Голові спеціалізованої вченої ради Д 73.052.04
при Черкаському державному технологічному університеті
18006, м. Черкаси, бульв. Шевченка, 460.

ВІДГУК
офіційного опонента

начальника кафедри захисту інформації та кібербезпеки факультету охорони державної таємниці та інформаційного протиборства Житомирського військового інституту імені С. П. Корольова заслуженого діяча науки і техніки України, доктора технічних наук, професора Грищука Руслана Валентиновича на дисертацію Бреус Роксолани Василівни "Генерація псевдовипадкових послідовностей операцій строгого стійкого криптографічного кодування на основі перетворення другого операнда", поданої нею на здобуття наукового ступеня кандидата технічних наук за спеціальністю 05.13.05 – комп'ютерні системи та компоненти

Актуальність теми

Зростання кількості кіберінцидентів в світі та Україні суттєво підвищує вимоги до комп'ютерних компонентів та систем, які використовуються в процесі забезпечення безпеки інформації, яка в них створюється, зберігається та передається. Розвиток технік криптоаналізу та поступова квантизація відповідних процедур ставить під загрозу компроментації більшість з відомих криптоперетворень з гарантованою стійкістю.

На часі пошук нових механізмів забезпечення строгого криптографічного перетворення одночасно швидких при застосуванні в системах потокового шифрування. Проте для таких перетворень на сьогодні ще й досі були недосліджені процеси синтезу груп двохрозрядних двохоперандних операцій строгого криптографічного перетворення. *Саме тому, враховуючи зв'язок теми дисертації Бреус Р. В. з означеними вище питаннями, вважаємо її вибір обґрунтованим, а саму тему актуальною.*

Оцінка обґрунтованості наукових положень, висновків та рекомендацій, сформульованих у дисертації, їх достовірність, новизна

Загальна характеристика дисертації

У **вступі** здобувачкою обґрунтовано актуальність обраної теми, показано її зв'язок з науковими програмами, планами, сформульовано мету і задачі дослідження, визначено об'єкт, предмет та методи дослідження, відображено наукову новизну й практичне значення одержаних результатів, наведено дані щодо особистого внеску, результати апробації, дані про публікації та структуру й обсяг роботи.

У **першому розділі** здобувачкою приведено результати аналізу сучасного стану та перспектив розвитку комп'ютерної криптографії. Зокрема в ході аналізу проблеми комп'ютеризованого захисту інформації в Україні *встановлено* основні причини, які призвели до кіберінцидентів. У ході проведення аналізу також *виявлено* основні випадки порушення безпеки інформації, яка підлягає захисту в комп'ютерних системах. За результатами оцінювання сучасного стану захисту інформації в комп'ютерних системах і мережах на прикладі провідних держав світу США, КНР, Австралії, держав-членів Європейського Союзу було *розглянуто* фактори, які мають найбільший вплив. Як результат, зроблено висновок – кіберпростір поступово стає новим середовищем

протистояння. Дієва протидія в кіберпросторі, як показано в розділі, неможлива без розроблення дієвих механізмів криптографічних перетворень.

У першому розділі також проведено критичний огляд існуючих операцій криптографічного перетворення, виходячи з результатів яких поставлено мету та частинні задачі дисертаційного дослідження.

Позитивною рисою першого розділу є те, що здобувачка всебічно підійшла до вивчення стану проблеми в рамках якої розв'язується наукове завдання, а саме розглянуто і елементи існуючої інституційної національної та міжнародної нормативно-правової бази в галузі, й існуючі недоліки в науковій царині дослідження. *Таким чином, одержані здобувачкою у першому розділі результати виступили коректним підґрунтям для постановки наукового завдання.*

У **другому розділі** *приведено результати* синтезу обернених двохрозрядних двохоперандних операцій строгого стійкого криптографічного кодування на основі перетворення другого операнда. З цією метою здобувачка *обґрунтувала та особисто розробила* технологію дослідження взаємозв'язків між прямими і оберненими двохрозрядними двохоперандними операціями строгого стійкого криптографічного кодування. *Позитивним є те*, що в результаті створення відповідної технології окрім усіх переваг, якими вона володіє, здобувачкою виявлено і недолік суть якого зводиться до висунення підвищених вимог до комп'ютерних систем, які будуть використовуватися для здійснення операцій криптоперетворень. Для усунення виявленого недоліку авторка далі у розділі встановлює взаємозв'язки між прямими і оберненими операціями в групі двохрозрядних двохоперандних операцій строгого стійкого криптографічного кодування. Виявлення таких зв'язків свідчить про *коректність запропонованого підходу*. Результати синтезу обернених двохрозрядних двохоперандних операцій строгого стійкого криптографічного кодування на основі встановлених взаємозв'язків дозволили одержати науково обґрунтований відповідний метод. Запропонований метод розкрито алгоритмічно, що виступає підґрунтям для створення на його основі відповідних криптографічних засобів.

Таким чином, у розділі доведено, що запропонований метод синтезу обернених двохрозрядних двохоперандних операцій строго стійкого криптографічного кодування на основі перетворення другого операнда шляхом реалізації моделі автомата побудови другого операнда оберненої операції, виступає практичним підґрунтям для застосування даних операцій.

Третій розділ дисертації здобувачка присвятила синтезу групи двохрозрядних двохоперандних операцій строгого стійкого криптографічного кодування на основі перетворення другого операнда відомої операції. Зокрема здійснено синтез групи двохрозрядних двохоперандних операцій строгого стійкого криптографічного кодування на основі першої операції, синтез групи двохрозрядних двохоперандних операцій строгого стійкого криптографічного кодування на основі другої операції та синтез групи двохрозрядних двохоперандних операцій строгого криптографічного кодування на основі третьої операції. У результаті проведених операцій, як узагальнення, здобувачкою розроблено метод синтезу групи двохрозрядних двохоперандних операцій строгого криптографічного кодування на основі заданої операції. Запропонований метод складається з шести послідовних та узгоджених між собою логічних кроків, виконання яких забезпечує досягнення збільшення варіативності алгоритмів в 24 рази, що обумовлено відповідною кількістю операцій.

Таким чином, запропонований у третьому розділі метод забезпечує можливість збільшення варіативності криптопримітивів при практичному застосуванні операцій строгого стійкого криптографічного кодування.

Четвертий розділ дисертації є заключним. Його здобувачкою присвячено розробленню методу генерації псевдовипадкових послідовностей двохрозрядних двохоперандних операцій строгого стійкого криптографічного кодування на основі перетворення другого операнда, а також практичній перевірці одержаних результатів. *Позитивною стороною* розробленого методу є те, що в його основу покладено узагальнені результати синтезу операцій криптоперетворення, дані по яким подані в узагальнених таблицях. Запропонований у розділі метод розкрито як у вигляді логічних послідовних кроків, так і алгоритмічно.

На підтвердження достовірності розроблених методів здобувачка в даному розділі також приводить результати практичної реалізації запропонованих генераторів взаємопов'язаних псевдовипадкових послідовностей прямих і обернених двохрозрядних двохоперандних операцій строгого стійкого криптографічного кодування на основі перетворення другого операнда. Як слідство для різних варіантів практичної реалізації здобувачка змогла *покращити метод* підвищення стійкості та надійності потокового шифрування та запропонувати його структурну схему.

Таким чином, отриманий у четвертому розділі метод відкриває можливості для його застосування з метою захисту інформації з підвищеними вимогами до конфіденційності.

У **висновках** приведено основні одержані результати, їх наукову та практичну цінність, дані щодо впровадження результатів роботи.

У **додатках** до дисертації наведено: список публікацій здобувачки за темою дисертації; відомості про апробацію результатів дисертації; копії актів впровадження.

Сформульовані в дисертації наукові положення, висновки та рекомендації достатньо повно обґрунтовані здобувачкою та викладені в доказовій формі.

Наукова новизна одержаних особисто здобувачкою результатів полягає у такому:

вперше розроблено метод синтезу обернених двохрозрядних двохоперандних операцій строгого стійкого криптографічного кодування на основі перетворення другого операнда шляхом реалізації моделі автомата побудови другого операнда оберненої операції, що забезпечило можливість практичного застосування даних операцій;

вперше розроблено метод синтезу групи двохрозрядних двохоперандних операцій строгого стійкого криптографічного кодування на основі перетворення другого операнда відомої операції шляхом виконання над ним двохрозрядної одноопераднодної операції, що забезпечило можливість збільшення варіативності криптопримітивів при практичному застосуванні даних операцій;

вперше розроблено метод генерації псевдовипадкових послідовностей двохрозрядних двохоперандних операцій строгого стійкого криптографічного кодування на основі перетворення другого операнда, що дозволяє значно спростити процес дослідження та синтезу групи операцій строгого стійкого криптоперетворення та робить можливим використання його при вдосконаленні методу підвищення криптостійкості і надійності потокового шифрування.

Достовірність наукових положень

Достовірність наукових положень дисертаційної роботи підтверджується:

коректною постановкою наукового завдання та часткових наукових задач дисертаційного дослідження (с. 33 дисерт. та с. 1 автореф.);

використанням в роботі теоретично обґрунтованих та широко апробованих на практиці методів криптографії, теорії інформації, теорії алгоритмів, методів дискретної математики, методів теорії ймовірностей, а також логіки;

збіжністю результатів практичної перевірки з відомими експериментальними даними інших академічних досліджень, відповідністю отриманих теоретичних результатів основним законам і явищам природи.

Наукове значення дисертаційної роботи полягає в подальшому розвитку методів побудови комп'ютерних систем та їх компонент, які забезпечують строгого стійке криптографічне кодування на основі перетворення другого операнда.

Практичне значення дисертації полягає в створенні на основі запропонованих методів дискретних моделей операцій та алгоритмів автоматичної генерації псевдовипадкових послідовностей операцій строгого стійкого кодування для систем потокового комп'ютерного шифрування.

Практична значущість одержаних результатів і достовірність наукових положень підтверджені актами впровадження (копії – с. 187–190 дисерт.) і про що зазначено в авторефераті на с. 3 та с. 4 відповідно. Зазначені факти підтверджують особистий внесок здобувача в науку.

Мова та стиль викладення дисертації та автореферату дозволяють зрозуміти суть розроблених наукових положень і одержаних практичних результатів. Дисертація і автореферат у цілому відповідають вимогам, які висуваються до їх оформлення відповідно до Порядку присудження наукових ступенів, затвердженого постановою Кабінету Міністрів України від 24.07.2013 р. № 567 (із змінами) та Вимог до оформлення дисертації, затверджених наказом Міністерства освіти і науки України від 12.01.2017 р. № 40. Зміст дисертації та автореферату викладено послідовно та логічно.

Підтвердження повноти викладу основних результатів дисертації в опублікованих працях

За напрямом дисертаційного дослідження здобувачкою опубліковано 10 наукових праць, з яких чотири – це наукові статті у фахових виданнях України, одна стаття в закордонному науковому виданні, одна колективна монографія, три матеріали міжнародних науково-технічних конференцій та одні тези в збірнику матеріалів міжнародного симпозіуму, проіндексованому в *Scopus*.

Перераховані публікації з достатньою повнотою відбивають наукові та практичні результати дисертації та у цілому відповідають вимогам до публікацій результатів дисертації на здобуття наукового ступеня кандидата наук, які висуваються наказом Міністерства освіти і науки України від 29.09.2019 р. №1220. З праць, що їх опубліковано у співавторстві, у дисертації використано лише ті результати, які отримано здобувачкою самостійно.

Зауваження щодо змісту дисертації та її оформлення

Зауваження та недоліки концептуального характеру

1. У дисертації здобувачка стверджує, що дослідження та побудова нових *операцій криптоперетворення* на сьогодні є особливо актуальним науковим завданням. З цією тезою не можливо не погодитися. Але вже далі по тексту роботи авторка відходить від даної тези і веде мову про *криптографічне кодування*, як один із напрямів комп'ютерної криптографії. На наш погляд, дане твердження приведено безальтернативно, без будь-яких пояснень, аргументів, що призводить до деяких розбіжностей з усталеними в криптографії поняттями.

2. За мету роботи здобувачка ставить підвищення швидкості потокового шифрування за рахунок генерації псевдовипадкових послідовностей групи двохрозрядних двохоперандних операцій строгого стійкого криптографічного кодування на основі перетворення другого операнда. Але при формулюванні наукової новизни положень в явному вигляді досить складно без ґрунтовного ознайомлення з усією

роботою встановити чи досягнута заявлена мета. Наприклад, числові показники досягнення мети приводяться в практичному значенні роботі, що цілком закономірно.

На наш погляд, згадані показники досягнення мети мають бути також в явному вигляді вербально формалізовані й в наукових положеннях, які захищаються. Такий підхід дозволив би здобувачці більш переконливо подати одержані в роботі нові наукові результати.

3. На наше глибоке переконання в кандидатські дисертації, що опонується пані Роксолана *розв'язала конкретне наукове завдання, що має істотне значення для подальшого розвитку комп'ютерних систем та їх компонентів*, а не важливу науково-технічну задачу. Важливою може бути тільки науково-прикладна або наукова проблема в докторській дисертації.

Зауваження та недоліки дискусійного характеру

1. У першому розділі роботи недостатньо переконливо приведено результати аналізу проблеми комп'ютеризованого захисту інформації в Україні. Зокрема не вистачає статистичних даних, які це підтверджують. Наприклад, яка кількість кіберінцидентів мала місце в Україні за останні роки. Приведення таких даних аргументовано підкреслило б обґрунтованість вибору теми, актуальність якої не викликає сумнівів.

Поряд з тим, справедливо слід відмітити, далі по розділу є схожі оцінки, що стосується таких розвинених держав світу, як США, КНР, держав-членів ЄС. Але вони, на жаль, дещо застаріли, хоча й присвячені найбільш відомим кіберінцидентам.

2. Ще одним недоліком першого розділу є деяка невизначеність у вимогах, які висуваються до гамуючих послідовностей γ_1 та γ_2 й до форми подання вихідної інформації I_ν, визначених на рис. 1.1 с. 32 дисертації.

3. У другому й третьому розділах дисертації здобувачка досить ґрунтовно у формалізованому вигляді розкриває процедури синтезу обернених двохрозрядних двохоперандних операцій строгого стійкого криптографічного кодування на основі встановлених взаємозв'язків, а також процедури синтезу групи двохрозрядних двохоперандних операцій строгого стійкого криптографічного кодування на основі першої операції відповідно. Поряд з тим така подача результатів дещо перевантажує текст дисертації. На наш погляд, можливо було б у першому та другому випадках подати ґрунтовно процедури синтезу для першої та останньої прямих та обернених операцій криптоперетворень, а всі інші винести у додатки.

Очевидно, що здобувачка таким оригінальним поданням намагалися всебічно підтвердити достовірність одержаних результатів.

4. З приведеного в четвертому розділі прикладу практичної реалізації запропонованих генераторів взаємопов'язаних псевдовипадкових послідовностей прямих і обернених двохрозрядних двохоперандних операцій строгого стійкого криптографічного кодування на основі перетворення другого операнда, досить складно встановити, виходячи з яких міркувань здобувачка зробила висновок про швидше на 15-20%, порівняно табличним методом синтезу операцій, генерування псевдовипадкових послідовностей.

5. У дисертації не знайшов місце експеримент, приведення б результатів якого на додачу до поданого прикладу, сприяли б більш переконливому підтвердженню достовірності одержаних наукових та практичних результатів.

Інші основні зауваження та недоліки

1. У дисертації по тексту зустрічаються деякі орфографічні, стилістичні та лінгвістичні некоректності. Наприклад на с. 13, 17, 38, 111, 162 та ін.

2. У дисертації не вистачає переліку скорочень, що суттєво б спростило навігацію по роботі.

3. У дисертації присутні деякі відхилення від вимог до оформлення наукових кваліфікаційних праць.

Зазначені недоліки дещо впливають на якість подання дисертації, але їх наявність не знижує практичної, а тим паче наукової цінності одержаних здобувачкою результатів.

Висновки

Отже, на основі критичного вивчення дисертації, автореферату дисертації та праць здобувачки, опублікованих за темою дисертації, об'єктивно **встановлено:**

дисертаційна робота Бреус Р. В. відповідає вимогам Порядку присудження наукових ступенів, затвердженого постановою Кабінету Міністрів України від 24.07.2013 р. № 567 (із змінами);

дисертаційна робота відповідає паспорту спеціальності 05.13.05 – комп'ютерні системи та компоненти;

зміст автореферату ідентичний основним положенням дисертації;

використання чужих наукових результатів без посилань на авторів у дисертації не виявлено, що свідчить про особистий внесок здобувачки в науку;

дисертація Бреус Р. В. є завершеною кваліфікаційною науковою працею, що місить нові науково обґрунтовані результати проведених здобувачкою досліджень, які вирішують конкретне наукове завдання, пов'язане з підвищенням швидкості потокового шифрування за рахунок генерації псевдовипадкових послідовностей групи двохрозрядних двохоперандних операцій строгого стійкого криптографічного кодування на основі перетворення другого операнда. Дане наукове завдання має істотне значення для подальшого розвитку методів побудови комп'ютерних систем та їх компонент, які забезпечують строгого стійке криптографічне кодування на основі перетворення другого операнда;

авторка дисертації, БРЕУС Роксолана Василівна заслуговує на присудження їй наукового ступеня кандидата технічних наук за спеціальністю 05.13.05 – комп'ютерні системи та компоненти.

Офіційний опонент –
начальник кафедри захисту інформації та кібербезпеки
факультету охорони державної таємниці та інформаційного протиборства
Житомирського військового інституту імені С. П. Корольова

заслужений діяч науки і техніки України,
доктор технічних наук,
професор

Руслан ГРИЩУК

"20" січня 2021 р.

Підпис професора Грищука Р. засвідчую
Начальник відділу персоналу та стройового

Олександр КОВАЛЬЧУК