ЧЕРКАСЬКИЙ ДЕРЖАВНИЙ ТЕХНОЛОГІЧНИЙ УНІВЕРСИТЕТ

НЕСТЕРЕНКО Оксана Борисівна

УДК 004.421.5:004.056.55

МЕТОДИ ТА ЗАСОБИ СИНТЕЗУ ОПЕРАЦІЙ ПОТОКОВОГО ШИФРУВАННЯ ЗА КРИТЕРІЄМ СТРОГОГО СТІЙКОГО КОДУВАННЯ

05.13.05 – комп’ютерні системи і компоненти

Автореферат

дисертації на здобуття наукового ступеня

кандидата технічних наук

Черкаси – 2019

Дисертацією є рукопис.

Роботу виконано в Черкаському державному технологічному університеті Міністерства освіти і науки України.

Науковий керівник: доктор технічних наук, професор
Рудницький Володимир Миколайович,
Черкаський державний технологічний університет,
завідувач кафедри інформаційної безпеки та
комп'ютерної інженерії.

Офіційні опоненти: доктор технічних наук, професор
Кулик Анатолій Ярославович,
Вінницький національний медичний університет
ім. М. І. Пирогова, завідувач кафедри біофізики,
інформатики та медичної апаратури;

доктор технічних наук, професор
Пархуць Любомир Теодорович,
Національний університет «Львівська політехніка»,
професор кафедри захисту інформації.

Захист відбудеться «27» *червня* 2019 р. о 10^{00} на засіданні спеціалізованої вченої ради К 73.052.04 при Черкаському державному технологічному університеті за адресою: 18006, Черкаси, бульвар Шевченка, 460.

З дисертацією можна ознайомитися в бібліотеці Черкаського державного технологічного університету за адресою: 18006, Черкаси, бульвар Шевченка, 460.

Автореферат розіслано «27» *травня* 2019 р.

Учений секретар
спеціалізованої вченої ради Е. В. Фауре

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Актуальність теми. Проблема захисту інформації завжди була, є і буде актуальною. На сьогоднішній день ця проблема стала принципово важливою для Державної служби України з надзвичайних ситуацій. Особливо велике значення має оперативність, достовірність і конфіденційність інформації для управління підрозділами в кризових ситуаціях, адже від них залежить безпека та життя людей.

За останні десятиліття значно зросла кількість робіт, пов'язаних із криптографією та криптоаналізом, які опубліковані у відкритих наукових виданнях. Накопичений значний теоретичний і практичний потенціал використовується не тільки для побудови, а і для злому криптосистем. Не зважаючи на всі ризики, криптографія на сьогоднішній день залишається найбільш ефективним і поширеним засобом інформації у кіберпросторі. Підтвердженням важливості розвитку криптографії є конкурси на стандарти криптографії, які постійно проводять як у нашій державі, так і в світі.

Важливий внесок у розвиток криптології та захисту інформації внесли такі вітчизняні та зарубіжні науковці, як К. Е. Шеннон, Дж. Л. Мессі, Б. Шнайєр, М. Хеллман, Ч. Г. Беннет, Б. У. Діффі, Р. Меркл, Н. Кобліц, А. Шамір, М. Мауер, І. Чанг, Р. Л. Рівест, Ж. Брассар, І. Д. Горбенко, А. М. Олексійчук, О. В. Гомонай, Р. А. Хаді, В. К. Усенко, В. М. Сидельніков, О. А. Логачов, С. О. Шестаков, А. Н. Фіонов, Б. Я. Рябко, Д. М. Голубчіков, У. Збінден, А. А. Молдовян, Л. В. Ковальчук та ін.

Не зважаючи на це, залишаються невирішеними багато задач, однією з яких є підвищення невизначеності результатів шифрування, особливо в криптосистемах, алгоритми яких використовують псевдовипадкові послідовності. Створення квантових комп'ютерів та стрімке збільшення хмарних сховищ вимагають застосування високошвидкісної потокової комп'ютерної криптографії, яка забезпечить максимальну невизначеність результатів шифрування.

Таким чином, можна констатувати, що тема дисертаційного дослідження «Методи та засоби синтезу операцій потокового шифрування за критерієм строгого стійкого кодування» є актуальною.

Зв'язок роботи з науковими програмами, планами, темами. Дисертаційна робота виконана відповідно до Постанови Президії НАНУ від 20.12.13 №179 «Основні наукові напрями та найважливіші проблеми фундаментальних досліджень у галузі природничих, технічних і гуманітарних наук Національної академії наук України на 2014–2018 рр.», а саме – пп. 1.2.8.1 «Розробка методів та інформаційних технологій розв'язання задач комп'ютерної криптографії та стеганографії»; Постанови Президії НАНУ від 30.01.2019 №30 «Про Основні наукові напрями та найважливіші проблеми фундаментальних досліджень у галузі природничих, технічних, суспільних і гуманітарних наук Національної академії наук України на 2019–2023 роки», а саме – пп. 1.2.8.1 «Розроблення методів та

інформаційних технологій розв'язання задач комп'ютерної криптографії та стеганографії»; 1.2.8.2 «Розроблення методів підвищення продуктивності систем асиметричної криптографії». Результати дисертаційної роботи включені в НДР «Методи та засоби захисту інформації МНС України на основі операцій криптографічного кодування» (ДР № 0112U003579), «Синтез операцій криптографічного перетворення з заданим характеристиками» (ДР№ 0116U008714), в яких автор брав участь як виконавець.

Мета і задачі дослідження. Основною метою дослідження є підвищення невизначеності результатів потокового шифрування за рахунок використання нових операцій криптоперетворення, синтезованих за критерієм строгого стійкого кодування.

Для досягнення поставленої мети сформульовано і вирішено такі задачі:

– розроблення методу синтезу операцій криптографічного перетворення інформації, які забезпечують максимальну невизначеність результатів шифрування;

– розроблення методу синтезу операцій за критерієм строгого стійкого кодування мінімальної складності;

– удосконалення методу синтезу програмних та апаратних засобів комп'ютерної криптографії для забезпечення підвищення невизначеності результатів шифрування.

Об'єкт дослідження – процеси комп'ютерного криптографічного захисту інформації.

Предмет дослідження – дослідження і синтез операцій криптографічного перетворення інформації за критерієм строгого кодування для систем потокового шифрування.

Методи дослідження. У процесі розробки методу синтезу операцій криптографічного перетворення інформації, які забезпечують максимальну невизначеність результатів шифрування, використовувався математичний апарат теорії інформації, теорії алгоритмів, теорії множин, криптографії, математичної логіки, методів дискретної математики, математичної статистики та комп'ютерного моделювання. Для розроблення методу синтезу операцій за критерієм строгого стійкого кодування мінімальної складності використовувались: теорія алгоритмів, теорії графів, криптографія, методи комп'ютерного моделювання, дискретної математики та математичної статистики. Для удосконалення методу синтезу програмних та апаратних засобів комп'ютерної криптографії для забезпечення підвищення невизначеності результатів шифрування використано теорії: інформації, ймовірності, алгоритмів, криптографії із застосуванням методів дискретної математики, комп'ютерного моделювання, обчислювального експерименту та математичної статистики.

Наукова новизна одержаних результатів. У процесі вирішення поставлених задач автором одержано такі результати:

1) вперше розроблено метод синтезу операцій за критерієм строгого стійкого кодування шляхом використання таблиць мінімальних відстаней за Хеммінгом для побудови таблиць істинності дискретних моделей, які забезпечують максимальну невизначеність результатів перетворення та збільшення варіативності криптоалгоритмів;

2) вперше розроблено метод синтезу операцій за критерієм строгого стійкого кодування мінімальної складності на основі використання операцій перестановки і гамування, шляхом встановлених обмежень та залежностей між операціями перетворення і таблицями мінімальних відстаней за Хеммінгом, які забезпечують максимальну невизначеність результатів перетворення при практично мінімальній складності схемотехнічної та програмної реалізації;

3) набули подальшого розвитку методи синтезу програмних і апаратних криптографічних засобів комп'ютерної техніки на основі використання нової групи операцій, побудованих за критерієм строгого стійкого кодування, шляхом застосування методів синтезу моделей операцій з новими властивостями, які забезпечили спрощення процесу синтезу програмних і апаратних криптографічних засобів і дозволили реалізувати синтез аналогічних засобів мінімальної складності без побудови таблиць істинності та мінімізації.

Практичне значення отриманих результатів. Практична цінність роботи полягає в доведенні розроблених методів до моделей, функціональних схем і програмних модулів для реалізації операцій потокового шифрування, які гарантовано забезпечують зміну кожного біта інформації з імовірністю одна друга.

Застосування отриманих моделей в алгоритмах потокового шифрування забезпечує відповідність згенерованих послідовностей вимогам NIST_STS. Крім того, застосування цих послідовностей в імовірнісних моделях на прикладі інтегральної моделі розвитку і припинення пожежі забезпечило підвищення точності моделювання.

Акти впровадження результатів дисертаційного дослідження додатково підкреслюють практичну цінність роботи.

Реалізація. Дисертаційна робота виконувалася відповідно до планів НДР Черкаського інституту пожежної безпеки ім. Героїв Чорнобиля Національного Університету цивільного захисту України та Черкаського державного технологічного університету. Одержані в ній теоретичні й практичні результати використані та впроваджені у таких закладах:

– Черкаський державний технологічний університет на кафедрі інформаційної безпеки та комп'ютерної інженерії – у матеріалах лекційних курсів «Основи криптографічного захисту інформації», «Комп'ютерні методи та засоби захисту інформації». Акт впровадження від 20.06.2017 р.;

– Приватне підприємство «Сенсорна Електроніка» – для забезпечення конкурентоспроможності та переваги над аналогами на ринках електронної техніки в частині пристроїв захисту інформації. Акт впровадження від 20.12.2018 р.

Особистий внесок здобувача. Усі нові результати дисертаційної роботи отримано автором самостійно. У наукових працях, опублікованих у співавторстві, з питань, що стосуються даного дослідження, автору належать: модифікація моделі ковзного шифрування [1], узагальнення результатів дослідження двохрозрядних операцій криптографічного кодування за критерієм строгого лавинного ефекту [2], встановлені закономірності для синтезу двохрозрядних операцій криптографічного кодування, які відповідають критерію ССК [3, 9, 13], технологія побудови вхідних даних для мінімізації моделі операцій які відповідають критерію ССК [4], моделі операцій ССК мінімальної складності [5, 12], моделі операцій, удосконалені та адаптовані для практичного застосування [6], моделі операцій, які відповідають критерію ССК [7, 10, 11], узагальнені моделі багатораундового ССК [14], генерація псевдовипадкових послідовностей із використанням операцій ССК [15, 16]. Результати, опубліковані в [8, 17, 18], отримані одноосібно.

Апробація результатів дисертації. Результати дисертаційної роботи доповідалися й обговорювалися на Другій міжнародній науково-технічній конференції «Проблеми інформатизації» (Черкаси – Тольятті, 2014), «Наукове забезпечення діяльності оперативно-рятувальних підрозділів (теорія та практика)» (Харків, 2014), Третій міжнародній науково-технічній конференції «Проблеми інформатизації» (Черкаси – Баку – Бельсько-Бяла – Полтава, 2015), П'ятій міжнародній науково-практичній конференції «Сучасні напрями розвитку інформаційно-комунікаційних технологій та засобів управління» (Полтава – Баку – Кіровоград, 2015), «Техника и технология. Актуальные научные проблемы. Рассмотрение, решение, практика» (Гданьск / Gdańsk, 2015), Всеукраїнській науково-практичній конференції з міжнародною участю «Надзвичайні ситуації: безпека та захист» (Черкаси, 2015), Пятій міжнародній науково-технічній конференції «Проблеми інформатизації» (Черкаси – Баку – Бельсько-Бяла – Полтава, 2016), Міжнародній науково-практичній конференції молодих учених «Проблеми та перспективи цивільного захисту» (Харків, 2017), Шостій міжнародній науково-технічній конференції «Проблеми інформатизації» (Черкаси – Баку – Бельсько-Бяла – Полтава, 2018).

Публікації. Основні результати дисертаційної роботи викладено в 18 друкованих працях, у тому числі: 7 статтях у наукових журналах і збірниках наукових праць, внесених до списку фахових видань України; 1 одноосібній статті в закордонному науковому виданні 1 колективній монографії; 9 тезах доповідей на міжнародних науково-технічних та науково-практичних конференціях, а також науково-практичних конференціях і семінарах.

Структура і обсяг дисертації. Робота складається зі вступу, чотирьох розділів, висновків, списку використаних джерел, додатків. Загальний обсяг дисертації – 161 сторінка. Основний зміст викладений на 155 сторінках, містить 49 таблиць, 4 рисунки. Список використаних джерел містить 115 найменувань. Робота містить 3 додатки.

ОСНОВНИЙ ЗМІСТ РОБОТИ

У **вступі** обґрунтована актуальність теми, сформульована мета дослідження та визначені задачі для її реалізації, наведені наукова новизна і практичне значення дисертаційної роботи.

Перший розділ присвячено аналізу якості систем криптографічного перетворення інформації. Обґрунтовується актуальність і необхідність проведення аналізу якості криптографічних систем. Проводиться огляд сучасних вимог до криптографічних систем та вибираються вимоги, які доцільно використовувати в даному дисертаційному дослідженні. Для подальшого дослідження проводиться аналіз відомих досліджень стосовно лавинного ефекту, який оцінюється критерієм строгого лавинного ефекту (СЛК). Детально аналізуються властивості лавинного ефекту та критерії їх оцінки. Проводиться огляд наукових досліджень стосовно надійності та безпеки криптографічних систем. Аналізуються підходи до оцінки стійкості криптографічних алгоритмів. Розглядаються атаки на криптоалгоритми, уточнюються особливості атак на асиметричну криптосистему. Розглядаються аспекти і чинники надійності криптосистем. На основі проведеного аналітичного огляду формулюються мета та задачі наукового дослідження.

Другий розділ присвячений дослідженню двохрозрядних операцій криптографічного перетворення інформації за критерієм строгого стійкого криптографічного кодування.

Проведене дослідження двохрозрядних елементарних функцій для криптоперетворення на відповідність СЛК ($\lambda_{слк} = 1/2$) показало, що жодна з елементарних функцій, на основі яких будуються всі 24 операції криптоперетворення, не відповідають вимогам критерію, бо не забезпечують зміну половини бітів інформації на повній множині вхідних даних. Результати дослідження наведено в табл. 1, де k – кількість змін бітів у результатах виконання елементарної функції при зміні вхідної інформації; $f_3(x) = x_1$; $f_5(x) = x_2$; $f_6(x) = x_1 \oplus x_2$; $f_9(x) = x_1 \oplus x_2 \oplus 1$; $f_{10}(x) = x_2 \oplus 1$; $f_{12}(x) = x_1 \oplus 1$.

Оскільки елементарні функції криптоперетворення не відповідають вимогам СЛК, то і всі операції, які будуються з даних елементарних функцій, також не відповідають вимогам даного критерію.

Для оцінки якості операцій криптоперетворення було запропоновано, по аналогії зі СЛК, ввести критерій строгого стійкого кодування (ССК). Криптографічний алгоритм, або операція криптографічного перетворення інформації задовольняє ССК, якщо незалежно від ключової послідовності та вхідної інформації кожний біт вихідної послідовності змінюється відносно вхідної інформації з імовірністю одна друга. Подальші дослідження показали, що лише 4 двохрозрядні операції з 24, які наведені в табл. 2, відповідають ССК.

Таблиця 1

Результати дослідження двохрозрядних елементарних функцій для криптоперетворення на відповідність СЛК

Вхідні дані														Інверсія x_1													
x_1	x_2	$f_3(x)$		$f_5(x)$		$f_6(x)$		$f_9(x)$		$f_{10}(x)$		$f_{12}(x)$		$\bar{x}_1$	x_2	$f_3(x)$		$f_5(x)$		$f_6(x)$		$f_9(x)$		$f_{10}(x)$		$f_{12}(x)$	
0	0	0	–	0	–	0	–	1	–	1	–	1	–	1	0	1	+	0	–	1	+	0	+	1	–	0	–
0	1	0	–	1	–	1	–	0	–	0	–	1	–	1	1	1	+	1	–	0	+	1	+	0	–	0	–
1	0	1	–	0	–	1	–	0	–	1	–	0	–	0	0	0	+	0	–	0	+	1	+	1	–	1	–
1	1	1	–	1	–	0	–	1	–	0	–	0	–	0	1	0	+	1	–	1	+	0	+	0	–	1	–
k		**0**		**0**		**0**		**0**		**0**		**0**		k		**4**		**0**		**4**		**4**		**0**		**0**	
Інверсія x_2														Інверсія x_1 і x_2													
x_1	$\bar{x}_2$	$f_3(x)$		$f_5(x)$		$f_6(x)$		$f_9(x)$		$f_{10}(x)$		$f_{12}(x)$		$\bar{x}_1$	$\bar{x}_2$	$f_3(x)$		$f_5(x)$		$f_6(x)$		$f_9(x)$		$f_{10}(x)$		$f_{12}(x)$	
0	1	0	–	1	+	1	+	0	+	0	–	1	+	1	1	1	+	1	+	0	–	1	–	0	–	0	–
0	0	0	–	0	+	0	+	1	+	1	–	1	+	1	0	1	+	0	+	1	–	0	–	1	–	0	–
1	1	1	–	0	+	0	+	1	+	0	–	0	+	0	1	0	+	1	+	1	–	0	–	0	–	1	–
1	0	1	–	1	+	1	+	0	+	1	–	0	+	0	0	0	+	0	+	0	–	1	–	1	–	1	–
k		**0**		**4**		**4**		**4**		**0**		**4**		k		**4**		**4**		**0**		**0**		**0**		**0**	

Таблиця 2

Таблиці істинності двохрозрядних операцій, які відповідають ССК

Вхідна інформація		Результати перетворення вхідної інформації							
		$F_{3,10}=\begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix}$		$F_{12,5}=\begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix}$		$F_{10,3}=\begin{bmatrix} x_2 \oplus 1 \\ x_1 \end{bmatrix}$		$F_{5,12}=\begin{bmatrix} x_2 \\ x_1 \oplus 1 \end{bmatrix}$	
0	0	0	1	1	0	1	0	0	1
0	1	0	0	1	1	0	0	1	1
1	0	1	1	0	0	1	1	0	0
1	1	1	0	0	1	0	1	1	0

Встановлено, якщо в двохрозрядних операціях інвертується один з переставлених бітів, то перестановка буде «плаваючою», а отже, біт буде інвертуватися і визначатися не тільки інверсією розряду в операції, а й вхідною інформацією. Відзначений факт показує можливість створення потокових шифрів, у яких результат побітового шифрування залежить не тільки від значення бітів гамуючої послідовності, а й від значення бітів інформації, яка шифрується.

В основу подальших досліджень було покладено гіпотезу про те що, при якісному шифруванні немає необхідності виконувати повторне шифрування. Моделі двохраундового застосування операцій, які відповідають вимогам ССК, наведені в табл. 3, а трьохраундового – у табл. 4.

Як видно з табл. 3, жодна з двохраундових моделей не відповідає вимогам критерію. Отримані трьохраундові моделі повністю співпадають з одноразундовими, а отже, при застосуванні трьохраундового шифрування його якість повністю співпадає з якістю одноразундового шифрування. Встановлено,

що при непарній кількості раундів результати шифрування будуть відповідати вимогам ССК, а при парній кількості раундів – не будуть відповідати вимогам.

Таблиця 3

Моделі двохраундового застосування операцій з ССК

Операція першого раунду шифрування	Операція другого раунду шифрування			
	$F_{3,10}(x)=\begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix}$	$F_{12,5}(x)=\begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix}$	$F_{10,3}(x)=\begin{bmatrix} x_2 \oplus 1 \\ x_1 \end{bmatrix}$	$F_{5,12}(x)=\begin{bmatrix} x_2 \\ x_1 \oplus 1 \end{bmatrix}$
$F_{3,10}(x)=\begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix}$	$F_{3,5}(x)=\begin{bmatrix} x_1 \\ x_2 \end{bmatrix}$	$F_{12,10}(x)=\begin{bmatrix} x_1 \oplus 1 \\ x_2 \oplus 1 \end{bmatrix}$	$F_{5,3}(x)=\begin{bmatrix} x_2 \\ x_1 \end{bmatrix}$	$F_{10,12}(x)=\begin{bmatrix} x_2 \oplus 1 \\ x_1 \oplus 1 \end{bmatrix}$
$F_{12,5}(x)=\begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix}$	$F_{12,10}(x)=\begin{bmatrix} x_1 \oplus 1 \\ x_2 \oplus 1 \end{bmatrix}$	$F_{3,5}(x)=\begin{bmatrix} x_1 \\ x_2 \end{bmatrix}$	$F_{10,12}(x)=\begin{bmatrix} x_2 \oplus 1 \\ x_1 \oplus 1 \end{bmatrix}$	$F_{5,3}(x)=\begin{bmatrix} x_2 \\ x_1 \end{bmatrix}$
$F_{5,12}(x)=\begin{bmatrix} x_2 \\ x_1 \oplus 1 \end{bmatrix}$	$F_{5,3}(x)=\begin{bmatrix} x_2 \\ x_1 \end{bmatrix}$	$F_{10,12}(x)=\begin{bmatrix} x_2 \oplus 1 \\ x_1 \oplus 1 \end{bmatrix}$	$F_{3,5}(x)=\begin{bmatrix} x_1 \\ x_2 \end{bmatrix}$	$F_{12,10}(x)=\begin{bmatrix} x_1 \oplus 1 \\ x_2 \oplus 1 \end{bmatrix}$
$F_{10,3}(x)=\begin{bmatrix} x_2 \oplus 1 \\ x_1 \end{bmatrix}$	$F_{10,12}(x)=\begin{bmatrix} x_2 \oplus 1 \\ x_1 \oplus 1 \end{bmatrix}$	$F_{5,3}(x)=\begin{bmatrix} x_2 \\ x_1 \end{bmatrix}$	$F_{12,10}(x)=\begin{bmatrix} x_1 \oplus 1 \\ x_2 \oplus 1 \end{bmatrix}$	$F_{3,5}(x)=\begin{bmatrix} x_1 \\ x_2 \end{bmatrix}$

Таблиця 4

Моделі трьохраундового застосування операцій з ССК

Операція третього раунду шифрування	Модель двохраундового застосування операцій			
	$F_{3,5}(x)=\begin{bmatrix} x_1 \\ x_2 \end{bmatrix}$	$F_{12,10}(x)=\begin{bmatrix} x_1 \oplus 1 \\ x_2 \oplus 1 \end{bmatrix}$	$F_{5,3}(x)=\begin{bmatrix} x_2 \\ x_1 \end{bmatrix}$	$F_{10,12}(x)=\begin{bmatrix} x_2 \oplus 1 \\ x_1 \oplus 1 \end{bmatrix}$
$F_{3,10}(x)=\begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix}$	$F_{3,10}(x)=\begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix}$	$F_{12,5}(x)=\begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix}$	$F_{5,12}(x)=\begin{bmatrix} x_2 \\ x_1 \oplus 1 \end{bmatrix}$	$F_{10,3}(x)=\begin{bmatrix} x_2 \oplus 1 \\ x_1 \end{bmatrix}$
$F_{12,5}(x)=\begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix}$	$F_{12,5}(x)=\begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix}$	$F_{3,10}(x)=\begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix}$	$F_{10,3}(x)=\begin{bmatrix} x_2 \oplus 1 \\ x_1 \end{bmatrix}$	$F_{5,12}(x)=\begin{bmatrix} x_2 \\ x_1 \oplus 1 \end{bmatrix}$
$F_{5,12}(x)=\begin{bmatrix} x_2 \\ x_1 \oplus 1 \end{bmatrix}$	$F_{5,12}(x)=\begin{bmatrix} x_2 \\ x_1 \oplus 1 \end{bmatrix}$	$F_{10,3}(x)=\begin{bmatrix} x_2 \oplus 1 \\ x_1 \end{bmatrix}$	$F_{3,10}(x)=\begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix}$	$F_{12,5}(x)=\begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix}$
$F_{10,3}(x)=\begin{bmatrix} x_2 \oplus 1 \\ x_1 \end{bmatrix}$	$F_{10,3}(x)=\begin{bmatrix} x_2 \oplus 1 \\ x_1 \end{bmatrix}$	$F_{5,12}(x)=\begin{bmatrix} x_2 \\ x_1 \oplus 1 \end{bmatrix}$	$F_{12,5}(x)=\begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix}$	$F_{3,10}(x)=\begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix}$

Для остаточного підтвердження гіпотези про недоцільність багатораундового шифрування необхідно провести дослідження зі збільшенням кількості раундів та розрядності операцій ССК.

Третій розділ присвячено розробці методу синтезу операцій криптографічного перетворення інформації за критерієм строгого стійкого криптографічного кодування.

Визначати операції ССК на основі аналізу таблиць істинності складно, тому що збільшення розрядності операцій приводить до факторіального збільшення задачі перебору.

Запропоновано етапи побудови 4 двохоперандних операцій, які досліджено: будується таблиця відстаней за Хеммінгом; видаляються з таблиці значення

відстаней всі, крім одиниці; замінивши в кожному рядку однакові значення відстаней, що залишилися, значенням рядка, отримаємо проміжну таблицю вибору варіантів підстановки; видаливши зсувом пусті клітинки, отримаємо таблицю вибору варіантів підстановки; послідовним вибором у кожному стовпчику результату шифрування значення першого рядка, не допускаючи повторів, отримаємо варіанти таблиць підстановок операцій ССК. Виконавши мінімізацію таблиць підстановки як таблиць істинності операцій перетворення, отримаємо відомі нам чотири операції, які наведені в табл. 5.

Таблиця 5

Результати синтезу операцій на основа відстаней за Хеммінгом

Варіанти вхідних даних			Варіанти вихідних даних для побудови операцій											
			1			2			3			4		
0	0	0	**1**	0	1	**1**	0	1	**2**	1	0	**2**	1	0
1	0	1	**0**	0	0	**3**	1	1	**0**	0	0	**3**	1	1
2	1	0	**3**	1	1	**0**	0	0	**3**	1	1	**0**	0	0
3	1	1	**2**	1	0	**2**	1	0	**1**	0	1	**1**	0	1
Результати побудови операцій			$F_{3,10}=\begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix}$			$F_{5,12}=\begin{bmatrix} x_2 \\ x_1 \oplus 1 \end{bmatrix}$			$F_{10,3}=\begin{bmatrix} x_2 \oplus 1 \\ x_1 \end{bmatrix}$			$F_{12,5}=\begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix}$		

Побудову чотирьохрозрядних операцій ССК проводимо аналогічно з урахуванням кодової відстані за Хеммінгом, рівної двом. При цьому довільно вибрані варіанти таблиць підстановки та результати їх мінімізації виділені однаковим маркуванням у таблиці варіантів підстановки (табл.6).

Таблиця 6

Вибір варіанта побудови операції, яка відповідає критерію ССК

	Цифри, які шифруються															
	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**
Варіанти побудови	3	2	1	0	1	0	0	1	1	0	0	1	0	1	2	3
	5	4	4	5	2	3	3	2	2	3	3	2	5	4	4	5
	6	7	7	6	7	6	5	4	4	5	6	7	6	7	7	6
	9	8	8	9	8	9	10	11	11	10	9	8	9	8	8	9
	10	11	11	10	13	12	12	13	13	12	12	13	10	11	11	10
	12	13	14	15	14	15	15	14	14	15	15	14	15	14	13	12
Моделі операцій	$F(x)=\begin{bmatrix} x_2 \oplus 1 \\ x_1 \oplus 1 \\ x_1 \oplus x_2 \oplus x_3 \\ x_1 \oplus x_2 \oplus x_4 \end{bmatrix}$				$F(x)=\begin{bmatrix} x_1 \cdot x_2 \vee x_1 \cdot x_3 \vee x_2 \cdot x_4 \\ \bar{x}_1 \cdot \bar{x}_2 \vee x_1 \cdot x_2 \cdot x_4 \vee x_1 \cdot x_3 \cdot \bar{x}_4 \\ \bar{x}_1 \cdot \bar{x}_2 \cdot x_4 \vee \bar{x}_1 \cdot x_2 \cdot x_3 \vee x_1 \cdot x_2 \cdot \bar{x}_3 \vee \\ \vee \bar{x}_1 \cdot x_2 \cdot \bar{x}_4 \vee x_1 \cdot \bar{x}_2 \cdot x_3 \cdot \bar{x}_4 \\ \bar{x}_1 \cdot \bar{x}_3 \cdot x_4 \vee \bar{x}_2 \cdot \bar{x}_3 \cdot \bar{x}_4 \vee \bar{x}_1 \cdot x_2 \cdot x_3 \vee \\ \vee x_1 \cdot x_3 \cdot \bar{x}_4 \end{bmatrix}$							$F(x)=\begin{bmatrix} x_2 \oplus 1 \\ x_1 \\ x_4 \\ x_3 \oplus 1 \end{bmatrix}$			

Узагальнивши отримані результати, було побудовано метод синтезу операцій за критерієм строгого стійкого кодування, алгоритм якого можна представити наступним чином:

1. Визначається розрядність операції криптоперетворення, яка співпадає з кількістю елементарних функцій в операції і є парним числом: $n = 2 \cdot k; \quad k \in N$.
2. Будується таблиця мінімальних кодових відстаней за Хеммінгом $2^n \times 2^n$.
3. Будується таблиця варіантів підстановки кодів перетворення шляхом послідовної реалізації:
   - відкоригованої таблиці відстаней за Хеммінгом, в якій залишені лише відстані за Хеммінгом, рівні k;
   - проміжної таблиці вибору варіантів підстановки, в якій залишені відстані за Хеммінгом, рівні k, замінені номерами рядків, в яких вони знаходяться;
   - таблиці вибору варіантів підстановки щляхом видалення незадіяних комірок.
4. Визначаються значення кодів від 0 до $2^n - 1$ так, щоб не було повторення кодів шляхом послідовної реалізації $M^* = \bigcap_{i=0}^{2^n-1} m_i^* = (m_i \in M_i) \wedge (m_i \notin M_{i-1}^*)$.
5. Перевіряється коректність отриманого варіанта таблиці підстановки, за рахунок виявлення можливих помилок та допущених при побудові таблиці. При програмній реалізації даний пункт дозволяє контролювати як результати побудови таблиці, так і наявність збоїв комп'ютерної техніки.
6. На основі отриманої таблиці підстановок будується таблиця істинності n-розрядної операції крипто перетворення, яка відповідає критерію ССК:
7. На основі таблиці істинності мінімізується n-розрядна математична модель операції крипто перетворення, яка відповідає критерію ССК.

Дослідження результатів криптографічного перетворення при збільшенні кількості раундів та розрядності операцій ССК підтвердили гіпотезу і показали, що виконання декількох раундів шифрування не приводить до підвищення невизначеності результатів криптоперетворення.

Четвертий розділ присвячено розробці методу синтезу операцій криптографічного перетворення інформації та оцінці можливості застосування синтезованих операцій у потоковому шифруванні.

В процесі аналізу синтезованих і досліджених моделей операцій, які відповідають ССК, було відмічено, що складність моделей відрізняється, а моделі операцій, які мають найменшу складність, складаються лише з перестановок і інверсій. Узявши це припущення за основу моделювання операцій, було отримано 42 чотирьохрозрядні операції. Результати моделювання, а також класифікація отриманих операцій наведені у табл.7.

На основі отриманих результатів було сформульовано метод синтезу операцій криптографічного перетворення інформації мінімальної складності за критерієм ССК. Сутність цього методу полягає в наступному: синтез операцій,

які задовольняють критерію ССК і мають мінімальну складність, проводиться на основі парних перестановок та інверсії шляхом інверсії половини бітів, за умови однієї інверсії в кожній парній перестановці.

Таблиця 7

Результати моделювання

Перестановки відсутні, інвертована половина біт					
$F_1=\begin{bmatrix}x_1\oplus1\\x_2\oplus1\\x_3\\x_4\end{bmatrix}$	$F_2=\begin{bmatrix}x_1\oplus1\\x_2\\x_3\oplus1\\x_4\end{bmatrix}$	$F_3=\begin{bmatrix}x_1\oplus1\\x_2\\x_3\\x_4\oplus1\end{bmatrix}$	$F_4=\begin{bmatrix}x_1\\x_2\oplus1\\x_3\oplus1\\x_4\end{bmatrix}$	$F_5=\begin{bmatrix}x_1\\x_2\oplus1\\x_3\\x_4\oplus1\end{bmatrix}$	$F_6=\begin{bmatrix}x_1\\x_2\\x_3\oplus1\\x_4\oplus1\end{bmatrix}$
Одна парна перестановка, інвертовано один з переставлених бітів і один не переставлений					
$F_7=\begin{bmatrix}x_1\oplus1\\x_4\oplus1\\x_3\\x_2\end{bmatrix}$	$F_8=\begin{bmatrix}x_1\oplus1\\x_4\\x_3\\x_2\oplus1\end{bmatrix}$	$F_9=\begin{bmatrix}x_1\\x_4\oplus1\\x_3\oplus1\\x_2\end{bmatrix}$	$F_{10}=\begin{bmatrix}x_1\\x_4\\x_3\oplus1\\x_2\oplus1\end{bmatrix}$	$F_{11}=\begin{bmatrix}x_1\oplus1\\x_2\\x_4\oplus1\\x_3\end{bmatrix}$	$F_{12}=\begin{bmatrix}x_1\oplus1\\x_2\\x_4\\x_3\oplus1\end{bmatrix}$	$F_{13}=\begin{bmatrix}x_1\\x_2\oplus1\\x_4\oplus1\\x_3\end{bmatrix}$	$F_{14}=\begin{bmatrix}x_1\\x_2\oplus1\\x_4\\x_3\oplus1\end{bmatrix}$
$F_{15}=\begin{bmatrix}x_1\oplus1\\x_3\oplus1\\x_2\\x_4\end{bmatrix}$	$F_{16}=\begin{bmatrix}x_1\oplus1\\x_3\\x_2\oplus1\\x_4\end{bmatrix}$	$F_{17}=\begin{bmatrix}x_1\\x_3\oplus1\\x_2\\x_4\oplus1\end{bmatrix}$	$F_{18}=\begin{bmatrix}x_1\\x_3\\x_2\oplus1\\x_4\oplus1\end{bmatrix}$	$F_{19}=\begin{bmatrix}x_2\oplus1\\x_1\\x_3\oplus1\\x_4\end{bmatrix}$	$F_{20}=\begin{bmatrix}x_2\oplus1\\x_1\\x_3\\x_4\oplus1\end{bmatrix}$	$F_{21}=\begin{bmatrix}x_2\\x_1\oplus1\\x_3\oplus1\\x_4\end{bmatrix}$	$F_{22}=\begin{bmatrix}x_2\\x_1\oplus1\\x_3\\x_4\oplus1\end{bmatrix}$
$F_{23}=\begin{bmatrix}x_3\oplus1\\x_2\oplus1\\x_1\\x_4\end{bmatrix}$	$F_{24}=\begin{bmatrix}x_3\oplus1\\x_2\\x_1\\x_4\oplus1\end{bmatrix}$	$F_{25}=\begin{bmatrix}x_3\\x_2\oplus1\\x_1\oplus1\\x_4\end{bmatrix}$	$F_{26}=\begin{bmatrix}x_3\\x_2\\x_1\oplus1\\x_4\oplus1\end{bmatrix}$	$F_{27}=\begin{bmatrix}x_4\oplus1\\x_2\oplus1\\x_3\\x_1\end{bmatrix}$	$F_{28}=\begin{bmatrix}x_4\oplus1\\x_2\\x_3\oplus1\\x_1\end{bmatrix}$	$F_{29}=\begin{bmatrix}x_4\\x_2\oplus1\\x_3\\x_1\oplus1\end{bmatrix}$	$F_{30}=\begin{bmatrix}x_4\\x_2\\x_3\oplus1\\x_1\oplus1\end{bmatrix}$
Дві парні перестановки, інвертовано по одному біту в кожній перестановці					
$F_{31}=\begin{bmatrix}x_2\oplus1\\x_1\\x_4\oplus1\\x_3\end{bmatrix}$	$F_{32}=\begin{bmatrix}x_2\oplus1\\x_1\\x_4\\x_3\oplus1\end{bmatrix}$	$F_{33}=\begin{bmatrix}x_2\\x_1\oplus1\\x_4\oplus1\\x_3\end{bmatrix}$	$F_{34}=\begin{bmatrix}x_2\\x_1\oplus1\\x_4\\x_3\oplus1\end{bmatrix}$	$F_{35}=\begin{bmatrix}x_3\oplus1\\x_4\oplus1\\x_1\\x_2\end{bmatrix}$	$F_{36}=\begin{bmatrix}x_3\oplus1\\x_4\\x_1\\x_2\oplus1\end{bmatrix}$
$F_{37}=\begin{bmatrix}x_3\\x_4\oplus1\\x_1\oplus1\\x_2\end{bmatrix}$	$F_{38}=\begin{bmatrix}x_3\\x_4\\x_1\oplus1\\x_2\oplus1\end{bmatrix}$	$F_{39}=\begin{bmatrix}x_4\oplus1\\x_3\oplus1\\x_2\\x_1\end{bmatrix}$	$F_{40}=\begin{bmatrix}x_4\oplus1\\x_3\\x_2\oplus1\\x_1\end{bmatrix}$	$F_{41}=\begin{bmatrix}x_4\\x_3\oplus1\\x_2\\x_1\oplus1\end{bmatrix}$	$F_{42}=\begin{bmatrix}x_4\\x_3\\x_2\oplus1\\x_1\oplus1\end{bmatrix}$

Даний метод дозволяє синтезувати моделі операцій парної розрядності, які відповідають вимогам ССК, наприклад:

$$F=\begin{bmatrix}x_2\\x_1\oplus1\end{bmatrix};\ F=\begin{bmatrix}x_1\oplus1\\x_2\oplus1\\x_3\\x_4\end{bmatrix};\ F=\begin{bmatrix}x_4\oplus1\\x_2\\x_3\oplus1\\x_1\end{bmatrix};\ F=\begin{bmatrix}x_1\\x_2\oplus1\\x_3\\x_5\oplus1\\x_4\\x_6\oplus1\end{bmatrix};\ F=\begin{bmatrix}x_3\\x_7\oplus1\\x_1\oplus1\\x_4\\x_5\oplus1\\x_8\oplus1\\x_2\\x_6\end{bmatrix}.$$

Як видно з наведених прикладів, дані моделі мають дійсно незначну, майже мінімальну складність.

Для вирішення третьої наукової задачі були запропоновано використовувати синтезовані операції потокового шифрування, а саме – в блоці шифрування.

Удосконалення методів синтезу програмно-апаратних засобів комп'ютерної криптографії полягає в побудові операцій криптоперетворення мінімальної складності без виконання етапів синтезу таблиць істинності та етапу мінімізації логічних функцій.

Проте для ефективного застосування в потокових шифрах синтезовані операції повинні одночасно обробляти два операнди, один з яких – інформація, другий – псевдовипадкова послідовність.

Варіанти поєднання синтезованих одноопераднних операцій в двохоперандні наведено на прикладах:

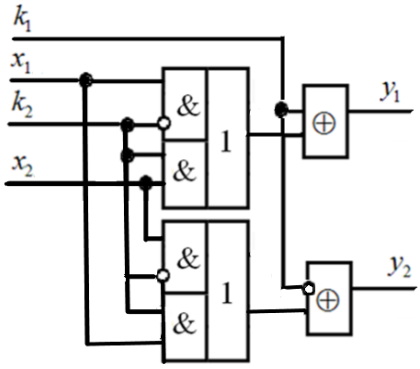
$$O=\begin{cases}\begin{bmatrix}x_1\\ x_2\oplus 1\end{bmatrix}, & якщо\ k_1=0;\ k_2=0\\ \begin{bmatrix}x_1\oplus 1\\ x_2\end{bmatrix}, & якщо\ k_1=0;\ k_2=1\\ \begin{bmatrix}x_2\\ x_1\oplus 1\end{bmatrix}, & якщо\ k_1=1;\ k_2=0\\ \begin{bmatrix}x_2\oplus 1\\ x_1\end{bmatrix}, & якщо\ k_1=1;\ k_2=1\end{cases};$$

$$O=\begin{cases}\begin{bmatrix}x_1\oplus 1\\ x_2\\ x_4\oplus 1\\ x_3\end{bmatrix}, & якщо\ k_1=0;\ k_2=0\\ \begin{bmatrix}x_1\oplus 1\\ x_2\\ x_4\\ x_3\oplus 1\end{bmatrix}, & якщо\ k_1=0;\ k_2=1\\ \begin{bmatrix}x_1\\ x_2\oplus 1\\ x_4\oplus 1\\ x_3\end{bmatrix}, & якщо\ k_1=1;\ k_2=0\\ \begin{bmatrix}x_1\\ x_2\oplus 1\\ x_4\\ x_3\oplus 1\end{bmatrix}, & якщо\ k_1=1;\ k_2=1\end{cases}$$

У табл. 8 і 9 наведені варіанти функціональних схем пристроїв реалізації групи двохрозрядних операцій двохоперандних операцій для апаратної реалізації у спеціалізованих комп'ютерних системах.

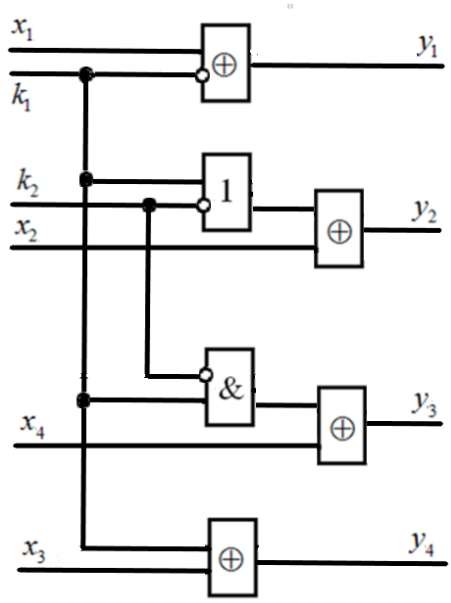
Таблиця 8

Функціональна схема пристрою реалізації групи двохрозрядних двохоперандних операцій, синтезованих за критерієм ССК

Функціональна схема	Операція перетворення першого аргументу	Значення другого аргументу
	$F_{3,10}(x)=\begin{bmatrix}x_1\\ x_2\oplus 1\end{bmatrix}$	$k_1=0;\ \ k_2=0$
	$F_{12,5}(x)=\begin{bmatrix}x_1\oplus 1\\ x_2\end{bmatrix}$	$k_1=0;\ \ k_2=1$
	$F_{5,12}(x)=\begin{bmatrix}x_2\\ x_1\oplus 1\end{bmatrix}$	$k_1=1;\ \ k_2=0$
	$F_{10,3}(x)=\begin{bmatrix}x_2\oplus 1\\ x_1\end{bmatrix}$	$k_1=1;\ \ k_2=1$

Таблиця 9

Функціональна схема пристрою реалізації групи чотирьохрозрядних двохоперандних операцій, синтезованих за критерієм ССК

Функціональна схема	Операція перетворення першого аргументу	Значення другого аргументу
	$F=\begin{bmatrix} x_1\oplus 1 \\ x_2 \\ x_4\oplus 1 \\ x_3 \end{bmatrix}$	$k_1=0;\quad k_2=0$
	$F=\begin{bmatrix} x_1\oplus 1 \\ x_2 \\ x_4 \\ x_3\oplus 1 \end{bmatrix}$	$k_1=0;\quad k_2=1$
	$F=\begin{bmatrix} x_1 \\ x_2\oplus 1 \\ x_4\oplus 1 \\ x_3 \end{bmatrix}$	$k_1=1;\quad k_2=0$
	$F=\begin{bmatrix} x_1 \\ x_2\oplus 1 \\ x_4 \\ x_3\oplus 1 \end{bmatrix}$	$k_1=1;\quad k_2=1$

Для забезпечення роботи систем комп'ютерного криптографічного захисту на основі персональних універсальних комп'ютерів необхідна програмна реалізація операцій. Для цього необхідно провести вдосконалення моделей двохоперандних операції ССК.

Вдосконалення моделі проведемо на прикладі операції, яка реалізована функціональною схемою, представленою у табл. 8. Для цього, виділивши з операції базову частину і частину інверсій, на основі виразу $O=O^{*}\oplus\overline{O}$ отримаємо:

$$O=\begin{cases}\begin{bmatrix} x_1 \\ x_2\oplus 1 \end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0 \\ \begin{bmatrix} x_1\oplus 1 \\ x_2 \end{bmatrix}, \text{якщо } k_1=0;\ k_2=1 \\ \begin{bmatrix} x_2 \\ x_1\oplus 1 \end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0 \\ \begin{bmatrix} x_2\oplus 1 \\ x_1 \end{bmatrix}, \text{ якщо } k_1=1;\ k_2=1 \end{cases} = \begin{cases}\begin{bmatrix} x_1 \\ x_2 \end{bmatrix}\oplus\begin{bmatrix} 0 \\ 1 \end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0 \\ \begin{bmatrix} x_1 \\ x_2 \end{bmatrix}\oplus\begin{bmatrix} 1 \\ 0 \end{bmatrix}, \text{якщо } k_1=0;\ k_2=1 \\ \begin{bmatrix} x_2 \\ x_1 \end{bmatrix}\oplus\begin{bmatrix} 0 \\ 1 \end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0 \\ \begin{bmatrix} x_2 \\ x_1 \end{bmatrix}\oplus\begin{bmatrix} 1 \\ 0 \end{bmatrix}, \text{ якщо } k_1=1;\ k_2=1 \end{cases}.$$

Вдосконалені моделі базової частини і частина інверсій будуть представлені так:

$$O^* = \begin{cases} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix}, \text{ якщо } k_1 = 0;\ k_2 = 0 \\ \begin{bmatrix} x_1 \\ x_2 \end{bmatrix}, \text{якщо } k_1 = 0;\ k_2 = 1 \\ \begin{bmatrix} x_2 \\ x_1 \end{bmatrix}, \text{ якщо } k_1 = 1;\ k_2 = 0 \\ \begin{bmatrix} x_2 \\ x_1 \end{bmatrix}, \text{якщо } k_1 = 1;\ k_2 = 1 \end{cases} = \begin{bmatrix} x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \\ x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \end{bmatrix}; \ \overline{O} = \begin{cases} \begin{bmatrix} 0 \\ 1 \end{bmatrix}, \text{ якщо } k_1 = 0;\ k_2 = 0 \\ \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \text{якщо } k_1 = 0;\ k_2 = 1 \\ \begin{bmatrix} 0 \\ 1 \end{bmatrix}, \text{ якщо } k_1 = 1;\ k_2 = 0 \\ \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \text{якщо } k_1 = 1;\ k_2 = 1 \end{cases} = \begin{bmatrix} k_2 \\ \bar{k}_2 \end{bmatrix}.$$

Виходячи з цього, вдосконалену модель двохрозрядної двохоперандної операції ССК можна представити наступним чином:

$$O = \begin{bmatrix} x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \\ x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \end{bmatrix} \oplus \begin{bmatrix} k_2 \\ \bar{k}_2 \end{bmatrix} = \begin{bmatrix} x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \oplus k_2 \\ x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \oplus \bar{k}_2 \end{bmatrix} = \begin{bmatrix} x_1 \cdot \bar{y}_1 \oplus x_2 \cdot y_1 \oplus y_2 \\ x_1 \cdot y_1 \oplus x_2 \cdot \bar{y}_1 \oplus \bar{y}_2 \end{bmatrix}.$$

Вдосконалення моделі операції значно спрощує її застосування як на програмному, так і апаратному рівнях.

Застосування отриманих моделей в алгоритмах потокового шифрування забезпечує відповідність згенерованих послідовностей вимогам NIST_STS, крім того, застосування даних послідовностей в імовірнісних моделях, на прикладі інтегральної моделі розвитку і припинення пожежі, забезпечило підвищення точності моделювання.

У **додатках** наведено акти впровадження результатів дисертаційної роботи, результати обчислювального експерименту та обов'язковий додаток.

ВИСНОВКИ

У дисертаційній роботі вирішено важливу науково-технічну задачу підвищення невизначеності результатів потокового шифрування за рахунок використання нових операцій криптоперетворення, синтезованих за критерієм строгого стійкого кодування:

1) вперше розроблено метод синтезу операцій за критерієм строгого стійкого кодування шляхом використання таблиць мінімальних відстаней за Хеммінгом, для послідовного перетворення її в проміжну таблицю вибору варіантів підстановки та таблицю вибору варіантів підстановки для побудови таблиць істинності дискретних моделей, які забезпечують максимальну невизначеність результатів перетворення та збільшення варіативності криптоалгоритмів;

2) вперше розроблено метод синтезу операцій за критерієм строгого стійкого кодування мінімальної складності на основі узагальнення теоретичних і

експериментальних досліджень, які забезпечили можливість використання лише операцій перестановки і гамування, шляхом встановлених обмежень та залежностей між операціями перетворення і таблицями мінімальних відстаней за Хеммінгом, які забезпечують максимальну невизначеність результатів перетворення при практично мінімальній складності схемотехнічної та програмної реалізації;

3) набули подальшого розвитку методи синтезу програмних і апаратних криптографічних засобів комп'ютерної техніки на основі використання нової групи операцій, побудованих за критерієм строгого стійкого кодування шляхом застосування методів синтезу моделей операцій із новими властивостями, які забезпечили спрощення синтезу програмних і апаратних криптографічних засобів. Синтез моделей операцій за критерієм строгого стійкого кодування мінімальної складності реалізовано без побудови таблиць істинності та етапу мінімізації булевих функцій, що значно спрощує побудову спеціалізованих програмно-апаратних засобів. Засоби, які синтезуються, забезпечують підвищення ефективності криптографічних алгоритмів шляхом розширення множини операцій для їх побудови, а також забезпечують максимальну невизначеність результатів шифрування на основі гарантованої зміни кожного біта інформації з імовірністю одна друга;

4) практична цінність роботи полягає в доведенні розроблених методів до моделей, функціональних схем і програмних модулів для реалізації операцій потокового шифрування, синтезованих за критерієм строгого стійкого кодування. Основний практичний результаті роботи полягає в побудові операцій потокового шифрування, які гарантовано забезпечують зміну кожного біта інформації з ймовірністю одна друга, забезпечують максимальну невизначеність результатів шифрування.

Застосування отриманих моделей в алгоритмах потокового шифрування забезпечує відповідність згенерованих послідовностей вимогам NIST_STS, крім того, застосування даних послідовностей в імовірнісних моделях, на прикладі інтегральної моделі розвитку і припинення пожежі, забезпечило підвищення точності моделювання.

Результати роботи впроваджено в приватному підприємстві «Сенсорна Електроніка», а також – у навчальний процес Черкаського державного технологічного університету.

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

1. Бабенко В. Г., Мельник О. Г., Нестеренко О. Б. Моделювання примітивів ковзного шифрування на основі рекурентних послідовностей. *Наука і техніка Повітряних Сил Збройних Сил України*. Харків: ХУПС ім. І. Кожедуба, 2015. С. 129–134.

2. Рудницький В. М., Шувалова Л. А., Нестеренко О. Б. Аналіз дворозрядних операцій криптографічного кодування за критерієм строгого лавинного ефекту. *Наукові праці:* наук.-метод. журн. Чорномор. держ. ун-ту ім. Петра Могили. Миколаїв, 2017.

3. Рудницький В. М., Шувалова Л. А., Нестеренко О. Б. Синтез операцій криптографічного перетворення за критерієм строгого стійкого кодування. *Вісник інженерної академії України:* часопис. Київ, 2016. Вип. 3. С. 105–108.

4. Рудницький В. М., Шувалова Л. А., Нестеренко О. Б. Метод синтезу операцій криптографічного перетворення за критерієм строгого стійкого кодування. *Вісник Черкаського державного технологічного університету. Серія: Технічні науки.* 2017. Вип. 1. С. 5–10.

5. Рудницький В. М., Шувалова Л. А., Нестеренко О. Б. Побудова примітивів строгого стійкого кодування мінімальної складності. *Вісник Черкаського державного технологічного університету. Серія: Технічні науки.* 2018. Вип. 1. С. 21–26.

6. Рудницький В. М., Лада Н. В., Федотова-Півень І. М., Пустовіт М. О., Нестеренко О. Б. Побудова двохрозрядних двохоперандних операцій строгого стійкого криптографічного кодування. *Системи управління, навігації та зв'язку:* зб. наук. праць ПНТУ ім. Юрія Кондратюка. 2018. Вип. 6 (52). С. 113–115.

7. Бабенко В. Г., Зажома В. М., Нестеренко О. Б. Метод вбудовування стегоповідомлення на основі ключового елементу. *Автоматизированные системы управления и приборы автоматики*. Харків, 2014. Вип. 168. С. 53–58.

8. Нестеренко О. Б. Исследование двухразрядных операций, удовлетворяющих критерию строгого стойкого кодирования, при многораундовом криптографическом преобразовании. *Wschodnioeuropejskie Czasopismo Naukowe* (East European sci. journal). 2018. No. 11 (39), part 2. С. 20–28. (Варшава, Польща).

9. Криптографічне кодування: обробка та захист інформації: кол. монографія / під ред. В. М. Рудницького. Харків: ДІСА ПЛЮС, 2018. 139 с.

10. Бабенко В. Г., Нестеренко О. Б., Рудницький С. В. Способи синтезу алгоритмів на основі операцій криптографічного перетворення інформації. *Проблеми інформатизації*: тези доп. Другої міжнар. наук.-техн. конф. (Черкаси – Тольятті, 25–26 листоп. 2014 р.). Черкаси: ЧДТУ; Тольятті: ТДУ, 2014. С. 10.

11. Зажома В. М., Нестеренко О. Б. Генерація псевдовипадкових послідовностей на основі фільтрації матричних операцій криптоперетворення. *Проблеми інформатизації:* тези доп. Третьої міжнар. наук.-техн. конф. (Черкаси – Баку – Бельсько-Бяла – Полтава). Черкаси: ЧДТУ; Баку: ВА ЗС АР; Бельсько-Бяла: УТіГН; Полтава: ПНТУ, 2015. 84 с.

12. Зажома В. М., Нестеренко О. Б. Вдосконалений метод вбудовування стегоповідомлення на основі ключового елементу. *Сучасні напрями розвитку інформаційно-комунікаційних технологій та засобів управління:* матеріали П'ятої

міжнар. наук.-техн. конф. (Полтава – Баку – Кіровоград – Харків). Полтава: ПНТУ; Баку: ВА ЗС АР; Кіровоград: КЛА НАУ; Харків: ДП «ХНДІ ТМ», 2015. 72 с.

13. Шувалова Л. А., Нестеренко О. Б. Синтез та аналіз криптографічних операцій за критерієм строгого стійкого кодування. *Проблеми інформатизації*: тези доп. Четвертої міжнар. наук.-техн. конф. (Черкаси – Баку – Бельсько-Бяла – Полтава, 3–4 листоп. 2016 р.). Черкаси: ЧДТУ; Баку: ВА ЗС АР; Бельсько-Бяла: УТіГН; Полтава: ПНТУ. С. 97.

14. Бабенко В. Г., Нестеренко О. Б., Пустовіт М. О. Дослідження результатів багатораундового шифрування, реалізованого на основі операцій строгого стійкого кодування . *Проблеми інформатизації:* тези доп. Шостої міжнар. наук.-техн. конф. (Черкаси – Баку – Бельсько-Бяла – Полтава, 14–16 листоп. 2018 р.). Черкаси: ЧДТУ; Баку: ВА ЗС АР; Бельсько-Бяла: УТіГН; Полтава: ПНТУ, 2018. С. 9–10.

15. Пустовіт М. О., Нестеренко О. Б., Матяш П. В. Моделювання розпилених водяних струменів для комп'ютеризованих симуляторів з гасіння пожеж в будівлях. Техника и технология. *Актуальные научные проблемы. Рассмотрение, решение, практика.* Гданьск, 2015. С. 22.

16. Пустовіт М. О., Нестеренко О. Б., Жаврук П. С. Комп'ютерне моделювання розпорошених водяних струменів для симулятора припинення горіння. *Надзвичайні ситуації: безпека та захист:* матеріали всеукр. наук.-практ. конф. з міжнар. участю. Черкаси: ЧІПБ ім. Героїв Чорнобиля НУЦЗ України, 2015. С. 311–314.

17. Нестеренко О. Б. Двораундове криптографічне кодування операціями зі строгим лавинним ефектом. *Проблеми та перспективи цивільного захисту:* матеріали міжнар. наук.-практ. конф. молодих учених (29–30 берез. 2017 р.). Харків: НУЦЗУ. С. 384.

18. Нестеренко О. Б. Вдосконалення систем моніторингу з надзвичайних ситуацій. *Наукове забезпечення діяльності оперативно-рятувальних підрозділів (теорія та практика).* Харків, 2014. С. 55.

АНОТАЦІЯ

Нестеренко О.Б. Методи та засоби синтезу операцій потокового шифрування за критерієм строгого стійкого кодування. – Рукопис.

Дисертація на здобуття наукового ступеня кандидата технічних наук за спеціальністю 05.13.05 – комп'ютерні системи і компоненти. – Черкаський державний технологічний університет, Черкаси, 2019.

Дисертаційна робота присвячена підвищенню невизначеності результатів потокового шифрування за рахунок використання нових операцій криптоперетворення й синтезованих за критерієм строгого стійкого кодування.

Для цього вперше розроблено метод синтезу операцій за критерієм строгого стійкого кодування шляхом використання таблиць мінімальних відстаней за Хеммінгом, які забезпечують максимальну невизначеність результатів

перетворення та збільшення варіативності криптоалгоритмів; розроблено метод синтезу операцій за критерієм строгого стійкого кодування мінімальної складності, на основі використання операцій перестановки і гамування, шляхом встановлених обмежень та залежностей між операціями перетворення і таблицями мінімальних відстаней за Хеммінгом, які забезпечують максимальну невизначеність результатів перетворення при мінімальній складність схемо технічної та програмної реалізації. Набули подальшого розвитку методи синтезу програмних і апаратних криптографічних засобів комп'ютерної техніки на основі використання нової групи операцій, побудованих за критерієм строгого стійкого кодування, шляхом застосування методів синтезу моделей операцій із новими властивостями, які забезпечили спрощення синтезу, а синтез моделей операцій за критерієм строгого стійкого кодування мінімальної складності реалізовано без побудови таблиць істинності їх мінімізації.

Ключові слова: захист комп'ютерної інформації, потокові шифри, операції криптографічного перетворення, синтез операцій, складність, стійкість, надійність.

АННОТАЦИЯ

Нестеренко О. Б. Методы и средства синтеза операций потокового шифрования по критерию строгого устойчивого кодирования. – Рукопись.

Диссертация на соискание ученой степени кандидата технических наук по специальности 05.13.05 – компьютерные системы и компоненты. – Черкасский государственный технологический университет, Черкассы, 2019.

Диссертационная работа посвящена повышению неопределенности результатов потокового шифрования за счет использования новых операций криптопреобразования, синтезированных по критерию строгого устойчивого кодирования.

Первый раздел посвящен анализу качества систем криптографического преобразования информации. На основе проведенного аналитического обзора современного состояния и тенденций развития компьютерной криптографии формулируются цель и задачи научного исследования. Второй раздел посвящен исследованию двухразрядных операций криптографического преобразования информации по критерию строгого устойчивого криптографической кодирования. Данный критерий предложено использовать для оценки качества операций криптопреобразования взамен строгого лавинного эффекта. Третий раздел посвящен разработке метода синтеза операций криптографического преобразования информации по критерию строгого устойчивого криптографической кодирования. Четвертый раздел посвящен разработке метода синтеза операций криптографического преобразования информации и оценке возможности применения синтезированных операций в потоковом шифровании.

В работе впервые разработан метод синтеза операций по критерию строгого устойчивого кодирования путем использования таблиц минимальных расстояний

по Хеммингу для построения таблиц истинности дискретных моделей, которые обеспечивают максимальную неопределенность результатов преобразования и увеличение вариативности криптоалгоритмов. Впервые разработан метод синтеза операций по критерию строгого устойчивого кодирования минимальной сложности на основе использования операций перестановки и смирения, путем установленных ограничений и зависимостей между операциями преобразования и таблицами минимальных расстояний по Хеммингу, которые обеспечивают максимальную неопределенность результатов преобразования при практически минимальной сложности схемотехнической и программной реализации. Получили дальнейшее развитие методы синтеза программных и аппаратных криптографических средств компьютерной техники на основе использования новой группы операций, построенных по критерию строгого устойчивого кодирования, путем применения методов синтеза моделей операций с новыми свойствами, которые обеспечили упрощение синтеза, а синтез моделей операций по критерию строгого устойчивого кодирования минимальной сложности реализован без построения таблиц истинности их минимизации.

Практическая ценность работы состоит в доведении соискателем полученных научных результатов до конкретных алгоритмов, моделей и вариантов функциональных схем специализированных дискретных устройств криптографического преобразования, которые обеспечивают максимальную неопределенность результатов при практически минимальной сложности технической реализации. На основании проведенных исследований получены следующие практические результаты: разработаны функциональные и структурные схемы устройств и алгоритмы реализации предложенных методов, которые в совокупности обеспечивают использование группы операций, синтезированных по критерию строгого устойчивого кодирования. Практическая ценность работы подтверждена актами внедрения основных результатов диссертационного исследования.

Ключевые слова: защита компьютерной информации, потоковые шифры, операции криптографического сложения, синтез операций, сложность, стойкость, надежность.

ABSTRACT

Nesterenko O.B. The methods and means of synthesizing the stream ciphering operations on the criterion of strict stable coding. – Manuscript.

PhD thesis, specialty: 05.13.05 – Computer Systems and Components. – Cherkasy State Technological University, Cherkasy, 2019.

The thesis is devoted to increasing the uncertainty of the stream ciphering results due to the use of new cryptographic transformations' operations synthesized by the criterion of strict stable coding.

For this purpose, a method for synthesizing the operations by the criterion of strict stable coding has been developed for the first time, using the Hamming minimum distances tables, which provide the maximum uncertainty of the transformation's results and increase the variability of cryptographic algorithms. The method for synthesizing operations by the criterion of strict stable coding of minimal complexity is developed, based on the use of permutation and subdued operations, by the established limitations and relationships between transformation operations and the tables of Hamming minimum distances, which provide the maximum uncertainty of the transformation results with the minimal complexity of the circuit-technical and program implementation. Further development methods for the synthesis of software and hardware cryptographic means of computer technology is done on the basis of the use of a new group of operations built on the criterion of strictly stable coding, by applying the methods of synthesis of models of operations with new properties, which provided simplification of synthesis. The synthesis of operations models according to the criterion of strictly stable encoding of minimal complexity is realized without the construction of tables of truth and their minimization

Keywords: the computer information protection, stream ciphers, cryptographic transformation operations, operations' synthesis, complexity, stability, reliability.