Голові разової спеціалізованої
вченої ради
Національного університету
«Львівська політехніка»
д.т.н., професору
Опірському Івану Романовичу

ВІДГУК ОФІЦІЙНОГО ОПОНЕНТА

кандидата технічних наук, доцента,
доцента кафедри інформаційної та кібернетичної безпеки
імені професора Володимира Бурячка
Київського столичного університету імені Бориса Грінченка
Соколова Володимира Юрійовича
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»)

1. Актуальність теми дисертації. Дисертаційна робота Рудої Х. С. відзначається високим рівнем актуальності, що обумовлено інтенсивним розвитком інформаційних технологій, масштабною цифровізацією суспільних процесів та зростанням обсягів персоніфікованих даних, які потребують захищених методів автентифікації. Серед сучасних біометричних технологій особливе місце посідає голосова автентифікація, яка поєднує дистанційність, безконтактність та інтуїтивну природність для користувача. Водночас прогрес у галузі генеративного штучного інтелекту, зокрема методів синтезу мовлення та клонування голосу (TTS, Voice Conversion), спричинив появу нових класів атак на біометричні системи, що знижує їхню надійність і потребує розроблення стійких до таких впливів архітектур.

У дисертації запропоновано методологічно обґрунтовані підходи до підвищення точності та захищеності голосових біометричних систем шляхом застосування глибинних нейронних архітектур і технологій машинного навчання, що відповідає актуальним тенденціям розвитку кібербезпеки. Значущість дослідження підсилюється його орієнтацією на протидію атакам типу voice spoofing, реалізованим із використанням синтетично згенерованих голосів, що є однією з ключових проблем сучасної біометрії.

Робота поєднує системний аналіз теоретичних засад побудови біометричних систем із практичною розробкою архітектур і методів тестування їхньої стійкості відповідно до вимог міжнародних стандартів.

Таким чином, дисертаційне дослідження є своєчасним і робить вагомий внесок у розвиток наукових основ і прикладних рішень створення високоточних, масштабованих та захищених від генеративних атак систем біометричної автентифікації за голосом.

2. Аналіз змісту дисертаційної роботи

Дисертація Рудої Х. С. є завершеною дослідницькою роботою, що складається з анотації, вступу, 4 розділів, висновків, списку використаної літератури та додатків.

У вступі обґрунтовано актуальність теми, сформульовано цілі та завдання дослідження, визначено наукову новизну та практичну цінність результатів дослідження, презентовано дані про апробацію та публікацію результатів дисертаційної роботи.

У першому розділі «Аналіз особливостей процесу розпізнавання людини за голосом» проведено огляд історичних передумов, теоретичних основ і практичних підходів до побудови систем голосової біометрії. Здійснено класифікацію методів від класичних і статистичних до нейромережевих та ембедінг-орієнтованих. Розглянуто текстозалежні й текстонезалежні системи, їхні переваги та обмеження, а також сучасні загрози, зумовлені клонуванням голосу і необхідність впровадження антиспуфінгових механізмів.

У другому розділі «Концептуальна модель голосової автентифікації на основі нейромережевих трансформерів» представлено модель, що поєднує класичні та нейромережеві підходи. Розглянуто етапи автентифікації — від збору та обробки сигналу до формування ембедінгу й порівняння шаблонів. Обґрунтовано використання моделей ECAPA-TDNN, TitaNet і WavLM, проведено порівняння методів екстракції ознак та розглянуто питання безпеки й відповідність стандартам.

У третьому розділі «Імплементація вдосконалення системи голосової автентифікації» реалізовано архітектуру системи на основі ембедінгів. Описано реєстрацію профілів, налаштування порогів та процедури верифікації. Запропоновано метод усереднення ембедінгів для стабільності при варіативності мовлення. Сформовано аудіодатасет для тестування, методику формування пар зразків та калібрування порогів, що підвищило точність і адаптивність системи.

У четвертому розділі «Оцінювання стійкості системи до атак типу voice spoofing» подано методику перевірки захисту від атак із використанням

синтетичного мовлення. Створено корпус зразків за допомогою RVC, XTTS, ElevenLabs і Tortoise для двох сценаріїв атак: з ідентичним і новим текстом. На основі ембедінгів (ECAPA, TitaNet, WavLM) проведено оцінку точності та впливу різних технологій клонування. Досліджено інтеграцію детекції синтетичного мовлення й когнітивних факторів як додаткового захисту.

У висновках підсумовано результати досліджень, надано кількісні оцінки ефективності запропонованих рішень та сформульовано рекомендації для практичного впровадження.

3. 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.

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

Дисертаційна робота містить нові наукові результати, що стосуються розвитку методів голосової біометрії в умовах зростання загроз з боку генеративних технологій. Розроблені підходи до побудови мовних ембедінгів, підвищення точності автентифікації та впровадження алгоритмів детекції синтетичного мовлення формують наукову основу для створення стійких до атак біометричних систем. Застосовані у дослідженні методи нейронних мереж і аналізу голосових ознак поєднують здобутки кібербезпеки, обробки сигналів та штучного інтелекту, що підкреслює міждисциплінарний характер роботи.

Отримані результати можуть бути використані для подальших наукових досліджень у галузях безпечних інформаційних систем, когнітивної біометрії та технологій захисту від генеративних атак. Вони доцільні для включення у програми навчальних курсів, що охоплюють кіберзахист, інтелектуальні системи обробки сигналів, біометричні технології та глибинне навчання. Такий підхід сприятиме формуванню у студентів компетентностей у сучасних напрямах кібербезпеки та практичних навичок побудови захищених біометричних систем, що є важливим для підготовки фахівців з інформаційних технологій, програмної інженерії та прикладної математики.

5. Ступінь обґрунтованості наукових положень дисертації, їх достовірність та новизна визначається послідовним формуванням дослідницьких завдань, поєднанням аналітичних, експериментальних і порівняльних методів, а також використанням сучасного інструментарію штучного інтелекту. У роботі вперше здійснено комплексне тестування нейромережевих моделей голосової автентифікації у поєднанні з антиспуфінговими механізмами, що дозволило отримати об'єктивні та відтворювані результати.

Достовірність отриманих висновків підтверджується масштабними експериментами на різних аудіокорпусах, включно з реальними голосовими

даними та синтетичними записами, згенерованими сучасними системами клонування голосу. Застосування формалізованих метрик (FAR, FRR, EER, DCF) та порівняльного аналізу моделей забезпечило статистичну верифікацію результатів та їх узгодженість із вимогами міжнародних стандартів.

Наукова новизна роботи полягає у поєднанні технологій глибинного навчання з методами детекції синтетичного мовлення, що дозволило створити архітектуру біометричної автентифікації, стійку до генеративних атак. Практична значущість підтверджується можливістю інтеграції запропонованих рішень у критично важливі інформаційні системи та їх впровадженням у навчальний і прикладний контекст.

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

7. Повнота оприлюднення результатів дисертаційної роботи. Основні результати дисертаційної роботи Рудої Х. С. 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 семінарів. Особистий внесок авторки у колективні публікації полягав у розробленні методичних підходів, організації та проведенні експериментальних досліджень, а також у науковій інтерпретації та узагальненні отриманих результатів.

8. Оцінка структури дисертації, її мови та стилю викладення. Структура дисертаційної роботи є чітко впорядкованою та повністю відповідає встановленим вимогам Міністерства освіти і науки України до дисертаційних досліджень на здобуття наукового ступеня доктора філософії. Кожен розділ логічно взаємопов'язаний та послідовно висвітлює сформульовані мету й завдання, методологічні засади дослідження, отримані результати та напрями їх практичного застосування.

Мова дисертації є грамотною, літературною та відповідає нормам академічного стилю. Виклад матеріалу відзначається чіткістю, науковою виваженістю та структурованістю, що сприяє його легкому сприйняттю. Текст роботи вирізняється коректним і послідовним використанням сучасної термінології у галузях інформаційної безпеки, біометричних технологій, цифрової обробки сигналів та машинного навчання.

Ознак порушення академічної доброчесності не встановлено. Усі використані літературні джерела оформлені відповідно до вимог і коректно процитовані з належним посиланням на першоджерела. Анотація дисертаційної роботи адекватно відображає її основний зміст, наукову новизну та сформульовані висновки.

9. Зауваження та дискусійні положення щодо змісту дисертаційної роботи.

1. У підрозділі 3.4.3 подано результати дослідження точності системи при збільшенні кількості користувачів, однак не проаналізовано вплив масштабування на продуктивність — зокрема, час верифікації, використання оперативної пам'яті та навантаження на обчислювальні ресурси. Для систем біометричної автентифікації, що передбачають роботу в реальному часі та підтримку великої кількості одночасних сесій, ці показники є важливими для оцінки придатності архітектури у практичних сценаріях.

2. Попри детальний опис архітектур нейромережевих моделей та аналіз різних метричних функцій, у роботі бракує узагальнюючих таблиць або графічних схем для порівняння характеристик цих моделей (кількість параметрів, час інференсу, використання ресурсів) та візуалізації відмінностей у показниках точності. Такі матеріали значно підвищили б наочність викладу та полегшили б сприйняття великих обсягів аналітичної інформації.

3. У висновках до розділу 4 наведено загальні рекомендації щодо впровадження механізмів детекції синтетичного мовлення, однак бракує чітких вказівок щодо інтеграції цих компонентів у запропоновану архітектуру системи (наприклад, послідовність застосування детектора, його вплив на час обробки запиту чи взаємодію з основним модулем автентифікації). Конкретизація цих аспектів дозволила б підвищити прикладну цінність роботи та спростити впровадження результатів у практичні рішення.

4. У підрозділі 3.2 «Метрики оцінювання ефективності системи» представлено результати обчислення показників FAR, FRR та EER, однак не наведено графічних залежностей цих метрик від порогових значень для різних моделей автентифікації. Такий аналіз дозволив би наочно показати компроміс між рівнем хибних відмов та хибних прийняттів, а також оцінити оптимальні точки роботи кожної моделі. Включення ROC-кривих або DET-графіків суттєво посилило б аналітичну складову розділу та надало додаткові аргументи для обґрунтування вибору порогових значень.

5. У розділі 4 «Оцінювання стійкості системи до атак» не розглянуто вплив параметрів вхідних даних на результати атак та ефективність захисних механізмів. Зокрема, відсутній аналіз залежності успішності атак від рівня шуму, типу записуючого обладнання чи умов оцифровування мовлення. Дослідження цих факторів дозволило б глибше оцінити реальні ризики використання системи у польових умовах і дало б змогу сформувати практичні рекомендації щодо мінімальних вимог до якості вхідного сигналу для забезпечення стабільної роботи системи.

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 12.01.2022 р. «Порядок присудження ступеня доктора філософії», а тому її можна рекомендувати до захисту, а авторка заслуговує на присудження ступеня доктора філософії.

Офіційний опонент:
кандидат технічних наук, доцент,
доцент кафедри інформаційної та
кібернетичної безпеки імені
професора Володимира Бурячка
Київського столичного університету
імені Бориса Грінченка

Володимир СОКОЛОВ