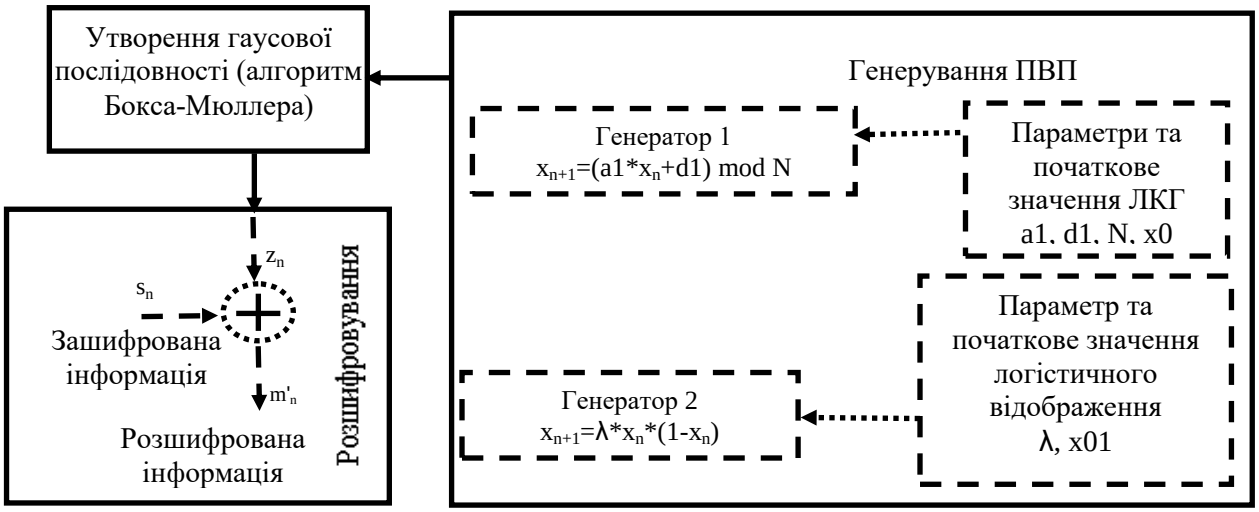


Рис.2.6. Блок-схема розшифровування інформації на приймальній стороні системи (a1, d1, x0 – параметри лінійного конгруентного генератора та його початкове значення; λ , x01 – парметр та початкове значення логістичного відображення; z_n – бінарна ПВП, m'_n – розшифрована послідовність, s_n – зашифрована послідовність)

Обернене перетворення дифузії має наступний вигляд:

$$I(k)=\{\phi(k)\oplus C(k)\oplus C(k-1)+N-\phi(k)\}\bmod N \quad (2.20)$$

Перетворення дифузії характеризується двома параметрами, що дорівнюють початковим значенням байтових послідовностей $C(0)$ та $\phi(0)$, що може бути представлене послідовністю бітів довжиною 1 байт.

Часова діаграма послідовності з гаусовим розподілом, отримана за алгоритмом Бокса-Мюллера, підтверджує її псевдовипадковий характер (рис.2.8).

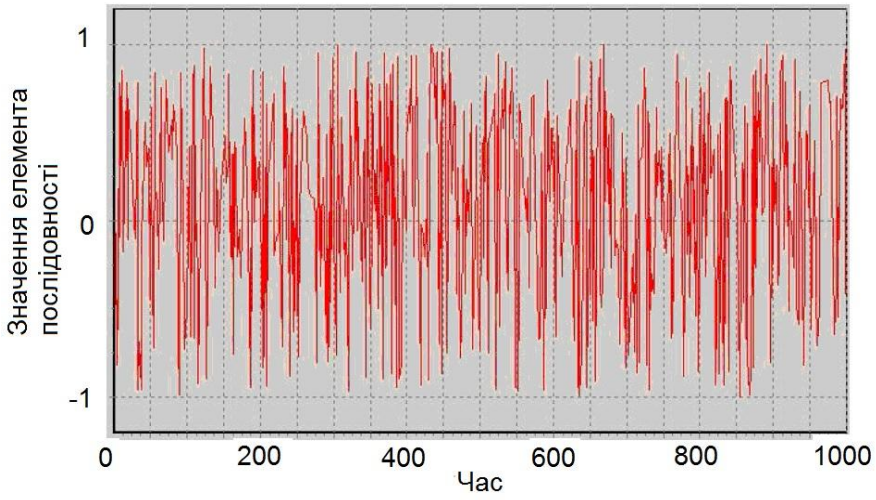
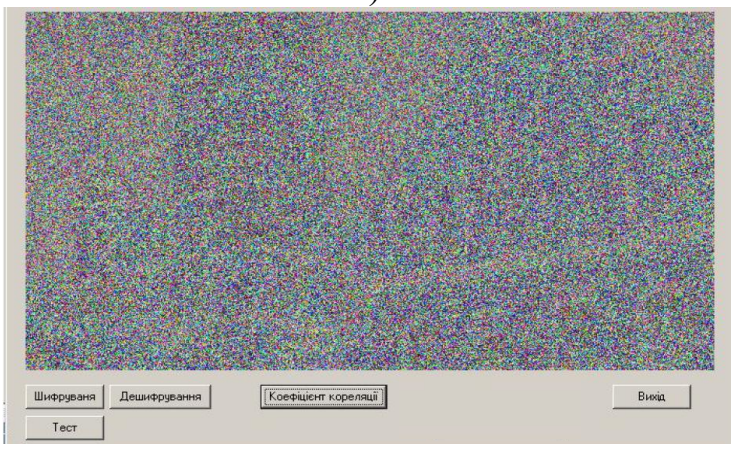


Рис.2.8. Часова діаграма гаусової ПВП, отриманої методом Бокса-Мюллера

На рис. 2.9 приведені результати використання описаного методу для шифрування кольорового зображення.

а)



б)

Рис.2.9. Кольорове зображення (а) , зашифроване зображення (б)

Критерієм якості шифрування світлини слугувало усереднене значення коефіцієнту кореляції між сусідніми пікселями зашифрованого та початкового зображень [186, 187].

$$C = \frac{N \cdot \sum_{i=1}^{N} x_j \cdot y_j - \sum_{j=1}^{N} x_j \cdot \sum_{j=1}^{N} y_j}{\sqrt{N \cdot \left\{ \sum_{j=1}^{N} x_j^2 - \left(\sum_{j=1}^{N} x_j \right)^2 \right\}} \cdot \sqrt{N \cdot \left\{ \sum_{j=1}^{N} y_j^2 - \left(\sum_{j=1}^{N} y_j \right)^2 \right\}}}, \qquad (2.21)$$

де x, y – значення градацій кольорів для двох сусідніх пік селів зображення, N – число пікселів, що вибрані для розрахунку коефіцієнту кореляції.

Значення коефіцієнту кореляції між пікселями початкового зображення знаходилося у межах 0,85..0,98, а для зашифрованого – у межах 0,01..0,06, що вказує на задовільну крипостійкість даного методу.

Розроблений алгоритм шифрування зображень був також протестований за допомогою гістограмного методу, суть якого полягає у розрахунку розподілу пікселів за інтенсивністю для 3-х базових кольорів [187, 188]. Гістограма інтенсивності пікселів приведена на рис.2.10.

а) б)

Рис.2.10. Гістограма інтенсивності пікселів кольорового зображення представленого на рис.2.9 (а); та зашифрованого зображення (б)

Із отриманих гістограм випливає, що розподіл інтенсивності зашифрованого зображення є рівномірним на проміжку можливих його значень 0…255, внаслідок чого зашифроване зображення набуває рівномірного сірого фону (рис.2.10б).

2.3. Шифрування цифрової інформації бінарними ПВП у системах з кодуванням джерела повідомлень

Розроблений метод шифрування інформації в процесі її економного кодування за допомогою бінарних послідовностей, формованих на основі ХК, генерованих за логістичним відображенням [32].

На рис.2.11 приведені блок-схема кодера та декодера системи передавання цифрової інформації, що забезпечує її стиснення та шифрування.

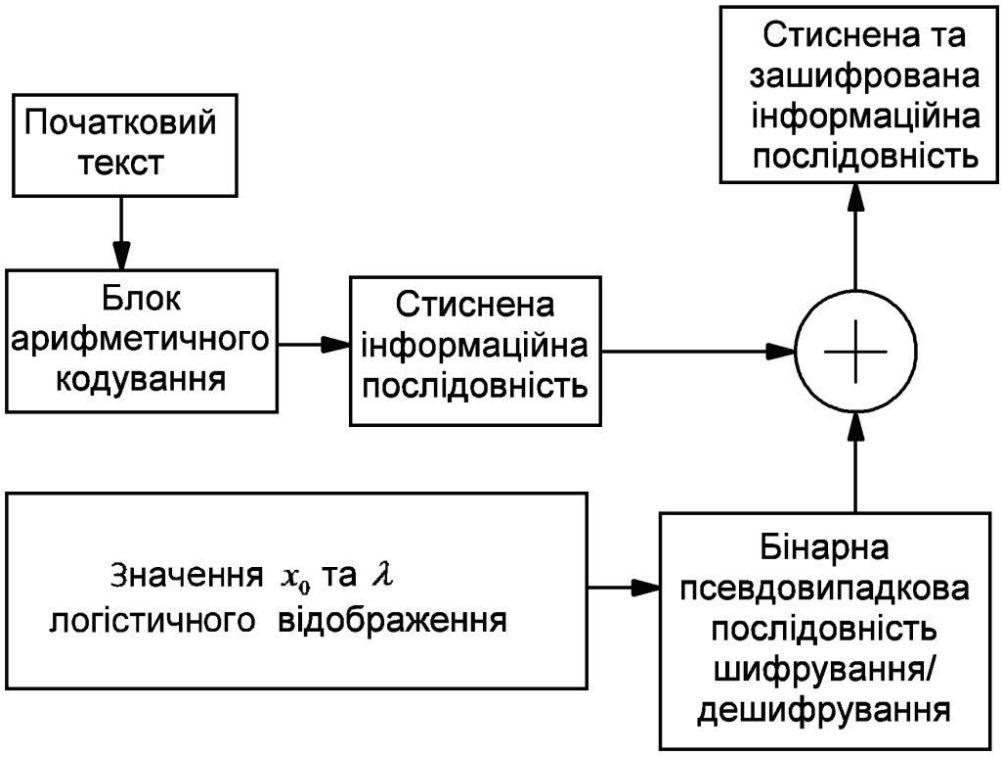


Рис.2.11. Блок-схема кодера стискування та шифрування за логістичним відображенням (λ, x_0 – параметр та початкове значення логістичного відображення)

На передавальній стороні спочатку будується табл. частот текстової інформації з використанням алфавіту ASCII з наступним її кодуванням блоком неадаптивного арифметичного кодування. На виході блоку арифметичного кодування формується двійкова послідовність, шифрування якої здійснюється шляхом її сумування за модулем 2 з бінарною ПВП, генерованою системою з дискретною функцією відображення.

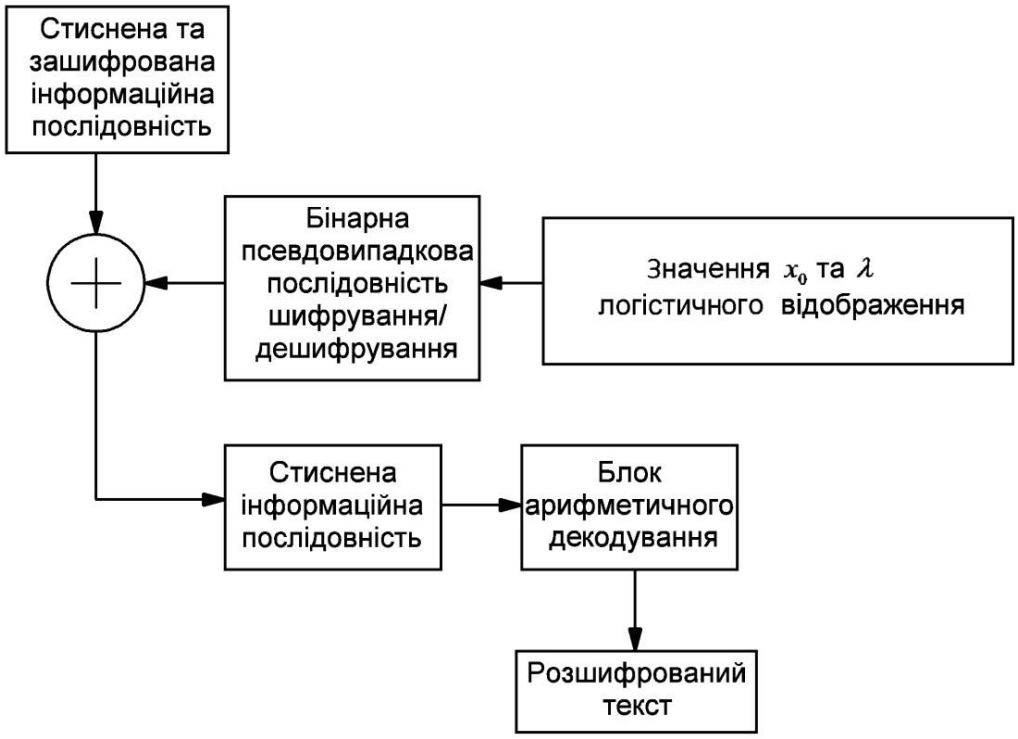


Рис.2.12. Блок-схема декодера системи передавання стисненої та зашифрованої інформації (λ, x_0 – параметр та початкове значення логістичного відображення)

На приймальній стороні системи процес дешифрування та декодування інформації здійснюється у зворотному порядку. Прийнята послідовність двійкових чисел сумується за модулем 2 із бінарною ПВП двійкових чисел, формованої на основі значень хаотичних коливань, що генеровані за тими ж значеннями параметра керування λ та x_0, що і коливання на стороні передавача. Далі отримана закодована послідовність двійкових чисел

декодується блоком арифметичного декодера. Результатом виконаних процедур отримуємо початковий текст у форматі ASCII.

При використанні алгоритму адаптивного арифметичного кодування відпадає необхідність формування та передавання таблиці частот передавальною стороною системи, що пояснюється наступним.

Звичайне арифметичне кодування передбачає, що кожному символу із алфавіту потужністю N (кількість символів, що утворюють алфавіт) ставлять у відповідність деяке дробове число із відрізка $\lfloor 0;1 \rfloor$. Попередньо цей відрізок поділяється на N частин. Довжини частин визначаються по-різному для звичайного та адаптивного арифметичного кодування [127].

Звичайний алгоритм арифметичного кодування передбачає визначення частоти повторення символів у кодованому тексті, причому довжини частин, на які розділяється одиничний відрізок, є пропорційними цим частотам [189]. Кодер зчитує перший символ тексту і вибирає відрізок, що відповідає даному символу. Кожен наступний символ потрібно кодувати використовуючи відрізок, обраний на попередньому кроці, з наступним його розділенням на n відрізків у відповідності з таблицею частот повторення символів у тексті. Таким чином, в ході арифметичного кодування на кожному кроці знаходимо деякий відрізок, довжина якого зменшується із кожною новою ітерацією. Будь-яке число, що належить відрізку, визначеному на останній ітерації, є шифром тексту (рис.2.13).

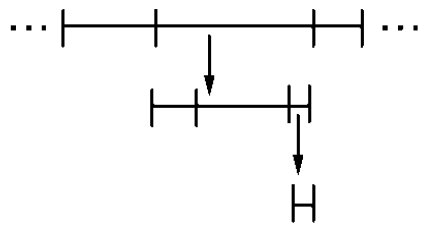


Рис.2.13. Неадаптивне арифметичне кодування

На стороні приймача відбувається процес декодування, що є оберненим до процесу кодування. Звичайний алгоритм арифметичного кодування передбачає,

що на стороні приймача є відомою табл. частоти повторення символів алфавіту у тексті. Отримавши число, декодер ставить йому у відповідність відрізок, до якого воно належить. Таким чином декодер розшифровує першу літеру. Далі вибраний відрізок знову розділяємо у відповідності із таблицею частот та ставимо у відповідність отриманому символу відповідний йому відрізок. Таким чином, декодується друга літера тексту. Процес повторюється до повного декодування тексту.

Існує декілька модифікацій алгоритму арифметичного кодування. Зокрема, поширеним є алгоритм арифметичного кодування [190], у якому замість десяткового числа генерується бітовий потік, а початковий відрізок з $(0;1)$ замінюється на відрізок $(0;65535)$. Цей алгоритм був покладений в основу розробленого методу арифметичного кодування з одночасним шифруванням стиснених інформаційних повідомлень. Розроблений алгоритм кодує початкові символи бітами в залежності від того, яким чином відображається відрізок на черговому кроці ітерації, а саме якщо цілком у праву половину попереднього відрізку, то програма генерує біти із одиничним значенням, а якщо цілком у ліву половину, то програма генерує біти із нульовим значенням. У випадку якщо відрізок не відображається повністю у ліву або праву половину відрізку, то кількість біт, що кодують даний символ збільшуємо на одиницю з продовженням обчислення для цього ж символу [190].

Перед виконанням алгоритму програма знаходить таблицю частот символів у початковому тексті та ініціює змінні, що використовуються в процесі кодування.

У адаптивному методі після кодування чергового символу здійснюється модифікація моделі тексту. Алгоритм такої модифікації оснований на тому, що кожне нове входження симолу призводить до збільшення його частоти, що у свою чергу визначає довжину інтервалу для цього символу.

Модифікаціями такого алгоритму є алгоритми, що поєднують кодування джерела інформації з її шифруванням. В якості алгоритмів кодування використовувалися арифметичне кодування та коди Шеннона-Фано і Хафмена.

У розробленому методі на відміну від існуючих методів стиснення та шифрування інформації [147, 189], у яких використовується процедура зміни частот символів у відповідності із ключем шифрування на кожному кроці алгоритму арифметичного кодування, здійснюється поєднання арифметичного адаптивного кодування із шифруванням шляхом додавання бітів стисненої інформаційної послідовності з бітами ПВП.

Цей алгоритм був проаналізований на прикладах текстів на різних мовах.

В процесі арифметичного кодування такого тексту здійснювався поділ відрізка на дві частини, що відповідають одному із двох можливих значень у вхідному потоці: «0» або «1». На кожному кроці арифметичного кодування міняються місцями відрізки, якщо бітом потоку шифрування є «1» і залишаються без змін, якщо бітом є «0».

Головне вікно розробленої у середовищі Borland C++ програми приведене на рис. 2.14.

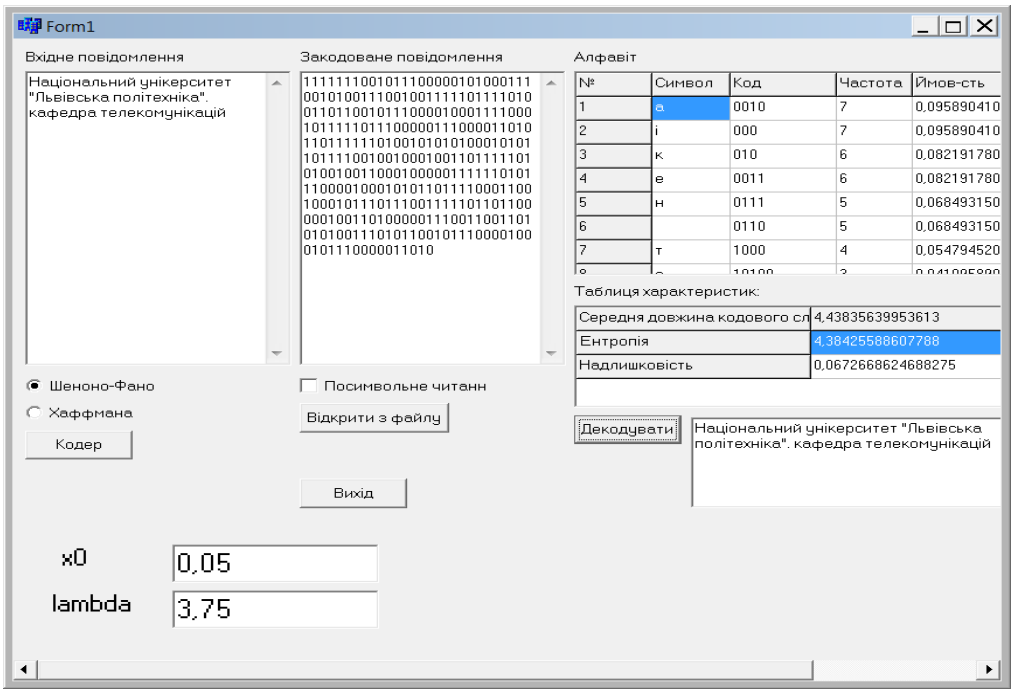


Рис.2.14. Вікно програми економного кодування джерела інформації та її шифрування бінарними ПВП

2.4. Криптографічне шифрування зображення на основі багатомірного узагальненого перетворення Пекаря

Шифрування зображень використовує ряд нелінійних алгоритмів: відображення Пекаря [191], відображення «кіт Арнольда» [192] та ін. [193].

У запропонованому алгоритмі [7] використовувалося узагальнене нелінійне перетворення Пекаря, в процесі якого здійснюється перестановка місцями координат пікселів без зміни їх інтенсивності та загальних розмірів зображення (рис.2.15).

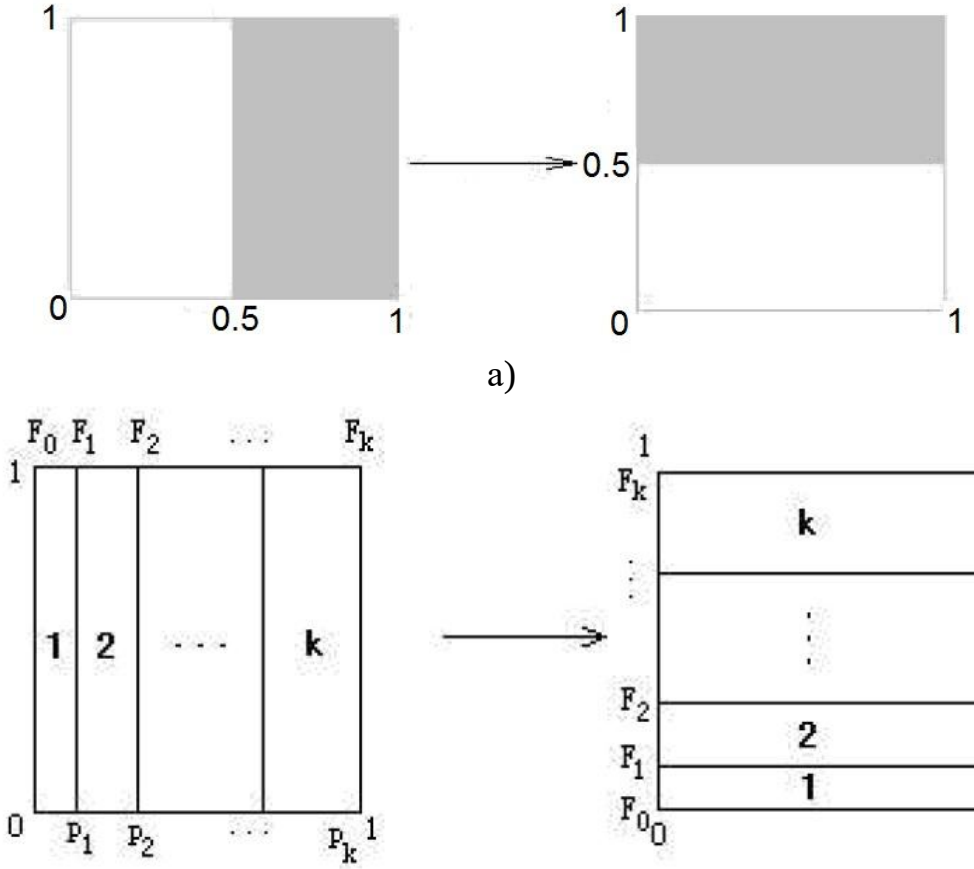


Рис.2.15. Класичне перетворення Пекаряи(а); узагальнене перетворення Пекаря (б), де 1, 2, …, k – послідовна нумерація прямокутників, що утворюють розбиття квадрата; F_0, F_1, F_2, …, F_k – координати кінців відрізків, на які розбивається одинична сторона квадрата; p_1, p_2, …, p_k – довжини відрізків, утворених розбиттям одиничної сторони квадрата [191]

Одно та двовимірне відображення Пекаря, що перетворює множину $I \times I$ саму в себе (рис. 2.15а), описується наступним виразом:

$$\begin{cases} (2 \cdot x, y/2), \textit{якщо } 0 \le x < 1/2 \\ 2 \cdot x, y/2 + 1/2, \textit{якщо } 1/2 \le x < 1 \end{cases} \qquad (2.22)$$

Таке перетворення називається відображенням Пекаря. Суть узагальненого відображення Пекаря полягає в наступному [191]. Одиничний квадрат розділяється на k вертикальних прямокутників (рис. 2.15б): $[F_{i-1}; F_i) \times [0,1)$; $i = 1,\ldots,k$; $F_i = p_1 + p_2 + \cdots + p_i$; $F_0 = 0$; $p_1 + p_0 + \cdots + p_k = 1$, де k – кількість прямокутників, на які розділяємо квадрат, i – поточний номер прямокутників, F_{i-1}, F_i – координати лівого та правого кінців прямокутника відповідно, p_i – довжина бічної горизонтальної сторони прямокутника.

Нижній правий кут i-го прямокутника розміщений у точці $F_i = p_1 + p_2 + \cdots + p_i$, $F_0 = 0$. Узагальнена схема Пекаря розтягує кожен прямокутник у горизонтальному напрямку з коефіцієнтом $1/p_i$, а у вертикальному напрямку стискує прямокутник з коефіцієнтом p_i (рис.2.15б). Аналітично схема може бути представлена у наступному вигляді:

$$\begin{aligned} &B(x,y) = \left(1/p_i \cdot (x - F_i), p_i \cdot y + F_i\right), \\ &(x,y) \in [F_i, F_i + p_i) \times [0,1) \end{aligned} \qquad (2.23),$$

де (x,y) – координати i-го прямокутника до перетворення, а $B(x,y)$ – його нові координати.

За допомогою дискретизованої схеми Пекаря встановлюється взаємнооднозначна відповідність між пікселями початкового та зашифрованого зображень. Пояснимо механізм шифрування за вказаною схемою.

Якщо розділити квадрат розміром $N \times N$ на вертикальні прямокутники розміром $N \times N_i$ пікселів, то дискретизована схема Пекаря описується наступним чином [191]:

$$(r,s) = [N/n_i \cdot (r - N_i) + s \cdot \mathrm{mod}(N/n_i), n_i/N \cdot (s - s \cdot \mathrm{mod}(N/n_i)) + N_i], \qquad (2.24)$$

де (r,s) – цілі числа, що означають координати пікселя, що знаходиться у i-му прямокутнику, n_i – довжина (у пікселях) i-го прямокутника, так що:

$$N_i \le r < N_i + n_i;\ 0 \le s < N, \quad (2.25)$$

Послідовність, що утворена k цілими числами $(n_1, n_2, \ldots, n_k)$ вибирається таким чином, щоб кожне ціле число n_i ділилося на N, а $N_i = n_1 + n_2 + \cdots + n_i$, $N = n_1 + \cdots + n_k$. Якщо не всі числа $\{n_i\}$ діляться на N, і множина точок являє собою прямокутник розмірами $M \times N$, то схема, що встановлює відповідність між пікселами (i, j) та (r,s) і може бути описана за допомогою наступного алгоритму:

$$(r,s) = B_d(i,j) = \left[\left(M_{i-1} \cdot N + j \cdot m_i + i - M_{i-1}\right)/M, \left(M_{i-1} \cdot N + j \cdot m_i + i - M_{i-1}\right) \bmod M\right] \quad (2.26)$$

Прямокутник розмірами $M \times N$ розділяється на вертикальні прямокутники N пікселів по висоті та m_i пікселів по ширині зображення. Послідовність, утворюється k цілими числами, $\{m_i\}$ вибираємо так, щоб $M_i = m_1 + \cdots + m_i$, $M = m_1 + m_2 + \cdots + m_k$, а $M_0 = 0$. Таким чином, дискретизоване двомірне відображення Пекаря, може бути описане аналітичним виразом (2.27).

Для шифрування використовувалось трьохмірне відображення Пекаря, що має у 2-3 рази більшу швидкодію за одновимірне та двохвимірне відображення і може використовуватись у системах реального часу.

Математичною моделлю трьохвимірного відображення (рис.2.16) є наступний вираз [191]:

$$\begin{cases} (2 \cdot x, 2 \cdot y, z/4), \text{ якщ } 0 \le x < 1/2 \cup 0 \le y < 1/2 \\ (2 \cdot x, 2 \cdot y - 1, z/4 + 1/2), \text{ якщ } 0 \le x < 1/2 \cup 1/2 \le y < 1 \\ (2 \cdot x - 1, 2 \cdot y, z/4 + 1/4), \text{ якщ } 1/2 \le x < 1 \cup 0 \le y < 1/2 \\ (2 \cdot x - 1, 2 \cdot y - 1, z/4 + 3/4), \text{ якщ } 1/2 \le x < 1 \cup 1/2 \le y < 1 \end{cases} \quad (2.27)$$

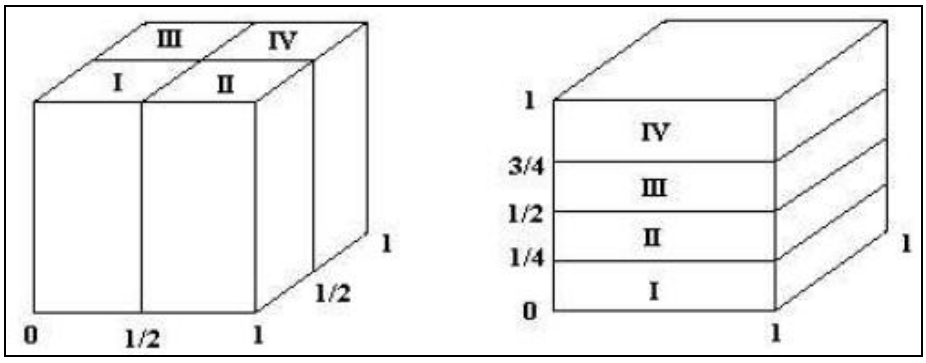


Рис. 2.16. Трьохвимірне відображення Пекаря (I, II, III, IV – нумерація паралелепіпедів, що утворюють розбиття куба із одиничним ребром) [191]

Аналогічно двовимірному відображенню Пекаря трьохвимірне відображення Пекаря також має узагальнену форму. Одиничний куб розділяється на паралелепіпеди (рис.2.14), що стискуються в одному напрямку і розтягуються в іншому. Далі смужки складаються таким чином, щоб вони утворили одиничний куб того ж об'єму. Інакше кажучи, одиничний куб розділяється на $k \times t$ блоків $[W_{i-1}, W_i) \times [H_{j-1}, H_j) \times [0,1)$, $i = 1,\ldots,k$, $j = 1,\ldots,t$, $W_i = w_1, w_2, \ldots, w_i$, $W_0 = 0$ таким чином, щоб виконувались співвідношення: $w_1 + w_2 + \cdots + w_k = 1$ і $H_j = h_1 + h_2 + \cdots + h_j$, $H_0 = 0$, $h_1 + h_2 + \cdots + h_t = 1$. Тоді узагальнена трьохвимірна схема Пекаря описуватиметься співвідношенням [191]:

$$B_3(x, y, z) = \left\lfloor 1/w_i \cdot (x - W_i), 1/h_j \cdot (y - H_j), w_i \cdot h_j \cdot z + L_{ij} \right\rfloor \qquad (2.28)$$

де $(x, y, z) \in [W_{i-1}, W_i) \times [H_{i-1}, H_i) \times [0,1)$, $L_{ij} = W_i \times h_j + H_j$, $i = 1,\ldots,k$, $j = 1,\ldots,t$. Потім трьохвимірна схема дискретизується, при цьому використовується довільний розмір кубу. Вважатимемо, що куб має розміри $W \times H \times L$ і розділяється на $k \times t$ блоків. Послідовність, утворена k цілими числами, $\{w_i\}$, вибирається таким чином, щоб виконувалися співвідношення: $W_i = w_1 + w_2 + \cdots + w_i$, $W = w_1 + w_2 + \cdots + w_k$ і $W_0 = 0$. Така ж процедура здійснюється для послідовності t цілих чисел, за умови, що $H_j = h_1 + h_2 + \cdots + h_j$, $H = h_1 + h_2 + \cdots + h_t$ і $H_0 = 0$.

Перетворення

$$(m',n',l') = B_{3D}(m,n,l) = \left[\left(S \bmod (W \times H) \right) \bmod W, \left[\frac{S \bmod (W \times H)}{W} \right], \left[\frac{S}{W \times H} \right] \right],$$

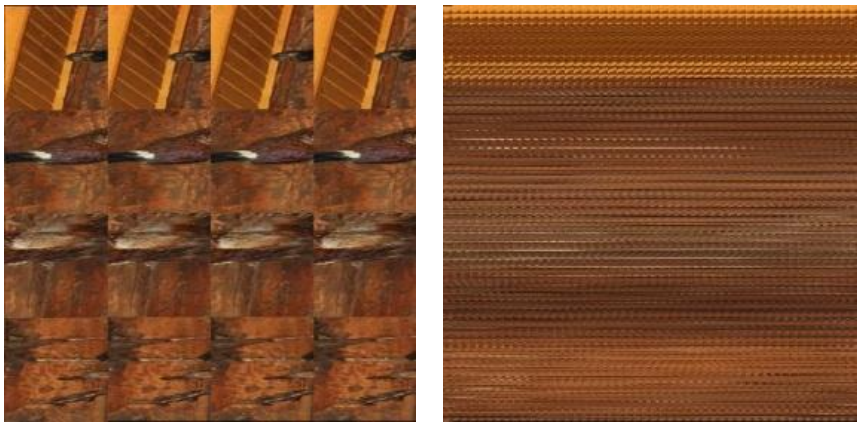
де

$$S = \left(H_{j-1} \times W + W_{i-1} \right) \times L + w_i \times h_j \times l + \left(n - H_{j-1} \right) \times w_i + \left(m - W_{i-1} \right) \qquad (2.29)$$

переводить довільну точку (m,n,l) кубу у точку з координатами (m',n',l') нового кубу.

Розроблена [7] програмна реалізація шифрування двохвимірних зображень з використанням трьохвимірного відображення Пекаря. Результати шифрування початкового зображення (рис.2.17) приведені на рис.2.18. На рис.2.19 приведені результати шифрування з додатковим використанням дифузії.

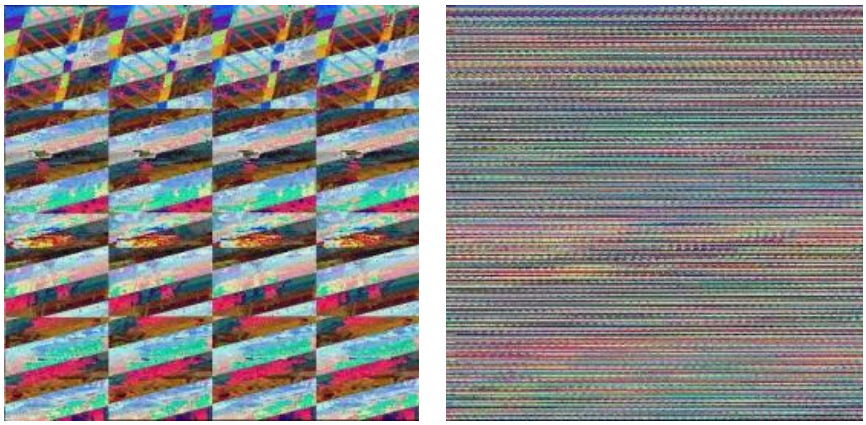
Рис.2.17. Початкове зображення 480x480 пікселів.



а) б)

Рис.2.18. Результат перетворення Пекаря із розділенням початкового зображення на 4 прямокутники (а) – та на 50 прямокутників (б)

Із отриманих результатів випливає, що розбиття зображення на п’ятдесят прямокутників та використання дифузії забезпечує задовільне шифрування початкового зображення.



а) б)

Рис.2.19. Результат перетворення Пекаря із використанням перетворення дифузії з розділенням початкового зображення на 4 прямокутники (а); – та на 50 прямокутників (б)

Порівняння швидкодії даного методу показало його ефективність у порівнянні із методом звичайного гамування, при цьому швидкодія методу приблизно на 15 відсоток вища, ніж у методі гамування, але при цьому зберігається якість шифрування (рис.2.9б).

2.5. Програмна реалізація шифрованого обміну текстовими повідомленнями із використанням алгоритму CRC-32

Псевдовипадкові числові послідовності відіграють важливу роль при побудові численних алгоритмів криптографічного та стеганографічного захисту телекомунікаційних систем та мереж. До таких алгоритмів відносять алгоритми взаємної ідентифікації, генерування сеансових ключів та ключів алгоритму RSA шифрування з відкритим ключем, тощо [180]. У таких алгоритмах ПВП відіграють роль ключів шифрування, що можуть бути використані у відомих стандартних алгоритмах. Відомо, що ключі до

стандартних алгоритмів шифрування мають характерні для криптографії довжини – 64, 128, 256, 512 та 1024 біти. У роботі досліджено властивості ПВП, що можуть бути використані у таких алгоритмах.

Проведені [24, 25, 30, 53] дослідження ПВП, генеровані системами з узагальненим відображенням Пекаря [26]:

$$x_n = -\frac{1}{\pi} \cdot \arccos\left(\cos 2^n \cdot \pi \cdot x_0\right) \quad (2.29)$$

та логістичним відображенням:

$$x_{n+1} = \lambda \cdot x_n \cdot \left(1 - x_n\right), \qquad (2.30)$$

де k, λ – параметри відображення, x_{n+1}, x_n, x_0 – наступне, поточне та початкове значення.

Слід очікувати, що послідовності генеровані системами з нелінійними функціями відображення володіють властивостями, що є відмінними від властивостей послідовностей генерованих за стандартом, що використовується для лінійних систем і приведений у [120].

Резонним є питання дослідження послідовностей генерованих системами з нелінійними функціями відображення на відповідність вимогам, що висуваються до послідовностей генерованих лінійними системами, а саме:

Збалансованість — різниця між кількістю бітів, що мають значення («0» і «1»).

Циклічність —кількості циклів з різними довжинами бітів. Під циклом розуміють неперервну послідовність однакових двійкових чисел. Виникнення іншої двійкової цифри автоматично розпочинає новий цикл. Довжина циклу дорівнює кількості цифр у такому циклі.

Кореляція – показник, що дорівнює нормованій на довжину послідовності різниці кількостей співпадань і неспівпадань у значеннях бітів для початкової та циклічно зсунутої на 1 біт.

Для генерування послідовностей та дослідження їх властивостей були розроблені відповідні програми у середовищі Microsoft Visual C++ 6.0. Генерування бінарних ПВП $B(x_0) = \{b_1, b_2, ..., b_n\}$ здійснювалося за правилом:

$$b_i = \begin{cases} 0, \text{ при } x_i \in X_0 \\ 1, \text{ при } x_i \in X_1 \end{cases} \qquad (2.31).$$

Множини X_0 і X_1 є неперервними відрізками числової вісі однакової довжини: $[0;1/2]$ та $[1/2;1]$ відповідно.

При дослідженнях початкові значення x_0 вибиралися на проміжку $(0;1)$ з кроком, рівним 0,1.

Генерування досліджуваних ПВП довжинами 64, 128, 256, 512, 1024 здійснювалося за схемою, приведеною на рис.2.20.

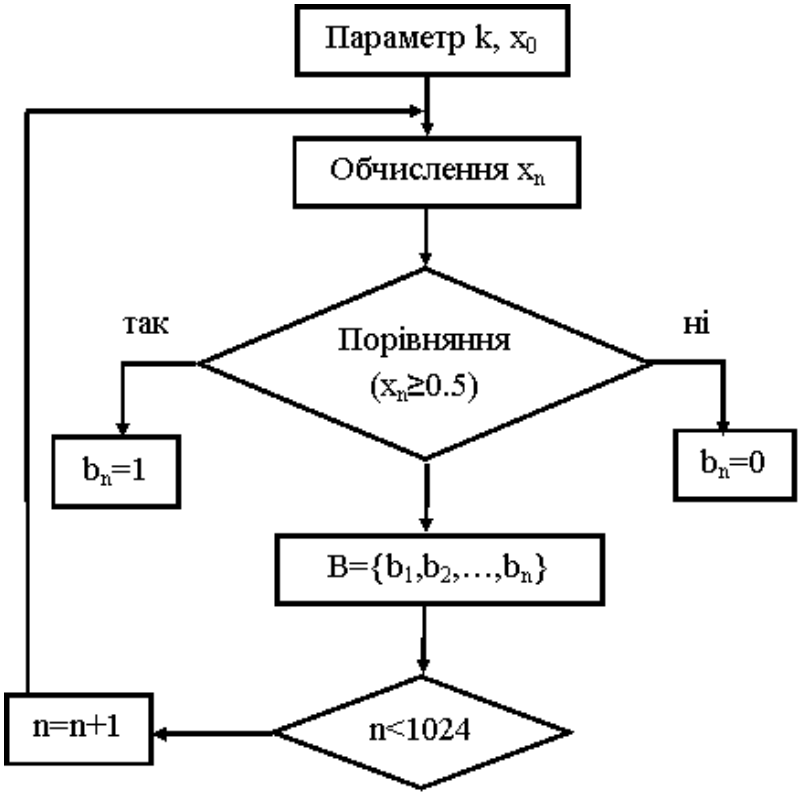


Рис. 2.20. Блок-схема генерування ПВП, де n – номер ітерації; k, x_0 параметри дискретного відображення та його початкове значення, x_n – значення дійсного числа, отриманого на черговому кроці ітерації, $B=\{b_1, b_2, \ldots, b_n\}$ – послідовність двійкових чисел

Оскільки обмеження по модулю для типу даних double в C++ дорівнює 10^{308}, то існує максимально можлива довжина послідовності n, що може бути генерована узагальненим відображенням Пекаря: $2^m = 10^{308}$, $n = 1024$ біт.

В таблиці 2.2 приведені значення параметра відображення Пекаря k, необхідні для генерування узагальнених послідовностей.

Таблиця 2.2.

Гранична довжина послідовності в залежності від параметру k

k	Довжина послідовності, n
64938	64
254	128
16	256
4	512
2	1024

На рисунку 2.21 приведена гістограма розподілу усереднених значень збалансованості послідовностей, генерованих за узагальненим відображенням Пекаря при початкових значеннях x_0 взятими з кроком 0,01 на відрізку (0;1).

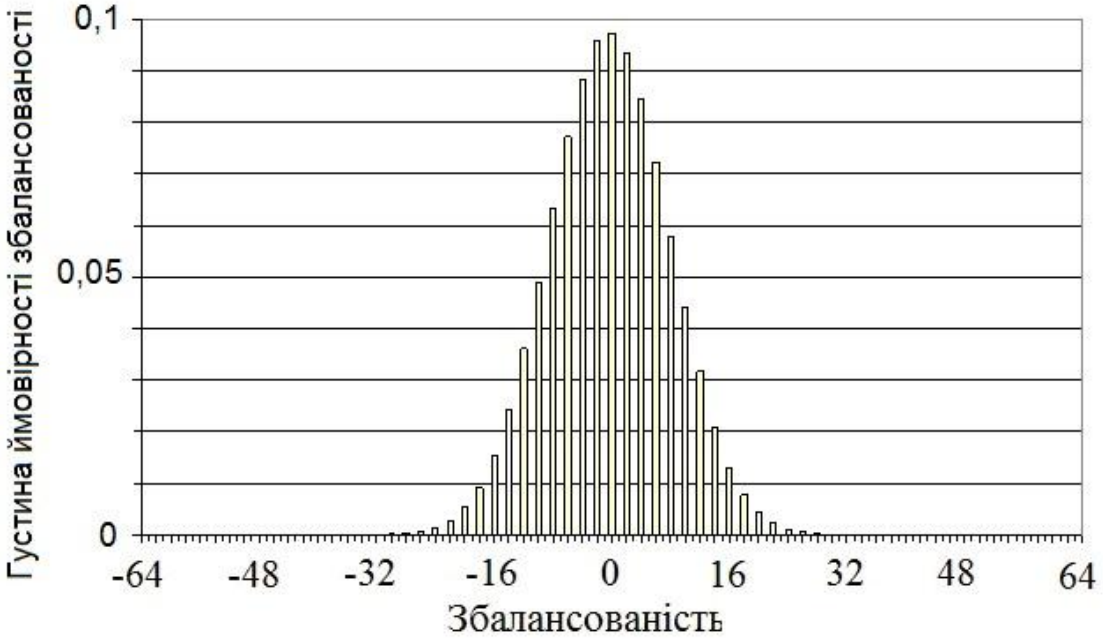


Рис.2.21. Усереднений по початкових значеннях x_0 розподіл густини ймовірностей значень збалансованості послідовностей.

Із отриманих результатів випливає, що значення збалансованості генерованих ПВП довжиною 1024 біти знаходяться в межах -30…+30, а їх розподіл є близьким до Гаусового із середнім значенням $M(L) \approx -0{,}6$ та дисперсією $\sigma_L^2 \approx 59{,}6$.

Дослідження циклічності послідовностей довжиною 64 біти проводились шляхом визначення кількості циклів довжиною 1, 2, 3, біт, 4-11 біт і більше 11 біт. В таблиці 2.3 приведені усереднені по початкових значеннях x_0 частки вкладів бітів циклів різної довжини у генеровану послідовність у порівнянні зі значеннями для ПВП, генерованих регістрами зсуву з оберненим лінійним зв'язком.

Таблиця 2.3

Циклічність послідовностей, генерованих на основі узагальненого відображення Пекаря.

Періодичні псевдовипадкові послідовності				
Довжина послідовності	64			
Довжина циклів, біт	1	2	3	≥ 4
Відносна кількість бітів бітів послідовностей у циклах	50	25	12,5	12,5
Кількість циклів	32	8	3	1
Абсолютна кількість бітів	32	16	9	7
Системи на основі дискретних відображень (ПВП генерована пороговим методом)				
Довжина послідовності	64			
Середнє значення і середньоквадратичне відхилення кількості циклів	16,79±4,49	7,31±2,51	3,86±1,77	3,82±1,48
Середнє значення і середньоквадратичне відхилення абсолютної кількості бітів послідовностей у циклах	16,79±4,49	14,63±5,04	11,59±5,31	18,98±8,46
Середнє значення і середньоквадратичне відхилення відносної частки бітів послідовностей у циклах	26,23±7,02	22,86±7,88	18,11±8,30	28,56±14,00

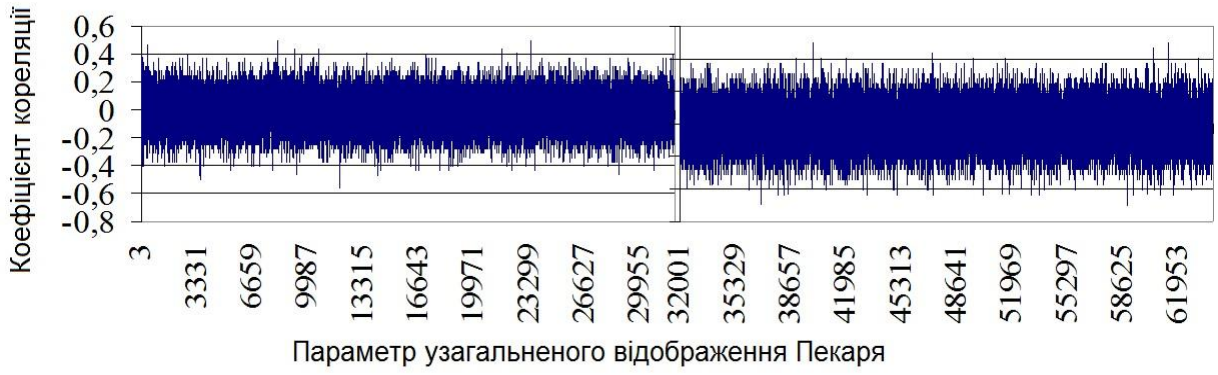
Із отриманих результатів можна зробити висновок про те, що значення циклічності значно відрізняються від стандартних значень [120] для циклів довжиною 1 та 4 бітів і більше. Частка бітів у циклах довжинами 1 та 4 біта і більше становить 26% та 29% відповідно. (для циклів зазначених довжин послідовностей генерованих регістром зсуву ця частка становить 12,5%).

Незначна кількість циклів довжиною більше 7 біт уможливлює використання послідовностей генерованих узагальненим відображенням Пекаря для генерування ключових послідовностей довжинами 64,128,256,512,1024 біти.

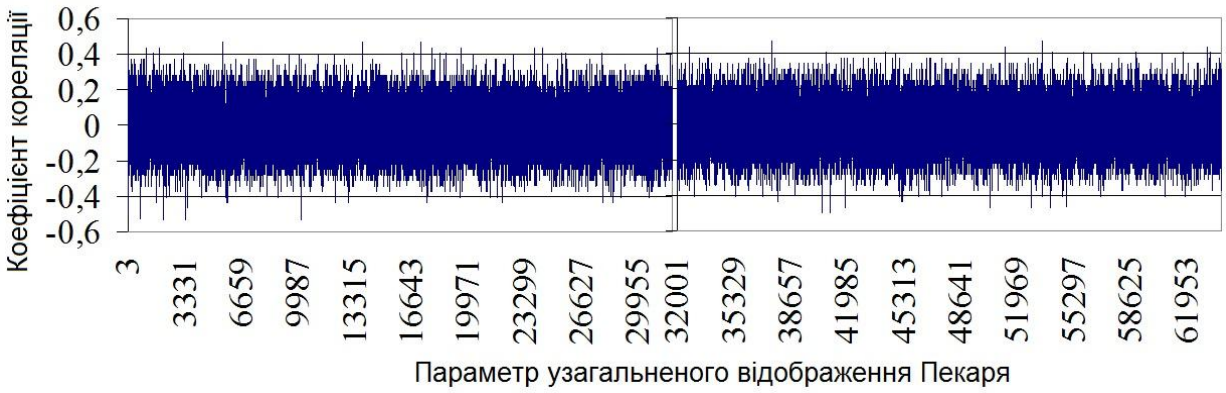
Визначення коефіцієнта кореляції для генерованих послідовностей проводилось порівнянням кожного біта генерованої послідовності з відповідним бітом послідовності, отриманої циклічним зсувом генерованої послідовності на 1 біт з подальшим обчисленням нормованої на довжину послідовності різниці між кількостями співпадань та неспівпадань значень бітів [120]:

$$k = \frac{Число_{співпадань} - Число_{розбіжностей}}{Довжина\_послідовності} \qquad (2.32)$$

Залежність коефіцієнта кореляції для ПВП, генерованих за узагальненим відображенням Пекаря від параметру k приведена на рис.2.20.



а)



б)

Рис.2.22. Залежність коефіцієнта кореляції послідовностей, генерованих за узагальненим відображенням Пекаря від значень параметра k: при x_0=0,3 (а) та при x_0=0,6 (б)

На рис.2.23 приведена гістограма усереднених на множинах $x_0 \in (0;1)$ та $k \in (2;64536)$ значень коефіцієнтів кореляції для ПВП генерованих за узагальненим відображенням Пекаря.

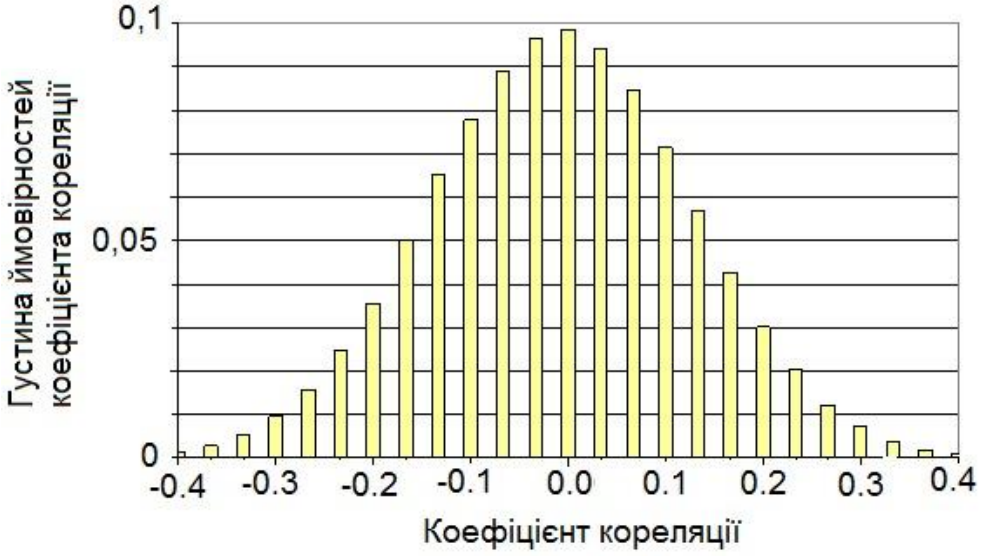


Рис. 2.23. Гістограма усереднених на множинах $x_0 \in (0;1)$ та $k \in (2;64536)$ значень коефіцієнтів кореляції ПВП, генерованих за узагальненим відображенням Пекаря

Із приведеної гістограми можна зробити висновок що розподіл густини ймовірностей значень коефіцієнта кореляції є близьким до розподілу Гауса із середнім значенням $M(k) \approx -0,01$ та дисперсією $\sigma_k^2 = 0.02$.

Дослідження періодичності послідовностей, що є фрагментами послідовності максимальної довжини (1024 біт) здійснювалося шляхом обчислення коефіцієнта кореляції послідовностями довжинами менше 512 біт та їх копіями, зміщеними на певну кількість біт. Значення коефіцієнта кореляції обчислювалося за виразом (2.32).

На рис.2.24 приведені залежності коефіцієнта кореляції від зміщення між послідовностями при різних початкових значеннях.

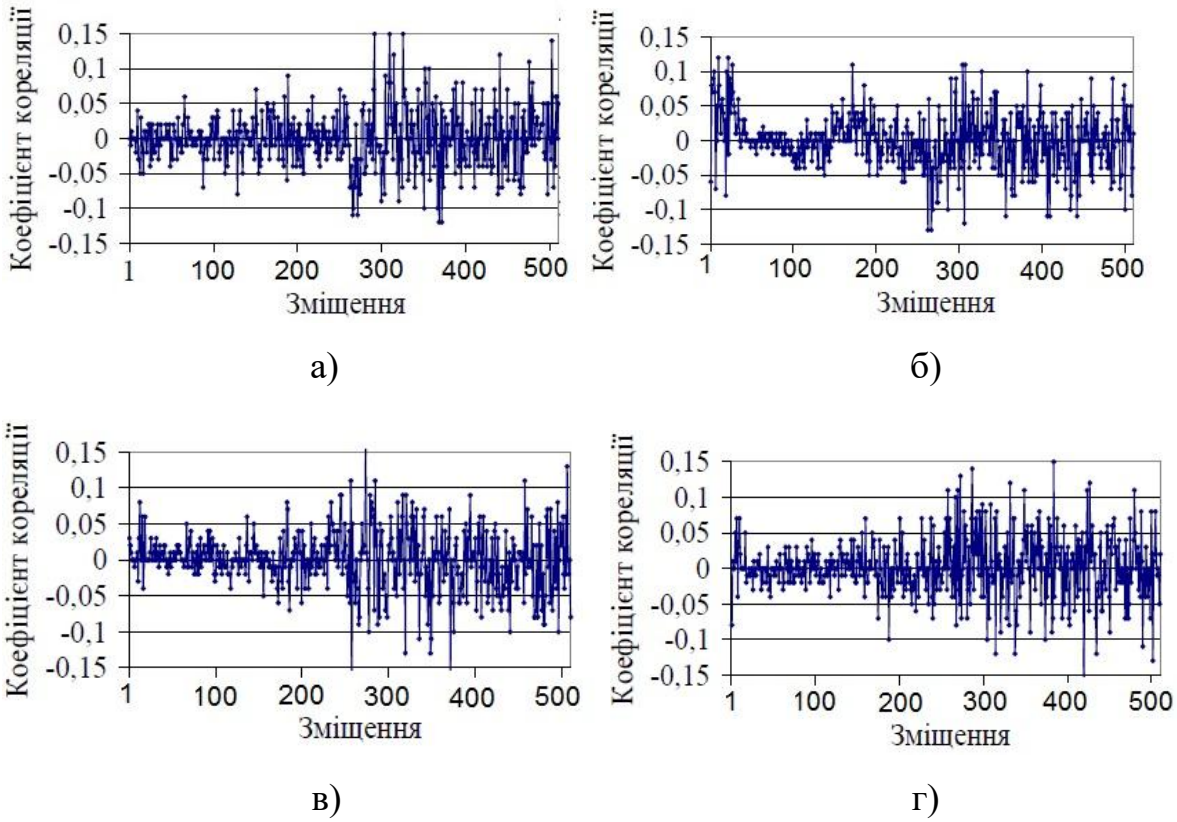


Рис. 2.24. Залежність коефіцієнта кореляції від зміщення між послідовностями для різних початкових значень динамічної змінної логістичного відображення при $x_0 = 0,05$ (а); при $x_0 = 0,25$ (б); при $x_0 = 0,56$ (в) та при $x_0 = 0,87$ (г)

Для послідовності фіксованої довжини обчислювали значення коефіцієнтів кореляції між усіма можливими послідовностями заданої довжини, зміщеними на певну кількість бітів з наступним їх усередненням. Таким чином були отримані залежності коефіцієнта кореляції для послідовностей довжинами 64, 128, 256, 512 та 1024 біти, що є характерними для криптографічних ключів.

Встановлено, що для послідовностей довжиною меншою 512 біт значення коефіцієнта кореляції знаходиться в межах $-0{,}15...0{,}15$.

На рис. 2.25 приведено усереднена на множині можливих значень початкового елементу $x_0 \in [0;1]$ із кроком 0,01 гістограма розподілу значень коефіцієнта кореляції бінарних ПВП, формованих за хаотичними коливаннями, генерованими узагальненим відображенням Пекаря.

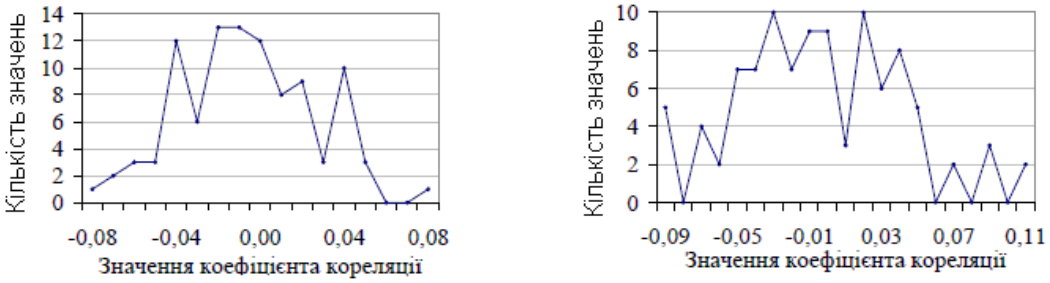


Рис.2.25. Гістограма розподілу значень коефіцієнту кореляції ПВП з довжинами 1024 біти (а) та 512 біт (б)

У межах точності чисельного моделювання можна зробити висновок, що ПВПє чутливими до початкових значень динамічної змінної (рис.2.26, 2.27).

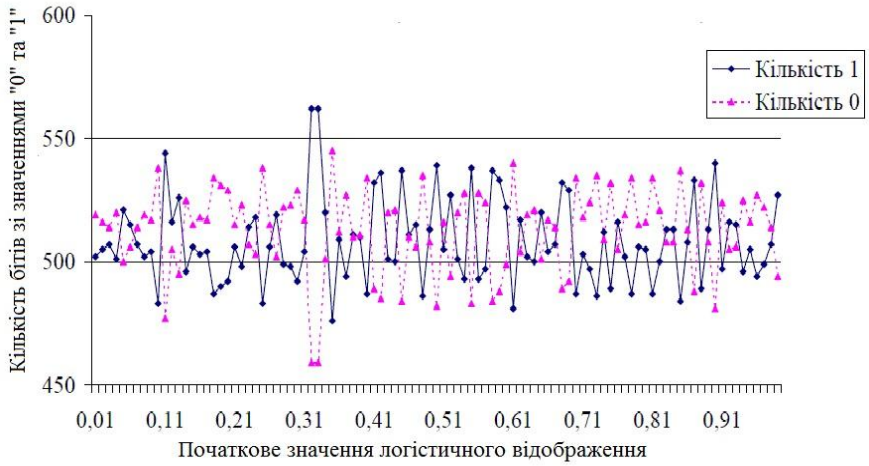


Рис. 2.26. Залежність кількості бітів «1» та «0» у послідовності довжиною 1024 біт від початкового значення динамічної змінної логістичного відображення

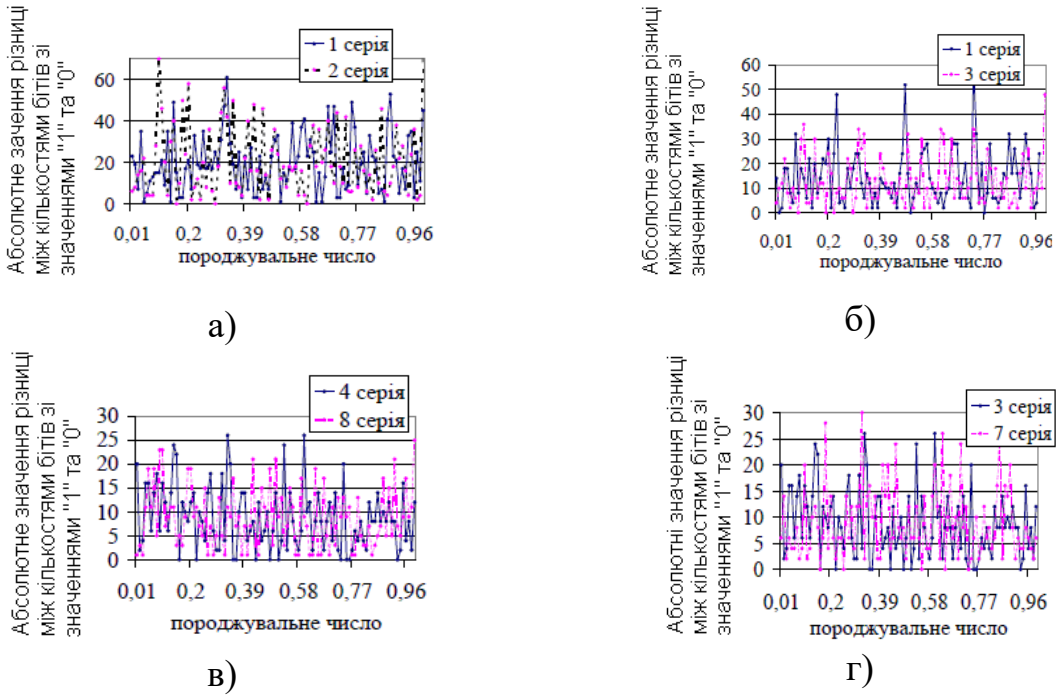


Рис. 2.27. Залежність абсолютних значень збалансованості довільно розташованих фрагментів довжиною 512 біт (а), 256 біт (б), 128 біт (в) та 64 біт (г) у послідовності довжиною 1024 біти

В таблиці 2.4 приведені отримані шляхом чисельного експерименту агреговані дані збалансованості послідовностей довжинами кратними 64 бітам

Таблиця 2.4.

Середнє значення збалансованості послідовностей довжинами кратними 64

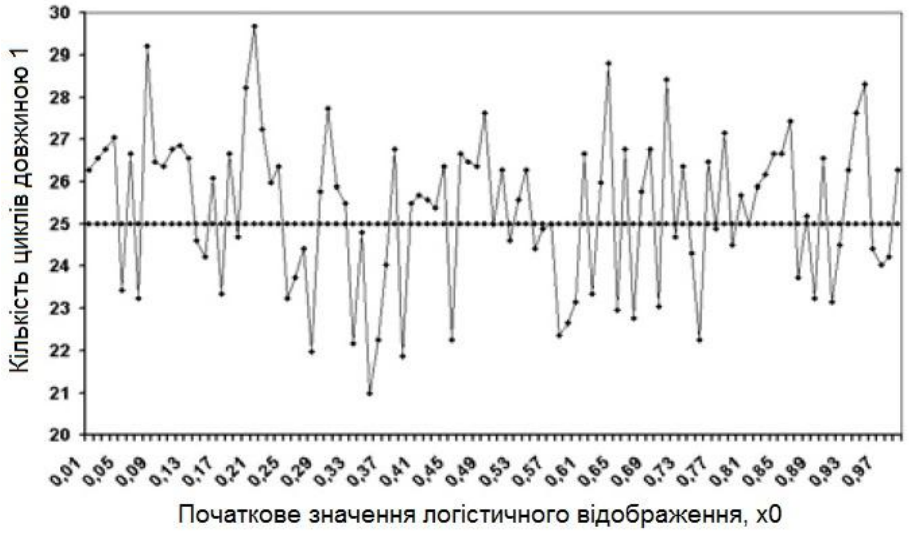
Довжина послідовності	**64**	**128**	**256**	**512**	**1024**
Середнє значення збалансованості	6	10	15	20	27
Середнє значення збалансованості, нормоване на довжину послідовності	0,094	0,078	0,059	0,039	0,026

Із отриманих результатів випливає, що кількість незбалансованих бітів у послідовності, генерованою за логістичним відображенням довжиною 1024 та її фрагментах довжинами кратними 64 збільшується, а їх частка у фрагментах зменшується.

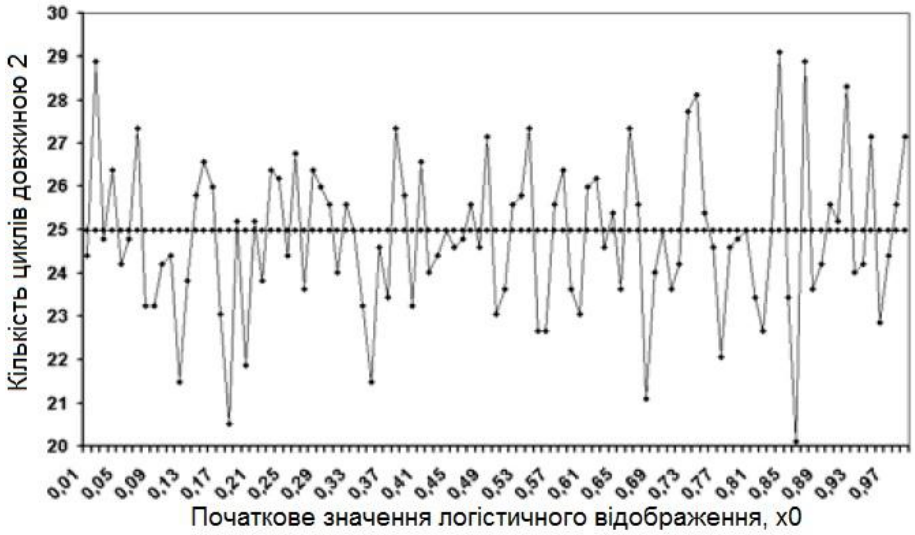
Із отриманих залежностей випливає, що збалансованість фрагментів послідовностей, генерованих логістичним відображенням значно перевищує 1, причому вона не залежить від їх розташування у послідовності з максимальною довжиною 1024 біти.

Значення циклічності послідовностей генерованих за логістичним відображенням, значно відрізняються від значень, що вважаються стандартом для лінійних систем (утворюють геометричну прогресію: 50 % бітів у циклах довжиною 1 біт, 25 відсотків у циклах довжиною 2 біти, 12.5 % у циклах довжиною 3 біти, 6.25 % у циклах довжиною 4 біти і т.д.). Було встановлено, що циклічність досліджуваних фрагментів не залежить від їх довжини і становить 50% для циклів довжинами 1 і 2 біт, 20 відсотків для циклів довжинами 3 біти і 30 відсотків для циклів довжиною 4 і більше біт. Слід зауважити, що із зменшенням довжини послідовності значно зростає статистична недостовірність, тому найменша довжина досліджуваної послідовності становила 64 біти.

Аналіз залежностей циклічності послідовностей довжиною 1024 біти від початкових значень динамічної змінної в інтервалі $(0;1)$ вказав на значне відхилення циклічності для конкретних значень початкового числа від усередненого по всій множині значення. При цьому відсутня певна закономірність залежності циклічності від значення породжувального числа (рис.2.28.)

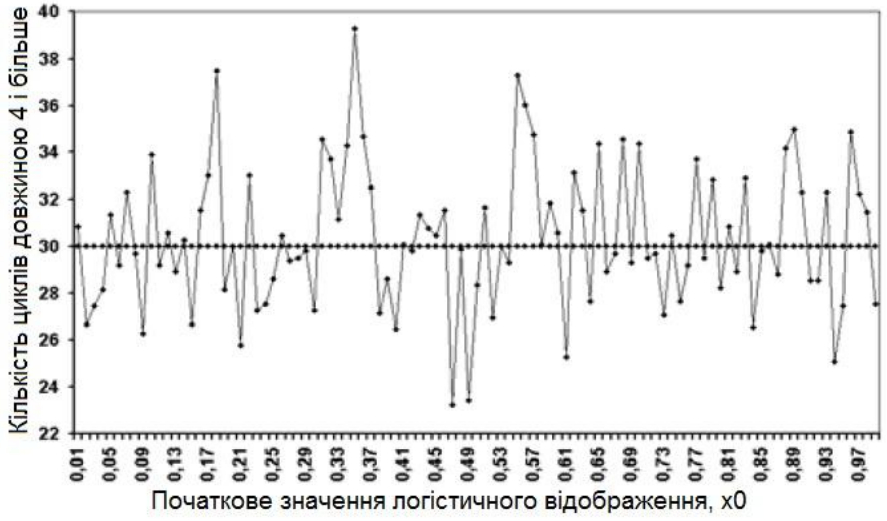


а)



б)

в)



г)

Рис. 2.28. Залежність кількості циклів довжинами 1 (а), 2 (б), 3 (в) та 4 і більше (в) для послідовності довжиною 1024 біт

Сумарна кількість бітів, що містяться у циклах одиничної довжини для послідовностей генерованих нелінійними схемами, значно відрізняється від типових значень. У генерованих послідовностях середня кількість бітів у циклах довжинами 1, 2, 3 та чотири і більше біт становить 25%, 20%, 30% відповідно (типові значення для послідовностей генерованих лінійними схемами становлять 50%, 12,5% та 12,5% відповідно).

Середні значення відносної кількості бітів у циклах різної довжини приведені в таблиці 2.5.

Таблиця 2.5.

Відносна кількість бітів у циклах різної довжини для послідовності довжиною 1024 біт

Довжина циклу / **Показники циклів**	**1**	**2**	**3**	**4,5,…,11**
Середнє значення частки бітів у циклах послідовності генерованої логістичним відображенням	25	25	20	39
Дисперсія відносної кількості бітів у циклах	3	3	5	9
Значення частки бітів у циклах послідовностей генерованих зсувовим регістром з лінійним оберненим зв’язком	50	25	12.5	12.5

Дослідження циклічності фрагментів послідовності довжинами в 512, 256, 128 та 64 біти показали, що частка бітів у циклах різних довжин не залежить від місця знаходження фрагментів у послідовності (початок, середина чи кінець послідовності). При цьому відносне значення кількості бітів у циклах довжинами 4 і більше біт становить більше 30 відсотків, як і для послідовності максимальної довжини 1024 біт.

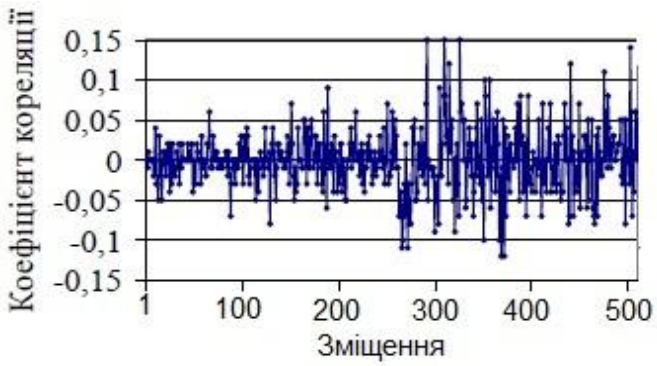


Рис.2.29. Залежність коефіцієнта кореляції від зміщення послідовності для початкового значення динамічної змінної $x_0 = 0.05$

На рис. 2.29 приведена залежність значення коефіцієнта кореляції від зміщення ПВП для фіксованого початкового значення динамічної змінної логістичного відображення $x_0 = 0.05$.

Значення коефіцієнта кореляції зміщених послідовностей, генерованих за логістичним відображенням, є на порядок більшими від мінімально можливого значення (1/500≈0,002), що вказує на їх слабку корельованість.

На рис.2.30 приведена залежність кількості значень коефіцієнта кореляції на множині (0;1) від значень початкового елемента логістичного відображення.

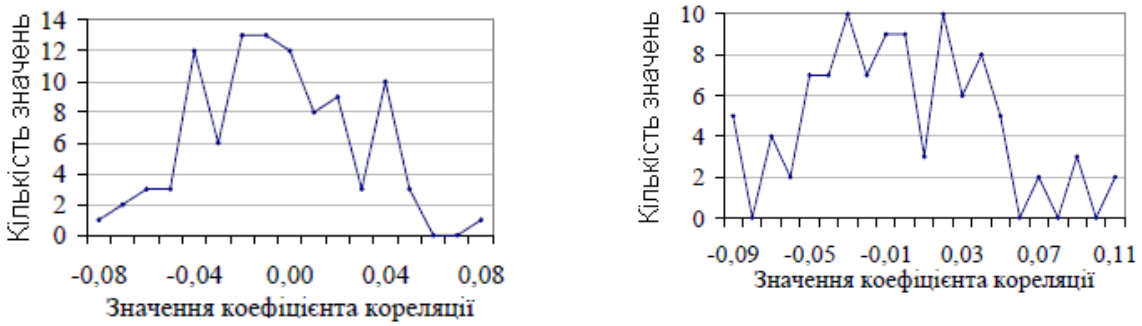


Рис.2.30. Розподіл значень коефіцієнта кореляції послідовністей довжиною 1024 біти (а) та 512 біт (б)

Послідовності, що генеровані за допомогою логістичного відображення є не періодичними. Для довжин менших 512 біт значення

коефіцієнту кореляції становили −0,15 до +0,15, а для довжин 512 і 1024 – 0,01…0,01.

Забезпечення конфіденційності передавання інформації у багатокористувальницьких системах є головною тенденцією у розвитку телекомунікаційних СПІ. Розроблена нами [8] багатокористувальницька СПІ використовує алгоритм блокового шифрування за допомогою операції XOR. Процес генерування ключа шифрування здійснювався з використанням логістичного відображення (2.37).

Величиною кроку дискретизації початкового значення визначається потужність простору ключів системи, що уможливлює ефективне розділення інформаційних потоків, призначених різним користувачам.

Крок дискретизації значень відображення x_n, x_{n+1} та параметру керування λ становив 5 десяткових знаків після коми.

Адресація даних здійснюється засобом TCP / IP протоколювання із використанням записаних на серверній частині програмного забезпечення статичних IP-адрес. Ключі та повідомлення, що передаються, зберігаються на клієнтській та серверній частинах програмного забезпечення. Визначення клієнта здійснюється шляхом обчислення та перевірки контрольних сум, що розраховані за алгоритмом CRC-32 стандартизованим у IEEE 802.3 [192], для початкового значення динамічної змінної та кількості кроків ітерації логістичного відображення. Процес розпізнавання даних клієнта можна вважати синхронізацією за її визначенням, оскільки при цьому має місце узгодження числових значень ключів логістичного відображення (рис. 2.31).

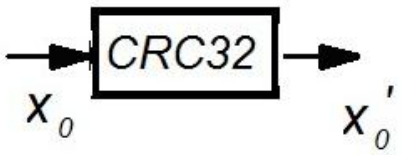


Рис.2.31. Початок процесу синхронізації (x_0 – початкове значення динамічної змінної, x_0' – контрольна сума, що розрахована за алгоритмом CRC-32)

Контрольна сума, що розрахована за початковим значенням динамічної змінної (x0) та кількістю ітерацій (n) періодично передається по відкритому каналу та порівнюється зі значенням, що зберігається на серверній частині, за схемою приведеною на рис.2.31. Період синхронізації визначається лічильником зовнішнього циклу, що контролює задану кількість ітерацій (n). У внутрішньому циклі відбувається генерування динамічної змінної логістичного відображення, що використовується для шифрування двійкового інформаційного потоку за дією XOR (рис.2.32).

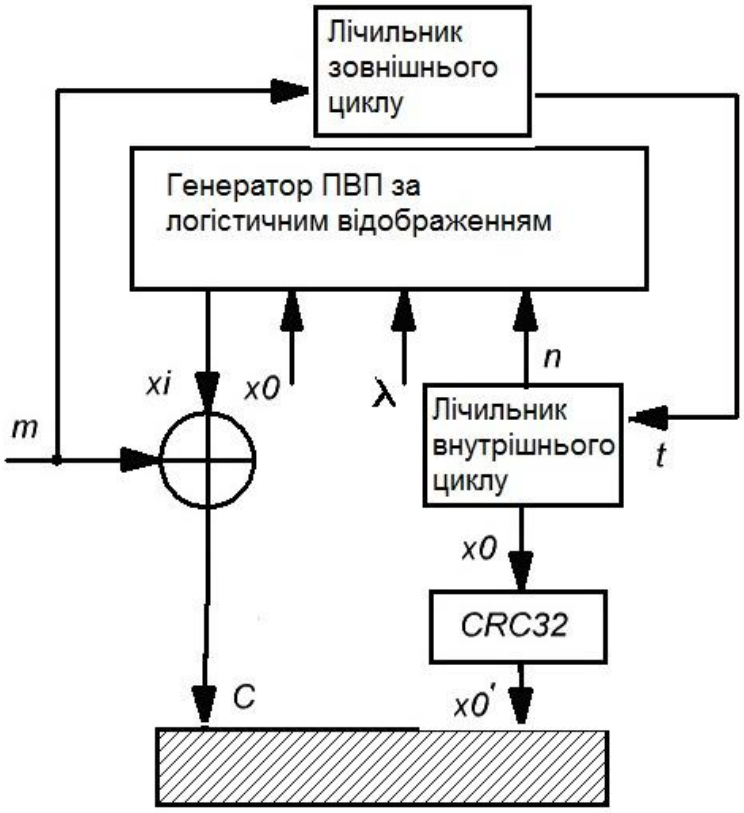


Рис. 2.32. Блокове шифрування та синхронізація (m – інформаційне повідомлення у двійковому форматі, x0, λ – початкове значення та параметр логістичного відображення, n – задана кількість ітерацій, xi – чергове значення логістичного відображення, що використовується у процесі потокового шифрування двійкового інформаційного повідомлення, C – зашифроване повідомлення, x0' – змінене за алгоритмом CRC-32 початкове значення логістичного відображення, t – період синхронізації)

Початок та завершення інформаційного обміну у СПІ визначається шляхом закриття та відкриття сесій з'єднання між серверною та клієнтською частинами. Набір команд, що реалізує передавання інформаційних повідомлень у захищеному режимі приведений у таблиці 2.6.

Таблиця 2.6

Команди, що супроводжують процес передавання інформації

№	Команда	Зміст команди
1	GET (опція) ADR (значення) LGN (логін)	Розпочинається сеанс з'єднання між клієнтським та серверним програмним забезпеченням. У тому випадку якщо ще не завершений попередній сеанс зв'язку, серверне програмне забезпечення розпочинає новий сеанс. Передавання інформації розпочинає тільки клієнтське програмне забезпечення. (опція) – значення контрольної суми, що розраховано за початковим значенням динамічної змінної x_n; ADR – команда, що передає IP-адресу; (value) – значення IP-адреси відправника повідомлення; LGN – команда, що передає назву адресата; (login) – назва адресата.
2	GETOUT	Відправка інформації клієнтській частині
3	GETIN	Відправка інформації серверній частині.
4	LGNX (логін)	Назва одержувача інформації (логін). Повідомлення без такої команди записується у загальний масив повідомлень.
5	ER1	Перевірка помилок, що виникли внаслідок дії команди GET із заданими параметрами. Сервер зупиняє сеанс зв'язку.
6	ER2	Помилка синхронізації. Неправильне значення контрольної суми. Обидві частини програмного забезпечення (клієнтська та серверна) повертаються до попереднього кроку ітерації.
7	ER3	Помилка виникає внаслідок неправильного розпізнавання назви одержувача. Сервер припиняє сеанс зв'язку.
8	ER4	Назва відправника повідомлення не може бути визначена серед тих, що записані у програмному забезпеченні одержувача повідомлення.
9	MSG (повідомлення)	Початок передавання повідомлення.

Продовження таблиці 2.6

10	CLR	Завершення сеансу передавання повідомлення (клієнтським програмним забезпеченням).
11	CLS	Завершення сеансу передавання (програмним забезпеченням одержувача повідомлення).
12	CS	Знаходження контрольної суми.

Алгоритм передавання та синхронізації передавальної сторони і одержувачів полягає в наступному:

– системний адміністратор визначає значення параметру керування λ та початкове значення x_0 динамічної змінної і присвоює їх кожному користувачеві як для клієнтського так і серверного програмного забезпечення;

– клієнтське програмне забезпечення розпочинає сеанс зв’язку за допомогою команди № 1;

– серверне програмне забезпечення здійснює відгук, використовуючи команди за номерами № 2, № 9, № 12 та № 4;

– клієнтське програмне забезпечення передає інформаційне повідомлення за допомогою команд № 3, № 9, № 12 та № 4. У випадку виникнення помилки серверне програмне забезпечення передає команди № 5 – № 8 замість команди № 9;

– сеанс зв’язку завершується однією з команд (№ 10 або № 11).

Розроблена система дає можливість під’єднувати до 20 користувачів. Кількість користувачів залежить від точності представлення параметрів системи шифрування (у розглядуваній системі використовувалось представлення дійсного числа з точністю 5 десяткових знаків). Підвищення точності представлення параметрів системи шифрування інформації уможливлює під’єднання більшої кількості користувачів, але при цьому зменшується швидкодія системи.

Задовільна для реального використання багатокористувальницька система у телекомунікаційних мережах передавання інформації може бути

реалізована відповідною структурою та моделлю даних. Структура моделі даних приведена на рис.2.31, а числові параметри інформаційного масиву, що мають відповідні поля у таблиці бази даних (табл. 2.7). Інформація зберігається у символьному масиві, що має стандарт кодування UTF-8 і використовує спеціальний символ розмітки масиву на блоки, внаслідок чого існує можливість конвертації даних у CSV-файл та обмін інформацією з іншим програмним забезпеченням.

У системі передавання передбачена можливість використання журналу фіксації редагування, збереження та зчитування інформації (рис.2.33 та таблиця 2.7) користувачами телекомунікаційної системи.

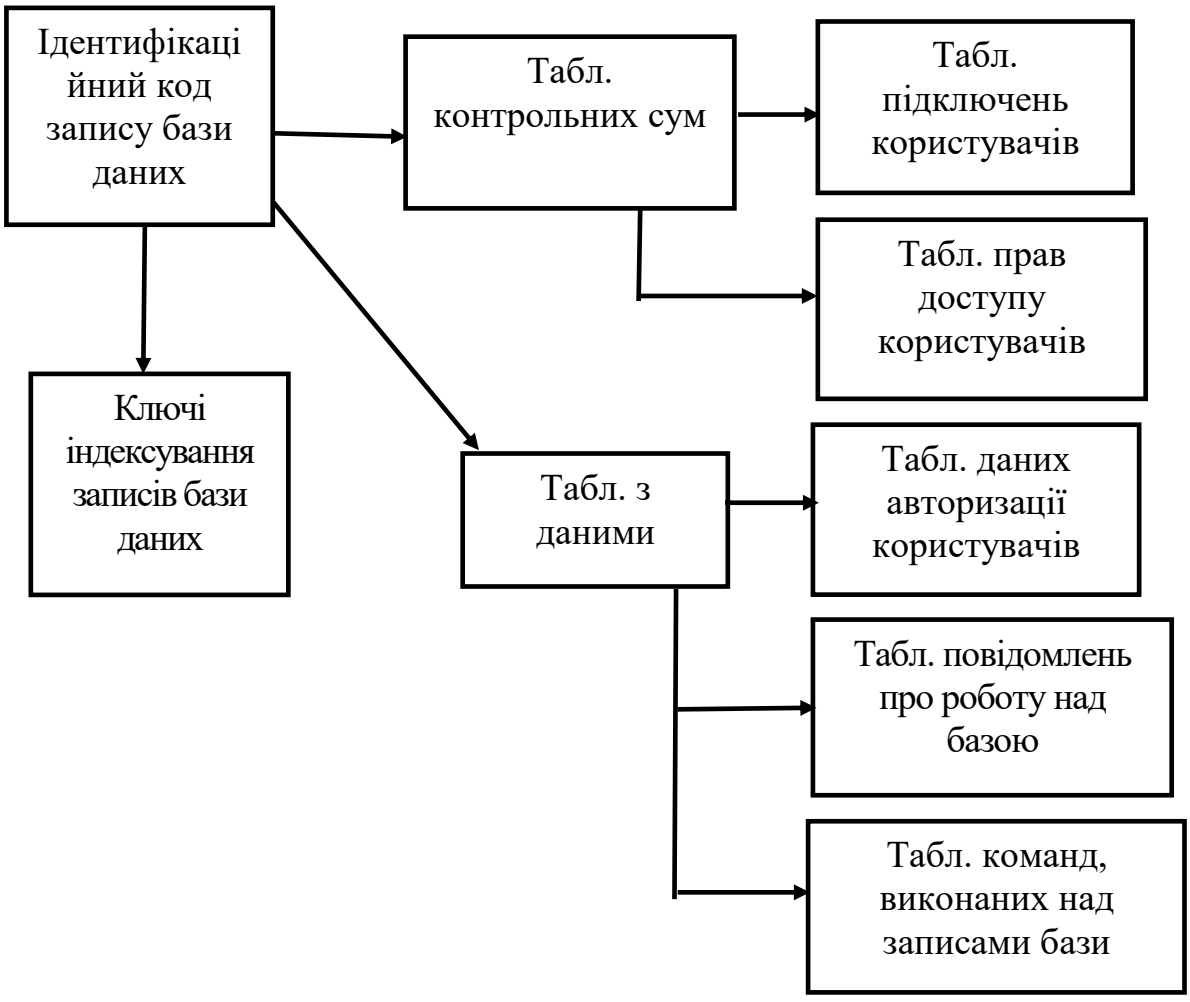


Рис.2.33. Структура моделі даних багатокористувацької системи передавання даних

Таблиця 2.7

Параметри моделі даних (відповідають полям таблиці бази даних)

Поле таблиці	**Зміст поля**
MSG	Відмітка про запис повідомлення
KRCS	Відмітка про журналювання дій над записами бази даних
LGN	Відмітка про журналювання підключених користувачів
DT	Відмітка про записування інформації у базу даних
NODE(x) x = (A , B , C , D)	Відмітка про журналювання прав користувачів (A – дозвіл на всі дії над записами бази даних, B – дозвіл лише на читання, C – дозвіл лише на оновлення, D-немає дозволу на роботу із записами бази даних)
;	Символ розділення записів інформаційного масиву бази даних
INFK	Короткий зміст запису у таблиці бази даних

2.6. Шифрування аналогового звукового сигналу біполярними ПВП формованими за логістичним відображенням

Для шифрування мовної інформації використовують методи цифрового скремблювання [195], додавання за модулем 2 (потокове шифрування) та стандартні методи шифрування (RSA, AES, DES).

Алгоритм RSA є криптосистемою з відкритим ключем шифрування, що є парою чисел e_A, n_A, відомих усім іншим користувачам та закритий ключ d_A, що є відомим лише користувачеві A. Тоді пара операцій шифрування/дешифрування може бути описана наступним виразом [196]:

$$c = m^{e_A} \bmod\left(\varphi\left(n_A\right)\right) \Rightarrow m = c^{d_A} \bmod\left(\varphi\left(n_A\right)\right), \quad (2.33)$$

де m – початкове повідомлення, c – зашифроване повідомлення, $\varphi\left(n_A\right) = n_A \cdot \prod_{i=1}^{k}\left(p_i - 1\right)$ – функція Ейлера числа n_A, p_i – прості числа, що

менші за число n_A, k – кількість таких чисел.

Шифр DES (1979) на даний час не використовується, внаслідок недостаньої потужності. Використовуваний розмір блоку становить 64 біти.

Шифр AES – це блоковий ітеративний шифр, що шифрує дані блоками, фіксованого на час виконання розміру, в 128, 192 і 256 бітів, тобто можливі довжини ключів становлять 128, 192 і 256 біт відповідно. При цьому перед початком шифрування текстове повідомлення потрібно перетворити у число, що є достатньо великим за модулем.

Найбільш ефективним із вказаних методів є побітове додавання за модулем 2 (вхідна послідовність оцифрованого звукового сигналу сумується за модулем 2 із деякою ключовою послідовністю. Розроблена [4] система передавання звукової інформації з її шифруванням бінарними послідовностями, формованими на основі ХК, генерованих логістичним відображенням (2.35). Для генерування бінарної випадкової послідовності використовується одномірне дискретне відображення (2.35), при цьому параметр керування може приймати значення в діапазоні $3{,}65\cdots3{,}95$.

Блок-схема СПІ, а також кодера і декодера системи приведені на рис. 2.34 та рис. 2.35.

Аналоговий аудіосигнал, що надходить від джерела інформації, подається на вхід аналого-цифрового перетворювача (АЦП), в якості якого слугує звукова карта персонального комп'ютера. Дискретне логістичне відображення генерує псевдовпадкові числа, на базі яких формується бінарна послідовність кодування у 8-бітовому представленні:

$$z_n = 0.b_{n1}b_{n2}\ldots b_{n8} = 2^{-1}\cdot b_{n1} + 2^{-2}\cdot b_{n2} + \ldots + 2^{-8}\cdot b_{n8} \quad (2.34)$$

Відліки оцифрованого аудіосигналу m_i сумуються за модулем 2 (операція XOR) із елементами бінарної послідовності кодування:

$$s_i = m_i \oplus z_i \quad (2.35)$$

Процес дешифрування здійснюється шляхом додавання за модулем 2 (XOR) бітів прийнятої послідовності з бітами ПВП, генерованої приймальною стороною системи. Синхронізація приймальної та передавальної сторін забезпечуються шляхом періодичного передавання поточних значень динамічної змінної системи з дискретною функцією відображення, що генерується передавальною стороною системи.

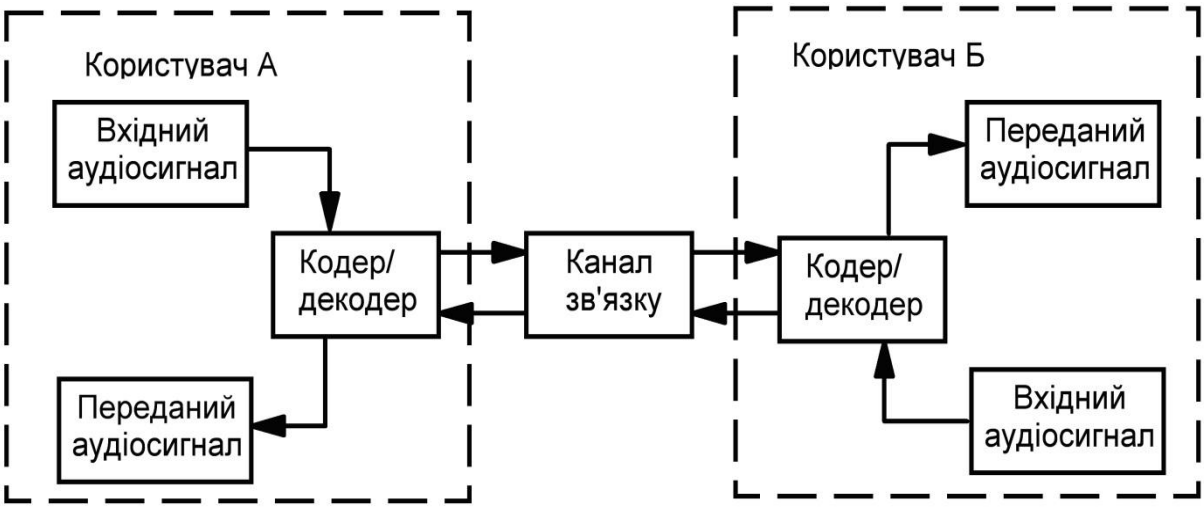
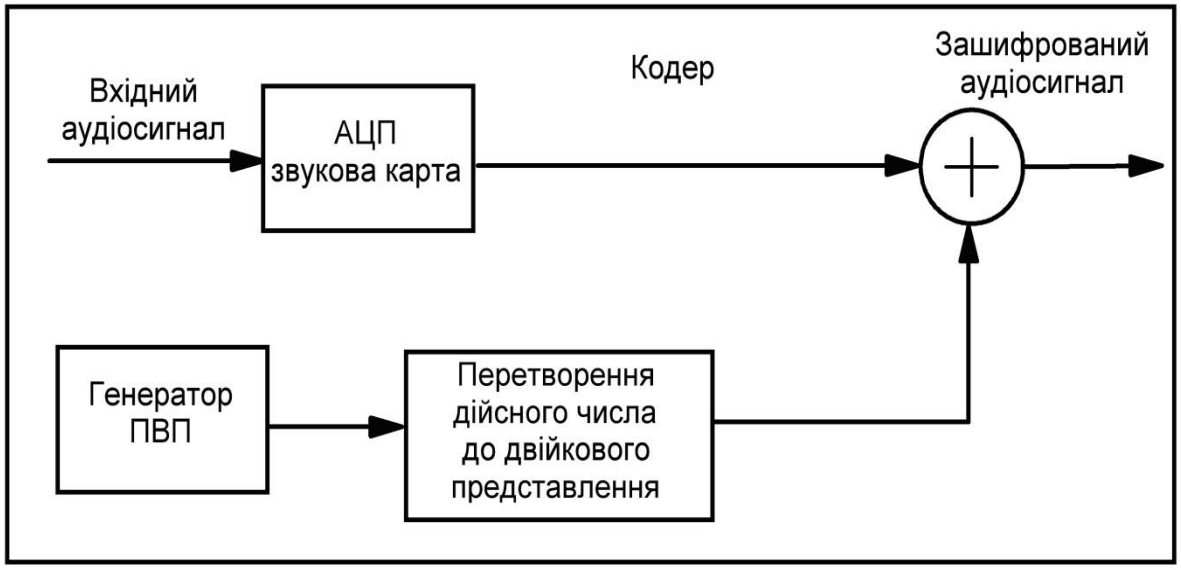
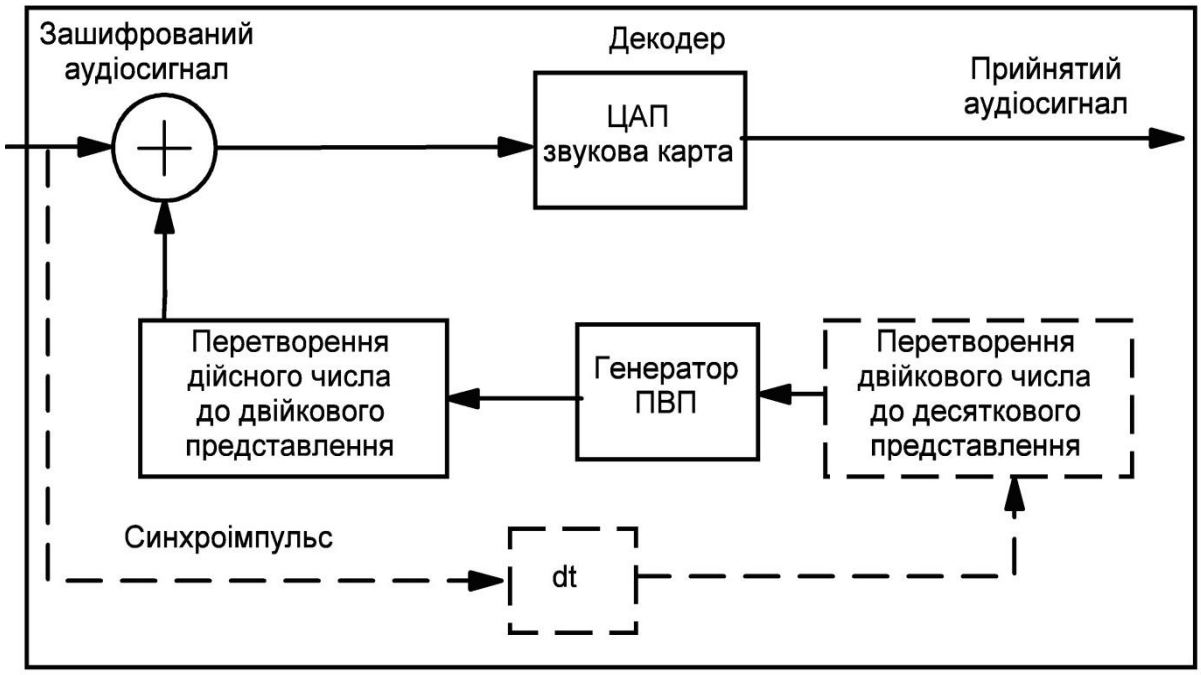


Рис.2.34. Блок-схема системи передавання аудіо-сигналу зашифрованого бінарною послідовністю формованої на основі хаотичних коливань



а)



б)

Рис.2.35. Кодер (а) та декодер (б) системи передавання аудіо-сигналу, dt – період дискретизації

Розшифрований цифровий сигнал подається на ЦАП, в якості якого може слугувати звукова карта персонального комп'ютера, в результаті чого отримується аудіо-сигнал.

У сучасних комп'ютерних системах передбачена можливість роботи із аудіо-сигналом за допомогою стандартної звукової карти. Дискретизація, перетворення та відтворення аудіосигналу у персональному комп'ютері здійснюється за допомогою спеціально розробленої програми, що використовує функції API для операційної системи Windows. Це забезпечується використанням сучасних середовищ розроблення програм на мовах C++ Builder, Visual C++, Delphi та інших.

Розглядувана система апробована нами [4] у програмному середовищі Delphi 7.0. Запропонована система забезпечує передавання інформації у режимі реального часу з використанням апаратних засобів доступу до мережі Internet. Для ідентифікування користувача системи достатньо знати лише його IP адресу. Розроблена програма забезпечує

оцифровування сигналу, що надходить з мікрофона на вхід вбудованої звукової карти комп'ютера із стандартною частотою дискретизації 44100 Гц; шифрування/дешифровування аудіосигналу у режимі реального часу та вибір необхідних початкових умов генерування ПВП.

Головні вікна програми приведені у Додатку А.

2.7. Пристрій шифрування мовного сигналу на основі ПВП

В даному пункті описана запропонована нами апаратна реалізація пристрою шифрування мовної інформації, що використовує генеровані за логістичним відображенням бінарні ПВП. При передаванні мовного сигналу в on-line режимі найкращим методом з точки зору швидкості та складності обчислень є так зване потокове шифрування бітами ПВП, зміст якого – у побітовому додаванні по модулю 2 (XOR) бітів інформаційної послідовності.

Практична реалізація пристроїв шифрування мовної інформації може бути здійснена з використанням сучасних цифрових технологій (мікроконтролерів, ПЛІС і т.д.). Нами [5] розроблена програмно-апаратна реалізація пристрою шифрування аудіоінформації на базі мікроконтролера PIC 18F2550. На рис.2.36, 2.37 приведені структурна та електрична принципова схеми пристрою шифрування аудіосигналу відповідно.

Цифрове оброблення мовної інформації здійснює мікроконтролер (рис.2.37), що може функціонувати в режимах генерування хаотичних сигналів (генератор шуму) та шифрування/дешифрування. Аналоговий мовний сигнал перетворюється у цифровий вбудованим 10-розрядним АЦП мікроконтролера з частотою дискретизації 8 КГц.

Шифрування оцифрованих сигналів здійснюється псевдовипадковими послідовностями, генерованими на основі одномірного дискретного логістичного відображення [5].

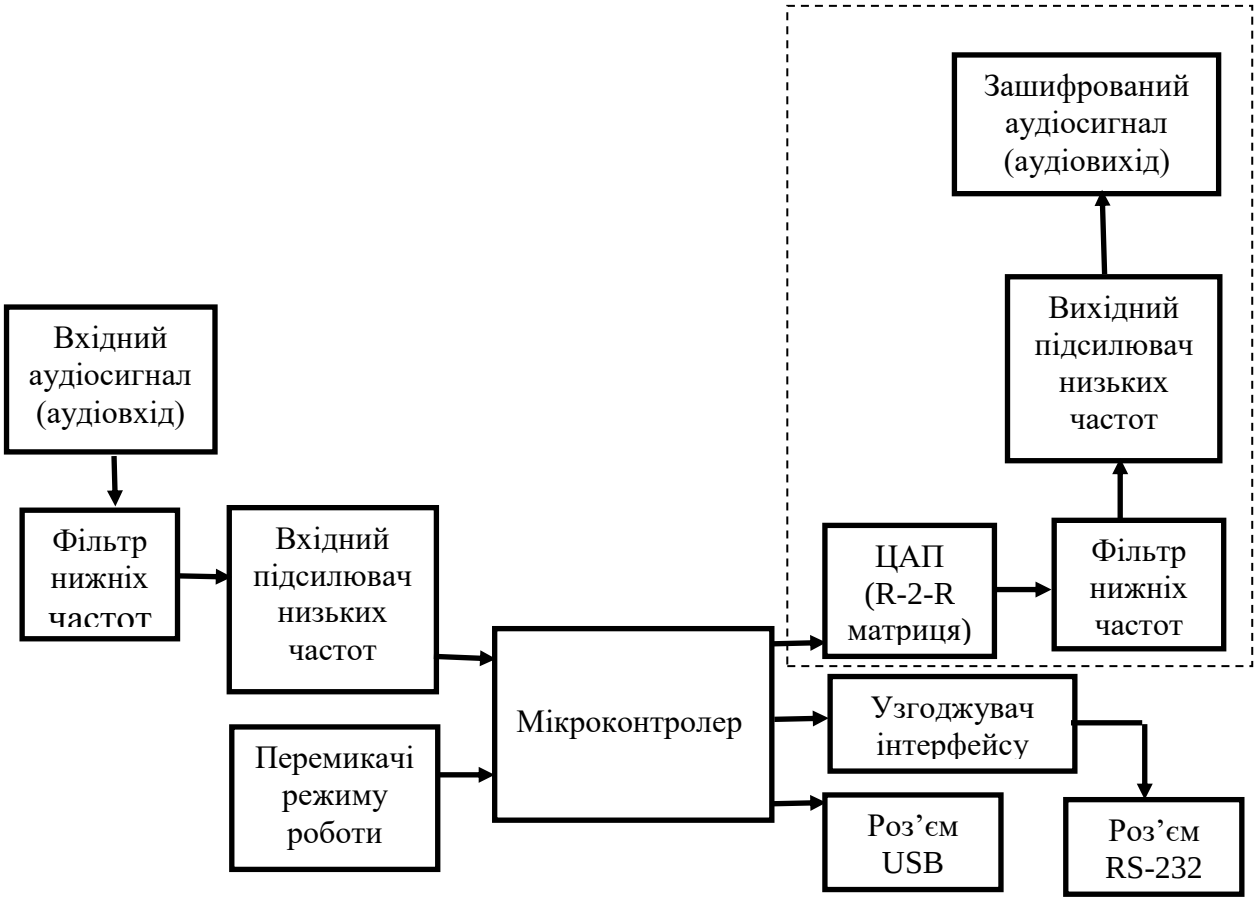


Рис.2.36. Функціональна схема пристрою шифрування мовної інформації

Біти цифрового мовного сигналу m_i додаються за модулем 2 з цифровим шифруючим сигналом z_i, формуючи зашифрований сигнал s_i:

$$s_i = m_i \oplus z_i \qquad (2.36)$$

Крипостійкість пристрою визначається точністю подання n параметру керування λ та початкового значення x_0 логістичного відображення, що представлені десятковими числами, обсяг простору ключів дорівнює:

$$N = \left(10^n\right)^2 \quad (2.37)$$

Значення параметру керування та початкового елемента логістичного відображення встановлюються в якості параметру програми, реалізованої на мові С за алгоритмом приведеним на рис.2.38.

Зв'язок контролера з комп'ютером здійснюється через порт USART та інтерфейси USB та COM (мікросхема MAX232).

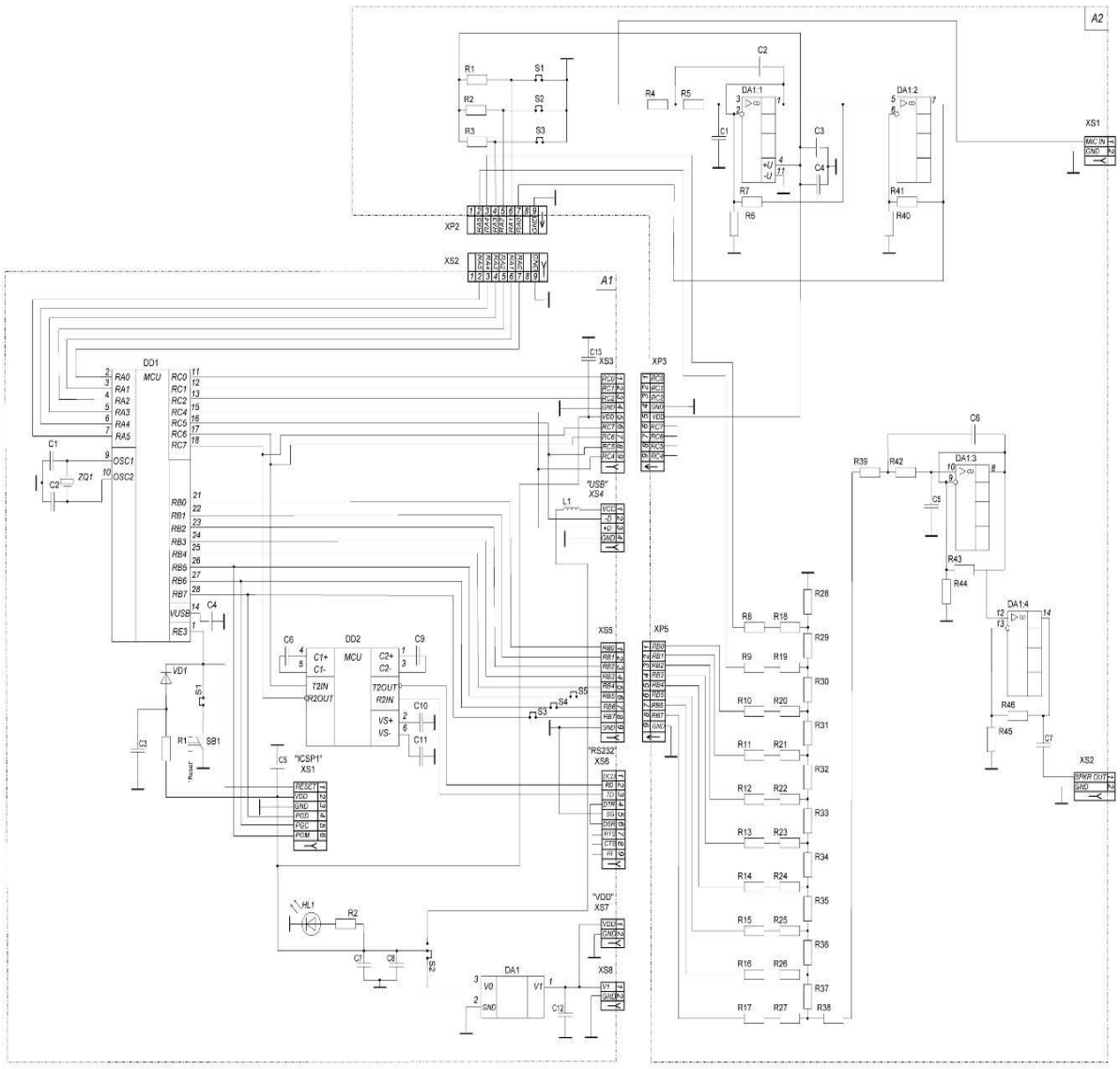


Рис. 2.37. Електрична принципова схема пристрою шифрування/дешифрування аудіо сигналів

Дешифрування здійснюється за тією ж операцією XOR, що має властивість зворотності, при цьому мікроконтролер генерує ту ж саму псевдовипадкову цифрову послідовність:

$$m_i = s_i \oplus z_i \quad (2.38)$$

Після дешифрування цифровий мовний сигнал передається на зовнішній цифро аналоговий перетворювач, що утворений матрицею R-2R.

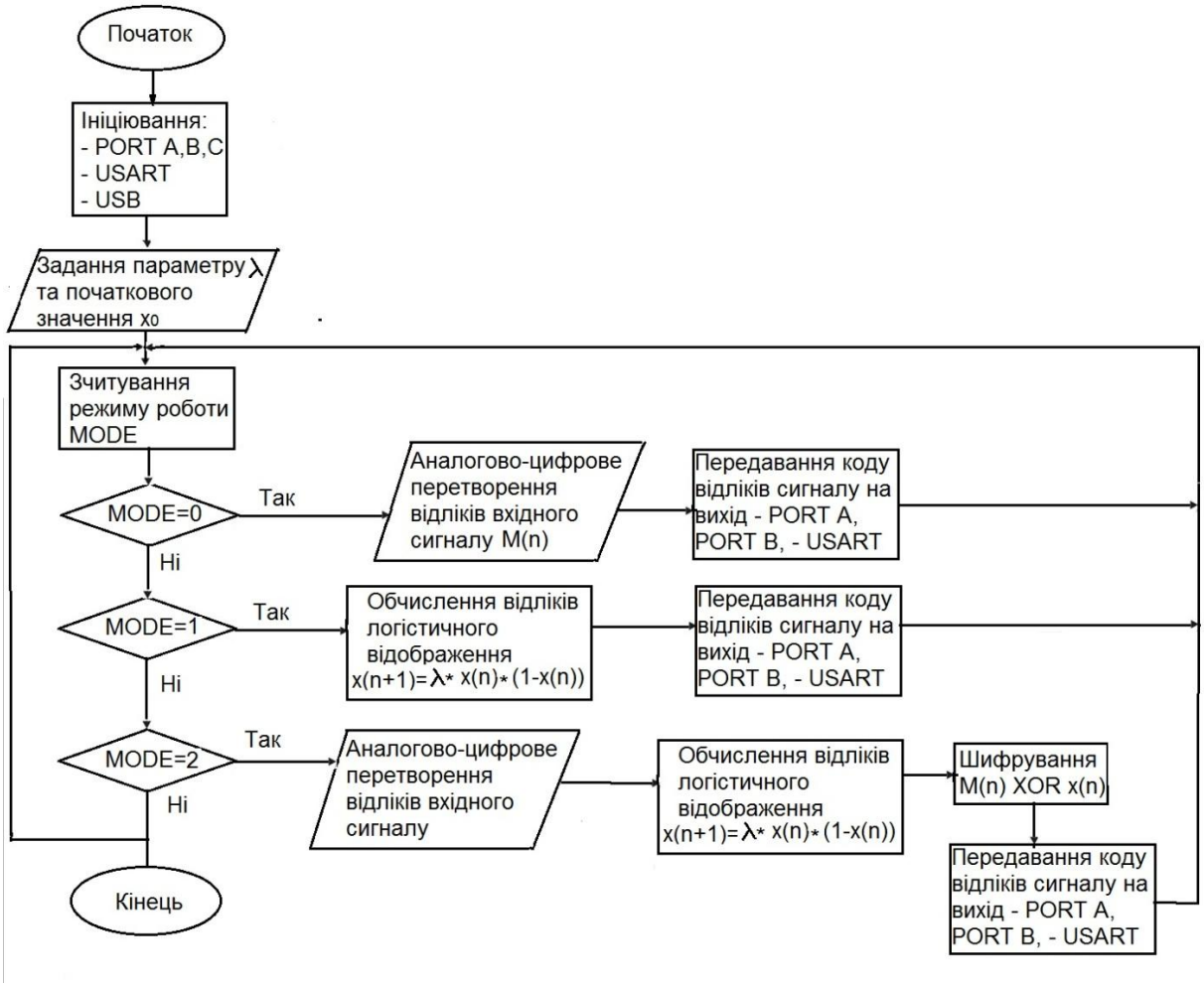
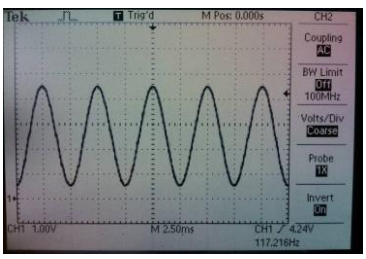
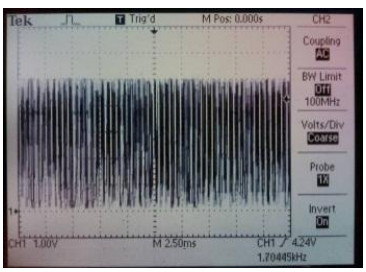


Рис. 2.38. Блок-схема алгоритму програми керування мікро контролера, де M(n) – інформаційне повідомлення перетворене у цифровий сигнал; x_0, λ – початкове значення та параметр логістичного відображення)

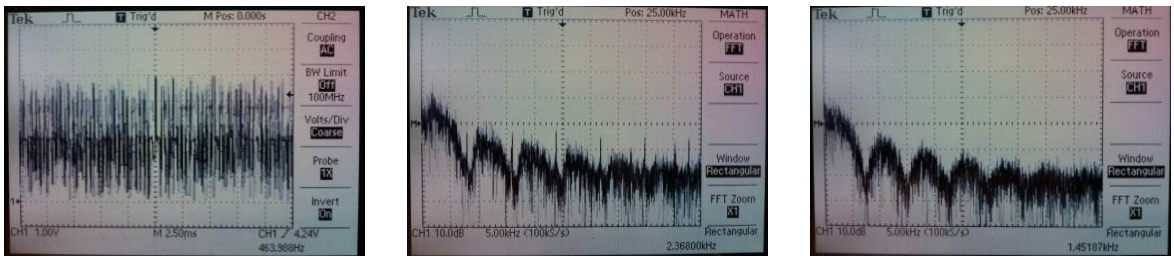
Для тестування роботи пристрою нами було здійснено шифрування та дешифрування гармонічного сигналу амплітудою 2В та частотою 100 Гц (рис. 2.39).



а)



б)



в) г) д)

Рис. 2.39. Вхідний сигнал (2В, 100 Гц) (а); хаотичний сигнал (λ=3,85; x_0=0,5) (б); зашифрований вхідний сигнал (в); спектр хаотичного сигналу (г); спектр зашифрованого сигналу (д)

На основі проведених досліджень можна зробити висновок про можливість використання мікро-контролерів для шифрування мовного сигналу.

2.8. Шифрування текстової інформації за допомогою зсувових регістрів пам’яті з нелінійною функцією оброблення

Відомим способом шифрування цифрової інформації є метод скремблювання, що базується на основі бінарних ПВП. Одним із поширених методів генерування бінарних ПВП на сьогоднішній день є використання зсувових регістрів пам’яті з лінійною функцією оброблення (LSFR) [120]. Кількість двійкових комбінацій, що можуть бути утворені на основі вмісту комірок регістра становить 2^n, де n — кількість комірок. Криптоаналітику достатньо знати усього $2 \cdot n$ біт тексту та його шифрограму, щоб заволодіти ключем заданої лінійної схеми шифрування. Слід зауважити, що підвищення криптостійкості таких систем можна досягти не тільки шляхом підвищення розрядності вмісту регістра а й використанням нелінійного оброблення вмісту регістрів зсуву.

Нами [15] запропонована програмна реалізація скремблера, основою якого є восьмирозрядний регістр пам’яті. Нелінійна функція оброблення вмісту регістру скремблера полягає в порівнянні 2 цілих чисел, що утворені його парними і непарними бітами [197]. В залежності від результату

порівняння на виході утворюється одне з двох можливих двійкових чисел: «0» або «1». З метою підвищення крипостійкості така схема шифрування була доповнена додатковою операцією лінійного конгруентного відображення чисельного представлення символу, що виконується перед скремблюванням. Блок-схема методу приведена на рис. 2.40.

Результати криптографічного перетворення скремблером вхідних даних при різних значеннях параметра c лінійного конгруентного генератора приведені на рис.2.41.

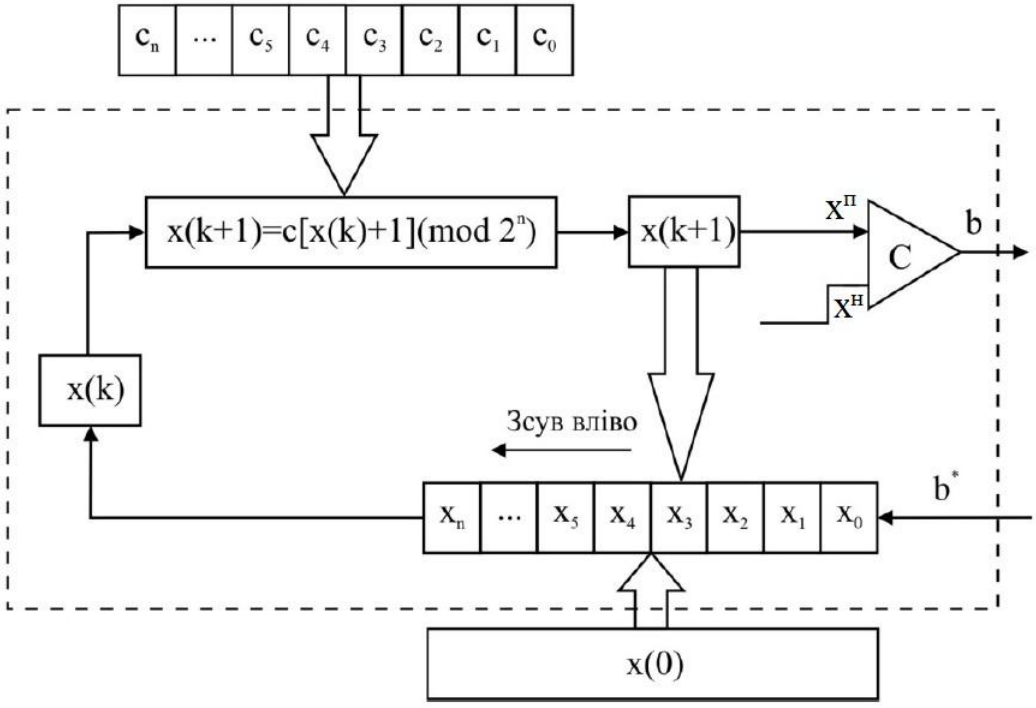
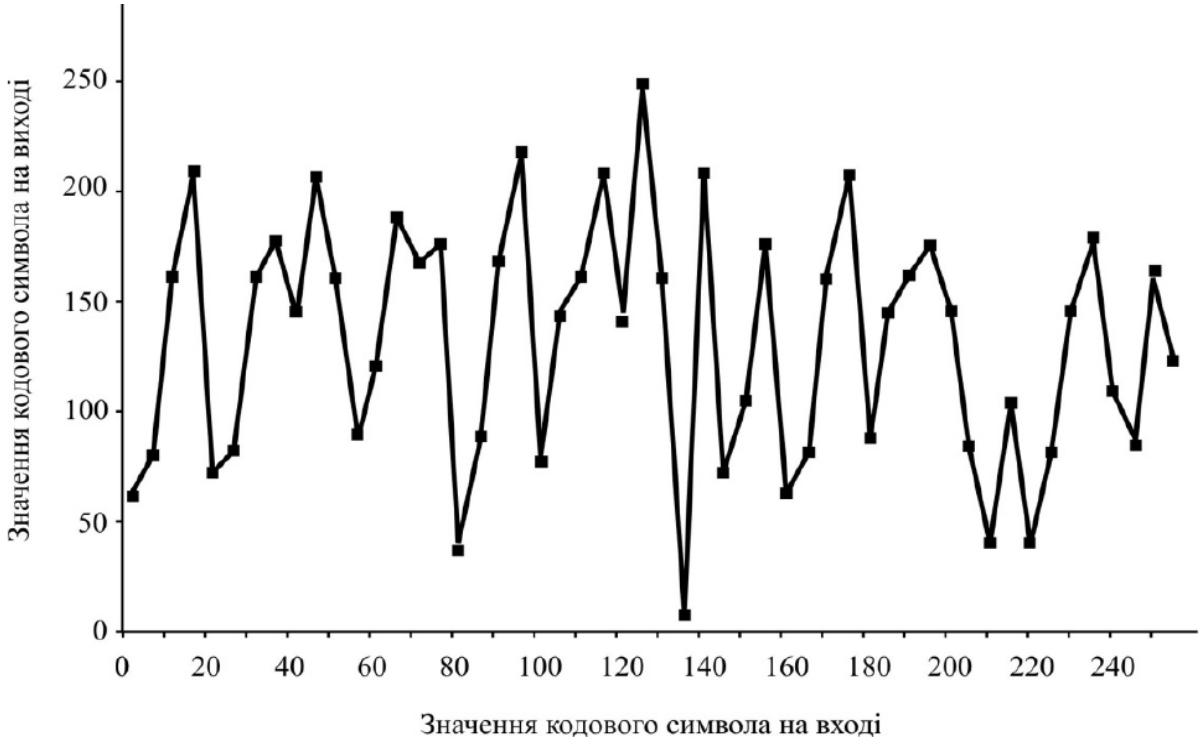
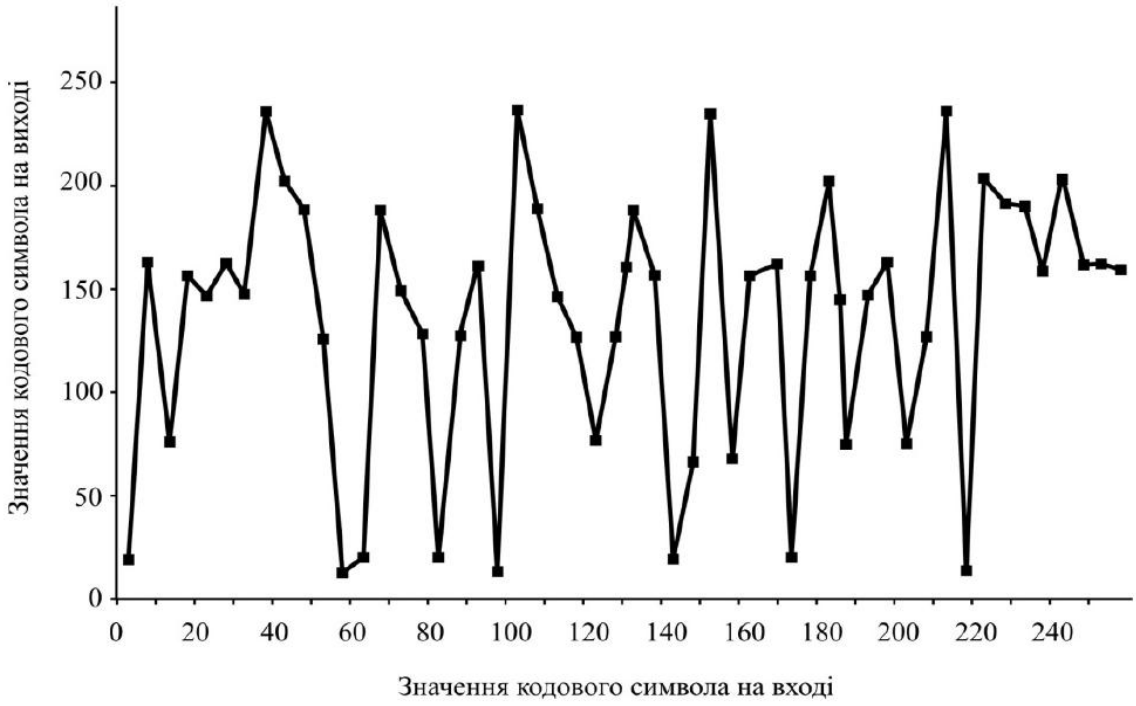


Рис.2.40. Блок-схема цифрового скремблера, реалізованого на регістрах пам’яті з нелінійною функцією обробки, де c – параметр логістичного відображення; $\{c_0, c_1, \ldots, c_n\}$ – біти двійкового представлення логістичного відображення; x(0) – початкове значення логістичного відображення; $\{x_0, x_1, \ldots, x_n\}$ – біти початкового значення логістичного відображення; x(k), x(k+1) – потокове та наступне значення логістичного відображення; b, b* – біт зашифрованого тексту, утворений на черговому кроці ітерації, $x^н$, $x^п$ – дійсні числа, утворені парними і непарними бітами числа x(k)

На основі якісного аналізу отриманих результатів можна зробити висновок про відсутність кореляції між вхідними та зашифрованим даними.



а)



б)

Рис.2.41. Криптографічне перетворення цифрової інформації за допомогою скремблера при різних значеннях параметра c: 21 (а) та 41 (б)

2.9. Моделювання канального кодування цифрових інформаційних повідомлень, шифрованих псевдовипадковими бінарними послідовностями

Нами [13] розроблена система цифрового зв'язку забезпечує шифрування інформації бінарними послідовностями, формованими на базі ПВП дійсних чисел.

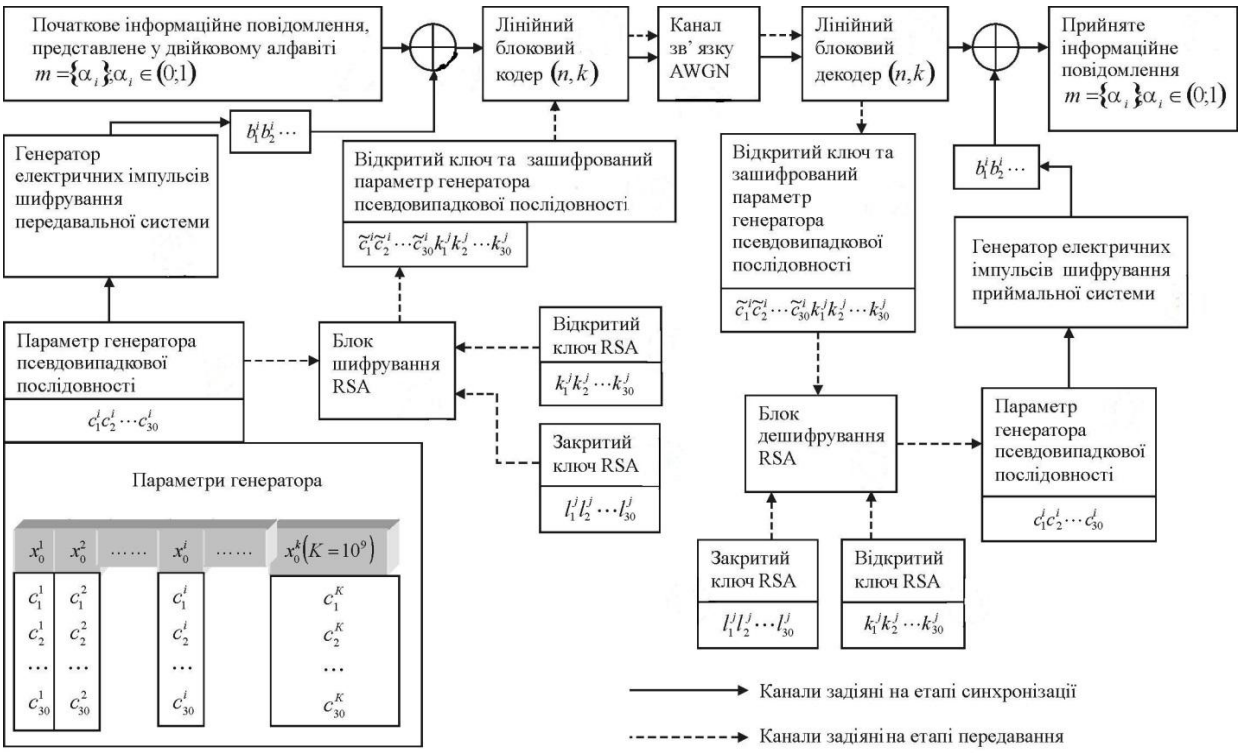


Рис. 2.42. Система цифрового зв'язку з шифруванням даних бінарними ПВП та кодуванням каналу лінійними блоковими кодами Хемінга

Передавач системи складається з наступних блоків: блоку генерування двійкових електричних імпульсів у відповідності із елементами бінарних ПВП. Ці імпульси використовуємо для шифрування інформаційного повідомлення шляхом його додавання за операцією XOR та послідовності електричних імпульсів, що сформовані у відповідності з ПВП; блоку

шифрування RSA, що використовується для шифрування параметрів генератора псевдовипадкових імпульсів.

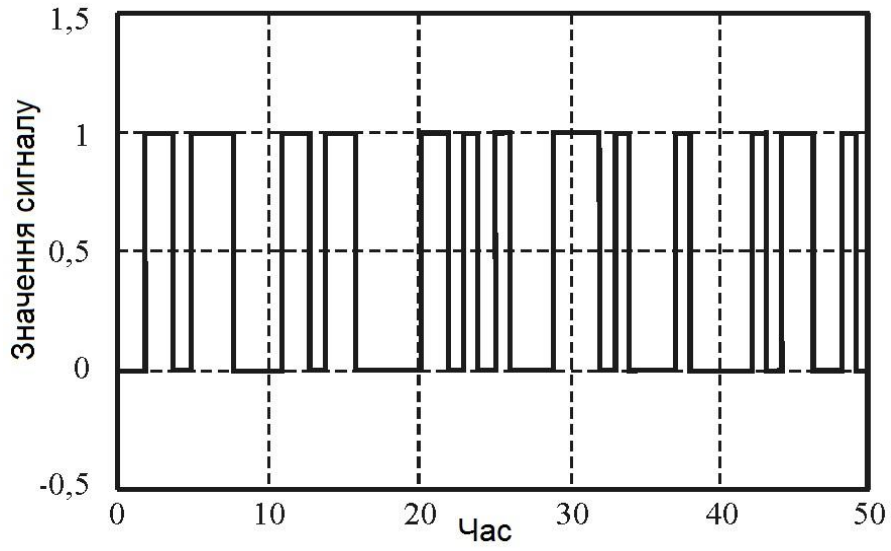
Передавання повідомлення відбувається у два етапи: 1-ий – синхронізація приймальної та передавальної частин, 2-ий – передавання інформаційного повідомлення. Канали передавання синхроімпульсів та інформаційного повідомлення зображені штриховою та суцільною лініями відповідно.

На етапі синхронізації передавач генерує послідовність синхронізації двійкових імпульсів, що відповідають представленню ключа та параметрів генератора x_{0i} та λ, зашифрованих методом RSA. Довжина цієї послідовності визначається розрядністю значень параметра генератора x_{0i}. В нашому випадку ми обмежувалися дев'ятим знаком після десяткової коми: {0,000000001; 0,000000002; 0,000000003;…; 0,999999998; 0,999999999; 1,000000000}. Елементи приведеної множини вказаних чисел можуть бути представлені тридцятирозрядними двійковими числами, кількість яких становить 2^{30}=107374182.

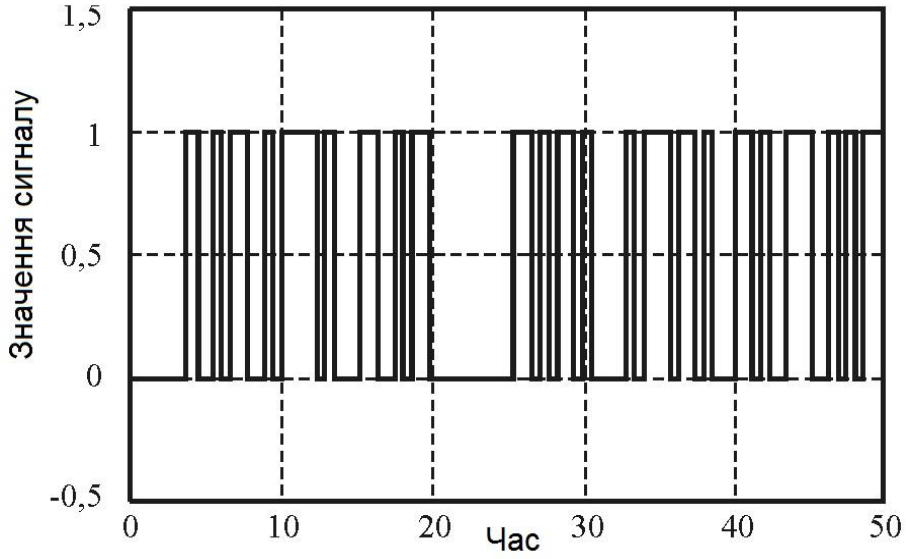
Блок шифрування RSA використовує для своєї роботи два ключі: відкритий (на схемі – $\{k_1^j k_2^j \cdots k_{30}^j\}$) і закритий (на схемі – $\{l_1^j l_2^j \cdots l_{30}^j\}$). Представлення відкритого ключа здійснювалося також цілим тридцятирозрядним двійковим числом. Тому вся довжина послідовності синхронізації становила 60 біт.

Вказана послідовність кодується лінійним блоковим кодером (n,k) та передається по каналу зв'язку з притаманним йому адитивним білим гаусовим шумом (AWGN).

При дослідженні впливу канального кодування на час синхронізації системи нами враховувалась зміна часових характеристик двійкових імпульсів цифрових сигналів закодованого інформаційного повідомлення при їх обробленні лінійними блоковими кодерами (рис. 2.43).



а)



б)

Рис.2.43. Часові діаграми сигналу на вході (а) та на виході (б) лінійного блокового кодера (7, 4)

У випадку канального кодування зашифрованого інформаційного повідомлення лінійним блоковим кодом (n,k) швидкість передавання канальних символів R_c дорівнюватиме:

$$R_c = R\,\frac{n}{k}, \qquad (2.39)$$

де R – швидкість передавання інформаційних бітів.

На вході приймача сигнал декодується декодером лінійного блокового коду (*n*,*k*). Після закінчення процесу синхронізації відбувається передавання інформаційного сигналу на проміжку часу $T_n = T - T_c$ (рис. 2.44).

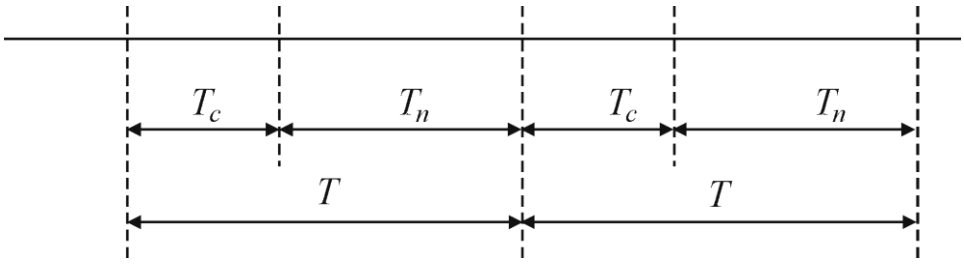


Рис.2.44. Часова схема роботи приймально-передавальної системи (Т – період синхронізації, Тс – тривалість синхронізації, Тп – тривалість передавання інформаційного повідомлення)

Після приймання послідовності імпульсів синхронізації $\left\{\tilde{c}_1^i \tilde{c}_2^i \cdots \tilde{c}_{30}^i k_1^j k_2^j \cdots k_{30}^j\right\}$ блок дешифрування RSA розшифровує послідовність $\left\{\tilde{c}_1^i \tilde{c}_2^i \cdots \tilde{c}_{30}^i\right\}$ за допомогою відкритого $\left\{k_1^j k_2^j \ldots k_{30}^j\right\}$ і закритого $\left\{l_1^j l_2^j \cdots l_{30}^j\right\}$ ключів. Таким чином приймальна сторона отримає значення параметрів генератора передавальної сторони. При цьому імпульси шифрування і дешифрування співпадають, оскільки оберненою до операції додавання за модулем 2 є ця ж операція: $(b_i \oplus 1) \oplus 1 = b_i$ і $(b_i \oplus 0) \oplus 0 = b_i$.

Вказані операції виконуються з кінцевою швидкістю, внаслідок чого тривалість синхронізації зростає (апаратна затримка) на величину що залежить від швидкодії елементної бази, на якій реалізовані блоки приймача і передавача системи.

Після встановлення синхронізації приймальної і передавальної сторін системи передавач передає зашифроване бітами бінарної послідовності інформаційне повідомлення, що формуються на основі чисел генерованих генератором ХС на пристрій ЛБК. Після проходження каналу зв’язку на приймальній частині сигнал декодується лінійним блоковим кодером з

наступним розшифруванням шляхом сумування по модулю 2 з послідовністю двійкових імпульсів, генерованих генератором приймача.

Нами [13] досліджений вплив шуму в каналі зв'язку на тривалість процесу синхронізації передавальної та приймальної частин системи, що зображена на рис. 2.44.

Коди Хемінга (Hamming codes) – це простий клас блокових кодів, що мають наступну структуру:

$$(n,k) = (2^m - 1, 2^m - 1 - m) \qquad (2.40).$$

Коди БЧХ (Bose-Chaudhuri-Hockquengem), що є узагальненням кодів Хемінга, дозволяють виправляти множинні помилки.

Виправна здатність лінійних блокових кодів визначається відстанню Хемінга d_H, значення якої обмежене зверху у відповідності зі співвідношенням Плоткіна:

$$d_H \le \frac{n \cdot 2^{k-1}}{2^k - 1} \qquad (2.41).$$

При великих значеннях *k* виконується співвідношення $2^k \gg 1$, тому:

$$d_H \le \frac{n}{2} \quad (2.42)$$

Шифрування повідомлень здійснюється бінарними послідовностями, формованими ПВП за співвідношенням:

$$x_i = m_i \oplus b_i \qquad (2.43)$$

Розділяючи інформаційну послідовність на блоки по *k* біт, на виході кодера (*n,k*) отримаємо відповідну послідовність кодових символів довжиною n:

$$x(n) = x(k) \cdot G(n,k) \qquad (2.44),$$

де *x(k)* – інформаційна послідовність довжиною *k* біт, *x(n)* – послідовність кодових символів довжиною *n* біт, *G(n,k)* – матриця генерування коду *(n,k)*.

Було встановлено, що шифрування інформаційних повідомлень бінарними послідовностями, сформованими на основі ПВП, не впливає на роботу ЛБК та не погіршує характеристики завадостійкого кодування [13].

Із результатів аналізу моделювання процесу синхронізації за допомогою імпульсів, що відповідають бітам представлення початкового значення x_0 генераторів, випливає, що лінійні блокові коди не тільки виявляють та виправляють помилки, але й забезпечують зменшення тривалості процесу синхронізації.

При дослідженнях тривалість часу синхронізації визначалась часом передавання двійкових імпульсів, кількість яких дорівнює кількості бітів бінарної послідовності, що задає з необхідною точністю значення параметру генерування x_0. Вважалося, що кількість імпульсів у сигналі синхронізації повинна бути збільшена на кількість інвертованих у каналі імпульсів внаслідок дії імпульсних завад.

Ймовірність помилки канального біта для бінарної фазової модуляції дорівнює:

$$p = Q\left(\sqrt{2 \cdot \frac{E_b}{N_0}}\right) \qquad (2.45),$$

де Q – інтеграл помилок $Q(x) = \frac{1}{\sqrt{2 \cdot \pi}} \cdot \int_x^{\infty} e^{-u^2/2} du$, E_b – енергія біта інформації, N_0 – спектральна густина потужності шуму в каналі.

Тоді середня кількість інвертованих біт у послідовності синхронізації довжиною N біт дорівнюватиме:

$$n_i = N \cdot p \qquad (2.46),$$

а необхідна кількість імпульсів у послідовності синхронізації становитиме:

$$\tilde{N} = N \cdot (1 + p) \quad (2.47).$$

При канальному кодуванні інформаційного повідомлення лінійними блоковими кодами (n,k) ймовірність помилки визначається за формулою:

$$p_c = Q\left(\sqrt{2 \cdot \frac{k}{n} \cdot \frac{E_c}{N_0}}\right) \quad (2.48).$$

Ймовірність помилки у декодованому біті дорівнює [120]:

$$P_B = \frac{1}{n} \cdot \sum_{j=t+1}^{n} \cdot C_n^j \cdot p_c^j \cdot (1 - p_c)^{n-j}, \qquad (2.49)$$

де t — кількість бітових помилок у одному кодовому слові, що може бути виправлена кодом.

Таким чином, довжина закодованої лінійним блоковим кодером (n,k) послідовності синхронізації N_c, та середня кількість інвертованих бітів у закодованій послідовності відповідно дорівнюватимуть:

$$N_c = N\frac{n}{k}, \qquad (2.50)$$

$$n_{ic} = N_c P_B = N\frac{n}{k}P_B \qquad (2.51).$$

Для дослідження впливу шумів каналу на час синхронізації вибиралася швидкість передавання бітів R=10 Мбіт/с.

Тривалість передавання послідовності синхронізації без кодування та з завадостійким кодуванням визначається за наступними формулами:

$$T_{0n} = \frac{\tilde{N}}{R} = N\frac{1+p}{R} \qquad (2.52),$$

$$T_n = \frac{\tilde{N}_c}{R_c} = \frac{N\frac{n}{k}(1+P_B)}{R\frac{n}{k}} = N\frac{1+P_B}{R} \qquad (2.53).$$

Залежність тривалості синхронізації від відносного рівня шуму для кодів Хемінга і БЧХ приведені на рисунках 2.45 і 2.46 відповідно. Для порівняння отриманих даних з роботами інших авторів [198] в якості характеристики каналу використовувався відносний рівень шуму (корінь квадратний з відношення потужності шуму до енергії канального біта, вираженого у Вт):

$$\eta = \sqrt{\frac{N_0}{E_b}}, \qquad (2.54)$$

що зв’язаний з параметром $\frac{E_b}{N_0}$, вираженим у децибелах наступним співвідношенням:

$$\eta = 10^{-0{,}05\left(\frac{E_b}{N_0}\right)_{\text{дБ}}} \qquad (2.55)$$

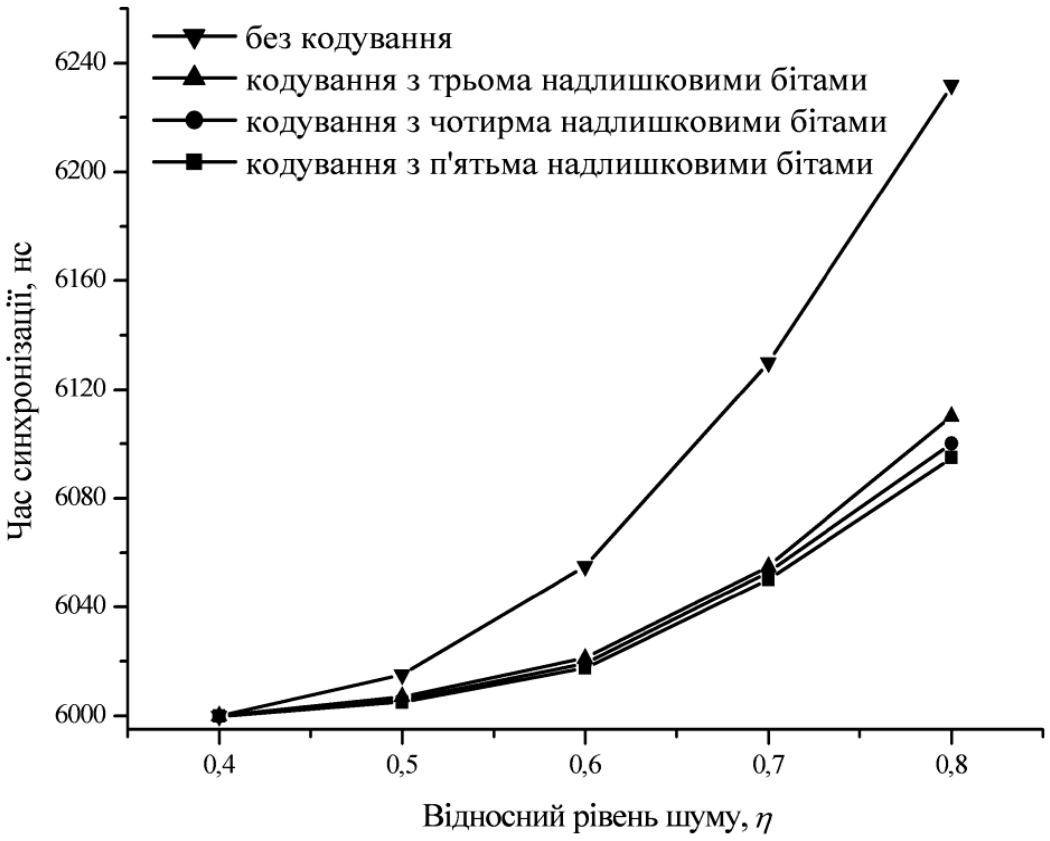


Рис. 2.45. Залежність тривалості синхронізації від значення відносного рівня шуму у каналі при використанні кодів Хемінга з кратністю виправлення помилки, рівної 1

На рис. 2.45 приведені дані для лінійних блокових кодів Хемінга ((7,4), (15,11), (31,26)). Із рис. 2.45 та 2.46 випливає що зменшення тривалості синхронізації обумовлене використанням канального кодування має місце для значень $\eta \in [0,4;0,8]$.

На рис. 2.46 приведені залежності тривалості часу синхронізації від рівня шуму для блокових кодів БЧХ та коду Голея.

В нашому випадку шуми каналу впливають на час синхронізації при η=0,4, тоді як у роботі інших авторів [198] це значення становить 0,3, що очевидно обумовлено використанням завадостійкого кодування лінійними блоковими кодами.

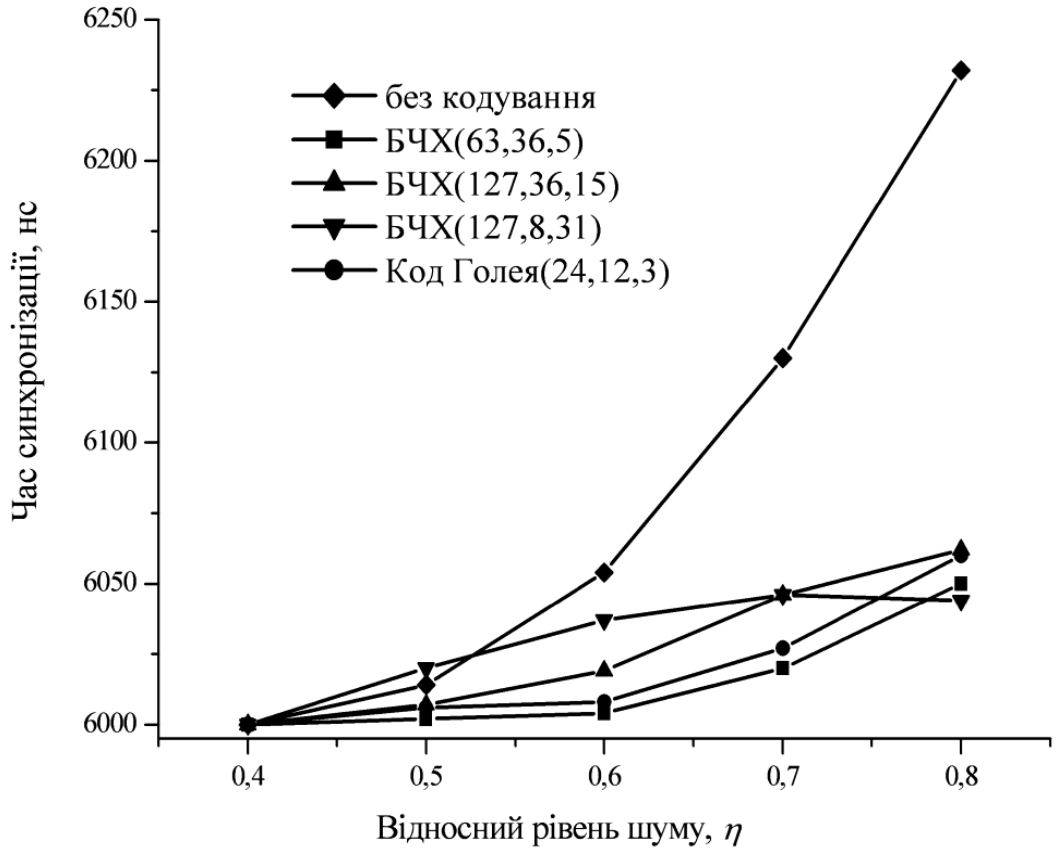


Рис. 2.46. Залежність тривалості синхронізації від значення відносного рівня шуму у каналі при використанні кодів БЧХ (остання цифра означає кратність помилки, яку виправляє кодер у блоці)

З отриманих залежностей випливає, що використання відносно простих схем лінійного блокового кодування призводить до зменшення часу синхронізації в межах 50…100 нс при значеннях η, що знаходиться у межах 0,4…0,8 для швидкості передавання 10 Мбіт/с. Для більш потужних схем канального кодування БЧХ та Голея зменшення тривалості синхронізації становить 100…200 нс.

ВИСНОВКИ

1. В результаті дослідження властивостей послідовностей генерованих пороговим методом за логістичним та узагальненим відображенням Пекаря встановлено, що залежність збалансованості послідовності від початкового значення динамічної змінної носить випадковий характер. Відхилення значень збалансованості послідовностей від одиниці збільшується зі збільшенням їх довжини і становить 6, 10, 15, 20 та 27 для довжин 64, 128, 256, 512 та 1024 біти відповідно. При цьому частка незбалансованих бітів у послідовності зменшується зі збільшенням їх довжини і становить: 9%, 8%, 6%, 4% та 3% для послідовностей довжиною 64, 128, 256, 512 та 1024 біти відповідно. Значення збалансованості фрагментів послідовності одинакової довжини не залежить від порядку їх розсташування у послідовності максимальної довжини 1024 біт. Розподіл густини ймовірності значень збалансованості є близьким до Гаусового із середнім значенням $M(L)=0$ та дисперсією $\sigma_0^2 = 6.47$.

2. На підставі отриманих усереднх значень встановлено, що циклічність послідовностей, генерованих досліджуваними відображеннями є гіршою від циклічності послідовностей, формованих за допомогою лінійного регістра зсуву. Частка кількості циклів довжинами 1, 2, 3 та 4 і більше біт становлять -24%; 2,14%; 5,61%; 15,94%.

3. Встановлено, що для генерованих логістичним відображенням послідовностей довжинами 64, 128, 256, значення коефіцієнта кореляції становить - 0.15…0.15, а для послідовностей із довжинами 512 і 1024 біта його значення знаходиться у межах −0,01…+0,01. Для послідовностей, генерованих за узагальненим відображенням Пекаря, значення коефіцієнтів кореляції знаходиться в межах від -0,4 до 0,4. Із отриманих результатів можна зробити висновок, що генеровані пороговим методом послідовності на основі логістичного відображення та узагальненого відображення Пекаря на

відміну від послідовностей генерованих модулярним методом та лінійними зсувовими регістрами із оберненим зв’язком є неперіодичними.

4. Запропонована система передавання інформації з її шифруванням бітами ПВП, формованими на основі хаотичних коливань, що генеруються логістичним відображенням. Синхронізація між передавальною та приймальною сторонами системи забезпечується шляхом передавання зашифрованої одним із стандартних методів (RSA) ключової послідовності, що є двійковим представленням початкового значення динамічної змінної та параметру λ логістичного відображення.

5. Розроблена СПІ передавання у реальному часі аудіо сигналів, що зашифровані псевдовипадковими послідовностями формовані на основі хаотичних коливань за логістичним відображенням із забезпеченням синхронізму приймальної та передавальної сторін системи періодичним передаванням потокових значень хаотичних коливань.

6. Досліджений ступінь кореляції сусідніх пікселів графічної інформації зашифрованої бінарними ПВП, що формуються поліноміальним методом із використанням генератора Бокса-Мюллера. Встановлено, що значення коефіцієнту кореляція між інтенсивностями сусідніх пікселів зменшується від 0,9 для початкового зображення до 0,05 для зашифрованого, а утворений після шифрування розподіл інтенсивності пікселів близький до рівномірного, внаслідок чого спостерігатиметься одноманітний сірий фон.

7. Розроблений метод одночасного стискування та шифрування інформації, що на відміну від відомих прискорює процес перетворення інформації, оскільки її шифрування здійснюється протягом кожної ітерації процесу економного кодування. Для кодування джерела інформації можуть використовуватися алгоритми Шенона-Фано, Хафмена та арифметичне адаптивне кодування.

8. Досліджена та реалізована на програмному рівні 3-вимірна дискретна модель відображення Пекаря для шифрування зображень шляхом перестановки його фрагментів. Встановлено оптимальне розбивання

початкового зображення на фрагменти, що забезпечує задовільне шифрування інформації.

9. Реалізована на програмному рівні багатокористувацька система передавання текстової інформації, кожному користувачеві якої присвоюється IP-адреса та ключ шифрування, що є бінарною послідовністю, формованої за значеннями параметра логістичного відображення та початкового значення хаотичного коливання. Розроблена система поряд із стандартною процедурою шифрування CRC32 використовує потокове шифрування інформації ПВП, генерованою за логістичним відображенням. Тестуванням роботи системи встановлено, що оптимальна кількість користувачів дорівнює двадцяти, якщо початкове значення динамічної змінної задається числом з п’ятьма знаками після коми.

10. Встановлено, що використання відносно нескладних схем лінійного блокового кодування (кодів Хемінга із 3-ма, 4-ма та 5-ма надлишковими бітами) зменшує час синхронізації на 0÷150 нс при відносному рівні шуму η=0,4÷0,8 та швидкості передавання даних 10 Мбіт/с. Для БХЧ кодів із 17, 91 та 119 надлишковими бітами (що здатні виправляти 5-, 15-, та 31-кратні моделі помилок та мають коефіцієнти надлишковості 0,57, 0,28 та 0,06 відповідно) час синхронізації зменшується на 0÷200 нс.

РОЗДІЛ 3. ВЛАСТИВОСТІ ПСЕВДОВИПАДКОВИХ КОЛИВАНЬ ГЕНЕРОВАНИХ СИСТЕМАМИ З НЕПЕРЕРВНОЮ ФУНКЦІЄЮ ВІДОБРАЖЕННЯ ТА ОСОБЛИВОСТІ ЇХ СИНХРОНІЗАЦІЇ

Аналіз літературних даних [57, 64, 65] показує, що вченими та інженерами проводяться систематичні дослідження генераторів хаотичних коливань, математичною моделлю яких є системи нелінійних рівнянь із квадратичними, кубічними [14] та нелінійностями більш високих порядків. Схемотехнічна реалізація таких систем вимагає використання аналогових помножувачів, що є досить вартісною технологією [16, 21]. Іншим методом генерування складних коливань є використання у коливальних контурах радіотехнічних елементів із кусково-лінійними характеристиками, окремі ділянки яких мають від'ємний опір [199, 200]. Від'ємний опір забезпечується використанням особливих електронних приладів, що використовують явище струмового віддзеркалювання і мають назву current-to-voltage converter.

В залежності від кількості точок зламу у вольт-вольтній характеристиці нелінійного елемента система генерує ХК, що характеризуються атракторами із різними за своєю складністю структурами – від одновиткового до багатовиткового [200], що є порівняним із системами вищого порядку, наприклад системою Лю. У даному розділі приведені дослідження систем із різними типами нелінійних характеристик – квадратичної (система четвертого порядку Лю), генераторів Чуа та кільцевих із три- та п'ятисегментними характеристиками.

3.1. Моделювання та експериментальні дослідження псевдовипадкових коливань, генерованих системою з неперервною функцією відображення, заданою чотирма диференційними рівняннями

Прикладом системи з неперервною нелінійною функцією відображення є система, що описується чотирма нелінійними диференційними рівняннями

першого порядку (3.1) [201]:

$$\begin{aligned}\dot{x} &= a\cdot(x-y)\\ \dot{y} &= b\cdot x - h\cdot x\cdot z + \lambda\cdot w\\ \dot{z} &= c\cdot x^2 - d\cdot z\\ \dot{w} &= -n\cdot y\end{aligned}, \quad (3.1)$$

де x, y, z, w – змінні системи; a, b, h, λ, c, d, n – параметри керування.

Як зазначалося у першому розділі, псевдовипадкова динаміка системи може бути описана декількома числовими характеристиками, до яких відносяться зокрема показники Ляпунова.

Система диференційних рівнянь (3.1) характеризується чотирма показниками Ляпунова, знаки яких визначають псевдовипадкову динаміку системи у сенсі її стійкості по Ляпунову.

У [57, 60] приведений детальний аналіз сигнатур систем із розмірністю 4 у залежності від знаків показників Ляпунова (табл. 3.1).

Таблиця 3.1.

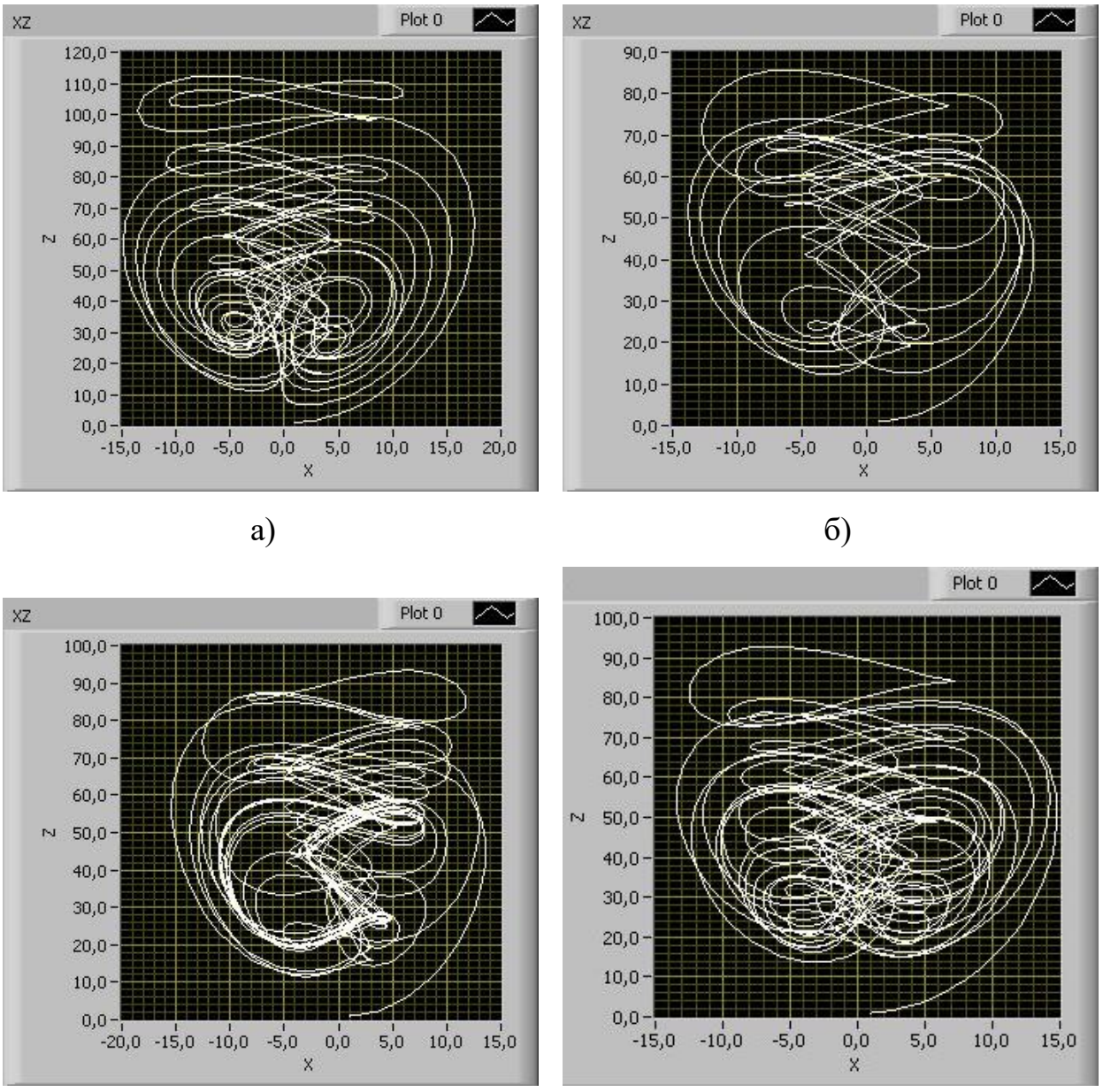
Види коливних процесів системи Лю в залежності від знаків її показників Ляпунова

Показники Ляпунова				**Динаміка системи**
λ_1	λ_2	λ_3	λ_4	
0	від'ємний	від'ємний	від'ємний	Періодичні коливання
0	0	від'ємний	від'ємний	Квазіперіодичні коливання
додатній	0	від'ємний	від'ємний	Песвдовипадкові коливання
додатній	додатній	0	від'ємний	Песвдовипадкові коливання з двома атракторами

Отже в системі Лю з чотирма змінними, можливі чотири варіанти псевдовипадкової динаміки [21] .

В результаті проведених нами досліджень було встановлено, що в залежності від значень параметра *n,* при фіксованих значеннях параметрів *a, b, c, d, h*, λ, в системі можуть виникати періодичні, квазіперіодичні, псевдовипадкові, та псевдовипадкові коливання з двома атракторами.

Чисельне моделювання поведінки системи Лю здійснювалося у середовищі LabView при наступних значеннях її параметрів: $a=15$, $b=30$, $h=1$, $\lambda=1$, $c=4$, $d=2.5$.



а) б)

в) г)

Рис.3.1. Проекція фазових траєкторій на площину *x*-*z*, генерованих системою Лю хаотичних коливань – псевдовипадкових коливань з двома атракторами при n = 20 (а); псевдовипадкових коливань при n = 42(б); квазіперіодичних при n = 70 (в) та періодичних коливань при n = 78 (г)

Із отриманих результатів моделювання фазових траєкторій (рис 3.1) випливає, що при значеннях n = 20 та 42 система генерує псевдовипадкові коливання з двома із одним атрактором відповідно. При значеннях n=78 та n=70 у системі мають місце періодичні та квазіперіодичні коливання відповідно.

Нами [21] проведено моделювання структурної і електричної схем генератора з неперервною функцією відображення, заданою системою диференційних рівнянь (3.1) та визначені значення номіналів компонентів електричної схеми генератора коливань. За отриманими результатами був виготовлений експериментальний зразок генератора псевдовипадкових коливань з використанням операційних підсилювачів КР140УД708 та аналогових помножувачів AD633JN.

При моделюванні значення амплітуди змінних були зменшенні на два порядки з метою узгодження амплітуд змінних системи (3.1) з робочими напругами електронних компонентів схеми. Внаслідок цього з врахуванням використовуваних при моделюванні значень параметрів система набуває наступного вигляду:

$$\begin{aligned} 0.1\cdot \dot{x}_1 &= 1.5\cdot y_1 - 1.5\cdot x_1 \\ 0.1\cdot \dot{y}_1 &= 3\cdot x_1 - x_1\cdot z_1 + 0.1\cdot w_1 \\ 0.1\cdot \dot{z}_1 &= 4\cdot x_1^2 - 0.25\cdot z_1 \\ 0.1\cdot \dot{w}_1 &= -0.1\cdot y_1 \end{aligned} \qquad (3.2)$$

У структурній схемі генератора псевдовипадкових коливань із двома атракторами, що описується системою рівнянь (3.2), (рис. 3.2), передбачене виконання дій додавання (W), множення (X), інтегрування (I) та інвертування за входом (U).

Електрична схема генератора коливань (рис.3.3), що відповідає вище приведеній структурній схемі, була реалізована на аналогових помножувачах AD633JN [202] та операційних підсилювачах КР140УД708 з різними схемами увімкнення.

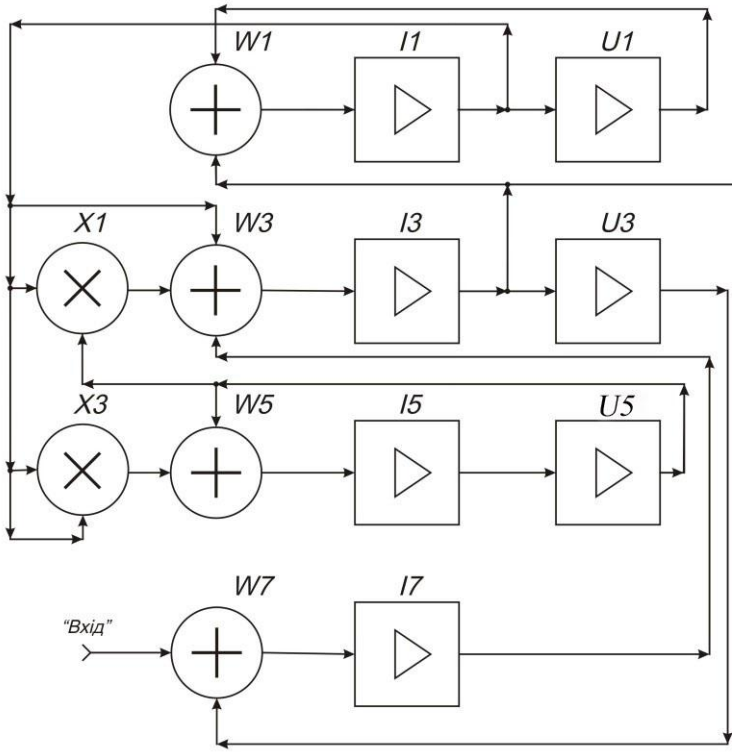


Рис.3.2. Структурна схема генератора коливань з неперервною функцією відображення, заданого системою диференційних рівнянь Лю,
W_1, W_3, W_5, W_7 – суматори; X_1, X_3 – помножувачі; I_1, I_3, I_5, I_7 – інтегруючі підсилювачі; U_1, U_3, U_5 – інвертуючі підсилювачі

Використовуючи закони Кірхгофа, систему диференційних рівнянь, що описує досліджувану електричну схему (рис.3.3) можна записати у наступному вигляді:

$$\begin{aligned}
\dot{U}_{C_1} &= -\frac{R_{10}\cdot R_{21}}{R_1\cdot R_{18}\cdot\left(C_1\cdot R_{14}\right)}\cdot U_{C_1} + \frac{R_{10}}{R_2\cdot\left(C_1\cdot R_{14}\right)}\cdot U_{C_2} \\
\dot{U}_{C_2} &= \frac{R_{11}}{R_5\cdot\left(C_2\cdot R_{15}\right)}\cdot U_{C_1} - k\cdot\frac{R_{11}\cdot R_{23}}{R_4\cdot R_{20}\cdot\left(C_2\cdot R_{15}\right)}\cdot U_{C_1}\cdot U_{C_3} + \frac{R_{11}}{R_3}\cdot U_{C_4} \\
\dot{U}_{C_3} &= \frac{R_{12}}{R_7\cdot\left(C_3\cdot R_{15}\right)}\cdot U_{C_1}^2 - \frac{R_{12}\cdot R_{23}}{R_6\cdot R_{20}\cdot\left(C_3\cdot R_{15}\right)}\cdot U_{C_3} \\
\dot{U}_{C_4} &= -\frac{R_{13}}{R_8\cdot\left(C_4\cdot R_{17}\right)}\cdot U_{C_2}
\end{aligned} \qquad (3.3),$$

де k – коефіцієнт, що дорівнює 1/10 $В^{-1}$.

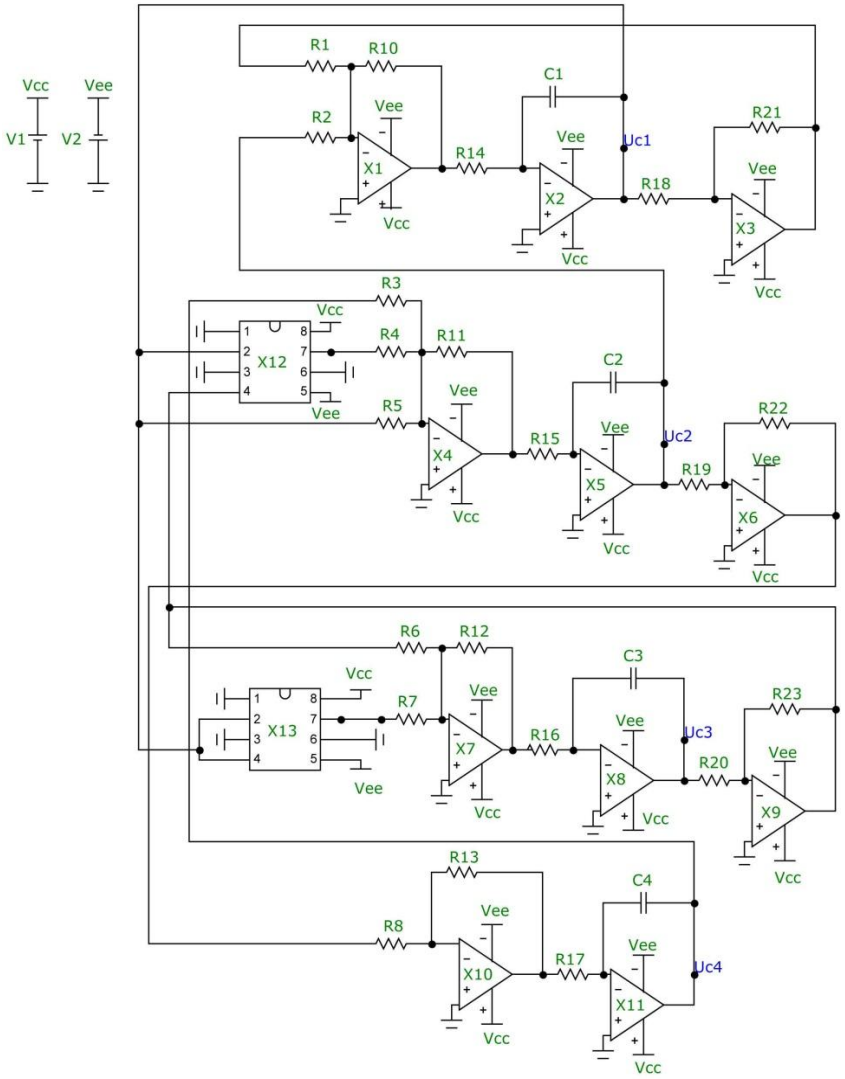


Рис.3.3. Схема електрична принципова генератора коливань з неперервною функцією відображення за допомогою системи диференційних рівнянь Лю

Вихідні напруги U_{C_1}, U_{C_2}, U_{C_3}, U_{C_4} на ємностях електричної схеми відповідають значенням чотирьох змінних x_1, y_1, z_1 та w_1 системи рівнянь (3.1). Вважаючи, що опори $R_{14};R_{15};R_{18};R_{20};R_{21};R_{23};R_0$, та ємності, $C_1;C_2;C_3;C_4;C_0$ рівні між собою і дорівнюють *10 кОм та 10пФ* відповідно із (3.3) отримаємо:

$$\begin{cases} (R_0 \cdot C_0)\cdot \dot{U}_{C_1} = -\dfrac{R_{10}}{R_1}\cdot U_{C_1} + \dfrac{R_{10}}{R_2}\cdot U_{C_2} \\ (R_0 \cdot C_0)\cdot \dot{U}_{C_2} = \dfrac{R_{11}}{R_5}\cdot U_{C_1} - \dfrac{R_{11}}{R_4}\cdot U_{C_1}\cdot U_{C_3} + \dfrac{R_{11}}{R_3}\cdot U_{C_4} \\ (R_0 \cdot C_0)\cdot \dot{U}_{C_3} = k\cdot \dfrac{R_{12}}{R_7}\cdot U_{C_1}^2 - \dfrac{R_{12}}{R_6}\cdot U_{C_3} \\ (R_0 \cdot C_0)\cdot \dot{U}_{C_4} = -\dfrac{R_{13}}{R_8}\cdot U_{C_2} \end{cases} \quad (3.4)$$

Прирівнюючи значення коефіцієнтів у рівняннях систем (3.2) та (3.4), розрахуємо номінали опорів R_1, R_2, R_3, R_4, R_5, R_6, R_7 та R_8 електричної схеми при значеннях параметрів системи $a=1{,}5$; $b=3$; $h=0{,}1$; $\lambda=1$; $c=4$; $d=0{,}25$:

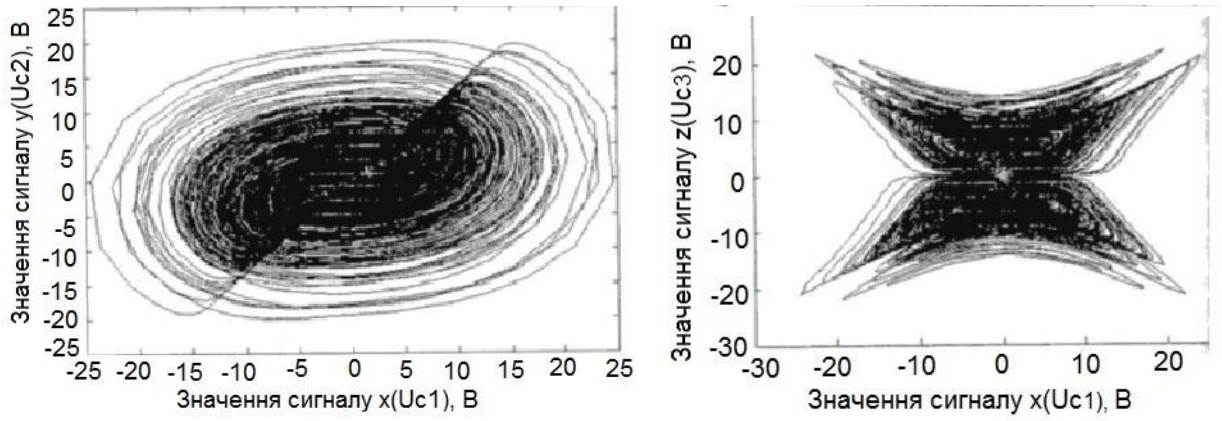
$$a=\frac{R_{10}}{R_1}=\frac{R_{10}}{R_2}=1{,}5\Rightarrow R_1=R_2=6{,}67\ кОм;\qquad b=\frac{R_{11}}{R_5}=3\Rightarrow R_5=3{,}34\ \text{кОм};$$

$$c=\frac{R_{12}}{R_7}=4\Rightarrow R_7=2{,}5\ \text{кОм};\qquad h=\frac{R_{11}}{R_3}=0{,}1\Rightarrow R_3=100\ кОм;$$

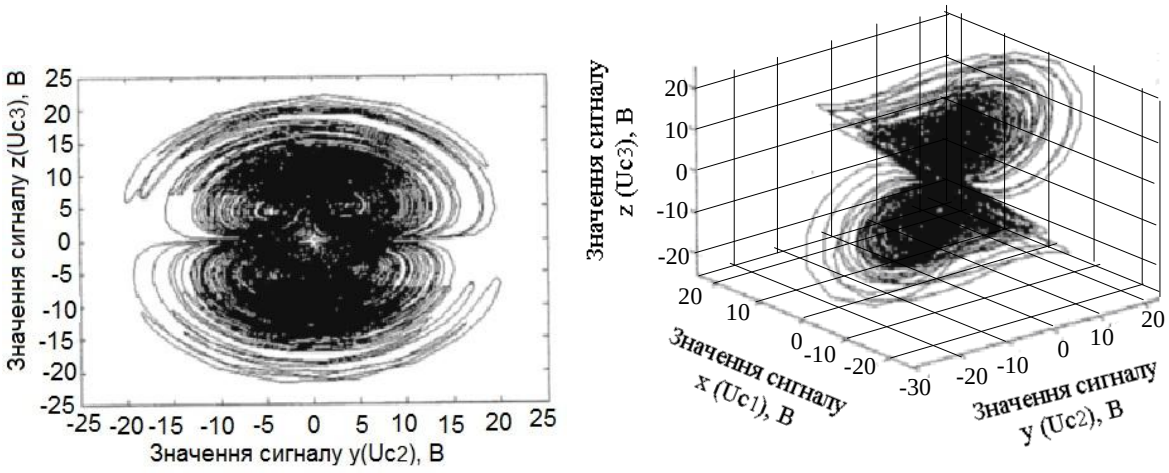
$$\lambda=\frac{R_{11}}{R_4}=1\Rightarrow R_4=10\ \text{кОм};\qquad d=\frac{R_{12}}{R_6}=0{,}25\Rightarrow R_6=40\ \text{кОм};$$

$$n=\frac{R_{13}}{R_8}=0{,}1\Rightarrow R_8=100\ кОм;\qquad R_0\cdot C_0=0{,}1\ мс.$$

Результати моделювання фазових траєкторій та часових діаграм динамічних змінних генеруються електричною схемою, заданою системою диференційних рівнянь Лю, приведені на рис.3.4 та рис.3.5.

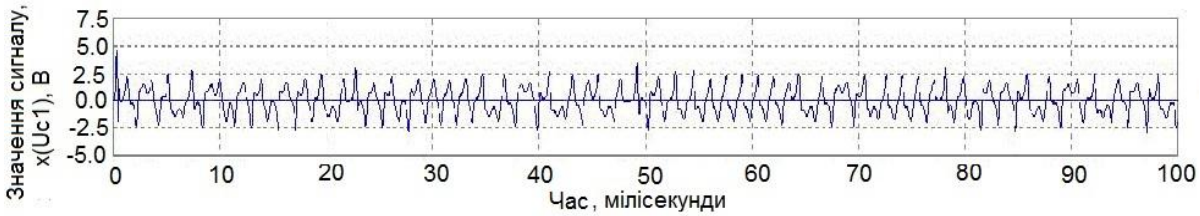


а) б)

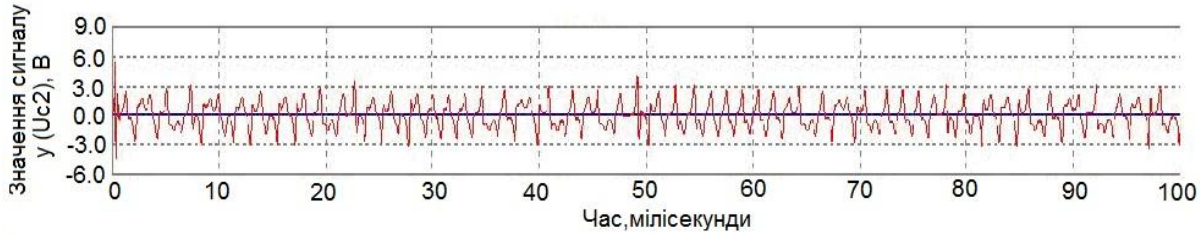


в) г)

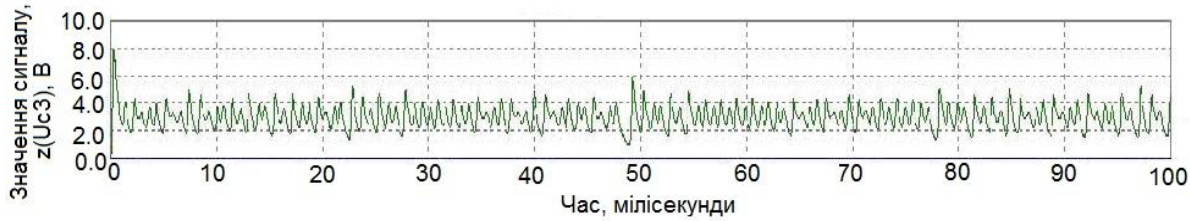
Рис.3.4. Фазові траєкторії системи, що описується диференційними рівняннями Лю для розрахованих значень опорів та ємностей в площинах– (x-y) напруги (U_{C1}- U_{C2}) (а), ($x-z$) напруги ($U_{C_1}-U_{C_3}$) (б), (y-z) напруги (U_{C2}- U_{C3}) (в) та у просторі (x-y-z) напруги (U_{C1}-U_{C2}-U_{C3}) (г)



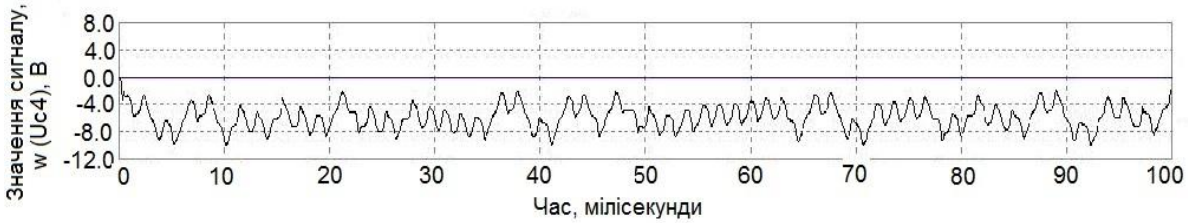
а)



б)



в)



г)

Рис.3.5. Часові залежності динамічних змінних x (U_{C_1}) (а); y (U_{C_2}) (б); z (U_{C_3}) (в); w (U_{C_4}) (г), генерованих системою (3.4)

Виходячи із отриманих результатів можемо зробити висновок, що часові залежності змінних системи та її фазові портрети підтверджують псевдовипадковий характер генерованих коливань.

В експериментальному зразку генератора псевдовипадкових коливань (рис.3.6) постійні резистори R_1, R_2, R_3, R_4, R_5, R_6, R_7 були замінені змінними, що забезпечувало налаштування генератора на відповідний тип коливань. В якості конденсаторів C_1, C_2, C_3 та C_4 використовувались багатошарові керамічні конденсатори.

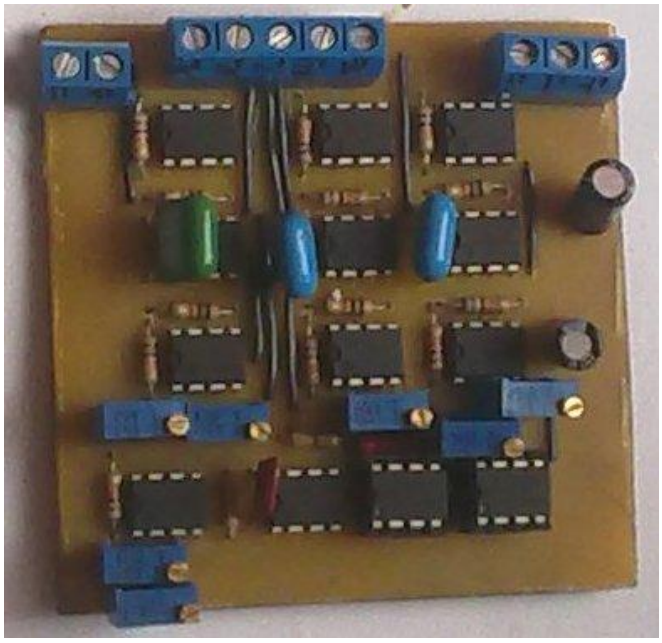


Рис.3.6. Експериментальний зразок генератора хаотичних коливань із двома атракторами

Номінали опорів експериментального зразка генератора мали наступні значення: $R_1 = 4{,}3$ кОм, $R_2 = 1{,}2$ кОм, $R_3 = 100$ кОм, $R_4 = 1$ кОм, $R_5 = 9{,}2$ кОм, $R_6 = 38$ кОм, $R_7 = 9{,}2$ кОм.

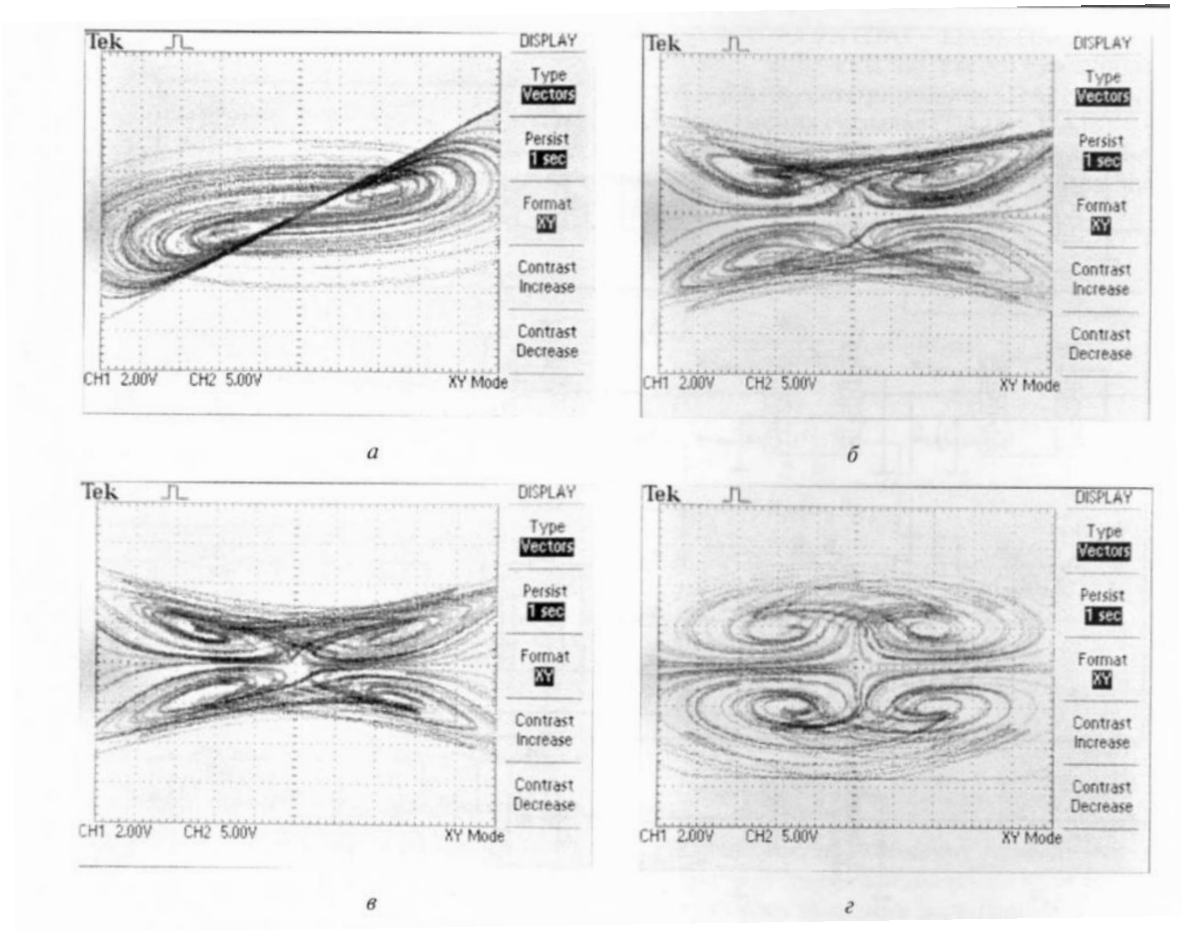


Рис. 3.7. Експериментальні фазові траєкторії системи (3.1) у площинах: – *x*-*y* (а),– *x*-*z* (б), *x*-*w* (в) та *y*-*z* (г)

Різні види коливних процесів забезпечувалися зміною опору R_8. Генерування ХК мали місце при значеннях опору R_8 рівних 2,3 кОм та 4,5 кОм, а періодичних та квазіперіодичних коливань при значеннях опору R_8 рівних 560 Ом та 170 Ом відповідно. Осцилограми фазових траєкторій вище вказаних коливних режимів приведені на рис. 3.7.

Із порівняння рис. 3.4 та рис. 3.7 випливає, що отримані в результаті моделювання та експериментальні фазові траєкторії корелюють між собою.

3.2. Синхронізація псевдовипадкових коливань систем Чуа та фільтрація сигналу в каналі зв'язку

Одним із підходів до вивчення синхронізації псевдовипадкових коливань є класичне поняття фази коливань, або фазова синхронізація. Використання такого підходу передбачає коректне визначення поняття фази для систем, що генерують ХК. Різниця між псевдовипадковими та періодичними коливаннями полягає насамперед у тому, що на відміну від періодичних, ХК мають суцільний спектр подібний до спектру шуму. Тому для ХК неможливо строго визначити поняття періоду (частоти), а отже і фази, що у класичному визначенні є інтегралом частоти по часу [29].

$$\varphi(t) = \int_0^t \omega(\tau) d\tau \qquad (3.5)$$

Розглянемо окремий клас систем, що утворюють багатоспіральні атрактори у фазовому просторі змінних системи з чітким максимумом на деякій частоті ω_0 (вузькосмугові коливання).

Однією із таких систем є генератор Чуа [199], електрична схема якого приведена на рис.3.8.

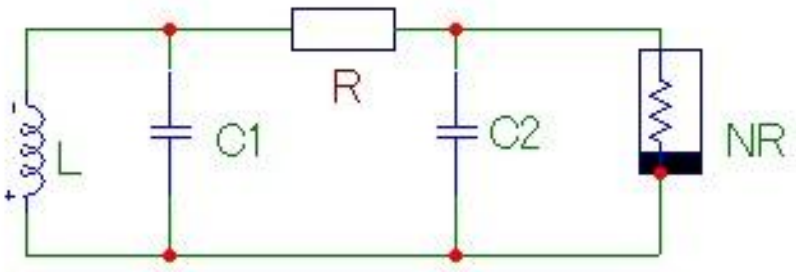


Рис.3.8. Електрична схема генератора Чуа з нелінійним елементом, реалізованим на базі діода: L – індуктивність; C1, C2 – ємності конденсаторів; R – опір резистора, NR – діод Чуа з вольтамепрною характеристикою приведеною на рис.3.9

Електричні елементи кола Чуа на рис. 3.8 мають наступні значення: L=18мГ (R_L=10 Ом), R=1.8 кОм, C2=100нФ, C1=10нФ [200].

Базовим елементом такої схеми є так званий «діод Чуа», з нелінійною характеристикою (рис.3.9), вольтамперна характеристика якого описується виразом (3.6).

$$f(u) = G_b \cdot u + \frac{1}{2} \cdot (G_a - G_b) \cdot (|u + E| - |u - E|), \qquad (3.6)$$

де G_a і G_b – коефіцієнти нахилу лінійних ділянок, розмірністю $[A/B]$, що мають зміст провідності нелінійного елемента при відповідних значеннях напруги, E – абсолютне значення напруги у точках зламу вольтамперної характеристики.

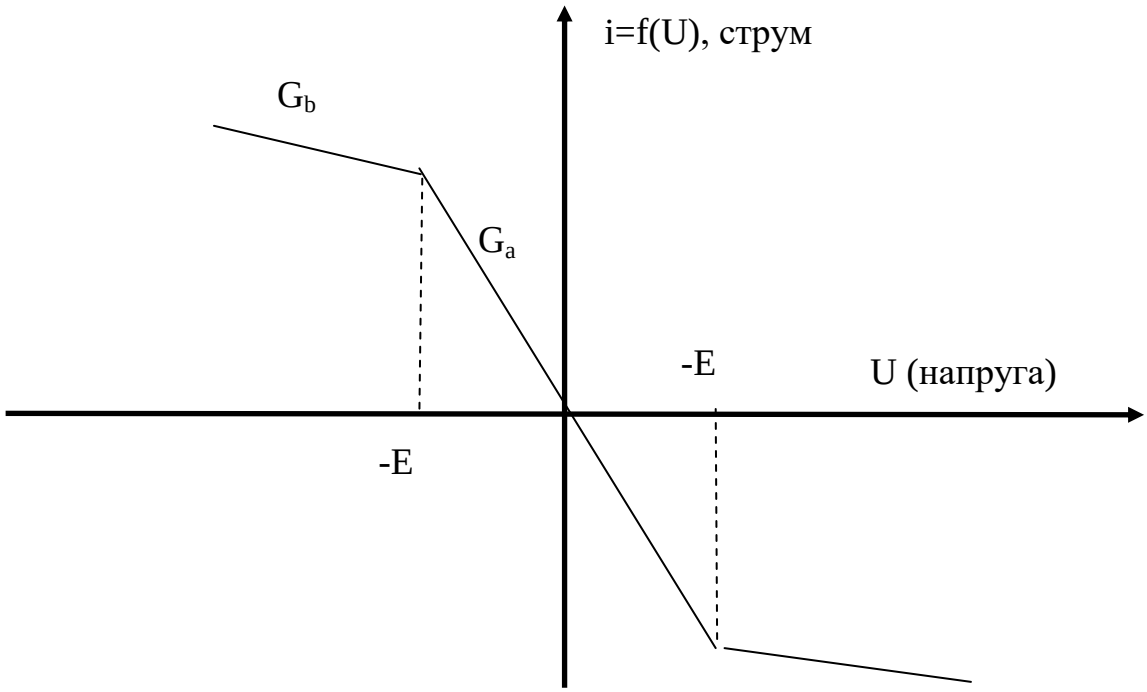


Рис.3.9. Вольтамперна характеристика діода Чуа, де Ga= - 757.58 мікросіменс, Gb= - 409.09 мікросіменс – коефіцієнти нахилу лінійних ділянок характеристики, E=1.075 Вольт – напруга у точці зламу ВАХ) [200]

Використовуючи перший та другий закони Кірхгофа, електричну схему (рис. 3.8) можна описати наступною системою диференційних рівнянь:

$$\begin{cases} L \cdot \dfrac{di}{dt} = -r \cdot i - U \\ C \cdot \dfrac{dU}{dt} = i + \dfrac{V - U}{R} \\ C \cdot \dfrac{dV}{dt} = \dfrac{V - U}{R} - f(V) \end{cases} \qquad (3.7)$$

де i та $f(V)$ – струми, що протікають через котушку індуктивності і нелінійний елемент, L – значення індуктивності котушки, C_1 та C_2 – значення ємностей конденсаторів, R –опір резистора, r – внутрішній опір котушки індуктивності.

Перше рівняння системи (3.9) описує суму напруг на елементах схеми при повному обході контуру (враховано, що спади напруг на котушці індуктивності та конденсаторі C_1 є однаковими і дорівнюють U, а різниця потенціалів на конденсаторі C_2 та нелінійному елементі дорівнює V).

Здійснимо нормування змінних U, V та часу t у системі (3.7) на абсолютну величину напруги у точках зламу вольтамперної характеристики E та сталої затухання контуру $\tau = R \cdot C$:

$$x = V/E,\ y = U/E,\ z = R \cdot i/E,\ t' = t/\tau \qquad (3.8)$$

Тоді система рівнянь кола Чуа записана у безрозмірних величинах, матиме наступний вигляд:

$$\begin{cases} \dot{x} = y - x - f(x) \\ \dot{y} = x - y + z \\ \dot{z} = \alpha \cdot y + \beta \cdot z \end{cases}, (3.9)$$

де: $\alpha = -\dfrac{R^2 \cdot C}{L}$ та $\beta = -\dfrac{r \cdot R \cdot C}{L}$.

Вольтамперна характеристика нелінійного елемента схеми у безрозмірних величинах матиме наступний вигляд:

$$f(U) \to g(x);$$
$$g(x) = m_0 \cdot x + \frac{1}{2} \cdot (m_1 - m_0) \cdot (|x+1| + |x-1|), \qquad (3.10)$$

де $m_0 = G_b \cdot R$, $m_1 = G_a \cdot R$.

Здійснимо моделювання системи передавання інформації вважаючи, що генератори ХК приймача та передавача системи можна описати однаковими рівняннями з різними параметрами α і β, а нелінійні елементи обох систем мають однакові вольтамперні характеристики. Канал зв'язку розглядатимемо як фільтр нижніх частот з відомою частотою зрізу (далі позначатимемо її як безрозмірну величину u), а сигнал, що пройшов через фільтр лінійно підсилюється (безрозмірний коефіцієнт підсилення позначимо через e).

Тоді електрична схема однонаправленого зв'язку синхронізованих генераторів Чуа матиме вигляд, приведений на (рис.3.10)

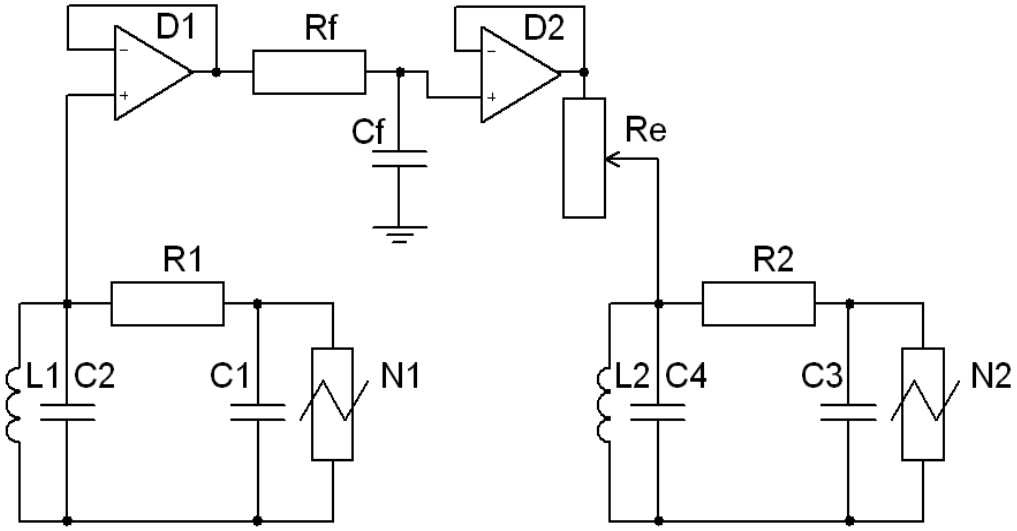


Рис.3.10. Електрична схема однопаправлено зв'язаних через фільтр низьких частот генераторів Чуа, де R1, R2, C1, C2, C3, C4, L1, L2, N1, N2 – номінали компонентів генераторів Чуа, Re =0…100 Ом – опір, що регулює силу зв'язку між генераторами, Rf, Cf – параметри фільтру низьких частот із чатотою зрізу 1 кГц

Системи рівнянь, що описують передавач та приймач СПІ можна записати у наступному вигляді:

Передавач:

$$\begin{cases} \dot{x}_1 = \alpha_1 \cdot \left(y_1 - x_1 - g\left(x_1\right)\right) \\ \dot{y}_1 = x_1 - y_1 + z_1 \\ \dot{z}_1 = -\beta_1 \cdot y_1 \end{cases} \quad (3.11)$$

Приймач:

$$\begin{cases} v = u \cdot \left(y_1 - v \right) \\ \dot{x}_2 = \alpha_2 \cdot \left(y_2 - x_2 - g\left(x_2\right)\right) \\ \dot{y}_2 = x_2 - y_2 + z_2 + e \cdot \left(v - y_2 \right) \\ \dot{z}_2 = -\beta_2 \cdot y_2 \end{cases} \quad (3.12)$$

де x_1, y_1, z_1 — безрозмірні змінні, що відповідають сигналам головної системи (передавач), x_2, y_2, z_2 – змінні, що відповідають сигналам керованої системи (приймач), v – безрозмірний сигнал на виході ФНЧ.

Дослідження процесу синхронізації генераторів Чуа приймальної та передавальної сторін системи здійснювалося при наступних значеннях параметрів: $\alpha_1 = 9$, $\alpha_2 = 9.15$, $\beta_1 = 16$, $\beta_2 = 16.2$.

Функція $g\left(x_i\right)$ описує ВАХ нелінійного елемента генераторів, що з врахуванням вищеприведених припущень має наступний вигляд:

$$g\left(x_i\right) = m_0 \cdot x_i + \frac{1}{2} \cdot \left(m_1 - m_0 \right) \cdot \left[\left| x_i + 1 \right| + \left| x_i - 1 \right| \right], \quad (3.13)$$

де $m_0 = 1.53$, $m_1 = -0.74$, $i = 1,2$ – індекс для головної та веденої систем відповідно.

При вище зазначених значеннях параметрів генератора Чуа траєкторії коливальних процесів у фазовому просторі утворюють спіралеподібний атрактор, ділянки якого розміщені у площинах, що перетинаються під тупим кутом, рівним приблизно 5/6 радіан (рис.3.11) [29].

Генерований сигнал є широкосмуговим, має один чітко виражений максимум на частоті 3 рад/с та 2 максимуми, з амплітудами, що дорівнюють 0,01 максимального значення амплітуди на частоті 0.3 рад/с і 3.8 рад/с (рис. 3.14).

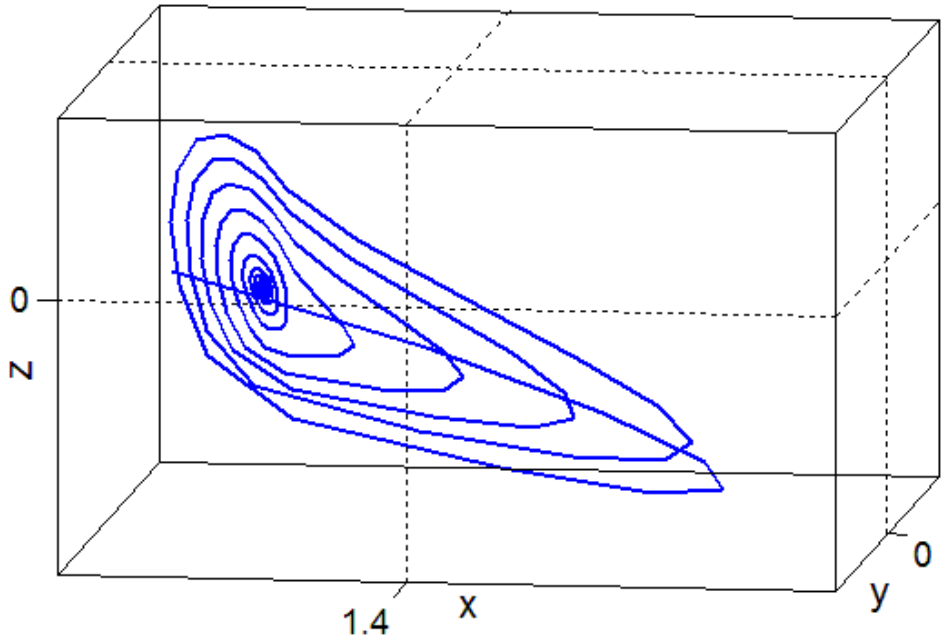


Рис.3.11. Атрактор системи Чуа у тривимірному фазовому просторі

Внаслідок того, що спектр сигналу має чіткий максимум, його фаза може бути визначена наступним чином:

$$\phi = arctg\frac{d\dot{z}}{d\dot{y}} + k \cdot \pi \text{ ,(3.14)}$$

де $k = 1, 2, \ldots$

У випадку близьких значень параметрів головної та веденої систем, їх фазові траєкторії з часом збігатимуться за умови, що обі системи мають стійку до будь-яких трансверсальних збурень атрактора загальну фазову траєкторію [202]. Таким «збуренням» можуть слугувати шуми в каналі зв'язку.

Слід зауважити, що навіть у випадку близьких за значенням параметрів систем, мають місце ступінчаті зриви їх синхронізації (так зване явище «on-off» чергування наявності або відсутності синхронізації систем) [29].

На рис.3.12 приведена розрахункова залежність максимальної амплітуди коливань у веденій системі від коефіцієнту зв'язку між системами та відносної частки зрізу ФНГ, що моделює канал системи.

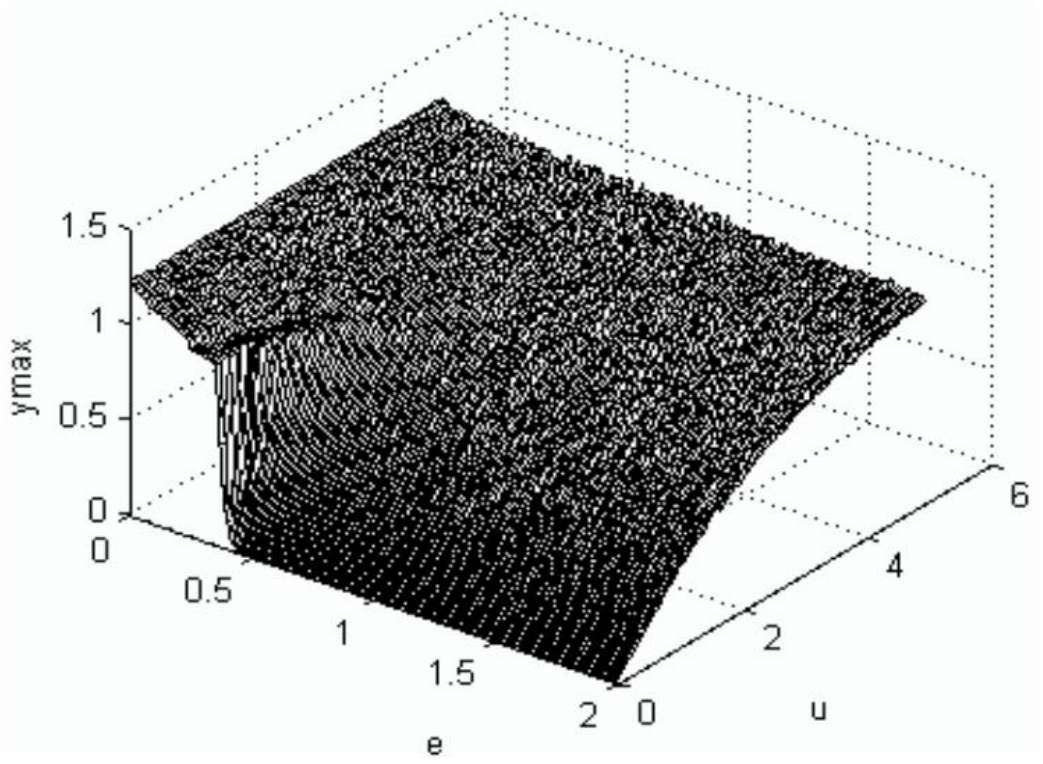
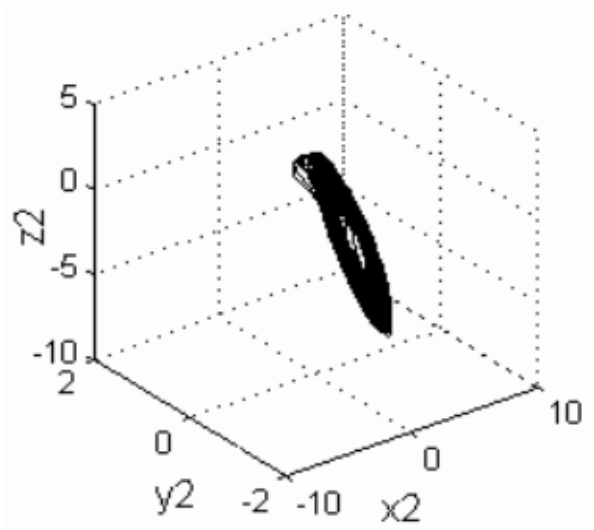
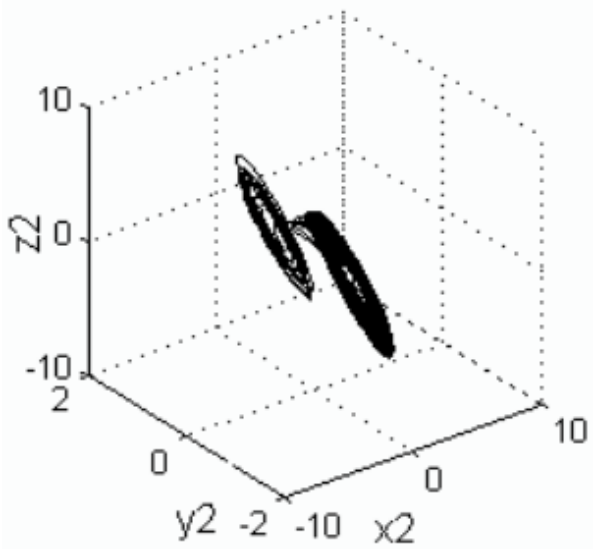


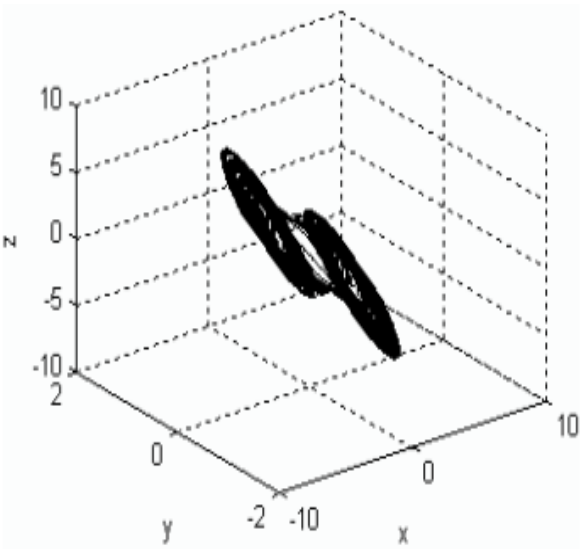
Рис.3.12. Залежність максимальної амплітуди коливань $y_{\max}$ у веденій системі від коефіцієнту зв'язку між системами e та відносної частоти зрізу u ФНГ, що моделює канал системи при $\alpha_1 = 9$

З отриманих результатів випливає, що при значеннях $e > 0.38$ та $u < 4$ має місце суттєва залежність максимальної амплітуди від частоти зрізу фільтра. При цьому генератор приймальної сторони системи може генерувати псевдовипадкові або періодичні коливання, а у фазовому просторі системи формується атрактор типу «стрічка» (рис.3.13а). При зростанні частоти зрізу фільтра u спостерігається виникнення псевдовипадкових коливань, що характеризується перехідною формою атрактора – від стрічки до подвійного завитка (3.13б). При значеннях параметрів $e < 0.38$ та $u > 4$ аналіз результатів моделювання вказує на виникнення псевдовипадкових коливань, що супроводжується виникненням атрактора типу повійний завиток (3.13в). При цьому амплітуда досягає своїх найбільших значень.



а)





б) в)

Рис.3.13. Атрактори генератора Чуа приймальної сторони системи передавання інформації у фазовому просторі при значеннях частоти зрізу u та коефіцієнта зв'язку між генераторами e: $u = 3$, $e = 1$ (а); $u = 4{,}1$, $e = 1$ (б); $u = 3{,}9$, $e = 3{,}9$ (в)

На рис. 3.14 приведений розрахований за часовою реалізацією нормований спектр потужності псевдовипадкового сигналу, генерованого генератором Чуа.

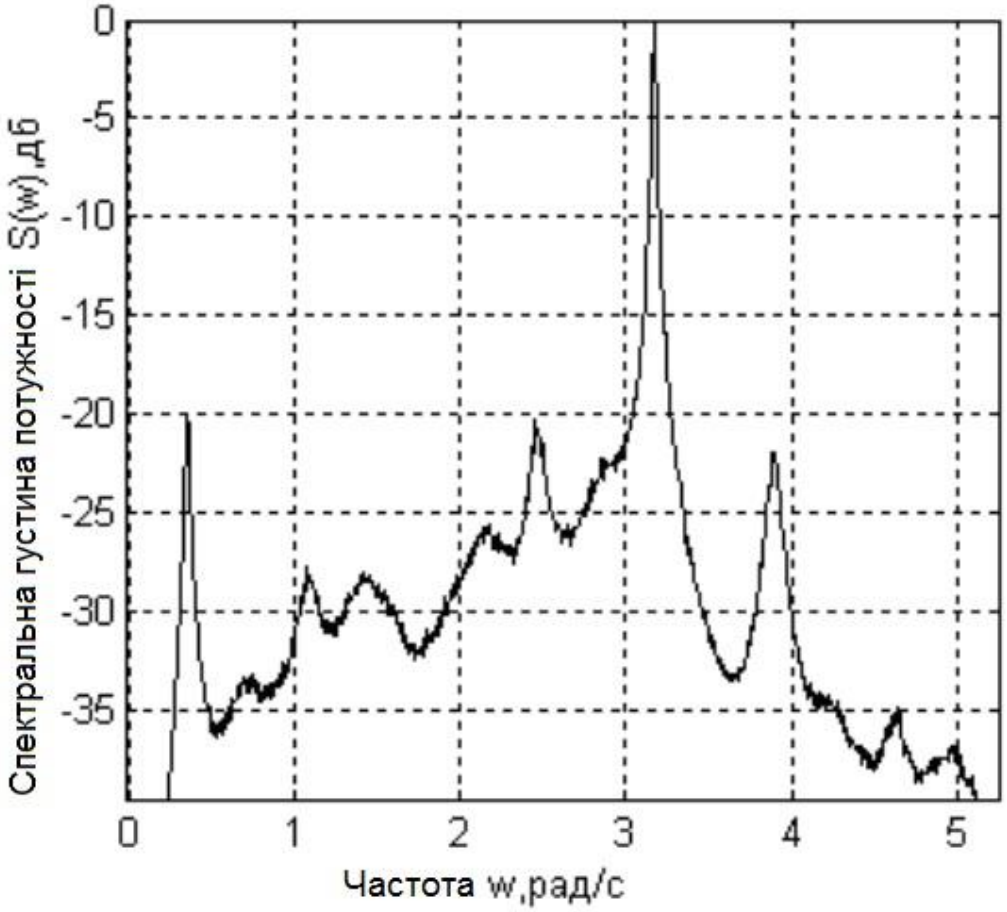


Рис.3.14. Нормований спектр потужності псевдовипадкового сигналу, що генерований електричним колом Чуа

Як бачимо, генерований сигнал є складним та широкосмуговим з максимальним значенням спектральної густини потужність на частоті $3{,}2$ рад/с. Коефіцієнт широкосмуговості сигналу, розрахований за формулою (3.15) приблизно дорівнює 0,9 [203].

$$\eta = \frac{f_u - f_l}{f_u + f_l} \quad (3.15)$$

де f_u, f_l – верхня та нижня частоти смуги сигналу.

Критерієм якості синхронізації приймача та передавача телекомунікаційної системи слугувала помилка синхронізації (3.16), що чисельно дорівнює евклідовій відстані між сигналами, генерованими колами Чуа передавальної та приймальної частин телекомунікаційної системи.

$$\rho = \sqrt{\frac{1}{N} \cdot \sum_{j=1}^{N} \left[\left(x_{1j} - x_{2j} \right)^2 + \left(y_{1j} - y_{2j} \right)^2 + \left(z_{1j} - z_{2j} \right)^2 \right]}, \qquad (3.16)$$

де індексами 1 та 2 позначаються динамічні змінні передавальної та приймальної сторін системи відповідно, N – кількість відліків сигналу, що відповідає часу його спостереження. Помилка синхронізації, що є мірою подібності часових реалізацій генерованих системами, дорівнює нулю у випадку повної синхронізації та відмінна від нуля в інших випадках.

На рис.3.15 приведена залежність помилки синхронізації двох генераторів із близькими за значеннями параметрами ($\alpha_1 = 9$, $\beta_1 = 16$, $\alpha_1 = 9.15$, $\beta_1 = 16.2$) від частоти зрізу фільтра та коефіцієнту зв'язку між ними.

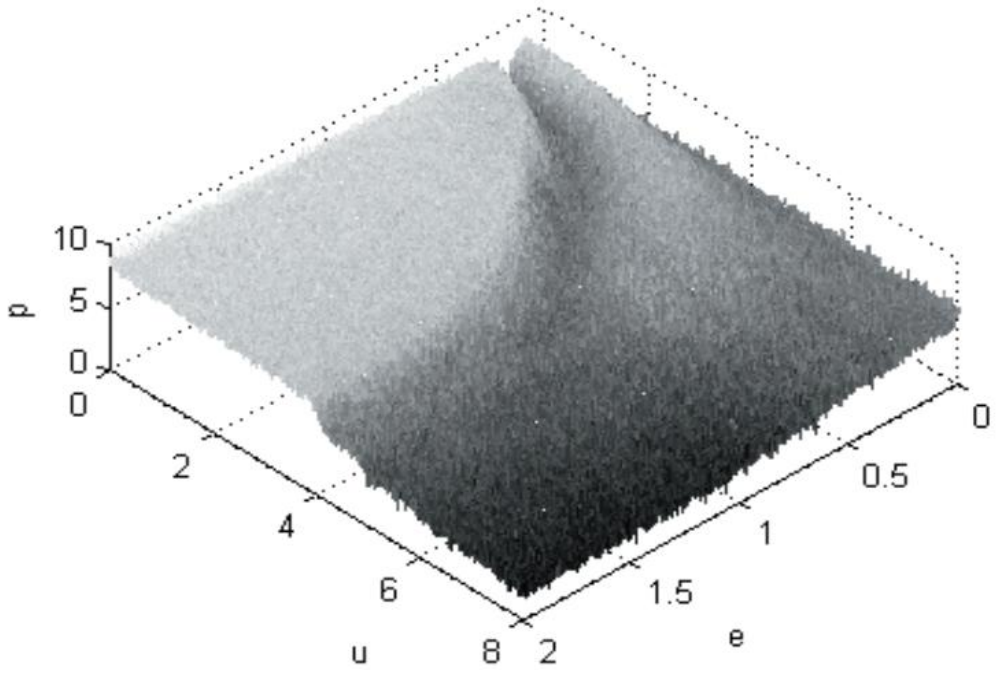


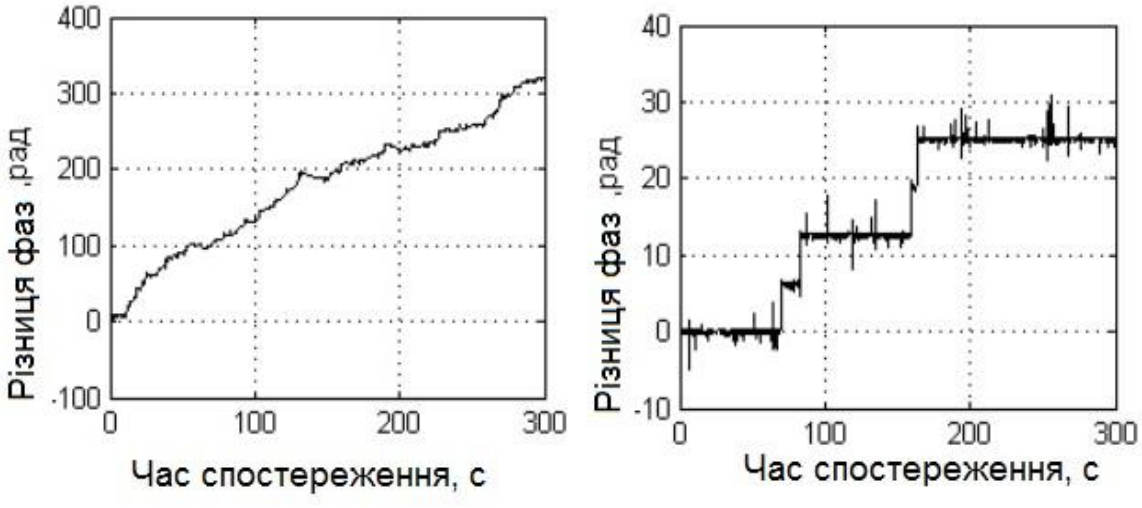
Рис. 3.15. Залежність помилки синхронізації двох генераторів від частоти зрізу та коефіцієнту зв'язку з незначним відхиленням параметрів ($\alpha_1 = 9$, $\beta_1 = 16$, $\alpha_1 = 9.15$, $\beta_1 = 16.2$)

Із приведеної залежності випливає, що на величину помилки синхронізації суттєво впливає частота зрізу фільтра u та коефіцієнту зв'язку e між генераторами. Крім того, правомірно зробити висновок про

відсутність фазової синхронізації між досліджуваними генераторами, що також підтверджено дослідженнями інших авторів [201].

В процесі досліджень нами [29] була розрахована різниця фаз коливань двох генераторів (формула 3.16) при різних значеннях параметрів u та e.

Результати моделювання приведені на рис. 3.16.



а) б)

Рис.3.16. Залежність миттєвої різниці фаз від часу спостереження при e=1, u=2 (а) та e=6, u=10 (б)

Із отриманих результатів можна зробити висновок про те, що при невеликих значеннях коефіцієнту зв'язку та частоти зрізу фільтра має місце повна десинхронізація – миттєва різниця фаз зростає у часі (рис.3.16а). При збільшенні значень вказаних параметрів проміжки часу синхронізації зростають. Отже, за умови фільтрування в каналі повна синхронізація генераторів Чуа приймальної та передавальної сторін системи не може бути досягнута. У такому випадку спостерігатиметься явище **on-off** чергування.

3.3. Дослідження процесів генерування псевдовипадкових коливань у кільцевому генераторі

Нами [22, 29] проведені дослідження режимів генерування псевдовипадкових коливань кільцевим автогенератором, блоки якого

послідовно об’єднуються в схему, що утворює єдине кільце зворотного зв’язку. Однонапрямленість зворотного зв’язку та розв’язка між підсистемами генератора забезпечуються реалізованими на операційних підсилювачах буферними пристроями з великим вхідним та малими вихідними опорами (рис. 3.17).

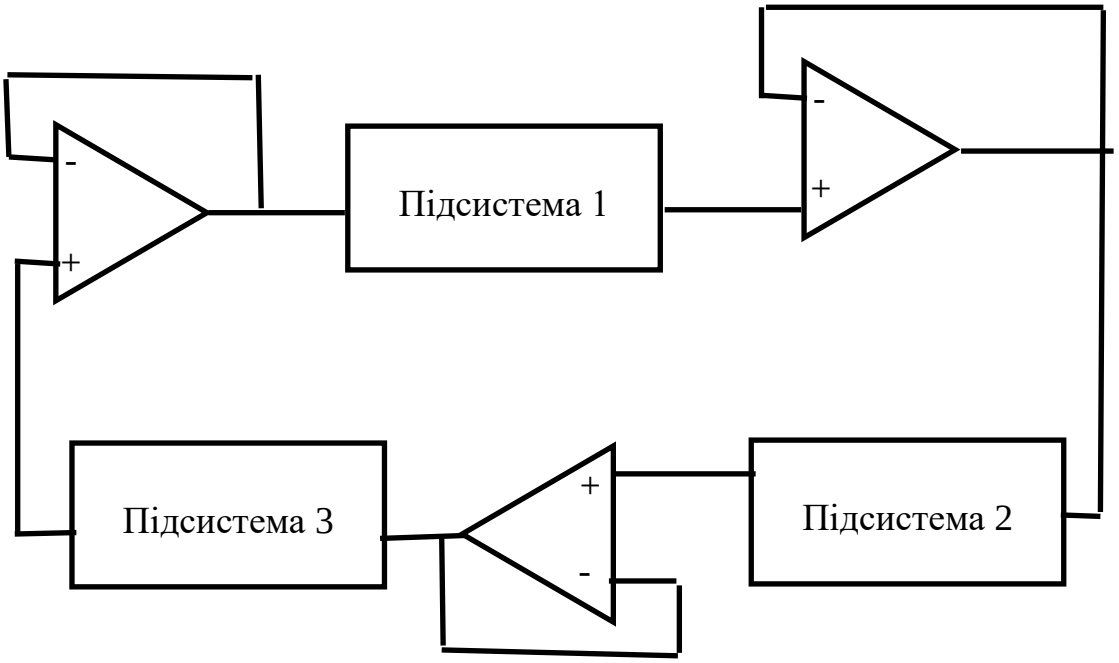
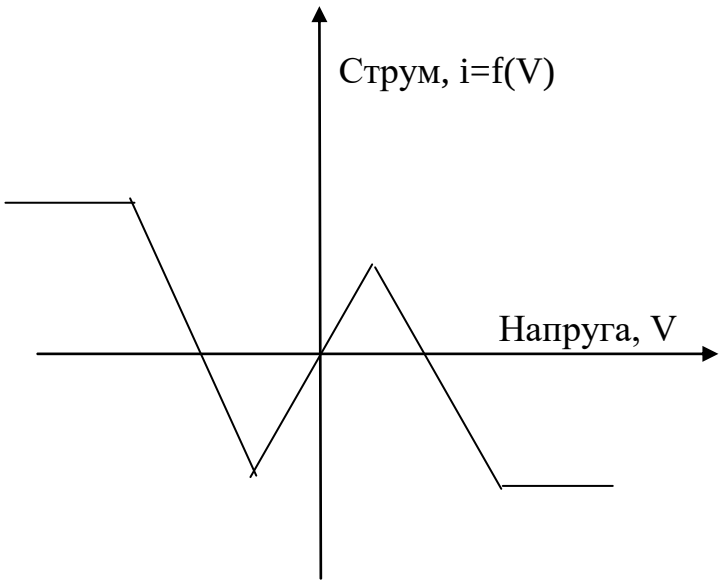


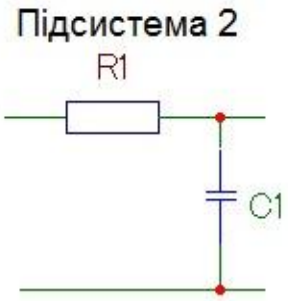
Рис.3.17. Блок-схема кільцевого генератора псевдовипадкових коливань з 1.5 степенями свободи, до складу якого входять 3 підсистеми [202]

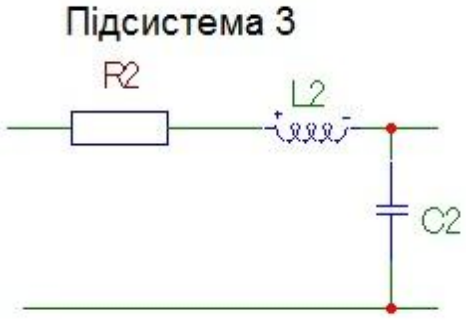
Блок-схема кінцевого генератора псевдовипадкових коливань складається із трьох підсистем, з’єднаних між собою кільцевою схемою. Підсистема 1 є пристроєм нелінійного вольт-вольтного перетворення вхідної напруги, підсистема 2 є фільтром нижніх частот 1-го порядку R_1C_1, а підсистема 3 – фільтром нижніх частот 2-го порядку $R_2L_1C_2$. Характеристика підсистеми 1 та електричні схеми підсистем 2 та 3 приведені на рис. 3.18.

Теоретичні дослідження [201] процесів генерування складної динаміки свідчать про широкі можливості вибору нелінійної характеристики підсистеми 1, що забезпечує виникнення псевдовипадкових коливань у системі.



а)





б) в

Рис.3.18. Характеристика нелінійного елемента (підсистеми 1) (а); та електрична схема підсистеми 2 (б) і підсистеми 3(в) [202]

Динаміка генератора з нелінійною характеристикою (3.17) включає різноманітні режими генерування стійких ХК у широкиму діапазоні значень параметрів генератора.

$$F(z) = M \cdot z \cdot \exp(-z^2), \quad (3.17)$$

де M – коефіцієнт підсилення.

Однак, характеристика, що описується виразом (3.17) є гладкою функцією, внаслідок чого відтворюваність та прецизійність режимів роботи такого генератора ускладнюються. Для забезпечення відтворюваності різноманітних режимів роботи генератора використовувався нелінійний

елемент з п’ятисегментною кусково-лінійною характеристикою, що описується наступним аналітичним виразом [201]:

$$F(z) = M \cdot \left[|z + E_1| - |z - E_1| + \frac{1}{2} \cdot \left(|z - E_2| - |z + E_2| \right) \right], \qquad (3.18)$$

де M – коефіцієнт підсилення, E_1 та E_2 – значення функції $F(z)$ у точках зламу характеристики елемента, що для спрощення розгляду вважатимемо рівними за абсолютною величиною (рис. 3.18а).

Вибір конкретних значень E_1, E_2 та M однозначно визначає характеристику нелінійного елемента.

Схемотехнічна реалізація елемента, що здійснює нелінійні перетворення напруги згідно з (3.18) приведена у наступному пункті.

Динамічні режими генератора можна описати системою диференційних рівнянь, отриманих згідно законам Кірхгофа для підсистем-чотириполюсників 2, 3 (рис.3.18б, в). Позначимо напруги на конденсаторах C_1 та C_2 через U_{C1} та U_{C2} відповідно. Оскільки розглядувана схема є кільцевою, то вихідні сигнали одних підсистем є вхідними сигналами інших. Опишемо зв’язки систем згідно порядку їх вмикання. Вхідним для підсистеми 1 є вихідний сигнал підсистеми 3 (тобто напруга U_{C2} на конденсаторі C_2), вхідним для підсистеми 3 є вихідний сигнал підсистеми 2 (тобто напруга U_{C1} на конденсаторі C_1), вхідним для підсистеми 2 є вихід підсистеми (1) (тобто значення нелінійно перетвореної напруги $F(U_{C2})$)

Підсистема 2 є фільтром нижніх частот першого порядку із вхідною напругою $F(U_{C2})$ та напругою на виході U_{C_1}. Згідно другому закону Кірхгофа зв’язок між напругами U_{C_1} та $F(U_{C2})$ описується наступним рівнянням:

$$C_1 \cdot R_1 \cdot \frac{dU_{C1}}{dt} = F(U_{C2}) - U_{C1} \qquad (3.19)$$

Підсистема (3) є фільтром нижніх частот другого порядку із вхідною напругою U_{C_1} та вихідною U_{C2}. Згідно другому закону Кірхгофа матимемо:

$$L_2 \cdot C_2 \cdot \frac{d^2 U_{C2}}{dt^2} + C_2 \cdot R_2 \cdot \frac{dU_{C2}}{dt} = U_{C1} - U_{C2} \quad (3.20)$$

Таким чином, система диференційних рівнянь, що описує динамічні режими кільцевого генератора матиме наступний вигляд:

$$\begin{cases} C_1 \cdot R_1 \cdot \dfrac{dU_{C1}}{dt} = F\left(U_{C2}\right) - U_{C1} \\ L_2 \cdot C_2 \cdot \dfrac{d^2 U_{C2}}{dt^2} + C_2 \cdot R_2 \cdot \dfrac{dU_{C2}}{dt} = U_{C1} - U_{C2} \end{cases} \quad (3.21)$$

Ввівши позначення $U_{C1} = x$, $z = U_{C2}$, $C_1 \cdot R_1 = T$, $\dfrac{R_2}{L_2} = \alpha$, $\dfrac{1}{\left(L_2 \cdot C_2\right)} = \omega^2$ та нову змінну $y = \dfrac{dU_{C2}}{dt} - \dfrac{R_2 \cdot U_{C2}}{L_2}$, отримаємо:

$$\begin{cases} \dfrac{dx}{dt} = \dfrac{F(z) - x}{T} \\ \dfrac{dy}{dt} = \omega^2 \cdot (x - z), \\ \dfrac{dz}{dt} = y - \alpha \cdot z \end{cases} \quad (3.22)$$

де α, ω, T, M, E_1, E_2 – параметри системи; $F(z)$ – значення функції, що є характеристикою нелінійного елемента в точці z.

Розв'язками системи (3.22) є залежні від часу змінні $x(t)$, $y(t)$ та $z(t)$. Знайдемо нерухомі точки системи (3.22):

$$\begin{cases} \dfrac{dx}{dt} = \dfrac{F(z) - x}{T} = 0 \\ \dfrac{dy}{dt} = \omega^2 \cdot (x - z) = 0 \\ \dfrac{dz}{dt} = y - \alpha \cdot z = 0 \end{cases} \quad (3.23)$$

Першою нерухомою точкою системи є її нулевий розв'язок, що матиме місце при будь-яких значеннях параметрів, і задовільняє другому та третьому

рівнянню системи. При цьому перше рівняння системи зводиться до тотожності:

$$F(0) = M \cdot \left(|E_1| - |-E_1| + \frac{1}{2} \cdot \left[|E_2| - |-E_2| \right] \right) \equiv 0 \qquad (3.24)$$

Систему (3.23) можна записати в наступному вигляді:

$$\begin{cases} F(z) = z \\ x = z \\ y = \alpha \cdot z \end{cases} \qquad (3.25)$$

Вважаючи, що значення функції $F(z)$ в точках зламу E_1 та E_2 є рівними за абсолютною величиною, - що дорівнює $|E_1|=|E_2|=|E\ldots$, та використовуючи явний вигляд $F(z)$, перше рівняння системи можна записати в наступному вигляді:

$$M \cdot \left[|z+E| - |z-E| + \frac{1}{2} \cdot \left(|z-E| - |z+E| \right) \right] = z \qquad (3.26)$$

Розв'яжемо рівняння (3.26) для трьох можливих значень $M<1$, $M=1$, $M>1$, скориставшись графічним методом (рис.3.20). M має зміст коефіцієнта підсилення аналогового сигналу нелінійним елементом.

Як випливає з рис.3.20 рівняння $F(z)=z$ має відмінні від нуля розв'язки лише для $M>1$(точки А, В). Знайдемо розв'язки рівняння (3.25) при умові, що z>0, тобто $z+E>0$; $z-E>0$. При цьому рівняння (3.26) приймає наступний вигляд:

$$M \cdot \left[z+E-z+E+\frac{1}{2} \cdot (z-E-z-E) \right] = z \Rightarrow z = M \cdot E \,. \qquad (3.27)$$

Таким чином розв'язком системи (3.25) є z=ME

Аналогічно при z<0 розв'язком системи (3.25) буде Z= - ME.

Отже, положення рівноваги матиме місце при наступних значеннях змінних системи:

$$\begin{cases} (x,y,z)_1 = (0,0,0) \\ (x,y,z)_{2,3} = \pm M \cdot E \cdot (1,\alpha,1) \end{cases} \qquad (3.28)$$

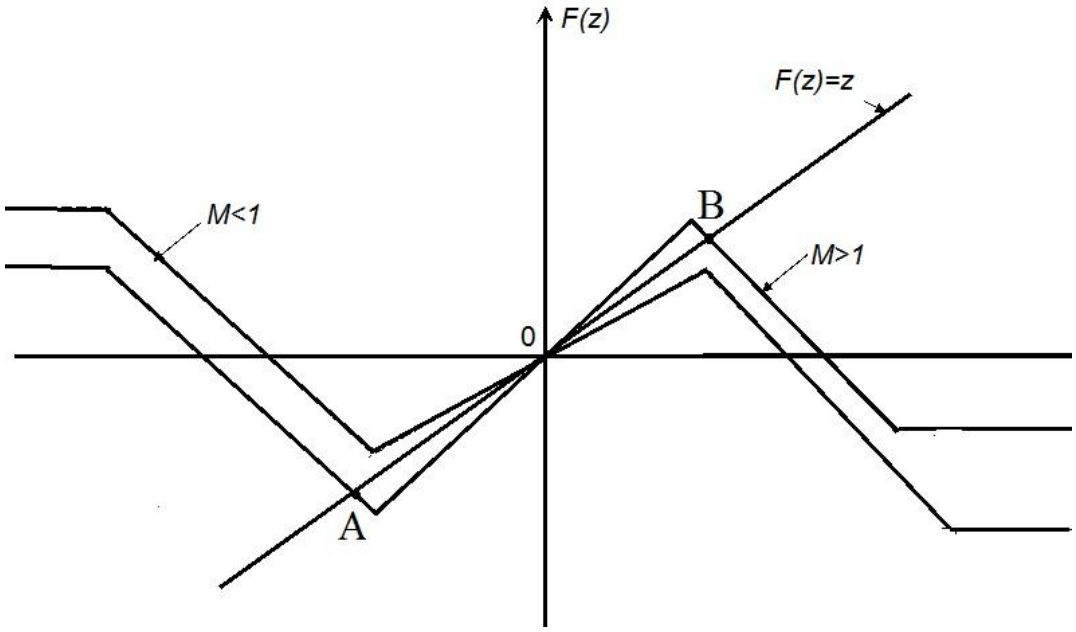


Рис. 3.20. Визначення нерухомих точок системи (3.22) графічним методом. M – параметр системи, що має зміст коефіцієнту підсилення, F(z) – нелінійна характеристика, що описується виразом 3.18

3.4. Дослідження процесів синхронізації псевдовипадкових коливань у кільцевому генераторі

Розклад значень параметрів використовуваних в експериментальних дослідженнях електронних компонентів визначається можливостями технологічного обладнання, що використовується для їх виготовлення. При реалізації генераторів псевдовипадкових коливань, наприклад на сигнальних процесорах, вплив неідентичності елементів може бути зведений до мінімуму. З іншої сторони, оскільки в аналогових конструкціях модулів повне усунення неідентичності елементів неможливе, то вирішення проблеми в такому випадку можливе шляхом зменшення впливу факторів збурення [203].

Оскільки кожен елемент, що входить до складу модуля передавача, потенційно може бути неідентичним по відношенню до свого аналогу в модулі приймача, то загальний підхід до вирішення цієї проблеми полягає у розробленні модулів простої конфігурації з мінімально можливим числом

елементів. Крім того, в різноманітних модулях з приблизно однаковим число елементів важливу роль відіграє їх конкретна структура. На рис.3.21 приведений вплив розкиду параметрів електронних компонентів модулів на якість синхронного відгуку в системах передавання інформації на основі кільцевого генератора з 1,5 степенями свободи (крива 1) та модифікованого кола Чуа (крива 2), принципова електрична схема якого приведена на рис.3.8. Із приведених залежностей випливає, що використання кільцевого генератора при рівних інших умовах дозволяє отримувати більш якісний синхронний відгук у порівнянні з колом Чуа, що обумовлене абсолютною стійкістю відгуку в парі ведуча-ведена система на базі кільцевого генератора [85].

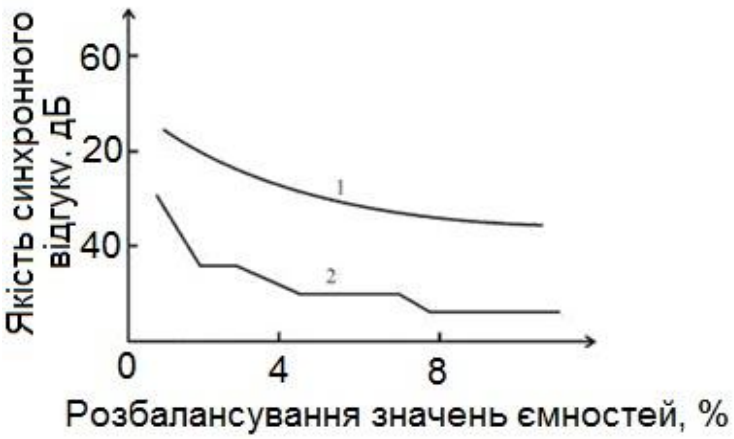


Рис.3.21. Вплив розкиду параметрів електронних компонентів генераторів псевдовипадкових коливань передавача і приймача на якість синхронного відгуку η: 1 –кільцевий генератор з 1,5 степенями свободи; 2 – генератор Чуа [85]

Нами [29] було проведено моделювання синхронізації двох кільцевих автогенераторів із врахуванням фільтрації в каналі зв’язку. Система рівнянь, що описує ведучий та ведений кільцеві автогенератори у безрозмірних змінних має наступний вигляд:

$$\begin{cases} \dot{x}_1 = \left(M \cdot F\left(z_1\right) - x_1\right) \cdot \beta_1 \\ \dot{y}_1 = 4 \cdot \pi^2 f^2 \cdot \left(x_1 - z_1\right) \\ \dot{z}_1 = y_1 - \alpha_1 \cdot z_1 \\ v = u \cdot \left(x_1 - v\right) \\ \dot{x}_2 = \left(M \cdot F\left(z_2\right) - x_2 \cdot \left(1 + e\right) + e \cdot v\right) \cdot \beta_2 \\ \dot{y}_1 = 4 \cdot \pi^2 f^2 \cdot \left(x_2 - z_2\right) \\ \dot{z}_2 = y_2 - \alpha_2 \cdot z_2 \end{cases} \quad (3.29),$$

де α_1; β_2; α_2; β_1 – параметри ведучого та веденого генераторів, x_1, y_1, z_1, x_2, y_2, z_2 – безрозмірні змінні, що відповідають сигналам ведучої та веденої систем відповідно, v – безрозмірна змінна, що описує сигнал на виході ФНЧ, e – параметр, що визначає чисельно силу зв'язку між ведучим та веденим генераторами, u – безрозмірна частота зрізу фільтра.

Для моделювання нами були обрані наступні значення параметрів: $\alpha_1 = 2{,}1$; $\alpha_2 = 2{,}15$; $\beta_1 = 1{,}38$; $\beta_1 = 1{,}39$; $M = 5$. При таких значеннях параметрів атрактори ведучої та веденої систем у 3-вимірному фазовому просторі співпадають (рис.3.22).

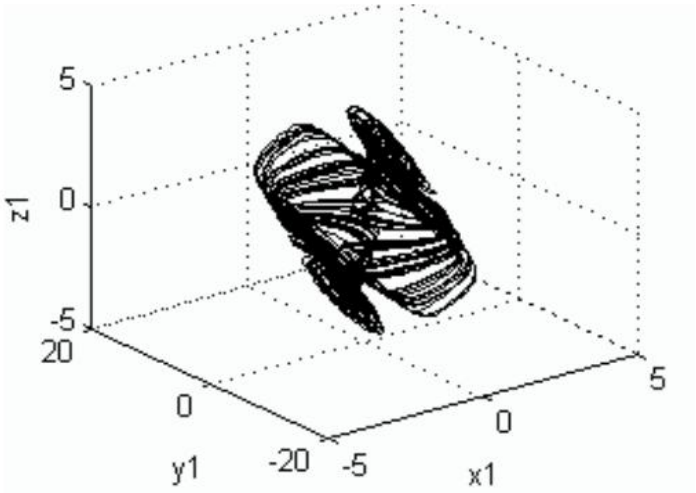


Рис.3.22. Хаотичні атрактори ведучого та веденого кільцевих генераторів у 3-вимірному фазовому просторі при значеннях параметрів ведучого та веденого генераторів $\alpha_1 = 2{,}1$; $\alpha_2 = 2{,}15$; $\beta_1 = 1{,}38$; $\beta_1 = 1{,}39$; $M = 5$

Внаслідок того, що генерований кільцевим автогенератором сигнал має широкосмуговий спектр, поняття фази для нього є нечітким, а визначення

помилки синхронізації можливе використовуючи функцію подібності між однотипними змінними генераторів передавача та приймача. Нормована функція подібності має наступний вигляд [202]:

$$G(\tau)=\sqrt{\frac{\left\langle\left(x_2(t+\tau)-x_1(t)\right)^2\right\rangle}{\left\langle x_1^2(t)\right\rangle\cdot\left\langle x_2^2(t)\right\rangle}} \qquad (3.30)$$

$$k=\min\left(G(\tau)\right)$$

У випадку повної синхронізації $k=0$. При зменшенні коефіцієнта зв'язку та частоти зрізу ФНЧ k зростає, тобто замість повної синхронізації матиме місце лаг-синхронізація. На рис.3.23 приведена залежність мінімального значення функції подібності від коефіцієнта зв'язку e при фіксованих u.

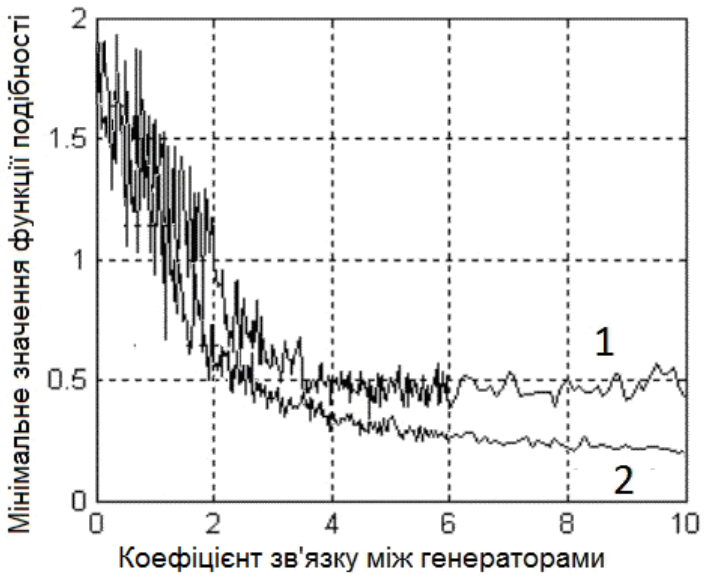


Рис.3.23. Залежність функції подібності від коефіцієнта зв'язку між генераторами для фіксованих значень частоти зрізу ФНЧ: при $u=1$ (1) та при $u=6$ (2).

Із отриманих результатів можна зробити висновок, що при значеннях коефіцієнта зв'язку $e>2$ генератори починають синхронізуватись, а збільшення частоти зрізу призводить до зменшення значення функції подібності.

Для експериментальної реалізації прецизійного кільцевого генератора використовувалася принципова схема приведена у [205].

Із результатів моделювання [84] випливає, що у випадку відмінних параметрів повна синхронізація кільцевих генераторів не спостерігається, а при збільшенні коефіцієнту зв'язку між генераторами має місце лаг-синхронізація.

Приведені на схемі операційні підсилювачі утворюють замкнуте коло зворотного зв'язку, внаслідок чого коливання, що виникають у кожній із підсистем, збуджують синхронізовані коливання у інших підсистемах. Генератор відноситься до класу кільцевих автоколивальних систем, в яких його складові послідовно з'єднуються в схему, що утворює єдине кільце зворотного зв'язку. З'єднання елементів генератора відбувається через буферні пристрої, що забезпечують однонапрямленість зворотного зв'язку генератора та розв'язку між ними.

Моделювання електричної схеми кільцевого генератора здійснювалося у середовищі Multisim 11 (рис.3.24). Принцип роботи нелінійного елемента, що дає можливість створювати кусково-лінійну характеристику, детально описаний у [199].

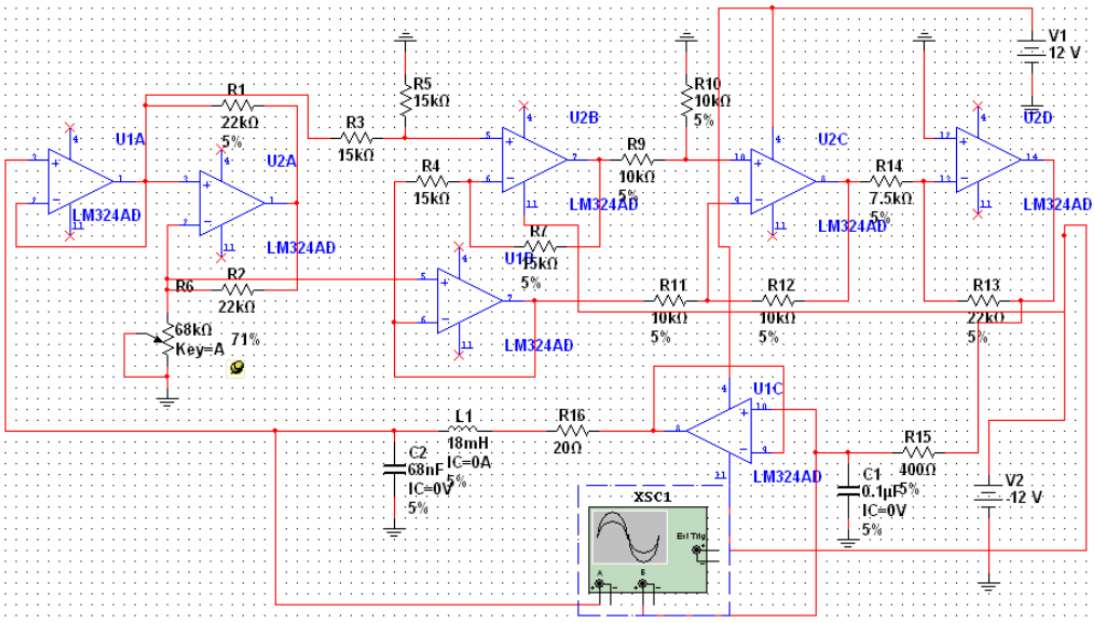


Рис.3.24. Моделювання електричної схеми кільцевого генератора у системі Multisim 11

На рис.3.25 приведений отриманий в результаті моделювання багатовитковий атрактор сигналів кільцевого генератора.

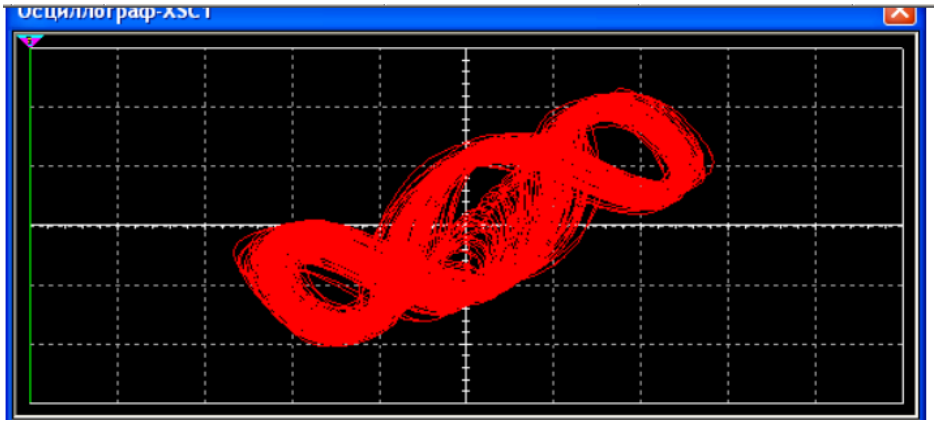


Рис.3.25. Атрактор псевдовипадкових траєкторій кільцевого генератора

Необхідно зазначити, що фазові портрети експериментально отриманих коливань не відповідали результатам моделювання. З метою приведення у відповідність експериментальних результатів з результатами моделювання проводилось додаткове налаштування опорів резисторів у колах зворотного зв'язку електричної схеми генератора (рис. 3.26).

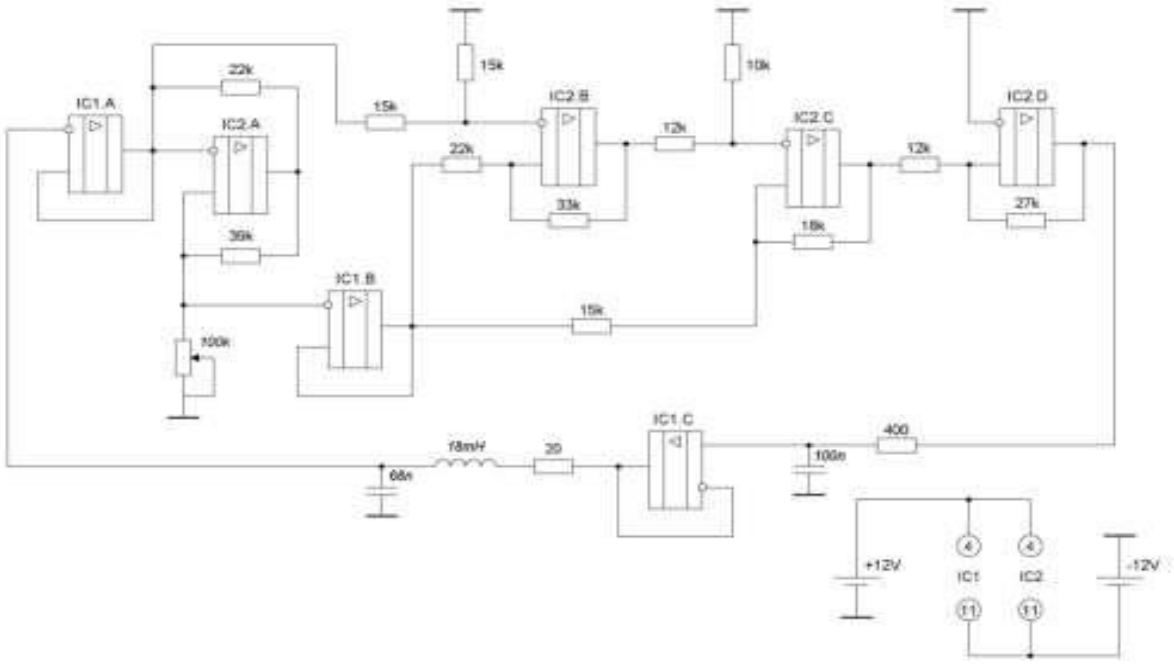
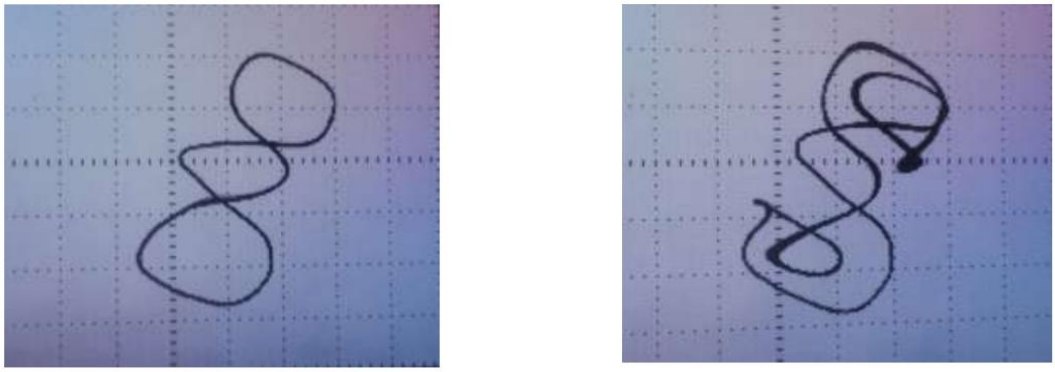


Рис. 3.26. Схема електрична принципова прецизійного генератора псевдовипадкових коливань

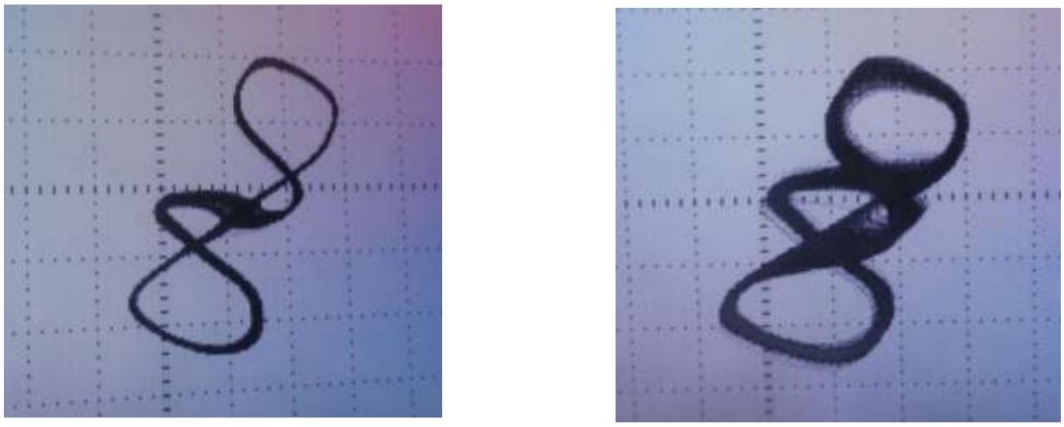
Лабораторний макет кільцевого генератора був виготовлений на базі операційних підсилювачів LM324A з напругою живлення ±12 В. До нелінійного елемента через буферні підсилювачі під'єднані фільтри нижніх частот (підсистеми 2 і 3 на рис.3.17), що утворюють з підсистемою 1 кільцевий генератор.

Зі збільшенням параметру M, що відіграє роль коефіцієнта підсилення у колі оберненого зв'язку, регулярні (періодичні) коливання (рис.3.27) втрачають стійкість і після ряду біфуркацій подвоєння переходять в псевдовипадкові коливання (рис.3.28). При цьому утворений атрактор є подібним до подвійної спіралі (рис.3.29).



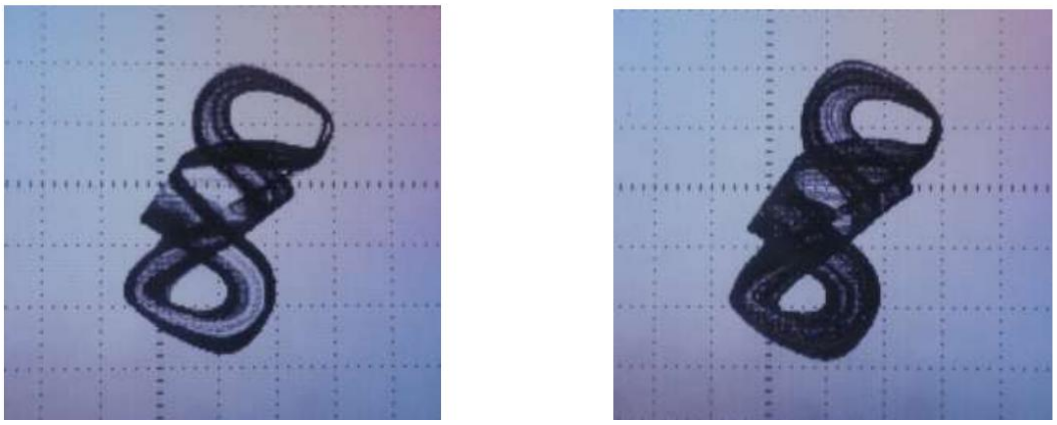
а) б)

Рис.3.27. Періодичний режим коливань у колі зворотного зв'язку при значеннях коефіцієнта підсилення $M = 1{,}1$ (а); $M = 1{,}7$ (б)



а) б)

Рис.3.28. Перехідний режим коливань у колі зворотного зв'язку при значеннях коефіцієнта підсилення: $M = 2{,}2$ (а) та $M = 2{,}9$ (б)



а) б)

Рис.3.29. Хаотичний режим коливань у колі зворотного зв’язку при значеннях коефіцієнта підсилення: $M = 3{,}5$(а) та $M = 5$ (б)

Експериментально показано, що у випадку підбору однакових параметрів усі генератори демонструють ідентичні за структурою та основними характеристиками псевдовипадкові коливання. Заміна операційних підсилювачів LM324A на їх аналоги КР1401УД2Б, та заміна пасивних елементів (в межах вказаної точності) не призводить до значних змін параметрів псевдовипадкових коливань. Результати досліджень, що отримані внаслідок таких замін виявилися ідентичними.

ВИСНОВКИ

1. У програмному середовищі LabView розроблена комп’ютерна модель системи Лю, на основі якої засобами чисельного моделювання досліджені коливні процеси, що можуть мати місце в системі. Показано, що в залежності від значень показників Ляпунова система може генерувати псевдовипадкові коливання із двома та одним атракторами, квазіперіодичні та періодичні коливання.

2. На основі комп’ютерної моделі розроблена принципова електрична схема генератора псевдовипадкових коливань та виготовлений експериментальний зразок генератора з неперервною функцією відображення, що описується системою із чотирьох диференційних рівнянь. Експериментальні дослідження макетних зразків підтверджують результати чисельного моделювання схемотехнічних рішень.

3. Досліджено систему генерування псевдовипадкових коливань, на базі схеми Чуа. Встановлено вплив коефіцієнта зв’язку між генераторами та частоти зрізу фільтра на процес синхронізації генераторів. В залежності від їх значень у веденій системі матимуть місце періодичні або псевдовипадкові коливання. За умови фільтрації сигналів у каналі зв’язку повна синхронізація між генераторами передавальної та приймальної сторін схеми Чуа неможлива навіть при незначній відмінності їх параметрів. При цьому має місце явище **on-off** чергування. У випадку невеликих значень коефіцієнта зв’язку та частоти зрізу фільтра має місце повна десинхронізація – миттєва різниця фаз лінійно зростає з часом. При збільшенні значень вказаних параметрів тривалість проміжків часу синхронізації зростатимуть.

4. Розроблено аналітичну модель кільцевого генератора та встановлена можливість генерування псевдовипадкових, перехідних та періодичних коливань у залежності від коефіцієнту підсилення у колі оберненого зв’язку, що підтверджено дослідженнями експериментального зразка генератора. Спектр генерованих псевдвоипадкових коливань є широкосмуговим з

достатньо рівномірним розподілом по частоті, внаслідок чого використання поняття фази при дослідженні процесів синхронізації кільцевих автогенераторів є неможливим. При аналізі коливних процесів доцільно використовувати функцію подібності однотипних змінних систем.

5. Встановлено, що синхронізація кільцевих автогенераторів має місце, якщо коефіцієнт зв’язку між генераторами e>2. Ця закономірність зберігається у широкому діапазоні частот зрізу ФНЧ. Збільшення частоти зрізу ФНЧ обумовлює зменшення значення функції взаємної кореляції до нуля. При цьому має місце повна синхронізація генераторів. При зменшенні зв’язку між кільцевими генераторами та частоти зрізу ФНЧ значення функції подібності збільшується, що обумовлює встановлення в системі лаг-синхронізації.

РОЗДІЛ 4. МОДЕЛЮВАННЯ ТА ДОСЛІДЖЕННЯ СИСТЕМ ПЕРЕДАВАННЯ ІНФОРМАЦІЇ НА БАЗІ ГЕНЕРАТОРІВ ХАОТИЧНИХ КОЛИВАНЬ З НЕПЕРЕРВНОЮ ФУНКЦІЄЮ ВІДОБРАЖЕННЯ

Протягом останніх двадцяти років були розвинуті три базові методики передавання інформації з використанням псевдовипадкових коливань — перемикання між генераторами псевдовипадкових коливань, додавання інформаційного сигналу до псевдовипадкового та модуляція хаотичним сигналом [84, 204]. У даному розділі приведені експериментальні дослідження та результати моделювання системи, що використовує перемикання між генераторами Лоренца із відмінними параметрами та системи на базі генераторів Лю із додаванням інформаційного та псевдовипадкового сигналу та кільцевих генераторів з підмішуванням інформаційного сигналу до хаотичної несучої.

4.1. Системи передавання інформації з маскуванням псевдовипадковим сигналом на базі генераторів Лю

Проведені дослідження впливу параметрів системи Лю на характер її динаміки і за отриманими результатами експериментально реалізований та досліджений макет схеми передавання інформації з маскуванням псевдовипадковим сигналом.

Дослідження хаотичних систем з метою виявлення та аналізу різних режимів синхронізації зручно проводити за співвідношенням дійсних частин показників Ляпунова, що приводяться у табл. 4.1 у випадку якщо розмірність веденої системи дорівнює 3.

На границі областей параметрів, при яких мають місце ті або інші співвідношення між дійсними частинами показників Ляпунова, що обумовлюють вказані у таблиці 4.1 основні види синхронізації, можуть існувати проміжні типи синхронного відгуку ведучої та веденої систем (*on-*

off-перемішування, нестійка узагальнена, нестійка фазова та інші види синхронізації).

Таблиця 4.1.

Співвідношення між дійсними частинами показників Ляпунова та видами синхронізації хаосу

Вид синхронізації хаосу	**Співвідношення дійсних частин показників Ляпунова**	**Примітка**
Повна	$\mathrm{Re}[\lambda_{1,2,3}]<0$	Синхронізація ідентичних хаотичних систем
Протифазна	$\mathrm{Re}[\lambda_{1,2,3}]<0$	Синхронізація дифузійно з'єднаних ідентичних хаотичних систем
Лаг	$\mathrm{Re}[\lambda_{1,2,3}]<0$	Синхронізація незначно розлаштованих хаотичних систем
Узагальнена	$\mathrm{Re}[\lambda_1]\approx 0$, $\mathrm{Re}[\lambda_{2,3}]<0$	Синхронізація ідентичних, систем із незначно розлаштованими параметрами та структурно різних хаотичних систем
Фазова	$\mathrm{Re}[\lambda_1]\geq 0$, $\mathrm{Re}[\lambda_{2,3}]<0$	Синхронізація фазокогерентних хаотичних систем (систем зі спіральним атрактором)
Синхронізація масштабів часу (спектральних складових)	$\mathrm{Re}[\lambda_{1,2,3}]<0$	Синхронізація довільних хаотичних систем (синхронізація окремих складових Фур'є-спектру)

Система Лю [201] є системою чотирьох нелінійних диференційних рівнянь першого порядку:

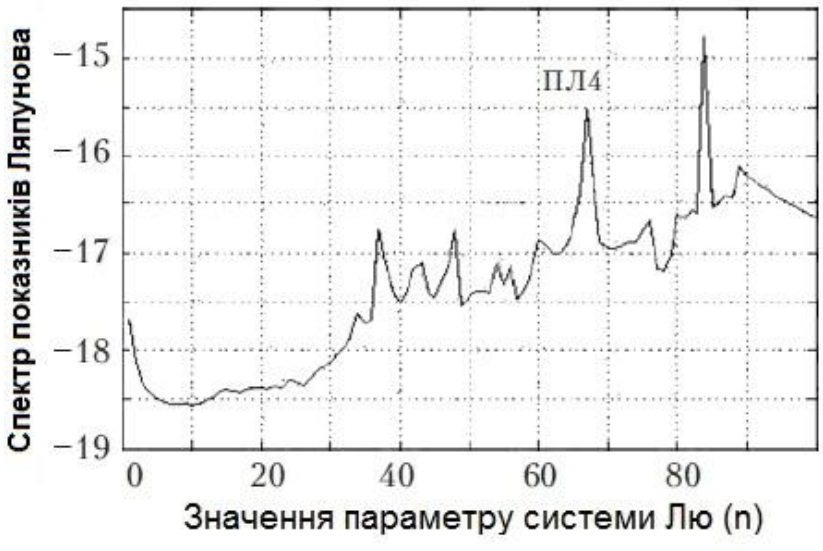
$$\begin{cases} \dot{x} = a \cdot (y - x) \\ \dot{y} = b \cdot x - h \cdot x \cdot z + \lambda \cdot w \\ \dot{z} = c \cdot x^2 - d \cdot z \\ \dot{w} = -n \cdot y \end{cases}, \qquad (4.1)$$

де x, y, z, w – змінні системи, a, b, h, λ, c, d та n – її параметри.

Дослідження спектру показників Ляпунова системи дає можливість встановити діапазони значень параметрів системи, при яких генеруються ХК з двома та одним атрактором, квазіперіодичні та періодичні коливання [14, 21].

На рис.4.1 приведені результати аналітичного розрахунку залежності дійсних частин показників Ляпунова системи Лю, що характеризують швидкість збігання або розходження її траєкторій у фазовому просторі в залежності від значень параметра n, що змінювався у межах 1…100.

а)



б)

Рис.4.1. Залежність дійсних частин показників Ляпунова системи Лю від параметру n при значеннях параметрів $a=15$, $b=30$, $h=1$, $\lambda=1$, $c=4$, $d=2{,}5$: (а) – ПЛ1, ПЛ2, ПЛ3 – три старші показники; (б) – ПЛ4 (четвертий показник)

Зокрема, генерування псевдовипадкових коливань, що можуть використовуватися для маскування інформаційних сигналів, мають місце при значеннях $n \in (38;42] \cup (48;57]$.

Головну і керовану системи Лю можна описати системами нелінійних диференційних рівнянь з квадратичною нелінійністю:

$$\begin{cases} \dot{x}_t = a \cdot (y_t - x_t) \\ \dot{y}_t = b \cdot x_t - h \cdot x_t \cdot z_t + \lambda \cdot w_t \\ \dot{z}_t = c \cdot x_t^2 - d \cdot z_t \\ \dot{w}_t = -n \cdot y_t \end{cases} \quad (4.2)$$

$$\begin{cases} \dot{x}_r = a \cdot (y_r - x_r) \\ \dot{y}_r = b \cdot x_r - h \cdot x_r \cdot z_r + \lambda \cdot w_r + e \cdot (y_t - y_r) \\ \dot{z}_r = c \cdot x_r^2 - d \cdot z_r \\ \dot{w}_r = -n \cdot y_r \end{cases} \quad (4.3)$$

де $y_t - y_r$ – помилка синхронізації головної та керованої систем.

Головна та керована системи формують псевдовипадкові сигнали $x_t(t)$, $y_t(t)$, $z_t(t)$, $w_t(t)$ та $x_r(t)$, $y_r(t)$, $z_r(t)$, $w_r(t)$ відповідно. Для прикладу розглянемо процес синхронізації сигналів $y_t(t)$ та $y_r(t)$ головної та керованої систем, використовуючи програмне середовище Micro-Cap 9.

Синхронізація генераторів псевдовипадкових коливань, що базується на розв'язках системи Лю, здійснювалась за схемою з лінійним зворотнім зв'язком (рис.4.2).

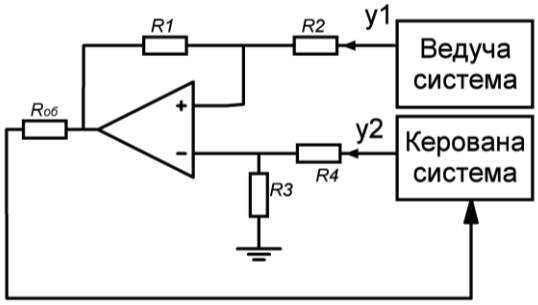
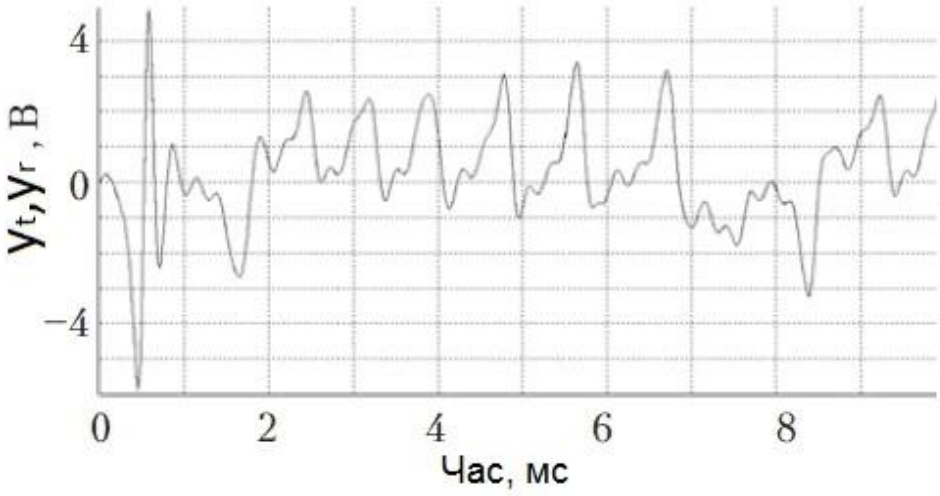


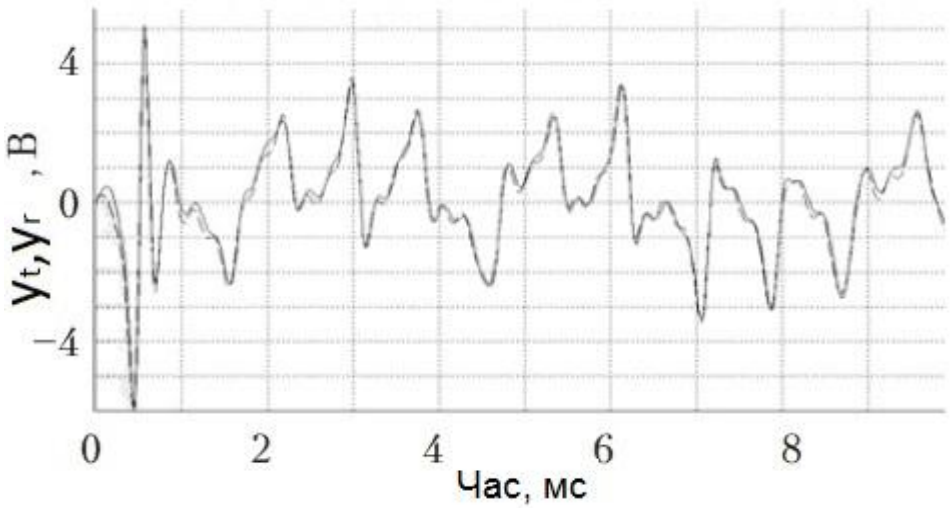
Рис.4.2. Функціональна схема синхронізації двох генераторів Лю, де y1, y2 – сигнали генераторів ХК; R1, R2, R3, R4 – опори номіналом 10 кОм, Rоб – змінюваний опір, що регулює коефіцієнт оберненого зв'язку номіналом від 100 Ом до 3 кОм

Номінальні значення резисторів R_1, R_2, R_3 та R_4 становили 10 кОм. Регулювання глибини зворотнього зв'язку між системами здійснювалася зміною сигналу $R_{об}$.

Оцінка ступеня корельованості між сигналами $y_t(t)$ та $y_r(t)$, що отримані при різних значеннях $R_{об}$, проводилась за часовими діаграмами (рис.4.3) та залежностями між амплітудами сигналів $y_t(t)$ і $y_r(t)$ (рис.4.4).

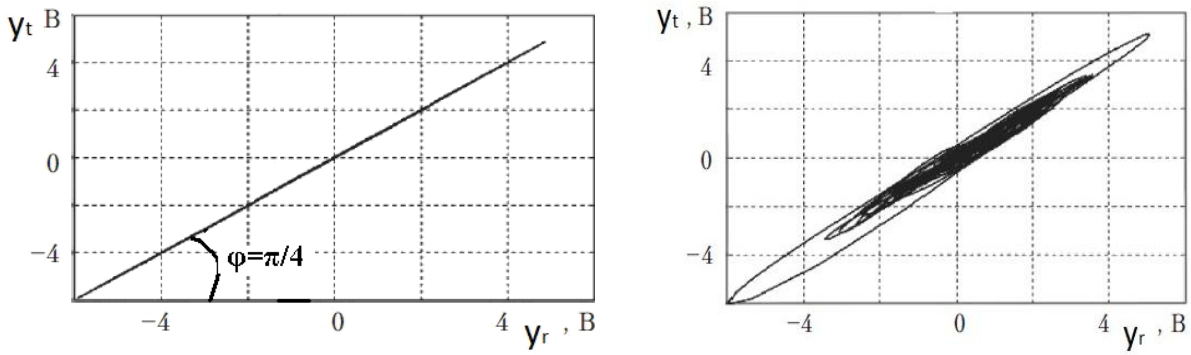


а)



б)

Рис.4.3. Часові діаграми псевдовипадкових сигналів приймача $y_r(t)$ та передавача $y_t(t)$ при різних значеннях опору у колі оберненого зв'язку $R_{об}=100\ Ом$ (а) та– $R_{об}=3kОм$ (б)

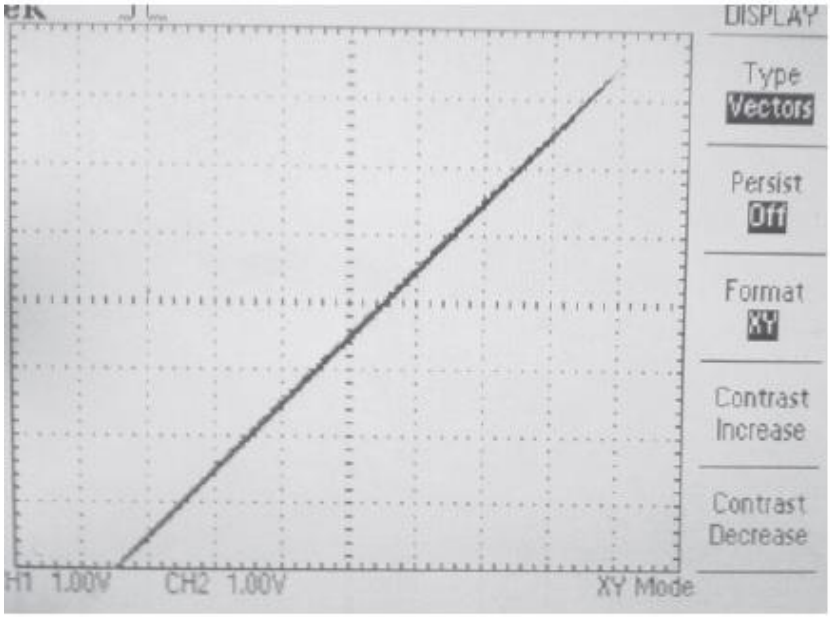


а) б)

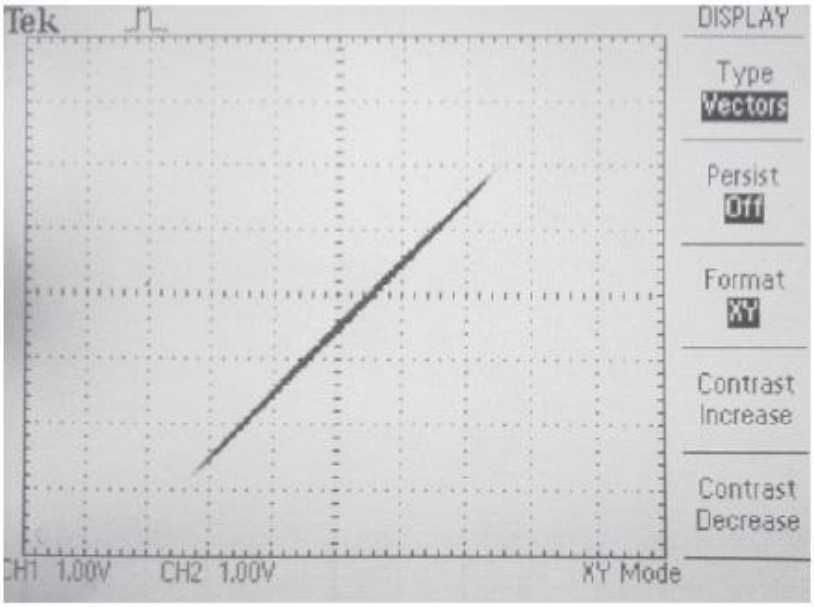
Рис.4.4. Залежності амплітуди сигналів $y_t(t)$ від $y_r(t)$ для досліджуваних генераторів системи передавання інформації при значеннях опору у колі оберненого зв'язку $R_{об}=100\ Ом$ (а) та $R_{об}=3kОм$ (б)

Із залежностей амплітуд сигналів $y_t(t)$ від $y_r(t)$ випливає, що при $R_{об}=100\ Ом$ залежність $y_t(t)$ від $y_r(t)$ є прямолінійною з кутом нахилу $\varphi=\pi/4$, що вказує на синхронну роботу генераторів приймальної та передавальної сторін систем (рис.4.4а). Подальше зростання опору $R_{об}$ призводить до повної десинхронізації генераторів (рис.4.4б).

Із експериментальних залежностей $x_t = f(x_r)$ та $y_t = f(y_r)$ (рис.4.5) випливає, що при встановленні синхронізації сигналів $y_r(t)$ та $y_t(t)$ матиме місце синхронізація сигналів $x_r(t)$ та $x_t(t)$.



а)



б)

Рис.4.5. Експериментальні дослідження синхронізації сигналів при $R_{об}$=100 Ом, що відповідають змінним x(а) та y(б)

Забезпечення синхронної роботи приймальної та передавальної сторін системи уможливлює маскування та передавання інформаційних повідомлень.

На рис.4.6 приведена структурна схема передавання інформації, що використовує генератори псевдовипадкових коливань на основі системи Лю.

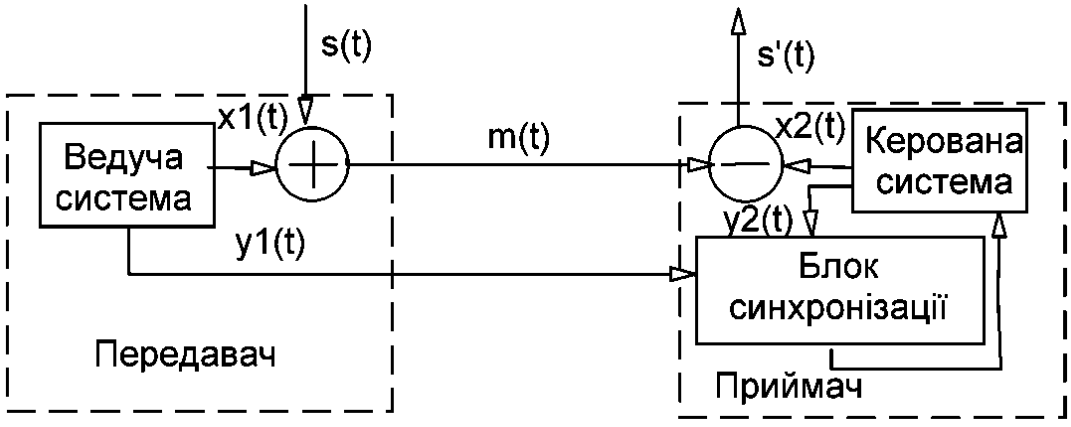
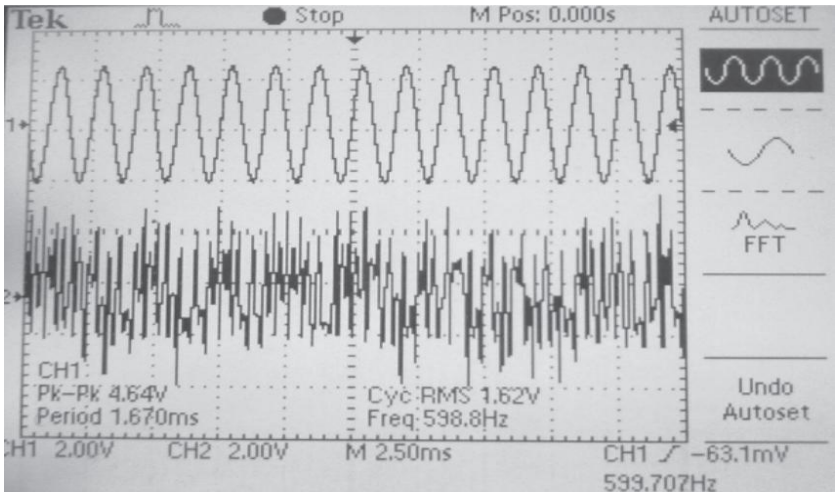
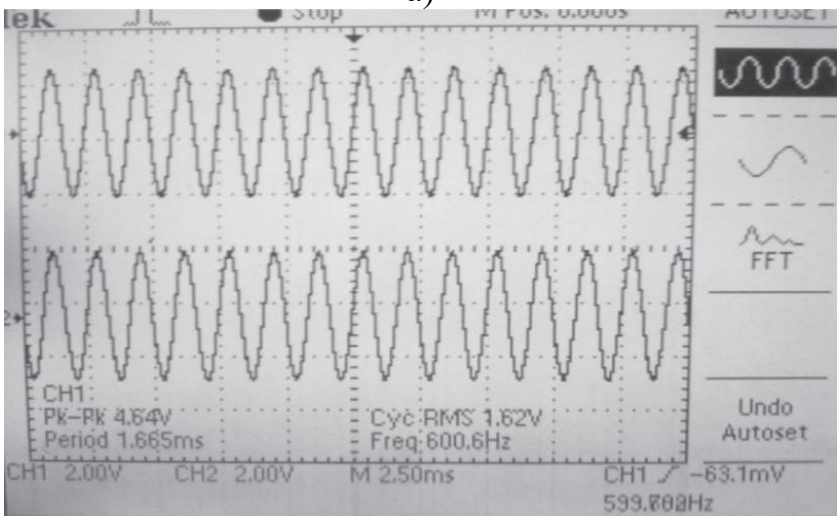


Рис.4.6. Структурна схема передавання інформації з маскуванням псевдовипадковим сигналом (s(t), s'(t) – передане та отримане інформаційні повідомлення, x1(t), y1(t) – ХК ведучої системи, x2(t), y2(t) – ХК керованої системи)

При маскуванні псевдовипадковим сигналом, що є одним з найпростіших способів прихованого передавання інформації, інформаційний сигнал доданий до псевдовипадкового у суматорі передавача передається у канал зв'язку. Синхронізація систем зв’язку забезпечується встановленням однакових псевдовипадкових коливань, генерованих генераторами приймальної та передавальної частин системи зв’язку. На приймальній стороні відбувається дешифрування інформаційного сигналу шляхом віднімання від прийнятого зашифрованого повідомлення сигналу, генерованого генератором приймальної сторони.



а)



б)

Рис 4.7. Експериментальні часові діаграми вхідного інформаційного та псевдовипадкового сигналів (а) та інформаційний сигнал на вході і виході системи (б)

Експериментальні результати тестування макету системи передавання інформації з використанням генераторів псевдовипадкових коливань здійснювалися шляхом передавання синусоїдального сигналу частотою $f = 600 Гц$ з амплітудою $A = 1{,}6 B$ (рис. 4.7).

Із отриманих результатів можна зробити висновок, що генеровані системою Лю псевдовипадкові сигнали можна використовувати у системах передавання інформації шляхом їх додавання до інформаційного сигналу.

4.2. Моделювання системи передавання інформації на базі псевдовипадкових сигналів, генерованих системою Лоренца

Нами [24] проведене моделювання телекомунікаційної системи (рис.4.8) передавання інформації (рис.4.7) з використанням перемикання псевдовипадкових режимів (CSK – chaos shift keying) генераторів передавальної сторони, що описуються системою Лоренца.

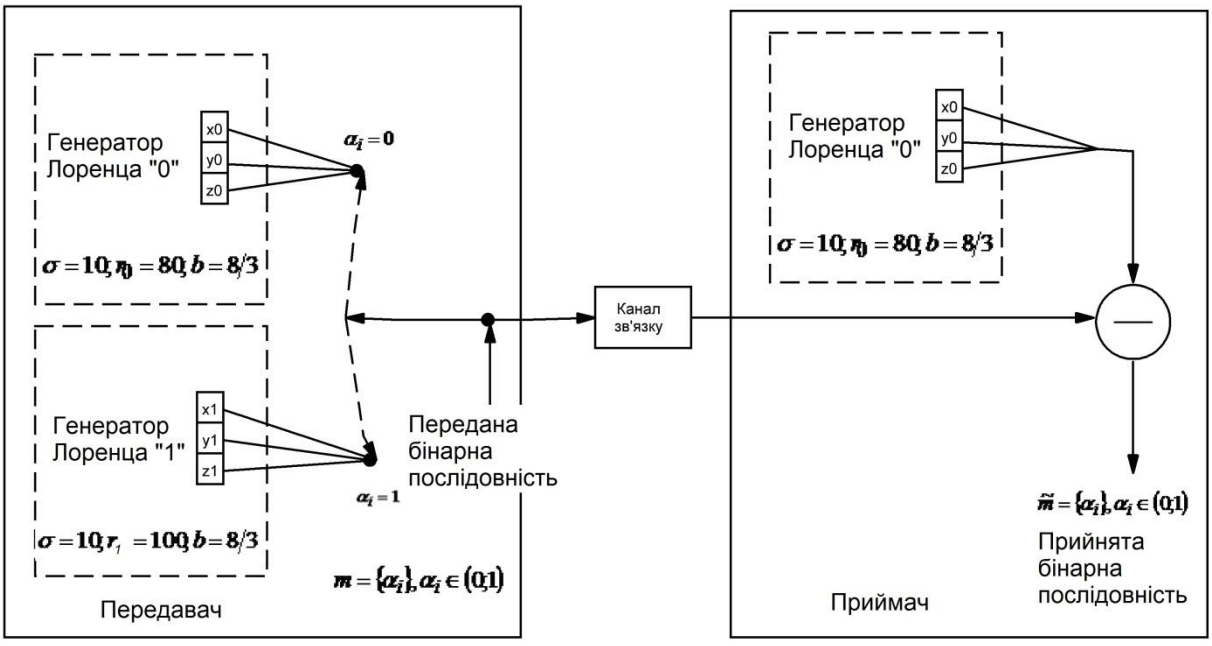


Рис. 4.8. Система передавання інформації із ключуванням, x_0, y_0, z_0 – змінні генератора Лоренца «0», x_1, y_1, z_1 – змінні генератора Лоренца «1», σ, r, b – параметри генераторів Лоренца, α_0, α_1 – двійкові символи, m, ḿ – передане та отримане інформаційне повідомлення

Розглянемо особливості, притаманні процесам синхронізації та передавання інформації, що відбуваються у досліджуваній системі. У порівнянні із хаотичним маскуванням маскування CSK-системою є більш завадостійким, оскільки наша система передавання даних містить два генератори хаотичних сигналів з різними параметрами, внаслідок чого в системі має місце **on-off** чергування (періодичні зриви синхронізації) [201].

Неперервні функції відображення генераторів передавальної та приймальної сторін системи описуються диференційними рівняннями Лоренца (4.4) та (4.5) відповідно:

$$\begin{cases} \dot{x}_0 = \sigma \cdot (y_0 - x_0) \\ \dot{y}_0 = r_0 \cdot x_0 - y_0 - x_0 \cdot z_0 \\ \dot{z}_0 = x_0 \cdot y_0 - b \cdot z_0 \end{cases} \quad (4.4)$$

$$\begin{cases} \dot{x}_1 = \sigma \cdot (y_1 - x_1) \\ \dot{y}_1 = r_1 \cdot x_1 - y_1 - x_1 \cdot z_1 \\ \dot{z}_1 = x_1 \cdot y_1 - b \cdot z_1 \end{cases} \quad (4.5)$$

Приведені системи відрізняються значеннями параметра r генераторів передавальної та приймальної сторін.

В основу функціонування системи покладено явище синхронізації генераторів Лоренца, що має місце за умови однакових значень параметрів генераторів приймальної та передавальної сторін системи [204], внаслідок чого різниця між значеннями сигналів, генерованих ними, з часом прямує до нуля. При різних значеннях параметрів генераторів встановлення синхронізації неможливе.

Слід зауважити, що шумоподібність генерованих сигналів забезпечує додаткову захищеність системи передавання інформації. Система Лоренца генерує хаотичні коливання при значеннях параметра r, що належать діапазону $25 < r < 120$, і фіксованих $\sigma = 10, b = 8/3$ [57].

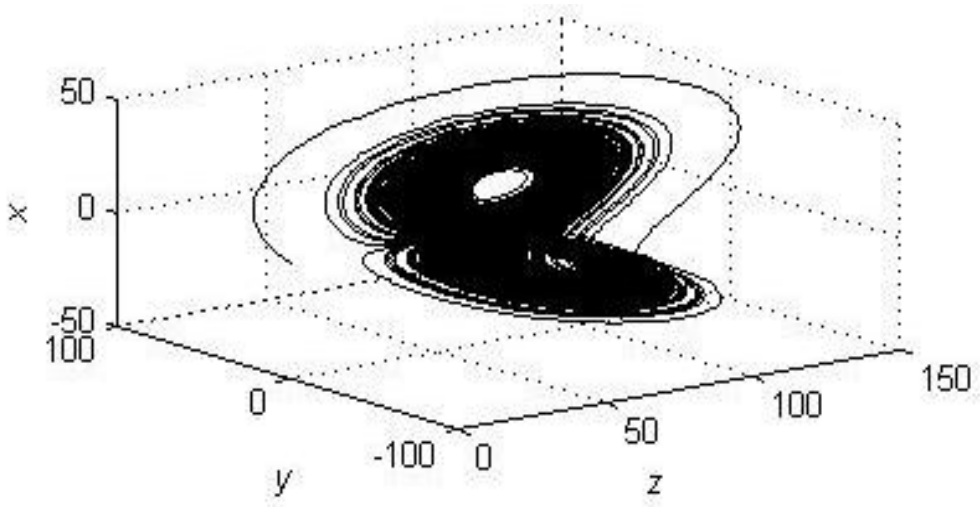


Рис.4.9. Атрактор, сформований розв’язками системи рівнянь Лоренца при значеннях параметрів $\sigma = 10$, $b = 8/3$, $r_1 = 100$

Моделювання атрактора системи здійснювалося при значеннях параметрів ($\sigma = 10$, $b = 8/3$, $r_0 = 80$, $r_1 = 100$), що забезпечують утворення хаотичних атракторів траєкторіями систем у їх фазовому просторі (рис.4.9).

Значення сигналу, що надходить у канал зв'язку, залежить від інформаційного біту. При передаванні «0» у канал зв’язку поступають сигнали від генератора з параметрами $\sigma = 10;\ b = 8/3;\ r_0 = 80$, а при передаванні «1» – від генератора з параметрами $\sigma = 10;\ b = 8/3;\ r_1 = 100$.

Приймач містить лише один генератор, значення параметрів якого в нашому випадку співпадають зі значеннями параметрів генератора передавача, налаштованого на інформаційний біт зі значенням «0». Розпізнавання значення інформаційного сигналу ґрунтується на явищі синхронізації. Якщо під час приймання зашифрованого біту має місце синхронізація між приймальною та передавальною сторонами системи, то прийнятий сигнал відповідає інформаційному біту «0». У випадку відсутності синхронізації прийнятий сигнал відповідає інформаційному біту «1».

Однією із вимог до систем передавання інформації є їх стійкість до завад, що мають місце у каналі зв’язку. Для достовірного передавання

інформації необхідне забезпечення стабільної синхронізації між передавачем та приймачем при передаванні біту зі значенням «0», і впевненість у відсутності синхронізації у протилежному випадку. Очевидно, що процес передавання буде якіснішим при більшому значенні різниці між рівнями сигналів, що відповідають «0» та «1». Ця різниця буде тим більшою, чим більша різниця між значеннями параметрів генераторів хаотичних коливань приймальної та передавальної сторін. Слід зауважити, що на процес синхронізації приймальної та передавальної сторін системи також впливає спосіб з'єднання генераторів хаотичних коливань Лоренца.

Із результатів чисельного моделювання (рис.4.10) випливає доцільність передавання сигналу, що відповідає змінній системи Лоренца x, подаючи його на вхід приймача, що описується другим рівнянням системи. Тоді система приймача описується наступним чином:

$$\begin{cases} \dot{x}_r = \sigma \cdot \left(y_r - x_r \right) \\ \dot{y}_r = r_0 \cdot x_{tr} - y_r - x_r \cdot z_r \\ \dot{z}_r = x_r \cdot y_r - b \cdot z_r \end{cases}, \quad (4.6)$$

де x_r, y_r, z_r – значення сигналів, що генеровані генератором Лоренца на приймальній стороні, x_{tr} – сигнал, що передається по каналу зв'язку.

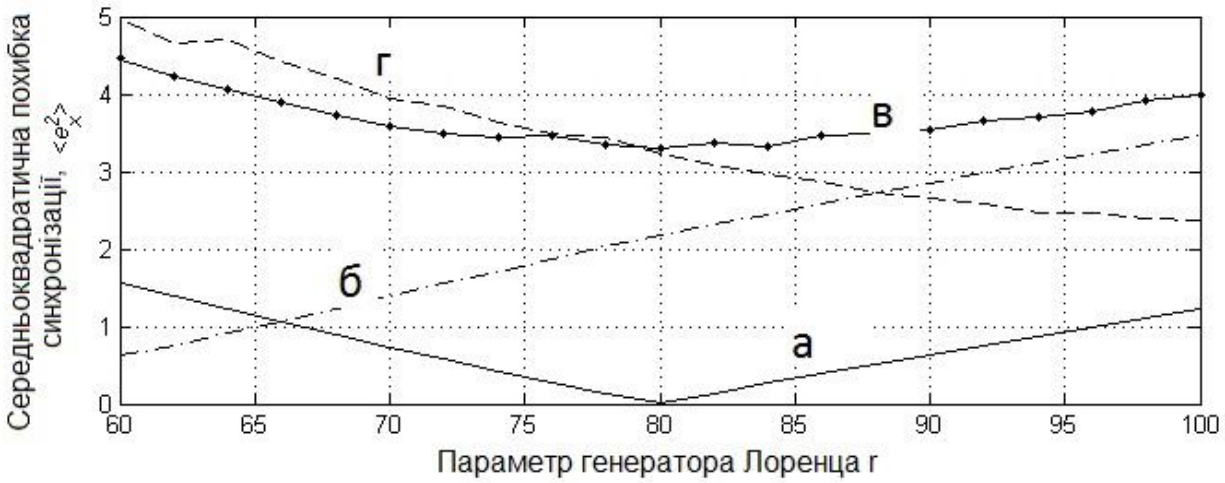


Рис. 4.10. Залежність середньоквадратичної похибки синхронізації від значення параметру при σ=10, b =8/3 (а); σ=15, b =8/3 (б); σ=20, b =8/3 (в) та σ=25, b =8/3 (г)

На рис.4.10 приведені графіки залежності середньоквадратичної похибки синхронізації від значення параметра r при різних значеннях параметрів σ і b.

Із отриманих результатів випливає, що підвищення завадостійкості може бути досягнуто використанням генераторів з великою різницею значень параметрів генераторів Лоренца «0» та «1». Необхідно зауважити, що генератори з різними параметрами генерують хаотичні сигнали з різними характеристиками (спектр та енергія сигналу), що погіршує прихованість процесу передавання інформації. Тому при моделюванні такої системи необхідно здійснювати пошук оптимальних рішень.

Про стабільність процесу синхронізації можна судити за величиною її похибки $e=\left[e_x,e_y,e_z\right]^T$, $e_x=x_r-x_0$, $e_y=y_r-y_0$, $e_z=z_r-z_0$, що задовольняє системі диференційних рівнянь (4.7):

$$\begin{cases}\dot{e}_x=-\sigma\cdot\left(e_x-e_y\right)\\ \dot{e}_y=-e_y-x_0\cdot e_z-e_x\cdot e_z\\ \dot{e}_z=x_0\cdot e_y+e_x\cdot e_y-b\cdot e_z\end{cases} \quad (4.7)$$

Якщо синхронізація має місце, то модуль вектора e асимптотично прямує до нуля (рис.4.11).

Стійкість процесу синхронізації можна дослідити розглянувши додатньо визначену функцію Ляпунова:

$$L(e)=\frac{1}{2}\cdot\left(\frac{1}{\sigma}\cdot e_x^2+e_y^2+e_z^2\right). \quad (4.8)$$

Умовою стійкості є від’ємне значення похідної від цієї функції:

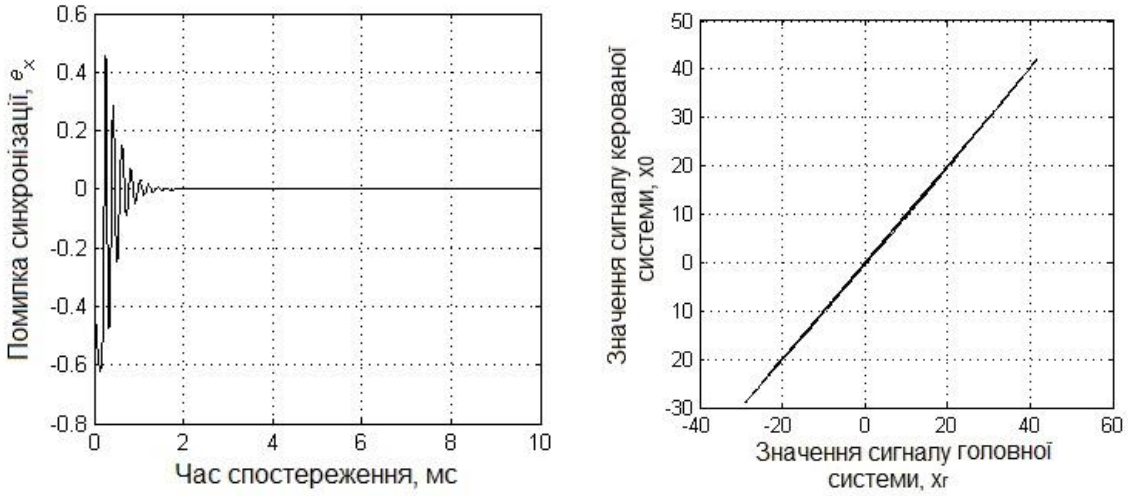
$$L(e)>0,\ \dot{L}(e)<0. \quad (4.9)$$

Використовуючи систему (4.7) запишемо значення першої похідної цієї функції:

$$\dot{L}(e)=-\left(e_x-\frac{1}{2}\cdot e_y\right)^2-\frac{3}{4}\cdot e_y^2-b\cdot e_z^2<0. \quad (4.10)$$

Оскільки значення функції $L(e)$ є додатнім, а значення її похідної – від'ємним, то згідно теоремі Ляпунова система (4.6) є стійкою для b>0.

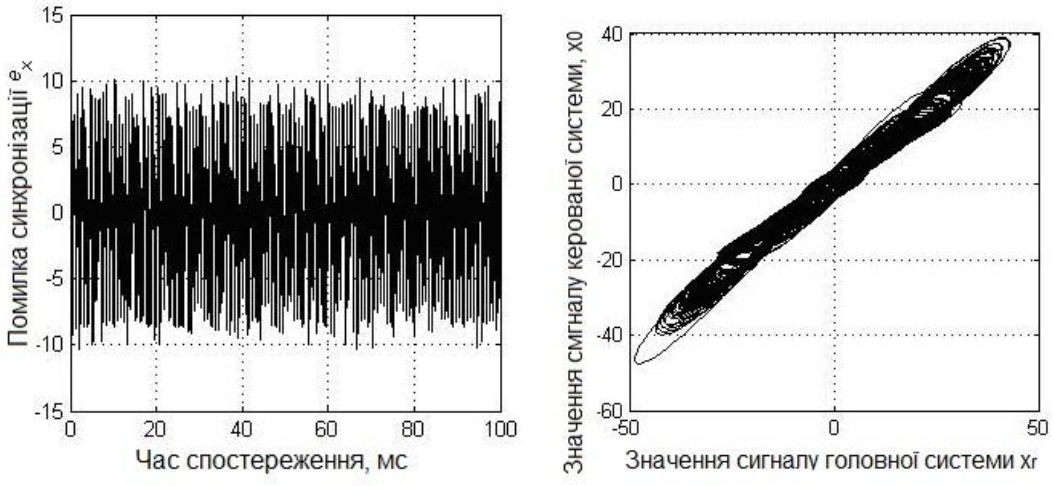
На рис.4.11, 4.12 приведена залежність помилки синхронізації від часу спостереження та залежність між прийнятим та генерованим сигналами приймальною стороною при наявності синхронізації та її відсутності відповідно. При передаванні біту «0» сигнал x на вході приймача x є синхронізованим із сигналом x_0 генерованим генератором хаосу приймальної сторони. При цьому різниця між ними $(x - x_0)$ експоненціально спадає до нуля (має місце синхронізація), рис.4.11 а, б.



а) б)

Рис.4.11. Часова залежність помилки синхронізації (а); залежність між прийнятим та генерованим приймальною стороною сигналами у випадку синхронного відгуку (б)

Протягом часу передавання біту «1» між сигналом на вході та сигналом, генерованим генератором хаосу приймальної сторони синхронізація відсутня, що підтверджується шумоподібним характером похибки синхронізації e_x та залежністю між прийнятим сигналом та сигналом, генерованим приймальною стороною (рис. 4.12).

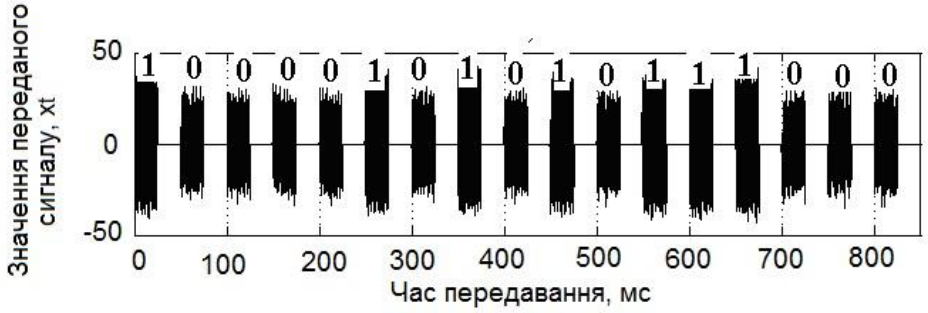


а) б)

Рис. 4.12. Часова залежність помилки синхронізації (а) та залежність між прийнятим та генерованим приймальною стороною сигналами у випадку синхронного відгуку (б)

У процесі передавання потоку двійкових даних у приймачеві відбувається чергування наявності та відсутності синхронізації на проміжках часу передавання одного біта (рис. 4.13,а).

а)



б)

Рис.4.13. Часові діаграми інформаційного повідомлення у RZ-коді (а) та сигналу, що передається (б)

Використання такого методу дає можливість декодувати двійкову інформацію з отриманого хаотичного сигналу. При цьому швидкість передавання бітів залежатиме від часу встановлення синхронізації. В початковий момент передавання кожного інформаційного біту спостерігається високий рівень помилки синхронізації, подальша картина залежить від значення переданого біта (рис.4.14).

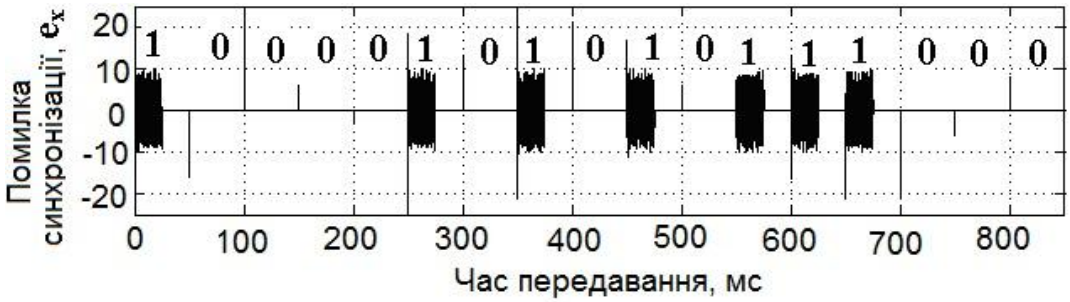


Рис.4.14. Режими встановлення синхронізації

4.3. Модель системи передавання інформації з підмішуванням інформаційного сигналу до хаотичної несучої, генерованої кільцевим автогенератором

Крім впливу зовнішніх шумів на хаотичний сигнал, що передається в каналі зв'язку, у більш узагальненому розгляді виникає необхідність враховувати також власні характеристики каналу, зокрема амплітудо-частотну і фазо-частотну характеристики. При цьому явища перетворення сигналу в каналі зв’язку можна змоделювати зміною фази і частоти, що виникають у процесі фільтрування сигналу. Для реальних каналів такі перетворення можна описати фільтром із обмеженою смугою пропускання, що значно спотворює проходження сигналу в області низьких та високих частот. Тому нами вибраний фільтр низьких частот у якості моделі каналу зв'язку.

Усунення ефектів впливу фільтрації у каналі зв'язку може здійснюватися наступними способами: використання вузькосмугових

хаотичних сигналів, побудова фазових коректорів (фазорів) у передавальному тракті системи. Можливості останнього методу є обмеженими для широкосмугових сигналів тому що точну задачу розв'язку корекції розв'язати важно, а інколи й неможливо, наближений розв’язок може не забезпечити бажаного результату оскільки у випадку проходження навіть відносно нескладних сигналів через нелінійні системи можуть виникати досить складні явища.

Нами [23] проведено дослідження залежності взаємної кореляції вихідного сигналу кільцевого генератора хаосу та інформаційного сигналу від потужності інформаційного сигналу при нелінійному підмішуванні інформаційного сигналу до хаотичного, що формується кільцевим автогенераторм [205]. Критерієм якості передавання інформації в системі було вибрано кореляцію між вхідним сигналом та сигналом на виході системи. Значення коефіцієнту кореляції між вказаними сигналами дає можливість зробити висновок про потенційне використання таких сигналів у системах передавання інформації.

Моделювання процесу передавання інформації здійснювалося для наступних інформаційних сигналів:

– синусоїдального сигналу $s = A \cdot \sin(2 \cdot \pi \cdot f \cdot t)$, де A, f – амплітуда та частота сигналу;

– частотно-модульованого синусоїдального сигналу $s = A \cdot \sin[2 \cdot \pi \cdot f_0 \cdot t - \psi \cdot \sin(2 \cdot \pi \cdot F \cdot t)]$, де A – амплітуда сигналу, f_0 – основна частота сигналу, ψ – індекс частотної модуляції, F – частота модулюючого сигналу.

Для забезпечення конфіденційності інформації спектр інформаційних сигналів повинен належати до спектру хаотичного сигналу. Нами було здійснено моделювання процесу передавання інформації з використанням підмішування інформаційного сигналу до хаотичного, генерованого

кільцевим генератором. При цьому на виході системи формується сигнал, що є сумою вхідного інформаційного та хаотичного сигналів:

$$u = z + s, \quad (4.11)$$

де z – хаотичний несучий сигнал, а s – інформаційний сигнал.

Для оцінювання подібності між інформаційним та хаотичним несучим сигналом, генерованого кільцевим генератором, обчислювалося максимальне значення коефіцієнта взаємної кореляції на часовому інтервалі τ:

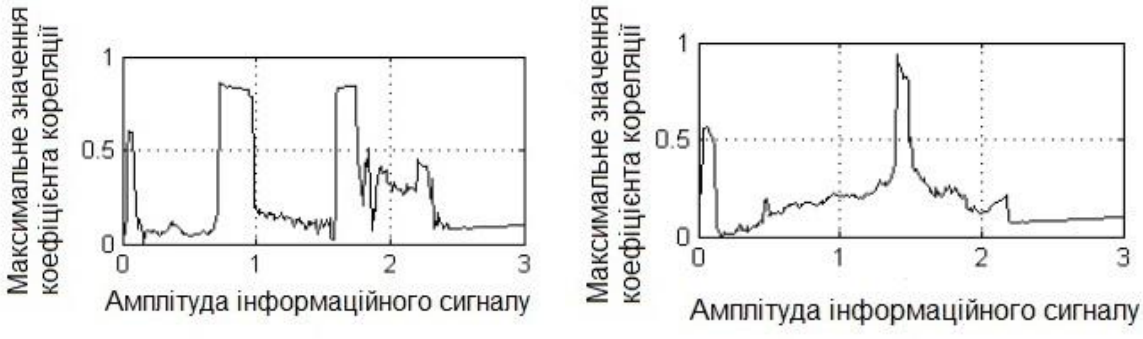
$$R_{\max} = \max_{z(t)}\left(R(\tau)\right) \quad (4.12)$$

$$R(\tau) = \frac{\langle z(t)\cdot s(t+\tau)\rangle - \langle z(t)\rangle \cdot \langle s(t+\tau)\rangle}{\sqrt{\left(\langle z^2(t)\rangle - \langle s^2(t)\rangle\right)\cdot\left(\langle z^2(t+\tau)\rangle - \langle s^2(t+\tau)\rangle\right)}} \quad (4.13)$$

Діапазону амплітуди інформаційного синусоїдального сигналу А відповідає діапазон відношення потужності підведеного до системи сигналу до потужності хаотичного сигналу $\mu = P_s / P_z \in [0;2{,}4]$.

Залежність максимального значення коефіцієнта взаємної кореляції між інформаційним і хаотичним несучим сигналами від амплітуди інформаційного сигналу при різних значеннях його частоти приведена на рис.4.15.

Із приведених залежностей випливає, що взаємодія (між синусоїдним та хаотичним сигналами) є суттєво нелінійною, інакше кажучи кільцевий автогенератор діє на синусоїдний сигнал як нелінійна система, внаслідок чого спостерігається декілька ділянок резонансної взаємодії між сигналами з максимальним значенням коефіцієнта кореляції близьким до одиниці.



а) б)

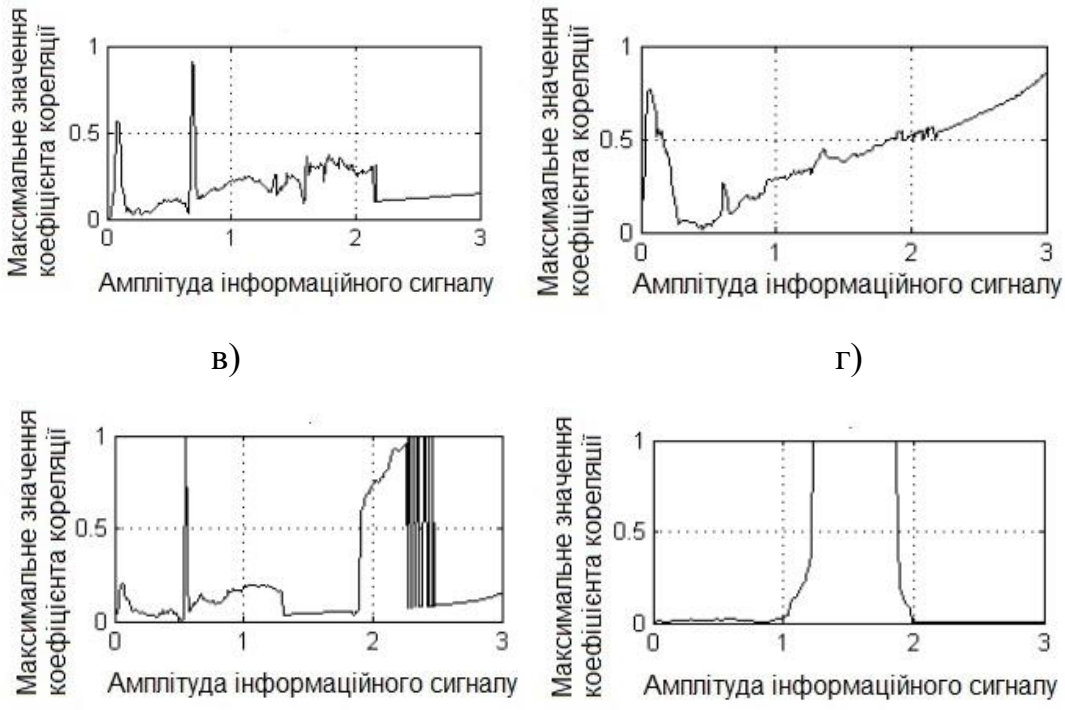


Рис.4.15. Залежність максимального значення коефіцієнта взаємної кореляції хаотичного несучого та інформаційного сигналів від його амплітуди при значеннях частоти $f = 0.4$ (а); $f = 0.5$ (б); $f = 0.8$ (в); $f = 1.0$ (г); $f = 1.2$ (д) та (е) $f = 2.0$ (е)

При цьому має місце захоплення частоти [85], оскільки ширина ділянок із високим значенням коефіцієнта взаємної кореляції є обмеженою. Для трьох значень частоти $f = 0.4$, $f = 1.2$, $f = 2.0$ мають місце широкі ділянки резонансу. Для частоти $f = 1.0$ спостерігається явище примусового згасання автоколивань генератора, що пояснює практично лінійне зростання коефіцієнта взаємної кореляції із амплітудою синусоїдного сигналу. Практичний інтерес представляють широкі ділянки із максимальним значенням коефіцієнта кореляції на рівні $R_{\max} \approx 0{,}5$, оскільки при цьому виявлення інформаційного сигналу є ускладненим, особливо в умовах завад. Високе значення коефіцієнта корляції означатиме, що прихований процес передавання інформації не спостерігається, оскільки система генерує сигнал,

що практично співпадає із інформаційним сигналом. Ширина ділянки є важливою, оскільки при цьому не потрібно чітко контролювати один із параметрів – амплітуду інформаційного сигналу, а це є дуже важливим для систем, що використовують хаотичну синхронізацію.

Структури хаотичних атракторів для сигналів з різними частотами та амплітудами також суттєво відрізняються між собою (рис.4.16).

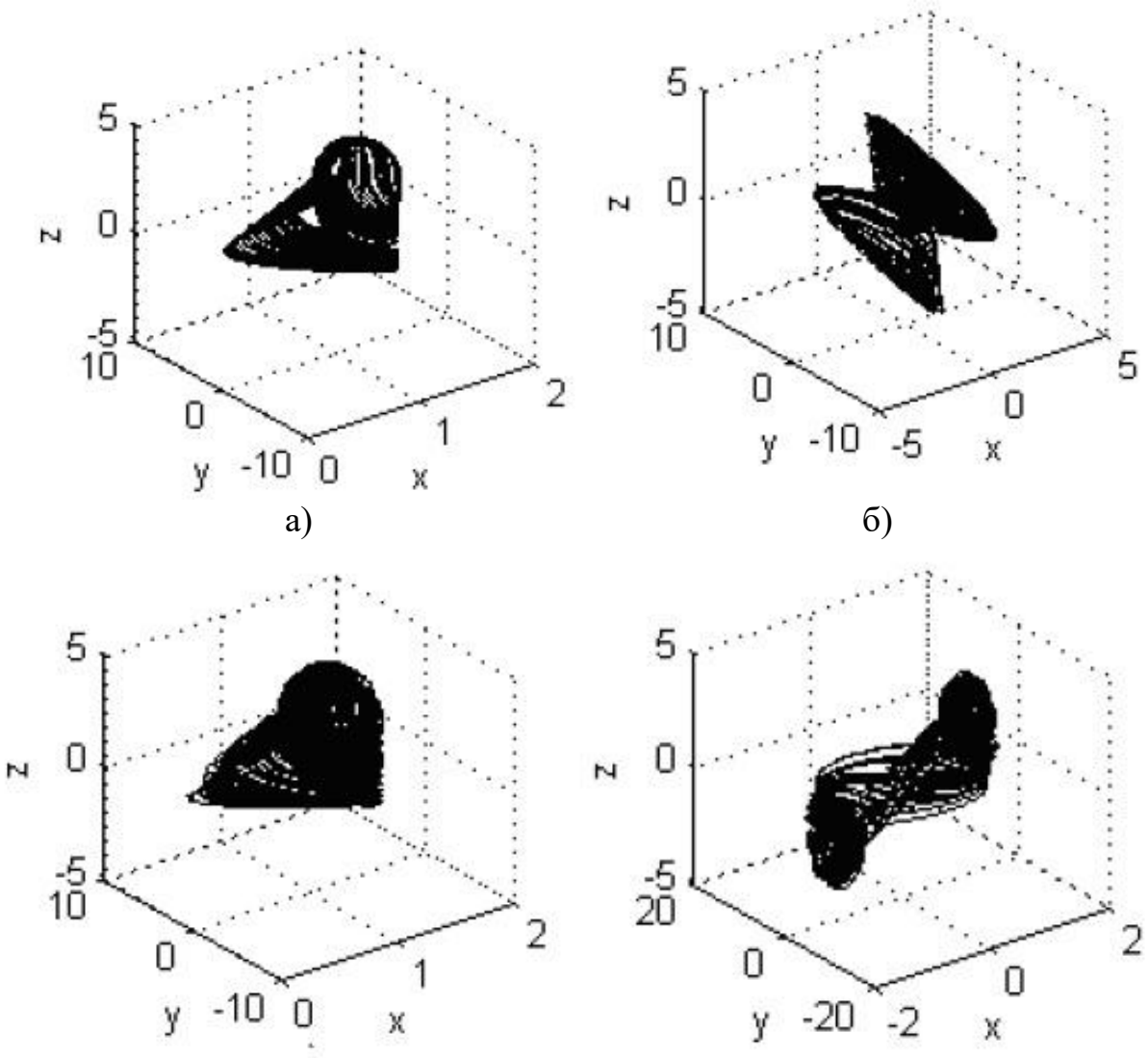
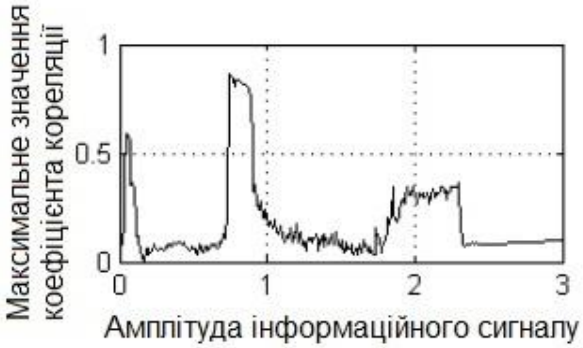


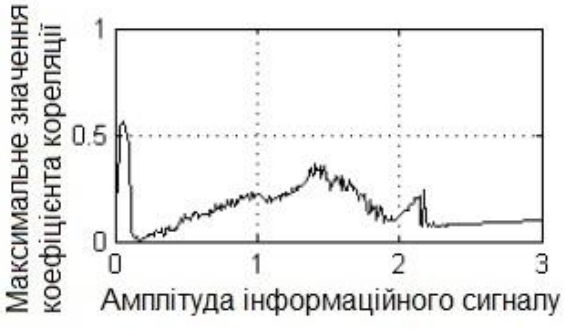
Рис. 4.16. Фазові портрети сигналів на виході кільцевого генератора при різних значеннях хаотичних сигналів, генерованих кільцевим генератором та сигналів на виході генератора: $A = 0$, $f = 0.5$ (а); $A = 0.2$, $f = 0.5$ (б); $A = 0.15$, $f = 1.0$ (в); $A = 0.2$, $f = 2.0$ (г)

Проведені також дослідження залежності максимального значення коефіцієнта взаємної кореляції між нелінійно підмішуваним частотно-модульованим сигналом та сигналом на виході генератора при різних значеннях частоти тонального сигналу.

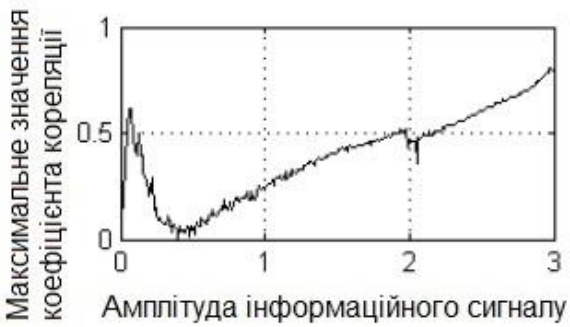
Якщо середня частота частотно-модульованого сигналу дорівнює середній частоті хаотичного генератора (рис.4.16в, $f = 1.0$), залежність максимального значення функції кореляції від амплітуди є подібною до відповідної залежності синусоїдального сигналу у всьому діапазоні значень амплітуди зовнішнього сигналу, а при частотах $f_0 = 0.5$, $f_0 = 0.8$ подібність має місце тільки при малих значеннях амплітуди (рис.4.16 а,б). Збільшення смуги частот частотно-модульованого сигналу з $F = 0.2 \cdot f_0$ до $F = 0.3 \cdot f_0$ за умови постійного середнього значення частоти частотно-модульованого сигналу призводить до зменшення максимального значення коефіцієнта кореляції (рис.4.16 в,г).



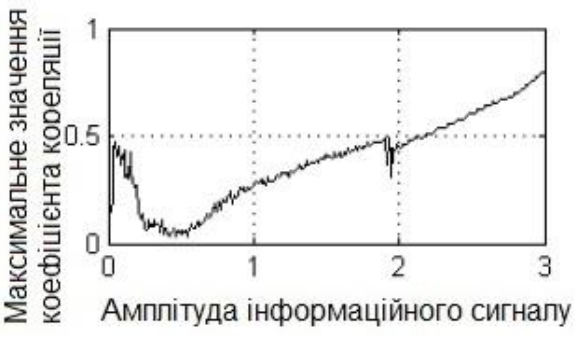
а)



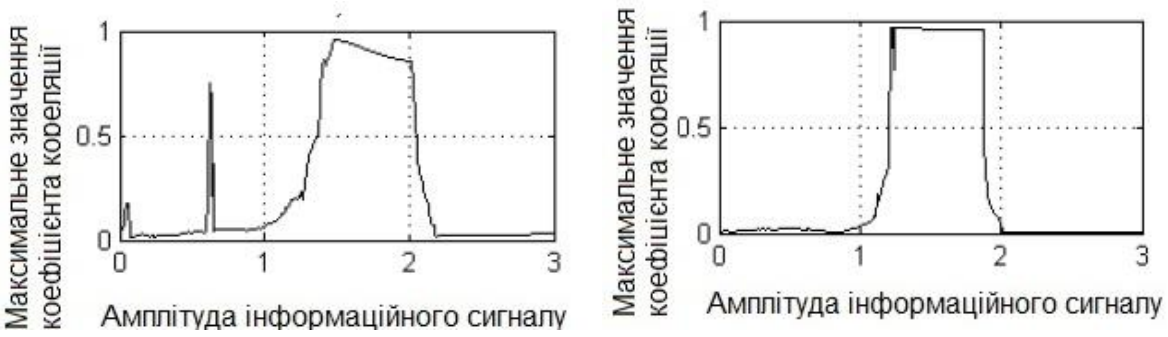
б)



в)



г)



д) е)

Рис.4.17. Залежність максимального значення коефіцієнта взаємної кореляції частотно-модульованого інформаційного сигналу з коефіцієнтом кореляції $\psi = 0.3$ та хаотично несучого при різних співвідношеннях частоти несучого та основної частоти вхідного сигналу $f_0 = 0.5$, $F = 0.2 \cdot f_0$ (а); $f_0 = 0.8$, $F = 0.2 \cdot f_0$ (б); $f_0 = 1.0$, $F = 0.1 \cdot f_0$ (в); $f_0 = 0.2$, $F = 0.2 \cdot f_0$ (г); $f_0 = 1.0$, $F = 0.3 \cdot f_0$ (д) та $f_0 = 1.5$, $F = 0.1 \cdot f_0$ (е)

При високому значенні частоти частотно-модульованого сигналу значення коефіцієнта кореляції залишається невеликим у широкому діапазоні зміни амплітуди сигналу (рис. 4.17 е). Високі значення коефіцієнта кореляції $R_{\max} \approx 1$ відповідають режиму синхронізації через подавлення автоколивань хаотичної системи.

Залежність коефіцієнта кореляції між інформаційним сигналом та вихідним сигналом генератора від амплітуди інформаційного сигналу є досить складною.

Високе значення коефіцієнта кореляції вказує що подібність хаотичного та інформаційного сигналі уможливлює передавання інформації в умовах дії завад. Але при цьому зменшується прихованість інформаційного сигналу внаслідок того, що спектр шифрованого сигналу подібний до спектру інформаційного, що є однією з причин уразливості розглядуваної системи передавання інформації.

Значення коефіцієнта кореляції залежать від параметрів інформаційного сигналу. В досліджуваному діапазоні частот та потужностей зовнішнього сигналу спостерігаються області, в яких кореляція є незначною, і в той же час спостерігається хаотичний режим коливань. При цьому потужність інформаційного і вихідного хаотичного сигналів може бути різною. Вказана властивість є важливою, оскільки шляхом зміни рівня інформаційного сигналу можна керувати якістю передавання інформації.

Оптимальними є умови, при яких коефіцієнт кореляції приймає середні значення. Для досліджуваної системи вхідний інформаційний сигнал повинен мати смугу частот, до якої не належить середня частота генератора.

З приведених результатів моделювання можна зробити висновок, що при частоті інформаційного сигналу, яка потрапляє у діапазон частот між основною частотою та субгармонікою хаотичного сигналу мають місце ділянки з малими значеннями коефіцієнта кореляції при різних значеннях амплітуди (потужності) зовнішнього сигналу.

При підмішуванні частотно-модульованого сигналу спостерігається подібність залежності коефіцієнта кореляції до залежності, що має місце при підмішуванні синусоїдального сигналу, якщо основна частота хаотичного та зовнішнього сигналів співпадають (рис. 4.14 г та 4.17 в, г), тобто кореляційні властивості залежать від форми інформаційного сигналу.

Таким чином нами розраховані залежності коефіцієнтів кореляції між інформаційним та хаотичним сигналом від глибини модуляції хаотичного сигналу для двох типів інформаційних сигналів: синусоїдних та частотно-модульованих коливань у системі з нелінійним підмішуванням інформаційного сигналу до генерованого кільцевим автогенератором хаотичного сигналу. Такі залежності були встановлені для різних значень частот синусоїдного сигналу та несучої і основної частот частотно-модульованого сигналу. Високе значення коефіцієнта кореляції між інформаційним та хаотичним несучим сигналами створює можливість передавання інформації в умовах дії завад, але при цьому зменшується

прихованість інформаційного сигналу внаслідок того, що спектр переданого сигналу подібний до спектру інформаційного, тому оптимальним є випадок середніх значень кореляції (на рівні 0,5).

ВИСНОВКИ

1. Шляхом чисельного моделювання спектру показників Ляпунова системи Лю встановлені області періодичних, квазіперіодичних, хаотичних та гіперхаотичних коливань. Знайдені діапазони значення змінного параметру, при яких виникають режими, що придатні для прихованого передавання інформації – періодичні, квазіперіодичні, хаотичні та гіперхаотичні коливання (при значеннях $n \in (38;42] \cup (48;57]$). Дослідження осцилограм експериментального зразка підтвердили результати моделювання роботи схеми в режимі хаосу.

2. Досліджений механізм встановлення синхронізації між двома хаотичними системами Лю (веденої і ведучої системи). Встановлені значення опору резистора кола оберненого зв'язку, що регулює глибину оберненого зв'язку між генераторами. Зміна опору від 100 Ом до 3 кОм призводить до розсинхронізації генераторів.

3. Розроблена математична модель системи передавання цифрової інформації з її кодуванням шляхом перемикання хаотичних режимів між двома генераторами коливань Лоренца, що відрізняються значеннями одного параметра.

4. Встановлена залежність середньоквадратичної похибки синхронізації від значенням параметрів генераторів Лоренца σ, r, b. Отримані оптимальні значення параметру $r \in (80;100)$, що забезпечують якісне предавання та декодування інформації у телекомунікаційних системах з використанням генераторів Лоренца.

5. На основі проведених досліджень встановлені оптимальні співвідношення параметрів системи з нелінійним підмішуванням інформаційного сигналу двох типів (синусоїдаьних та частотно-модульованих коливань) до хаотичного сигналу, генерованого кільцевим автогенератором, при яких має місце оптимальне значення коефіцієнта

кореляції між інформаційним та хаотичним сигналами, що дорівнюють 0,5. Вони відповідають наступним значенням основної частоти та частоти модуляції: $f = 0.4$, $f = 0.8$ для синусоїдального сигналу і $f_0 = 0.5$, $F = 0.2 \cdot f_0$ для частотно-модульованого сигналу при коефіцієнті модуляції хаотичної несучої $A \approx 2$.

РОЗДІЛ 5. ВЛАСТИВОСТІ СИГНАЛІВ ТИПУ ФРАКТАЛЬНИЙ ГАУСОВИЙ ШУМ ТА ПОБУДОВА ЗАВАДОСТІЙКИХ ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ НА ЇХ ОСНОВІ

На зміну СПІ що використовують сигнали із простою структурою приходять системи із складними за своєю структурою коливаннями. Така структура коливань може забезпечити базу сигналу, що сягає сотень, а іноді тисяч одиниць [206].

Як показують фундаментальні праці [207] складні коливання та системи є «не лише хаотичними але й фрактальними». Результативність досліджень процесів передавання інформації може суттєво покращитися якщо враховувати фрактальність псевдовипадкових переносників, або використовувати сигнали, які апріорі виявляють фрактальні властивості.

Найпоширенішими сигналами із фрактальними властивостями є сигнали типу «фрактальний вейвлет» та «фрактальний гаусовий шум». Можливості генерування таких сигналів є обумовлені розвитком цифрових технологій ПЛІС [176].

У даному розділі приведені дослідження властивостей ФГШ та описана система передавання інформації, що його використовує.

Крім того ФГШ можуть використовуватися з метою моделювання процесу забезпечення якості обслуговування у моделі розподілу мультисервісного трафіку [208].

Наслідком нерівномірності навантаження на телекомунікаційну систему, виникненням пікових навантажень та їх спадання є самоподібність часових залежностей інтенсивності навантаження системи.

На основі досліджених властивостей ФГШ нами проведено моделювання процесів проходження трафіку через телекомунікаційну систему методом системи масового обслуговування (СМО).

5.1. Аналогія між фрактальним гаусовим шумом та броунівським рухом

Статистичні характеристики фрактального гаусового шуму, що може бути використаний для кодування інформації в телекомунікаційних системах, є аналогічними характеристикам броунівського руху.

Одномірним броунівським рухом частинки є її зміщенням вздовж прямої лінії, значення якого є випадковими [209-211] з нормальною густиною розподілу ймовірності:

$$p(\xi,\tau)=\frac{1}{\sqrt{4\cdot\pi\cdot D\cdot\tau}}\cdot\exp\left(-\frac{\xi^2}{4\cdot D\cdot\tau}\right), \qquad (5.1)$$

де

ξ –крок в момент часу $t=n\cdot\tau$,

$\sigma^2=2\cdot D\cdot\tau$ — дисперсія кроку броунівської частинки,

D – коефіцієнт дифузії броунівської частинки,

τ – інтервал спостереження броунівського руху.

Приріст координати броунівської частинки за час $2\cdot\tau$ дорівнює сумі двох незалежних приростів $\xi=\xi_1+\xi_2$ [62]. По аналогії значення координати броунівської частинки X в момент часу $t=n\cdot\tau$ дорівнюватиме:

$$X(t=n\cdot\tau)=\sum_{i=0}^{n}\xi_i, \qquad (5.2)$$

де $\{\xi_i\}$ – є вибіркою зміщень частинки, що мають місце на інтервалі часу $t_i=\tau\cdot i,\ 0\le i\le n$.

Часові діаграми координати броунівської частинки, побудовані на основі аналітичних виразів (5.1) та (5.2) для двадцяти різних статистичних реалізацій приведені на рис.5.1.

В силу статистичних властивостей, зокрема нормального розподілу густини ймовірності координати броунівської частинки для різних часових зрізів (рис.5.2а та 5.3), броунівському руху притаманна властивість самоподібності (стохастична еквівалентність [212]).

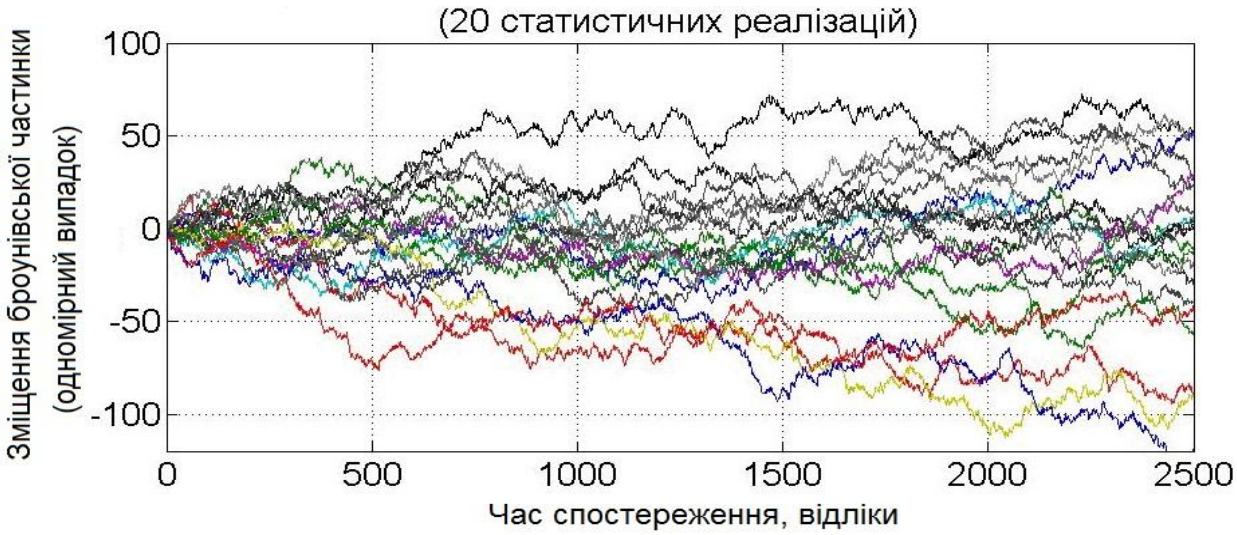


Рис. 5.1. Часові залежності координати броунівської частинки для двадцяти різних статистичних реалізацій

Густина розподілу (5.3), математичне сподівання (5.4) та дисперсія (5.5) зміщення броунівської частинки описуються наступними виразами:

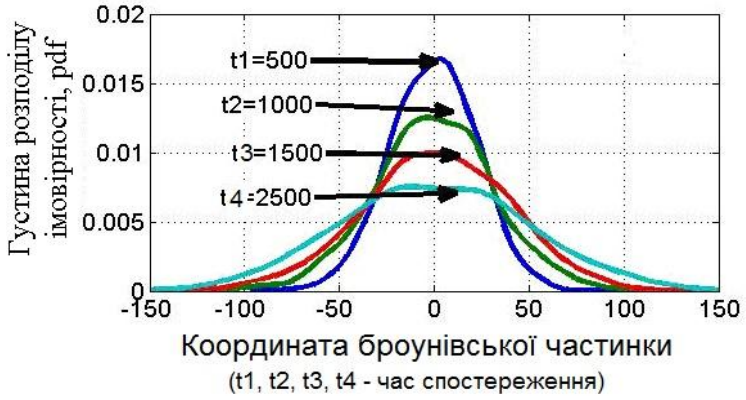
$$P\left(X\left(t\right)-X\left(t_0\right)\right)=\frac{1}{\sqrt{4\cdot\pi\cdot D\cdot\left|t-t_0\right|}}\cdot\exp\left(-\frac{\left[X\left(t\right)-X\left(t_0\right)\right]^2}{4\cdot D\cdot\left|t-t_0\right|}\right),\quad(5.3)$$

$$\overline{\mathrm{X}\left(\mathrm{t}\right)-X\left(t_0\right)}=0,\qquad(5.4)$$

$$\overline{\left[\mathrm{X}\left(\mathrm{t}\right)-X\left(t_0\right)\right]^2}=2\cdot D\cdot\left|t-t_0\right|,\ (5.5)$$

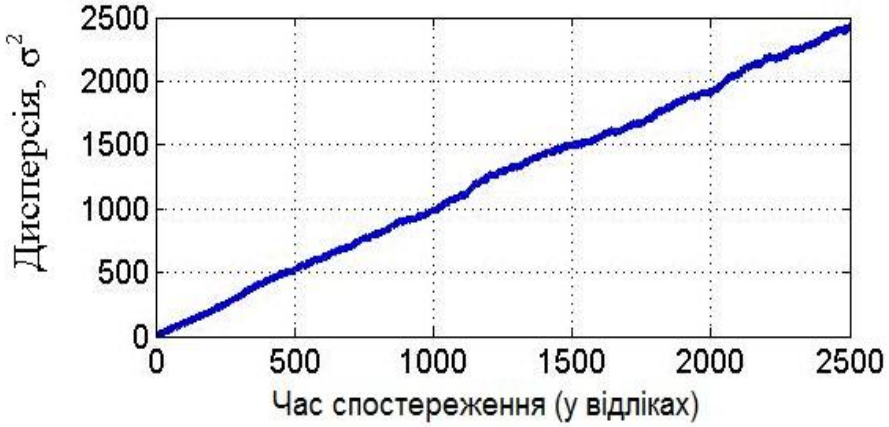
де $\left(t_0,t\right)$ –часовий інтервал, протягом якого відбувається зміщення.

При масштабуванні часу (збільшення інтервалу спостереження у n разів) густина розподілу ймовірності по координаті зберігає гаусів характер (рис. 5.3).

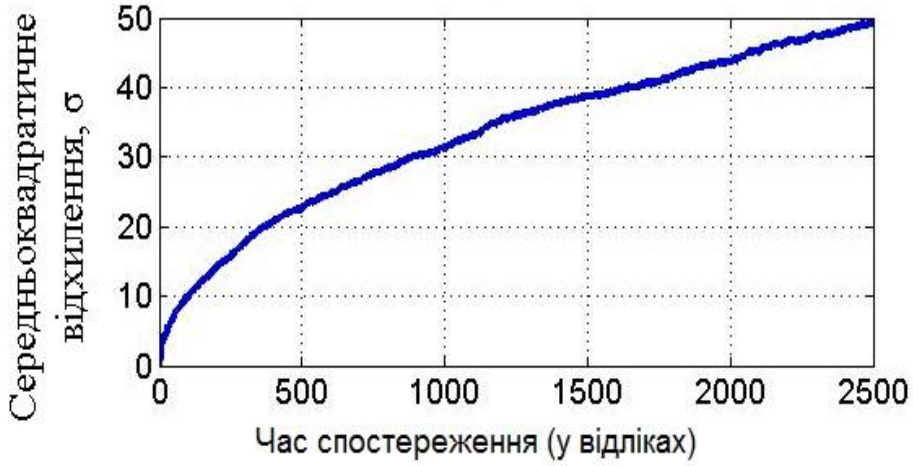


а)

б)

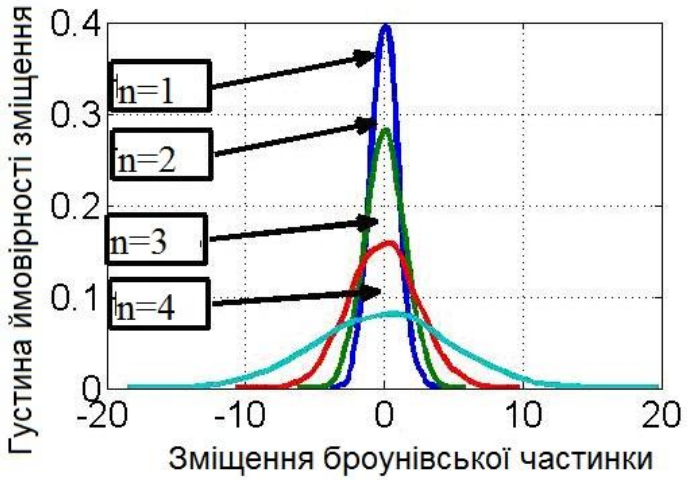


в)

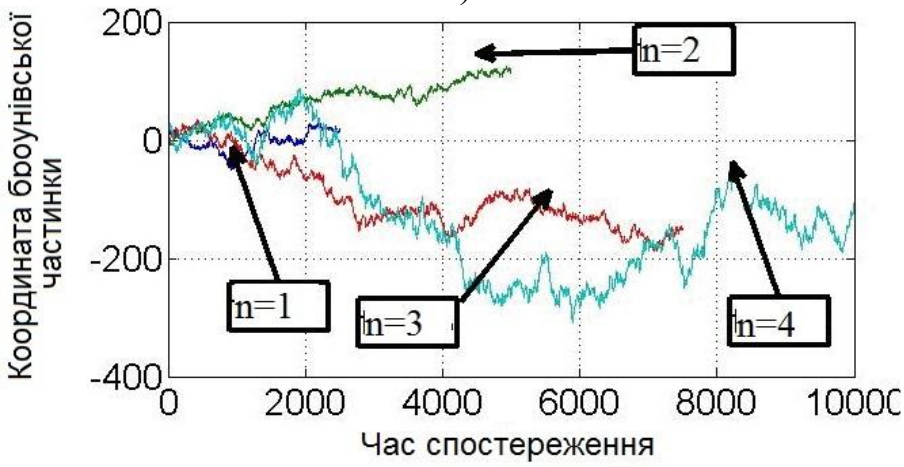


г)

Рис.5.2. Статистичні властивості та самоподібність броунівського руху – густина ймовірності розподілу (а); математичне сподівання координати (б); дисперсія координати (в) та середнє квадратичне відхилення (г)



а)



б)

Рис. 5.3. Статистичні характеристики броунівського руху при різних значеннях коефіцієнту n масштабування по часу. Розподіл густини ймовірності зміщення броунівської частинки (а) та часова залежність координати броунівської частинки при значеннях коефіцієнту часового масштабування $n = 1, 2, 3, 4$ (б)

Для описання сигналів типу фрактальний гаусів шум, використовувався перехід від класичного броунівського руху до процесу Вінера, що описується математичною моделлю, отриманою Мандельбротом [62].

Часова залежність приросту процесу Вінера (або узагальненого броунівського руху) описується наступною степеневою залежністю:

$$X(t) - X(t_0) = \xi \cdot |t - t_0|^H \quad (\mathrm{t} \geq \mathrm{t}_0), \qquad (5.6)$$

де ξ – величина, розподілена за нормальним законом, H – показник Херста [62].

Результати моделювання часової залежності координати вінерівського процесу при різних значеннях показника Херста приведені на рис.5.4. Для випадку H=0,5 має місце броунівський рух.

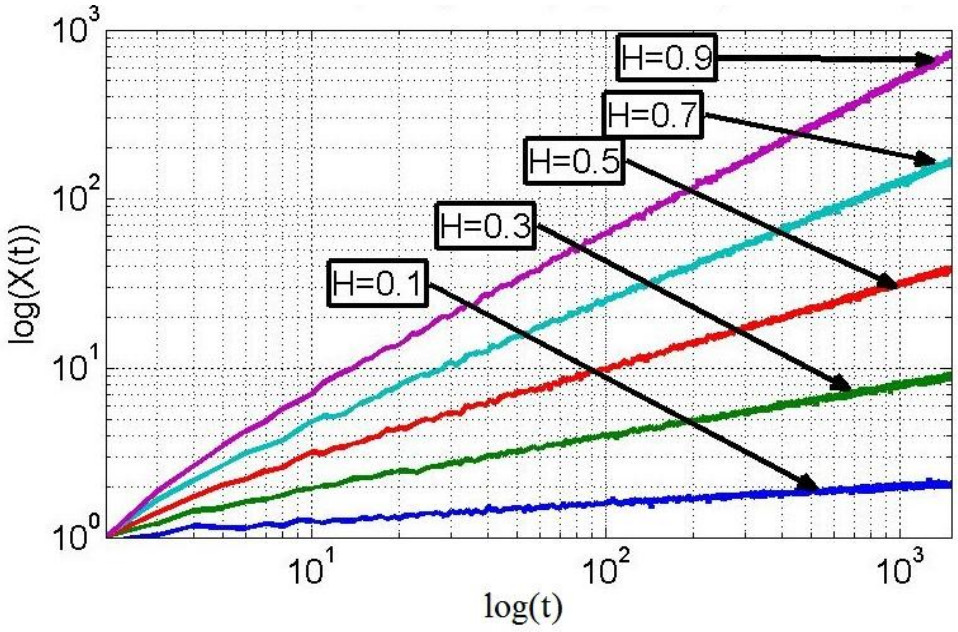


Рис.5.4. Часова залежність координати узагальненого броунівського руху (вінерівського процесу) для різних показників Херста (H – показник Херста)

Використовуючи теорію марківських процесів, Мандельброт та ван Несс отримали більш точну математичну модель узагальненого броунівського руху [62]:

$$X_H(t) - X_H(0) = \frac{1}{\Gamma\left(H + \frac{1}{2}\right)} \cdot \int_{-\infty}^{t} K\left(t - t'\right) dX\left(t'\right), \qquad (5.7)$$

$$K\left(t - t'\right) = \begin{cases} \left(t - t'\right)^{H-1/2} & \text{при } 0 \le t' \le t \\ \left(t - t'\right)^{H-1/2} - \left(-t'\right)^{H-1/2} & \text{при } t' \le 0 \end{cases} \qquad (5.8),$$

де $\Gamma(x)$ – гамма-функція :

$$\Gamma(x) = \int_0^{\infty} e^{-t} \cdot t^{x-1} dt, \qquad (5.9)$$

Отримана Мандельбротом формула (5.7) використовувалася нами в якості математичної моделі фрактального гаусового шуму (ФГШ) [10, 11, 17, 42, 43, 45, 47].

Генерування ФГШ здійснювалося згідно формулам (5.7-5.8). При цьому у (5.7) стохастичний інтеграл був замінений сумою скінченого часового ряду, вважаючи що:

– час t приймає цілі значення на скінченному інтервалі;

– $dX\left(t^{'}\right)$ замінюємо на $n^{-1/2} \cdot \xi_i$, де $\{\xi_i\}$ – скінченний набір випадкових чисел розподілених за гаусовим законом з одиничною дисперсією та нульовим математичним сподіванням, n – параметр масштабування у часі, найменше значення якого дорівнює 1;

– час $t^{'} = i \cdot n,\ i \in (-\infty; t/n]$;

– верхню межу інтегрування замінюємо на $n \cdot t$;

– нижню межу замінюємо на $n \cdot (t - M)$, значення M визначає кількість доданків суми, що замінює стохастичний інтеграл.

– різницю приростів розглядуємо на інтервалі $(t-1; t)$.

В результаті виконаних перетворень отримаємо вираз, що описує залежну від декількох параметрів послідовність дійсних чисел:

$$X_H(t) - X_H(t-1) = \frac{1}{\Gamma\left(H + \frac{1}{2}\right)} \cdot \sum_{i=n\cdot(t-M)}^{n\cdot t} K\left(t - \frac{1}{n}\right) \cdot n^{-1/2} \cdot \xi_i, \qquad (5.10)$$

де H – показник Херста, n – коефіцієнт масштабування у часі, значенням якого визначається точність обчислень; M – цілочисельний параметр, від якого залежить нижня границя при обчисленні суми, що є заміною стохастичного інтеграла.

Вираз (5.10) є дискретною моделлю фрактального броунівського руху.

5.2. Дослідження властивостей фрактальгного гаусового шуму

Нами [10, 11, 41] досліджувалися властивості фрактального гаусового шуму, що описується наступною математичною моделлю:

$$S(t,H,n)\approx\frac{n^{-1/2}}{\Gamma(H+1/2)}\cdot\left[\sum_{i=0}^{n\cdot(t+1)-1}\left(t+1-\frac{i}{n}\right)^{H-1/2}\cdot\xi_i-\sum_{i=0}^{n\cdot t-1}\left(t-\frac{i}{n}\right)^{H-1/2}\cdot\xi_i\right] \quad (5.11),$$

де $\Gamma(H+1/2)$ – гамма-функція, H – показник Херста, n – коефіцієнт масштабування у часі, що є цілим числом, найменше значення якого дорівнює 1, $\{\xi_i\}$ – скінчений набір випадкових чисел розподілених за гаусовим законом з одиничною дисперсією та нульовим математичним сподіванням, S – значення відліку ФГШ, t – момент часу, у який визначається значення відліку ФГШ.

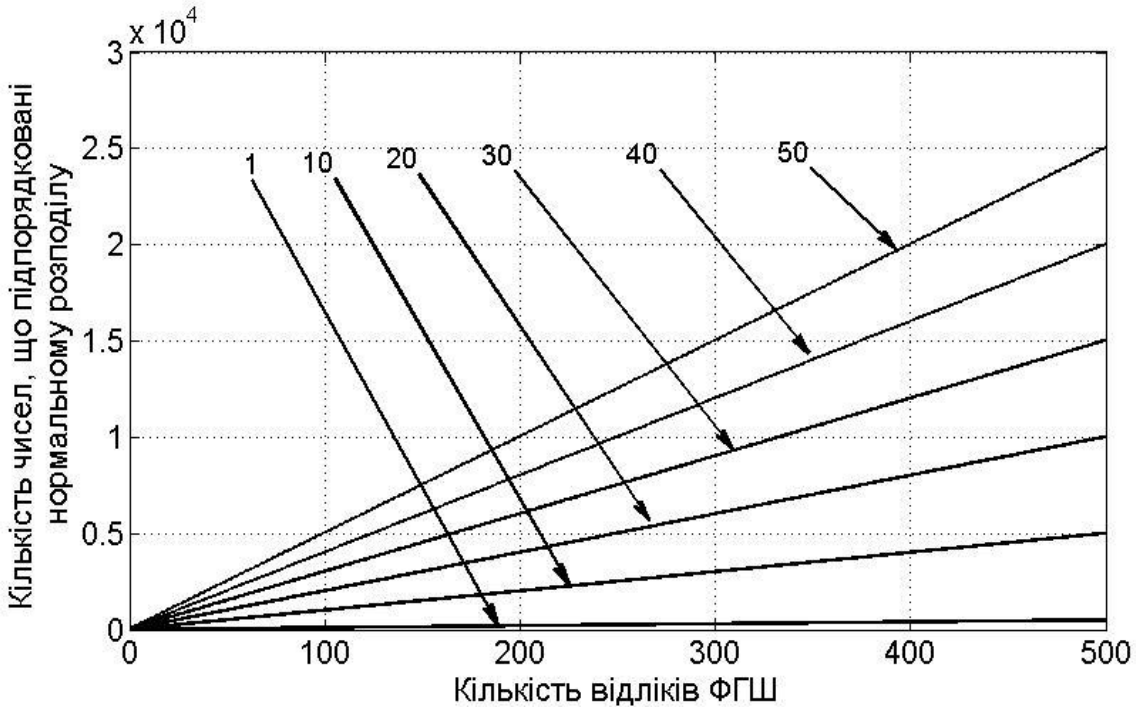


Рис.5.5. Залежність кількості випадкових дійсних чисел, необхідних для формування заданої кількості ФГШ при різних значеннях коефіцієнту часового масштабування

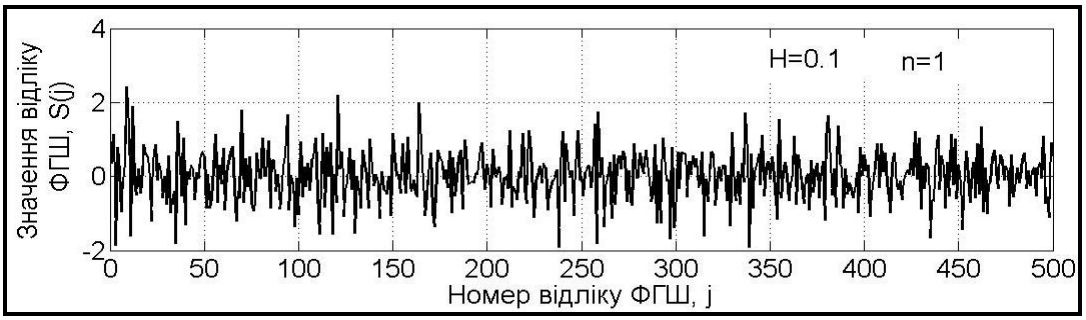
Математична модель ФГШ (5.11) містить параметр n, зміст якого відображає масштабування досліджуваного процесу по часу. Очевидно, що обсяг обчислень значень ФГШ залежить від коефіцієнту часового масштабування. Тому, з метою формування широкосмугового фрактального сигналу із заданими властивостями при мінімальних часових затратах, виникає необхідність оптимізації значень коефіцієнта масштабування.

Із приведеної на рис.5.5 залежності кількості випадкових дійсних чисел, необхідних для формування ФГШ, при різних значеннях коефіцієнтів часового масштабування, випливає, що вона зростає прямо пропорційно тривалості ФГШ (кількості його відліків), а швидкість зростання тим більша, чим більше значення коефіцієнту часового масштабування.

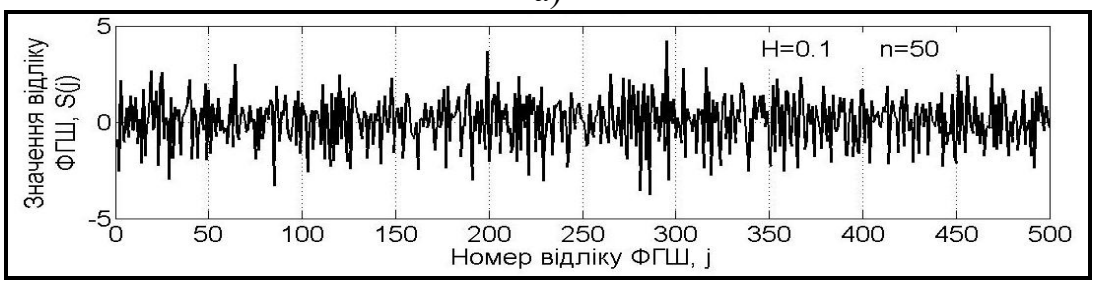
Із аналізу часових діаграм сигналів типу ФГШ з показниками Херста H=0,1; H=0,5 та 0,9 для двох значень параметру часового масштабування, $n=1$ та $n=50$, можна зробити висновок про їх шумоподібну природу.

Нами досліджувалися сигнали типу ФГШ, утворені 500-ми відліками, оскільки, як буде показано, така кількість відліків забезпечує задовільне передавання інформації при відносності сигнал / шум $=-7{,}5$ *дБ*.

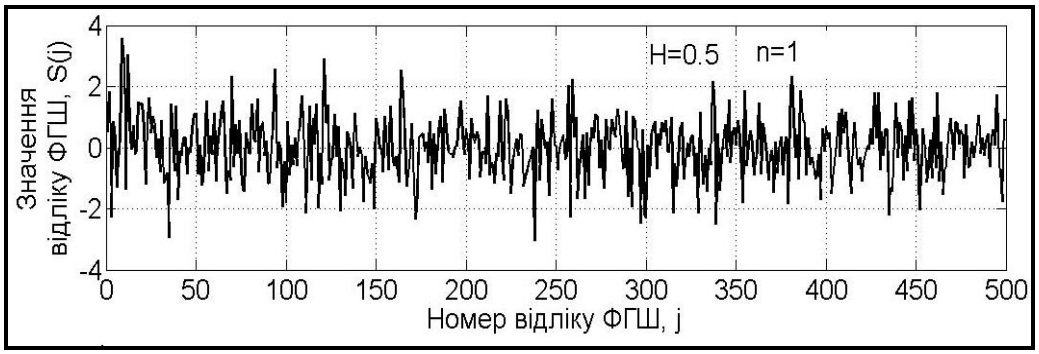
Із приведених на рис.5.6 часових діаграм сигналів типу ФГШ можна зробити висновок про їх хаотичний характер.



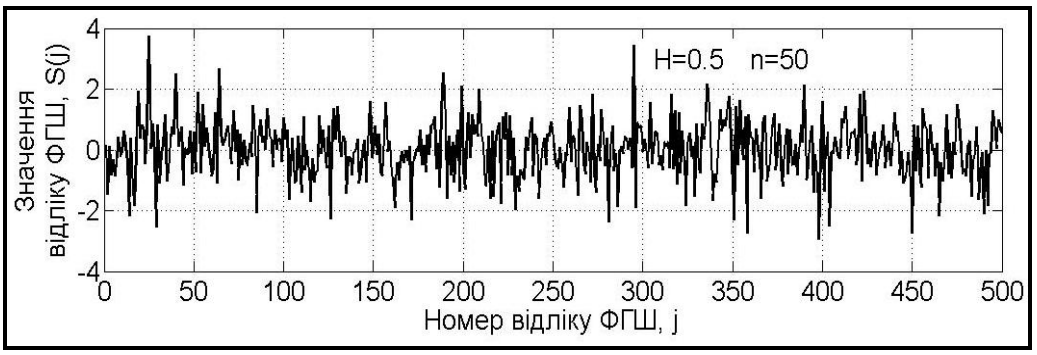
а)



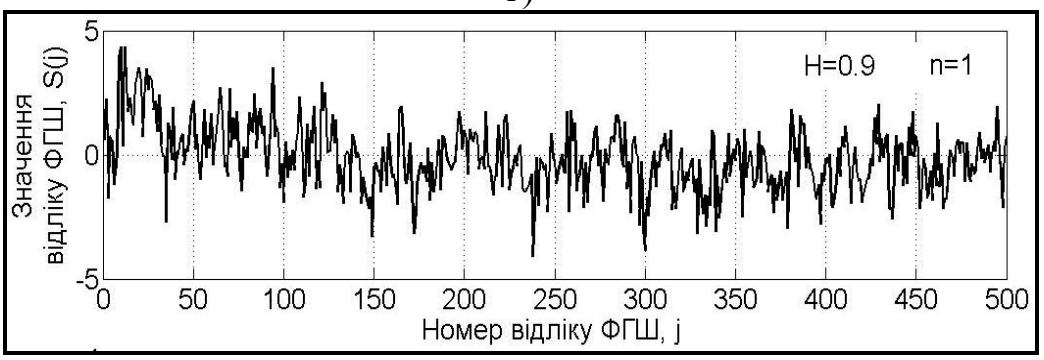
б)



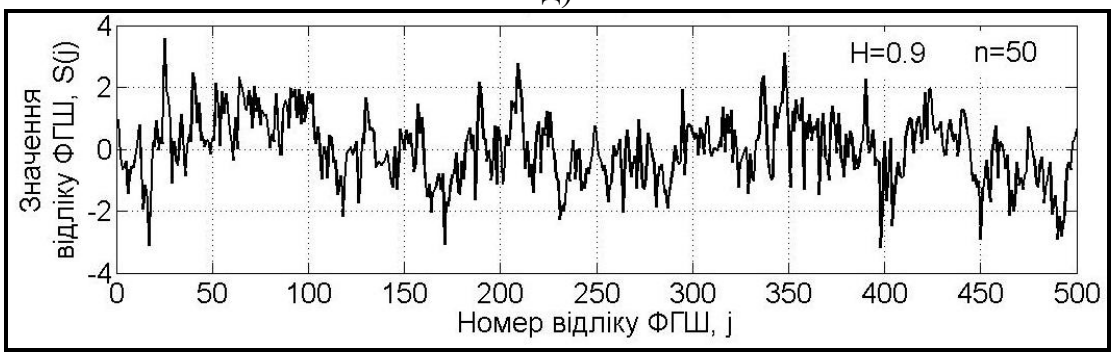
в)



г)



д)



е)

Рис. 5.6. Часові діаграми ФГШ з різними показниками Херста H=0,1; 0,5; 0,9 при значеннях коефіцієнтів часового масштабування n=1, 50.

Для дослідження спектральних характеристик ФГШ використовувались частотні залежності спектральної густини потужності, що

розраховувалась усередненням вибірок сигналу отриманих шляхом дискретного перетворення Фур'є за формулою [213]:

$$W(\omega)=\lim_{m\to\infty}\frac{1}{2\cdot m+1}\cdot\overline{\left|\sum_{k=-m}^{m}S(k)\cdot e^{-j\cdot\omega\cdot k\cdot T}\right|^2}, \quad (5.12)$$

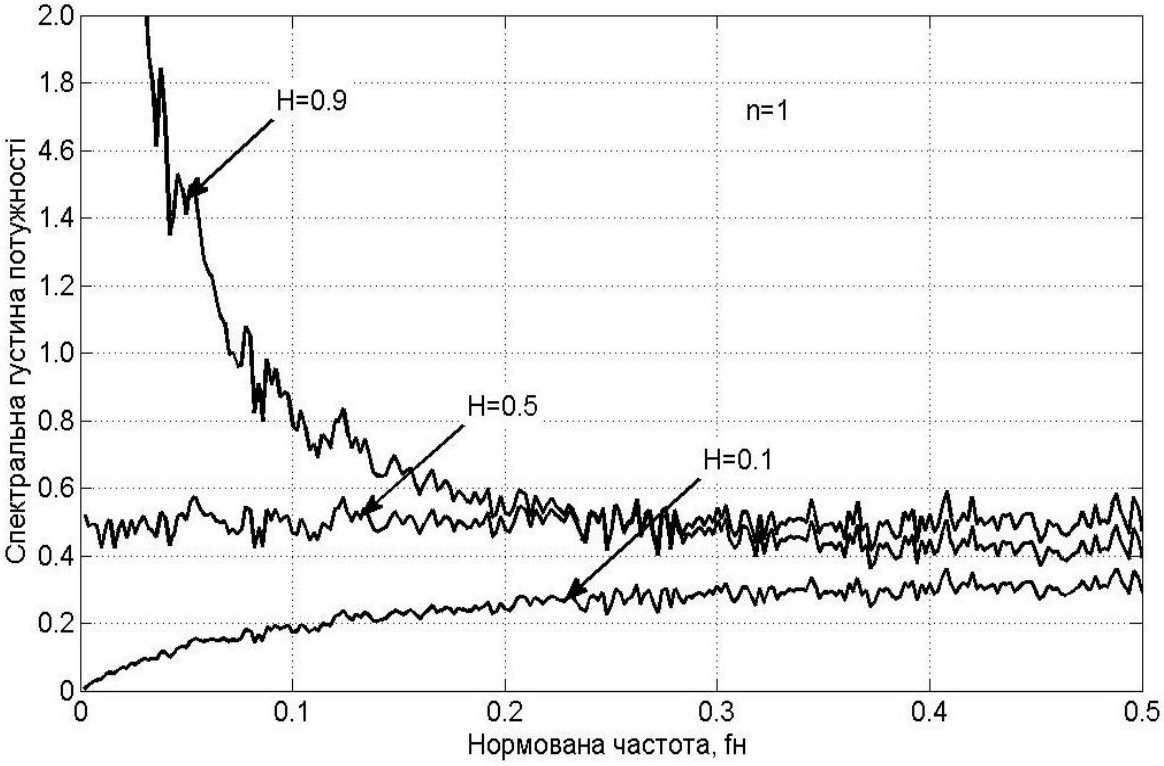
де $S(k)$ – значення k-го відліку сигналу типу ФГШ;

T – період дискретизації.

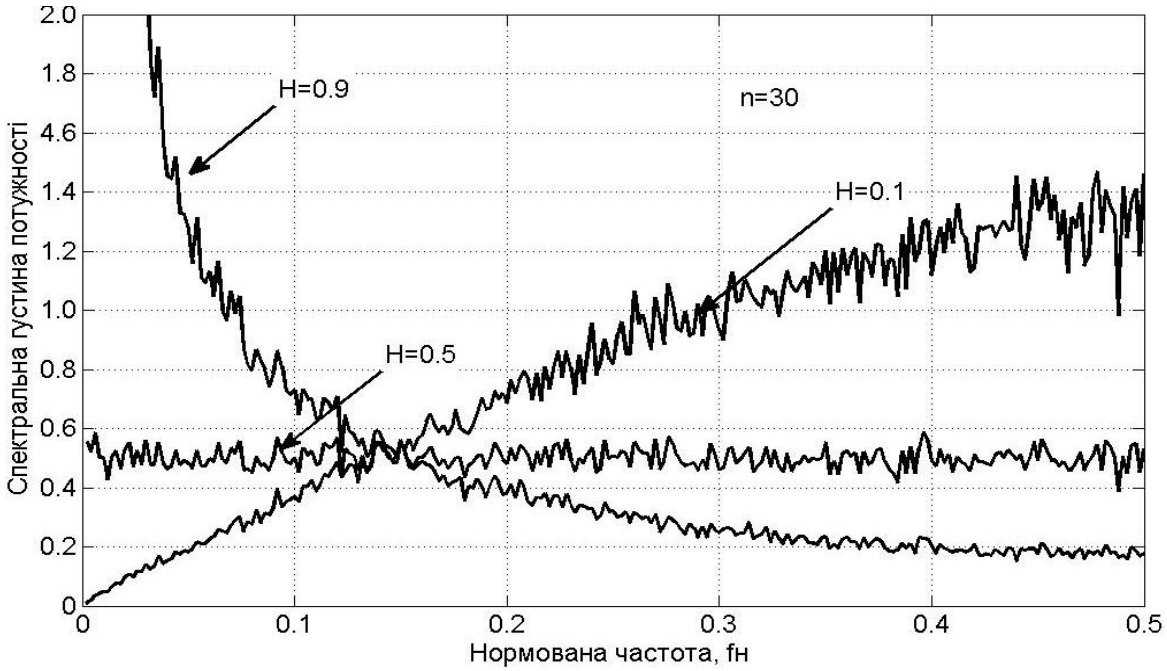
Для сигналу ФГШ, що формований 500 відліками, спектральна густина потужності дорівнюватиме:

$$W(\omega)=\frac{1}{1001}\cdot\overline{\left|\sum_{k=0}^{500}S(k\cdot T)\cdot e^{-j\cdot\omega\cdot k\cdot T}\right|^2}, \quad (5.13)$$

На рис. 5.7 приведена залежність спектральної густини потужності від нормованої частоти сигналів типу ФГШ з показниками Херста 0,1; 0,5 ; 0,8 при різних значеннях коефіцієнту часового масштабування.



а)



б)

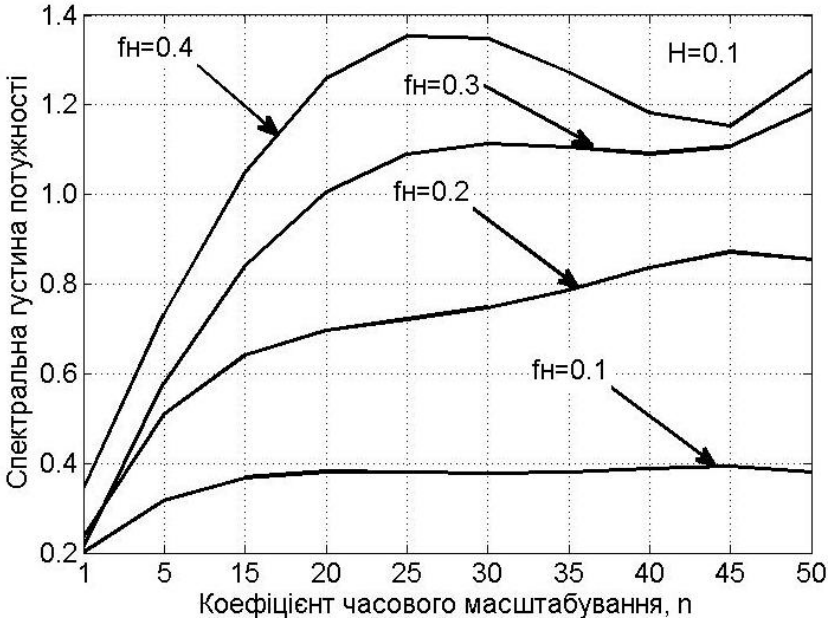
Рис.5.7. Залежність спектральної густини потужності від нормованої частоти сигналів ФГШ з показниками Херста 0,1; 0.5; 0.9 при значеннях коефіцієнтів часового масштабування: (а) –n=1; (б) –n=30.

Із отриманих залежностей випливає, що залежність спектральної густини потужності сигналів ФГШ з показником Херста H=0.5 є ідентичною зі спектром білого гаусового шуму у всьому діапазоні нормованих частот.

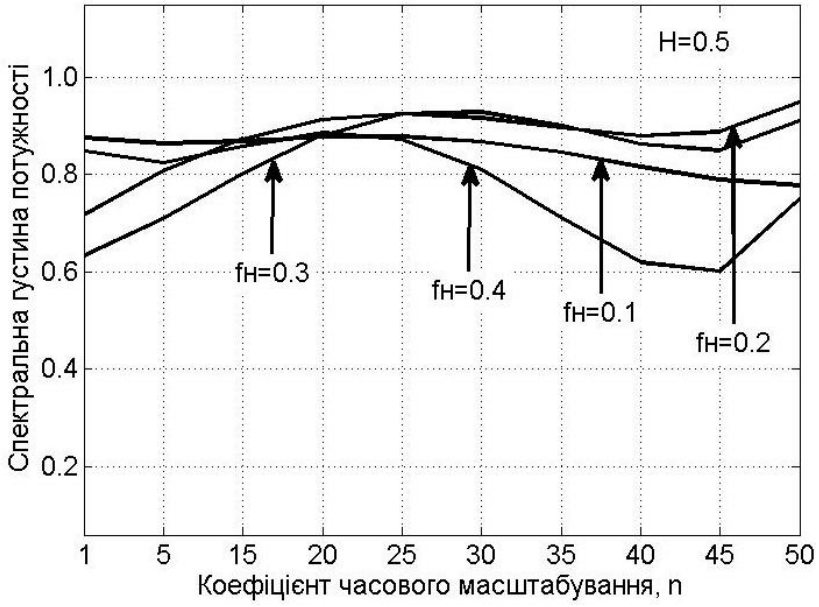
Для сигналів ФГШ з показником Херста $H = 0.9$ має місце домінуючий вплив низькочастотних складових при обох значеннях коефіцієнта часового масштабування. Залежність спектральної густини потужності від частоти сигналів ФГШ з H=0,1 при $n = 1$ є слабкою. При $n = 30$ спектральна густина потужності сигналів ФГШ з ростом частоти, зростає. Отримані результати стосовно характеру залежності спектральної густини потужності сигналів з різними показниками Херста корелюють із результати отриманими Мандельбротом [66], який встановив, що при збільшенні показника Херста високочастотна складова зменшується.

На рис.5.8 приведена розрахункова залежність спектральної густини потужності від коефіцієнту часового масштабування при значеннях

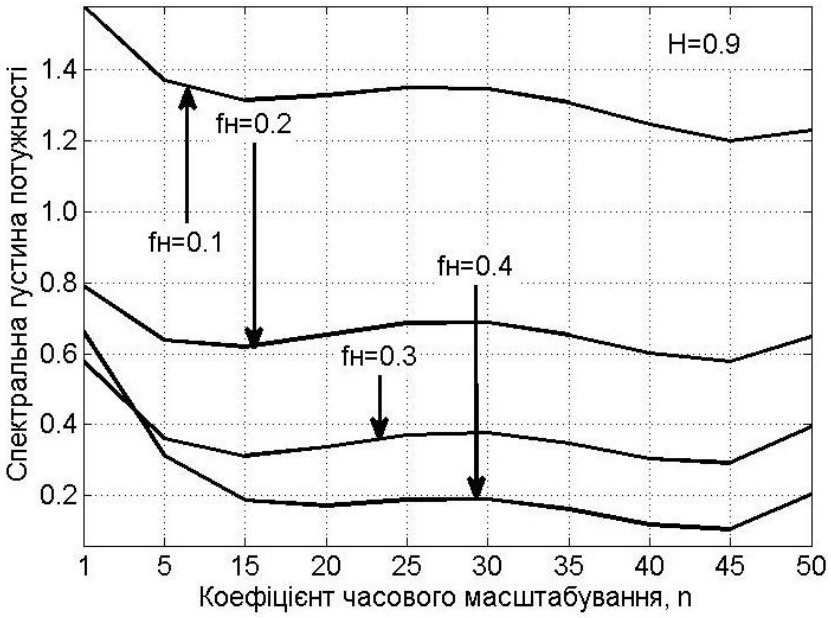
нормованої частоти $f_н = 0{,}1$; $f_н = 0{,}2$; $f_н = 0{,}3$; $f_н = 0{,}4$. На основі отриманих результатів можна зробити висновок про те, що у спектрі ФГШ із показником Херста H=0,1 збільшується частка високочастотної складової. Для ФГШ з показниками Херста H=0,5; H=0,9 значний вплив коефіцієнта часового масштабування на їх спектр не спостерігається. Така закономірність у спектрах ФГШ із вищезазначеними показниками Херста підтверджується залежностями, що приведені на рис. 5.8.



а)



б)

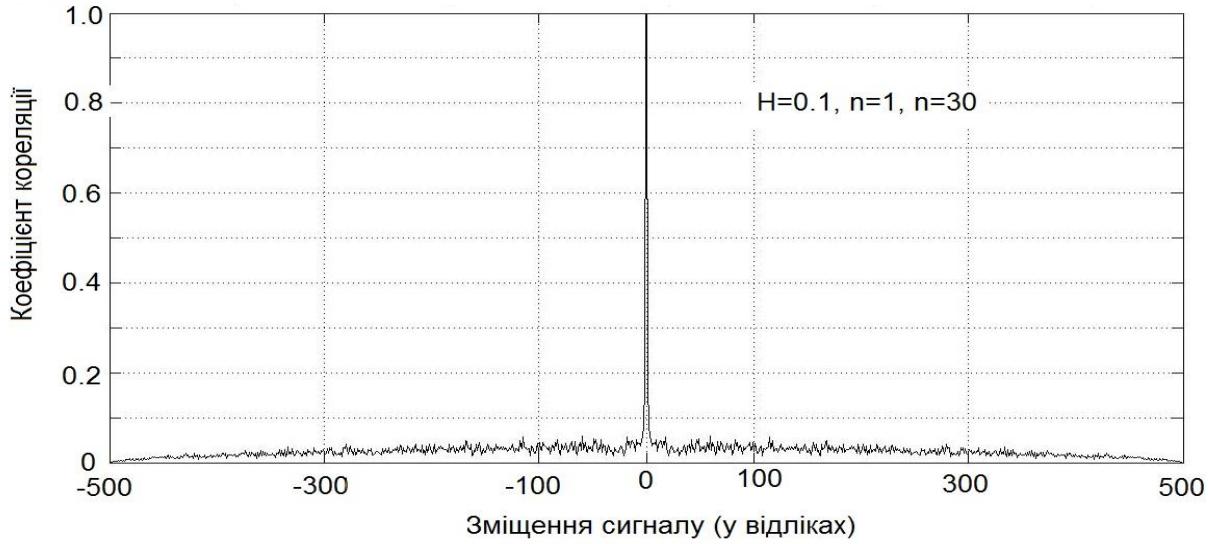


в)

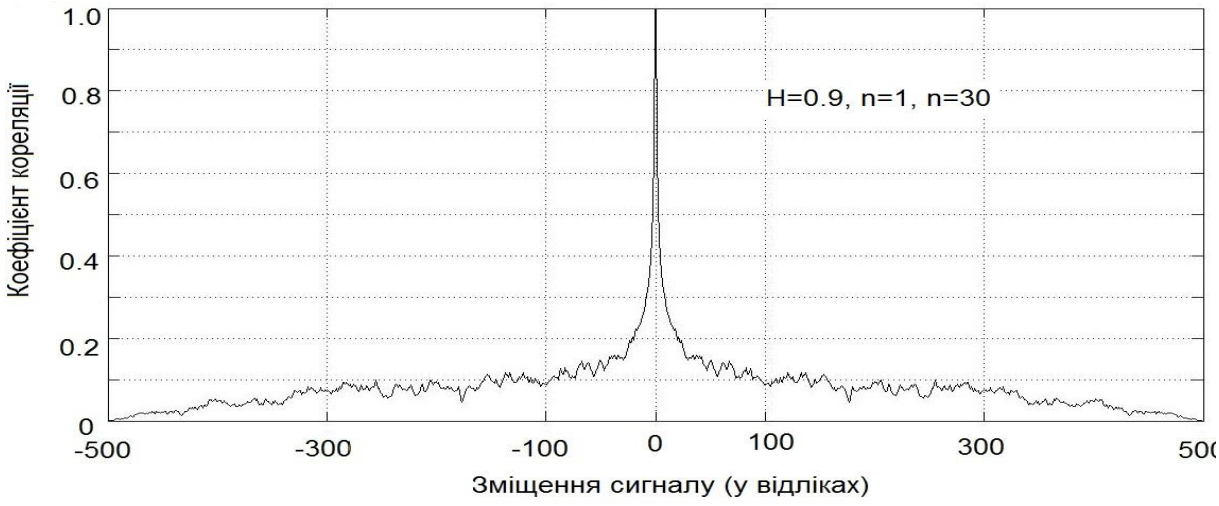
Рис.5.8. Залежність спектральної густини потужності сигналів ФГШ від коефіцієнту часового масштабування при значеннях показника Херста: H=0,1(а); H=0,5 (б); H=0,9 (в) і нормованих частотах f_H =0,1; 0,2; 0,3; 0,4.

Спектр ФГШ (рис.5.8) вказує на їх шумоподібний характер, що підтверджується також як залежностями їх автокореляційних функцій від часового зміщення між сигналами та їх копіями (рис.5.9) так їх часовими діаграмами (рис.5.6). Необхідно зауважити, що параметр часового масштабування не впливає на функцію автокореляції. Між функціями автокореляції сигналів типу ФГШ з показниками Херста H=0,9 та H=0,1; 0,5 має місце певна відмінність (рис.5.9).

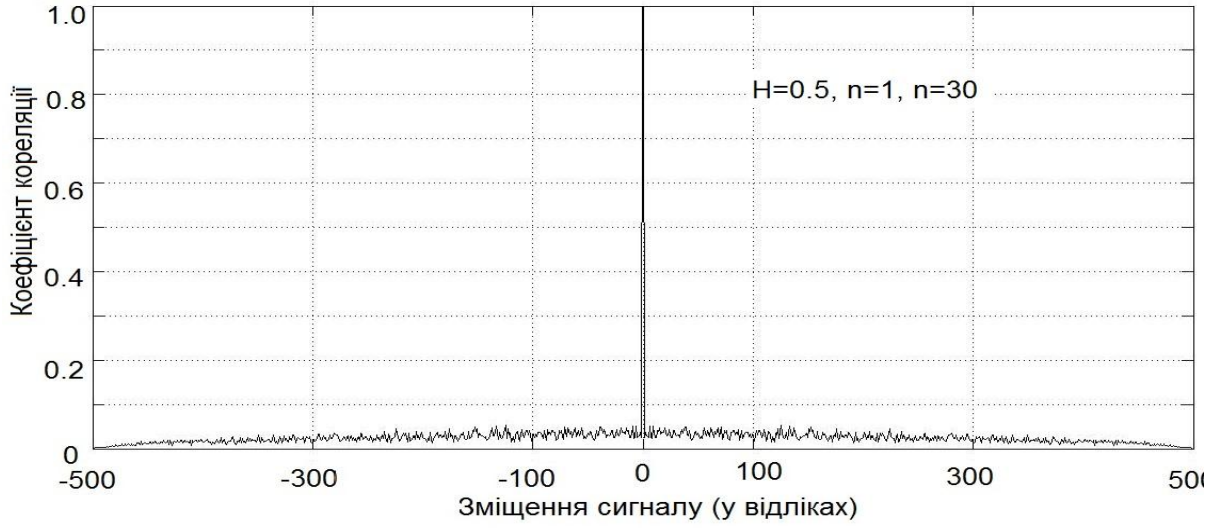
Із приведених залежностей (рис.5.9) випливає, що для сигналів з показниками Херста *H=0.1* та *H=0.5* спостерігається незначна кореляції сигналу з його копіями при їх часовому зсуві в межах від -500 до 500 відліків, а для сигналів з показником Херста *H=0.9* коефіцієнт автокореляції в зазначеному діапазоні приймає значення 0 ÷ 0,2.



а)



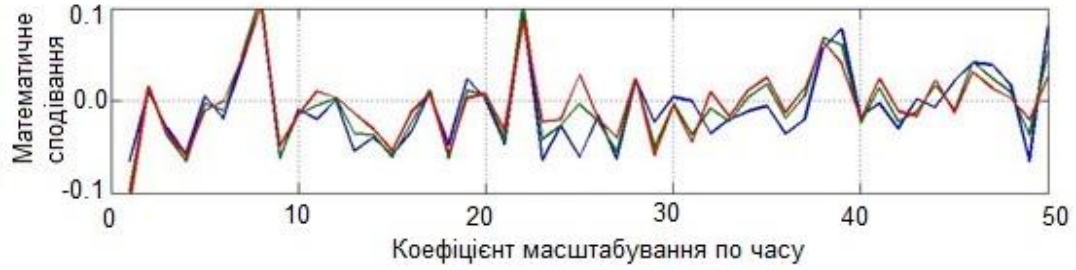
б)



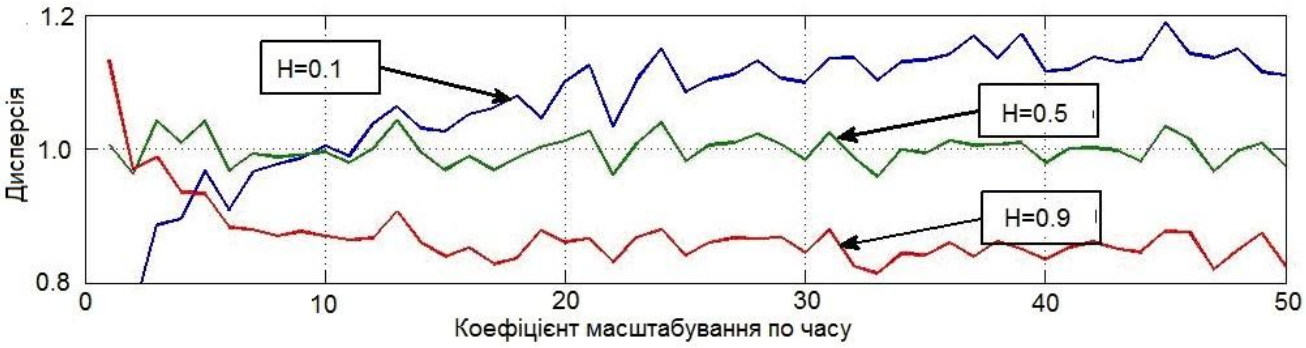
в)

Рис.5.9. Залежність автокореляційної функції ФГШ від зміщення між сигналом та його копіями при значеннях коефіцієнту масштабування n=1; 30 і показниках Херста: H=0,1 (а); H=0,5 (б); H=0,9(в)

На рис.5.10 приведені залежності математичного сподівання та дисперсії фрактального сигналу від значення коефіцієнту часового масштабування n, що впливає на точність проведення розрахунків. При зміні значення коефіцієнта n в межах від 1 до 20 має місце зростання дисперсії сигналу з показником Херста 0.1, а значення дисперсії сигналів з показниками Херста 0.9 і 0.5 в досліджуваному діапазоні значень коефіцієнта часового масштабування n залишаються незмінними в межах похибки розрахунків (рис.5.10, а). Математичне сподівання сигналів ФГШ з показниками H=0,1; 0,9; 0,5 не залежить від значення коефіцієнту масштабування по часу (рис. 5.10, б).



а)



б)

Рис.5.10. Залежність математичного сподівання (а) та дисперсії ФГШ з показниками Херста H=0,1; 0,5; 0,9 від коефіцієнту масштабування по часу

На рис.5.11а, б, в приведені розраховані розподіли густини ймовірності значень сигналів типу ФГШ з показниками Херста H = 0,1; 0,9; 0,5 та

координати броунівської частинки при різних значеннях коефіцієнту часового масштабування n.

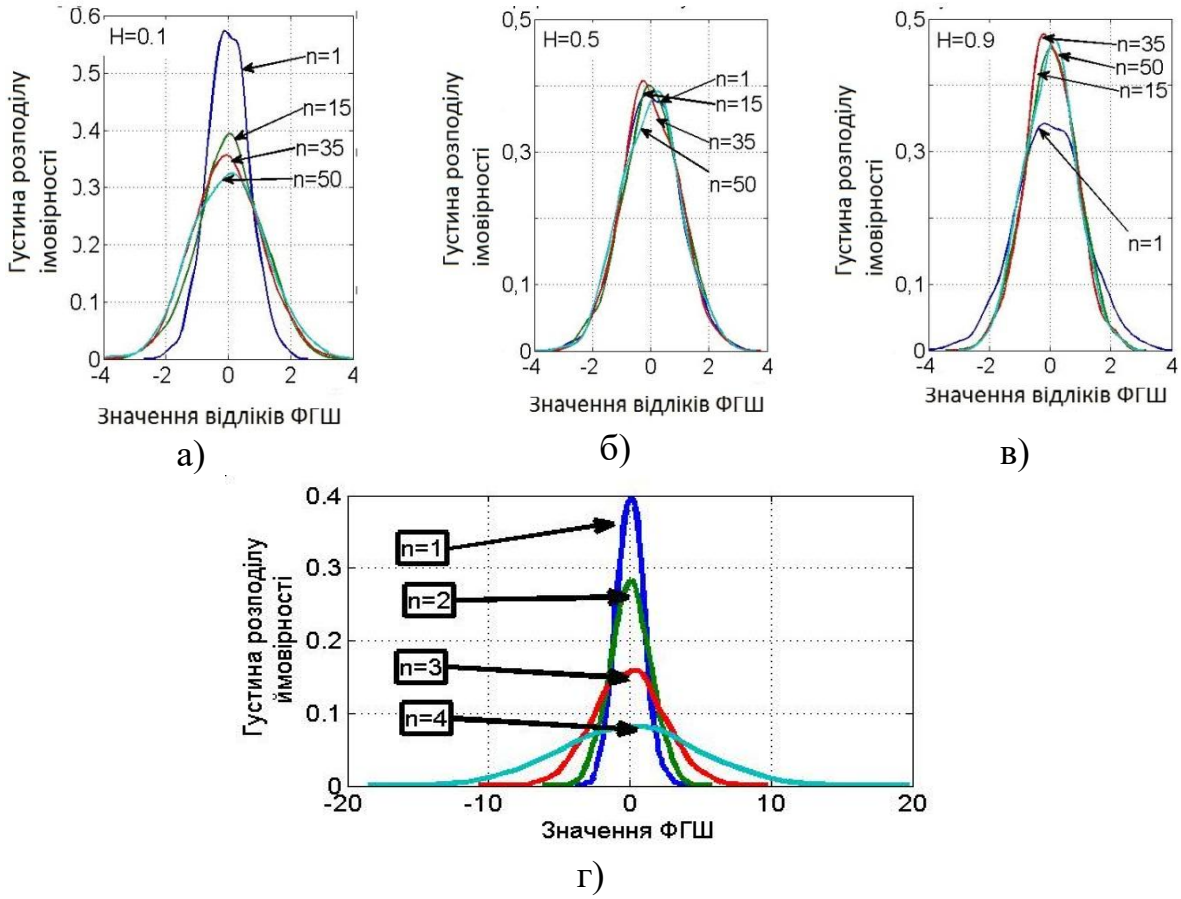


Рис. 5.11. Розподіл густини ймовірності значень сигналів ФГШ з показниками Херста формованих 500 відліками з показниками Херста H=0,1(а); H=0,5 (б); H=0,9 (в) та розподіл координат броунівської частинки при різних значеннях коефіцієнта часового масштабування (г)

Аналіз залежностей дозволяє зробити висновок, що розподіл густини ймовірності значень відліків ФГШ є гаусовим аналогічно розподілу значень координат броунівської частинки (рис. 5.11, г).

Як бачимо, максимальне значення густини розподілу значень сигналів типу ФГШ з показниками Херста H=0.1 зменшується при збільшенні коефіцієнта часового масштабування що аналогічне розподілу координат броунівської частинки.

Із отриманих результатів випливає, що форма кривих розподілу змінюється зі зміною значення коефіцієнта часового масштабування для сигналів з H=0,1 та 0,9. Це підтверджує отримані раніше результати стосовно збільшення дисперсії з ростом n для ФГШ з показником Херста H=0.1 та коливний характер залежності для сигналів з показником Херста H=0.9. Для сигналів з показником Херста H=0,5 значення дисперсії не залежить від n.

Шляхом моделювання було встановлено, що дисперсія ФГШ не залежить від кількості відліків сигналу (рис. 5.12).

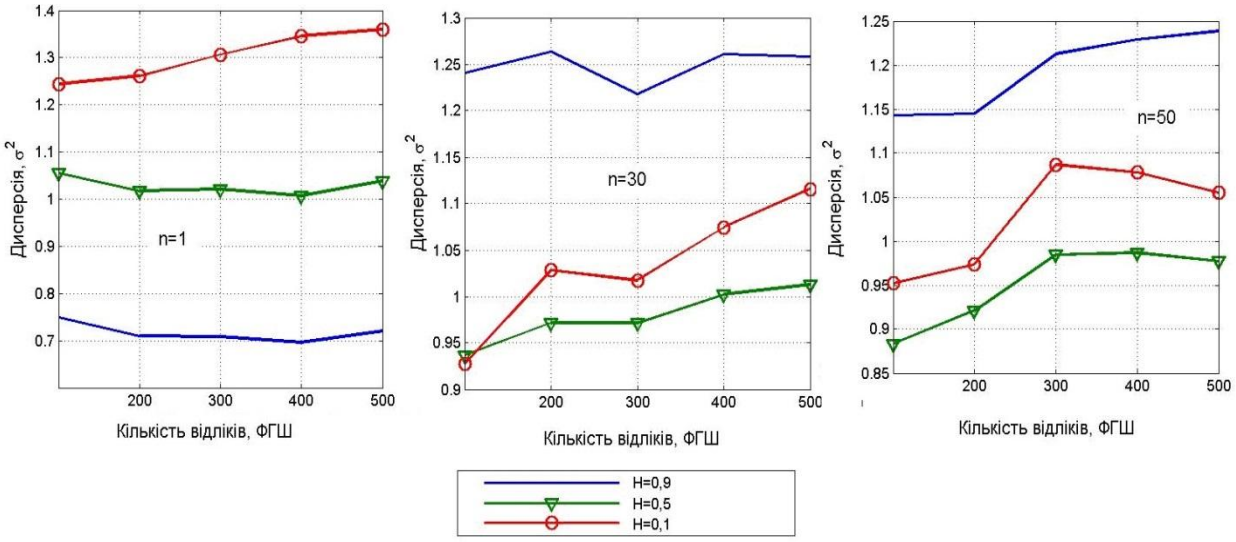


Рис.5.12. Залежність дисперсії ФГШ з показниками Херста H=0,9; 0,5; 0,1 від кількості відліків для різних значень коефіцієнтів часового масштабування:– n=1(а); n=30 (б) та n=50 (в)

На рис. 5.13 приведена залежність максимального значення густини ймовірності розподілу значень ФГШ з показником Херста H=0,1; 0,5; 0,9 від значення параметру масштабування. Для сигналу з показником Херста H=0.1 спостерігається зменшення максимального значення густини імовірності, що корелює з результатами, отриманими на основі аналізу гаусових кривих розподілу значень амплітуд ФГШ (рис.5.11).

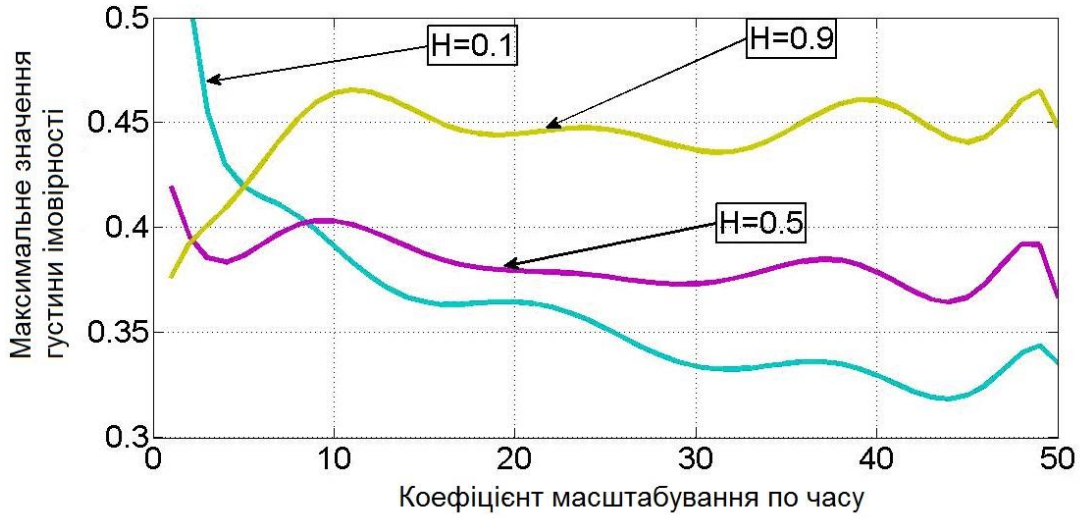


Рис. 5.13. Залежність максимального значення густини ймовірності розподілу значень ФГШ з показникми Херста H=0,1; 0,5; 0,9 від коефіцієнта масштабування по часу

5.3. Метод кластерного кодування інформації у телекомунікаційних системах на базі сигналів зі структурою ФГШ

За результатами досліджень властивостей сигналів типу ФГШ розроблений нами [17, 31, 48] метод кодування каналу зв'язку телекомунікаційної системи з використанням кластерів, що утворені сукупністю точок їх фазових портретів. Значення відліків фрактальних сигналів визначалися за виразом (5.11).

Слід очікувати, що фазові портрети сигналів ФГШ з різними показниками Херста відрізняються між собою. Таким чином, поставивши у відповідність інформаційним бітам «0» та «1» сигнали типу ФГШ з різними показниками Херста, можна здійснювати їх розпізнавання за фазовими портретами відповідних їм сигналів.

На рис.5.14 приведені кластери, утворені 300-ма відліками сигналів типу ФГШ, що є множинами точок їх фазового простору.

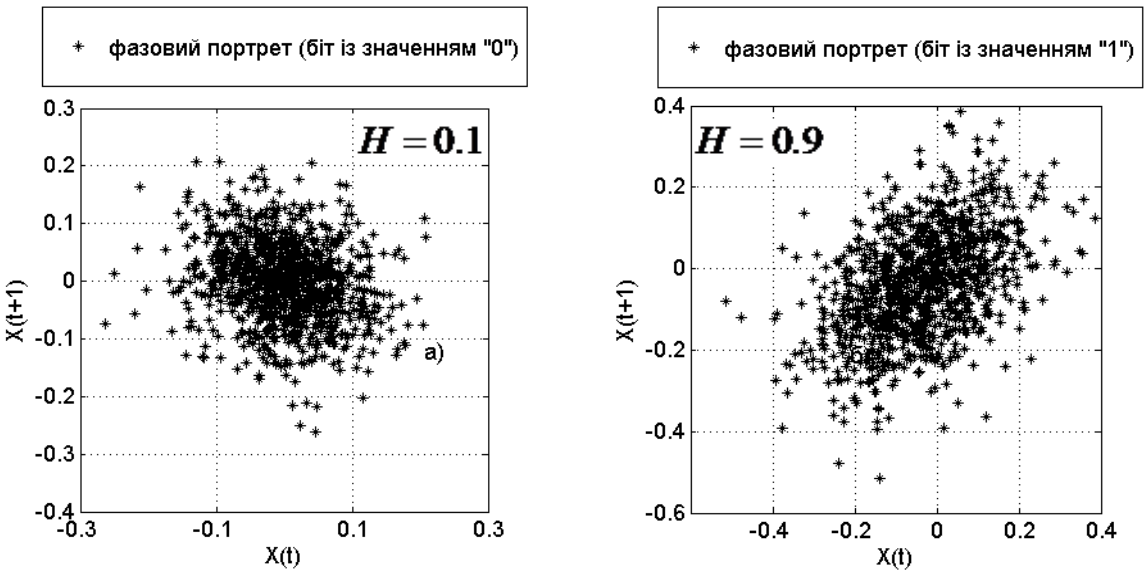


Рис. 5.14. Кластери сигналів ФГШ з показниками Херста H=0,1; 0,9 у фазовому просторі, що відповідають інформаційним бітам «0» (а) та «1» (б)

При цьому біту зі значенням «1» відповідає кластер, що є сукупністю точок у фазовому просторі, утворений 300-ма відліками носійного сигналу, генерованого при значеннях параметра Херста $H = 0.9$, а біту зі значенням «0» – кластер, що утворений 300-ма відліками носійного фрактального сигналу зі значенням параметра $H = 0.1$.

Встановивши критерій розпізнавання фазових портретів сигналів типу ФГШ, що відповідають логічним 1 і 0, можна здійснювати декодування інформаційних бітів. В якості такого критерію був вибраний названий нами параметр розпізнавання кластера, що є коренем квадратним із суми квадратів відстаней точок кластера від його центру (надалі називатимемо цю величину параметром розпізнавання кластера):

$$d_1 = \sqrt{\sum_{i=1}^{N}\left[\left(X^{(0.9)}(i) - X_0\right)^2 + \left(X^{(0.9)}(i+1) - Y_0\right)^2\right]} \qquad (5.14),$$

$$d_0 = \sqrt{\sum_{i=1}^{N}\left[\left(X^{(0.1)}(i) - X_0\right)^2 + \left(Y^{(0.1)}(i+1) - Y_0\right)^2\right]} \quad (5.15),$$

де

d_1 – параметр розпізнавання кластера, утвореного сигналом, що передає біт зі значенням «1»; d_0 – параметр розпізнавання кластера, утвореного сигналом, що передає біт зі значенням «0»; N – кількість відліків носійного сигналу;

$X_0 = \sum_{i=1}^{N} X(i)/N$, $Y_0 = \sum_{i=1}^{N-1} X(i+1)/N$ – координати центра кластера;

$X^{(0.9)}(i)$ –*i*-ий відлік носійного сигналу з показником Херста $H = 0.9$, що відповідає інформаційному біту «1»);

$X^{(0.1)}(i)$ –*i*-ий відлік носійного сигналу з показником Херста $H = 0.1$, що відповідає інформаційному біту «0»);

При цьому має місце співвідношення:

$$\begin{aligned} Y^{(0.1)}(i) &= X^{(0.1)}(i+1) \\ Y^{(0.9)}(i) &= X^{(0.9)}(i+1) \end{aligned} \qquad (5.16)$$

Похибка визначення параметру розпізнавання кластера, що виникає внаслідок особливостей генерування програмним середовищем MATLAB множини з розподілом Гауса визначалася шляхом багатократного проведення однотипних обчислень з подальшим усередненням отриманих результатів. Результати обчислень показують, що при значеннях 1⋯10 розпізнавального параметру похибка його визначення не перевищує 5%.

На рис.5.15 приведені розрахункові залежності значень параметрів розпізнавання кластерів носійних сигналів типу ФГШ від кількості їх відліків для інформаційного біта «1» та «0» при відсутності шумів у каналі.

Ефективність кластерного канального кодування оцінювалась для каналу з білим адитивним гаусовим шумом (AWGN). Очевидно, що в розробленій системі можливе безпомилкове розпізнавання сигналів логічного нуля та одиниці при умові, якщо різниця між значенням відповідних параметрів розпізнавання кластерів, що відповідають логічним 1 та нуля, за абсолютною величиною більша за похибку обчислення:

$$|d_1 - d_0| > \varepsilon, \qquad (5.17)$$

де

ε – похибка визначення параметра розпізнавання кластерів.

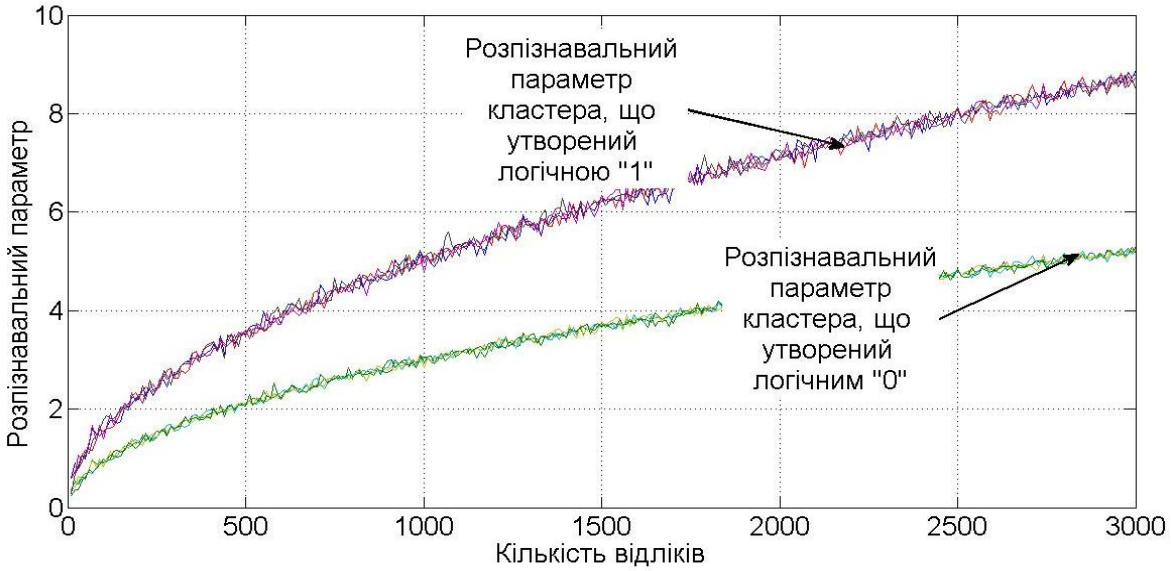


Рис. 5.15. Залежність значень параметрів розпізнавання кластерів сигналів типу ФГШ, що відповідають інформаційним бітам «1» та «0» від кількості їх відліків

Дослідження впливу шуму каналу на якість передавання інформації здійснювалася шляхом додавання до переданого сигналу адитивного білого гаусового шуму.

При цьому значення відліків сигналу, що поступає з каналу на вхід приймача, дорівнює:

$$X_r^{(H)}(i) = X^{(H)}(i) + R(i), \qquad (5.18)$$

де

$X_r^{(H)}(i)$ – значення відліків сигналу на вході приймача;

$X^{(H)}(i),\ R(i)$ – значення відліків сигналу та шуму на виході передавача.

Якість передавання інформації в умовах наявності шуму в каналі визначалася за мінімальним значенням співвідношенням сигнал/шум, при

якому можливе розпізнавання інформаційних бітів:

$$SNR = 10 \cdot \lg\left[\frac{P_c}{P_ш}\right], \qquad (5.19)$$

де

P_c – потужність сигналу;

$P_ш$ – потужність шуму.

Оскільки математичне сподівання сигналів типу ФГШ дорівнює нулю, то для P_c і $P_ш$ матимемо:

$$P_ш = D(R), \text{ (5.20);}$$

$$P_c = D\left(X^{(H)}\right), \qquad (5.21)$$

де

$D(R)$ та $D\left(X^{(H)}\right)$ – дисперсії адитивного білого гаусового шуму в каналі системи зв'язку та носійного сигналу ФГШ відповідно.

Значення дисперсії $D(R)$ сигналу, що моделює завади в каналі, задавалися генеруванням підпорядкованим гаусовому розподілу значень числових рядів в межах 0,01…10. За граничне значення відношення сигнал/шум приймалося значення, при якому розпізнавальні параметри кластерів рівні між собою. Значення дисперсії $D\left(X^{(H)}\right)$ робочих сигналів ФГШ становили від 0,5 (при H=0.1) до 1,4 (при H=0.9).

Отримані в результаті моделювання залежності мінімальних значень сигнал/шум від кількості відліків, при яких можливе розпізнавання інформаційних бітів для різних статистичних реалізацій, приведені на рис.5.16. Із отриманих результатів випливає, що співвідношення с/ш, при якому можливе розпізнавання зменшується від 10 ДБ при 50 відліках до 0 ДБ при 100 відліках. При 500 відліках це співвідношення становить -7.5 Дб. Похибка обчислення співвідношення с/ш становила 2.5 ДБ. Підвищення точності можливо при значному збільшенні обсягів обчислень шляхом

використання технологій паралельного програмування на кластерних обчислювальних системах.

Рис. 5.16. Залежність мінімального значення сигнал/шум, необхідного для розпізнавання бітів інформаційної послідовності від кількості відліків носійних сигналів різних статистичних реалізацій

Криві, що приведені на рис.5.16, відповідають різним статистичним реалізаціям сигналів типу фрактальний гаусовий шум, що використовуються для передавання логічних «0» та «1». На основі отриманих результатів можна зробити висновок, що завадостійкість зростає зі збільшенням кількості відліків сигналів використовуваних для передавання бітів «1» та «0».

Граничне значення відношення сигнал/шум не залежить від методу декодування, а визначається роздільною здатністю розпізнавального параметру кластерів (рис.5.17).

На рис.5.17 приведені залежності нормованих значень розпізнавальних параметрів кластерів на значення в точці їх рівності, що утворені зашумленими сигналами типу ФГШ, (з показниками Херста H=0,9 та 0,1) від співвідношення сигнал/шум. Кількість відліків сигналів ФГШ становить 500.

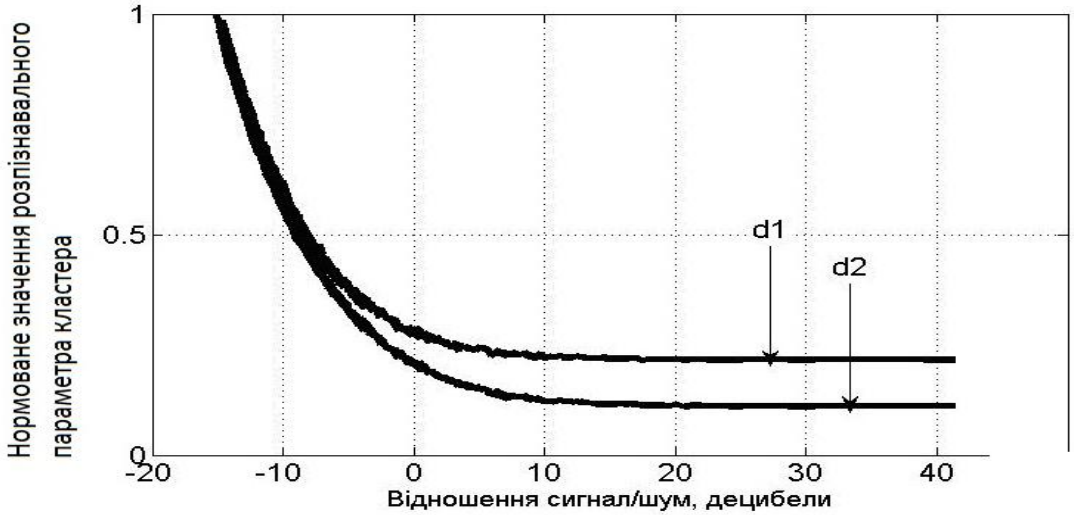


Рис.5.17. Залежності нормованих значень параметрів розпізнавання кластерів в точці їх рівності за наявності гаусового шуму в каналі зв'язку від відношення сигнал/шум. d_1, d_2 – розпізнавальні параметри ФГШ з показником Херста H=0,9 та H=0,1 – а) і б) відповідно

В результаті проведених досліджень розроблена [31] структурна схема системи передавання інформації з кластерним кодуванням (рис.5.18), принцип роботи якої полягає в наступному.

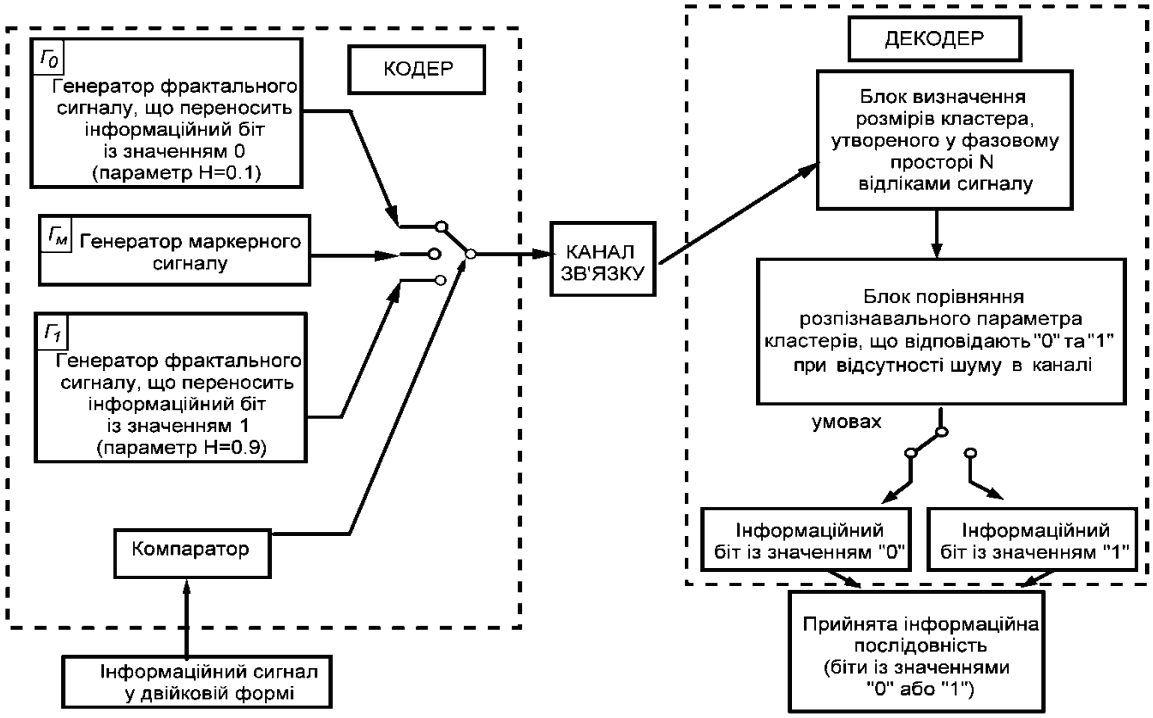


Рис. 5.18. Структурна схема системи передавання інформації з кластерним кодуванням.

При надходженні на вхід компаратора логічної одиниці (рис.5.18) вмикається генератор носійного сигналу Γ_1, що генерує для кодування логічної «1» сигнал зі значенням параметра Херста $H = 0.9$, а при надходженні логічного нуля вмикається генератор сигналів Γ_0, що генерує для кодування логічного «0» сигнал зі значенням параметра Херста $H = 0.1$.

Декодування інформації відбувається шляхом порівняння значення параметру розпізнавання прийнятого фрактального сигналу зі значенням параметру розпізнавання фрактальних сигналів, що відповідає логічній одиниці та нулю, переданих по каналу без шуму.

Розпізнавання бітів здійснювалося за значеннями параметрів розпізнавання сигналів, d_1 і d_2, що визначаються за формулами (5.14 та 5.15):

На рис.5.19 приведена часова діаграма інформаційної послідовності 1100111100, закодованої методом кластерного кодування з використанням маркерного сигналу.

З діаграми можна зробити висновок про хаотичний характер закодованої послідовності.

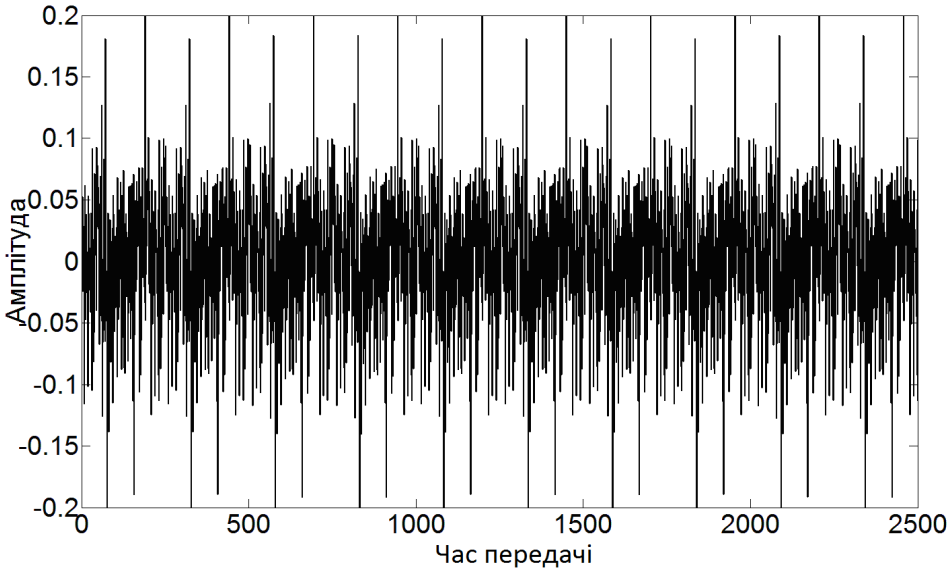


Рис. 5.19. Часова діаграма закодованої кластерним методом інформаційної послідовності 1100111100 за умов відсутності шуму в каналі при 200-х та 50-ти відліках носійного та маркерного сигналів відповідно

З метою забезпечення синхронізації передавальної та приймальної сторін системи зв’язку у проміжку між передаванням закодованих інформаційних бітів через канал зв’язку передаються маркерні сигнали, формовані генератором $Г_м$ зі значенням параметра Херста $H=0.4$.

Моделювання процесу синхронізації приймальної та передавальної сторін системи передавання інформації здійснювалося з використанням маркерних сигналів, що передаються в проміжку між сусідніми інформаційними бітами (рис. 5.20).

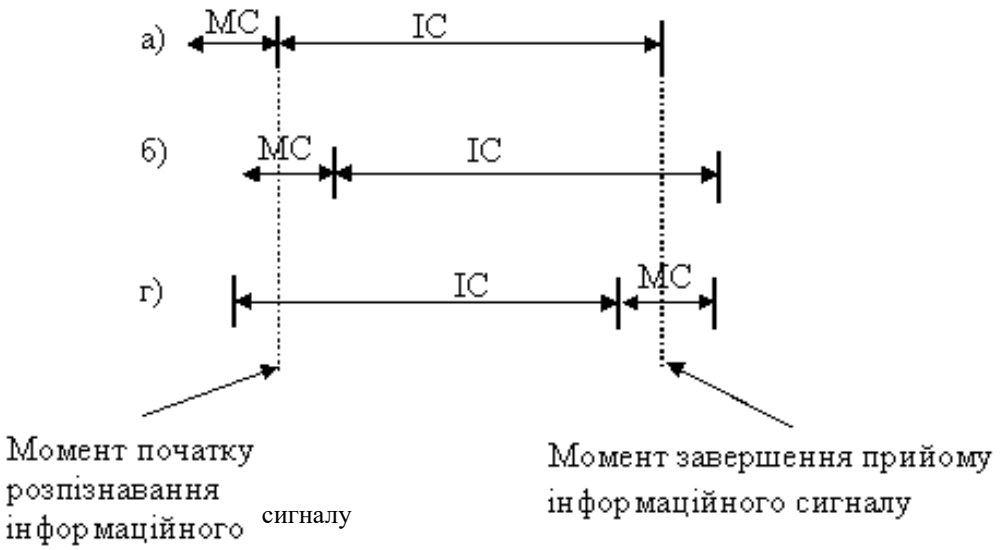


Рис. 5.20. Маркерна синхронізація приймальної та передавальної сторін системи передавання інформації. Помилка синхронізації відсутня (а); синхронізація відбувається із запізненням (б) та синхронізація відбувається із випередженням (в). (ІС – інформаційний сигнал, МС – маркерний сигнал)

Тривалість маркерного сигналу зазвичай є меншою ніж тривалість сигналів, що відповідають інформаційним бітам. У випадку ідеальної синхронізації сигналів (рис.5.20,а) момент приймання інформаційного біту розпізнається приймачем без будь-якої похибки. Якщо виникає помилка в синхронізації, то можливе приймання маркерного сигналу в якості інформаційного.

Результати чисельного моделювання процесу синхронізації у досліджуваній системі кластерного кодування були отримані при тривалості маркерного сигналу, що дорівнює 50 відлікам. Тривалість сигналів, що передають інформаційні біти змінювалась у межах від 50 до 500 відліків при значеннях помилки синхронізації 10, 20, 30 та 40 відліків маркерного сигналу (рис.5.21). Наявність похибки синхронізації призводить до зниження завадостійкості системи передавання інформації.

Результати проведеного моделювання процесу синхронізації показують, що система кластерного кодування є досить стійкою до десинхронізації за умови передавання додаткового маркерного сигналу.

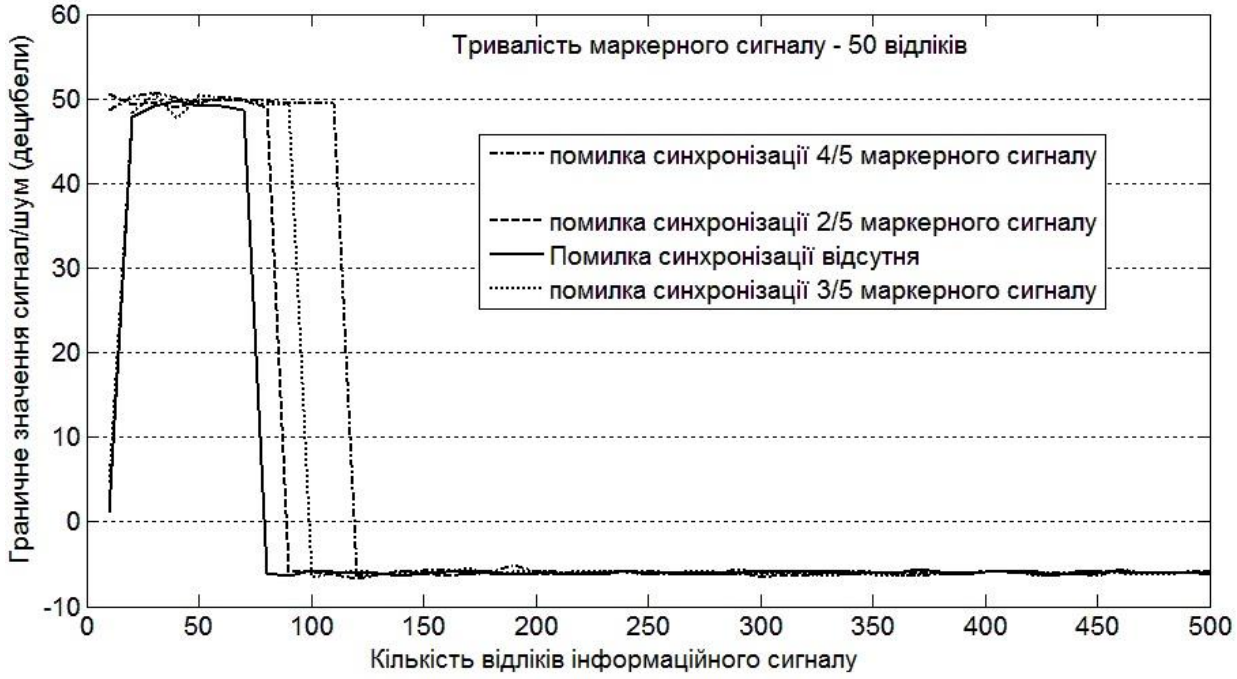


Рис.5.21. Залежність граничного значення сигнал/шум від кількості відліків інформаційного сигналу при різних значеннях помилки синхронізації

Із отриманих результатів моделювання процесу синхронізації (рис.5.21) випливає, що система є стійкою до похибки встановлення початку відліку інформаційного сигналу. Її максимальне значення якої становить 0,8 % значень тривалості маркерного сигналу. Забезпечення завадостійкості системи при цьому досягається збільшенням порогового значення кількості

відліків (від 60 до 140), при якому граничне значення співвідношення сигнал/шум суттєво зменшується.

Нами [31] розроблена система передавання інформації, розпізнавання інформаційних бітів в якій здійснюється без використання маркерного сигналу. У розробленій системі (рис.5.22) бінарні символи повідомлення подаються парою імпульсів протилежної полярності однакової тривалості та амплітуди [54]. Символ 1 подається парою імпульсів – додатнім і від'ємним, а 0 – від'ємним і додатнім.

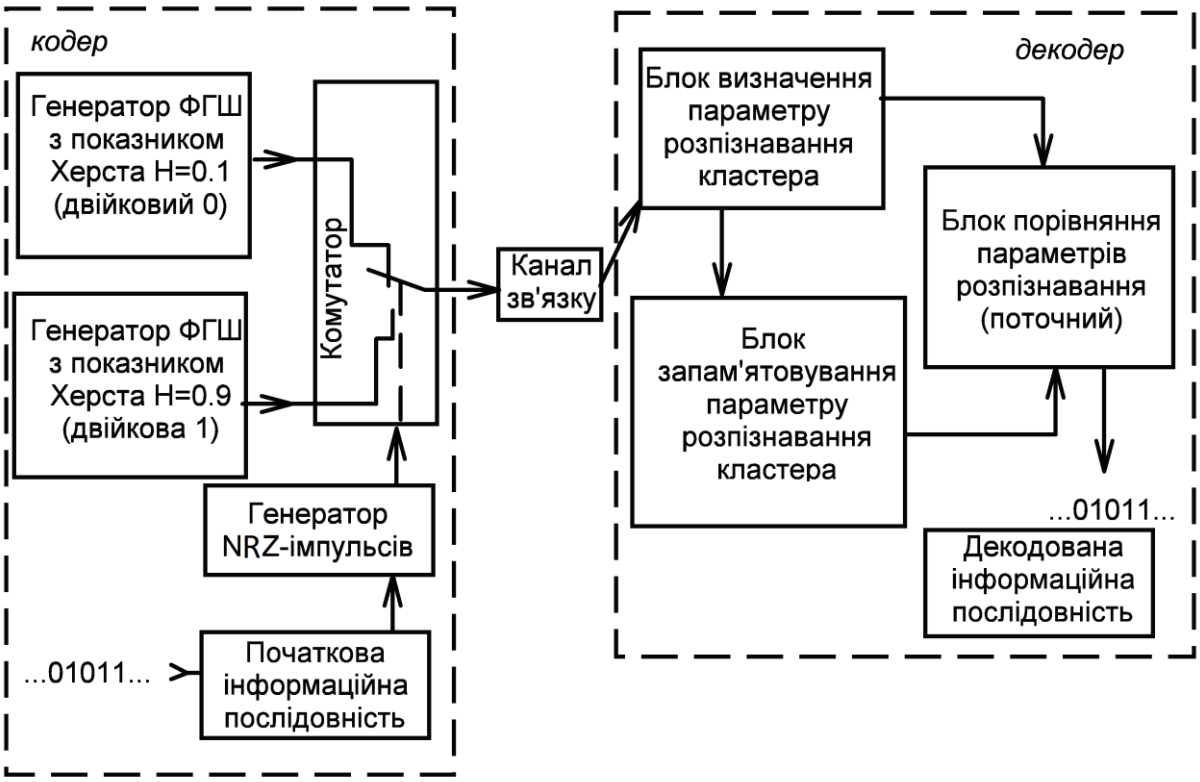


Рис. 5.22. Блок-схема системи передавання інформації із застосуванням кластерного кодування за низьким та високим рівнями манчестерського цифрового формату

Таким чином, біполярні символи будуть кодуватися двома хаотичними сигналами. Символ 1 кодуватиметься спочатку сигналами типу ФГШ з показником Херста рівним 0,9 на протязі першої половини тривалості біта, а на другій половині – сигналом типу ФГШ з показником Херста рівним 0,1.

Біполярний символ 0 буде кодуватися сигналами типу ФГШ в

оберненому порядку. На протязі першої половини – сигналом типу ФГШ з показником Херста рівним 0,1, а на протязі другої половини – сигналом типу ФГШ з показником Херста рівним 0,9.

Таким чином, якщо різниця між значеннями параметра розпізнавання сигналу, переданого на протязі другої половини тривалості біта співпадає зі значенням розпізнавання параметра, переданого на протязі першої половини тривалості наступного біта не перевищує похибку вимірювань, то сусідні біти матимуть значення 10 або 01. Якщо ця різниця буде більшою, ніж похибка обчислень, то сусідніми бітами будуть 00 або 11.

В розробленій СПІ знання рівня шуму каналу для декодування цифрових інформаційних сигналів є не обов'язковим, оскільки для прийняття рішення стосовно прийнятого біту достатньо мати значення першого біту. Рішення стосовно значення наступного біту приймаються за різницею значень їх розпізнавальних параметрів. На рис 5.23 приведені часові діаграми вихідної та зашифрованої послідовності 10100.

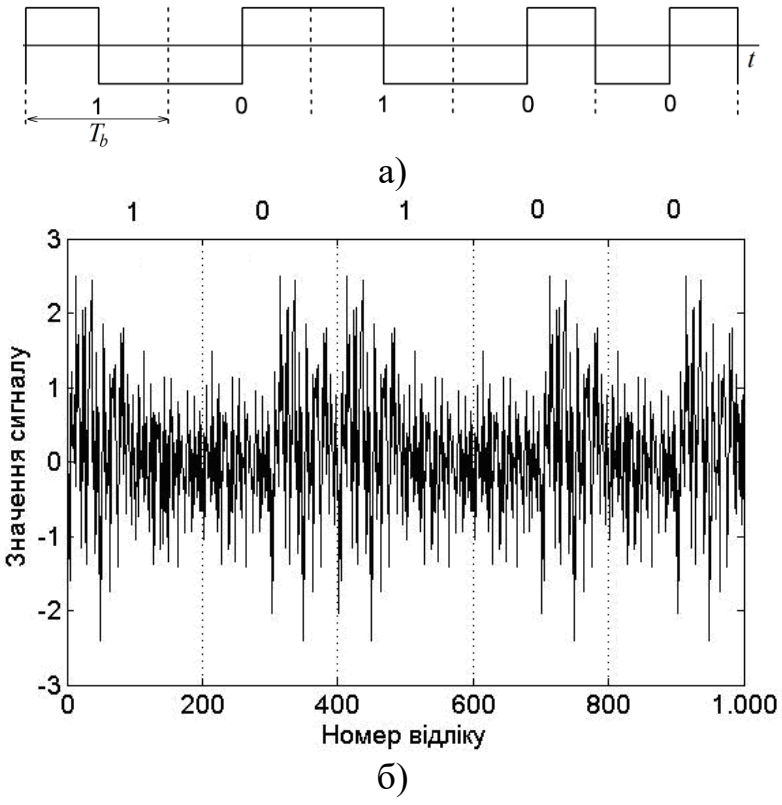


Рис. 5.23. (а) – вихідна інформаційна послідовність «10100»; б) – закодований хаотичний сигнал для послідовності «10100»

Напрям дослідження систем передавання інформації, що використовують фрактальні сигнали, виник недавно, і кількість праць, присвячених даній тематиці є відносно невеликою, що обумовлено складністю генерування таких сигналів. Проте підвищення швидкодії мікропроцесорної техніки уможливлює апаратну реалізацію таких систем [176]. Привабливою особливістю фрактальних сигналів є їх широкосмуговатість, внаслідок чого вони можуть забезпечити роботу систем передавання інформації в умовах багатопроменевого поширення сигналів.

На сьогоднішній день відомі системи передавання інформації з використанням сигналів типу «фрактальний вейвлет» та фрактальний гаусовий шум [175-179]. Сигнали типу «фрактальний вейвлет» генеруються шляхом застосування алгоритму оберненого перетворення Фур'є до сигналу, спектр якого має властивість геометричної самоподібності. Для передавання біта зі значенням «1» використовується фрактальний сигнал певної тривалості, а для передавання біта зі значенням «0» використовується пауза, або відсутність сигналу.

У системі, що базується на сигналах типу ФГШ детектування бітів інформаційного повідомлення здійснюється за оцінюванням функції максимальної правдоподібності [177].

Основою розробленого [17, 31] методу кластерного кодування та системи приймання-передавання інформації є кодування розпізнавання інформаційних бітів за кластерами сигналів типу ФГШ.

Порівняльні характеристики систем передавання інформації з використанням різних методів генерування хаотичних сигналів приведені в таблиці 5.1.

Отримані результати можна порівняти із іншими методами, що використовуються в системах з високим рівнем шумів у каналі. Зокрема, може бути використаний метод, що базується на синхронізації хаотичних генераторів передавача та приймача (табл. 5.1). Але у таких системах значення аналогічного рівня граничного відношення сигнал/шум можливий

за умови майже однакових значень параметрів хаотичних систем. Якщо рівень розкиду значень електропараметрів компонентів перевищує 2%, то синхронізація неможлива [22].

Таблиця 5.1.

Характеристики систем передавання інформації з використанням хаотичних сигналів у якості носійних

№ п/п	**Тип носійного сигналу**	**Спосіб кодування інформаційних бітів**	**Стеганографія**	**Граничне значення відношення сигнал/шум**
1	Фрактальний гаусів шум	Кластерне кодування	+	-7,5 дБ
2	Фрактальний вейвлет	Відсутність сигналу у випадку логічного нуля, сигнал заданої тривалості у випадку логічної одиниці	-	-10 дБ
3	Хаотичний сигнал, генерований системою Реслера	Синхронізація генераторів передавача та приймача	+	-10 дБ
4	Фрактальний гаусів шум	Визначення функції максимальної правдоподібності	+	10 дБ

Завадостійкість СПІ із кластерним кодуванням є порівняна із завадостійкістю систем, що використовують фрактальні сигнали типу «вейвлет» [176] або хаотичні сигнали, генеровані системою Реслера. Але на відміну від запропонованої нами системи, система з використанням фрактального сигналу типу «вейвлет» не володіє властивістю стеноганографії, оскільки один із бітів при цьому кодується відсутністю сигналу. Крім того, для реалізації генераторів за системою Реслера необхідно

забезпечити розкид електричних параметрів електронних компонентів не більше 2%.

5.4. Моделювання проходження трафіку у телекомунікаційній системі на основі систем масового обслуговування з вхідним потоком, що моделюється фрактальним гаусовим шумом

Сигнали типу ФГШ можуть бути застосовані у телекомунікаційних системах для дослідження проходження трафіків, що обумовлено притаманною їм властивістю самоподібності [214]. Нами досліджені проходження трафіку в телекомунікаційній системі з використанням моделей систем масового обслуговування з потрійною маршрутизацією. При цьому проводилось порівняння проходження трафіків, що описуються ймовірною моделлю з рівномірним та Пуассонівським розподілом і самоподібним з різними показниками Херста [2].

При моделюванні ТКС широко використовуються аналітичні методи теорії систем масового обслуговування (СМО), імовірнісно-часові графи, диференційні та різницеві рівняння, кольорові мережі Петрі [208, 215]. Ці методи уможливлюють отримання аналітичних розв’язків доволі складних систем, але за умови, що вхідний потік СМО описується імовірнісною моделлю з рівномірним або пуасонівським розподілом.

У той же час в літературних джерелах, де описані експериментально отримані часові діаграми інтенсивності трафіку, зокрема в мережі Інтернет, вказують на те, що вхідний процес є складнішим [214]. Тому для моделювання проходження трафіку в ТКС доцільно вибрати метод імітаційного моделювання СМО, важливою особливістю якого на відміну від аналітичних методів моделювання СМО, придатних для потоків з рівномірним розподілом, є можливість вибору довільної імовірнісної моделі вхідного потоку.

Моделювання топології телекомунікаційної мережі, що використовує багатоканальну маршрутизацію Інтернет-трафіка приведена на рис.5.24.

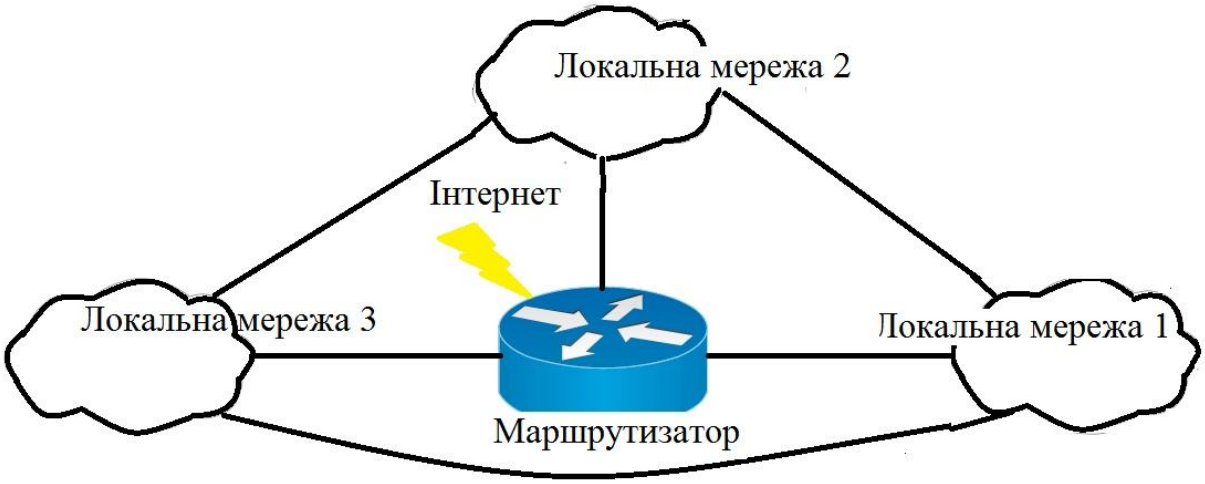


Рис.5.24. Топологія mesh-мережі з багатоканальною маршрутизацією

Моделювання здійснювалось з використанням програм пакету State Flow Simulink для 3-канальної системи масового обслуговування з буферизацією завдань та безмежною чергою (рис.5.25) в припущенні, що пропускна здатність кожного вузла та інтенсивність вхідного потоку дорівнюють 60 та $1.8 \cdot 10^3$ запитів за годину відповідно.

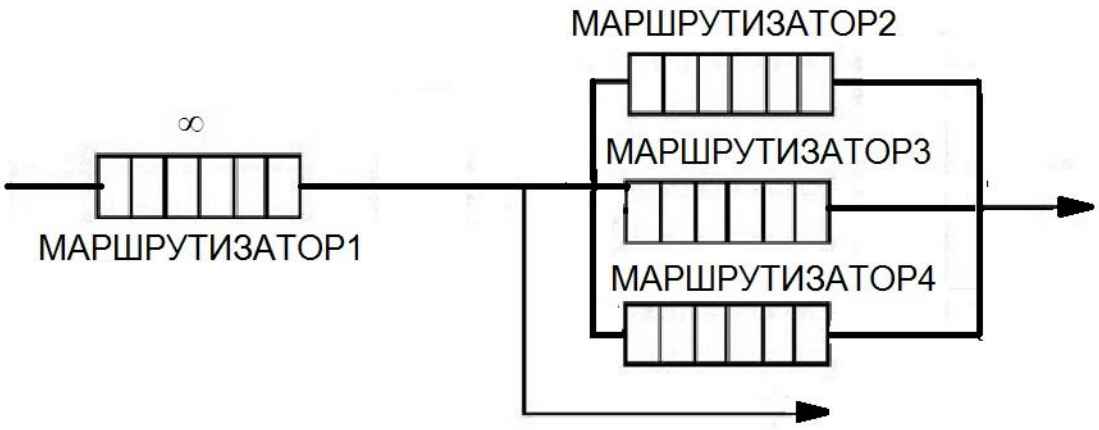


Рис.5.25. Багатокагальна модель мережі з маршрутизацією та буферизацією пакетів (МАРШРУТИЗАТОР1 – маршрутизатор з нескінченною чергою, МАРШРУТИЗАТОР2, МАРШРУТИЗАТОР3, МАРШРУТИЗАТОР4 – паралельні маршрутизатори з скінченною чергою)

Пуасонівський потік (рис.5.26) є випадковим процесом, що характеризується значенням імовірності кількості запитів *N*:

$$p(N,\tau) = \frac{(\lambda \cdot \tau)^N \cdot e^{-\lambda \cdot \tau}}{N!} \quad (5.22),$$

де N — кількість запитів, τ — час надходження запитів, $p(N,\tau)$ — імовірність того, що протягом часу τ надходить N запитів, λ — інтенсивність потоку.

Для моделювання самоподібних потоків використовувався так званий фрактальний гаусів шум, математична модель якого описується виразом (5.11). Генерування дійсних чисел ξ_i із гаусовим розподілом за алгоритмом Бокса-Міллера базується на використанні двох різних лінійних конгруентних генераторів.

Суть розробленого нами методу моделювання трафіку із самоподібним розподілом полягає у наступному:

– від генерованих у відповідності з виразом (5.11) значень віднімаємо мінімальне значення того ж числового ряду, що уможливлює отримання трафіку з невід'ємними значеннями;

– члени утвореного числового ряду помножуємо на однаковий коефіцієнт, значення якого вибираємо за умови, щоб отримані числові ряди мали однакові значення інтенсивності;

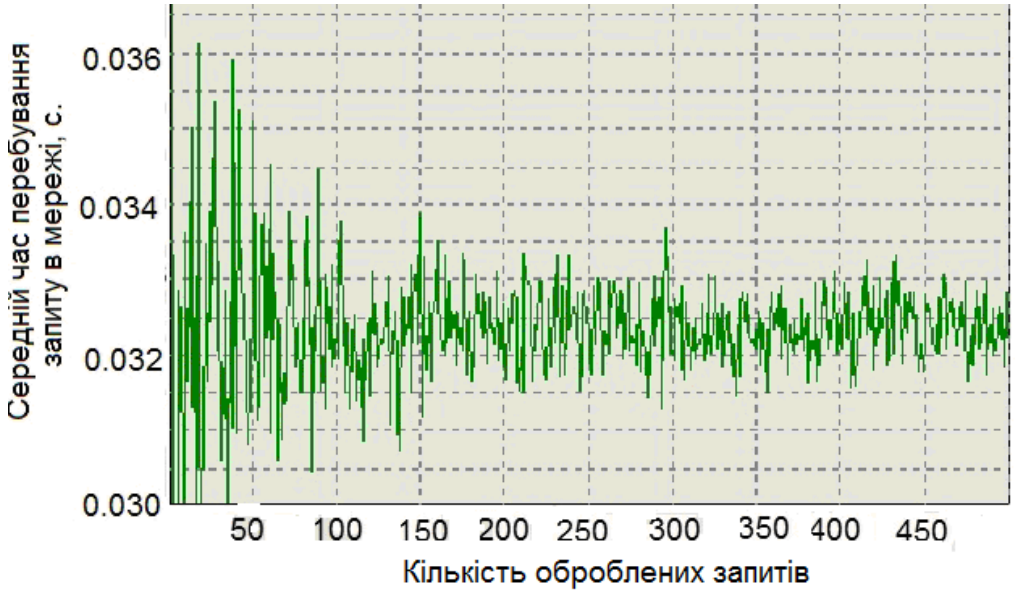
– отримані значення заокруглюємо до цілого числа, поскільки вони являють собою кількість пакетів, що надходять у мережу за один часовий інтервал, і є однаковою для усіх видів трафіку;

– часові проміжки між надходженнями пакетів протягом однієї часової ітерації у системі вважаємо оберенено пропорційними до кількості пакетів, що поступили протягом однієї ітерації.

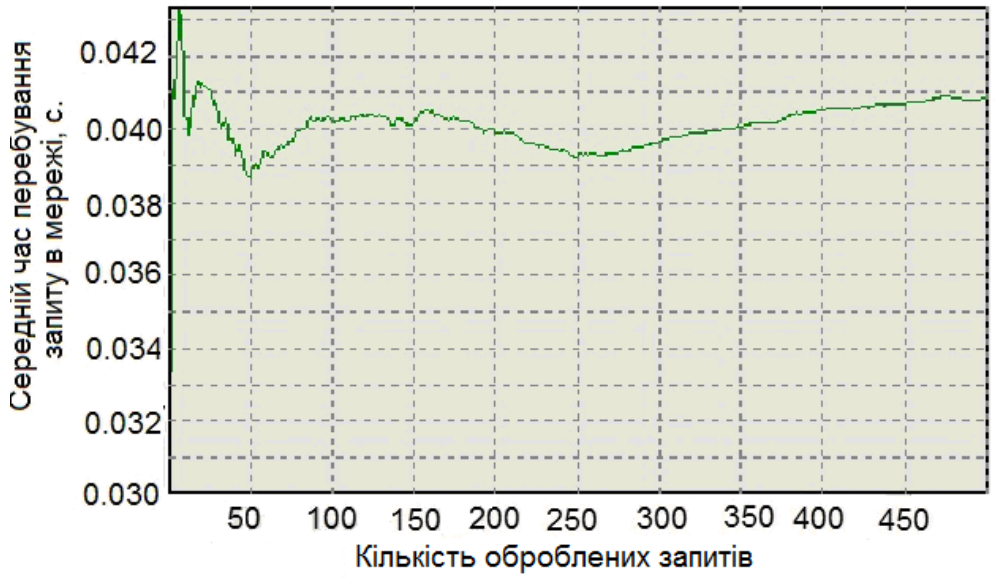
Таким чином отримуємо задану інтенсивність потоку, що моделюється цілими числами протягом кожної часової ітерації;

За результатами розрахунку середнього часу перебування пакету в мережі в залежності від її навантаження при різних інтенсивностях потоку, було встановлено, що для значення інтенсивності потоку $0.9 \cdot 10^5$ запитів/годину спостерігається вирівнювання процесу проходження пакетів. Це означає , що середній час перебування пакету в мережі не залежить від кількості пакетів.

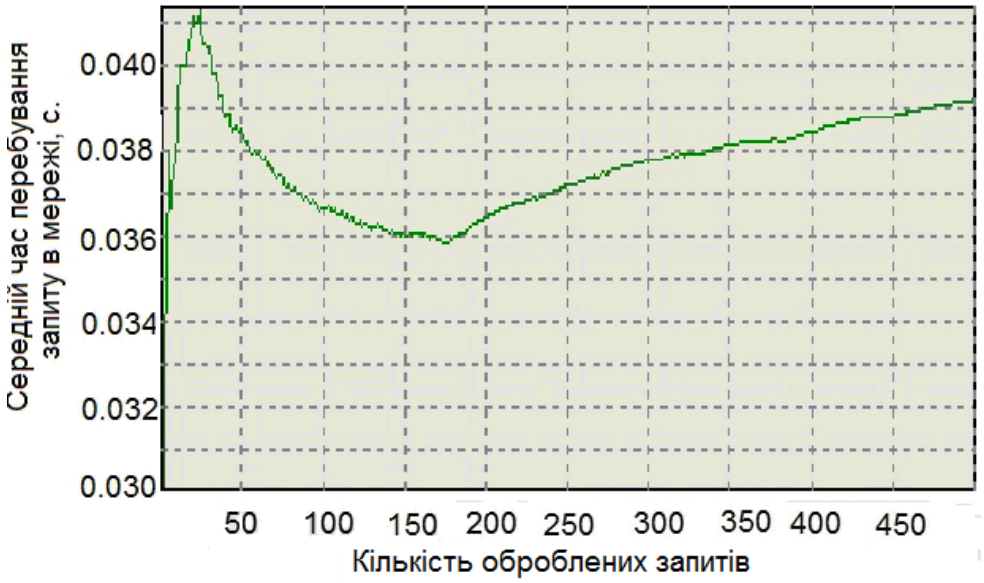
Також було встановлено, що трафік з різними видами розподілу проходить через мережу по-різному (рис.5.26).



а)



б)



в)

Рис.5.26. Залежність часу проходження трафіку від кількості оброблених запитів для інтенсивності вхідного потоку рівній $0.9 \cdot 10^5$ запитів/годину рівномірним (а), пуасонівським (б) та самоподібним при значенні показника Херста 0,3 (в)

Найбільше значення середнього часу перебування пакету має місце для пуасонівського трафіку (рис.5.26). Розраховане усереднене значення середнього часу перебування пакета у мережі для потоків з різними розподілами приведене у таблиці 5.2.

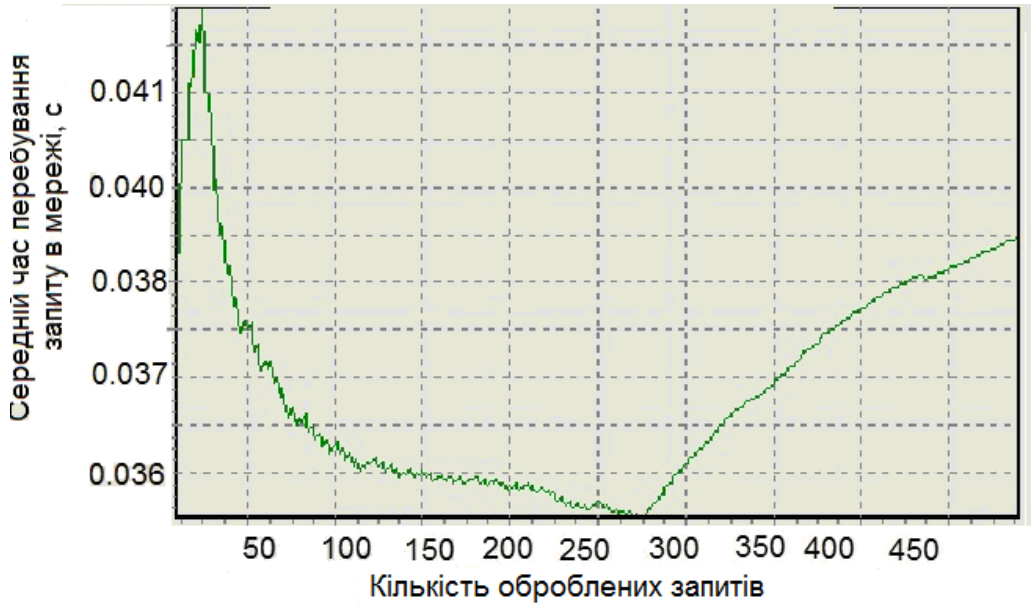
Таблиця 5.2.

Усереднене значення середнього часу перебування пакета у мережі для різних ймовірнісних моделей трафіку

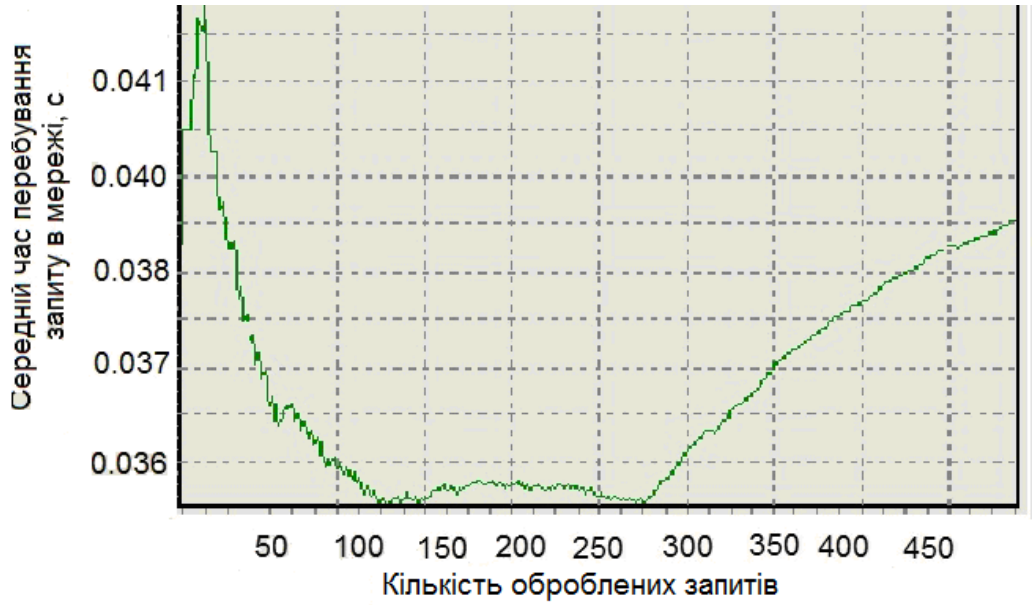
Вид трафіку	Середній час перебування пакету в мережі, сек.
Рівномірний	0,033
Пуасонівський	0,041
Самоподібний	0,039

Встановлена нами залежність проходження самоподібного трафіку при різних значеннях показників Херста приведена на рис. 5.27. Із отриманих

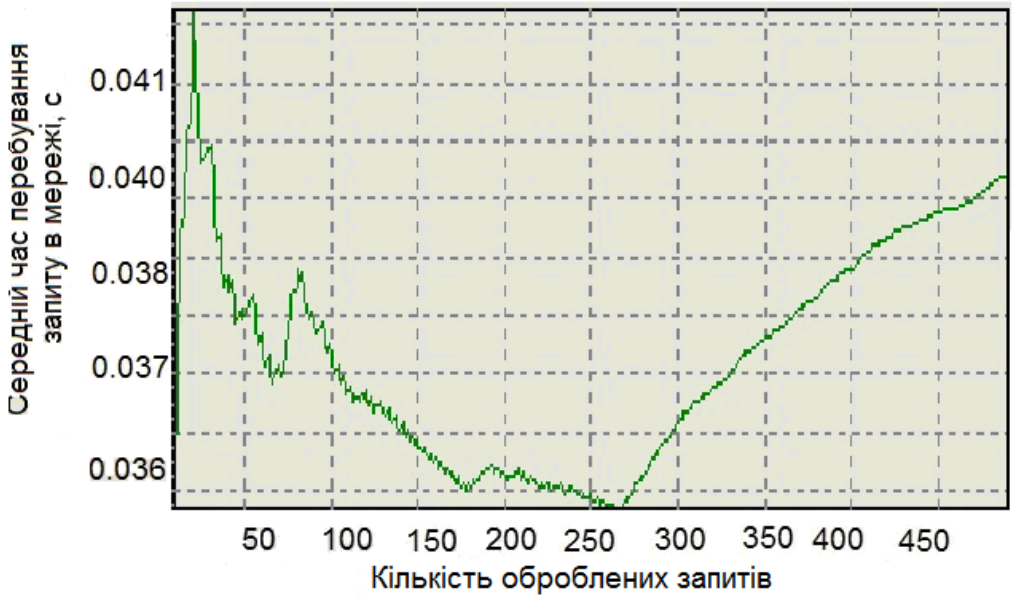
результатів дослідження залежності часу проходження самоподібного трафіку з різними показниками Херста випливає, що мінімальне середнє значення проходження самоподібного трафіку має місце при умові, що кількість пакетів дорівнює 270, 120…270, та 270 для H=0,1; 0,5 та 0,9 відповідно.



а)



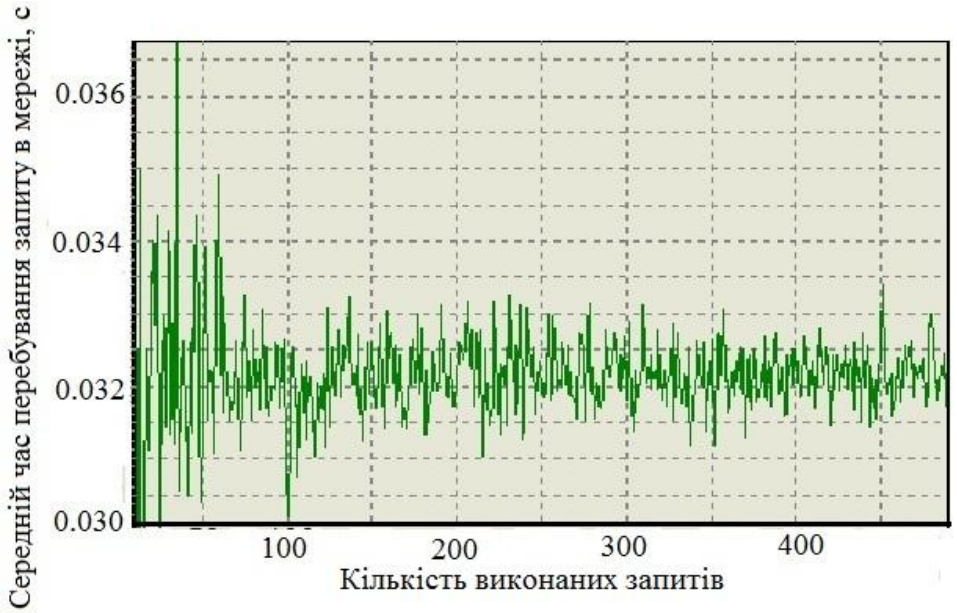
б)



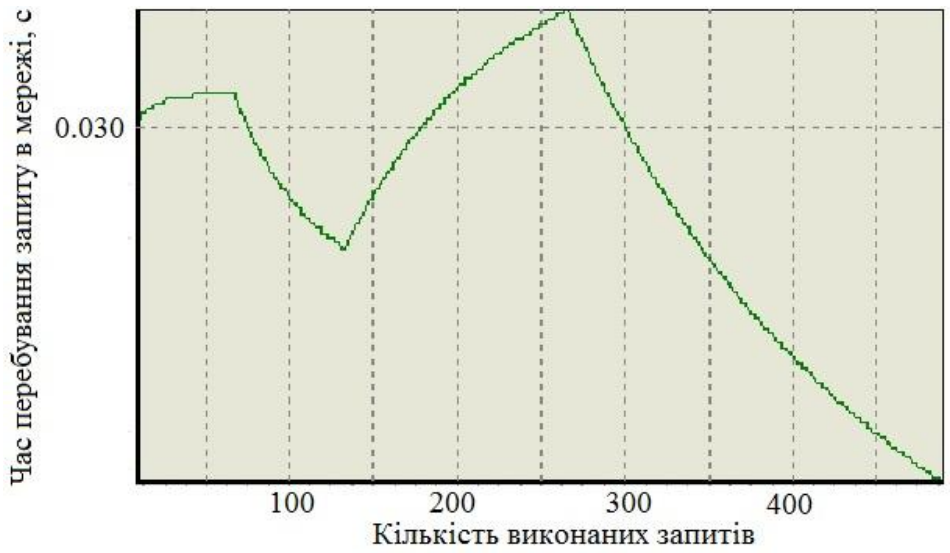
в)

Рис.5.27. Залежність характеристик вихідного потоку від кількості оброблених запитів при інтенсивності вхідного потоку рівній $0.9 \cdot 10^5$ запитів/годину для самоподібного вхідного трафіку з показниками Херста: H=0.1 (а), H=0.3 (б) та H=0.9 (в)

При зменшенні інтенсивності вхідного трафіку до $1.8 \cdot 10^3$ характеристики проходження мережі потоками із Пуасонівським та самоподібним розподілами є ідентичними та відрізняються від рівномірного (рис. 5.28).



а)



б)

Рис.5.28. Середній час перебування пакетів у мережі при інтенсивності вхідного потоку $1.8 \cdot 10^3$ запитів/годину для рівномірного (а) та для пуасонівського і самоподібного трафіків (б)

В результаті проведеного моделювання було встановлено, що для трафіків змодельованих різними потоками мають місце розбіжності. Зокрема, результати отримані для потоку із рівномірним розподілом відрізняються від результатів, отриманих при моделюванні трафіку самоподібним та Пуасонівським потоками. При цьому потоки із самоподібним та Пуасонівським розподілами є ідентичними при інтенсивності порядка $1.8 \cdot 10^3$ запитів/годину.

При збільшенні інтенсивності до $0.9 \cdot 10^5$ запитів/годину значення середнього часу проходження одного пакета для потоків із рівномірним розподілами становить $33 \cdot 10^{-3}$с , а для потоків із самоподібним $39 \cdot 10^{-3}$ та пуасонівським розподілами – $41 \cdot 10^{-3}$ с, що на наш погляд є досить значною розбіжністю.

Встановлено також, що має місце істотна залежність середнього часу від коефіцієнта самоподібності (показника Херста) потоку. При цьому

середній час проходження пакетів залишається однаковим, але процеси проходження суттєво відрізняються між собою.

Головне вікно програми та частина програмного коду написаного на мові Delphy приведені у Додатку Б

ВИСНОВКИ

1. Сигнали типу ФГШ з різними показниками Херста є хаотичними з гаусовим розподілом густини ймовірності їх значень та нульовим математичним сподіванням. Дисперсія сигналів з показником Херста H=0.1 зростає, а для сигналів з H=0.9 зменшується зі збільшенням значення коефіцієнту часового масштабування, а значення дисперсії сигналів з H=0.5 не залежать від коефіцієнту часового масштабування.

2. Встановлено, що коефіцієнт часового масштабування впливає на спектральну густину потужності сигналів з H=0,1 та 0,9. Для сигналів з H=0,9 домінує низькочастотна складова. Для сигналів з H=0,1 збільшення коефіцієнту часового масштабування призводить до лінійного зростання спектральної густини потужності з частотою.

3. Сигнали типу ФГШ з показником Херста H=0,1; 0,5 є слабокорельованими з їх копіями в діапазоні часового зсуву $[-500;500]$. Для сигналів з H=0,9 спостерігається кореляція з копіями у вище вказаних діапазонах в межах від 0…0,2.

4. Розроблена система кластерного кодування є стійкою до впливу канального шуму, причому завадостійкість системи кластерного кодування зростає зі збільшенням кількості відліків. В результаті проведених досліджень встановлено, що граничне значення сигнал/шум, що уможливлює розпізнавання інформаційних бітів, становить -7,5 дБ при 500 відліках сигналу.

5. Розроблений метод розпізнавання сигналів типу ФГШ за значенням так названого параметру розпізнавання кластерів, що дорівнює кореню квадратному із суми квадратів відстаней точок кластера від його центру.

6. У розробленій системі передавання інформації з кластерним кодуванням інформації синхронізація приймальної та передавальної сторін системи може здійснюватися маркерними сигналами незначної тривалості у

порівнянні з тривалістю несучих сигналів. Це забезпечує безпомилкове розпізнавання бітів при помилці синхронізації, що дорівнює 0,8 тривалості маркерного сигналу.

7. Розроблена система приймання/передавання інформації з представленням бінарних символів «1» і «0» сигналами манчестерського цифрового формату, що уможливлює декодування інформації без використання маркерного сигналу.

8. Розроблений метод моделювання самоподібних потоків Інтернет-трафіку з використанням фрактального Гаусового шуму. При значенні інтенсивності $0.9 \cdot 10^5$ запитів/годину середній час проходження одного пакета для потоків із рівномірним, самоподібним та пуасонівським розподілами становить $33 \cdot 10^{-3}$с, $39 \cdot 10^{-3}$ та $41 \cdot 10^{-3}$с відповідно, що обумовлено неможливістю компенсації пікових навантажень часовими проміжками простою мережі.

РОЗДІЛ 6. ФРАКТАЛЬНІ СИГНАЛИ ГРЕБІНКОВОЇ СТРУКТУРИ: ВЛАСТИВОСТІ ТА ПРАКТИЧНІ АСПЕКТИ ВИКОРИСТАННЯ У ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ

Головним недоліком відомих способів генерування фрактальних сигналів для вирішення радіофізичних та телекомунікаційних задач з метою ефективного використання радіоефіру в умовах складних електромагнітних обставин (сигнали, що модульовані фрактальними послідовностями [216], фрактальні вейвлети [175], фрактальний гаусовий шум [174], надширокосмугові радіоімпульси [217]). Є складність їх практичної реалізації. Тому існує потреба в нових методах генерування самоподібних сигналів, що поєднують велику інформаційну місткість та простоту генерування.

У цьому розділі розроблений та досліджений новий клас складних сигналів, що отримав назву фрактальний сигнал гребінкової структури. Розрахунок бази сигналу методом шумового еквіваленту показав, що, значення бази сигналу становить 200. Апробована система передавання цифрової інформації, що використовує ФСГС в якості переносника двобітових комбінацій.

6.1. Математична модель фрактальних сигналів гребінкової структури

Фрактальні сигнали (ФС) є новим класом широкосмугових сигналів, що можуть бути використані у завадостійких та криптостійких системах зв’язку [17, 174, 175, 216, 217].

Практична реалізація фрактальних сигналів, описаних авторами [173, 174] передбачає використання вартісної елементної бази, (зокрема, відлагоджувальної плати SPARTAN-3 з програмованою логічною інтегральною схемою XIINX SC3S200). Крім того для генерування сигналів з

невеликою похибкою квантування розрядність АЦП схеми повинна бути не меншою 12 біт [118].

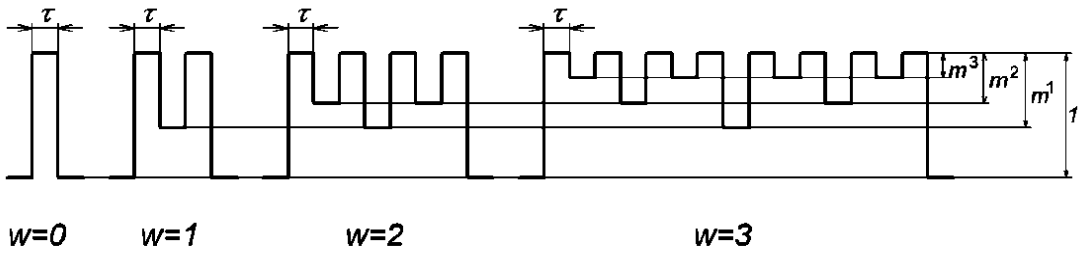
Розроблені нами [3, 6] фрактальні сигнали гребінкової структури (ФСГС), що формуються прямокутними імпульсами однакової тривалості та із амплітудами, значення яких підпорядковані певній закономірності та потребують значно простіших схемо-технічних рішень пристроїв для їх генерування.

Розглянемо алгоритм формування фрактального сигналу гребінкової структури на прикладі сигналу, структура якого складається з трьох імпульсів. Початковим елементом сигналу є прямокутний імпульс, що вважається фрактальним імпульсом гребінкової структури нулевого порядку ($w = 0$) (рис.6.1а). Амплітуди першого та третього імпульсів дорівнюють амплітуді фрактального сигналу нулевого порядку, а амплітуда другого імпульсу є меншою вдвічі. Утворену послідовність імпульсів вважатимемо фрактальним сигналом гребінкової структури 1-го порядку ($w = 1$) (рис.6.1б).

Для сигналів,структура яких складається із 7 прямокутних імпульсів однакової тривалості, амплітуди імпульсів з непарними номерами дорівнюють амплітуді фрактального сигналу нулевого порядку, амплітуда четвертого імпульсу є вдвічі меншою, а амплітуди 2-го та 6-го імпульсів становлять ¾ амплітуди сигналу мулевого порядку (рис.6.1в). Такий сигнал є фрактальним сигналом гребінкової структури другого порядку. По аналогії, структура фрактального сигналу 3-го порядку складатиметься із 15 імпульсів і матиме вигляд, приведений на рис 6.1г.

Отримаємо математичну модель ФСГС довільного порядку, використовуючи результати аналізу часової діаграми фрактального сигналу третього порядку (рис.6.2).

Верхній індекс на діаграмі (рис.6.2) означає порядковий номер імпульсу у рівні, нижній індекс – номер рівня у фракталі, (наприклад, u_3^2 – другий імпульс 3-го рівня).



а) б) в) г)

Рис.6.1 Фрактальні сигнали нулевого порядку (а); першого порядку (б); другого порядку (в); третього порядку (г) (m – коефіцієнт утворення фрактального імпульсу, τ – тривалість елементарного імпульсу)

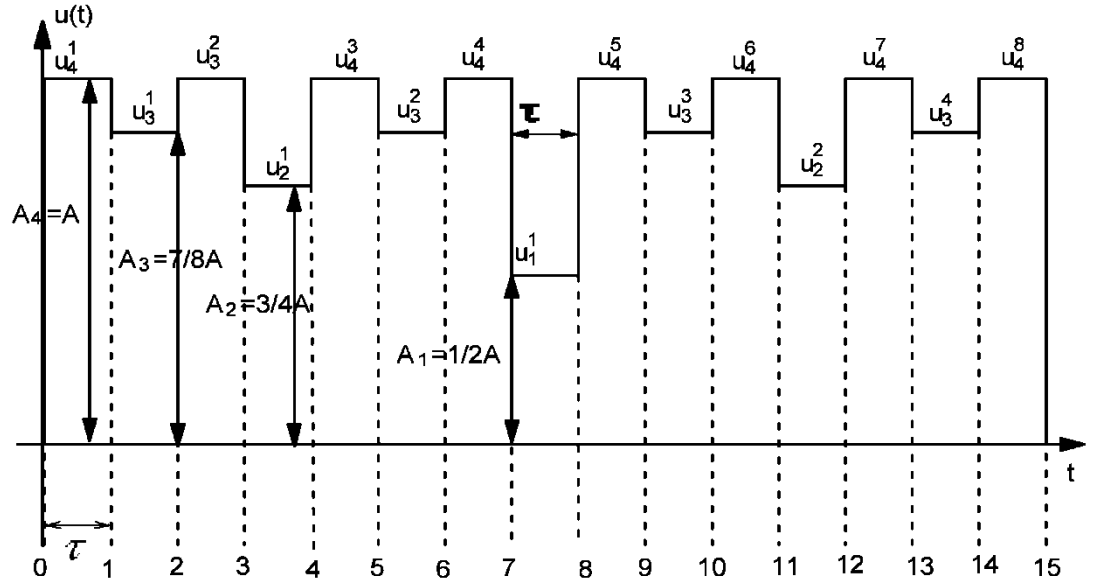


Рис.6.2. Часова діаграма фрактального імпульсу 3-го порядку ($w=3$), $m=\frac{1}{2}$

(τ тривалість одного імпульсу, $u_4^1, u_3^1, .. u_4^8$ – значення імпульсів, нижній індекс – номер рівня, верхній – номер імпульсу в рівні, А – максимальне значення імпульсів)

Очевидно, що елементарні імпульси можна згрупувати за однаковими амплітудами (далі називатимемо їх сигналами одинакового рівня). Нумерацію рівнів розпочнемо з першого рівня, якому належить імпульс найменшої амплітуди. Тоді кількість рівнів значень амплітуд імпульсів l, що входять до фрактального сигналу w-порядку l дорівнює:

$$l = w + 1 \qquad (6.1)$$

Кількість елементарних імпульсів на кожному наступному рівні збільшується вдвічі у порівнянні з попереднім для фрактального сигналу будь-якого порядку

$$n_i^w = 2 \cdot n_i^w,\ \ n_i^w = 2^{i-1},\ i = 1,2,\ldots,l \quad (6.2)$$

Значення амплітуди імпульсів l –го рівня ФСГС дорівнюватиме:

$$A_i = A \cdot \left[1 - m^i\right],\ i = 1,2,\ldots,l-1,\ A_{i=l} = A \quad (6.3)$$

Зокрема для ФСГС третього рівня (рис. 6.2) матимемо:

$$l = 4,\ i = 1,2,3,4,\ A_1 = \frac{1}{2} \cdot A,\ A_2 = \frac{3}{4} \cdot A,\ A_3 = \frac{7}{8} \cdot A,\ A_4 = A.$$

Загальна кількість прямокутних імпульсів n_w однакової тривалості τ у фрактальному сигналі є сумою членів геометричної прогресії:

$$n_w = \sum_{i=1}^{l} n_w^i = 2^{w+1} - 1, \qquad (6.4)$$

Зазначимо, що загальна кількість рівнів у фрак талах, порядок яких відрізняється на одиницю, задовільняє співвідношенню:

$$n_{w+1} = 2 \cdot n_w + 1 \quad (6.5)$$

де n_{w+1} та n_w – кількість імпульсів у фрактальних сигналах $w+1$ та w-порядків відповідно. Для фрактального сигналу нулевого порядку $n_0 = 1$.

Тривалість фрактального імпульсу w – порядку дорівнює:

$$T_w = n_w \cdot \tau = \left(2^{w+1} - 1\right) \cdot \tau \ (6.6)$$

Зокрема, для фрактального сигналу третього порядку (рис.6.2: $w = 3$, $n_3 = 15,\ T_3 = 15 \cdot \tau,\ l = 4$, а кількість імпульсів з різними рівнями амплітуди дорівнюватиме:

$$l = 1,\ n_1^3 = 1;$$

$$l = 2,\ n_2^3 = 2;$$

$$l = 3,\ n_3^3 = 4,$$

$$l = 4,\ n_3^3 = 8.$$

Початкові часові моменти перших імпульсів t_{i-1}^1 і t_i^1 задовільняють співвідношенню:

$$t_{i-1}^1 = 2 \cdot t_i^1 + \tau,\ t_l^1 = 0 \qquad (6.7)$$

Для фрактального сигналу третього порядку (рис.6.2), матимемо: $t_4^1 = 0,\ t_3^1 = \tau,\ t_2^1 = 3 \cdot \tau,\ t_1^1 = 7 \cdot \tau.$

По аналогії (6.5) та (6.6) початковий часовий момент першого імпульсу i-го рівня фрактального сигналу w-порядку дорівнюватиме:

$$t_i^1 = \left(2^{w+!-i} - 1\right) \cdot \tau \quad (6.8),$$

або

$$t_i^1 = \left(\frac{n_w + 1}{2^i} - 1 \right) \cdot \tau \ (6.9).$$

Зауважимо, що послідовність імпульсів кожного рівня є періодичною. При цьому період послідовностей збільшується вдвічі при зменшенні номера рівня на одиницю, а період імпульсів вищого рівня становить $2 \cdot \tau$:

$$T_{i-1} = 2 \cdot T_i,\ T_i = 2 \cdot \tau,\ T_i = 2^{w-i+2} \cdot \tau, \ (6.10)$$

Для фрактального сигналу третього порядку (рис. 6.2) матимемо:

$$T_4 = 2 \cdot \tau;\ T_3 = 4 \cdot \tau,\ T_2 = 8 \cdot \tau$$

Часовий момент початку k-го елементарного імпульсу дорівнюватиме:

$$t_i^k = t_i^1 + (k-1) \cdot T_i \ (6.11)$$

Так для фрактального сигналу структура якого приведена на рис.6.2 матимемо:

$$t_1^1 = 7 \cdot \tau;$$

$$t_2^1 = 3 \cdot \tau;\ t_2^2 = 3 \cdot \tau + T_2 = 11 \cdot \tau;$$

$$t_3^1 = \tau;\ t_3^2 = \tau + T_1 = 5 \cdot \tau;\ t_3^3 = \tau + 2 \cdot T_1 = 9 \cdot \tau;\ t_3^4 = \tau + 3 \cdot T_1 = 13 \cdot \tau;$$

$$t_4^1 = 0;\ t_4^2 = T_1 = 2 \cdot \tau;\ t_4^3 = 2 \cdot T_1 = 4 \cdot \tau;\ t_4^4 = 3 \cdot T_1 = 6 \cdot \tau;$$

$t_4^5 = 4 \cdot T_1 = 8 \cdot \tau$; $t_4^6 = 5 \cdot T_1 = 10 \cdot \tau$; $t_4^7 = 6 \cdot T_1 = 12 \cdot \tau$; $t_4^8 = 7 \cdot T_1 = 14 \cdot \tau$.

Аналітичний вираз для послідовності імпульсів, виражених через одиничні імпульси, матиме наступний вигляд:

$$\begin{aligned} u(t) &= \sum_{i=1}^{l} A_i \cdot \sum_{k=1}^{n_i^w} U_i^k(t); \\ u(t) &= \sum_{i=1}^{l} A_i \cdot \left[\sum_{k=1}^{n_i^w} \left\{ \Theta\left(t - t_i^k\right) - \Theta\left(t - t_i^k - \tau\right) \right\} \right], \end{aligned} \qquad (6.12)$$

де $\Theta(t)$ – функція Хевісайда, $U_i^k(t)$ – k-й імпульс прямокутної форми одиничної амплітуди.

Математична модель фрактальних сигналів гребінкової структури може бути виражена наступним чином:

$$x(t) = \sum_{i=1}^{w+1} A_i \left(\sum_{k=1}^{2^{w-1}} U_i^k(t) \right) = \sum_{i=1}^{w+1} A_i \cdot \left\{ \sum_{k=1}^{2^{w-1}} \left[\theta\left(t - t_i^k\right) - \theta\left(t - t_i^k - \tau\right) \right] \right\}, \qquad (6.13)$$

де w – порядок фракталу; i – номер рівня у фракталі (рис.6.2) одиничної амплітуди $\theta(t)$ – функція Хевісайда; τ – тривалість елементарного прямокутного імпульсу.

6.2. Спектральна густина потужності фрактального сигналу гребінкової структури

Для розрахунку спектральної густини потужності фрактального сигналу гребінкової структури скористаємося властивістю його симетрії. Виберемо систему координат таким чином, щоб вісь ординат поділяла фрактальний сигнал навпіл (рис.6.3). Тоді часові моменти початку прямокутних імпульсів фрактального сигналу будуть зміщені вліво на половину тривалості сигналу $\left(\left(2^{w+1} - 1\right) \cdot \tau / 2\right)$:

$$t_i'^k = t_i^1 + (k-1)\cdot T_i - n_w \cdot \tau = \left(2^{w+1-i} - 1\right)\cdot \tau + (k-1)\cdot 2^{w-i+2}\cdot \tau - \left(2^{w+1} - 1\right)\cdot \tau/2;$$
$$t_i'^k = \tau \cdot \left[2^{w+1-i} - 1 + (k-1)\cdot 2^{w-i+2} - 2^w + 1/2\right] = \tau \cdot \left[k \cdot 2^{w-i+2} - 2^{w+1-i} - 2^w - 1/2\right]; \quad (6.14)$$
$$t_i'^k = \tau \cdot \left\{2^w \cdot \left[2^{1-i}\cdot(2\cdot k - 1) - 1\right] - 1/2\right\}.$$

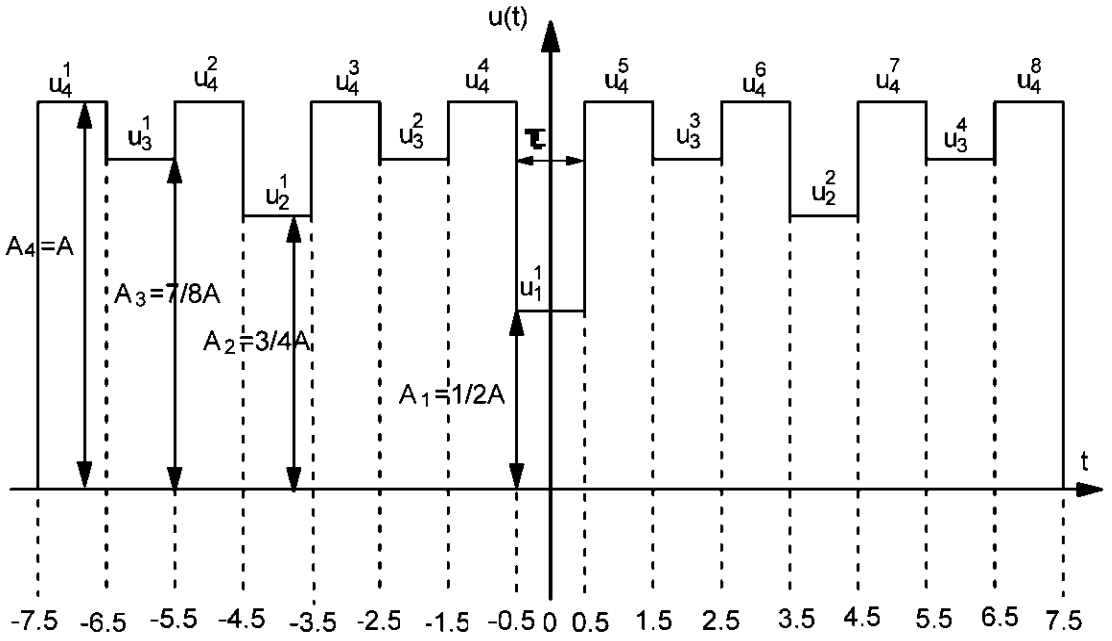


Рис.6.3. Часова діаграма фрактального імпульсу 3-го порядку ($w = 3$), $m = \frac{1}{2}$ у системі координат з початком відліку, що відповідає середині сигналу ($u_4^1, u_3^1, \ldots u_4^8$ – значення імпульсів, нижній індекс – номер рівня, верхній – номер імпульсу в рівні, А – максимальне значення амплітуди імпульсів)

Згідно прямому перетворенню Фур'є, спектральна густина сигналу дорівнюватиме:

$$S(j\cdot\omega) = F[u(t)] = F\left[\sum_{i=1}^{w+1} A_i \cdot \sum_{k=1}^{2^{i-1}} U_i^k\left(t'\right)\right] \qquad (6.15)$$

Використовуючи властивість лінійності перетворення Фур'є, виразимо спектральну густину сигналу через спектральну густину одиничного прямокутного імпульсу:

$$S(j\cdot\omega) = \sum_{i=0}^{w+1} A_i \cdot \sum_{k=1}^{2^{l-1}} F\left[U_i^k\left(t'\right)\right], \quad (6.16)$$

$$S_1(j\cdot\omega)=F\left[U_i^k(t')\right]=\int_{t'^k_i}^{t'^k_i+\tau}e^{-j\cdot\omega\cdot t}dt=\frac{e^{-j\cdot\omega\cdot t}}{-j\cdot\omega}\Bigg|_{t'^k_i}^{t'^k_i+\tau}=\frac{e^{-j\cdot\omega\cdot t'^k_i}-e^{-j\cdot\omega\cdot\left(t'^k_i+\tau\right)}}{j\cdot\omega} \quad (6.17)$$

Для подальших розрахунків визначимо часові моменти початку та закінчення прямокутних імпульсів, що входять у формулу (6.16) для імпульсів 4-го рівня сигналу, що є зображеним на рис.6.3:

$$t'^1_4=-7.5\cdot\tau;\ t'^1_{з4}=-6.5\cdot\tau;\ t'^2_4=-5.5\cdot\tau;\ t'^2_{з4}=-4.5\cdot\tau;t'^3_4=-3.5\cdot\tau;\ t'^3_{з4}=-2.5\cdot\tau;$$

$$t'^4_4=-1.5\cdot\tau;\ t'^4_{з4}=-0.5\cdot\tau;\ t'^5_4=0.5\cdot\tau;\ t'^5_{з4}=1.5\cdot\tau;\ t'^6_4=2.5\cdot\tau;\ t'^6_{з4}=3.5\cdot\tau;$$

$$t'^7_4=4.5\cdot\tau;\ t'^7_{з4}=5.5\cdot\tau;\ t'^8_4=6.5\cdot\tau;\ t'^8_{з4}=7.5\cdot\tau.$$

Легко бачити, що експоненти у формулі (6.16) можна перегрупувати таким чином, щоб отримати різницю експонент із протилежними знаками показників. Для фрактального сигналу третього порядку (рис.6.3) матимемо:

$$t'^1_4=-7.5\cdot\tau;\ t'^8_{з4}=7.5\cdot\tau; \qquad t'^3_4=-3.5\cdot\tau;\ t'^6_{з4}=3.5\cdot\tau;$$
$$t'^1_{з4}=-6.5\cdot\tau;\ t'^8_4=6.5\cdot\tau; \qquad t'^3_{з4}=-2.5\cdot\tau;\ t'^6_4=2.5\cdot\tau;$$
$$t'^2_4=-5.5\cdot\tau;\ t'^7_{з4}=5.5\cdot\tau; \qquad t'^4_4=-1.5\cdot\tau;\ t'^5_{з4}=1.5\cdot\tau;$$
$$t'^2_{з4}=-4.5\cdot\tau;\ t'^7_4=4.5\cdot\tau; \qquad t'^4_{з4}=-0.5\cdot\tau;\ t'^5_4=0.5\cdot\tau$$

Узагальненням такого перегруповування доданків є співвідношення між номерами імпульсів одного рівня:

$$\begin{aligned}
&k+k'=n_i^w+1=2^{i-1}+1\\
&k'=2^{i-1}+1-k\\
&t'^{k'}_i=\tau\cdot\left\{2^w\cdot\left[2^{1-i}\cdot(2\cdot k'-1)-1\right]-1/2\right\}\\
&t'^{k'}_i=\tau\cdot\left\{2^w\cdot\left[2^{1-i}\cdot\left(2\cdot\left(2^{i-1}+1-k\right)-1\right)-1\right]-1/2\right\}\\
&t'^{k'}_i=\tau\cdot\left\{2^w\cdot\left[2^{1-i}\cdot(1-2\cdot k)\right]-1/2\right\}
\end{aligned} \quad (6.18)$$

З врахуванням спектральної густини одного прямокутного імпульсу, спектральну функцію фрактального сигналу $w-$го рівня можемо записати наступним чином:

$$S(j\cdot\omega)=\sum_{i=1}^{w+1}A_i\cdot\sum_{k=1}^{2^{i-1}}\frac{e^{-j\cdot\omega\cdot t'^{k}_{i}}-e^{-j\cdot\omega\cdot\left(t'^{k}_{i}+\tau\right)}}{j\cdot\omega}=$$

$$A_1\cdot\frac{e^{-j\cdot\omega\cdot t'^{1}_{1}}-e^{-j\cdot\omega\cdot\left(t'^{1}_{1}+\tau\right)}}{j\cdot\omega}+\sum_{i=2}^{w+1}A_i\cdot\sum_{k=1}^{2^{i-2}}\left[\frac{e^{-j\cdot\omega\cdot t'^{k}_{i}}-e^{-j\cdot\omega\cdot\left(t'^{k'}_{i}+\tau\right)}}{j\cdot\omega}-\frac{e^{-j\cdot\omega\cdot t'^{k'}_{i}}-e^{-j\cdot\omega\cdot\left(t'^{k}_{i}+\tau\right)}}{j\cdot\omega}\right]$$

(6.19)

У формулі (6.19) перший доданок відповідає імпульсу першого рівня ФСГС.

Введемо позначення:

$$\begin{aligned}&\omega\cdot\tau/2=\alpha_0\\&\omega\cdot\tau\cdot2^{w}\cdot\left[2^{1-l}\cdot(2\cdot k-1)-1\right]=\alpha_i^{k};\end{aligned}\quad(6.20)$$

З урахуваннях цих позначень змінимо показники експонент у (6.19):

$$\begin{aligned}&-\omega\cdot t'^{1}_{1}=\omega\cdot\tau/2;\\&-\omega\cdot\left(t'^{1}_{1}+\tau\right)=-\omega\cdot\tau/2\end{aligned}\quad(6.21)$$

$$\begin{aligned}&-\omega\cdot t'^{k}_{i}=-\omega\cdot\tau\cdot\left\{2^{w}\cdot\left[2^{1-i}\cdot(2\cdot k-1)-1\right]-1/2\right\}=\alpha_0-\alpha_i^{k}\\&-\omega\cdot\left(t'^{k'}_{i}+\tau\right)=-\omega\cdot\tau\cdot\left\{2^{w}\cdot\left[2^{1-i}\cdot(1-2\cdot k)-1\right]-1/2+1\right\}\\&-\omega\cdot\left(t'^{k'}_{i}+\tau\right)=\alpha_i^{k}-\alpha_0\end{aligned}\quad(6.22)$$

$$\begin{aligned}&-\omega\cdot t'^{k'}_{i}=-\omega\cdot\tau\cdot\left\{2^{w}\cdot\left[2^{1-i}\cdot(1-2\cdot k)-1\right]-1/2\right\}=\alpha_0+\alpha_l^{k}\\&-\omega\cdot\left(t'^{k}_{i}+\tau\right)=-\omega\cdot\tau\cdot\left\{2^{w}\cdot\left[2^{1-i}\cdot(2\cdot k-1)-1\right]-1/2+1\right\}\\&-\omega\cdot\left(t'^{k'}_{i}+\tau\right)=-\alpha_0-\alpha_i^{k}\end{aligned}\quad(6.23)$$

$$S(j\cdot\omega)=$$

$$A_1\cdot\frac{e^{j\cdot\omega\cdot\tau/2}-e^{-j\cdot\omega\cdot\tau/2}}{j\cdot\omega}+\sum_{i=2}^{w+1}A_l\cdot\sum_{k=1}^{2^{l-2}}\left[\frac{e^{j\cdot\left(\alpha_0-\alpha_i^{k}\right)}-e^{-j\cdot\left(\alpha_0-\alpha_i^{k}\right)}}{j\cdot\omega}-\frac{e^{j\cdot\left(\alpha_0+\alpha_i^{k}\right)}-e^{-\left(\alpha_0+\alpha_i^{k}\right)}}{j\cdot\omega}\right]$$

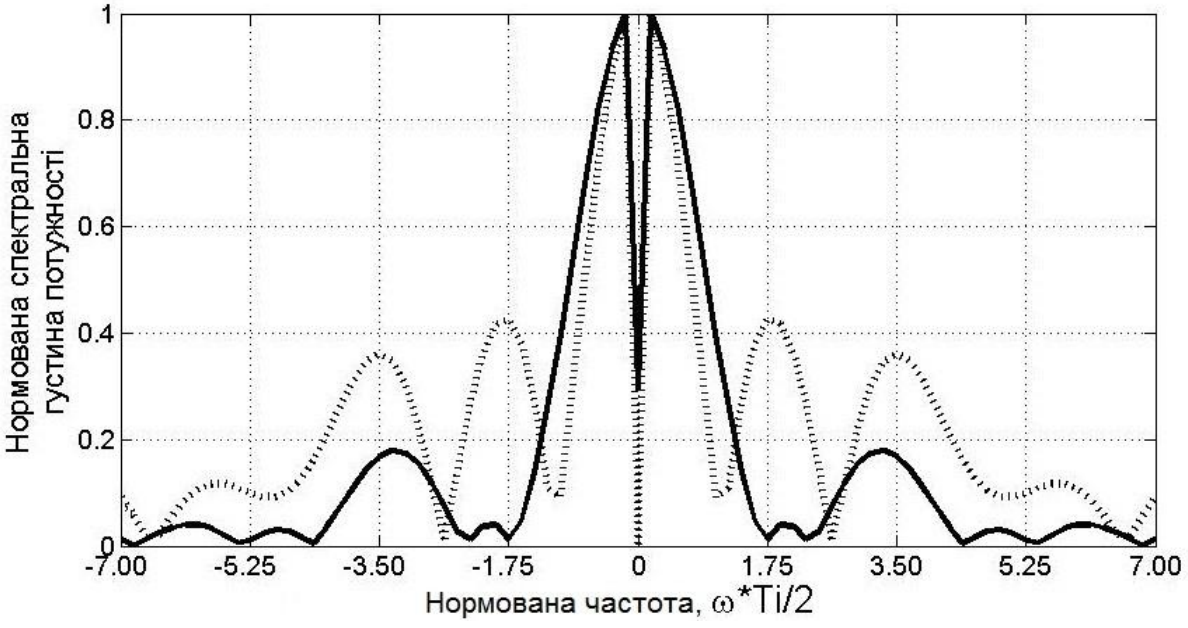
(6.24)

Використовуючи формулу Ейлера для експоненційного представлення функції синус, формулу (6.24) можна записати наступним чином:

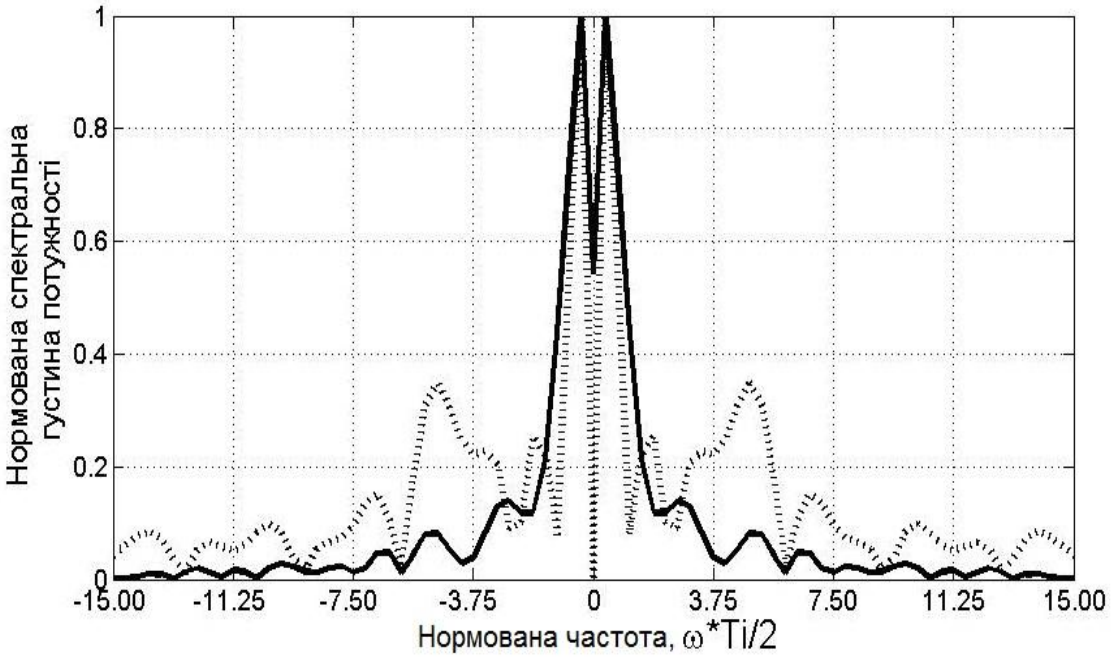
$$
\begin{aligned}
S(j\cdot\omega) &= \frac{2A_1}{\omega}\cdot\sin(\omega\cdot\tau/2)+\frac{2}{\omega}\cdot\sum_{i=2}^{w+1}A_i\cdot\sum_{k=1}^{2^{i-2}}\left[\sin\left(\alpha_0-\alpha_i^k\right)-\sin\left(\alpha_0+\alpha_i^k\right)\right]= \\
&= \frac{2A_1}{\omega}\cdot\sin(\omega\cdot\tau/2)+\frac{4}{\omega}\cdot\sum_{l=2}^{w+1}A_i\cdot\sum_{k=1}^{2^{i-2}}\left[\sin\left(\frac{\alpha_0-\alpha_i^k-\alpha_0-\alpha_i^k}{2}\right)\cdot\cos\left(\frac{\alpha_0-\alpha_i^k+\alpha_0+\alpha_i^k}{2}\right)\right]= \\
&= \frac{2A_1}{\omega}\cdot\sin(\omega\cdot\tau/2)+\frac{4}{\omega}\cdot\sum_{i=2}^{w+1}A_i\cdot\sum_{k=1}^{2^{i-2}}\left[\sin\left(-\alpha_i^k\right)\cdot\cos\left(\alpha_0\right)\right]= \\
&= \frac{2A_1}{\omega}\left[\sin\left(\frac{\omega\tau}{2}\right)-2\sum_{i=2}^{w+1}\left(1-m^i\right)\sum_{k=1}^{2^{i-2}}\sin\alpha_i^k\cos\alpha_0\right]= \\
&= \frac{2A_1}{\omega}\left[\sin\left(\frac{\omega\tau}{2}\right)-2\cos\alpha_0\sum_{i=2}^{w+1}\left(1-m^i\right)\sum_{k=1}^{2^{i-2}}\sin\alpha_i^k\right]
\end{aligned}
\qquad (6.25)
$$

На рис.6.4 приведена розрахована спектральна густина потужності $\left(\left|S(j\cdot\omega)\right|^2\right)$, для ФСГС другого, третього та четвертого порядків. Із вищеописаного алгоритму побудови випливає, що спектральна густина фрактального сигналу першого порядку є спектральною густиною симетричного відносно осі прямокутного імпульсу амплітудою A та тривалістю τ:

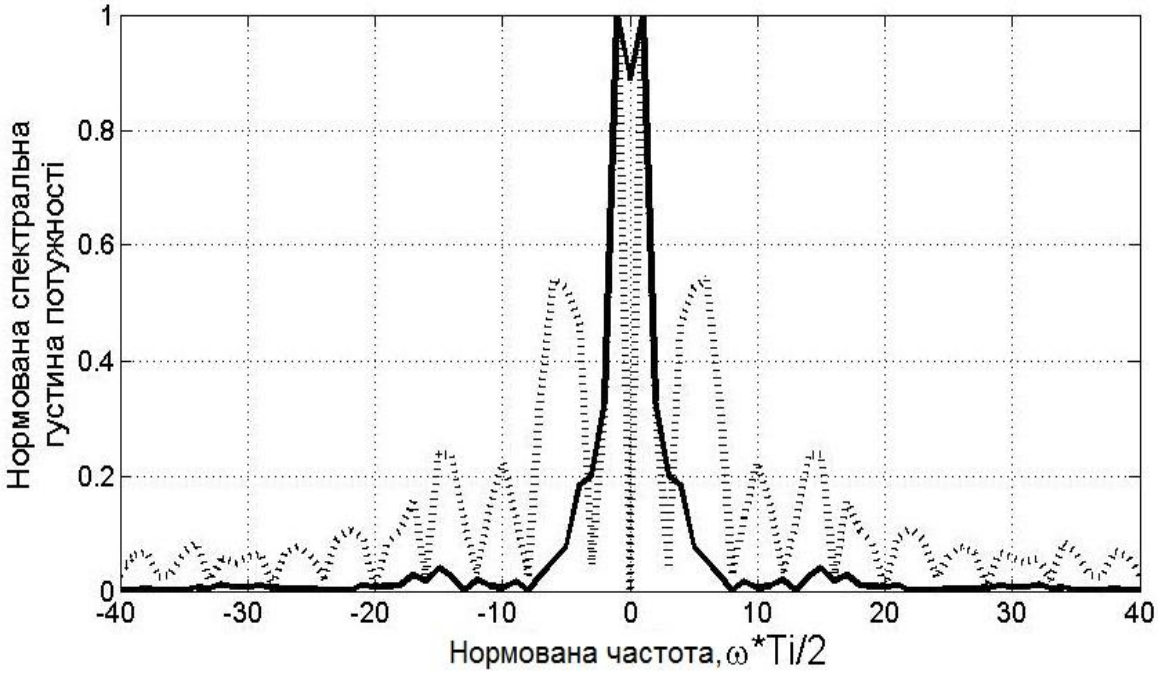
$$
\left|S(j\cdot\omega)\right|^2=\left|\frac{2A}{\omega}\cdot\frac{\sin(\omega\cdot\tau/2)}{2}\right|^2=\left[\frac{A\cdot\tau}{2}\cdot\frac{\sin(\omega\cdot\tau/2)}{\omega\cdot\tau/2}\right]^2=\left(\frac{A\cdot\tau}{2}\right)^2\cdot\sin c^2(\omega\cdot\tau/2) \qquad (6.26)
$$



а)



б)



в)

Рис.6.4. Нормована спектральна густина потужності (штриховою кривою показана спектральна густина потужності сигналу без врахування постійної складової фрактальних сигналів другого порядку (w=2) (а); третього порядку (w=3) (б); четвертого порядку (w=4) (в) (ω – циклічна частота, Ti – повна тривалість фрактального імпульсу)

На осі абсцис приведені значення половини добутку частоти на тривалість фрактального імпульсу. Пунктирною лінією на рис.6.4 зображена нормована спектральна густина потужності сигналу ФСГС з вилученою постійною складовою.

Слід зауважити, що результати розрахунків спектральної густини потужності ФСГС за допомогою алгоритму швидкого перетворення Фур'є, та результати, приведені на рис. 6.4, співпадають між собою.

Із отриманих результатів можна зробити висновок, що чим меншим є порядок ФСГС, тим подібніша його спектральна густина потужності до спектральної густини потужності одиничного імпульсу. Якщо вилучити постійну складову із сигналу, то спектр сигналу буде сегментованим із рівновіддаленими максимумами $\Delta f = \frac{1}{T_i}$.

Широкосмуговими називаються такі сигнали, коефіцієнт широкосмуговості яких (добуток ширини спектру сигналу на його тривалість $B = F \cdot Ts$) більше одиниці [218].

При оцінюванні бази ФСГС ширина їх спектральної смуги визначалася методом шумового еквіваленту [219]:

$$F_{eff} = \frac{1}{G_{\max}} \int_0^{\infty} G(f)\,df, \quad (6.27)$$

де F_{eff} - ефективна ширина спектра частот сигналу; $G_{\max}$ - максимальне значення спектральної густини потужності сигналу; $G(f)$ - спектральна густина потужності сигналу на частоті f.

Розрахована залежність бази ФСГС від їх порядку при різних значеннях коефіцієнту утворення приведена на рис. 6.5.

Із отриманих результатів випливає, що сигнали даного класу є широкосмуговими а їх база зростає зі збільшенням порядку w, і зменшується зі збільшенням коефіцієнту утворення m значення бази.

Значення коефіцієнта завадостійкості, що характеризує рівень відновлення робочих сигналів за допомогою корелятора [219] з їх суміші із завадами, визначалися згідно виразу:

$$\lambda = \frac{\int_0^{T_s} s^2(t)\,dt}{\int_0^{T_s} s^2(t)\,dt + \left|\int_0^{T_s} s(t)\cdot n(t)\,dt\right|} \quad (6.28)$$

де $\int_0^{T_s} s^2(t)\,dt$ – автокореляційна функція робочого сигналу в нулі; $\int_0^{T_s} s(t)\cdot n(t)\,dt$ – взаємна кореляційна функція робочого сигналу і завади в нулі; $s(t)$ – корисний сигнал; $n(t)$ – сигнал завади.

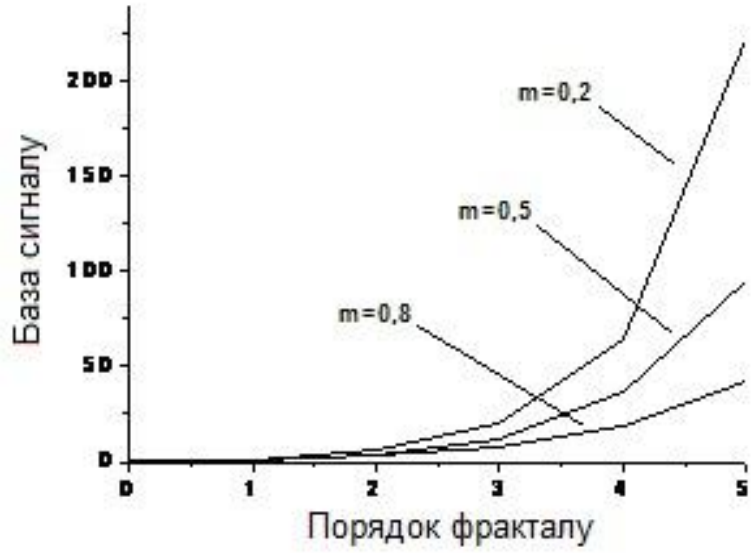


Рис.6.5. Залежність бази фрактального сигналу від його порядку для різних значень коефіцієнту утворення (m – коефіцєнт утвореня фракталу)

Розрахункова залежність коефіцієнта завадостійкості ФСГС від його порядку при різних значеннях коефіцієнту утворення приведена на рис. 6.6.

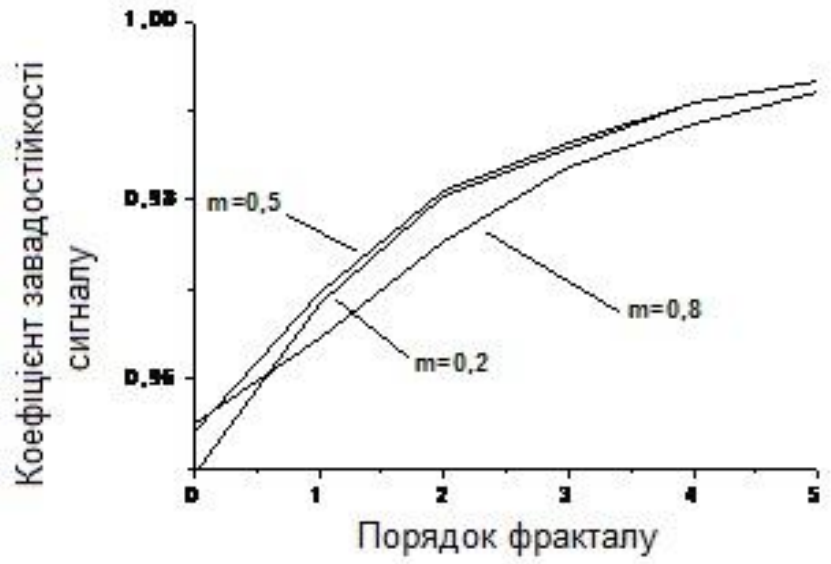


Рис.6.6. Залежність коефіцієнта завадостійкості фрактального сигналу від його порядку для різних значень коефіцієнту утворення (m – коефіцєнт утвореня фракталу)

Криві залежності коефіцієнту завадостійкості від порядку фракталу співпадають (рис.6.6) для сигналів зі значенням коефіцієнту утворення 0,2 та 0,5 при значеннях порядку фракталів $w \geq 2$. З ростом порядку фракталу коефіцієнт завадостійкості прямує до одиниці.

6.3. Кореляційні властивості фрактальних сигналів гребінкової структури

Чисельні розрахунки спектральної густини, автокореляційної функції (АКФ) та фазового портрету здіснюватимемо на прикладі ФСГС третього порядку з коефіцієнтом утворення ½ і тривалістю елементарного фрагменту 2 мкс при умові відсутності шумів в каналі. Часова діаграма досліджуваних сигналів приведена на рис.6.7.

Спектральна густина досліджуваних сигналів (рис.6.8) є подібною до спектральної густини сигналів прямокутної форми з чітко вираженими локальними максимумами на частотах, що є кратними основній частоті.

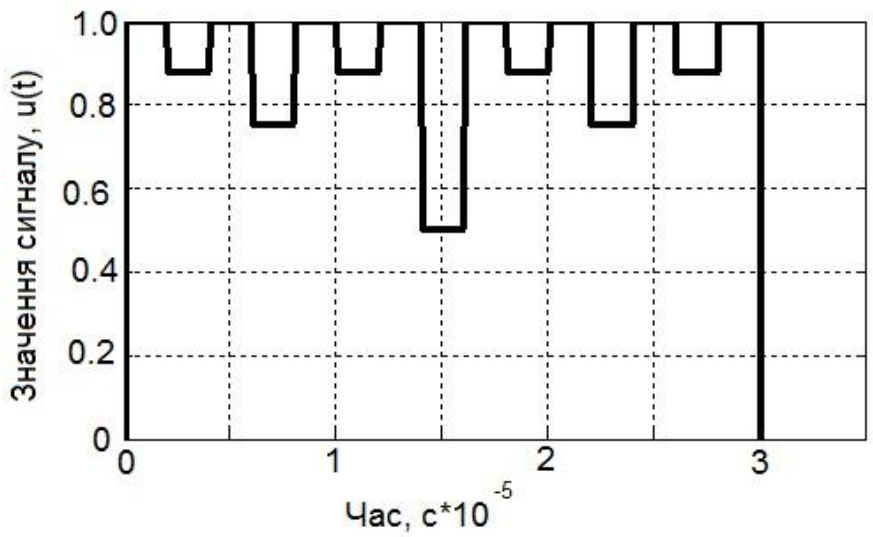


Рис.6.7. Часова діаграма ФСГС третього порядку w=3 (порядок фракталу); $m = \frac{1}{2}$ (коефіцієнт утворення); $\tau = 2$ мкс (тривалість одного імпульсу)

Гармонічні складові групуються під огинаючою спектру елементарного імпульсу.

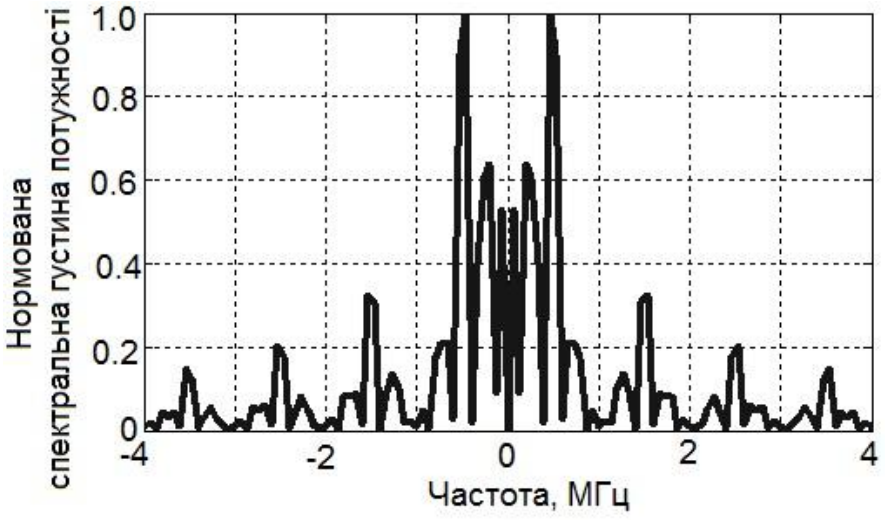
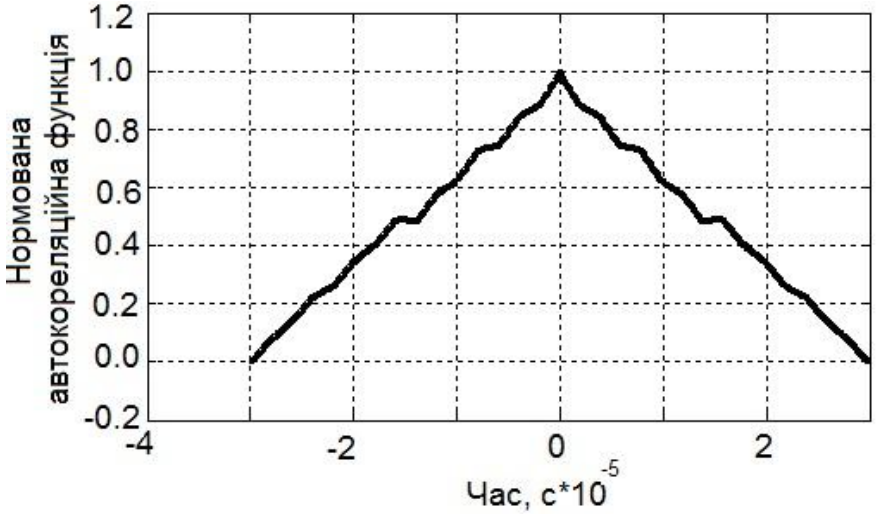
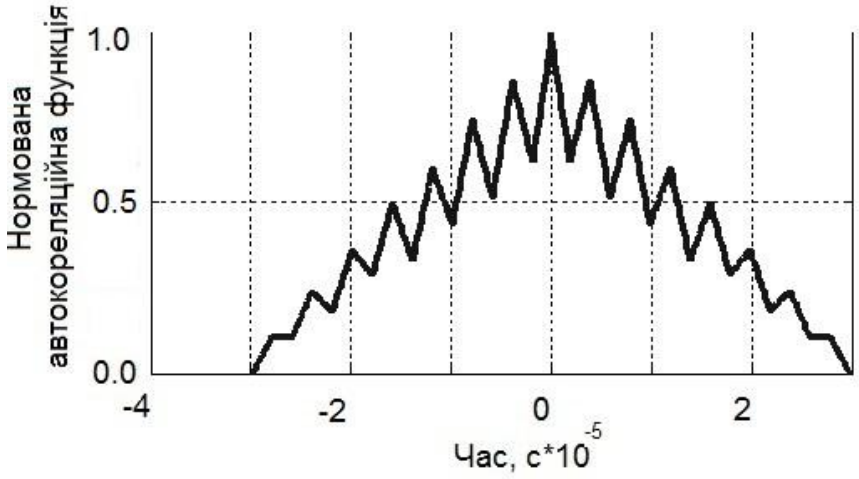


Рис.6.8. Спектральна густина ФСГС третього порядку з коефіцієнтом утворення m=0,5 (постійна складова із сигналу вилучена).

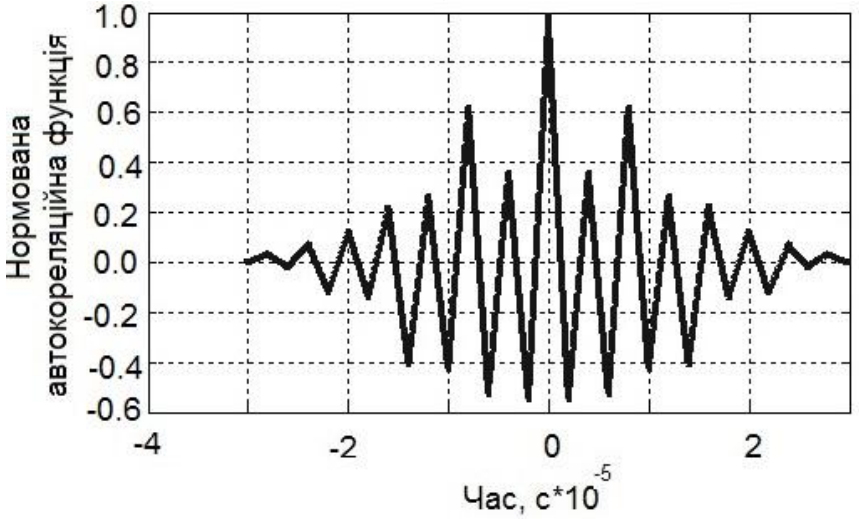
Автокореляційна функція (АКФ) ФСГС є подібною до АКФ прямокутного імпульсу при значеннях коефіцієнту утворення $m \le 0,5$ (рис.6.9а).



а)



б)



в)

Рис.6.9. Автокореляційна функція ФСГС третього порядку з коефіцієнтом утворення m=0,5(а); m=0,8 (б); m=0,5 (в) (постійна складова з сигналу вилучена).

При значеннях коефіцієнту утворення в межах $m=0{,}5\ldots1$ АКФ має пилкоподібний характер (рис. 6.9б). При вилученні постійної складової із ФСГС його АКФ має вигляд АКФ осциляційної функції (рис. 6.9в).

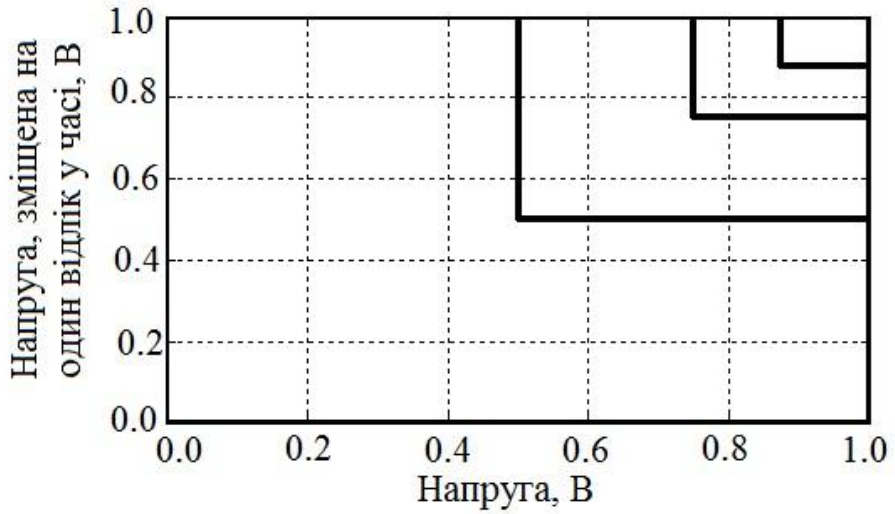


Рис.6.10. Фазовий портрет ФСГС третього порядку з коефіцієнтом утворення $m=0{,}5$.

Із аналізу фазового портрету ФСГС (рис. 6.10) випливає, що фрактальні сигнали належать до регулярних часових сигналів.

6.4. Апаратна реалізація кодера та декодера системи передавання двійкових даних з використанням фрактального сигналу гребінкової структури

Кодер і декодер системи передавання інформації з використанням ФСГС складаються з блоку керування та керованого блоку. Блоки керування кодера та декодера є ідентичними, а їх керовані блоки мають різні схемотехнічні рішення [3, 38].

Модуль керування (рис.6.11) здійснює генерування і розпізнавання сигналів та виконує функцію обміну даними з комп’ютером.

Функцію програмованого ядра у модулі керування виконує мікроконтролер PIC18F2550 (DD1) фірми MicroChip [220], тактова частота

якого визначається частотою зовнішнього генератора DA1 (КХО-210 40.0 MHz) [221] .

Обмін даними між мікроконтролером та комп’ютером здійснюється за допомогою портів USART (гніздо XP2) або USB (гніздо XP1). Міросхема MAX232 (DD2) узгоджує інтерфейс RS-232 (COM-порта комп’ютера) із портом USART мікроконтролера.

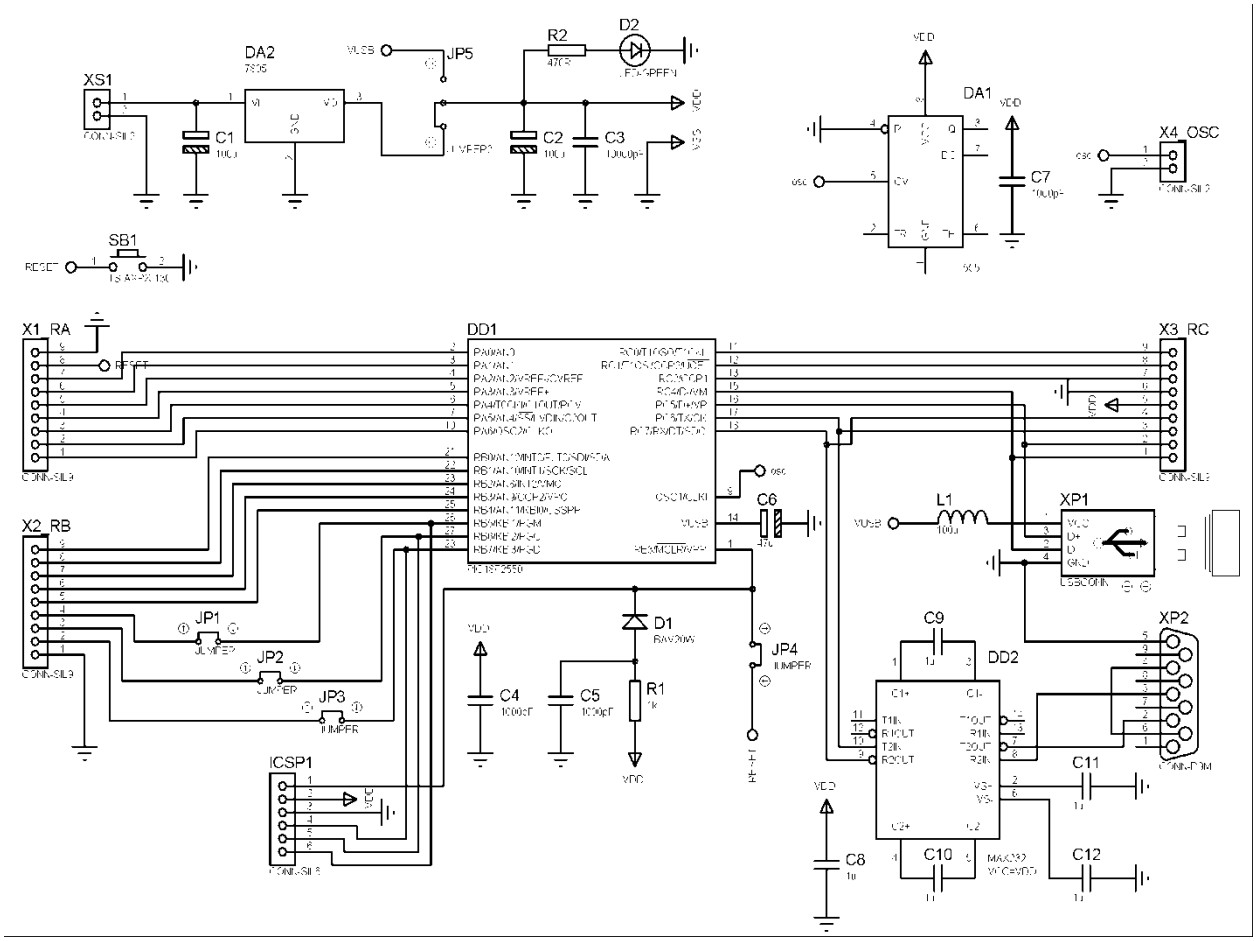


Рис.6.11. Схема електрична принципова модуля керування кодера та декодера системи передавання інформації з використанням ФСГС.

Схема модуля керування реалізована на мікросхемах з одно полярним живленням +5В, величина якого регулюється інтегральним стабілізатором LM7805, завдяки чому напруга живлення схеми кодера може становити +15В.

Схема електрична принципова керованого модуля кодеру приведена на рис.6.12. Реалізація керуючого та керованого модулів кодеру за приведеними схемами дозволяє формувати фрактальні сигнали гребінкової структури будь-якого порядку.

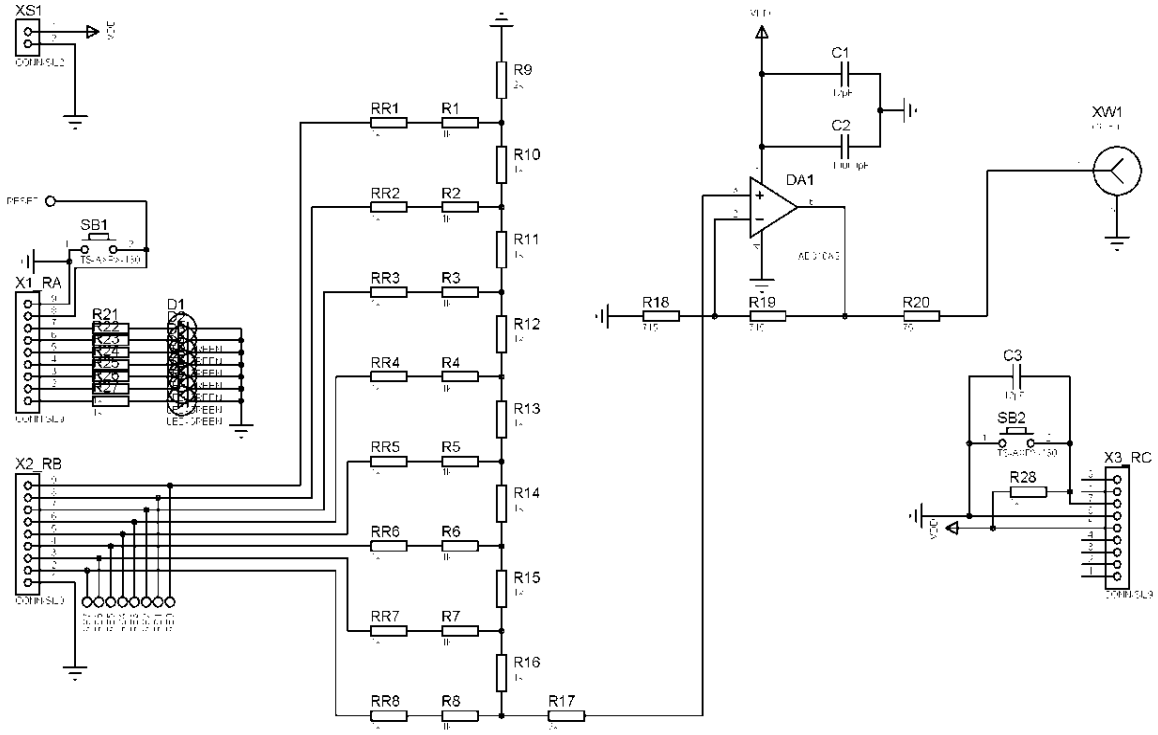


Рис.6.12. Схема електрична принципова керованого модуля кодера

Послідовності кодів, що утворюють фрактальний сигнал, є зведеними в таблицю, що записана в пам’ять мікроконтролера. Перетворення у фрактальний сигнал відбувається за допомогою матриці R-2R, утвореної резисторами (R1÷R8, R1÷R16), що уможливлює здійснення паралельного цифро-аналогового перетворення (ЦАП) . Велике співвідношення між значеннями опорів транзисторних ключів порту мікроконтролера RB у закритому та відкритому станах ($R_з / R_0 = 2 \cdot 10^6$) дозволяє використовувати їх для комутації струму в ЦАП. Задовільні характеристики лінійності перетворення цифрового коду у напругу забезпечуються невисоким розкидом значень опорів резисторів, що утворюють матрицю за рахунок їх однакового номіналу та належності до однієї виробничої партії.

Узгодження вихідного опору R-2R матриці та хвильового опору коаксіального кабелю, по якому передавалася інформація за допомогою фрактальних сигналів, було досягнуто шляхом використання операційного підсилювача AD810 (DA1).

Кодер системи здійснює генерування та перетворення у фрактальний сигнал заданого порядку послідовності двійкового коду на виходах порту RB у відповідності з інформаційними бітами, що находять із комп'ютера передавальної сторони.

Тривалість фрактальних сигналів залежить від тактової частоти та довжини блоку програми, що генерує заданий сигнал. З метою підвищення швидкодії системи для генерування фрактальних сигналів використовувалася табл. із записаними значеннями амплітуди елементарних прямокутних імпульсів, що формують структуру фрактального сигналу.

Зчитування значень послідовності відліків фракталу з відповідного рядка таблиці відбувається у відповідності зі значеннями бітів вхідного інформаційного байту, що надходить із комп'ютера. Це забезпечує мінімально можливу для даної групи МК тривалість фрактального імпульсу. Блок-схема алгоритму роботи записаної у МК програми приведена на рис.6.13.

Алгоритмом передбачене кодування інформації двох бітовими символами («00», «01», «10» та «11»), тому програма повинна забезпечувати генерування та розпізнавання фрактальних сигналів гребінкової структури чотирьох різних рівнів. Синхронізація моменту передавання кожного байту між передавачем та приймачем здійснюється шляхом передавання сигналу синхронізації.

Підпрограма розпізнавання кодової послідовності, що відповідає заданому фракталу, написана на мові програмування «асемблер» з мінімальною кількістю команд.

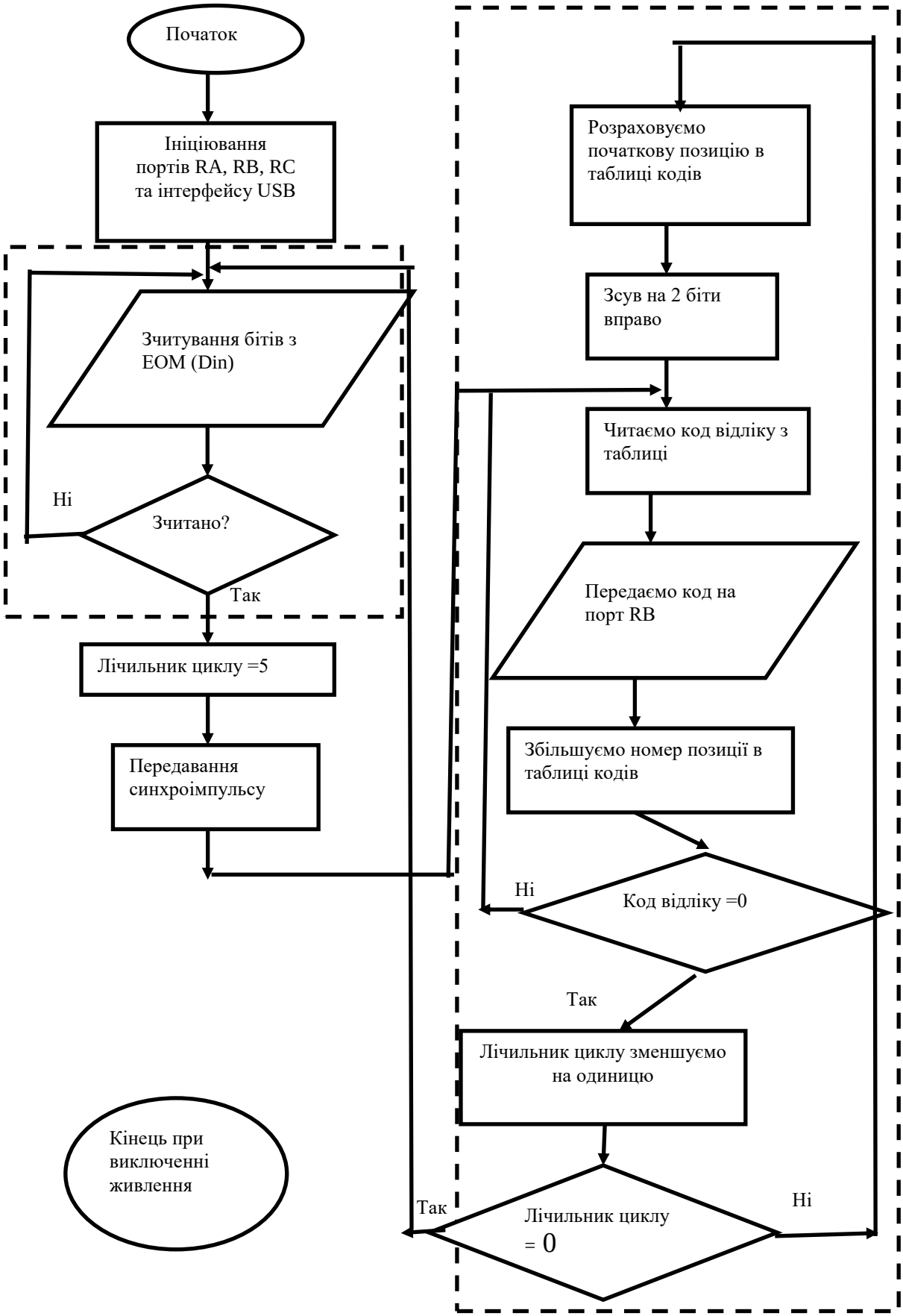


Рис.6.13. Блок-схема алгоритму роботи програми

Система дає можливість генерувати фрактальні імпульси тривалістю 20 мкс при частоті тактового генератора 4 МГц. Пауза між імпульсами, протягом якої передається синхроімпульс, становить 40 мкс.

У декодері мікроконтролер здійснює декодування прийнятих фрактальних імпульсів та передає отриману інформацію на комп'ютер приймальної сторони системи. Схема керованого модуля декодера ФСГС приведена на рис.6.14.

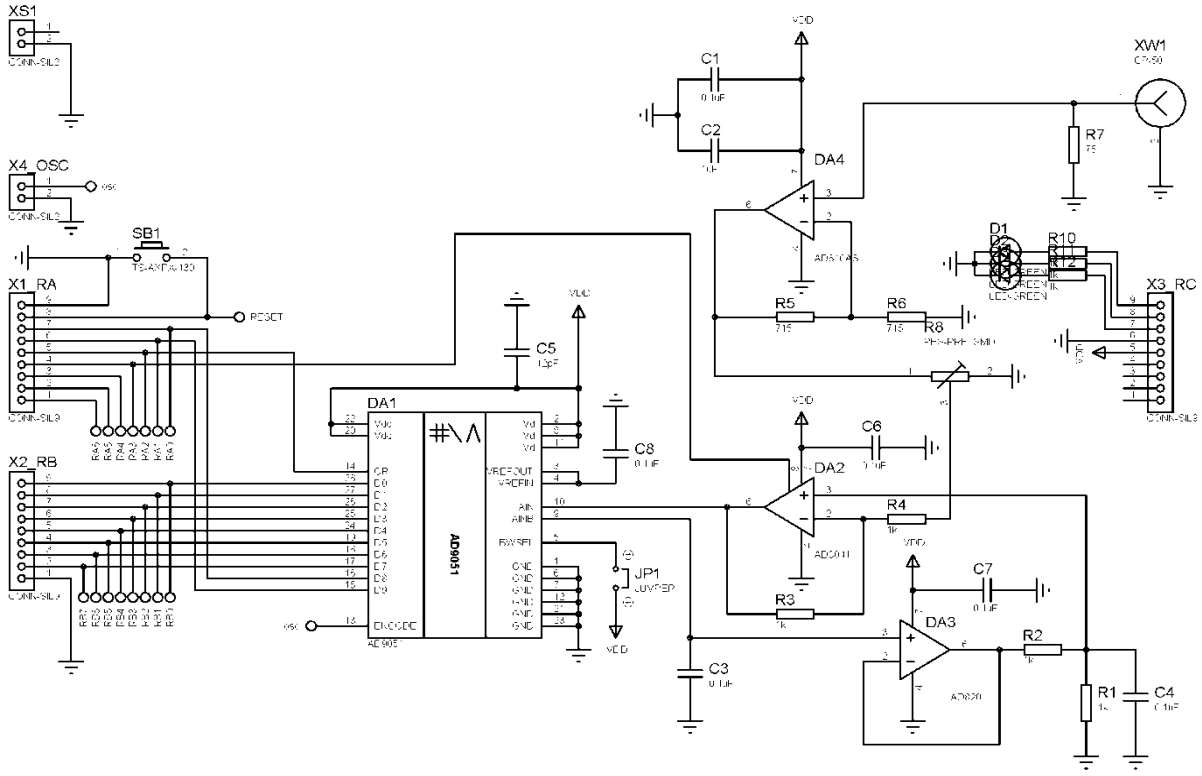


Рис.6.14. Схема електрична принципова керованого модуля декодера

Перетворення сигналу з аналогової форми у цифрову здійснюється АЦП AD9051 фірми Analog Devices, що забезпечує декодування сигналу із необхідною швидкодією. На вході схеми операційні підсилювачі AD820 і AD8041 дозволяють здійснити перетворення однополярного сигналу.

Узгодження хвильового опору коаксіального кабелю із вхідним опором мікроконтролера здійснюється за допомогою операційного підсилювача AD810 (DA4).

Розроблений алгоритм дає можливість визначити порядок фрактального імпульсу. Процес декодування фрактальних сигналів гребінкової структури здійснюється на базі значень суми амплітуд елементарних імпульсів, що його утворюють. Момент початку та завершення фрактального сигналу визначається за допомогою визначення різниці між кодом на вході порта RB та нульовим сигналом.

На рис.6.15 приведені експериментальні часові діаграми фрактальних сигналів гребінкової структури, отримані за допомогою осцилографа TEKTRONIX. Тактова частота мікроконтролера задавалася кварцевим резонатором і становила 4 МГц.

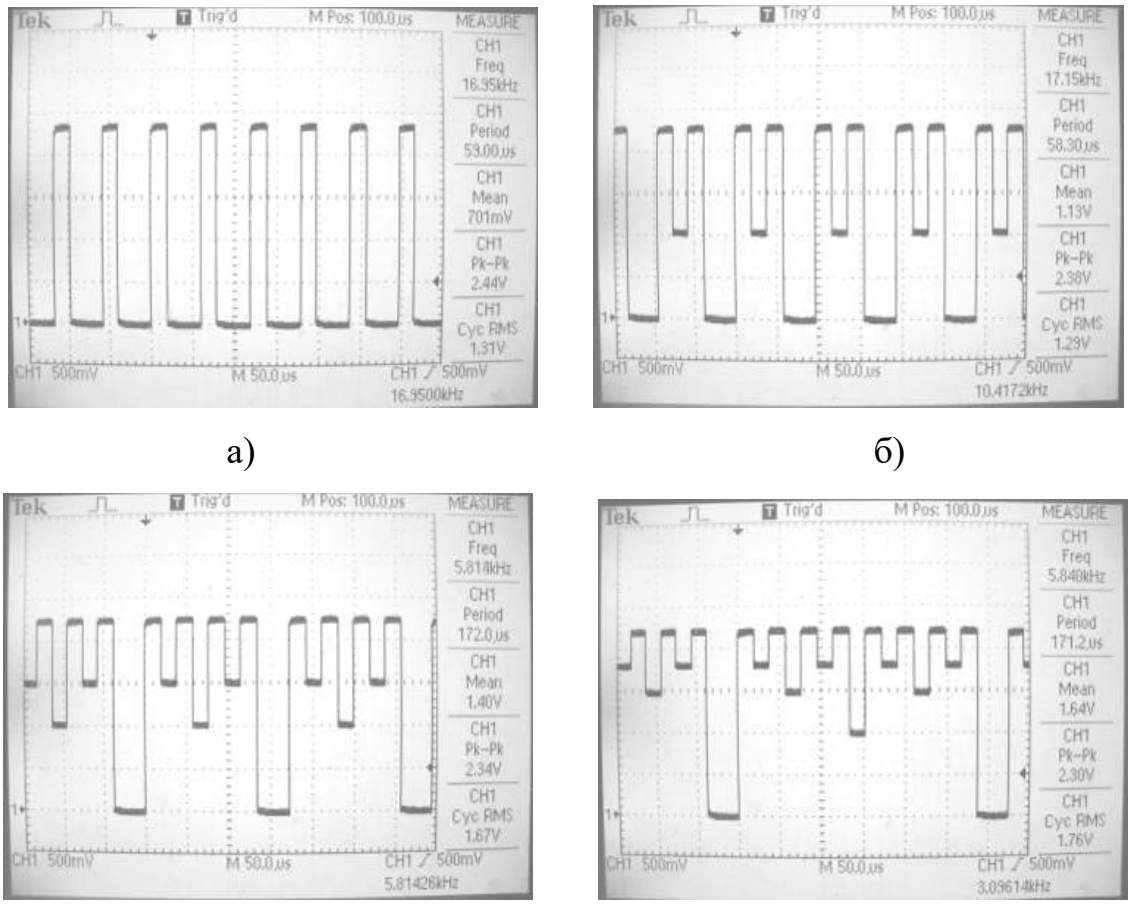
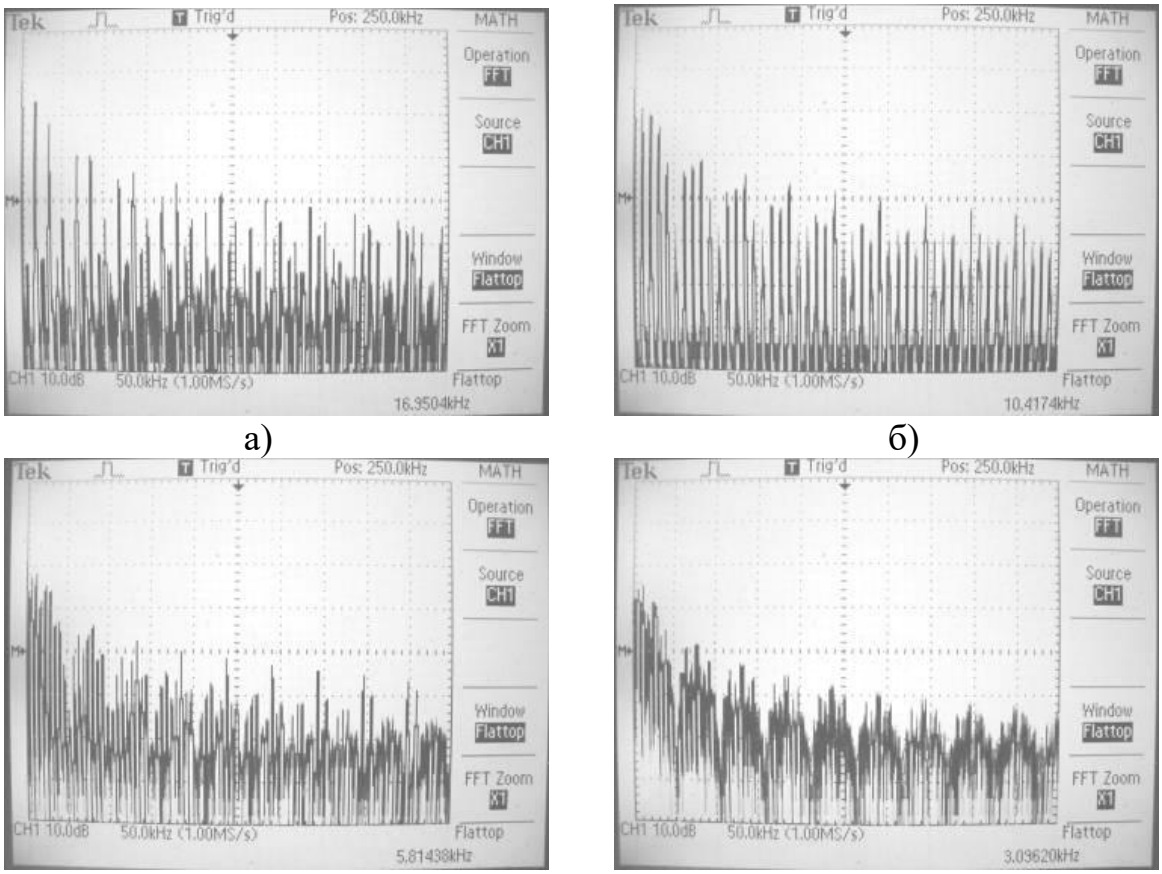


Рис.6.15. Експериментальні осцилограми генерованих фрактальних сигналів порядків w=0 (а); w=1 (б); w=2 (в); w=3 (г)

Найменша тривалість фрагментів генерованих фрактальних імпульсів при тактовій частоті контролера 40 МГЦ становила 2 мкс., що забезпечувало можливість передавання даних зі швидкістю біля 80000 біт/с при кодуванні логічної одиниці фракталом першого порядку, а нуля – паузою між імпульсами. При кодуванні логічних одиниці та нуля фракталами різних порядків швидкість передачі інформації визначається структурою інформаційних послідовностей (довжиною фрагментів, утвореними логічними одиницями або нулями). Кодування інформаційних n-розрядних інформаційних символів може здійснюватися фрактальними сигналами різних порядків, їхня загальна кількість становить 2^n.

На рис.6.16 приведені експериментальні амплітудні спектри фрактальних сигналів, генерованих експериментальним зразком кодера системи.



а) б)

в) г)

Рис.6.16. Експериментальні амплітудні спектри генерованих кодером системи ФСГС різних порядків w=0 (а); w=1 (б); w=2 (в); w=3 (г)

Спектри фрактальних сигналів, що досліджувались у діапазоні частот 0÷500 КГц відповідають обвідній спектру прямокутного імпульсу. Отримані експериментальні результати в основному співпадають із результатами теоретичного моделювання (рис. 6.4).

Тестування кодера та декодера здійснювалося шляхом передавання текстової інформації між двома комп'ютерами. Зв'язок між блоками кодера та декодера здійснювався по коаксіальному кабелю довжиною 10 м із хвилевим опором 75 Ом. Було встановлено, що переданий текст із тисячі символів безпомилково декодується приймальною стороною.

ВИСНОВКИ

1. Розроблений тип фрактальних сигналів (так звані фрактальні сигнали гребінкової структури) та отримана їх математична модель. Досліджені їх енергетичні та кореляційні властивості і отримана математична модель спектральної густини сигналу.

2. Збільшення порядку фракталу призводить до росту рівня постійної складової в порівнянні з іншими спектральними складовими. Генерування фрактального сигналу подібного до „білого” шуму може бути здійснено шляхом вилучення постійної складової із сигналу.

3. Проведені дослідження залежності бази ФСГС від їх порядку та коефіцієнта утворення. Встановлено, що значення бази ФСГС різко зростає зі збільшенням порядку сигналу. Для сигналу п’ятого порядку значення його бази є більшим 200.

4. Розроблені та експериментально реалізовані кодер та декодер ФСГС. Результати експериментальних досліджень їх властивостей співпадають з результатами моделювання.

5. Досліджений фрактальний сигнал можна використовувати для підвищення завадостійкості систем передавання інформації. Розрахункове значення коефіцієнта завадостійкості становить 0,91…0,96.

6. Реалізований експериментальний макет системи передавання інформації на базі двох персональних комп’ютерів, що з’єднані коаксіальним кабелем. Блоки кодера та декодера якого реалізовані на основі мікроконтролерів. Тестування макета системи передавання інформації підтвердили можливість їх використання в системах передавання інформації.

ОСНОВНІ РЕЗУЛЬТАТИ РОБОТИ ТА ВИСНОВКИ

1. В результаті проведеного аналізу літературних джерел встановлено, що важливе місце в сучасних телекомунікаційних системах належить носійним широкосмуговим сигналам, які забезпечують прихованість передавання інформації та підвищують їх крипто та завадостійкість. Базуючись на результатах аналізу обґрунтована необхідність створення методів і моделей програмно-апаратної реалізації функціональних вузлів завадостійких ТКС на базі хаотичних коливань та фрактальних сигналів.

2. В результаті дослідження властивостей послідовностей генерованих пороговим методом за логістичним та узагальненим відображеннями Пекаря встановлені однакові закономірності щодо їх збалансованості. Залежність збалансованості послідовності від початкового значення динамічної змінної носить випадковий характер. Відхилення значень збалансованості послідовностей від одиниці збільшується зі збільшенням їх довжини і становить 6, 10, 15, 20 та 27 для довжин 64, 128, 256, 512 та 1024 біти відповідно. При цьому частка незбалансованих бітів зменшується зі збільшенням довжини послідовностей і становить: 9%, 8%, 6%, 4% та 3% для послідовностей довжиною 64, 128, 256, 512 та 1024 біти відповідно. Значення збалансованості фрагментів послідовності одинакової довжини не залежить від порядку їх розташування у цій послідовності. Розподіл густини ймовірності значень збалансованості є близьким до Гаусового із середнім значенням $M\left(L\right)=0$ та дисперсією $\sigma_0^2=6.47$.

3. Набула подальшого вдосконалення модель системи обміну зашифрованими текстовими повідомленнями, що використовує зручний для обміну інформацією csv-формат файлів і стандартний алгоритм CRC-32 для синхронізації клієнтської та серверної частин із шифруванням переданих повідомлень. Ключами алгоритму слугують генеровані пороговим методом на основі логістичного відображення ПВП. Показано, що при точності

представлення параметра та початкового значення логістичного відображення рівній п’яти десятковим знакам після коми, простір ключів шифрування у системі становить 2^{29}. З підвищенням точності представлення параметрів системи забезпечується збільшення потужності простору ключів; однак при цьому швидкодія обміну між користувачами інформації зменшується внаслідок збільшення часових затрат на реалізацію алгоритму **CRC-32**.

4. Моделюванням впливу канального кодування на процес встановлення синхронізації встановлено, що використання відносно нескладних схем лінійного блокового кодування (кодів Хемінга із 3-ма, 4-ма та 5-ма надлишковими бітами) зменшує час синхронізації до 150 нс при відносному рівні шуму $\eta=0,4\div0,8$ та швидкості передавання даних 10 Мбіт/с; при використанні складніших блокових кодів із 27, 91 та 119 надлишковими бітами час синхронізації зменшується до 200 нс.

5. На основі проведених досліджень процесу синхронізації кільцевих автогенераторів встановлено, що при розкидах значень їх параметрів менших 1.5% та при значеннях коефіцієнту зв’язку між ними більших 2, спостерігається синхронізація у широкому діапазоні частот зрізу ФНЧ. Збільшення частоти зрізу ФНЧ обумовлює зменшення значення функції взаємної кореляції до нуля, внаслідок чого має місце синхронна робота кільцевих генераторів. При зменшені коефіцієнта зв’язку між кільцевими генераторами та частоти зрізу ФНЧ, значення функції взаємної кореляції збільшується, що призводить до втрати синхронізації між генераторами. При дослідженні процесів синхронізації генераторів Чуа в умовах фільтрації сигналів у каналі зв’язку встановлено, що повна синхронізація між генераторами передавальної та приймальної сторін схеми Чуа неможлива навіть при незначній відмінності їх параметрів ($\approx1.5\%$). При значеннях сили зв’язку $e=6$ та частоти зрізу $u=10$ спостерігається явище **on-off** чергування.

6. На основі проведених досліджень встановлені співвідношення параметрів системи з нелінійним підмішуванням синусоїдальних та

частотно-модульованих інформаційних сигналів до генерованих кільцевим генератором псевдовипадкових сигналів. Оптимальне значення коефіцієнта кореляції становить 0,5: значення частоти синусоїдного сигналу становлять $f_0 = 0.4$ та $f_0 = 0.8$, а значення основної частоти і частоти модуляції частотно-модуьованого сигналу дорівнюють $f_0 = 0.5$ та $F = 0.2 \cdot f_0$.

7. Досліджені енергетичні, спектральні та кореляційні властивості сигналів типу фрактальний гаусів шум генерованих з використанням дискретної моделі Мандельброта. Встановлено, що значення фрактального гаусового шуму підпорядковуються нормальному закону у широкому діапазоні значень параметру часового масштабування n=1…50, а залежності дисперсії від цього параметру відрізняються для сигналів з різними показниками Херста. Значення дисперсії для сигналів з H=0,1 зростають від 0,8 до 1,2, залишаються незмінними для сигналів з H=0,5 та зменшуються від 1,2 до 0,9 для сигналів з H=0,9. При цьому математичне сподівання дорівнює 0. Вплив параметру часового масштабування на залежність спектральної характеристики ФГШ показника Херста має місце тільки для сигналів із H=0,1 (збільшується частка високочастотних коливань у спектрі сигналу), що вірогідно обумовлено виникненням додаткових високочастотних коливань зі зменшенням часового масштабу, частота яких є співрозмірною із оберненим значенням часового масштабу.

8. Досліджені фізичні обмеження завадостійкості системи кодування цифрової інформації кластерами, що утворені у фазовому просторі відліками ФГШ. Встановлено, що використання сигналу типу фрактальний гаусовий шум для кодування інформаційних бітів уможливлює їх розпізнавання при співвідношенні сигнал/шум -7,5 дБ при 500 відліках сигналу. Запропонований метод декодування шляхом порівняння параметрів кластерів, що утворені сусідніми інформаційними сигналами, може забезпечувати роботу телекомунікаційних систем в умовах складних електромагнітних обставин.

9. Показано, що система передавання інформації з кластерним кодуванням/декодуванням є стійкою до похибки синхронізації приймальної та передавальної сторін системи. Встановлено, що при використанні в якості сигналу синхронізації 50 відліків дискретного ФГШ з показником Херста рівним 0,4 та одиничним коефіцієнтом часового масштабування максимальне значення похибки синхронізації, при якому можливе розпізнавання інформаційних бітів, становить 80% його тривалості.

10. Вперше запропонований більш точний метод оцінювання мінімального значення співвідношення сигнал/шум, необхідного для розпізнавання інформаційних бітів шляхом моделювання шумів рядами з Гаусовим розподілом.

11. Набули подальшого розвитку методи синтезу широкосмугових сигналів із самоподібною структурою. Вперше запропоновані фрактальні сигнали гребінкової структури, розроблена їх математична модель та досліджені енергетичні спектральні і кореляційні властивості. Збільшення кількості твірних елементів самоподібної структури запропонованого сигналу складної конструкції призводить до значного зростання значення бази сигналу. При значенні коефіцієнту утворення 0,2 та п’яти твірних елементах сигналу його база становить 200.

12. ФСГС з малим значенням порядку фракталу за своїми кореляційними та спектральними властивостями є подібними до одиничних прямокутних імпульсів. Спектр фрактальних сигналів гребінкової структури є сегментованим із рівновіддаленими максимумами спектральної густини потужності ($\Delta f = 10/T_i$). Значення бази сигналів становить ≈200, що вказує на можливість їх використання у завадостійких системах передавання інформації. За результатами досліджень на основі мікроконтролера PIC18F2550 розроблені кодер та декодер для кодування/декодування цифрової інформації. Результати експериментальних досліджень процесу передавання цифрової інформації закодованої ФСГС з використанням розроблених кодера/декодера

підтверджують можливість їх використання в телекомунікаційних системах.

13. За результатами досліджень властивостей ФГШ встановлені закономіпності прохождення самоподібних потоків Інтернет-трафіку в наближенні, що вони є самоподібними і описуються математичною моделлю фрактального гаусового шуму. При збільшенні інтенсивності до $0.9 \cdot 10^5$ запитів/годину результати моделювання середнього часу проходження трафіку через систему для потоків із різними типами розподілу показують значні розбіжності у значенні середнього часу проходження кожного запиту, що становлять 33; 39; 41 мс для рівномірного, самоподібного та пуасонівського розподілів відповідно. Встановлено також, що має місце істотна залежність середнього часу від коефіцієнта самоподібності (показника Херста) потоку. При цьому середній час проходження пакетів залишається однаковим, але процеси проходження суттєво відрізняються між собою.

14. Встановлено, що середній час проходження запиту через телекомунікаційну систему для трафіку змодельованого самоподібним та Пуасонівським розподілами добре корелюють між собою і становлять 32 та 30 мс відповідно та відрізняються від результатів для потоків із рівномірним розподілом при інтенсивності порядка $1.8 \cdot 10^3$ запитів/годину.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Бобало, Ю.Я. Прикладне застосування теорії хаотичних систем у телекомунікаціях : монографія / Ю. Я. Бобало, С. Д. Галюк, М. М. Климаш, Р.Л. Політанський. – Дрогобич – Львів: Коло, 2015. – 184 ст.

2. Bobalo Y. Traffic simulation in a telecommunication system based on queuing systems with different input flows / Y. Bobalo, R. Politanskyi, M. Klymash // Econtechmod. An international quarterly journal on economics in technology, new technologies and modelling processes. – 2015. – Vol. 4, № 1. – P. 11-15.

3. Bobalo, Y. Design and hardware implementation of fractal comb-structured signals / Y. Bobalo, A. Veriha, M. Klymash, B. Mandziy and R. Politanskyi // Smart Computing Review. – 2014. – Vol. 4, No. 6. – P. 469-459.

4. Bobalo Y. Hardware and software realization of the transmission of audio information encrypted by chaotic sequences / Y. Bobalo, Z. Hotra, O. Hres, R. Politanskyi // IAPGOS. – 2014. – Vol. 4. – P. 53-55.

5. Гресь, О.В. Апаратна реалізація пристрою шифрування мовної інформації / О.В. Гресь, А.Д. Верига, Р.Л. Політанський, О.В. Дробик// Сучасний захист інформації. – 2014. – № 3. – С. 71-78.

6. Верига, А.Д. Кодер и декодер фрактальных сигналов гребенчатой стуктуры / А.Д. Верига, Р.Л. Политанский // Технология конструирования в электронной аппаратуре. Системы передачи и обработки данных. — 2014. — №4. —С. 13—21.

7. Бобало, Ю.Я. Дослідження алгоритму криптографічного захисту зображення на основі багатомірного узагальненого перетворення Пекаря / Ю. Я. Бобало, Р.Л. Політанський, М.М. Климаш, Г.В. Косован // Системи обробки інформації. — 2014. — Випуск 7, № 123. — С. 118—120.

8. Eliiashiv, Oleg M. Software implementation of Multi-User Text Messaging System Using Logistic Map / Oleg M. Eliiashiv, Leonid F. Politanskiy,

Ruslan L. Politanskiy, Nazariy G. Hladun // Eastern European Scientific Journal. — 2014. — № 3. — P. 238—243.

9. Политанский, Р.Л. Система передачи данных с шифрованием хаотическими последовательностями / Р.Л. Политанский, П. М. Шпатарь, О.В. Гресь, А.Д. Верига // Технология конструирования в электронной аппаратуре. Системы передачи и обработки данных. — 2014. — №2-3. — 28—31.

10. Bobalo, Yuriy. Energetical properties of fractal brownian signal with different Herst indexes / Yuriy Bobalo, M. Klymash, Ruslan Politanskiy // Computational problems of electrical engineering. — 2013. — Vol. 3, № 2. — P.6—9.

11. Бобало, Ю.Я. Вплив кофцієнту часового масштабування сигналів типу фрактальний гаусів шум на його енергетичні, статистичні та кореляційні властивості / Ю. Я. Бобало, Р.Л. Політанський, М.М. Климаш, А.Д. Верига // Системи обробки інформації. — 2013. — Випуск 7, № 114. — С. 164—171.

12. Гресь, О.В. Алгоритм шифрування інформації з використанням псевдовипадкових послідовностей / О.В. Гресь, Р.Л. Політанський, П.М. Шпатар, А.Д, Верига // Наукові записки українського науково-дослідного інституту зв'язку. Науково-виробничий збірник. — 2013. — № 1/25. — С. 88-93.

13. Політанський, Р.Л. Кодування каналу передавання даних, шифрованих псевдовипадковими послідовностями / Р.Л. Політанський, Л.Ф. Політанський, П.М. Шпатар, П.В. Іванюк // Восточно-Европейский журнал передовых технологий. — 2013. — Т. 61, № 1/9. —С. 61—65.

14. Иванюк, П.В. Генератор хаотических сигналов на основе системы дифференциальных уравнений с четырьмя переменными / П.В. Иванюк, Л.Ф. Политанский, Р.Л. Политанский // Applied Radio Electronics. — 2012. — № 3/11. — С.347—354.

15. Політанський, Р. Л. Моделювання схем шифрування інформації з використанням псевдовипадкових послідовностей / Р. Л. Політанський, Л.Ф. Політанський, П.М. Шпатар, О.В. Гресь // Восточно-Европейский журнал передовых технологий. — 2012. — Т. 57, № 3/9. — С. 50—52.

16. Іванюк, П.В. Хаотичне маскування інформаційних сигналів з використанням генератора на базі системи Лю / П.В. Іванюк, Л.Ф. Політанський, Р.Л. Політанський, О.М. Еліяшів // Технология и конструирование в электронной аппаратуре. Системи передачі та обробки інформації. — 2012. — № 3.—С. 11 – 17.

17. Політанський, Р.Л. Метод кластерного кодування / Р.Л. Політанський, М. М. Климаш // Восточно-Европейский журнал передових технологий. — 2012. — Т. 59, № 5/3. — С. 50 — 54.

18. Політанський, Р.Л. Шифрування інформації з використанням псевдовипадкових гаусових послідовностей / Р.Л. Політанський, П.М. Шпатар, О.В. Гресь, В.Я. Ляшкевич // Восточноевропейский журнал передовых технологий. — 2012. — Т.60, № 6/11. — С. 8—10.

19. 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.

20. Еліяшів, О.М. Дослідження властивостей нелінійного елемента передавача хаотичної системи зв’язку / О.М. Еліяшів, В.Б. Русин, Л.Ф. Політанський, М.Я. Кушнір, Р. Л. Політанський // Радиоэлектроника и информатика. Научно-технический журнал. — 2011. — № 2 (53). — С. 12—17.

21. Іванюк П.В. Дослідження хаотичних процесів, генерованих системою Лі / П. В. Іванюк, Л. Ф. Політанський, Р. Л. Політанський // Восточно-Европейский журнал передовых технологий. Информационно-управляющие системы. — 2011. —№ 52.— С. 11—15.

22. Іволга Л.Г. Прецизійний генератор хаосу в інваріантних системах зв’язку [Електронний ресурс] / Л.Г. Іволга, Л.Ф. Політанський, Р.Л.

Політанський // Проблеми телекомунікацій. – 2011. – № 1 (3). – С. 106 – 116. – Режим доступу до журн.: http://pt.journal.kh.ua/2011/1/1/111_ivolga_chaos.pdf.

23. Політанський, Р.Л. Исследование зависимости корреляции между несущим и информационным сигналом в системах с динамическим хаосом / Р.Л. Политанский, Л.Ф. Политанский, С.Д. Галюк, Н.Я. Кушнир // Восточно-Европейский журнал передовых технологий. Информационные технологии. — 2011. — № 50 — С. 20—25.

24. Політанський, Р.Л. Система передавання даних з використанням генераторів хаосу / Р.Л. Політанський, Політанський Л.Ф., Гресь О.В., Галюк С.Д. // Всеукраинский межведомственный научно-технический сборник. «Радиотехника». — 2011. — № 164. — С. 66—71.

25. Политанский, Р.Л. Збалансованість псевдовипадкових послідовностей, генерованих нелінійними схемами / Р.Л Политанский, Л. Ф. Политанский, П. В. Иванюк // Всеукраинский межведомственный научно-технический сборник. «Радиотехника». — 2010. — № 160. — С. 356—359.

26. Політанський, Р.Л. Властивості псевдовипадкових послідовностей, генерованих картами хаосу / Р.Л. Політанський, З. Ю. Готра // Збірник наукових праць «Комп’ютерні технології друкарства». — 2010. С. 97-105.

27. Політанський, Р.Л. Збалансованість псевдовипадкових послідовностей, генерованих нелінійними схемами / Р.Л. Політанський, Л.Ф. Політанський, П.В. Іванюк // «Радіоелектроніка та телекомунікації», видавництво НУ «ЛП». — 2010. — № 680. — С. 165—169.

28. Еліяшів, О.М. Багатокористувальницька система зв’язку з використанням хаотичної частотної модуляції сигналу / Л.Ф. Політанський, М.Я. Кушнір, Р.Л. Політанський, О.М. Еліяшів // Східно–Європейський журнал передових технологій. — 2010. — №1/5(43). — С. 44 — 47.

29. Галюк, С.Д. Синхронізація хаотичних систем і фільтрація сигналів в каналі зв'язку / С.Д. Галюк, М.Я. Кушнір, Л.Ф. Політанський, Р.Л.

Політанський // Східно-Європейський журнал передових технологій. — 2010. — № 1/5(43). — С. 20—24.

30. Політанський, Р.Л. Дослідження властивостей циклічності псевдовипадкових послідовностей бітів / Р.Л. Політанський, Л. Ф. Політанський, М. Я. Кушнір // Восточно-Европейский журнал передовых технологий. Системы управления. — 2009. — № 42. — С. 64—66.

31. Пат. 106856 Україна, МПК H04L 9/00. Система приймання-передавання цифрової інформації / Бобало Ю.Я., Верига А.Д., Климаш М.М., Політанський Р.Л; заявник і патентовласник Національний Університет «Львівська політехніка». – № a2012 08429; заяв. 09.07.2012; опубл. 10.10.2014, Бюл. № 19.

32. Пат. на корисну модель № 76468 Україна, МПК H03M 7/00, H03M 7/30 (2006.01), H03M 13/07. Система кодування/декодування інформації з шифруванням/ Політанський Л.Ф., Політанський Р.Л., Гресь О.В.; заявник і патентовласник Чернівецький Національний Університет імені Юрія Федьковича. – № и2012 05880; заяв. 14.05.2012; опубл. 10.01.2013, Бюл. № 1.

33. Пат. 101591 Україна, МПК G09B 9/00, G06F 7/00, G06F 11/00, H03M 7/14. Пристрій для вивчення згорткового кодування / Політанский Л.Ф., Політанський Р.Л, Сендульський М. В.; заявник і патентовласник Чернівецький Національний Університет ім. Юрія Федьковича – № a2012 08429; заяв. 09.07.2012; опубл. 10.04.2013, Бюл. № 7.

34. Політанський, Р.Л. Широкосмугові сигнали у телекомунікаційних системах / Ю.Я. Бобало, А.Д. Верига, С.Д. Галюк, М. М. Климаш, Р.Л. Політанський, // IV-а Міжнародна науково-практична конференція «Фізико-технологічні проблеми радіотехнічних пристроїв, засобів телекомунікацій, нано- та мікроелектроніки. – Чернівці, Жовтень, 2014, С. 25-26.

35. Політанський Р.Л. База та коефіцієнт завадостійкості фрактальних сигналів гребінкової структури / Р.Л. Політанський, А.Д. Верига, В.В. Лесінський // IV-а Міжнародна науково-практична конференція «Фізико-

технологічні проблеми радіотехнічних пристроїв, засобів телекомунікацій, нано- та мікроелектроніки. – Чернівці, Жовтень, 2014, С. 60

36. Гресь О.В. Пристрій генерування хаотичних сигналів на основі дискретних одномірних відображень / О.В. Гресь, Р.Л. Політанський, А.Д. Верига, М.М. Іванчук // IV-а Міжнародна науково-практична конференція «Фізико-технологічні проблеми радіотехнічних пристроїв, засобів телекомунікацій, нано- та мікроелектроніки. – Чернівці, Жовтень, 2014. С. 83-84.

37. Ruslan Politanskyi. The Data Transfering Systems With Using of the Chaotic Signals Non-coherent Detection / R. Politanskyi, M. Klymash, Y. Bobalo // «Modern Problems of Radio Engineering, Telecommunications, and Computer Science». – Lviv-Slavske, Ukraine. – March 1. – 2014. – P. 433.

38. Верига, А.Д. Декодер фрактальних сигналів гребінкової структури / А. Д. Верига, Р. Л. Політанський // III Міжнародна науково-практична конференція «Фізико-технологічні проблеми радіотехнічних пристроїв, засобів телекомунікацій, нано- та мікроелектроніки». —Чернівці, Україна. — Жовтень, 2013.

39. Гресь, О. В. Система передавання аудіо-інформації з шифруванням хаотичними послідовностями / О. В. Гресь, Р. Л. Політанський, П. М. Шпатар // III Міжнародна науково-практична конференція «Фізико-технологічні проблеми радіотехнічних пристроїв, засобів телекомунікацій, нано- та мікроелектроніки». —Чернівці, Україна. —Жовтень, 2013.

40. Політанський, Р.Л. Вплив коефіцієнту часового масштабування на властивості фрактального гаусового шуму / Р. Л. Політанський, М. М. Климаш // II Міжнародна науково-практична конференція «Інформаційні проблеми теорії акустичних, радіоелектронних і телекомунікаційних систем». — Крим. — Вересень, 2013.

41. Шпатар, П. М. Система передавання даних з шифруванням хаотичними послідовностями / П. М. Шпатар, Р. Л. Політанський, О. В. Гресь, Є. І. Болонна // IV Міжнародна науково-практична конференція

«Обробка сигналів і негаусівських процесів». — Черкаси, Україна. — Травень, 2013.

42. Politanskiy, R.L. Spectra of pulse signals formed on the basis of the fractal brownian signals (fbs) / R. L. Politanskiy, M.M. Klymash // XII International Conference «The experience of designing and application of CAD systems in microelectrinics». — Lviv, Ukraine. — February, 2013. —P. 295 – 296.

43. Політанський, Р.Л. Енергетична ефективність широкосмугової системи, що використовує фрактальні сигнали / Р.Л. Політанський // VI Международный научно-технический симпозиум «Новые технологии в телекоммуникациях». — Киев, Украина. — Січень, 2013. С. 60—63.

44. Політанський, Л.Ф. Алгоритм шифрування даних з використанням псевдовипадкових послідовностей / Л.Ф. Політанський, П.М. Шпатар, О.В. Гресь, Р.Л. Політанський // VI Международный научно-технический симпозиум «Новые технологии в телекоммуникациях». — Киев, Украина. — Січень, 2013. С. 54.

45. Politansky, R. Application of the Self-Similarity of Chaotic Processes for Digital Communication Systems / R. Politanskyi, L. Politanskyi, P. Ivanyuk // XIth International Conference «Modern Problems of Radio Engineering, Telecommunications, and Computer Science». – Lviv-Slavske, Ukraine. – February. – 2012. — P. 433.

46. Гресь, О.В. Шифрування інформації з використанням псевдовипадкових гаусових послідовностей / О.В. Гресь, П.М. Шпатар, Р.Л. Політанський // II Міжнародна науково-практична конференція «Фізико-технологічні проблеми радіотехнічних пристроїв, засобів телекомунікацій, нано- та мікроелектроніки». — Чернівці, Україна. — Жовтень, 2012. — С. 89.

47. Політанський, Р.Л. Дослідження методу кластерного кодування / Р.Л. Політанський, М.М. Климаш // II Міжнародна науково-практична конференція «Фізико-технологічні проблеми радіотехнічних пристроїв,

засобів телекомунікацій, нано- та мікроелектроніки». — Чернівці, Україна. — Жовтень, 2012. — С. 18—19.

48. Politansky, L. Data Transmission System Using Pseudorandom Sequences / L. Politansky, R. Politansky, P. Shpatar, A. Gres // VII Міжнародна Науково-технічна конференція «Сучасні інформаційно-комунікаційні технології». – Ялта, Крим. – Жовтень, 2012. – С.76-78.

49. Політанський, Л.Ф. Система передавання даних з використанням псевдовипадкових послідовностей в кодах Хемінга / Л.Ф. Політанський, Р.Л. Політанський, М.Г. Рождественська, О.В. Гресь // Труди XII-ї Міжнародної науково-практичної конференції «Сучасні інформаційні та електронні технології». – Одеса, Україна. – Травень. – 2011. – С. 156.

50. Іванюк, П.В. Моделювання системи, що породжує гіперхаос, в програмному середовищі LabView / П.В. Іванюк, Л.Ф. Політанський, Р.Л. Політанський // І Всеукраїнська науково-практична конференція «Фізико-технологічні проблеми радіотехнічних пристроїв, засобів телекомунікації, нано- та мікроелектроніки». — Чернівці, Україна. — Жовтень, 2011. — С. 139—141.

51. Іванюк, П.В. Оцінки чисельних характеристик систем детермінованого хаосу / П.В. Іванюк, Р.Л. Політанський // І-а Всеукраїнська науково-практична конференція «Фізико-технологічні проблеми радіотехічних пристроїв, засобів телекомунікацій, нано- та мікроелектроніки». — Чернівці, Україна. — Жовтень, 2011. — С. 107—110.

52. Політанський, Р.Л. Система передачі даних з використанням хаотичної маніпуляції / Р.Л. Політанський, Л.Ф. Політанський, О.В. Гресь, М. Г. Рождественська // IV Міжнародна науково-технічна конференція молодих вчених «Комп'ютерні науки та інженерія». — Львів, Україна. — 2010. — С. 127—128.

53. Політанський, Р.Л. Дослідження псевдовипадкових послідовностей, генерованих картами хаосу / Р.Л. Політанський, З.Ю. Готра // IV Міжнародна

науково-технічна конференція і II студентська науково-технічна конфренція «Проблеми телекомунікацій». — Київ, Україна. — 2010. — С. 127—128.

54. Мандзій, Б. А. Основи теорії сигналів / Б.А. Мандзій, Р.І. Желяк // Підручник. За ред. Б.А. Мандзія. Львів: Видавничий дім «Ініціатива». — 2008. — 240 с.

55. Романов, Б.Н. Теория электрической связи. Сообщения, сигналы, помехи, их математические модели: учебное пособие / Б. Н. Романов, С. В. Краснов; Ульяновский государственный технический университет. — У. : Университет, 2008.— 128 с.— Библиогр. : с. 84—85.

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

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

58. Кяргинский, Б. Е. Генераторы на биполярных транзисторах различной мощности / Б. Е. Кяргинский // Электронная техника. Сер. СВЧ-техника. — 1993. — Т. 457, Вып. 3. — с. 3-7.

59. Pecora, M.L. Fundamentals of synchronization in chaotic systems, concepts, and applications / Louis M. Pecora, Thomas L. Carroll, Gregg A. Johnson, and Douglas J. Mar // Chaos. – 1997. – V. 7, № 4. – P. 520—543.

60. Шустер, Г. Детерминированный хаос: Введение: пер. с нем. — В.:; М.: Мир, 1988.—240с.

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

62. Федер Е. Фракталы: Пер. С англ. – М.: Мир, 1991. – 254 с., ISBN 5-03-001712-7.

63. Oprean, C. Fractality evidence and long-range dependence on capital markets: a Hurst exponent evaluation / C. Oprean, C.Tănăsescu //Fractals. – 2014. –Vol. 22, No. 4. – P. 1450010-1–1450010-16.

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

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

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

67. Takens, F Detecting strange attractors in turbulence / F. Takens // Dynamical Systems and Turbulence. Lecture Notes in Mathematics. — 1980. — Vol. 898. — P. 366—381.

68. Шарковский, А. Н. Сосуществование циклов непрерывного отображения прямой в себя /А.Н. Шарковский // Украинский математический журнал. — 1964.— №1. —С.61—71.

69. Шарковский, А. Н. Притягивающие множества, не содержащие циклов /А.Н. Шарковский // Украинский математический журнал. — 1968. — №1. — С.136—142.

70. Шарковский, А.Н. Разностные уравнения и их приложения / А.Н. Шарковский, Ю.Л. Майстренко, Е. Ю. Романенко; под общ. ред. А.Н. Шарковского; АН УРСР— Киев.: Наукова думка, 1986. —280 с.

71. Silva, C. P. Introduction to Chaos-Based Communications and Signal Processing / C. P. Silva, A. M. Young // IEEE Aerospace Conference Reprint. – 2000. – P. 21.

72. Feigenbaum, M. J. The Universal Properties of Nonlinear Transformations / Feigenbaum M. J. // J. Stat. Phys. — 1979. — № 21. — P. 669.

73. Лоскутов, А.Ю. Основы теории сложных систем. – М.-Ижевск: Институт компьютерных исследований, 2007. – 620 с.

74. Pomeau, Y. Intermittent Transition to Turbulence in Dissipative Dynamical Systems / Y. Pomeau, P. Manneville // Comm. Math. Phys. – 1980. – № 74. – P. 189.

75. Lorenz, E. N. Deterministic nonperiodic flow / E. N. Lorenz // J. Atmos. Sci. — 1966. —Vol. 20. — № 2. — P. 130-141.

76. Chen, G. Yet another chaotic attractor / G. Chen, T. Ueta // Int J. of Bifurcation and Chaos. — 1999. — № 9. —P.1465—1466.

77. Rössler, O.E. An equation for continuous chaos / O.E. Rössler // Phys. Lett. — 1976. — Vol. A57, № 5. — P. 397, 395.

78. Rössler, O.E. An equation for hyperchaos / O.E. Rössler // Phys. Lett. — 1979. — Vol. A71, № 2,3. — P. 155—159.

79 . Sprott, J.C. Some simple chaotic flows / J.C. Sprott // Phys. Rev. — 1994. — Vol. E50, № 2. — P.647—650.

80. Jinhu Lu, The compound structure of a new chaotic attractor. [Текст] / Jinhu Lu, Guanrong Chen, Suochun Zhang // Chaos, solitons and fractals. – 2002. – No. 14. – P. 669–672.

81. Luo Xiao-Hua, Circuitry implementation of a novel four-dimensional nonautonomous hyperchaotic Liu system and its experimental studies on synchronization control [Текст] / Luo Xiao-Hua at al. // Chinese Physics B. – 2009. Vol. 18 No. 6. – P. 2168–2175.

82. Banerjee, S. Lyapunov function, parameter estimation, synchronization and chaotic cryptography / S. Banerjee, A. R. Chowdhury // Commun. Nonlinear Sci. Numer. Simulat. — 2009. — Vol. 14. — P. 2248—2254.

83. Benettin, G. Lyapunov characteristic exponents for smoth dynamical systems and for Hamiltonian systems: A method for computing all of them. P. I: Theory. P. II: Numerical application / G. Benettin, L. Galgani, A. Giorgilli, J.-M. Strelcyn // Meccanica. — 1980. — Vol.15. — P.9—30.

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

85. Анищенко, В.С. Сложные колебания в простых системах / В.С. Анищенко. – М.: Наука, 1999. с. 311.

86. Udwadia, F. E. Computation of Lyapunov characteristic exponents for continuous dynamical systems / F.E. Udwadia, H. F. von Bremen // Math. Phys. — 2002. — Vol. 53. — P.123-146.

87. Пиковский А. Синхронзация: фундаментальное нелинейное явление / А. Пиковский, М. Розенблюм, Ю. Куртс. – М.: Техносфера, 2003. – 508 с.

88. Czeisler, C.A. Stability, precision, and near-24-hour period of the human circadian pacemaker / C.A. Czeisler, J. F. Duffy, T. L. Shanahan, E. N. Brown, J. F. Mitchell, D. W. Rimmer, J. M. Ronda, E. J. Silva, J. S. Allan, J. S. Emens, D. J. Dijk, R.E. Kronauer // Science. — 1999. — Vol. 284. — P. 2177—2181.

89. Buck, J. Mechanism of rhythmic synchronous flashing of fireflies / J. Buck, E. Buck // Science. — 1968. — Vol. 159. — P.1319—1327.

90. Anishchenko, V.S. Entrainment between heart and weak noninvasive forcing / V. S. Anishchenko, A.G. Balanov, N.B. Janson, N.B. Igosheva, G.V. Bordyugov // Int J. Bifurc. Chaos. — 2000. — Vol. 10. — № 10. — P. 2339-2348.

91. Stern, E.A. Membrane potential synchrony of simultaneously recorded striatal spiny neurons in vivo / E.A. Stern, D. Jaeger, and C. J. Wilson // Nature. — 1998. —Vol. 394. — P. 475—478.

92. Lin, L.A. Resonant Phase Patterns in a Reaction-Diffusion System / A. L. Lin, M. Bertram, K. Martinez, H. L. Swinney, A. Ardelea, G. F. Garey // Phys. Rev. Lett. — 2000. — Vol. 84, № 18. — P. 4240—4243.

93. Homessa, C. H. Cycles and chaos in a socialist economy / C.H. Homesa, H. E. Nusseb, A. Simonovits // Journal of Economic Dynamics and Control. — 1995. — Vol. 19, № 1-2. — P. 155—179.

94. LeBaron, B. Chaos and nonlinear forecastability in economics and finance / B. LeBaron // Philosophical Transactions: Physical Sciences and Engineering. — 1994. — Vol. 348, № 1688. — P. 397—404.

95. Kiel, L. D. Chaos theory in the social sciences: foundation and applications / L. D. Kiel, W.E. Elliot // University of Michigan Press. — 1996. — 349 p.

96. Дербенцев, В. Д. Синергетичні та економфізичні методи дослідження динамічних та структурних характеристик економічних систем / В.Д. Дербенцев, О. А. Сердюк, В. М. Соовйов, О.Д. Шарапов // Монографія. – Черкаси: Брама-Україна. – 2010. – 287 с.

97. Fujisaka, H. Stability theory of synchronized motions in coupled oscillatory systems / H.Fujisaka, T. Yamada // Prog. Theor. Phys. — 1983. — Vol. 69. — P.32—46.

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

99. Pecora, L.M. Synchronization in Chaotic Systems / L.M. Pecora, T.L. Carroll // Phys.Rev Lett. — 1990. —Vol. 64 — P. 821.

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

101. Marino, I.P. Channel coding in communications using chaos / I. P. Marino, L. Lopez, M. A.F. Sanjuan // Physics Letters A. — 2002. — Vol. 295, № 2. — P. 185—191.

102. Bollt, E. Dynamics of coding in communicating with chaos / E. Bolt, Y. C. Lai // Phys. Rev. E. — 1998. — Vol. 58, № 2. — P. 1724—1736.

103. Baptista, M.S. Cryptography with chaos / M.S. Baptista // Phys. Lett. A. — 1998. — Vol. 240, № 1-2. — P. 50—54.

104. Jakimovski, G. Chaos and Cryptography: Block Encryption Ciphers Based on Chaotic Maps / G. Jakimovski, L. Kocarev // IEEE Trans. on circ. and syst. I: Fund. Theory and appl. — 2001. — Vol. 48, № 2. — P. 163—169.

105. Oliviera, L.P. Cryptography with chaotic mixing / L.P. de Oliveira, M. Sobottka // Chaos, Solitons and Fractals. — 2008. — Vol. 35, № 3. — P. 466—471.

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

107. Bocaletti, S. The synchronization of chaotic systems / S. Bocaletti, J. Kurths, D.L. Valladares, C.S. Zhou // Physics Report. — 2002. — Vol. 36, № 1-2. — P.1—101.

108. Kapitaniak, T. Synchronization of chaotic systems / T. Kapitaniak // Phys. Rev. E. — 1994. — Vol. 50, № 2. — P.1642—1644.

109. Stojanovski, T. Driving and synchronization by chaotic impulses / T. Stojanovski, L. Kocarev, U. Parlitz // Phys. Rev. E. — 1996. — Vol. 54, № 18. — P.2128—2131.

110. Silva, C. P. Introduction to Chaos-Based Communications and Signal Processing / C. P. Silva, A. M. Young // IEEE Aerospace Conference Reprint. – 2000. – P. 21.

111. Liao, Teh-Lu. Adaptive synchronization of chaotic systems and its application to secure communications / The-Lu Liao, Shin-Hwa Tsai // Chaos, Solitons and Fractals. – 2000. – v. 11. – p. 1387-1396.

112. Yang, T. A survey of chaotic secure communication systems / Tao Yang // International Journal of Computational Cognition. — 2004. V. 2, № 2. — P. 81—130.

113. Yang, T. Secure Communication via Chaotic Parameter Modulation / T. Yang, L. O. Chua // IEEE Transaction on Cercuits and Systems – I: Fundamental Theory and Application. – 1996. – Vol. 46, N 9. – 817-819.

114. Volkovskii, R. Multi-User Communication using Chaotic Frequency Modulation / R. Volkovskii, S.C. Young, L. S. Tsimring and N. F. Rulkov // Proc. International Symposium NOLTA ’01. P. 561-564.

115. Volkovskii, A. R. Synchronization an communication using chaotic frequency modulation / A.R. Volkovskii and L. S. Tsiming // Int. J. Circ. Theor. Appl. — 1999. — Vol. 27. — P. 569-567.

116. Koronovskii, A.A. On the use of chaotic synchronization for secure communication / A.A. Koronovskii, O. I. Moskalenko, A. E. Hramov // Physics-Uspekhi. – 2009. – Vol. 12, № 52. – P. 1213-1238.

117. Electronic encryption device and method: Pat № 6078665 USA: H04/L 9/28 / Anderson R., Schultz G. R., Heptig J. P.,; assignee Intelligent Security systems. Inc. — № 08/954795; 21.10.97; 20.06.00, — 11 p.

118. INDOCRYPT 2001, the 2nd International Conference on Cryptology in India (INDOCRYPT'2001, 16-20 December, 2001, Indian Institute of Technology, Madras, Chennai, India), LNCS, vol. 2247,pp. 316-329.

119. Chaos-based Pseudo-Random Number Generators and Chip Implementation. Zhong Li, Ping Li, Yaobin Mao, W.A. Halang. Proceedings of the 16th IFAC World Congress, 2005, pp. 837-837.

120. Скляр, Б. Цифровая связь. Теоретические основы и практическое применение: пер. с англ. — М.: Издательский дом «Вильямс», 2007. — 1104 с.

121. Berrou, C. Near optimum error correcting coding and decoding: Turbo-codes / C. Berrou, A. Glavieux // IEEE Trans. Commun. — 1996. — Vol. 44. — P. 1261-1271.

122. Pseudo-random bit generator based on couple chaotic systems and its applications in stream-cipher cryptography. Li Shujun, Mou Xuanqin and Cai Yuanlong. Progress in Cryptology - INDOCRYPT 2001, the 2nd International Conference on Cryptology in India (INDOCRYPT'2001, 16-20 December, 2001, Indian Institute of Technology, Madras, Chennai, India), LNCS, vol. 2247,pp. 316-329.

123. Patent № 6.788.787 B1 USA, G06F 1/02. Pseudorandom number generator, stream encryption method, and stream encrypting communication method / K. Shono, O. Ueno, T. Ishihara; Assigne Yazaki Corp. — Appl. N 09/512.284, filed Feb. 24.2004; Pub date Sep. 7.2004.

124. Raymond, S.T. A Chaotic Real-time Cryptosystem using a Switching Algorithmic-based Linear Congruential Generator (SLCG) / S. T. Raymond, W. S.

Henry // International Journal of Computer Science and Network Security. — 2006. — Vol.6, N 8B. — P. 116-124.

125. Han, S. Security of a key agreement protocol based on chaotic maps / S. Han. — Chaos, Solitons and Fractals. — 2008. — N 38. P. 794-768.

126. Li C. Cryptanalysis of a data security protection scheme for VoIP / C. Li, S. Li, D. Zhang, G. Chen // IEEE Proceedings -Vision, Image & Signal Processing. — 2006. — Vol. 153, N. 1. — P. 1-10.

127. Аграновский, А.В. Практическая криптография: алгоритмы и их программирование/ А.В. Аграновский, Р.А. Хади – М.:СОЛОН-Пресс, 2002. 256 с.

128. Alvarez, G. Cryptanalyzing a discrete-time chaos synchronization secure communication system / G. Alvarez, F. Montoya, M. Romera, G. Pastor // Chaos, Solitons and Fractals. — 2004 . — № 1. — P. 689—694.

129. Wang, X. Error function attack of chaos synchronization based encryption schemes / X.Wang, M. Zhan, C.-H. Lai, H. Gang // Chaos, Solitons and Fractals. — 2004. — Vol. 14, № 1. — P.128—136.

128. Rhouma, R. On the security of a spatiotemporal chaotic cryptosystem / R. Rhouma, B. Safya. Chaos — 2007. — N 17. — PP. 033117-1/033117/5.

131. Alvarez, G. Breaking projective chaos synchronization secure communication using filtering and generalized synchronization / G. Alvarez, S. Li, F. Montoya, G. Pastor, M. Romera // Chaos, Solitons and Fractals. — 2005. N 24. — P. 775-783.

132. Parker, A. T. Reconstructing the keystream from a chaotic encryption scheme / A. T. Parker, K. M. Short // IEEE Trans. on Circ. and Syst. — 2001. — Vol. 48, N 5. — P. 624-630.

133. Huang, F. Cryptosystem using chaotic keys // F. Huang, Zh. Guan // Chaos, Solitons and Fractals. — 2005. — N 23. — P. 851-855.

134. Li, C. Cryptanalysis of two chaotic encryption schemes based on circular bit shift and XOR operations / C. Li, S. Li, G. Alvarez, G. Chen, K.Lo // Physics Letters A. — 2007. — Vol. 369, N. 1-2. — P. 23-30.

135. Pat. №: 0,050,614 A1 USA, Int. cl. H04L 9/00. Robust hyper-chaotic encryption-decryption system and method for digital secure-communication / W. W. Lin, C.H. Li; Appl. N 11/503,276, filed Aug.14.2006; Pub. date Mar.01.2007.

136. Shannon, C. E. Communication Theory of Secrecy Systems / C.E. Shannon // Bell Systems Technical Journal. — 1949. — Vol. 28. — P. 656—715.

137. Feistel, H. Cryptography and Computer Privacy / Feistel H. // Scientific American. — 1973. — Vol. 228. — P. 15—23.

138. Alvarez G. Some basic cryptographic requirements for chaos-based cryptosystems / G. Alvarez, S. Li // International Journal of Bifurcation and Chaos. — 2006. — Vol. 16, N. 8. — P. 2129-2151.

139. Pat. № 6,078,665 USA, H04L 9/28. Electronic Encryption device and method / Anderson R., Schultz G. R., Heptig J. P.; assigne Intelligent Security Systems Inc. — Appl. №.08/954.795; filed Oct.21.1997; Pub. date Jun.20.2000.

140. Mitchell, D. Nonlinear Key Generators / D. Mitchell // Cryptologia. — 1990. — Vol. 14. — P. 350-354.

141. Li, S. On the dynamical degradation of digital piecewise linear chaotic maps / S. Li, G. Chen, X. Mou // Int. J. of Bifurcation and Chaos. – 2005. – N 10. – PP. 3119-3151.

142. Oliveira, P.L. Cryptography with chaotic mixing / P.L. Oliveira, M. Sobbotka. — Chaos, Solitons and Fractals. — 2008. — N 35. — P. 466-471.

143. Kocarev, L. Public-key encryption with chaos / L. Kocarev, M. Sterjev // Chaos. – 2004. – Vol. 14. – P. 1078-1082.

144. Pat. № 7,106,864 B2 USA, Int. cl. H04L 9/00, H04K 1/00, H04L 9/28. Chaos-based data protection using time-discrete dynamical systems / Kocarev L., Jakimoski G., Rizzotto G., Amato P.; Assigne STMicroelectronics S.r.l. – Appl. N 10/319,432; filed Dec.12.2002; Pub. Date Sep. 12.2006.

145. Pat. №: 6,587,563 B1 USA, Int. cl. H04L 9/00. Cryptographic systems using chaotic dynamics / R. E. Crandall; assigne Apple Computer Inc. – Appl. N 08/801,939, filed Feb.15.1997; Pub. date Jul.01.2003.

146. Устюжанін А. Е. Разробка асоціативної пам’яті для систем автономного адаптивного управління на основі систем детермінованого хаосу: автореф. дис. на здобуття наукового ступеня к-та фіз.-мат. наук: спец. 05.13.11 “Математичне і програмне забезпечення ЕОМ, комплексів та КМ” / Устюжанін Андрій Євгенович;

147. Pat. № 7,110,547 B2 USA, Int. cl. H04L 9/00. Method and Apparatus for the compression and decompression of image files using a chaotic systems / Short K. M.; Assigne University of New Hampshire – Appl. N 09/756,814; filed Jan.9.2001; Pub. date Sep. 19.2006.

148. Patent № 2003/0182246A1 USA, G06F 17/60; H04K 1/00; H04N 7/167. Applications of fractal and/or chaotic techniques / Johnson W. N. H., Blackledge J. M., Murray B. L. — Appl. № 10/149256; filed Dec.11.2000 ; Pub. date 25.09.2003.

149. Li, S. Improving Security of a Chaotic Encryption Approach / S. Li, X. Mou, Y. Cai. Physics Letters A. — 2001. — Vol. 290, N 3-4. — P. 127-133.

150. Grzybowski, J.M.V. Synchronization of the unified chaotic system and application in secure communication / J.M.V. Grzybowski, M. Rafikov, J.M. Balthazar // Commun. Nonlinear Sci. Numer. Simulat.— 2009. — Vol. 14. — P. 2793—2806.

151. Pat. № 7,215,772 B2 USA, Int. Cl. G06F 11/30. Method and apparatus for remote digital key generation / K. M. Short; Assigne Chaoticom Inc. – Appl. N 10/099,812, filed Mar.18.2002; Pub. date May.08.2007.

152. Papadimitrou, S. Secure communication protocols with discrete nonlinear chaotic maps / A. Bezerianos, T. Bountis, G. Pavlides // Journal of Systems Architecture. — 2001. — N 47. — P. 61-72.

153. Wong K. A More Secure Chaotic Cryptographic Scheme based on Dynamic Look-up Table / K. Wong, K. Man, S. Li, X. Liao // Circuits, Systems and Signal Processing. — 2005. — Vol. 24, Issue 5. — P 571-584.

154. Memon, Q. A. Synchronized chaos for network security / Qurban A. Memon // Computer Communications. — 2003. — Vol. 26. — P. 498—505.

155. Lü, H. A new spatiotemporally chaotic cryptosystem and its security and performance analyses / H. Lü, S. Wang, X. Li, G. Tang, J. Kuang, W. Ye, G. Hu // Chaos. — 2004. — V. 14, № 3. — P. 128-629.

156. Escribano, F. J. Evaluation of channel coding and decoding algorithms using discrete chaotic maps / F. J. Escribano, L. Lopez, M. A. F. Sanjuan // Chaos. — 2006. — Vol. 16. — P. 013103-1—013103-12.

157. Schimming, T. K. Coded Modulations Using Chaotic Systems Controlled by Small Pertubations / T. Schimming, K. Oshima, and M. Hasler//In International Conference on Nonlinear Theory and its Applications NOLTA, Xi'an, 2002.

158. Li, S. Analog Chaos-based Secure Communications and Cryptanalysis: A Brief Survey / S. Li , G. Alvarez, Z. Li, W. A. Halang // 3rd International IEEE Scientific Conference on Physics and Control. — Potsdam, Germany. —2007.

159. Xiaogang, Wu. Analyzing and improving a chaotic encryption method / Wu Xiaogang, Hu Hanping, Zhang Baoliang // Chaos, Solitons and Fractals. — 2004. – № 22. – P. 367-373.

160. Castanon M. S. S. A Simple Deterministic Lorenz Chaotic-Based Methodology to cipher and Decipher Information / M. S. S. Castanon, C. A. Ibanez, J. C. M. Garcia // Computation Sistemas. — 2007. — Vol. 11, № 1. — P. 26—38.

161. Prokhorov, M. D. Encryption and decryption of information in chaotic communication systems governed by delay-differential equations / M. D. Prokhorov, V. I. Ponomarenko // Chaos, Solitons and Fractals. — 2008. — Vol. 35. — P. 871—877.

162. Patent № 7076065B2 USA, H04L 9/16. Chaotic privacy system and method / Sheman R. H., Kchao C., Pettilohn B.; Assigne Lockheed Martin Corporation. — filed May. 11.2001; Pub. date JUL.11.2006.

163. Bu S. Improving the security of chaotic encryption by using a simple modulation method / S. Bu, B.-H. Wang // Chaos, Solitons and Fractals. — 2004. — № 19. — P. 919—924.

164. Solak, E. On the security of a class of discrete-time chaotic cryptosystems / E. Solak // Physics Letters A. — 2004. — Vol. 320. — P. 389-395.

165. Brocker, J. Analyzing communication schemes using methods from nonlinear filtering / J. Brocker, U. Parlitz // Chaos. — 2003. — V. 13, № 1. — P. 195—208.

166. Nagarajan, V. Performance enhancement of MC-DS/CDMA system using chaotic spreading sequence / V.Nagarajan, P.Dananjayan // Journal of Theoretical and Applied Information Technology. — 2008. — V. 16, № 11.— P. 995—1001.

167. Шахтарин, Б. И. / Случайные процессы в радиотехнике. М: «Радио и связь». — 2000. – с. 584.

168. Shannon, C. E. A Mathematical Theory of Communication/ C. E. Shannon // The Bell System Technical Journal. – 1948. – V. 27. – P. 623-656.

169. Осипов, М. Л. Сверхширокополосная радиодокация / М. Л. Осипов // Радиотехника. — 1995. — № 3. — С. 3—6.

170. Хармут, Х. Ф. / Несинусоидальные волны в радиолокации и связи. М: «Радио и связь». — 1985. – с. 376.

171. Проксис, Дж. Цифровая связь / Дж. Проксис. – М.: Радио и связь. – 2000. – 800 с.

172. Бондарєв, А. П. Пристрої цифрових систем стільникового зв’язку / А. П. Бондарєв, Б. А. Мандзій, С. В. Давиденко Л.: «Видавництво Львівської Політехніки». — 2011. – 224 с.

173. Корн, Г. Довідник по математике. Для научных работников и инженеров. Определения, теоремы, формулы / Г. Корн, Т. Корн. – М.: Наука. – 1974. – 831 с.

174. Потапов А.А. О фрактальных радиосистемах, дробных операторах, скейлинге, и не только… . – Глава в кн.: Фракталы и дробные операторы (Коллективная монография) / С предисловием акад. Ю.В. Гуляева и чл.-корр. РАН С.А. Никитова / Под ред. А.Х. Гильмутдинова.- Казань: Изд-во "Фән" Академии наук РТ, 2010.- С. 417 – 472.

175. Болотов, В.Н. Выделение фрактальных сигналов в условиях сложной электромагнитной обстановки / В.Н. Болотов, Ю. В. Ткач // Элктромагнитные явления. – Т.3, № 2(10). – 2003. – 211—227 с.

176. Bolotov, V.N. Fractal Communication System / V.N. Bolotov, S. E. Kolesnikov, Yu.V. Tkach, Ya. Yu Tkach, P. V. Khupchenko. – Electromagnetic Phenomena. – 2007. – V. 7, № 1 (18). —p. 174–179.

177. Васюта, К.С. Метод передачи информации, основанный на манипуляции показателя херста фрактального (“цветного”) гауссовского шума / К.С. Васюта // Системи обробки інформації. —2010. — випуск 6 (87). — с. 62—65.

178. Щербінін, С.О. Метод застосування випадкових процесів з α-стабільними розподілами для прихованої передачі цифрової інформації за рахунок варіації властивостей їх розподілів / С.О. Щербінін // Фізико-технологічні проблеми радіотехнічних пристроїв, засобів телекомунікацій, нано- та мікроелектроніки. Матеріали II Міжнародної науково-практичної конференції. – Жовтень, 2012. — С. 87-88.

179. Парфенов, В. И. Анализ систем передачи информации, основаный на манипуляции статистическими характеристиками случайного процесса. – Киев.: Изв. Вузов. Радиотехника. – 2010. — Т. 53, № 3. — С. 42-49.

180. Столингс, В. Криптография и защита сетей/ В. Столингс. – М.: издательский дом «Вильямс». – 2001. – 670 с.

181. Горяинов, В.Т. Статистическая радиотехника: Примеры и задачи: учеб. Пособие / В.Т. Горяинов, А.Г. Журавлев, В.И. Тихонов ; под. общ. ред. В.И. Тихонова ; — 2-е изд., перераб. и доп. — М.: Сов. Радио, 1980. — 544 с.

182. Математичні основи криптографії / Г.В. Кузнецов, В.В. Фомичов, С.О. Сушко, Л.Я. Фомичова . — Д. : НГУ, 2004. – 391 с.

183. Кособуцький, П.С. Статистичні та Монте-Карло алгоритми моделювання випадкових процесів у макро- і мікросистемах у MathCAD / П.С. Кособуцький – Львів: Видавництво Львівської політехніки. – 2014. – 412 с.

184. Дунаев, В.В. HTML, скрипты и стили / В.В. Дунаев – СПб.: БХВ-Петербург. — 2005. – 832 с.

185. Mao, Y. Chaos-based image encryption. Handbook of Computational Geometry for Pattern Recognition, Computer Vision, Neurocomputing and Robotics / Y. Mao, G. Chen. — Springer-Verlag, NY. — 2004, in press.

186. Pareek, N. K. Image encryption using chaotic logistic map / N. K. Pareek, P. Vinod, K. K. Sud // Image and Vision Computing. — 2006. —№ 24. — P. 926-934.

187. Болтенко, В.А. Анализ алгоритмов хаотического шифрования изображений / В. А. Болтенков, Е. С. Никольский // Цифрові технології. — 2010. — № 7. — С. 61-66.

188. Pareek, N. K. Cryptography using multiple one-dimensional chaotic maps / N. K. Pareek, V. Patidar, K. Sud // Commun. Non-linear Sci. Numer. Simul. — 2005. — № 10(7). — P. 715-723.

189. Bo, M. A novel chaotic encryption scheme based on arithmetic coding / L. Xiaofeng, C. Yong // Chaos, Solitons and Fractals. — 2008. — № 38. — PP. 1523-1531.

190. Ватолин, Д. Методы сжатия данных. Устройство архиваторов, сжатие изображений и видео / Д. Ватолин, А. Ратушняк, М. Смирнов, В. Юркин. – М.: ДИАЛОГ-МИФИ. – 2003. – 384 с.

191. Mao Y., A novel fast image encryption scheme based on 3d chaotic baker maps / Yaobin Mao, Guanrong Chen, Shiguo Lian // International Journal of Bifurcation and Chaos. — 2004. — Vol. 14, №. 10. — P. 3613-3624.

192. Chen, G. A symmetric image encryption scheme based on 3D chaotic cat maps / Guanrong Chen, Yaobin Mao, Charles K. Chui // Chaos, Solitons and Fractals. — 2004. — № 21. — PP. 749-761.

193. Jiri, F. Symmetric ciphers based on two-dimensional chaotic maps / F. Jiri // Int. J. Bifurcation and Chaos. — 1998. — Vol. 8, N 6. — P. 1259–1284.

194. Philip Koopman. "32-Bit Cyclic Redundancy Codes for Internet 3Applications". // The International Conference on Dependable Systems and Networks . – 2002. – 459–468 pp.

195. Шахов, В.Г. Моделирование защиты речевой информации с помощью персонального компьютера/ В.Г. Шахов, Нопин С.В. // Омский научный вестник. — 2004. — V. 29, № 4. — С .124–126.

196. Henk, A.S. Fundamentals of cryptology. A Professional Reference and Interactive Tutorial / A. S. Henk. B: «Kluwer academic publisher». – 2000. – p. 480.

197. Mao, Y. A Chip Performing Chaotic Stream Encryption / Y. Mao, W. Liu, Z. Li, P. Li, W. A. Halang // Studies in Computational Intelligence (SCI). — 2007. — Vol. 42. — P. 307—332.

198. Andreyev Yu. V. CDMA communications using maps with stored information / Yu. V. Andreyev, A. S. Dmitriev, D. A. Kuminov, S. O. Starkov // European Conference on Circuit Theory and Design. – Budapest.– 1997. – P. 324–329.

199. Chua, L. Chua’s circuits implementation. Yesterday, today and tonorrow / L. Chua // World Scientific Series on Nonlinear Science Series A. – 2009. – Vol. 65. – P. 244.

200. Chua, L. A gallery of Chua attractors / L. Chua // World Scientific Series on Nonlinear Science Series A. – 2008. – Vol. 61. – P. 600.

201. Wang Fa-Qiang, Hyperchaos evolved from the Liu chaotic system. [Текст] / Wang Fa-Qiang, Liu Chong-Xin // Chinese Physics. 2006. – Vol. 15 No. 5. – P. 963–968.

202. Datasheet on AD633 [Електронний ресурс]: електронний ресурс компанії AD. – Режим доступу до сайту www.analog.com/static/imported-files/data_ sheets/ AD633.pdf.

203. Мун, Ф. Хаотические колебания: вводный курс для научных работников и инженеров. – М.: Мир. – 1990. – 312 с.

204. Orue, A.B. et al. Determination of the parameters for a Lorenz system and application to break the security of two-channel chaotic cryptosystems / A. B.

Orue, V. Fernandez, G. Alvareza, G. Pastora, M. Romera, Shujun Li, F. Montoya // Physics Letters A. — 2008. — N 372. — PP. 5588–5592.

205. Дмитриев, А.С. Структура периодических орбит хаотической автоколебательной системы, описываемой разностными уравнениями 2-го порядка / А.С. Дмитриев, А.И. Панас, С.О. Стаков // Радиетехника и электоника. — 1994. — Т. 39, № 9. — С. 1392-1401.

206. Радзімовський Б. К. Синтез телекомунікаційних сигналів на основі хаотичних коливань : автореф. дис. ... канд. техн. наук : 05.12.13 / Б. К. Радзімовський; Одес. нац. акад. зв'язку ім. О.С. Попова. - Одеса, 2014. - 20 с. - укр.

207. Фракталы в физике / Под. ред. Я. Г. Синая и И.М. Халатникова. – М.: Мир. – 1988.

208. Климаш, М.М. Модель забезпечення параметрів якості обслуговування системи розподілу мультисервісного трафіку/ М.М. Климаш, О.А. Лаврів, Б.А. Бугиль, Р.І. Бак // Вісник Національного університету «Львівська політехніка». – 2011. – № 705. – С. 138-145.

209. Mandelbrot, B.B. Computer experiments with fractional Gaussian noises. Part 1. Averages and variances / B.B. Mandelbrot, J. R. Wallis // Water Resours. Res. — 1969. — Vol. 5. — P. 228—241.

210. Mandelbrot, B.B. Computer experiments with fractional Gaussian noises. Part 1. Averages and variances / B.B. Mandelbrot, J. R. Wallis // Water Resours. Res. — 1969. — Vol. 5. — P. 228—241.

211. Mandelbrot, B.B. Fractls: Form, Chance, and Dimension / B.B. Mandeldrot. San-Francisco, 1980.

212. Леви, П. Стохастические процессы и броуновское движение: пер. с фр. — P.: Editions Jacques ; M.: «Наука», 1972. — 275с.

213. Сергиенко, А.Б. Цифровая обработка сигналов / А. Б. Сергиенко — СПб.: Питер. — 2002. — 608 с.

214. Лосев, Ю.И. Методы и модели обмена информацией в распрределенных адаптивных распределительных сетях с временной

параметризацией параллельных процессов / Ю. И. Лосев, С.И. Шматков, К.М. Руккас // монография. – Х.: ХНУ имени В.Н. Каразина, 2011. – 204 с.

215. Кельтон В., Лоу А. Имитационное моделирование. Классика CS.3-е изд.-СПб.:Питер;Киев:Издательская группа BHV, 2004.-847 с.

216. Новікова, О.Б. Фрактальний сплайн-модель широкосмугового сигналу / О.Б. Новікова // Видавництво НУ «ЛП». – 2012. – № 738. – С. 28 – 33.

217. Лазоренко, О.В., Потапов А.А., Черногор Л. Ф. Фрактальные сверхширокополосные сигналы / Глава в кн.: Струков А. В., Потапов А. А., Черногор Л. Ф. и др. Информационная безопасность: методы шифрования / С предисловием акад. Н. А. Кузнецова // Под ред. Е.М. Сухарева. Кн. 7.— М.: Радиотехника. — 2011. – С. 151 – 187.

218. Сумик, М.М. Теорія сигналів / М.М. Сумик, І.Н. Прудиус, Р.М. Сумик. – Львів: Видавництво «Бескид Біт». – 2008. – 232 с.

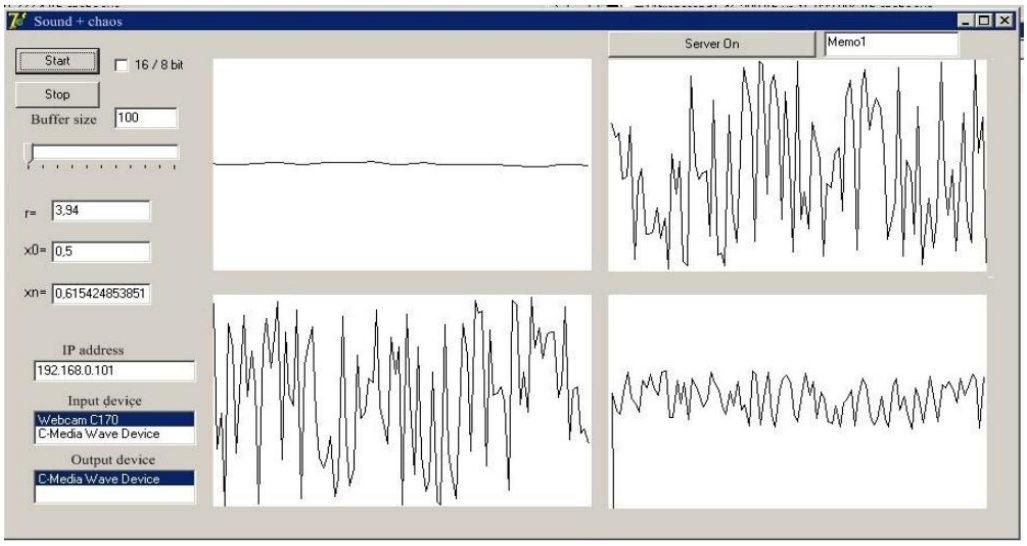
219. Харкевич А.А. Спектры и анализ.– М.: Государственное издание физико-математической литературы.– 1962.– С. 23.

220. Угрюмов Е. П. Цифровая схемотехника. СПб, БХВ-Петербург, 2004.

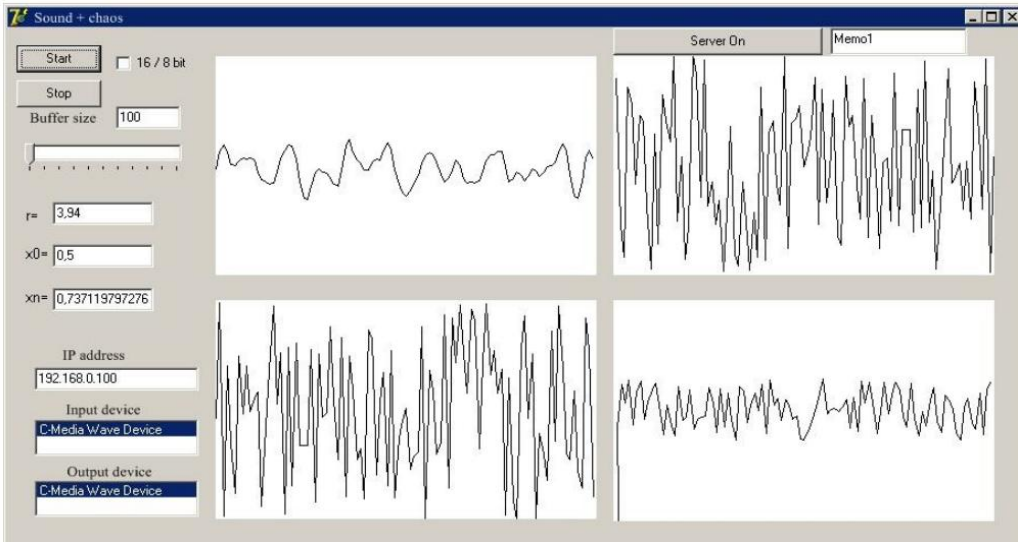
221. Datasheet on PIC18F2550 [Електронний ресурс]: електронний ресурс компанії Microchip. – Режим доступу до сайту www.microchip.com/downloads/en/devicedoc/30292.pdf.

ДОДАТКИ

ДОДАТОК А: Програмні вікна системи обміну аналоговим звуковим сигналом шифрованими ПВП генерованими за логістичним відображенням

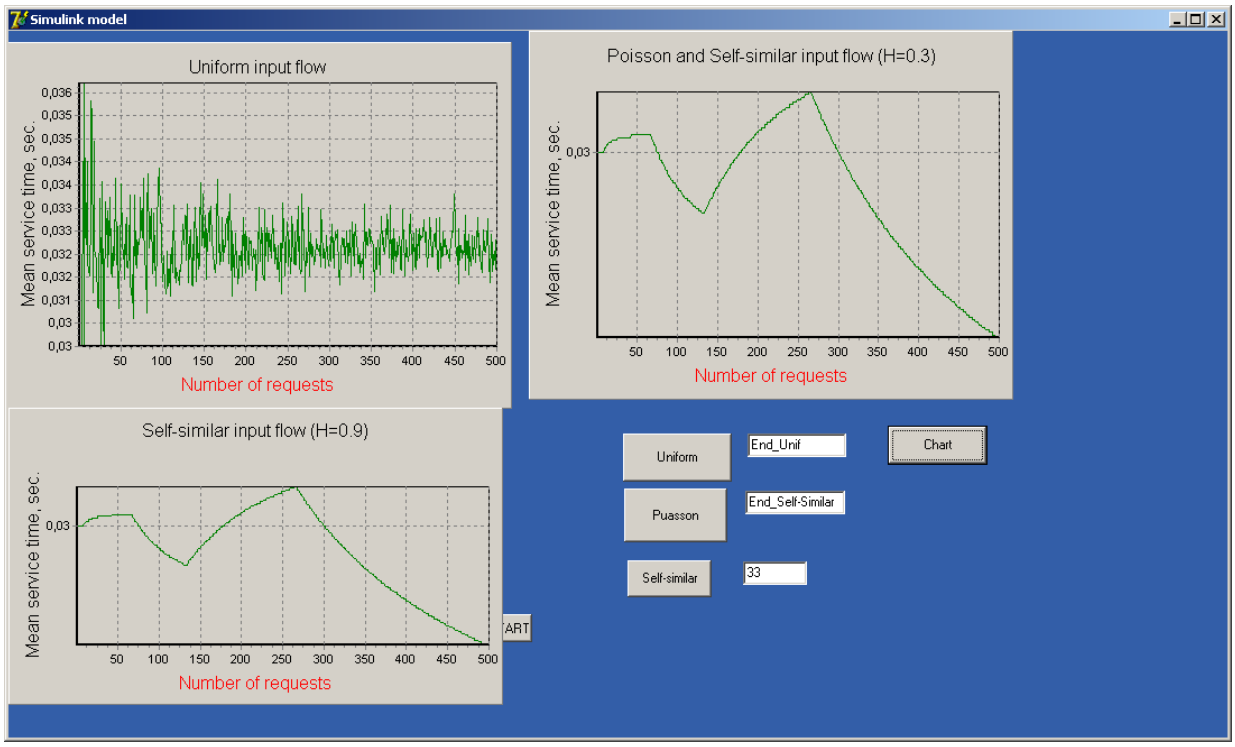


а)

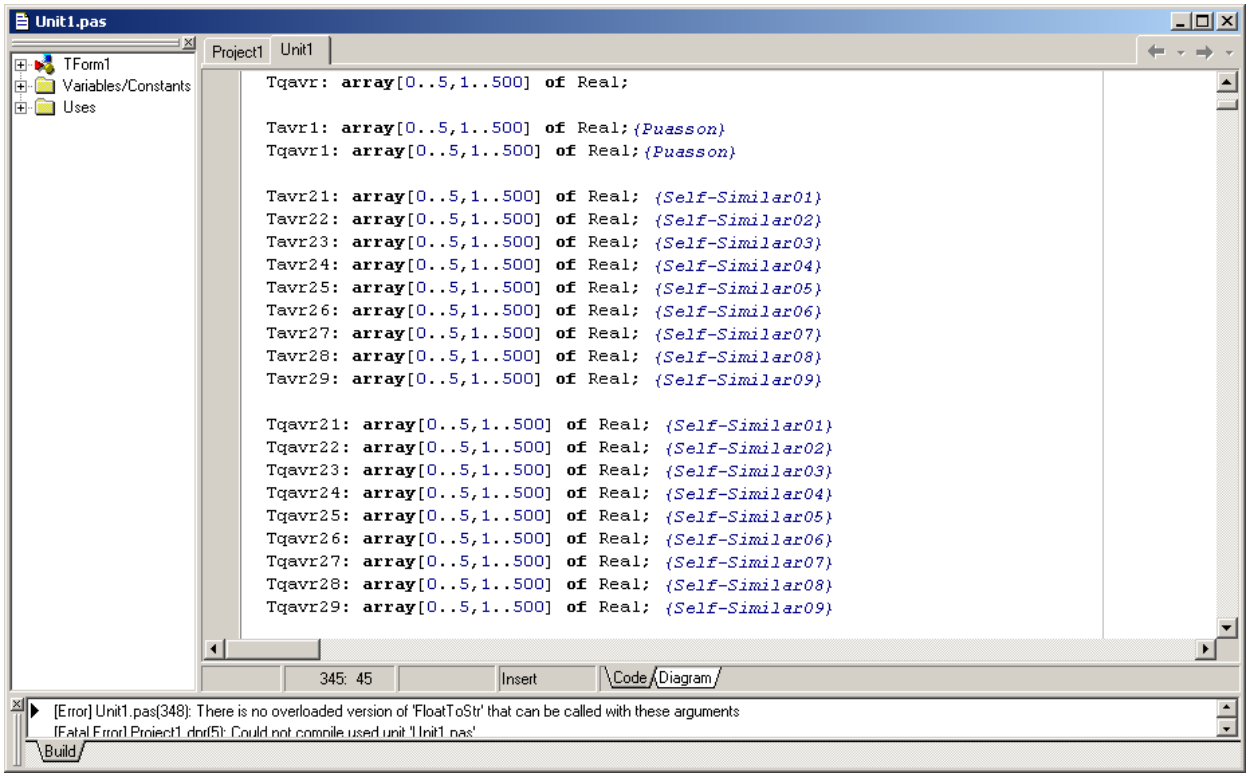


б)

ДОДАТОК Б: Програма моделювання проходження трафіку методом СМО



Головне вікно програми



Приклад фрагменту коду у середовищі Delphy

ДОДАТОК В: Акти впровадження виконаних робіт

КОДЕК - ФАКТОР

Украина г.Днепропетровск наб. Ленина, д. 29а
тел. (0562) 41-64-93 факс (0562) 41-64-23

«ЗАТВЕРДЖУЮ»
Директор Науково-
Технічного Центра ТОВ
«КОДЕК-фАКТОР ЛТД»
_____ Боневич Я. С.
«12» 08 2015 р.

АКТ № 257/08.2015

цим Актом засвідчую, що актуальність та достовірність отриманих автором результатів підтверджена результатами вимірювання інтенсивності трафіку та виявлення годин, на які припадають пікові навантаження.

Результати дисертаційного дослідження доцента кафедри РТ та ІБ Чернівецького Національного Університету імені Ю. Федьковича Політанського Руслана Леонідовича використані на ТОВ «КОДЕК-ФАКТОР ЛТД» використані співробітниками Науково-Технічного Центра.

Голова комісії: _____ Боневич Я. В.

Члени комісії: _____ Потапчук Г.Ю.

_____ Сомко П.В.

«EPHARMONE»

99007, м. Севастополь, вул. Котовського, 47: (0692) 565142: (0692) 420811Факс:(0692) 460471

А К Т

об использовании результатов кандидатской диссертационной работы доцента кафедры РТ и ИБ Политанського Руслана Леонидовича

Комиссия в составе:
Председатель Осипова Р. М.,
члены комиссии: Божко А. Ф., Маринич К. Л..

Составили настоящий акт о том, что результаты исследований прохождения трафика через систему с тройной маршрутизацией с использованием модели систем массового обслуживания интересны с точки зрения возможности анализа построения сети и её оптимизации. Указанные результаты дают возможности прогнозировать интенсивность трафика, проходящего через телекоммуникационные сети предприятия и в случае необходимости подключать к сети дополнительные узлы, уменьшит нагрузку и повысит качество обслуживания абонентов.

Актуальность и достоверность полученных автором результатов подтверждена результатами измерения интенсивности трафика и выявления часов, на которые приходятся пиковые нагрузки.

Вывод: *Использование указанных результатов позволяет: повысить качество предоставляемых услуг.*

Председатель комиссии:
_____ **Осипов Р. М.**

Члены комиссии:
_____ **Божко А. Ф.**

_____ **Маринич К. Л.**

М. П.

"УТВЕРЖДАЮ"
Директор Севастопольского государственого
приборостроительного завод «Парус»
Бекчинтаев Г. Д.
"23" 07 2015 г.

А К Т

внедрение результатов диссертации доцента кафедры РТ и ИБ Черновецького Национального Университета имени Ю. Федьковича Политанського Руслана Леонидовича на СГПЗ «Парус»

Члены комисии в составе; директора СГПЗ «Парус» Бекчинтаева Т.Н. директора МП «КЕМПИНГ» Антонов В. С., заступника директора Васюгина В. П., начальника измерительной лабораторий составили этот акт о том что, результаты роботы Политанського Р. Л., в область исследований прохождения трафика через систему с тройной маршрутизацией с использованием модели систем массового обслуживания интересны с точки зрения возможности анализа построения сети и её оптимизации Предоставляет возможности прогнозировать интенсивность трафика, проходящего через телекоммуникационные сети предприятия и в случае необходимости подключать к сети дополнительные узлы, уменьшит нагрузку и повысит качество обслуживания абонентов.

Актуальность и достоверность полученных автором результатов подтверждена результатами измерения интенсивности трафика и выявления часов, на которые приходятся пиковые загрузки

Достоверность полученных результатов подтверждаю.

Директор МП «КЕМПИНГ» **Антонов В. С.**

ПАТ «ТК Энергия»

м. Харків, 05624, вул.. Фрунзе, 36. Тел..(067) 651-25-68: (050) 462-58-92

«ЗАТВЕРДЖУЮ»
Директор ПАТ«ТК Энергия»
_____ І. В. Тягло
«___» _____20__р.

АКТ
про впровадження результатів дисертаційної роботи
Політанського Руслана Леонідовича

Члени комісії у складі головного інженера ПАТ «ТК Энергия» Кудрявцев С. К., завідувача електронної лабораторії, Бащенко А. О., провідного інженера Бесенкова В. П., склали цей акт про те, що результати дисертаційної роботи Политанського Р. Л..

Використані на підприємстві ПАТ «ТУ Энергия» для забезпечення дослідження проходження трафіку із самоподібним розподілом через систему з потрійною маршрутизацією із використанням моделі систем масового обслуговування та аналізу побудови мережі та її оптимізації.

Вказані результати дають можливості прогнозувати інтенсивність трафіку, що проходить через телекомунікаційні мережі підприємства та у випадку необхідності підтримикати до мережі додаткові вузли, що зменшить навантаження та підвищить якість обслуговування її абонентів.

Голова комісії:

Кудрявцев С. К. _____

Члени комісії:

Бащенко А. О. _____

Бесенкова В. П. _____

Директор ПАТ «ТК Энергия»

_____ І. В. Тягло

HAVEN TRADING CORP. CORPORATE SEAL 1994 LIBERIA

Укртелеком

А к т № 12/594

в п р о в а д ж е н н я р е з у л ь т а т і в д и с е р т а ц і ї

Доцента кафедри РТ та ІБ
Чернівецького Національного
Університету імені Ю. Федьковича
Політанського Руслана Леонідовича
на Чернівецької філії ПАТ «UTEL»

Актуальними результатами, що були отримані автором, є дослідження процесів синхронізації псевдовипадковими послідовностями, що генеровані пороговим методом і довжини яких є характерними для криптографії: 64, 128, 256, 512 та 1024 біти. Такий метод синхронізації впроваджений у технологіях стільникового зв'язку третього покоління, що набуває поширення в Україні згідно проведених тендерів.

Актуальність та достовірність отриманих автором результатів підтверджена дає можливість прогнозувати активне впровадження та розвиток зазначених технологій синхронізації у телекомунікаційних мережах, що діють на теренах України або впровадження яких щойно розпочалося.

Директор ЧФ ПАТ «UTEL» **С. Я. Чайка**

Публічне акціонерне товариство «UTEL»
вул. Червоноармійська, 7, м. Чернівці, 58002, Україна
р/р 260087370 в ПАТ «Райффайзен Банк Аваль» м. Чернівці, МФО 356464, код ЄДРПОУ 22838086,
індивідуальний податковий номер 215607626656, свідоцтво № 35478958 видане 19.04.2002 р. СДПІ у
м. Києві по роботі з ВПП

Utel

ПАТ "Укртелеком"
Вх. № 03-136
Від "___" _____ 2009 р.

Публічне акціонерне товариство «Укртелеком»
Чернівецька філія

укртелеком
краще починається сьогодні

Акт

впровадження результатів дисертації доцента кафедри РТ та ІБ Чернівецького Національного Університету імені Ю. Федьковича Політанського Руслана Леонідовича на Чернівецької філії ПАТ «Укртелеком»

Результати досліджень проходження трафіку із самоподібним розподілом через систему з потрійною маршрутизацією із використанням моделі систем масового обслуговування є цікавими з точку зору можливості аналізу побудови мережі та її оптимізації. Вказані результати дають можливості прогнозувати інтенсивність трафіку, що проходить через телекомунікаційні мережі підприємства та у випадку необхідності підмикати до мережі додаткові вузли, що зменшить навантаження та підвищить якість обслуговування її абонентів.

Актуальність та достовірність отриманих автором результатів підтверджена результатами вимірювання інтенсивності трафіку та виявлення годин, на які припадають пікові навантаження.

Укртелеком Центр телекомунікаційних Ідентифікаційний код 22838086

Директор ЧФ ПАТ «Укртелеком» **П. Ф. Робулець**

Головний інженер ЧФ ПАТ «Укртелеком» **О. Г. Даналакій**

ЗАТВЕРДЖЕНО
Проректор з наукової роботи
Чернівецького Національного
Університету
імені Ю. Федьковича
П.М. Фочук
«____» _____2015 р.

АКТ

Впровадження результатів науково-дослідної роботи
Політанського Руслана Леонідовича
«Розробка завадозахищених систем передавання інформації на основі псевдовипадкових коливань та фрактальних сигналів»

Комісія у складі:

Голова: Директор Інституту фізико-технічних та комп'ютерних наук, проф., д.ф.-м.н. Ангельський Олег В'ячеславович
(посада, прізвище, ім'я, по-батькові)

Члени комісії: Доцент кафедри радіотехніки та інформаційної безпеки, кт.н. Шпатар Петро Михайлович
(посада, прізвище, ім'я, по-батькові)

Асистент кафедри радіотехніки та інформаційної безпеки, к.т.н. Саміла Андрій Петрович
(посада, прізвище, ім'я, по-батькові)

Асистент кафедри радіотехніки та інформаційної безпеки, к.т.н. Еліяшів Олег Миронович
(посада, прізвище, ім'я, по-батькові)

Комісія встановила, що запатентована та розроблена у співавторстві система вивчення згорткового кодування впроваджена у навчальному курсі «Теорія інформації та кодування», що викладається студентам 3-го курсу денної форми навчання за напрямом підготовки 6.170102 «Системи технічного захисту інформації».

Голова комісії: О.В. Ангельський

Члени комісії: П.М. Шпатар

А.П. Саміла

О.М. Еліяшів

«19» жовтня 2015 р.