ВИСНОВОК

про наукову новизну, теоретичне та практичне значення результатів дисертації Іосіфова Євгена Анатолійовича на тему «Методи та засоби забезпечення безпечного розпізнавання та параметризації результатів обробки голосової інформації», поданої на здобуття ступеня доктора філософії з галузі знань 12 Інформаційні технології за спеціальністю 125 Кібербезпека

Актуальність теми дослідження. Сучасний світ характеризується стрімким розвитком інформаційних технологій, які суттєво впливають на всі сфери суспільства, зокрема на організаційну та національну безпеку. Водночас, зростання обсягів цифрових комунікацій та інформаційних потоків створює нові виклики для організацій і державних органів у сфері збору та аналізу даних. Однак, дане завдання ускладнюється через величезні масиви інформації, які надходять у вигляді дзвінків, голосових повідомлень та текстових даних, що потребує ефективних методів обробки. Причиною такого розповсюдження є людський природний спосіб комунікації – мовлення. Така трансформація призвела до необхідності впровадження автоматизованих систем аналізу, що, в свою чергу, призводить до підвищення ефективності реагування на потенційні загрози.

Кількість і вектори кіберзагроз та інформаційних атак постійно зростає. Цьому зокрема сприяло підвищення інтересу до технологій розпізнавання голосової мови та обробки природної мови з боку зловмисників, і як відповідь з боку державних установ та організацій, як інструментів для забезпечення безпеки. Тому безпечна обробка природної мови означає процес обробки та інтерпретації мовлення або тексту за допомогою технологій штучного інтелекту з дотриманням вимог безпеки і приватності, що включає захист аудіоданих від витоків, несанкціонованого доступу, дотримання конфіденційності суб'єктів, спотворення змісту або маніпуляцій, а також із урахуванням правових та етичних аспектів.

В результаті, виникає необхідність у впровадженні сучасних технологій розпізнавання та обробки природної мови в системи організаційної і державної безпеки. Водночас, існують технічні, етичні та правові аспекти, які потребують детального аналізу. Однак, в зв'язку з важливістю балансу між забезпеченням

безпеки та удосконалення процедури розпізнавання природньої мови, ці питання набувають особливої актуальності.

У даному контексті, розгляд та розуміння різних підходів, методів та сучасних практик застосування технологій розпізнавання мови стають важливими. Так, одним із найперспективніших підходів вважається використання методів машинного навчання та глибоких нейронних мереж для підвищення точності розпізнавання та аналізу мовних даних.

Особистий внесок здобувача полягає у виборі теми дисертації, обґрунтуванні та формулюванні мети, об'єкта, методів досліджень, визначенні завдань наукового дослідження, проведенні теоретичного обґрунтування та обробленні й аналізі даних, формулюванні висновків. В дослідженні автором:

– проаналізовано поточний стан проблеми захисту аудіоінформації та підходів до її захисту;

– вдосконалено моделі комбінування методів роботи з природною мовою і розпізнавання емоцій в потоці голосовох інформації;

– визначені особливості програмної реалізації алгоритмів для розпізнавання голосової інформації та формування параметрів для забезпечення інформаційної безпеки;

– запропоновано та обґрунтовано модель маркування немаркованих даних для їхнього використання при тренуванні моделей;

– побудовано модель переносу знання між моделями для підвищення точності розпізнавання емоцій в голосовій інформації;

– здійснено детальний аналіз сучасних підходів і алгоритмів для роботи з природною мовою, в тому числі для аналізу намірів суб'єктів;

– проведено експериментальні дослідження моделі сегментування і підготовки несегментованого тексту;

– проведено порівняльний аналіз алгоритмів та моделей глибинного навчання для розпізнавання природної мови;

– визначені критерії аналізу функціонування алгоритмів та формування вимог до наборів аудіоданих для тренування моделей для роботи з голосовою інформацією;

– запропоновано та обґрунтовано вдосконалений прототип системи розпізнавання емоційного стану суб'єкту при аналізі його голосової інформації.

Зв'язок роботи з науковими програмами, планами, темами. Дисертацію виконано безпосередньо пов'язаний з реалізацією доктрини інформаційної безпеки України, Стратегії інформаційної безпеки та Стратегії

кібербезпеки України. Дисертація виконана відповідно до планів наукової і науково-технічної діяльності Київського столичного університету імені Бориса Грінченка в рамках науково-дослідної роботи: «Методи та моделі забезпечення кібербезпеки інформаційних систем переробки інформації та функціональної безпеки програмно-технічних комплексів управління критичної інфраструктури» (06.22–06.27 рр., реєстраційний номер 0122U200483).

Мета дослідження полягає в підвищенні ефективності застосування безпечного розпізнавання та параметризації результатів обробки голосової інформації в інформаційно-комунікаційних системах завдяки комбінуванню підходів при формуванні розмічених аудіоданих для навчання мовних моделей та в процесі навчання та донавчання цих моделей.

Завдання дослідження:

– проаналізувати поточний стан і підходи до забезпечення безпеки голосової інформації, як одного із ключових елементів персональних даних суб'єкта, а також розглянути сучасні архітектуру та структуру елементів інформаційно-комунікаційних систем, які працюють із аудіоданими;

– провести детальний аналіз метрик природної мови та критеріїв для оцінювання якості її обробки;

– розробити модель автоматизованого конвеєру для створення навчальних наборів даних з нерозмічених аудіозаписів та визначити критерії оцінки роботи цієї моделі;

– визначити способи підвищення ефективності розпізнавання мовної інформації при одночасній роботі із кількома мовами при визначенні емоційного стану суб'єкта;

– формалізувати переваги, обмеження, ризики та виклики при впровадженні та застосуванні методів розпізнавання голосової інформації;

– сформулювати вимоги до даних для навчання мовних моделей та дослідити доступні мовні корпуси для української мови;

– покращити сегментацію неформатованого тексту з використанням мовного моделювання та маркування послідовностей;

– дослідити нові підходи до розпізнавання багатомовних емоцій шляхом оцінки переносу між різними мовами, а також запропонувати спосіб підготовки та валідації вхідних даних;

– запропонувати підходи до підвищення точності розпізнавання природної мови для близькоспоріднених мов;

– вибрати мови із низької точністю для проведення експериментів та провести за допомогою них тренінг моделі, а також верифіковати результати експериментів.

Об'єкт дослідження: процес забезпечення безпеки голосової інформації та емоційного стану при побудові розподіленої інформаційно-комунікаційної системи.

Предмет дослідження: методи та засоби забезпечення безпечного розпізнавання та параметризації результатів обробки голосової інформації як ключових елементів формування дієвої політики інформаційної безпеки підприємства або державної установи на основі реалізації базових положень щодо обробки природної мови.

Методи дослідження. Для проведення досліджень в дисертаційній роботі використовувалися 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; прихована і гібридна прихована марковські моделі; коннекціоністська модель часової класифікації; послідовна модель; методи трансформеру та конвеєру для безперервних потоків аудіоданих; методи валідації експериментальних результатів; методи моделювання систем управління інформаційною безпекою, етичні обмеження.

Експериментальна база дослідження. Достовірність дисертації підтверджується документами про впровадження у діяльність кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка Київського столичного університету імені Бориса Грінченка (акт від 27.08.2024 року), «Ender Turing OÜ» (Таллінн, Естонія, акт від 07.09.2024 року) і «PP 2 SPV Limited Liability Company» (Ольштин, Польща, акт від 17.07.2024 року), а також опублікованими працями та апробацією результатів наукового дослідження на конференції.

Наукова новизна одержаних результатів полягає у вирішенні актуальних наукових питань теоретичного обґрунтування та розроблення практичних рекомендацій щодо підвищенні рівня безпеки аудіоінформації, що обробляється в інформаційно-комунікаційних системах підприємств критичної інфраструктури та державних органів, за рахунок розробки й впровадження методів та засоби забезпечення безпечного розпізнавання та параметризації результатів обробки голосової інформації.

Основні положення і результати дослідження, які виносяться на захист та характеризують наукову новизну й особистий внесок дисертанта, полягають у такому:

1. Вперше запропонований та математично обґрунтований метод автоматизованого конвеєру для створення навчальних наборів даних з нерозмічених аудіозаписів. При вирішенні завдання навчання на невеликій кількості нерозмічених даних реалізується підхід автоматичного отримання високоточного маркування, на відміну від існуючих методів навчання на великому об'ємі нерозмічених даних. Це дозволяє тренувати мовні моделі при наявності незначного обсягу аудіоданих, що значно знижує вартість формування тренувального набору даних порівняно з ручним і пришвидшує процес маркуванням щонайменше на 85%.

2. Вперше запропонований метод підвищення точності розпізнавання природної мови для близькоспоріднених мов. При вирішенні завдання розпізнавання природної мови фокус і увага концентруються саме на точності, на відміну від існуючих методів розпізнавання, в яких основна увага приділяється якомога ширшому покриттю мов. Це дозволяє вбудовувати розроблений метод в системи ідентифікації про інциденти, в яких точність визначення природної мови впливає на їхній подальший аналіз, що, в свою чергу, підвищує точність роботи таких систем в середньому на 19,7% і мінімізує хибні спрацювання.

3. Вдосконалений метод сегментації неформатованого тексту з використанням мовного моделювання та маркування послідовностей. Це дозволяє в подальшому використовувати розмічені на основі аудіоданих тексти та підвищити за рахунок цього ефективність підсистем розпізнавання мови та намірів.

4. Набув подальшого розвитку метод розпізнавання багатомовних емоцій шляхом оцінки переносу між різними мовами, що сукупно з методикою розпізнавання природної мови дає можливість більш точно визначати поріг емоційності для різних мов і тим самим мінімізувати нелегітимні спрацьовування в середньому на 18%. Також враховано рівень природної емоційності окремих народів, що дозволило відкалібрувати дані для впровадження заходів безпеки на державному рівні.

Теоретичне значення результатів дисертації. Результати досліджень представлені у вигляді наукових положень, висновків і рекомендацій. Розроблені автором і викладені у дисертації наукові положення, висновки та

пропозиції мають високий рівень обґрунтованості. Опрацьовано значну кількість наукових та фахових джерел вітчизняних і зарубіжних вчених, здійснено їх аналіз та запропоновано власні підходи, що стосуються підвищення рівня безпеки аудіоінформації, що обробляється в інформаційно-комунікаційних системах підприємств критичної інфраструктури та державних органів.

Дисертація характеризується науковою глибиною та логічністю. Іосіфов Є.А. володіє ґрунтовними знаннями предмета дослідження, а також методології досліджень. Основні положення, висновки та рекомендації теоретичного та практичного характеру є обґрунтованими та достовірними. Результатом проведеного наукового дослідження є досягнення визначеної мети шляхом виконання поставлених дисертантом завдань, про що свідчать висновки до кожного розділу та дисертації загалом.

Практична значення результатів дисертації полягає в тому, що в дослідженні запропоновано метод автоматизованого конвеєру для створення навчальних наборів даних з нерозмічених аудіозаписів, який дозволяє тренувати мовні моделі при наявності незначного обсягу (від 250 год.) маркованих аудіоданих, що знижує вартість формування тренувального набору даних порівняно з ручним маркуванням на 94% та пришвидшує щонайменше на 85% швидкість маркування, що в свою чергу знижує вартість тренування моделей на 61% та пришвидшує процес навчання щонайменше на 69%. Метод підвищення точності розпізнавання природної мови для близькоспоріднених мов підвищує точність роботи систем розпізнавання в середньому на 19,7%, медіанне значення відповідає 17,6%. Також метод сегментації неформатованого тексту з використанням мовного моделювання та маркування послідовностей застосовується разом із іншими запропонованими методами та є невід'ємною частиною системи розпізнавання природної мови. А за рахунок використання методу розпізнавання багатомовних емоцій шляхом оцінки переносу між різними мовами стало можливим мінімізувати нелегітимні спрацьовування вхідної системи на 18%.

Слід відзначити розробки дисертанта, які мають практичну цінність та доведені до практичного використання. Розробки та рекомендації мають практичне застосування у діяльності:

– Київського столичного університету імені Бориса Грінченка – впроваджені в освітній процес кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка Факультету інформаційних технологій та

математики Київського столичного університету імені Бориса Грінченка у робочих програмах навчальних дисциплін спеціальності 125 Кібербезпека першого (бакалаврського), другого (магістерського) та третього (освітньо-наукового) рівнів вищої освіти та впроваджені в програмно-апаратне забезпечення лабораторій безпеки інформаційних активів, антивірусного захисту інформації, систем технічного та криптографічного захисту інформації (акт від 27.08.2024);

– «Ender Turing OÜ» (Таллінн, Естонія) – застосовані для удосконалення існуючих механізмів виявлення намірів в голосових даних та сповіщення користувачів (акт від 07.09.2024 року);

– «PP 2 SPV Limited Liability Company» (Ольштин, Польща) – використані для розпізнавання мови й емоцій для ефективної роботи інтегрованих систем аналузі голосової інформації (акт від 17.07.2024 року).

Апробація результатів дисертації. Матеріали дисертаційного дослідження обговорювалися на міжнародних наукових конференціях:

1. International Workshop on Modern Machine Learning Technologies and Data Science (MoMLeT&DS), 2022.

2. International Conference on Computer Science, Engineering and Education Applications (ICCSEEA), 2021 і 2022.

3. Workshop on Cybersecurity Providing in Information and Telecommunication Systems (CPITS), 2021 і 2022.

Публікації. Основні результати дисертації висвітлено у 9 наукових публікаціях, із них 1 – одноосібна, 8 – у співавторстві: 4 статті (з них 3 у співавторстві) у наукових виданнях, включених на дату опублікування до переліку наукових фахових видань України; 5 публікацій (з них усі у співавторстві),у яких додатково висвітлено результати дисертації.

Наукові статті, опубліковані у наукових виданнях, включених на дату опублікування до переліку наукових фахових видань України:

1. **Іосіфов, Є.** (2023). Комплексний метод по автоматичному розпізнаванню природньої мови та емоційного стану. *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка»*, *3*(19), 146–164. https://doi.org/10.28925/2663-4023.2023.19.146164.

2. Марценюк, М., Козачок, В., Богданов, О., **Іосіфов, Є.**, & Бржевська, З. (2023). Аналіз методів виявлення дезінформації в соціальних мережах за допомогою машинного навчання. *Електронне фахове наукове видання*

«Кібербезпека: освіта, наука, техніка», *2*(22), 148–155. https://doi.org/10.28925/2663-4023.2023.22.148155.

3. **Іосіфов, Є.**, & Соколов, В. (2024). Методи аналізу природної мови та застосування нейронних мереж в кібербезпеці. *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка»*, *4*(24), 398–414. https://doi.org/10.28925/2663-4023.2024.24.398414.

4. **Іосіфов, Є.**, & Соколов, В. (2024). Порівняльний аналіз методів, технологій, сервісів та платформ для розпізнавання голосової інформації в системах забезпечення інформаційної безпеки. *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка»*, *1*(25), 468–486. https://doi.org/10.28925/2663-4023.2024.25.468486.

Наукові публікації, у яких додатково висвітлено результати дисертації:

1. Romanovskyi, O., **Iosifov, I.**, Iosifova, O., Sokolov, V., Kipchuk, F., & Sukaylo, I. (2021). Automated Pipeline for Training Dataset Creation from Unlabeled Audios for Automatic Speech Recognition. *Lecture Notes on Data Engineering and Communications Technologies, 83*, 25–36. https://doi.org/10.1007/978-3-030-80472-5_3 (Scopus).

2. Iosifova, O., **Iosifov, I.**, Sokolov, V., Romanovskyi, O., & Sukaylo, I. (2021). Analysis of Automatic Speech Recognition Methods. *In Workshop on Cybersecurity Providing in Information and Telecommunication Systems (CPITS), 2923*, 252–257. (Scopus).

3. **Iosifov, I.**, Iosifova, O., Sokolov, V., Skladannyi, P., & Sukaylo, I. (2021). Natural Language Technology to Ensure the Safety of Speech Information. *In Workshop on Cybersecurity Providing in Information and Telecommunication Systems II (CPITS-II), 3187*(1), 216–226. (Scopus).

4. **Iosifov, I.**, Iosifova, O., Romanovskyi, O., Sokolov, V., & Sukailo, I. (2022). Transferability Evaluation of Speech Emotion Recognition Between Different Languages. *Lecture Notes on Data Engineering and Communications Technologies, 134*, 413–426. https://doi.org/10.1007/978-3-031-04812-8_35 (Scopus).

5. Romanovskyi, O., **Iosifov, I.**, Iosifova, O., Sokolov, V., Skladannyi, P., & Sukaylo, I. (2022). Prototyping Methodology of End-to-End Speech Analytics Software. *In 4th International Workshop on Modern Machine Learning Technologies and Data Science (MoMLeT&DS), 3312*, 76–86. (Scopus).

Особистий внесок здобувача. Всі наукові результати, що виносяться на захист, одержано здобувачем самостійно.

У статті «Аналіз методів виявлення дезінформації в соціальних мережах за допомогою машинного навчання» опублікованій у співавторстві, внесок Іосіфова Є.А. полягає в огляді існуючих підходів до виявлення фейкових новин з точки зору машинного навчання для забезпечення кібербезпеки, що загалом складає 30% тексту статті.

У статті «Методи аналізу природної мови та застосування нейронних мереж в кібербезпеці» опублікованій одноосібно, внесок Іосіфова Є.А. полягає у проведені аналізу існуючих методів розпізнавання природної мови та застосування їх в забезпеченні інформаційної безпеки, що загалом складає 80% тексту статті.

У статті «Порівняльний аналіз методів, технологій, сервісів та платформ для розпізнавання голосової інформації в системах забезпечення інформаційної безпеки» опублікованій у співавторстві, внесок Іосіфова Є.А. полягає у дослідженні і порівняння технологій, підходів, алгоритмів та платформ для розпізнавання голосової інформації та формування параметрів для забезпечення інформаційної безпеки, що загалом складає 50% тексту статті.

У статті «Automated Pipeline for Training Dataset Creation from Unlabeled Audios for Automatic Speech Recognition» опублікованій у співавторстві, внесок Іосіфова Є.А. полягає у побудові моделі автоматизованого конвеєра для маркування нерозмічених даних для їхнього використання при тренуванні моделей, що загалом складає 40% тексту статті.

У статті «Analysis of Automatic Speech Recognition Methods» опублікованих у співавторстві, внесок Іосіфова Є.А. полягає у дослідженні і порівнянні підходів і алгоритмів для розпізнавання природної мови, що загалом складає 45% тексту статті.

У статті «Natural Language Technology to Ensure the Safety of Speech Information» опублікованих у співавторстві, внесок Іосіфова Є.А. полягає у дослідженні алгоритмів та формуванні вимог до наборів аудіоданих для тренування моделей для роботи з голосовою інформацією та забезпечення їхньої безпеки, що загалом складає 65% тексту статті.

У статті «Transferability Evaluation of Speech Emotion Recognition Between Different Languages» опублікованій у співавторстві, внесок Іосіфова Є.А. полягає у побудові моделі переносу знання між мовними моделями для підвищення точності розпізнавання емоцій в голосовій інформації, що загалом складає 60% тексту статті.

У статті «Prototyping Methodology of End-to-End Speech Analytics Software» опублікованих у співавторстві, внесок Іосіфова Є.А. полягає у апробації методології на реальних задачах і у розробці прототипу системи розпізнавання і аналізу голосової інформації, що загалом складає 45% тексту статті.

Структура та обсяг дисертації. Дисертація складається зі вступу, трьох розділів, висновків, списку використаних джерел із 175 найменувань на 26 сторінках і 8 додатків. Загальний обсяг роботи становить 214 сторінок серед яких 179 сторінки основного тексту, 34 рисунки і 20 таблиць.

Оцінка мови та стилю дисертації. Дисертація написана науковою українською мовою. Стиль викладу матеріалу логічний і послідовний. Зміст роботи повністю висвітлює результати наукових досліджень. Текст роботи має смислову цілісність, послідовність і завершеність, що забезпечує легкість і доступність сприйняття матеріалу.

Дотримання здобувачем академічної доброчестності в дисертації та наукових публікаціях, в яких висвітлено наукові результати дисертації. На підставі вивченого тексту дисертації і наукових публікацій, результатів автоматизованої перевірки на плагіат та їх експертної оцінки, встановлено, що дисертація і наукові публікації виконані самостійно, не містять академічного плагіату, фальсифікації, фабрикації.

Відповідність дисертації вимогам, що представляються до дисертацій на здобуття ступеня доктор філософії. Дисертація Іосіфова Є.А., на тему «Методи та засоби забезпечення безпечного розпізнавання та параметризації результатів обробки голосової інформації» є завершеним науковим дослідженням, в якому отримано нові обґрунтовані результати. Дисертацію виконано на достатньо високому рівні, її результати мають наукову новизну і практичну значимість. Основні положення дисертації опубліковані в наукових фахових виданнях і міжнародних виданнях, що входять до наукометричної бази Scopus та оприлюднювались на міжнародних науково-практичних конференціях. Дисертаційне дослідження відповідає обраній темі, розкриває її суть та підтверджує, що автором повністю вирішено поставлені у роботі завдання.

Рішення:

1. Дисертація Іосіфова Євгена Анатолійовича на тему «Методи та засоби забезпечення безпечного розпізнавання та параметризації результатів обробки голосової інформації», подана на здобуття ступеня доктора філософії з галузі знань 12 Інформаційні технології за спеціальністю 125 Кібербезпека, є завершеною, самостійною роботою, що містить науково обґрунтовані результати, актуальність, наукову новизну, теоретичне та практичне значення і відповідає пп. 6–9 Порядку присудження ступеня доктора філософії та скасування рішення разової спеціалізованої вченої ради закладу вищої освіти, наукової установи про присудження ступеня доктора філософії, затвердженого постановою Кабінету Міністрів України від 12.01.2022 №44 (зі змінами), наказу Міністерства освіти і науки України від 12.01.2017 №40 «Про затвердження Вимог до оформлення дисертації», затвердженого Міністерством юстиції України 03.02.2017 за №155/30023.

2. Дисертація Іосіфова Євгена Анатолійовича та наукові публікації, у яких висвітлено наукові результати дисертації, виконано на належному науковому рівні з дотриманням академічної доброчесності.

3. Іосіфов Євген Анатолійович на високому рівні оволодів методологією наукової діяльності, набув теоретичних знань, відповідних умінь, навичок та компетентностей. Здобувач вільно володіє матеріалом.

4. Рекомендувати дисертацію Іосіфова Євгена Анатолійовича на тему «Методи та засоби забезпечення безпечного розпізнавання та параметризації результатів обробки голосової інформації» до публічного захисту у разовій спеціалізованій вченій раді для присудження Іосіфову Є.А. ступеня доктора філософії з галузі знань 12 Інформаційні технології за спеціальністю 125 Кібербезпека.

Головуючий –
кандидат технічних наук, доцент
завідуючий кафедри інформаційної
та кібернетичної безпеки
імені професора Володимира Бурячка
Київського столичного університету
імені Бориса Грінченка

Павло СКЛАДАННИЙ