Голові спеціалізованої вченої ради
Д 26.861.05 при Державному університеті
інформаційно-комунікаційних технологій
03110, Україна, м. Київ, вул. Солом'янська,
7

ВІДГУК

офіційного опонента доктора технічних наук, професора,
завідувача кафедри кібербезпеки, Національного технічного університету
«Харківський політехнічний інститут» Євсеєва Сергія Петровича
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

Постійне зростання обсягів передавання, обробки та зберігання даних, поширення розподілених, хмарних і вбудованих систем, а також підвищені вимоги до швидкодії й енергоефективності обчислень зумовлюють необхідність пошуку нових математичних підходів до побудови криптографічних алгоритмів.

Особливої ваги в цьому контексті набуває використання системи залишкових класів (СЗК) як альтернативного математичного апарату, що дозволяє реалізувати парадигму побудови криптографічних перетворень на принципах паралелізму, модульності, реконфігурованості та підвищеної функціональної стійкості.

Водночас використання СЗК у криптографії вимагає розроблення нових методів і засобів побудови криптографічних алгоритмів, формалізації процедур виконання базових операцій, оцінювання обчислювальної складності, забезпечення криптографічної стійкості та коректності перетворень у цілочисельних і поліноміальних кільцях. Це зумовлює необхідність створення теоретично обґрунтованих і практично орієнтованих рішень, здатних забезпечити ефективний захист інформації в сучасних умовах.

Аналіз наукових праць свідчить, що питання побудови цілісної методології криптографічного захисту інформації на основі цілочисельної, поліноміальної та ієрархічних СЗК, розроблення ефективних симетричних і асиметричних криптоалгоритмів, а також методів, які дають змогу знизити часову складність

основних криптографічних операцій залишаються недостатньо дослідженими та потребують подальшого розвитку.

Отже, дисертаційна робота Якименка Ігоря Зіновійовича, яка присвячена розробленню методів і засобів криптографічного захисту інформації на основі цілочисельної, модифікованої досконалої форми, поліноміальної та ієрархічної СЗК є важливою, актуальною та своєчасною.

2. Зв'язок роботи з науковими програмами, темами

Дисертаційна робота виконувалася відповідно до плану науково-дослідних робіт кафедр комп'ютерної інженерії, спеціалізованих комп'ютерних систем та кібербезпеки Західноукраїнського національного університету: «Паралельні методи та засоби реалізації алгоритмів захисту інформації в комп'ютерних мережах з використанням математичного апарату еліптичних кривих» (номер державної реєстрації 0109U000035), «Опрацювання багаторозрядних чисел в системі залишкових класів» (номер державної реєстрації 0115U001607), «Розробка теоретичних засад методів формування та цифрового опрацювання даних у розподілених спеціалізованих комп'ютерних системах» (номер державної реєстрації 0112U008458), «Теоретичні основи та апаратні засоби підвищення продуктивності роботи безпровідних сенсорних мереж» (номер державної реєстрації 0117U000414), «Виконання завдань Перспективного плану розвитку наукового напряму "Технічні науки" Західноукраїнського національного університету. Розробка методів та алгоритмів захищеного зберігання даних» (номер державної реєстрації 0121U114705), «Методи, алгоритми та засоби надійного захищеного зберігання даних на основі модулярних коригуючих кодів» (номер державної реєстрації 0118U003182), «Розробка алгоритмів надійного розподіленого зберігання даних на основі модулярних коригуючих кодів» (номер державної реєстрації 0118U100457), «Стійкі до криптоаналізу методи та засоби шифрування в поліноміальних системах» (номер державної реєстрації 0123U104713).

3. Ступінь обґрунтованості наукових положень, висновків і рекомендацій

Представлена на розгляд дисертаційна робота Якименка Ігоря Зіновійовича відзначається високим ступенем наукової обґрунтованості та характеризується послідовною і логічно побудованою структурою. Автор спирається на ґрунтовний аналіз результатів досліджень вітчизняних і зарубіжних науковців, присвячених проблемам криптографічного захисту інформації, теорії чисел, модульної арифметики та застосуванню СЗК у сучасних криптографічних перетвореннях.

Усі наукові положення, висновки та рекомендації, сформульовані в дисертації, базуються на строгому математичному апараті, коректно виведених аналітичних залежностях та узгоджуються з відомими теоретичними результатами. Достовірність отриманих результатів підтверджується проведеним аналізом обчислювальної складності запропонованих методів і алгоритмів, а також результатами чисельних і програмних експериментів.

Загалом ступінь обґрунтованості наукових положень, висновків і рекомендацій, викладених у дисертаційній роботі, не викликає сумнівів і свідчить про високий рівень виконаного дослідження.

Достовірність наукових положень, висновків і рекомендацій, наведених у дисертаційній роботі, підтверджується доцільністю та коректністю застосування математичного апарату теорії чисел і модульної арифметики, методів алгоритмічного аналізу, а також засобів комп'ютерного та імітаційного моделювання криптографічних перетворень. Отримані результати ґрунтуються на строгих теоретичних викладках і узгоджуються з відомими положеннями сучасної криптографії.

Достовірність наукових висновків також забезпечується коректним формулюванням мети та завдань дослідження і їх відповідністю реальним умовам застосування криптографічних систем; використанням достатнього обсягу експериментальних даних, отриманих у процесі програмного моделювання та чисельних експериментів, а також порівнянням результатів, отриманих із застосуванням запропонованих методів, з відомими методами.

Крім того, практична значущість і достовірність отриманих результатів підтверджується їх впровадженням у практичну діяльність, що засвідчено відповідними актами про впровадження, наведеними в додатках до дисертаційної роботи.

4. Наукова новизна отриманих результатів

Вперше розроблено симетричний криптоалгоритм у системі залишкових класів, який за рахунок розбиття відкритого повідомлення на залишки по відповідних попарно взаємнопростих модулях (ключах) та використання китайської теореми про залишки дозволяє розпаралелити обчислювальний процес, зменшити розмірність операндів та на основі побудованих аналітичних виразів встановити розрядність та кількість модулів системи залишкових класів для забезпечення такої ж стійкості, як і сучасний симетричний криптоалгоритм AES-256.

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 інформаційних потоків.

Вперше розроблено криптографічний алгоритм, 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 (ключами) 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, спеціалізованого програмного забезпечення та побудувати єдину стратегію криптографічного захисту інформаційних потоків на основі системи залишкових класів.

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 алгоритми шифрування 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, в свою чергу, призводить до збільшення швидкодії та зменшення часової складності поліноміальних алгоритмів шифрування.

4. Практичне значення результатів роботи

Розроблено алгоритмічне та програмне забезпечення для дво- і тримодульної криптосистеми Рабіна та криптосистеми Ель-Гамаля на СЗК із застосуванням векторно-модульного методу, що суттєво зменшило часову складність криптографічних операцій.

Реалізовано симетричні та асиметричні криптоалгоритми в СЗК, що підтвердило ефективність запропонованих методів і дозволяє їх впровадження у сучасні інформаційні системи.

Створено програмне забезпечення для ієрархічного та поліноміального симетричного шифрування в СЗК, яке забезпечує високу швидкодію та адаптивне налаштування параметрів, зручне для практичного використання.

Результати досліджень впроваджені або плануються до впровадження (підтверджено відповідними актами) в Акціонерному товаристві «Тернопільобленерго» (№5291/24 від 17.12.2025 р.), ТзОВ НВФ «Інтеграл» (№03-07/2025 від 07.03.2025 р.), ТзОВ завод «Рempобуттехніка» (№ЦКБ/04-25 від 10.02.2025 р.), Управлінні кібербезпеки та цифрового розвитку відділу цифрової трансформації Міністерства енергетики України, Департаменті Бюро економічної безпеки України (від 12.01.2025 р.), використані при виконанні п'яти науково-дослідних робіт у Західноукраїнському національному університеті (ЗУНУ) (від 05.12.2025 р.), у навчальному та науковому процесах факультету комп'ютерних інформаційних технологій ЗУНУ (від 5.09.2025 р.).

5. Повнота викладу результатів у наукових публікаціях та апробація

За результатами досліджень, які викладені в дисертації, опубліковано 61 наукову працю, серед яких розділи у 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, відповідно до класифікації SCImago Journal and Country Rank або Journal Citation Reports, три статті віднесено до квартилю Q2, три – до квартилю Q3 та одна – до квартилю Q4) та 28 публікацій у матеріалах міжнародних та всеукраїнських конференцій (з них 22 публікації включено в наукометричні бази Scopus та/або Web of Science), 2 патенти на корисну модель. Одна стаття, розділ монографії і одні тези написані автором одноосібно.

Опубліковані роботи в повній мірі охоплюють основні результати дисертаційних досліджень.

6. Оформлення дисертації та автореферату

За своїм змістом дисертація Якименка І.З. відповідає діючим вимогам щодо дисертацій на здобуття наукового ступеня доктора наук і являє собою наукову працю, яка містить сукупність наукових положень та результатів, виставлених автором для публічного захисту, має внутрішню єдність і свідчить про особистий внесок автора у науку. Оформлення дисертації відповідає вимогам Державних стандартів України. Текст дисертації написаний грамотною технічною мовою, ясно та зрозуміло.

7. Відповідність дисертаційної роботи вимогам спеціальності та нормативним документам

Зміст дисертаційної роботи повністю відповідає паспорту спеціальності 05.13.21 – Системи захисту інформації, зокрема таким його пунктам: «Математичні моделі інформаційних структур, що потребують захисту, шифрів, шифросистем та криптографічних протоколів»; «Шифри, шифросистеми, криптографічні протоколи та способи вибору систем криптозахисту, адекватних прийнятій політиці безпеки інформації»; «Математичні й обчислювальні методи розрахунку надійності криптосистем, прогнозування оцінок криптографічної стійкості, розв'язання завдань криптографічного аналізу та синтезу шифросистем і криптографічних протоколів», профілю спеціалізованої вченої ради Д 26.861.05 та основним положенням дисертації та відображає її основний зміст, наукові та практичні результати. Підтверджую **відсутність академічного плагіату, фабрикації, фальсифікації** у дисертації та авторефераті Якименко І.З.

8. Недоліки та зауваження.

1. У дисертаційній роботі значну увагу приділено теоретичному обґрунтуванню криптографічних алгоритмів на основі цілочисельної,

поліноміальної та ієрархічної СЗК і дослідженню стійкості до криптоаналітичних атак. Водночас доцільним було б більш детально розглянути питання стійкості запропонованих криптосхем до сучасних атак побічними каналами (time-based, power analysis), що є актуальним для практичних реалізацій у вбудованих та апаратно-орієнтованих системах.

2. У п.п. 5.3–5.4 дисертації, та на сторінки 22 (рис. 8), присвячених аналізу обчислювальної складності криптографічних перетворень, основний акцент зроблено на асимптотичних оцінках часової складності. Разом з тим, порівняльний аналіз використання пам'яті та вимог до апаратних ресурсів для різних варіантів реалізації алгоритмів у СЗК подано фрагментарно і міг би бути розширений. Також не зрозуміло чому не використовувались програмні застосунки оцінки криптостійкості, наприклад NIST STS 822, який забезпечує оцінки випадковості сформованих криптограм не залежно від алгоритму шифрування.

3. Програмна реалізація розроблених криптоалгоритмів детально описана з точки зору архітектури та функціональних можливостей (п.п. 6.1 (стор. 275–276), автореферат стор. 29, рис. 13). Проте в роботі обмежені результати тестування програмного забезпечення в умовах великих обсягів даних або реального навантаження, що могло б додатково підтвердити практичну ефективність запропонованих рішень. Також не наведені данні щодо оцінки обчислювальної складності та енергетичної ємності запропонованих рішень. Крім того не має визначення рівня безпеки за класифікацією НІСТ США у постквантовий період для запропонованих криптоалгоритмів.

4. У дисертації наведено ґрунтовний аналіз класичних криптографічних алгоритмів і методів на основі системи залишкових класів. Водночас порівняння із сучасними постквантовими криптографічними підходами здійснено переважно на концептуальному рівні і могло б бути доповнене кількісними експериментальними показниками.

5. У дисертаційному дослідженні значна увага приділяється використанню модифікованої досконалої форми системи залишкових класів, як базису для побудови асиметричних криптосистем. Проте з наукової та практичної точок зору, роботу можна було б суттєво посилити шляхом проведення порівняльного аналізу та розгляду можливості застосування інших форм системи залишкових класів. Наприклад, поліноміальна системи залишкових класів у полях Галуа або системи зі спеціальним набором модулів виду 2^n-1, 2^n, 2^n+1, які мають свої унікальні властивості щодо швидкодії виконання модульних операцій. Автор міг би

обґрунтувати, чому саме МДФ є оптимальною у порівнянні з цими альтернативами для реалізації асиметричних протоколів.

6. У переліку напрямів подальших досліджень варто було б більш чітко сформулювати можливості використання запропонованих методів у сучасних кіберфізичних системах та розподілених середовищах, зокрема в умовах обмежених обчислювальних ресурсів.

7. Безумовно розроблення нових методів і засобів криптографічного захисту інформації на основі цілочисельної, модифікованої досконалої форми, поліноміальної та ієрархічної дозволяє підвищенні ефективність захисту інформаційних потоків на основі заміни в алгоритмах шифрування операції множення операцією додавання, використання цілочисельної, МДФ, поліноміальної та ієрархічної системи залишкових класів для розробки нових криптографічних алгоритмів. Але автору слід було звернути увагу і на економічну складову отриманих результатів. У роботі не має їх вартісного аналізу, техніко економічного обґрунтування вирішення практичних задач впровадження нових методів і засобів криптографічного захисту інформації.

Вказані зауваження і недоліки не впливають на загальну позитивну оцінку виконаного дисертаційного дослідження та не зменшують її наукову новизну та практичну значущість і не знижують загального позитивного сприйняття проведеного обсягу досліджень.

9. Загальна оцінка роботи, її відповідність встановленим вимогам

Дисертаційна робота Якименка Ігоря Зіновійовича на тему «Методи та засоби криптографічного захисту інформації на основі системи залишкових класів» є завершеною кваліфікаційною науковою роботою, яка містить нові науково обґрунтовані положення, які в сукупності вирішують актуальну науково-прикладну проблему розробки методів, засобів та методології криптографічного захисту інформації на основі цілочисельної, модифікованої досконалої форми, поліноміальної та ієрархічної систем залишкових класів, що забезпечить підвищення рівня стійкості та ефективності криптосистем.

Вважаю, що за актуальністю, повнотою досліджень, науковою новизною, практичною цінністю одержаних результатів дисертаційна робота відповідає вимогам «Порядку присудження та позбавлення наукового ступеня доктора наук», затвердженого постановою Кабінету Міністрів України від 17 листопада 2021 року №1197 та вимогами до опублікування результатів дисертацій на здобуття наукових ступенів доктора і кандидата наук, затвердженим Наказом Міністерства освіти і науки України від 23.09.2019 року №1220 «Про опублікування результатів

дисертацій на здобуття наукових ступенів доктора і кандидата наук» (зі змінами внесеними Наказом МОН України від 27.05.2022 № 496), а її автор, Якименко Ігор Зіновійович, заслуговує на присудження наукового ступеня доктора технічних наук за спеціальністю 05.13.21 – «Системи захисту інформації».

Офіційний опонент:
доктор технічних наук, професор,
Лауреат національної премії ім. Бориса Патона,
завідувач кафедри кібербезпеки,
Національний технічний університет
«Харківський політехнічний інститут» Сергій ЄВСЕЄВ