

ВИТЯГ

з протоколу № 1 розширеного засідання 14.05.2026 року
відділу чисельних методів та комп'ютерного моделювання для публічної
презентації здобувача поза аспірантурою наукового співробітника Інституту
кібернетики В.М. Глушкова НАН України
Баранова І.А. щодо наукових результатів дисертації
«Паралельні алгоритми симетричної криптографії»
на здобуття наукового ступеня доктора філософії
за спеціальністю 113 Прикладна математика
та висновок про наукову новизну, теоретичне та практичне значення
результатів дисертації

Присутні на засіданні:

головуючий на засіданні д.ф.-м.н., професор, завідувач відділу оптимізації
чисельних методів Інституту кібернетики імені В.М. Глушкова НАН України
академік НАН України Задірака Валерій Костянтинівич;

д.ф.-м.н., професор, заступник директора за наукової роботи Інституту
кібернетики імені В.М. Глушкова НАН України, академік НАН України Хіміч
Олександр Миколайович;

д.ф.-м.н., с.н.с, в.о. завідувача відділу чисельних методів та комп'ютерного
моделювання Інституту кібернетики імені В.М. Глушкова НАН України, Попов
Олександр Володимирович;

перший проректор Державного університету інформаційно-
комунікаційних технологій член-кореспондент НАН України Корченко
Олександр Григорович;

д.т.н., с.н.с., професор кафедри Математичних методів захисту інформації
Навчально-наукового фізико-технічного інституту Національного технічного
університету України «Київський політехнічний інститут імені Ігоря
Сікорського» член-кореспондент НАН України Кудін Антон Михайлович;

к.ф.-м.н., с.н.с., старший науковий співробітник відділу методів
комбінаторної оптимізації та інтелектуальних інформаційних технологій
Інституту кібернетики імені В.М. Глушкова НАН України Ходзінський
Олександр Миколайович;

к.ф.-м.н., с.н.с., провідний науковий співробітник відділу оптимізації
чисельних методів Інституту кібернетики імені В.М. Глушкова НАН України
Швідченко Інна Віталіївна;

к.ф.-м.н., с.д., провідний науковий співробітник відділу чисельних методів

та комп'ютерного моделювання Інституту кібернетики імені В.М. Глушкова НАН України Ніколаєвська Олена Анатоліївна;

к.ф.-м.н., старший науковий співробітник відділу чисельних методів та комп'ютерного моделювання Інституту кібернетики імені В.М. Глушкова НАН України Чистякова Тамара Василівна;

к.ф.-м.н., старший науковий співробітник відділу чисельних методів та комп'ютерного моделювання Інституту кібернетики імені В.М. Глушкова НАН України Чистяков Олексій Валерійович;

к.ф.-м.н., старший науковий співробітник відділу чисельних методів та комп'ютерного моделювання Інституту кібернетики імені В.М. Глушкова НАН України Сидорук Володимир Антонович;

к.ф.-м.н., старший науковий співробітник відділу чисельних методів та комп'ютерного моделювання Інституту кібернетики імені В.М. Глушкова НАН України Єршов Павло Сергійович;

молодший науковий співробітник відділу чисельних методів та комп'ютерного моделювання Інституту кібернетики імені В.М. Глушкова НАН України Марченко Микита Анатолійович;

молодший науковий співробітник відділу чисельних методів та комп'ютерного моделювання Інституту кібернетики імені В.М. Глушкова НАН України Дученко Олександр Сергійович;

молодший науковий співробітник відділу чисельних методів та комп'ютерного моделювання Інституту кібернетики імені В.М. Глушкова НАН України Ляшко Віктор Сергійович;

молодший науковий співробітник відділу чисельних методів та комп'ютерного моделювання Інституту кібернетики імені В.М. Глушкова НАН України Нестеренко Алла Никифорівна;

аспірант відділу інтелектуальних інформаційних технологій Інституту кібернетики імені В.М. Глушкова НАН України Кучер Владислав Васильович.

Науковий керівник: д.ф.-м.н., професор, заступник директора за наукової роботи Інституту кібернетики імені В.М. Глушкова НАН України, академік НАН України Хіміч Олександр Миколайович.

Тема дисертації затверджена Вченою радою Інституту кібернетики імені В.М.Глушкова НАН України.

Дисертаційна робота виконана у відділі чисельних методів та комп'ютерного моделювання Інституту кібернетики імені В.М. Глушкова НАН України.

ПОРЯДОК ДЕННИЙ:

Публічна презентація аспірантом Інституту кібернетики В.М. Глушкова НАН України Барановим І.А. наукових результатів дисертації «Паралельні алгоритми симетричної криптографії» на здобуття наукового ступеня доктора філософії за спеціальністю 113 Прикладна математика, обговорення дисертації та висновок про наукову новизну, теоретичне та практичне значення

результатів дисертації.

СЛУХАЛИ:

Публічну презентацію аспірантом Інституту кібернетики В.М. Глушкова НАН України Барановим І.А. наукових результатів дисертації «Паралельні алгоритми симетричної криптографії» на здобуття наукового ступеня доктора філософії за спеціальністю 113 Прикладна математика.

В процесі обговорення результатів дисертації брали участь:

д.ф.-м.н., професор, завідувач відділу оптимізації чисельних методів Інституту кібернетики імені В.М. Глушкова НАН України академік НАН України Задірака Валерій Костянтинівич;

д.ф.-м.н., професор, заступник директора за наукової роботи Інституту кібернетики імені В.М. Глушкова НАН України, академік НАН України Хіміч Олександр Миколайович;

д.ф.-м.н., с.н.с, в.о. завідувача відділу чисельних методів та комп'ютерного моделювання Інституту кібернетики імені В.М. Глушкова НАН України, Попов Олександр Володимирович;

перший проректор Державного університету інформаційно-комунікаційних технологій член-кореспондент НАН України Корченко Олександр Григорович;

д.т.в., с.н.с., професор кафедри Математичних методів захисту інформації Навчально-наукового фізико-технічного інституту Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського» член-кореспондент НАН України Кудін Антон Михайлович

к.ф.-м.н., с.н.с., старший науковий співробітник відділу методів комбінаторної оптимізації та інтелектуальних інформаційних технологій Інституту кібернетики імені В.М. Глушкова НАН України Ходзінський Олександр Миколайович;

к.ф.-м.н., с.д., провідний науковий співробітник відділу чисельних методів та комп'ютерного моделювання Інституту кібернетики імені В.М. Глушкова НАН України Ніколаєвська Олена Анатоліївна.

УХВАЛИЛИ:

Затвердити наступний висновок про наукову новизну, теоретичне та практичне значення результатів дисертації Баранова І.А. «Паралельні алгоритми симетричної криптографії» на здобуття наукового ступеня доктора філософії за спеціальністю 113 Прикладна математика.

Дисертація присвячена розробці та дослідженню нових блочних симетричних криптографічних алгоритмів, в тому числі для паралельних комп'ютерів, що базуються на оригінальних криптографічних перетвореннях типу "кубик Рубіка" з ключозалежним вибором операцій. Основна увага приділялася підвищенню продуктивності за рахунок розпаралелювання

обчислень, в тому числі на багатоядерних процесорах (з використанням MPI) та графічних прискорювачах (CUDA), а також покращенню криптографічної стійкості шляхом ускладнення внутрішньої структури алгоритмів.

У роботі отримано такі основні результати:

Вперше розроблено блочний симетричний криптографічний алгоритм WBC1 на основі обертань кубика Рубіка, у якому шифрування реалізується через тривимірні перестановки та циклічні побітові зсуви. Такий підхід забезпечує високий рівень дифузії, нелінійності та значний простір перестановок, що підвищує стійкість алгоритму до brute-force, диференціального та лінійного криптоаналізу.

Вперше розроблено модифікацію алгоритму WBC2, у якій використано ключезалежні таблиці перестановок, динамічну S-box та раундові ключі. Це дозволило підвищити лавинний ефект, збільшити ентропію шифртексту та забезпечити додаткову стійкість у white-box моделі.

Вперше розроблено паралельні модифікації блочно-симетричних криптографічних алгоритмів PWBC1, PWBC1.1, PWBC2 та PWBC2.1 для багатоядерних систем, а також GPU-орієнтовану реалізацію PWBC2Cuda. Запропонований підхід забезпечує незалежну паралельну обробку блоків даних, ефективне масштабування в MPI- та CUDA-середовищах і дозволяє поєднати високий рівень криптографічної стійкості з підвищеною продуктивністю при обробці великих обсягів інформації.

Запропоновані алгоритми забезпечують високий рівень криптографічної стійкості, підтверджений статистичними тестами, аналізом ентропії, лавинного ефекту та тестуванням NIST STS, а також можуть бути використані для захисту мультимедійних даних, інформаційних ресурсів і високопродуктивних обчислювальних систем, зокрема в умовах паралельної та GPU-орієнтованої обробки даних.

Наукова новизна та практичне значення отриманих результатів полягає в розробці нових блочно-симетричних криптографічних алгоритмів та їх паралельних модифікацій, орієнтованих на забезпечення високої криптографічної стійкості та ефективності обробки великих обсягів даних. Розроблені алгоритми можуть бути впроваджені в навчальний процес, а також використані при розробці програмних засобів захисту інформації, систем обробки великих даних і спеціалізованих криптографічних застосунків.

Автор дисертації є виконавцем таких науково-дослідницьких тем Інституту кібернетики імені В.М. Глушкова НАН України:

ВФ 150.3.1230 «Розроблення моделей та методів високопродуктивних обчислень та їх застосування» (Державний реєстраційний номер 0122U200449; I

кв. 2022 р. – IV кв. 2023 р.);

2.1/23-П / В.П.150.4.1230 " Розробити платформу високопродуктивних обчислень на базі суперкомп'ютера СКІТ для задач кібербезпеки, математичного моделювання, інженерії " (Державний реєстраційний номер 0123U101573; 0124U003282, I кв. 2023 р. – IV кв. 2024 р.,)

Результати дисертації є істотним внеском у розроблення методів і засобів дослідження цифрових платформ як класу складних динамічних систем. Вони достатньо повно опубліковані в 15 наукових публікаціях, серед яких 4 – статті у наукових фахових виданнях України, 1 – публікації, що індексуються в наукометричній базі Scopus (1 публікація у колективній монографії Scopus), 2 авторські свідоцтва, 7 – тези доповідей на міжнародних наукових конференціях:

1. Баранов І.А. Некоторые подходы к эффективной реализации блочных матричных алгоритмов на MIMD – компьютерах. Проблемы програмування. 2008. №3. С. 103-110.

2. Баранов І.А. Параллельный алгоритм PWBC1. Компьютерная математика. 2010. № 2. С. 96-101.

3. Баранов І.А. Параллельный алгоритм PWBC1 с использованием технологии CUDA. Штучний інтелект. 2010. №2. С. 97

4. Баранов І.А. Криптографічний аналіз складності симетричного блочного алгоритму WBC1. Кібернетика та комп'ютерні технології. 2025. № 1. С. 64–73. <https://doi.org/10.34229/2707-451X.25.1.6>

5. Baranov, I. (2025). Implementations of Block Symmetric Cryptography Algorithm WBC1 for Computers with Parallel Architecture. In: Arai, K. (eds) Intelligent Computing. CompCom 2025. Lecture Notes in Networks and Systems, vol 1426. Springer, Cham. https://doi.org/10.1007/978-3-031-92611-2_20

6. Баранов І.А. Криптографічний аналіз складності та апробація симетричного блочного алгоритму WBC2. Кібернетика та комп'ютерні технології. 2026. № 1. С. 94–107. <https://doi.org/10.34229/2707-451X.26.1.8>

7. А.С. Баранов І.А., Хіміч О.М., Ніколаєвська О.А. Свідоцтво про реєстрацію авторського права на твір в Державній службі інтелектуальної власності України: Комп'ютерна програма "Комплекс програм Rubikrypt для шифрування та розшифрування даних на основі симетричних блочних криптографічних алгоритмів WBC1 та WBC2" . № 141653; опубл. 15.01.2026. Оригінал: CR1809150126

8. А.С. Баранов І.А., Хіміч О.М., Ніколаєвська О.А. Свідоцтво про реєстрацію авторського права на твір в Державній службі інтелектуальної власності України: Комп'ютерна програма " Комплекс програм P-Rubikrypt для шифрування та розшифрування даних на основі паралельних симетричних

блочних криптографічних алгоритмів PWBC1, PWBC1.1, PWBC2, PWBC2.1 та PWBCcuda ". № 145496; опубл. 13.04.2026. Оригінал: CR3637130426

9. Баранов І.А. Алгоритм WBC1. *Питання оптимізації обчислень (ПОО-XXXV): міжнародний симпозіум*, 24 – 29 вересня, 2009. С. 47

10. Баранов І.А. Реалізація блочних матричних алгоритмів на MIMD-комп'ютерах. *Сучасні проблеми прикладної математики та інформатики: XV Всеукр. наук. конф.*, 23-25 вересня, 2008 р. С. 52

11. Баранов І.А. Трёхмерный криптографический алгоритм WBC1. *Питання оптимізації обчислень – XXXIII: міжнародний симпозіум*, 23 – 28 вересня, 2007 р. С. 22

12. Баранов І.А. Некоторые подходы к эффективной реализации блочных матричных алгоритмов на MIMD – компьютерах. *Шоста міжнародна науково-практична конференція з програмування УкрПРОГ'2008*, 27-29 травня 2008 р., Україна, Київ С. 103-110.

13. Баранов І.А. Деякі підходи до ефективної реалізації паралельного симетричного алгоритму PWBC1 з використанням CUDA. *Питання оптимізації обчислень (ПОО- XLII): міжнародний симпозіум*, 21-25 вересня 2015. С. 140-141

14. Баранов І.А. Деякі підходи до аналізу криптографічної складності симетричного блочного алгоритму WBC1. *XIII Міжнародна науково-практична конференція «Глушковські читання. Сучасна кібернетика 2024»*, 6 грудня 2024 р. С. 15-18

15. Baranov Igor. Implementations of block symmetric cryptography algorithm WBC1 for computers with parallel architecture. *Computing Conference 2025*, 19 & 20 June 2025 in London, United Kingdom.

Вказані публікації відповідають Постанові Кабінету Міністрів України №44 від 12 січня 2022 року (зі змінами) «Про затвердження Порядку присудження ступеня доктора філософії та скасування рішення разової спеціалізованої вченої ради закладу вищої освіти, наукової установи про присудження ступеня доктора філософії».

Для захисту дисертаційної роботи запропоновано такий склад разової спеціалізованої вченої ради:

голова – д.ф.-м.н., професор, завідувач відділу оптимізації чисельних методів Інституту кібернетики імені В.М. Глушкова НАН України академік НАН України Задірака Валерій Костянтинівич;

рецензент – к.ф.-м.н., с.н.с., старший науковий співробітник відділу методів комбінаторної оптимізації та інтелектуальних інформаційних технологій Інституту кібернетики імені В.М. Глушкова НАН України Ходзінський Олександр Миколайович;

рецензент – к.ф.-м.н., с.н.с., провідний науковий співробітник відділу оптимізації чисельних методів Інституту кібернетики імені В.М. Глушкова НАН України Швідченко Інна Віталіївна;

опонент - перший проректор Державного університету інформаційно-комунікаційних технологій член-кореспондент НАН України Корченко Олександр Григорович;

опонент - д.т.н., с.н.с., професор кафедри Математичних методів захисту інформації Навчально-наукового фізико-технічного інституту Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського» член-кореспондент НАН України Кудін Антон Михайлович.

Голова засідання
академік НАН України,
док. фіз.-мат. наук, проф.,
завідувач відділу оптимізації чисельних
методів Інституту кібернетики
імені В.М. Глушкова НАН України

Валерій ЗАДІРАКА

Секретар засідання
канд. фіз.-мат. наук,
старший науковий співробітник
відділу чисельних методів та
комп'ютерного моделювання
Інституту кібернетики
імені В.М. Глушкова НАН України



Володимир СИДОРУК

Підпис	<i>В. Задірака</i>
	<i>В. Сидорук</i>
ЗАСВІДЧУЮ	
Зав. канц.	<i>Сидорук</i>
ІК НАН України	