

Облікова картка дисертації

I. Загальні відомості

Державний обліковий номер: 0826U004430

Особливі позначки: відкрита

Дата реєстрації: 07-08-2026

Статус: Наказ про видачу диплома

Реквізити наказу МОН / наказу закладу: Наказ ВНТУ №394 від 23.09.2026р.



II. Відомості про здобувача

Власне Прізвище Ім'я По-батькові:

1. Ціхоцький Микита Сергійович

2. Mykyta Tsikhotskyi

Кваліфікація:

Ідентифікатор ORCID ID: Не застосовується

Вид дисертації: доктор філософії

Аспірантура/Докторантура: так

Шифр наукової спеціальності: 125

Назва наукової спеціальності: Кібербезпека та захист інформації

Галузь / галузі знань: інформаційні технології

Освітньо-наукова програма зі спеціальності: Кібербезпека

Дата захисту: 07-09-2026

Спеціальність за освітою: Кібербезпека

Місце роботи здобувача: Організація відсутня

Код за ЄДРПОУ: 00000000

Місцезнаходження: -----, 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 15581

Повне найменування юридичної особи: Вінницький національний технічний університет

Код за ЄДРПОУ: 02070693

Місцезнаходження: вул. Хмельницьке шосе, Вінниця, Вінницький р-н., 21021, 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: Вінницький національний технічний університет

Код за ЄДРПОУ: 02070693

Місцезнаходження: вул. Хмельницьке шосе, Вінниця, Вінницький р-н., 21021, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

V. Відомості про дисертацію

Мова дисертації: Українська

Коди тематичних рубрик: 50.37.23

Тема дисертації:

1. Методи криптографічного захисту зображень
2. Methods of cryptographic image protection

Реферат/анотація:

1. Ціхоцький М. С. Методи криптографічного захисту зображень. Дисертація на здобуття наукового ступеня доктора філософії в галузі знань 12 «Інформаційні технології» за спеціальністю 125 «Кібербезпека». Вінницький національний технічний університет, Вінниця, 2026. Дисертаційна робота присвячена підвищенню ефективності криптографічного захисту зображень у розподілених інформаційних системах. Актуальність дослідження зумовлена потребою захищеного зберігання, передавання та резервного копіювання графічних даних, для яких небажаним є розміщення повного відкритого подання на одному вузлі. У роботі розглянуто поєднання шифрування зображень із розподілом їх секретного вмісту на частки, що дає змогу формалізувати умови доступу та зменшити ризик відновлення зображення за окремими фрагментами. Метою дисертаційної роботи є пришвидшення процесів шифрування та розподілу секретного вмісту зображень шляхом розробки методів і засобів шифрування та схем розподілу секрету типу (n,n) та (k,n) . Об'єктом дослідження є процеси шифрування зображення та розподілу секретного вмісту зображень. Предметом дослідження є методи та засоби шифрування зображення та розподілу секретного вмісту

зображень. Наукова новизна дисертаційної роботи полягає у розробленні методу шифрування зображень, методу порогового розподілу секретного вмісту зображень за (k,n) -схемою та удосконаленні методу розподіленого зберігання зображень за (n,n) -схемою. Запропонований метод шифрування ґрунтується на поєднанні побайтової підстановки та перестановки елементів у межах усього вектора зображення. Для формування відтворюваної перестановки використано псевдовипадкову послідовність, поділ простору індексів на піддіапазони та систему лічильників. У роботі розроблено методи розподілу секретного вмісту зображень за (n,n) - та (k,n) -схемами. Для (n,n) -схеми використано попередньо зашифроване зображення, що дає змогу пришвидшити формування часток. Для (k,n) -схеми запропоновано використання дилерської складової, яка забезпечує відновлення зашифрованого вектора за допустимою множиною часток і зменшує сумарний обсяг індивідуальних часток. Також розроблено програмні засоби реалізації запропонованих методів, зокрема варіанти шифрування SP та PS, коаліційну і спрощену реалізації порогового розподілу. Експериментальна перевірка підтвердила працездатність запропонованих методів. Оцінювання статистичних властивостей зашифрованих зображень показало наближення розподілу байтів до рівномірного, зростання ентропії та зменшення кореляційних залежностей між сусідніми елементами. Тестування за методикою NIST SP 800-22 підтвердило відсутність виражених закономірностей у сформованих бітових послідовностях. Для запропонованих схем розподілу підтверджено коректність відновлення за допустимими множинами часток і зменшення сумарного обсягу даних для розглянутих конфігурацій. Практичне значення результатів полягає у можливості використання розроблених методів і програмних засобів у системах захищеного зберігання, передавання та відновлення зображень, зокрема в розподілених і пірингових середовищах. Результати дисертаційної роботи впроваджено в ТОВ «Каскад-Безпека», ТОВ «ІНТЕРНЕТ-РЕКЛАМА РІА» та в освітній процес кафедри захисту інформації Вінницького національного технічного університету. Ключові слова: криптосистема, шифрування, розшифрування, розподіл конфіденційних зображень, розподілені обчислення, група довірених користувачів, пірингова мережа, кіберзагроза, маршрутизація, приховування даних, біомедичні зображення, JPEG, стиснення зображень, статистичний аналіз, показник якості.

2. Tsikhotskyi M. S. Methods of Cryptographic Protection of Images. Dissertation for the degree of Doctor of Philosophy in the field of knowledge 12 "Information Technologies", specialty 125 "Cybersecurity". Vinnytsia National Technical University, Vinnytsia, 2026. The dissertation is devoted to improving the efficiency of cryptographic protection of images in distributed information systems. The relevance of the research is determined by the need for protected storage, transmission and backup of graphical data when storing a complete open representation of an image on a single node is undesirable. The work considers the combination of image encryption with the sharing of secret image content into separate shares, which makes it possible to formalize access conditions and reduce the risk of recovering the image from individual fragments. The aim of the dissertation is to speed up the processes of encryption and sharing of the secret content of images by developing encryption methods and tools as well as secret sharing schemes of the (n,n) and (k,n) types. The object of the research is the processes of image encryption and sharing of secret image content. The subject of the research is methods and tools for image encryption and sharing of secret image content. The scientific novelty of the dissertation consists in the development of an image encryption method, a threshold method for sharing the secret content of images according to a (k,n) scheme, and the improvement of a distributed image storage method according to an (n,n) scheme. The proposed encryption method is based on the combination of byte-wise substitution and permutation of elements within the entire image vector. A pseudorandom sequence, division of the index space into subranges, and a system of counters are used to form a reproducible permutation. The dissertation develops methods for sharing the secret content of images according to (n,n) and (k,n) schemes. For the (n,n) scheme, a pre-encrypted image is used, which speeds up the share generation procedure. For the (k,n) scheme, the use of a dealer component is proposed; this component provides recovery of the encrypted vector by an admissible set of shares and reduces the total volume of individual shares. Software tools implementing the proposed methods have also been developed, including the SP and PS encryption variants and coalition-based and simplified implementations of threshold sharing. Experimental verification confirmed the operability of the

proposed methods. Evaluation of the statistical properties of encrypted images showed that the byte distribution approaches a uniform one, entropy increases, and correlations between neighboring elements decrease. Testing according to NIST SP 800-22 confirmed the absence of pronounced patterns in the generated bit sequences. For the proposed sharing schemes, the correctness of recovery by admissible sets of shares and the reduction of the total data volume for the considered configurations were confirmed. The practical significance of the obtained results lies in the possibility of using the developed methods and software tools in systems for protected storage, transmission and recovery of images, particularly in distributed and peer-to-peer environments. The results of the dissertation have been implemented at "КАСКАД-Безпека" LLC, "ІНТЕРНЕТ-РЕКЛАМА RIA" LLC, and in the educational process of the Information Protection Department of Vinnytsia National Technical University. Keywords: cryptosystem, encryption, decryption, sharing confidential images, distributed computing, group of trusted users, peer-to-peer network, cyber threat, routing, data hiding, biomedical images, JPEG, image compression, statistical analysis, quality indicator.

Державний реєстраційний номер ДіР:

Пріоритетний напрям розвитку науки і техніки: Інформаційні та комунікаційні технології

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

Підсумки дослідження: Нове вирішення актуального наукового завдання

Публікації:

- 1. Ціхоцький М.С., Лужецький В.А. Аналіз методів розподілу секрету Електронне фахове наукове видання "Кібербезпека: освіта, наука, техніка", вип. 1, вип. 25, с. 279–293, Вер 2024.
- 2. Luzhetsky V., Tsikhotskyi M. Image encryption and distribution method based on LFSR and counters. Information Technologies and Computer Engineering, 22(3), 77-88, 2025.
- 3. Лужецький В.А., Ціхоцький М.С. Розподіл секретного вмісту даних за (k,n)-схемою з використанням зашифрованих блоків. Вісник Вінницького політехнічного інституту. №5, 113-120, 2025.
- 4. Лужецький В.А., Ціхоцький М.С. Схема порогового розподілення секрету «k,n» МНПК «ІТКМ-2024». 21 – 24 травень 2024.
- 5. Лужецький В.А., Ціхоцький М.С. Протокол анонімної передачі зображень / Міжнародна науково-практична конференція "Інформаційні технології та комп'ютерне моделювання" (МНПК «ІТКМ-2024»). 227-228. 18 – 22 травень 2026.
- 6. Ціхоцький М.С. Метод розподілу зашифрованого зображення за (k,n)-схемою з використанням коаліцій учасників / Матеріали міжнародної науково-практичної інтернет-конференції «Молодь в науці: дослідження, проблеми, перспективи (МН-2026)» Вінниця: ВНТУ, 2026.
- 7. Ціхоцький М. С. Протокол розподіленого зберігання медичних даних. ITSec: Безпека інформаційних технологій : Матеріали XV Міжнар. науково-техн. конф., м. Тернопіль, 27–29 трав. 2026 р. Тернопіль-Київ : ТНТУ-ДУІКТ, 2026. С. 82–84.

Наукова (науково-технічна) продукція: методи, теорії, гіпотези

Соціально-економічна спрямованість: удосконалення методів захисту інформації

Охоронні документи на ОПІВ:

Впровадження результатів дисертації: Планується до впровадження

Зв'язок з науковими темами:

VI. Відомості про наукового керівника/керівників (консультанта)

Власне Прізвище Ім'я По-батькові:

1. Лужецький Володимир Андрійович
2. Volodymyr Luzhetskyi

Кваліфікація: д. т. н., професор, 01.05.02, 05.13.05

Ідентифікатор ORCID ID: 0009-0003-2218-1527

Додаткова інформація:

Повне найменування юридичної особи: Вінницький національний технічний університет

Код за ЄДРПОУ: 02070693

Місцезнаходження: вул. Хмельницьке шосе, Вінниця, Вінницький р-н., 21021, 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. Антошук Світлана Григорівна
2. Svitlana H. Antoshchuk

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

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

Додаткова інформація: <https://publons.com/researcher/8393582500>;
https://scholar.google.com.ua/citations?user=6_30H00AAAAJ&hl=ru; Web of Science ResearcherID:
8393582500; <https://www.scopus.com/authid/detail.uri?authorId=8393582500>

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. Авраменко Віктор Васильович
2. Viktor V. Avramenko

Кваліфікація: к.т.н., доц., 05.13.01

Ідентифікатор ORCID ID: 0000-0002-6317-6711

Додаткова інформація:

Повне найменування юридичної особи: Сумський державний університет

Код за ЄДРПОУ: 05408289

Місцезнаходження: вул. Харківська, Суми, Сумський р-н., 40007, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

Рецензенти

Власне Прізвище Ім'я По-батькові:

1. Майданюк Володимир Павлович

2. Volodymyr P. Maidaniuk

Кваліфікація: к. т. н., доцент, 05.13.05

Ідентифікатор ORCID ID: 0000-0002-2386-6603

Додаткова інформація:

Повне найменування юридичної особи: Вінницький національний технічний університет

Код за ЄДРПОУ: 02070693

Місцезнаходження: вул. Хмельницьке шосе, Вінниця, Вінницький р-н., 21021, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

Власне Прізвище Ім'я По-батькові:

1. Куперштейн Леонід Михайлович

2. Leonid M. Kupershtein

Кваліфікація: к. т. н., доц., 05.13.05

Ідентифікатор ORCID ID: 0000-0001-6737-7134

Додаткова інформація:

Повне найменування юридичної особи: Вінницький національний технічний університет

Код за ЄДРПОУ: 02070693

Місцезнаходження: вул. Хмельницьке шосе, Вінниця, Вінницький р-н., 21021, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

VIII. Заключні відомості

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

Романюк Олександр Никифорович

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

Романюк Олександр Никифорович

**Відповідальний за підготовку
облікових документів**

Іванчук Ярослав Володимирович

Реєстратор

Юрченко Тетяна Анатоліївна

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



Юрченко Тетяна Анатоліївна