

## ВІДГУК

офіційного опонента

професор кафедри безпеки інформації та телекомунікацій  
Національного технічного університету "Дніпровська політехніка",  
доктора технічних наук, професора Корченко Анни Олександрівни  
на дисертаційну роботу Підласого Дмитра Андрійовича  
"Метод синтезу СЕТ-операцій на основі елементарних функцій операцій,  
керованих інформацією", яка подається на здобуття наукового ступеня  
доктора філософії за спеціальністю 123 – комп'ютерна інженерія  
галузі знань 12 – Інформаційні технології

**1. Актуальність теми.** На сучасному етапі розвитку інформаційних технологій криптографічні методи та засоби є одним із найдієвіших механізмів забезпечення інформаційної безпеки. Інтенсивний науково-технічний прогрес сприяє появі нових викликів у сфері захисту інформації, що обумовлює необхідність як розроблення нових криптографічних алгоритмів, так і подальшого вдосконалення та оптимізації наявних методів і засобів криптографічного захисту. Одним із перспективних напрямів сучасного розвитку криптографії є застосування розширеного спектра криптографічних операцій, в тому числі СЕТ-операцій на основі елементарних функцій операцій, керованих інформацією, що створює передумови для вдосконалення наявних і розроблення нових криптографічних алгоритмів. Розширений спектр криптографічних операцій забезпечує більшу свободу під час конструювання криптоалгоритмів, дозволяючи адаптувати їх до різних вимог щодо рівня безпеки, продуктивності та апаратної реалізації. Рациональний вибір і комбінування СЕТ-операцій дає можливість оптимізувати швидкодію алгоритмів, скоротити обчислювальні витрати та зменшити споживання пам'яті, що особливо важливо для вбудованих систем, IoT-пристроїв і мобільних платформ. Крім того, висока значущість та недостатня практична вирішеність завдань, таких як побудова операцій криптографічного перетворення над великою кількістю змінних, розроблення методів використання синтезованих операцій у криптографічних алгоритмах визначає безперечну новизну цього дослідження, а розгляд питань, пов'язаних із цією тематикою, має як теоретичне, так і практичне значення у сучасних умовах. Тому пошук нових і

вдосконалення наявних методів захисту інформації, спрямованих на розробку методів підвищення якості систем комп'ютерної криптографії за рахунок синтезу та використання СЕТ-операцій на основі елементарних функцій операцій, керованих інформацією є актуальним завданням.

Актуальність і особливу значимість теми дисертаційного дослідження Підласого Дмитра Андрійовича підкреслює її зв'язок з науково-дослідними роботами «Методи та засоби синтезу груп симетричних двооперандних операцій криптографічного кодування для малоресурсних криптоалгоритмів» (ДР № 0121U114390) та «Дослідження шляхів розвитку потокового шифрування на основі криптографічного кодування» (ДР № 0121U114389).

Таким чином, враховуючи наведені аргументи, актуальність теми дисертаційного дослідження Підласого Дмитра Андрійовича «Метод синтезу СЕТ-операцій на основі елементарних функцій операцій, керованих інформацією» не викликає жодних сумнівів.

**2. Ступінь обґрунтованості наукових положень дисертації та їх достовірність.** Основні наукові результати дослідження, запропоновані метод синтезу елементарних функцій операцій, керованих інформацією, на основі відомих дискретних моделей елементарних функцій, отриманих за результатами обчислювального експерименту та метод синтезу 3Сі-квантових СЕТ-операцій на основі елементарних функцій операцій, керованих інформацією, шляхом синтезу базових груп симетричних однооперандних СЕТ-операцій за критерієм простоти їх побудови та критерієм відмінності відповідних елементарних функцій, чітко сформульовані, достатньо обґрунтовані та не викликають сумнівів. Достовірність наукових положень дисертації забезпечується:

- використанням у процесі досліджень методів дискретної математики і комп'ютерного моделювання, основ теорії СЕТ-шифрування, теорії ймовірностей і теорії алгоритмів, обчислювального експерименту, дискретно-казуальної логіки;
- проведенням дослідження псевдовипадкових послідовностей на виході засобів формування, що реалізують запропоновані методи формування, за допомогою статистичних пакетів тестування NIST;
- відповідністю проведених експериментальних досліджень виконаним теоретичним розрахункам.

### **3. Найбільш вагомі наукові результати, одержані здобувачем особисто.**

У дисертаційній роботі розв'язано актуальне науково-технічне завдання, яка полягає у підвищенні варіативності малоресурсних потокових шифрів випадкової підстановки за рахунок розроблення та впровадження методу синтезу СЕТ-операцій на основі елементарних функцій операцій, керованих інформацією, які забезпечують можливість подвійного управління процесом криптографічного перетворення, як від ключової послідовності, так і від вхідної інформації, при збільшенні кількості таблиць підстановки, що реалізуються в криптоалгоритмі.

### **4. Наукова новизна отриманих результатів** полягає в наступному:

- вперше запропоновано метод синтезу елементарних функцій операцій, керованих інформацією, на основі відомих дискретних моделей елементарних функцій, отриманих за результатами обчислювального експерименту, за допомогою встановлення і формалізації взаємозв'язків між дискретними змінними, що забезпечило можливість побудови повних множин дискретно-алгебраїчних і дискретно-казуальних моделей елементарних функцій операцій, керованих інформацією, для спрощення подальшого дослідження синтезу СЕТ-операцій на основі елементарних функцій операцій, керованих інформацією;
- вперше побудовано метод синтезу 3Сі-квантових СЕТ-операцій на основі елементарних функцій операцій, керованих інформацією, шляхом синтезу базових груп симетричних однооперандних СЕТ-операцій за критерієм простоти їх побудови та критерієм відмінності відповідних елементарних функцій, багатоваріантного представлення СЕТ-операцій дискретно-казуальними моделями, мінімізації взаємозв'язків у кортежі однооперандних СЕТ-операцій при побудові двооперандної СЕТ-операції, що забезпечило можливість подвійного управління процесом криптографічного перетворення при зменшенні складності реалізації СЕТ-операцій;
- удосконалено системи потокового шифрування на основі випадкових підстановок шляхом застосування двооперандних СЕТ-операцій на основі елементарних функцій операцій, керованих інформацією, і генераторів модифікованих СЕТ-операцій, що забезпечило можливість подвійного управління процесом криптографічного перетворення від ключової послідовності і від вхідної інформації, збільшило кількість таблиць підстановки

до 192 (кількість SET-операцій в групі операцій на основі елементарних функцій операцій, керованих інформацією) для перетворення 3 Сі-квантів інформації (3 біт інформації). Стійкість результатів шифрування до статистичного криптоаналізу відповідає вимогам методики NIST STS.

**5. Практична цінність результатів** полягає у розробленні нових моделей і SET-операцій, придатних для побудови сучасних комп'ютерних криптографічних систем. На їх основі запропоновано функціональні схеми та алгоритми реалізації криптографічних перетворень із використанням елементарних функцій і операцій, керованих інформацією. Запропоновані рішення забезпечують побудову криптографічних систем із подвійним керуванням процесом шифрування, розширюють варіативність алгоритмів завдяки використанню 192 таблиць підстановки та 4096 варіантів базових груп для синтезу симетричних двооперандних SET-операцій. Реалізація цих операцій забезпечує псевдовипадкові міжсимвольні перетворення і розсіювання символів, що підвищує стійкість шифрування до статистичного криптоаналізу відповідно до методики NIST STS.

Додатково практична цінність дисертаційного дослідження підтверджується наведеною в додатку дисертації довідкою про впровадження системи потокового шифрування реалізованої на рівні програмного модуля системи управління роботизованим комплексом "MOROZ-02L".

**6. Оцінка змісту та завершеності роботи.** Дисертаційна робота складається зі вступу, чотирьох розділів, висновків (загалом 145 сторінок основного тексту), списку використаних джерел (126 найменувань), додатків (14 сторінок).

**У вступі** обґрунтовано актуальність дослідження, наведені посилання на роботи науковців за обраним напрямом дослідження, показано зв'язок роботи з науковими програмами, планами та темами, визначено мету та завдання роботи, визначено об'єкт і предмет дослідження, наведено методи наукових досліджень, що використовувалися в роботі. Наведено наукову новизну та практичне значення отриманих результатів, а також відомості про апробацію та публікації результатів дослідження.

**У першому розділі** на основі аналізу сфер застосування малоресурсного комп'ютеризованого захисту цифрової інформації обґрунтовано необхідність

розвитку засобів малоресурсної криптографії. Встановлено, що більшість існуючих малоресурсних криптоалгоритмів є спрощеними версіями традиційних криптографічних алгоритмів. Проаналізовано сучасний стан і перспективи розвитку СЕТ-шифрування, що стало підґрунтям для визначення мети та завдань дисертаційного дослідження.

**У другому розділі** на основі дискретних моделей елементарних функцій операцій, керованих інформацією, побудовано їх дискретно-алгебраїчні моделі. Встановлено, що вибір логічної операції визначається значенням будь-якого з управляючих Сі-квантів інформації, що дало змогу запропонувати багатоваріантний метод синтезу моделей. Для спрощення синтезу й аналізу СЕТ-операцій запропоновано використання дискретно-казуальних моделей, які забезпечують багатоваріантне представлення елементарних функцій операцій, керованих інформацією.

**У третьому розділі** встановлено, що кожен СЕТ-операцію на основі елементарних функцій, керованих інформацією, можна реалізувати у 27 варіантах. Запропоновано підхід до побудови базової групи лише із симетричних СЕТ-операцій, що спрощує їх синтез і аналіз. Розроблено моделі синтезу базових груп за критеріями простоти та відмінності елементарних функцій, а також моделі формування груп СЕТ-операцій із використанням перестановок та інверсій, які стали основою удосконаленого методу синтезу 3Сі-квантових однооперандних СЕТ-операцій.

**У четвертому розділі** запропоновано метод синтезу двохоперандних СЕТ-операцій на основі поєднання симетричних однооперандних операцій, що зменшує ресурсні витрати криптографічної системи. Розроблено дискретно-казуальні моделі двохоперандних СЕТ-операцій за критеріями простоти побудови та відмінності елементарних функцій, а також досліджено особливості побудови криптографічних систем на їх основі. Встановлено, що запропоновані системи забезпечують подвійне керування процесом шифрування, використання до 192 модифікованих таблиць підстановок для перетворення 3Сі-квантів інформації та відповідають вимогам методики NIST STS за стійкістю до статистичного криптоаналізу.

**У висновках** наведено основні теоретичні та практичні результати наукового дослідження, які підтверджують досягнення поставленої мети.

У додатках до дисертації подано довідку про впровадження результатів дисертаційного дослідження, список публікацій, у яких опубліковано основні наукові результати дисертації, опис пакета статистичних тестів NIST STS та результати тестування шифрограм за допомогою пакету NIST STS.

**7. Основні наукові результати**, що отримані в дисертації, викладені здобувачем у 15 друкованих працях, у тому числі 4 статтях у фахових виданнях України, з яких 1 стаття проіндексована в наукометричній базі Scopus, 4 статтях у закордонних виданнях; в одноосібному розділі 1 колективної монографії; в 1 монографії, опублікованій у співавторстві, 3 тезах доповідей на міжнародних науково-технічних та науково-практичних конференціях.

**8. Оформлення дисертації.** Дисертаційне дослідження оформлено згідно з вимогами положення про "Порядок присудження наукових ступенів".

**9. Відсутність (наявність) порушень принципів академічної доброчесності.** У процесі оцінювання дисертаційного дослідження ознак порушення принципів академічної доброчесності не встановлено.

#### **10. Зауваження по дисертації.**

1. У першому розділі дисертації наведено ґрунтовний огляд літературних джерел, однак їх аналіз має переважно описовий характер. Недостатньо уваги приділено критичному порівнянню існуючих підходів до синтезу СЕТ-операцій із визначенням їх переваг, недоліків та обмежень. Зокрема, доцільно було б чіткіше показати, якою мірою відомі підходи забезпечують варіативність криптографічного перетворення, можливість управління процесом перетворення та складність реалізації СЕТ-операцій. У зв'язку з цим недостатньо чітко окреслено місце запропонованого автором методу серед існуючих наукових підходів та його відмінності від відомих рішень. Наведення порівняльного критичного аналізу дозволило б більш переконливо обґрунтувати постановку наукової задачі та наукову новизну запропонованого підходу.

2. У тексті дисертаційного дослідження вживаються терміни «СЕТ-операція» та «модель СЕТ-операції». На мою думку, доцільно уточнити зміст цих понять та забезпечити послідовність їх використання в тексті дисертації.

3. Основний обсяг другого розділу присвячено дослідженню елементарних функцій та побудові їх дискретних, дискретно-алгебраїчних і дискретно-казуальних моделей. Запропонований метод синтезу моделей

елементарних функцій операцій, керованих інформацією, представлено переважно у вигляді послідовності етапів його реалізації. На мою думку, доцільно було б доповнити цей опис узагальненою формальною постановкою методу із чітким визначенням множини вхідних даних, вихідних результатів, допустимих перетворень та умов його застосування. Це сприяло б більш однозначному розумінню методу та можливостей його подальшої алгоритмізації і програмної реалізації.

4. У третьому розділі автором запропоновано коефіцієнт зміни кількості елементарних функцій при криптографічному перетворенні блоків інформації (формула 3.11, с. 96), який використовується для оцінювання варіативності застосування СЕТ-операцій. На мою думку, доцільно було б більш детально обґрунтувати область застосування цього коефіцієнта, його інтерпретацію, граничні значення та можливість використання для порівняння різних груп і типів СЕТ-операцій. Окремого уточнення потребує питання можливості узагальнення запропонованого показника для оцінювання багатооперандних операцій та криптографічних систем потокового шифрування в цілому.

5. У третьому розділі дисертаційної роботи зазначено, що запропонований метод синтезу базової групи СЕТ-операцій дозволяє зменшити складність синтезу та дослідження повної групи СЕТ-операцій. Водночас доцільно було б навести кількісну оцінку такого зменшення складності та порівняти запропонований підхід із повним перебором можливих варіантів. Зокрема, бажано показати, який вигравш забезпечує застосування запропонованого методу за кількістю аналізованих операцій, комбінацій або необхідних обчислювальних процедур. Це дозволило б більш переконливо підтвердити ефективність запропонованого методу.

6. У четвертому розділі автор недостатньо повно розкрив особливості програмної реалізації запропонованих криптографічних систем. Зокрема, доцільно було б навести структуру програмного модуля, особливості реалізації основних алгоритмічних компонентів та оцінити ресурсні характеристики програмної реалізації.

7. У четвертому розділі доцільно було б детальніше проаналізувати результати статистичного тестування запропонованих криптографічних систем, наведені на рис. 4.10-4.11 та в табл. 4.7. Зокрема, потребує додаткового пояснення різниця між результатами тестування двох досліджуваних криптографічних систем, а також інтерпретація отриманих статистичних

показників і їх зв'язок із заявленим підвищенням варіативності криптографічного перетворення.

8. Для підвищення об'єктивності результатів дослідження оцінювання статистичних властивостей результатів шифрування, проведене на основі тестів NIST STS, на мою думку, доцільно було б доповнити використанням системи тестування DIEHARD.

Вважаю, що наведені зауваження не знижують науковий рівень і практичну цінність дисертаційної роботи, а також не впливають на її загальну позитивну оцінку.

## **11. Висновок.**

Дисертаційна робота Підласого Дмитра Андрійовича є завершеною науковою працею, виконаною на актуальну тему, а сукупність отриманих у ній теоретичних і практичних результатів розв'язує важливе науково-технічне завдання підвищення якості систем комп'ютерної криптографії за рахунок синтезу та використання СЕТ-операцій на основі елементарних функцій операцій, керованих інформацією, які забезпечують можливість подвійного управління процесом криптографічного перетворення.

Дисертаційна робота виконана на належному науковому рівні, є самостійним і завершеним науковим дослідженням та не порушує принципів академічної доброчесності. Отримані в дисертації результати характеризуються науковою новизною, є достатньо обґрунтованими та достовірними, а сформульовані висновки відповідають поставленим завданням дослідження. Результати роботи мають теоретичне та практичне значення для розвитку методів і засобів комп'ютерної криптографії.

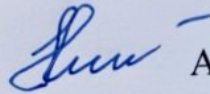
Дисертація за актуальністю, науковою новизною, достовірністю отриманих результатів, обґрунтованістю висновків і практичною цінністю відповідає вимогам, що висуваються до дисертаційних робіт на здобуття ступеня доктора філософії, зокрема «Вимогам до оформлення дисертації», затвердженим наказом Міністерства освіти і науки України від 12.01.2017 № 40 (зі змінами), та «Порядку присудження ступеня доктора філософії та скасування рішення разової спеціалізованої вченої ради закладу вищої освіти, наукової установи про присудження ступеня доктора філософії», затвердженому постановою Кабінету Міністрів України від 12 січня 2022 р. № 44 (у редакції постанови Кабінету Міністрів України від 03 травня 2024 р. № 507).

Таким чином, дисертаційна робота Підласого Дмитра Андрійовича відповідає вимогам, що висуваються до дисертаційних робіт на здобуття

ступеня доктора філософії за спеціальністю 123 «Комп'ютерна інженерія» галузі знань 12 «Інформаційні технології», а її автор, Підласий Дмитро Андрійович, заслуговує на присудження ступеня доктора філософії за спеціальністю 123 «Комп'ютерна інженерія».

**Офіційний опонент:**

професор кафедри безпеки інформації та телекомунікацій  
Національного технічного університету  
«Дніпровська політехніка»  
доктор технічних наук, професор

 Анна КОРЧЕНКО

Підпис Корченко А.О. підтверджую.  
Учений секретар Вченої ради



 Таїсія КАЛЮЖНА