ВИСНОВОК

про наукову новизну, теоретичне та практичне значення результатів дисертації Хамітова Віталія Миколайовича на тему «Моделі та методи підвищення конфеденційності та цілісності обміну зображеннями для групи довірених користувачів», поданої на здобуття наукового ступеня доктора філософії за спеціальністю 122 – Комп'ютерні науки, в галузі знань 12 – Інформаційні технології

Актуальність теми дисертаційної роботи теми зумовлена тим, що для низки професійних галузей потрібно здійснювати обмін зображеннями по відкритих каналах зв'язку з забезпеченням конфіденційності та цілосності зображень. До таких галузей належали телемедицина, криміналістичні та судові експертизи, передача супутникових зображень високого дозволу, інтернет речей. При цьому важливою вимогою є те, що обмін зображеннями має здійснюватися оперативно та бути ресурсонезалежним. Таким чином актуальною науково-технічним завданням є розробка моделей та методів обміну зображеннями для групи довірених користувачів з застосуванням нових підходів до шифрування зображень, що забезпечують виконання вимог конфеденційності та цілісності. Саме це завдання вирішується у роботі **Хамітова Віталія Миколайовича.**

Метою дослідження є підвищення рівня забезпеченості конфіденційності та цілісності цифрових зображень шляхом удосконалення методів захисних перетворень на основі хаотичних відображень.

Для досягнення мети дослідження необхідно вирішити такі завдання:

– провести аналіз основних проблем, обмежень та викликів, які виникають задачах створення механізмів забезпечення конфіденційності та цілісності обміну зображеннями для групи довірених користувачів;

– удосконалити критерій якості шифрування для оцінки якості шифрування зображень;

– удосконалити метод шифрування цифровими зображень на основі хаотичного відображення Tent з управлінням;

– удосконалити модель побудови псевдовипадкових послідовностей Фібоначчі;

– розробити метод обміну цифровими зображеннями для групи довірених користувачів;

– провести експериментальні дослідження, апробацію і впровадження отриманих теоретичних результатів.

Об'єкт дослідження – процес обміну цифровими зображеннями для групи довірених користувачів зображення.

Предмет дослідження – моделі та методи забезпечення конфеденційності та цілісності обміну зображеннями для групи довірених користувачів

Зв'язок дисертаційної роботи з науковими програмами, науковими напрямами Університету та кафедри

Дисертаційну роботу виконано у відповідності до пріоритетних тематичних напрямів наукових досліджень і науково-технічних розробок на період до 31 грудня року, наступного після припинення або скасування воєнного стану в Україні (Постанова Кабінету Міністрів України від 30.04.2024 р. № 476), згідно п. 1.2.1.1, 1.2.1.4, 1.2.4.6 і 1.2.1.7 «Основних наукових напрямів та найважливіших проблем фундаментальних досліджень у галузі природничих, технічних, суспільних і гуманітарних наук Національної академії наук України на 2019–2023 роки» (постанова Президії НАН України від 30.01.2019 р. № 30) та також у відповідності до планів науково-дослідних робіт Національного університету «Одеська політехніка» при виконанні держбюджетної теми: НДР роботи № 719-61/161 – «Інтелектуальна підтримка прийняття рішень при проєктуванні кісткових замінників для лікування воєнних травм» (номер державної реєстрації 0124U000388). Дисертант приймав участь у виконанні вказаних тем як співвиконавець (акт впровадження від 25.12.2025)

Особистий внесок здобувача в отриманні наукових результатів

Основні наукові положення, висновки і рекомендації, що містяться в дисертації та виносяться на захист, отримано здобувачем особисто в період з 2022 по 2026 рік.

У статті [1] внесок здобувача полягає в розробці методу шифрування зображень виходячи з хаотичного відображення Tent, який дозволив на підставі короткого ключа (насіння) згенерувати довгу псевдовипадкову послідовність; в статті [2] – отримала подальшого розвитку модель побудови псевдовипадкових послідовностей; у статтях [3, 10] – розроблено метод обміну зображеннями групи довірених користувачів, який відрізняється багаторівневим захистом, у статті [4] – запропоновано застосування для формування псевдовипадкових послідовністей нової динамічної системи, а саме узагальнене відображення Тент з керуванням, яке стабілізує цикли заданої довжини; у статті [5, 13] – показано важливість забезпечення захисту інформації в складних організаційно-технічних системах; у статті [6] – показано важливість забезпечення захист інформації в складних організаційно-технічних системах; у роботі [7] – показано доцільність нелінійних дискретних відображень для побудови псевдохаотичних криптосистем; у роботі [8, 11] – запропоновано інтегральний показник якості шифрування зображень; у роботі [9, 12] – досліджено метод обміну конфіденційними зображеннями з групою довірених користувачів.

Достовірність та обґрунтованість отриманих результатів та запропонованих автором рішень, висновків, рекомендацій

При вирішенні поставлених у дисертаційній роботі задач обґрунтовано використання інструментарію математичного та імітаційного моделювання. Всі зазначені в роботі припущення при моделюванні є загальноприйнятими та підтверджуються узгодженістю з розробками в сфері комп'ютерних наук.

Достовірність та обґрунтованість наукових положень, висновків та рекомендацій підтверджується даними експериментальних досліджень та практичними результатами.

Методи дослідження – системний аналіз; процесний підхід – для вивчення процесів, які відбуваються при обміні цифровими зображеннями для групи довірених користувачів; дискретна математика та теорія множин – для опису моделей з застосуванням хаотичних відображень та послідовностей; стеганографічні методи та теорія динамічних систем для удосконалення методів підвищення конфіденційності та цілісності обміну зображеннями для групи довірених користувачів.

Ступінь новизни основних результатів дисертаційної роботи порівняно з відомими дослідженнями аналогічного характеру.

Основний науковий результат полягає у розв'язанні важливої науково-практичної задачі підвищення конфіденційності та цілісності обміну зображеннями для групи довірених користувачів в інформаційних системах прикладного призначення.

У рамках виконаних досліджень отримано такі наукові результати:

– удосконалено інтегральний критерій якості захисних перетворень, який поєднує різні метрики якості шифрування (кореляційні, ентропійні та метрики резистентності), що побудований методом ідеальної точки, що дозволило проводити комплексне оцінювання якості шифрування та проводити обґрунтований вибір потокових та блочних шифрів;

– запропоновано метод захисного перетворення зображень на основі хаотичного відображення Тент з управлінням, що дозволило на підставі короткого ключа (насіння) згенерувати довгу псевдовипадкову послідовність, що значно підвищило швидкодію шифрування та дешифрування при збереженні стійкості шифрування за інтегральним критерієм якості;

– отримала подальший розвиток модель побудови псевдовипадкових послідовностей, яка заснована на зв'язку між похідними поліномів Чебишева другого роду та поліномами Чебишева, а також на зв'язку згорнутих чисел k-перетину послідовності Фібоначчі з похідними поліномів Чебишева другого роду через числа Люка, що дало можливість отримати сімейство узагальнених

послідовностей Фібоначчі, які можуть бути використані для підвищення рівня забезпечення цілосності інформації при її обміні у групі довірених користувачів;

– розроблено метод обміну зображеннями групи довірених користувачів, який відрізняється багаторівневим захистом з застосуванням захистного перетворння на основі модифікованого хаотичного відображення Тент та швидкодіючого протоколу на основі еліптичних кривих Монтґомері, що дозволило підвищило швидкодію шифрування та дешифрування при збереженні стійкості.

Наукове та практичне значення результатів дисертаційного дослідження

Наведені в дисертації результати досліджень дозволяють зробити висновок про наукову значимість роботи, що підтверджується проведеним моделюванням для обґрунтування ефективності запропонованих рішень. Теоретичне і практичне значення наукових положень можна оцінити як досить високе, що відкриває перспективи для галузі інформаційних технологій. Результати наукових досліджень здобувача є практично значимими, а саме:

Розроблений в дисертаційній роботі метод обміну зображеннями групи довірених користувачів, який відрізняється багаторівневим захистом з застосуванням шифрування на основі модифікованого хаотичного відображення Тент дозволив підвищити швидкодію шифрування та дешифрування при збереженні стійкості шифрування.

Розроблена в дисертаційній роботі модель побудови псевдовипадкових послідовностей дозволяє отримати сімейство узагальнених послідовностей Фібоначчі, які можуть бути використані для підвищення рівня забезпечення цілісності інформації для широкого кола завдань криптографічного захисту інформації. Отримані послідовності є оригінальними і згідно з поданою заявою були представлені в енциклопедії OEIS під номером A395431.

Розроблені в роботі наукові положення та практичні результати отримали впровадження у діяльності державного підприємства «Український науково-дослідний інститут медицини транспорту Міністерства охорони здоров'я України»

(*акт ДПУКРНДІ МТ МОЗ України від 02 березня 2026 р.*), у діяльності Військово-медичного клінічного центру Південного регіону (*довідка від 05 березня 2026 р.*) та знайшли відображення у навчальному (*довідка про впровадження результатів № 2100/61-07 від 30 грудня 2025 року*) та у науково-дослідницькому процесі (*довідка про впровадження результатів № 704/61-07 від 24.04.2026*) Національного університету «Одеська політехніка».

Повнота опублікування результатів дисертаційного дослідження та особистий внесок здобувачки до всіх наукових публікацій, опублікованих у співавторстві та зарахованих за темою дисертації

Основні результати дисертаційної роботи викладено у 13 публікаціях, зокрема 6 статей, з них – 4 статті у фахових періодичних виданнях України з технічних наук, з яких 2 – у категорії А (індексується в Scopus); 2 – у категорії Б, 2 статті у інших виданнях, 7 тез доповідей у матеріалах міжнародних наукових конференцій.

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

1. *Dmitrishin D. V.; Khamitov V. M.; Antoshchuk S. G.; Boltenkov V. O.* A Modified Image Encryption Algorithm Based on the chaotic Tent Map. *Herald of Advanced Information Technology* . 2026. 9(1). P. 9–19. https://doi.org/10.15276/hait.09.2026.01. *Видання включено до переліку наукових фахових видань України (категорія А). Видання включено до наукометричної бази SCOPUS*

https://hait.od.ua/index.php/journal/article/view/247

2. *Khamitov, V. M.* .; Dmitrishin, D. V. .; Stokolos, A. M. .; Gray, D. A. . Convolved Numbers of K-Section of the Fibonacci Sequence: Properties, Consequences. *Herald of Advanced Information Technology*. 2026. 9 (2). P. 129–139. https://doi.org/10.15276/hait.09.2026.09. *Видання включено до переліку наукових фахових видань України (категоріяБ). Видання включено до наукометричної бази SCOPUS.*

https://hait.od.ua/index.php/journal/article/view/247

3. *Khamitov V. M.* .; Boltenkov V. O. .; Antoshchuk S. G. A Method for Operative Sharing Confidential Images Among a Group of Trusted Users. AAIT. 9 (2). P. 200 -207. https://doi.org/10.15276/aait.09.2026.14. *Видання включено до переліку наукових фахових видань України (категорія Б)* .https://aait.od.ua/index.php/journal/article/view/252

4. *V. Khamitov*, S. Antoshchuk. Application of nonlinear discrete maps to construct pseudo-chaotic cryptosystems . *Proceedings of Odessa Polytechnic University*, 2025. Issue 2(72). P. 186-203. https://doi.org/10.15276/opu.2.70.2024.19. *Видання включено до переліку наукових фахових видань України (категорія Б)*
https://pratsi.op.edu.ua/index.php/pratsi/article/view/558

5. *Dyadyura, K., Prokopovich, I., Khamitov, V., Sikach, T., Vershkov, O.* Application of the Dynamic Programming Method in Process Measurement Problems When Assessing Interoperability. *Lecture Notes in Mechanical Engineering.* 2025. P. 699–711. https://DOI: 10.1007/978-3-031-82746-4_62
Видання включено до наукометричної бази SCOPUS

6. *Dyadyura K., Oborskyi G., Prokopovych I., Khamitov V., Holubiev M.* (2024). Optimal management in the operation of complex technical systems. *Journal of Engineering Sciences (Ukraine).* 2024. Vol. 11(1). P. B1–B9. https://doi.org/10.21272/jes.2024.11(1).b1. *Видання включено до наукометричної бази SCOPUS.*

7. Дмитришин Д. В., *Хамитов В. М.*, Болтьонков В. О., Антощук С. Г. Використання нелінійних дискретних відображень для побудови псевдохаотичних криптосистем. *Інформатика. Культура. Техніка.* 2025. Т.2. С. 209-214. https://doi.org/10.15276/ict.02.2025.31. *Видання включено до переліку наукових фахових видань України (категорія Б).*
https://ict.od.ua/index.php/journal/uk/issue/view/3

8. *Khamitov V.*, Dmytryshyn D., Gray D., and Stokolos A. Analytic summation of series involving higher-order derivatives of Chebyshev polynomials of the second kind and their applications to convolved linear recurrent sequences arXiv:2605.03200v2 [math.CV] https://doi.org/10.48550/arXiv.2605.03200

9. *Хамітов В. М.*, Болтьонков В. О. Формування інтегрального показника якості шифрування зображень //Global Interdisciplinary Summit: Frontier of Science and Future Technologies. Proceedings of International Scientific and Practical Conference. April 3, 2026 in Khalifa University Campus, Dubai, UAE. Prague: Publishing house Education and Science s.r.o., 2026. P. 143 – 146.

10. *Khamitov Vitaly*, Boltenkov Viktor. Method for exchange of confidential images to a group of trusted users //Collection of Scientific Papers with the Proceedings of the 8th International Scientific and Practical Conference «Global Directions in Scientific Research and Technological Development» (April 6-8, 2026, Valencia, Spain). European Open Science Space. 2026. P. 68 – 70.

11. *Хамітов В.М.*, Болтьонков В.О. Формування інтегрального показника якості шифрування зображень. Сучасні інформаційні технології та системи штучного інтелекту: матеріали 2-ї Міжнародної науково-практичної конференції. Частина 2. Харків -Яремче, 27-29 квітня 2026 р. – Х.: ХНУРЕ, 2026. С. 44-45

12. *Хамітов В.М.* Аналіз можливостей формування групи довірених користувачів для роботи із конфіденційними зображеннями *Матеріали XVI Міжнародної наукової конференції «Modern Information Technology – 2026»*, Одеса, 14–15 травня 2026 р. С. 179 – 180.

13. *В. Хамітов*, В. Болтьонков, С. Антощук. Система обміну конфіденційними зображеннями у групі довірених користувачів для медичного закладу. Сучасні технології біомедичної інженерії : матеріали *V Міжнародної науково-технічної конференції (6–8 травня 2026 р., м. Одеса, Україна).Odesa : Ecologiya, 2026. С. 182–184.

Апробація результатів дисертаційної роботи

Основні положення і практичні результати дисертаційної роботи доповідалися та одержали схвалення на таких конференціях:

XI Міжнародній науково-практичній конференції «ІНФОРМАТИКА. КУЛЬТУРА. ТЕХНІКА» «ІКТ-25»;

8th International Scientific and Practical Conference «Global Directions in Scientific Research and Technological Development» (April 6-8, 2026, Valencia, Spain);

International Scientific and Practical Conference. April 3, 2026 in Khalifa University Campus, Dubai, UAE;

2-й Міжнародній науково-практичній конференції. Харків -Яремче, 27-29 квітня 2026;

XVI Міжнародній науковій конференції «Modern Information Technology – 2026», Одеса, 14–15 травня 2026;

5th International Scientific and Technical Conference "Modern technologies of biomedical engineering" May 06-08, 2026, Odesa, Ukraine.

Відповідність дисертаційної роботи вимогам, що передбачено пунктами 6 і 7 «Порядку присудження ступеня доктора філософії та скасування рішення разової спеціалізованої вченої ради закладу вищої освіти, наукової установи про присудження ступеня доктора філософії»

З огляду на актуальність теми дисертації, обґрунтованість наукових положень, висновків і рекомендацій, які сформульовані в дисертації, сформульовану новизну, практичну цінність, повноту викладення в наукових публікаціях, відсутність порушень академічної доброчесності дисертаційна робота є завершеної науковою працею, що відповідає вимогам спеціальності 122 «Комп'ютерні науки».

За актуальністю, науковою новизною, теоретичним, методичним та практичним значення, обґрунтованістю одержаних результатів та оформленням, дисертаційна робота відповідає чинним вимогам Міністерства освіти і науки України, зокрема, п. п. 6 і 7 «Порядку присудження ступеня доктора філософії та скасування рішення разової спеціалізованої вченої ради закладу вищої освіти, наукової установи про присудження ступеня доктора філософії», а її автор — **Хамітов Віталій**

Миколайович — заслуговує на присудження їй ступеня доктора філософії у галузі знань 12 «Інформаційні технології» за спеціальністю 122 «Комп'ютерні науки».

Головуюча на засіданні
доктор технічних наук, професор,
професор кафедри інформаційних систем
Навчально-наукового інституту
комп'ютерних систем
Національного університету
«Одеська політехніка» Галина ЩЕРБАКОВА