# РЕЦЕНЗІЯ

кандидата технічних наук, доцента Миронець Ірини Валеріївни
на дисертацію Рудницької Юлії Володимирівни
**«Інформаційна технологія моделювання симетричних операцій криптографічного кодування для захищених інформаційних систем критичної інфраструктури»,**
яку подано на здобуття ступеня доктора філософії
за спеціальністю 126 Інформаційні системи та технології
галузь знань 12 Інформаційні технології

**1. Актуальність теми дослідження.**

У зв'язку із збільшенням кількості випадків несанкціонованого доступу до конфіденційної інформації в комунікаційних системах та комп'ютерних мережах та постійним зростанням ризиків порушення безпеки захищених інформаційних систем однією з актуальних задач інформаційної безпеки є пошук нових методів шифрування, які б забезпечували достатньо високий рівень криптографічної стійкості та були б простими в апаратній та програмній реалізаціях з урахуванням особливостей сучасних мікропроцесорів. Одним із шляхів покращення ефективності застосування криптографічних алгоритмів для шифрування інформації може бути збільшення кількості операцій придатних для криптографічного перетворення інформації.

Вдосконалення функцій криптографічного перетворення можливо здійснювати шляхом синтезу та дослідження множини операцій криптографічного додавання за модулем два з точністю до перестановки з метою виявлення груп операцій, які можуть бути застосовані в якості операції криптографічного додавання за модулем два. Адже виявлені додаткові операції, дозволять розширити кількість операцій, що застосовуються у блокових та потокових шифрах. Пошук та синтез таких операцій можливо реалізувати на основі виявлення взаємозв'язків між операціями, що використовуються при синтезі операцій криптографічного перетворення. Слід відмітити, що збільшення кількості операцій придатних для реалізації криптографічних перетворень, з однієї сторони, розширює можливості розробників криптоалгоритмів, а з іншої, ускладнює роботу криптоаналітиків.

Пошук та синтез нових операцій криптографічного перетворення даних дозволить будувати алгоритми захисту інформації з кращими криптографічними властивостями, що і робить дане дослідження актуальним.

**2. Наукова новизна одержаних результатів.**

Наукова новизна дисертаційної роботи полягає у створенні нових методів синтезу модифікованих операцій криптографічного кодування, що забезпечило можливість автоматизації генерування та дослідження симетричних двохоперандних операцій та їх послідовностей для застосування в захищених інформаційних системах критичної інфраструктури.

У дисертації розроблені нові методи синтезу операцій:

– метод синтезу моделей симетричних двохоперандних операцій криптографічного кодування на основі кортежів симетричних одноопераднних операцій, який дозволив побудову раніше невідомих симетричних двохоперандних операцій, а результати його застосування надали можливість наповнення бази знань для автоматизації досліджень операцій криптографічного захисту інформації;

– метод синтезу груп моделей симетричних двохоперандних операцій криптографічного кодування для блокового шифрування на основі заданої симетричної двохоперандної операції, що дозволяє забезпечити можливість збільшення варіативності криптоалгоритмів.

**3. Теоретичне та практичне значення одержаних результатів.**

У дисертаційній роботі виконано розробку нових методів синтезу моделей операцій криптографічного кодування на основі запропонованої концепції: метод синтезу моделей симетричних двохоперандних операцій криптографічного кодування на основі одноопераднних операцій; метод синтезу груп симетричних двохоперандних модифікованих операцій блокового шифрування.

У дисертаційному дослідженні запропоновано інформаційну технологію, яка може бути застосована для створення нових методів моделювання та аналізу операцій криптографічного кодування, використання якої спрямоване на виявлення та дослідження нових операцій криптографічного перетворення, застосування яких на етапі алгоритмічного синтезу створює умови для покращення визначених показників ефективності криптографічних алгоритмів. Застосування даної інформаційної технології дозволить забезпечити розробників криптографічних алгоритмів новими можливостями для побудови систем захисту інформації, а також використання нового автоматизованого інструментарію щодо проведення досліджень процесів покращення захищеності інформаційних систем критичної інфраструктури.

Практична цінність роботи полягає у розробці алгоритмів реалізації розроблених методів, що використані при створенні елементів програмного забезпечення запропонованої інформаційної технології.

З вище зазначеного можливо зробити висновок, що дана робота має значний науковий і практичний інтерес.

**4. Структура роботи, оцінка змісту дисертації та її завершеність.**

Основний текст дисертації складає 155 сторінок; загальний обсяг дисертаційної роботи - 162 сторінки.

Анотація до роботи містить скорочений опис основної суті та результатів проведеного дослідження.

Вступ до дисертації містить обґрунтування актуальності та наукової новизни дисертаційного дослідження. Також тут визначено мету та завдання, об'єкт і предмет дослідження та методи, використані при написанні роботи.

У першому розділі дисертації проведено аналітичний огляд моделей і методів захисту інформації в інформаційних системах критичної інфраструктури, визначено перспективні напрямки їх використання для розвитку інформаційних систем і технологій з метою автоматизації проведення наукових досліджень щодо підвищення захищеності інформаційних систем критичної інфраструктури. Розкрито основну проблематику роботи, що стосується процесів автоматизації моделювання та дослідження симетричних двохоперандних операцій, які використовуються при побудові криптоалгоритмів. Сформульовано мету та задачі наукового дослідження.

Другий розділ дисертації присвячено дослідженню різних підходів щодо синтезу моделей симетричних двохоперандних операцій криптографічного кодування та визначенню їх якісних і кількісних характеристик. Розділ містить побудову методу синтезу моделей симетричних двохоперандних операцій криптографічного кодування на основі кортежів симетричних одноопераднних операцій та його реалізацію у вигляді описаного алгоритму.

У третьому розділі дисертації запропоновано концепцію синтезу модифікованих двохоперандних операцій, використання якої дозволило одержати дві нові групи симетричних двохоперандних операцій. Розроблено метод синтезу груп моделей симетричних двохоперандних операцій криптографічного кодування для блокового шифрування на основі заданої симетричної двохоперандної операції, описано алгоритм його реалізації.

Четвертий розділ дисертації присвячено удосконаленню методів побудови інформаційних систем та технологій моделювання і дослідження

операцій криптографічного кодування. Розроблено структуру інформаційної системи, яка забезпечує реалізацію ієрархічної інформаційної технології моделювання симетричних двохоперандних операцій криптографічного кодування та наведено алгоритми її функціонування. Наведено опис структури бази даних та бази знань, що забезпечують необхідні вертикальні і горизонтальні зв'язки в даній технології.

Висновки, зроблені наприкінці роботи, відповідають заявленій меті та завданням дисертації.

Дисертаційна робота є цілком завершеною науковою працею, а наукове завдання дисертації - повністю виконане. Здобувач має достатній рівень володіння методологією наукової діяльності.

**5. Відсутність (наявність) порушень принципів академічної доброчесності**

Ознак порушень принципів академічної доброчесності не встановлено.

**6. Повнота викладення дисертації в опублікованих працях**

Результати, отримані в дисертаційній роботі, відображено у 12 наукових працях, а саме:

– 5 наукових статей, що опубліковані в фахових виданнях України категорії Б;

– 2 наукові праці, які включені до наукометричної бази Scopus;

– 5 тез міжнародних науково-технічних конференцій.

Отже, рівень наукових публікацій здобувача є цілком достатнім.

**7. Зауваження та недоліки дисертації щодо її оформлення і змісту.**

Запропоноване дисертаційне дослідження заслуговує позитивної оцінки, але варто звернути увагу на такі виявлені недоліки та зауваження:

1. Список публікацій здобувача містить 5 тез доповідей в матеріалах міжнародних науково-технічних конференцій, а у вступі в підрозділі апробація результатів дисертації та публікації вказано 4.

2. Із тексту роботи не зрозуміло чому групу двохрозрядних двохоперандних операцій криптографічного кодування на основі додавання за модулем чотири слід називати як групу двохрозрядних двохоперандних операцій криптографічного кодування на основі лівостороннього додавання.

3. У назві підрозділу 2.1 автор використовує формулювання «об'єднання за модулем», що є незрозумілим за змістом поняттям.

4. Із тексту роботи не зрозуміло, які саме результати дисертаційної роботи включені в НДР Черкаського державного технологічного

університету: «Дослідження шляхів розвитку потокового шифрування на основі криптографічного кодування» (ДР № 0121U114389), у яких автор брала участь як виконавець. Адже методи синтезу симетричних двохоперандних операцій криптографічного кодування описано для реалізації блокового шифрування.

5. На стор. 123 дисертаційної роботи автор використовує поняття "полегшений криптоалгоритм", тоді як пояснення такого алгоритму у тексті роботи не надає.

6. На рис. 4.2 зображено структуру системи контролю результатів синтезу, яка містить блок аналізу властивостей. Але які саме властивості перевіряються не конкретизовано, у тексті роботи лише зазначено "операцій з заданими властивостями".

Зазначимо, що, незважаючи на вказані недоліки та зауваження, запропоноване дисертаційне дослідження справляє позитивне враження та є предметом наукового та практичного інтересу.

**8. Висновок щодо відповідності дисертації вимогам, які висуваються до ступеня доктора філософії.**

Розглянуте дисертаційне дослідження здобувача Рудницької Юлії Володимирівни на тему «Інформаційна технологія моделювання симетричних операцій криптографічного кодування для захищених інформаційних систем критичної інфраструктури» цілком відповідає вимогам до дисертаційного дослідження на здобуття ступеня доктора філософії, наведеним у Постанові Кабінету Міністрів України №44 від 12.01.22 «Про затвердження Порядку присудження ступеня доктора філософії та скасування рішення разової спеціалізованої вченої ради закладу вищої освіти, наукової установи про присудження ступеня доктора філософії». Дисертація може бути представлена для офіційного захисту в разовій спеціалізованій вченій раді. Автор дисертації заслуговує на присудження ступеня доктора філософії за спеціальністю 126 Інформаційні системи та технології галузі знань 12 Інформаційні технології.

**Рецензент**
к.т.н., доцент,
доцент кафедри інформаційної безпеки
та комп'ютерної інженерії,
учений секретар
Черкаського державного
технологічного університету Ірина МИРОНЕЦЬ