МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ЛЬВІВСЬКА ПОЛІТЕХНІКА»

Політанський Руслан Леонідович

УДК 621.391, 621.391.8

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

05.12.02 – телекомунікаційні системи та мережі

Автореферат дисертації на здобуття наукового ступеня
доктора технічних наук

Львів − 2016

Дисертацією є рукопис
Робота виконана у Національному університеті «Львівська політехніка» Міністерства освіти і науки України

Науковий консультант - доктор технічних наук, професор
Бобало Юрій Ярославович,
Національний університет «Львівська політехніка», ректор

Офіційні опоненти: доктор технічних наук, професор,
Лісовий Іван Павлович,
Одеська національна академія зв'язку ім. О.С.Попова Міністерства освіти і науки України, м. Одеса, професор кафедри телекомунікаційних систем

доктор технічних наук, професор,
Бараннік Володимир Вікторович,
Харківський університет Повітряних Сил імені Івана Кожедуба Міністерства оборони України, м. Харків, провідний науковий співробітник Наукового центру Повітряних Сил

доктор технічних наук, професор,
Сундучков Костянтин Станіславович,
Національний технічний університет України «Київський політехнічний інститут» Міністерства освіти і науки України, м. Київ, професор кафедри інформаційно-телекомунікаційних мереж

Захист відбудеться "5" лютого 2016 року о 10 годині на засіданні спеціалізованої вченої ради Д 35.052.10 у Національному університеті «Львівська політехніка» за адресою: 79013, м. Львів, вул. Степана Бандери, 12, ауд. 226.

З дисертацією можна ознайомитись у науковій бібліотеці Національного університету «Львівська політехніка» за адресою: 79013, м. Львів, вул. Професорська, 1.

Автореферат розісланий "15" грудня 2015 р.

Учений секретар
спеціалізованої вченої ради А.П. Бондарєв

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

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 держбюджетних науково-дослідних тем «Дослідження та розроблення телекомунікаційних мережних систем для застосувань телематики та телеметрії» (ДБ/КОМ), (2011-2012 рр.), № держреєстрації 0111U001223, а також «Фізико-технологічні проблеми радіотехнічних пристроїв та засобів телекомунікацій та інформаційних технологій», (2011-2012 рр.), № держреєстрації 0111U000183, у яких 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 характеризується 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 близьке до одиниці значення коефіцієнту завадостійкості, 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 може бути використаний 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, 25 – тез та матеріалів 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 Международний 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 негаусівських 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 8 сторінках, 161 рисунок, 10 таблиць, загальний обсяг роботи становить 300 сторінок.

ОСНОВНИЙ ЗМІСТ РОБОТИ

У **вступі** наведена загальна характеристика роботи, обґрунтовано актуальність теми досліджень, сформульовані мета та задачі досліджень, розкритий зв'язок роботи з науковими планами та програмами, вказана новизна та практична цінність отриманих результатів, відзначений особистий внесок автора, наведені дані про апробацію та практичне впровадження, публікації та структуру роботи.

У **першому** розділі – **«Сучасний стан проблеми генерування та застосування хаотичних широкосмугових сигналів у телекомунікаційних системах»** – на основі опрацьованих літературних джерел проаналізовані теоретичні основи використання теорії хаосу у передаванні інформації та методи формування сигналів на основі хаотичних коливань, генерованих системами з дискретними та неперервними функціями відображення, розглянуті тенденції розвитку систем передавання інформації на основі псевдовипадкових коливань та фрактальних сигналів.

Проведено аналіз праць вітчизняних та закордонних вчених присвячених дослідженню процесів у системах, що використовують псевдовипадкові та фрактальні (самоподібні) сигнали для кодування цифрової інформації; розглянуті методи їх формування, зроблено висновок щодо доцільності використання таких сигналів з метою забезпечення оптимального співвідношення сигнал/шум.

Значна кількість праць присвячених використанню шумоподібних сигналів в інфокомунікаційних системах дає можливість зробити висновок щодо доцільності проведення досліджень методів синтезу нових сигналів, складних конструкцій, зокрема псевдохаотичних та фрактальних широкосмугових сигналів.

Системи з хаотичною динамікою детально вивчаються протягом останніх декількох десятків років вченими усього світу. До найбільш вагомих внесків у сучасну теорію хаотичних систем слід віднести досягнення як вітчизняних (Шарковський О. М., Кириченко О.О., Захарченко М.В., Матвійчук Я.М.) наукових шкіл, так і зарубіжних, які представлені вченими Навальської Дослідницької Лабораторії (Кароль, Пекора), Варшавського Технологічного Університету (Збігнев Коштульський), Каліфорнійський університет (Леон Чуа). Сучасні теоретичні дослідження опираються на математичний апарат, який був розвинений раніше: теорія звичайних диференційних рівнянь, теорія стійкості по Ляпунову, теорія Марківських ланцюжків, ентропія інформаційних систем, які є складовими телекомунікаційної системи, теорія дробового диференціювання та інтегрування (показано, що існує нижня границя систем із дробовими розмірностями, починаючи з якої у динамічній системі є можливим генерування хаотичних коливань, сьогоднішні наукові погляди дають можливість вважати, що така границя становить 1.5). Алгоритми, які розроблені на основі математичного апарату теорії хаотичних систем, є досить складними, але сучасний стан обчислювальної техніки уможливлює їх реалізацію.

Враховуючи сучасний стан розвитку методів шифрування, кодування та

передавання інформації в телекомунікаційних системах окреслена низка наукових завдань, що вирішувались автором дисертаційної роботи:

− перенесення математичних умов виникнення псевдовипадкових (хаотичних) коливань на співвідношення для параметрів електронних схем генераторів хаотичних коливань;

− пошук нових класів сигналів, що забезпечують завадостійку роботу телекомунікаційних систем (зокрема широкосмугових фрактальних сигналів) з метою завадостійкого передавання інформації;

− дослідження процесів встановлення синхронізації генераторів хаотичних коливань приймальної та передавальної сторін телекомунікаційної системи;

− дослідження взаємодії (кореляції) між хаотичним переносником та інформаційним сигналом (модуляція хаотичного переносника інформаційним сигналом);

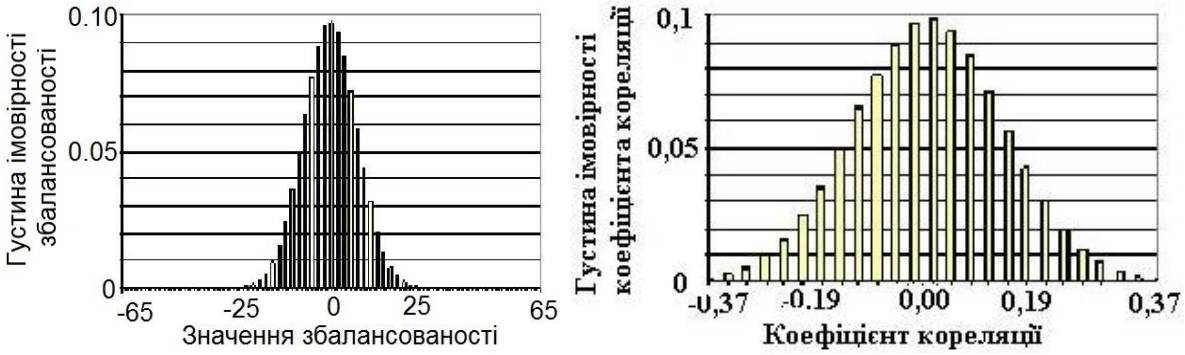
− дослідження методів шифрування інформаційних повідомлень псевдовипадковими бінарними послідовностями.

У **другому** розділі – «**Моделі цифрових систем зв'язку з шифруванням інформації псевдовипадковими бінарними послідовностями, формованими хаотичними коливаннями з дискретною функцією відображення**» – 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, а також вплив канального кодування на тривалість процесу синхронізації генераторів хаотичних коливань передавальної та приймальної сторін системи передавання інформації.

На рис.1 приведені статистично усереднені на множині початкових значень $x_0 \in [0;1]$ розподіли густини імовірності збалансованості та корельованості ПВП, що генеровані пороговим методом (1) на основі логістичного відображення (2):

$$b_n = \begin{cases} 0, \text{ для } x_n \in [0;0,5] \\ 1, \text{ для } x_n \in (0,5;1] \end{cases} \qquad (1); \qquad x_n = 4 \cdot x_{n-1} \cdot (1 - x_{n-1}) \qquad (2).$$

Генеровані за вищеприведеним алгоритмом послідовності були використані для формування ключів при розробленні моделі шифрованого чату для захищеного обміну текстовими повідомленнями із клієнт-серверною архітектурою (рис.2), що базується на технології Phyton з використанням блокового шифрування за алгоритм CRC-32 згідно критеріям IEEE 802.3 (рис.2).



а) б)

Рис.1. Розподіл густини ймовірності усереднених на множині початкових значень збалансованості (а) і коефіцієнту кореляції (б) ПВП, генерованих за логістичним відображенням

Закодована згідно стандарту UTF-8 інформація зберігається у символьному масиві зі спеціальним символом його розбивки на блоки. Це уможливлює конвертацію даних у CSV-файл та обмін інформацією з системами з іншим програмним забезпеченням. Адресація даних здійснюється TCP/IP протоколюванням із використанням статичних IP-адрес, що записані та розпізнаються на серверній частині програмного забезпечення, яка крім цього забезпечує збереження ключів та переданих повідомлень (рис.2).

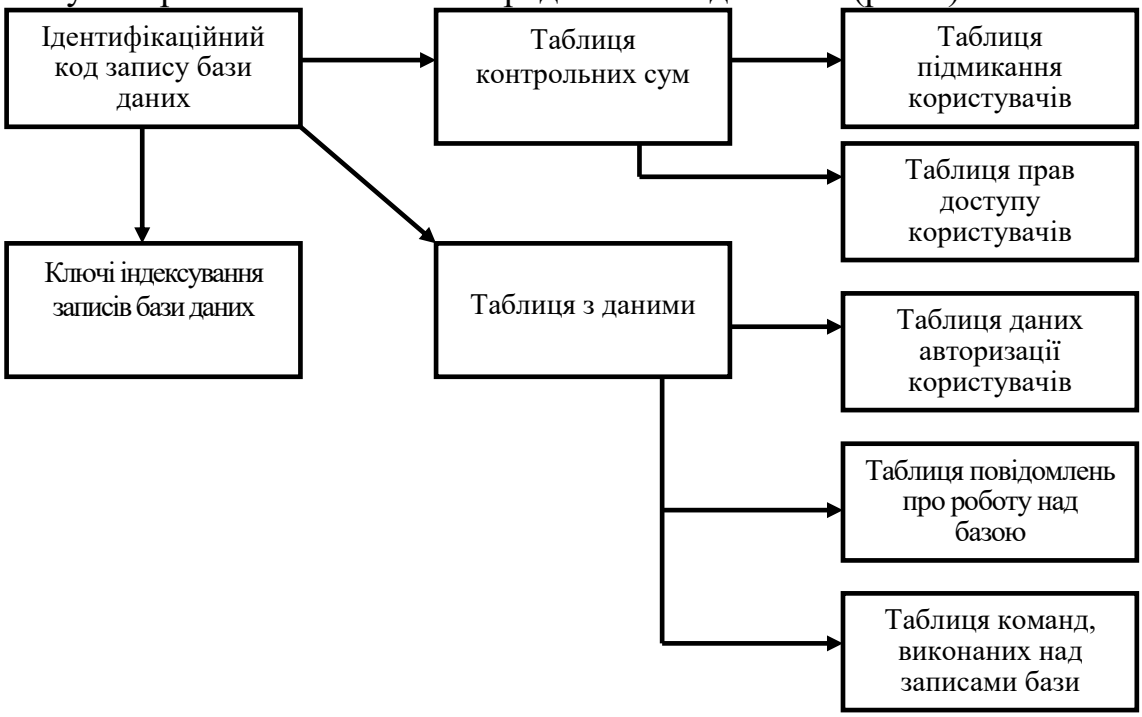


Рис.2. Структура багатокористувацької системи передавання даних

Встановлення клієнта та забезпечення синхронізації між клієнтською та серверною частинами здійснюється шляхом обчислення та перевірки за алгоритмом CRC-32 контрольних сум після виконання заданого числа ітераційних циклів і зміни початкових значень динамічної змінної (рис.3). Кількість користувачів у дослідженій моделі забезпечувалась представленням початкових значень хаотичного коливання та параметру системи генерування

п’ятьма знаками після коми і становила 20 клієнтів і може бути збільшена шляхом підвищення розрядності, але при цьому швидкодія обміну текстовими повідомленнями зменшується.

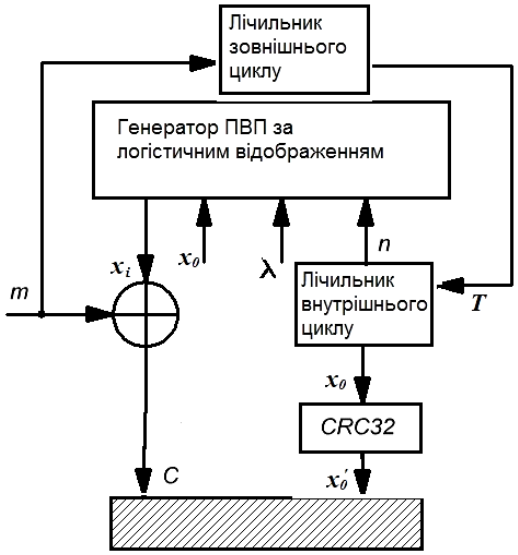


Рис.3. Алгоритм блокового шифрування та синхронізації у багатоканальних системах передавання інформації, де m – інформаційне повідомлення у двійковому форматі, x_0, λ – початкове значення хаотичних коливань та параметр логістичного відображення, n – задана кількість ітерацій, x_i – потокове значення хаотичного коливання, що використовується у процесі потокового шифрування двійкового інформаційного повідомлення, C – зашифроване повідомлення, $x_{0'}$ – змінене за алгоритмом CRC-32 початкове значення логістичного відображення, T – період синхронізації)

Дослідження впливу канального кодування на тривалість встановлення процесу синхронізації між приймальною та передавальною сторонами системи передавання інформації здійснювалось у припущенні, що довжина послідовності синхронізації повинна бути збільшена на кількість інвертованих бітів під дією завад у каналі зв’язку.

Середня кількість інвертованих біт у послідовності синхронізації довжиною N біт дорівнюватиме:

$$n_i = N \cdot p_C \tag{3},$$

де N – довжина послідовності, p_c – ймовірність помилки канального біта, що для бінарної фазової модуляції визначається за формулою:

$$p_C = Q\left(\sqrt{2 \cdot \frac{E_b}{N_0}}\right) \tag{4},$$

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

Довжина збільшеної послідовності синхронізації на кількість інвертованих бітів визначатиметься виразом:

$$\tilde{N} = N \cdot (1 + p_C) \tag{5}.$$

У випадку використання канального кодування інформаційного повідомлення лінійними блоковими кодами (n,k) ймовірність помилки канального біту дорівнюватиме:

$$p_C = Q\left(\sqrt{2 \cdot \frac{k}{n} \cdot \frac{E_c}{N_0}}\right) \tag{6}.$$

Ймовірність помилки у декодованому кодовому слові становитиме:

$$p_B = \frac{1}{n} \cdot \sum_{j=t+1}^{n} C_n^j \cdot p_c^j \cdot (1 - p_c)^{n-j} \quad (7),$$

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

Таким чином, довжина N_C закодованої послідовності синхронізації лінійним блоковим кодером (n,k) становитиме:

$$N_C = N \cdot \frac{n}{k} \quad (8),$$

а середня кількість інвертованих бітів у ній:

$$n_{ic} = N_C \cdot p_B = N \cdot \frac{n}{k} \cdot p_B \quad (9).$$

Дослідження впливу шумів каналу на час синхронізації здійснювалося при значенні швидкості передавання бітів:

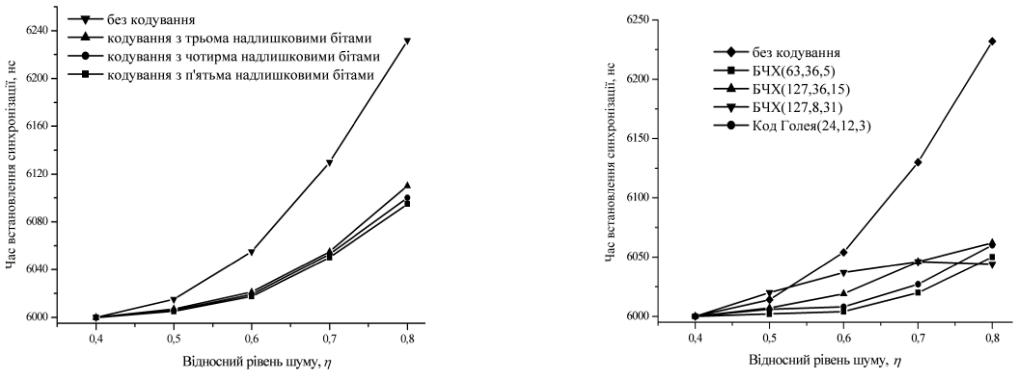
$$R = \frac{N}{T} = 10 \text{ Мбіт/с} \quad (10)$$

Таким чином тривалість передавання послідовностей синхронізації без кодування та з завадостійким кодуванням відповідно дорівнюватиме:

$$T_{on} = \frac{\tilde{N}}{R} = N \cdot \frac{1+p}{R} \quad (11),$$

$$T_n = \frac{\tilde{N}_c}{R_c} = \frac{N \cdot \frac{n}{k} \cdot (1 + p_B)}{R \cdot \frac{n}{k}} = N \cdot \frac{1 + p_B}{R} \quad (12).$$

На рис. 4 приведені результати досліджень впливу канального кодування на тривалість процесу встановлення синхронізації.



а) б)

Рис.4. Залежність тривалості процесу встановлення синхронізації між приймальною та передавальною сторонами СПІ від рівня шуму в каналі при використанні кодів Хемінга (а) та Боуза-Чоудхурі-Хоквінгема (БЧХ) (б). Остання цифра означає кількість помилкових бітів у блоці, що виправляються кодером

Із отриманих залежностей часу встановлення синхронізації від відносного рівня шуму в каналі випливає, що використання кодів БЧХ зменшує тривалість процесу на 200 нс.

Дискретні відображення, що генерують хаос, можуть використовуватись у криптографії. Дослідження методів шифрування зображень показують, що специфіка поставлених задач потребує використання нелінійних алгоритмів, один із яких базується на узагальненому відображенні Пекаря, суть якого полягає у перестановці місцями координат пікселів без зміни їх інтенсивності та загальних розмірів зображення. Геометрична інтерпретація класичного двовимірного відображення Пекаря приведена на рис. 5

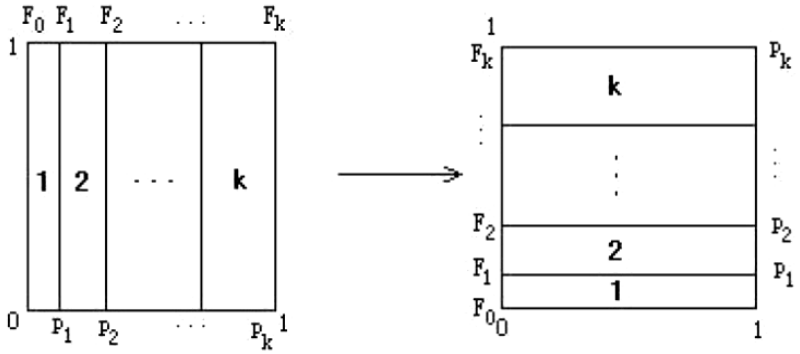


Рис.5. Узагальнене перетворення Пекаря (1, 2, …, k – послідовна нумерація квадратів, що утворюють розбиття квадрата; F_0, F_1, F_2, …, F_k – координати кінців відрізків, що утворюють розбиття одиничної сторони квадрата; p_1, p_2, …, p_k – довжини відрізків, що утворюють розбиття одиничної сторони квадрата)

Одиничний квадрат поділяється на k вертикальних прямокутників (рис. 5 а): $[F_{i-1};F_i)\times[0,1)$; $i=1,\ldots,k$; $F_i=p_1+p_2+\cdots+p_i$; $F_0=0$; $p_1+p_0+\cdots+p_k=1$, де i – потоковий номер прямокутників, F_{i-1},F_i – координати лівого та правого кінців прямокутника відповідно, p_i – довжина бічної горизонтальної сторони прямокутника. Узагальнене відображення Пекаря розтягує кожен прямокутник у горизонтальному та стискає у вертикальному напрямках з коефіцієнтами $1/p_i$ та p_i відповідно (рис.5 б). Аналітично схема перетворення може бути представлена у наступному вигляді:

$$B(x,y)=[1/p_i\cdot(x-F_i),\ p_i\cdot(y+F_i)],\quad (x,y)\in[F_i,F_i+p_i)\times[0,1) \qquad (13),$$

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

Узагальненням двовимірного відображення є його тривимірний аналог. За результатами досліджень з використанням розробленої програми встановлено, що використання трьохмірного відображення Пекаря, забезпечує збільшення швидкості шифрування біля 15%.

Результати шифрування початкового зображення (рис. 6а) приведені на рис.6 б та рис.6 в. На рис.7 приведені результати шифрування з додатковим використанням дифузії.

а) б) в)

Рис.6. Початкове зображення 480x480 пікселів (а); результат перетворення Пекаря із розділенням початкового зображення на 4 прямокутники (б) та на 50 прямокутників (в).

а) б)

Рис.7. Результат перетворення Пекаря із використанням перетворення дифузії з розділенням початкового зображення на 4 прямокутники (а) та на 50 прямокутників (б)

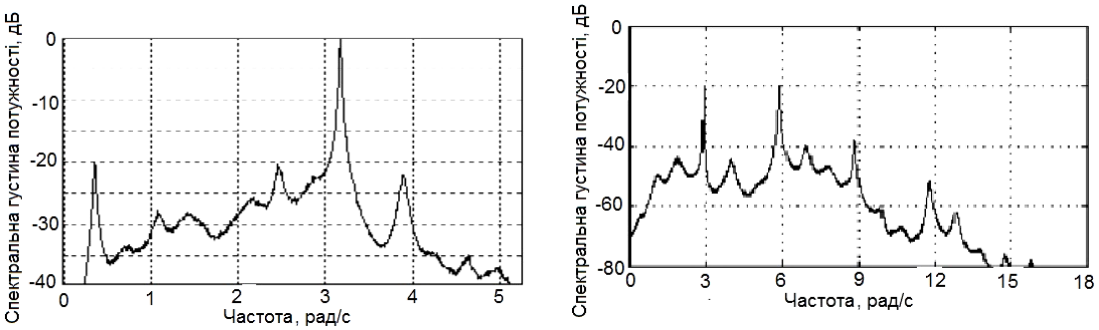
У **третьому** розділі – «**Властивості псевдовипадкових коливань генерованих системами з неперервною функцією відображення та особливості їх синхронізації**» – експериментально досліджені явища синхронізації генераторів хаотичних коливань з неперервною функцією відображення. Визначені області допустимих значень їх параметрів, що забезпечують завадостійкість та криптостійкість систем передавання інформації з використанням хаотичних коливань.

Відмінність спектрів хаотичних коливань, генерованих генератором Чуа та кільцевим генератором (рис.8) обумовлена різними функціями та складністю характеристик їх нелінійних елементів.

Оскільки спектри потужності хаотичних коливань, генерованих генераторами Чуа, мають чіткий максимум, то при дослідженні процесів їх синхронізації може бути використана миттєва різниця фаз, розрахована за формулою:

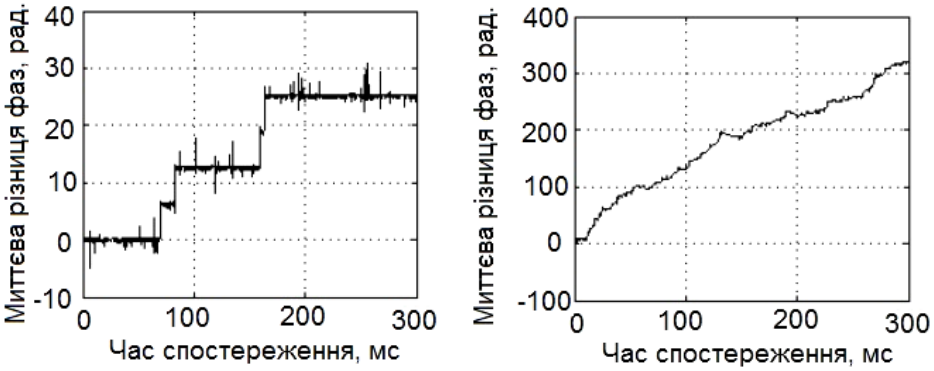
$$\omega(t) = \frac{d\varphi(t)}{dt} \tag{14}$$

Аналіз залежності миттєвої різниці фаз у з'єднаних генераторах Чуа від часу спостереження показує, що при значеннях коефіцієнта зв'язку $e = 6$ та частоти зрізу $u = 10$ (рис.9 а) має місце **on-off** синхронізація. При менших значеннях коефіцієнта зв'язку та частоти зрізу миттєва різниця фаз зростає майже за лінійним законом (рис.9 б), що вказує на відсутність синхронізації.



а) б)

Рис. 8. Нормовані спектри потужності ПВС, генерованих електричним колом Чуа (а) та кільцевим генератором (б)



а) б)

Рис.9. Залежність миттєвої різниці фаз синхронізованих генераторів Чуа від часу спостереження у випадку лаг-синхронізації при значеннях параметрів e=6; u= 10 (а) та у випадку відсутності синхронізації при значеннях параметрів e=1; u=2 (б)

Моделювання синхронізації двох кільцевих автогенераторів також здійснювалось із врахуванням фільтрації в каналі зв’язку. Система рівнянь, що описує ведучий та ведений кільцеві автогенератори у безрозмірних змінних має наступний вигляд:

$$\begin{cases} \dot{x}_1 = \left(M \cdot F\left(z_1\right) - x_1\right) \cdot \beta_1 \\ \dot{y}_1 = 4 \cdot \pi^2 f^2 \cdot \left(x_1 - z_1\right) \\ \dot{z}_1 = y_1 - \alpha_1 \cdot z_1 \\ v = u \cdot \left(x_1 - v\right) \\ \dot{x}_2 = \left(M \cdot F\left(z_2\right) - x_2 \cdot \left(1+e\right) + e \cdot v\right) \cdot \beta_2 \\ \dot{y}_1 = 4 \cdot \pi^2 f^2 \cdot \left(x_2 - z_2\right) \\ \dot{z}_2 = y_2 - \alpha_2 \cdot z_2 \end{cases}, \qquad (15)$$

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 коефіцієнт зв’язку між ведучим та веденим генераторами, u – безрозмірна частота зрізу фільтра.

При значеннях параметрів моделювання α_1=2,1; α_1=2,15; β_1=1,38; β_2=1,39; *M=5* атрактори ведучої та веденої систем у 3-вимірному фазовому просторі співпадають (рис.10).

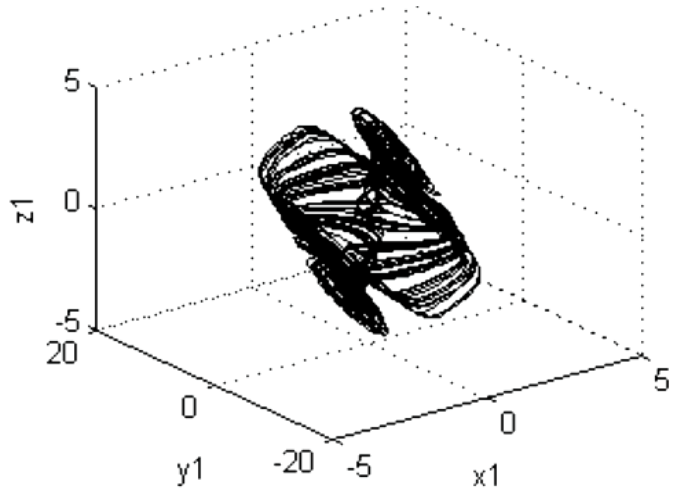


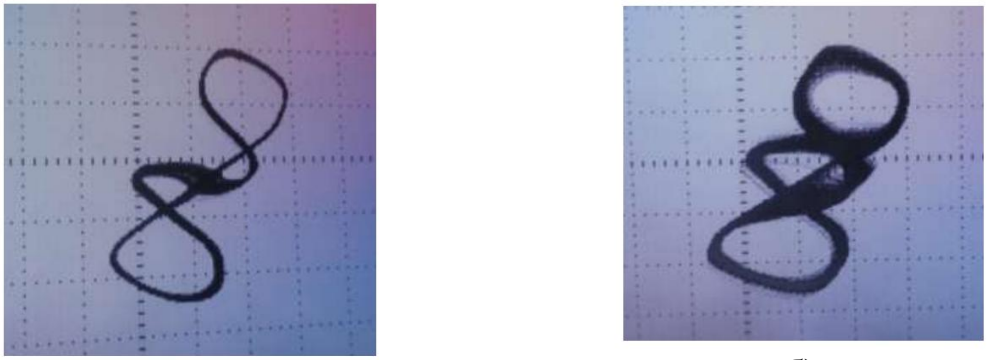
Рис.10. Хаотичні атрактори ведучого та веденого кільцевих генераторів у 3-вимірному фазовому просторі при значеннях параметрів ведучого та веденого генераторів $\alpha_1 = 2{,}1$; $\alpha_2 = 2{,}15$; $\beta_1 = 1{,}38$; $\beta_1 = 1{,}39$; $M = 5$

Ідентичність за структурою та основними характеристиками псевдовипадкових коливань ведучого та веденого генераторів була підтверджена експериментально.

Зі збільшенням параметру *M*, що відіграє роль коефіцієнта підсилення у колі оберненого зв'язку, регулярні (періодичні) коливання (рис.11) втрачають стійкість і після ряду біфуркацій подвоєння переходять в псевдовипадкові коливання (рис.12). При цьому утворений атрактор є подібним до подвійної спіралі (рис.13).

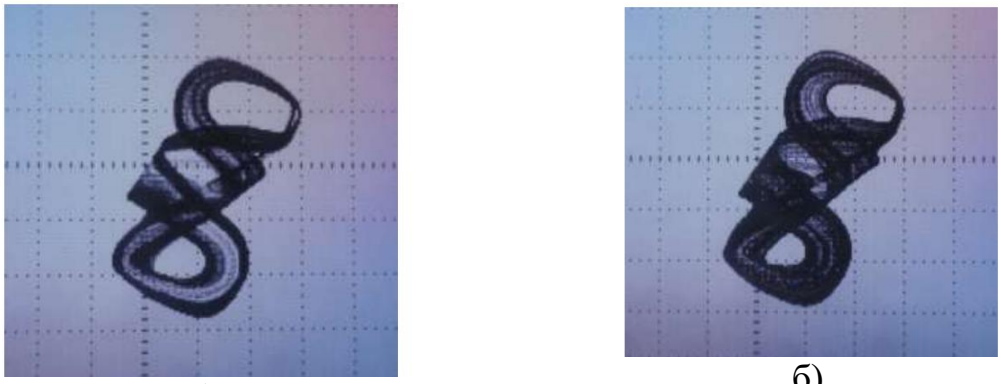
а) б)

Рис.11. Періодичний режим коливань у колі зворотного зв'язку при значеннях коефіцієнта підсилення *M=1,1* (а); – *M=1,7* (б)



а) б)

Рис.12. Перехідний режим коливань у колі зворотного зв'язку при значеннях коефіцієнта підсилення: *M=2,2* (а) та *M=2,9* (б)



а) б)

Рис.13. Хаотичний режим коливань кільцевих генераторів при значеннях коефіцієнта підсилення у колі зворотного зв’язку *M=3,5* (а) та *M=5* (б)

Оскільки у спектрах сигналів, генерованих кільцевим генератором (рис.8б) явно виражений максимум не спостерігається, то ступінь синхронізму між генераторами ведучої та веденої системи визначався за функцією подібності (16, 17), що не залежить від поняття фази сигналу.

$$G(\tau)=\sqrt{\frac{\left\langle \left(x_2(t+\tau)-x_1(t)\right)^2 \right\rangle}{\sqrt{\left\langle x_1^2(t)\right\rangle \cdot \left\langle x_2^2(t)\right\rangle}}}, \qquad (16)$$

де $x_1(t)$ – змінна ведучої системи, $x_2(t)$ – змінна веденої системи;

$$k=\min(G(\tau)) \qquad (17)$$

Приведені залежності функції подібності (рис.14) між однотипними сигналами ведучого та веденого кільцевого генератора від коефіцієнта зв’язку між ними при двох значеннях частоти зрізу ФНЧ ($u=1$, $u=6$), що моделює канал зв’язку, вказують на можливість встановлення синхронних коливань при значеннях коефіцієнту зв’язку e>2.

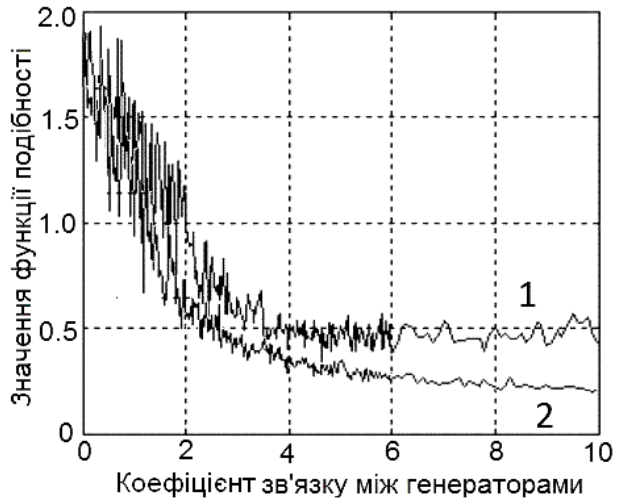


Рис.14. Залежність функції подібності між однотипними сигналами ведучого та веденого кільцевих генераторів від коефіцієнта зв’язку між ними при значеннях частоти зрізу ФНЧ: $u=1$ (крива 1) та $u=6$ (крива 2)

У **четвертому** розділі – «**Моделювання та дослідження систем передавання інформації на базі генераторів хаотичних коливань з неперервною функцією відображення**» – приведені результати досліджень

процесів прихованого передавання інформаційних сигналів маскованих псевдовипадковим переносником на базі хаотичних коливань, генерованих системою Лоренца та кільцевим генератором.

Система передавання інформації з її маскуванням шляхом перемикання режимів роботи генераторів псевдовипадкових коливань (CSK – chaos shift keying), що описуються системою Лоренца (рис.15) є більш завадозахищеною у порівняння із системою, що базується на додаванні до інформаційного сигналу псевдовипадкового переносника.

При передаванні біту «0» сигнал x на вході приймача є синхронізованим із псевдовипадковим сигналом x_0, що генерований на приймальній стороні телекомунікаційної системи. При цьому різниця між ними $(x - x_0)$ експоненціально спадає з часом до нуля (рис.16 а), що вказує на встановлення синхронізації між генератором передавальної та приймальної сторін телекомунікаційної системи.

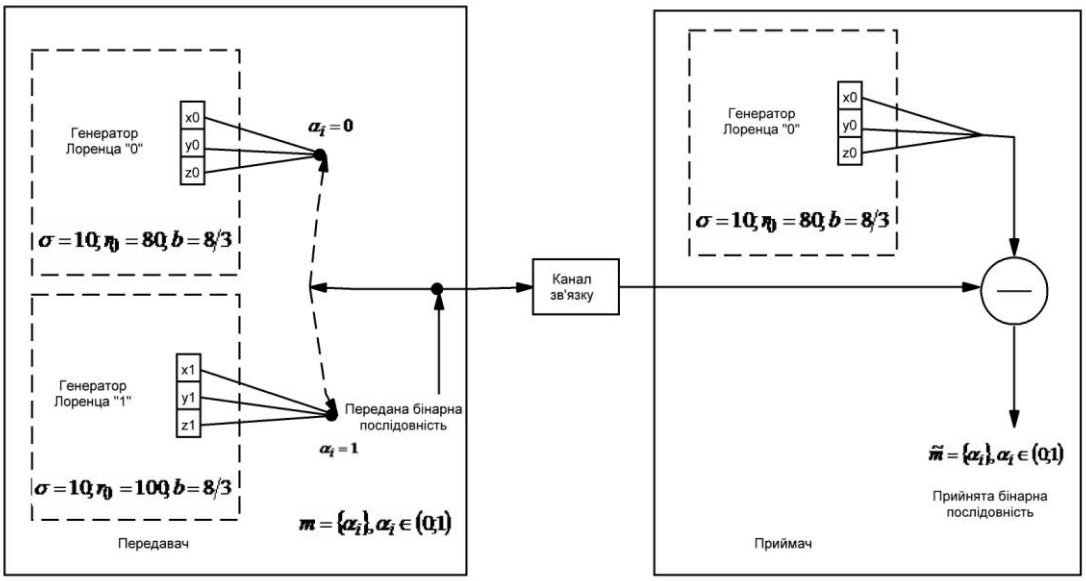
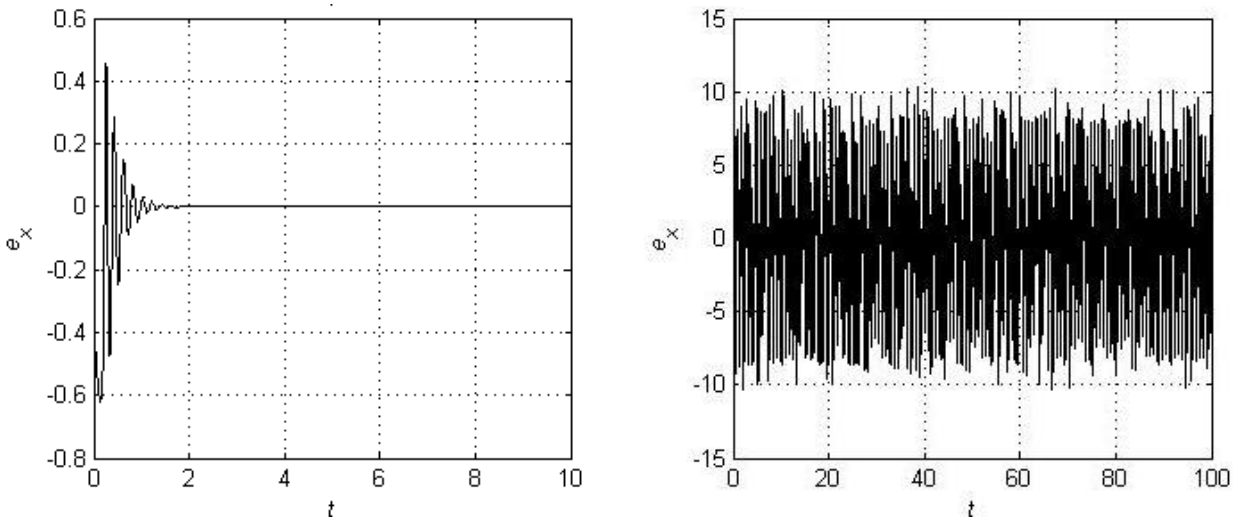


Рис.15. Структурна схема передавання інформації з перемиканням генераторів псевдовипадкових сигналів



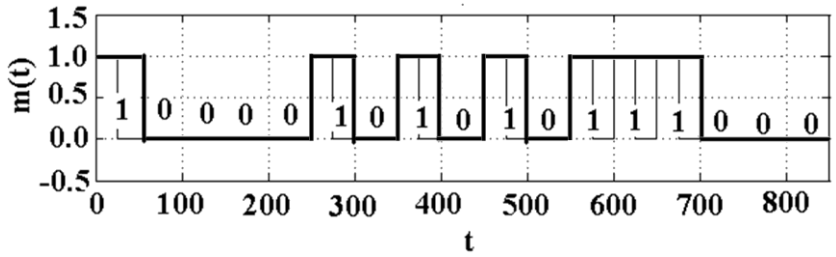
а) б)

Рис. 16. Часова залежність помилки синхронізації у випадку синхронного відгуку між передавачем та приймачем (а) та його відсутності (б)

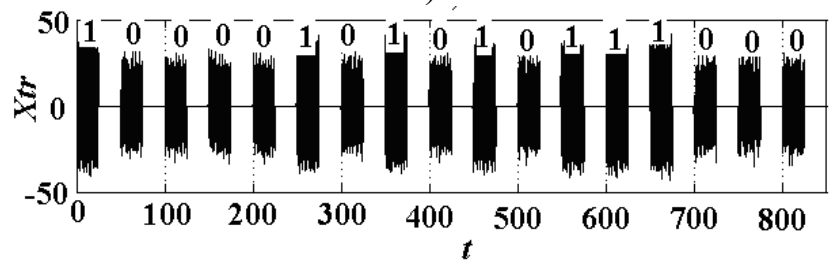
Протягом часу передавання біту «1» між генерованим сигналом на вході та сигналом, генерованим на приймальній стороні, синхронізація відсутня, що підтверджується шумоподібним характером похибки синхронізації (рис.16 б).

Використання такого методу дає можливість декодувати двійкову інформацію з отриманого псевдовипадкового сигналу.

У процесі передавання потоку двійкових даних (рис.17 а, 17 б), що містить біти «0» і «1», у приймачеві відбувається чергування наявності та відсутності синхронізації на проміжках часу передавання інформаційних бітів (рис. 18).



а)



б)

Рис.17. Часова діаграма інформаційного повідомлення у RZ цифровому форматі (а) та сигналу, що передається (б)

При цьому швидкість передавання бітів залежатиме від часу встановлення синхронізації. В початковий момент передавання кожного інформаційного біту спостерігається високий рівень похибки синхронізації, а її часова діаграма залежить від значення переданого біта (рис.18).

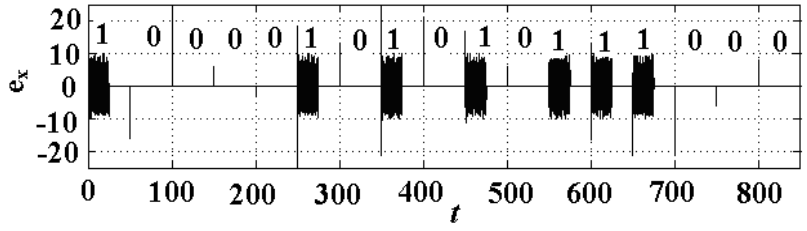


Рис.18. Режими встановлення синхронізації між генераторами приймальної та передавальної сторін телекомунікаційної системи

На рис.19 та рис.20 приведені результати дослідження процесу проходження інформаційного сигналу через кільцевий автогенератор шляхом моделювання залежності нормованої функції кореляції (18), (19) між

інформаційним сигналом та сигналом на виході системи у залежності від амплітуди інформаційного сигналу.

$$R(\tau)=\frac{\langle z(t)\cdot s(t+\tau)\rangle-\langle z(t)\rangle\cdot\langle s(t+\tau)\rangle}{\sqrt{\left(\langle z^2(t)\rangle-\langle s^2(t)\rangle\right)\cdot\left(\langle z^2(t+\tau)\rangle-\langle s^2(t+\tau)\rangle\right)}} \tag{18}$$

$$R_{\max}=\max_{z(t)}\left(R(\tau)\right) \tag{19}$$

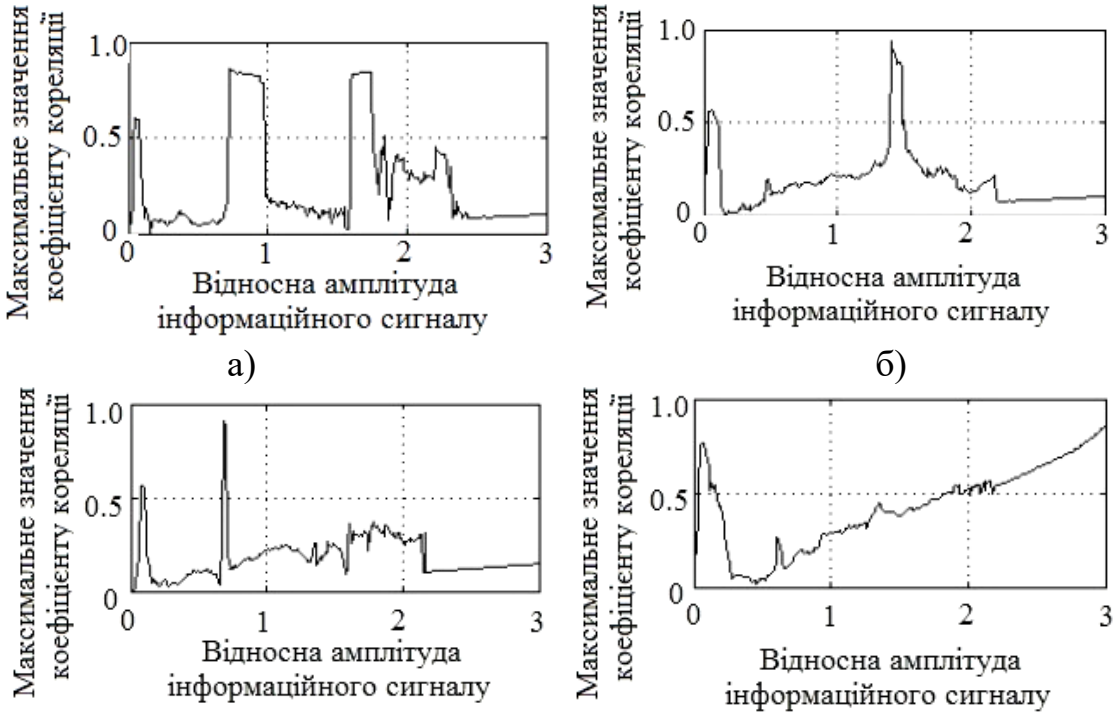
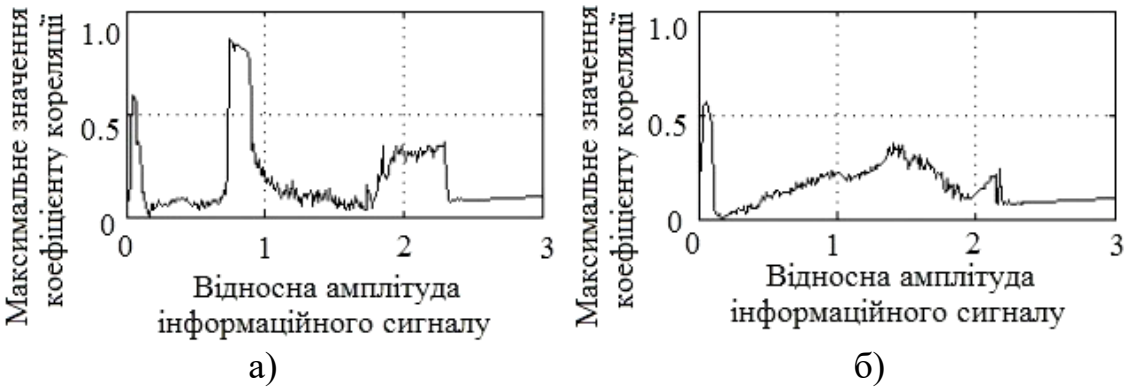
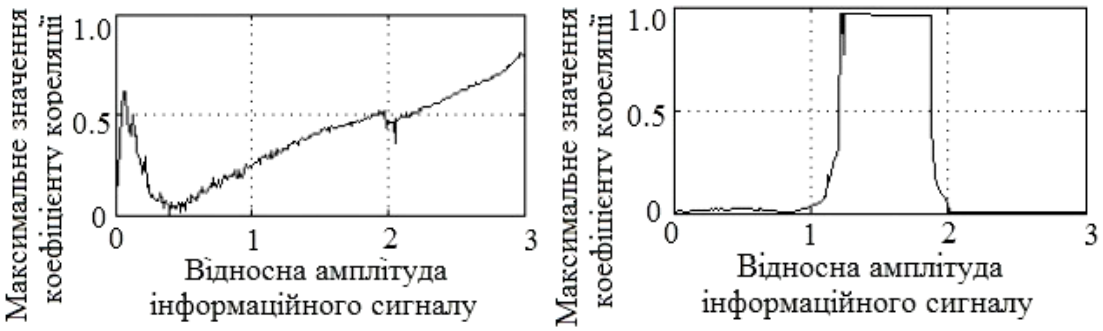


Рис.19. Залежність максимального значення коефіцієнту взаємної кореляції між інформаційним синусоїдальним та псевдовипадковим сигналом, що генерується кільцевим автогенератором від відносної амплітуди інформаційного сигналу при різних нормованих частотах (f_0): $f_0=0.4$ – а); $f_0=0.5$ – б); $f_0=0.8$ – в); $f_0=1.0$ – г).

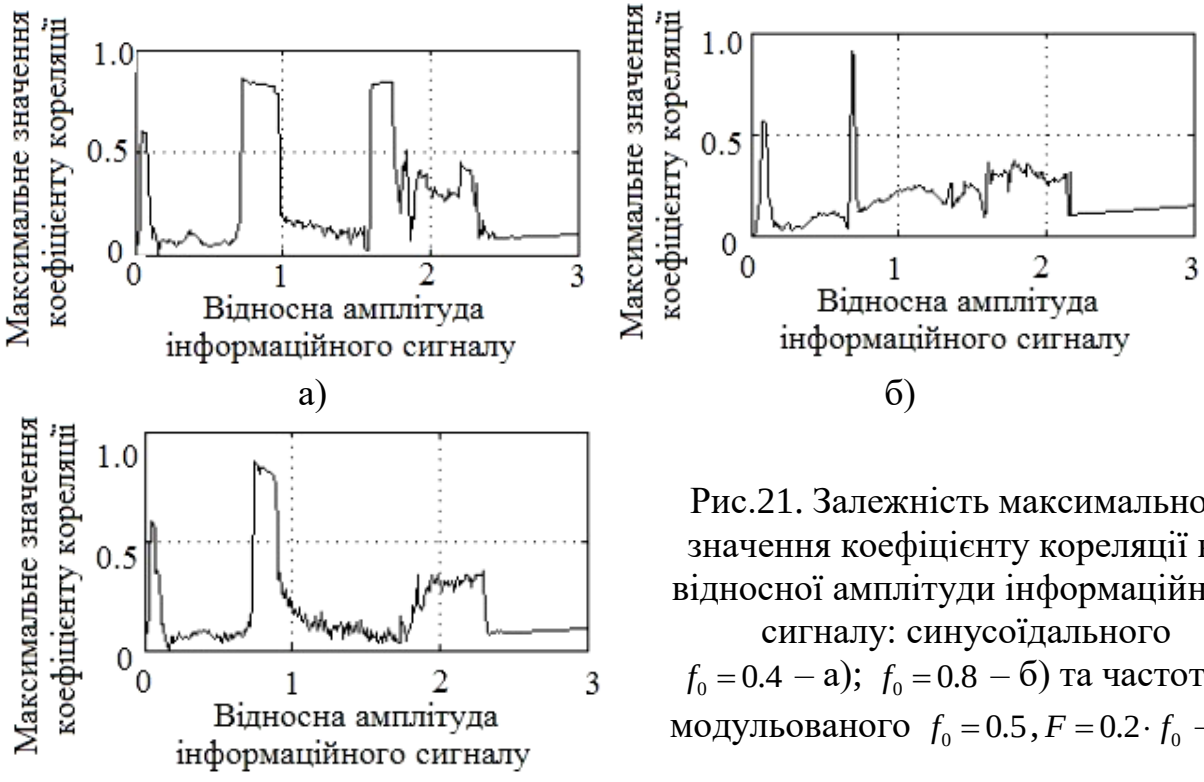




в) г)

Рис.20. Залежність максимального значення коефіцієнту взаємної кореляції між вхідним частотно-модульованим та псевдовипадковим сигналами від відносної амплітуди інформаційного сигналу при різних нормованих частотах (f_0) та частотах модуляції (F): $f_0 = 0.5$, $F = 0.2 \cdot f_0$ – а); $f_0 = 0.8$, $F = 0.2 \cdot f_0$ – б); $f_0 = 1.0, F = 0.1 \cdot f_0$ – в); $f_0 = 1.5$, $F = 0.1 \cdot f_0$ – г).

Великі значення коефіцієнта кореляції вказують на подібність псевдовипадкового та інформаційного сигналів. При цьому має місце зменшення прихованості інформаційного сигналу, що є однією із причин уразливості системи передавання інформації. При малих значеннях коефіцієнта кореляції виділення інформаційного сигналу в умовах дій завад у каналі унеможливлюється. Оптимальне значення коефіцієнта кореляції приблизно дорівнює $0{,}5$ (рис.21).



а) б)

в)

Рис.21. Залежність максимального значення коефіцієнту кореляції від відносної амплітуди інформаційного сигналу: синусоїдального $f_0 = 0.4$ – а); $f_0 = 0.8$ – б) та частотно-модульованого $f_0 = 0.5, F = 0.2 \cdot f_0$ – в).

У **п’ятому** розділі – **«Властивості сигналів типу фрактальний гаусовий шум та телекомунікаційні системи на їх основі»** – приведені результати

досліджень енергетичних, статистичних та кореляційних властивостей сигналу типу фрактальний гаусовий шум, описаний запропонований метод кластерного кодування та телекомунікаційна система передавання інформації на його основі.

На рис. 22 приведені отримані методом усереднення за реалізаціями залежності спектральної густини потужності (20) представлених 500 відліками сигналів ФГШ із показниками Херста 0.1, 0.5 та 0.9 від коефіцієнту часового масштабування при значеннях нормованої частоти $f_н = 0,1$; $f_н = 0,2$; $f_н = 0,3$; $f_н = 0,4$.

$$W(\omega) = \frac{1}{1001} \cdot \overline{\left| \sum_{k=0}^{500} S(k \cdot T) \cdot e^{-j \cdot \omega \cdot k \cdot T} \right|^2} \qquad (20)$$

де W - усереднена спектральна густина потужності для 500 відліків ФГШ, ω - циклічна частота, S - значення відліку сигналу в момент часу kT, T - період дискретизації.

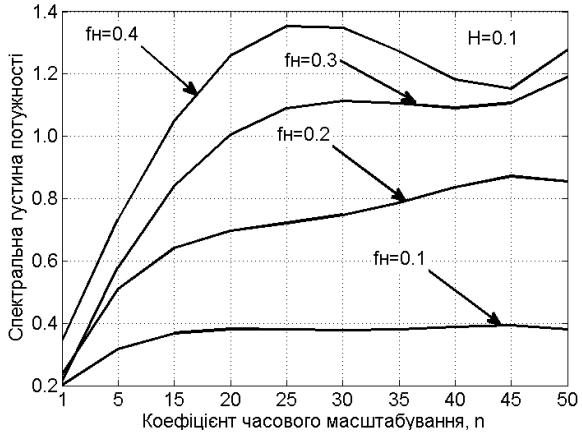


Рис.22. Залежність спектральної густини потужності від коефіцієнту масштабування для сигналів ФГШ з показниками показниками Херста H=0,1; при різних значеннях нормованої частоти ($f_Н$)

Із отриманих результатів випливає, що у спектрі ФГШ із показником Херста H=0,1 (рожевий шум) збільшується частка високочастотної складової: при збільшенні коефіцієнта часового масштабування від 1 до 50 значення спектральної густини потужності зростає в два та три рази для значень нормованої частоти 0,1 і 0,4 відповідно. Для ФГШ з показниками Херста H=0,5 (білий шум); H=0,9 (сірий шум) явно виражений вплив коефіцієнта часового масштабування на їх спектр не спостерігається.

Дослідження статистичних властивостей ФГШ підтвердили їх самоподібність у сенсі збереження статистичних характеристик (розподіл є близьким до Гаусового).

За результатами проведених досліджень властивостей ФГШ здійснювалось моделювання трафіку у системах масового обслуговування. Дослідження процесів проходження трафіку в телекомунікаційних системах підпорядкованих рівномірному, Пуасонівському та самоподібному розподілу здійснювалося на базі моделей систем масового обслуговування з потрійною маршрутизацією.

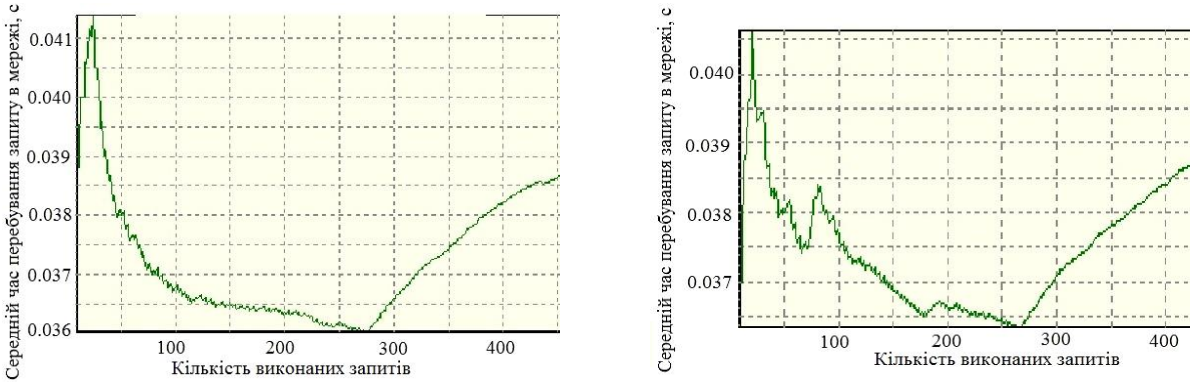
При моделюванні процесів проходження трафіку використовувалась розроблена у середовищі Delphy 7.0 програма з буферизацією завдань та безмежною чергою в припущенні, що пропускна здатність кожного вузла і інтенсивність вхідного потоку дорівнюють 60 запитів/сек та $1.8 \cdot 10^3$

запитів/годину відповідно.

В результаті проведених досліджень 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 із самоподібним та Пуасонівським потоками. При цьому потоки із самоподібним та Пуасонівським розподілами є ідентичними при їх інтенсивності порядку $1.8 \cdot 10^3$ запитів/годину.

При збільшенні інтенсивності вхідного потоку до $1.0 \cdot 10^5$ запитів/годину обчислені значення середнього часу проходження одного запиту для потоків із самоподібним та пуасонівським розподілами є більшими за середній час проходження потоку із рівномірним розподілом на $8 \cdot 10^{-3}$ с та $2 \cdot 10^{-3}$ с відповідно. Це дає можливість зробити висновок що пікові навантаження суттєво збільшують середній час перебування запиту (на 6…25%), оскільки черга у системі не може бути скомпенсованою часовими проміжками, протягом яких інтенсивність потоку є меншою за пропускну здатність вузла.

Встановлено, що при збільшенні інтенсивності до $1.0 \cdot 10^5$ запитів/годину має місце суттєва відмінність процесів проходження пакетів через систему при різних значеннях показників Херста для самоподібного потоку (рис.23).



а) б)

Рис.23. Залежність середнього часу перебування запитів від кількості виконаних запитів для самоподібного вхідного трафіку з показниками різними показниками Херста: (а) – H=0.1; (б) – H=0.9

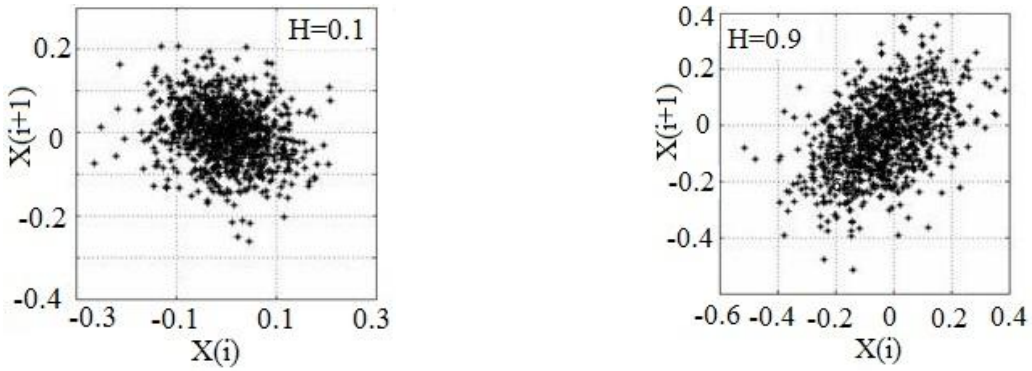
Відмінність утворених у фазовому просторі кластерів сигналами ФГШ з різними показниками Херста була покладена в основу методу кодування цифрової інформації, що отримав назву «кластерне кодування». При цьому логічний нуль відповідає сигналу з показником Херста H=0,1, а логічна одиниця – сигналу з показником Херста H=0,9.

На рис.24 приведені кластери утворені 300-ми відділками сигналів типу ФГШ з показниками Херста H=0,1 та 0,9, що генеровані за наступною математичною моделлю:

$$X^{(H)}(i) \approx \frac{1}{\Gamma\left(H+\frac{1}{2}\right)} \cdot \left\{ \sum_{j=0}^{\left[n\cdot(i+1)-1\right]} \left[(i+1) - \frac{j}{n} \right]^{H-1/2} \cdot \xi(j) - \sum_{j=0}^{i\cdot n-1} \left(i - \frac{j}{n} \right)^{H-1/2} \cdot \xi(j) \right\}, \qquad (21)$$

де H – параметр Херста, n – параметр масштабування у часі самоподібного

сигналу (мінімальне значення цього параметру дорівнює 1), $X^{(H)}(i)$ – значення i-того відліку сигналу з параметром Херста H, $\xi(i)$ – значення i-того відліку сигналу з гаусовим розподілом значень з нульовим математичним сподіванням та дисперсію σ^2.



а) б)

Рис.24. Кластери сигналів ФГШ у фазовому просторі, з показниками Херста H = 0,1 – а) та H = 0,9 – б).

Розпізнавання кластерів здійснюється за значенням так званого «параметра розпізнавання», що визначаються за формулами:

$$d_1 = \sqrt{\sum_{i=1}^{N}\left[\left(x^{(0,9)}(i) - x_0\right)^2 + \left(y^{(0,9)}(i) - y_0\right)^2\right]}\ , \qquad (22)$$

$$d_0 = \sqrt{\sum_{i=1}^{N}\left[\left(x^{(0,1)}(i) - x_0\right)^2 + \left(y^{(0,1)}(i) - y_0\right)^2\right]}, \qquad (23)$$

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. Формування кластерів здійснювалося за наступними співвідношеннями:

$$y^{(0,1)}(i) = x^{(0,1)}(i+1) \qquad (24); \qquad y^{(0,9)}(i) = x^{(0,9)}(i+1) \qquad (25).$$

Із приведеної залежності (рис.25) абсолютних значень розпізнавальних параметрів кластерів сигналів, що відповідають логічним «0» та «1», від кількості їх відліків випливає, що різниця між ними зростає зі збільшенням кількості відліків. Похибка визначення розпізнавальних параметрів кластерів не перевищувала 5%.

Обчислення розпізнавальних параметрів кластерів ФГШ на приймальній стороні системи з врахуванням білого Гаусового шуму у каналі зв'язку здійснювалося шляхом додавання значень відліків ФГШ адитивного білого Гаусового шуму (AWGN):

$$x_r^{(H)}(i) = x^{(H)}(i) + R(i), \qquad (26)$$

де $x_r^{(H)}(i)$, $R(i)$ – значення відліків сигналу та шуму на вході приймача; $x^{(H)}(i)$ – значення відліків сигналу на виході передавача.

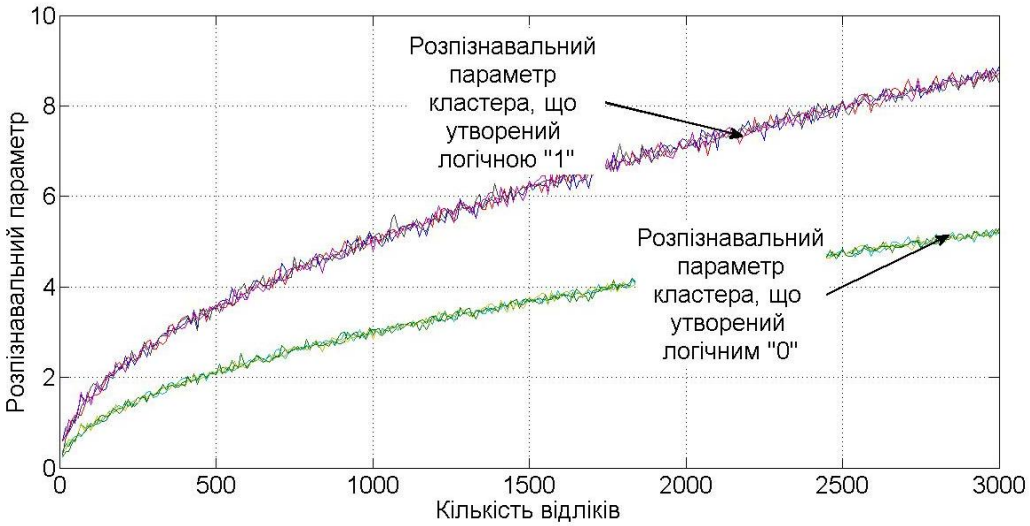


Рис.25. Залежність абсолютних значень розпізнавальних параметрів кластерів сигналів, що відповідають логічним «1» та «0» від кількості відліків в умовах незашумленого каналу

Якість передавання інформації в умовах зашумленого каналу визначалася мінімальним значенням відношення сигнал/шум (27) при якому можливе розпізнавання інформаційних бітів за різницею значень розпізнавальних параметрів, отриманого із залежностей нормованих значень d_1 і d_2 (рис.26):

$$SNR = 10 \cdot \lg\left[\frac{P_c}{P_ш}\right], \qquad (27)$$

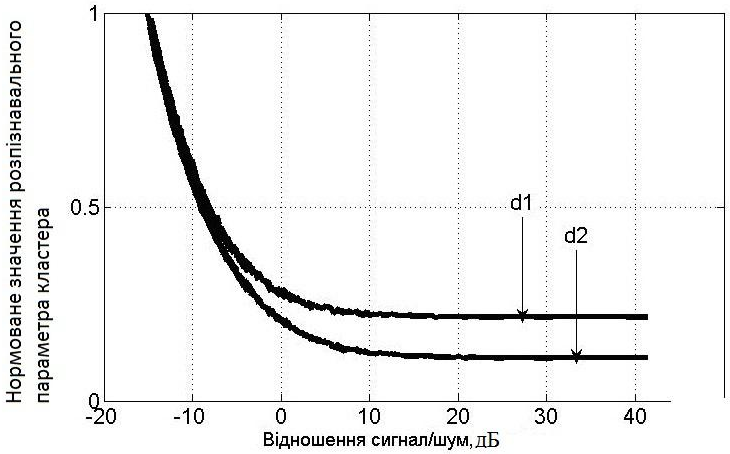


Рис.26. Залежність нормованих значень розпізнавальних параметрів кластерів сигналів, що відповідають логічним «1» та «0»

Із отриманих залежностей мінімальних значень відношення сигнал/шум, при яких можливе розпізнавання логічного 0 та 1, від кількості відліків сигналу при різних статистичних реалізаціях (рис.27) випливає, що відношення с/ш, при якому можливе їх розпізнавання зменшується від 10 дБ при 50 відліках до 0 дБ при 100 відліках, а при 500 відліках це відношення становить - 7,5 дБ. Похибка обчислення відношення с/ш становила 2.5 дБ.

На основі отриманих результатів досліджень властивостей сигналів ФГШ

запропонована система приймання/передавання (рис.28) цифрової інформації, у якій розпізнавання бітів здійснюється шляхом порівняння розпізнавальних параметрів кластерів, формованих сигналами ФГШ з показниками Херста, що відповідають низькому та високому рівням манчестерського коду, без врахування рівня шуму на приймальній стороні системи.

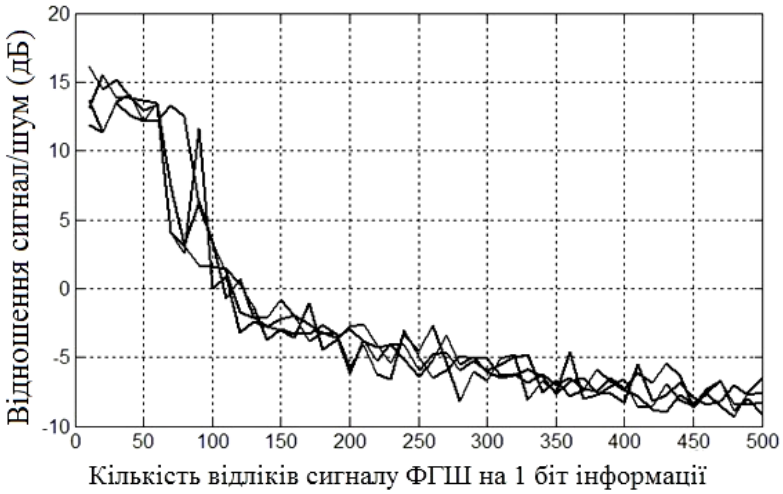


Рис. 27. Залежність мінімального значення відношення сигнал/шум, необхідного для розпізнавання бітів інформаційної послідовності від кількості відліків сигналів ФГШ, що використовується для їх кодування при різних статистичних реалізаціях.

Кодер системи (рис.28) містить два генератори відліків ФГШ із показниками Херста 0,1 та 0,9, що кодують високий та низький рівні манчестерського коду відповідно; комутатор, конвертер з коду „без повернення до нуля” в „манчестерський” код.

До складу приймача входить блок визначення параметру розпізнавання кластерів, утворених у фазовому просторі відліками прийнятого сигналу, блок запам’ятовування параметру розпізнавання, та блок порівняння параметрів розпізнавання поточного та попереднього кластерів.

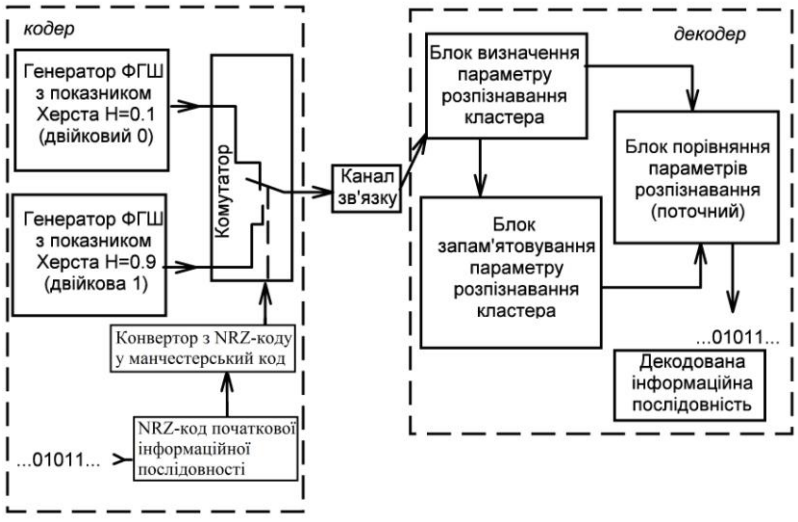


Рис.28. Блок-схеми приймання/передавання інформації на основі порівняння параметрів кластерів бітів інформаційної в манчестерському цифровому форматі

У манчестерському цифровому форматі кодування нулів та одиниць забезпечується перепадом потенціалу всередині кожного імпульсу (одиниці з низького до високого, а нуля – навпаки). Якщо вхідний біт відповідає логічній „1”, то на протязі першого такту підмикається генератор з параметром Херста H =0.1, а на протязі другого – генератор з H =0.9. Якщо вхідний біт відповідає

логічному „0”, то на протязі першого такту підмикається генератор з параметром Херста H =0.9, а на протязі другого – генератор з H =0.1.

Розпізнавання бітів інформації є можливим шляхом порівняння значень параметрів розпізнавання кластерів першого такту текучого імпульсу та другого такту попереднього. При цьому, на відміну від інших методів декодування, відпадає необхідність розрахунку рівня потужності шуму.

У **шостому** розділі – **«Фрактальні сигнали гребінкової структури: властивості та практичні аспекти використання у телекомунікаційних системах»** – розроблено новий метод генерування фрактальних сигналів гребінкової структури (ФСГС), що складаються з електричних імпульсів прямокутної форми однакової тривалості та різних амплітуд значення яких залежить від формованого ними рівня фракталу. (рис.29), досліджені їх властивості і запропоновано практичну реалізацію системи кодер/декодер таких сигналів. Експериментально отримані часові та спектральні характеристики таких сигналів та досліджені їх властивості. Генерування сигналів здійснювалося з використанням кодера, реалізованого на мікросхемі **PIC 18F2550.**

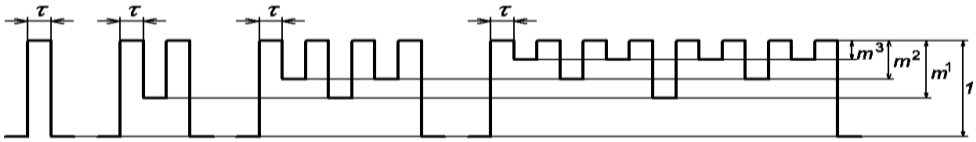


Рис.29. Фрактальні сигнали першого, другого, третього та четвертого порядків, m – коефіцієнт утворення фрактального сигналу, τ – тривалість одного імпульсу

Початковим елементом є одиничний прямокутний імпульс, тривалість якого поділяється на три рівні частини ($w=1$, рис.29). На першому та третьому часових інтервалах значення сигналу, що формується дорівнюють амплітуді вихідного імпульсу. На другому інтервалі значення сигналу, що формується є меншим ніж амплітуда вихідного імпульсу в $1/m=2$ рази. Назвемо сформований фрактал фракталом 2-го порядку ($w=2$, рис.29). На наступному етапі перший та третій інтервали фрактального сигналу першого порядку рівні амплітуді вихідного сигналу поділяється знову на три часові інтервали однакової тривалості. При цьому забезпечується зменшення значення сигналу на другому інтервалі у $1/m^2=4$ рази. Назвемо сформований фрактал фракталом 3-го порядку ($w=3$, рис.29). Наступний крок повторює попередню процедуру зі зменшенням амплітуди 2-го імпульсу в $1/m^3=8$ раз утворюючи фрактал 4-го порядку ($w=4$, рис.29), і т.д.

З метою зменшення числа відліків сформованого фрактального імпульсу та спрощення апаратної реалізації генератора доцільно тривалість всіх часових інтервалів (фрагментів) вибирати однаковою (рис.29).

Математична модель ФСГС має наступний вигляд:

$$u(t)=\sum_{i=1}^{l}A_i\cdot\sum_{k=1}^{n_i^w}U_i^k(t), \tag{28}$$

де w – порядок фракталу; m – коефіцієнт масштабування фрактального імпульсу; $A_i=A\cdot\left[1-m^i\right]$ – значення амплітуди імпульсів на i-тому рівні; $n_i^w=2^{i-1}$ – кількість імпульсів на i-тому рівні; $U_i^k(t)$ – k-ий одиничний імпульс прямокутної форми i-го рівня; τ – тривалість елементарного прямокутного імпульсу.

Спектральна густина фрактального сигналу, описується наступним виразом:

$$S(j\cdot\omega)=\frac{2A_1}{\omega}\left[\sin\left(\frac{\omega\tau}{2}\right)-2\cos\alpha_0\sum_{i=2}^{w+1}\left(1-m^i\right)\sum_{k=1}^{2^{i-2}}\sin\alpha_i^k\right], \tag{29}$$

де $\alpha_0=\omega\cdot\tau/2$, $\alpha_l^k=\omega\cdot\tau\cdot2^w\cdot\left[2^{1-i}\cdot(2\cdot k-1)-1\right]$.

На рис.30 приведені графіки спектральної густини потужності ($|S(j\cdot\omega)|^2$), що розраховані для значення w=4.

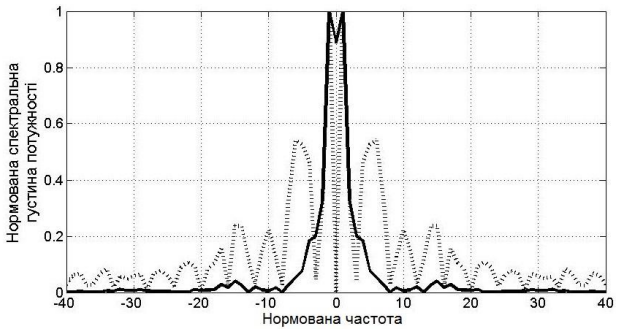
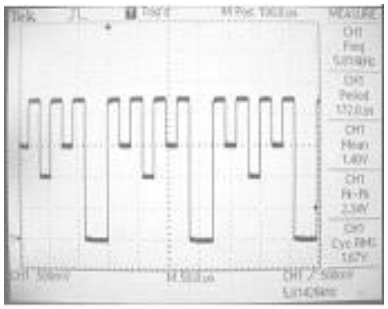


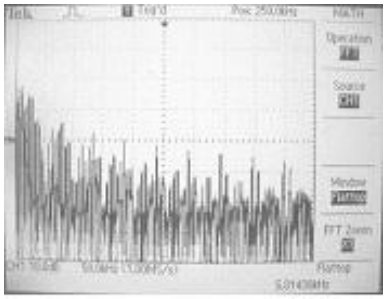
Рис.30. Нормована спектральна функція ФСГС четвертого порядку (штриховою лінією показана с.г.п. без урахування постійної складової

Експериментально отримані часові діаграми та спектр ФСГС генерованих кодером на базі мікроконтролера PIC18F2550 приведені на рис. 31.

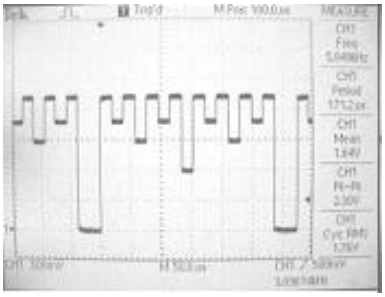
Тактова частота контролера, що задавалася ввімкненим у схему кварцовим резонатором, дорівнювала 4 МГц, що забезпечувало формування фрагментів генерованих фрактальних сигналів тривалістю 2 мкс.

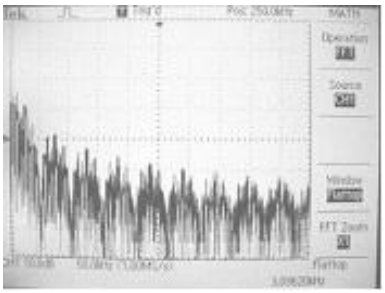


а)



б)





в) г)

Рис.31. Експериментальні осцилограми та амплітудні спектри генерованих ФСГС: третього порядку – а), б); четвертого порядку – в), г)

При оцінюванні бази запропонованих сигналів ширина їх спектральної смуги визначалася методом шумового еквіваленту:

$$F_{eff} = \frac{1}{G_{\max}} \cdot \int_0^{\infty} G(f)\,df\,, \qquad (30)$$

де F_{eff} – ефективна ширина спектра частот сигналу; $G_{\max}$ – максимальне значення спектральної густини потужності сигналу; $G(f)$ – спектральна густина сигналу.

Розрахована залежність бази ФСГС від їх порядку при різних значеннях коефіцієнту утворення приведена на рис.32.

Рис.32. Залежність бази фрактального сигналу від його порядку для різних значень коефіцієнту утворення

Із отриманих результатів випливає, що база запропонованих сигналів даного класу може перевищувати 200, тобто вони є широкосмуговими.

Алгоритм формування ФСГС уможливлює кодування інформації двобітовими символами («00», «01», «10» та «11») з використанням чотирьох рівнів фракталів.

Синхронізація моменту передавання кожного біту між передавачем та приймачем здійснюється шляхом передавання сигналу, що розділяє інформаційні біти.

Отримані результати можуть бути використані в завадостійких системах передавання інформації на базі кодера/декодера ФСГС з однаковими пристроями керування.

ОСНОВНІ РЕЗУЛЬТАТИ РОБОТИ ТА ВИСНОВКИ

Науковим результатом дисертаційної роботи є розв'язок важливої наукової проблеми – розроблення методів і моделей програмно-апаратної реалізації функціональних вузлів завадостійких телекомунікаційних систем та мереж із кодуванням інформації хаотичними коливаннями та фрактальними сигналами:

1. В результаті проведеного аналізу літературних джерел встановлено, що важливе місце в сучасних телекомунікаційних системах належить несівним 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 однакової довжини не залежить від порядку їх розташування у цій послідовності. Розподіл густини ймовірності значень збалансованості є близьким до Гаусового із середнім значенням $M(L)=0$ 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 η=0,4÷0,8 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 (≈1.5%). 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-модульованого 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, які генерувалися 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 закономірності проходження 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 близько $1.8 \cdot 10^3$ запитів/год.

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

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. 459-469.

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. — Вип. 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, Mykhaulo Klymash, Ruslan Politanskiy // Computational problems of electrical engineering. — 2013. — Vol. 3, № 2. — P.6-9.

11. Бобало, Ю.Я. Вплив кофіцієнту часового масштабування сигналів типу фрактальний гаусів шум на їх 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. Характер розподілу збалансованості псевдовипадкових послідовностей генерованих картою Бейкера/ 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, 10’2014. - 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». — АР 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 // I 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 // I-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.

АНОТАЦІЯ

Політанський Р.Л. Розроблення завадозахищених систем передавання інформації на основі псевдовипадкових коливань та фрактальних сигналів. – На правах рукопису.

Дисертація на здобуття наукового ступеня доктора технічних наук за спеціальністю 05.12.02 – телекомунікаційні системи та мережі. – Національний університет «Львівська політехніка» Міністерства освіти і науки України, місто Львів, 2015.

В дисертації розроблено нові методи генерування складних сигналів, зокрема сигналів, які отримали назву фрактальних сигналів 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.

Показано, що канальне завадостійке кодування лінійними блоковими кодами зменшує тривалість синхронізації.

Проведені дослідження основних властивостей бінарних ПВП, формованих за пороговим методом на базі ПВК, генерованих системами із дискретною функцією відображення.

Досліджені процеси проходження гармонічних та частотно-модульованих сигналів через кільцевий автогенератор, що можуть бути використані у системах передавання інформації із додаванням псевдовипадкового та інформаційного сигналів. Методом математичного моделювання функції взаємної кореляції між вхідним інформаційним та хаотичним сигналом генератора визначені співвідношення між амплітудою інформаційного сигналу та потужністю псевдовипадкового сигналу, при яких процес передавання має властивість прихованості та стійкості до завад у каналі. Досліджені та експериментально змодельовані процеси передавання гармонічного сигналу, доданого до хаотичного сигналу генератора Лю методом виділення із сигналу генерованого керованим генератором у схемі синхронізації із оберненим зв’язком; встановлена множина значень одного із параметрів, при якому система Лю здатна генерувати псевдовипадкові коливання.

Досліджені фізичні границі завадостійкості системи кодування цифрової інформації, заснованої на порівнянні параметрів кластерів утворених у фазовому просторі відліками прийнятого сигналу; запропонована та запатентована структурна схема декодера, використання якої забезпечує можливість декодувати інформацію без необхідності визначення рівня шуму в каналі в умовах складних електромагнітних обставин.

Ключові слова: бінарні псевдовипадкові послідовності, синхронізація псевдовипадкових коливань, фрактальні сигнали, фазовий простір, канальне кодування.

АННОТАЦИЯ

Политанский Р.Л. Разработка помехозащищенных систем передачи информации на основе псевдослучайных колебаний и фрактальных сигналов. – На правах рукописи.

Диссертация на соискание ученой ступени доктора технических наук по специальности 05.12.02 – телекоммуникационные системы и сети. – Национальный Университет «Львивська политэхника» Министерства образования и науки Украины, город Львов, 2015.

В диссертации разработан новый метод генерирования сложных сигналов, в частности сигналов, получивших название фрактальных сигналов гребенчатой структуры. Вычислена методом шумового эквивалента база сигнала. Апробирована система передачи цифровой информации, использующая фрактальные сигналы гребенчатой структуры в качестве переносчика двухбитных комбинаций.

Проведены исследования, показывающие, что помехоустойчивое кодирование линейными блоковыми кодами приводит к эффекту снижения времени, требуемого для установления синхронизации в каналах с шумами.

В диссертации рассмотрены основные свойства – цикличность, сбалансированность и периодическая функция автокорреляции бинарных псевдослучайных последовательностей, генерируемых пороговым методом с помощью дискретных отображений. Указанные свойства позволяют использовать исследованные ПВП в предложенной системе передачи информации в качестве шифрующего потока: при синхронизации приемника и передатчика предложено использовать алгоритм CRC-32, в качестве ключа использующий ПВП, сгенерированные пороговым методом.

Разработан и исследован новый класс фрактальных сигналов гребенчатой структуры и апробирована система передачи цифровой информации, использующая его в качестве несущего сигнала.

Предложены и исследованы несколько систем скрытой и помехоустойчивой передачи аналоговых сигналов, основанные на явлении синхронизации псевдослучайных колебаний систем Лю, Лоренца, Чуа, а также кольцевых автогенераторов.

Предложен метод кодирования цифровой информации, основанный на сравнении и анализе кластеров, образованных в фазовом пространстве принимаемого сигнала. Исследованы физически возможные границы помехоустойчивости, предложен метод декодирования, использование которого не предусматривает определение уровня шума в приемной части системы.

Ключевые слова: бинарные псевдослучайные последовательности, синхронизация псевдослучайных колебаний, фрактальные сигналы, экономное кодирование, фазовое пространство, канальное кодирование.

SUMMARY

Politanskyi R. L. The development of noise immunity systems using pseudorandom and fractal signals. – The Manuscript.

Thesis for a DSc degree on speciality 05.12.02 – telecommunication systems and networks – Lviv Polytechnic National University, Ministry of Education and Science of Ukraine, Lviv, 2015.

In the thesis there was developed a new method of complex signals generation, which were called fractal comb-structured signal. The calculation by the method of noise equivalent revealed that the value of the base of this signal can reach up to 200 units.

In the thesis investigated methods to improve secrecy of telecommunication systems which transmit an encrypted text messages through open channel of communication system using stream encryption method for text encoding, which uses binary pseudorandom number sequences as a key.

It is shown that the using of linear block codes led to reduction the duration of synchronization in the noisy channel.

In the thesis are provided the research of the basic properties of binary pseudorandom sequences, which are formed with the aid of threshold method, based on pseudorandom sequences of real numbers, generated by system with discrete mapping function.

The processes of transmitting of harmonic and frequency-modulated signals through ring oscillator have been investigated. These processes can be used in the system of data transferring with adding of pseudorandom and informational signals. The method of mathematical modeling features cross-correlation between the input information and the chaotic signal generator by the ratio between the amplitude information signal and power pseudo-random signal in which the transmission process tends secrecy and resistance to noise in the channel. Experimentally investigated and modeled processes transmission harmonic signal added to the chaotic signal generator Liu allocation method of signal generated by a controlled oscillator circuit in synchronization with the feedback; set one set of values of the parameters in which the system is able to generate pseudo fluctuations.

Investigated the physical boundaries of the coding system noise immunity of digital information, which is based on a comparison of parameters of clusters formed in the phase space samples the received signal; proposed and patented a block diagram of a decoder, the use of which provides the ability to decode the information without the need to determine the level of noise in the channel in terms of complex electromagnetic conditions.

And developed and investigated a new class of complex signals, called fractal comb-structure signal. Calculation base signal noise equivalent method revealed that the base value is 200. The system of digital information transfer using fractal comb-structure signal as a carrier signal have been constructed.

The thesis describes the main characteristics (cyclical, balance and correlation) of a binary pseudo-random sequences generated by the threshold method using discrete chaotic maps. For the audio transmission system method for synchronizing transmitter and receiver which uses the transmission of the current value of the discrete chaotic map is proposed. Several noise-immunity and crypto systems based

on the phenomenon of chaotic synchronization of Liu, Lorenz, Chua and ring oscillators systems are proposed and investigated.

The method of cluster coding is proposed and its noise-immunity is investigated, the method of decoding is developed which can operate under difficult noise conditions.

A new class of broadband signals is proposed and investigated, which called fractal comb-structure signal and the system of transmission of digital information is constructed, which uses this signal as a working signal.

Key words: pseudorandom binary sequences, chaotic synchronization, fractal signals, source coding, phase space, channel coding.

Скорочення, що прийняті в авторефераті:

СПІ – система передавання інформації;

ПВС – псевдовипадкові сигнали;

ПВК – псевдовипадкові 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 конгруентний генератор;

ФНЧ – фільтр низьких частот;

ТКС – телекомунікаційна система.

Здано в набір 27.11.2015. Підписано до друку 11.12.2015.
Формат 60х90 1/16. Зам. № 3026.
Тираж 150 прим. Обсяг 2,3 умовн. друк. арк.
Віддруковано на видавничому устаткуванні фірми RISO
у друкарні ПП «Арк-сервіс».
79005, м. Львів, вул. Драгоманова, 16.