Міністерство освіти і науки, молоді та спорту України

Харківський національний університет радіоелектроніки

ІСАЄВ СЕРГІЙ ОЛЕКСАНДРОВИЧ

УДК 681.3.06 (043.3)

ОБЧИСЛЮВАЛЬНІ МЕТОДИ СИНТЕЗУ НЕЛІНІЙНИХ ВУЗЛІВ ЗАМІН ДЛЯ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ СИМЕТРИЧНИХ КРИПТОПЕРЕТВОРЕНЬ

05.13.21 – системи захисту інформації

Автореферат дисертації на здобуття наукового ступеня
кандидата технічних наук

Харків – 2013

Дисертацією є рукопис.

Робота виконана у Харківському національному університеті ім. В.Н. Каразіна Міністерства освіти і науки, молоді та спорту України.

Науковий керівник:
доктор технічних наук, професор
Сорока Леонід Степанович, Харківський національний університет ім. В.Н. Каразіна, професор кафедри безпеки інформаційних систем та технологій.

Офіційні опоненти:
- доктор технічних наук, доцент
Олексійчук Антон Миколайович, Інститут спеціального зв'язку та захисту інформації, Національний технічний університет «Київський політехнічний інститут», професор спеціальної кафедри №1;

- доктор технічних наук, професор
Потій Олександр Володимирович, Харківський університет Повітряних Сил ім. І. Кожедуба, начальник кафедри радіоелектронних систем пунктів управління Повітряних Сил.

Захист відбудеться «_____» _____ 2013 р. о ____ годині на засіданні спеціалізованої вченої ради К 64.052.05 у Харківському національному університеті радіоелектроніки за адресою: 61166, м. Харків, просп. Леніна,14.

З дисертацією можна ознайомитися у бібліотеці Харківського національного університету радіоелектроніки за адресою: 61166, м. Харків, просп. Леніна,14.

Автореферат розісланий «___»_____ 2013 року.

Вчений секретар
спеціалізованої вченої ради К 64.052.05 І.В. Лисицька

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Актуальність теми. Один з основних та найбільш ефективних методів захисту інформації полягає у її криптографічному перетворенні, тобто з використанням спеціальних (ключових) даних інформація перетворюється з метою приховування/відновлення її вмісту, підтвердження її справжності, цілісності, авторства та ін. Найбільший розвиток і застосування у системах захисту інформації знайшли симетричні криптографічні засоби, які, згідно з класичними положеннями теорії секретних систем, будуються на основі послідовного виконання простих та обчислювально ефективних блоків перетворень (криптопримітивів): блоків нелінійних замін (S-блоків), блоків лінійного розсіювання (блоків перестановок) та деяких функціональних перетворень, наприклад, зсув, складання за модулем та ін.

Основним та найбільш важливим елементом сучасних симетричних криптографічних засобів захисту інформації є нелінійні вузли замін, криптографічні властивості яких безпосередньо впливають на ефективність розроблювальних механізмів безпеки інформаційних технологій. Традиційний підхід їх формування базується на використанні математичного апарату булевої алгебри і, зокрема, методів формування криптографічних булевих функцій. Однак криптографічні показники формувальних S-блоків, такі як нелінійність (NL) та автокореляція (AC), що забезпечують стійкість шифрів до диференційного, лінійного та інших методів криптографічного аналізу, далекі від оптимальних. Перспективним шляхом вирішення цього протиріччя є, на наш погляд, використання математичного апарату недвійкових функцій з перетворенням у арифметиці скінчених полів. Таким чином, актуальною науково-технічною задачею, яка має важливе значення як для розвитку окремого напрямку сучасної теорії захисту інформації, так і для вирішення прикладних питань підвищення безпеки симетричних криптоперетворень, є розробка математичних моделей та обчислювальних методів формування нелінійних вузлів замін з покращеними властивостями з використанням математичного апарату недвійкових криптографічних функцій.

Зв’язок роботи з науковими програмами, планами, темами. Напрями досліджень тісно пов'язані з науково-дослідною роботою "Математичне і комп'ютерне моделювання інформаційних процесів у складних природних і технічних системах" (0112U002098), виконаною відповідно до планів наукової та науково-технічної діяльності кафедри безпеки інформаційних систем і технологій ХНУ імені В.Н. Каразіна.

Мета та задачі дослідження. *Метою дисертаційної роботи* є підвищення ефективності симетричних криптоперетворень на основі синтезу нелінійних вузлів замін з покращеними властивостями.

Відповідно до мети роботи необхідно розв’язати наукову задачу, яка полягає у розробці та дослідженні обчислювальних методів синтезу нелінійних вузлів замін з покращеними властивостями для підвищення ефективності симетричних криптоперетворень.

Для досягнення мети необхідно розв’язати такі часткові задачі:

1. Дослідити перспективні напрямки у розвитку обчислювальних методів синтезу нелінійних вузлів замін для підвищення ефективності симетричних криптопе-

ретворень. Обґрунтувати вибір напрямку досліджень.

2. Розвинути обчислювальний метод прогнозування оцінок ефективності симетричних криптоперетворень на основі дослідження диференційних та лінійних властивостей зменшених моделей шифрів. Дослідити вплив характеристик нелінійних вузлів замін на ефективність симетричних криптоперетворень.

3. Дослідити та розвинути методи оцінки обчислювальної ефективності ймовірнісного (побітового) синтезу регулярних нелінійних вузлів замін із заданими криптографічними показниками.

4. Розвинути математичну модель регулярних нелінійних вузлів замін симетричних криптоперетворень з використанням недвійкових криптографічних функцій, формалізувати процес формування нелінійних вузлів замін.

5. Дослідити та удосконалити обчислювальний метод синтезу нелінійних вузлів замін (метод імітації відпалу). Розробити критерії пошуку недвійкових криптографічних функцій, ввести динамічні коефіцієнти цінових функцій обчислювального пошуку.

Об'єктом досліджень є процес синтезу нелінійних вузлів замін симетричних криптоперетворень.

Предметом досліджень є обчислювальні методи синтезу нелінійних вузлів замін симетричних криптоперетворень для підвищення ефективності симетричних криптоперетворень.

Методи досліджень*:* для розвитку обчислювального методу прогнозування оцінок ефективності симетричних криптоперетворень, дослідження впливу характеристик нелінійних вузлів замін на ефективність симетричних криптоперетворень використано методи теорії захисту інформації, математичний апарат булевої алгебри та методи статистичного моделювання; для дослідження та розвитку методів оцінки обчислювальної ефективності ймовірнісного (побітового) синтезу регулярних нелінійних вузлів замін із заданими криптографічними показниками використано методи математичного моделювання, математичний апарат кореляційного та спектрального аналізу, методи теорії ймовірностей і математичної статистики; для розвитку математичної моделі регулярних нелінійних вузлів замін симетричних криптоперетворень, дослідження та удосконалення обчислювального методу синтезу нелінійних вузлів замін (методу імітації відпалу) використано методи теорії захисту інформації, математичний апарат булевої алгебри та методи теорії скінчених полів.

Наукова новизна одержаних результатів. У дисертаційній роботі отримано теоретичне узагальнення та нове вирішення важливого науково-технічного завдання розробки та дослідження обчислювальних методів синтезу нелінійних вузлів замін з покращеними властивостями для підвищення ефективності симетричних криптоперетворень. Отримано такі наукові результати:

1. Набула подальшого розвитку математична модель регулярних нелінійних вузлів замін симетричних криптоперетворень, яка відрізняється від відомих розробленим аналітичним описом S-блоків через недвійкові криптографічні функції над скінченим полем $GF(2^m)$. Запропонована модель дозволяє у термінах теорії скінчених полів формалізувати процес формування нелінійних вузлів замін, використовувати методи кореляційного та спектрального аналізу над $GF(2^m)$ для дослідження криптографічних властивостей формувальних S-блоків.

2. Удосконалено обчислювальний метод синтезу нелінійних вузлів замін (метод імітації відпалу), який відрізняється від відомих запропонованим критерієм пошуку недвійкових криптографічних функцій, які аналітично задають підстановлювальне перетворення, а також введеними динамічними коефіцієнтами цінових функцій обчислювального пошуку, що дозволяє спростити процес формування блоків підстановок симетричних криптоперетворень з необхідними показниками нелінійності та автокореляції .

3. Набув подальшого розвитку обчислювальний метод прогнозування оцінок ефективності симетричних криптоперетворень на основі дослідження диференційних та лінійних властивостей зменшених моделей шифрів, який відрізняється від відомих урахуванням показників нелінійності та автокореляції використовуваних нелінійних вузлів замін, що дозволяє прогнозувати обчислювальні затрати шифрування, необхідні для досягнення асимптотичних диференційних та лінійних властивостей випадкової підстановки з урахуванням криптографічних властивостей використовуваних блоків підстановок .

4. Набули подальшого розвитку методи оцінки обчислювальної ефективності ймовірнісного (побітового) синтезу регулярних нелінійних вузлів замін із заданими криптографічними показниками, які відрізняються від відомих накладеними системами обмежень на компонентні булеві функції і урахуванням основних криптографічних показників (нелінійності та автокореляції), що дозволяє оцінювати обчислювальну ефективність неалгебраїчних методів синтезу блоків підстановок симетричних криптоперетворень.

Практичне значення одержаних результатів.

1. Розроблено обчислювальні алгоритми і програмну реалізацію запропонованого методу синтезу S-блоків, які дозволяють формувати регулярні нелінійні вузли замін n×2 і n×4 (4×2, 4×4, 6×2, 6×4, 8×2) з використанням спектральних та кореляційних властивостей недвійкових криптографічних функцій над скінченим полем $GF(2^m)$. Проведено обчислювальний пошук регулярних нелінійних вузлів замін n×2 і n×4 за введеними критеріями та показниками стійкості, сформовано блоки підстановок 8×2 з показниками NL = 116, AC = 24, 6×4 з показниками NL = 24, AC = 24, а також бієктивні вузли замін 4×4 з показниками NL = 4, AC = 8. Встановлено, що сформовані S-блоки володіють покращеними властивостями.

2. Отримано оцінки ефективності 16-бітних версій блокових симетричних шифрів з використанням нелінійних вузлів замін з різними показниками нелінійності та автокореляції. Отримано оцінки обчислювальних витрат, необхідних для досягнення 16-бітними версіями блокових симетричних шифрів асимптотичних диференційних та лінійних властивостей випадкової підстановки 16×16. Отримані оцінки дозволили обґрунтувати вплив криптографічних властивостей блоків замін на ефективність симетричних криптоперетворень.

3. Отримано оцінки обчислювальної ефективності методів ймовірнісного (побітового) синтезу регулярних нелінійних вузлів замін m×m із заданими криптографічними показниками. Отримані оцінки дозволили встановити межі обчислювальності ($m \le 6$) досліджуваних побітових методів, обґрунтувати необхідність розробки нових моделей і неалгебраїчних методів синтезу блоків підстановок для $m > 6$.

4. Вироблено практичні рекомендації з використання розроблених моделей та

методів формування нелінійних вузлів замін для удосконалення блокових симетричних криптоперетворень. Обґрунтовано рекомендації з ймовірнісного синтезу нелінійних вузлів замін симетричних криптоперетворень, зокрема, запропоновані рішення використано для розробки пропозицій щодо формування S-блоків симетричних криптоперетворень, які можуть бути застосовані у перспективному алгоритмі блокового симетричного шифрування.

Обґрунтованість і достовірність наукових положень дисертації підтверджується: несуперечливістю з основними положеннями теорії захисту інформації, коректним використанням методів досліджень, а також збігом результатів експериментальних досліджень з теоретичними розрахунками за аналітичними виразами.

Результати дисертаційних досліджень використано у науково-дослідній роботі «Математичне і комп'ютерне моделювання інформаційних процесів у складних природних і технічних системах», № 0112U002098. Отримано акти реалізації результатів досліджень на виробництві у діяльності ТОВ «Мікрокрипт Текнолоджіс» (від 17.09.2012 р.) та у навчальному процесі Харківського національного університету імені В.Н. Каразіна (від 18.09.2012 р.).

Особистий внесок здобувача. Всі результати, наведені у роботі, отримано здобувачем самостійно. Їх основний зміст викладений в статтях [1–8]. У статтях, написаних у співавторстві, здобувачеві належать такі результати: у [1] запропоновано систему обмежень на компонентні криптографічні булеві функції, програмно реалізовано обчислювальну модель формування нелінійних вузлів замін симетричних криптографічних засобів захисту інформації; у [2] розроблено нелінійні вузли замін зменшених моделей блокових симетричних шифрів з різними показниками стійкості за нелінійністю та автокореляцією, розвинуто обчислювальний метод прогнозування оцінок ефективності симетричних криптоперетворень на основі дослідження диференційних властивостей зменшених моделей блокових симетричних шифрів з урахуванням показників нелінійності та автокореляції використовуваних нелінійних вузлів замін; у [3] розвинуто методи оцінки обчислювальної ефективності ймовірнісного (побітового) синтезу регулярних нелінійних вузлів замін із заданими криптографічними показниками нелінійності та автокореляції; у [4] розвинуто обчислювальний метод прогнозування оцінок ефективності симетричних криптоперетворень на основі дослідження лінійних властивостей зменшених моделей блокових симетричних шифрів з урахуванням показників нелінійності та автокореляції використовуваних нелінійних вузлів замін; у [5] отримано оцінки ефективності зменшених версій блокових симетричних шифрів відносно диференційного криптоаналізу з використанням вузлів замін з різними показниками стійкості; у [6] запропоновано використання методу швидкого розрахунку лінійних властивостей зменшених моделей блокових симетричних шифрів, що дозволило отримати оцінки ефективності 16-бітних шифрів відносно лінійного криптоаналізу; у [7] розвинуто математичну модель регулярних нелінійних вузлів замін симетричних криптоперетворень з використанням недвійкових криптографічних функцій; у [8] удосконалено обчислювальний метод синтезу нелінійних вузлів замін (метод імітації відпалу), розроблено критерії селекції недвійкових криптографічних функцій обчислювального методу синтезу нелінійних вузлів замін, синтезовано нелінійні

вузли замін 8×2 та 6×4 з покращеними показниками нелінійності та автокореляції.

Апробація результатів дисертації здійснювалась на 12-ти наукових конференціях, що мають безпосереднє відношення до теми роботи: науково-практичних конференціях «Застосування інформаційних технологій у підготовці та діяльності сил охорони правопорядку», Харків, 2010, 2012 [12, 19]; VI-й Науковій конференції «Новітні технології – для захисту повітряного простору», Харків, 2010 [15]; Науково-технічній конференції з міжнародною участю «Комп'ютерне моделювання в наукоємних технологіях», Харків, 2010 [18]; I-й Міжнародній науково-технічній конференції «Інформаційні технології в навігації і управлінні: стан та перспективи розвитку», Київ, 2010 [17]; proceedings "Statistical methods of signal and data processing", Київ, 2010 [14]; Міжнародній науково-практичній конференції «Перспективи розвитку інформаційних та транспортно-митних технологій у митній справі, зовнішньоекономічній діяльності та управлінні організаціями», Дніпропетровськ, 2011 [13]; VI-й Міжнародній науково-практичній конференції «Наука и социальные проблемы общества: информатизация и информационные технологии», Харків, 2011 [20]; II-й Міжнародній науково-практичній конференції «Інформаційні технології та комп'ютерна інженерія», Харків, 2011 [10]; III-й Міжнародній науково-практичній конференції «Проблеми і перспективи розвитку IT-індустрії», Харків, 2011 [11]; III-й Міжнародній науково-практичній конференції «Інформаційні технології та захист інформації», Харків, 2012 [9]; I-й Міжнародній науково-технічній конференції «Захист інформації і безпека інформаційних систем», Львів, 2012 [16].

Публікація результатів роботи. Результати роботи опубліковані в 20 друкованих працях. До них входять 8 статей, опублікованих у наукових фахових виданнях України, а також 12 матеріалів у збірниках праць наукових конференцій.

Структура та обсяг дисертації. Дисертаційна робота складається із вступу, чотирьох розділів, загального висновку, списку використаних джерел та трьох додатків. Загальний обсяг дисертації складає 189 сторінок, з яких основний зміст викладено на 139 сторінках друкованого тексту, 0 сторінок рисунків, 7 сторінок таблиць, 17 рисунків, 39 таблиць. Список використаних джерел складається з 120 найменувань на 14 сторінках, 3 додатки на 29 сторінках.

ОСНОВНИЙ ЗМІСТ

У **вступі** обґрунтовано актуальність завдання, що вирішується, сформульовано мету, об'єкт та задачі досліджень, визначено наукову новизну та практичну значущість отриманих результатів, наведено відомості про їх апробацію та реалізацію, а також характеристику публікацій.

У **першому розділі** дисертації проведено дослідження перспективних напрямків у розвитку обчислювальних методів синтезу нелінійних вузлів замін для підвищення ефективності симетричних криптоперетворень, обґрунтовано вибір напрямку досліджень.

Забезпечення безпеки сучасних інформаційних систем і технологій покладається на засоби захисту інформації, зокрема симетричні криптоперетворення. Поряд з високою швидкістю та простотою практичної реалізації симетричні криптоалгоритми дозволяють забезпечити високу стійкість до різних методів криптографічного

аналізу.

Проведений аналіз сучасних симетричних криптоперетворень дозволяє констатувати, що основним та найбільш важливим їх елементом є нелінійні вузли замін (S-блоки), криптографічні властивості яких безпосередньо впливають на ефективність забезпечення безпеки інформаційних технологій. Традиційний підхід формування S-блоків базується на використанні математичного апарату булевої алгебри і, зокрема, криптографічних булевих функцій.

Проведені дослідження дозволили встановити сукупність криптографічних показників та критеріїв стійкості нелінійних вузлів замін у термінах булевої алгебри. Показано, що найбільш важливими для забезпечення стійкості блокового симетричного криптоперетворення відносно лінійного та диференційного видів криптоаналізу є показники нелінійності та автокореляції. Однак значення цих показників далекі від оптимальних, що впливає на ефективність симетричних криптоперетворень інформації.

Таким чином, для підвищення ефективності симетричних криптографічних засобів захисту інформації потрібно вдосконалення математичних моделей та обчислювальних методів формування нелінійних вузлів замін з покращеними властивостями.

Другий розділ дисертації присвячений подальшому розвитку обчислювального методу прогнозування оцінок ефективності симетричних криптоперетворень на основі дослідження диференційних та лінійних властивостей зменшених моделей шифрів, дослідженню впливу показників нелінійних вузлів замін NL та AC на ефективність симетричних криптоперетворень.

Для розв’язання цієї задачі використовується підхід з оцінки стійкості блокових симетричних шифрів (БСШ) до методів диференційного та лінійного криптоаналізу, який полягає в порівнянні властивостей досліджувальних зменшених моделей шифрів з властивостями випадкових підстановок. На підставі теоретичних оцінок середнього значення максимумів таблиць диференційних різниць та таблиць лінійних апроксимацій випадкової 16-бітної підстановки здійснюється оцінка ефективності зменшених моделей БСШ у вигляді мінімального числа циклів алгоритму шифрування, при якому реалізується асимптотичний показник середнього значення максимуму повних диференціалів та максимуму лінійного корпусу. При цьому увага зосереджена на дослідженні впливу показників нелінійності та автокореляції використовуваних вузлів замін на ефективність зменшених моделей БСШ відносно диференційного та лінійного криптоаналізу.

Розроблена методика статистичних досліджень диференційних та лінійних властивостей зменшених моделей БСШ та оцінки впливу на них криптографічних показників нелінійних вузлів замін полягає в наступному. В дослідженні розглядаються властивості зменшених моделей шифрів, поданих на український конкурс, а також американського стандарту шифрування AES. Обґрунтовується структура зменшених моделей БСШ, розробляються нелінійні вузли замін 4×4 двох видів: один – з свідомо кращими криптографічними показниками нелінійності та атокореляції, ніж інший. Вузли замін з покращеними показниками мають показники NL = 4, AC = 8. Другий вид S-блоків має показники NL = 2, AC = 16. Оцінка властивостей стійкості зменшених моделей шифрів проводиться у середньостатистичному значенні, тобто

обчислюються середні за множиною ключів (очікувані) значення максимумів. Для обробки результатів статистичного експерименту використовуються методи математичної статистики та перевірки гіпотез. Визначаються показники порівняння експериментальних даних: середні та абсолютні за множиною 100 таблиць (100 випадкових ключів шифрування) значення максимумів таблиць диференційних різниць та таблиць лінійних апроксимацій зменшених моделей шифрів.

Результати статистичних експериментів наведено у таблицях 1 – 4. Сірим кольором позначено комірки таблиці, які показують вихід зменшених моделей шифрів до асимптотичного значення максимумів.

Таблиця 1 - Абсолютні значення максимуму таблиць диференційних різниць

Шифр / # *r*	Mini-AES		Mini-ADE		Міні-Лабіринт		Міні-Калина		Міні-Мухомор	
	AC=16	AC=8	AC=16	AC=8	AC=16	AC=8	AC=16	AC=8	AC=16	AC=8
1	32768	16384	32768	16384	-	-	7168	6144	65536	65536
2	5632	4096	7680	5120	-	-	1376	640	16384	6144
3	896	352	1312	1024	262	128	38	24	4608	3072
4	36	22	48	38	20	22	22	22	2304	224
5	22	22	20	24	22	24	22	22	156	60
6	24	20	22	22	22	24	24	24	36	20

Таблиця 2 - Абсолютні значення максимуму таблиць лінійних апроксимацій

Шифр / # *r*	Mini-AES		Mini-ADE		Міні-Лабіринт		Міні-Калина		Міні-Мухомор	
	NL=2	NL=4	NL=2	NL=4	NL=2	NL=4	NL=2	NL=4	NL=2	NL=4
1	24576	16384	24576	16384	-	-	18432	12288	18432	12288
2	10240	10240	14336	12288	-	-	7808	4480	18432	9728
3	4736	4352	6400	4352	2082	1444	2000	936	12496	8396
4	1268	940	1544	932	884	914	890	912	12581	8450
5	912	900	906	896	902	902	898	900	12746	8667
6	890	922	898	880	900	906	896	912	12609	8696

Таблиця 3 - Середні значення максимуму таблиць диференційних різниць та довірчий інтервал

# *r*	Mini-AES		Mini-ADE		Міні-Лабіринт		Міні-Калина		Міні-Мухомор	
	AC=16	AC=8	AC=16	AC=8	AC=16	AC=8	AC=16	AC=8	AC=16	AC=8
1	32768 ±0	16384 ±0	30392,3 ±770,4	16384 ±0	-	-	6082,6 ±183,6	3732,5 ±112,6	65536 ±0	65536 ±0
2	5437,4 ±0	3036,2 ±14,7	4910,1 ±23,7	3353,6 ±16,2	-	-	826,9 ±4	382,4 ±1,8	14187,5 ±68,7	5770,2 ±27,9
3	817,4 ±19,8	274,2 ±6,6	672 ±16,2	307,2 ±7,4	102 ±2,4	37,5 ±0,9	24,8 ±0,6	19,4 ±0,4	2496,3 ±60,4	1802,2 ±43,6

Продовження таблиці 3

	Mini-AES		Mini-ADE		Міні-Лабіринт		Міні-Калина		Міні-Мухомор	
#r	AC=16	AC=8	AC=16	AC=8	AC=16	AC=8	AC=16	AC=8	AC=16	AC=8
4	26 ±0,4	19,3 ±0,3	23 ±0,3	20,5 ±0,3	19,1 ±0,3	19 ±0,3	19 ±0,4	19,1 ±0,5	542,7 ±9,4	125,5 ±2,1
5	19,1 ±0,1	19 ±0,1	19,1 ±0,4	19,1 ±0,4	19 ±0,3	19,2 ±0,3	19,1 ±0,6	19,2 ±0,6	46,3 ±0,8	29,7 ±0,5
6	19,2 ±0,1	18,8 ±0,1	19,2 ±0,2	19,2 ±0,2	19,1 ±0,3	19 ±0,3	19,1 ±0,6	19,4 ±0,6	19,5 ±0,4	18,9 ±0,4

Таблиця 4 - Середні значення максимуму таблиць лінійних апроксимацій та довірчий інтервал

	Mini-AES		Mini-ADE		Міні-Лабіринт		Міні-Калина		Міні-Мухомор	
#r	NL=2	NL=4	NL=2	NL=4	NL=2	NL=4	NL=2	NL=4	NL=2	NL=4
1	24576 ±0	16384 ±0	24576 ±0	16384 ±0	-	-	13640 ±405	9349 ±237	18432 ±3674	11602 ±5424
2	10240 ±0	9165 ±121	11571 ±780	9093 ±94	-	-	5724 ±208	3546 ±84	18432 ±3578	8499 ±6122
3	4494 ±48	3658 ±66	4684 ±164	3510 ±62	1616 ±51	1070 ±38	1205 ±60	831 ±84	8561 ±5950	7929 ±6134
4	983 ±18	827 ±7	988 ±37	829 ±8	823 ±5	826± 6	819 ±6	820 ±7	9426 ±5703	7605 ±6180
5	821 ±6	821 ±6	825 ±6	821 ±5	820 ±7	821± 5	821 ±6	823 ±6	9190 ±5826	7661 ±6235
6	823 ±6	822 ±7	825 ±7	820 ±6	820 ±6	823± 7	826 ±6	825 ±6	9493 ±5751	7739 ±6215

Результати статистичних досліджень диференційних та лінійних властивостей зменшених моделей БСШ добре узгоджуються між собою, а також з теоретичними оцінками асимптотичних значень випадкових підстановок. Аналіз отриманих результатів свідчить про те, що використання S-блоків з покращеними показниками нелінійності та автокореляції дозволяє для деяких шифрів на один цикл шифрування вийти раніше до асимптотичного показника максимуму диференційних таблиць та таблиць лінійних апроксимацій, а для інших – посилити ці властивості.

Число операцій для реалізації раунду перетворень одного шифру може істотно відрізнятися від числа операцій, необхідних для реалізації раунду іншого шифру (те ж саме відноситься і до витрат пам’яті). Тому для більш точної оцінки ефективності шифрів проведено оцінку обчислювальної ефективності розглянутих БСШ, а саме визначено кількість елементарних операцій, необхідних для шифрування одного блоку даних і витрат оперативної пам’яті в бітах, необхідних для зберігання викори-

стовуваного у процесі шифрування ключового матеріалу і ключових даних. Отримані оцінки наведені в таблицях 5, 6.

Отримані оцінки дозволяють прогнозувати ефективність БСШ відносно диференційного та лінійного криптоаналізу з урахуванням показників стійкості використовуваних нелінійних вузлів замін.

Таблиця 5 - Обчислювальні витрати шифрів

# r	AES	ADE	Лабі-бі-ринт	Ка-ли-на	Му-хо-мор
1	48	48	212	125	71
2	84	84	280	181	122
3	120	120	348	237	173
4	156	156	416	293	224
5	192	192	484	349	275
6	228	228	552	405	326
7	264	264	620	461	377
8	30	3 0	688	517	428
9	336	336	-	573	479
10	393	393	-	629	530

Таблиця 6 - Витрати пам’яті шифрів

# r	AES	ADE	Лабі-бі-ринт	Ка-лина	Му-хо-мор
1	4096	4096	8448	18432	4096
2	4096	8192	8448	18432	4096
3	4096	12288	8448	18432	4096
4	4096	16384	8448	18432	4096
5	4096	2480	8448	18432	4096
6	4096	24576	8448	18432	4096
7	4096	28672	8448	18432	4096
8	4096	32768	8448	18432	4096
9	4096	36864	-	18432	4096
10	4352	41216	-	18432	4096

Оскільки задачу проектування практичного алгоритму БСШ слід розглядати як задачу мінімізації витрат на реалізацію криптоперетворення, яке забезпечує необхідні показники криптостійкості – наведені оцінки свідчать, що використання S-блоків з покращеними показниками нелінійності та автокореляції дозволяє скоротити необхідні обчислювальні витрати. Таким чином, завдання дисертаційного дослідження обґрунтовано.

Третій розділ дисертації присвячений дослідженню та подальшому розвитку методів оцінки обчислювальної ефективності ймовірнісного (побітового) синтезу регулярних нелінійних вузлів замін із заданими криптографічними показниками.

Ймовірнісний побітовий метод синтезу S-блоків m×m полягає в знаходженні S-блоку випадковим відбором m m-бітних булевих функцій, які його описуватимуть. Метод складається з двох кроків: 1) формування множини булевих функцій $\Delta = \{f_1, f_2, \ldots, f_N\}$, які відповідають накладеним критеріям криптографічної стійкості; 2) пошуку S-блоку за множиною Δ.

Оскільки побітові методи синтезу S-блоків m×m із заданими показниками криптографічної стійкості мають випадковий характер, необхідно встановити наскільки швидко (як функція від m) ці методи стають нездійсненними. Теоретичні розрахунки роботи Люка О’Коннора показують практичні межі розмірів S-блоків, які можуть бути ефективно синтезовані, використовуючи побітові методи синтезу.

В роботі проведено аналіз жадібного алгоритму та алгоритму гілок і меж пошуку S-блоків за множиною сформованих булевих функцій, показуються теоретичні оцінки ефективності алгоритмів пошуку. Результати експериментальних досліджень ефективності двох алгоритмів пошуку з урахуванням накладених критеріїв стійкості

нелінійності та автокореляції нелінійних вузлів замін наведено у таблицях 7, 8. У таблицях використовуються такі позначення: «# ф.» - кількість сформованих булевих функцій, «NP» – кількість експериментів, «IWP» – кількість експериментів, для яких S-блок було знайдено, «API» - середня кількість S-блоків, знайдених в кожному з експериментів, «Вип.» – пошук серед випадково сформованих булевих функцій, «Ст.» – пошук серед булевих функцій з високою нелінійністю та низькою автокореляцією. Тип синтезованих вузлів замін позначений таким чином: «-» – синтезується бієктивний випадковий S-блок, «F» – критерії відбору накладено тільки на координатні булеві функції S-блоку, «S» – на координатні булеві функції та їх лінійні комбінації, «L» – S-блок синтезується з накладеним критерієм високої нелінійності NL, «LA» – на S-блок накладено критерії високої нелінійності та низької автокореляції.

Таблиця 7 - Результати для жадібного алгоритму

m	# ф.	NP	% невдач		Тип
			Вип.	Ст.	
4	100	5000	19,1	16,2	-
4	100	5000	19,4	18,9	F:L
4	100	5000	26,6	16,8	F:LA
4	100	5000	67,4	56,9	S:L
4	300	5000	67,1	55,6	S:LA
5	10000	1000	36,1	34,5	-
5	10000	1000	53,0	34,9	F:L
5	10000	1000	96,7	35,5	F:LA
5	500000	1000	100	95,4	S:L

Таблиця 8 - Результати для алгоритму гілок та меж

m	# ф.	IWP		API		Тип
		Вип.	Ст.	Вип.	Ст.	
4	20	87	85	3,6	3,8	-
4	20	77	88	2,4	3,3	F:L
4	20	56	75	1,4	3,5	F:LA
4	50	100	100	17,1	32,1	S:L
4	50	85	99	3,6	7,5	S:LA
5	120	38	37	0,6	0,5	-
5	120	6	44	0,1	0,6	F:L
5	120	4	4	0 1	0,6	F:LA
5	500	100	100	92	860	F:L
5	500	0	100	0	898	F:LA
5	2000	38	100	0,5	5,6	S:L

Дослідження показали, що алгоритм гілок і меж виявився більш ефективним алгоритмом пошуку, ніж жадібний алгоритм. Отримані експериментальні оцінки добре погоджуються з теоретичними розрахунками. Оцінка середнього розміру дерева пошуку алгоритму гілок та меж з урахуванням накладених критеріїв нелінійності та автокореляції нелінійних вузлів замін проведено за допомогою методу Монте-Карло (табл. 9).

Таблиця 9 - Оцінка розміру дерева пошуку алгоритму гілок та меж

m	# ф.	Тип	Сер. розмір дерева пошуку
4	20	-	136,6±0,7
4	20	F:L	149,8±1,2
4	20	F:LA	136,8±0,8
4	50	S:L	838,5±6,2
4	50	S:LA	570±2,9
5	120	-	5611,2±40,2

Результати показують істотно зростаючий (із зростанням розміру S-блоку) розмір дерева пошуку алгоритму гілок та меж. Отримані оцінки вказують на те, що знаходження m-бітних бієктивних нелінійних вузлів замін з показниками високої нелінійності та низької автокореляції, використовуючи ймовірнісні побітові

Продовження таблиці 9

m	# ф.	Тип	Сер. розмір дерева пошуку
5	500	F:L	321110±3043,1
5	500	F:LA	402130±4580,1
5	1000	S:L	3251880±21980,3
5	10000	S:LA	278475100±2065128
6	8000	-	355650800±3368649
6	8000	F:L	488942560±6551134
6	8000	F:LA	566570560±6353469
6	8000	S:L	881840±3123,7
6	8000	S:LA	809840±3457,1
6	8000	-	355650800±3368649
6	8000	F:L	488942560±6551134

методи синтезу, для розмірності m > 6 – нездійсненне завдання. Крім того, незалежно від ефективності алгоритму пошуку, потужність множини Δ, необхідної для того, щоб перестановка була знайдена надзвичайно велика для m ≥ 8. Таким чином, класичний ймовірнісний метод синтезу криптографічно стійких вузлів замін є непрактичним вже для m = 6 і нездійсненним для m > 6 необхідність розробки нових моделей та обчислювальних методів синтезу нелінійних вузлів замін обґрунтовано.

Четвертий розділ дисертації присвячений розвитку математичної моделі регулярних нелінійних вузлів замін симетричних криптоперетворень з використанням недвійкових криптографічних функцій, дослідженню та удосконаленню обчислювального методу синтезу нелінійних вузлів замін (методу імітації відпалу).

Введемо основні поняття та визначення математичного апарату нелінійних вузлів замін через недвійкові функції, які описують відображення n-бітних блоків вхідних даних у m-бітні вихідні блоки у нелінійному вузлі замін у вигляді функцій відображення F: $GF(2^n) \to GF(2^m)$.

Недвійковою (над полем $GF(2^{n_1})$) *функцією* $F(X_1,...,X_{n_2})$ від n_2 змінних є функція, яка здійснює відображення із поля $GF((2^{n_1})^{n_2})$ усіх векторів $X=(X_1,...,X_{n_2})$ довжини n_2 з елементами із $GF(2^{n_1})$ в поле $GF(2^{n_1})$. Кожна недвійкова функція $F(X_1,...,X_{n_2})$ може бути подана в алгебраїчній нормальній формі (АНФ), тобто як сума добутків складових координат:

$$F(X_1,...,X_{n_2}) = \Lambda_0 + \Lambda_1 X_1 + ... + \Lambda_n X_n + \Lambda_{12} X_1 X_2 + \Lambda_{13} X_1 X_3 + ... + \Lambda_{12...n_2} X_1 X_2 ... X_n, \quad (1)$$

де $\Lambda_0, \Lambda_1, ..., \Lambda_{12}, ..., \Lambda_{12...n_2}$ – унікальні константи із $GF(2^{n_1})$, підсумовування та множення також проводиться у полі $GF(2^{n_1})$.

Поле $GF((2^{n_1})^{n_2})$ складається з $2^{n_1 n_2}$ векторів $A_i = (A_1^i, A_2^i, ..., A_{n_2}^i)$, $A_j^i \in GF(2^{n_1})$:

$$A_0 = (0,...,0,0),\ A_1 = (0,...,0,1),\ \ldots,\ A_{2^{n_1}-1} = (0,...,0,2^{n_1}-1),\ A_{2^{n_1}} = (0,...,1,0),$$

$$A_{2^{n_1}+1} = (0,...,1,1),\ \ldots,\ A_{(2^{n_1})^{n_2}-1} = (2^{n_1}-1,...,2^{n_1}-1,2^{n_1}-1).$$

Поле $GF((2^{n_1})^{n_2})$ ізоморфно полю $GF(2^n)$, $n = n_1 n_2$, тобто маємо взаємооднозначну функціональну відповідність множини векторів

$A_i = (A_1^i, A_2^i, ..., A_{n_2}^i) \in V_{n_2}$ з елементами з поля $GF(2^{n_1})$ та двійкових векторів $\alpha_i = (\alpha_1^i, \alpha_2^i, ..., \alpha_n^i) \in V_n$.

Таблицею істинності недвійкової (над полем $GF(2^{n_1})$) функції F називається послідовність з елементами із $GF(2^{n_1})$, яка визначена як:

$$\left(F(X)\middle|X \in GF^{n_2}(2^{n_1})\right) = \left(F(A_0), F(A_1), ..., F(A_{2^{n_1 n_2}-1})\right).$$

Послідовністю недвійкової (над полем $GF(2^{n_1})$) функції F називається послідовність з $2^{n_1 n_2}$ (1,-1)- кортежів довжини n_1 кожний, яка визначається як:

$$\left(\left((-1)^{(F(X))_1}, (-1)^{(F(X))_2}, ..., (-1)^{(F(X))_{n_1}}\right)\middle|X \in GF^{n_2}(2^{n_1})\right) =$$

$$= \begin{pmatrix} \left((-1)^{(F(A_0))_1}, (-1)^{(F(A_0))_2}, ..., (-1)^{(F(A_0))_{n_1}}\right), \\ \left((-1)^{(F(A_1))_1}, (-1)^{(F(A_1))_2}, ..., (-1)^{(F(A_1))_{n_1}}\right), ..., \\ \left((-1)^{\left(F(A_{2^{n_1 n_2}})\right)_1}, (-1)^{\left(F(A_{2^{n_1 n_2}})\right)_2}, ..., (-1)^{\left(F(A_{2^{n_1 n_2}})\right)_{n_1}}\right) \end{pmatrix},$$

де під $\left(F(X)\right)_j$ розуміють j-й біт числа $F(X) \in GF(2^{n_1})$.

Розглянемо криптографічні властивості функцій F', які реалізують відображення із $GF^{n_2}(2^{n_1})$ у $GF^m(2^{n_1})$, де $1 \le m \le n_2$. Нехай $M_{n_2}^m$ є множина таких функцій F', а B_{n_2} - множина недвійкових функцій $F(X_1, ..., X_{n_2})$ від n_2 змінних, тобто функцій, які реалізують відображення із $GF^{n_2}(2^{n_1})$ у $GF(2^{n_1})$. Тоді будь-яку функцію із $M_{n_2}^m$ можна розглядати як функцію, яка складається з m недвійкових функцій $F(X_1, ..., X_{n_2})$ від n_2 змінних, тобто m-вихідних координатних функцій із B_{n_2}. У більш загальному поданні, компонентна функція із $M_{n_2}^m$ є ненульовою лінійною комбінацією її координатних недвійкових функцій із B_{n_2}. Таким чином, функція відображення $F': GF^{n_2}(2^{n_1}) \to GF^m(2^{n_1})$, яка реалізує нелінійний вузол замін, записується через множину

$$F' = (F_1(X_1, ..., X_{n_2}), ..., F_m(X_1, ..., X_{n_2})),$$

де $F_i(X_1, ..., X_{n_2}) \in B_{n_2}$.

У роботі розгляд обмежено функцією з m = 1, тобто розглядаються тільки функції $F' = F_i(X_1, ..., X_{n_2})$, які реалізують відображення із $GF^{n_2}(2^{n_1})$ у $GF(2^{n_1})$. Введена формалізація функціонального відображення $F: GF^{n_2}(2^{n_1}) \to GF(2^{n_1})$ є природним

узагальненням підходу до подання регулярних нелінійних вузлів замін у вигляді сукупності компонентних булевих функцій. Дійсно, використовуючи традиційний підхід до опису функціонального відображення n-бітних блоків вхідних даних у m- бітні вихідні блоки функцію $F: GF^n(2) \to GF^m(2)$, де $n = n_1 n_2$, $m = n_1$, можна подати у вигляді кортежу $F = \{f_1(x_1,...,x_n), f_2(x_1,...,x_n),..., f_m(x_1,...,x_n)\}$ із $m = n_1$ булевих функцій від $n = n_1 n_2$ булевих змінних кожна.

За аналогією до перетворення Уолша-Адамара введемо *спектральне перетворення* недвійкової функції $F(X_1,...,X_{n_2}) \in B_{n_2}$:

$$\bar{F}(W) = \sum_{X \in GF^{n_2}(2^{n_1})} \sum_{i=1}^{n_1} (-1)^{(F(X))_i + (G_W(X))_i}, \qquad (2)$$

де під $G_W(X)$ розуміють W-у недвійкову афінну функцію від n_2 змінних із множини A_n:

$$A_n = \left\{ a_0 + \sum_{i=1}^{n_2} a_i X_i \mid a_i \in GF(2^{n_1}), 0 \le i \le n \right\}. \qquad (3)$$

Також як вектор w у випадку булевого опису визначає вигляд двійкових функції $g_w(x)$, у випадку недвійкового опису вектор W задає вигляд недвійкових афінних функцій $G_W(X)$. Якщо $G_W(X)$ у (2) пробігає усі недвійкові лінійні функції (з $a_0 = 0$ у (3)) говоритимемо, що функція $\bar{F}(W)$ визначає *неповний спектр* недвійкової функції $F(X_1,...,X_{n_2}) \in B_{n_2}$ (спектр з лінійних функцій). Якщо $G_W(X)$ у (2) пробігає усі недвійкові лінійні та афінні функції (з $a_0 \in GF(2^{n_1})$ у (3)) говоритимемо, що функція $\bar{F}(W)$ задає *повний спектр* недвійкової функції $F(X_1,...,X_{n_2}) \in B_{n_2}$ (спектр з усіх афінних функцій).

У матричному вигляді введене спектральне перетворення задається у вигляді матричного множення послідовності недвійкової функції $\left(\left((-1)^{(F(X))_1}, (-1)^{(F(X))_2}, ..., (-1)^{(F(X))_{n_1}} \right) \middle| X \in GF^{n_2}(2^{n_1}) \right)$ на матрицю $H^*_{2^{n_1 n_2}}$ порядку $2^{n_1 n_2}$, рядки якої утворені послідовностями недвійкових лінійних (для неповного спектра) та афінних (для повного спектра) функцій (що є аналогом матриці Уолша-Адамара H_{2^n} порядку 2^n):

$$\left(\bar{F}(W) \middle| W \in GF^{n_2}(2^{n_1}) \right) = \left(\left((-1)^{(F(X))_1}, (-1)^{(F(X))_2}, ..., (-1)^{(F(X))_{n_1}} \right) \middle| X \in GF^{n_2}(2^{n_1}) \right) \cdot H^*_{2^{n_1 n_2}}.$$

Елементами матриці $H^*_{2^{n_1 n_2}}$ є (1,-1)-кортежі довжини n_1 кожен, які визначені правилом формування послідовності недвійкової функції.

За аналогією до кореляційного перетворення булевих функцій введемо *кореляційне перетворення* недвійкових функцій $F(X_1,...,X_{n_2}) \in B_{n_2}$:

$$R(S) = \sum_{X \in GF^{n_2}(2^{n_1})} \sum_{i=1}^{n_1} (-1)^{(F(X))_i + (F(X+S))_i}. \qquad (4)$$

Розглянемо найбільш ефективний на сьогоднішній день обчислювальний метод синтезу регулярних нелінійних вузлів замін – метод імітації відпалу, який застосовує критерій пошуку так звані цінові функції. Проведений аналіз показав, що найбільш ефективними ціновими функціями даного обчислювального методу синтезу S-блоків з високою нелінійністю та низькою автокореляцією є такі:

$$\mathrm{cost}(f) = \sum_{\omega \in GF^n(2)} \left| \left| \bar{F}(\omega) \right| - X \right|^R, \tag{5}$$

$$\mathrm{cost}(f) = \sum_{s \in GF^n(2)} \left| \left| r(s) \right| - X \right|^R, \tag{6}$$

$$\mathrm{cost}(f) = \sum_{\omega \in GF^n(2)} \left| \left| \bar{F}(\omega) \right| - X \right|^R + \sum_{s \in GF^n(2)} \left| \left| r(s) \right| - X \right|^R, \tag{7}$$

де $\bar{F}(\omega)$, $r(s)$ – коефіцієнти відповідних спектрів криптографічної булевої функції. Параметри X та R – вагові коефіцієнти, що забезпечують свободу для експериментування і підбору оптимальних значень.

Запропоновані в роботі нові критерії пошуку (цінові функції) криптографічних функцій з необхідними показниками нелінійності та автокореляції засновані на заміні коефіцієнтів спектральних перетворень компонентних булевих функцій, які складають нелінійний вузол замін, на відповідні коефіцієнти спектральних перетворень недвійкової функції, яка задає S-блок. Крім того вводяться *динамічні вагові коефіцієнти* замість статичних X з (5) – (7). Цінові функції приймають вигляд:

$$\mathrm{cost}(F) = \sum_{W \in GF^{n_2}(2^{n_1})} \left| \bar{F}(W) - \bar{B}(W) \right|^R, \tag{8}$$

$$\mathrm{cost}(F) = \sum_{S \in GF^{n_2}(2^{n_1})} \left| R(S) - BR(S) \right|^R, \tag{9}$$

$$\mathrm{cost}(F) = \sum_{W \in GF^{n_2}(2^{n_1})} \left| \bar{F}(W) - \bar{B}(W) \right|^R + \sum_{S \in GF^{n_2}(2^{n_1})} \left| R(S) - BR(S) \right|^R, \tag{10}$$

де $\bar{B}(W)$ та $BR(S)$ – коефіцієнти спектрального та кореляційного перетворень відповідно до деякої випадкової недвійкової бент-функції.

Під час дослідження критеріїв пошуку криптографічних недвійкових функцій було використано різновид цінових функцій з використанням - замість коефіцієнтів спектрального та кореляційного перетворень F(W), R(S) - відстані за Хеммінгом між таблицями істинності недвійкової функції F(X) та послідовностями відповідних афінних/лінійних недвійкових функцій $G_W(X)$ (для дослідження нелінійності), послідовностями F(X+S) (для дослідження автокореляції). Даний різновид критеріїв було умовно позначено «гіршим» випадком.

У таблиці 10 наведено результати експериментальних досліджень ефективності обчислювального методу синтезу нелінійних вузлів замін 8×2 із запропонованими ціновими функціями.

Таблиця 10 - Результати дослідження обчислювального методу синтезу S-блоків 8×2

Цінові функції	Статичні коефіцієнти		Динамічні коефіцієнти	
	NL	AC	NL	AC
F(W)	110	56	114	24
F(W), гірш.	108	56	**116**	**24**
R(S)	110	48	114	24
R(S), гірш.	112	40	114	24
F(W)+R(S)	112	40	114	24
F(W)+R(S), гірш.	112	40	114	24

Таблиця 11 - Порівняння ефективності обчислювальних методів синтезу S-блоків 8×2

Метод синтезу	NL	AC
Випадкова генерація	108	56
Генетичні алгоритми	110	48
Імітація відпалу (булеві функції)	114	32
Імітація відпалу (недвійкові функції)	112	40
Імітація відпалу (недвійкові функції, динамічні вагові коефіцієнти)	**116**	**24**

Отримані експериментальні результати добре узгоджуються з експериментальними результатами обчислювальних методів синтезу класичного підходу (табл. 11). Отримано кращі на сьогоднішній день результати.

Зазначимо, що специфікація сьогодні діючого в Україні стандарту симетричного шифрування ГОСТ 28147-89 не передбачає набору S-блоків, але надає розробникам можливість їх самостійного вибору. У відкритій літературі для аналізу стійкості алгоритму ГОСТ 28147-89 відносно диференційного та лінійного криптоаналізу використовується набір з восьми S-блоків 4×4 стандарту Р 34.11-94, які застосовувались Центральним банком Російської Федерації.

Наведений аналіз криптографічних показників стійкості зазначеного набору S-блоків S1 - S8 (табл. 12) показує, що S-блоки специфікації Р 34.11-94 не мають оптимальних показників нелінійності та автокореляції. Використовуючи запропоновану математичну модель недвійкових функцій та удосконалений обчислювальний метод синтезу нелінійних вузлів замін, розроблено власний набір S-блоків S1* - S8* 4×4 з покращеними показниками нелінійності та автокореляції.

У процесі синтезу S-блоків S1* - S8* додатково накладено критерій мінімізації показників d, d', l вузлів замін, необхідних для оцінки практичної стійкості шифру ГОСТ 28147-89 відносно диференційного та лінійного криптоаналізу:

$$d = \max\left\{2^{-t}\sum_{k\in V_t}\delta(S(k+\alpha)\oplus S(k),\beta):\alpha,\beta\in V_t\setminus\{0\}\right\}, \qquad (11)$$

$$d' = \max\left\{2^{-t}\sum_{\substack{k\in V_t:\\ \nu(\alpha,k)=a}}\delta(S(k+\alpha)\oplus S(k),\beta):\alpha,\beta\in V_t\setminus\{0\},a\in\{0,1\}\right\}, \qquad (12)$$

$$l = \max\left\{ 2^{-t} \sum_{k \in V_t} \left(2^{-t} \sum_{x \in V_t} (-1)^{\beta S(x+k) \oplus \alpha x} \right)^2 : \alpha, \beta \in V_t \setminus \{0\} \right\}, \qquad (13)$$

де V_t – множина усіх t-мірних булевих векторів, випадковий вектор $(x_1,...,x_t) \in V_t$ ототожнюється з числом $x = 2^{t-1}x_1 + ... + 2^0 x_t$, S – S-блок, складання «+» у формулах виконується за модулем 2^t, $\delta(\cdot,\cdot)$ – символ Кронекера ($\delta(u, v) = 1$, якщо u = v, інакше $\delta(u, v) = 0$), $\nu(\alpha, k)$ - біт переносу в t цифру в сумі α і k у кільці $\mathbb{Z}$.

Таблиця 12 - Аналіз показників S-блоків ГОСТ Р 34.11-94 та пропонованих

	S-блок								
Показн.	S1	S2	S3	S4	S5	S6	S7	S8	S1*-S8*
NL	2	2	2	2	2	2	2	4	4
AC	16	16	16	16	16	16	16	16	8
d	0,375	0,25	0,375	0,25	0,375	0,25	0,25	0,1875	0,125
d'	0,3125	0,1875	0,1875	0,1875	0,1875	0,1875	0,1875	0,1875	0,125
l	0,289	0,25	0,289	0,3125	0,2812	0,25	0,25	0,25	0,25

У таблицях 13 - 14 наведено оцінки практичної стійкості шифру ГОСТ 28147-89 відносно диференційного та лінійного криптоаналізу для восьми циклів шифрування, які отримано згідно з роботою А.М. Олексійчука та Л.В. Ковальчук, присвяченій оцінкам практичної стійкості ГОСТ-подібних шифрів.

Таблиця 13 - Оцінки практичної стійкості ГОСТ 28147-89 відносно диференційного криптоаналізу з використанням різних наборів S-блоків

#r / S-блоки	17	…	26	27	28	29	30	31	32
S1-S8	$2^{-18,56}$	…	$2^{-27,84}$	$2^{-29,25}$	$2^{-29,52}$	$2^{-30,93}$	$2^{-32,35}$	$2^{-32,61}$	$2^{-34,02}$
S1*-S8*	2^{-36}	…	2^{-54}	2^{-57}	2^{-57}	2^{-60}	2^{-63}	2^{-63}	2^{-66}

Таблиця 14 - Оцінки практичної стійкості ГОСТ 28147-89 відносно лінійного криптоаналізу з використанням різних наборів S-блоків

#r / S-блоки	25	26	27	28	29	30	31	32
S1-S8	$2^{-26,85}$	$2^{-28,53}$	$2^{-30,21}$	$2^{-30,21}$	$2^{-31,88}$	$2^{-33,56}$	$2^{-33,56}$	$2^{-35,24}$
S1*-S8*	2^{-32}	2^{-34}	2^{-36}	2^{-36}	2^{-38}	2^{-40}	2^{-40}	2^{-42}

Аналіз отриманих оцінок демонструє, що використання нелінійних вузлів замін з покращеними властивостями дозволило підвищити ефективність симетричного алгоритму ГОСТ 28147-89 відносно диференційного та лінійного криптоаналізу.

Таким чином, використання запропонованої математичної моделі та удосконаленого обчислювального методу синтезу нелінійних вузлів замін через недвійкові криптографічні функції дозволяє синтезувати S-блоки з покращеними властивостя-

ми нелінійності та автокореляції, використання яких, у свою чергу, підвищує ефективність симетричних криптоперетворень відносно диференційного та лінійного криптоаналізу.

ВИСНОВКИ

У дисертаційній роботі отримано теоретичне узагальнення та нове вирішення важливого науково-технічного завдання розробки та дослідження обчислювальних методів синтезу нелінійних вузлів замін з покращеними властивостями для підвищення ефективності симетричних криптоперетворень.

1. Проведений аналіз сучасних симетричних криптоперетворень та їх математичних операцій показав, що основним та найбільш важливим елементом є нелінійні вузли замін, криптографічні властивості яких безпосередньо впливають на ефективність забезпечення безпеки інформаційних технологій. Проведені дослідження показників стійкості та методів формування нелінійних вузлів замін дозволили встановити, що значення показників стійкості формувальних S-блоків не є оптимальними, що впливає на ефективність симетричних криптоперетворень. Перспективним шляхом вирішення цього протиріччя є використання математичного апарату недвійкових функцій з перетворенням у арифметиці скінчених полів. Обґрунтовано необхідність вдосконалення математичних моделей та обчислювальних методів формування нелінійних вузлів замін з покращеними властивостями для підвищення ефективності симетричних криптографічних засобів захисту інформації.

2. Найбільш важливими науковими результатами дисертаційного дослідження є розвинута математична модель регулярних нелінійних вузлів замін симетричних криптоперетворень, що дозволяє у термінах теорії скінчених полів формалізувати процес формування нелінійних вузлів замін, використовувати методи кореляційного та спектрального аналізу над $GF(2^m)$ для дослідження криптографічних властивостей формувальних S-блоків; удосконалений обчислювальний метод синтезу нелінійних вузлів замін (метод імітації відпалу) з розробленими критеріями пошуку недвійкових криптографічних функцій, що дозволяє спростити процес формування блоків підстановок симетричних криптоперетворень з необхідними показниками нелінійності та автокореляції; розвинутий обчислювальний метод прогнозування оцінок ефективності симетричних криптоперетворень на основі дослідження диференційних та лінійних властивостей зменшених моделей шифрів, що дозволяє прогнозувати обчислювальні затрати шифрування, необхідні для досягнення асимптотичних диференційних та лінійних властивостей випадкової підстановки з урахуванням криптографічних властивостей використовуваних блоків підстановок; розвинуті методи оцінки обчислювальної ефективності ймовірнісного (побітового) синтезу регулярних нелінійних вузлів замін із заданими криптографічними показниками, що дозволяє оцінювати обчислювальну ефективність неалгебраїчних методів синтезу блоків підстановок симетричних криптоперетворень.

3. Найбільш важливими практичними результатами дисертаційного дослідження є сформовані нелінійні вузли замін з покращеними властивостями; отримані оцінки ефективності зменшених версій блокових симетричних шифрів з використанням нелінійних вузлів замін з різними показниками нелінійності та автокореляції, що до-

зволили обґрунтувати вплив криптографічних властивостей блоків замін на ефективність симетричних криптоперетворень; отримані оцінки обчислювальної ефективності методів ймовірнісного (побітового) синтезу регулярних нелінійних вузлів замін m×m із заданими криптографічними показниками, що дозволили встановити межі обчислювальності ($m \leq 6$) досліджуваних побітових методів, обґрунтувати необхідність розробки нових моделей і неалгебраїчних методів синтезу блоків підстановок для $m > 6$.

4. Вироблено практичні рекомендації з використання розробленої моделі та методу формування нелінійних вузлів замін для удосконалення блокових симетричних криптоперетворень. Обґрунтовано рекомендації з ймовірнісного синтезу нелінійних вузлів замін симетричних криптоперетворень, зокрема, запропоновані рішення використані для розробки пропозицій щодо формування S-блоків симетричних криптоперетворень, які можуть бути застосовані у перспективному алгоритмі блокового симетричного шифрування для підвищення його ефективності відносно диференційного та лінійного криптоаналізу.

5. Результати дисертаційної роботи рекомендується використовувати при проведенні науково-дослідних та дослідно-конструкторських робіт зі створення нових криптографічних засобів захисту інформації. Результати досліджень будуть корисні для підготовки спеціалістів у вищих навчальних закладах Міністерства освіти і науки, молоді та спорту України при вивченні учбових дисциплін з математичного моделювання, обчислювальної техніки, теорії захисту інформації, теорії інформації та кодування.

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ

1. Сорока Л.С. Вероятностная модель формирования нелинейных узлов замен для симметричных криптографических средств защиты информации / Л.С. Сорока, А.А. Кузнецов, И.В. Московченко, С.А. Исаев // Системи обробки інформації. – 2009. – Вип. 3(77). – С. 101 – 104.
2. Сорока Л.С. Исследование дифференциальных свойств блочно-симметричных шифров / Л.С. Сорока, А.А. Кузнецов, И.В. Московченко, С.А. Исаев // Системи обробки інформації. – 2010. – Вип. 6(87). – С. 286 – 292.
3. Сорока Л.С. Исследование вероятностных методов формирования нелинейных узлов замен / Л.С. Сорока, А.А. Кузнецов, С.А. Исаев // Системи обробки інформації. – 2011. – Вип. 8(98). – С. 113 – 122.
4. Сорока Л.С. Исследование линейных свойств мини-версий блочно-симметричных шифров / Л.С. Сорока, А.А. Кузнецов, С.А. Исаев // Сучасний захист інформації. – 2011. – Вип. 3. – С. 83 – 93.
5. Долгов В.И. Дифференциальные свойства блочных симметричных шифров / В.И. Долгов, А.А. Кузнецов, С.А. Исаев // Электронное моделирование. – 2011. – Том 33, № 6. – С. 81 – 99.
6. Кузнецов А.А. Линейные свойства блочных симметричных шифров, представленных на украинский конкурс // А.А. Кузнецов, И.В. Лисицкая, С.А. Исаев // Прикладная радиоэлектроника. – 2011. – Том 10, № 2. – С. 135 – 140.
7. Кузнецов А.А. Математическая модель регулярных нелинейных узлов замен с

использованием аппарата недвоичных криптографических функций / А.А. Кузнецов, С.А. Исаев, В.В. Фролов // Системи управління, навігації та зв'язку: збірник наукових праць. – 2012. – Вип. 3(23). – С. 81 – 86.

8. Кузнецов А.А. Вычислительный метод синтеза регулярных нелинейных узлов замен с использованием недвоичных криптографических функций / А.А. Кузнецов, С.А. Исаев, В.В. Фролов // Збірник наукових праць Харківського університету Повітряних Сил. – 2012. – Вип. 4(33). – С. 148 – 153.
9. Московченко І.В. Сравнительные исследования эффективности эвристических методов вероятностного формирования криптографических булевых функций / І.В. Московченко, С.О. Ісаєв // Системи обробки інформації: інформаційні технології та захист інформації. – Х.:ХУ ПС, 2012. - Випуск 4(102), том 1. – С. 207 – 208.
10. Сорока Л.С. Исследование линейных характеристик уменьшенных моделей блочно-симметричных шифров / Л.С. Сорока, А.А. Кузнецов, С.А. Исаев // ІІ Міжнародна науково-практична конференція «Інформаційні технології та комп'ютерна інженерія»: Тези доповідей. – Х.:ХНЕУ. – 2011. – С. 93 – 94.
11. Кузнецов А.А. Исследование вероятностных методов формирования нелинейных узлов замен / А.А. Кузнецов, С.А. Исаев // Системи обробки інформації: проблеми і перспективи розвитку ІТ-індустрії. Вип. 7(97). – Харків. – 2011. – С. 132 – 133.
12. Сорока Л.С. Методы эвристического формирования нелинейных узлов замен блочных симметричных шифров / Л.С. Сорока, А.А. Кузнецов, И.В. Московченко, С.А. Исаев // Застосування інформаційних технологій у підготовці та діяльності сил охорони правопорядку. Збірник тез доповідей науково-практичної конференції. – Харків. – 2012. – С. 72 – 73.
13. Сорока Л.С. Исследование методов формирования нелинейных узлов замен / Л.С. Сорока, А.А. Кузнецов, С.А. Исаев // Перспективи розвитку інформаційних та транспортно-митних технологій у митній справі, зовнішньоекономічній діяльності та управлінні організаціями. Матеріали міжнародної науково-практичної конференції. – Дніпропетровськ. – 2011. – С. 244 – 246.
14. Kuznetsov A. Differential Properties of Mini-Versions of Block Symmetric Ciphers / A. Kuznetsov, R. Serhiienko, S. Isaev, P. Laptii // Statistical methods of signal and data processing. Proceedings. – Kiev:NAU-Druk. – 2010. – P. 147 – 150.
15. Кузнецов А.А. Исследование дифференциальных свойств мини-версий SPN шифров / А.А. Кузнецов, Р.В. Сергиенко, С.А. Исаев // Новітні технології – для захисту повітряного простору. Шоста наукова конференція Харківського університету Повітряних Сил ім. Івана Кожедуба. Тези доповідей. – Х.:ХУ ПС. – 2010. – С. 122 – 123.
16. Кузнецов О. Евристичні методи синтезу нелінійних вузлів замін симетричних шифрів / О. Кузнецов, Л. Сорока, І. Московченко, С. Ісаєв // Захист інформації і безпека інформаційних систем. Матеріали І-ї міжнародної науково-технічної конференції. – Л.:Львівська політехніка. – 2012. – С. 150 – 151.
17. Кузнецов А.А. Дифференциальные свойства мини-версий блочно-симметричных шифров / А.А. Кузнецов, С.А. Исаев, П.А. Лаптий // Інформаційні технології в навігації і управлінні: стан та перспективи розвитку. Матеріали першої міжнаро-

дної науково-технічної конференції. – К.:ЦНДІ НіУ. – 2010. – С. 23.
18. Сергиенко Р.В. Математические модели и вычислительные методы построения нелинейных узлов замен симметричных криптографических средств защиты информации / Р.В. Сергиенко, И.В. Московченко, С.А. Исаев // Компьютерное моделирование в наукоемких технологиях (КМНТ-2010). Труды научно-технической конференции с международным участием. Часть 2. – Х.: ХНУ. – 2010. – С. 228 – 230.
19. Сергиенко Р.В. Исследование методов формирования регулярных S-боксов для блочных симметричных шифров / Р.В. Сергиенко, И.В. Московченко, С.А. Исаев // Застосування інформаційних технологій у підготовці та діяльності сил охорони правопорядку: збірник тез доповідей науково-практичної конференції академії внутрішніх військ МВС України. – Харьков. – 2010. – С. 59.
20. Долгов В.И. Линейные свойства симметричных шифров, представленных на украинский конкурс / В.И. Долгов, А.А. Кузнецов, С.А. Исаев // Наука и социальные проблемы общества: информатизация и информационные технологи. Сборник научных трудов VI-й Международной научно-практической конференции – Х.:ХНУРЕ. – 2011. – С. 260 – 261.

АНОТАЦІЯ

Ісаєв С.О. Обчислювальні методи синтезу нелінійних вузлів замін для підвищення ефективності симетричних криптоперетворень. – На правах рукопису.

Дисертація на здобуття наукового ступеня кандидата технічних наук за спеціальністю 05.13.21 – системи захисту інформації. – Харківський національний університет радіоелектроніки, Харків, 2012.

Дисертаційна робота присвячена підвищенню ефективності симетричних криптоперетворень на основі синтезу нелінійних вузлів замін з покращеними властивостями. В роботі знаходить свій подальший розвиток математична модель регулярних нелінійних вузлів замін симетричних криптоперетворень з використанням недвійкових криптографічних функцій в арифметиці скінчених полів; удосконалено обчислювальний метод синтезу нелінійних вузлів замін (метод імітації відпалу) шляхом розробки критеріїв пошуку з використанням спектральних та кореляційних властивостей недвійкових криптографічних функцій та динамічних вагових коефіцієнтів; розвинуто обчислювальний метод прогнозування оцінок ефективності симетричних криптоперетворень на основі дослідження диференційних і лінійних властивостей зменшених моделей шифрів з урахуванням показників нелінійності та автокореляції використовуваних нелінійних вузлів замін; розвинуто методи оцінки обчислювальної ефективності ймовірнісного (побітового) синтезу регулярних нелінійних вузлів замін із заданими криптографічними показниками. Основними практичними результатами роботи є сформовані нелінійні вузли замін з покращеними властивостями; оцінки ефективності зменшених версій блокових симетричних шифрів з використанням нелінійних вузлів замін з різними показниками нелінійності та автокореляції; оцінки обчислювальної ефективності методів ймовірнісного (побітового) синтезу регулярних нелінійних вузлів замін m×m із заданими криптографічними показниками.

Вироблено практичні рекомендації з використання розроблених моделей та методів формування нелінійних вузлів замін для удосконалення блокових симетричних криптоперетворень. Запропоновані рішення використано для розробки S-блоків симетричних криптоперетворень, які можуть бути застосовані у перспективному алгоритмі блокового симетричного шифрування для підвищення ефективності відносно диференційного та лінійного криптоаналізу.

Ключові слова: вузол замін, нелінійність, автокореляція, блоковий симетричний шифр, ефективність симетричних криптоперетворень.

АННОТАЦИЯ

Исаев С.А. Вычислительные методы синтеза нелинейных узлов замен для повышения эффективности симметричных криптопреобразований. – На правах рукописи.

Диссертация на соискание ученой степени кандидата технических наук по специальности 05.13.21 – системы защиты информации. Харьковский национальный университет радиоэлектроники, Харьков, 2012.

Диссертационная работа посвящена повышению эффективности симметричных криптопреобразований на основе синтеза нелинейных узлов замен с улучшенными свойствами. Проведенный анализ современных симметричных криптопреобразований и их математических операций показал, что основным и наиболее важным элементом являются нелинейные узлы замен, криптографические свойства которых непосредственно влияют на эффективность обеспечения безопасности информационных технологий. Проведенные исследования показателей стойкости и методов формирования нелинейных узлов замен позволили установить, что значения показателей стойкости формируемых S-блоков не являются оптимальными, что влияет на эффективность симметричных криптопреобразований. Обоснована необходимость совершенствования математических моделей и вычислительных методов формирования нелинейных узлов замен с улучшенными свойствами для повышения эффективности симметричных криптографических средств защиты информации.

В работе развивается математическая модель регулярных нелинейных узлов замен симметричных криптопреобразований с использованием недвоичных криптографических функций в арифметике конечных полей; совершенствуется метод синтеза нелинейных узлов замен (метод имитации отжига) путем разработки критериев поиска с использованием спектральных и корреляционных свойств недвоичных криптографических функций и динамических весовых коэффициентов; развивается вычислительный метод прогнозирования оценок эффективности симметричных криптопреобразований на основе исследования дифференциальных и линейных свойств уменьшенных моделей шифров с учетом показателей нелинейности и автокорреляции используемых нелинейных узлов замен; развиваются методы оценки вычислительной эффективности вероятностного (побитового) синтеза регулярных нелинейных узлов замен с заданными криптографическими показателями. Основными практическими результатами работы являются сформированные нелинейные узлы замен с улучшенными свойствами; оценки эффективности уменьшенных версий блочных симметричных шифров с использованием нелинейных узлов замен с

разными показателями нелинейности и автокорреляции; оценки вычислительной эффективности методов вероятностного (побитового) синтеза регулярных нелинейных узлов замен m×m с заданными криптографическими показателями.

Выработаны практические рекомендации по использованию разработанной модели и усовершенствованного метода формирования нелинейных узлов замен для совершенствования блочных симметричных криптопреобразований. Предложенные решения использованы для разработки S-блоков симметричных криптопреобразований, которые могут быть применены в перспективном алгоритме блочного симметричного шифрования для повышения эффективности относительно дифференциального и линейного криптоанализа.

Ключевые слова: узел замен, нелинейность, автокорреляция, блочный симметричный шифр, эффективность симметричных криптопреобразований.

ABSTRACT

Isaev S.A. Computational synthesis methods of nonlinear substitution blocks to improve the efficiency of symmetric crypto transformations. – Manuscript.

Thesis for the candidate degree of technical sciences on speciality 05.13.21 – information security systems. – Kharkiv, National University of Radio Electronics, Kharkiv, 2012.

The thesis is dedicated to increasing the efficiency of symmetric cryptotransformations based on the synthesis of nonlinear substitution boxes with improved properties. The mathematical model of regular nonlinear boxes of cryptotransformations using symmetric non-binary cryptographic functions in arithmetic of finite fields is developed, method for the synthesis of nonlinear substitution boxes (the method of simulated annealing) through the development of search criterions using spectral and correlation properties of non-binary cryptographic functions and dynamic weights is improved; computational method for forecasting efficiency evaluations of symmetric cryptotransformations based on the study of differential and linear properties of the reduced cipher models with accounting of nonlinearity and autocorrelation properties of used nonlinear substitution boxes is developed, computational methods for evaluating the computational effectiveness of probabilistic (bit-to-bit) synthesis of regular nonlinear substitution boxes with given cryptographic properties are developed. The main practical results of the work are generated nonlinear substitution boxes with improved properties, evaluations of the effectiveness of reduced versions of block symmetric ciphers with the use of nonlinear substitution boxes with different properties of nonlinearity and autocorrelation, evaluations of the computational efficiency of the probabilistic methods (bit-to-bit) for synthesis of regular nonlinear substitution boxes m×m with given cryptographic properties.

Practical recommendations on the use of developed model and improved method of synthesis of nonlinear substitution boxes for perfecting the block symmetric cryptotransformations are made. The proposed solutions are used to design S-boxes of symmetric cryptotransformations, which can be used in a perspective block symmetric encryption algorithm to improve the efficiency towards differential and linear cryptanalysis.

Keywords: substitution box, nonlinearity, autocorrelation, block symmetric cypher, efficiency of symmetric cryptotransformations.

Підп. до друку 04.04.2013. Формат 60х84 1/16. Спосіб друку – ризографія.
Умов. друк. арк. 1,3. Облік. вид. арк. 1,2. Тираж 100 прим.
Зам № 2-233. Ціна договірна.

ХНУРЕ. Україна. 61166, Харків, просп. Леніна, 14

Віддруковано в навчально-науковому
видавничо-поліграфічному центрі ХНУРЕ
61166, Харків, просп. Леніна, 14