ВІДГУК

офіційного опонента,
завідувача кафедри кібербезпеки та програмного забезпечення
Центральноукраїнського національного технічного університету,
доктора технічних наук, професора
Смірнова Олексія Анатолійовича,
на дисертаційну роботу Якименка Ігоря Зіновійовича на тему "Методи та засоби криптографічного захисту інформації на основі системи залишкових класів", подану на здобуття наукового ступеня доктора технічних наук за спеціальністю 05.13.21 – системи захисту інформації

1. Актуальність теми дослідження та зв'язок з науковими програмами, планами та темами

Актуальність дисертації зумовлена тим, що переважна більшість сучасних інформаційно-телекомунікаційних систем потребує не лише криптографічно стійкого, а й високопродуктивних методів під час опрацювання та передавання даних. Водночас підвищення стійкості класичних симетричних та асиметричних криптоалгоритмів традиційно досягається збільшенням довжин ключів і розрядності операндів, що приводить до зниження швидкодії та ускладнює практичну реалізацію й експлуатацію засобів захисту. У дисертації обґрунтовано, що найбільш перспективним шляхом підвищення продуктивності криптоперетворень є розпаралелення обчислень, а природні передумови для цього надає непозиційна система залишкових класів (СЗК).

Додатково актуальність підсилюється тим, що зі зростанням обчислювальних можливостей криптоаналітичні атаки на поширені криптосистеми стають дедалі більш практично реалізованими, що формує запит на нові підходи й алгоритми з кращим співвідношенням «стійкість/швидкодія». У роботі аргументовано поєднання СЗК з поліноміальною арифметикою, як основи побудови нових криптоалгоритмів та використання ієрархічних форм СЗК для оптимізації операцій і зменшення обсягу обчислень. Це напряму відповідає сформульованому в дисертації об'єктивному протиріччю між потребою забезпечення високої криптографічної стійкості при передаванні великих обсягів конфіденційної інформації та необхідністю підвищення швидкодії шифрування/розшифрування.

Отже, тема дисертації є своєчасною та безумовно актуальною науково-прикладною проблемою, оскільки спрямована на розроблення методів, засобів і методології криптографічного захисту на основі цілочисельної, модифікованої досконалої, поліноміальної та ієрархічної СЗК, а також на зниження обчислювальної складності за рахунок реалізації множення/експоненціювання через операції додавання з використанням векторно-модульних алгоритмів.

Дисертаційна робота виконувалась згідно з планами науково-дослідних робіт Західноукраїнського національного університету.

2. **Ступінь обґрунтованості наукових положень, висновків і рекомендацій.**

Отримані результати є обґрунтованими та достовірними, це підтверджується значним обсягом здійснених досліджень, поданим фактичним матеріалом та його науковою інтерпретацією, практичним використанням запропонованих розробок та апробацією на наукових конференціях.

Обґрунтованість і достовірність наукових положень, висновків і рекомендацій забезпечено коректним застосуванням основних положень теорії чисел, теорії алгоритмів та методів криптографії.

Достовірність висновків та рекомендацій підкріплена результатами моделювання, а також відповідними публікаціями.

3. Наукова новизна результатів дослідження.

В дисертаційній роботі виконано теоретичне обґрунтування та отримано рішення актуальної науково-прикладної проблеми підвищення стійкості та ефективності криптосистем шляхом створення нових методів, засобів та методології криптографічного захисту інформації в системі залишкових класів.

Наукова новизна відображена у наступних отриманих результатах, які мають теоретичну цінність:

– вперше розроблено симетричний криптоалгоритм у системі залишкових класів, який за рахунок розбиття відкритого повідомлення на залишки по відповідних попарно взаємнопростих модулях та використання китайської теореми про залишки дозволяє розпаралелити обчислювальний процес;

– вперше розроблено високопродуктивні симетричні та асиметричні криптоалгоритми на основі системи залишкових класів та її модифікованої досконалої форми, які за рахунок довільної заміни базисних чисел в процесі шифрування на попарно взаємнопрості з відповідними модулями додаткові ключі дозволяють підвищити криптостійкість та забезпечити необхідний рівень захисту;

– вперше розроблено криптографічний метод, в якому за рахунок шифрування відкритого тексту у вигляді залишків за допомогою китайської теореми про залишки і розшифрування на основі операції пошуку залишків за відповідними модулями забезпечується підвищення швидкості розшифрування інформації без втрати стійкості алгоритму;

– вперше розроблено одно- та двоключові симетричні криптографічні методи в поліноміальній системі залишкових класів, які за рахунок заміни в процесі шифрування базисних поліномів на довільно вибрані попарно взаємнопрості з модулями поліноми дозволяють створити додаткову структурну неоднозначність, ускладнити криптоаналіз через необхідність розв'язання NP-повної задачі та збільшити криптографічну стійкість;

– вперше розроблено симетричні методи шифрування/розшифрування інформаційних потоків в ієрархічній цілочисельній та поліноміальній системах залишкових класів, які за рахунок представлення зашифрованого тексту наборами залишків за відповідними модулями та розпаралелення процесу обчислень

дозволяють підвищити стійкість криптоалгоритму та збільшити його швидкодію;

– вперше розроблено методологію криптографічного захисту інформації в системі залишкових класів, яка за рахунок застосування векторно-модульних методів модулярного множення та експоненціювання, цілочисельної, модифікованої досконалої форми, поліноміальної та ієрархічної систем залишкових класів дає змогу забезпечити збільшення стійкості, зменшення часової складності, підвищення швидкодії алгоритмів;

– отримав подальший розвиток метод пошуку оберненого полінома в кільці Z[x] на основі методу невизначених коефіцієнтів, який за рахунок усунення операції пошуку найбільшого спільного дільника двох поліномів дозволив зменшити часову складність та підвищити швидкодію алгоритму при його використанні в поліноміальних криптосистемах;

– отримали подальший розвиток поліноміальний, дво- та тримодульний цілочисельні асиметричні криптосистеми Рабіна, які за рахунок заміни операції множення на операцію додавання та використання векторно-модульного методу модулярного множення дозволяють зменшити часову складність криптографічних перетворень і підвищити швидкодію реалізації алгоритмів;

– удосконалено методи відновлення полінома за його залишками в кільці Z[x], які за рахунок використання операції додавання добутку модулів або їх залишків за відповідними модулями дозволяють уникнути обчислювально громіздкої процедури пошуку мультиплікативного оберненого полінома, що призводить до збільшення швидкодії та зменшення часової складності поліноміальних алгоритмів шифрування.

4. Зміст дисертації та відповідність встановленим вимогам

Дисертаційна робота є завершеною науковою працею, яка містить вступ, шість розділів, висновки, список використаних джерел нараховує 331 найменувань та 2 додатки на 35 сторінках. Дисертації має 420 сторінки, з яких 347 містять основний текст. У роботі є 99 рисунків і 65 таблиць.

У *вступі* обґрунтована актуальність наукової проблеми, сформульовані мета та задачі досліджень, визначені об'єкт та предмет досліджень, відображені основні наукові результати, висновки, їх практичне значення та інші кваліфікаційні параметри, згідно з чинним законодавством.

У *першому розділі* виконано аналіз сучасних криптографічних методів захисту інформації: проаналізовано симетричні та асиметричні алгоритми, визначено їх переваги й обмеження, наведено порівняльні характеристики із фокусом на часову складність і стійкість до квантових загроз; встановлено, що «вузьким місцем» асиметричних схем є модулярне множення, експоненціювання та обчислення оберненого елемента. Автором обґрунтовано доцільність застосування СЗК та її форм (у т.ч. ієрархічної/гібридної) завдяки природній паралелізації, роботі з меншими розрядностями та відсутності переносів, а також розглянуто потенціал поліноміальної арифметики в Z[x] для побудови криптоалгоритмів. Сформульовано висновок про потребу нових криптоалгоритмів, які поєднують різні математичні підходи для підвищення ефективності та стійкості

в умовах зростання обчислювальних можливостей і квантових викликів.

У *другому розділі* запропоновано й обґрунтовано удосконалені реалізації асиметричних криптосистем Рабіна та Ель-Гамаля на основі СЗК, де "складні" операції множення/експоненціювання максимально заміщуються операціями додавання та ефективними векторно-модульними процедурами.

Для тримодульної криптосистеми Рабіна запропоновано використовувати векторно-модульний метод модулярного множення, що дає змогу замінити модулярне множення додаванням відібраних компонент.

Для етапу розшифрування Рабіна запропоновано: 1) метод пошуку квадратного кореня за модулем, який спирається на додавання та перевірку "повного квадрата"; 2) розв'язання систем конгруенцій методом додавання добутку модулів як менш складну альтернативу КТЗ/алгоритму Гарнера.

Проведено аналітичне порівняння часових складностей і показано, що запропоноване удосконалення для тримодульного Рабіна оптимізує обчислення, в результаті отримуємо перехід від кубічної до квадратичної складності.

Запропоновано концепцію спільного застосування СЗК з векторно-модульним алгоритмом модулярного експоненціювання, де складні множення багаторозрядних чисел замінюються додаванням і табличним пошуком.

У *третьому розділі* сформовано теоретичну основу побудови симетричних і асиметричних криптоалгоритмів у СЗК. Розроблено підходи до формування наборів модулів однакової розрядності в МДФ СЗК, проаналізовано їх властивості та показано закономірності, що дають змогу раціональніше використовувати розрядну сітку при реалізації. На цій базі запропоновано принципи побудови криптоперетворень у СЗК, де основну роль відіграють вибір модулів і структура представлення даних у вигляді залишків.

Розроблено симетричні методи шифрування в СЗК і МДФ СЗК, а також окремий симетричний підхід на основі КТЗ із розбиттям блоку на підблоки та відновленням даних через операції з залишками. Проведено оцінювання криптостійкості й складності криптоаналізу на основі теореми розподілу простих чисел і функції Ейлера; встановлено, як кількість модулів і їх розрядність впливають на рівень захисту та обчислювальну складність атак, а також отримано аналітичні залежності й графічні ілюстрації цих зв'язків.

Запропоновано асиметричні криптоалгоритми на основі СЗК і МДФ СЗК, у яких системи модулів трактуються як секретні параметри, а відкриті ключі реалізуються через коефіцієнти відновлення, що забезпечує додатковий запас стійкості при зростанні розрядності та кількості модулів.

Четвертий розділ присвячений розробці теоретичних засад поліноміальних криптографічних перетворень у кільці Z[x] та в поліноміальній СЗК. Запропоновано новий підхід до знаходження оберненого полінома за модулем на основі методу невизначених коефіцієнтів і виконано порівняння з класичними методами, що спираються на алгоритм Евкліда. Показано, що усунення процедури пошуку НСД поліномів дає відчутний виграш у часовій ефективності; отримано аналітичні оцінки та графічні залежності, які демонструють зростання ефективності зі збільшенням степенів поліномів.

Також запропоновано методи відновлення полінома за його залишками, які базуються на операціях додавання добутків модулів/залишків і дозволяють розпаралелити обчислення та уникнути обов'язкового пошуку мультиплікативного оберненого полінома (на відміну від підходів типу Гарнера). Обґрунтовано, що такі методи зменшують часову складність і знижують "важкість" проміжних операцій, а їх ефективність логарифмічно зростає зі степенями поліномів, хоча зменшується зі збільшенням кількості модулів.

Розроблено поліноміальні криптоалгоритми і виконано оцінювання їх криптостійкості. Показано, що криптоаналіз запропонованих поліноміальних алгоритмів має комбінаторний характер і може зводитися до NP-повних задач, а рівень стійкості істотно залежить від параметрів поліномів і поля Галуа та оптимального вибору кількості модулів. Обґрунтовано перспективність поліноміальної СЗК як основи для нових високостійких і водночас придатних до обмежених ресурсів криптографічних рішень.

У *п'ятому розділі* розроблено теоретичні основи ієрархічних симетричних криптоалгоритмів у СЗК. Запропоновано симетричний алгоритм на базі ієрархічної СЗК з багаторівневою структурою, яка дає змогу на кожному рівні зменшувати розрядність модулів і гнучко керувати співвідношенням "захищеність/швидкодія" через вибір кількості рівнів, модулів та їх розрядностей. Проведено експериментальне дослідження та показано, що стійкість алгоритму зростає зі збільшенням кількості модулів, їх розрядності та рівнів ієрархії; виконано порівняння з AES-256 і визначено параметричні області, де запропонований підхід забезпечує співмірний рівень криптостійкості при більшій варіативності налаштувань.

Запропоновано ієрархічний поліноміальний симетричний криптоалгоритм у поліноміальній СЗК: відкритий текст подається поліномом із коефіцієнтами-символами, секретні ключі задаються системою незвідних поліномів, а шифрування реалізується через обчислення залишків за цими модулями. Ступінчасте зменшення порядку поліномів-модулів на кожному рівні знижує обчислювальні витрати та забезпечує адаптивний підбір параметрів під потрібний рівень захисту.

Сформовано методологію криптографічного захисту в СЗК, яка об'єднує цілочисельну, МДФ та поліноміальну СЗК в єдиний підхід до проєктування й оптимізації симетричних та асиметричних рішень. Методологія включає застосування векторно-модульних процедур для основних операцій, а також ефективні поліноміальні методи (зокрема для оберненого елемента та відновлення за залишками), що разом дозволяє досягати високого рівня захисту за мінімальних обчислювальних витрат.

У *розділі шість* виконано програмну реалізацію симетричних і асиметричних криптоалгоритмів, що підтвердило їх працездатність, коректність і практичну придатність для застосування. Реалізоване ПЗ показало ефективність використання СЗК у процесах шифрування/дешифрування за рахунок декомпозиції обчислень і природної паралелізації, що забезпечує прискорення ключових процедур.

Реалізовано алгоритми для ієрархічної СЗК та поліноміальної СЗК і підтверджено можливість масштабування параметрів (кількість рівнів, модулів,

розрядність) для адаптації під задані вимоги безпеки й продуктивності. Практичні експерименти засвідчили, що поєднання векторно-модульного представлення з підходами, де дорогі операції оптимізуються, зменшує часову складність криптографічних перетворень; також перевірено працездатність методів відновлення та знаходження обернених поліномів у поліноміальних криптопроцедурах.

Результати розділу підтверджують, що створене ПЗ є ефективним, масштабованим і придатним до інтеграції в прикладні системи захисту інформаційних потоків із підвищеними вимогами до швидкодії та стійкості.

У *висновках* сформульовано основні наукові результати.

Сформульовані у роботі висновки повною мірою представляють отримані у дисертаційному дослідженні результати, мають належний науковий рівень та відповідають вимогам до результатів докторської дисертації. Дисертаційна робота має завершену обґрунтовану структуру, що повною мірою розкриває досягнуту мету та виконані завдання дослідження.

У *додатках* наведені документи, що підтверджують впровадження результатів дисертаційної роботи та код основних програмних модулів.

5. Оформлення дисертації та автореферату

Автореферат в повному обсязі відображає основні наукові результати дисертаційної роботи, практичну значущість та висновки.

Дисертаційна робота та автореферат оформлені у відповідності з чинними вимогами, що ставляться до докторських дисертаційних робіт. Дисертаційна. Робота має завершену обґрунтовану структуру та форму представлення, що повною мірою розкриває досягнуту мету та виконані завдання дослідження.

Результати кандидатської дисертації в докторській дисертації не використовувались.

6. Практичне значення результатів дисертаційної роботи

Практичне значення одержаних результатів полягає в розробленні та програмній реалізації комплексу алгоритмічних і програмних засобів для симетричних і асиметричних криптоперетворень у системі залишкових класів, зокрема для дво- та тримодульної криптосистеми Рабіна, криптосистеми Ель-Гамаля та ієрархічного симетричного криптоалгоритму, із застосуванням векторно-модульних методів множення й експоненціювання та розпаралелення обчислень, що забезпечило суттєве зниження часової складності й підвищення швидкодії шифрування/дешифрування порівняно з традиційними підходами; отримані переваги підтверджено емпірично, що створює підґрунтя для впровадження розроблених рішень у інформаційні системи та багаторівневі системи захисту даних, а також для практичного використання програмного забезпечення симетричного шифрування в поліноміальній СЗК із можливістю адаптивного налаштування параметрів і спрощенням пояснення складних процедур шифрування.

7. Повнота викладення основних результатів дисертаційної роботи в опублікованих працях

Основні результати дисертації з достатньою повнотою відображено в 61 науковій праці, з яких 5 колективних монографій, 26 публікацій у наукових фахових виданнях України та закордонних виданнях, в тому числі 11 статей включено в наукометричні бази Scopus та/або Web of Science (з них три статті віднесено до квартилю Q2, чотири – до квартилю Q3 та одна – до квартилю Q4), 2 патенти на корисну модель. Одна стаття, розділ монографії і одні тези написані автором одноосібно. Результати апробовано на науково-технічних конференціях, що зафіксовано в 29 опублікованих тезах та доповідях конференцій. Аналіз внеску автора в публікації по питаннях, висвітлених в дисертації, показав, що внесок Ігоря Якименка ***є вирішальним***.

8. Зауваження до дисертаційної роботи та автореферату

1. У таблиці 1.12 "квантову стійкість" подано загальними словами «підвищена/ найвища /вразливий» без пояснення критерію та моделі загрози. У рядку «Крипто-стійкість» наведені значення для AES/DES/3DES, але для запропонованих криптосистем на основі СЗК відповідні клітинки заповнені формулами – відповідно ускладнюється порівняння.
2. У тексті роботи зустрічаються кількісні висновки про перевищення стійкості AES-256, однак такі твердження потребують строгого визначення метрики порівняння.
3. Опис окремих процедур розшифрування потребує уточнення: наприклад, розв'язання систем порівнянь через "додавати модуль p стільки разів…" і далі "додавати добуток pq…" – це по суті лінійний пошук, який для великих модулів може бути досить складним (пункт 2.3).
4. Запропонована ітеративна процедура пошуку оберненого елемента "послідовним додаванням" потребує додаткового обґрунтування, так як без оцінки очікуваної кількості кроків вона може бути складнішою за використання розширеного алгоритму Евкліда.
5. В пункті 3.5 Асиметричні алгоритми шифрування у системі залишкових класів зазначено, що обидва абоненти мають вибрати системи модулів, відомі тільки їм обом – тобто є попередньо узгоджений секрет, що робить схему близькою до симетричної й піднімає питання розповсюдження ключів.
6. Поміняні позначеннями параметрів (сторінка 145) (k і l): спочатку вказано, що *l* – розрядність модулів, k – кількість модулів, але далі написано «при кількості модулів l=5… з розрядностями k=139…».
7. Доцільно було більше уваги приділити опису методики проведення експериментів.
8. Уроботі зустрічаються описки, орфографічні та граматичні помилки.

Незважаючи на вказані зауваження та недоліки, загалом оцінка дисертації позитивна.

9. Загальні висновки

Дисертаційна робота Ігоря Якименка на тему "Методи та засоби криптографічного захисту інформації на основі системи залишкових класів", яка подана на здобуття наукового ступеня доктора технічних наук за спеціальністю 05.13.21 – системи захисту інформації, є завершеною науковою працею, в якій. Вирішено важливу науково-прикладну проблему яка полягає в розробці методів, засобів та методології криптографічного захисту інформації в системі залишкових класів, які забезпечують підвищення рівня стійкості та ефективності криптосистем.

Автореферат дисертаційної роботи відповідає змісту дисертації та відображає його в повному обсязі. Ознаки академічного плагіату в роботі відсутні.

Опубліковані Ігорем Якименком наукові праці за темою дослідження повністю відображають основні положення дисертації та пройшли необхідну апробацію.

Зміст роботи, виконані дослідження та отримані результати відповідають паспорту спеціальності 05.13.21 – системи захисту інформації.

Зважаючи на актуальність дисертаційного дослідження, новизну теоретичних положень, практичну цінність результатів, рівень висвітлення результатів дослідження в публікаціях, вважаю, що дисертаційна робота відповідає вимогам щодо дисертацій на здобуття наукового ступеня доктора наук, зокрема, пп. 6, 7, 8, 9 «Порядку присудження та позбавлення наукового ступеня доктора наук» затвердженого Постановою Кабінету Міністрів України № 117 від 17 липня 2021 р., а її автор, Якименко Ігор Зіновійович, заслуговує на присудження йому наукового ступеня доктора технічних наук за спеціальністю 05.13.21 – системи захисту інформації.

ОФІЦІЙНИЙ ОПОНЕНТ

Завідувач кафедри кібербезпеки та програмного забезпечення
Центральноукраїнського національного технічного університету
доктор технічних наук професор Олексій СМІРНОВ

«09» 02 2026 р.

Підпис офіційного опонента доктора технічних наук професора Смірнова Олексія Анатолійовича засвідчую:
Проректор з наукової роботи та міжнародних зв'язків
Центральноукраїнського національного технічного університету,
кандидат технічних наук, доцент Андрій ТИХИЙ