МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ОДЕСЬКА НАЦІОНАЛЬНА АКАДЕМІЯ ЗВ'ЯЗКУ ІМ. О.С. ПОПОВА

КОСОВАН ГРИГОРІЙ ВАСИЛЬОВИЧ

УДК 004.056.55

СИНТЕЗ ГЕНЕРАТОРІВ ПСЕВДОВИПАДКОВИХ ПОСЛІДОВНОСТЕЙ ІЗ НЕЛІНІЙНОЮ ДИНАМІКОЮ ДЛЯ ЗАХИСТУ ІНФОРМАЦІЇ В ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ

05.13.21 – системи захисту інформації

Автореферат
дисертації на здобуття наукового ступеня
кандидата технічних наук

Одеса – 2018

Дисертацією є рукопис
Робота виконана у Чернівецькому національному університеті імені Юрія Федьковича Міністерства освіти і науки України

Науковий керівник кандидат фізико-математичних наук, доцент
Кушнір Микола Ярославович,
Чернівецький національний університет
імені Юрія Федьковича,
доцент кафедри радіотехніки
та інформаційної безпеки

Офіційні опоненти: доктор технічних наук, професор
Толюпа Сергій Васильович,
Київський національний університет ім. Тараса Шевченка, професор кафедри кібербезпеки та захисту інформації;

доктор технічних наук, доцент
Корчинський Володимир Вікторович,
Одеська національна академія зв'язку ім. О. С. Попова, доцент кафедри інформаційної безпеки та передачі даних

Захист відбудеться "08" лютого 2019 року о 11:00 годині на засіданні спеціалізованої вченої ради Д 41.816.02 в Одеській Національній академії зв'язку ім. О.С. Попова за адресою: 65029, м. Одеса, вул. Кузнечна 1, ауд. 223.

З дисертацією можна ознайомитися в Одеській національній академії зв'язку ім. О.С. Попова (65029, м. Одеса, вул. Кузнечна 1).

Автореферат розісланий «____» _____ 20___ р.

Учений секретар
спеціалізованої вченої ради М. В. Рожновський

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Актуальність теми. Починаючи з 1980-х років ідея використання цифрових хаотичних систем та генераторів псевдовипадкових послідовностей (ПВП) для проектування нових шифрів привертала все більшу увагу. Використання хаосу в криптографії обумовлено властивостями хаотичних систем. Використовуючи їх розробники створюють нові генератори ПВП та методи шифрування інформації на їх основі з сильними криптографічними властивостями.

Фізики поділяють системи на стійкі та нестійкі. У стійких системах малі збурення затухають і системи повертаються до стаціонарного стану, а в хаотичних (нестійких) системах малі збурення зростають з часом. Хаотичні системи володіють екстремальною чутливістю до початкових умов, тобто малі відхилення в початковому стані системи призводять до зміни всієї траєкторії системи в майбутньому. Саме тому непередбачуваність поведінки детермінованих систем є основною причиною використання таких систем при проектуванні криптографічних методів. В цілому є два шляхи використання хаосу для застосування в захищених системах: аналогові хаотично захищені системи зв'язку (головним чином засновані на техніці синхронізації хаосу) і цифрові хаотичні шифри (реалізовані на комп'ютерах).

Найбільш стрімко хаос в криптографії почали використовувати в другій половині 1990-х рр., і були отримані значні досягнення при створенні нових методів шифрування. Так само в другій половині 1990-х був здійснений криптоаналіз ряду запропонованих хаотичних шифрів та було встановлено недоліки, що можуть бути їм притаманні. Проте значна частина запропонованих методів шифрування взагалі не була піддана криптоаналізу через відсутність чітких критеріїв оцінки їх захищеності. Тим не менше були сформовані загальні шляхи розроблення методів шифрування та сформовані рекомендації щодо підвищення їх захищеності.

В наш час над проблемою використання динамічного хаосу в криптографії активно працюють вітчизняні та зарубіжні наукові колективи. Увага, яку приділяють криптографічним методам, що використовують хаотичні системи, свідчить про перспективу цього напряму досліджень.

Одним із перспективних напрямків досліджень є синтез генераторів псевдовипадкових послідовностей (ПВП) на основі хаосу та розроблення на їх основі методів шифрування інформації. Використання таких генераторів при розробленні методів шифрування обумовлене їх статистичними характеристиками.

Проте важливим питанням в проектуванні методів шифрування залишається аналіз захищеності методів, реалізованих на основі генераторів ПВП, на який впливає динамічна деградація цифрових хаотичних систем. Також досі залишаються відкритими питання щодо статистичних властивостей одновимірних та багатовимірних хаотичних систем, що реалізовуються в комп'ютерах. Завданнями дисертаційної роботи є проведення аналізу існуючих генераторів ПВП та методів шифрування на їх основі, синтез нових генераторів ПВП на основі одно- та багатовимірних хаотичних систем та удосконалення

методів шифрування інформації на основі отриманих ПВП генераторів. Це і обумовлює актуальність дисертаційної роботи.

Науково-прикладним завданням, розв'язанню якого присвячена дисертаційна робота, є синтез та дослідження характеристик генераторів ПВП на основі одно- та багатовимірних хаотичних систем, а також вдосконалення існуючих методів шифрування інформації на їх основі.

Зв'язок роботи з науковими програмами, планами, темами. Обрані напрями дисертаційного дослідження безпосередньо пов'язані із науково-технічними завданнями, сформульованими в Постанові Кабінету Міністрів України № 942 від 7.09.2011 р. із змінами, внесеними постановою КМ № 556 від 23.08.2016 р. "Про затвердження переліку пріоритетних тематичних напрямів наукових досліджень і науково-технічних розробок на період до 2020 року" та виконувались в рамках держбюджетної науково-дослідної роботи кафедри радіотехніки та інформаційної безпеки Чернівецького національного університету імені Юрія Федьковича: "Фізико-технологічні проблеми радіотехнічних пристроїв та засобів телекомунікацій і інформаційних технологій" (Держ. реєстр. №0111U000183, 2013-2015 рр.), а також "Методи та засоби передавання, оброблення і зберігання інформації в інфо-комунікаційних системах" (Держ. реєстр. №0116U001433, 2016-2020рр.).

Мета роботи і завдання досліджень. Метою дисертаційної роботи є аналіз та синтез генераторів ПВП на основі одно- та багатовимірних динамічних систем, а також їх використання при вдосконаленні методів шифрування інформації та оцінка їх стійкості при криптографічних атаках.

Для досягнення поставленої мети необхідно розв'язати наступні задачі:

– провести аналіз відомих у літературі генераторів ПВП на основі хаотичних систем та методів шифрування інформації на їх основі;

– дослідити статистичні властивості псевдовипадкових послідовностей, генерованих одновимірними хаотичними системами та розробити нові генератори ПВП на основі одно- та багатовимірних хаотичних систем;

– розробити і дослідити криптографічні властивості методів шифрування текстової інформації, зображень та бінарних файлів на основі генераторів ПВП, побудованих із використанням хаотичних систем;

– розробити програмне забезпечення для реалізації отриманих методів шифрування.

Об'єкт дослідження -- процес формування псевдовипадкових послідовностей на базі хаотичних систем, а також процеси криптографічного закриття інформації за допомогою синтезованих генераторів ПВП.

Предмет дослідження -- генератори псевдовипадкових послідовностей на основі одно- та багатовимірних хаотичних систем для захисту інформації в телекомунікаційних системах.

Методи дослідження: під час розв'язання поставлених завдань у роботі використовувалися методи чисельного інтегрування систем нелінійних диференційних рівнянь, математичне моделювання нелінійної динаміки (біфуркаційні діаграми, фазові портрети), методи теорії імовірності і випадкових процесів для дослідження статистичних характеристик псевдовипадкових генераторів та елементи криптоаналізу для оцінки стійкості методів шифрування.

Наукова новизна роботи полягає в наступному:

до основних наукових результатів, що одержані в дисертаційній роботі, можна віднести наступні:

1. Удосконалено генератор ПВП бітів, на основі двох одновимірних хаотичних систем, формованих операцією сумування по модулю два відповідних елементів псевдовипадкових послідовностей генерованих одновимірними хаотичними генераторами (логістичне та кубічне відображення). Це дало змогу збільшити обсяг простору ключів при задані початкових умов з точністю до 5-го знаку після коми з 10^{10} до 10^{25} ключів.

2. Вперше запропоновано генератор формування псевдовипадкових послідовностей на основі двох нелінійних хаотичних систем, значення хаотичних коливань, генерованих логістичним відображенням в якому слугують динамічним пороговим рівнем прийняття рішення щодо значення бітів у псевдовипадкових послідовностях, генерованих системою Лоренца. При значеннях хаотичних коливань, генерованих системою Лоренца, що є більшими значень генерованими логістичним відображенням, приймається рішення про формування логічної “1” і логічного “0” в протилежному випадку, що ускладнює розпізнання динамічної поведінки хаотичної системи і збільшує обсяг ключового простору до 10^{40}.

3. Удосконалено класичний метод М. Баптісти шифрування текстової інформації шляхом використання двох хаотичних систем (система Ресслера та кубічне відображення). Система Ресслера слугує генератором початкових умов для кубічного відображення, генеровані значення хаотичних коливань якої визначають номер ітерації для шифрування знаків первинного алфавіту. Внаслідок цього обсяг ключового простору збільшується з 10^{10} до 10^{45}.

4. Удосконалено метод шифрування зображень на основі формованих логістичною, квадратною та кубічною функціями хаотичних відображень сіток пікселів, внаслідок чого обсяг ключового простору зріс від 10^{13} до 10^{23}.

Практичне значення отриманих результатів.

1. Здійснено синтез генераторів псевдовипадкових послідовностей бітів для телекомунікаційних систем, що ефективно реалізуються на практиці програмними засобами.

2. Розроблене програмне забезпечення формування псевдовипадкових послідовностей бітів для шифрування конфіденційної інформації.

3. Проведена оцінка статистичних характеристик псевдовипадкових послідовностей, генерованих на базі одно- та багатовимірних систем з нелінійною динамікою.

4. Розроблено програмне забезпечення алгоритмів шифрування тексту і зображень на основі одно- та багатовимірних систем з нелінійною динамікою.

5. Отримані в роботі результати відображені в матеріалах НДР та впроваджені в навчальний процес на кафедрі радіотехніки та інформаційної безпеки Чернівецького національного університету ім. Ю. Федьковича, що підтверджується відповідними актами впровадження. Практична цінність роботи в тому, що отримані результати придатні для інженерного проектування

захищених систем зв’язку та баз даних в телекомунікаційних систем, що підтверджено актом впровадження основних результатів дослідження на ПАТ “Укртелеком”.

Результати роботи впроваджені в науковий та навчальний процеси кафедри радіотехніки та інформаційної безпеки.

Достовірність отриманих результатів підтверджується узгодженістю теоретичних розрахунків та результатів моделювання із експериментально отриманими даними.

Особистий внесок здобувача. Основні результати дисертаційної роботи були отримані автором самостійно. Постановка задач, розробка методів їх вирішення, пояснення й інтерпретація результатів здійснено або особисто автором, або спільно з керівником. У роботах, опублікованих у співавторстві, особистий внесок здобувача такий: [1] – розробка блокового методу шифрування зображення на основі детермінованих хаотичних систем, моделювання детермінованих хаотичних систем, оцінка стійкості криптографічного методу проти різного роду атак, аналіз кореляції між сусідніми пікселями зображення; [2] – розробка генератора псевдовипадкових послідовностей бітів із динамічним пороговим рівнем прийняття рішення, моделювання роботи генератора в середовищі LabView; [3] – розробка способу шифрування зображень із використанням трьох одновимірних хаотичних відображень; [4] – розробка методу шифрування текстової інформації на основі двох детермінованих динамічних систем, моделювання детермінованих хаотичних систем, оцінка стійкості криптографічного методу проти різного роду атак; [5] – вдосконалено метод криптографічного захисту зображення на основі двовимірного узагальненого перетворення пекаря шляхом розширення його до тривимірного і застосуванням додаткової дифузії в процесі шифрування; [6] – дослідження статистичних властивостей генератора псевдовипадкових послідовностей бітів із динамічним пороговим рівнем прийняття рішення; [7] – дослідження статистичних властивостей бітових послідовностей генерованих двома методами: перший – із застосуванням порогового методу прийняття рішення про значення генерованого біту та другий – шляхом перетворення генерованого десяткового значення в двійкове представлення; [8] – генерування псевдовипадкових послідовностей для формування широкосмугового сигналу; [9] – розробка системи передачі даних на основі теорії динамічного хаосу; [10] – розробка програмного забезпечення для дослідження хаотичних систем; [11] – моделювання роботи методу шифрування на основі двовимірного та одновимірного відображень; [12] – розробка методу шифрування інформації на основі двох динамічних систем для захищеної бази даних, [13] – вибір динамічних систем та розробка методу шифрування текстової інформації на основі двох динамічних систем, [14] – здійснена оцінка стійкості методів шифрування зображення проти атаки грубої сили та проведено оцінку швидкості шифрування; [15] – розробка генератора псевдовипадкових послідовностей на основі детермінованого хаосу; [16] – формування псевдовипадкових послідовностей генераторами на основі одновимірних хаотичних систем.

Апробація результатів дисертації. Основні результати дисертаційної роботи доповідалися і обговорювалися на восьми міжнародних науково-технічних та науково-практичних конференціях.

Публікації. Основні результати дисертації опубліковано в 16 наукових працях: 1 патент України на корисну модель, 5 статей, які опубліковані в наукових журналах, що включені до Переліку фахових видань України; 2 статті в закордонних періодичних наукових виданнях; 8 публікацій у матеріалах міжнародних науково-технічних та науково-практичних конференцій, 1 з яких індексується у міжнародій науковометричній базі Scopus.

Структура та об'єм дисертації. Дисертація складається із анотації, вступу, чотирьох розділів, висновків та списку літератури. Загальний обсяг дисертації становить 176 сторінки та містить 37 рисунок і 19 таблиць. Список використаних джерел складається з 208 найменувань.

ОСНОВНИЙ ЗМІСТ РОБОТИ

У вступі обґрунтовано актуальність теми дисертаційної роботи, сформульовано мету, завдання, визначено об'єкт і предмет, представлено наукову новизну та практичне значення одержаних автором результатів, зазначено особистий внесок здобувача, а також дані щодо апробації результатів та публікацій за темою дисертації.

У **першому розділі "Загальні принципи використання хаотичних систем для захисту інформації"** здійснено аналіз літературних джерел, присвячених дослідженню теоретичних та прикладних аспектів використання детермінованого хаосу в криптографії, висвітлено основні положення застосування хаотичних систем при генеруванні ПВП та створенні криптографічних методів шифрування інформації.

Представлено короткий історичний огляд створення криптографічних методів шифрування інформації з використанням детермінованих хаотичних систем. Розглянуто приклади реалізації хаотичних потокових та блокових шифрів на основі генераторів ПВП. Наведено приклади реалізації потокових методів шифрування текстової інформації, потокового методу шифрування на основі операції XOR та блокового методу шифрування зображення за допомогою логістичного відображення. Одними із основних завдань, що необхідно виконати - здійснити синтез генераторів ПВП на основі одно- та багатовимірних хаотичних систем та удосконалити існуючі методи шифрування інформації.

Створення генераторів ПВП на основі декількох динамічних систем є найбільш перспективним напрямком при розробці стійких методів шифрування інформації.

На основі аналізу літературних джерел сформульовані завдання дисертаційних досліджень.

Другий розділ "Синтез генераторів псевдовипадкових послідовностей на основі одно- та багатовимірних хаотичних систем" присвячений питанням аналізу генераторів ПВП на основі одновимірних хаотичних систем

та синтезу ГПВП на основі одно- та багатовимірних хаотичних систем, з метою уможливлення їх застосування при розробці методів шифрування інформації на основі хаосу.

Генератори ПВП на основі хаосу можуть бути легко реалізовані на комп'ютері використовуючи програмне середовище, але при цьому будь-яка хаотична система перестає бути дійсно випадковою та стає псевдовипадковою, що відбувається внаслідок зменшення множини можливих станів, тобто виникає повторюваність через великі проміжки часу. Розв'язання даної проблеми можливе шляхом збільшення точності обчислень та за рахунок використання поєднання різних одно- або багатовимірних хаотичних систем.

Розглянемо це на прикладі дослідження характеристик та статистичних властивостей псевдовипадкових бітових послідовностей, генерованих одновимірними відображеннями, а саме логістичним (1), квадратним (2) та кубічним (4), на основі яких буде здійснено синтез генераторів ПВП та побудовані методи шифрування.

$$x_{n+1} = r x_n (1 - x_n), \tag{1}$$

$$y_{n+1} = 1 - \mu y_n^2, \tag{2}$$

$$z_{n+1} = a - b z_n + z_n^3, \tag{3}$$

де $x_0 \in (0;1)$, $y_0 \in (0;1)$ та $z_0 \in (0;1)$ – початкові стани хаотичних систем, $r \in (3,57;4]$, $\mu \in (1,4;2]$, $a \in (-0,6;0,6)$ та $b \in (0,8;2,5)$ - параметри керування.

Під час дослідження періодичності одновимірних відображень було використано значення змінних генерованих одновимірними відображеннями із довільно обраних ітерацій. При цьому змінювалась точність обчислення від 2-го до 15-го знаку після коми та максимальна кількість повторних розв'язків склала 10^8 ітерацій. Номер ітерації, при якій відбулася повторна генерація значення і є періодом повторення.

З отриманих результатів випливає, що період повторної генерації послідовності, зі збільшенням точності обчислення, швидше зростає для послідовностей, генерованих квадратним та кубічним відображеннями. Період повторення кубічного відображення для 9 знаків після коми перевищував 10^8 ітерацій, для квадратного при 8 знаках, а для логістичного при 14 знаках.

Для дослідження властивостей псевдовипадкових послідовностей, формованих трьома одновимірними відображеннями, генерування їх здійснювалось за двома методами. Перший метод полягає в тому, що випадкове значення, генероване хаотичною системою порівнюється з величиною порогу прийняття рішення. Якщо це значення більше порогу прийняття рішень то йому присвоювалась логічна "1", а якщо менше – то логічний "0". Другий метод генерування полягає в двійковому представленні значення, генерованого одновимірним відображенням.

Кожна послідовність, довжиною 16000000 біт, генерувалася при певному значенні початкових умов в програмному середовищі Delphi 7 з фіксованою точністю обчислення в 10 знаків після коми. Для проведення статистичних

досліджень кожного з генераторів використовувався набір статистичних тестів NIST STS 1,6.

З отриманих результатів дослідження статистичних характеристик випливає, що 75 % усіх генерованих послідовностей відповідають умовам всіх 15-ти статистичних тестів і є псевдовипадковими.

Встановлено, що спосіб генерування псевдовипадкової послідовності із перетворенням генерованого значення в двійкове представлення, є кращим для використання в криптографії.

Проведені статистичні дослідження показали, що генератори на основі одновимірних хаотичних систем з пороговим методом визначення значення генерованого біту генерують дійсно псевдовипадкові послідовності у вузькому діапазоні ключів. Одним із способів розв'язання проблеми при генеруванні псевдовипадкових послідовностей на основі одновимірних хаотичних систем пороговим методом є використання комбінацій із декількох різних хаотичних відображень. Слід зазначити, що використання двох і більше одновимірних відображень призводить до збільшення кількості ключів та зростання потужності ключового простору. При цьому генерація різних траєкторій, з їх наступним перемішуванням, приховує внутрішні стани динамічних систем і унеможливлює встановлення аналітиком певних відомостей про використані динамічні системи.

Запропонований генератор ПВП побудований із використанням логістичної (1) та кубічної (3) функції відображення, що генерують псевдовипадкові бітові послідовності із наступним поєднанням їх між собою. В даному генераторі відбувається часта зміна початкових умов, а саме після генерування 12-ти байт змінюється секційний ключ, а після генерування 48 байт змінюються загальні значення початкових умов. Часта зміна початкових значень дозволила значно підвищити захищеність генерованих послідовностей і криптостійкість методу шифрування на основі такого генератора.

Початкові умови для обох хаотичних відображень отримуються із зовнішнього секретного ключа, а параметри задаються користувачем. В такій схемі генерування обидві системи використовується для генерації значень, що перетворюються в бітову послідовність, за допомогою якої шифрується будь-яка бітова інформація. Початкова умова для другого відображення змінюється в процесі шифрування на основі генерованих значень першого відображення. Під час генерування діапазони вихідних значень обох відображень розбиваються на дві рівні частини, що не перекриваються між собою та утворюють рівень прийняття рішень, чи згенеровано логічний "0" чи логічна "1". Якщо генероване значення потрапляє в інтервал значень менших або рівних значенню порогового рівня то генерується логічний "0", в іншому випадку логічна "1".

Дві хаотичні системи володіють різним діапазоном вихідних значень. Перша система генерує випадкові числа для оновлення параметрів другої, а також генерує послідовність бітів, що являє собою ключову під послідовність. Друга система генерує потік бітів, що використовується в якості другої ключової підпослідовності. Вихідна псевдовипадкова послідовність є результатом додавання по модулю два елементів двох під послідовностей.

Шифрування інформації за допомогою даного генератора здійснюється шляхом поєднання інформаційної послідовності з ключовою за допомогою операції XOR. Для того, щоб можливо було розшифрувати повідомлення, зашифроване таким генератором внаслідок використання операції XOR, потрібно повністю відтворити процес генерації ПВП і повторно здійснити операцію XOR на приймальній стороні.

Для перевірки псевдовипадкових послідовностей на статистичні властивості було використано набір статистичних тестів NIST STS 2.1.2. Для цього були генеровані три псевдовипадкові послідовності з довільно вибраним ключем. Результати тестування приведені в табл. 1.

Таблиця 1

Результати статистичних тестів для трьох ПВП

Ключ генерування Тип тесту	K= cnbk[fvth189653 P_{value}	K= mjphrs58ltzx42 P_{value}	K= 7624nrs4q8 P_{value}
Частотний (монобітний тест)	0,595549	0,946308	0,419021
Частотний тест по блокам	0,275709	0,075719	0,867692
Тест серій	0,935716	0,334538	0,816537
Тест найдовшої серії з одиниць	0,055361	0,474986	0,129620
Тест рангу бінарних матриць	0,494392	0,897763	0,924076
Тест на основі дискретного перетворення Фур'є	0,739918	0,455937	0,419021
Тест на співпадіння з шаблоном без перекриття	0,102526	0,311542	0,275709
Тест шаблону з перекриттям	0,719747	0,137282	0,383827
Універсальний математичний тест Мауера	0,657933	0,474986	0,191687
Тест лінійної складності	0,779188	0,759756	0,574903
Тест серій	0,236810	0,304126	0,657933
Тест на основі апроксимації ентропії	0,035174	0,071601	0,455937
Тест накопичувальних сум	0,455937	0,129620	0,719747
Тест випадкових блукань	0,366918	0,186566	0,568055
Тест варіантів випадкових блукань	0,867692	0,484646	0,468595

З отриманих результатів випливає, що всі три послідовності пройшли набори статистичних тестів і це свідчить про високу ефективність роботи запропонованого генератора. Крім того результати показали, що мінімальне значення проходження кожного тесту, за винятком Тесту варіантів випадкових блукань, складає приблизно 0,960, а мінімальне значення проходження тестів варіантів випадкових блукань складає приблизно 0,941.

Генеровані послідовності були перевірені і за іншими критеріями, зокрема визначалась інформаційна ентропія генератора:

$$H(s) = \sum_{i=0}^{2^l-1} p(s_i) \log_2 \frac{1}{p(s_i)}. \qquad (4)$$

де $p(s_i)$ показує ймовірність символу s_i.

Табл. 2 показує інформаційну ентропію 3-х послідовностей розміром 10000000 бітів генерованих запропонованим генератором, що пройшли статистичну перевірку.

Таблиця 2

Інформаційна ентропія 3-х послідовностей, генерованих на основі двох одновимірних систем та операції XOR

Ключ генерування	Значення інформаційної ентропії
cnbk[fvth189653	7,999999951161936
mjphrs58ltzx42	7,999999968188625
7624nrs4q8	7,999999662513748

Для перевірки, чи дійсно змінились псевдовипадкові послідовності при зміні ключа генерування, можна визначити коефіцієнт кореляції між ними. Коефіцієнт кореляції Пірсона визначається як

$$r_{x,y} = \frac{\operatorname{cov}(x,y)}{\sigma_x \sigma_y}\ , \tag{5}$$

де $\operatorname{cov}(x,y) = \frac{1}{n}\sum_{i=1}^{n}(x_i - \bar{x})(y_i - \bar{y})\sigma_x = \frac{1}{n}\sum_{i=1}^{n}(x_i - \bar{x})^2\ \sigma_y = \frac{1}{n}\sum_{i=1}^{n}(y_i - \bar{y})^2$ з $\sigma_x \neq 0$ і $\sigma_y \neq 0$ використовується в якості міри для визначення кореляції між бітами в двох послідовностях. Значення коефіцієнтів кореляції приведені в табл. 3.

Таблиця 3

Значення коефіцієнтів кореляції між трьома псевдовипадковими послідовностями, генерованими двома одновимірними відображеннями та операцією XOR

Між послідовностями 1-2	Між послідовностями 1-3	Між послідовностями 2-3
0,000448918348949287	0,000180640565828867	0,000443037426172707

З отриманих результатів випливає, що кореляція між генерованими псевдовипадковими послідовностями повністю відсутня.

На основі запропонованого генератора було реалізовано метод шифрування інформації із використанням логістичної та кубічної функції відображення та було здійснено дослідження ефективності використання такого генератора при шифруванні зображень та бітових файлів.

В процесі дослідження методу шифрування проводився аналіз кореляції між сусідніми пікселями оригінального та зашифрованого зображення як по горизонталі, так і по вертикалі. Розрахунок кореляції здійснювався за наступною формулою

$$C_p = \frac{N\sum_{j=1}^{N} x_j y_i - \sum_{j=1}^{N} x_j - \sum_{j=1}^{N} y_i}{\sqrt{\left\{N\sum_{j=1}^{N} x_j^2 - \left(\sum_{j=1}^{N} x_j\right)^2\right\}}\sqrt{\left\{N\sum_{j=1}^{N} y_j^2 - \left(\sum_{j=1}^{N} y_i\right)^2\right\}}}, \tag{6}$$

де x та y – значення градацій кольору двох сусідніх пікселів, N – число пікселів зображення, вибраних для розрахунку коефіцієнту кореляції.

Для аналізу кореляції було використано зображення “Поле” та встановлено, що кореляція між двома сусідніми пікселями оригінального зображення складає по горизонталі 0,93 та по вертикалі 0,89, а після шифрування по горизонталі 0,078 та вертикалі 0,036.

Далі для підтвердження ефективності використання генератора ПВП на основі двох одновимірних хаотичних систем та операції XOR було здійснено оцінку інформаційної ентропії оригінального та зашифрованого зображення, результати оцінки приведені в табл. 4.

Крім того, з метою оцінки якості методів шифрування зображень використовується цілий ряд значень на основі пікселів:

– середньоквадратична помилка (MSE)
– відношення пікового сигналу до шуму (PSNR).

Таблиця 4

Отримані значення інформаційної ентропії оригінального та зашифрованого зображення

Тип зображення	Складова R	Складова G	Складова B
Оригінальне	7,72772772462904	7,24906293699095	6,93656002880145
Зашифроване	7,999591831385	7,99954577792749	7,99959292922143

Ефективність виконання процедури дешифрування вимірюється піковим відношення сигнал-шум (PSNR). Нехай $C(i,j)$ і $P(i,j)$ будуть рівнями інтенсивності кольору пікселів в і-му рядку j-м стовпці $H \times W$ шифру вхідного зображення, відповідно. MSE між цими двома зображення визначається наступним чином:

$$MSE = \frac{1}{H \times W} \sum_{i=0}^{H-1} \sum_{j=0}^{W-1} \left| C(i,j) - P(i,j) \right|^2 , \tag{7}$$

$$PSNR = 20 \times \log_{10} \left(\frac{255}{sqrt(MSE)} \right). \tag{8}$$

Зображення зі значенням PSNR 30 дБ або більше в загальному прийнято вважати зображенням з хорошою якістю шифрування.

Для того щоб перевірити, скільки пікселів було змінено в зображенні, були використані два загальні показники NPCR і UACI:

– кількість змінених пікселів в зображенні (NPCR);
– уніфікована середня зміна інтенсивності пікселів (UACI).

NPCR -- це кількість пікселів, що змінили свою інтенсивність в процесі шифрування зображення. UACI -- уніфікована середня зміна інтенсивності пікселів, що визначає середню інтенсивність відмінностей між вхідним зображенням і зашифрованим зображенням. NPCR зображення і визначається наступним чином:

$$NPCR = \frac{\sum_{i,j} D(i,j)}{H \times W}, \tag{9}$$

$$D(i,j) = \begin{cases} 0 \; if \; C_1(i,j) = C_2(i,j) \\ 1 \; if \; C_1(i,j) \neq C_2(i,j) \end{cases}. \tag{10}$$

Ще одна міра, UACI, визначається за наступною формулою

$$UACI = \frac{1}{H \times W} \sum_{i,j} \frac{\left| C_1(i,j) - C_2(i,j) \right|}{255} \times 100 \; \%. \tag{11}$$

Результати тестування такими методиками приведені в табл. 5.

Таблиця 5

Значення ефективності шифрування
для трьох складових зображення MSE, PSNR, NPCR та UACI

Складова	MSE	PSNR	NPCR	UACI (%)
Червона	9502,4	8,3524	99,59	31,23
Зелена	7422,2	9,4254	99,61	27,93
Синя	12298,35	7,2323	99,56	35,01

Оскільки запропонований генератор може бути використаний для шифрування будь-яких бітових файлів, тому необхідно здійснити перевірку показників якості шифрування бітових файлів різного розміру і формату. Для цього використаємо файли формату pdf, mp3 та jpeg. Результати оцінки інформаційної ентропії оригінальних та зашифрованих файлів різних форматів представлені в табл. 6.

Таблиця 6

Результати оцінки ефективності шифрування бітової інформації
оригінальних та зашифрованих файлів різних форматів

Тип файлу	Ентропія	Коефіцієнт кореляції	MSE	PSNR	NPCR	UACI (%)
Оригінальний pdf	7,665	0,3814	10505,14	7,9167	99,604	32,825
Зашифрований pdf	7,999	0,0005				
Оригінальний mp3	7,9785	0,2888	10821,22	7,788	99,607	33,308
Зашифрований mp3	7,9999	0,0241				
Оригінальний Jpeg	7,9762	0,6761	10853,202	7,7752	99,604	33,356
Зашифрований Jpeg	7,9999	0,0657				

В процесі розробки методу шифрування на основі синтезованого генератора було здійснено оцінку стійкості методу шифрування бітової інформації на основі двох динамічних систем та операції XOR до атаки грубої сили та визначено швидкість шифрування. Було встановлено, що розмір ключового простору, при використанні ключа розміром 10 символів, складає $C = 256^{10}$ у випадку використання алфавіту $A = 256$ символів з ASCII коду, або $C = 2^{80}$ якщо ключ представляти в бітовому значенні. Далі якщо прийняти, що потужність крипто-аналітичної системи $S = 1000$ паролів/с, то для методу шифрування текстової інформації на основі двох хаотичних динамічних систем час підбору паролю складає $3{,}7 \cdot 10^{14}$ років. Крім того була визначена швидкість шифрування інформації запропонованим методом і вона становить 0,6 Мбіт/с.

Також в другому розділі було вперше запропоновано генератор ПВП бітів на основі двох динамічних систем зі змінним значенням порогового рівня прийняття рішення про значення генерованого біту, проведено моделювання процесу генерації ключа шифрування інформації, досліджено властивості псевдовипадкових послідовностей генерованих послідовностей та здійснено реалізацію методу шифрування інформації на основі запропонованого генератора.

Генератор ПВП бітів побудований на основі двох хаотичних систем. Перша система - це система Лоренца (12), друга – логістичне відображення (1).

$$\begin{aligned} \dot{x} &= -a(x-y) \\ \dot{y} &= cx - y - xz, \\ \dot{z} &= bz + xy \end{aligned} \tag{12}$$

де x, y та z - динамічні змінні, a, b, c - параметри системи Лоренца.

Система Лоренца та логістичне відображення генерують значення змінних, що використовується при формуванні ключа шифрування. В процесі генерування значення змінних системи Лоренца порівнюються із значеннями, генерованими логістичним відображенням. В результаті порівняння значень системи Лоренца та логістичного відображення при умові $h_x, h_y, h_z \geq x_n$ генерується логічна “1”, в іншому випадку – логічний “0”, де h_x, h_y, h_z - приведені до одиничного інтервалу значення змінних системи Лоренца та x_n - значення, генеровані логістичним відображенням. Проводячи таку операцію для всіх трьох змінних системи Лоренца, отримуються три різні бінарні послідовності k_1, k_2, k_3, що за допомогою операції XOR перемішуються між собою, в результаті чого утворюється загальний ключ шифрування.

$$k_1 \oplus k_2 \oplus k_3 = K. \tag{13}$$

Отриманий загальний ключ шифрування за допомогою операції XOR додається до інформаційної послідовності, в результаті чого утворюється зашифрована інформаційна послідовність.

Був проведений аналіз стійкості методу шифрування на основі генератора зі змінним значенням порогового рівня прийняття рішення про значення генерованого біту до атаки грубої сили та встановлено швидкість шифрування. В результаті аналізу було встановлено, що час підбору паролю атакою грубої сили складає $4 \cdot 10^{20}$ років, а швидкість шифрування інформації становила 0,9 Мбіт/с.

Генерована послідовність була протестована набором статистичних тестів NIST STS-2,1,2. В процесі тестування встановлено, що генерована послідовність задовольняє умовам всіх 15-ти тестів. Також було здійснено перевірку показників якості шифрування бітових файлів різного розміру і формату. Для цього використаємо файли формату doc, pdf та mp3. Результати оцінки інформаційної ентропії оригінальних та зашифрованих файлів різних форматів представлені в табл. 7.

Таблиця 7

Результати оцінки ефективності шифрування бітової інформації оригінальних та зашифрованих файлів різних форматів

Тип файлу	Ентропія	Коефіцієнт кореляції	MSE	PSNR	NPCR	UACI (%)
Оригінальний doc	7,8743	0,0687	8056,16	9,0695	98,436	26,981
Зашифрований doc	7,9502	0,0079				
Оригінальний pdf	7,8740	0,0657	7757,68	9,2334	98,4461	26,524
Зашифрований pdf	7,9762	0,0063				
Оригінальний mp3	7,8734	0,0657	7788,49	9,2162	98,488	26,577
Зашифрований mp3	7,9757	0,0063				

У третьому розділі “Метод шифрування текстової інформації із застосуванням двох хаотичних систем” запропоновано метод шифрування, що поєднує динамічну систему Ресслера та кубічне відображення. Система Ресслера (14) генерує початкові умови для кубічного відображення (3), що безпосередньо шифрує текстове повідомлення. При цьому збільшується кількість ключів шифрування з 2-х до 10, що значно підвищує криптостійкість методу шифрування в порівнянні з методом Баптісти та методом шифрування на основі системи Лоренца.

$$\begin{cases} \dot{x} = -y - z \\ \dot{y} = x + py \\ \dot{z} = q + z\left(x - r\right) \end{cases}. \qquad (14)$$

Для рівняння (14) x, y та z - динамічні змінні системи Ресслера, p, q та r - значення статичних параметрів системи.

Процес шифрування відбувається наступним чином. Спочатку, задавши початкові умови системи Ресслера, генеруються початкові умови для кубічного відображення. Далі, задавши параметри контролю кубічного відображення, визначається діапазон вихідних значень кубічного відображення, що розбивається на 256 рівних інтервалів згідно обраного алфавіту та за кожним інтервалом закріплюється символ вибраного алфавіту (ASCII код). Беручи першу, генеровану системою Ресслера початкову умову і підставляючи її в рівняння (3), ітеруємо його до попадання значення кубічного відображення в інтервал, закріплений за символом. Номер ітерації, при якому відбулося потрапляння в інтервал, буде шифром символу вхідного повідомлення.

Розшифрування повідомлення здійснюється аналогічно процесу шифруванню. При цьому замість символів повідомлення беруться номери ітерацій. Номер ітерації - це кількість ітерацій кубічного відображення, що необхідно здійснити для отримання значення і визначення інтервалу, в який воно потрапило. Отримавши інтервал, встановлюється відповідний йому символ вхідного тестового повідомлення.

За допомогою мови програмування Delphi 7 був реалізований запропонований метод шифрування. Для ілюстрації роботи методу було вибране наступне повідомлення: “A first application of chaos for encryption messages using chaos was proposed Baptista”, що складається із 89 символів. В результаті шифрування отримано повідомлення, що складається із 89 груп цифр:

374 231 342 265 467 2 524 1759 115 376 955 229 137 351 772 1395 2699 337 537 2285 449 153 170 209 485 114 415 390 531 426 1156 693 651 127 20 784 154 1340 3326 361 429 891 462 161 716 1083 559 166 1512 415 38 712 145 520 1348 355 44 886 110 13 219 111 1735 751 455 315 665 601 334 76 29 215 813 281 109 623 874 666 23 182 296 448 293 31 517 830 584 775 95.

Також було встановлено, що в процесі роботи методу шифрування текстової інформації однакові символи шифруються різною кількістю ітерацій, що обумовлено використанням різних початкових умов для шифрування кожного окремого символу. Слід зауважити, що різні символи вхідного

повідомлення можуть бути зашифровані однаковою кількістю ітерацій, що затрудняє проведення криптоаналізу повідомлення.

Запропонований метод шифрування був підданий ряду криптографічних атак на основі апроксимації хаотичних орбіт. Атаки були спрямовані на відновлення значень початкової умови, параметрів контролю кубічного відображення, визначення потужності алфавіту та визначення діапазону вихідних значень кубічного відображення. Було встановлено що запропонований метод є стійким до такого роду атак. Криптостійкість обумовлена використанням двох динамічних систем, що призвело до збільшення кількості ключів шифрування. В запропонованому методі шифрування використовується вісім ключів шифрування (x_0, y_0, z_0, p, q, r, a, b).

Під час практичної реалізації шифрування тексту запропонованим методом була здійснена оцінка швидкості шифрування/розшифрування, що при шифруванні складає 60 символів за секунду (480 біт/с), а при розшифруванні – 1600 символів за секунду (12,8 кбіт/с). Оцінка стійкості до атаки грубої сили показала, що час підбору паролю для методу шифрування текстової інформації на основі двох хаотичних динамічних систем складає $3{,}17 \cdot 10^{39}$ років.

У четвертому розділі "Метод шифрування зображення за допомогою генераторів псевдовипадкових чисел на основі одновимірних хаотичних систем" вдосконалено методи шифрування зображень на основі одновимірних відображень, здійснено аналіз захищеності зашифрованого зображення, а також гістограмний та кореляційний аналіз оригінальних та зашифрованих зображень.

Вдосконалений метод побудований на основі накопичувальних відображень сіток із використанням трьох одновимірних відображень, а саме логістичного (1) квадратного (2) та кубічного (3) та не використовує техніку блокового шифрування.

Головна ідея запропонованого методу шифрування зображення полягає в тому, що будь-яке зображення може бути представлено як сітка пікселів, кожен з яких має окремий колір. Колір пікселя, це комбінація трьох компонент: червоної, синьої, зеленої, кожна з яких приймає ціле значення $C = \left(C_r, C_g, C_b\right)$ в межах $0 \div 255$. Таким чином, можна створити три паралельні хаотичні відображення сітки, перетворюючи кожен з цих трьох компонент кольору в відповідне значення змінних відображення, $x_C = \left(x_C^r, x_C^g, x_C^b\right)$, та використати ці значення як початкові умови $x_C = x_0$ для трьох різних одновимірних відображень.

Процес шифрування складових кольору пікселя відбувається однаково, але із використанням різних хаотичних систем. Шифрування червоної складової відбувається із використанням логістичного відображення. Для цього задається значення параметру контролю r та визначається діапазон вихідних значень змінних відображення $x_{\min}$ та $x_{\max}$. Початкова умова визначається шляхом перетворення компонент кольору C кожного пікселя в змінну x_C відповідного відображення в сітці, при цьому використовується наступне перетворення:

$$x_C = x_{\min} + \frac{C\delta x}{255}, \tag{15}$$

де $\delta x = x_{\max} - x_{\min}$.

Процес шифрування зображення відбувається послідовно, починаючи від першого до останнього пікселя. Для шифрування першого пікселя $(i=1)$ в якості початкової умови береться значення складової кольору останнього пікселя x_C^m тобто, $x_0^1 = x_C^m$. Проводимо n ітерацій логістичним відображенням та отримаємо змінну відображення x_n^1, до якої додаємо значення складової кольору пікселя x_C^1 і отримуємо зашифроване значення складової кольору першого пікселя. Сумарне значення використовуються як початкова умова для наступного відображення (пікселя), тобто, $x_0^2 = x_n^1 + x_C^1$.

Повторивши процес шифрування для трьох компонент кольору (червона, зелена, синя), накладаємо три складові одна на одну та отримуємо зашифроване зображення.

Процес розшифрування зображення відбувається у зворотному напрямку по відношенню до процесу шифрування, тобто з останнього пікселя до першого. При цьому в якості початкової умови для розшифрування останнього пікселя береться зашифроване значення передостаннього та ітерується ту ж саму кількість разів, що й в процесі шифрування. Віднявши отримане значення від зашифрованого значення складової кольору останнього пікселя отримаємо розшифроване значення складової пікселя. Процес повторюється для всіх пікселів зашифрованого зображення.

Для відновлення значення складової кольору першого пікселя використовується розшифроване значення складової кольору останнього пікселя m, тобто x_C^m, як початкова умова для розшифрування складової кольору першого пікселя. Ітеруємо необхідну кількість разів та віднімаємо від отриманого значення зашифроване значення першого пікселя.

Захищеність зашифрованого зображення вдосконаленим методом в цілому залежить від значень параметрів контролю одновимірних відображень. Це означає, що з часом даний метод міг бути зламаний методом перебору у випадку використання одного лише логістичного відображення для всіх трьох складових кольору. Саме з цієї причини було введено ще два відображення, що мають різні значення параметрів контролю. Зловмиснику прийдеться перебрати всі можливі комбінації чотирьох параметрів a, b, r, μ щоб підібрати необхідні межі, тобто $x_{\min}$ та $x_{\max}$. Отже, запропоноване нами вдосконалення методу значно підвищило його стійкість.

Також під час роботи методу був проведений аналіз кореляції між сусідніми вертикальними та горизонтальними пікселями. Коефіцієнти кореляцій визначались безпосередньо перед шифруванням та після шифрування і складають 0,976 по горизонталі та 0,960 по вертикалі до шифрування, і 0,044 та 0,006 після шифрування відповідно.

В процесі розроблення методу шифрування на основі накопичувального відображення сіток було здійснено оцінку його стійкості до атаки грубої сили, що складає $3{,}07 \cdot 10^{12}$ років, а також визначено швидкість шифрування, що становить 3,04 Мбіт/с при одному циклі шифрування, а при двох та трьох циклах шифрування 1,45 Мбіт/с та 0,97 Мбіт/с відповідно.

Удосконалення методу шифрування зображення на основі накопичувальних відображень сіток призвело до значного підвищення захищеності. Покращення відбулося за рахунок збільшення кількості ключів шифрування, що є результатом використання трьох одновимірних відображень. Особливістю даного методу є те, що самі пікселі беруть участь у формуванні ключа шифрування, що постійно змінюється в процесі роботи методу. Дана особливість робить метод шифрування придатним для шифрування тільки кольорових зображень. Чим різноманітніша кольорова гама зображень, тим краще проходить процес шифрування.

ВИСНОВКИ

В дисертаційній роботі розв’язано актуальну наукову задачу, присвячену синтезу генераторів ПВП на основі хаотичних систем та удосконалено методи шифрування текстової інформації і зображень. Здійснено комп’ютерне моделювання основних складових методів шифрування, аналіз їх захищеності, практичну реалізацію та дослідження можливості використання в системах передавання інформації. Проведені дослідження дозволили зробити такі основні результати та висновки:

1. Вдосконалено генератор псевдовипадкових послідовностей бітів шляхом використання двох різних одновимірних хаотичних систем, а саме логістичної та кубічної функції відображення, внаслідок чого збільшено кількість ключів шифрування із 4-х до 5-ти, а використання двох різних відображень ускладнює можливість реалізації атак як грубої сили так і інших типів атак.

2. Встановлено, що генеровані псевдовипадкові послідовності бітів є стійкими до атак грубої сили і при використанні пароля довжиною 80 бітів (10 символів коду ASCII) час підбору складає $3{,}7 \cdot 10^{14}$ років, швидкість шифрування – 0,6 Мбіт/с.

3. Запропонований генератор формування псевдовипадкових послідовностей на основі двох нелінійних хаотичних систем, в якому значення хаотичних коливань, генерованих логістичним відображенням, слугують динамічним пороговим рівнем прийняття рішень щодо значення бітів у псевдовипадкових послідовностях, генерованих системою Лоренца. Обсяг ключового простору становить 10^{40}.

4. В результаті дослідження процесу шифруванні інформації з використанням двох хаотичних систем (система Лоренца та логістичне відображення) встановлено, що швидкість шифрування інформації становить 0,9 Мбіт/с, а час підбору паролю атакою грубої сили становить $4 \cdot 10^{20}$ років.

5. Запропоновано метод шифрування текстової інформації на основі двох динамічних систем, що уможливило шифрування кожного символу повідомлення з використанням окремо генерованої початкової умови. Широкий діапазон зміни значень ускладнює підбір використаних в процесі шифрування початкових умов та параметрів систем.

6. Аналіз процесу шифрування текстової інформації запропонованим методом на основі двох хаотичних систем (система Лоренца та кубічне відображення) ускладнює швидке і достовірне розшифрування зашифрованих повідомлень. Встановлено, що час підбору ключа шифрування атакою грубої сили становить $3{,}17 \cdot 10^{39}$ років. Швидкість шифрування зазначеним методом становить 60 символів за секунду. Отриманий результат є наслідком використання детермінованих динамічних систем і ітеративного принципу досягнення необхідного інтервалу значень динамічної змінної кубічного відображення, що закріплений за символом повідомлення згідно обраного алфавіту і значень параметрів контролю.

7. З метою підвищення захищеності зашифрованих зображень запропоновано використання трьох одновимірних відображень для шифрування складових кольору пікселя. Внаслідок цього кількість ключів шифрування збільшилась з 4 до 7, для формування яких використовувались попередньо сформовані пікселі.

8. Встановлено, що час підбору паролю із 7-ми елементів та точності задання 5 знаків після коми становить $3{,}07 \cdot 10^{12}$ років. Швидкість шифрування обумовлена кількістю повторних шифрувань зображень і становить 1,45 Мбіт/с для двох циклів шифрування та 0,97 Мбіт/с для 3-х циклів.

СПИСОК ПУБЛІКАЦІЙ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

1. Гресь О.В. Блочне шифрування інформації з використанням детермінованих хаотичних систем / Гресь О.В., Косован Г.В., Шпатар П.М., Ластівка Г.І. // Науковий вісник Чернівецького університету “Комп’ютерні системи та компоненти”. – 2011, том 2, випуск 3. - С. 85 - 91.

2. Косован Г.В. Моделювання алгоритму генерування ключа шифрування інформації на основі динамічних систем / Косован Г.В., Кушнір М.Я., Політанський Л.Ф. // Східно-Європейський журнал передових технологій. – 2013, 4/9. - С. 39 - 43.

3. Пат.UA 80695 U, МПК H04L 9/24, H03M 7/00 Спосіб шифрування зображення з використанням хаотичного відображення / Політанський Л.Ф. Кушнір М.Я., Косован Г.В.; власник Чернівецький національний університет імені Юрія Федьковича.-u2012 14061; подання заявки 10.12.2012; опубліковано 10.06.2013, Бюл.№11.

4. Косован Г.В. Алгоритм шифрування інформації на основі довх хаотичних динамічних систем для захищених систем зв’язку / Косован Г.В., Кушнір М.Я., Політанський Л.Ф. // Захист інформації. жовтень-грудень 2013,Том 15, випуск 4. – С. 299 - 306.

5. Бобало Ю.Я.Дослідження алгоритму криптографічного захисту зображення на основі багатомірного узагальненого перетворення пекаря / Бобало Ю.Я., Політанський Р.Л., Климаш М.М., Косован Г.В. // Системи обробки інформації : збірник наукових праць. – Х.: Харківський університет Повітряних Сил імені Івана Кожедуба, 2014. – Вип. 7 (123). – С. 178 - 181.

6. Mykola Kushnir Computer modeling of information properties of deterministic chaos / Mykola Kushnir, Sergii Galiuk, Volodymyr Rusyn, Grygorii Kosovan, Dmytro Vovchuk // Proceedings of the 7th Chaotic Modeling and Simulation (CMSIM). 2 - 2015. - 178 – 181 P.

7. Gregorii V. Kosovan Research of Binary Sequences Statistical Properties Generated on Chaotic Mappings / Gregorii V. Kosovan, Ruslan L. Politanskij, Nazar G. Hladun // Eastern European Scientific Journal. Ausgabe 4 – 2015. 6 Pp.

8. Anatolii Semenko Creation of pseudo-random sequences based on chaos for forming of wideband signal / Anatolii Semenko, Nataliya Bokla**,** Nikolai Kushnir, Grygorii Kosovan // Information and Telecommunication Sciences. Volume 9, Number 2. July–December 2017. - 5 - 10 P.

9. Політанський Л.Ф. Система передачі даних на основі теорії динамічного хаосу / Політанський Л.Ф., Шпатар П.М., Гресь О.В., Косован Г.В. // 11-а міжнародна практична конференція CIET-2010. - 24-28 травня 2010. – Україна. - Одеса. - 215 С.

10. Шпатар П.М. Пограмний комплекс для дослідження хаотичних систем / Шпатар П.М., Галюк С.Д., Іванюк П.В., Косован Г.В., Значко Н.І. // 12-а міжнародна практична конференція CIET-2011. – 23-27 травня 2011. - Україна. - Одеса. – 163 С.

11. Кушнір М.Я. Алгоритм шифрування на основі двомірного та одновимірного відображень / Кушнір М.Я., Косован Г.В., Круліковський О.В. // 2-а Всеукраїнська науково-практична конференція “Фізико-технологічні проблеми радіотехнічних пристроїв, засобів телекомунікацій, нано- та мікроелектроніки”. – 25-27 жовтня 2012. - Україна. - Чернівці. – 90 С.

12. Косован Г.В. Захищена база даних з шифруванням інформації на основі хаотичних систем / Косован Г.В., Крояло П.М., Кушнір М.Я. // 3-я Всеукраїнська науково-практична конференція “Фізико-технологічні проблеми радіотехнічних пристроїв, засобів телекомунікацій, нано- та мікроелектроніки”. – 24-26 жовтня 2013. - Україна. - Чернівці. – 87 С.

13. Косован Г.В. Алгоритм шифрування текстової інформації на основі двох динамічних хаотичних систем / Косован Г.В., Крояло П.М., Кушнір М.Я. // Перша міжнародна науково-практична конференція “Проблеми інфокомунікацій. Наука і техніка”. – 9-11 жовтня 2013 р. – Україна. – Харків. - С. 61 - 63.

14. Косован Г.В. Аналіз захищеності методів шифрування зображень на основі одномірних відображень/ Косован Г.В. // П’ята міжнародна науково-технічна конференція “Захист інформації і безпека інформаційних систем” 02 - 03 червня 2016, Львів, Україна. - С. 114 - 115.

15. Anatolii Semenko Forming of wideband signal by means of its modulation with pseudo-random sequence created on the basis of a chaotic determined signal /

Anatolii Semenko, Nataliya Bokla**,** Nikolai Kushnir, Grygorii Kosovan // The Second International Conference on Information and Telecommunication Technologies and Radio Electronics UkrMiCo'2017. - September 11-15 2017. – Odessa. – Ukraine. 444 – 447 P.

16. Anatolii Semenko Features of creating based on chaos pseudo-random sequences / Anatolii Semenko, Nataliya Bokla**,** Nikolai Kushnir, Grygorii Kosovan // Proceedings of the XIV International Conference "Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering" TCSET' 2018. – February 20-24 2018. – Lviv-Slavske. – Ukraine. - 1087 - 1091 P.

АНОТАЦІЯ

Косован Г.В. Синтез генераторів псевдовипадкових послідовностей із нелінійною динамікою для захисту інформації в телекомунікаційних системах. - На правах рукопису.

Дисертація на здобуття наукового ступеня кандидата технічних наук за спеціальністю 05.13.21 - системи захисту інформації. - Одеська Національна академія зв'язку ім. О.С. Попова Міністерства освіти і науки України, Одеса, 2018.

Робота присвячена вирішенню задач присвячених синтезу генераторів ПВП на основі одно та багатовимірних хаотичних систем для удосконалення методів шифрування інформації, аналізу захищеності розроблених методів, їх практичної реалізації та дослідження можливості використання в системах передавання інформації.

В результаті досліджень, що виконані у межах дисертаційної роботи показано, що використання тільки однієї хаотичної системи для генерування ПВП з хорошими статистичними властивостями не дає можливості забезпечити достатнього рівня захищеності методів шифрування інформації, а вирішенням цієї проблеми є використання комбінацій із одно та багатовимірних хаотичних систем для побудови ПВП генераторів із великим періодом повторення і задовольняючими властивостями для шифрування інформації. Зокрема, приведено програмну реалізацію запропонованих генераторів на мові програмування Delphi 7 та показано, що генеровані ними послідовності відповідають вимогам статистичних тестів NIST SP 800-22.

На основі отриманих результатів були побудовані методи шифрування інформації на основі синтезованих генераторів ПВП та операції XOR. Також на основі отриманих результатів статистичних тестів було запропоновано вдосконалення методів шифрування текстової інформації, зображень та бітових файлів. Показано ефективність роботи вдосконалених методів шифрування та їх практичну реалізацію. Встановлено, що використання поєднання декількох хаотичних систем при розробці методів шифрування призводить до збільшення кількості ключів шифрування, зростання ключового простору і таким чином зростанням стійкості до різного роду атак.

Ключові слова: детермінований хаос, хаотична система, синтез, генерування, псевдовипадкова послідовність, метод, шифрування, розшифрування, криптографія, математичне моделювання, стійкість.

АННОТАЦИЯ

Косован Г.В. Синтез генераторов псевдослучайных последовательностей из нелинейной динамикой для защиты информации в телекоммуникационных системах. -- На правах рукописи.

Диссертация на соискание учёной степени кандидата технических наук по специальности 05.13.21 -- системы защиты информации. -- Одесская Национальная академия связи им. О.С. Попова Министерство науки и образования Украины, Одесса, 2018.

Робота направлена на решению важной научно-прикладной задачи связанной с синтезом генераторов ПВП на основаие одно и многомерных хаотических систем, а также усовершенствованию методов шифрования информации на их основе, анализа защищенности разработанных методов, их практической реализации и исследованию возможности их использования в системах защищенной передачи информации.

В результате исследований, проделанных в ходе исполнения данной диссертационной работы показано, что использование лишь одной хаотической системы для генерации ПВП с хорошими статистическими свойствами не дает возможности обеспечить достаточный уровень защиты методов шифрования информации. Решением этой проблемы является использование комбинаций из одно и многомерных хаотических систем для построения ПВП генераторов из большим периодом повторения для шифрования информации. Непосредственно, было произведено программную реализацию предложенных генераторов на языке программирования Delphi 7 и показано, что генерированные ими последовательности полностью соотвецтвуют требованиям статистических тестов NIST SP 800-22.

На основание полученных результатов были построены методы шифрования информации на основе синтезированных генераторов ПВП и операции XOR. Также на основе полученных результатов статистических тестов было предложено усовершенствование методов шифрования текстовой информации, изображений и битовых файлов. Показано эффективность роботы усовершенствованных методов шифрования и их практическую реализацию. Определено, что использование сочетания нескольких хаотических систем при разработке методов шифрования приводит к увеличению количества ключей шифрования, увеличения ключевого пространствия и таким образом к увеличения стойкости к разного рода криптоатакам.

Ключевые слова: детерминированный хаос, хаотическая система, синтез, генерирование, псевдослучайная последовательность, метод, шифрование, дешифрование, криптография, математическое моделирование, стойкость.

ABSTRACT

Kosovan G. V. Synthesis of pseudo-random sequence generators with nonlinear dynamics for protection of information in telecommunication systems. -- Manuscript.

PhD. thesis in Engineering Science, Major Option 05.13.21 -- Information Security Systems. -- O.S. Popov Odessa national academy of telecommunications of the Ministry of Education and Science of Ukraine, Odessa, 2018.

The work is aimed at solving an important scientific and applied problem related to the synthesis of PVP generators based on one and multi-dimensional chaotic systems, the construction of methods for encryption of information based on them, analysis of the resistance of the developed methods, their practical implementation and research of the possibility of their use in systems of secure information transmission.

As a result of the research carried out during the execution of this thesis, it is shown that the use of only one chaotic system for the generation of PVP with good statistical properties does not provide an opportunity to provide a sufficient level of protection of information encryption methods. The solution to this problem is to use combinations of one and multi-dimensional chaotic systems to construct PVP generators with a long repetition period to encrypt information. Directly, the program implementation of the proposed generators in the Delphi 7 programming language was performed and it was shown that the sequences generated by them completely correspond to the requirements of statistical tests NIST SP 800-22.

Based on the obtained results methods of information encryption based on synthesized PVP generators and XOR operations were constructed. Also, based on the results of statistical tests, it was proposed to improve the methods of encryption of textual information, images and bit files. The efficiency of improved encryption methods and their practical implementation is shown. It is determined that the use of a combination of several chaotic systems in the development of encryption methods leads to an increase in the number of encryption keys, increasing the key space, and thus to increasing the resistance to various crypto attacks.

Key words: deterministic chaos, chaotic system, synthesis, generation, pseudorandom sequence, method, encryption, decryption, cryptography, mathematical modeling, stability.

Підписано до друку 26.12.2018 р.
Формат 60/88/16. Обсяг 0,9 др. арк.
Тираж 100 прим. Зам. № 6299.
Віддруковано у редакційно-видавничому відділі ОНАЗ ім. О.С. Попова
м. Одеса, вул. Ковалевського, 5
тел. 70-50-494