РЕЦЕНЗІЯ

кандидата технічних наук, доцента,
доцента кафедри захисту інформації
Національного університету «Львівська політехніка»
Костяк Марини Юріївни
на дисертацію
Рудої Христини Степанівни
«УДОСКОНАЛЕННЯ МЕТОДІВ ТА ЗАСОБІВ БІОМЕТРИЧНОЇ АВТЕНТИФІКАЦІЇ ЗА ГОЛОСОМ З ЗАСТОСУВАННЯМ ТЕХНОЛОГІЙ МАШИННОГО НАВЧАННЯ»

подану до захисту на здобуття наукового ступеня доктора філософії за спеціальністю 125 «Кібербезпека» (галузь знань 12 «Інформаційні технології»)

Актуальність теми дисертації. Сучасний етап розвитку інформаційно-комунікаційних технологій характеризується інтенсивною інтеграцією цифрових сервісів та інтелектуальних систем у різні сфери діяльності, що зумовлює необхідність удосконалення механізмів встановлення ідентичності користувачів. Біометрична автентифікація за голосом є одним із найбільш перспективних напрямів, оскільки поєднує зручність використання, технологічну доступність та високий рівень сумісності з існуючими інформаційними платформами.

Водночас розвиток генеративних моделей мовлення на основі глибинних нейронних мереж істотно трансформував умови функціонування систем біометричної автентифікації. З одного боку, ці технології відкривають нові можливості для вдосконалення обробки мовних сигналів, з іншого – формують передумови для появи високоточних атак, здатних імітувати індивідуальні голосові характеристики користувачів. У поєднанні з впливом варіативності мовлення, акустичних завад та технічної неоднорідності це вимагає впровадження адаптивних методів, здатних забезпечити достовірність автентифікації у реальних умовах експлуатації.

Дисертаційне дослідження Рудої Христини Степанівни спрямоване на формування науково обґрунтованих підходів до підвищення ефективності голосової біометрії шляхом використання технологій машинного навчання та моделей побудови мовних ембедінгів. Розроблені методи забезпечують підвищення точності автентифікації, інваріантність до впливу сторонніх факторів та стійкість до атак із застосуванням синтетичного мовлення, що визначає їхню значущість для розвитку прикладних рішень у сфері захисту інформації та суміжних галузях.

Зв'язок теми дисертації з державними програмами, науковими напрямами університету та кафедри. Дисертаційне дослідження виконано в межах держбюджетної науково-дослідної роботи держбюджетної науково-дослідної роботи: «Дослідження стійкості біометричних систем автентифікації до атак із застосуванням технології клонування голосу на основі глибинних нейронних мереж» (№ держреєстрації 0124U000407). Основні положення та результати дисертаційної роботи впроваджено у навчальний процес кафедри Захист інформації Національного університету "Львівська політехніка".

Наукова новизна основних результатів дисертації полягає у такому:

1) Одержала подальший розвиток концепція удосконалення голосової автентифікації, в основу якої покладено широке і комплексне застосування на різних структурних рівнях технологій машинного навчання та штучного інтелекту з урахуванням міжнародних стандартів у сфері біометричної безпеки. Це створює методологічну основу до забезпечення стійкості системи в умовах зростаючих кіберзагроз, підвищення дискримінаційної здатності моделей у багатокористувацьких сценаріях та в реальних умовах застосування.

2) Вдосконалено такі ключові структурні комоненти системи біометричної автентифікації як модулі порівняння, налаштування та реєстрації голосових зразків шляхом застосування нейромережевих і трансформерних голосових моделей і обґрунтованого вибору метричних функцій. Це збільшує інваріантність голосової автентифікації до міжсесійних варіацій та масштабування, а відтак підвищує достовірність верифікаційних рішень біометричної системи в умовах багатокористувацьких сценаріїв.

3) Вперше розроблено та застосовано методику оцінювання стійкості до атак із застосуванням синтетично згенерованого мовлення, зокрема на основі генеративних моделей (RVC, ElevenLabs, XTTS, Tortoise), що дозволяє верифікувати ефективність системи згідно з вимогами ISO/IEC 30107-3:2023 щодо тестування Presentation Attack Detection. Виявлено, що всі протестовані моделі демонструють вразливість до атак з застосуванням клонування голосу, що стало підставою для рекомендації впровадження детекторів синтетичного мовлення як обов'язкового компонента систем біометричної голосової автентифікації.

4) Розроблено емпіричну методику тестування стійкості системи до атак підміни із використанням синтетичних голосів, згенерованих моделями RVC, XTTS, ElevenLabs та Tortoise, що дозволяє верифікувати ефективність системи згідно з вимогами ISO/IEC 30107-3:2023 щодо тестування Presentation Attack Detection (PAD). Виявлено, що всі протестовані моделі демонструють вразливість до атак з застосуванням клонування голосу, що стало підставою

для рекомендації впровадження детекторів синтетичного мовлення як обов'язкового компонента систем біометричної голосової автентифікації.

5) Вперше реалізовано та зіставлено підходи до виявлення синтетичного мовлення на основі генеративної моделі ElevenLabs і авторської моделі MFCC+SVM. Отримані результати покладено в основу рекомендацій щодо впровадження універсальних антиспуфінгових механізмів у архітектуру голосових біометричних систем.

Ступінь обґрунтованості наукових положень дисертації і їх достовірність та новизна визначається чіткою структуризацією дослідницьких завдань, комплексним аналізом теоретичних і прикладних аспектів предметної області та методологічно виваженим підходом до вибору інструментарію. У роботі застосовано сучасні методи математичного моделювання, алгоритми побудови мовних ембедінгів та глибинні нейронні архітектури доповнені експериментальними дослідженнями стійкості систем до атак із використанням синтетичного мовлення. Проведені експерименти із залученням різнорідних корпусів реальних та штучно згенерованих голосових даних підтверджують валідність отриманих результатів та їх відтворюваність. Інтеграція технологій машинного навчання та механізмів детекції синтетичного мовлення у контексті біометричної автентифікації відображає інноваційний характер дослідження та формує його наукову новизну.

Наукове значення виконаного дослідження із зазначенням можливих наукових галузей та розділів програм навчальних курсів, де можуть бути застосовані отримані результати. Отримані у дисертаційній роботі результати, що охоплюють розроблення концептуальної моделі системи голосової автентифікації, удосконалення алгоритмів побудови мовних ембедінгів та впровадження методів детекції синтетичного мовлення, мають вагоме значення для подальшого розвитку наукових досліджень у галузях кібербезпеки, біометрії та штучного інтелекту. Запропоновані методи можуть бути використані для створення високоточних біометричних систем автентифікації, а також для дослідження стійкості таких систем до атак із застосуванням генеративних моделей мовлення.

Результати роботи доцільно інтегрувати у навчальні курси, що охоплюють тематику інформаційної безпеки, обробки сигналів, машинного навчання, аналізу даних та біометричних технологій. Використання розроблених методів у навчальному процесі сприятиме формуванню у студентів компетентностей у галузях сучасних технологій кіберзахисту, моделювання мовних ознак та застосування нейронних мереж у практичних задачах. Це забезпечує міждисциплінарну цінність роботи для спеціальностей,

пов'язаних з інформаційними технологіями, комп'ютерною інженерією та прикладною математикою.

Практичне значення одержаних результатів полягає у тому, що:

1. Розроблено та реалізовано архітектуру системи голосової автентифікації на основі вбудованих векторів, яка забезпечує відповідність принципам надійності, масштабованості та обмеження доступу до біометричних шаблонів, визначеним у ISO/IEC 24745:2022 та ISO/IEC 19795-1:2021. Впровадження архітектури в експериментальному середовищі дозволило досягти точності автентифікації до 96%.
2. Імплементовано модель виявлення синтетичного мовлення на основі MFCC+SVM, яка забезпечує точність виявлення атак до 89.75%, при цьому точність класифікації справжніх голосів залишається низькою (25.96%), що свідчить про потребу додаткових рішень. Модель відповідає вимогам ISO/IEC 30107-1:2023 до PAD-механізмів і рекомендована до застосування як додатковий рівень захисту в багатофакторних біометричних системах, що працюють із критичними даними.
3. Створено тестовий корпус голосових даних, за допомогою якого проведено порівняльне оцінювання ефективності мовних моделей у сценаріях підробки голосу з різним лінгвістичним наповненням.
4. Результати порівняльного тестування моделей TitaNet, ECAPA-TDNN, WavLM та PyAnnote можуть слугувати основою для обґрунтованого вибору архітектури в задачах біометричної автентифікації, орієнтованих на великомасштабні користувацькі бази. Зокрема, модель TitaNet продемонструвала найвищу стійкість до масштабування: збільшення числа зареєстрованих користувачів від 10 до 70 зумовило зниження точності в середньому на 3,55%. Оцінювання масштабованості здійснювалася згідно методологічних положень стандарту ISO/IEC 19795-2:2007, який регламентує сценарне тестування з варіативною чисельністю суб'єктів як одного з ключових параметрів експериментального дизайну.
5. Результати оцінювання ресурсної ефективності моделей TitaNet, ECAPA-TDNN та WavLM вказали на їхню придатність для розгортання на обчислювальних платформах з обмеженими ресурсами. Зокрема, модель WavLM-base-plus-sv забезпечує автентифікацію з точністю 93% витрачаючи на зіставлення голосових векторів в середньому 4.34 мс. Це означає, що модель, будучи заімплементованою на периферійних пристроях із обмеженими резурсами задовольняє вимоги до швидкодії необхіді для роботи в реальному часі. Отримані результати відповідають критеріям ефективності, визначеним у ISO/IEC 29167-1:2014, та засвідчують можливість застосування

у вбудованих біометричних рішеннях, мобільних пристроях і системах контролю доступу.

Повнота оприлюднення результатів дисертаційної роботи. Основні результати дисертаційної роботи Рудої Христини викладено у чотирнадцяти наукових публікаціях, а саме: у восьми статтях (із них шість – у фахових наукових виданнях України та дві – у закордонних періодичних виданнях), розділі монографії і п'яти матеріалах наукових конференцій і семінарах. Особистий внесок здобувача у колективно опублікованих працях полягав у формуванні підходів, реалізації експериментів та інтерпретації їх результатів.

Зауваження до дисертаційної роботи.

1. Недостатня деталізація інтеграції розробленої системи у реальні інфраструктури. У підрозділі 3.2. наведено результати тестування моделей ECAPA-TDNN, TitaNet та WavLM у контрольованих умовах та обґрунтовано їх ефективність для задач голосової автентифікації. Проте опис інтеграції системи в реальні корпоративні середовища автентифікації (наприклад, з урахуванням вимог ISO/IEC 30107 чи роботи у складі SIEM/SOAR-платформ) є обмеженим. Додатковий аналіз продуктивності у високонавантажених сценаріях та опис архітектури при масштабуванні до тисяч користувачів значно посилив би прикладну цінність роботи.

2. Обмежений порівняльний аналіз методів детекції синтетичного мовлення. Підрозділ 4.3.2. містить порівняння власної реалізації детектора на основі MFCC+SVM із комерційною системою ElevenLabs, що дозволило виявити переваги обраних підходів у сценаріях атак зі згенерованими голосами. Проте не розглянуто альтернативні архітектури, наприклад, моделі на основі спектрограм та CNN або трансформерні детектори. Розширений аналіз підвищив би репрезентативність отриманих висновків щодо стійкості запропонованих методів до різних типів атак.

3. Обмежений аналіз впливу акустичних та технічних факторів на точність. Хоча в підрозділі 3.4. наведено результати для варіантів мовлення, що включають шумові завади та міжсесійні відмінності, бракує глибшого аналізу впливу характеристик мікрофонів і каналів зв'язку на продуктивність системи. Врахування більшої кількості реалістичних умов (зокрема VoIP-передачі, різних побутових пристроїв) надало б дослідженню додаткову практичну вагомість.

4. Обмежена увага до етичних і правових аспектів застосування голосової біометрії. У підрозділі 1.4, де здійснено огляд сучасних технологій голосової біометрії, лише побіжно згадуються питання захисту персональних даних і регуляторні вимоги. Врахування міжнародних нормативів, таких як GDPR, дало б змогу ширше оцінити умови впровадження розроблених методів.

Наведені зауваження не знижують загальної позитивної оцінки дисертаційної роботи.

Висновок

Дисертаційна робота Рудої Христини Степанівни «Удосконалення методів та засобів біометричної автентифікації за голосом з застосуванням технологій машинного навчання», є завершеним та цілісним науковим дослідженням, в якому одержано вагомі наукові результати, а також має практичну цінність у сфері кібербезпеки. Дисертаційне дослідження відповідає спеціальності 125 «Кібербезпека»та вимогам наказу Міністерства освіти і науки України «Про затвердження вимог до оформлення дисертації», постанові Кабінету Міністрів України №44 від 12.01.2022р. «Порядок присудження ступеня доктора філософії...», а тому її можна рекомендувати до захисту, а авторка заслуговує на присудження ступеня доктора філософії.

Офіційний рецензент
кандидат технічних наук, доцент,
доцент кафедри захисту інформації
Національного університету
“Львівська політехніка” Марина КОСТЯК

Підпис к.т.н, доцента Костяк М.Ю.
засвідчую

Міністерство освіти і науки України • Національний університет "Львівська політехніка" • ЗКПО 02071010 •

Проректор Микола ЛОГОЙДА