Отримано
06.01.2025
Голова спеціалізованої
вченої ради
ДФ 26.133.078
д.т.н., проф. Н.В. Корнієнко

Голові спеціалізованої вченої ради
ДФ 26.133.078 у Київському столичному
університеті імені Бориса Грінченка
доктору технічних наук, професору,
професору кафедри інформаційної
та кібернетичної безпеки імені
професора Володимира Бурячка
Факультету інформаційних технологій
та математики Київського столичного
університету імені Бориса Грінченка
КОРШУН Наталії Володимирівні

РЕЦЕНЗІЯ

КРЮЧКОВОЇ Лариси Петрівни, доктора технічних наук, професора, професора кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка Київського столичного університету імені Бориса Грінченка, на дисертацію **ІОСІФОВА Євгена Анатолійовича «Методи та засоби забезпечення безпечного розпізнавання та параметризації результатів обробки голосової інформації»**, подану на здобуття ступеня доктора філософії за спеціальністю 125 Кібербезпека.

1. Актуальність дисертаційного дослідження

У сучасному світі, де інформація стала основним ресурсом, технології розпізнавання голосу та обробки природної мови набувають все більшого значення. Зростання обсягів цифрових комунікацій та необхідність оперативного аналізу великих масивів даних роблять ці технології критично важливими для багатьох галузей, включаючи державне управління, комерційний сектор та повсякденне життя. Разом з цим існують суттєві виклики, пов'язані з забезпеченням безпеки, конфіденційності та ефективності обробки голосової інформації.

Більшість сучасних моделей навчання потребують великих обсягів розмічених даних, які не завжди доступні для ряду мов. Це обмежує можливості застосування передових технологій у країнах, де ці мови є основними. Розробка

методів автоматизованого створення навчальних наборів даних з нерозмічених аудіозаписів може значно знизити вартість та прискорити процес тренування моделей, що є надзвичайно важливим для розвитку локальних технологій та забезпечення мовного розмаїття у цифровому просторі.

Актуальність теми дослідження полягає в необхідності розробки нових методів і засобів, які б дозволили підвищити ефективність і безпеку розпізнавання та параметризації голосової інформації. В умовах зростаючих кіберзагроз та підвищеної уваги до захисту особистих даних питання безпечної обробки аудіоданих стає надзвичайно важливим. Крім того, розвиток технологій машинного та глибинного навчання відкриває нові можливості для вдосконалення систем розпізнавання мовлення, але водночас вимагає вирішення проблем, пов'язаних з якістю та кількістю навчальних даних.

Запропоноване дослідження відповідає нагальним потребам сучасного суспільства у забезпеченні ефективної та безпечної обробки голосової інформації. Розробка методів, що поєднують підготовку навчальних аудіоданих та підходи до навчання і налаштування мовних моделей, має великий потенціал для практичного застосування в різних галузях. Це сприятиме не лише технологічному прогресу, але й захисту прав громадян та забезпеченню національної безпеки.

Таким чином, вдосконалення систем розпізнавання мовлення на підприємствах як критичної інфраструктури, так і комерційного напрямку за допомогою методів машинного та глибинного навчання є вкрай актуальним та своєчасним для побудови систем нового покоління.

2. Наукова новизна результатів дисертації

Новизна результатів дисертаційного дослідження **ІОСІФОВА Євгена Анатолійовича** зумовлена тим, що *вперше розроблено методи автоматизованого конвеєру* для створення навчальних наборів даних з нерозмічених аудіозаписів і *метод підвищення точності розпізнавання розмовної мови для близькоспоріднених мов*. Також *вдосконалено методи*

сегментації неформатованого тексту з використанням мовного моделювання та маркування послідовностей і *розпізнавання багатомовних емоцій* шляхом оцінки переносу між різними мовами.

3. Теоретичне і практичне значення результатів дисертації

Теоретичне значення дисертації **ІОСІФОВА Євгена Анатолійовича** не викликає сумніву, оскільки здобувач пропонує застосовувати безпечне розпізнавання та параметризацію результатів обробки голосової інформації, що виявляється у заміні традиційних моделей, заснованих на ідеї наявності великих наборів розмічених даних, на користь автоматизації процесу створення навчальних наборів даних з нерозмічених аудіозаписів через ключові фактори:

– підвищення вимог до конфіденційності та захисту персональних аудіоданих. Зі зростанням регуляторних стандартів та законодавчих актів, таких як GDPR і HIPAA, необхідність у надійних методах обробки аудіоданих стає критично важливою. Це вимагає розробки інноваційних технологій для структурованого аналізу та пошуку аудіоінформації з урахуванням вимог конфіденційності та етичних норм;

– переосмислення методів розпізнавання мовлення та обробки природної мови, тому що із розвитком генеративних моделей і збільшенням обчислювальних можливостей, традиційні підходи, що покладаються на великі розмічені набори даних, виявляються менш ефективними. Це стимулює створення нових методів, зокрема автоматизації формування навчальних даних з нерозмічених аудіозаписів, для більш ефективного вирішення сучасних завдань;

– посилення ролі хмарних технологій у зберіганні та обробці аудіоданих. Широке впровадження хмарних сервісів для зберігання конфіденційної аудіоінформації піднімає питання безпеки та приватності. Це вимагає впровадження методів деперсоналізації та видалення чутливої інформації з аудіопотоків, щоб забезпечити належний рівень захисту даних;

– необхідність оперативного виявлення та реагування на загрози, оскільки

системи розпізнавання мовлення часто не обладнані механізмами негайного реагування на виявлені ризики, стає важливим розробляти інтегровані рішення, які забезпечують миттєве сповіщення про інциденти, що має мінімізувати потенційні збитки та забезпечити швидку реакцію на нові загрози;

– виклики точного розпізнавання емоцій у мультикультурних середовищах. Поширення діпфейків та спотворених аудіоданих ускладнює ідентифікацію справжніх емоцій та намірів. Це може призвести до перенавантаження систем фальшивими запитами, тому необхідно розробляти ефективні методи розпізнавання емоцій, особливо в умовах обмежених ресурсів та відсутності розмічених даних.

– складнощі безперервного моніторингу та обробки голосових даних, що вимагає високоефективних методів для швидкого реагування та аналізу. Це включає як негайне виявлення та дію, так і можливість детального розслідування подій після їх виникнення;

– експоненційне зростання обсягів голосової інформації в епоху цифрових комунікацій. З розвитком телеконференцій та інших онлайн-платформ, особливо в умовах дистанційної роботи, значно збільшилися обсяги та тривалість аудіорозмов. Велика кількість нерозмічених транскриптів потребує ефективних методів сегментації та обробки тексту, щоб забезпечити їх подальше використання в задачах обробки природної мови;

– зростання кіберзагроз, спрямованих на аудіодані та системи розпізнавання мовлення. Зі збільшенням кількості кібератак, що націлені на викрадення або маніпуляцію аудіоінформації, виникає необхідність розробки більш надійних методів захисту та виявлення таких загроз у системах обробки мовлення.

Таким чином, наукове обґрунтування забезпечення безпечного розпізнавання та параметризації результатів обробки голосової інформації набуває вагомості, оскільки воно гармонізується із сучасним ландшафтом кібербезпеки, розв'язує проблеми, пов'язані з появою потужних генеративних моделей, стрімкому зростанню обчислювальних можливостей та еволюцією

характеру кіберзагроз. Цей підхід забезпечує прогнозовану та адаптивну реакцію на виклики, які виникають при захисті персональної голосової інформації в системах критичної інфраструктури та приватних підприємств.

4. Наукова обґрунтованість результатів дослідження, наукових положень, висновків і рекомендацій, сформульованих у дисертації, та їхня достовірність

Наукова обґрунтованість результатів дослідження зумовлена глибоким опрацюванням теоретичних джерел та їх аналізом. Наукові положення, висновки і результати, які представлено в дисертації **ІОСІФОВА Євгена Анатолійовича**, є теоретично і емпірично обґрунтованими та достовірними. Вони базуються на використанні загальнонаукових та спеціальних методів дослідження, таких як: методи порівняльного аналізу; теорія ймовірності та математичної статистики; критичний аналіз обмежень та ризиків застосування; технологія рекурентних нейронних мереж; архітектура енкодерів-декодерів і механіки для формування уваги; марківські моделі, коннекціоністська модель часової класифікації тощо. Загальні висновки дисертації логічні та переконливі. Вони повністю висвітлюють хід дослідження, поставлені завдання та результати проведеної роботи.

5. Зв'язок теми дисертаційного дослідження з науковими планами, програмами, фундаментальними та прикладними дослідженнями

Дисертаційне дослідження виконано відповідно до планів наукової і науково-технічної діяльності кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка Київського столичного університету імені Бориса Грінченка в рамках науково-дослідної роботи №0122U200483 «Методи та моделі забезпечення кібербезпеки інформаційних систем переробки інформації та функціональної безпеки програмно-технічних комплексів управління критичної інфраструктури» (КСУБГ, м. Київ). Результати наукових досліджень впроваджені в «Ender Turing ÓÜ» (Таллінн, Естонія, акт від

07.09.2024 року) і «PP 2 SPV Limited Liability Company» (Ольштин, Польща, акт від 17.07.2024 року).

6. Рівень виконання поставленого наукового завдання та оволодіння здобувачем методологією наукової діяльності

Визначені в дисертації завдання здобувач виконав на високому рівні. Чітко сформульовано мету і завдання дослідження, застосовано доцільні методи для вирішення задач і досягнення поставленої мети. Представлений текст дисертаційної роботи демонструє, що **ІОСІФОВ Євген Анатолійович** опанував методологію наукової діяльності, уміло застосовує її на практиці, а отже, оволодів необхідними для рівня доктора філософії компетенціями.

7. Апробація результатів дисертації

Повнота викладу основних результатів дисертації у наукових публікаціях. У наукових публікаціях у повному обсязі висвітлено наукові результати дисертації відповідно до мети та поставлених завдань. Наукові результати дисертації висвітлено у 9 наукових працях (із них одна одноосібна): 4 статті у наукових фахових виданнях України, 5 публікацій (з них усі у співавторстві), у яких додатково висвітлено результати дисертації у наукових виданнях, включених до міжнародної наукометричної бази Scopus. Основні положення, висновки і результати дослідження викладались у процесі виступів і обговорень на науково-практичних міжнародних конференціях. В роботах, опублікованих у співавторстві, зазначено особистий внесок здобувача.

8. Структура та зміст дисертації, її самостійність, завершеність, відповідність вимогам щодо оформлення й обсягу

Зміст дисертаційного дослідження **ІОСІФОВА Євгена Анатолійовича** «Методи та засоби забезпечення безпечного розпізнавання та параметризації результатів обробки голосової інформації» охоплює основні аспекти теми, відповідає меті та завданням дослідження. Робота містить анотацію, вступ, три

розділи основної частини з підпунктами, висновки до розділів, загальні висновки, список використаних джерел з 207 найменувань (з них 175 є унікальними) та восьми додатків. Робота містить 20 таблиць та 34 рисунки. Обсяг основного тексту дисертації складається з 179 сторінок друкованого тексту. Контекст дисертаційного дослідження вирізняється логічністю, індивідуальним і творчим авторським підходом до задуму дисертації, обізнаністю здобувача в методологічному інструментарії, підходах, методах, принципах, обґрунтованістю висновків, оригінальному баченні дискусійних проблем.

У вступній частині здобувачем обґрунтовано актуальність теми дослідження, її зв'язок із науковими програмами, планами, темами, сформульовано об'єкт, предмет, мету і завдання дослідження, інформаційну базу, методи дослідження, наукову новизну і практичне значення роботи, особистий внесок здобувача, дані про апробацію отриманих результатів та публікації за темою дисертації.

У першому розділі «Аналіз існуючих методів розпізнавання та параметризації результатів обробки голосової інформації» **ІОСІФОВИМ Євгеном Анатолійовичем** проведено аналіз існуючих методів розпізнавання та параметризації результатів обробки голосової інформації. Розглядається еволюція технологій роботи з природною мовою, включаючи історію машинного та глибинного навчання, основні концепти та механізми цих технологій. Здобувач детально аналізує сучасні методи обробки природної мови, а також досліджує різні підходи до автоматичного розпізнавання мови, включаючи приховані марківські моделі та наскрізні моделі розпізнавання. На завершення формується наукове завдання дослідження та окреслюються підходи до навчання мовних моделей.

У другому розділі «Підходи до підвищення безпеки та ефективності розпізнавання голосової інформації» здобувачем розглянуто підходи до підвищення безпеки та ефективності розпізнавання голосової інформації. Здобувач аналізує методи забезпечення безпеки голосових даних в контексті кіберзагроз та ролі голосової інформації в інформаційних системах. Описуються

метрики та критерії оцінювання якості розпізнавання, а також пропонується метод автоматизованого конвеєра для створення навчальних наборів даних з нерозмічених аудіозаписів. Викладено способи підвищення ефективності розпізнавання мовної інформації, зокрема розпізнавання багатомовних емоцій та підвищення точності для близькоспоріднених мов, а також обмеження та ризики використання цих методів у системах кібербезпеки.

Третій розділ роботи «Методи сегментації, розпізнавання та підвищення точності обробки природної мови для забезпечення інформаційної безпеки підприємства» зосереджується на методах сегментації, розпізнавання та підвищення точності обробки природної мови для забезпечення інформаційної безпеки підприємства. Здобувач визначає вимоги до даних для навчання мовних моделей та аналізує доступні мовні корпуси для української мови. Пропонується метод сегментації неформатованого тексту з використанням мовного моделювання та маркування послідовностей, підтриманий експериментальним порівнянням різних підходів. Представлено вдосконалений метод розпізнавання багатомовних емоцій шляхом оцінки переносу між різними мовами, який, у порівнянні з існуючими методами, дає можливість більш точно визначати поріг емоційності для різних мов і, тим самим, мінімізувати нелегітимні спрацьовування.

9. Дотримання академічної доброчесності у дисертації та наукових публікаціях. Відсутність (наявність) академічного плагіату, фабрикації, фальсифікації

Аналіз тексту дисертаційного дослідження та публікацій дозволяє стверджувати, що **ІОСІФОВ Євген Анатолійович** дотримувався правил академічної доброчесності, в тексті не знайдено некоректного цитування, ознак плагіату, фабрикації чи фальсифікації. Дисертаційна робота є оригінальним завершеним науковим дослідженням, що відповідає вимогам, які висуваються Міністерством освіти і науки України до оформлення дисертацій на здобуття наукового ступеня доктора філософії.

10. Дискусійні положення, недоліки та зауваження до дисертації

Принципових зауважень щодо структури, основних положень та концепції дисертації **ІОСІФОВА Євгена Анатолійовича** немає. Оцінюючи загалом позитивно наукове і практичне значення отриманих дисертантом результатів, дозволю собі висловити зауваження і рекомендації до окремих положень дисертації:

1. Розділ 2.3.3 щодо реалізації алгоритму конвеєра не надає достатньо інформації про конкретні кроки, особливо стосовно очищення та попередньої обробки даних. А твердження про досягнення найсучаснішого WER 5,24 для української мови потребує ретельного порівняння з існуючими моделями та надання деталей щодо умов тестування. Вказаний час (84 години) на створення 2 500 годин навчального набору даних потребує додаткового контексту щодо використаних обчислювальних ресурсів, також було б корисно деталізувати характеристики апаратного забезпечення.

2. В роботі не розглянуто альтернативні архітектури нейронних мереж, які могли б бути ефективними для задачі розпізнавання емоцій, що обмежує повноту дослідження.

3. Обґрунтування вибору мови програмування Python є неповним, аргументи щодо продуктивності та масштабованості не є переконливими. Включення кодових прикладів або псевдокоду підвищило б розуміння деталей реалізації конвеєра і зробило б розділ більш практичним.

4. В розділі 3.2 не обґрунтований вибір розміру блоку в 16 токенів та його вплив на результати, а також відсутній аналіз впливу різних гіперпараметрів на продуктивність моделей та їх оптимізацію.

5. Табл. 3.2 потребує додаткових пояснень, для кращого розуміння не вистачає детального опису прикладів маркування послідовностей.

6. Не розглянуто можливість використання мультимодальних даних (зображення, жести) для покращення точності розпізнавання емоцій, що є актуальним напрямком у цій сфері. При описі архітектури моделі ECAPA-

TDNN не надано повного пояснення щодо вибору параметрів та гіперпараметрів моделі.

7. У табл. 3.4 недостатньо інформації щодо ліцензійних умов використання наборів даних, що є важливим для легального відтворення експериментів іншими дослідниками. Також у розділі 3.3.3 відсутній детальний опис процесу підготовки та валідації даних, яким чином, наприклад, здійснювалося випадкове вибирання даних для тестових та валідаційних наборів. Не надано пояснення асиметричної поведінки моделей між парами мов, як-то у випадку пар FR-ZN та DE-FA.

8. У розділі 3.4.2 не надано достатньо деталей про процес попередньої обробки даних, зокрема про те, як було підготовлено та очищено дані перед навчанням. У розділі 3.4.4 не надано достатньо інформації про параметри навчання моделей, зокрема про вибір гіперпараметрів та їх оптимізацію.

9. Табл. 3.14 містить інформацію про розмір навчальних наборів даних, але не надає деталей про їхню якість та різноманітність, що може впливати на результати.

10. У розділі 3.4.5 не обговорено можливість перенавчання моделей, особливо при навчанні на обмежених та незбалансованих даних. Не наведено деталей про використані оптимізаційні алгоритми та функції втрат, що ускладнює відтворення експериментів.

В цілому, зазначені зауваження не знижують наукової та практичної цінності проведеного **ІОСІФОВИМ Євгеном Анатолійовичем** дослідження і не впливають на загальну позитивну оцінку дисертації.

11. Загальний висновок про рівень набуття здобувачем теоретичних знань, відповідних умінь, навичок та компетентностей

ІОСІФОВ Євген Анатолійович на високому рівні оволодів методологією наукової діяльності, набув теоретичних знань, умінь, навичок та компетентностей. Здобувач вільно володіє матеріалом дослідження та має достатній досвід для проведення самостійних дослідницьких робіт.

12. Загальна оцінка дисертації і наукових публікацій щодо їхнього наукового рівня з урахуванням дотримання академічної доброчесності та щодо відповідності вимогам

Аналіз дисертаційної роботи **ІОСІФОВА Євгена Анатолійовича** на тему «Методи та засоби забезпечення безпечного розпізнавання та параметризації результатів обробки голосової інформації» і наукових публікацій дає підстави для висновку про те, що робота є завершеним, цілісним науковим дослідженням, виконана на актуальну тему, містить елементи наукової новизни та має теоретичне й практичне значення. Дисертація оформлена відповідно до вимог наказу №40 Міністерства освіти і науки України «Про затвердження вимог до оформлення дисертацій» від 12 грудня 2017 р. Дисертація за формою і змістом відповідає вимогам, викладеним у Порядку присудження ступеня доктора філософії та скасування рішення разової спеціалізованої вченої ради закладу вищої освіти, наукової установи про присудження ступеня доктора філософії, затвердженого постановою №44 Кабінету Міністрів України від 12 січня 2022 р. (зі змінами). **ІОСІФОВ Євген Анатолійович**, автор дисертації на тему «Методи та засоби забезпечення безпечного розпізнавання та параметризації результатів обробки голосової інформації», може представити роботу на кафедральному науковому семінарі з рекомендацією її до подальшого захисту в разовій спеціалізованій Вчені раді закладу вищої освіти за спеціальністю 125 Кібербезпека, галузі знань 12 Інформаційні технології.

Рецензент:
доктор технічних наук, професор
професор кафедри інформаційної
та кібернетичної безпеки
імені професора Володимира Бурячка
Київського столичного університету
імені Бориса Грінченка

Лариса КРЮЧКОВА

КИЇВСЬКИЙ СТОЛИЧНИЙ УНІВЕРСИТЕТ ІМЕНІ БОРИСА ГРІНЧЕНКА Код ЄДРПОУ 45307965 * УКРАЇНА *

КИЇВСЬКИЙ СТОЛИЧНИЙ УНІВЕРСИТЕТ ІМЕНІ БОРИСА ГРІНЧЕНКА
Код ЄДРПОУ 45307965
ВЛАСНИЙ ПІДПИС
Л. Крючкової ЗАСВІДЧУЮ
(ПІБ)
начальник ВК
(посада)