67-72-108/2
20.05.2021

ВІДГУК

офіційного опонента
на дисертаційну роботу **Сабодашка Дмитра Володимировича**
«Вдосконалення методів і засобів біометричної автентифікації на основі електрокардіограми», подану на здобуття наукового ступеня доктора філософії за спеціальністю 125 – Кібербезпека
(Галузь знань 12 – Інформаційні технології)

Актуальність теми дисертації

Сучасні біометричні системи повинні відповідати таким вимогам як універсальність, унікальність, довговічність, вимірюваність тощо. Сьогодні вже опубліковано десятки наукових публікацій, присвячених застосуванню електрокардіограми (ЕКГ) як біометричного маркера. Досліджено методи автентифікації, що базуються як на виділенні характерних точок (fiducial points) ЕКГ, так і на основі безпосереднього опрацювання вибірок ЕКГ-сигналу. Застосовано класифікатори, що працюють за різними алгоритмами машинного навчання, а одержані результати показали досить високу точність розпізнавання. Проте на шляху застосування ЕКГ у реальних біометричних системах автентифікації залишалися недослідженими низка важливих питань, зокрема стабільність ЕКГ як біомаркера на довготривалому часовому інтервалі, вплив варіабельності серцевого ритму на точність системи ідентифікації тощо. У зв'язку з цим, покращення технічних і експлуатаційних характеристик біометричних систем автентифікації за ЕКГ-сигналом на основі поєднання технологій цифрового оброблення сигналів і машинного навчання, є актуальною науково-практичною задачею галузі кібербезпеки. Саме розв'язанню цієї роботи і присвячена дисертація Сабодашка Д.В.

Зв'язок роботи із науковими програмами, планами, темами

Дисертаційна робота Сабодашка Д.В.. виконана на кафедрі захисту інформації Національного університету «Львівська політехніка». Тема дисертації відповідає науковому напрямку кафедри. Дисертаційні дослідження виконувалися в межах держбюджетних НДР:

- «Розвиток теоретичних засад створення комплексних систем безпеки автоматизованих і комунікаційних систем» (номер державної реєстрації 0115U006722; терміни виконання - 2018-2020 рр.);
- «Розроблення та удосконалення методів і засобів захисту інформації для протидії несанкціонованому доступу в інформаційно-

комунікаційних мережах» (номер державної реєстрації 0119U101690; терміни виконання - 2020-2022 рр.).

Ступінь обґрунтованості, наукових положень та висновків, їх достовірність

Обґрунтованість наукових положень та висновків, сформульованих у дисертаційній роботі, є достатньою й базується на детальному аналізі джерел за даною проблемою, чіткій постановці мети і задач дисертації, використанні сучасних методів дослідження, а також у якісному та аргументованому формулюванні висновків.

Достовірність та обґрунтованість запропонованих методів і засобів підтверджується результатами експериментальних досліджень та коректним застосуванням методів системного і порівняльного аналізу, теорії систем і цифрового оброблення сигналів, машинного навчання, математичної статистики, імітаційного моделювання. Тому можна стверджувати, що висновки та практичні рішення, наведені у роботі, коректні, достатньо обґрунтовані й можуть бути рекомендовані до використання для покращення технічних і експлуатаційних характеристик біометричних систем автентифікації за ЕКГ-сигналом.

Важливість результатів, що отримані в роботі для науки та практичного використання

Основними науково-обґрунтованими результатами є:

1. Вперше розроблено підхід до виправлення залишкових артефактів у ЕКГ-сигналах, який складається із трьох етапів - формування референційного образу біометричного маркера, виявлення фрагментів із промахами та, власне, заміна цих фрагментів на відповідні значення із образу, застосування якого дає змогу підвищити достовірність результатів автентифікації.

2. Вперше для етапу виявлення фрагментів із промахами виконано дослідження впливу гіперпараметрів (тривалість ковзного вікна і поріг допустимого відхилення вибірки) на точність автентифікації, що дало змогу знайти оптимальні їх значення за критерієм мінімальної похибки.

3. Вперше запропоновано метод формування референційного образу ЕКГ-маркера на основі статистичної моделі, який є невимогливим до обчислювальних ресурсів та може бути використаний для виправлення залишкових артефактів у ЕКГ-сигналах у системі біометричної автентифікації.

4. Вперше запропоновано метод формування референційного образу ЕКГ-маркера на базі нечіткої нейромережевої моделі, а його застосування

для виправлення залишкових артефактів у ЕКГ-сигналах дає змогу зменшити похибки автентифікації першого і другого роду відповідно у 4 та 3 рази.

5. Розроблено метод темпоральної нормалізації серцевого ритму, який здійснює часову трансформацію ЕКГ-сигналу з приведення тривалості циклу до наперед встановленого значення, а його застосування дає змогу підвищити точність автентифікації.

6. Досліджено короткотривалу та довготривалу стійкість сигналу ЕКГ багатьох користувачів, за результатами якого доведено можливість практичного застосування електрокардіограми як біометричного маркера в реальних системах автентифікації.

Практичне значення отриманих результатів:

- Досліджено швидкодію систем біометричної автентифікації імплементованих на основі персонального комп'ютера та платформи Raspberry Pi.
- На основі розробленого методу виявлення та виправлення промахів у ЕКГ-сигналах розроблено програмний модуль, застосування якого підвищує точність систем автентифікації на понад 7%.
- На основі розробленого методу темпоральної нормалізації ЕКГ-сигналів розроблено програмний модуль, який забезпечує стійкість нейромережевого автентифікатора до перенавчання, та підвищує його точність на 8%.
- Розроблено кожен із компонентів структурної схеми систем біометричної автентифікації та біометричну систему в цілому. Перевірено ефективність системи біометричної автентифікації імплементованої на платформі Raspberry Pi 3
- Зібрано та розміщено у відкритому доступі власний набір даних, який містить понад 1800 ЕКГ-записів від 115-ти осіб. Даний набір даних використано для перевірки ефективності розроблених методів.
- Теоретичні та практичні результати роботи впроваджено у діяльність ТОВ "СВІФТ СОЛЮШНС" (м. Харків) та в навчальному процесі НУ «Львівська політехніка».

Повнота висвітлення результатів в опублікованих працях, апробація роботи

Наукові положення та отримані результати достатньо повно представлені в опублікованих автором наукових працях та апробовані на наукових конференціях в Україні та закордоном, зокрема:

- V Міжнародна науково-технічна конференція «Захист інформації і

безпека інформаційних систем» (2–3 червня 2016 року, Львів 2016, Україна);

- The 9th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (21-23 вересня, 2017 року, Бухарест, Румунія);
- VI Міжнародна науково-технічна конференція «Захист інформації і безпека інформаційних систем» (1–2 червня 2017 року, Львів 2017, Україна);
- The 3rd International Scientific Conference on Brain-Computer Interfaces (13–14 березня 2018 року, Ополе, Польща);
- The 2018 IEEE 4th International Symposium on Wireless Systems within the International Conferences on Intelligent Data Acquisition and Advanced Computing Systems (20-21 вересня 2018року, Львів, Україна);
- VII Міжнародна науково-технічна конференція "Захист інформації і безпека інформаційних систем"(30-31 травня 2019, Львів, Україна);
- Міжвідомчі міжрегіональні семінари Наукової Ради НАН України «Технічні засоби захисту інформації» (14 березня 2019 року, 14 травня 2020 року, Львів, Україна);
- IX Międzynarodowa Konferencja Studentów oraz Doktorantów „Inżynier XXI wieku" (6 грудня 2019, Бельсько-Бяла, Польща).

Основні положення дисертації опубліковано у 13 наукових працях, з яких: 1 розділ у колективній монографії, 1 статтю у науковому періодичному виданні іншої держави, що включене до міжнародної наукометричної бази даних (Scopus), 1 статтю у серійному науковому виданні іншої держави, що включене до міжнародної наукометричної бази даних (Scopus), 5 статей у наукових фахових виданнях України з технічних наук та 5 наукових публікацій у збірниках матеріалів та тез конференцій, з яких 2 включені до баз даних WoS, Scopus.

Структура дисертації цілком відповідає логіці й послідовності вирішення поставлених задач. Наукова робота складається з анотації, вступу, чотирьох розділів, висновків, переліку використаних джерел та додатків.

У вступі обґрунтовано актуальність теми, а також наведено об'єкт, предмет і мету дослідження, положення наукової новизни і практичної цінності; визначено основні методи дослідження; надано інформацію про особистий внесок здобувача в спільних публікаціях, апробаціях на науково-технічних та науково-практичних конференціях.

У першому розділі розглянуто основні режими роботи і подано порівняльну характеристику сучасних систем біометричної автентифікації. Проведено порівняння найпоширеніших біометричних маркерів за

допомогою формалізованих критеріїв (універсальність, унікальність, постійність, вимірюваність, продуктивність, прийнятність, стійкість до обману, ціна, тощо). Представлено детальний опис електрокардіограми (ЕКГ) як біометричного маркера в системах розпізнавання, показано його переваги і проблеми на шляху практичного застосування в системах автентифікації. Проаналізовано відомі підходи опрацювання ЕКГ-сигналу на основі виділення характерних точок (fiducial points) та без такого виділення (non-fiducial point), тобто на основі інтелектуального аналізу повного набору вибірок ЕКГ-сигналу. Сформульовано завдання дисертаційного дослідження.

У другому розділі розглянуто особливості процесу автентифікації за ЕКГ-сигналом. Формалізовано структуру біометричної системи розпізнавання. Наведено детальний опис і функції кожного із структурних елементів. Розглянуто перспективні підходи до покращення технічних і експлуатаційних характеристик біометричної системи ЕКГ-автентифікації. Передовсім, обґрунтовано доцільність введення в ланцюг опрацювання електрокардіограми двох додаткових компонент: компонента темпоральної нормалізації ЕКГ-сигналу, що покликана забезпечити інваріантність результатів автентифікації до зміни частоти серцевого ритму, тим самим підвищивши достовірність роботи біометричної системи; компонента виявлення та коригування артефактів у ЕКГ-сигналі, яка за допомогою інструментарію статистики або машинного навчання підвищує точність і швидкодію системи біометричної автентифікації. Подано методики оцінювання ефективності методів і засобів біометричної автентифікації на основі ЕКГ-сигналу. Представлено сформовану автором базу записів електрокардіограм (Lviv Biometric Dataset), яка на момент написання дисертації містила 1809 записів виміряних у 115 суб'єктів на часовому горизонті понад два роки. Базу Lviv Biometric Dataset викладено у відкритий доступ, поряд із іншими базами ЕКГ-записів.

Третій розділ спрямовано на розроблення моделей та методів для покращення характеристик біометричних систем автентифікації на основі ЕКГ. Спрощений і зручний для систем автентифікації відбір ЕКГ-потенціалів із пальців лівої і правої рук призводить до зниження якості запису. Частотні смуги корисного сигналу і завад перекриваються, тому після цифрової фільтрації у ЕКГ-записах спостерігаються залишкові артефакти. Описані у літературних джерелах підходи спираються на виявлення і відкидання фрагментів ЕКГ з аномальними відхиленнями. У роботі вперше запропоновано не відкидати, а виправляти фрагменти з аномальними

відхиленнями, що важливо для збереження необхідного обсягу даних для класифікатора і скорочення часу відбору ЕКГ. Розроблено підхід до виправлення залишкових артефактів у ЕКГ-сигналах, який складається із трьох етапів: 1. Формування референційного образу біометричного маркера; 2. Виявлення фрагментів ЕКГ-сигналу із промахами; 3. Заміна цих фрагментів на відповідні значення із референційного образу. Застосування такого підходу дає змогу суттєво підвищити достовірність результатів автентифікації. Запропоновано і досліджено два методи формування референційного образу ЕКГ-маркера для виправлення залишкових артефактів у ЕКГ-сигналах у системі біометричної автентифікації: на основі невимогливої до обчислювальних ресурсів формальної статистичної моделі; на базі нечіткої нейромережевої моделі, що дає змогу зменшити похибки автентифікації першого і другого роду відповідно у 4 та 3 рази. Для етапу виявлення фрагментів із промахами виконано дослідження впливу гіперпараметрів (тривалість ковзного вікна і поріг допустимого відхилення вибірки) на точність автентифікації, що дало змогу знайти оптимальні їх значення за критерієм мінімальної похибки. Розроблено та апробовано інструментарій для темпоральної нормалізації ЕКГ-сигналу. Серед сучасних методів класифікації здійснено вибір оптимального для побудови системи автентифікації. Досліджено придатність біометричної системи автентифікації до масштабування, а саме визначено вплив збільшення числа користувачів на точність автентифікації.

У четвертому розділі імплементовано біометричну систему автентифікації з покращеними характеристиками на основі використання розроблених автором моделей і методів. Зокрема, щоб показати можливість імплементації біометричної системи ЕКГ-автентифікації на пристроях з обмеженими обчислювальними ресурсами імплементовано біометричну систему на базі мікрокомп'ютера Raspberry Pi 3B. Проведено дослідження швидкодії імплементованої біометричної системи, за результатами якого сформовано рекомендації для імплементації біометричних систем автентифікації як на основі персональної робочої станції, так і на базі мікрокомп'ютера Raspberry Pi. Досліджено часову стабільність ЕКГ-сигналів на довготривалих проміжках часу (роки, місяці), а також визначено ступінь впливу варіативності інформативних ознак електрокардіограми на точність автентифікації. Результати досліджень засвідчили, що ЕКГ є стабільним маркером і може застосовуватися у реальних системах автентифікації, причому система здатна адекватно розпізнавати користувачів упродовж

тривалого часу без необхідності проміжного калібрування. Таким чином, доведено високий потенціал і перспективність електрокардіограми, як біометричного маркера, для побудови надійних систем автентифікації.

У висновках сформульовані основні результати дисертаційної роботи.

Відсутність (наявність) порушення академічної доброчесності

У дисертаційній роботі відсутні порушення академічної доброчесності. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело.

Зауваження щодо змісту і результатів роботи:

1. Формулювання наукової новизни у дисертаційній роботі виконано не з використанням традиційного підході (ступінь новизни, науковий результат, відмінність від аналогів, отриманий ефект), що ускладнює оцінювання наукових результатів у порівнянні з відомими методами та підходами;

2. Пункти 5 та 6 наукової новизни не містять ступеня новизни, з огляду на це важко оцінити їх оригінальність, тобто чи вони запропоновані вперше, чи удосконалені, чи отримали подальший розвиток.

3. У першому розділі роботи в табл. 1.4 наведено аналіз відомих підходів за предметом досліджень. Проте, на мою думку, дисертанту варто було б більше уваги приділити вибору й обґрунтуванню критеріїв для проведення аналізу, що дозволило б виділити більшу кількість невирішених завдань у цьому напрямку.

4. Другий розділ дисертації містить огляд загальновідомих алгоритмів машинного навчання, які, я вважаю, мали б бути винесені у перший оглядовий розділ. У другому розділі варто було б більше уваги приділити практичним аспектам застосування цих алгоритмів у власних розробках.

5. У четвертому розділі дисертаційної роботи автор проводить тестування продуктивності біометричних систем автентифікації імплементованих на основі мікрокомп'ютера Raspberry Pi, проте не наводить чіткої методики проведення експерименту (загальноприйнятої у біометрії, або запропонованої особисто здобувачем).

Однак зазначені зауваження не носять принциповий характер і не знижують цінності проведеного здобувачем дослідження, актуальності, новизни та практичної значущості дисертаційної роботи.

Висновки щодо відповідності дисертації встановленим вимогам

Дисертаційна робота за актуальністю, науковою новизною, практичним значенням, особистим внеском автора, обсягом і рівнем публікацій, достовірністю відповідає встановленим вимогам до дисертацій. Результати роботи викладено чітко, послідовно та логічно, висновки за розділами та загальні висновки дисертації містять якісні і кількісні наукові та практичні результати. За поставленою метою та вирішеними задачами, об'єктом та предметом досліджень, отриманими результатами робота Сабодашка Дмитра Володимировича відповідає спеціальності 125 – Кібербезпека.

Висновки щодо дисертації в цілому

За результатами аналізу змісту дисертації вважаю, що дисертація Сабодашка Дмитра Володимировича є завершеним науковим дослідженням, у якому розв'язана важлива науково-технічна задача щодо пошуку ефективних шляхів покращення технічних і експлуатаційних характеристик біометричних систем автентифікації за ЕКГ-сигналом.

Враховуючи актуальність, наукову новизну і практичне значення одержаних результатів, вважаю, що дисертаційна робота «Вдосконалення методів і засобів біометричної автентифікації на основі електрокардіограми» цілком відповідає вимогам «Порядку проведення експерименту з присудження ступеня доктора філософії» (Постанови Кабінету Міністрів України №167 від 06 березня 2019 року), а її автор Сабодашко Дмитро Володимирович заслуговує присудження ступеня доктора філософії за спеціальністю 125 – Кібербезпека.

Офіційний опонент

заступник декана факультету
кібербезпеки, комп'ютерної та
програмної інженерії Національного
авіаційного університету,
доктор технічних наук, доцент С. О. Гнатюк

«19» травня 2021 р.

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ
01132330
МІСТО КИЇВ

Підпис гр. Гнатюка С.О.
засвідчую
Вчений секретар
Національного авіаційного університету
М. Ленковський