

## **ВІДГУК**

### **офіційного опонента**

**доктора технічних наук, професора Бондаренка Олега Володимировича**  
на дисертацію Замули Олександра Андрійовича на тему: «Моделі і методи синтезу складних сигналів з необхідними властивостями для захищених телекомунікаційних систем», поданої на здобуття наукового ступеня доктора технічних наук за спеціальністю 05.12.02 – телекомунікаційні системи та мережі.

#### ***1. Актуальність теми***

Відповідно до основних положень Закону України «Про основи національної безпеки України», Концепції національної програми інформатизації та державних науково-технічних програм щодо створення перспективних телекомунікаційних систем й технологій, пріоритетними напрямками державної політики в інформаційній сфері є: розробка і впровадження перспективних методів та засобів захисту інформаційного простору України; створення необхідних засобів та режимів отримання, зберігання й використання інформації; створення розвинутої інфраструктури забезпечення її безпеки. Підвищення вимог до швидкого прийняття рішення і доведення до виконавців (користувачів) інформації в умовах внутрішніх і зовнішніх впливів, що обумовлені дією станцій (абонентів), що працюють у визначеному діапазоні частот, та станцій, що здійснюють цілеспрямовану протидію функціонуванню критичних додатків телекомунікаційної системи (ТКС), в значній мірі не враховується існуючими інформаційними технологіями. В ряді додатків телекомунікаційних систем для вирішення завдань інформаційної безпеки залучаються системи та засоби криптографічного захисту інформації, що потребує значних матеріальних витрат та здійснення сукупності організаційних, інженерно-технічних заходів та засобів. Одним з перспективних напрямів покращення показників ефективності ТКС, зокрема інформаційної безпеки, завадозахищеності, є застосування технології розширеного спектру, коли для передачі даних використовується смуга частот, що значно перевищує дійсно необхідну. Для реалізації цього напрямку створюють, зокрема, фазоманіпульовані широкосмугові сигнали-переносники даних, властивості яких цілком визначаються властивостями дискретних послідовностей, по закону яких маніпулюють фазу високочастотної несучої. При цьому необхідно відмітити,

що використовувані на сьогодні класи дискретних послідовностей не можуть забезпечити необхідні, особливо для ТКС критичного призначення, показники завадостійкості й структурної скритності (завадозахищеності), а також імітостійкості, інформаційної скритності (інформаційної безпеки). Вищезазначене дозволяє стверджувати, що в дисертаційній роботі розглядається дуже важлива і актуальна наукова проблема, що полягає у підвищенні завадозахищеності та інформаційної безпеки ТКС на основі удосконалення методологічних основ побудови ТКС, шляхом розробки методів інформаційного обміну, а також методів синтезу нових класів нелінійних дискретних складних сигналів з необхідними ансамблевими, кореляційними, структурними властивостями.

Таким чином, дисертаційна робота Замули О.А. є актуальною, оскільки спрямована на вирішення важливих для науки і практики проблем покращення перспективних методів та засобів захисту інформаційного простору нашої держави.

## ***2. Загальна характеристика роботи***

Дисертація складається із вступу, шести розділів, висновків, списку використаних джерел та додатків. Повний обсяг дисертації становить 438 сторінок друкованого тексту, у тому числі 10 сторінок – таблиць, 17 сторінок – перелік використаних джерел, що містить 150 найменувань, 123 сторінок додатків.

У першому розділі розв'язано наукову задачу проблеми дисертаційних досліджень, а саме: проведено аналіз сучасного стану і проблем теорії інформаційних комунікацій; наведено дослідження проблеми захищеності інформацій в ТКС; визначено чинники, що породжують проблему, яка сформульована; обґрунтовано вибір критеріїв і показників ефективності досліджуваних процесів.

У другому розділі дисертації розв'язано задачу проблеми досліджень і отримано два наукових результати, які пов'язані з розробкою методів синтезу систем нелінійних дискретних сигналів (НС) з поліпшеними властивостями.

У третьому розділі дисертації вирішені задачі дослідження і отримані наукові результати, що полягають в розробці методу синтезу систем складних нелінійних криптографічних дискретних сигналів із заданими властивостями.

У четвертому розділі дисертації розв'язані задачі проблеми досліджень і отримано наукові результати, що пов'язані з отриманням математичної моделі структури складних нелінійних сигналів та методу оцінки властивостей нелінійних дискретних сигналів.

У п'ятому розділі дисертації розглянуто принципи технічної реалізації модульних операцій в модулярній системі числення (МСЧ). Наведено три принципи технічної реалізації модульних операцій в МСЧ.

У шостому розділі дисертації вирішені задачі проблеми досліджень і отримано науковий результат, що відноситься до розробки удосконаленого методу інформаційного обміну на основі зміни (в процесі передачі даних) відповідності: біт повідомлення – складний сигнал і використання як фізичного переносника даних НС з необхідними властивостями.

### ***3. Ступінь обґрунтованості наукових положень, висновків і рекомендацій, сформульованих у дисертації***

Обґрунтованість основних положень дисертаційної роботи визначається, передусім, аргументованою постановкою задач досліджень, які демонструють комплексний підхід здобувача до пошуку шляхів вирішення наукової проблеми. Постановка і формалізація задач досліджень виконана з урахуванням повного набору чинників отриманих рішень, що впливають на коректність роботи. Вибір методів інформаційного аналізу структури фізичних переносників виконаний на основі глибокого вивчення їх властивостей і параметрів, що визначають часткові показники питомої ефективності комунікаційних протоколів фізичного рівня. У роботі використані математично коректні теоретичні і експериментально-обчислювальні методи, що базуються на фундаментальних визначеннях теорії інформації і інформаційних технологій, теорії інформаційної безпеки і потенційної завадостійкості, теорії систем сигналів, лінійної алгебри і дослідження операцій. Обґрунтованість сформульованих висновків і рекомендацій підкріплюється коректними аналітичними викладеннями, які в максимальній мірі позбавлені непотрібної громіздкості і легко піддаються перевірці. Особливо це стосується ключових викладень в другому, третьому, п'ятому розділах роботи, де, із залученням математичного апарату полів Галуа, знаходження оптимальних рішень задач дискретної і комбінаторної оптимізації, розділів теорії чисел (теорія порівнянь та теорія подільності). Для підтвердження обґрунтованості теоретичних результатів і висновків автор

використовував методи предметного імітаційного моделювання на основі моделей гауссових каналів. Формулювання основних результатів не суперечать фундаментальним висновкам статистичної теорії передачі і обробки інформації.

#### ***4. Достовірність результатів роботи***

Основним підтвердженням достовірності є збіг теоретичних результатів, отриманих в роботі аналітичними методами, з результатами експериментально-статистичних перевірок з використанням множини моделей, відомості щодо яких надано в додатках до роботи. Для підтвердження достовірності власних висновків автор використовував результати аналізу значної сукупності загальновизнаних джерел у вибраній предметній області. До показника достовірності можна віднести використання та впровадження отриманих наукових результатів на підприємствах промисловості і у вищих учбових закладах, що підтверджується актами впровадження.

#### ***5. Новизна одержаних результатів***

Новизна отриманих результатів полягає в розвитку теорії і методології побудови телекомунікаційних систем на основі розробки методів синтезу та оцінки властивостей систем нелінійних сигналів з покращеними властивостями, методів реалізації арифметичних операцій в медулярній системі числення, а також методу інформаційного обміну даними. Надана сукупність математичних моделей і методів, які складають теоретичні і методологічні основи структурної та функціональної побудови телекомунікаційних систем для покращення їх показників ефективності. Найбільш цінними, з точки зору новизни являються такі.

##### **Вперше отримано:**

- метод синтезу нелінійних криптографічних дискретних складних сигналів, який використовує випадкові (псевдовипадкові) процеси, і дозволяє створювати сигнали з необхідними ансамблевими, структурними та кореляційними властивостями, що дає можливість покращити показники завадозахищеності та інформаційної безпеки ТКС в умовах зовнішніх і внутрішніх впливів;

- математичну модель структури складних нелінійних дискретних сигналів у кінцевих полях, що визначає залежність характеристик елементів мультиплікативної групи поля Галуа і символів дискретних послідовностей, синтезованих з використанням характеристик елементів мультиплікативної групи поля, що дозволяє визначити значення показників завадозахищеності (структурної скритності) дискретних сигналів;

- метод реалізації арифметичних модульних операцій додавання і віднімання, заснований на табличному принципі реалізації арифметичних операцій за допомогою використання спеціального коду табличного множення, що дозволяє підвищити швидкодію виконання модульних операцій додавання і віднімання;

- метод реалізації арифметичної модульної операції множення, заснований на використанні табличного принципу шляхом використання процедури порозрядного визначення результату операції, що дозволяє підвищити швидкодію виконання модульних операцій модульного множення.

#### **Удосконалено:**

- метод синтезу нелінійних дискретних складних сигналів, у якому, на відміну від відомих, використовується залежність між елементами та індексами елементів кінцевого поля, що дозволяє підвищити швидкодію синтезу сигналів;

- метод синтезу нелінійних дискретних складних сигналів, у якому, на відміну від відомих, використовуються механізми спрямованого (обмеженого) перебору сигналів для відбору сигналів, які відповідають певним вимогам, що дозволяє підвищити продуктивність синтезу системи сигналів з необхідними властивостями;

- метод оцінки властивостей нелінійних дискретних складних сигналів, у якому на відміну від відомих, використано алгебраїчні властивості елементів кінцевого поля, що дозволяє збільшити швидкодію процесу дослідження властивостей сигналів, і, таким чином, підвищити продуктивність синтезу системи сигналів з необхідними властивостями;

- метод синтезу всієї системи нелінійних дискретних сигналів, у якому, на відміну від відомих, використовується процедура зчитування та запису (за певним правилом) символів сигналу для формування всієї множини сигналів, що відноситься до цієї системи сигналів, що дозволяє підвищити продуктивність їх синтезу;

- метод інформаційного обміну даними, в якому, на відміну від відомих, застосовується зміна відповідності: біт повідомлення - складний сигнал і, як складні сигнали, застосовуються нелінійні дискретні сигнали з необхідними ансамблевими, структурними та кореляційними властивостями, що дозволяє покращити показники інформаційної безпеки та завадозахищеності;

- метод реалізації арифметичних модульних операцій додавання і віднімання, який, на відміну від відомих, заснований на використанні принципу кільцевого зсуву, за допомогою представлення залишків числа двійковим кодом, за рахунок використання властивостей циклічних перестановок вмісту кільцевого регістра, що дозволяє підвищити швидкодію виконання модульних операцій.

На основі розроблених та удосконалених в дисертації методів синтезу систем нелінійних дискретних складних сигналів, а також методів швидкої реалізації модульних операцій, в роботі надано алгоритми для їх реалізації, у відповідності з якими синтезовано клас апаратних засобів формування і обробки даних, на які отримано 14 авторських свідоцтв про винаходи та патентів України на корисну модель, що підтверджує новизну та практичну значущість отриманих в дисертації наукових результатів.

## ***6. Повнота викладу основних наукових результатів у опублікованих працях.***

Основні наукові результати, які отримані в роботі, в належній мірі опубліковані в 73 наукових працях, в тому числі: 1 - монографія, 40 - наукових статей, 14 - авторські свідоцтва на винаходи та патенти України. Основні результати досліджень доповідались і були схвалені на 14 - ти міжнародних форумах і міжнародних науково-технічних конференціях. Результати досліджень відображені в 6 звітах про НДР.

Зміст автореферату, в частині основних положень і результатів, зроблених висновків та запропонованих рекомендацій достатньою мірою відображає зміст дисертації.

## ***7. Відповідність дисертації встановленим вимогам***

Дисертація написана сучасною науково-технічною мовою, послідовно та логічно. Оформлення дисертації відповідає вимогам, що пред'являються

до дисертаційних робіт, та вимогам Постанови КМУ від 24.07.2013 р. № 567, а також зі змінами і доповненнями №656 від 19.08.2015 р. та №1159 від 30.12.2015 р до цієї Постанови. Автореферат достатньо повно та ідентично розкриває зміст дисертації, адекватно висвітлює зміст роботи. Стиль викладу матеріалів досліджень, наукових положень, висновків і рекомендацій забезпечує доступність їх сприйняття.

### ***8. Зауваження до дисертаційної роботи***

До недоліків роботи можна віднести наступні:

1. В 5-му розділі дисертації були розглянуті методи швидкої обробки сигналів на основі використання медулярної системи числення (МСЧ). Однак при цьому не були розглянуті фактори, що обумовлюють процес швидкої реалізації цифрової обробки даних. Так, в розділі не визначено, за рахунок яких характеристик системи обробки даних (СОД), наприклад, об'єму обладнання, досягають підвищення швидкодії. Вищезазначені обставини не дозволяють комплексно (системно) оцінити переваги застосування методів реалізації арифметичних операцій в МСЧ, що запропоновані в роботі.

2. Відомо, що однією з складових завадозахищеності ТКС є енергетична скритність системи (і це відзначається в роботі). При радіоелектронній протидії ефективна завада може бути організована тільки після виявлення присутності скритної системи в ефірі та оцінки таких її параметрів як частотний діапазон, смуга частот, яку займає сигнал. Якщо параметри сигналу-фізичного переносника даних не відомі станції протидії, остання мусить розглядати сигнал, що перехоплює, у вигляді випадкового і оснований його виявлення тільки на факті появи або відсутності деякого надлишку енергії в діапазоні частот, який є найбільш очікуваним для станції протидії. В дисертаційній роботі (у четвертому розділі) наводяться результати досліджень ансамблевих, кореляційних, структурних властивостей сигналів, методи синтезу яких наведено у другому та третьому розділах дисертації. Було б доцільно (у зазначеному контексті, тобто для оцінки енергетичної скритності системи) провести дослідження спектральних властивостей систем складних сигналів, що запропоновані в роботі.

3. В роботі не досить коректно визначено поняття «необхідні» властивості сигналів, і яким чином визначаються ті самі «необхідні»

властивості сигналів при їх застосуванні в телекомунікаційних системах при вирішенні задач підвищення показників ефективності системи. На наш погляд, було б цілком вірним, якщо під необхідними властивостями розуміти можливість варіювати, наприклад, в залежності від вимог, які висуваються до системи, властивостями застосовуваної системи сигналів. Цілком зрозуміло (і це відзначається в роботі), що одночасне рішення задач з досягнення показників, наприклад, імітостійкості та завадостійкості, може бути суперечливим. Тому власник системи (інформації) повинен знаходити компромісне рішення зазначених задач при застосуванні сигналів-фізичних переносників інформації з відповідними (необхідними) кореляційними, ансамблевими та ін. властивостями. Наприклад, коли висуваються досить жорсткі умови щодо показника імітостійкості функціонування системи, повинні бути застосовані системи сигналів, що мають покращені ансамблеві властивості, при цьому можуть бути знижені (не суттєво) вимоги до кореляційних властивостей сигналів (тобто - завадостійкості).

4. В дисертаційній роботі (в розділі 6) надано опис та теоретичне обґрунтування методу інформаційного обміну даними в ТКС на основі зміни відповідності: біт повідомлення-складний нелінійний сигнал. Застосування цього методу, як показано в роботі, забезпечує досягнення мети дисертаційних досліджень, - підвищення показників ефективності телекомунікаційної системи, а саме: захист від нав'язування хибних повідомлень (імітостійкість), інформаційну та структурну скритність системи. Однак, в наданих матеріалах не наведено відомості щодо аспектів практичної реалізації запропонованого методу (апаратна реалізація пристроїв, що реалізують відповідні етапи методу, характеристика пристроїв (об'єм пам'яті, що необхідний для формування і зберігання форм складних сигналів; продуктивність пристроїв формування та обробки даних для реалізації методу у реальному часі тощо)).

5. В дисертаційній роботі розроблено і наведено (у відповідних додатках дисертації) програмне забезпечення (ПЗ), яке реалізує запропоновані методи синтезу систем нелінійних дискретних сигналів, теоретичні основи яких отримано в ході дисертаційних досліджень, а також ПЗ, яке використовується для дослідження властивостей синтезованих систем нелінійних дискретних сигналів. Було б доцільно навести загальні характеристики ПЗ, що було розроблено в ході дисертаційних досліджень.



6. В дисертаційній роботі вперше отримано та удосконалено низку методів, що мають на меті підвищення швидкодії арифметичних операцій, що виконуються під час формування та обробки сигналів (розділ 5), а також методів синтезу та дослідження властивостей систем сигналів (розділи 2-4), які забезпечують підвищення продуктивності синтезу систем сигналів. У відповідних розділах наведено вигоди, що може бути отриманий при застосуванні цих методів. При цьому відсутні інтегральні оцінки позитивного ефекту (з точки зору, швидкодії та продуктивності), що може бути досягнутий при комплексному впровадженню усіх вищезазначених методів.

7. В дисертації і авторефераті багато не загальноприйнятих скорочень, що ускладнює труднощі в сприйнятті матеріалу.

Вказані недоліки не знижують загального позитивного враження від роботи.

## **9. Висновки**

1. Дисертаційна робота Замули Олександра Андрійовича є завершеною самостійною науковою працею, в якій отримано науково обґрунтовані результати, що в сукупності дозволяють вирішити важливу і актуальну науково-прикладну проблему, що полягає у підвищенні завадозахищеності та інформаційної безпеки телекомунікаційної системи (ТКС) на основі удосконалення методологічних основ побудови ТКС, шляхом розробки методів інформаційного обміну, а також методів синтезу нових класів нелінійних дискретних складних сигналів з необхідними ансамблевими, кореляційними і структурними властивостями.

2. Дисертація відповідає спеціальності 05.12.02 – телекомунікаційні системи та мережі.

3. Матеріали дисертації достатньо апробовані, доповідались на українських і міжнародних конференціях, висвітлені в 73 наукових публікаціях, з них: 1 монографія, 40 статей, 14 тез доповідей та інше.

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

5. Структура дисертації (поділ на розділи та підрозділи) є обґрунтованою.

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

7. Робота відповідає вимогам до докторських дисертацій згідно п. 9, 10, 12-14 «Порядку присудження наукових ступенів», а здобувач заслуговує присудження наукового ступеня доктора технічних наук за спеціальністю 05.12.02 – телекомунікаційні системи та мережі.

Офіційний опонент:

проректор з навчальної роботи

Одеської національної академії

зв'язку ім. О. С. Попова

доктор технічних наук, професор

 О.В. Бондаренко

“09” 03 2016 р.

