

Облікова картка дисертації

I. Загальні відомості

Державний обліковий номер: 0826U005119

Особливі позначки: відкрита

Дата реєстрації: 03-09-2026

Статус: Запланована

Реквізити наказу МОН / наказу закладу:



II. Відомості про здобувача

Власне Прізвище Ім'я По-батькові:

1. Хамітов Віталій Миколайович

2. Vitalii M. Khamitov

Кваліфікація:

Ідентифікатор ORCID ID: 0009-0001-3045-8245

Вид дисертації: доктор філософії

Аспірантура/Докторантура: так

Шифр наукової спеціальності: 122

Назва наукової спеціальності: Комп'ютерні науки

Галузь / галузі знань: інформаційні технології

Освітньо-наукова програма зі спеціальності: Комп'ютерні науки

Дата захисту: 25-08-2026

Спеціальність за освітою: Систем управління і автоматики

Місце роботи здобувача: Організація відсутня

Код за ЄДРПОУ: 0000000000

Місцезнаходження: 00000, Київ, 00000, Україна

Форма власності: Змішана

Сфера управління:

Ідентифікатор ROR:

III. Відомості про організацію, де відбувся захист

Шифр спеціалізованої вченої ради (разової спеціалізованої вченої ради): PhD 16417

Повне найменування юридичної особи: Національний університет "Одеська політехніка"

Код за ЄДРПОУ: 43861328

Місцезнаходження: пр. Шевченка, Одеса, 65044, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

IV. Відомості про підприємство, установу, організацію, в якій було виконано дисертацію

Повне найменування юридичної особи: Національний університет "Одеська політехніка"

Код за ЄДРПОУ: 43861328

Місцезнаходження: пр. Шевченка, Одеса, 65044, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

V. Відомості про дисертацію

Мова дисертації: Українська

Коди тематичних рубрик: 20.54.02, 20.56.01

Тема дисертації:

1. Моделі та методи підвищення конфіденційності та цілісності обміну зображеннями для групи довірених користувачів
2. Models and methods for increasing the confidentiality and integrity of image sharing for a group of trusted users

Реферат/анотація:

1. Актуальність роботи пов'язана з розробкою моделі та методів підвищення конфіденційності та цілісності обміну зображеннями для групи довірених користувачів. Проведено аналіз проблеми підвищення конфіденційності та цілісності обміну зображеннями для групи довірених користувачів. Удосконалено інтегральний критерій якості шифрування, який поєднує різні метрики якості шифрування (кореляційні, ентропійні та метрики резистентності), побудований методом ідеальної точки, що дозволило проводити комплексне оцінювання якості шифрування та проводити обґрунтований вибір поточкових та блочних шифрів. Математичною основою для побудови нових методів генерації псевдовипадкових криптосистем є одновимірне відображення Тента із додатково введеним у це відображення предикативним управлінням. Запропоновано метод генерації псевдовипадкових послідовностей на основі відображення Тента. Проведено аналіз основних статистичних характеристик розроблених псевдовипадкових послідовностей для заданого ключа, який свідчить про їх псевдовипадковий характер, про відсутність закономірностей між окремими

частинами послідовності, що дозволяє рекомендувати їх для використання в криптографічних методах. Перевагою наведеного рішення є коротка довжина ключа та незалежність алгоритму від застосовуваної апаратно-програмної платформи. Розроблено метод шифрування зображень на основі хаотичного відображення Тент з управлінням, що дозволило на підставі короткого ключа (насіння) генерувати довгу псевдовипадкову послідовність, що значно підвищило швидкодію шифрування та розшифрування 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 цілісності інформації при її обміні нею у групі довірених користувачів. Запропоновано методику дослідження ефективності протоколів групового узгодження ключів. Показано, що при формуванні груп довірених користувачів з невеликим числом користувачів та малою динамікою найбільш ефективним є поєднання протоколу Бурместера-Десмедта та еліптичної кривої Монтгомері. Розроблено метод обміну зображеннями групи довірених користувачів, який відрізняється багаторівневим захистом з застосуванням захисного перетворення на основі модифікованого хаотичного відображення Тент та швидкодіючого протоколу на основі еліптичних кривих Монтгомері, що дозволило підвищити швидкодію шифрування та розшифрування при збереженні стійкості. Загалом, результати апробації свідчать про практичну придатність запропонованих методів до впровадження в системи реального часу. Висновки, отримані на основі експериментальних вимірювань та порівнянь із базовими підходами, підтверджують доцільність їх використання в інформаційних системах. Результати дисертаційної роботи 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 та науково-дослідницькому процесі Національного університету «Одеська політехніка».

2. The relevance of the work is related to the development of a model and methods for increasing the confidentiality and integrity of image exchange for a group of trusted users. The problem of increasing the confidentiality and integrity of image sharing for a group of trusted users was analyzed. An integrated encryption quality criterion has been improved, which combines various encryption quality metrics (correlation, entropy, and resistance metrics), constructed using the ideal point method, which allowed for a comprehensive assessment of encryption quality and a reasoned selection of stream and block ciphers. The mathematical basis for constructing new methods for generating pseudorandom cryptosystems is the one-dimensional Tent mapping with predicative control additionally introduced into this mapping. A method for generating pseudorandom sequences based on the Tent mapping is proposed. An analysis of the main statistical characteristics of the developed pseudorandom sequences for a given key is carried out, which indicates their pseudorandom nature, the absence of regularities between individual parts of the sequence, which allows us to recommend them for use in cryptographic methods. The advantage of the presented solution is the short key length and the independence of the algorithm from the hardware and software platform used. A method of image encryption based on a chaotic Tent mapping with control is proposed, which allows generating a long pseudo-random sequence based on a short key (seed), which significantly increases the speed of encryption and decryption while maintaining the stability of encryption according to the integral quality criterion. The model for constructing pseudorandom sequences has been further developed, which is based on the connection between the derivatives of Chebyshev polynomials of the second kind and Chebyshev polynomials, as well as on the connection of the collapsed numbers of the k -section of the Fibonacci sequence with the derivatives of Chebyshev polynomials of the second kind through Luke numbers, which made it possible to obtain a family of generalized Fibonacci sequences that can be used to increase the level of ensuring the integrity of information when it is exchanged in a group of trusted users. A methodology for studying the effectiveness of group key agreement protocols is proposed. It is shown that when forming groups of

trusted users with a small number of users and low dynamics, the most effective is the combination of the Burmester-Desmedt protocol and the Montgomery elliptic curve. The method for exchanging images of a group of trusted users has been developed, which is characterized by multi-level protection using a protective transformation based on a modified chaotic Tent mapping and a high-speed protocol based on Montgomery elliptic curves, which allowed increasing the speed of encryption and decryption while maintaining stability. In general, the results of the testing indicate the practical suitability of the proposed methods for implementation in real-time systems. The conclusions obtained on the basis of experimental measurements and comparisons with basic approaches confirm the feasibility of their use in information systems. The results of the dissertation work were implemented in the activities of the state enterprise «Ukrainian Scientific Research Institute of Transport Medicine of the Ministry of Health of Ukraine» (act of the State Enterprise Ukrainian Scientific Research Institute of Transport Medicine of the Ministry of Health of Ukraine dated March 2, 2026), in the activities of the Military Medical Clinical Center of the Southern Region (certificate dated March 5, 2026) and were reflected in the educational and scientific research process of the Odesa National Polytechnic University

Державний реєстраційний номер ДіР:

Пріоритетний напрям розвитку науки і техніки: Фундаментальні наукові дослідження з найбільш важливих проблем розвитку науково-технічного, соціально-економічного, суспільно-політичного, людського потенціалу для забезпечення конкурентоспроможності України у світі та сталого розвитку суспільства і держави

Стратегічний пріоритетний напрям інноваційної діяльності: Розвиток сучасних інформаційних, комунікаційних технологій, робототехніки

Підсумки дослідження: Нове вирішення актуального наукового завдання

Публікації:

- 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>
- 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>
- 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>
- 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>
- 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
- 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](https://doi.org/10.21272/jes.2024.11(1).b1)
- Дмитришин Д. В., Хамитов В. М., Болтъонков В. О., Антошук 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>
- 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>

- Хамітов В. М., Болтънков 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
- 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
- Хамітов В.М., Болтънков 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
- 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
- В. Хамітов, В. Болтънков, С. Антошук. 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

Наукова (науково-технічна) продукція: програмні продукти, програмно-технологічна документація

Соціально-економічна спрямованість: забезпечення промисловості чи населення новим видом інформаційно-комунікаційних послуг

Охоронні документи на ОПІВ:

Впровадження результатів дисертації: Впроваджено

Зв'язок з науковими темами: 0124U000388

VI. Відомості про наукового керівника/керівників (консультанта)

Власне Прізвище Ім'я По-батькові:

1. Антошук Світлана Григорівна

2. Svitlana H. Antoshchuk

Кваліфікація: д. т. н., професор, 05.13.06

Ідентифікатор ORCID ID: 0000-0002-9346-145X

Додаткова інформація:

Повне найменування юридичної особи: Національний університет "Одеська політехніка"

Код за ЄДРПОУ: 43861328

Місцезнаходження: пр. Шевченка, Одеса, 65044, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

VII. Відомості про офіційних опонентів та рецензентів

Офіційні опоненти

Власне Прізвище Ім'я По-батькові:

1. Смеляков Кирило Сергійович
2. Kyrylo Smelyakov

Кваліфікація: д.т.н., професор, 01.05.02

Ідентифікатор ORCID ID: 0000-0001-9938-5489

Додаткова інформація:

Повне найменування юридичної особи: Харківський національний університет радіоелектроніки

Код за ЄДРПОУ: 02071197

Місцезнаходження: проспект Науки, Харків, Харківський р-н., 61166, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

Власне Прізвище Ім'я По-батькові:

1. Казакова Надія Феліксівна
2. Надія F. Kazakova

Кваліфікація: д.т.н., професор, 05.13.06

Ідентифікатор ORCID ID: 0000-0003-3968-4094

Додаткова інформація:

Повне найменування юридичної особи: Одеський національний економічний університет

Код за ЄДРПОУ: 02071079

Місцезнаходження: вул. Преображенська, Одеса, 65082, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

Рецензенти

Власне Прізвище Ім'я По-батькові:

1. Григоренко Світлана Миколаївна
2. Svitlana M. Hryhorenko

Кваліфікація: к.т.н., 05.13.21

Ідентифікатор ORCID ID: 0009-0006-4551-8243

Додаткова інформація:

Повне найменування юридичної особи: Національний університет "Одеська політехніка"

Код за ЄДРПОУ: 43861328

Місцезнаходження: пр. Шевченка, Одеса, 65044, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

Власне Прізвище Ім'я По-батькові:

1. Сперанський Віктор Олександрович

2. Viktor O. Speranskyi

Кваліфікація: к.т.н., доц., 01.05.02

Ідентифікатор ORCID ID: 0000-0002-8042-1790

Додаткова інформація:

Повне найменування юридичної особи: Національний університет "Одеська політехніка"

Код за ЄДРПОУ: 43861328

Місцезнаходження: пр. Шевченка, Одеса, 65044, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

VIII. Заключні відомості

**Власне Прізвище Ім'я По-батькові
голови ради**

Щербакова Галина Юріївна

**Власне Прізвище Ім'я По-батькові
головуючого на засіданні**

Щербакова Галина Юріївна

**Відповідальний за підготовку
облікових документів**

Антощук Світлана Григорівна

Реєстратор

Юрченко Тетяна Анатоліївна

**Керівник відділу УкрІНТЕІ, що є
відповідальним за реєстрацію наукової
діяльності**



Юрченко Тетяна Анатоліївна