Облікова картка дисертації

I. Загальні відомості

Державний обліковий номер: 0825U003396

Особливі позначки: відкрита

Дата реєстрації: 12-08-2025

Статус: Запланована

Реквізити наказу МОН / наказу закладу:

II. Відомості про здобувача

Власне Прізвище Ім'я По-батькові:

1. Руда Христина Степанівна

2. Khrystyna S. Ruda

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: 22-08-2025

Спеціальність за освітою: кібербезпека

Місце роботи здобувача:

Код за ЄДРПОУ:

Місцезнаходження:

Форма власності:

Сфера управління:

Ідентифікатор ROR: Не застосовується

III. Відомості про організацію, де відбувся захист

Шифр спеціалізованої вченої ради (разової спеціалізованої вченої ради): PhD 10472

Повне найменування юридичної особи: Національний університет "Львівська політехніка"

Код за ЄДРПОУ: 02071010

Місцезнаходження: вул. Степана Бандери, буд. 12, Львів, 79013, 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 "Львівська політехніка"

Код за ЄДРПОУ: 02071010

Місцезнаходження: вул. Степана Бандери, буд. 12, Львів, 79013, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

V. Відомості про дисертацію

Мова дисертації: Українська

Коди тематичних рубрик: 20.56.02

Тема дисертації:

1. Удосконалення методів та засобів біометричної автентифікації за голосом з застосуванням технологій машинного навчання

2. Advancement of methods and tools for voice-based biometric authentication using machine learning technologies.

Реферат:

1. В роботі обґрунтовано доцільність використання нейромережевих технологій машинного навчання для підвищення точності та стійкості голосової біометричної автентифікації. Запропоновано концептуальну модель системи, що реалізує поєднання класичних методів обробки мовного сигналу з сучасними нейронними архітектурами (ECAPA-TDNN, TitaNet, WavLM) і використовує векторні ембедінги для представлення голосових ознак. Проведено формалізацію основних етапів автентифікаційного процесу, зокрема відбору мовного сигналу, його попередньої обробки, екстракції ознак та верифікації особи на основі порівняння ембедінгів. Розроблено та реалізовано експериментальну методику оцінювання ефективності системи в умовах spoofing-атак із використанням синтетичних голосових зразків, згенерованих за допомогою сучасних моделей голосового клонування (RVC, VITS, XTTS, ElevenLabs). Проведено аналіз стійкості до атак із різними типами текстового контенту та здійснено порівняння результативності

нейромережевих архітектур. Досліджено вплив масштабування системи та варіативності мовців на рівень точності верифікації. У першому розділі «Аналіз особливостей процесу розпізнавання людини за голосом» здійснено комплексний аналіз історичних передумов, теоретичних засад та практичних підходів до побудови систем біометричної автентифікації за голосом. Проведено класифікацію методів голосової автентифікації за принципами їх реалізації – від класичних і статистичних моделей до сучасних нейромережевих архітектур і ембедінг-орієнтованих підходів. Деталізовано архітектурні особливості відповідних моделей та проаналізовано їхній потенціал для реалізації атак типу voice spoofing. Наголошено на необхідності впровадження антиспуфінгових механізмів, а також розглянуто етичні виклики, пов'язані з використанням синтетичних голосів, що формує підґрунтя для подальшого дослідження стійкості систем до подібних загроз. У другому розділі «Концептуальна модель голосової автентифікації на основі нейромережевих трансформерів» запропоновано концептуальну модель сучасної системи голосової біометрії, що інтегрує класичні та нейромережеві підходи до обробки мовного сигналу. Розглянуто ключові етапи процесу автентифікації: від відбору й попередньої обробки голосового зразка до формування голосового ембедінгу та здійснення верифікації шляхом порівняння тестового і реєстраційного шаблонів. Обґрунтовано ефективність використання глибоких моделей, зокрема ECAPA-TDNN, TitaNet і WavLM, у задачах побудови стійких до шуму і варіативності вхідних даних представлень користувача. Проведено порівняльний аналіз класичних (MFCC, LPC, i-vector) та сучасних нейромережевих методів екстракції ознак, показано їхні переваги й недоліки. Особливу увагу приділено проблемам безпеки, впровадженню стандартів ISO/IEC 30107 і C2PA, а також формуванню моделей, здатних протистояти атакам із застосуванням синтетичних голосів. У третьому розділі «Імплементація вдосконалення системи голосової автентифікації» здійснено практичну реалізацію та всебічний аналіз роботи вдосконаленої системи біометричної автентифікації за голосом. Побудована архітектура системи на основі ембедінгів, де описано механізми реєстрації голосових профілів, налаштування порогових значень та процедуру верифікації користувачів. Проведено порівняння властивостей косинусної, евклідової, мангеттенської та Махаланобісової відстаней, із акцентом на доцільності використання косинусної відстані як найбільш стійкої до акустичних флуктуацій. Деталізовано модулі обробки тестових зразків, екстракції ембедінгів за допомогою моделей ECAPA, TitaNet, WavLM, а також процедури прийняття рішень на основі обчисленої відстані. Запропоновано методику побудови тестових пар зразків для розрахунку FAR і FRR, проведено калібрування порогів для кожної моделі з урахуванням її метричних властивостей, яка дозволила забезпечити адаптивність системи до різних моделей ембедінгів і покращити загальну точність класифікації. У четвертому розділі «Оцінювання стійкості системи до атак типу voice spoofing з використанням технологій клонування голосу» представлено експериментальну методику перевірки захищеності біометричної системи автентифікації за голосом у сценаріях, що моделюють цілеспрямовані атаки із застосуванням синтетичного мовлення. Для дослідження було згенеровано масштабний корпус аудіозразків за допомогою моделей RVC, XTTS, ElevenLabs і Tortoise, що імітували голоси зареєстрованих користувачів у системі. Здійснено класифікацію результатів автентифікації на основі косинусної подібності ембедінгів, отриманих за допомогою моделей ECAPA, TitaNet, WavLM та інших. Продемонстровано залежність точності класифікації від типу клонувальної технології та сценарію текстового наповнення. У висновках викладено основні результати і рекомендації, які випливають з проведених досліджень, представлено та охарактеризовано кількісні оцінки показників ефективності в умовах використання запропонованих рішень.

2. The paper substantiates the feasibility of using neural network machine learning technologies to improve the accuracy and stability of voice biometric authentication. A conceptual model of a system is proposed that implements a combination of classical speech signal processing methods with modern neural architectures (ECAPA-TDNN, TitaNet, WavLM) and uses vector embeddings to represent voice features. The main stages of the authentication process are formalized, in particular, speech signal selection, its pre-processing, feature extraction and face verification based on embedding comparison. An experimental methodology for assessing the effectiveness of the system under spoofing attacks using synthetic voice samples generated using modern voice cloning models (RVC, VITS, XTTS, ElevenLabs) is developed and implemented. An analysis of resistance to attacks

with different types of text content is carried out and the effectiveness of neural network architectures is compared. The influence of system scaling and speaker variability on the level of verification accuracy is studied. In the first section, “Analysis of the features of the voice recognition process,” a comprehensive analysis of historical background, theoretical foundations, and practical approaches to building voice biometric authentication systems is carried out. Voice authentication methods are classified according to the principles of their implementation. The architectural features of the corresponding models are detailed and their potential for implementing voice spoofing attacks is analyzed. The need to implement anti-spoofing mechanisms is emphasized, and ethical challenges associated with the use of synthetic voices are considered, which forms the basis for further research into the resistance of systems to such threats. In the second section, “Conceptual model of voice authentication based on neural network transformers,” a conceptual model of a modern voice biometrics system is proposed that integrates classical and neural network approaches to speech signal processing. The key stages of the authentication process are considered: from the selection and pre-processing of a voice sample to the formation of a voice embedding and verification by comparing the test and registration templates. The effectiveness of using deep models, in particular ECAPA-TDNN, TitaNet and WavLM, in the tasks of building user representations that are resistant to noise and variability of input data is substantiated. A comparative analysis of classical (MFCC, LPC, i-vector) and modern neural network methods for feature extraction is carried out, their advantages and disadvantages are shown. Special attention is paid to security issues, the implementation of ISO/IEC 30107 and C2PA standards, as well as the formation of models capable of resisting attacks using synthetic voices. In the third section, “Implementation of the Improvement of the Voice Authentication System”, a practical implementation and a comprehensive analysis of the operation of the improved biometric voice authentication system are carried out. The architecture of the system based on embeddings is built, where the mechanisms for registering voice profiles, setting threshold values, and the user verification procedure are described. The properties of cosine, Euclidean, Manhattan, and Mahalanobis distances are compared, with an emphasis on the feasibility of using cosine distance as the most resistant to acoustic fluctuations. The modules for processing test samples, extracting embeddings using the ECAPA, TitaNet, and WavLM models, as well as the decision-making procedures based on the calculated distance are detailed. A method for constructing test pairs of samples for calculating FAR and FRR is proposed, and thresholds are calibrated for each model taking into account its metric properties, which allowed ensuring the adaptability of the system to different embedding models and improving the overall classification accuracy. The fourth section, “Evaluation of the system’s resistance to voice spoofing attacks using voice cloning technologies,” presents an experimental methodology for testing the security of a biometric voice authentication system in scenarios that simulate targeted attacks using synthetic speech. For the study, a large-scale corpus of audio samples was generated using the RVC, XTTS, ElevenLabs, and Tortoise models that simulated the voices of registered users in the system. The authentication results were classified based on the cosine similarity of embeddings obtained using the ECAPA, TitaNet, WavLM, and other models. The dependence of the classification accuracy on the type of cloning technology and the text content scenario was demonstrated. The conclusions present the main results and recommendations that arise from the research conducted, and quantitative assessments of the performance indicators under the conditions of using the proposed solutions are presented and characterized.

Державний реєстраційний номер ДіР: № 0124U000407

Пріоритетний напрям розвитку науки і техніки: Інформаційні та комунікаційні технології

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

Підсумки дослідження: Теоретичне узагальнення і вирішення важливої наукової проблеми

Публікації:

- 1. Руда Х. С. Дослідження масштабованості біометричних систем автентифікації на основі вбудовування голосу // Social Development and Security. – 2025. – Т. 15, №. 1. – Р. 161–170.
- 2. Руда Х. С., Сабодашко Д. В., Микитин Г. В., Швед М. Є., Бордуляк С. М., Коршун Н. Порівняння методів цифрової обробки сигналів та моделей глибинного навчання у голосовій аутентифікації // Кібербезпека: освіта, наука, техніка. – 2024. – № 5 (25). – С. 140–160.
- 3. Заєць І. С., Бридінський В. А., Сабодашко Д. В., Руда Х. С., Хома Ю. В., Швед М. Є. Використання ембедінгів голосу в інтегрованих системах для діаризації мовців та виявлення зловмисників // Комп'ютерні системи та мережі. – 2024. – Вип. 6, № 1. – С. 54–66.
- 4. Микитин Г. В., Руда Х. С. Концептуальний підхід до виявлення deepfake-модифікацій біометричного зображення засобами нейронних мереж // Комп'ютерні системи та мережі. – 2024. – Вип. 6, № 1. – С. 124–132.
- 5. Микитин Г. В., Руда Х. С., Яремчук Ю. Є. Методологія безпеки нейромережевих інформаційних технологій виявлення deepfake модифікацій біометричного зображення // Вісник Вінницького політехнічного інституту. – 2024. – № 1 (172). – С. 74–80.
- 6. Zaiets I., Brydinskyi V., Sabodashko D., Khoma Y., Ruda K. Integrated system for speaker diarization and intruder detection using speaker embeddings // CEUR Workshop Proceedings. – 2024. – Vol. 3654: Cybersecurity providing in information and telecommunication systems 2024. Proceedings of the workshop cybersecurity providing in information and telecommunication systems (CPITS 2024) Kyiv, Ukraine, February 28, 2024 (online).
- 7. Dudykevych V., Yevseiev S., Mykytyn G., Ruda K., Hulak H. Detecting deepfake modifications of biometric images using neural networks // CEUR Workshop Proceedings. – 2024. – Vol. 3654: Cybersecurity providing in information and telecommunication systems 2024. Proceedings of the workshop cybersecurity providing in information and telecommunication systems (CPITS 2024) Kyiv, Ukraine, February 28, 2024 (online).

Наукова (науково-технічна) продукція:

Соціально-економічна спрямованість:

Охоронні документи на ОПІВ:

Впровадження результатів дисертації: Впроваджено

Зв'язок з науковими темами: № 0124U000407

VI. Відомості про наукового керівника/керівників (консультанта)

Власне Прізвище Ім'я По-батькові:

1. Микитин Галина Василівна

2. Halyna V. Mykytyn

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

Ідентифікатор ORCID ID: Не застосовується

Додаткова інформація:

Повне найменування юридичної особи: Національний університет "Львівська політехніка"

Код за ЄДРПОУ: 02071010

Місцезнаходження: вул. Степана Бандери, буд. 12, Львів, 79013, 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. Соколов Володимир Юрійович
2. Volodymyr Y. Sokolov

Кваліфікація: к. т. н., доцент, 05.13.06

Ідентифікатор ORCID ID: Не застосовується

Додаткова інформація:

Повне найменування юридичної особи: Київський столичний університет імені Бориса Грінченка

Код за ЄДРПОУ: 02136554

Місцезнаходження: вул. Бульварно-Кудрявська, 18/2, Київ, 04053, Україна

Форма власності: Державна

Сфера управління: Департамент освіти і науки, молоді та спорту виконавчого органу Київської міської ради (Київської міської державної адміністрації)

Ідентифікатор ROR:

Власне Прізвище Ім'я По-батькові:

1. Субач Ігор Юрійович
2. Ihor Y. Subach

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

Ідентифікатор ORCID ID: Не застосовується

Додаткова інформація:

Повне найменування юридичної особи: Національний технічний університет України "Київський політехнічний інститут імені Ігоря Сікорського"

Код за ЄДРПОУ: 02070921

Місцезнаходження: проспект Берестейський, буд. 37, Київ, 03056, Україна

Форма власності:

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR: Не застосовується

Рецензенти

Власне Прізвище Ім'я По-батькові:

1. Хома Володимир Васильович

2. Volodymyr V. Khoma

Кваліфікація: д.т.н., професор, 05.11.05

Ідентифікатор ORCID ID: Не застосовується

Додаткова інформація:

Повне найменування юридичної особи: Національний університет "Львівська політехніка"

Код за ЄДРПОУ: 02071010

Місцезнаходження: вул. Степана Бандери, буд. 12, Львів, 79013, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

Власне Прізвище Ім'я По-батькові:

1. Костяк Марина Юріївна

2. Maryna Y. Kostiak

Кваліфікація: к.т.н., доцент, 05.13.21

Ідентифікатор ORCID ID: Не застосовується

Додаткова інформація:

Повне найменування юридичної особи: Національний університет "Львівська політехніка"

Код за ЄДРПОУ: 02071010

Місцезнаходження: вул. Степана Бандери, буд. 12, Львів, 79013, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

VIII. Заключні відомості

Власне Прізвище Ім'я По-батькові голови ради	Опірський Іван Романович
Власне Прізвище Ім'я По-батькові головуючого на засіданні	Опірський Іван Романович
Відповідальний за підготовку облікових документів	Пархуць Любомир Теодорович
Реєстратор	УкрІНТЕІ

Керівник відділу УкрІНТЕІ, що є відповідальним за реєстрацію наукової діяльності

Юрченко Тетяна Анатоліївна