

63-72-7/1
15.01.16

Голові спеціалізованої вченої ради Д 35.052.10
Національного університету "Львівська політехніка"
79013, Львів-13, вул. С. Бандери, 12

ВІДГУК

офіційного опонента доктора технічних наук, професора, начальника кафедри бойового застосування та експлуатації АСУ Харківського університету Повітряних Сил ім. Івана Кожедуба Баранніка Володимира Вікторовича на дисертаційну роботу Політанського Руслана Леонідовича "Розроблення заводозахищених систем передавання інформації на основі псевдовипадкових коливань та фрактальних сигналів", подану на здобуття наукового ступеня доктора технічних наук за спеціальністю 05.12.02 – телекомунікаційні системи та мережі

1. Актуальність теми дисертації

Сучасною тенденцією розвитку систем, що здійснюють кодування, шифрування та передавання інформації є використання широкосмугових сигналів зі значно більшою базою ніж база сигналів генерованих стандартними методами. Ширина спектру таких сигналів обумовлена їх структурою, вони володіють властивістю дельта-корельованості, що забезпечує значний рівень заводостійкості процесу передавання інформації. Іншим позитивним аспектом застосування зазначених сигналів є «приховане передавання інформації», або стеганографія, що унеможливує проведення успішного криптоаналізу, і виявлення самого факту передавання інформації.

В якості прикладу таких сигналів можна привести сигнально-кодові конструкції та відносно менш досліджені сигнали типу фрактальний гаусовий шум.

Широке впровадження систем цифрового зв'язку обумовило розвиток складних технологій детектування сигналів, що базуються в основному на енергетичних критеріях. При цьому вимірюється потужність процесу, аналізуються адитивні енергетичні прирости корисних сигналів над потужністю шумів, що уможливує розпізнавання сигналів в умовах, коли потужність шуму може в рази перевищувати потужність сигналу.

2. Загальна характеристика роботи

Дисертаційна робота Політанського Руслана Леонідовича присвячена розробленню методів і моделей програмно-апаратної реалізації функціональних вузлів заводостійких телекомунікаційних систем та мереж із кодуванням інформації хаотичними коливаннями та фрактальними сигналами.

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.

У вступі наведено загальну характеристику дисертаційної роботи, обґрунтовано актуальність теми, сформульовано мету та задачі досліджень, обґрунтована наукова новизна одержаних результатів. Розглянуто зв'язок роботи з науковими темами, реалізацію і впровадження результатів роботи. Подано відомості про апробацію результатів роботи та публікації, особистий внесок претендента у отриманні у співавторстві наукові результати.

У першому розділі проаналізовані тенденції використання хаотичних коливань та фрактальних сигналів у телекомунікаційних системах, систематизовані технології, що використовуються в системах передавання інформації на основі псевдовипадкових коливань та фрактальних сигналів. Враховуючи сучасний стан розвитку методів шифрування, кодування та передавання інформації в телекомунікаційних системах зроблено висновок про необхідність розроблення нових типів сигналів на базі псевдовипадкових коливань із властивостями самоподібності.

У другому розділі приведені результати дослідження властивостей збалансованості, циклічності та корельованості бінарних псевдовипадкових послідовностей, що генеровані пороговим методом на основі дискретних хаотичних відображень. Розроблена математична модель впливу канального блокового кодування на тривалість процесу синхронізації; встановлені оптимальні параметри і розроблена програмна реалізація криптографічного шифрування зображень на основі дискретного тривимірного відображення зсув Бернуллі; приведені моделі телекомунікаційних систем, із синхронізацією приймальної та передавальної сторін системи.

У третьому розділі досліджені процеси генерування коливань у кільцевому генераторі та генераторі Чуа, шляхом моделювання знайдені параметри генераторів, при яких у системах виникають псевдовипадкові коливання. Досліджені характеристики синхронізації генераторів Чуа та кільцевих генераторів з лінійним підсиленням керуючого сигналу, що надходить до веденої системи через канал, змодельований фільтром низьких частот, зроблені висновки щодо впливу на процес синхронізації значень коефіцієнту підсилення сигналу та частоти зрізу фільтру низьких частот.

У четвертому розділі проведено моделювання та експериментальні дослідження коливань формованих системою Лю та їх синхронізація, що є основою системи передавання інформації із псевдовипадковим переносником, знайдений спектр показників Ляпунова, що відповідає різним режимам коливань у генераторів – стохастичний, псевдовипадковий, квазіперіодичний та періодичний; розроблена електронна схема та виконаний

експериментальний зразок генератора, що генерує коливання, описані системою Лю; досліджено процес синхронізації генераторів Лоренца та система передавання інформації, що ґрунтується на перемиканні між двома генераторами псевдовипадкових коливань, знайдені оптимальні параметри генераторів передавача та приймача з точки зору оптимізації помилки синхронізації; досліджено проходження інформаційних сигналів двох типів через кільцевий генератор, на основі досліджень знайдені оптимальні амплітуда, основна частота та частота модуляції інформаційних сигналів, при яких проходження сигналу є прихованим та завадостійким.

У п'ятому розділі приведені результати досліджень впливу параметру часового масштабування на енергетичні, статистичні та кореляційні властивості сигналу типу ФГШ з різними показниками Херста, вперше показано, що збільшення параметру часового масштабування підвищує вклад високочастотних коливань у спектр сигналу із показником Херста менше 0,5; описаний та досліджений метод кластерного кодування у випадку використання сигналів ФГШ, запропонована система декодування цього методу, що оснований на порівнянні розпізнавальних параметрів кластерів у фазовому просторі і у якій непотрібно визначати значення потужності завад на приймальній стороні системи; запропонований і досліджений спосіб синхронізації приймальної та передавальної сторін системи, що використовує маркерний сигнал. Досліджені процеси проходження самоподібного трафіку через багатоканальну систему масового обслуговування.

У шостому розділі приведені результати дослідження фрактальних сигналів гребінкової структури (ФСГС), що складаються із електричних імпульсів прямокутної форми однакової тривалості та мають різні амплітуди, що зменшуються на частини кратні степені 2; розроблена математична модель цього сигналу, на основі якої знайдений аналітичний вираз для спектральної густини потужності сигналу, розрахована база сигналу. На базі мікроконтролера PIC18F2550 розроблені кодер та декодер цифрової інформації, що використовує ФСГС 4 перших порядків для кодування двійкових діад 00, 01, 10, 11; приведені експериментальні часові та спектральні діаграми сигналів.

3. Ступінь обґрунтованості наукових положень, висновків, рекомендацій, наданих в дисертації, їх достовірність

Обґрунтованість і достовірність наукових результатів та висновків отриманих у процесі виконання досліджень підтверджена:

- використанням сучасних методів математичного та комп'ютерного моделювання;
- співставленням теоретично отриманих результатів із експериментальними дослідженнями лабораторних макетів окремих

функціональних вузлів телекомунікаційної системи;

- детальним та всебічним аналізом результатів отриманих на основі розроблених фізичних моделей;

- проведені дослідження фрактальних сигналів гребінкової структури підтверджені експериментом.

- достовірність отриманих претендентом науково-практичних результатів засвідчено актами впровадження;

- отримані нові результати гармонійно розвивають основні засади теорії передавання інформації;

- матеріали дисертації доповідались і обговорювались на 17 міжнародних і всеукраїнських науково-технічних конференціях, а також на наукових семінарах.

4. Наукова новизна результатів, отриманих в дисертаційній роботі

Наукова новизна не викликає ніяких сумнівів і міститься в наступних положеннях:

1. Розвинуто метод оцінювання впливу канального кодування на перебіг процесу встановлення синхронізації між генераторами хаотичних коливань приймальної та передавальної сторін телекомунікаційної системи. На основі створеної математичної моделі показано, що використання відносно нескладних схем лінійного блокового кодування забезпечує зменшення часу встановлення синхронізації приймальної та передавальної сторін системи на 100...200 нс.

2. Дістали подальшого розвитку методи дослідження синхронних коливань автоколивальних систем, що генерують широкосмугові сигнали із використанням різних критеріїв якості синхронного відгуку. Досліджений вплив параметрів зв'язку між двома автоколивними системами (гранична верхня частота каналу та коефіцієнт зв'язку) для кільцевого генератора та генератора Чуа. Встановлені значення параметрів системи Лоренца, при яких є уможливлення якісного передавання інформації у телекомунікаційних системах.

3. Набули подальшого розвитку дослідження сигналів типу «гаусовий кольоровий шум». З використанням методу усереднення за реалізаціями були отримані залежності енергетичних кореляційних та статистичних властивостей сигналів даного типу.

4. Вперше розроблено метод декодування цифрової інформації, кодованої сигналами типу фрактальний гаусовий 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. Встановлено, що розпізнавання інформаційних бітів закодованих ФГШ, із показником Херста 0,9 та 0,1 можливе при співвідношенні сигнал/шум у каналі рівному -7,5 дБ і значенні похибки синхронізації рівному 80% тривалості маркерного сигналу.

5. Вперше розроблено метод декодування представленої у манчестерському коді цифрової інформації, що закодована псевдовипадковими сигналами типу ФГШ (250 відліків дискретних ФГШ із показником Херста 0,9 та 0,1 для нижнього та високого рівнів відповідно). Метод базується на оцінюванні та порівнянні значень розпізнавальних параметрів кластерів сусідніх сигналів, та є стійким до дії зовнішніх електромагнітних факторів і уможливило процес декодування без визначення рівня шуму в каналі.

6. Вперше запропонований новий тип широкосмугових сигналів із значенням бази, що сягає сотень одиниць та показано, що такі сигнали є дельтакорельовані.

5. Повнота викладу наукових положень, висновків, рекомендацій в опублікованих працях

Основні наукові та практичні результати дисертаційної роботи доповідались та обговорювались на науково-технічних конференціях та науково-практичних семінарах 2010-2015 рр.

За результатами досліджень опубліковано 53 наукові праці. Серед них: 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, 20 – тези та матеріали доповідей на конференціях; 23 статті індексовані у міжнародних науково-метричних базах, 2 патенти на винахід та 1 патент на корисну модель.

6. Відповідність дисертації встановленим вимогам

Стосовно оформлення роботи особливих зауважень немає. Робота побудована згідно вимог, викладених у Бюлетені ВАК України та вимогам Постанови КМУ від 28.06.97р. за № 644, а також змінам і доповненням до цієї Постанови; якісно оформлена, перелік літературних джерел містить посилання на праці зарубіжних і вітчизняних науковців, охоплює широкий період часу, починаючи із робіт класиків – Шеннона, Харкевича, тощо і закінчуючи роботами, що опубліковані протягом останніх 5 років, включаючи транзакти IEEE.

Зміст автореферату добре висвітлює матеріал, що приведений у дисертації, прослідковується кореляція між поставленими науковими задачами, пунктами наукової новизни та основними результатами і висновками по дисертаційній роботі.

7. Важливість для науки і народного господарства одержаних результатів та шляхи їх використання

Аналізуючи роботу загалом варто зауважити актуальність наукових та науково-технічних завдань, що були поставлені в дисертаційній роботі:

розроблення моделей передавання шифрованої потоковим методом текстової, графічної, мовної та звукової інформації; дослідження процесів синхронізації приймальної та передавальної сторін системи шляхом надсилання псевдовипадкових послідовностей; подальший аналіз явищ синхронного відгуку у нелінійних автоколивних системах різної структури; дослідження можливості завадостійкого передавання інформації у системах, що володіють властивостями стеганографії; розроблення та дослідження властивостей нових класів самоподібних сигналів, складність яких поряд із малою тривалістю елементарних імпульсів, що утворюють їх, забезпечує високе значення бази сигналів.

Практичне значення отриманих автором результатів прослідковується у кожному розділі дисертації. Дослідження властивостей генерованих псевдовипадкових послідовностей із характерними для криптографії довжинами 1024, 512 та 256 біт вказують на можливість їх використання у стандартних алгоритмах шифрування інформації в якості ключів. Вирішена специфічна прикладна задача, що полягає у зменшенні затрат машинного часу за рахунок використання запропонованого алгоритму, що базується на трьохвимірному перетворенні Пекаря. У розділі, що стосується досліджень методу кластерного кодування та декодування інформаційних бітів, описаний метод їх розпізнавання при потужності шуму в каналі, що значно перевищує потужність корисного сигналу. В останньому розділі дисертаційної роботи описана апаратна реалізація системи передавання цифрової інформації.

В результаті роботи одержані наукові практичні та теоретичні результати, що знайшли впровадження на підприємствах ПАТ «Укртелеком», Чернівецької філії для прогнозування інтенсивності трафіку, що проходить через телекомунікаційні мережі підприємства; на підприємстві ПАТ «ТК Енергія», 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.

8. Зауваження до дисертаційної роботи

До дисертації та автореферату є ряд зауважень:

1. В одному із пунктів наукової новизни вказано «Вперше методом усереднення за реалізаціями ... властивостей сигналів типу фрактальний гаусів шум», хоча на мій погляд більш коректно було би «Набули подальшого розвитку дослідження сигналів типу фрактальний гаусовий шум...».

2. У пункті наукової новизни, що відображає результати досліджень завадостійкості системи передавання інформації слід було б вказати хоча би орієнтовно швидкість передавання інформації, що може бути досягнута при деякій заданій тривалості елементарних імпульсів, що формують носійний сигнал.

3. В роботі не вказано, що результати проведених досліджень можна було б використовувати у стеганографічних системах для прихованого передавання інформації.

4. На ст. 44-45 зазначено, що для забезпечення ортогональності сигналів необхідно забезпечення дельта-корельованості та нульового часового проміжку інтегрування, хоча достатнім є виконання хоча б однієї з цих умов. Варто також зауважити, що останню умову приводити недоцільно виходячи зі змісту процесу детектування сигналів.

5. При дослідженнях синхронізації генераторів хаотичних коливань у третьому та четвертому розділах розглядаються схеми з'єднання головного та веденого генераторів хаотичних коливань, але в дисертації не зазначено, які коливання збуджувалися у веденій системі – лише вимушені, чи сума вимушених та вільних коливань генератора.

6. Запропонований автором термін «кластерне кодування» не відображає в цілому суть методу, який включає в себе процеси кодування і декодування.

7. Формула, що визначає розпізнавальний параметр кластера у просторі прийнятого сигналу може бути спрощена шляхом усунення дії обчислення квадратного кореня, що не вплине на значимість та зміст отриманих результатів, але значно спростить алгоритм здійснення обчислень.

Однак, зазначені зауваження не впливають на загальну позитивну оцінку результатів дисертаційної роботи.

Загальні висновки

1. Дисертаційна робота Політанського Руслана Леонідовича є завершеною науковою працею, що містить нові науково обгрунтовані результати, важливі для подальшого розвитку телекомунікаційних систем, що експлуатуються в умовах дії завад та до яких ставляться вимоги конфіденційності передавання інформації.

2. Сукупність наукових положень, сформульованих та обгрунтованих у дисертаційній роботі, має практичну цінність і становить вирішення наукової проблеми розроблення методів і моделей програмно-апаратної реалізації функціональних вузлів завадостійких телекомунікаційних систем та мереж із кодуванням інформації хаотичними коливаннями та фрактальними сигналами.

3. Дисертаційна робота за змістом відповідає вимогам “Паспорту” спеціальності 05.12.02 – телекомунікаційні системи та мережі.

4. Матеріали дисертації є достатньо апробованими, доповідались на всеукраїнських і міжнародних конференціях, висвітлені у 53 наукових публікаціях, з них 1 монографія, 25 статей у фахових виданнях України, 4 у зарубіжних виданнях, включених до науково-метричних баз, 20 публікацій у збірниках тез конференцій, опубліковано 2 патенти на винахід та 1 патент на корисну модель.

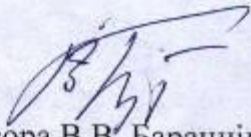
5. Автореферат об'єктивно і з необхідною повнотою відображає зміст і основні положення дисертації.

6. Наведені зауваження не змінюють загальну позитивну оцінку наукової значимості і практичної цінності дисертаційної роботи.

7. За науковим рівнем, практичною цінністю, апробацією та публікаціями дисертаційна робота відповідає вимогам пп. 9, 10, 13, "Порядку присудження наукових ступенів і присвоєння вченого звання старшого наукового співробітника", а її автор – Політанський Руслан Леонідович – заслуговує присудження наукового ступеня доктора технічних наук за спеціальністю 05.12.02 – телекомунікаційні системи та мережі.


Офіційний опонент

Начальник кафедри бойового застосування та експлуатації АСУ
Харківського університету Повітряних Сил
імені Івана Кожедуба
доктор технічних наук, професор


В.В. БАРАНІК

Підпис доктора технічних наук, професора В.В. Баранніка засвідчую

ТВО начальник штабу
Харківського університету Повітряних Сил
полковник


А.А. ЛУК'ЯНЧИКОВ

