Голові спеціалізованої вченої ради
Д 64.820.01

**61050, м. Харків, пл. Фейєрбаха, 7**

**ВІДГУК**

офіційного опонента
на дисертаційну роботу ЗАМУЛИ Олександра Андрійовича
«Моделі і методи синтезу складних сигналів з необхідними властивостями для захищених телекомунікаційних систем»,
представлену на здобуття наукового ступеня доктора технічних наук
за спеціальністю 05.12.02 – телекомунікаційні системи та мережі

**Актуальність теми дисертаційної роботи та її зв'язок роботи з науковими програмами, планами, темами.**

Найважливішою компонентою великого переліку інформаційних технологій є комплекс взаємозв'язаних процесів забезпечення віддаленої взаємодії об'єктів інформаційних систем, що реалізовує операції обробки і передачі інформації. При прогресуючому рості навантажень інформаційного трафіку особливо важливим є подолання протиріччя між зростаючими вимогами до продуктивності телекомунікацій і природними фізичними обмеженнями реальних каналів з завадами. Ці обмеження є наслідком зростаючого числа інформаційних систем, одночасно працюючих в єдиному інфокомунікаційному просторі. Перевантаженість ефіру при явно недостатньому задоволенні потреб мереж передачі даних може стати причиною кризи в розвитку розподілених інформаційно-управляючих систем. Найбільш відповідальними і проблемними рівнями інформаційних протоколів взаємодії відкритих систем є технології канального і фізичного рівнів. Міра значущості цих рівнів визначається наявністю обмеженої пропускної спроможності реальних каналів передачі інформації, що функціонують в умовах дефіциту доступного енергетичного і частотного ресурсу. При цьому найважливішим параметром, що визначає показники ефективності технологій інформаційного обміну, являється рівень питомих частотних і енергетичних витрат, необхідних для забезпечення необхідної якості комунікації. Виникає протиріччя між жорсткими вимогами щодо забезпеченням достовірності, конфіденційності, цілісності, істинності даних, що зберігаються та передаються по проводових та безпроводових лініях зв’язку телекомунікаційних систем, з одного боку, та існуючими моделями, методами та технологіями управління те-

лекомунікаційними мережами, інформаційною безпекою, послугами та якістю обслуговування, з іншого боку. Вищезазначене, насамперед, обумовлено тим, що в процесі інформаційного обміну протягом тривалого часу відповідність: біт повідомлення–сигнал (фізичний переносник інформації) є фіксованим, а в якості сигналів застосовують так звані лінійні класи сигналів, які мають обмежені ансамблеві, структурні, кореляційні властивості, що не дозволяє забезпечувати у ряді додатків телекомунікаційних систем (ТКС) необхідні показники ефективності функціонування системи. На сьогодні на практиці існує гостра необхідність в нових наукових принципах та технологічних рішеннях, здатних задовольнити зростаючі вимоги до систем передачі даних в телекомунікаційних системах, насамперед, критичного призначення щодо ефективного використання мережевого ресурсу зв'язку. У зв’язку з вищенаведеним тема роботи, що розглядається, бачиться досить актуальною.

Автором розв'язана важлива наукова проблема, яка полягає в 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 і структурними властивостями. Дослідження, результати яких викладені в дисертації, проводились згідно з державними планами НДР, програмами та договорами, які виконуються в Харківському національному університеті імені В.Н. Каразіна та Харківському національному університеті радіоелектроніки.

**Ступінь новизни, обґрунтованості та достовірності наукових положень, висновків і рекомендацій, сформульованих у дисертаційній роботі.**

У дисертаційній роботі Замули О.А. отримано такі основні науково обґрунтовані результати:

- уперше 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;

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

- уперше отримано 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;

- уперше отримано 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, використовуються механізми спрямованого (обмеженого) перебору сигналів для відбору сигналів, які відповідають певним вимогам, що дозволяє підвищити продуктивність синтезу системи

- удосконалено 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 синтезу сигналів;

- удосконалено 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;

- удосконалено 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 та ін.

Обґрунтованість отриманих результатів виходить з аргументованого використання апробованих методів теорії інформації і захисту інформації, теорії потенційної завадостійкості, теорії вірогідності і випадкових процесів, теорії систем сигналів і оптимальних методів прийому сигналів, математичних методів оптимізації і дослідження операцій.

Аналітичні оцінки, які отримані автором, підкріплені відповідними викладеннями.

Слід зазначити прагнення автора до повного обліку усіх чинників, що впливають на ефективність отримуваних рішень. У роботі використано математично коректну постановку цілого ряду оптимізаційних завдань, які вирішено у

рамках дисертаційних досліджень. Додатковим обґрунтуванням отриманих виводів і рекомендацій, поза сумнівом, являються результати імітаційного моделювання, які надано в додатках до роботи.

Основні результати роботи не суперечать фундаментальним положенням теорії інформації, теорії захисту інформації та теорії потенційної завадостійкості. Головним підтвердженням достовірності результатів є збіг теоретично отриманих результатів з даними численних моделей, а також повторюваність результатів для різних умов проведення обчислювальних експериментів. Достовірність результатів підтверджена практичним застосуванням їх на підприємствах промисловості і в учбовому процесі, про що свідчать представлені акти впровадження. До позитивних якостей викладу матеріалу в дисертації слід віднести численні кількісні оцінки приросту часткових показників ефективності інформаційного обміну.

**Практичне значення наукових положень, висновків і рекомендацій, сформульованих у дисертації.**

Практичні результати дисертаційного дослідження можуть використовуватись для синтезу складних сигналів з необхідними властивостями для захищених телекомунікаційних систем.

Також практична значимість підтверджена чотирма актами впровадження результатів наукових досліджень.

**Повнота викладення наукових і прикладних результатів дисертації в опублікованих роботах.**

Наукові результати дисертаційних досліджень Замули О.А. опубліковані у 73 друкованих роботах, зокрема у монографії та 40 статтях у наукових спеціалізованих виданнях, затверджених Міністерством освіти і науки України, з яких більшість входить до міжнародних науково метричних баз. Основні результати дисертаційної роботи у цих публікаціях відображено достатньо повно, а в авторефераті наведено лише основні з них.

**Відповідність дисертаційної роботи спеціальності.**

Дисертаційна робота відповідає формулі паспорту спеціальності 05.12.02 – телекомунікаційні системи та мережі (технічні науки), оскільки вона спрямована на розроблення і дослідження моделей і методів синтезу складних сигналів з необхідними властивостями для захищених телекомунікаційних систем.

Об’єкт та предмет дослідження, мета дослідження відповідають паспорту спеціальності 05.12.02 – телекомунікаційні системи та мережі.

**Рекомендації щодо використання результатів дисертації.**

Розроблені та обґрунтовані в дисертаційній роботі моделі та методи можуть бути рекомендовані для синтезу складних сигналів з необхідними властивостями для захищених телекомунікаційних систем.

**Оцінка змісту дисертації, її завершеності й оформлення.**

Побудова дисертації відповідає прийнятим для наукового дослідження нормам. Дисертація складається із вступу, шости розділів, висновків по дисертації, списку використаної літератури та додатків. Повний обсяг дисертації складає 438 сторінок, у тому числі: 298 сторінок основного тексту (включаючи 10 таблиць на окремих листах), бібліографія зі 150 найменувань на 17 сторінках та додатки на 123 сторінках. Таким чином, обсяг дисертаційної роботи відповідає нормам, встановленим для докторських дисертацій з технічних наук.

Усі положення, винесені на захист, висвітлені в тексті дисертації. Зміст дисертаційної роботи відповідає її назві.

Дисертація написана грамотною науковою мовою та оформлена відповідно до існуючих нормативних документів, текст і графічний матеріал виконані акуратно з використанням комп'ютерної техніки.

Зміст автореферату повністю відповідає змісту дисертації і достатньо повно відбиває її основні положення.

**Зауваження та недоліки.**

В процесі ознайомлення з роботою виникли такі зауваження та недоліки:

1. В дисертаційній роботі наведено аналіз та відповідні розрахунки стосовно застосування динамічного режиму передачі даних, коли з часом змінюється відповідність: біт повідомлення - складний сигнал, для вирішення, насамперед, задач покращення показників інформаційної безпеки (а саме, імітостійкості). Однак, впровадження такого методу інформаційного обміну може забезпечити й вирішення задач підвищення показників іншої складової інформаційної безпеки - інформаційної скритності (або криптографічної стійкості) телекомунікаційної системи. Було б доцільно провести дослідження й в цьому напрямку.

2. В роботі запропонована система кількісних та якісних критеріїв оцінки ефективності функціонування телекомунікаційної системи. Було б доцільно ввести й інтегральні критерії - умовні та безумовні, для оцінки інформаційної безпеки, завадозахищеності, продуктивності тощо.

3. В дисертаційній роботі наведено достатньо глибокий аналіз кореляційних властивостей систем сигналів, теоретичні основи синтезу яких запропоновано в роботі. При цьому досліджені авто- взаємно- та стикові кореляційні властивості в періодичному та аперіодичному режимах передачі сигналів. І це, безумовно, є важливим, з точки зору, оптимізації сигнально-кодових структур для забезпечення необхідних показників завадостійкості прийому сигналів в телекомунікаційних системах. Однак, в роботі недостатньо уваги приділено дослідженню кореляційних властивостей у частотній області. Це є особливо актуальним, якщо в каналі присутні нелінійності.

4. В роботі є досить оригінальними дослідження кореляційних властивостей систем сигналів, методи синтезу яких отримано в ході дисертаційних досліджень, в частині пошуку таких представників нелінійних сигналів, що мають нульові бокові пелюстки поблизу центрального піку кореляційних функцій. Однак, потребує більш детального дослідження ймовірнісний розподіл саме таких бокових пелюстків.

5. В дисертаційній роботі запропоновано метод синтезу нелінійних складних сигналів, який, у порівнянні з відомими методами, забезпечує значний виграш у швидкої при синтезі сигналів. Однак, аналіз етапів реалізації метода, свідчить, що формування сигналів здійснюється, по суті, після реалізації етапу формування елементів кінцевого поля. А чи досліджувалася можливість формування сигналів послідовно? Якщо це є можливим, то виграш у продуктивності синтезу системи сигналів був би ще більш значним.

6. Аналіз наданих в дисертації матеріалів досліджень дозволяє переконатися в тому, що застосування запропонованих в роботі систем нелінійних сигналів дозволить покращити показники завадозахищеності (структурної скритності та завадостійкості), інформаційної безпеки (імітостійкості та інформаційної скритності) каналів зв'язку телекомунікаційних систем. Однак, в системі, в якій реалізуються визначені в роботі принципи інформаційного обміну, є необхідним забезпечити тактову та циклову синхронізацію. Тому в роботі необхідно було б провести обґрунтування класів дискретних сигналів, які повинні буди застосовані з метою синхронізації сторін інформаційного обміну.

7. В дисертаційній роботі обґрунтовується необхідність покращення показників інформаційної безпеки та завадозахищеності телекомунікаційних систем на базі безпроводових ліній зв'язку в умовах зовнішніх та внутрішніх впливів на систему. Було б доцільним виконати оцінки вищезазначених показників саме в умовах конкретно визначених зовнішніх і внутрішніх завад (впливів).

8. В дисертаційній роботі запропоновано методи реалізації модульних операцій додавання (віднімання), які застосовують різні принципи виконання операцій (табличний принцип реалізації арифметичних операцій за допомогою використання спеціального коду табличного множення та принцип кільцевого зсуву, за допомогою представлення залишків числа двійковим кодом). На жаль, в роботі не наведено обмеження та рекомендації щодо застосування того чи іншого метода в системах обробки даних для підвищення швидкодії виконання вищезазначених арифметичних операцій.

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

Незважаючи на вищезазначені недоліки та зауваження, можна зробити висновок про те, що дисертаційна робота Замули Олександра Андрійовича «Моделі і методи синтезу складних сигналів з необхідними властивостями для

захищених телекомунікаційних систем» є завершеним дослідженням, в якому отримані нові науково обґрунтовані результати, що в сукупності містить закінчене рішення актуальної науково-прикладної проблеми, яка полягає у підвищенні завадозахищенності та інформаційної безпеки телекомунікаційних систем. Результати дисертаційного дослідження в сукупності є суттєвими для розвитку теорії та практики завадозахищенності у телекомунікаційних мережах. Розглянута дисертаційна робота відповідає вимогам пп. 9, 10, пп. 12 – 14 «Порядку присудження наукових ступенів і присвоєння вченого звання старшого наукового співробітника», затвердженого постановою Кабінету Міністрів України від 24 липня 2013 р. № 567, що ставляться до докторських дисертацій, а її автор – Замула Олександр Андрійович, заслуговує присудження наукового ступеня доктора технічних наук за спеціальністю 05.12.02 – телекомунікаційні системи та мережі.

Офіційний опонент
провідний науковий співробітник наукового центру Повітряних Сил
Харківського університету Повітряних Сил імені Івана Кожедуба
доктор технічних наук
професор Г.А. КУЧУК

“ 25 ” лютого 2016 р.

Підпис Кучука Г.А. засвідчую.

ТВО начальника штабу – першого заступника
начальника Харківського університету Повітряних Сил
А.А. ЛУК’ЯНЧИКОВ

“ 25 ” лютого 2016 р.

Вхідний № 02/02-16
“ 26 ” лютого 2016 р.
УкрДУЗТ