ЗАТВЕРДЖУЮ:

Перший проректор Державного університету інформаційно-комунікаційних технологій

_____ Олександр КОРЧЕНКО

«20» 11 2025 р.

ВИСНОВОК

про наукову новизну, теоретичне та практичне значення результатів дисертаційної роботи Якименка Ігоря Зіновійовича на тему «Методи та засоби криптографічного захисту інформації на основі системи залишкових класів», поданої на здобуття наукового ступеня доктора технічних наук за спеціальністю 05.13.21 «Системи захисту інформації»

Актуальність теми дослідження.

Актуальність роботи викликана тим, що на сучасному етапі розвитку науки і в процесі функціонування криптографічних методів захисту існує таке об'єктивне протиріччя між потребою забезпечення високої криптографічної стійкості та передавання великих обсягів конфіденційної інформації, з одного боку, та забезпечення підвищення швидкодії процесу шифрування/розшифрування.

Враховуючи викладене, актуальною науково-технічною проблемою є підвищення ефективності захисту інформаційних потоків на основі заміни в алгоритмах шифрування операції множення операцією додавання, використання цілочисельної, модифікованої досконалої форми, поліноміальної та ієрархічної систем залишкових класів для розробки нових криптографічних алгоритмів, яка виникає в результаті об'єктивного протиріччя між потребою забезпечення високої криптографічної стійкості та передавання великих обсягів конфіденційної інформації, з одного боку, та забезпечення підвищення швидкодії процесу шифрування/розшифрування.

Достовірність та наукова новизна одержаних результатів.

Достовірність одержаних результатів підтверджуються строгою постановкою задач, вибором адекватних експерименту граничних умов і методів розв'язку, зрозумілим трактуванням основних положень і висновків, співпаданням деяких результатів з результатами робіт інших авторів у серії граничних випадків, позитивними рецензіями опублікованих статей і представлених на різних конференціях доповідей.

Зв'язок роботи з науковими програмами, планами, темами.

Дисертаційна робота виконувалася у рамках таких науково-дослідних держбюджетних та госпдоговірних 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» (Державний реєстраційний номер 0109U000035), «Опрацювання багаторозрядних чисел в системі залишкових класів» (Державний реєстраційний номер 0115U001607), «Розробка теоретичних засад методів формування та цифрового опрацювання даних у розподілених спеціалізованих комп'ютерних системах» (Державний реєстраційний номер 0112U008458), «Теоретичні основи та апаратні засоби підвищення продуктивності роботи безпровідних сенсорних мереж» (Державний реєстраційний номер 0117U000414), «Виконання завдань Перспективного плану розвитку наукового напряму "Технічні науки" Західноукраїнського національного університету. Розробка методів та алгоритмів захищеного зберігання даних» (Державний реєстраційний номер 0121U114705), «Методи, алгоритми та засоби надійного захищеного зберігання даних на основі модулярних коригуючих кодів» (Державний реєстраційний номер 0118U003182), КБ №86-2018 «Розробка алгоритмів надійного розподіленого зберігання даних на основі модулярних коригуючих кодів» (Державний реєстраційний номер 0118U100457), КБ №49-2023 «Стійкі до криптоаналізу методи та засоби шифрування в поліноміальних системах» (Державний реєстраційний номер 0123U104713).

Мета і завдання дослідження.

Метою дисертаційної роботи є підвищення рівня стійкості та ефективності криптосистем шляхом створення нових методів, засобів та методології криптографічного захисту інформації в системі залишкових класів.

Для досягнення поставленої мети у дисертаційній роботі необхідно розв'язати низку взаємопов'язаних задач:

1) проаналізувати сучасні методи, алгоритми та засоби захисту інформаційних потоків з метою визначення перспектив підвищення їх

стійкості на основі використання різних форм СЗК та поліноміальних систем числення;

2) удосконалити та підвищити ефективність алгоритмічного забезпечення для реалізації асиметричних криптосистем Рабіна та Ель-Гамаля на основі операції додавання та векторно-модульного алгоритму модулярного множення та експоненціювання;

3) удосконалити та підвищити ефективність методів пошуку оберненого полінома за модулем та відновлення полінома за його залишками на основі методу невизначених коефіцієнтів;

4) розробити симетричний та асиметричний криптографічні алгоритми в СЗК та дослідити їх стійкість до криптоаналітичних атак;

5) розробити криптографічний одноключовий та двоключовий алгоритми в поліноміальній СЗК та дослідити їх стійкість;

6) розробити ієрархічний цілочисельний та поліноміальний криптографічні алгоритми на основі СЗК та дослідити їх стійкість;

7) розробити алгоритмічне та програмне забезпечення запропонованих методів шифрування;

8) розробити методологію криптографічного захисту інформації на основі заміни в алгоритмах шифрування операції множення операцією додавання, з використанням цілочисельної, модифікованої досконалої форми, поліноміальної та ієрархічної систем залишкових класів для розробки нових криптографічних алгоритмів.

Об'єкт дослідження – процеси шифрування інформаційних потоків на основі системи залишкових класів.

Предмет дослідження – методи та засоби криптографічного захисту інформації на основі цілочисельної та поліноміальної систем залишкових класів.

Методи дослідження.

Проведені дослідження ґрунтуються на застосуванні математичних основ алгебри і теорії чисел (для розробки методів пошуку оберненого полінома, відновлення полінома за його залишками, реалізації китайської теореми про залишки (КТЗ)), теорії алгоритмів (для оцінки стійкості відомих та розроблених методів), методах криптографії (для розробки тримодульної криптосистеми Рабіна, векторно-модульної криптосистеми Ель-Гамаля), програмуванні (для реалізації симетричних, асиметричних цілочисельних криптоалгоритмів в СЗК та симетричних криптоалгоритмів в поліноміальній СЗК), теорії множин (для побудови методології захисту інформаційних потоків на основі цілочисельної та поліноміальної СЗК), статистиці (для обробки експериментальних результатів).

Наукова новизна одержаних результатів полягає у наступному:

1) 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;

2) 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;

3) 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;

4) 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;

5) 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;

6) 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;

7) 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;

8) 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;

9) 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.

Нові науково обгрунтовані положення прикладні рекомендації і висновки проведених досліджень схвалені та прийняті до впровадження в Акціонерному товаристві «Тернопільобленерго» (№5291/24 від 17.12.2025 р.), ТзОВ НВФ «Інтеграл» (№03-07/2025 від 07.03.2025 р.), ТзОВ завод «Рембутехніка» (№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.).

В роботі фактів академічного плагіату, фабрикації, фальсифікації не виявлено.

Апробація результатів дисертації.

Основні результати дисертаційної роботи доповідались і обговорювались на таких міжнародних та всеукраїнських конференціях, школах, семінарах, як: International Conference on Advanced Computer Information Technologies (2025, 2024, 2023, 2022, 2021, 2020, 2018 роки), Intelligent Information Technologies and Systems of Information Security (2021 рік), International Conference on Computer Sciences and Information Technologies (CSIT) (2020 рік), Conference on Computer Science and Information Technologies (2020 рік), International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (2020, 2018, 2016 роки), IEEE

International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS) (2019, 2017, 2015, 2012 роки), VI Всеукраїнська школа-семінар молодих вчених і студентів «Сучасні комп'ютерні інформаційні технології» (ACIT) (2018 рік), Науково-технічна конференція «Інформаційні моделі, системи та технології» (2018 рік), Міжнародна науково-технічна конференція молодих учених та студентів «Актуальні задачі сучасних технологій» (2018 рік), International Conference The Experience of Designing and Application of CAD Systems in Microelectronics (CADSM) (2017, 2015 роки), Міжнародна науково-технічна конференція ITSec-2025 Безпека інформаційних технологій (2025, 2024 роки), International Conference on Control, Automation and Systems (ICCAS–2016) (2016 рік), Міжнародна науково-практична конференція «Сучасні інформаційні та електронні технології» (2014 рік).

Наукові праці, в яких опубліковані основні наукові результати дисертації:

Статті:

1. Yakymenko I., Kasianchuk M., Martyniuk O., Martyniuk S. A Symmetric Cryptoalgorithm Based on a Hierarchical Residue Number System. International Journal of Computing, 2025. 24(1), pp. 92-101. https://doi.org/10.47839/ijc.24.1.3880 (Scopus)
2. Yakymenko I., Karpinski M., Shevchuk R., Kasianchuk M. Symmetric Encryption Algorithms in a Polynomial Residue Number System. Journal of Applied Mathematics., 2024, pp. 1-12. DOI:10.1155/2024/4894415 (Scopus).
3. Nykolaychuk Ya., Yakymenko I., Vozna N., Kasianchuk M. Residue Number System Asymmetric Cryptoalgorithms. Cybernetics and Systems Analysis. 2022, Vol. 58, No. 4, P.611-618. http://jnas.nbuv.gov.ua/article/UJRN-0001335526. https://doi.org/10.1007/s10559-022-00494-7. (Scopus).
4. Shevchuk R., Yakymenko I., Karpinski M., Shylinska I., Kasianchuk M. Finding the inverse of a polynomial modulo in the ring Z[x] based on the method of undetermined coefficients. Computer Science. vol. 25. no. 2. 2024. pp.1-14. DOI:10.7494/csci.2024.25.2.5740 (Scopus).
5. M. M. Kasianchuk, I. Z. Yakymenko, Ya. M. Nykolaychuk Symmetric Cryptoalgorithms in the Residue Number System. Cybernetics and Systems Analysis, 2021, Vol 57, Issue 2, p.184-189. https://doi.org/10.1007/s10559-021-00358-6
6. Nykolaychuk Ya., Kasianchuk M., Yakymenko I. Theoretical Foundations of the Modified Perfect form of Residue Number System. Cybernetics and Systems Analysis. 2016. Vol. 52, №2. pp. 219-223 (Scopus). DOI: 10.1007/s10559-016-9817-2
7. Nykolaychuk Ya., Kasianchuk M., Yakymenko I. Theoretical Foundations for the Analytical Computation of Coefficients of Basic Numbers of

Krestenson's Transformation. Cybernetics and Systems Analysis. 2014. Vol. 50, № 5. pp. 649-654 (Scopus). DOI: 10.1007/s10559-014-9654-0

8. Iakymenko I., Kasianchuk M., Kinakh I., Karpinski M. Construction of distributed thermal or piezoelectric sensor based on residue systems. Przeglad Elektrotechniczny. 2017. №1. pp. 290-294 (Scopus). DOI: 10.15199/48.2017.01.69

9. Kasianchuk M., Yakymenko I., Yatskiv S., Gomotiuk O., Bilovus L. The Method of Joint Execution of the Basic Operations of the Rabin Cryptosystem. CEUR Workshop Proceedings, 2023, 3373, pp. 425–436. https://ceur-ws.org/Vol-3373/paper28.pdf (Scopus).

10. Kasianchuk M., Yakymenko I., Yatskiv V., Karpinski M., Yatskiv S. Method of Multi-Bit Numbers Multiplication in Residue Number System for Asymmetric Cryptosystems. CEUR Workshop Proceedings, 2022, 3156, pp. 365–377. https://ceur-ws.org/Vol-3156/paper27.pdf . (Scopus).

11. Stanislaw Zawislak, Mykhailo Kasianchuk, Igor Iakymenko, Daniel Jancarczyk Methods of Crypto-stable Symmetric Encryption in the Residual Number System. Procedia Computer Science. Volume 207, 2022, pp. 128-137. DOI:10.1016/j.procs.2022.09.045 (Scopus)

12. Yakymenko I., Kasianchuk M., Shylinska I. A Method for Polynomial Recovery from its Resudues Based on Addition in Z[x] Ring. Informatics and Mathematical Methods in Simulation Vol.14 (2024), No. 4, pp. 305-313. DOI:10.15276/imms.v14.no4.305.

13. Якименко І. З., Касянчук М. М., Івасьєв С. В. Криптосистема Рабіна на основі операції додавання. Математичне та комп'ютерне моделювання. Серія: Технічні науки № 19, 2019. 145–150 с. DOI: https://doi.org/10.32626/2308-5916.2019-19.145-150

14. Якименко І. З. Удосконалення реалізації криптоалгоритму Ель-Гамаля на основі системи залишкових класів. Інформатика та математичні методи в моделюванні, 2018, 8, № 1. С. 69-77. DOI: 10.15276/imms.v8.no1.69

15. Касянчук М.М., Якименко І.З., Івасьєв С.В., Мандебура Н.М., Неміш В.М. Дослідження часових характеристик апаратної реалізації методів пошуку оберненого елемента за модулем. Вісник Хмельницького національного університету. Технічні науки. 2017. №6 (255). С. 191-197.

16. Касянчук М.М., Якименко І.З., Івасьєв С.В., Момотюк О.В. Експериментальне дослідження програмної реалізації методів пошуку оберненого елемента за модулем. Інформатика та математичні методи в моделюванні. 2017. Т.7, №3. С. 178–186.

17. Касянчук М.М., Якименко І.З., Івасьєв С.В., Маслияк Б.О. Метод розширення набору модулів модифікованої досконалої форми системи залишкових класів. Математичне та комп'ютерне моделювання: Технічні науки. 2017. В.15. С.73-78.

18. Касянчук М.М., Якименко І.З., Паздрій І.Р., Івасьєв С.В. Експериментальне дослідження програмної реалізації сумісного виконання

алгоритму Евкліда та множення. Інформатика та математичні методи в моделюванні. 2017. Т.7, №1-2. С. 29–36.

19. Касянчук М.М., Якименко І.З., Дубчак Л.О., Рендзеняк Н.А., Мандебура Н.М. Модифікований метод шифрування Рабіна з використанням різних форм системи залишкових класів. Вісник Хмельницького національного університету. Технічні науки. 2017. №1(245). С. 127-131.

20. Касянчук М.М., Якименко І.З., Долинюк Т.М., Рендзеняк Н.А. Експериментальне дослідження програмної реалізації методів модулярного експоненціювання. Інформатика та математичні методи в моделюванні. 2015. Т.5, №4. С. 376–382.

21. Івасьєв С.В., Якименко І.З., Касянчук М.М. Вдосконалений алгоритм пошуку символів Якобі. Оптико-електронні інформаційно-енергетичні технології. 2015. Том 29, № 1. С. 45-50.

22. Касянчук М.М., Якименко І.З., Паздрій І.Р., Николайчук Я.М. Аналітичний пошук модулів досконалої форми системи залишкових класів та їх застосування в китайській теоремі про залишки. Вісник Хмельницького національного університету. Технічні науки. 2015. №1(221). С. 170-176.

23. Николайчук Я. М., Касянчук М.М., Якименко І.З., Івасьєв С.В. Ефективний метод модулярного множення в теоретико-числовому базисі Радемахера–Крестенсона. Вісник Національного університету «Львівська політехніка». Комп'ютерні системи та мережі. 2014. № 806. С. 195-199.

24. Якименко І.З., Касянчук М.М., Тимошенко Л.М., Гребень Н.Є. Алгоритми опрацювання інформаційних потоків в комп'ютерних системах. Інформатика та математичні методи в моделюванні. 2013. Т.3, №3. С. 266–274.

25. Якименко І.З., Касянчук М.М., Кімак В.Л. Теоретичні основи зменшення часової та апаратної складності систем захисту інформаційних потоків на основі еліптичних кривих з використанням теоретико-числового базису Радемахера-Крестенсона. Вісник Національного університету «Львівська політехніка» «Комп'ютерні системи та мережі». 2012. №745. С. 190–197.

26. Николайчук Я.М., Касянчук М.М., Якименко І.З., Долинюк Т.М. Теоретичні основи виконання модулярних операцій множення та експоненціювання в теоретико–числовому базисі Крестенсона–Радемахера. Інформатика та математичні методи в моделюванні. 2011. №2. С. 123–130.

27. Zadiraka V., Yakymenko I., Kasianchuk M., Ivasiev S. Theoretical and numerical Krestenson's basis and its application to problems of cryptographic protection and factorization of multidigit numbers, Computer technologies in information security: collective monograph, By edited V.Zadiraka, Ya.Nykolaichuk, Ternopil: Kart-blansh, 2015. P. 216-260. Ch. 5.

28. Yakymenko I., Kasyanchuk M., Volynskyi O. Fundamental application-oriented tasks in Krestenson base, Methods of effective protection of information

flows: collective monograph, By edited V.Zadiraka, Ya.Nykolaichuk, Ternopil: Terno-graf, 2014. P. 149-185. Ch.6.

29. Kasianchuk M., Yakymenko I., Ivasiev S. High-Productivity Methods of Finding Residues Multidigital Numbers By Modulo, in Inżynier XXI Wieku: VI Międzynarodowa Konferencja studentow oraz doktorantow, 02.12.2016: monografia, 1st ed., Bielsko – Biała (Poland): Akademia Techniczno-Humanistyczna w Bielsku-Białej. 2016. pp. 123-130. Chapter in monograph.

30. Якименко І. Алгоритми побудови модифікованої досконалої форми системи залишкових класів. Спеціалізовані комп'ютерні технології в інформатиці: Колективна монографія. Під ред. В.Задіраки, Я.Николайчука. Тернопіль: Бескиди, 2017. С. 580-604.

31. Kasianchuk M., Yakymenko I., Ivasiev S. Theoretical foundations for creating five modular modified perfect form of the system of residual classes, in Inżynier XXI Wieku: VII Międzynarodowa Konferencja studentow oraz doktorantow, 08.12.2017: monografia, 1st ed., Vol.2., Bielsko – Biała (Poland): Akademia Techniczno-Humanistyczna w Bielsku-Białej, 2017, pp. 123-130. Chapter in monograph.

Матеріали конференцій:

32. Yakymenko I., Kasianchuk M., Martyniuk O., Martyniuk S., Martyniuk A., Yakymenko Y. A Symmetric Cryptoalgorithm in a Polynomial Hierarchical Residual Number System. Proceedings International Conference on Advanced Computer Information Technologies, ACIT., 2025, pp. 501-504. DOI: 10.1109/ACIT65614.2025.11185808

33. Yakymenko I., Martyniuk O., Martyniuk S., Yakymenko Y., Kasianchuk M. Hierarchical Encryption in a Residual Number System. Proceedings International Conference on Advanced Computer Information Technologies, ACIT., 2024, pp. 496–499 (Scopus). DOI: 10.1109/ACIT62333.2024.10712567

34. Shevchuk R., Yakymenko I., Kasianchuk M. Encryption Using Residue Number System: Research Trends and Future Challenges. Proceedings International Conference on Advanced Computer Information Technologies, ACIT2024, 2024, pp. 552–559 (Scopus). DOI: 10.1109/ACIT62333.2024.10712566

35. Shevchuk R., Karpinski M., Kasianchuk Yakymenko I., Melnyk A., Tykhyi R. Software for Improve the Security of Kubernetes-based CI/CD Pipeline. Proceedings International Conference on Advanced Computer Information Technologies, ACIT2023, 2023, pp. 420–425. (Scopus). DOI: 10.1109/ACIT58437.2023.10275654

36. Yakymenko I., Kasianchuk M., Shylinska I., Shevchuk R., Yatskiv V., Karpinski M. Polynomial Rabin Cryptosystem Based on the Operation of Addition. 12th International Conference on Advanced Computer Information Technologies, ACIT 2022, 2022, pp. 345–350. DOI:10.1109/ACIT54803.2022.9913089 (Scopus).

37. Yakymenko I., Kasianchuk M., Yatskiv V., Shevchuk R., Koval V., Yatskiv S. Sustainability and Time Complexity Estimation of Cryptographic

Algorithms Main Operations on Elliptic Curves. 2021 11th International Conference on Advanced Computer Information Technologies (ACIT). pp. 494-498 (Scopus). DOI: 10.1109/ACIT52158.2021.9548534

38. Mykhailo Kasianchuk, Ihor Yakymenko, Vasyl Yatskiv, Stepan Ivasiev, Andriy Sverstiuk. Same Bit-Size Moduli Formation of Residue Number System for Application in Asymmetric Cryptography. IntelITSIS 2021. pp. 301-308.

39. Yakymenko I., Shylinska I., Kasianchuk M., Bilovus L., Gomotiuk O. Algorithmic Support for Rabin Three-Modular Cryptosystem Based on the Operation of Addition. IEEE 15th International Conference on Computer Sciences and Information Technologies (CSIT). 2020. pp. 328-331 (Scopus).

40. Kasianchuk M., Yakymenko I., Karpinski M., Shevchuk R., Karpinskyi V., Shylinska I. Theoretical Bases for Reducing the Time Complexity of the Rabin Cryptosystem. Conference on Computer Science and Information Technologies. 2020. pp. 628-639. (Scopus). DOI: 10.1007/978-3-030-63270-0_43

41. Ivasiev S., Kasyanchuk M., Yakymenko I., Gomotiuk O., Shylinska I., Bilovus L. Algorithmic support for Rabin cryptosystem implementation based on addition.10th International Conference on Advanced Computer Information Technologies (ACIT). 2020. pp. 779-782. (Scopus). DOI: 10.1109/ACIT49673.2020.9208923

42. Yakymenko I., Kasianchuk M., Ivasiev S., Shevchuk R., Batko Y., Vasylkiv V. Method for Determining Prime and Relatively Prime Numbers of 2n+k Type Based on the Periodicity Property. 10th International Conference on Advanced Computer Information Technologies (ACIT), Deggendorf, Germany. 2020. pp. 751–754. https://doi.org/10.1109/ACIT49673.2020.9208812 (Scopus).

43. Yakymenko I., Kasianchuk M., Gomotiuk O., Tereshchuk G., Ivasiev S., Basistyi P. Elgamal cryptoalgorithm on the basis of the vector-module method of modular exponentiation and multiplication. IEEE 15th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET). 2020. pp. 926-929. (Scopus). DOI: 10.1109/TCSET49122.2020.235572

44. Karpinski M., Rajba S., Zawislak S., Warwas K., Kasianchuk M., Ivasiev S., Yakymenko I. A method for decimal number recovery from its residues based on the addition of the product modules, 2019 10th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS). Metz, France. 2019. pp.13-17. https://doi.org/10.1109/IDAACS.2019.8924395. (Scopus).

45. Kasianchuk M., Yakymenko I., Ivasiev S., Shevchuk R., Tymoshenko L. The method of factorizing multi-digit numbers based on the operation of adding odd numbers. CEUR Workshop Proceedings 8th International Conference Advanced Computer Information Technologies ACIT. June 2018. 2018, pp. 232-235, (Scopus).

46. Ivasiev S., Yakymenko I., Kasianchuk M., Shevchuk R., Karpinski M., Gomotiuk O. Effective algorithms for finding the remainder of multi-digit numbers.

Advanced Computer Information Technology (ACIT–2019): Proceedings of the International Conference. 2019, pp. 175-178. (Scopus). DOI: 10.1109/ACITT.2019.8779899

47. Yakymenko I., Kasianchuk M., Ivasiev S., Melnyk A., Nykolaichuk Y. Realization of RSA cryptographic algorithm based on vector-module method of modular exponention. In Proceedings of the 2018 14th International Conference on Advanced Trends in Radioelecrtronics. Telecommunications and Computer Engineering (TCSET), Lviv-Slavske, Ukraine, 20–24 February 2018. 2018. pp. 550–554.

48. Якименко І.З., Касянчук М.М., Кінах Я.І., Власюк І.М., Суслін В.В. Удосконалення реалізації асиметричних криптоалгоритмів на основі системи залишкових класів. Матеріали VI Всеукраїнської школи-семінару молодих вчених і студентів «Сучасні комп'ютерні інформаційні технології» (ACIT). 2018. с. 79.

49. Карпінський, М. П., Кінах, Я. І., Яциковська, У. О., Якименко, І. З., Касянчук, М. М. Удосконалення архітектури комп'ютерної мережі для програмної реалізації криптоаналітичних алгоритмів. Матеріали V науково-технічної конференції „Інформаційні моделі, системи та технології". 2018. С. 93.

50. Карпінський М. П., Кінах Я. І., Войтенко, О. С., Паславський, В. Р., Якименко, І. З., Касянчук, М. М. Теоретичний аналіз інформаційної безпеки в комп'ютерних мережах. Збірник тез доповідей VI Міжнародної науково-технічної конференції молодих учених та студентів „Актуальні задачі сучасних технологій". 2, 2017. С.81-82.

51. Rajba T., Klos-Witkowska A., Ivasiev S., Yakymenko I., Kasianchuk M. Research of time characteristics of search methods of inverse element by the module in: Proc. IEEE 9th Intern. Conf. on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS-2017) (Bucharest, Romania. 21–23 Sept, 2017), 2017. pp. 82–85. https://doi.org/10.1109/IDAACS.2017.8095054. (Scopus).

52. Kasianchuk M., Yakymenko I., Pazdriy I., Melnyk A., Ivasiev S., Rabin's modified method of encryption using various forms of system of residual classes. 14th International Conference The Experience of Designing and Application of CAD Systems in Microelectronics (CADSM), 2017. pp. 222-224. (Scopus). DOI: 10.1109/CADSM.2017.7916120

53. Якименко І.З. Методологія криптографічного захисту інформації на основі цілочисельної, модифікованої досконалої та поліноміальної систем залишкових класів, Матеріали XIV Міжнародної науково-технічної конференції ITSec-2025 Безпека інформаційних технологій, 22-24 травня 2025, м. Тернопіль (Україна). 2025. С. 224-228.

54. Karpiński M., Ivasiev S., Yakymenko I., Kasianchuk M., Gancarczyk T. Advanced method of factorization of multi-bit numbers based on Fermat's

theorem in the system of residual classes. International Conference on Control, Automation and Systems (ICCAS–2016): Proceedings. Gyeongju, Korea. V.1. 2016. pp.1484–1486 (Scopus). DOI: 10.1109/ICCAS.2016.7832500

55. Nykolaychuk Ya., Ivas'ev S., Yakymenko I., Kasianchuk M. Test of verification of multidigit numbers on simplicity on the basis of method of vector and modular multiplication. Modern Problems of Radio Engineering, Telecommunications and Computer Science (TCSET–2016): Proceedings of the XIII–th International Conference. L'viv–Slavske. 2016. pp.534-536 (Scopus). DOI: 10.1109/TCSET.2016.7452107

56. Kozaczko D., Ivasiev S., Yakymenko I., Kasianchuk M. Vector Module Exponential in the Remaining Classes System. Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS–2015): Proceedings of the 2015 IEEE 8th International Conference. Warsaw, Poland. V.1. 2015. pp.161–163 (Scopus). DOI: 10.1109/IDAACS.2015.7340720

57. Kasianchuk M., Yakymenko I., Pazdriy I., Zastavnyy O. Algorithms of findings of perfect shape modules of remaining classes system. The Experience of Designing and Application of CAD Systems in Microelectronics (CADSM-2015): Proceedings of the XIII International Conference. Polyana-Svalyava. 2015. pp.168-171 (Scopus). DOI: 10.1109/CADSM.2015.7230866

58. Ivas'ev S., Kasyanchuk M., Yakymenko I., Nykolaychuk Ya. Fundamental Backgrounds of the Discrete Logarithms Theory in the Rademacher–Krestenson's Basis. Modern Problems of Radio Engineering, Telecommunications and Computer Science (TCSET–2012): Proceedings of the XI–th International Conference. L'viv–Slavske. 2012. 93 P. (Scopus).

59. Касянчук М.М., Якименко І.З., Тимошенко Л.М., Івасьєв С.В., Николайчук Я.М. Векторно-модульний метод модулярного множення. Сучасні інформаційні та електронні технології: Матеріали Міжнародної науково-практичної конференції. Одеса. 2014, С. 152.

Патенти:

60. Пат. 159225 Україна МПК G06F 7/00 (2025.01). Накопичуючий синхронізований двійковий суматор / Николайчук Я.М., Грига В.М., Якименко І.З., Грига Л.П., № u 2024 04320 заявл. 03.09.2024; опубл. 08.05.2025, Бюл. №19/2025.

61. Пат. 160091 Україна МПК G06F7/04. Пристрій порівняння даних, представлених у непозиційній системі залишкових класів / Николайчук Я.М., Якименко І.З., Івасьєв С.В, Грига В.М. № u202404328 заявл. 03.09.2024; опубл. 06.08.2025, Бюл. № 32/2025.

Структура та обсяг дисертації.

Дисертація складається з анотації, змісту, вступу, шістьох розділів, загальних висновків, списку використаних джерел і додатків. Основний текст роботи викладено на 347 сторінках. Список використаних джерел нараховує

331 найменувань на 38 сторінках. Робота містить 65 таблиць та 99 рисунків (з них 10 таблиць і 6 рисунків займають повну сторінку), 2 додатків на 35 сторінках. Загальний обсяг роботи 420 сторінок.

Повнота викладення матеріалів дисертації в публікаціях та особистий внесок у них автора.

Основні наукові положення та результати дослідження опубліковано автором самостійно та у співавторстві у 61 наукових працях загальним обсягом 29 друк. арк. (з них 17,4 друк. арк. належать особисто автору), серед яких 5 колективних монографій обсягом 7,7 друк. арк. (з них 5,4 друк. арк. авторські), 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, чотири – до квартилю Q3 та одна – до квартилю Q4) обсягом 13,25 друк. арк. (з них 7,95 друк. арк. авторські) та 28 публікацій у матеріалах міжнародних та всеукраїнських конференцій (з них 22 публікацій включено в наукометричні бази Scopus та/або Web of Science) обсягом 7,05 друк. арк. (з них 4,23 друк. арк. авторські), 2 патенти на корисну модель обсягом 1 друк. арк. (з них 0,6 друк. арк. авторські). Одна стаття, розділ монографії і одні тези написані автором одноосібно. Матеріали відтворюють основний зміст роботи та наукові результати дисертації і відповідають нормативним вимогам МОН України.

Наукові публікації відповідають вимогам п. 8 Порядку присудження та позбавлення наукового ступеня доктора наук (Постанова Кабінету Міністрів України від 17 листопада 2021 р. №1197) та наказу МОН України №1220 від 23.09.2019 р. «Про опублікування результатів дисертацій на здобуття наукових ступенів доктора і кандидата наук».

Оцінка мови та стилю дисертації.

Дисертаційна робота написана грамотною діловою українською мовою з науковим стилем викладення її змісту, характеризується цілісністю, смисловою завершеністю, логічною послідовністю розгляду питань, об'єктивністю викладення, точністю використання спеціальної термінології, ясністю і стислістю, чітко структурована, а стиль викладу матеріалу дослідження, наукових положень, висновків і рекомендацій забезпечує легкість і доступність їх сприйняття. Застосована у роботі наукова термінологія є загальновизнаною, стиль викладення результатів теоретичних та експериментальних досліджень, нових наукових положень, висновків і рекомендацій забезпечує доступність їх сприйняття та використання.

ЗАГАЛЬНИЙ ВИСНОВОК:

Вважати, що дисертаційна робота **Якименка Ігоря Зіновійовича на тему: «Методи та засоби криптографічного захисту інформації на основі системи залишкових класів»,** яка подана на здобуття ступеня доктора наук, за актуальністю, ступенем новизни, науковим рівнем та практичною цінністю, змістом та оформленням повністю відповідає вимогам п. 7, 9 Порядку присудження та позбавлення наукового ступеня доктора наук (Постанова Кабінету Міністрів України від 17 листопада 2021 р. № 1197) та наказу МОН України № 40 від 12.01.2017 р. «Про затвердження вимог до оформлення дисертації».

Рекомендувати дисертаційну роботу **Якименка Ігоря Зіновійовича на тему: «Методи та засоби криптографічного захисту інформації на основі системи залишкових класів»** до захисту на здобуття ступеня доктора наук у спеціалізованій вченій раді Д 26.861.05 з присудження наукового ступеня доктора наук за спеціальностями 05.13.06 «Інформаційні технології (технічні науки)», 05.13.21 «Системи захисту інформації (технічні науки)».

Рецензенти:

Директор Навчально-наукового
інституту кібербезпеки та захисту інформації,
д.т.н., професор Євгенія ІВАНЧЕНКО

Професор кафедри систем
та технологій кібербезпеки,
д.т.н., професор Світлана КАЗМІРЧУК

Професор кафедри управління
кібербезпекою та захистом інформації,
д.т.н., професор Віталій САВЧЕНКО