Затверджую
Проректор з наукової роботи
Національного університету
«Львівська політехніка»

_____

«__05__» _____ 2025 р.

Висновок
про наукову новизну, теоретичне та практичне значення результатів дисертації «Удосконалення методів та засобів біометричної автентифікації за голосом з застосуванням технологій машинного навчання» здобувача наукового ступеня доктора філософії за спеціальністю *125 Кібербезпека* (галузь знань *12 Інформаційні технології*
Рудої Христини Степанівни
наукового семінару кафедри захисту інформації

1. Актуальність теми дисертації

Сучасний цифровий ландшафт стрімко змінюється під впливом розвитку технологій штучного інтелекту, автоматизації, глобальної комунікації та зростаючого обсягу персональних даних, що передаються через мережі. Автентифікація користувача — ключовий компонент у будь-якій системі безпеки, яка функціонує в умовах недовіри. Зважаючи на слабкість традиційних методів автентифікації, біометричні системи стають основним інструментом встановлення цифрової ідентичності, особливо в секторах, де потрібно одночасно забезпечити зручність, захищеність і безперервність доступу.

Голосова біометрія, як різновид поведінкової автентифікації, має низку переваг порівняно з іншими біометричними ознаками: вона не потребує фізичного контакту, забезпечує автентифікацію на відстані, і є природною для користувача в комунікаційних середовищах. За оцінками аналітичної компанії MarketsandMarkets, глобальний ринок голосової біометрії зростатиме на понад 20% щороку та перевищить $3,9 млрд до 2026 року.

Однак, прогрес у генеративному моделюванні мовлення, призвів до появи нових класів атак на біометричні системи — presentation attacks, у яких зловмисник використовує не реальний голос, а штучно згенерований аудіосигнал. Проблема посилюється через масову доступність рішень для клонування голосу, що створює критичний ризик для будь-якої системи, яка покладається на голос як фактор автентифікації. У цьому контексті виникає потреба у розробці нових методів, здатних забезпечити не лише точну автентифікацію користувача, а й ефективне виявлення спроб використання синтетичного мовлення. Особливої актуальності набувають рішення, що базуються на глибинному навчанні та нейромережевих підходах, здатні адаптуватися до різноманітних умов експлуатації. Тому створення стійких до spoofing-атак систем голосової автентифікації є пріоритетним напрямом сучасних досліджень у галузях кібербезпеки, штучного інтелекту та біометрії, що має важливе як теоретичне, так і прикладне значення.

2. Зв'язок теми дисертації з державними програмами, науковими напрямами університету та кафедри

Дисертаційні дослідження виконано відповідно до наукового напряму кафедри захисту інформації Національного університету "Львівська політехніка".

Окремі частини роботи виконано в межах держбюджетної науково-дослідної роботи: «Дослідження стійкості біометричних систем автентифікації до атак із застосуванням технології клонування голосу на основі глибинних нейронних мереж» (№ держреєстрації 0124U000407).

3. Особистий внесок здобувача в отриманні наукових результатів

Запропоновано концептуальну модель вдосконалення методів і засобів біометричної автентифікації за голосом, яка є основою для обґрунтування структури та етапів реалізації процесу розпізнавання та критеріїв оптимального вибору нейромережевих методів виділення та обробки голосових ознак у порівнянні з класичними для забезпечення високої точності та стійкості голосової автентифікації.

Створено архітектурну модель системи голосової автентифікації і реалізовано її на основі метрики косинусної відстані і, на цій основі, проведено експериментальне дослідження точності, продуктивності та масштабованості систем голосової автентифікації у просторі нейромережевих моделей - TitaNet, ECAPA-TDNN, WavLM та обгрунтовано практичні рекомендації щодо налаштування порогових значень відсікання для забезпечення високої точності та стабільності автентифікаційних рішень.

Розроблено експериментальну методику оцінювання стійкості системи до атак voice-spoofing на основі сучасних технологій клонування голосу та імплементовано підходи до детекції синтетичного мовлення та здійснено порівняльне тестування за вектором переваг кожної з моделей і, на цій основі, сформульовано рекомендації щодо інтеграції механізмів протидії spoofing-атакам в архітектурі системи голосової автентифікації.

4. Достовірність та обґрунтованість отриманих результатів та запропонованих автором рішень, висновків, рекомендацій грунтується на: системному підході до постановки завдань досліджень, цілісному механізмі оптимального вибору критеріїв побудови математичних моделей процедури автентифікації за голосом; достовірність підтверджується практичною реалізацією інтегрального комп'ютерного моделювання із застосуванням технологій машинного навчання у просторі біометричної голосової автентифікації.

5. Ступінь новизни основних результатів дисертації порівняно з відомими дослідженнями аналогічного характеру

Наукова новизна роботи полягає в розробці та дослідженні нових методів, підходів та аналізу стійкості систем біометричної автентифікації за голосом:

1. *Отримала подальший розвиток* методологія класифікації та аналізу сучасних методів голосової автентифікації, що передбачає структуризацію систем за принципами дії (класичні, статистичні, нейромережеві), а також комплексне порівняння текстозалежних і текстонезалежних підходів. Це забезпечило обґрунтовану основу для вибору архітектур, орієнтованих на стійкість і точність у реальних умовах застосування.
2. *Вперше розроблено* концептуальну модель системи голосової автентифікації, яка об'єднує структурно-функціональні блоки (реєстрація, обробка, верифікація) на основі нейромережевих технологій (CNN, LSTM, Transformers) з урахуванням міжнародних

стандартів у сфері біометричної безпеки. Це створює технологічне підґрунтя для впровадження біометричних рішень у системах підвищеної надійності.

3. *Удосконалено* архітектуру системи голосової автентифікації на основі ембедінгів, що включає реалізацію модулів порівняння, налаштування та реєстрації голосових зразків із використанням обґрунтованих метричних функцій. Це дозволяє досягти стабільної точності верифікаційних рішень за умов міжсесійних варіацій та масштабованих багатокористувацьких сценаріїв.
4. *Вперше запропоновано та імплементовано* експериментальну методику оцінювання стійкості до атак із застосуванням синтетично згенерованого мовлення, зокрема на основі генеративних моделей (RVC, ElevenLabs, XTTS, Tortoise). Створений тестовий корпус дозволив провести порівняльне оцінювання ефективності моделей ембедінгів у spoofing-сценаріях з різним лінгвістичним наповненням.
5. *Вперше реалізовано та зіставлено* підходи до детекції синтетичного мовлення на основі фірмового рішення ElevenLabs і авторської моделі MFCC+SVM. Отримані результати лягли в основу практичних рекомендацій щодо впровадження універсальних антиспуфінгових механізмів у архітектуру голосових біометричних систем.

6. Перелік наукових праць, які відображають основні результати дисертації

Основні результати дослідження викладено у тринадцяти наукових публікаціях, а саме: у восьми статтях і п’яти тезах виступів на науково-практичних заходах.

Особистий внесок здобувача у колективно опублікованих працях полягає у формуванні та розробці ключових ідей та результатів. Основні положення та результати дисертації викладені в таких наукових працях здобувача:

Статті у наукових фахових виданнях України:

1. Дудикевич В. Б., Микитин Г. В., Руда Х. С. Застосування глибокого навчання для виявлення deepfake модифікацій біометричного зображення // Сучасна спеціальна техніка. – 2022. – № 1(68). – С. 13–22. *Особистий внесок здобувача: розроблено архітектуру системи аналізу біометричних даних; проведено експериментальну оцінку ефективності моделі у контексті інформаційної безпеки.*
2. 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). – P. 391–397. *Особистий внесок здобувача: виконано адаптацію архітектури глибокого навчання для обробки біометричних даних; проаналізовано результати роботи моделі за різними конфігураціями параметрів.*
3. 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). – P. 228–238. *Особистий внесок здобувача: реалізовано модуль виділення ембедінгів мовців; проведено тестування інтегрованої системи діаризації та виявлення зловмисників.*
4. 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. *Особистий внесок здобувача: досліджено ефективність використання ембедінгів мовлення у багатокомпонентних системах; здійснено оцінку точності та продуктивності методів діаризації.*

5. 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. *Особистий внесок здобувача: сформульовано концептуальну модель системи обробки біометричних даних; реалізовано її прототип із використанням згорткових нейромереж.*
6. 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. *Особистий внесок здобувача: досліджено загрози безпеці в біометричних системах; запропоновано методологічні засади захисту таких систем на основі нейромережевих рішень.*
7. 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. *Особистий внесок здобувача: проведено порівняльний аналіз традиційних та глибинних методів обробки мовного сигналу; запропоновано критерії вибору оптимальної архітектури для задачі голосової автентифікації.*
8. Руда Х. С. Дослідження масштабованості біометричних систем автентифікації на основі вбудовування голосу // Social Development and Security. – 2025. – Vol. 15, iss. 1. – P. 161–170. *Особистий внесок здобувача: виконано дослідження масштабованості систем на основі ембедінгів голосу; проведено серію експериментів з різною кількістю користувачів.*

Наукові публікації у збірниках матеріалів та тез конференцій:

9. Руда Х. С. Використання візуальних і неявних артефактів для виявлення deepfake-модифікацій у біометричних зображеннях // Сучасні методи, інформаційне, програмне та технічне забезпечення систем керування організаційно-технічними та технологічними комплексами : матеріали VIII Міжнародної науково-технічної Internet-конференції (Київ, 26 листопада 2021 року). – 2021. – С. 207–208. Особистий внесок здобувача: реалізовано попередню обробку вхідних даних для покращення якості екстракції ознак біометричного зображення.
10. Dudykevych V., Mykytyn H., Ruda K. The concept of a deepfake detection system of biometric image modifications based on neural networks // 2022 IEEE 3rd KhPI Week on Advanced Technology : conference proceedings, Kharkiv, 3–7 October 2022. – 2022. – P. 585–588. Особистий внесок здобувача: сформульовано загальні засади побудови систем аналізу біометричних даних із використанням нейромережевих моделей; здійснено підбір архітектури відповідно до вимог системи.
11. Микитин Г. В., Руда Х. С., Хома Ю. В. Categorization of deepfake methods: a comparison of single-shot and multi-shot transfer approaches // Захист інформації і безпека інформаційних систем : матеріали IX Міжнародної науково-технічної конференції (Львів, 25–26 травня 2023 р.). – 2023. – С. 109–110. Особистий внесок здобувача: класифіковано методи генерації біометричних даних та проведено їх систематичний аналіз; визначено ефективність підходів до передачі знань у нейромережевих структурах.
12. Сабодашко Д. В., Руда Х. С., Швед М. Є., Бордуляк С. М. Технологія ембедінгів голосу та діаризація мовців // XX International Scientific and Practical Conference «Scientific Research:

Modern Challenges and Prospects» : collection of abstracts, April 24–26, 2024, Prague, Czech Republic. – 2024. – P. 72–74. Особистий внесок здобувача: досліджено механізми формування голосових ембедінгів у задачах розділення мовців; виконано аналіз параметрів, що впливають на якість діаризації.

13. Руда Х. С., Микитин Г. В. Методи детекції синтетичних аудіозаписів, створених системами клонування голосу // Scientific Research in the Age of Virtual Reality: Exploring New Frontiers : collection of abstracts of LII International Scientific and Practical Conference (December 18–20, 2024), Montreal, Canada. – 2024. – P. 132–136. Особистий внесок здобувача: виконано огляд сучасних методів обробки синтетичного мовлення; запропоновано підхід до оцінювання достовірності голосових зразків у системах автентифікації

Наукові праці, які додатково відображають наукові результати дисертації

14. Mykytyn H., Ruda K., Shved M. The paradigm of building secure information technologies for detecting deepfake modifications of biometric images based on neural networks // Informatyka techniczna i sztuczna inteligencja: колективна монографія. – Chapter in a collective monograph. – Bielsko-Biała: Wydawnictwo naukowe Uniwersytetu Bielsko-Bialskiego, 2024. – P. 43–50. Особистий внесок здобувача: проаналізовано вразливості біометричних систем до атак із застосуванням штучного інтелекту; обґрунтовано підходи до побудови систем захисту на основі глибинного навчання.

7. Апробація основних результатів дослідження на конференціях, симпозіумах, семінарах тощо

Основні результати дисертаційного дослідження апробовано на міжнародних наукових та науково-практичних конференціях, наукових школах та консорціумах, семінарах:

- Сучасні методи, інформаційне, програмне та технічне забезпечення систем керування організаційно-технічними та технологічними комплексами (VIII Міжнародна науково-технічна Internet-конференція, Київ, 26 листопада 2021 року)
- 2022 IEEE 3rd KhPI Week on Advanced Technology (Kharkiv, 3–7 October 2022)
- Захист інформації і безпека інформаційних систем (IX Міжнародна науково-технічна конференція, Львів, 25–26 травня 2023 р.)
- XX International Scientific and Practical Conference «Scientific Research: Modern Challenges and Prospects» (April 24–26, 2024, Prague, Czech Republic)
- LII International Scientific and Practical Conference «Scientific Research in the Age of Virtual Reality: Exploring New Frontiers» (December 18–20, 2024, Montreal, Canada)
- Наукові семінари кафедри захисту інформації (2021-2025 рр.).

8. Наукове значення виконаного дослідження із зазначенням можливих наукових галузей та розділів програм навчальних курсів, де можуть бути застосовані отримані результати

Наукові результати, отримані автором, можуть бути використані для вдосконалення технологій автентифікації користувачів у системах з підвищеними вимогами до безпеки, зокрема в умовах зростаючої загрози голосових фальсифікацій. Запропоновані методи мають практичне застосування в галузях біометрії, штучного інтелекту та інформаційної безпеки. Також результати виконаних досліджень можуть бути використані у навчальному процесі кафедри захисту інформації Національного університету “Львівська політехніка”, зокрема для студентів спеціальності “125 – Кібербезпека та захист інформації” у межах дисципліни “Гарантоздатність автоматизованих систем”.

9. Практична цінність результатів дослідження із зазначенням конкретного підприємства або галузі народного господарства, де вони можуть бути застосовані

Методи виявлення синтезованого мовлення та вдосконалення біометричної автентифікації за голосом, розроблені в межах даного дослідження, значно підвищують рівень захисту інформаційних систем від сучасних загроз, зокрема атак із використанням клонованих голосів. Інтеграція нейромережевих моделей та алгоритмів глибинного навчання забезпечує високу точність верифікації користувачів і дозволяє ефективно виявляти підроблені голосові сигнали. Основні результати дисертаційної роботи були використані з метою підвищення безпеки автентифікаційних систем у прикладних проектах у сфері інформаційної безпеки в компанії UNIDATALAB LTD.

10. Оцінка структури дисертації, її мови та стилю викладення

Дисертаційна робота викладена на 162 сторінках та складається з анотації, змісту, переліку скорочень, вступу, чотирьох основних розділів, списку використаних джерел з 100 найменувань, а також 4 додатки. За структурою, мовою та стилем викладення дисертація відповідає вимогам МОН України. Робота написана грамотною українською мовою з використанням сучасної наукової термінології, а стиль викладення матеріалу є послідовним та логічним.

У ході обговорення дисертації до неї не було висунуто жодних зауважень щодо самої суті роботи.

11. З врахуванням зазначеного, **на науковому семінарі кафедри захисту інформації ухвалили:**

11.1. Дисертація Рудої Христини Степанівни на тему "Удосконалення методів та засобів біометричної автентифікації за голосом з застосуванням технологій машинного навчання" є завершеним науковим дослідженням, у якому вирішено актуальне науково-практичне завдання підвищення ефективності та захищеності голосових біометричних систем. Робота спрямована на застосування нейромережевих технологій, що забезпечують високу точність верифікації особи та стійкість до атак із використанням клонованого мовлення. Отримані результати мають вагоме значення для розвитку галузі знань 12 "Інформаційні технології".

11.2. Основні наукові положення, методичні розробки, висновки та практичні рекомендації, викладені у дисертаційній роботі, логічні, послідовні, аргументовані, достовірні, достатньо обґрунтовані. Дисертація характеризується єдністю змісту.

11.3. У 13 наукових публікаціях відображені основні результати дисертації, з них 8 статей у наукових фахових виданнях України, та 5 матеріалів конференцій).

11.4. Дисертація відповідає вимогам наказу МОН України № 40 від 12.01.2017р. «Про затвердження вимог до оформлення дисертації», Порядку присудження ступеня доктора філософії та скасування рішення разової спеціалізованої вченої ради закладу вищої освіти, наукової установи про присудження ступеня доктора філософії (Постанова Кабінету Міністрів України від 12 січня 2022 р. № 44, зі змінами).

11.5. Дисертація є результатом самостійних досліджень, не містить елементів фальсифікації, компіляції, плагіату та запозичень, що констатує відсутність порушення академічної доброчесності. Використання текстів інших авторів мають належні посилання на відповідні джерела.

доброчесності. Використання текстів інших авторів мають належні посилання на відповідні джерела.

11.6. З урахуванням наукової зрілості та професійних якостей Рудої Христини Степанівни дисертаційна робота "Удосконалення методів та засобів біометричної автентифікації за голосом з застосуванням технологій машинного навчання" рекомендується для подання до розгляду та захисту у разовій спеціалізованій вченій раді.

За затвердження висновку проголосували:

"за"	***40***	***(сорок)***
"проти"	***–***	***(немає)***
"утримались"	***–***	***(немає)***

Головуючий на засіданні фахового семінару, д.т.н., професор, завідувач кафедри захисту інформації — Іван ОПІРСЬКИЙ

Рецензенти:

д.т.н., професор, професор кафедри захисту інформації — Володимир ХОМА

к.т.н., доцент, доцент кафедри захисту інформації — Марина КОСТЯК

Відповідальний в ІКТА за атестацію PhD, д.т.н., професор, професор кафедри захисту інформації — Любомир ПАРХУЦЬ

"27" 05 2025 р.