МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
УКРАЇНСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ ЗАЛІЗНИЧНОГО ТРАНСПОРТУ

ЗАМУЛА ОЛЕКСАНДР АНДРІЙОВИЧ

УДК 621.391

МОДЕЛІ І МЕТОДИ СИНТЕЗУ СКЛАДНИХ СИГНАЛІВ З НЕОБХІДНИМИ ВЛАСТИВОСТЯМИ ДЛЯ ЗАХИЩЕНИХ ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ

05.12.02 – телекомунікаційні системи та мережі

Автореферат
дисертації на здобуття наукового ступеня
доктора технічних наук

Харків – 2016

Дисертацією є рукопис.
Робота виконана у Харківському національному університеті імені В.Н. Каразіна.

Науковий консультант: доктор технічних наук, професор
Горбенко Іван Дмитрович,
Харківський національний університет імені В.Н. Каразіна, професор кафедри безпеки інформаційних систем і технологій.

Офіційні опоненти: доктор технічних наук, професор
Бондаренко Олег Володимирович,
Одеська національна академія зв'язку ім. О. С. Попова, проректор з навчальної роботи;

доктор технічних наук, професор
Климаш Михайло Миколайович,
Національний університет «Львівська політехніка», завідувач кафедри телекомунікацій;

доктор технічних наук, професор
Кучук Георгій Анатолійович,
Харківський університет Повітряних Сил імені Івана Кожедуба, провідний науковий співробітник наукового центру Повітряних Сил.

Захист відбудеться « 25 » березня 2016 року о 14^{00} годині
на засіданні спеціалізованої вченої ради Д 64.820.01
61050, м. Харків, пл. Фейєрбаха, 7.

З дисертацією можна ознайомитись в бібліотеці
Українського державного університету залізничного транспорту,
61050, м. Харків, пл. Фейєрбаха, 7.

Автореферат розісланий « 08» лютого 2016 р.

Учений секретар
спеціалізованої вченої ради
к.т.н., доцент К.А. Трубчанінова

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Актуальність теми. Указом Президента України № 287/2015 введено в дію рішення Ради національної безпеки і оборони України від 6 травня 2015 року "Про Стратегію національної безпеки України". У Стратегії ...., зокрема, до актуальних загроз національної безпеки України віднесені загрози інформаційній безпеці, загрози кібербезпеці та безпеці інформаційних ресурсів (уразливість об'єктів критичної інфраструктури, державних інформаційних ресурсів до кібератак). У даному документі визначено основні напрями державної політики національної безпеки України, до яких належать: необхідність удосконалення та розвитку на сучасній технологічній базі системи управління, захищених телекомунікацій, розвідки, радіоелектронної боротьби; забезпечення інформаційної безпеки.

Рівень інформатизації держави визначається насамперед розвитком інфотелекомунікацій, як сукупності мережних ресурсів, призначених для виробництва та надання телекомунікаційних, інформаційних й інших послуг. Основу інфотелекомунікацій утворюють інформаційні мережі, які, в свою чергу, базуються на телекомунікаційних мережах. З появою нових телекомунікаційних технологій, орієнтованих на пакетний спосіб передачі інформації, використання різних середовищ передачі (оптичне волокно, радіочастотний ресурс), і забезпечення мобільного зв'язку, з'явилася можливість істотно підвищити продуктивність, ефективність і якість обслуговування телекомунікаційних мереж, а також розширити діапазон послуг, які ними надаються. З'явилися десятки фундаментальних робіт у сфері науки і техніки, які охоплюють теоретичні та методологічні основи побудови телекомунікаційних систем (ТКС). Це наукові праці таких авторів, як: Hsiao-Hwa Chen, K. Fazel, S. Kaiser, Christopher Cox, Hooshang Chafouri-Shiraz, M. Massoud Karbassian, О.В. Бондаренко, М.Н. Климаш, Г.А. Кучук та ін. До основних параметрів ефективності ТКС належать: надійність, живучість, пропускна здатність мережі, якість обслуговування, рентабельність і вартість, завадозахищеність, інформаційна безпека тощо. Перспективним напрямом забезпечення безпеки інформаційних ресурсів є використання технології розподіленого спектра (широкосмугових шумоподібних сигналів). Використовувані методи формування та обробки даних, а також класи широкосмугових сигналів, які застосовуються як фізичний переносник даних, не дозволяють забезпечити необхідні (для тих чи інших додатків ТКС) показники інформаційної безпеки (імітостійкість, інформаційна скритність) і завадозахищеності (структурна скритність і завадостійкість прийому). Таким чином, підвищення вимог до інформаційної безпеки, завадозахищеності ТКС, продуктивності формування та обробки даних в умовах внутрішніх і зовнішніх загроз (впливів) зумовлюють об'єктивно існуюче науково-технічне протиріччя, на вирішення якого і спрямована мета даної роботи. До перших найбільш важливих результатів у галузі широкосмугових ТКС або розподілених систем слід віднести дослідження, які були опубліковані у наукових працях Р.Вудворда, К. Шеннона і В.А. Котельникова S. Golomb, N.Zierler, R. Gold, T. Kasami, DV Sarvate, M.P. Pursley та ін. Значний внесок у розвиток широкосмугової ідеології зробили вчені Я.Д. Ширман, І.М. Аміантов, Л.Є. Варакин, М.Б. Свердлик, В.Б. Пестряков, І.Д. Горбенко, В.П. Іпатов та багато

інших. В існуючих системах, значною мірою протягом тривалого часу в каналі синхронізації передається один і той самий широкосмуговий сигнал лінійної форми, а в інформаційному каналі, відповідність: біт (m біт) повідомлення - сигнал лінійної форми (2^m сигналів) з часом залишається фіксованим. Такий метод інформаційного обміну в ТКС дозволяє порушнику, на основі визначення параметрів використовуваних у системі сигналів, здійснити постановку навмисних завад з мінімальними енергетичними затратами. Крім того, станція протидії може здійснити нав'язування режимів роботи системи (режим синхронізації, передача помилкових повідомлень). Вищезазначене може призвести до істотного погіршення показників функціонування ТКС.

Таким чином, вирішення важливої науково-прикладної проблеми, яка 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 і структурними властивостями, є актуальним.

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

Напрями досліджень тісно пов'язані з низкою науково-дослідних (НДР) і дослідно-конструкторських робіт (ДКР), виконаних відповідно до планів наукової і науково-технічної діяльності Харківського національного університету імені В. Н. Каразіна, Харківського національного університету радіоелектроніки. Результати досліджень отримано в ході вирішення окремих завдань таких НДР: «Обгрунтування вимог, розробка та впровадження інфраструктури електронного цифрового підпису в МОНУ» (№ Держреєстрації 0106U006221); «Напрями, методи і засоби вдосконалення та розвитку національної інфраструктури відкритих ключів (№Держреєстрації 0109U002573); «Розвиток, стандартизація, уніфікація, вдосконалення та впровадження інфраструктури відкритих ключів, включаючи національну систему електронного цифрового підпису (ЕЦП)» (№Держреєстрації 0111U002628); «Аналіз стану, визначення напрямків розвитку, стандартизація, вдосконалення, розробка та впровадження криптографічних систем, включаючи систему електронного цифрового підпису (ЕЦП)» (№Держреєстрації 0113U000363); «Методи, системи та засоби криптографічного захисту інформації з гарантованим рівнем стійкості і підвищеною швидкодією» (№Держреєстрації 0115U002431); «Математичне та комп'ютерне моделювання інформаційних процесів у складних природних і технічних системах" (№Держреєстрації 0112U002098).

Мета та задачі дослідження. Метою роботи є покращення показників завадозахищеності та інформаційної безпеки захищеної ТКС в умовах зовнішніх і внутрішніх впливів на основі розвитку теорії та практики інформаційного обміну, а також методів синтезу складних нелінійних дискретних сигналів з необхідними властивостями. Для досягнення поставленої мети необхідно розв’язати такі задачі:

1. Дослідження проблеми захищеності інформаційного обміну в ТКС. Виявлення причин, що породжують зазначену наукову проблему, вибір критеріїв оцінки та показників ефективності досліджуваних процесів і обґрунтування напрямків досліджень.

2. Математичне обгрунтування, розробка та дослідження методів синтезу нелінійних дискретних складних сигналів у кінцевих полях з покращеними ансамблевими, кореляційними, структурними властивостями з метою підвищення завадозахищеності та інформаційної безпеки ТКС.

3. Розробка моделі структури складних нелінійних дискретних сигналів у кінцевих полях з метою визначення структурної скритності даного класу сигналів для оцінки показників завадозахищеності та інформаційної безпеки ТКС.

4. Розробка та дослідження методів синтезу нелінійних криптографічних дискретних складних сигналів з покращеними ансамблевими, кореляційними, структурними властивостями з метою підвищення завадозахищеності та інформаційної безпеки ТКС.

5. Дослідження властивостей нових синтезованих класів нелінійних дискретних складних сигналів для використання в ТКС як фізичний переносник інформації.

6. Розробка методів оцінки властивостей нелінійних дискретних складних сигналів, які дозволять знизити обчислювальні витрати на реалізацію процесу знаходження (відбору) складних сигналів з покращеними ансамблевими, кореляційними і структурними властивостями.

7. Розробка програмних моделей отриманих методів синтезу нелінійних дискретних складних сигналів для практичного використання в ТКС.

8. Розробка та удосконалення методів швидкої реалізації модульних операцій.

9. Удосконалення методів інформаційного обміну в ТКС з метою покращення показників завадозахищеності та інформаційної безпеки ТКС.

Об'єктом дослідження є процеси інформаційного обміну та управління цим обміном, що протікають в ТКС та мережах.

Предметом дослідження є методи підвищення завадозахищеності, інформаційної безпеки та продуктивності обробки даних ТКС на основі розробки методів інформаційного обміну, синтезу нових класів нелінійних дискретних сигналів з необхідними властивостями.

Методи дослідження. Сукупність методів досліджень визначена суттю вирішуваних наукових завдань проблеми досліджень і включає: положення теорії інформації і завадостійкого кодування, теорії систем зв’язку та теорії систем сигналів, теорії криптографічного захисту інформації, теорії ймовірностей і випадкових процесів, методи аналізу та синтезу, теорії чисел, груп, кілець, полів, методи теорії цифрових автоматів, які використані в аналітичній розробці методів управління ТКС (реалізація динамічного режиму передавання даних у системі), при вирішенні завдань синтезу систем сигналів з визначеними властивостями, для дослідження шляхів удосконалення процесу обробки і оцінки параметрів складних переносників інформації та під час розробки методів реалізації основних модульних операцій в модулярній системі числення; методи для знаходження оптимальних рішень задач дискретної і комбінаторної оптимізації під час розробки удосконаленого методу синтезу систем сигналів із заданими властивостями. Основні практичні результати отримано з використанням методів математичного та імітаційного моделювання, теорії ймовірності та математичної статистики.

Наукова новизна отриманих результатів зумовлена теоретичним узагальненням та новим вирішенням важливої науково-прикладної проблеми, яка 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 і структурними властивостями.

Отримано такі **наукові результати.**

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 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;

- 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 синтезу сигналів;

- 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.

Отримані наукові результати в сукупності є розвитком теорії інформаційного обміну, теорії синтезу систем складних нелінійних дискретних сигналів, теорії швидкої реалізації операцій в дійсній числовій області обчислень і спрямовані на покращення показників ефективності ТКС: завадозахищеності та інформаційної безпеки, продуктивності.

Практичне значення отриманих результатів дисертаційних досліджень полягає у тому, що:

1. Вперше отримано метод синтезу складних нелінійних криптографічних сигналів (КС), який використовує випадкові або псевдовипадкові процеси, і створює послідовності символів (сигналів) певного алфавіту, які відповідають вимогам незворотності, нерозрізненості, непередбачуваності, і володіють необхідними ансамблевими і кореляційними властивостями. Практичне використання даної системи сигналів дозволить підвищити скритність функціонування ТКС. Так, для періоду сигналу порядку 1000 елементів структурна скритність КС перевищує даний показник для лінійних класів сигналів (М послідовностей) більш ніж в 30 разів. Характеристики кореляційних функцій синтезованих КС не поступаються, а в ряді випадків перевершують відповідні характеристики лінійних сигналів. Зокрема, КС мають поліпшені, порівняно з М послідовностями, взаємно кореляційні властивості. Застосування синтезованих систем КС дозволить, наприклад, у ході використання КС з періодом 256 елементів як синхронізуючі послідовності, більш ніж на 3 дБ підвищити завадостійкість прийому сигналів. За рахунок поліпшених ансамблевих властивостей КС, виникає можливість підвищити показники інформаційної безпеки. Так, імітостійкість системи в ході застосування КС з періодом сигналу 1023 елемента більш ніж 10^5 разів вище, ніж під час застосування лінійних класів сигналів (наприклад, М - послідовностей). Крім покращення показників імітостійкості системи забезпечується більш високий рівень завадостійкості прийому сигналів. Покращені порівняно з лінійними класами сигналів ансамблеві властивості КС дозволяють підвищити інформаційну скритність системи.

2. Удосконалено метод синтезу системи КС на основі спрямованого (обмеженого) перебору всіх можливих сигналів для відбору таких, які відповідають заданим вимогам, що дозволяє підвищити продуктивність процесу синтезу системи сигналів (від 45 до 60 відсотків).

3. Удосконалено метод синтезу систем нелінійних сигналів (НС) у кінцевих полях, що дозволяє підвищити (за рахунок поліпшених кореляційних властивостей) завадостійкість прийому. Так, під час використання нелінійних сигналів як синхропослідовності (при періоді сигналу 256 елементів) завадостійкість прийому КС на 4 дБ вище, ніж у випадку використання лінійних класів сигналів. Отримані методи дозволяють підвищити продуктивність синтезу системи. Так, для періоду нелінійного сигналу 10098 елементів (обсяг системи складає 2 880 сигналів) виграш у ході використання розробленого методу синтезу сигналів порівняно з відомим методом складає більше 720 разів.

4. Розроблено методи табличної реалізації модульних операцій в медулярній системі числення (МСС) з використанням спеціального коду табличного подання операндів, які дозволяють, залежно від величини l-байтового (l = 1 - 4, 8) машинного слова, наприклад, у ході виконання операції модульного множення від 64 до 4096 разів скоротити час виконання операцій, порівняно з використанням суматорного методу в позиційній системі числення.

5. На основі розроблених і вдосконалених методів синтезу систем НС, швидкої реалізації модульних операцій розроблено алгоритми для їх реалізації, відповідно до яких синтезований клас апаратних засобів формування і обробки сигналів у ТКС, на які отримано 14 патентів України, що підтверджує новизну і практичну значущість отриманих у дисертації наукових результатів роботи.

6. Розроблено моделі та методи синтезу систем НС з необхідними для тих чи інших додатків ТКС властивостями, отримано обчислювальні алгоритми і програмну реалізацію зазначених моделей і методів, а також дослідження властивостей нових класів нелінійних сигналів.

7. Розроблено метод інформаційного обміну даними, в якому, за певним законом змінюється з часом відповідність: біт повідомлення - складний сигнал, і як складні сигнали застосовуються сигнали з необхідними ансамблевими, структурними та кореляційними властивостями, що дозволяє підвищити завадозахищеність й інформаційну скритність ТКС. Так, у ході реалізації динамічного режиму функціонування системи і використання множини нелінійних дискретних сигналів з періодом 10000 елементів, імітостійкість системи на три порядки вище, ніж під час використання лінійних дискретних сигналів з трирівневою функцією кореляції, які є кращими з погляду ансамблевих і кореляційних властивостей у даному класі сигналів.

Отримані в роботі результати знайшли практичне впровадження і використання:

- у процесі побудови телекомунікаційної системи в приватному акціонерному товаристві «Інститут інформаційних технологій» (м. Харків), відповідно до Договору №0003 / 01-15 від 08.07.15. (Акт використання від 28.09. 2015р.);

- під час виконання науково-дослідних робіт з розробки перспективних засобів зв'язку та визначення шляхів модернізації «малогабаритної завадозахищеної короткохвильової радіостанції малої потужності», яка розроблена і виготовлена в Державному підприємстві «Центральне конструкторське бюро «Протон» (м. Харків) (Акт впровадження від 23.09. 2015р.);

- під час виконання науково-дослідних і дослідно-конструкторських робіт: «Побудова моделюючого комплексу для управління функціонуванням корабельного з'єднання»; «Дослідження і розробка методів забезпечення живучості комп'ютерних інформаційних мереж для високотехнологічних об'єктів» в Інституті проблем реєстрації інформації Національної Академії наук України (м. Київ), (Акт впровадження від 07.09. 2015р.);

- у навчальному процесі кафедри безпеки інформаційних систем і технологій Харківського національного університету ім. В.Н. Каразіна під час викладання дисциплін «Управління інформаційною безпекою», «Комплексні системи захисту інформації: проектування, впровадження, супровід», «Нормативно-правове забезпечення інформаційної безпеки», що підтверджується Актом використання від 21.09. 2015р.

Достовірність отриманих результатів підтверджується збіжністю результатів експериментальних досліджень з теоретичними результатами, отриманими за виведеними аналітичними виразами, і обґрунтовується їх несуперечністю основним положенням теорії оптимальних методів прийому, теорії систем сигналів, теорії захисту інформації, теорії кінцевих полів Галуа та теорії чисел.

Публікації. Результати дисертації опубліковані в 73 наукових працях (з них 13 виконані без співавторства) [6,15,24,27,29 - 30,33,41 - 42,45,55-56,58], в тому числі, 1 - монографія , 40 - наукових статей, тези доповідей та тексти виступів опубліковані у збірниках Трудів міжнародних форумів та міжнародних науково-практичних конференцій [41- 58]. Результати досліджень відображені в 6 звітах про НДР.

Особистий внесок здобувача. Усі основні наукові положення, результати, висновки та рекомендації дисертації отримано здобувачем особисто. У наукових працях, виконаних у співавторстві і опублікованих у наукових фахових виданнях України, а також у зарубіжних виданнях, які входять до науково-метричної бази, особистий внесок здобувача в статті полягає у тому, що: в роботі [1] наведено концепцію та політику безпеки інформації в телекомунікаційних системах, у яких вирішуються завдання забезпечення інформаційної безпеки; в [2] - аналіз методів аутентифікації об'єктів даних і суб'єктів ТКС; у [3] -визначено умови забезпечення абсолютної стійкості в ході реалізації послуг цілісності та автентичності повідомлень; в [4] - запропоновано алгоритми реалізації операцій додавання, множення на основі стиснення цифрових даних таблиць; в [5] - запропоновано метод підвищення продуктивності обробки даних в автоматизованих системах управління; в [6] - наведено порівняльний аналіз методів аналізу та управління ризиками інформаційної безпеки, сформульовано пропозиції щодо використання методів оцінки ризиків (впливів) в телекомунікаційних системах; в [7] - запропоновано структуру процесу обробки інформації на основі застосування модулярної системи числення; в [8] - розроблено метод реалізації операції додавання в модульній системі числення; в [9] - розроблено метод обробки інформації в модулярній системі числення; в [10] - запропоновано метод реалізації операції додавання і віднімання за рахунок унітарного кодування залишків чисел на

основі принципу кільцевого зсуву в модульній системі числення; в [11] - сформульовано принципи проектування систем захисту інформації в ТКС; у [12] - наведено математичну модель побудови структури дискретної послідовності, яка дозволяє отримати оцінку структурної скритності НС; у [13] – наведено аналіз несанкціонованих впливів на ТКС і формулюються пропозиції щодо застосування методів оцінки ризиків інформаційної безпеки; в [14] розроблено метод синтезу НС у кінцевих полях; у 15] - розроблено метод синтезу всієї системи НС у кінцевих полях; в [16] - розроблено метод синтезу похідних НС у кінцевих полях і наводяться результати досліджень кореляційних, ансамблевих і структурних властивостей цих сигналів; у [17] - наведено аналіз можливих внутрішніх впливів (загроз) на ТКС і формулюються пропозиції щодо застосування методів захисту від впливів; у [18] - наведено порівняльний аналіз методів оцінки впливу на ТКС та розроблено пропозиції щодо застосування методів оцінки впливів на основі теорії нечітких множин; у [19] - проведено дослідження методів пошуку та протидії зовнішнім впливам на ресурси ТКС; у [20] - досліджено методи генерації випадкових і псевдовипадкових послідовностей для реалізації динамічного режиму функціонування ТКС; у [21] - визначено критерії та показники синтезу систем сигналів із заданими властивостями для використання сигналів у захищеній ТКС; у [22] - вводяться і обгрунтовуються показники оцінки захищеності ТКС від зовнішніх і внутрішніх загроз; у [23] наводено аналіз загроз інформаційної безпеки, завадозахищеності, енергетичної та структурної скритності ТКС, обгрунтовуються показники захищеності та методи протидії від відповідних загроз, у тому числі, на рівні джерела складних сигналів; у [25] – введено показники та критерії оцінки розв'язання однієї з задач теорії оптимального прийому сигналів - оцінка параметрів сигналів, висуваються вимоги щодо кореляційних властивостей сигналів; у [26] - розроблено метод генерації псевдовипадкових послідовностей символів, для реалізації динамічного режиму функціонування каналу ТКС; у [27] - наведено дослідження ансамблевих властивостей НС; в [28] запропоновано показники оцінки захищеності інформації від зовнішніх загроз, і запропоновано заходи і методи протидії загрозам порушення цілісності та конфіденційності даних абонентів ТКС; у [29] – визначено необхідні й достатні умови забезпечення абсолютної інформаційної скритності ТКС; у [30] - розроблено метод синтезу багатофазних нелінійних дискретних сигналів, наведено оцінки ансамблевих і кореляційних властивостей таких сигналів; у [31] - розроблено метод побудови генератора псевдовипадкових послідовностей на основі паралельних обчислень з використанням графічних процесорів; у [32] - наведено порівняльний аналіз систем виявлення та перекриття несанкціонованих впливів на ресурси ТКС, сформульовано пропозиції щодо застосування методів і засобів протидії впливам у сучасних ТКС; у [33] - наведено результати досліджень властивостей НС; в [34] - розроблено метод синтезу нелінійних криптографічних дискретних сигналів (КС) із заданими властивостями; в [35] - розроблено удосконалений метод інформаційного обміну на основі динамічної зміни відповідності: біт повідомлення - складний сигнал, визначено необхідні і достатні умови забезпечення в ТКС показників завадозахищеності та інформаційної безпеки; в [36] - визначено критерії та показники властивостей генераторів

випадкових (псевдовипадкових) послідовностей символів, що використовуються для формування дискретних сигналів і генераторів керуючих сигналів у ТКС; в [37] - наведено аналіз міжнародних стандартів у сфері управління інформаційною безпекою та сформульовано пропозиції щодо застосування міжнародних стандартів у ході створення систем захисту в ТКС; у [38] - розроблено удосконалений метод синтезу КС на основі спрямованого перебору для підвищення продуктивності процесу синтезу сигналів з необхідними властивостями; в роботі [39, 40] наведено результати досліджень властивостей дискретних сигналів, запропоновано можливі сфери використання таких сигналів у додатках ТКС.

Апробація результатів дисертації. Основні результати досліджень доповідались і були схвалені на 14 - ти міжнародних форумах і міжнародних науково-технічних конференціях, а саме: I - й Міжнародній конференції «Глобальні інформаційні системи. Проблеми і тенденції розвитку ». - Харків. ХНУРЕ. - 2006, [41]; XIII - й Міжнародній науково-практичній конференції. «Безпека інформації в інформаційно-телекомунікаційних систем. - Запоріжжя, 2010. Класичний приватний університет, Запорізький національний технічний університет, Академія наук вищої школи України. - 2010 [42]; XIII - й Міжнародній науково-практичній конференції. «Безпека інформації в інформаційно-телекомунікаційних системах». Київ. - 2010 [43-44]; Міжнародній науково-практичній конференції «Перспективи розвитку інформаційних та транспортно - митних технологій у митній справі, зовнішньоекономічної діяльності та управлінні організаціями», м. Дніпропетровськ. - 2011 [45]; 14 - й Міжнародній науково-практичній конференції. «Безпека інформації в інформаційно-телекомунікаційних системах». Київ. - 2011 [46]; 4 -му Міжнародному радіоелектронному форумі «Прикладна радіоелектроніка. Стан та перспективи розвитку». - Харків, АНПРЕ. 2011 [47 - 49]; 15-й Ювілейній Міжнародній науково-практичній конференції «Безпека інформації в інформаційно-телекомунікаційних системах». Київ. - 2012. [50 - 51]; 16-й Міжнародній науково-практичній конференції. Київ. - 2013 [52]; Міжнародній науково-технічній конференції «Комп'ютерне моделювання в наукоємних технологіях» (КМНТ-2014). Харків, ХНУ імені В.Н. Каразіна - 2014 [53]; «РТ - 2014». 10 - й Міжнародній науково - технічній конференції. Сучасні проблеми радіотехніки та телекомунікацій. - Севастополь, 2014 [54]; П'ятій міжнародній науково-технічній конференції «Сучасні напрямки розвитку інформаційно-комунікаційних технологій і засобів управління». - Полтава: ПНТУ; Баку; ВА ЗС АР; Кіровоград; КЛА НАУ; Харків; ДП «ХНДІ ТМ» - 2015 [55]; Науково-технічній конференції: Інформаційна безпека України, м. Київ. - 2015 [56 - 57]; IV й Міжнародній науково-технічній конференції «Захист інформації і безпека інформаційних систем», Львів. - 2015 [58].

Структура дисертаційної роботи. Дисертаційна робота складається із вступу, шести розділів, висновків, які містять основні результати досліджень, переліку використаних джерел і додатків. Повний обсяг дисертації становить 438 сторінок, у тому числі 10 сторінок - таблиць, 17 - сторінок переліку використаних джерел, що містить 150 найменувань, 123 сторінок додатків.

ОСНОВНИЙ ЗМІСТ РОБОТИ

Вступ дисертаційної роботи містить: обґрунтування актуальності теми дослідження; інформацію про зв’язок дисертаційної роботи з науковими програмами; мету роботи та окремі задачі досліджень; формулювання об’єкта, предмета і методів дослідження; характеристику наукової новизни та практичного значення отриманих результатів досліджень, а також особистого внеску здобувача; наведено дані щодо реалізації, апробації та публікації наукових і практичних результатів дисертації.

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

Специфіка семирівневої моделі взаємодії відкритих систем визначає нижчі рівні телекомунікаційних протоколів (фізичний і канальний), як найбільш критичні, щодо вирішення проблем підвищення продуктивності комунікаційних технологій у розподілених інформаційних системах, завадозахищеності та інформаційної безпеки. Тому основними напрямками розвитку ТКС в умовах зростаючих інформаційних навантажень, обмеженості фізичного ресурсу каналів і ліній передачі даних, зовнішніх та внутрішніх втручань є розроблення та дослідження моделей і методів підвищення пропускної здатності, завадозахищеності, достовірності та інформаційної безпеки ТКС. До основних показників ефективності функціонування ТКС належить: пропускна здатність, завадозахищеність, продуктивність, інформаційна безпека, живучість, своєчасність доставки повідомлень та ін. Під завадозахищеністю ТКС слід розуміти її здатність виконувати завдання в умовах радіоелектронного заглушення (РЕП) з боку станції протидії. РЕП включає радіотехнічну розвідку (РР) і радіопротидію (РП). РР передбачає встановлення факту роботи ТКС і визначення її параметрів (частотний діапазон, займана смуга, закон модуляції, інтервал часу, що займаний сигналом тощо), необхідних для радіопротидії. Метою РП є створення умов, що ускладнюють роботу ТКС. Очевидно, що постановка завад буде тим ефективніше, чим більше інформації виявить станція протидії про параметри ТКС. Якщо станція протидії може здійснити виявлення факту роботи ТКС і параметрів сигналу з імовірністю $P_р$, і реалізувати порушення роботи ТКС з імовірністю $P_н$, тоді для оцінки завадозахищеності можна використовувати показник $P_{пз}$

$$P_{пз} = 1 - P_р P_н, \qquad (1)$$

Імовірність $P_н$ залежить від можливості роботи ТКС в умовах дії завад. Тому величина $P_{пу} = 1 - P_н$ може бути прийнята як показник завадостійкості прийому сигналів-переносників даних. Як показник завадозахищеності ТКС може бути також використана ймовірність заглушення радіоканалу ($P_{под.}$), яка визначається зі

співвідношення: $P_{под.} = P_р P_{оп}(1 - P_р)P_{уп}$, де: $P_р$ - ймовірність розвідки параметрів складного сигналу; $P_{оп}$ - ймовірність застосування «оптимальної» завади, тобто завади зі структурою та енергією, близькими до структури та енергії випромінюваного сигналу; $P_{уп}$ - ймовірність застосування станцією протидії завади, потужність якої істотно перевищує потужність випромінюваного сигналу, а смуга частот, у якій зосереджена завада, повністю перекриває спектр, відведений для передачі даних користувачів системи. Аналіз показує, що можливості заглушення радіоканалу універсальною або загороджувальною завадою обмежені. У такому випадку, як випливає з останнього виразу, ймовірність заглушення системи значною мірою визначається захищеністю системи від впливу оптимальних завад, створюваних станцією протидії. У свою чергу постановка такого роду завад залежить від енергетичної, структурної та часової скритності функціонування системи. Енергетичну скритність радіоканалу визначимо як здатність системи функціонувати з таким енергетичним потенціалом, якого недостатньо для того, щоб станція протидії здійснювала перехоплення і прийом інформації з необхідною достовірністю: $S_e = P\ E/N_0 < G_{вим.}$, де: E/N_0 - відношення енергії сигналу до спектральної щільності потужності шуму на вході вирішального пристрою приймача станції протидії; $G_{вим.}$ - значення відношення E/N_0 для прийому даних з необхідною достовірністю. Структурна скритність характеризує здатність ТКС протистояти заходам, спрямованих на ототожнення виявленого сигналу з одним з множини апріорно відомих сигналів (розпізнаванням форми сигналу, яка визначається способами його кодування і модуляції). Введемо поняття структурної скритності складного сигналу у вигляді співвідношення

$$S_{сс} = \frac{\prod_{i=1}^{L} M_i^*}{\prod_{i=1}^{L} M_i}, \qquad (2)$$

де: M_i^* - координати складного сигналу, які необхідно знати для того, щоб визначити M_i-M_i^* координати, L – розмірність простору координат.

Для випадку використання в системі фазоманіпульованих сигналів, вираз (2) набуде вигляду

$$S_{сс} = l/N, \qquad (3)$$

де l - число символів, яке необхідно знати, для визначення правила (закону) формування N-l символів.

Інформаційна безпека ТКС - це здатність системи забезпечувати захист від знищення, модифікації, блокування інформації, її несанкціонованого витоку або від порушення встановленого порядку її маршрутизації. Однією зі складових інформаційної безпеки є інформаційна скритність (ІС) ТКС. Під ІС системи розумітимемо її здатність приховувати смисловий зміст повідомлень, способи формування повідомлень (сигналів), сам факт передачі сигналів. Як показник оцінки ІС використовують, так званий, безпечний час ($T_{без.}$):

$$T_{без.} = M/(K \cdot \gamma), \qquad (4)$$

де: γ - продуктивність системи, що здійснює спроби несанкціонованого отримання змісту повідомлення, що вимірюється числом переборів варіантів за секунду; M - число можливих варіантів встановлення відповідності: біт повідомлення - складний сигнал; $K = 3{,}1 \cdot 10^7$ (кількість секунд на рік). Складовою інформаційної безпеки (поряд з ІС) є система імітозахисту. Під імітозахищеністю розуміють комплекс організаційно-технічних заходів і засобів, а також законодавчих норм, які спрямовані на забезпечення певного рівня імітостійкості. По суті імітостійкість забезпечується наданням таких послуг як цілісність, справжність (автентичність), а також застосуванням різних криптографічних протоколів. Як показали дослідження, забезпечити необхідну в ТКС імітостійкість можливо на рівні джерела складних сигналів. У цьому випадку імітостійкість (I_c) залежить від: розміру простору сигналів M; числа дозволених до використання в інтервалі часу t сигналів Z; числа спроб нав'язування (імітації) C і політики нав'язування X:

$$I_c = F(M,Z,C,X); \tag{5}$$

$$I_c = C / Z, \text{ якщо } 1 < C < Z \text{ і } I_c = 1, \text{ якщо } C > Z. \tag{6}$$

$$I_c = 1 - P_{нав.} \tag{7}$$

$$P_{нав.} = C / M. \tag{8}$$

Завадостійкість - характеризує здатність ТКС функціонувати в умовах впливу на систему різних завад і визначається відношенням:

$$q^2 = B\rho^2, \tag{9}$$

де: $\rho^2 = P_c / P_п$, ($P_c, P_п$ - потужності сигналу і завади відповідно); $q^2 = E / N_0$ (E – енергія, що приходиться на один біт, $N_0 = P_п / F$ - спектральна щільність потужності завади в смузі F сигналу); B - база сигналу.

Завадостійкість ТКС характеризується ймовірністю помилки ($P_{пом.}$) і визначається зі співвідношення:

$$P_{пом.} = 1 - F(H), \tag{10}$$

де: інтеграл ймовірності $$F(x) = \frac{1}{\sqrt{2\pi}} \int_x^{\infty} \exp\left(\frac{-t^2}{2}\right) dt, \tag{11}$$

$$H = \sqrt{[(E_0 + E_1) / N_0](1 - R)}; \tag{12}$$

E_0, E_1 – енергії відповідно сигналів $U_0(t)$, $U_1(t)$;

$$R = \frac{2}{E_0 + E_1} \int_0^T S_j(t) S_j(t) dt. \tag{13}$$

Коефіцієнт R з точністю до постійної збігається з коефіцієнтом кореляції сигналів $U_0(t)$, $U_1(t)$. Аналіз співвідношень (9) - (13) показує, що завадостійкість прийому сигналів визначається $\rho^2 = P_c / P_п$ і базою сигналу B, та значенням . У теорії зв'язку найбільш поширеною моделлю служить канал з адитивним білим гаусівським шумом, в якому ймовірність трансформації каналом заданого вхідного сигналу в те чи інше вихідне спостереження експоненціально зменшується із

зростанням квадрата Евклідової відстані між переданим сигналом і вихідним спостереженням:

$$P[y(t)\,|\,S(t)] = k\exp(-\frac{1}{N_0}\cdot d(s,y)), \qquad (14)$$

де k - константа, яка не залежить від $S(t)$ і $y(t)$, - спектральна щільність потужності одностороннього білого шуму; а Гілбертова відстань між $S(t)$ і $y(t)$ визначається як:

$$d(S,y) = \sqrt{\int_0^T [y(t) - S(t)]^2 dt}. \qquad (15)$$

У разі рівної ймовірності всіх повідомлень джерела оптимальною стратегією спостерігача, що забезпечує мінімальну помилку переплутування дійсно переданого з деяким іншим сигналом, є правило (критерій) максимальної правдоподібності (МП): після того, як коливання $y(t)$ прийнято, рішення приймається на користь того сигналу, для якого ймовірність трансформації його каналом у прийняте спостереження $y(t)$ є найбільшим (порівняно з ймовірностями для інших сигналів). МП рішення для гаусівського каналу може бути перетворено в правило мінімуму відстані:

$$d(S_j,y) = \min d(S_i,y) => H_j, \qquad (16)$$

тобто рішення приймається на користь сигналу $S_j(t)$, оскільки він найбільш близький (в сенсі Гілбертової відстані) до спостереження $y(t)$ серед усіх конкуруючих сигналів. Розкривши дужки в (15), приходимо до співвідношення

$$d^2(S_i, y) = \int_0^T y^2(t)dt - 2\int_0^T y(t)\cdot S(t) + \int_0^T S^2(t)dt = \|y\|^2 - 2Z_i + \|S_i\|^2, \qquad (17)$$

де

$$Z_i = (y_i, S_i) = \int_0^T y(t)S(t)dt \qquad (18)$$

Правило мінімуму відстані (16) може бути сформульовано як правило максимуму кореляції:

$$Z_j - \frac{E_j}{2} = \max(Z_i - \frac{E_j}{2}) \Rightarrow H_j. \qquad (19)$$

Вираз (19) означає, що з M можливих сигналів з однаковою енергією фактично прийнятим вважається той, який має максимум кореляції зі спостереженням $y(t)$. На сьогодні відсутні регулярні методи синтезу сигналу (ДС), що є оптимальними за мінімаксним критерієм. У дисертаційній роботі пропонуються методи синтезу дискретних сигналів (ДС), що є оптимальними за мінімаксним критерієм, і які дозволяють істотно (порівняно з відомими методами перебору) скоротити обсяг обчислень зі знаходження ДС із заданими властивостями і покращити показники ефективності ТКС, зокрема, завадозахищеності та інформаційної безпеки. Аналіз стану захищеності інформаційного обміну в різних додатках ТКС з урахуванням введених у роботі показників ефективності показав, що необхідні значення завадозахищеності (зокрема, енергетичної та структурної скритності, завадостійкості прийому) та

інформаційної безпеки (інформаційної скритності й імітостійкості) можуть бути реалізовані на основі застосування в ТКС широкосмугових шумоподібних сигналів з необхідними ансамблевими, структурними та кореляційними властивостями, а процес інформаційного обміну здійснюється із застосуванням динамічної зміни відповідності: біт повідомлення - складний сигнал.

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

Проектування широкосмугових систем багато в чому грунтується на знаходженні ДС з відповідними ансамблевими, кореляційними, структурними, технологічними та іншими властивостями. Технологічні властивості (правила побудови) ДС, що застосовуються сьогодні в ряді ТКС, засновані на лінійних законах побудови, зокрема, використовують лінійні регістри зі зворотними зв'язками. Структурна скритність, ансамблеві, а в ряді випадків і кореляційні властивості таких сигналів не дозволяють забезпечувати необхідні значення завадостійкості, структурної та інформаційної скритності, імітостійкості та деяких інших показників функціонування захищених ТКС. У розділі 2 наводиться опис отриманих вперше в ході дисертаційних досліджень і вдосконалених методів синтезу одного класу НС - характеристичних дискретних сигналів (ХДС). У даному розділі розглянуто N-позиційні ХДС з дворівневою періодичною функцією автокореляції (ПФАК), побудова яких базується на використанні характеру мультиплікативної групи поля $GF(p^n)$ для $N = 4x + 2 = p^n - 1$ и $N = 4x = p^n - 1$ (де: x=1,2,3,...,n - ступінь розширення поля $GF(p^n)$). Скористаємося поняттям двозначного характеру мультиплікативної групи і сформулюємо правила кодування для даної системи сигналів:

$$\left.\begin{aligned} \mu_i &= \psi(\Theta^i + 1), \text{ якщо } \Theta^i + 1 \equiv 0 (\mathrm{mod}\ p); \\ \mu_i &= 1, \qquad \text{якщо } \Theta^i + 1 \equiv 0 (\mathrm{mod}\ p); \end{aligned}\right\}, \tag{20}$$

$$\left.\begin{aligned} \mu_i &= \psi(\Theta^i + 1), \text{ якщо } \Theta^i + 1 \equiv 0 (\mathrm{mod}\ p); \\ \mu_i &= -1, \qquad \text{якщо } \Theta^i + 1 \equiv 0 (\mathrm{mod}\ p); \end{aligned}\right\}, \tag{21}$$

де θ - первісний елемент поля.

Правило кодування (20) призводить до сигналу з дворівневою періодичною функцією автокореляції (ПФА) $R_\mu(m) = \{-2, 2\}$, а правило кодування (21) – к $R_\mu(m) = \{0, -4\}$. Таким чином, ХДС відносяться до так званих мінімаксних дискретних послідовностей. Об'єм системи ХДС становить

$$M = \varphi(N) / n, \tag{22}$$

де $\varphi(N)$ - функція Ейлера.

Метод формування ХДС тривалістю N, що базується на комплексному використанні апарату теорії полів Галуа, теорії чисел і комбінаторики зважаючи на застосування складених у теорії чисел таблиці елементів та індексів елементів поля Галуа, вже при $n \geq 1$ і $N \geq 100$ стає важко реалізованим. Вищезазначене пояснюється

насамперед тим, що при гомоморфному відображенні елементів поля a_i в множину символів дискретної послідовності в ході використання комплексно-значної функції $\psi(a_i) = W_i = -e^{j\pi U_i}$, необхідно розв'язувати в середньому $L/2$ порівнянь виду

$$a_i \equiv \Theta_j^{U_i} (\mathrm{mod}\ P),\ i = \overline{0, P-1}, \tag{23}$$

де: $U_i = \overline{0, P-2}$ - індекс елемента поля $GF(P)$; j - j-й первісний елемент поля; P - характеристика поля Галуа.

Для розв'язання порівнянь виду (23) у відомому методі використовуються попередньо розраховані таблиці елементів та індексів елементів полів Галуа. Відомий також метод формування ХДС, що заснований на рекурентній залежності між елементами та індексами елементів поля Галуа, при цьому стає можливим алгоритмизувати процедури формування символів ХДС. Однак обчислювальна складність такого методу залишається значною:

$$t_{\sum} = N(t_y + t_{сл} + 3t_з + (N-2)t_{сч} + (N+1)t_п), \tag{24}$$

де $t_y, t_{сл}, t_з, t_{сч}, t_п$ - час виконання операцій множення, додавання, записи, зчитування і порівняння відповідно. Аналіз виразу (24) показує, що основні часові витрати в ході побудови ХДС пов'язані з квадратичними членами $N(N-2)t_{сч}, N(N+1)t_{ср}$.

Під час дисертаційних досліджень розроблено метод синтезу нелінійних сигналів (ХДС) у базисі простих і розширених полів Галуа, що має значно меншу обчислювальну складність порівняно з зазначеними вище методами. Синтез ХДС у простому полі $GF(P)$ базується на використанні найменшого за значенням первісного елемента поля $GF(P)$) і задається твердженням 1.

Твердження 1. Нехай характер мультиплікативної групи поля фіксується функцією

$$\psi(a_i) = e^{j\pi U_i}, \tag{25}$$

тоді метод побудови характеристичного сигналу описується такими етапами:

1. Формується масив елементів - чисел $A_i, i = \overline{0, P-2}$ поля $GF(P)$:

$$A(i) = \Theta_j^i (\mathrm{mod}\ P). \tag{26}$$

2. Формується група чисел поля GF(P), відповідно до правила:

$$H(i) = A(i) + 1, \text{ якщо } \Theta_j^i + 1 = 0(\mathrm{mod}\ P);$$

$$H(i) = 1, \text{ якщо } \Theta_j^i + 1 \equiv 0(\mathrm{mod}\ P). \tag{27}$$

3. Формується масив індексів $X(i), i = \overline{0, P-2}$, значеннями якого є відповідні елементу поля індекси i+1, що упорядковані за вмістом за адресою:

$$A(i) : X(i) = X\ A(i)\ . \tag{28}$$

4. Будується масив індексів J(i), значенями якого є індекси масиву X(i), що вибираються за адресою $H(i) : J(i) = X[H(i)], i = \overline{0, P-2}$.

5. Обчислюється характер елементів поля за правилом:

$$\psi(a_i)=\psi[J(i)]=\begin{cases}1, \text{ якщо } J(i)\equiv 0(\text{mod } 2);\\ -1, \text{ якщо } J(i)\equiv 0(\text{mod } 2).\end{cases} \quad (29)$$

Під час досліджень розроблено метод синтезу ХДС у розширених полях Галуа. Нехай $GF(P^n)$ - розширення n-й ступеня поля $GF(P)$, а елементи-поліноми, ступені яких не перевищує n, обчислюються над полем $GF(P)$; $\Phi_k(x)$ і θ_j; $(\Phi_k(x),\theta_j)$ - відповідно k-й первісний, незвідний над полем $GF(P^n)$ поліном, а θ_j - j-й первісний елемент поля. Функція характерів гомоморфного відображення елементів поля $GF(P^n)$ над полем $GF(2)$ зафіксована функцією $\psi(a_i)=e^{(j\pi ui)}$, причому елемент-поліном поля a_i визначається з роз'язання порівняння $a_i\equiv\theta_j(u^i) \bmod \Phi_k(x),P$, а $u_i=\overline{(0,P^n-2)}$ є множина чисел-індексів, упорядкованих за зростанням. Тоді основними етапами методу синтезу ХДС у поле $GF(P^n)$ є такі:

1. Формується масив індексів $u_i^{'}=u_i+1, i=\overline{0,P^n-2}$, упорядкованих за зростанням, і масив елементів-поліномів A(i) поля $GF(P^n)$:

$$A(i)=\theta_j^i(\text{mod } \Phi_k(x),\ P). \quad (30)$$

2. Формується масив H(i) елементів-поліномів поля $GF(P^n)$, елементи якого зсунені за значенням на одиницю щодо значень масиву A(i):

$$\begin{gathered}H(i)=A(i)+1, \text{ якщо } \theta_j^i+1\neq 0(\text{mod } \Phi_k(x),\ P),\\ H(i)=1, \text{ якщо } \theta_j^i+1\equiv 0(\text{mod } \Phi_k(x),\ P).\end{gathered} \quad (31)$$

3. Масив індексів u_i записується в масив X(i) за адресами, що визначені десятковим поданням елементів - поліномів A(i).

4. Формується масив індексів $J(i), i=\overline{(0,P^n-2)}$, шляхом зчитування з масиву X(i) індексів, обираних за адресами, які є десятковим поданням поліномів H(i).

5. Обчислюється для всіх значень масиву індексів J(i) двозначний характер мультиплікативної групи поля (символи ХДС) за правилом

$$\psi(a_i)=\psi(\theta_j^i+1)=-\psi(J(i))=\begin{cases}1, \text{ якщо } J(i)\equiv 0(\text{mod}2),\\ -1, \text{ якщо } J(i)\neq 0(\text{mod}2).\end{cases} \quad (32)$$

Обчислювальна складність (t_c) методу синтезу сигналів ХДС, як випливає з Твердження 1, може бути визначена з виразу:

$$t_c=N(t_y+t_{сл}+t_{ср}+4t_{сч}+t_з)=N(t_y+t_{сл}+t_{ср}+5t_з) \quad (33)$$

Аналіз (33) показує, що час побудови ХДС із застосуванням отриманих методів лінійно залежить від періоду послідовності, що формується, тоді як для відомого методу (вираз (24)), залежність - квадратична. Виграш у часі синтезу нелінійних сигналів у кінцевих полях із застосуванням розроблених методів в порівнянні з відомим методом становить: для періоду N=1018-106,5 рази; для періоду N=4000-417 рази; для періоду N=9972-1039,6 рази.

Для синтезу всієї системи НС, необхідно виконувати кроки 1-5 наведених вище методів синтезу для кожного з первісних елементів поля. Для досить великих періодів сигналів і в ході реалізації в системі динамічного режиму передачі

інформації, за якого здійснюється зміна відповідності: біт повідомлення - складний сигнал, застосування відомого методу синтезу сигналів вимагає значних часових і обчислювальних витрат. Для синтезу всієї системи ізоморфізмів нелінійних сигналів у реальному часі, зокрема для практичної реалізації динамічного режиму передачі інформації, був розроблений удосконалений метод. Пропонований метод побудови системи ізоморфізмів для числа елементів коду задається таким твердженням.

Твердження 2. Якщо над ХДС $\{W_i\}, i = \overline{1, N}$ з кількістю елементів (періодом) N виконати операцію децимації з коефіцієнтом децимації C, де C - взаємно просте з N ($C \in \varphi(N)$), то результуюча послідовність (код) $\{V_i\}$ є ізоморфізмом коду $\{W_i\}$. Процедура децимації означає вибір (з подальшим зчитуванням) кожного C-го символу коду і запис отриманих таким чином символів, згідно з правилом

$$V_i = (W_i + C) \bmod N. \qquad (34)$$

У роботі доведено ідентичность розробленого методу синтезу системи сигналів на основі децимації символів одного з ізоморфізмів ХДС і методу синтезу, заснованого на теорії різницевих множин (РМ). На рис. 1 зображено граф відповідностей множин НС, побудованих з використанням методу РМ v_i і розробленого методу на основі децимації ізоморфізму w_i. Аналіз зв'язків вузлів графа вказує на ідентичність (з точністю до циклічного зсуву) ізоморфізмів, побудованих з використанням даних методів. На рис. 1 введено позначення: оператор $\overline{T}$ означає дзеркальне відображення ізоморфізмів, отриманих за різними методами; $\overline{T}^{-r}$ - дзеркальне відображення із зсувом вліво на r символів коду; T^{-r} - на r одиниць вліво; T^{r} - на r одиниць вправо. Виграш у часі в ході використання розробленого методу синтезу системи НС на основі децимації ізоморфізму порівняно із застосуванням методу РМ для періоду сигналу 1020 елементів складає більш ніж 16 разів, а при періоді сигналу 2380 елементів - більш ніж 28 разів.

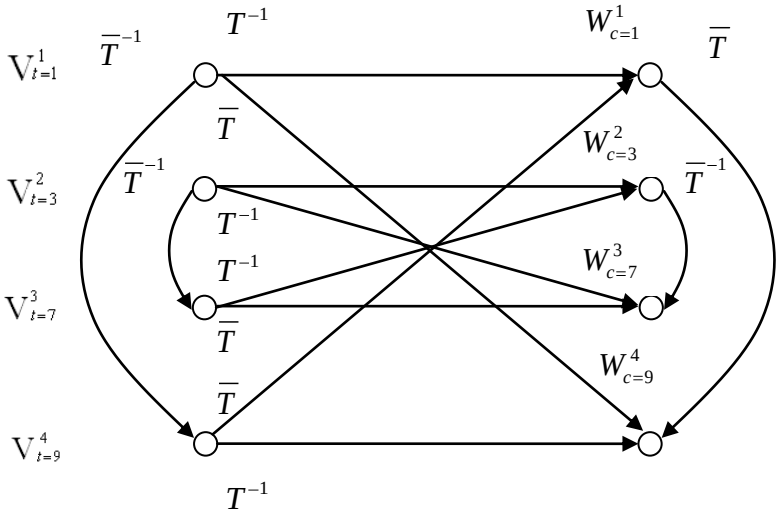

Рис 1. Граф відповідностей ізоморфізмів, побудованих методами децимації і різнісної множини при N = 10

Під час досліджень розроблено програмну модель отриманого методу синтезу всієї системи НС у кінцевих полях. Виконано комп'ютерне моделювання параметрів,

використовуваних при синтезу системи: первісні елементи поля, примітивні поліноми ступеня n, коефіцієнти децимації та ін. Розроблено технічні рішення, що реалізують запропоновані методи синтезу НС у простих і розширених полях Галуа, а також синтезу системи сигналів на основі децимації і зчитування елементів послідовності, на які отримано 5 авторських свідоцтв на винаходи, що підтверджує новизну і практичну значущість отриманих в дисертації наукових результатів.

У **третьому розділі** дисертації вирішено четверта і сьома задачі дослідження і отримано два наукових результати.

В умовах внутрішніх і зовнішніх несанкціонованих впливів порушників на ТКС фактично, для будь-якого повідомлення, блоку даних або програмного коду необхідно реалізувати ряд послуг (функцій) безпеки. До основних послуг інформаційної безпеки належать: конфіденційність, цілісність, справжність (автентичність) інформації. Зазначені послуги повною мірою можуть бути надані за допомогою використання криптографічних перетворень та протоколів. У розділі 1 було показано, що зазначені послуги, а також послуга завадозахищеності, які надаються ТКС, значною мірою визначаються кореляційними, структурними та ансамблевими властивостями складних сигналів - фізичних переносників даних користувачів. У ТКС знайшли застосування множини лінійних рекурентних послідовностей, множини Касамі, Голда та ін.), що володіють порівняно невеликими значеннями бічних пелюсток авто і взаємно - кореляційних функцій. Однак зазначені сигнали мають низьку структурну скритність, їх ансамблеві властивості є обмеженими. Тому актуальною є задача розробки теорії і практики синтезу та аналізу систем дискретних сигналів з необхідними властивостями. Необхідність застосування захищених ТКС змушує дослідників по-новому подивитися як на режими функціонування захищених радіоканалів, так і на аспекти формування та застосування складних сигналів. Продуктивним кроком, з погляду нового напряму використання систем складних сигналів, є синтез так званих систем криптографічних сигналів (КС). Під час досліджень вперше отримано метод синтезу складних нелінійних КС, що дозволяє створювати: великі ансамблі дискретних послідовностей практично будь-якого періоду з заданими, але фізично реалізованими значеннями бічних пелюсток авто - взаємної і стикової функцій кореляції в періодичному і аперіодичному режимах роботи; послідовності з статистичними характеристиками кореляційних функцій (КФ), аналогічними характеристиками кращих, з погляду кореляційних функцій, лінійних класів сигналів; послідовності, які відповідають вимогам незворотності, нерозрізненості, непередбачуваності, і володіють необхідними структурними та ансамблевими властивостями, що дозволяє покращити показники завадозахищеності, імітостійкості, структурної скритності ТКС, а також завадостійкості прийому сигналів в умовах впливу структурних, загороджувальних, ретрансльованих та інших видів завад. З урахуванням вимог забезпечення в системі необхідних значень криптографічної стійкості та структурної скритності (завадозахищеності) як джерело криптографічного сигналу обгрунтовано вибір алгоритму симетричного блокового шифрування з лічильником, що задається національним стандартом ДСТУ 7624: 2014.

Метод синтез систем складних нелінійних криптографічних дискретних сигналів (КС) із заданими властивостями включає такі дії.

1. Генерація масиву псевдовипадкових послідовностей символів заданого періоду з використанням криптографічного алгоритму (джерел випадкових або псевдовипадкових послідовностей символів).
2. Тестування отриманих послідовностей із застосуванням критеріїв та показників якості генераторів, які визначені міжнародними та відомчими стандартами.
3. Формування дискретних послідовностей (ДП) символів з необхідним (для того чи іншого додатка системи) періодом.
4. Відбір ДП, значення бічних пелюсток періодичної функції автокореляції (ПФАК) яких близькі до границі «щільної упаковки».
5. Отримання матриці станів авто- і взаємно-кореляційних функцій усіх можливих пар послідовностей, які пройшли відбір за результатами попереднього кроку.
6. Обробка матриці, яка полягає в тому, що здійснюється відбір послідовностей, які відповідають границям «щільної упаковки» для відповідних кореляційних функцій.

В роботі наведено обґрунтування необхідності реалізації зазначених вище дій (кроків) методу синтезу сигналів. Також обґрунтовано визначення терміну «криптографічний сигнал». Під нелінійним криптографічним дискретним сигналом, пропонується розуміти послідовності символів довільного алфавіту, як правило побудови яких використовуються випадкові або псевдовипадкові процеси, і є таким, що задовольняє вимогам незворотності, нерозрізненості, непередбачуваності, і який володіє визначеними ансамблевими і кореляційними властивостями. Застосування КС дозволяє покращити показники завадозахищеності, імітостійкість, структурної скритності ТКС, а також завадостійкості прийому сигналів в умовах впливу структурних, загороджувальних, ретрансльованих, вузькосмугових та інших видів завад. Особлива властивість таких систем сигналів: можливість їх відновлення у просторі та часі із застосуванням ключів і інших параметрів, які використовуються в процесі синтезу сигналів. У таблиці 1, відповідно до описаного вище методу, наведено результати синтезу КС для деяких значень періоду послідовностей. Аналіз даних таблиці 1 показує, що для періоду послідовності, наприклад, 63 число пар КС, що відповідають встановленому граничному значенню - 17, становить понад 12 10^6 (12214869). Для послідовностей з трирівневою функцією взаємної кореляції (ФВК), число пар, що відповідають даній «границі» складає лише 975 пар. Таким чином, ансамбль нелінійних КС більш ніж в 10^5 разів перевищує ансамбль зазначених лінійних сигналів. Перевищення обсягу криптографічних сигналів над ансамблем, складеного з М-послідовності становить більш ніж 10^7 разів. В четвертому розділі дисертації більш детально наведено результати досліджень кореляційних, структурних та ансамблевих властивостей нелінійних КС.

Знаходження дискретних сигналів з необхідними характеристиками зводиться, по суті, до перебору всіх можливих варіантів, що належать деякій системі сигналів, і відбору тих сигналів, які відповідають відомим граничним оцінкам. Обчислювальна складність таких методів досить значна. Під час досліджень отримано удосконалений метод синтезу нелінійних КС, заснований на використанні скороченого (спрямованого) перебору на основі застосування методу «гілок і меж»,

що дозволяє підвищити продуктивність (швидкодію) процесу синтезу сигналів. Сформульовано і доведено твердження, які дозволяють в ході розв'язання задачі синтезу сигналів з покращеними властивостями, відмовитися від повного перебору всіх можливих варіантів сигналів, і пошук здійснювати через «відсів» підмножин допустимих рішень, які свідомо не містять оптимальних рішень. Далі, розбиття на підмножини решти множини сигналів може спростити задачу знаходження шуканого сигналу з заданими властивостями. Розроблено програмну модель, що реалізує запропоновані методи синтезу КС. Дослідження, зокрема, показали, що запропонований метод синтезу системи сигналів забезпечує виграш у продуктивності в ході синтезу системи нелінійних КС від 45 до 60 відсотків порівняно з методом повного перебору.

У розділі 4 дисертації показано, що послідовності символів, на основі яких створені КС, за своїми структурними властивостями відповідають вимогам, що висуваються до генераторів випадкових послідовностей символів і, таким чином, за своїми структурними властивостями суттєво перевищують властивості відомих класів сигналів. Показано, також, що КС володіють суттєво покращеними, ніж відомі сигнали ансамблевими властивостями, що створює передумови для покращення показників ефективності ТКС, а саме імітостійкості й інформаційної скритності.

Таблиця 1

Кореляційні властивості КС

Період КС	Граничне значення	ПФАК	АФАК	ПФВК		АФВК
		КількістьКС, що відповідають границі	КількістьКС, що відповідають границі	Загальна кількість пар	Кількість пар КС, що відповідають границі	Кількість пар КС, що відповідають границі
31	9	7 743	3 622	29 977 024	1 465 137	14 537 423
63	17	10 868	7 166	59 056 712	12 214 869	54 822 445
127	23	3482	1302	6 062 162	47 053	1 619 780
511	59	3819	1951	7 292 380	122 835	3 466 713
1 023	100	8 513	6 194	36 235 584	5 293 538	35 083 491

У **четвертому розділі** дисертації розв'язані третя і п'ятя задачі проблеми досліджень і отримано два наукових результата, що пов'язані з отриманням математичної моделі структури складних нелінійних сигналів та методу оцінки властивостей нелінійних дискретних сигналів. Комплексне вирішення проблеми забезпечення завадозахищеності та інформаційної безпеки функціонування ТКС може бути досягнуто, в тому числі, на основі реалізації динамічного режиму передачі інформації, за якого відповідність: біт повідомлення – сигнал змінюється з часом за законом, визначення якого порушником, можливо з ймовірністю, що не перевищує допустимого значення, і застосування сигналів з необхідними

кореляційними, ансамблевими, статистичними, структурними властивостями. Імітостійкість радіоканалу зі складними каналами залежить від розмірності ансамблю (обсягу системи) використовуваних сигналів. Для НС, методи синтезу яких наведено в розділі 2, об'єм системи ХДС дорівнює $M = \phi(N)/2n$. Зауважимо, що об'єм системи лінійних класів сигналів визначається виразом M=φ(N)/m, де m - ступінь примітивного полінома, на основі якого синтезований лінійний сигнал. У табл. 2 наведено узагальнені дані про число значень L, для яких (відповідно до правил побудови) можуть бути створені М – послідовності і ХДС, а також об'єми зазначених систем сигналів.

Таблиця 2

Ансамблеві властивості різних дискретних сигналів

	Число значень L		Об'єм системи	
ΔL	ХДС	М-послідовності	ХДС	М-послідовності
$0-10^2$	30	4	456	8
$0-10^3$	186	9	29291	79
$0-10^4$	1269	11	2152943	554

Аналіз наведених аналітичних співвідношень і даних табл. 2 показує, що на інтервалі довжин від 50 до 1500, М – послідовності існують тільки для 5 значень періоду, доступне число послідовностей Лежандра становить 114, число ХДС для цього інтервалу довжин становить 225. Об'єм системи, складеної з ХДС в інтервалі тривалостей до 10000 символів більш ніж в 3 10^3 разів перевищує обсяг системи, складеної з М-послідовностей. Об'єм системи сигналів може бути збільшений за рахунок залучення автоморфізмів (циклічних зсувів) ізоморфізмів сигналів. При цьому потужність авто- і ізоморфного кодування M_{ai} в класі ХДС при заданому періоді послідовності N може бути визначена зі співвідношення

$$M_{ai} = \varphi(N)/2n. \qquad (38)$$

У класі похідних ХДС, теоретичні основи побудови яких наведені в розділі 2 дисертації, потужність похідного авто- і ізоморфного кодування ($M_{паі}$) дорівнює:

$$M_{паі} = (N+2)\varphi(N)(\varphi(N)-2n)/8n^2. \qquad (39)$$

У таблиці 3 наведені значення $M_{паі}$ для деяких значень N, що обчислені з використанням співвідношення (39).

Таблиця 3

Потужність похідного авто- і ізоморфного кодування в класі характеристичних сигналів

N	256	508	1018	2098	4000	5002	9010
M_{ai}	$5{,}2\cdot10^5$	$4{,}0\cdot10^6$	$3{,}3\cdot10^7$	$2{,}9\cdot10^8$	$1{,}3\cdot10^8$	$3{,}6\cdot10^9$	$1{,}2\cdot10^{10}$

У таблиці 4 наведено порівняльну характеристику об'єму системи різних класів складних сигналів, у тому числі КС, теоретичні основи синтезу яких наведені в розділі 3.

Таблиця 4

Ансамблеві властивості різних класів сигналів

Клас сигналів	Період послідовності	Значення границі «щільної упаковки»	Кількість пар послідовностей, що відповідають границі
М-послідовності	511	63	276
ПФВКТ	511	33	147500
КС	511	63	2666671
М- послідовності	1023	160	435
ПФВКТ	1023	65	338000
КС	1023	100	5293538

Аналіз даних таблиці 4 показує, що для періоду послідовності N=1023, виграш в обсязі системи сигналів, при незначному збільшенні значень бічних піків ПФВК по відношенню до граничного значення, порівняно з послідовностями з трирівневою ПФВК, становить більш ніж 15 разів, а в порівнянні з М - послідовностями (при менших значеннях бічних пелюсток ПФВК КС) - більш ніж 10^3 разів.

Вперше отримано математичну модель структури складних нелінійних дискретних сигналів у кінцевих полях, що обумовлена залежністю 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.

Твердження 4. Нехай $a_1, a_2, ..., a_{(P-1)/2}$ — елементи поля GF(P), тоді елементи поля $a_{(P-1)/2+1}, a_{(P-1)/2+2}, ..., a_{P-1}$ залежать від $(P-1)/2$ елементів і визначаються з співвідношення:

$$a_{(P-1)/2+i} = P - a_i, \tag{40}$$

де $i = \overline{1,(P-1)/2}$.

Проілюструємо на прикладі можливість побудови $((P-1)/2+i)-x$ елементів поля за відомими першими $(P-1)/2$ елементах. Нехай характеристика поля $P=13$, первісний елемент поля $\Theta = 2$.

Знайдемо елементи даного поля:

$$\begin{aligned} &a_1 = 2^0 \bmod 13 = 1; a_2 = 2^1 \bmod 13 = 2; a_3 = 2^2 \bmod 13 = 4; a_4 = 2^3 \bmod 13 = 8; \\ &a_5 = 2^4 \bmod 13 = 3; a_6 = 2^5 \bmod 13 = 6; a_7 = 2^6 \bmod 13 = 12; a_8 = 2^7 \bmod 13 = 11; \\ &a_9 = 2^8 \bmod 13 = 9; a_{10} = 2^9 \bmod 13 = 5; a_{11} = 2^{10} \bmod 13 = 10; a_{12} = 2^{11} \bmod 13 = 7. \end{aligned} \tag{41}$$

Скористаємося рівнянням (40) для отримання $((P-1)/2+i)-x$ елементів поля

$$\begin{aligned} &(i = \overline{1,(P-1)}): a_7 = a_{(P-1)/2+1} = P - a_1 = 12; a_8 = a_{(P-1)/2+2} = P - a_2 = 11; \\ &a_9 = a_{(P-1)/2+3} = P - a_3 = 9; a_{10} = a_{(P-1)/2+4} = P - a_4 = 5; a_{11} = a_{(P-1)/2+5} = P - a_5 = 10; \\ &a_{12} = a_{(P-1)/2+6} = P - a_6 = 7. \end{aligned}$$

Порівняння відповідних елементів поля, наведених у (40) з елементами поля, що отримано з використанням (41) показує, що вони ідентичні.

Для довільно обраного первісного елемента Θ_l поля множення

$$(\Theta_l^i \Theta_l^{P-1-i}) \bmod P \equiv 1 (\bmod P). \qquad (42)$$

Справедливість (42) випливає з того, що для простого P $\varphi(P) = P - 1$. З теореми Ейлера випливає, що $\Theta^{\varphi(P)} = \Theta^{P-1} \equiv 1 (\bmod P)$, тому $(\Theta_l^i \Theta_l^{P-i-1}) \bmod P = \Theta^{P-1} \equiv 1 (\bmod P)$. З огляду на те, що порівняння (42) виконується за будь-яких Θ_l і P, при i=1, елемент поля a_2 однозначно пов'язаний з елементом a_{P-1}, при i=2, елемент поля a_3 пов'язаний з елементом a_{P-2} і т.д. Аналіз (42) показує, що елементи поля a_1 і a_{P-2}, a_2 і a_{P-2} є мультиплікативно зворотніми. У зв'язку із зазначеним, в полі Галуа залежними є і характери елементів поля або символи ХДС, що побудовані в полі. Ця залежність визначається твердженням 5.

Твердження 5. Нехай характери елементів поля (символи ХДС у полі GF(P)) визначаються зі співвідношення

$$W_i = \psi(a_i) = \exp(j\pi u_i), \qquad (43)$$

а індекси елементів поля u_i знаходять з розв'язання рівняння

$$a_i = \Theta_l^i + 1 = \Theta_l^{U_i} (\bmod P),$$

тоді характери $(P-1)/2+1+i\,(i = \overline{1,(P-1)/2-1})$ елементів поля (символи сигналу) залежать від характерів $P-1\,/2-i$ перших елементів поля, причому

$$W_{P-i} = (-1)^i W_{i+1}. \qquad (44)$$

Проілюструємо справедливість твердження 5 на прикладі. Нехай характеристика поля $P = 13$, а первісний елемент поля $\Theta = 2$. Ізоморфізм ХДС для зазначених даних має вигляд: $W = \{-11-111-1111-1-1-1\}$.

Встановимо залежність характерів (символів ХДС) у полі GF(13). При $i = 1$ $W_2 = -W_2$, $i = 2$ $W_{11} = W_3$, $i = 3$ $W_{10} = -W_4$, $i = 4$ $W_9 = W_5$, $i = 5$ $W_8 = -W_6$. Результат буде таким самим, якщо для встановлення залежності символів НС застосувати (44).

Використання твердження 5 дозволяє визначити (P-1)/2+i символи ХДС $(i = \overline{1,(P-1)/2})$ за відомими першими (P-1)/2-i символам. У цьому випадку не визначені лише перший і ((P-1)/2+i)-й символи ХДС, але ((P-1)/2+i)-й символ ХДС визначається правилом кодування ХДС. Дійсно, відомо, що елемент поля $\Theta^{(P-1)/2} = N$, тоді $\Theta^{(P-1)/2} + 1 = N + 1 (\bmod P) \equiv 0 (\bmod P)$. Відповідно до правила кодування ХДС, якщо $\Theta^i + 1 \equiv 0 (\bmod P)$, то символ сигналу - це «1». Для ХДС число символів К, що приймають значення «1», дорівнює K=N/2. Це означає, що перший символ ХДС може бути довизначеним, якщо відомі P-2 символів сигналу. Таким чином, для визначення станцією протидії закону формування ХДС (подолання структурної скритності), їй необхідно мати відомості про не менш ніж половину символів із загального періоду сигналу, що вказує на більш високий рівень структурної скритності ХДС порівняно з лінійними класами сигналів. Застосування складних сигналів дозволяє підвищити захищеність ТКС при впливі структурних і деяких інших типів завад у межах смуги частот, займаної сигналом. У зв'язку з цим важливим завданням є вибір сигналів, що забезпечують мінімально можливий рівень взаємних завад, який в основному визначається допустимим рівнем

максимальних піків взаємнокореляційних функцій (ВКФ). З використанням розробленого програмного забезпечення виконано дослідження кореляційних властивостей складних НС у кінцевих полях Галуа і нелінійних КС. У таблиці 5 наведено узагальнені статистичні характеристики різних кореляційних функцій найбільш широко застосовуваних дискретних послідовностей. Аналіз даних, наведених у табл. 2 і 5, свідчить про те, що значення максимальних бічних викидів КС, а також статистичні характеристики даного класу сигналів не поступаються відповідним характеристикам сигналів, побудованих з використанням М-послідовностей, при цьому ансамблеві і структурні властивості НС перевершують відповідні властивості лінійних класів сигналів. Під час досліджень сформульовано і доведено твердження, що дозволили розробити вдосконалений метод оцінки властивостей НС, заснований на алгебраїчних властивостях елементів кінцевих полів, реалізація якого призводить до істотно меншого (порівняно з відомими методами перебору) обсягу обчислень щодо знаходження сигналів з заданими значеннями кореляційних функцій з метою підвищення продуктивності процесу синтезу системи сигналів з необхідними властивостями.

Таблиця 5

Статистичні характеристики кореляційних функцій дискретних сигналів

Тип сигналів	Характеристики	$\frac{R_{макс}}{\sqrt{N}}$	$\frac{m_{\lvert R\rvert}}{\sqrt{N}}$	$\frac{D^{1/2}_{\lvert R\rvert}}{\sqrt{N}}$	$\frac{D^{1/2}_{R}}{\sqrt{N}}$
ХДС	АФАК	1,0 – 1,8	0,5	0,4	0,5
	ПФАК	0,1 – 1,9	0,2	0,1	0,2
	МИФАК	1,4 – 2,6	0,6	0,5	0,8
	АФВК	1,9 – 3,2	1,0	0,8	1,0
	ПФВК	2,5 – 3,6	1,0	0,8	1,2
	СФВК	2.1 – 5,0	0,9	0,7	1,1
М-послідовності	АФАК	0,7...1,25	0,32	0,26	0,41
	ПФАК	1/√L	1/√L	0	0
	МИФАК	1,3...2,3	0,66	0,49	0,82
	АФВК	1,4...5,0	0,54	0,48	0,73
	ПФВК	1,9...6,0	0,8	0,62	1,0
	СФВК	2,0...5,1	0,83	0,62	1

Твердження 6. Нехай W_μ і W_ν є ХДС з числом символів N, які побудовані за допомогою децимації вихідного сигналу W_1 (сигнал, побудований за найменшим із значень первісних елементів поля) відповідно за коефіцієнтами μ і ν, а μ' і ν', - нові коефіцієнти децимації, причому, $\nu' = \nu \cdot x (\mathrm{mod}\, N)$, де x – ціле число, таке, що найбільший спільний дільник (НСД) чисел і дорівнює 1. Тоді децимація вихідного ХДС W_1 за коефіцієнтами μ' і ν' дає нові пари, реалізації ПФВК яких (значення бічних пелюсток функції кореляції), є результат децимації значень бічних пелюсток ПФВК пари ХДС W_μ і W_ν.

З урахуванням твердження 6 можуть бути визначені всі бажані пари ХДС, тобто пари, що мають мінімальні значення бічних пелюсток функції кореляції.

Відомі методи оцінки ПФВК вимагають проведення розрахунків значень викидів для всіх можливих поєднань пар сигналів.

Сформульовано і доведено твердження, яке призводить до зменшення обсягу обчислень для знаходження ДП, які мають необхідні кореляційні властивості. Назвемо $\|R\|$ - взаємнокореляційною матрицею, номерами рядків і стовпців якої, є коефіцієнти децимації, відповідно до яких формуються ХДС. На перетині рядків і стовпців матриці розміщені значення максимальних бічних викидів ПФВК для пар ХДС.

Твердження 7. Нехай $\|R\|$ є матриця максимальних значень бічних пелюсток ПФК пар ХДС w_i і w_j $(i,j=\overline{1,M})$ розмірності $M\times M$, причому M є число ізоморфізмів ХДС, а рядки і стовпці матриці позначені значеннями упорядкованих за зростанням коефіцієнтів децимації. Тоді перший рядок матриці, що містить значення бічних пелюсток ПФВК вихідного ізоморфізму з усіма іншими ізоморфизмами, містить всі $M-1$ можливі значення бічних пелюсток ПФВК, які дають пари w_i і w_j.

Твердження вказує на той факт, що для знання значень максимальних бічних викидів ПФВК поєднань всіх пар ХДС достатньо розрахувати реалізації ПФВК вихідного сигналу w_1 з усіма $w_2, w_3, \ldots, w_{M-1}$ ізоморфізмами, тобто реалізації ПФВК для першого рядка матриці. Виграш у продуктивності синтезу системи сигналів, що досягається в ході використання розробленого методу оцінки властивостей сигналів, може бути визначений з виразу

$$K=(C^2_{\varphi(N)}/2)/\varphi(N), \qquad (45)$$

де $\varphi(N)$ - функція Ейлера.

Так, для періоду ХДС N=10098, $\varphi(N)$=2880 і виграш К у продуктивності в ході використання розробленого методу порівняно з відомими методами становить 720 разів. Розроблено імітаційну (програмну) модель, яка реалізує запропонований метод оцінки властивостей нелінійних дискретних сигналів.

З метою дослідження статистичних (структурних) властивостей нелінійних КС використано одну з методик статистичних випробувань, а саме, NIST 800-22. Результати тестування показали, що КС за своїми статистичними властивостями близькі до властивостей випадкових послідовностей, тобто відповідають властивостям непередбачуваності символів, незворотності, випадковості, рівноймовірності, незалежності та однорідності. Результати досліджень властивостей НС у кінцевих полях Галуа і нелінійних КС, теоретичні основи синтезу яких були наведені в розділах 2 і 3 дисертації показали, що зазначені сигнали володіють з одного боку, структурними властивостями, аналогічними властивостям випадкових послідовностей, а з іншого, - кореляційними властивостями, близькими до властивостей кращих лінійних класів сигналів, зокрема, послідовностей з трирівневою функцією взаємної кореляції. При цьому ансамблеві властивості нових класу сигналів істотно перевершують ансамблеві властивості лінійних класів сигналів. Зазначене дозволяє покращити показники завадозахищеності, імітостійкості, структурної та інформаційної скритності ТКС, а

також завадостійкості прийому сигналів в умовах впливу структурних, загороджувальних, ретрансльованих та інших видів завад.

У **п'ятому розділі** дисертації вирішено восьму задачу проблеми досліджень і отримано три наукових результати.

З метою пошуку шляхів підвищення швидкодії процесу формування та обробки сигналів у ТКС в розділі розглянуто принципи технічної реалізації модульних операцій в модулярній системі числення (МСЧ). Наведено три принципи технічної реалізації модульних операцій в МСЧ. Суматорний принцип (методи реалізації модульних операцій, які засновані на суматорному принципі, припускають використання малорозрядних двійкових суматорів за модулем m_i). Принцип кільцевого зсуву (ПКЗ) (методи реалізації модульних операцій, що засновані на цьому принципі, припускають використання кільцевих регістрів). Табличний (матричний) принцип реалізації арифметичних операцій (ТП) (методи реалізації модульних операцій, що засновані на табличному принципі, припускають використання малорозрядних матричних постійних запам'ятовуючих пристроїв). Відзначимо основні недоліки суматорного принципу реалізації арифметичних операцій, що не дозволяють домогтися високої швидкодії реалізації процесу формування та обробки сигналів у ТКС: складність синтезу двійкових суматорів; великий час перетворення інформації для значних розрядних сіток подання даних, яке визначається максимальною основою МСЧ; складність реалізації операції множення; неефективність використання двійкових елементів, внаслідок надмірності максимальних чисел, які можуть бути надані суматорами, порівняно з величинами основи МСЧ; низька достовірність обчислень за рахунок можливих помилок, які виникають в процесі обчислень або в процесі переносів проміжних значень результату порозрядного підсумовування. Особливість ПКС полягає в тому, що результат арифметичної операції $(a_i \pm b_i) \bmod m_i$ за довільним модулем m_i МСЧ, заданої сукупністю $\{m_j\}$ $(j = \overline{1,n})$ основ, визначається тільки за рахунок циклічних зсувів заданої цифрової структури даних. Дійсно, відома теорема Келі встановлює ізоморфізм між елементами кінцевої абельової групи і елементами групи перестановок. Один з наслідків теореми Келі є висновок про те, що відображення елементів абельової групи на групу всіх натуральних чисел є гомоморфним. Ця обставина дозволяє організувати процес визначення результату арифметичних операцій у МСЧ за допомогою використання ПКС. Так, операнд у МСЧ, подається набором з n залишків $\{a_i\}$, утворених шляхом послідовного ділення вихідного числа A на n попарно простих чисел $\{m_i\}$, $(i = \overline{1,n})$. У цьому випадку сукупність залишків безпосередньо ототожнюється з сумою n простих полів Галуа виду $\sum_{i=1}^{n} GF(m_i)$. На основі використання ПКС у розділі удосконалено метод реалізації арифметичних модульних операцій додавання і віднімання, який за допомогою подання залишків числа двійковим кодом, за рахунок використання властивостей циклічних перестановок вмісту кільцевого регістра, що дозволяє підвищити швидкодію виконання модульних операцій. Дані методи засновані на реалізації такої сукупності аналітичних співвідношень:

$$(a_i + \beta_i) = a_i - (m_i - b_i) \bmod m_i, \quad (46)$$

$$(a_i - \beta_i) = a_i + (m_i - b_i) \bmod m_i, \quad (47)$$

$$a_i + \beta_i = a_i' + \beta_i' = (a_i + m_i/2) + (\beta_i - m_i/2), \quad (48)$$

$$\{a_i\beta_i (\bmod m_i) + (m_i - a_i)\beta_i \bmod m_i\} \bmod m_i \equiv 0 (\bmod m_i), \quad (49)$$

$$(m_i - a_i)\beta_i \bmod m_i \equiv m_i - a_i\beta_i (\bmod m_i), \quad (50)$$

$$\{a_i\beta_i (\bmod m_i) + (m_i - a_i)\beta_i \bmod m_i\} \bmod m_i \equiv 0 (\bmod m_i), \quad (51)$$

$$(m_i - a_i)\beta_i \bmod m_i \equiv m_i - a_i\beta_i (\bmod m_i). \quad (52)$$

Вихідні дані подаються у вигляді

$$P_{\text{исх}}^{(m_i)} = \left[P_0(a_0) \| P_1(a_1) \| P_1(a_1) \| \ldots \| P_{m_i-1}(a_{m_i-1}) \right],$$

де $\|$ - операція конкатенації (приєднання); $P_v(a_v)$ - k-розрядний двійковий код, що відповідає значенню a_v-го залишку $(a_v = \overline{0, m_i - 1})$ числа за модулем m_i; $k = [\log_2(m_i - 1) + 1]$. При цьому:

$$\left[P_0(\alpha_0) \| P_1(\alpha_1) \| \ldots \| P_{m_i-1}(a_{m_i-1}) \right] = \left[P_z(a_z) \| P_{z+1}(a_{z+1}) \| \ldots \| P_0(a_0) \| \ldots \| P_{m_i-1}(a_{m_i-1}) \right]^z;$$

$$\left[P_0(a_0) \| P_1(a_1) \| \ldots \| P_{m_i-1}(a_{m_i-1}) \right]^{-z} = \left[P_{m_i-1-z}(a_{m_i-1-z}) \| \ldots \| P_{m_i-z}(a_{m_i-z1}) \| \ldots \| P_0(a_0) \| P_1(a_1) \| \ldots \| P_{m_i-z-2}(a_{m_i-z-2}) \right],$$

де

$$z = \begin{cases} +\beta_i, \text{якщо } 0 \le \beta \le (m_i - 1)/2; \\ -(m_i - \beta_i), \text{ якщо } (m_i + 1)/2 \le \beta_i \le m_i - 1, \end{cases}$$

$$z = \begin{cases} +\beta_i, \text{ якщо } 0 \le \beta \le (m_i - 1)/2; \\ +(m_i - \beta_i), \text{ якщо } (m_i + 1)/2 \le \beta_i \le m_i - 1. \end{cases}$$

Час складання двох залишків $(a_i + b_i) \bmod m_i$ у МСЧ визначається математичним виразом $T_{\substack{\text{мсс} \\ m_i}}^{(+)} = K_{1i} \cdot K_{2i} \cdot t_{\text{сдв}}$, де K_{1i} - значення другого доданка в сумі $(a_i + b_i) \bmod m_i$ (кількість розрядів кільцевого регістру зсуву (КРЗ), на яке (в позитивному напрямку) зсувається початковий вміст КРЗ), тобто, $K_{1i} = \overline{0, m_i - 1}$; K_{2i} - кількість двійкових розрядів у одному розряді КРЗ за модулем m_i, тобто $K_{2i} = [\log(m_i - 1)] + 1$; $K_{1i} \cdot K_{2i}$ - кількість двійкових розрядів, що зсуваються в позитивному (проти годинникової стрілки) напрямку КРЗ; $t_{\text{сдв}} = 3 \cdot \tau_B$ - час "зсуву" одного двійкового розряду; τ_B - час спрацьовування одного логічного вентиля (елемента І, АБО). Для довільного модуля m_i МСЧ час складання двох залишків a_i і b_i визначається як:

$$T_{\substack{\text{мсс} \\ m_i}}^{(+)} = 3 \cdot K_{1i} \cdot \{[\log_2(m_i - 1)] + 1\} \cdot \tau_B. \quad (53)$$

Основна перевага запропонованого методу порівняно з позиційною системою числення (ПСС), полягає в можливості досягнення більш високої швидкодії обробки даних, ніж при суматорному методі, а також у зменшенні імовірності виникнення помилок у процесі визначень результату операції позиційного двійкового суматора.

У розділі на основі використання ТП розроблено два табличних методи: метод реалізації арифметичних модульних операцій додавання і віднімання, за допомогою використання спеціального коду табличного множення, що дозволяє підвищити швидкодію виконання модульних операцій додавання і віднімання, і метод реалізації арифметичної модульної операції множення, шляхом використання процедури порозрядного визначення результату операції, що дозволяє підвищити швидкодію виконання модульної операції модульного множення. Дані методи засновані на реалізації такої сукупності аналітичних співвідношень:

$$a_i b_i + a_i(m_i - b_i) \equiv 0(\mathrm{mod}\, m_i), \tag{54}$$

$$a_i b_i + b_i(m_i - a_i) \equiv 0(\mathrm{mod}\, m_i), \tag{55}$$

$$[(\gamma_a, a_i') + (\gamma_\beta, b_i')] + \{[m_i - (\gamma_a, a_i')] - (\gamma_\beta, b_i')\} = 0(\mathrm{mod}\, m_i) \tag{56}$$

$$(\gamma_a, a_i') + (\gamma_b, b_i') = m_i - \{[m_i - (\gamma_a, a_i')] - (\gamma_b, b_i')\}, \tag{57}$$

$$(\gamma_a, a_i') - (\gamma_b, b_i') = \{(\gamma_a, a_i') + [m_i(\gamma_b, b_i')]\}, \tag{58}$$

де $\gamma_a, \gamma_b = \begin{cases} 0, \text{ якщо } 0 \le a_i\,(b_i) \le \dfrac{m_i - 1}{2}, \\ 1, \text{ якщо } \dfrac{m_i + 1}{2} \le a_i\,(b_i) \le m_i - 1, \end{cases}$ $\gamma_i = \begin{cases} \overline{\gamma_i}, \text{ якщо } \gamma_a \ne \gamma_b, \\ \gamma, \text{якщо } \gamma_a = \gamma_b. \end{cases}$

Суть запропонованих у дисертації табличних методів обробки даних полягає в реалізації, на основі використання спеціального коду табличного подання даних, сукупності дій і прийомів, спрямованих на підвищення швидкодії реалізації операцій формування та обробки сигналів. Переваги методів табличної реалізації модульних операцій: надвисока швидкодія обробки даних (результат операції може бути отриманий в момент надходження вхідних даних, тобто в один такт і, таким чином, час виконання арифметичних операцій в МСЧ збігається з тактовою частотою обчислювача, що принципово неможливо для позиційних обчислювальних машин при існуючій елементній базі; табличні схеми мають високу надійність, оскільки реалізуються у вигляді компактних ПЗУ (в цьому випадку весь тракт системи обробки даних будується за блоковим принципом, що покращує ремонтопридатність системи обробки даних); простота табличних схем і дешифраторів, що мають кількість виходів, які відповідають значенням основ МСЧ. Результати розрахунку і порівняльного аналізу часу реалізації модульних операцій в МСЧ, на основі використання табличного принципу, показали наступне. При реалізації операції модульного складання (віднімання) з використанням табличного методу, залежно від величини l - байтового (l = 1, 2, 3, 4, 8) машинного слова даних, в 7,5 - 63,5 рази ефективніше, а для операції модульного множення, в 64 - 4096 разів ефективніше за часом виконання арифметичних модульних операцій, ніж використання суматорного методу в ПСС. На основі розроблених і вдосконаленого методів швидкої реалізації модульних операцій в розділі наведено алгоритми для їх реалізації, згідно з якими синтезований клас засобів обробки даних з формування сигналів у ТКС, на які отримано 9 патентів України, що підтверджує новизну і практичну значущість отриманих у дисертації наукових результатів роботи.

У **шостому розділі** дисертації вирішені сьома і шоста 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. Дослідження показали, що необхідні показники інформаційної безпеки (імітостійкість, інформаційна скритность) і завадозахищеності радіоканалу ТКС можуть бути забезпечені за рахунок застосування динамічного режиму функціонування радіоканалу з застосуванням нелінійних складних сигналів. Під динамічним режимом функціонування радіоканалу розумітимемо радіоканал, у якому форми випромінюваних сигналів або їх параметри змінюються з часом за законом, визначити який станція протидії може з імовірністю, що не перевищує допустимого значення. У розділі наводяться теоретичні основи удосконаленого методу динамічного режиму функціонування радіоканалу ТКС. Сформульовано і доведено твердження, які дають необхідні і достатні умови теоретичної (абсолютної) інформаційної та структурної скритності ТКС на рівні джерела складних сигналів. Суть удосконаленого методу обміну даними в ТКС полягає в наступному. Символи повідомлення від джерела інформації, які подані у вигляді m біт, надходять у динамічний модулятор, у якому відповідно до символів керуючої послідовності, здійснюється вибір 2^m з M складних сигналів і таким чином встановлюється відповідність: m біт – 2^m складних сигналів. Після визначено розробником системи часу T, відповідність m біт – 2^m складних сигналів змінюється за певним законом (правилом). Станція протидії може реалізовувати різні стратегії впливу на ТКС: перехоплення переданих сигналів та їх аналіз; спроби розпізнавання сигналів і визначення закону їх випромінювання; формування і постановка завад з метою нав'язування хибних повідомлень та ін. У демодуляторі на станції прийому після виявлення прийомним пристроєм синхропослідовності (СП) з необхідними значеннями ймовірності помилкової тривоги ($P_{лт.}$), пропуску сигналу ($P_{пр.}$), визначається момент часу, починаючи з якого в радіоканалі реалізується динамічний режим роботи, проводиться розрізнення одного з дозволених інформаційних сигналів. Після демодуляції формуються m біт повідомлення, які надходять одержувачу повідомлень. Необхідні значення зазначених імовірностей, а також значення показника структурної скритності системи (S_c) можуть бути забезпечені за рахунок: вибору сигналів з покращеними кореляційними, ансамблевими, структурними властивостями; забезпечення необхідної бази сигналів; використання радіоканалу з заданими значеннями ймовірності помилки $P_{пом.}$. Для випадку, якщо в радіоканалі параметрами, що змінюються, є кодова форма сигналу, що вибирається з певного ансамблю сигналів або різних ансамблів, а також несуча частота, то існує M станів системи:

$$M = M_f M_{кф} , \qquad (59)$$

де M_f – загальна кількість несучих частот; $M_{кф}$ – загальна кількість кодових форм складних сигналів.

Якщо динамічний режим, що реалізований із застосуванням методу «з поверненням», при якому на кожному інтервалі mT часу передачі m біт інформації дозволеними для випромінювання на частотах $M_f^д$ є $M_{кф}^д$ складних сигналів і вибираються вони відповідно до значень символів керуючої послідовності (гами), то ймовірність нав'язування складного сигналу визначається з використанням виразу:

$$P_{нав/сигн.} = k\frac{M_{f^д}M_{кф^д}}{M_f M_{кф}}, \qquad (60)$$

де k – число спроб, що застосовує станція протидії з метою нав’язування хибних повідомлень.

У таблицях 6-8 наведено значення ймовірностей нав'язування $P_{нав./с}$ на сигнал у ході використання як СП М-послідовностей, ХДС і характеристичних ПОС (ХПОС). Як параметри динамічного режиму, приймемо: M_f=1024, $M_f^д$=1, $M_{кф.}^д$=16.

Таблиця 6

Значення імовірності нав’язування хибного сигналу в ході застосування М-послідовностей

N	63	127	255	1023	4095
$P_{нав./с}$ при M_f=1	$4\cdot10^{-2}$	$7\cdot10^{-3}$	$3{,}8\cdot10^{-3}$	$2{,}6\cdot10^{-5}$	$2{,}6\cdot10^{-7}$
$P_{нав./с}$ при M_f=1024	$4\cdot10^{-5}$	$7\cdot10^{-6}$	$3{,}8\cdot10^{-6}$	$2{,}6\cdot10^{-7}$	$2{,}6\cdot10^{-8}$

Таблиця 7

Значення імовірності нав’язування хибного сигналу в ході застосуванні ХДС

N	66	172	255	1032	4000	10000
$P_{нав./с}$ при M_f=1	$1{,}5\cdot10^{-2}$	$2{,}1\cdot10^{-3}$	$9{,}6\cdot10^{-4}$	$8{,}8\cdot10^{-5}$	$4{,}8\cdot10^{-6}$	$7{,}8\cdot10^{-7}$
$P_{нав./с}$ при M_f=1024	$2{,}4\cdot10^{-6}$	$2\cdot10^{-6}$	$9{,}6\cdot10^{-6}$	$8{,}86\cdot10^{-8}$	$4{,}8\cdot10^{-9}$	$7{,}8\cdot10^{-10}$

Аналіз даних таблиць 6-8 показує, що в ході реалізації в радіоканалі динамічного режиму і використанні нелінійних ХПОС вже при періоді сигналу N=256 і кількості несучих частот M_f=1024 забезпечуються високі показники з погляду імітостійкості.

Таблиця 8

Значення імовірності нав’язування хибного сигналу в ході застосуванні ХПОС

N	64	100	256	512	1024	4000
$P_{нав./с}$ при M_f=1	$1{,}7\cdot10^{-5}$	$8\cdot10^{-6}$	$5{,}6\cdot10^{-8}$	$4\cdot10^{-6}$	$1{,}8\cdot10^{-10}$	$8\cdot10^{-11}$
$P_{нав./с}$ при M_f=1024	$1{,}7\cdot10^{-9}$	$7{,}8\cdot10^{-9}$	$5{,}6\cdot10^{-11}$	$4\cdot10^{-9}$	$1{,}8\cdot10^{-13}$	$7{,}8\cdot10^{-14}$

Виконано оцінку захищеності ТКС від нав'язування помилкових повідомлень, яка визначається зі співвідношення:

$$P_{нав./пов.} = (2^{-k})^n, \qquad (61)$$

де: 2^{-k} - число можливих станів джерела керуючої послідовності, яке визначається ансамблем дискретних сигналів - переносників інформації; n - довжина повідомлення, що надана в бітах.

У таблиці 9 наведено значення імовірності нав'язування $P_{нав./пов.}$ повідомлення для дискретних сигналів, отриманих на основі М-послідовностей, ПФВКТ і нелінійних КС. Як розмірність повідомлення вибрано значення n=32. У розрахунках $P_{нав./пов.}$, для випадку застосування в системі нелінійних КС, були відібрані послідовності, кореляційні характеристики яких близькі до оптимальних граничних значень з точки зору ПФВК ($R_{мах} \leq 1{,}5\sqrt{N}$).

Таблиця 9

Значення ймовірності нав'язування на повідомлення для різних систем дискретних сигналів

Період сигналу	Значення $P_{нав./пов.}$ для систем сигналів:		
	М-послідовності	ПФВКТ	Нелінійні КС
31	2^{-96}	2^{-288}	2^{-672}
63	2^{-96}	2^{-320}	2^{-768}
127	2^{-160}	2^{-448}	2^{-640}
1023	2^{-192}	2^{-608}	2^{-736}

Як видно з даних таблиці 9, значення $P_{нав./пов.}$ для нелінійних КС значно менші, ніж у випадку використання лінійних класів сигналів.

У стандарті UMTS (третє покоління системи з кодовим поділом каналів) як код первинної синхронізації використовується бінарна послідовність довжиною 256, що володіє аперіодичними бічними пелюстками аж до ¼, тобто $R_{max}=64$. Як альтернатива зазначеним послідовностям можуть бути запропоновані КС і НС у кінцевих полях (теоретичні основи синтезу зазначених систем сигналів наведені в розділах 2-3 даної роботи). В ході досліджень було показано, що виграш з завадостійкості і, отже, й завадозахищеності, в ході використання нелінійних КС (порівняно з використанням послідовностей, застосовуваних у стандарті UMTS), становить 3 дБ, а в ході використання як СП нелінійних ХДС виграш становить понад 4 дБ.

Серед систем фазоманіпульованих сигналів багато є таких, що утворені на базі систем Уолша. Відомо, що авто- і взаємнокореляційні функції послідовностей Уолша мають великі бічні пелюстки функції кореляції. Для покращення кореляційних властивостей сигналів формують похідні системи сигналів (ПСС). Була висловлена гіпотеза про можливість використання як основи - нелінійних КС і нелінійних сигналів у кінцевих полях, теоретичні основи синтезу яких розроблені під час досліджень .

Дисертаційні дослідження щодо синтезу похідних систем сигналів (ПСС) на основі систем нелінійних сигналів показали, що статистичні характеристики ПСС близькі до відповідних характеристик лінійних і нелінійних класів сигналів. При цьому значення максимальних бічних піків функцій взаємної кореляції ПСС менше, ніж у широко використовуваних у сучасних ТКС лінійних М послідовностей. Для ПСС, що створені на основі нелінійних КС з періодом 64 двійкових елементів, число пар сигналів, для яких значення максимальних бічних піків взаємно кореляційної функції (ВКФ) не перевищують 17 (так звана межа «щільної упаковки», що досягається в класі кращих з точки зору ВКФ послідовностей з трирівневою ПФВК),

становить 4,5 10^6 або 85% із загального числа можливих поєднань пар сигналів. При цьому ПСС мають покращені (порівняно з лінійними класами сигналів) ансамблеві і структурні властивості. Розроблено комплекс програмних засобів, що дозволив реалізовувати синтез ПСС і вирішувати завдання, які пов'язані з дослідженням властивостей зазначених систем сигналів.

Для вирішення завдань пошуку, виявлення, розрізнення сигналів важливо мати сигнали, для яких функція кореляції має нульові пелюстки поблизу центрального піку тіла невизначеності. Розроблений програмний комплекс дозволяє здійснювати пошук послідовностей, які володіють вказаними властивостями. Зокрема, було встановлено, що для КС з періодом 256 символів існує 302 сигнали, для яких бічні пелюстки ПФАК мають один і більше нульових викидів функції кореляції поблизу центрального піку, і більш ніж 215 000 пар сигналів, для яких бічні пелюстки ПФВК мають нульові значення. Наведені вище оцінки дозволяють стверджувати, що в ТКС, в якій як метод інформаційного обміну реалізується динамічний режим передачі даних і застосовуються нелінійні класи сигналів, забезпечуються високі показники завадозахищеності та інформаційної безпеки.

ВИСНОВКИ

У дисертації проведено теоретичне узагальнення і отримано нове вирішення науково - прикладної проблеми підвищення 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 та структурними властивостями.

1. До основних показників ефективності функціонування ТКС належать: пропускна здатність, завадозахищеність (завадостійкість, структурну та енергетичну скритність), інформаційна безпека (імітостійкість, інформаційна скритність), живучість, достовірність, продуктивність тощо. У процесі досліджень виконано аналіз проблем інформаційної безпеки, скритності і завадозахищеності існуючих ТКС, отримано сукупність часткових показників ефективності ТКС.

Аналіз методів інформаційного обміну в ТКС показує, що протягом тривалого часу в інформаційному каналі, тобто на фізичному рівні, відповідність: біт повідомлення - сигнал протягом часу залишається фіксованою, а як фізичні переносники даних застосовуються сигнали, що засновані на лінійних правилах побудови, і які володіють низькою структурною скритністю, обмеженими ансамблевими властивостями. У зазначених умовах, у процесі інформаційної протидії, можливими стратегіями порушника є: визначення змісту повідомлень, в ході використанні легальними абонентами ТКС алгоритмів криптографічного захисту даних; фальсифікація повідомлень; порушення цілісності даних; постановка різних типів завад та ін. Такий вплив порушника на систему може призвести до істотного погіршення показників ефективності ТКС (завадозахищеності, інформаційної безпеки, імітостійкості, імовірнісно-часових показників передачі повідомлень, живучості та ін.).

2. Проведені дослідження та порівняльний аналіз відомих методів покращення показників інформаційної безпеки та завадозахищеності показали, що одним з перспективних напрямів комплексного забезпечення необхідних значень зазначених показників є реалізація в радіоканалах ТКС динамічного режиму функціонування, коли протягом часу відповідність m біт - 2^m складних сигналів змінюється за складним законом (наприклад, за законом псевдовипадкової або випадкової послідовності), а як складні сигнали застосовуються сигнали, що засновані на нелінійних принципах побудови.

3. Найбільш важливими науковими результатами, що отримані в дисертації, є наступні.

Вперше отримано метод синтезу нелінійних криптографічних дискретних складних сигналів (КС), 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. Покращення зазначених показників ефективності досягається, зокрема, за рахунок можливості формування, із застосуванням отриманого методу, великих ансамблів дискретних послідовностей практично будь-якого періоду з необхідними (для тих чи інших додатків системи) значеннями бічних пелюсток функцій авто, - взаємної і стикової кореляційних функцій (КФ) в періодичному і аперіодичному режимах роботи, а також статистичними характеристиками КФ, які не поступаються аналогічним характеристикам кращих, з погляду КФ, лінійних класів сигналів. Зазначене дає можливість підвищити завадостійкість прийому сигналів до 4дБ. Нелінійні дискретні сигнали мають покращені, порівняно з лінійними класами сигналів, ансамблеві властивості. Так, для періоду послідовності N=1023 елементи, об'єм системи, складений з нелінійних КС більш ніж в 15 разів перевищує об'єм системи сигналів, що складається з сигналів з трирівневою функцією взаємної кореляції, і більш ніж в 1200 разів - обсяг системи, складеної з М-послідовностей. За рахунок поліпшених ансамблевих властивостей КС і динамічної зміни відповідності: біт повідомлення – складний сигнал, виникає можливість покращити показники інформаційної безпеки. Так, імітостійкість системи в ході застосування КС з періодом сигналу 1023 елемента на п'ять порядків вище, ніж при застосуванні лінійних класів сигналів (наприклад, М-послідовностей). При цьому необхідно підкреслити, що при вирішенні завдання покращення показників імітостійкості системи забезпечується й високий рівень завадостійкості прийому сигналів. Покращені, порівняно з лінійними класами сигналів, ансамблеві властивості КС дозволяють підвищити інформаційну скритність системи. Крім того, синтезовані з використанням розробленого методу КС, як показали результати проведеного тестування, за своїми статистичними властивостями, близькі до властивостей випадкових послідовностей, тобто володіють (за критерієм (3)) практично ідеальною структурною скритністю, оскільки володіють властивостями непередбачуваності символів послідовності, незворотності, випадковості, рівноймовірності та незалежності символів послідовності, що дає можливість збільшити структурну скритність ТКС.

Вперше отримано математичну модель структури складних нелінійних дискретних сигналів (НС) 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. Показано, що для визначення закону (правила) побудови нелінійних дискретних сигналів у кінцевих полях необхідно знати не менше половини символів з періоду сигналу. Наприклад, для періоду сигналу 1023 елемента виграш (з погляду структурної скритності) в ході використання отриманих у роботі систем сигналів, порівняно з сигналами лінійної форми (М-послідовностями), становить 50 разів, а при періоді 8192, - понад 300 разів.

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.

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

Результати розрахунку і порівняльного аналізу часу реалізації арифметичних модульних операцій в модулярній системі числення, на основі використання табличного принципу показали таке, що: при реалізації операції модульного складання (віднімання) з використанням табличного методу, залежно від величини l-байтового ($l = \overline{1-4,8}$) машинного слова, в 7,5 - 63,5 рази ефективніше, а для операції модульного множення, в 64 - 4096 разів ефективніше за часом виконання арифметичних модульних операцій, ніж при використанні суматорного методу в позиційній системі числення. Удосконалений 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. Так, виграш у часі синтезу сигналу із застосуванням отриманого методу, порівняно з відомим, для періоду сигналу 256 елементів, становить - 25,5 разів, а для періоду 9972 елементів - 1039,6 рази.

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

послідовностей з періодом від 256 до 2000 елементів із застосуванням розробленого методу складає 40 - 60 відсотків порівняно з методом синтезу системи сигналів, що заснований на переборі всіх можливих варіантів послідовностей. В ході реалізації розглянутого методу можливі пропуски (втрати) під час знаходженні сигналів із заданими властивостями, але, як показали дослідження, відсоток таких втрат незначний, і для зазначених періодів становить не більше 8 відсотків.

Удосконалено метод оцінки властивостей нелінійних дискретних складних сигналів, у якому на відміну від відомих, використані алгебраїчні властивості елементів кінцевого поля, що дозволяє збільшити швидкодію процесу дослідження властивостей сигналів, і, таким чином, підвищити продуктивність синтезу системи сигналів з необхідними властивостями. Так, для періоду сигналу 10098 елементів (обсяг системи складає 2880 сигналів), виграш у продуктивності синтезу системи сигналів із заданими властивостями в ході використання розробленого методу, порівняно з відомим методом, становить 720 разів.

Удосконалено метод синтезу 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. Застосування такого методу дозволяє отримати виграш в ході формування всієї системи нелінійних дискретних сигналів характеристичного типу (з використанням програмної моделі), порівняно з відомим, при періоді сигналу, що формується, 1020 елементів, - в 16 разів, а при періоді 2380 - 26 разів.

Розвинено теоретичні та методологічні основи функціональної побудови ТКС, у тому числі, з динамічним кодуванням, що включають обгунтовані і доведені необхідні і достатні умови забезпечення необхідних показників завадозахищеності, інформаційної та структурної скритності системи на рівні джерела складних сигналів. Розроблено удосконалений метод інформаційного обміну даними, в якому, на відміну від відомих, застосовуються принципи динамічного радіоканалу на основі здійснення зміни відповідності: біт повідомлення - складний сигнал і використання, як складних сигналів, нелінійних дискретних сигналів з необхідними властивостями, що дозволяє покращити показники інформаційної безпеки та завадозахищеності. Так імовірність нав’язування хибного повідомлення (при довжині повідомлення 32 біта) в ході застосування нелінійних криптографічних сигналів з періодом 1024 елементів складає 2^{-736}.

4. На основі розроблених і удосконалених у дисертації методів синтезу систем нелінійних сигналів, швидкої реалізації модульних операцій наведено алгоритми для їх реалізації, відповідно до яких синтезований клас апаратних засобів формування і обробки сигналів, на які отримано 14 авторських свідоцтв на винаходи і патентів України, що підтверджує новизну і практичну значущість отриманих в дисертації наукових результатів роботи.

5. Розроблено комплекс програмних засобів, який реалізує методи синтезу та дослідження властивостей нових класів складних нелінійних дискретних сигналів.

6. Обгрунтованість отриманих результатів підтверджується комплексним урахуванням повного набору факторів, що впливають на показники ефективності

функціонування ТКС. Додатковим підтвердженням обгрунтованості є збіг результатів, отриманих аналітичними методами, з даними численних імітаційно-математичних моделей, які використовують характеристики реальних реалізацій сигналів і завад, а також несуперечливістю розроблених аналітичних описів і формулювань основним положенням теорії захисту інформації, теорії інформації, теорії систем сигналів, теорії потенційної завадостійкості. Крім того, достовірність підтверджується використанням деяких з отриманих результатів у практичних технічних розробках на підприємствах промисловості.

7. Наукові та практичні результати дисертаційної роботи доцільно використовувати:

- під час проведення науково-дослідних та дослідно-конструкторських робіт з розробки методів і засобів синтезу систем дискретних сигналів, що використовуються в ТКС;
- у перспективних радіоканалах ТКС у вигляді технічних засобів формування, обробки і передачі інформації фізичного рівня, зокрема, для організації завадозахищених інформаційних каналів розподілених телекомунікаційних мереж;
- в ході вивчення навчальних дисциплін з теорії телекомунікаційних і інформаційних мереж.

8. Сукупність отриманих у дисертації наукових результатів, їх позитивна оцінка обгрунтованості та достовірності, наукової та практичної значущості, дозволяють вважати сформульовану наукову проблему вирішеною, а поставлену мету: забезпечення завадозахищеності та інформаційної безпеки телекомунікаційної системи в умовах зовнішніх і внутрішніх впливів на основі розвитку теорії синтезу нових класів складних нелінійних дискретних сигналів з необхідними властивостями, а також теорії і практики інформаційного обміну в телекомунікаційній системі - досягнутою.

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Статті в наукових фахових виданнях та виданнях, що входять до науково-метричних баз:

1. Бондаренко М.Ф. Методологические основы концепции и политики безопасности информационных технологий [Текст]/ М.Ф.Бондаренко, И.Д. Горбенко, А.А. Замула // Радиотехника, Харьков, ХНУРЭ. – 2001. – Вып. 119. – С. 5–16.

2. Замула А.А. Методы аутентификации в безусловно-стойких криптосистемах [Текст]/ А.А.Замула, Г.Н. Гулак // Радиотехника. Харьков, ХНУРЭ. – 2001. – Вып. 119. – С. 69–77.

3. Замула А.А. Методы обеспечения аутентификации с введеним избыточности [Текст]/ А.А. Замула, И.Д. Горбенко // Радиотехника. Харьков, ХНУРЭ – 2001. – Вып. 119. – С. 77–81.

4. Краснобаев В.А. Алгоритмы сжатия табличных цифровых данных результатов выполнения арифметических операций в системе остаточных классов

[Текст]/ В.А. Краснобаев А.А. Замула., Я.В. Илюшко // Радиотехника. Всеукр. Межвед. науч.-техн. сб. – 2005. – Вып. 141. – С. 217–225.

5. Барсов В.И. Метод повышения производительности и отказоустойчивости нейрокомпьютеров обработки криптографической информации автоматизированных систем управления специального назначения на основе модулярной арифметики [Текст]/ В.И. Барсов., В.А.Краснобаев, А.А. Замула, Я.В. Илюшко // Прикладная радиоэлектроника, Х.: ХНУРЭ. – 2007. – №2. – С. 282–289.

6. Замула А.А. Методология анализа рисков и управлення рисками [Текст]/ А.А. Замула // Радиотехника. Харьков, ХНУРЭ – 2002. – Вып. 126. – С.56–71.

7. Барсов В.И. Концепция создания системы обработки информации беспилотных летательных аппаратов на основе использования кодов модулярной арифметики [Текст]/ В.И. Барсов, А.А. Сиора, В.А. Краснобаев, А.А. Замула, // Прикладная радиоэлектроника. Научно-технический журнал. – 2008. – Том 7, № 3. – С. 304–307.

8. Мартиненко С.О. Метод технічної реалізації арифметичних операцій у модулярній системі числення на основі використання принципу кільцевого зсуву [Текст] / С.О.Мартиненко, В.А. Краснобаєв, С.О.Кошман, О.А Замула, М.С. Деренько // Вісник ХНТУСГ імені Петра Василенка. – 2009. – Вип. 87. – С. 71–73.

9. Краснобаев В.А Метод обработки криптографической информации в модулярной системе счисления, основанный на принципе кольцевого сдвига [Текст]/ В.А. Краснобаев, С.О. Мартыненко, Ж.В. Дейнеко, А.А. Замула, А.А. Баклыков. // Прикладная радиоэлектроника. Научно-технический журнал. Тематический выпуск, посвященный проблемам обеспечения безопасности информации. – 2009. – Том 8, № 3. – С. 343–350.

10. Мартиненко С.О. Метод снижения вычислительной сложности реализации RSA криптопреобразований на основе использования принципа кольцевого сдвиги в модулярной системе счисления [Текст] / С.О. Мартиненко, В.А. Краснобаев, О.А. Замула // Прикладная радиоелектроника: науч.- техн. журнал – 2010. – Том 9, № 3. – С. 454 – 459.

11. Землянко Ю.В. Принципи та порядок розробки комплексних систем захисту інформації в інформаційно – телекомунікаційних системах [Текст]/ Ю.В.Землянко, О.А.Замула, О.О.Ткач // Прикладная радиоелектроника: науч.- техн. Журнал. – 2010. – Том 9, № 3 – С. 460–469.

12. Горбенко И.Д. Синтез одного класса дискретних сигналов в полях Галуа [Текст]/ И.Д. Горбенко, Е.П. Колованова, А.А. Замула, Т.А. Ярыгина // Прикладная радиоелектроника: науч.- техн. Журнал. – 2011. – Том 10, № 2. – С. 240–244.

13. Замула А.А. Методология анализа рисков инфомационной безопасности при проектировании информационных систем с использованием нечетких сетей [Текст]/ А.А. Замула, Б.В. Волобуев., В.И. Черныш // Наука і техніка Повітряних Сил Збройних Сил України: наук.- техн. журнал. Харьков. – 2011. – № 2. – С. 94–98.

14. Замула А.А. Метод синтеза сигналов с заданными ограничениями на уровень боковых лепестков корреляционной функции [Текст] / А.А. Замула, Р.И. Киянчук, Т.Е. Ярыгина, Е.П. Колованова // Восточно – европейский журнал передових технологий: науч.- техн. журнал – 2011. – № 5/9 (53). – С. 30–34.

15. Замула А.А. Метод построения множества изоморфизмов характеристических кодов [Текст] / А.А. Замула // Інформаційно – керуючі системи на залізничному транспорті: науч.- техн. Журнал. – 2011, № 5 (90) – С. 32–37.

16. Горбенко И.Д. Методы построения и исследования свойств производных нелинейных рекуррентных последовательностей [Текст]/ И.Д. Горбенко, А.А. Замула, Р.И. Киянчук //Радиотехника: Всеукраинский межведомственный научно – техничнеский сборник. – 2011. – Выпуск 166. – С. 125–133.

17. Замула А.А. Защита информации в информационно-телекоммуникационной системе от внутреннего нарушителя [Текст]/ А.А. Замула, А.П. Шумар //Радиотехника: Всеукраинский межведомственный научно – техничнеский сборник – 2011, Выпуск 165 – С. 213–217.

18. Chernisn V.I. Assessing security Risks Using the Apparatus of Fuzzy Logic Theori / V.I. Chernisn, K.I. Ivanov, A.A. Zamula [Текст]// Вісник Харківського національного університету імені В.Н. Каразіна. Серія «Математичне моделювання. Інформаційні технології. Автоматизовані системи управління». – 2011 – № 987. Випуск 18. – С.145–151.

19. Замула А.А. Исследование уязвимости коммуникационной сети в процессе аудита информационной безопасности [Текст]/ А.А. Замула, К.И. Іванов // Науково-технічний журнал “Інформаційні-керуючі системи на залізничному транспорті. – 2012. – №2. – С. 56–59.

20. Замула А.А. Методы генерации псевдослучайных последовательностей и оценка их свойств [Текст]/ А.А. Замула, Д.А. Семченко // Прикладная радиоелектроника. – 2012. –Том 2. – С. 76–79.

21. Горбенко И.Д. Синтез систем сигналов с заданными корреляционными свойствами, законами формирования, структурными и ансамблевыми свойствами [Текст]/ И.Д.Горбенко, А.А. Замула // Прикладная радиоелектроника. Научно-технический журнал. Харьков. – 2012. – Том 2. – С. 293–298.

22. Замула А.А. Количественная оценка уязвимостей информационно-телекоммуникационных систем [Текст]/ А.А. Замула, С.А. Сирота, Н.И. Косиковская // Радиотехника. Всеукраинский Научно-технический сборник. – 2012. – №171, вып. 4. – С. 171–177.

23. Замула А.А. Визначення найбільш небезпечних загроз в методиці оцінки інформаційних ризиків [Текст]/ А.А. Замула, В.И. Черныш. // Науково-технічний журнал “Інформаційні-керуючі системи на залізничному транспорті. – 2012 – №3. – С.76–80.

24. Замула А.А. Предложения по построению широкополосных систем передачи со сложными сигналами [Текст]/ А.А. Замула // Радиотехника №171. Всеукраинский Научно-технический сборник. – 2012. – Вып 4. – С. 177–185.

25. Замула А.А. Оценивание временной задержки сигнала с использованием технологии распределенного спектра [Текст]/ Ю.В. Землянко // Науково-технічний журнал “Інформаційні-керуючі системи на залізничному транспорті – 2012. – №4. – С. 58–63.

26. Замула А.А. Генераторы псевдослучайных чисел, основанные на дискретном логарифме [Текст]/ А.А. Замула, Д.А. Семченко // Научно-технический

журнал Технологический аудит и резервы производства. Харьков. – 2013. – № 5 (13). – С. 28–31.

27. Замула А.А. Ансамблевые свойства характеристических дискретних сигналов [Текст] / А.А. Замула // Науково-технічний журнал Системи обробки інформації. Харьков. – 2013.– Випуск 8 (115). – С. 213–216.

28. Замула А.А. Оценка защищенности информационных систем от угроз [Текст]/ Землянко Ю.В., Коваль С.Г. // Системи управління, навігації та зв'язку. – 2013. – Випуск 3 (27). – С. 123–128.

29. Замула О.А. Теоретичні основи побудови криптографічних систем абсолютної стійкості [Текст]/ Замула О.А. // Науково-технічний журнал Системи обробки інформації. – 2013. – Випуск 4 (111). – С. 101–106.

30. Замула А.А. Метод построения многофазных характеристических дискретных сигналов [Текст]/ А.А. Замула // Всеукраинский Научно-технический сборник Радиотехника. – 2013. – Вып. 172. - С. 47–51.

31. Замула А.А. Методы построения генераторов псевдослучайных последовательностей на основе параллельных вычислений с использованием графических процессоров [Текст]/ А.А.Замула, Д.А. Семченко // Наука і техніка Повітряних сил Збройних сил України. – 2014. – № 1 (14). – С. 182–186.

32. Замула А.А. Системы обнаружения и предотвращения вторжений [Текст]/ А.А. Замула, В.Л. Морозов // Радиотехника: Всеукраинский межведомственный научно – техничнеский сборник. – 2014. – Вып. 176. – С. 122 – 127.

33. Замула А.А. Мощность метода кодирования характеристических дискретних сигналов [Текст]/ А.А. Замула // Системи обробки інформації. – Х. ХУПС, 2014р. – Вып. 2 (118).– С. 162–168.

34. Горбенко И.Д. Синтез систем сложных сигналов с заданными свойствами корреляционных функций для приложений многопользовательских систем с кодовым разделением абонентов [Текст]/ А.А. Замула, Е.А. Семенко // Системи обробки інформації:– Х.: ХУПС. – 2014. – Вып. 9 (125).– С. 25–30.

35. Замула А.А. Условия реализации динамического режима функционирования в системе связи [Текст]/ А.А.Замула, Е.А.Семенко, Д.А. Семченко // Збірник наукових праць Харківського університету Повітряних сил. – 2014. – № 3 (40). – С. 113–116.

36. Замула О.А. Аналіз і обґрунтування критеріїв і показників ефективності криптографічних генераторів псевдовипадкових чисел [Текст]/ А.А. Замула, Д.О. Семченко, Ю.В. Землянко // Системи обробки інформації:– Х.: ХУПС. – 2014р. – Вып. 4 (120).– С. 131–136.

37. Замула А.А. Практические аспекты имплементации международных стандартов в систему организации воздушного движения Украины [Текст]/ А.А.Замула, В.И. Черныш // Информационное противодействие угрозам терроризма. Научно-технический журнал: Россия. – 2014. – №22. – С. 111–118.

38. Горбенко И.Д. Ускоренный метод синтеза дискретных сигналов с необходимыми свойствами для приложений телекоммуникационных систем и сетей

[Текст]/ Замула А.А., Семенко Е.А // Системи обробки інформації:– Х.: ХУПС. – 2015. – Вип. 3 (128).– С. 71–74.

39. Замула А.А. Перспективы применения нелинейных дискретных сигналов в современных телекоммуникационных системах и сетях [Текст]/ А.А. Замула, Е.А Семенко // Системи обробки інформації:– Х.: ХУПС. – 2015. – Вип. 5 (130).– С. 129–134.

40. Горбенко И.Д. Ансамблевые и корреляционные свойства криптографических сигналов для приложений телекоммуникационных систем и сетей [Текст]/ Замула А.А., Семенко Е.А // Радиотехника: Всеукраинский межведомственный научно – техничнеский сборник – 2015. – Вып. 181. – С. 110 – 117.

Тези доповідей у збірниках міжнародних форумів та науково-практичних конференцій:

41. Замула А.А. Методы управления средствами сетевой безопасности [Текст] / Замула А.А.// І-я международная конференция «Глобальные информационные системы. Проблемы и тенденции развития». – Харьков. ХНУРЭ. – 2006. – С. 316–317.

42. Замула О.А. Концепція створення комплексних систем захисту інформації в сучасних інформаційно-телекомунікаційних системах [Текст] / Замула О.А. // Системний аналіз. Інформатика. Управління (САІУ-2010): Тези доповідей Всеукраїнської науково-практичної конференції (м. Запоріжжя, 04-05 березня 2010 року)/ Міністерство освіти і науки України, Класичний приватний університет, Запорізький національний технічний університет, Академія наук вищої школи України. – Запоріжжя: Вид-во КПУ. – 2010. – С. 72–73.

43. Замула А.А. Теория и практика оценивания информационных рисков с использованием математического аппарата нечеткой логики [Текст] / Замула А.А., Одарченко А. // XIII Международная научно-практическая конференция. «Безопасность информации в информационно-телекоммуникационных системах». Киев. – 2010. – С. 47–48.

44. Замула О. Принципи створення комплексних систем захисту інформації в сучасних інформаційно-телекомунікаційних системах [Текст] / Замула О., Одарченко О., Халіна О. // XIII Международная научно-практическая конференция. «Безопасность информации в информационно-телекоммуникационных системах». Киев. – 2010. – С. 103–104.

45. Замула А.А. Использование технологи распределенного спектра при решении некоторых классических задач приема сигналов в корпоративних системах [Текст] / Замула А.А. // Міжнародна науково-практична конференція «Перспективи розвитку інформаційних та транспортно-митних технологій у митній справі, зовнішньо економічній діяльності та управлінні організаціями», м. Дніпропетровськ. – 2011. – С. 164–166.

46. Замула А.А. Оценивание рисков информационной безопасности в современных информационных системах [Текст] / Замула А.А.,Черныш В.И.,

Иванов К.И. // 14 Международная научно-практическая конференция. «Безопасность информации в информационно-телекоммуникационных системах». Киев. – 2011. - С. 31.

47. Горбенко И.Д. Защита ресурсов информационной системы на основе сложных сигналов [Текст] / Горбенко И.Д., Замула А.А. //. 4 –й Международный радиоэлектронный форум «Прикладная радиоэлектроника. Состояние и перспективы развития».Сборник научных трудов. Т.II. Международная конференція «Телекоммуникационные системы и технологи». – Харьков, АНПРЭ. - 2011. – С. 298 – 301.

48. Горбенко И.Д. Метод построения многофазных характеристических дискретных сигналов [Текст] / Горбенко И.Д., Замула А.А., Киянчук Р.И. // 4 –й Международный радиоэлектронный форум «Прикладная радиоэлектроника. Состояние и перспективы развития».Сборник научных трудов. Т.II. Международная конференція «Телекоммуникационные системы и технологи». – Харьков. АНПРЭ. – 2011. – С. 295 – 297.

49. Замула А.А. Метод формирования множества дискретных сигналов с заданными корреляционными свойствами [Текст] / Замула А.А., Ярыгина Т.Е. // 4 –й Международный радиоэлектронный форум «Прикладная радиоэлектроника. Состояние и перспективы развития».Сборник научных трудов. Т.II. Международная конференція «Телекоммуникационные системы и технологи». – Харьков. АНПРЭ. – 2011. – С. 307 – 310.

50. Замула А.А. Критерии оценки генераторов псевдослучайных последовательностей для криптографических приложений /Замула А.А., Семченко Д.А. [Текст] //15 Юбилейная Международная научно-практическая конференция. «Безопасность информации в информационно-телекоммуникационных системах» . – 2012. – С. 63 – 64.

51. Замула А.А. Ранжирование угроз при помощи метода анализа иерархий [Текст] / Замула А.А., Черныш В.И. // 15 Юбилейная Международная научно-практическая конференция. «Безопасность информации в информационно-телекоммуникационных системах». Киев. – 2012. – С. 64 – 65.

52. Замула А.А. Методы построения генераторов, основапнные на дискретном логарифме [Текст] /Замула А.А., Семченко Д.А. //16-я Международная научно-практическая конф. Киев. – 2013. – С. 33–34.

53. Замула А.А. Обнаружение атак систем анализа сетевого трафика [Текст] / Замула А.А., Алиференко Р.И. // Международная научно-техническая конференция «Компьютерное моделирование в наукоемких технологиях» (КМНТ-2014). Харьков, ХНУ имени Каразина В.Н.– 2014 – С. 11–14.

54. Замула А.А. Модели оценки рисков информационной безопасности [Текст] / Замула А.А., Черныш В.И. // Современные проблемы радиотехники и телекоммуникаций «РТ – 2014». Материалы 10-й международной научно – технической конференции. (Севастополь, 12-17 мая 2014 г.). – С. 315.

55. Замула А.А. Методы противодействия преднамеренным помехам в телекоммуникационных системах и сетях [Текст] / Замула А.А. // Сучасні напрями розвитку інформаційно-комунікаційних технологій та засобів управління. Матеріали

п’ятої міжнародної науково-технічної конференції. – Полтава: ПНТУ; Баку; ВА ЗС АР; Кіровоград; КЛА НАУ; Харків; ДП «ХНДІ ТМ». – 2015. – С. 64.

56. Замула А.А. Метод оптимизации выбора дискретних сигналов в целях обеспечения информационной безопасности в многопользовательских телекоммуникационных системах [Текст] / Замула А.А. // Інформаційна безпека України: Наукові доповіді та тези учасників науково-технічної конференції. м. Київ. – 2015. – С.104–105.

57. Замула А.А. Программный комплекс генерации и исследования дискретных последовательностей для приложений информационной безопасности в телекоммуникационных системах [Текст] / Замула А.А., Семенко Е.А // Інформаційна безпека України: Наукові доповіді та тези учасників науково-технічної конференції. м. Київ. – 2015. – С.105–106.

58. Замула О.А. Оцінка ефективності телекомунікаційної системи з кодовим поділом абонентів, що використовує нелінійні дискретні сигнали [Текст] / Замула А.А. // Матеріали IV міжнародної науково-технічної конференції «Захист інформації і безпека інформаційних систем». м. Львів. – 2015. – С. 81–83.

59. Замула, А.А., Связь, навигация, наблюдение в системе организации воздушного движения [Текст] / В.И. Черныш, А.В. Ефремов: монографія. – Харьков: Издательство Лидер, 2014. – 208 с.

Авторські свідоцтва на винахід та Державні патенти України на корисну модель:

60. А.с. 1455976 СССР. H03K 3/84 Устройство для формирования псевдослучайных сигналов [Текст] / Горбенко И.Д., Замула А.А., Родионов С.В., Левин П.Ю., Гавриленко (СССР). – №4210710; заявл. 16.03.87; опубл. 01.10.1988.

61. А.с. 1441413 СССР. H06F 15/20 Устройство для формирования элементов расширенных полей Галуа GF (Pn) и кодовых последовательностей на их основе [Текст] / Горбенко И.Д., Замула А.А., Глазин Д.Е, Бычковский И.А., Захаров А.Т. (СССР). – №4230384; заявл. 15.01.87; опубл. 01.08.1988.

62. А.с. 1360545 СССР. 4H 03K 3/84 Устройство для формирования псевдослучайных сигналов / Горбенко И.Д., Замула А.А., Стасев Ю.В., Бессарабенко К.В., Борисов В.И. (СССР). – №4017635, заявл. 06.02.86; опубл. 15.08.1987.

63. А.с. 1326162 СССР. 4H 03K 3/84 Устройство для формирования псевдослучайных сигналов. [Текст] / Горбенко И.Д., Замула А.А., Стасев Ю.В., Кулешов В.Л., Мясоедов А.П. (СССР). – №3970022; заявл. 28.10.85; опубл. 22.03.1987.

64. А.с. 1353310 СССР. 4H 03K 3/84 Устройство для формирования псевдослучайных сигналов. [Текст] / Горбенко И.Д., Замула А.А., Стасев Ю.В., Кулешов В.Л., Давыдов Г.П., Аносов А.М. (СССР).– №4020323; заявл. 11.02.86; опубл. 15.07.1987..

65. Пат. № 49054 Україна, Пристрій для виявлення помилок у модулярній системі числення [Текст] / Горбенко І.Д.; – Мартиненко С.О., Замула О.А.,

Краснобаєв В.А., Горбенко Ю.І., Дейнеко Ж.В.; власник Харківський національний університет радіоелектроніки. – опубл. 12.04.2010, Бюл. № 7.

66. Пат. № 49711 Україна, Спосіб виявлення помилок у системі обробки цифрової інформації, що функціонує у модулярній системі числення [Текст] / Горбенко І.Д., Мартиненко С.О., Замула О.А., Краснобаєв В.А., Горбенко Ю.І.; власник Харківський національний університет радіоелектроніки. – опубл. 11.05.2010, Бюл. № 9.

67. Пат. № 49712 Україна, Пристрій для додавання і віднімання чисел за модулем М в модулярної системи числення [Текст] / Горбенко І.Д., Мартиненко С.О., Замула О.А., Краснобаєв В.А., Бобух В.А., Горбенко Ю.І.; власник Харківський національний університет радіоелектроніки, – опубл. 11.05.2010, Бюл. № 10.

68. Пат. № 62490 Україна, Пристрій для порівняння чисел у класі лишків [Текст] / Горбенко І.Д., Загумена К.В., Замула О.А., Краснобаєв В.А., Горбенко Ю.І.; власник Харківський національний університет радіоелектроніки, – опубл. 25.08.2011, Бюл. № 16.

69. Пат. № 62313 Україна, Табличний пристрій для множення двох чисел за модулем m класу лишків [Текст] / Горбенко І.Д., Загумена К.В., Замула О.А., Краснобаєв В.А., Горбенко Ю.І.; власник Харківський національний університет радіоелектроніки, – опубл. 25.07.2011, Бюл. № 16.

70. Пат. № 60078 Україна, Табличний пристрій для множення чисел за модулем m у класі лишків [Текст] / Горбенко І.Д., Дугін М.В., Замула О.А., Краснобаєв В.А., Горбенко Ю.І.; власник Харківський національний університет радіоелектроніки. – опубл. 10.06.2011, Бюл. № 11.

71. Пат. № 61798 Україна Пристрій для піднесення чисел до квадрата за модулем m класу лишків [Текст] / Горбенко І.Д., Загумена К.В., Замула О.А., Краснобаєв В.А., Горбенко Ю.І.; власник Харківський національний університет радіоелектроніки. – опубл. 25.07.2011, Бюл. № 14.

72. Пат. № 92155 Україна Пристрій для перетворення позиційного двійкового коду у лишок за довільним модулем [Текст] / Горбенко І.Д., Замула О.А., Краснобаєв В.А., Горбенко Ю.І.; власник Харківський національний університет радіоелектроніки, – опубл. 11.08.2014, Бюл. № 15.

73. Пат. № 91894 Україна Пристрій для перетворення позиційного двійкового коду у лишки за двома довільними модулями [Текст] / Горбенко І.Д., Замула О.А., Краснобаєв В.А., Горбенко Ю.І.; власник Харківський національний університет радіоелектроніки, – опубл.25.07.2014, Бюл. № 14.

АНОТАЦІЯ

Замула О.А. Моделі і методи синтезу складних сигналів з необхідними властивостями для захищених телекомунікаційних систем. – Рукопис.

Дисертація на здобуття наукового ступеня доктора технічних наук за спеціальністю 05.12.02 – телекомунікаційні системи та мережі. – Український державний університет залізничного транспорту, Харків, 2016.

У дисертаційній роботі вирішується актуальна науково-прикладна проблема, яка полягає в підвищенні завадозахищеності та інформаційної безпеки телекомунікаційної системи в умовах внутрішніх і зовнішніх впливів на основі розробки моделей і методів синтезу систем складних нелінійних дискретних сигналів з покращеними властивостями.

Метою роботи є покращення показників ефективності телекомунікаційної системи, а саме, - завадозахищеності та інформаційної безпеки на основі вдосконалення методологічних основ побудови телекомунікаційної системи шляхом розробки методів інформаційного обміну, моделей та методів синтезу нових класів нелінійних дискретних складних сигналів з необхідними ансамблевими, кореляційними, структурними властивостями.

У дисертаційній роботі вперше отримано: метод синтезу складних нелінійних дискретних криптографічних сигналів, що використовує випадкові (псевдовипадкові) процеси, і дозволяє створювати сигнали з необхідними ансамблевими, структурними та кореляційними властивостями, що дає змогу покращити показники завадозахищеності та інформаційної безпеки телекомунікаційної системи в умовах зовнішніх і внутрішніх впливів; математична модель структури складних нелінійних дискретних сигналів у кінцевих полях Галуа, яка визначає залежність характерів елементів мультиплікативної групи поля Галуа та символів дискретних послідовностей, що дає змогу встановити значення показників завадозахищеності (структурної скритності) дискретних сигналів; метод реалізації арифметичних модульних операцій складання та віднімання, які засновані на табличному принципі реалізації арифметичних операцій шляхом використання спеціального коду табличного множення, що дозволяє підвищити швидкодію виконання модульних операцій складання та віднімання; метод реалізації арифметичної модульної операції множення, який заснований на використанні табличного принципу, шляхом використання процедури порозрядного визначення результату операції, що дозволяє підвищити швидкодію виконання операцій модульного множення. В ході дисертаційних досліджень удосконалено: метод синтезу нелінійних дискретних складних сигналів, у якому, на відміну від відомих, застосовується залежність між елементами й індексами елементів кінцевого поля, що дозволяє підвищити швидкодію синтезу сигналів; метод синтезу нелінійних дискретних криптографічних сигналів, у якому, на відміну від відомих, використовуються механізми направленого (обмеженого) перебору сигналів, для визначення таких, які відповідають відповідним вимогам щодо властивостей сигналів, що дозволяє підвищити продуктивність синтезу сигналів; метод оцінки властивостей дискретних сигналів, у якому на відміну від відомих, застосовані 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 послідовності сигналу для формування всієї множини сигналів, що відноситься до цієї системи сигналів, що дозволяє підвищити продуктивність

синтезу сигналів; метод інформаційного обміну даними, у якому, на відміну від відомих, застосовується зміна, за певним правилом, відповідності біт повідомлення – складний сигнал, і як складні сигнали застосовуються нелінійні дискретні сигнали з необхідними ансамблевими, структурними та кореляційними властивостями, що дає змогу покращити показники інформаційної безпеки та завадозахищеності; метод реалізації арифметичних модульних операцій складання та віднімання, який, на відміну від відомих, заснований на використанні принципу кільцевого зсуву, шляхом надання залишків числа двійковим кодом, за рахунок використання властивостей циклічних перестановок вмісту кільцевого регістру, що дозволяє підвищити швидкодію виконання модульних операцій.

Ключові слова: завадозахищеність, скритність, завадостійкість, кореляційні властивості, система сигналів, дискретний сигнал, арифметична модульна операція, медулярна система числення, синтез сигналів, динамічний режим функціонування, криптографічний сигнал, ізоморфізм.

АННОТАЦИЯ

Замула А.А. Модели и методы синтеза сложных сигналов с необходимыми свойствами для защищенных телекоммуникационных систем. – Рукопись.

Диссертация на соискание ученой степени доктора технических наук по специальности 05.12.02 - телекоммуникационные системы и сети. - Украинская государственная академия железнодорожного транспорта, Харьков, 2016.

Диссертация посвящена решению актуальной научно-прикладной проблеме, которая состоит в повышении помехозащищенности и информационной безопасности телекоммуникационной системы в условиях внутренних и внешних воздействий на основе разработки моделей и методов синтеза систем сложных нелинейных дискретных сигналов с улучшенными свойствами.

Целью работы является улучшение показателей эффективности телекоммуникационной системы, а именно, помехозащищенности и информационной безопасности на основе совершенствования методологических основ построения телекоммуникационной системы путем разработки методов информационного обмена, моделей и методов синтеза новых классов нелинейных дискретных сложных сигналов с требуемыми ансамблевыми, корреляционными, структурными свойствами.

В диссертационной работе впервые получены: метод синтеза сложных нелинейных дискретных криптографических сигналов, использующий случайные (псевдослучайные) процессы, и позволяющий создавать сигналы с необходимыми ансамблевыми, структурными и корреляционными свойствами, и, на этой основе, улучшить показатели помехозащищенности и информационной безопасности телекоммуникационной системы в условиях внешних и внутренних воздействий; математическая модель структуры сложных нелинейных дискретных сигналов в конечных полях Галуа, которая, на основе установленной зависимости характеров элементов мультипликативной группы поля Галуа и символов дискретных последовательностей, позволяет определить значения показателей

помехозащищенности (структурной скрытности) дискретных сигналов; метод реализации арифметических модульных операций сложения и вычитания, основанный на табличном принципе реализации арифметических операций путем использования специального кода табличного умножения, что позволяет повысить быстродействие выполнения модульных операций сложения и вычитания; метод реализации арифметической модульной операции умножения, основанный на использовании табличного принципа путем использования процедуры поразрядного определения результата операции, что позволяет повысить быстродействие выполнения операций модульного умножения. В ходе диссертационных исследований усовершенствованы: метод синтеза нелинейных дискретных сложных сигналов, в котором, в отличие от известных, применяется зависимость между элементами и индексами элементов конечного поля, что позволяет повысить быстродействие синтеза сигналов; метод синтеза нелинейных дискретных криптографических сигналов, в котором, в отличие от известных, используются механизмы направленного (ограниченного) перебора сигналов для отбора сигналов, отвечающих соответствующим требованиям, что позволяет повысить производительность синтеза сигналов; метод оценки свойств дискретных сигналов, в котором в отличие от известных, использованы алгебраические свойства элементов конечного поля, что позволяет увеличить быстродействие процесса исследования свойств сигналов и, таким образом, повысить производительность синтеза системы сигналов с необходимыми свойствами; метод синтеза всей системы нелинейных дискретных сигналов, в котором, в отличие от известных, используется процедура считывания и записи (по определенному правилу) символов последовательности сигнала для формирования всего множества сигналов, относящихся к этой системе сигналов, что позволяет повысить производительность синтеза сигналов; метод информационного обмена данными, в котором, в отличие от известных, осуществляется смена, по определенному правилу, соответствия: бит сообщения - сложный сигнал и, в качестве сложных сигналов, применяются нелинейные дискретные сигналы с необходимыми ансамблевыми, структурными и корреляционными свойствами, что позволяет улучшить показатели информационной безопасности и помехозащищенности; метод реализации арифметических модульных операций сложения и вычитания, который, в отличие от известных, основан на использовании принципа кольцевого сдвига, путем представления остатков числа двоичным кодом, за счет использования свойств циклических перестановок содержимого кольцевого регистра, что позволяет повысить быстродействие выполнения модульных операций.

Сформирована совокупность безусловных частных показателей эффективности, интегральный безусловный критерий защищенной телекоммуникационной системы. Формализованы требования (ограничения) на безусловные показатели, сформулирована постановка проблемы. Разработаны математическое и программное обеспечение, реализующие предложенные методы и вычислительные алгоритмы синтеза систем сложных нелинейных дискретных сигналов в конечных полях Галуа и систем сложных нелинейных дискретных криптографических сигналов. Разработанное программное обеспечение позволяет:

генерировать нелинейные криптографические сигналы для практически любого периода и нелинейные дискретные сигналы в конечных полях Галуа для значений периодов, определенных правилами построения; определять значения минимальных и максимальных боковых выбросов различных корреляционных функций; сравнивать полученные значения с известными, потенциально достижимыми границами для соответствующих корреляционных функций; присваивать реализациям синтезированных последовательностей, а также параметрам, используемым для синтеза сигналов, уникальные идентификаторы (специальные радиоданные), которые необходимы для оптимальной обработки сигналов; рассчитывать статистические характеристики различных корреляционных функций синтезированных сигналов; проводить исследования ансамблевых характеристик синтезированных сигналов. Компоненты программной компьютерной реализации разработанных методов синтеза и исследования свойств синтезированных систем сигналов представлены в приложениях к диссертационной работы. Программное и математическое обеспечение, полученное в ходе исследований, реализующее методы синтеза и исследования свойств систем нелинейных сигналов, практически готово к возможному использованию в составе опытных образцов и элементов современных цифровых коммуникационных средств. На основе разработанных и усовершенствованных методов синтеза систем нелинейных сигналов, методов быстрой реализации модульных операций в диссертации представлены алгоритмы для их реализации, в соответствии с которыми синтезирован класс средств формирования и обработки данных, на которые получено 14 патентов Украины и авторских свидетельств на изобретения, что подтверждает новизну и практическую значимость полученных в диссертации научных результатов работы.

Для проведения экспериментальных исследований эффективности функционирования телекоммуникационной системы с использованием предлагаемого метода информационного обмена и систем сложных нелинейных дискретных сигналов разработана имитационная модель. Полученные результаты свидетельствуют о том, что телекоммуникационные системы, в которых реализуется метод динамической смены соответствия: бит сообщения - сложный сигнал, а в качестве сложных сигналов используются различные классы нелинейных сигналов, теоретические основы которых разработаны в ходе диссертационных исследований, обладают улучшенными показателями помехозащищенности (структурной скрытности, помехоустойчивости), информационной безопасности (информационной скрытности, имитостойкости).

Ключевые слова: помехозащищенность, скрытность, помехоустойчивость, корреляционные свойства, система сигналов, дискретный сигнал, арифметическая модульная операция, модулярная система счисления, синтез сигналов, динамический режим функционирования, криптографический сигнал, изоморфизм.

ABSTRACT

O.A. Zamula Models and methods of the synthesis of complex signals with the required properties for secure telecommunication systems. – Manuscript.

The thesis for the degree of Doctor of Technical Science with a specialization in 05.12.02 – telecommunication systems and networks. – Ukrainian National University of Railway Transport, Kharkiv, 2016.

The thesis is focused on solving a relevant scientific and applied problem that is increasing telecommunication system (TCS) interference immunity and information security under internal and external influences. The work objective is to improve the TCS performance, namely interference immunity and information security by improving telecommunication system methodological foundations by developing methods of information exchange, models and methods of synthesis of new classes of nonlinear discrete complex signals with the required properties.

The thesis first obtained: the method of synthesis of complex nonlinear discrete cryptographic signals which uses random (pseudorandom) processes, and allows to create signals with necessary ensemble, structural and correlation properties, making it possible to improve the performance of the TCS interference immunity and information security in terms of internal and external effects; mathematical model of the structure of complex nonlinear discrete signals in finite Galois field, which determines the dependence of characters of elements of the multiplicative group of Galoi field and discrete sequences symbols giving a chance to set the values of interference immunity (structural secrecy) of the digital signals; method of implementing modular arithmetic operations of addition and subtraction based on the tabular principle of implementing arithmetic operations by using a special code of tabular multiplication which improves the performance speed of module operations of addition and subtraction; method of implementing multiplication modular arithmetic operation based on using a tabular principle by a successive procedure of the result determining operation, which improves the performance of modular multiplication operations. During the thesis research were improved: the method of synthesis of nonlinear discrete complex signals, which unlike the known ones uses the interdependence between the elements and elements final field indices that can increase the speed of signals synthesis; synthesis method of nonlinear discrete cryptographic signals, in which unlike the known ones, the directional (limited) enumeration of signals mechanisms are used to determine those meeting the relevant requirements for the properties of the signals allowing to improve signals synthesis performance; method for assessing the discrete signals properties which in contrast to the known ones uses algebraic properties of finite field elements allowing to increase the performance speed of the signals properties research process, and thus improve the signals with the required properties system synthesis performance; method of synthesis of the entire system of nonlinear discrete signals, which in contrast to the known ones uses the procedure of reading and writing (defined by a rule) of signal sequence characters for the formation of the entire set of signals related to the signals system that can increase the performance of the signals synthesis; methods of informational data exchange, which unlike the known ones apply the change, defined by a rule, matching bit message - a complex signal, and nonlinear

discrete signals with the required ensemble, structural and correlation properties that are used as complex signals, which makes it possible to improve information security and interference immunity performance; method of implementing modular arithmetic operations of addition and subtraction, which unlike the known ones is based on a principle of using a circular shift by presenting number residues by a binary code through the use of cyclic permutations properties of the content circulating register that can increase the performance speed of module operations.

Key words: correlation properties, cryptographic signal, discrete signal, dynamic operation mode, interference immunity, isomorphism, medullary number system, modular arithmetic operation, noise immunity, secrecy, signals system, and signals synthesis.

ЗАМУЛА ОЛЕКСАНДР АНДРІЙОВИЧ

УДК 621.391

МОДЕЛІ І МЕТОДИ СИНТЕЗУ СКЛАДНИХ СИГНАЛІВ З НЕОБХІДНИМИ ВЛАСТИВОСТЯМИ ДЛЯ ЗАХИЩЕНИХ ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ

АВТОРЕФЕРАТ

дисертації на здобуття наукового ступеня
доктора технічних наук

Віддруковано згідно з оригіналом автора

Підписано до друку «18» 12. 2015 р.
Формат паперу 60х84 1/16. Папір офсетний
Умовн.-друк.арк. 3,0. Тираж 100. Зам. № ___.

Видавець

Свідоцтво серія