67-72-08/2
16.02.2018

Голові спеціалізованої вченої ради Д 35.052.10 у Національному університеті «Львівська політехніка» 79013, м. Львів, вул. С. Бандери, 12.

# ВІДГУК

офіційного опонента на дисертацію **Круліковського Олега Валерійовича** «Синтез генераторів псевдовипадкових послідовностей на основі багатовимірних нелінійних динамічних систем», поданої до захисту на здобуття наукового ступеня кандидата технічних наук за спеціальністю 05.12.13 – радіотехнічні пристрої та засоби телекомунікацій.

**Актуальність теми дисертаційного дослідження.**

Враховуючи останні досягнення в розвитку інформаційних технологій стає очевидним той факт, що збільшуються обсяги передавання, оброблення та зберігання інформації, у тому числі і інформації з обмеженим доступом. Зростає багатогранність та складність розв'язання проблем інформаційної безпеки. При цьому, як відомо, найбільш ефективними засобами захисту даних з обмеженим доступом є шифрування та кодування. Однак постійне покращення методів і засобів криптоаналізу та радіорозвідки зумовлює систематичне підвищення вимог до засобів передавання інформації з обмеженим доступом.

Сучасні телекомунікаційні системи використовують сигнали з великою інформаційною ємністю. Формування сигналів довільної ємності є актуальним науково-практичним завданням при розробленні нових радіотехнічних пристроїв. Ці обставини вимагають розвитку нових областей дослідження та покращення сучасних генераторів сигналів з великою інформаційною ємністю.

Таким чином задача синтезу генераторів сигналів з підвищеною інформаційною ємністю на основі багатовимірних нелінійних динамічних систем є актуальною науково-практичною задачею.

Враховуючі вищесказане, тема дисертаційного дослідження Круліковського О.В. є **актуальною**. Отже, здобувачем вирішується актуальне наукове та практичне завдання - аналіз, синтез та практична реалізація генераторів псевдовипадкових та випадкових послідовностей на основі багатовимірних нелінійних динамічних систем з метою формування сигналів довільної ємності при розробленні нових радіотехнічних пристроїв.

**Зв'язок роботи з науковими програмами, планами, темами.**

Напрям досліджень тісно пов'язаний з рядом науково-дослідних робіт, виконаних протягом декількох років відповідно до планів наукової і науково-

технічної діяльності кафедри радіотехніки та інформаційної безпеки Чернівецького національного університету імені Юрія Федьковича та в межах науково-дослідницьких робіт: "Фізико-технологічні проблеми радіотехнічних пристроїв та засобів телекомунікацій і інформаційних технологій" (Держ. реєстр. №0111U000183, 2013-2015 рр.), а також "Методи та засоби передавання, оброблення і зберігання інформації в інфо-комунікаційних системах" (Держ. реєстр. №0116U001433, 2016-2017 рр.)

**За структурою** дисертаційна робота складається з анотації, вступу, п'яти розділів, які містять основні наукові результати, загальних висновків, списку використаних джерел та двох додатків.

У ***вступі*** обґрунтовано актуальність напрямку дослідження, наведено зв'язок роботи із науковими програмами, планами, темами, сформульовані мета та задачі дослідження, відображені наукова новизна та практична цінність роботи, особистий внесок здобувача, наведені відомості про апробацію результатів дисертації та публікації. Визначено об'єкт та предмет дослідження, надана загальна характеристика роботи у відповідності з діючими вимогами до дисертаційних робіт.

***Перший розділ*** дисертації має оглядовий характер. В ньому проведено аналіз аспектів використання генераторів псевдовипадкових послідовностей на базі нелінійних динамічних систем, висвітлено основні положення теорії нелінійних динамічних систем. Детально розглянуто властивості хаотичних систем, що обумовлюють переваги їх використання у системах передавання інформації. Розкрито сутність детермінованого хаосу під яким розуміють складні неперіодичні коливання, що породжуються нелінійними динамічними системами. При цьому нелінійність системи є необхідною, але недостатньою умовою для виникнення хаосу. Можливість застосування генераторів псевдовипадкових послідовностей на базі детермінованого хаосу в системах передавання інформації обумовлена існуванням методу їх відтворюваності. На основі аналізу літературних джерел за тематикою роботи сформульовано завдання дисертаційних досліджень.

***Другий розділ*** присвячений питанням аналізу та синтезу генераторів псевдовипадкових послідовностей на базі нелінійних динамічних систем, з метою уможливлення їх застосування у пристроях формування та оброблення інформаційних сигналів. В розділі проаналізовано принципи побудови генераторів псевдовипадкових послідовностей і сформульовані вимоги щодо їх використання в системах передавання інформації. Показано, що розв'язання проблеми повторюваності псевдо хаосу можливе шляхом збільшення середньої довжини циклу та тривалості перехідного процесу за рахунок підвищення прецизійності обчислень та введення псевдовипадкових періодичних збурень, а

також переходом до багатовимірних систем. Зазначено, що особливістю хаотичних систем є відвідування їх траєкторіями областей фазового простору, з дробовими значеннями фрактальних розмірностей з різними частотами внаслідок чого розподіл значень послідовностей, генерованих такими системами є нерівномірним.

Крім того в розділі показано, що при виборі хаотичних систем перевагу слід надавати таким, що характеризуються суцільною діаграмою біфуркацій без вікон періодичності. Використання всієї множини початкових умов з області притягування атрактора при виборі простору ключів є некоректним і призводить до неправильної оцінки його обсягу.

В розділі підкреслено, що використання багатовимірних систем для розв'язання задачі циклічності є найбільш доцільним, оскільки середні тривалості циклу та перехідного процесу при виході траєкторії на цикл залежать від кореляційної розмірності єдиним способом збільшення середньої тривалості циклу є збільшення кореляційної розмірності хаотичної системи.

В кінці розділу запропоновано для реалізації генераторів псевдовипадкових послідовностей з великими значеннями їх періоду використовувати генератори послідовностей на ПЛІС.

У ***третьому розділі*** представлено апаратну реалізацію генераторів псевдовипадкових послідовностей на базі багатовимірних хаотичних систем та результати дослідження генерованих ними послідовностей на відповідність критеріям псевдовипадковості згідно набору статистичних тестів NIST.

Також за допомогою чисельних методів Ейлера та Рунге-Кути здобувачем детально досліджено розв'язки нелінійних диференційних рівнянь математичної моделі мемристивної хаотичної системи та встановлено, що середня тривалість циклу знаходиться в межах певних ітерацій і не залежить від кроку зазначеної дискретизації.

***Четвертий розділ*** присвячено проведенню дослідження динамічних режимів роботи та запропоновано схемотехнічну реалізацію генераторів випадкових послідовностей на базі хаотичних систем Тратаса і Лоці.

В розділі проведено детальний аналіз ітераційних діаграм який дозволив зробити висновок, що система Тратаса за типом функції нелінійного перетворення еквівалентна двом тентовим відображенням, що з'єднані слабким зворотнім зв'язком та представлена її технічна реалізація. Показано, що гіперхаотичні коливання мають місце в широкому діапазоні значень параметрів керування.

***П'ятий розділ*** присвячено проведенню дослідження криптостійкості методу перестановок пікселів на основі відображення Чирікова. Проаналізовано та

визначені недоліки методу шифрування растрових зображень з незалежними етапами дифузії і перестановки та показано можливість розкриття шифру.

Запропоновано спосіб шифрування стійкий до атаки вибраним відкритим текстом, в якому ключ перестановки визначається результатом дифузії. Для перестановок пікселів пропонується використання удосконаленого двовимірного відображення Чирікова.

В розділі розроблено метод захисту зображень на основі перестановок пікселів, що базуються на модифікованому відображенні Чирікова та дифузії кольору пікселів шляхом шифрування бінарними псевдовипадковими послідовностями, генерованими розробленими генераторами псевдовипадкових послідовностей.

У ***висновках*** викладено найважливіші наукові та практичні результати, які одержані в дисертації.

***Список використаних джерел*** оформлений згідно з вимогами стандарту та складається з 125 найменувань наукової літератури за темою дисертації.

***Додатки*** містять: акти впровадження результатів дисертаційної роботи, список публікацій здобувача за темою дисертації та відомості про апробацію результатів дисертації

**Ступінь обґрунтованості наукових положень, висновків і рекомендацій, сформульованих в дисертації.**

Викладені в дисертації наукові положення, а також висновки та рекомендації є практико-теоретичними положеннями, які перевірені обчислювальними та практичними експериментами.

Обґрунтованість та достовірність отриманих результатів дисертаційного дослідження, висновків та рекомендацій підтверджується узгодженістю теоретичних розрахунків та результатів моделювання із експериментально отриманими даними.

**До основних нових наукових результатів**, які одержані в дисертаційній роботі, можна віднести:

1. Вперше запропоновано метод синтезу псевдовипадкових послідовностей на основі багатовимірних відображень із кільцевим зв'язком, що відрізняється від відомих використанням найменш значущих збалансованих бітів, що дало змогу формувати великі ансамблі послідовностей, які доцільно використовувати в радіотехнічних пристроях та засобах телекомунікацій.

2. Вперше запропоновано метод збільшення періоду реалізацій хаотичних систем шляхом підвищення їх розмірності, який відрізняється від існуючих урахуванням кореляційної розмірності нелінійної динамічної системи та дає змогу передбачити середню тривалість періоду повторення послідовностей.

3. Удосконалено метод генерування псевдохаотичних послідовностей на основі програмної реалізації математичних моделей мемристивних хаотичних систем, який відрізняється від існуючих обгрунтованим використанням чисельного методу інтегрування Ейлера, що дає змогу збільшити швидкість генерування цих послідовностей при збереженні однакової середньої довжини періоду повторення та статистичних характеристик.

4. Удосконалено двовимірне відображення Чирікова шляхом введення додаткової нелінійності, що дало змогу збільшити потужність простору ключів перестановок для відповідних матриць.

**Повнота викладення результатів дисертаційних досліджень в опублікованих працях здобувача.**

Основні результати дисертаційної роботи викладені у 15 наукових працях (6 статей, 9 тез доповідей). Всі статті у фахових виданнях України та в іноземних наукових періодичних виданнях, які включені до міжнародних наукометричних баз: 3 - Index Copernicus, 6 - Google Scholar. З них 2 англомовні роботи, а також 9 матеріалів та тез доповідей міжнародних науково-практичних конференцій.

Таким чином, кількість та якість наукових робіт здобувача з теми дисертації відповідають вимогам МОН України до дисертацій на здобуття наукового ступеня кандидата технічних наук.

**Оцінка мови та стилю викладання дисертації та автореферату.**

Дисертація Круліковського О. В. написана з дотриманням прийнятої термінології, стиль викладення матеріалу забезпечує доступність його сприйняття спеціалістом, а науковий рівень дисертації відповідає існуючим вимогам до кандидатських дисертацій.

Зміст автореферату достатньо повно відображає основні положення, що викладені у дисертаційній роботі Круліковського О. В.

**Практичне значення** роботи полягає у:

- схемотехнічній реалізації генераторів випадкових сигналів на базі двовимірних відображень Лоці та Тратаса із кільцевим зв'язком;
- дослідженні періодичності розв'язків логістичного відображення при реалізації на ПЛІС із використанням арифметики з фіксованою комою;
- розробленні та реалізації апаратного рішення для генераторів псевдовипадкових послідовностей на базі ПЛІС, що уможливлює формування псевдовипадкових послідовностей на основі багатовимірних відображень із кільцевим зв'язком довільної розмірності;
- розробленні апаратного рішення методу генерування псевдохаотичних послідовностей на основі математичних моделей неперервних хаотичних систем з використанням в якості нелінійного елементу мемристивної структури.

Отримані в дисертаційній роботі наукові та практичні результати використовуються для формування цифрових хаотичних послідовностей на базі програмованих логікових мікросхем, зокрема для передавання інформаційних сигналів у системах зв'язку (ПАТ «Укртелеком»), при дослідженнях процесів формування хаотичних коливань на базі мемристивних структур (ОКБ «Рута»), а також впроваджені в навчальний процес на кафедрі радіотехніки та інформаційної безпеки Чернівецького національного університету імені Юрія Федьковича, що підтверджується відповідними актами впровадження. Все це дає змогу позитивно оцінити розглянуте дисертаційне дослідження, відзначити його наукову новизну та практичне значення, самостійність виконання та високий теоретичний рівень.

В цілому позитивно оцінюючи дисертаційне дослідження Круліковського О. В., необхідно зазначити наявність у ньому деяких дискусійних моментів та висловити наступні **зауваження**:

1. Хоча у першому розділі і проведено детальний аналіз моделей генераторів хаотичних коливань та здійснено аналіз можливостей їх застосування в телекомунікаційних системах, було б доречним навести визначення використаних в роботі термінів: детермінований хаос; атрактор; показник Ляпунова та зробити порівняльний аналіз властивостей періодичних, хаотичних та випадкових сигналів.

2. В 3 розділі дисертаційної роботи не деталізовано особливостей апаратної реалізації на ПЛІС розробленої математичної моделі мемристивної хаотичної системи за допомогою чисельного методу Рунге-Кутти.

3. В дисертаційній роботі приведені розроблені схеми генераторів сигналів Лоці і Тратаса, наведено перелік та значення параметрів елементів схем (резисторів, конденсаторів і т.п.), проте не вказано їх клас точності тобто допустимі відхилення від номінальних значень, що може суттєво впливати на роботу запропонованих генераторів.

4. На рис. 4.13 приведено фазові портрети, що відповідають гіперхаотичним режимам, а саме експериментальні осцилограми гіперхаотичних коливань сигналів системи Тратаса, проте з рисунку не зрозуміло масштаб величин на осях координат.

5. В 5 розділі дисертаційної роботи не наведено значення потужності простору ключів, відображення, що використано для перестановок пікселів.

6. Дослідження динамічних режимів багатовимірних систем Тратаса та Лоці, що наведені у розділі 4 п.4.1 необхідно було описати у розділі 3.1.

**Відповідність дисертації встановленим вимогам і загальні висновки.**

Дисертаційна робота Круліковського Олега Валерійовича «Синтез генераторів псевдовипадкових послідовностей на основі багатовимірних

нелінійних динамічних систем» відповідає паспорту спеціальності 05.12.13 – радіотехнічні пристрої та засоби телекомунікацій, та профілю спеціалізованої вченої ради Д 35.052.10.

Викладене дозволяє зробити загальний висновок, що дисертаційна робота «Синтез генераторів псевдовипадкових послідовностей на основі багатовимірних нелінійних динамічних систем» є завершеною кваліфікаційною науковою працею, що виконана автором особисто на належному рівні, яке вирішує актуальну наукову задачу та має наукову й практичну цінність.

Таким чином, дисертаційна робота «Синтез генераторів псевдовипадкових послідовностей на основі багатовимірних нелінійних динамічних систем» відповідає вимогам п.п. 9,11,12,13 "Порядку присудження наукових ступенів", затвердженого постановою Кабінету Міністрів України від 24 липня 2013 р. № 567 (із змінами, внесеними згідно з Постановою КМ № 656 від 19.08.2015р., №1159 від 30.12.2015р., та №567 від 27.07.2016 р.), а її автор, Круліковський Олег Валерійович заслуговує на присудження йому наукового ступеня кандидата технічних наук за спеціальністю 05.12.13 – радіотехнічні пристрої та засоби телекомунікацій.

ОФІЦІЙНИЙ ОПОНЕНТ

професор кафедри кібербезпеки та захисту інформації
факультету інформаційних технологій Київського
національного університету імені Тараса Шевченка
доктор технічних наук,
старший науковий співробітник В.С. Наконечний

Підпис засвідчую
Вчений секретар ННЦ
Караульна Н.В.
13.02.2017