Голові спеціалізованої вченої ради
Д 73.052.04 при Черкаському державному
технологічному університеті

18006, м. Черкаси, бульв. Шевченка, 460,
корп. 1.

ВІДГУК

офіційного опонента на дисертаційну роботу Бабенко Віри Григорівни "Методологія синтезу операцій перетворення інформації для комп'ютерної криптографії" на здобуття наукового ступеня доктора технічних наук за спеціальністю 05.13.05 – комп'ютерні системи та компоненти.

Актуальність теми дисертації.

Дисертаційна робота Бабенко Віри Григорівни присвячена розробці нової методології синтезу операцій перетворення інформації для комп'ютерної криптографії. Необхідність розробки цієї методології обумовлена розширенням спектру функцій та можливостей використання засобів комп'ютерної техніки у всіх сферах життєдіяльності суспільства, а також змінами погляду наукового суспільства на технології постквантової інженерії та формат формалізованих даних, що необхідно оброблювати.

При цьому існуючі тенденції розвитку та поширення спектру завдань, що вирішують комп'ютерні засоби, збільшення ризиків кібернетичних впливів та вторгнень, розповсюдження шкідливих програмних та апаратних засобів генерації кібернетичних зловживань та аномалій, нечітка природа отриманих формалізованих даних, обумовлюють високий рівень вимог щодо оперативності та стійкості процедур захисту інформації. Особливу актуальність ця проблема набуває при впровадженні операцій перетворення інформації для комп'ютерної криптографії.

На жаль, існуючий стан методологічного забезпечення систем захисту інформації, показує існуючи недоліки, що пов'язані з недосконалістю методів та засобів комп'ютерної криптографії.

Таким чином, проблема підвищення ефективності функціонування систем комп'ютерної криптографії шляхом створення методології синтезу операцій перетворення інформації та побудови криптографічних примітивів на їх основі є актуальною.

Дослідження в дисертаційній роботі проводилися у відповідності з наступними нормативними актами.

1. Концепція Національної програми інформатизації, схвалена Законом України «Про Концепцію Національної програми інформатизації» від 4 лютого 1998 г. N 75/98-ВР.

2. Закон України «Про телекомунікації» від 18.11.2003 р. № 1280-IV.

4. Постанова Кабінету Міністрів України від 29.03.2006 №373 «Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах» (зі змінами 2006, 2011 рр.).

5. Плани наукової та науково-технічної діяльності Черкаського державного технологічного університету в рамках науково-дослідницьких робіт: «Методи та засоби захисту інформації МНС України на основі операцій криптографічного кодування» (ДР № 0112U003579), «Криптографічне кодування: методи та засоби реалізації (частина 2)» (ДР № 0113U001475), «Ефективність систем інформаційної безпеки», шифр НДР «Безпека» (ДРН 0113U004731), «Ефективність систем інформаційної безпеки» (Шифр «Перетворення»), «Синтез операцій криптографічного перетворення з заданим характеристиками» (ДР № 0116U008714), «Розробка методів та засобів оцінки ефективності соціоінжинірингу» (ДР № 0116U008715), при виконанні держбюджетної теми № 36Б115 «Розробка методів синтезу тестових моделей поведінки програмних об'єктів, підвищення оперативності передачі та захисту інформації у телекомунікаційних системах» (ДР № 0115U003103) (Кіровоградський національний технічний університет), в яких автор брав участь як виконавець.

Основний зміст роботи.

У вступі обґрунтовано актуальність дисертації, визначено мету, об’єкт та предмет дослідження. Сформульовано завдання дослідження та наведено основні наукові та практичні результати. Відзначено особистий внесок здобувача, апробацію результатів дисертаційної роботи на конференціях, наведено відомості про публікації та структуру роботи.

У першому розділі здобувачем проводиться аналітичний огляд та дослідження стандартних вимог до криптографічних систем. Для здійснення аналізу розглянуто принципи побудови й схеми криптологічних систем, проведений аналіз сучасних криптосистем та виокремлені основні характеристики ефективності функціонування системи криптографічного захисту, у заключній частині розділу формулюються наукові завдання та здійснюється постановка науково-технічної проблеми дисертаційного дослідження.

У другому розділі дисертаційної роботи вперше розроблена методологія синтезу операцій криптографічного перетворення інформації на основі існуючих та розроблених методів синтезу операцій прямого, оберненого та взаємного криптографічного перетворення шляхом їх класифікації та узагальнення, що забезпечило теоретичну можливість побудови нових операцій для конструювання алгоритмів комп'ютерної криптографії з покращеними показниками ефективності.

У третьому розділі на прикладі вибраної із класифікації групи елементарних функцій розширеного матричного крипторетворення, у рамках розробленої методології побудовано комплекс математичних моделей та методів синтезу елементарних функцій та операцій криптоперетварення, які в сукупності забезпечили можливість вдосконалення систем комп'ютерної криптографії та підтвердили коректність основних положень методології.

Четвертий розділ дисертаційної роботи присвячений розробці удосконаленню методи побудови криптографічних примітивів на прикладі примітивів ковзного шифрування на основі матричних операцій криптографічного перетворення та отриманих узагальнених рекурентних

послідовностей для побудови моделей шляхом їх паралельної реалізації, що забезпечило підвищення швидкості шифрування до 2 разів та стійкості до лінійного крипто аналізу.

П’ятий розділ присвячено розробці технології синтезу операцій для мультиопераційних матричних криптографічних примітивів на основі побудови нових груп операцій з точністю до перестановки шляхом використання запропонованої табличної моделі операції криптоперетворення. Вперше розроблено модель двохоперандної операції криптоперетворення на основі табличного представлення, яка забезпечила можливість проведення обчислювального експерименту для пошуку комутативних та некомутативних криптографічних операцій. Розроблено технологію синтезу двохоперандних матричних операцій для матричних моделей криптографічного перетворення з метою розширення кількості операцій криптографічного перетворення інформації в матричних операціях криптографічного перетворення. Використання даної технології забезпечує синтез мультиопераційних матричних криптографічних примітивів.

Основною метою шостого розділу є виконання порівняльних досліджень. На основі дослідження зміни властивостей результатів криптографічного перетворення в залежності від вибору різної основи модуля запропоновані способи та рекомендації щодо застосування матричних операцій криптографічного перетворення на основі суми за модулем для шифрування інформації. За допомогою проведеного тестування статистичних властивостей запропонованих способів реалізації криптографічного перетворення інформації пакетом тестів NIST STS обґрунтовано ефективність використання операції додавання за модулем 2 в якості кінцевої за умови використання комбінації операцій додавання за будь-яким іншим 2n модулем з метою підвищення стійкості до лінійного криптоаналізу. Проведена оцінка статистичних властивостей криптоалгоритмів на основі пакету тестів NIST STS підтвердила можливість застосування даних крипто алгоритмів в системах захисту інформації. Аналіз результатів тестування підтвердив доцільність використання

операцій криптографічного перетворення інформації для синтезу нових та вдосконалення існуючих криптоалгоритмів.

Наукова новизна дисертаційної роботи.

1. Вперше запропонована методологія синтезу операцій криптографічного перетворення інформації на основі існуючих та розроблених методів синтезу операцій прямого, оберненого та взаємного криптографічного перетворення шляхом їх класифікації та узагальнення, що забезпечило можливість розширення бази операцій, використання яких дозволяє вдосконалювати існуючі та синтезувати нові криптоалгоритми і криптопримітиви.

2. Вперше розроблено технологію синтезу операцій для мультиопераційних матричних криптографічних примітивів на основі побудови нових груп операцій з точністю до перестановки шляхом використання запропонованої табличної моделі операції криптоперетворення, що дозволило за рахунок варіативності операцій підвищити криптостійкість існуючих криптопримітивів.

3. Удосконалено методи побудови криптографічних примітивів на прикладі примітивів ковзного шифрування на основі матричних операцій криптографічного перетворення та отриманих узагальнених рекурентних послідовностей для побудови моделей шляхом їх паралельної реалізації, що забезпечило підвищення швидкості шифрування (до двох разів) та стійкості до лінійного криптоаналізу.

4. Удосконалено методи синтезу та аналізу криптографічних алгоритмів на основі узагальненої моделі криптоалгоритму, шляхом послідовно-паралельної реалізації операцій криптографічного перетворення інформації на макро- та мікрорівнях, що забезпечило можливість вирішення протиріч між криптостійкістю, складністю та швидкістю для досягнення заданої ефективності, виходячи з задач проектування.

5. Отримали подальший розвиток математичні моделі та методи синтезу елементарних функцій та операцій криптоперетворення на основі

запропонованої методології та вибраної групи нелінійних елементарних функцій шляхом вдосконалення математичного апарату для синтезу прямих та обернених матричних моделей не афінних дискретних перетворень, що в сукупності забезпечило можливість синтезу операцій нелінійних криптографічних перетворень.

Ступінь обґрунтованості наукових положень, висновків і рекомендацій, сформульованих у дисертації, та їх достовірність.

Обґрунтованість та достовірність наукових положень, висновків і рекомендацій дисертації забезпечується коректним використанням відповідного математичного апарату і підтверджується співставленням з результатами експериментальних досліджень.

Практична значимість отриманих результатів полягає в доведенні здобувачем отриманих наукових результатів до конкретних інженерних методик, алгоритмів, моделей та варіантів побудови криптографічних алгоритмів.

На підставі проведених досліджень одержано такі практичні результати: розроблено методологію синтезу операцій криптографічного перетворення інформації в рамках запропонованої концепції побудови алгоритмів захисту інформації на їх основі з можливістю підбору оптимальних показників криптостійкості та швидкодії, що дає змогу покращити ефективність функціонування системи криптографічного захисту в цілому; розроблено технологію побудови та використання криптопримітивів на основі синтезованих операцій криптографічного перетворення інформації з можливістю їх паралельного виконання, що дає виграш у швидкості та часі здійснення перетворення безпосередньо інформації; запропоновано варіанти реалізації на програмному та апаратному рівнях нових груп криптографічних операцій заданої розрядності, що володіють властивостями афінності та нелінійності, зокрема матричного та розширеного матричного перетворення. Застосування синтезованих операцій криптографічного перетворення на основі запропонованих варіантів комбінації використання матричного та розширеного

матричного перетворення при конструюванні алгоритмів дає можливість збільшити криптостійкість (від 2166 до 28157 разів) пропорційно відносно потокового шифрування при зменшенні часу шифрування (від 1,3 до 8 разів).

Практична цінність роботи підтверджена актами впровадження на підприємствах і організаціях: НВК «Фотоприлад», «Науково-дослідний інститут «Акорд» та ПП «Сенсорна електроніка» (м. Черкаси), ТОВ «Люменс-груп» (м. Кіровоград) та в освітній процес у навчальних закладах: Черкаському державному технологічному університеті, Черкаському національному університеті імені Б. Хмельницького, Національному аерокосмічному університеті імені М. Є. Жуковського «ХАІ», Кіровоградському національному технічному університеті.

Апробація результатів роботи та публікації.

Основні положення дисертаційної роботи доповідалися та обговорювалися більш ніж на 10 міжнародних та всеукраїнських наукових семінарах та конференціях, серед яких: міжнародна науково-практична конференція «Інтегровані інтелектуальні робототехнічні комплекси» (Київ, 2009, 2014); всеукраїнські науково-технічна та науково-практична конференції: «Інтегровані комп'ютерні технології в машинобудуванні ІКТМ-2011» (Харків, 2011), «Інформаційна безпека держави, суспільства та особистості» (Кіровоград, 2015), восьма наукова конференція ХУПС ім. І. Кожедуба «Новітні технології – для захисту повітряного простору» (Харків, 2012); п'ятнадцята міжнародна науково-технічна конференція «Моделирование, идентификация, синтез систем управления (МИССУ-2012)» (Канака, Крим, 2012), перша міжнародна заочна науково-практична конференція «Информационные системы и технологии: управление и безопасность» (Тольятті-Русе, 2012), міжнародні науково-практичні конференції: «Методи та засоби кодування, захисту й ущільнення інформації» (Вінниця, 2013, 2016) та «Інформаційні технології та комп'ютерна інженерія» (ІТКІ-2014) (Вінниця, 2014); міжнародні науково-практичні конференції: «Проблеми інформатизації» (Черкаси, 2009, 2013, 2016-2019) та «Інформаційні технології в освіті, науці і

техніці» (Черкаси, 2014, 2016); п’ята міжнародна науково-технічна конференція «Сучасні напрями розвитку інформаційно-комунікаційних технологій та засобів управління» (Харків, 2015); міжнародні науково-практичні конференції: «Проблеми науково-технічного та правового забезпечення кібербезпеки у сучасному світі «ПНПЗК-2016»» (Харків, 2016), «Наукова думка інформаційного століття» (Дніпро, 2017), «Інноваційні тенденції сьогодення у сфері природничих, гуманітарних та точних наук» (Івано-Франківськ, 2017), «Наука у контексті сучасних глобалізаційних процесів» (Полтава, 2017), «Науковий і інноваційний потенціал сьогодення» (Ополе, Польща, 2018), Second International Workshop on Computer Modeling and Intelligent Systems (CMIS-2019) (Запоріжжя, 2019).

Основні результати дисертаційної роботи викладено в 90 друкованих працях, а саме: 49 наукових статтях у журналах, з них 40 – у фахових виданнях України, 6 статтях у наукових фахових виданнях за кордоном, 7 монографіях, з яких 2 видані за кордоном, 4 деклараційних патенти на корисну модель та 30 тезах доповідей на міжнародних та всеукраїнських наукових конференціях і семінарах.

Відповідність автореферату дисертації. Зміст автореферату є ідентичним до змісту дисертації й повною мірою відображає основні завдання, наукову новизну, практичне значення, висвітлює всі отримані результати, висновки та запропоновані рекомендації.

Зауваження по роботі:

1. У першому розділі дисертаційного дослідження (підрозділ 1.4) автор, на мій погляд, некоректно робить висновок про залежність швидкодії виконання крипто алгоритму від складності, це ставить під сумнів коректність виявленого протиріччя між складністю, криптостійкістю та швидкістю.

2. У висновках підрозділу 2.1.4. другого розділу задекларовано про зменшення складності алгоритмів побудови базових операцій криптографічного перетворення інформації, але кількісних значень цього зменшення не наведено.

3. У підрозділі 2.2.2. автор роботи функції 2.7.3. та 2.7.4. декларує як алгоритм. На мій погляд це некоректне формулювання наведених функцій.

4. У другому розділі автор не надає числових даних щодо підвищення оперативності доступу до конфіденційних інформаційних ресурсів з використанням методу синтезу операцій матричного криптографічного взаємного перетворення.

5. Також у другому розділі не наведено даних про покращення показників ефективності при конструюванні алгоритмів захисту.

6. У п’ятому розділі вказано, що розглянута технологія отримання операцій криптографічного перетворення у матричних криптографічних алгоритмах може бути застосована для побудови операцій з більшою кількістю операндів різної розрядності. Але механізмів цього застосування, переваг та результатів не наведено, тому достовірність цього висновку викликає сумнів.

7. У шостому розділі наведено результати практичних досліджень та експериментів, але нажаль достовірність цих результатів за допомогою статистичних методів не оцінено.

8. Результати перевірки та оцінки ефективності запропонованих методів автор представила у шостому розділі, при цьому було використано ряд пакетів та тестів (NIST, DIEHARD та ін.), а також апаратних засобів. Нажаль наведені результати підтверджують факт переваг окремих визначених показників, а не ефективності функціонування систем комп’ютерної криптографії і цілому.

9. В роботі зроблено ряд суперечливих висновків. Наприклад:

- підрозділ 2.1.3. декларує у назві про розробку методів синтезу матричних операцій криптографічного перетворення, але насправді у цьому підрозділі наведено опис методу синтезу операцій криптоперетворень на основі додавання за модулем два;
- підрозділ 2.1.4. має назву «Аналіз способів запису елементарних функцій та криптографічних операцій», але у висновках по цьому підрозділу декларується про розробку методу;
- розділ чотири має назву «Реалізація криптопримітивів матричними

операціями криптографічного перетворення», а у висновках вказується про удосконалення методу побудови криптографічних примітивів.

Відзначені зауваження не ставлять під сумнів основні наукові та практичні результати, і суттєво не впливають на загальну позитивну оцінку дисертаційної роботи.

Висновок.

Дисертаційна робота Бабенко Віри Григорівни представляє собою завершене актуальне наукове дослідження. В роботі отримано нові науково-обґрунтовані результати, які дозволяють розвинути наукові методики та технології ідентифікації стану в комп'ютерних та комп'ютеризованих системах.

Вважаю, що докторська дисертація Бабенко Віри Григорівни за актуальністю теми, ступенем обґрунтованості наукових положень, рівнем апробації та публікацій, науковою новизною та практичною цінністю отриманих результатів відповідає вимогам, що висуваються до докторських дисертацій згідно п. 9, 10, 12 «Порядку присудження наукових ступенів», затвердженого постановою Кабінету Міністрів України від 24 липня 2013 р. № 567, а сам автор заслуговує на присудження наукового ступеня доктора технічних наук за спеціальністю 05.13.05 – комп'ютерні системи та компоненти.

Офіційний опонент
завідувач кафедри обчислювальної техніки та програмування
Національного технічного університету «Харківський політехнічний інститут»

д.т.н., проф. Сергій СЕМЕНОВ

Підпис
ЗАСВІДЧУЮ:
ВЧЕНИЙ СЕКРЕТАР
ІОНАЛЬНОГО ТЕХНІЧНОГО УНІВЕРСИТЕТУ
ВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ"
Заковоротний О.Ю.
08 2020 р.

МІНІСТЕРСТВО ОСВІТИ * Національний технічний університет "Харківський політехнічний інститут" * код 02071180 * УКРАЇНИ