

## **ВІДГУК**

офіційного опонента д.т.н., професора Рашкевича Ю. М.  
на дисертаційну роботу Ковтуна В'ячеслава Васильовича  
«Інформаційні технології для підвищення гарантоздатності інформаційних  
систем критичного застосування із автентифікацією суб'єкта за голосом»,  
що представлена на здобуття наукового ступеня доктора технічних наук за  
спеціальністю 05.13.06 – інформаційні технології

### **1. Актуальність теми дисертації**

Вплив інфосфери на розвиток сучасного суспільства безупинно зростає. Відповідно, забезпечення інформаційної безпеки стає одним з пріоритетів національної політики держави. Комплекс проблем, що узагальнюються терміном «гарантоздатність», а в вужчому контексті – «конфіденційність», в останній період часу визначається, перш за все, швидким поширенням нових інформаційних технологій, що є результатом проникнення комп’ютеризації в усі сфери людської діяльності. Їх функціональність спричиняє зростання залежності від інформаційних систем та сервісів і є базисом для появи нових видів загроз інтересам окремих громадян, підприємств, організацій, суспільства в цілому. Вразливість окремих осіб, установ і держави до загроз конфіденційності особливо зростає при використанні інформаційних мереж – як загального користування, так і корпоративних. Цьому сприяє також поширення тенденції до розподіленої обробки даних, пов’язаної з використанням дистанційного режиму і телекомунікаційних технологій (чому, нажаль, критично посприяла світова епідемія захворювання на COVID-2019). Також все більших масштабів приймають кримінальні напрямки комп’ютерної діяльності. У зв’язку з цим найважливішим завданням стає створення і застосування нових ефективних технологій забезпечення конфіденційності та узбереження інформаційних ресурсів.

Розвиток нових моделей, методів і засобів забезпечення конфіденційності покликаний, перш за все, запобігти загрозам доступу до інформаційних ресурсів особам, які такої привілеї не мають. Для вирішення цієї задачі необхідно визначити множину ідентифікаторів і створити спеціалізовану процедуру ідентифікації для всіх осіб-користувачів. Сучасні технології такої автентифікації будуються на різноманітних методах і засобах біометричної ідентифікації людини. Однією з найпоширеніших біометричних характеристик людини є голос, якому властивий ряд індивідуальних особливостей, які відносно легко вимірюти (це, наприклад, спектр мовленнєвого сигналу). До переваг процедури автентифікації за голосом можна також віднести її комфортність при повсякденному використанні і порівняно невисоку вартість набору необхідних апаратних засобів. Втім, існуючим методам автентифікації особи за голосом властивий і ряд серйозних недоліків. До них, перш за все, відноситься невисока роздільна здатність методів аналізу мовленнєвих сигналів і порівняно значний відсоток помилок як першого роду (помилковий недопуск особи, яка має право на доступ), так і найбільш небезпечних помилок другого роду (помилковий допуск до конфіденційної інформації осіб, які такого права

не мають). Особливо згадані недоліки посилюються коли процедура автентифікації відбувається в реальних акустичних умовах, коли на процес фонакції впливає широкий спектр збурюючих зовнішніх факторів.

Відзначимо, що істотне підвищення достовірності автентифікації досягається при вдалому поєднанні біометричних голосових методів верифікації зі спеціальними фізичними індивідуальними захисними засобами, наприклад, смарт-картами. Втім, незважаючи на емпірично доведену ефективність, теоретичного обґрунтування взаємозв'язку між оцінками конфіденційності і моделлю організації змішаного процесу автентифікації досі немає. Ця обставина підкреслює актуальність і необхідність досліджень, спрямованих на створення моделей, методів і технологій підвищення конфіденційності інформаційних систем за рахунок впровадження голосової автентифікації користувачів за умови науково обґрутованого опису впливу таких новацій на супутні показники гарантоздатності цільових інформаційних систем.

## **2. Мета і основні завдання дослідження**

Метою дисертаційної роботи є підвищення гарантоздатності інформаційної системи критичного застосування (ІСКЗ) з автентифікацією суб'єкта за голосом шляхом розроблення і реалізації методів і засобів для оптимізації такого класу систем за обраним атрибутом гарантоздатності. Для досягнення поставленої мети в дисертації сформульовано і вирішено наступні завдання:

- проаналізувати сучасний стан проблемно-орієнтованого моделювання інформаційних систем критичного застосування в таксономії гарантоздатності та оцінити вплив від застосування біометричних методів автентифікації суб'єктів-користувачів, зокрема, за голосом, на значення конфіденційності як атрибути гарантоздатності;
- узагальнити положення цифрового оброблення сигналів, математичної статистики і теорії фонакції в інформаційній технології автентифікації суб'єкта за індивідуальністю голосу;
- аналітично описати міру розрізнення між еталонним і емпіричним образами в параметричному просторі індивідуальності голосів;
- формалізувати процес компенсації шумів у фонограмі мовленнєвого сигналу в контексті задачі автентифікації суб'єкта за голосом;
- формалізувати і оптимізувати модель процесу класифікації в задачі автентифікації суб'єкта за мовленнєвим матеріалом із шумом на основі застосування технологій машинного навчання;
- створити концепцію забезпечення конфіденційності сеансу суб'єкт-системної інформаційної взаємодії з двофакторною авторизацією, зокрема, із верифікацією суб'єкта-користувача за голосом в якості другого фактору;
- формалізувати методи оптимізації інформаційної системи критичного застосування за обраним атрибутом гарантоздатності із постановкою відповідних задач математичного програмування;

### **3. Основні результати та наукова новизна дисертаційних досліджень**

Наукова новизна результатів, представлених в дисертаційній роботі, полягає в тому, що автором

*вперше запропоновано:*

- інформаційну технологію автентифікації суб'єкта за індивідуальністю голосу, відмінністю якої є те, що мовленнєвий сигнал представляється сумою модулювального і полігармонійного несного коливань в системі квазідетермінованих або стохастичних моделей індивідуальності голосу, що дозволяє отримати компактний, інформативний і адекватний параметричний опис індивідуальності сегментів з високим і помірним рівнем вокалізації в просторі усередненої частоти основного тону та амплітуди несних гармонік;

- метод оцінювання рівня відношення сигнал/шум у емпіричному мовленнєвому сигналі, в якому, на відміну від інших, мовленнєвий сигнал представляється сумою модулювального та полігармонійного несного коливань і білого шуму з використанням уточненої квазідетермінованої моделі індивідуальності голосу, що дозволяє визначати рівень шуму як у вокалізованих, так і у невокалізованих сегментах мовленнєвого сигналу;

- метод обчислення відстані між еталонним і емпіричним мовленнєвими сигналами, що параметризовані в системі моделей індивідуальності голосу, відмінністю якого є те, що для визначення довірчих інтервалів варіювання значень характеристичних параметрів враховується оцінка відношення сигнал/шум в емпіричному мовленнєвому сигналі, що дозволяє визначити поріг достовірної для верифікації суб'єкта за голосом;

- інформаційну технологію для оптимізації цільової інформаційної системи критичного застосування за обраним атрибутом гарантоздатності, яка, на відміну від інших, описується в системі марковських, напівмарковських і керованих напівмарковських моделей конфіденційності, цілісності, готовності, функційної безпечності, живучості та безвідмовності, що дозволяє віднайти оптимальний варіант ІСКЗ шляхом вирішення відповідної задачі математичного програмування;

- методи формалізації відношень «рівень конфіденційності – цілісність» та «рівень конфіденційності – готовність» для цільової ІСКЗ, в яких, на відміну від інших, для конкурючих атрибутів гарантоздатності заданих напівмарковськими моделями, здійснено постановку однокритеріальних задач оптимізації, що дозволяє визначити оптимальні параметри досліджуваної системи.

*удосконалено:*

- модель процесу автентифікації суб'єкта машиною опорних супер-та і-векторів за параметризованим представленням мовленнєвого сигналу з шумом, в якій, на відміну від існуючих, до представлених моделлю суміші гаусівських розподілів характеристичних параметрів емпіричного мовленнєвого сигналу застосовується мультиваріантний метод компенсування шумів, що дозволило підвищити конфіденційність процесу автентифікації, готовність цільової інформаційної системи і оптимізувати процес навчання імовірнісного класифікатора.

- метод адаптації згорткової нейромережі для автентифікації суб'єкта за мовленнєвим сигналом з шумом, в якому, на відміну від існуючих, вхідна спектrogramа параметризується з'єднаним з першим, згортковим, шаром нейромережі банком фільтрів Габора, синтезованим у формалізмі теорії спектрально-темпоральних рецептивних полів, що дозволяє орієнтувати процес інтерпретації вхідної спектrogramи нейромережею на вирішення задачі автентифікації суб'єкта за голосом та, за рахунок введення bottleneck-шару, отримати новий набір характеристичних параметрів для опису індивідуальності мовленнєвого сигналу з шумом.

#### **4. Ступінь обґрунтування наукових положень, висновків і рекомендацій, сформульованих у дисертації**

Теоретичні результати, представлені в дисертаційній роботі, автор отримав із застосуванням загальновизнаних методів, заснованих на комплексному використанні теорії математичного моделювання, аналітичних і обчислювальних методах теорії імовірності і математичної статистики, методах теорії випадкових процесів, методах математичного аналізу, методах теорії розпізнавання образів, методах теорії фонакції, методах цифрової обробки сигналів, методах теорії надійності, методах теорії інформаційної безпеки, методах математичного програмування, методах теорії прийняття рішень, методах машинного навчання, методах планування експерименту тощо.

Всі теоретичні положення дисертаційної роботи достатньо обґрунтовані. Достовірність результатів досліджень забезпечується коректністю та строгістю постановки завдань, коректністю використання математичного апарату під час доведення основних наукових положень. Достовірність наукових результатів підтверджується збігом даних, які отримано за допомогою запропонованих методів та моделей, з експериментальними даними.

Матеріали дисертаційної роботи обговорювалися на численних міжнародних наукових конференціях і семінарах. Позитивні результати апробації і акти впровадження додатково підтверджують достовірність теоретичних положень. Дисертаційна робота містить висунуті автором науково обґрунтовані теоретичні та експериментальні результати, наукові положення, які характеризується єдністю змісту і підтверджують значний особистий внесок здобувача.

Практичне значення отриманих результатів узагальнено у вигляді:

- концепції двофакторної автентифікації суб'єкта-користувача із верифікацією за індивідуальними особливостями його голосу в якості другого фактору;
- методик і алгоритмів для параметризації мовленнєвих сигналів, зокрема, з шумом, у формалізмі моделей індивідуальності голосу;
- методики прийняття рішень в задачі класифікації суб'єкта за параметризованим мовленнєвим сигналом з шумом із застосуванням імовірнісних класифікаторів, штучних нейромереж, методу найкращих оцінок тощо;

- методики регуляризації глибоких нейромереж і бустінгу процесу їх навчання з орієнтацією на застосування в задачі автентифікації суб’єкта за голосом;
- методики формування політики безпеки програмної складової інформаційної системи критичного застосування;
- методики і алгоритму для оптимізації обраного атрибуту гарантоздатності цільової ICK3;
- методики оптимізації залежності конфіденційності процесу автентифікації і готовності інформаційній системі критичного застосування.

Результати роботи впроваджені у: Innovative Institute for Material Studies of Intel Research Practice (USA); відділі розпізнавання та синтезу звукових образів Міжнародного науково-навчального центру інформаційних технологій та систем НАН України та МОН України (м. Київ); ARS Online OÜ (a part of the Advertising Agencies Industry, Estonia); Polski Dom Nowych Mediów (Poland); хмельницькому міському комунальному підприємству «Хмельницькінфоцентр» (м. Хмельницький); львівському комунальному підприємству «Міський центр інформаційних технологій» (м. Львів); департаменті інформаційних технологій Вінницької міської ради (м. Вінниця); КНП ДОЗ Він. МР «Центр первинної медико-санітарної допомоги №3» (м. Вінниця); ДОЗК Він. ОДА МОЗ України «Вінницький обласний центр медико-соціальної експертизи» (м. Вінниця); КП «Вінницький інформаційний центр» (м. Вінниця), ТОВ «Вінницяелектроконтакт» (м. Вінниця), ТОВ «Агро-промсервіс» (м. Немирів).

## **5. Повнота відображення в публікаціях**

За результатами виконаних теоретичних і експериментальних досліджень опубліковано 32 наукові роботи – зокрема 1 монографія та 31 стаття, з яких: 11 статей у виданнях, проіндексованих у міжнародних наукометричних базах, зокрема, 8 статей у Scopus та 3 статті у Web of Science; 25 статей опубліковано у наукових фахових виданнях України, що входять до переліку, затвердженого МОНУ. Автор чітко сформулював особистий внесок в статтях, опублікованих із співавторами.

## **6. Структура та обсяг дисертації**

Дисертаційна робота включає, зокрема, з вступ, шість розділів, висновки, список використаних джерел та одинадцять додатків. Загальний обсяг роботи становить 566 сторінок, із них обсяг основного тексту – 386 сторінок, 82 рисунки, 6 таблиць, список використаних джерел включає 352 найменування та займає 29 сторінок, одинадцять додатків займають 180 сторінок.

## **7. Оцінка змісту дисертації**

У вступі обґрутовано актуальність обраної теми дисертації, сформульовано мету, основні задачі досліджень і наукову новизну отриманих результатів. Розглянуто практичне значення, реалізацію й впровадження результатів дисертації. Визначено зв’язок роботи з науковими програмами, планами організацій, де виконувалася робота, також особистий внесок автора в

роботах, які виконані в співавторстві. Наведено відомості про публікації і апробацію роботи.

В **першому** розділі наведені результати аналізу теоретичної забезпеченості процесу оцінювання гарантоздатності інформаційної системи критичного застосування із автентифікацією суб'єкта за голосом як комплексного явища. Здійснено огляд теоретичних розробок з оцінювання гарантоздатності інформаційних систем. Представлено описову таксономію та проаналізовано структуру інформаційної системи критичного застосування як підкласу інформаційних систем, призначених для забезпечення інформаційної підтримки критичних систем. Проведено огляд технологій підвищення конфіденційності інформаційних систем методами біометричної автентифікації, зокрема за голосом. В результаті проведеного аналізу вибрано напряму і мету та здійснено постановку завдань дослідження.

У **другому** розділі пропонуються моделі індивідуальності голосу в мовленнєвому сигналі для розв'язання задачі автентифікації суб'єкта за голосом. Формалізовано базову й уточнену квазідетерміновані моделі індивідуальності голосу в мовленнєвому сигналі. Пропонуються стохастичні інтерпретації створених квазідетермінованих моделей. Описуються ефективні методи представлення характеристичних параметрів створених моделей індивідуальності голосу у часовому і частотному вимірах у контексті вирішуваної задачі. Формалізується бікомпонентна модель класифікації фрагментів мовленнєвих сигналів відповідно до їх інформативності для автентифікації суб'єкта за голосом.

В **третьому** розділі систематизується процес встановлення адекватності емпіричних мовленнєвих сигналів і їх опис математичними моделями, представленими у другому розділі, в контексті задачі автентифікації суб'єкта за голосом. Представлено методику верифікації математичних моделей індивідуальності голосу за значенням обраного критерію. Формалізовано процес оцінювання порогу прийняття рішень в задачі автентифікації суб'єкта за голосом відповідно до рівня відношення «сигнал»/«шум» у аналізованому мовленнєвому сигналі. Здійснено емпіричну верифікацію і аналіз отриманих теоретичних результатів моделювання індивідуальності голосу в мовленнєвому сигналі.

В **четвертому** розділі оцінюється вплив шумів акустичного оточення приймачів мовленнєвого сигналу на конфіденційність процесу автентифікації суб'єкта за голосом. Запропоновано моделі компенсування шумів у мовленнєвих сигналах, які стали основою для синтезу імовірнісних моделей процесу автентифікації суб'єкта за мовленнєвим матеріалом із шумом, практичним наслідком яких стало удосконалення відповідних методів прийняття рішень. Враховуючи значну ресурсовитратність процесу класифікації як неодмінної складової процесу автентифікації суб'єкта за голосом, проведено дослідження з оптимізації методів прийняття рішень щодо особи суб'єкта, зокрема методами машинного навчання.

В **п'ятому** розділі відображені структурні і функціональні особливості інформаційної системи критичного застосування із автентифікацією суб'єкта за

голосом. Показано, що адекватні моделі гарантоздатності можна вважати інтегральною характеристикою, яка забезпечує формальну оцінку конфіденційності, готовності, цілісності, безвідмовності, обслуговуваності, інтенсивності відмов і напрацювань на відмову інформаційних систем критичного застосування. В отриманих моделях атрибути гарантоздатності враховано архітектурні особливості інформаційного середовища цільової системи, важливість її інформаційних ресурсів, специфіку процесу автентифікації та формування системної політики безпеки тощо. Зважаючи на конкуруючу сутність атрибутів конфіденційність-готовність та цілісність-готовність, представлено відповідні моделі взаємозалежності цих інтегральних складових гарантоздатності із утворенням відповідних критеріїв.

В шостому розділі представлено аналітичні методи обчислення характеристичних параметрів моделей індивідуальності голосу для досліджуваних екземплярів мовленнєвих сигналів. Отримано адаптації цих методів залежно від того, відомі значення усталених параметрів моделей індивідуальності голосу для досліджуваного екземпляру мовленневого сигналу, чи ні. Формалізовано інформаційну технологію автентифікації суб'єкта за індивідуальністю голосу та узагальнений метод і інформаційну технологію для оптимізації обраного атрибуту гарантоздатності цільової інформаційної системи критичного застосування.

Дисертаційна робота написана технічно грамотною мовою, автор логічно викладає основні положення, із дотриманням наукового стилю і вимог до оформлення. Зміст дисертаційної роботи відповідає прийнятим вимогам та правилам проведення та оформлення результатів наукових досліджень. Сформульовані у дисертаційній роботі завдання дослідження розв'язані, внаслідок чого отримані нові наукові та практичні результати. Усі одержані наукові результати висвітлені в тексті дисертації. Автореферат в достатньо повній мірі відображає основний зміст дисертації. Застосована у дисертаційній роботі наукова термінологія є загальновизнаною, стиль викладення результатів теоретичних і практичних досліджень, нових наукових положень, висновків і рекомендацій забезпечує доступність їх сприйняття.

## 8. Зауваження до дисертації

1. Недоліком першого розділу дисертаційної роботи є брак саме аналізу і узагальнення, що ускладнює простеження взаємозв'язку між вмістом розділу і сформульованою в його кінці постановкою завдань дослідження.

2. У роботі автор не наводить обмеження до застосування розроблених моделей індивідуальності голосу в мовленнєвому сигналі та створених на їх основі окремих методів та інформаційної технології автентифікації суб'єкта за індивідуальністю голосу в цілому, особливо це стосується їх застосування в умовах реального акустичного середовища.

3. Автором запропоновано метод оцінювання рівня відношення сигнал/шум в мовленому сигналі, який представляється сумою модулювального та полігармонійного несного коливань і білого шуму в просторі моделей індивідуальності голосу. Проте шуми акустичного оточення мовця не завжди

мають випадковий характер, що характерно, наприклад, для багатьох техногенних джерел шуму. За таких умов допустимість використання в запропонованому автором методі моделі білого шуму потребує додаткового обґрунтування.

4. Наведені в підрозділі 4.2 моделі і методи машинного навчання, адаптовані автором до процесу класифікації в задачі автентифікації суб'єкта за мовленнєвим сигналом із шумом описані недостатньо. Наприклад, при описі архітектури згорткової нейромережі взагалі не згадано про шар активації.

5. З огляду на відсутність в тексті роботи чіткого визначення специфіки класу інформаційних систем критичного застосування, додаткового обґрунтування вимагає вичерпність та несуперечність параметричного простору атрибутів гарантоздатності, представлена на рис. 6.18.

6. Недоліком роботи можна вважати незбалансованість обсягу її розділів (наприклад, розділ 5 удвічі більший за обсягом від кожного із розділів 2 та 3), що призвело до перевищення обсягу основної частини дисертаційної роботи у порівнянні із рекомендованим.

Визначені недоліки не знижують цінність одержаних автором наукових та прикладних результатів дисертаційної роботи.

## 9. Узагальнена оцінка дисертаційної роботи

Дисертаційна робота Ковтуна В'ячеслава Васильовича «Інформаційні технології для підвищення гарантоздатності інформаційних систем критичного застосування із автентифікацією суб'єкта за голосом» є цілісним, завершеним науковим дослідженням, спрямованим на вирішення важливої наукової проблеми підвищення гарантоздатності інформаційної системи критичного застосування із автентифікацією суб'єкта за голосом. Вміст дисертаційної роботи відповідає напрямкам досліджень, викладеним у паспорті спеціальності 05.13.06 - інформаційні технології.

Вважаю, що за актуальністю обраної теми, достовірністю і обґрунтованістю висновків, новизною досліджень, значимістю отриманих результатів для науки і практики дисертаційна робота повністю відповідає п.п. 9, 10, 12 «Порядку присудження наукових ступенів», що затверджено постановою Кабінету Міністрів України № 567 від 24.07.2013 р., щодо докторських дисертацій, а здобувач, Ковтун В'ячеслав Васильович, заслуговує присудження наукового ступеня доктора технічних наук за спеціальністю 05.13.06 - інформаційні технології.

Офіційний опонент,  
член Національного  
агентства кваліфікацій,  
доктор технічних наук, професор

Ю. М. Рашкевич

Григорій Рашкевич Ю.М.

