Голові спеціалізованої вченої ради
Д 64.820.01
в Українському державному
університеті залізничного транспорту
м. Харків, майдан Фейєрбаха, 7

**ВІДГУК**

офіційного опонента
доктора технічних наук, професора Климаша Михайла Миколайовича 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

**Актуальність теми**

В умовах розвитку сучасних технологій, введення в експлуатацію нових систем управління і зв'язку, а також розвитку комп'ютерних та інформаційних технологій, створюється єдиний інформаційно-телекомунікаційний простір України, відбувається поступовий перехід систем зв'язку і автоматизації на сучасні цифрові способи передачі і обробки інформації, здійснюється автоматизація процесів управління. Причому вимоги до цілісності, достовірності, конфіденційності, істинності в процесі зберігання, передачі і обробки інформації постійно підвищуються, особливо в системах критичного призначення державного та регіонального рівня. Виконання даних вимого нерозривно пов'язане з необхідністю узагальнення вже накопиченого світового досвіду у сфері інфокомунікацій і цілком залежить від ступеня впровадження передових інформаційних технологій передачі і обробки інформації. Бурхливе зростання інфокомунікацій і постійний розвиток технічних засобів їх забезпечення сприяють тому, що постановка завдань управління телекомунікаційними мережами, трафіком, інформаційною безпекою, послугами та якістю обслуговування істотно змінюються. Між тим, такі показники ефективності телекомунікаційних систем (ТКС), як завадозахищеність, інформаційна безпека, в суттєвій мірі, залежать від властивостей фізичних переносників інформації — сигналів. Відомо, що в сучасних ТКС використовують сигнали, що засновані на, так званих, лінійних правилах побудови і в процесі передачі даних відповідність:

біт повідомлення – сигнал є фіксованою. Вищезазначене не дозволяє забезпечити, особливо в критичних додатках ТКС, вимоги щодо захисту від введення в систему хибних повідомлень, порушення конфіденційності даних, визначення порушником структури (правила побудови) сигналу, а також вимоги щодо завадостійкості прийому сигналів в умовах дії природних та штучно створених різноманітних завад. Тому можна вважати, що тема дисертаційної роботи Замули О.А. та науково-прикладна проблема, що вирішується і пов'язана з підвищенням 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, є актуальними.

**Оцінка змісту і загального рівня роботи. Новизна наукових результатів, що одержані.**

У рамках сформульованої проблеми здобувач визначив дев'ять основних завдань досліджень, рішення яких послідовно викладається в матеріалах дисертації. Слід зазначити, що виклад матеріалу в роботі побудований з урахуванням дотримання строгого логічного взаємозв'язку окремих компонент досліджень, що, поза сумнівом, є позитивною якістю дисертації. Викликає схвалення широке використання автором досить оригінальних математичних прийомів. Усе це, за наявності безлічі конкретних програмних моделей, свідчить про достатню повноту вирішення наукової проблеми і досягнення поставленої в роботі мети.

Наукові результати, що надані в дисертації утворюють сукупність моделей та методів, які умовно можна розділити на три групи.

Перша група об'єднує результати, що дозволяють безпосередньо констатувати, що при їх застосуванні забезпечується підвищення показників ефективності функціонування ТКС, а саме, завадостійкості, структурної та інформаційної скритності, імітостійкості. До цієї групи результатів можна віднести 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;

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;

До другої групи наукових результатів можна віднести результати, що мають на меті удосконалення існуючих моделей та методів синтезу

нелінійних складних дискретних сигналів, а також дослідження властивостей систем сигналів. Застосування вищезазначених результатів дозволить виконувати оцінку властивостей запропонованих в роботі систем сигналів, а також підвищити продуктивність синтезу сигналів, що надає можливість реалізовувати динамічну зміну відповідності: біт повідомлення – складний сигнал у реальному часі і, таким чином, покращити показники завадозахищеності та інформаційної безпеки ТКС. До таких результатів можна віднести такі.

Вперше 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 поля, що дозволяє визначити значення показників завадозахищеності (структурної скритності) дискретних сигналів.

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 криптографічних 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 синтезу сигналів.

До третьої групи наукових результатів можна віднести сукупність методів реалізації арифметичних операцій, які виконуються в процесі формування обробки даних.

Вперше 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;

- метод реалізації арифметичної модульної операції множення, заснований на використанні табличного принципу шляхом застосування

процедури порозрядного визначення результату операції, що дозволяє підвищити швидкодію виконання модульних операцій модульного множення.

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.

Ця проблема повністю відповідає напрямам, вказаним в паспорті спеціальності 05.13.06 – інформаційні технології.

**Обгрунтованість і достовірність результатів** сумнівів не викликає, оскільки автор у своїх міркуваннях спирається на загальноприйняті положення теорії інформації і теорії захисту інформації, теорії чисел та теорії груп, кілець, полів, приводить досить прозорі математичні докази і широко використовує методи моделювання і обчислювального експериментування.

Основні результати дисертації опубліковані в 73 наукових працях, вони неодноразово обговорювалися на різних конференціях і форумах і отримали схвалення провідних фахівців. Наукова новизна технічних рішень підтверджена 14 авторськими свідоцтвами і патентами. Обгрунтованість результатів, висунутих здобувачем, ґрунтується на узгодженості даних експериментів і наукових висновків. Достовірність результатів роботи підтверджується коректним використанням теоретичних і експериментальних методів обґрунтування отриманих результатів, висновків і рекомендацій. Достовірність експериментальних даних забезпечується використанням сучасних засобів і методик проведення досліджень.

**До числа недоліків роботи можна віднести наступні.**

1. В дисертації як метод швидкої обробки даних, наданий табличний метод обробки даних в медулярній системи числення (МСЧ). При цьому, передбачається єдиний підхід для різних по значенню модулів (основ) МСЧ. На наш погляд при реалізації значних по значенню модулів (наприклад, $m \geq 53$) можна було б застосувати багатоступеневу МСЧ. Такий підхід сприяв би зниженню кількості логічних елементів таблиць модульного складання (віднімання) та множення. Це, у свою чергу, сприяло б зниженню кількості обладнання системи обробки даних телекомунікаційної системи.

2. В дисертації цілком слушно, з метою підвищення продуктивності процесу синтезу системи нелінійних дискретних сигналів, запропоновано використання методу «гілок та границь». Дійсно, суть методу полягає у використанні обмеженості множини рішень і заміні їх повного перебору обмеженим перебором і, таким чином, в находженні оптимальних рішень різноманітних задач оптимізації, в тому числі, дискретної та комбінаторної оптимізації. В роботі отримані результати, які свідчать, що застосування такого підходу дійсно приводить до виграшу в продуктивності синтезу сигналів. При цьому необхідно зазначити, що традиційно метод «гілок та границь» використовують для задач з цільовою функцією, що цілком

залежить від шуканих змінних. Однак в роботі не достатньо обґрунтована лінійність цільової функції по відношенню до систем нелінійних сигналів.

3. В дисертаційній роботі показано, що при застосуванні в системі запропонованого методу інформаційного обміну даними та систем нелінійних сигналів, методи синтезу яких отримані здобувачем, можуть бути покращені такі показники ефективності телекомунікаційної системи, як імітостійкість, завадостійкость, структурна скритність та ін. При цьому не наведено будь-яких відомостей відносно можливих втрат, вартості впровадження запропонованих методів інформаційного обміну даними та систем нелінійних сигналів.

4. В дисертаційній роботі наведено результати порівняльного аналізу властивостей (ансамблевих, кореляційних, структурних) запропонованих в роботі систем нелінійних складних сигналів з властивостями систем лінійних сигналів. При цьому, на наш погляд, розглянутий обмежений спектр можливих сигналів. Мається на увазі, що нелінійні сигнали, їх властивості, порівнюються з властивостями М-послідовностей, множин Голда, Касамі та деяких інших. При цьому було б доцільно, на наш погляд, провести порівняльний аналіз синтезованих в роботі систем сигналів з такими класами сигналів, як сигнали, що засновані на використанні властивостей циклічних орбіт групових кодів, сигнали Рида-Мюллера, Диджилок та ін.

5. Відомо, що в теорії зв’язку найбільш розповсюдженою моделлю каналу зв’язку є канал з адитивним білим гаусівським шумом. Такий підхід є адекватним, коли має місце передача даних з використанням амплітудної або амплітудно-фазової модуляції, коли ймовірність помилки залежить від відношення потужності сигналу до потужності загального впливу завад, що припускає можливість апроксимації впливу завад гаусівським законом. Але можливі інші ситуації (М-ічна передача даних, оцінка параметрів сигналу, вплив структурних завад тощо), коли показники якості прийому сигналів визначаються не лише значенням відношення вищезазначених потужностей. Ці питання, на наш погляд, не знайшли достатньо глибокого розгляду та оцінки в і дисертаційній роботі.

6. В дисертаційній роботі достатньо докладно викладено питання щодо формування систем нелінійних сигналів, теоретичні основи синтезу яких отримано в ході дисертаційних досліджень. При цьому в роботі не достатньо висвітлені питання, щодо оптимальної обробки таких сигналів-фізичних переносників даних при їх прийомі одержувачем. Було б важливим розробити протокол інформаційного обміну, який би містив перелік параметрів, які необхідні для того, щоб станція -одержувач мала можливість формувати копії можливих сигналів для прийому сигналів при кореляційній обробки (узгодженій фільтрації) в прийомній частині телекомунікаційної системи. Крім того, було б доцільно визначити механізми захисту зазначених параметрів протоколу від можливості несанкціонованого впливу на них з боку порушника.

Незважаючи на вищезазначені недоліки робота, в цілому, справляє цілком позитивне враження.

**Висновок.**

Дисертаційна робота Замули Олександра Андрійовича являє собою закінчене вирішення актуальної науково-прикладної проблеми. Зміст роботи та отримані результати відповідають паспорту спеціальності 05.12.02 – телекомунікаційні системи та мережі. Автореферат з необхідною повнотою відображає зміст дисертації. Робота відповідає вимогам до докторських дисертацій згідно п. 9, 10, 12-14 «Порядку присудження наукових ступенів і присвоєння вченого звання старшого наукового співробітника», а здобувач заслуговує присудження наукового ступеня доктора технічних наук за спеціальністю 05.12.02 – телекомунікаційні системи та мережі.

Офіційний опонент,

завідувач кафедри телекомунікацій

Національного університету

«Львівська політехніка»,

доктор технічних наук, професор М.М. Климаш

Підпис професора Климаша М.М. засвідчую,

Вчений секретар

Національного університету

«Львівська політехніка» Р.Б. Брилинський

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ "ЛЬВІВСЬКА ПОЛІТЕХНІКА" ЗКПО 02071010

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ Український державний університет залізничного транспорту №01116472

Вхідний № 01/02-16
«25» лютого 2016 р.
УкрДУЗТ