ВИСНОВОК
про наукову новизну, теоретичне та практичне значення результатів дисертації
КОРОТКОГО ТИМОФІЯ КОНСТЯНТИНОВИЧА
на тему:
«Ієрархічна інформаційна система моделювання і дослідження алгоритмів потокового CET-шифрування»

для здобуття ступеня доктора філософії за спеціальністю 126 – Інформаційні системи та технології

Публічна презентація наукових результатів дисертації відбулася на засіданні кафедри інформаційних технологій проектування (далі – ІТП) Черкаського державного технологічного університету (далі – ЧДТУ) 9 червня 2026 року, протокол № 14/01.

ПРИСУТНІ:
Прокопенко Т.О., завідувач кафедри ІТП, д.т.н., професор;
Тесля Ю.М., професор кафедри ІТП, д.т.н., професор;
Лавданська О.В., доцент кафедри ІТП, к.т.н., доцент;
Ланських Є.В., доцент кафедри ІТП, к.т.н., доцент;
Рудницький С.В., доцент кафедри ІТП, к.т.н., доцент;
Рудницька Ю. В., асистент, доктор філософії з інформаційних систем;
Катаєв Д.С., старший викладач кафедри ІТП, к.т.н.;
Бабенко В. Г., завідувач кафедри інформаційної безпеки та комп'ютерної інженерії, д.т.н., професор;
Чепинога А.В., декан факультету інформаційних технологій та систем, к.т.н., доцент;
Федоров Є.Є., професор кафедри статистики та прикладної математики, д.т.н., професор;
Рудницький В.М., головний науковий співробітник Державного науково-дослідного інституту випробувань та сертифікації озброєння та військової техніки, д.т.н., професор;
Єременко В.С., завідувач кафедри інформаційно-вимірювальних технологій, Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського», д.т.н., професор;
Кучук Г.А., професора кафедри комп'ютерної інженерії та програмування, Національний технічний університет «Харківський політехнічний інститут», д.т.н., професор;
Підкуйко О.І., асистент, доктор філософії з інформаційних систем;
Прокопенко В.А., асистент, доктор філософії з інформаційних систем;

Тему дисертації було затверджено на засіданні вченої ради факультету інформаційних технологій і систем 1 червня 2026 року (протокол №13). Наукові керівники: д.т.н., професор Бабенко Віра Григорівна, к.т.н., доцент

Рудницький Сергій Володимирович – призначені наказом ЧДТУ №135/03/03 від 18.05.2026.

1. Актуальність теми дослідження.

За останні декілька десятиліть швидкий розвиток інформаційних систем призвів до зростання цінності інформації як для суспільства взагалі, так і для кожної окремої людини зокрема. Проте почала зростати небезпека несанкціонованого втручання в роботу інформаційних систем. Значення та вагомість наслідків таких втручань з часом збільшилися настільки, що навіть розвинені держави, їх промислові та фінансові структури стали заручниками своїх інформаційних технологій. Тому важливою проблемою є постійне підвищення якості систем захисту інформації. Одним із основних напрямків розвитку систем захисту інформації є криптографічний захист.

Проте в криптології залишається цілий ряд задач і проблем, вирішення яких має важливе науково-технічне й загальнодержавне значення. Особливо гострими проблеми стійкості криптографічних систем стали після створення квантових комп'ютерів. Одним із перспективних шляхів розвитку криптографії є CET-шифрування. Воно базується на використанні CET-операцій і забезпечує побудову малоресурсних потокових шифрів випадкової підстановки. На даний час CET-операції і CET-шифрування знаходяться на стадії переходу від концептуальних і теоретичних досліджень до варіантів практичної реалізації. Але без комп'ютерного моделювання і оцінки результатів дуже складно забезпечити ефективний перехід від теорії до практики. Стосовно CET-шифрування, яке забезпечує факторіальний ріст можливих варіантів реалізації при збільшенні довжини блока криптоперетворення, автоматизація процесу дослідження разом з удосконаленням теорії моделювання CET-операцій і їх груп є необхідною умовою побудови перспективних потокових шифрів. Виходячи з цього тема дисертаційного дослідження «Ієрархічна інформаційна система моделювання і дослідження алгоритмів потокового CET-шифрування» є актуальною.

Дисертаційне дослідження виконано в рамках науково-дослідних робіт: «Дослідження шляхів розвитку потокового шифрування на основі криптографічного кодування» (ДР № 0121U114389); «Інформаційна технологія психолінгвістичного аналізу тексту для стеганографічних систем» (ДР № 0123U102085), в яких автор був виконавцем.

Метою дисертаційної роботи є підвищення продуктивності дослідження CET-операцій при побудові перспективних стійких алгоритмів потокового шифрування на основі розширення можливостей ієрархічної інформаційної системи моделювання і дослідження CET-операцій за рахунок встановлення нових і уточнення існуючих взаємозв'язків між моделями ієрархічних рівнів які в сукупності забезпечать автоматизований синтез і аналіз симетричних та несиметричних однооперандних і багатооперандних

СЕТ-операцій, а також генераторів їх псевдовипадкових послідовностей для потокового СЕТ-шифрування.

Для досягнення вказаної мети в дисертаційні роботі виділено наступні задачі дослідження:

- удосконалити технологію побудови удосконалених моделей некомутативних двохрозрядних двохоперандних СЕТ-операції за результатами обчислювального експерименту;
- удосконалити метод синтезу двохоперандних двохрозрядних операцій криптографічного перетворення для забезпечення можливості побудови як симетричних так і несиметричних СЕТ-операцій;
- удосконалити метод побудови двохрозрядних двохоперандних операцій які допускають перестановку операндів на основі об'єднання двохрозрядних одноопераднних операцій криптографічного перетворення;
- розробити модель ієрархічної інформаційної системи моделювання і дослідження симетричних і несиметричних СЕТ-операцій реалізація якої забезпечить побудову перспективних стійких мало ресурсних алгоритмів потокового шифрування.

Об'єктом дослідження є процеси автоматизації моделювання і дослідження малоресурсного шифрування.

Предметом дослідження є моделі, методи і засоби побудови ієрархічної інформаційної системи моделювання і дослідження алгоритмів потокового СЕТ-шифрування.

Методи дослідження. У процесі виконання роботи використовувався математичний апарат теорії інформації, теорії алгоритмів, криптографії, логіки, методи комп'ютерного моделювання і дискретної математики, математичної статистики та комп'ютерного моделювання.

2. Формулювання наукового завдання, нове розв'язання якого отримано в дисертації.

У дисертаційній роботі вирішена актуальна науково-прикладна задача розробки нової ієрархічної інформаційної системи моделювання і дослідження СЕТ-операцій яка забезпечать автоматизований синтез і аналіз симетричних та несиметричних одноопераднних і багатоопераднних СЕТ-операцій, а також генераторів їх псевдовипадкових послідовностей для побудови систем потокового СЕТ-шифрування.

3. Наукові положення, розроблені особисто дисертантом, їхня новизна.

Дисертаційне дослідження містить у собі наступні наукові положення, розроблені особисто дисертантом:

1) вперше побудована модель ієрархічної інформаційної системи моделювання і дослідження симетричних і несиметричних СЕТ-операцій, на основі методів синтезу СЕТ-операцій і груп СЕТ-операцій, шляхом вдосконалення моделей, методів і технології побудови комутативних і

некомутативних СЕТ-операції, а також генераторів псевдовипадкових наборів СЕТ-операцій, що дозволило встановлювати нові залежності між моделями синтезу симетричних і несиметричних операцій, які приводять до розширення взаємозв'язків між моделями ієрархічних рівнів інформаційної системи, реалізація якої забезпечить експериментальну підтримку для побудову перспективних стійких мало ресурсних алгоритмів потокового шифрування;

2) удосконалено технологію побудови удосконалених моделей некомутативних двохрозрядних двохоперандних СЕТ-операції за результатами експерименту, на основі побудови удосконалених моделей СЕТ-операцій за результатами експерименту, шляхом встановлення взаємозв'язків між моделями до і після перестановки операндів, що забезпечило зменшення складності моделювання некомутативних СЕТ-операцій на основі реалізації прямого переході від побудованої моделі СЕТ-операції до моделі СЕТ-операції з переставленими операндами;

3) удосконалено метод синтезу двохоперандних двохрозрядних операцій криптографічного перетворення на основі метод синтезу симетричних операцій, шляхом застосування в якості першої базової операції несиметричної операції криптоперетворення та додаткової побудови оберненої операції за результатами обчислювального експерименту, що забезпечили можливість додаткового синтезу несиметричних двохоперандних двохрозрядних операцій подвійного циклу;

4) удосконалено метод побудови двохрозрядних двохоперандних операцій які допускають перестановку операндів на основі об'єднання двохрозрядних одноопераднних операцій криптографічного перетворення, шляхом встановлення взаємозв'язків між прямими і оберненими операціями, що дозволило змоделювати всі двохрозрядні двохоперандні операцій, які допускають перестановку операндів.

4. Обґрунтованість і достовірність наукових положень, висновків і рекомендацій, які захищаються.

Наукові положення, висновки та рекомендації роботи обґрунтовані в повній мірі. Обґрунтованість отриманих теоретичних результатів дисертації базується на коректному застосуванні математичний апарат теорії інформації, теорії алгоритмів, криптографії, логіки, методи комп'ютерного моделювання і дискретної математики, математичної статистики та комп'ютерного моделювання.

Достовірність досліджень підтверджується не розбіжністю отриманих теоретичних результатів з результатами обчислювального експерименту, успішною реалізацією розроблених моделей та алгоритмів у складі програмного комплексу.

5. Рівень теоретичної підготовки здобувача, його особистий внесок у розв'язання конкретного наукового завдання. Рівень обізнаності здобувача з результатами наукових досліджень інших учених.

Дисертантом виконано змістовне дослідження предметної області, розглянуто основні моделі, методи та засоби малоресурсної криптографії, інформаційних систем моделювання криптоперетворень, ієрархічних систем і технологій моделювання. На основі опрацювання значної кількості літературних джерел, наукових публікацій автором роботи в максимальній мірі враховані останні наукові досягнення в обраному напрямку дослідження. Отримані результати свідчать про ґрунтовні теоретичні знання дисертанта в областях інформаційних систем і криптографії, зокрема в галузі інформаційних систем і технологій моделювання криптографічних перетворень і криптографічних систем, математичного та імітаційного моделювання, математичної статистики та теорії дослідження.

6. Наукове та практичне значення роботи.

Наукове значення роботи полягає в розробці нових та вдосконаленні відомих моделей та методів криптоперетворень, які в сукупності забезпечили побудови ієрархічної інформаційної системи маделювання і дослідження алгоритмів потокового СЕТ-шифрування.

Практична цінність дисертаційної роботи полягає в тому, що отримані наукові результати доведено здобувачем до конкретних моделей, інженерних методик розрахунку, та отриманих варіантів застосування моделей генераторів псевдовипадкових послідовностей СЕТ-операцій.

7. Використання результатів роботи.

На підставі проведених досліджень побудовано програмний макет ієрархічнаої інформаційної системи моделювання і дослідження алгоритмів потокового СЕТ-шифрування. Дана інформаційна система забезпечує розширення спектру аналізуємих 2Сі-квантових СЕТ-операцій які допускають перестановку операндів з 96 симетричних до 576 симетричних та несиметричних 2Сі-квантових СЕТ-опрерацій які допускають перестановку операндів, а також до 10623 2Сі-квантових СЕТ-опрерацій які недопускають перестановку операндів. Дана інформаційна система забезпечить дослідження систем потокового шифрування в яких може бути використано до $65 \cdot 10^{35}$ несиметричних двохоперандних СЕТ-операцій, з яких 1 625 702 400 3Сі-квантові СЕТ-операції що допускають перестановку операндів.

Практичне значення результатів роботи підтверджується їх впровадженням в навчальний процес Черкаського державного технологічного університету:

- на кафедрі інформаційних технологій проектування при підготовці бакалаврів за спеціальністю 126 «Інформаційні системи та технології»

в курсі лекцій з дисциплін «Системи інформаційної безпеки», а також при виконанні курсових і кваліфікаційних робіт;

- на кафедрі інформаційної безпеки та комп'ютерної інженерії при підготовці бакалаврів за спеціальністю 123 «Комп'ютерна інженерія» в курсі лекцій з дисциплін «Безпека програмного забезпечення», «Арифметичні та логічні структури комп'ютерів», а також при виконанні кваліфікаційних робіт магістрів за спеціальністю 123 «Комп'ютерна інженерія» освітньої програми «Системне програмування».

8. Повнота викладу матеріалів дисертації.

За матеріалами дисертаційного дослідження опубліковано 16 друкованих працях, зокрема: у 8 статтях у фахових виданнях України із яких 2 статті в фахових журналах категорії А і проіндексовані в науково-метричній базі SCOPUS, 3 статтях опублікованих за кордоном із яких 1 стаття включена до науково-метричної бази SCOPUS (1 квартіль), одноосібному розділі колективної монографії, і в матеріалах двох міжнародних науково-технічних конференцій, однієї міжнародної науково-практичної конференції, міжнародного академічного форума та науково-практичної конференції Національної Академії Національної гвардії України.

Повний перелік публікацій:

Статті у наукових фахових виданнях України та періодичних виданнях, які індексуються у міжнародній наукометричній базі Scopus:

1. В. Рудницький, Н. Лада, В.Бабенко, В. Ларін, Т. Короткий (2025) Модель побудови множини симетричних двохоперандних СЕТ-операцій, які допускають перестановку операндів шляхом поєднання одноопераднних операцій. Innovative Technologies and Scientific Solutions for Industries. Харківський національний університет радіоелектроніки та ДП «Південний національний конструкторсько-дослідний інститут аерокосмічної промисловості» №3. 2025. – с .126-136. (SCOPUS, у фаховому виданні) DOI: https://doi.org/10.30837/2522-9818.2025.3.126 https://journals.uran.ua/itssi/article/view/340558

2. Rudnytskyi, V., Lada, N., Herashchenko, M., Korotkyi, T. & Stebetska, T. (2024) Modeling relationships in non-commutative two-operand two-bit cet-operations of a double cycle when permuting the operands. Technology audit and production reserves. Scientific journal. Vol. 3 No 2 (77), 2024. p.30-35. (SCOPUS, у фаховому виданні) DOI: 10.15587/2706-5448.2024.306980 https://journals.uran.ua/tarp/article/view/306980

3. Ларін В. Моделювання множин двохоперандних трьохрозрядних операцій криптоперетворення шляхом поєднання одноопераднних СЕТ-операцій. / В.В. Ларін, М.Ю. Гусак, Т.К. Короткий, О.М. Гук, О.Л. Кащишин

// Збірник наукових праць Харківського національного університету Повітряних Сил. – Х.: ХНУПС, 1 (83), 2025. DOI: https://doi.org/10.30748/zhups.2025.83.06 – С. 56 – 62. (У фаховому виданні)

4. Рудницький С.В., Ларін В.В., Підласий Д.А., Короткий Т.К. Синтез двохоперандних двохрозрядних СЕТ-операцій шляхом поєднання одноопераднних двохрозрядних СЕТ-операцій. Наука і техніка Повітряних Сил України. Щоквартальний науково-технічний журнал. Вип. 4(57) 2024. с.71-79 (У фаховому виданні) DOI: 10.30748/nitps.2024.57.09

5. В. Рудницький, В. Бабенко, С. Рудницький, Т. Короткий Генерація послідовності несиметричних СЕТ-операцій з точністю до перестановки другого операнда Інформаційні технології та суспільство / [головний редактор О. Попов]. – Київ : Міжрегіональна Академія управління персоналом, 2025. – Випуск 1 (16). – С/221-226. (У фаховому виданні)

6. Рудницький В.М., Бабенко В.Г., Рудницький С.В., Короткий Т.К., Ковтюх В.А. Особливості груп несиметричних СЕТ-операцій синтезованих з точністю до перестановки першого операнда Вчені записки ТНУ імені В.І. Вернадського. Серія: Технічні науки. Том 36 (75) № 4 2025 – С. 265-271. (У фаховому виданні)
https://www.tech.vernadskyjournals.in.ua/journals/2025/4_2025/part_2/37.pdf

7. Semenov, S.; Rudnytskyi, V.; Lada, N.; Krivtsun, V.; Korotkyi, T.; Zazhoma, V.; Wasiuta, O. Stream Encryption Cryptographic Systems Based on Asymmetric Cet Operations with an Accuracy of Permutation. *Appl. Sci.* 2026, *16*, 4987. https://doi.org/10.3390/app16104987 (SCOPUS)

8. Рудницький В. М., Лада Н. В., Рудницька Ю. В., Короткий Т. К. Моделювання симетричних двохоперандних операцій криптографічного кодування на основі об'єднання одноопераднних операцій. Сучасна спеціальна техніка, 2021. №4 с. 32-38. (У фаховому виданні)

9. Короткий Т. К. Дослідження і синтез некомутативних двохрозрядних двохоперандних СЕТ-операцій які допускають перестановку операндів. Технології розвитку безпілотних систем. Том 1. Малоресурсний захист інформації в безпілотних системах. Монографія / під ред. В.М. Рудницького. – Черкаси : видавець Вовчок О.Ю., 2025. –с165-205. ISBN 978-617-7508-50-1

10. V. Rudnytskyi, N. Lada , V. Larin, O. Melnyk, T. Stabetska, T. Korotkyi, D. Pidlasyi Usage of non-commutative two-operand CET-operations in limited resources stream ciphers Journal of Xidian University Volume 18 – Issue 5 – May 2024 Page No: 1105-1120.
https://doi.org/10.5281/Zenodo.11253625

11. Rudnytskyi, V., Lada, N., Larin, V., Tkachenko, V., Korotkyi, T., Pidlasyi, D. & Tarasenko, D. (2024). Information system for modeling and research of pseudorandom sequences of CET-operations for post quantum stream encryption systems. Journal of Xidian University. Vol. 18, Issue 7, July 24, 1284 – 1298. (SCOPUS) https://xadzkjdx.cn/index.php/volume-18-issue-7-july-24/ DOI:https://doi.org/10.5281/Zenodo.13096683

Тези доповідей у збірниках праць міжнародних наукових конференцій:

12. Рудницька Ю. В. Короткий Т. К. Інформаційна технологія моделювання та дослідження симетричних СЕТ-операцій. Проблеми інформатизації : Десята міжнар. наук.-техн. конф.: тези доп. Черкаси – Баку – Бельсько-Бяла – Харків, 24 – 25 листоп. 2022 р. Черкаси: ЧДТУ; Баку: ВА ЗС АР, Бельсько-Бяла: УТіГН, Харків: НТУ «ХПІ», 2022. Т. 1. С. 40.

13. Рудницький В.М., Ларін В.В., Лада Н.В, Короткий Т.К. Сучасний стан та перспективи розвитку СЕТ-шифрування / Воєнні інновації в сучасних війнах: Збірник тез Міжнародного академічного форуму/Центральний науково-дослідний інститут Збройних Сил України – К.: 7БЦ, 2024. – с.39-40.

14. Короткий Т.К, Ковтюх В.А. Моделювання і дослідження генераторів двохоперандних СЕТ-операцій для мало ресурсної криптографії. Актуальні проблеми розвитку сучасної науки: виклики та перспективи : збірник тез Міжнародної науково-практичної конференції здобувачів вищої освіти і молодих вчених (м. Запоріжжя, 29 квіт.). Запоріжжя : ЗНУ, 2025. с.472.
https://dspace.znu.edu.ua/jspui/handle/12345/25952

15. Рудницький В. М., Лада Н. В., Короткий Т. К. Вдосконалення технології побудови некомутативних СЕТ-операцій. Сучасні напрямки розвитку інформаційно-комунікаційних технологій та засобів управління. Тези доповідей 15 міжнародної науково-технічної конференції 24-25 квітня 2025 р. Том 1: секції 1, 5. Баку-Харків-Жиліна-2025. С.41.
https://doi.org/10.32620/ICT.25.t1

16. Рудницький В.М., Ларін В.В., Нікорчук А.І., Короткий Т.К. Особливості застосування малоресурсної криптографії в безпілотних комплексах. Проблемні питання щодо експлуатації та відновлення автобронетанкової техніки в Національній гвардії України:. Тези доповіді науково-практичної конференції 27 травня 2025р. м.Золочів. Харків НАНГУ 2025. с. 35–37.

Усі основні положення й результати дисертаційної роботи, що захищаються, одержані автором самостійно. У наукових працях, опублікованих у співавторстві, з питань, що стосуються цього дослідження, автору належать: побудова моделей комутативних і некомутативних двохоперандних СЕТ-операцій на основі об'єднання одноопераднних операцій за результатами обчислювального експерименту [1, 8, 9], встановлені взаємозв'язки в моделях некомутативних СЕТ-операціях при перестановці операндів [2], побудова множин 2 і 3 Сі-квантових СЕТ-операцій з точністю до перестановки на основі поєднання одноопераднних двохрозрядних СЕТ-операцій [3, 4], моделювання результатів генерацій псевдовипадкових послідовностей не комутативних СЕТ-операцій з точністю до перестановки другого операнда [5] і першого операнда [6], модифікація СЕТ-операцій і статистичний аналіз [7], структура, архітектура та модель

інформаційної системи моделювання і дослідження алгоритмів потокового СЕТ-шифрування [12, 13, 16], взаємозв'язок між рівнями ієрархії системи при моделюванні генераторів СЕТ-операцій [15], особливості застосування генераторів СЕТ-операцій в безпілотних комплексах [16], результати аналізу напрямків дослідження не комутативних СЕТ-операцій [12, 14].

Результати аналізу роботи за допомогою перевірки тексту дисертації з використанням системи turnitin та аналізу отриманих результатів свідчать про відповідність роботи принципам академічної доброчесності.

9. Апробація матеріалів дисертації. Результати дисертаційної роботи доповідалися й обговорювалися на Десятій міжнародній науково-технічній конференції «Проблеми інформатизації» (Черкаси – Баку – Бельсько-Бяла – Харків, 2022), Міжнародному академічному форумі «Воєнні інновації в сучасних війнах» (Київ, 2024), Міжнародній науково-практичній конференції здобувачів вищої освіти і молодих вчених «Актуальні проблеми розвитку сучасної науки: виклики та перспектив» (Запоріжжя, 2025), Пятнадцята міжнародна науково-технічна конференція «Сучасні напрямки розвитку інформаційно-комунікаційних технологій та засобів управління» (Баку-Харків-Жиліна, 2025), Науково-практичній конференції «Проблемні питання щодо експлуатації та відновлення автобронетанкової техніки в Національній гвардії України» (Золочів, 2025).

10. Оцінка мови та стилю дисертації.

Дисертацію написано з дотриманням норм і правил граматики, а стиль викладу в ній матеріалів досліджень, наукових положень, висновків і рекомендацій забезпечує легкість і доступність їх сприйняття.

Дисертація повною мірою відповідає пунктам 6, 7, 8 «Порядку присудження ступеня доктора філософії та скасування рішення разової спеціалізованої вченої ради про присудження ступеня доктора філософії в Черкаському державному технологічному університеті». Робота містить нові науково обґрунтовані результати проведених здобувачем досліджень, які виконують конкретне наукове завдання, що має істотне значення для галузі знань 12 – Інформаційні технології.

Дисертацію виконано державною мовою та відповідно до наявних вимог щодо оформлення.

11. Відповідність змісту дисертації освітньо-науковій програмі, з якої вона подається до захисту.

Зміст дисертації повністю відповідає спеціальності 126 – Інформаційні системи та технології освітньо-наукової програми «Інформаційні системи та технології».

12. Рекомендація дисертації до захисту.

Враховуючи рівень наукових досліджень, актуальність теми роботи та наукову новизну отриманих результатів, учасники фахового семінару кафедри інформаційних технологій проектування одноголосно ухвалили рішення затвердити висновок про наукову новизну, теоретичне та практичне значення результатів дисертації Короткого Тимофія Констянтиновича на тему «Ієрархічна інформаційна система моделювання і дослідження алгоритмів потокового CET-шифрування»» та рекомендувати до захисту у разовій спеціалізованій вченій раді Черкаського державного технологічного університету для здобуття ступеня доктора філософії за спеціальністю 126 – Інформаційні системи та технології галузі знань 12 – Інформаційні технології.

У голосуванні брали участь 15 осіб. Результати голосування:
«ЗА» – 15,
«ПРОТИ» – немає,
УТРИМАЛИСЬ – немає.

Головуючий
завідувач кафедри інформаційних
технологій проектування,
д.т.н, професор Тетяна ПРОКОПЕНКО
09.06.2026