Міністерство освіти і науки України
Вінницький національний технічний університет

КОВТУН В'ЯЧЕСЛАВ ВАСИЛЬОВИЧ

УДК 681.327.12

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ДЛЯ ПІДВИЩЕННЯ ГАРАНТОЗДАТНОСТІ ІНФОРМАЦІЙНИХ СИСТЕМ КРИТИЧНОГО ЗАСТОСУВАННЯ ІЗ АВТЕНТИФІКАЦІЄЮ СУБ'ЄКТА ЗА ГОЛОСОМ

05.13.06 – інформаційні технології

АВТОРЕФЕРАТ
дисертації на здобуття наукового ступеня
доктора технічних наук

Вінниця – 2021

Дисертацією є кваліфікаційна наукова праця на правах рукопису.

Робота виконана у Вінницькому національному технічному університеті Міністерства освіти і науки України.

Науковий консультант доктор технічних наук, професор
Бісікало Олег Володимирович,
Вінницький національний технічний університет,
декан факультету комп'ютерних систем і автоматики.

Офіційні опоненти: доктор технічних наук, професор
Зайченко Юрій Петрович,
Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», професор кафедри математичних методів системного аналізу;

доктор технічних наук, професор
Рашкевич Юрій Михайлович,
Національне агентство кваліфікацій, член агентства;

доктор технічних наук, професор
Харченко В'ячеслав Сергійович,
Національний аерокосмічний університет ім. М. Є. Жуковського «Харківський авіаційний інститут», завідувач кафедри комп'ютерних систем, мереж і кібербезпеки.

Захист відбудеться «08» квітня 2021 р. о 15.00 годині на засіданні спеціалізованої вченої ради Д 05.052.01 у Вінницькому національному технічному університеті за адресою: 21021, м. Вінниця, Хмельницьке шосе, 95, ГНК, ауд. 210.

З дисертацією можна ознайомитись у бібліотеці Вінницького національного технічного університету за адресою: 21021, м. Вінниця, Хмельницьке шосе, 95, ГНК.

Автореферат розісланий «04» березня 2021 р.

Вчений секретар
спеціалізованої вченої ради С. М. Захарченко

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Обґрунтування вибору теми досліджень. Інтеграція інформаційних систем у всі сегменти сучасного суспільства є звершеним фактом. Властивостями споживати, виробляти, накопичувати і узагальнювати інформацію зараз наділені не тільки складні комп'ютерні системи, а й звичайні побутові речі. Втім, найбільш важливе значення має об'єкт, у який інтегрується інформаційна система. Серед існуючих класів автоматизованих систем окреме місце займають так звані критичні системи [1]–[10], які функціонують із високою надійністю та безпекою, зберігаючи прогнозований рівень цих комплексних характеристик під час експлуатації за рахунок закладених на етапі проектування механізмів протидії впливу визначених класів негативних факторів. Якщо із критичною системою трапляється надзвичайна ситуація, це може завдати значних матеріальних, репутаційних, а головне, людських втрат. Зв'язок критичних систем із інформаційним простором забезпечують спеціальні комплекси програмних засобів, відомі як інформаційні системи критичного застосування (ІСКЗ). Основною характеристикою такого класу інформаційних систем можна вважати прогнозованість процесу функціонування в умовах впливу як відомих, так і не відомих негативних факторів. Втім, прогнозованість не є достатньо наукомістким терміном. У актуальних вітчизняних і закордонних наукових роботах [11]–[28] авторства таких вчених як Лапріє Дж.-С. (Laprie J.-C.), Авізеніс А. (Avizienis A.), Ренделл Б. (Randell B.), Романовський О. (Romanovsky A.), Найт Дж. (Knight J.), Аль-Кувейті М. (Al-Kuwaiti M.), Харченко В., Замойський В. (Zamojski W.), Нікол Д. (Nicol D.), Дуган Дж. (Dugan J.), Арлат Ж. (Arlat J.), Теслер Г., Федухин А., Ігнатов В., Шубінський І., Царев Р., Махаржан С. (Maharjan S.), Захді Ф. (Zahedi F.), Долініна О., Лунго Дж. (Lungo J.), Літтлвуд Б. (Littlewood B.) і нормативних документах [29] IEC61508, ITU E800, IEEE 982.1, IEEE 1332, IEEE 1413, IEEE 1624, IEEE 1633, ECSS-Q-80-3, ECSS-Q-30A, IAEA NS-G-1.3 залежно від галузі, якій належить критична система, вводиться відповідна таксономія якісних показників функціонування цільових систем із введенням, зокрема, метрик для оцінювання інформаційних системних компонентів. Все частіше при цьому вживається термін «гарантоздатність» (англ. dependability). Однак, в роботах, що існують, не розглядаються в комплексі усі принципи підвищення гарантоздатності інформаційних систем критичного застосування, зокрема для найважливіших атрибутів – конфіденційності, цілісності, готовності, функційної безпечності, живучості, безвідмовності. Не запропоновано єдиного системного підходу для оцінки цих атрибутів гарантоздатності, що є необхідною умовою функціонування інформаційних систем критичного застосування як класу.

Таким чином, для вирішення актуальної ***науково-прикладної проблеми*** забезпечення гарантоздатності інформаційних систем критичного застосування необхідно розв'язати об'єктивне протиріччя між:

– існуванням розподілених структурованих інформаційних систем критичного застосування, ключовою ознакою яких є прогнозованість поведінки при експлуатації;

– наявністю технологій, що забезпечують взаємодію між множинами суб'єктів-користувачів, системних сервісів та інформаційних ресурсів, але не

гарантують повноцінного функціонування ІСКЗ в умовах впливу негативних факторів;

– зростаючими вимогами до рівня конфіденційності, цілісності та готовності ІСКЗ, з одного боку, і неможливістю одночасного їх забезпечення з причини об'єктивного обмеження системних обчислювальних ресурсів та існування у зловмисників напрацьованих технологій нейтралізації стандартних методів автентифікації суб'єктів-користувачів, з іншого боку.

Зв'язок роботи з науковими програмами, планами, темами. Представлені у дисертаційній роботі теоретичні і прикладні результати отримано автором у рамках кафедральної науково-дослідної роботи №46К4 «Методи моделювання та оптимізації складних систем на основі інтелектуальних технологій» на кафедрі комп'ютерних систем управління Вінницького національного технічного університету. Апробація представлених в дисертаційній роботі результатів відбувалася, зокрема, під час участі автора в міжнародному науково-методичному проекті «Establishing Modern Master-level Studies in Information Systems» (реєстраційний номер 561592-EPP-1-2015-1- FR-EPPKA2-CBHE-JP, фінансування ЄС). Тематика роботи дозволяє реалізувати прийняті у Законі України №2469-VIII від 21.06.2018 «Про основні засади забезпечення кібербезпеки України» та конкретизовані у Постанові Кабінету міністрів України № 518 від 19 червня 2019 р. «Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури» принципи, напрями та заходи впровадження і розбудови державної системи захисту критичної інфраструктури держави. Завдання дослідження, розв'язані у дисертаційній роботі, відповідають змісту проекту Закону України «Про критичну інфраструктуру та її захист», оприлюдненому 16.06.2020 р. на офіційному сайті Міністерства розвитку економіки, торгівлі та сільського господарства України.

Мета і завдання дослідження. **Мета** дисертаційної роботи полягає у підвищенні гарантоздатності інформаційної системи критичного застосування з автентифікацією суб'єкта за голосом шляхом розроблення і реалізації методів і засобів для оптимізації такого класу систем за обраним атрибутом гарантоздатності, а саме, конфіденційністю, цілісністю, готовністю, функційною безпечністю, живучістю, безвідмовністю.

Для досягнення поставленої мети в дисертаційній роботі необхідно виконати такі науково-технічні **завдання**:

– проаналізувати сучасний стан проблемно-орієнтованого моделювання інформаційних систем критичного застосування як виділеного підкласу інформаційних систем; дослідити вразливості інформаційних систем критичного застосування як комплексного явища в таксономії гарантоздатності; оцінити вплив від застосування біометричних методів автентифікації суб'єктів-користувачів, зокрема, за голосом, на значення конфіденційності як атрибуту гарантоздатності;

– узагальнити положення цифрового оброблення сигналів, математичної статистики і теорії фонації в інформаційній технології автентифікації суб'єкта за індивідуальністю голосу, заснованої на аналітичних квазідетермінованих, стохастичних, комплексних моделях опису індивідуальності голосу у

мовленнєвому сигналі із можливістю динамічного оцінювання рівня відношення «сигнал/шум» в останньому;

– аналітично описати міру розрізнення між еталонним і емпіричним образами в параметричному просторі індивідуальності голосів для попереднього оцінювання значення порогу прийняття рішень відповідно до рівня відношення «сигнал»/«шум» у емпіричному мовленнєвому сигналі;

– формалізувати процес компенсації шумів у фонограмі мовленнєвого сигналу в контексті задачі автентифікації суб'єкта за голосом і орієнтацією на застосування в імовірнісних моделях процесу автентифікації суб'єкта за мовленнєвим матеріалом із шумом, описаним сумішшю гаусівських розподілів;

– 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 двохфакторною авторизацією, зокрема, із верифікацією суб'єкта-користувача за голосом в якості другого фактору;

– створити модель політики безпеки програмної складової інформаційної системи критичного застосування із можливістю оптимізації цільової системи у метриці готовність-цілісність як відповідної задачі математичного програмування;

– формалізувати методи оптимізації інформаційної системи критичного застосування за значенням індикаторів функційної безпечності та живучості із постановкою відповідних задач математичного програмування;

– створити комплекс моделей оцінювання безвідмовності для довільного екземпляру класу інформаційних систем критичного застосування, модельованого керованим напівмарковським процесом.

– у формалізмі створених моделей конфіденційності, цілісності, готовності, функційної безпечності, живучості та безвідмовності інформаційної системи критичного застосування сформулювати методику підвищення значення обраного з цих атрибутів гарантоздатності, як основний елемент профільної інформаційної технології.

Об'єктом дослідження є процеси забезпечення гарантоздатності інформаційної системи критичного застосування.

Предметом дослідження є моделі, методи і засоби інформаційних технологій для підвищення гарантоздатності інформаційної системи критичного застосування із автентифікацією суб'єкта за голосом.

Методи дослідження. Для виконання поставлених у роботі завдань було використано: методи математичного моделювання; аналітичні і обчислювальні методи теорії імовірності і математичної статистики; методи теорії випадкових процесів; методи математичного аналізу; методи теорії розпізнавання образів; методи теорії фонації; методи цифрового оброблювання сигналів; методи теорії надійності; методи теорії інформаційної безпеки; методи математичного програмування; методи теорії прийняття рішень; методи машинного навчання; методи планування експерименту.

Наукова новизна отриманих результатів полягає в тім, що:

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 частота основного тону та амплітуди несних гармонік.

– запропоновано 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.

– запропоновано метод обчислення відстані між еталонним і емпіричним мовленнєвими сигналами, що параметризовані в системи 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.

– запропоновано 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.

– запропоновано методи формалізації відношень «рівень конфіденційності – цілісність» та «рівень конфіденційності – готовність» для цільової ІСКЗ, в яких, на відміну від інших, для конкуруючих 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 сумішей 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 спектрограма 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 спектрограми 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.

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 ІСКЗ;

– 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 підприємстві «Хмельницькінфоцентр» (м. Хмельницький); львівському комунальному підприємстві «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).

Публікації. За результатами виконаних теоретичних і експериментальних досліджень опубліковано 32 наукові роботи – зокрема, 1 монографія [60] та 31 стаття, з яких: 11 статей у виданнях, проіндексованих у міжнародних наукометричних базах даних (МНМБД), у т.ч. 8 статей [43], [48], [49], [57], [59], [82]–[84] у МНМБД Scopus та 3 статті [45, 51, 54] у МНМБД Web of Science; 25 статей опубліковано у наукових фахових виданнях України, що входять до переліку, затвердженого МОНУ [30]–[42], [44]–[47], [50]–[56], [58]. З наведеного

списку 8 наукових праць [43], [48]–[51], [54], [57], [59], [82] опубліковані англійською мовою.

Особистий внесок здобувача. Всі результати дисертаційної роботи, які винесені на захист, отримані автором самостійно. У наукових працях, опублікованих не одноосібно авторові дисертаційної роботи належать: [1] – метод виділення складових сегментів у мовленнєвому сигналі; [2] – модель і метод оцінювання впливу завад на достовірність роботи інформаційно-вимірювальної системи розпізнавання голосу; [3] – метод виділення основного тону на основі модифікованої математичної моделі слухової системи людини; [4] – метод оцінювання метрологічних характеристик інформаційно-вимірювальної системи автоматизованого розпізнавання голосів; [5] – узагальнення стану проблеми розробки ефективних систем пошуку ключових слів; [6] – метод пошуку ключових слів у мовленнєвому сигналі; [7] – модель і метод оцінювання надійності автоматизованих систем розпізнавання мовців критичного застосування; [8] – модель і метод узагальнення інформації множини мікрофонів у автоматизованій системі розпізнавання мовця критичного застосування; [9] – метод синтезу і навчання комітету нейромереж у автоматизованій системі розпізнавання мовців критичного застосування; [10] – метод оптимізації алфавіту інформативних ознак для автоматизованої системи розпізнавання мовців критичного застосування; [11] – метод представлення ознак у автоматизованій системі розпізнавання мовця критичного застосування; [12] – методика дослідження ефективності ознак розпізнавання мовців при використанні згорткових нейромережі і її прикладна реалізація; [13] – метод детектування мовленнєвої активності в автоматизованій системі розпізнавання мовця критичного застосування; [14] – модель нейромережевого класифікатора для модуля розпізнавання мовця у складі автоматизованої системи критичного застосування; [15] – метод підвищення шумостійкості автоматизованої системи розпізнавання мовця критичного застосування; [16] – метод оптимального синтезу нейромережевого класифікатора з врахуванням положень теорії спектрально-темпоральних рецептивних полів для застосування в автоматизованій системі розпізнавання мовця критичного застосування; [17] – метод підвищення інформативності основного тону для розпізнаванні мовців згортковими нейромережами; [19] – алгоритм і постановка експерименту з прикладного моделювання рангових конфігурацій; [20] – базова модель автоматизованої системи розпізнавання мовця критичного застосування; [22] – метод застосування СТРП-ознак в задачі автентифікації мовця; [23] – метод оцінювання надійності сеансу розпізнавання особи автоматизованою системою розпізнавання мовця критичного застосування; [24] – метод адаптації PLDA для прийняття рішень у автоматизованій системі розпізнавання мовця критичного застосування із нейромережевим класифікатором; [25] – модель оцінювання цілісності інформаційної системи критичного застосування і метод синтезу оптимальної системної політики безпеки; [28] – модель компенсування шумів у фонограмі мовленнєвого сигналу; [30] – модель готовності інформаційної системи критичного застосування і метод її прикладного застосування; [32] – модель безвідмовності інформаційної системи критичного застосування і метод її

прикладного застосування; [33] – метод оптимізації безвідмовності інформаційної системи критичного застосування; [34] – моделі функційної безпечності та живучості інформаційної системи критичного застосування і методи їх прикладного застосування.

Апробація матеріалів дисертації. Основні положення дисертації були оприлюднені і обговорені на: XXXIX–XLIX Науково-технічних конференціях підрозділів Вінницького національного технічного університету НТКП ВНТУ (2010–2020 рр., Вінниця); II, III, IV Міжнародних наукових конференціях Вимірювання, контроль та діагностика в технічних системах (ВКДТС) (2015 р., 2017 р., Вінниця); XI–XIV Міжнародних конференціях Контроль і управління в складних системах (КУСС) (2010 р., 2012 р., 2014 р., 2016 р., 2018 р., Вінниця); IV–VIII Міжнародних конференціях з оптико-електронних інформаційних технологій Фотоніка-ODS (2012 р., 2014 р., 2016 р., 2018 р., Вінниця); 9th International Conference on Advanced Computer Information Technology (ACIT) (2019 р., Чехія), 10th International Conference on Advanced Computer Information Technology (ACIT) (2020 р., Германія), 11th International Conference on Dependable Systems, Services and Technologies (DESSERT) (2020 р., Київ), 1st International Workshop on Intelligent Information Technologies & Systems of Information Security (IntelITSIS 2020) (2020 р., Хмельницький), Problems of Infocommunications. Science and Technology (PIC S&T′2020) (2020 р., Харків).

Структура та обсяг дисертації. Дисертація складається, зокрема, з вступу, шести розділів, висновків, списку використаних джерел та одинадцяти 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, 10 додатків займають 180 сторінок.

ОСНОВНИЙ ЗМІСТ РОБОТИ

У **вступі** обґрунтовано актуальність теми дисертації, визначено науково-прикладну проблему, що потребує розв’язання, показано зв’язок роботи з науковими програмами, планами, темами. Сформульовано мету і основні задачі досліджень, визначено наукову новизну та практичну цінність одержаних результатів. Наведено дані про особистий внесок здобувача, апробацію результатів, основні праці, опубліковані за темою дисертації.

В **першому розділі** наведені результати аналізу теоретичної забезпеченості процесу оцінювання гарантоздатності ІСКЗ із автентифікацією суб’єкта за голосом як комплексного явища. Здійснено огляд теоретичних розробок з оцінювання гарантоздатності інформаційних систем. Представлено описову таксономію та проаналізовано структуру ІСКЗ як підкласу інформаційних систем, призначених для забезпечення інформаційної підтримки критичних систем. Проведено огляд технологій підвищення конфіденційності інформаційних систем методами біометричної автентифікації, зокрема за голосом.

Гарантоздатність є комплексною експлуатаційною характеристикою інформаційно-управляючих систем, коректність реалізації сервісів яких визначається взаємозв’язаною множиною показників-атрибутів. При цьому надійність характеризується безвідмовністю, функційною безпечністю і

живучістю, а інформаційна безпека – конфіденційністю, готовністю і цілісністю. Як наочно продемонстровано на рис. 1, еволюція інформаційно-управляючих систем є мотивуючим фактором для розвитку теоретичного апарату гарантоздатності.

Визначення гарантоздатності як властивості інформаційних систем надавати сервіси, яким можна виправдано довіряти, є особливо актуальним, якщо досліджувана інформаційно-управляюча система є складовою критичної системи. У складі таких інформаційних систем критичного застосування виділяють, зокрема, інформаційні ресурси, інформаційне середовище, систему інформаційної безпеки та керовані нею підсистеми захисту від несанкціонованого доступу та розмежування доступу тощо. Реалізація сервісів відбувається у виділених інформаційних процесах із інтегрованим контролем цілісності та конфіденційності. Узагальнену структурну схему ІСКЗ представлено на рис. 2. Запропонована структуризація ІСКЗ органічно розкриває націлений на обробку інформації прикладний рівень моделі OSI. Проведена аналогія корисна тим, що у моделі OSI система утворюється відкритою ієрархічно організованою композицією автономних логічних об’єктів-вузлів. Ієрархічно-блочне представлення інформаційної системи дозволяє аналітично описати локальну та глобальну політики безпеки. Правила локальної політики визначають допустимі переходи між станами логічних вузлів у складі системи, а правила глобального політики регламентують послідовність переходів для реалізації відповідних персоніфікованих сервісів.

+ ОПТИМІЗАЦІЯ (ПАРЕТО-ОПТИМІЗАЦІЯ) ЗА ОБРАНИМ АТРИБУТОМ ГАРАНТОЗДАТНОСТІ						**Синтез гарантоздатних ІУ інфраструктур в умовах конкуренції за ресурси**
+ КОНФІДЕНЦІЙНСТЬ, ЦІЛІСНІСТЬ					**Синтез гарантоздатних ІУС із негарантозданих компонентів**	
+ ФУНКЦІОНАЛЬНА БЕЗПЕКА				**Синтез функціонально-безпечних ІУС із низько конфіденційних апаратних і програмних локальних та мережевих компонентів**		
+ ГОТОВНІСТЬ			**Синтез комп. систем заданої готовності з ненадійних апаратних і програмних компонентів**			
+ ЖИВУЧІСТЬ		**Синтез живучих цифрових систем із ненадійних інтегральних компонентів**				
БЕЗВІДМОВНІСТЬ	**Синтез безвідмовних пристроїв із ненадійних компонентів**					
Системи	***Аналого-цифрові системи***	***Цифрові обчисл. системи***	***Комп’ютери і комп. системи***	***ІУС і мережі***	***Розподілені і web-системи***	***ІТ-інфраструктури***
Елементи	***Транзистори***	***Інтегральні схеми***	***Великі інт. і схеми і програмні додатки***	***Сервера, мережеві компоненти***	***Кластери і web-сервіси***	***Кіберфізичний простір Індустрії 4.0***
Визначні системні вади	***Обмежена безвідмовність***		***Прогр., апаратні та комплексні відмови***	***Фізична та інформаційна вразливість***	***Інформаційна вразливість***	***Слабка зв’язність***

Рисунок 1 – Еволюція інформаційно-управляючих систем в таксономії гарантоздатності.

Рисунок 1 є авторською адаптацією запропонованої науковою школою проф. Харченка В. С. концепції еволюції гарантоздатних систем у її прикладному застосуванні щодо інформаційно-управляючих систем з акцентуванням уваги на розвитку інформаційної складової.

Рисунок 2 – Узагальнена структурна схема інформаційної системи критичного застосування.

Варіативність захисних механізмів ІСКЗ забезпечується дотриманням раціонального балансу між значенням атрибутів конфіденційності та готовності в умовах обмеження обчислювальних ресурсів. При цьому застосування для автентифікації суб'єктів-користувачів традиційної схеми «логін-пароль» не виключає її принципового недоліку який полягає у відокремленості особи, що авторизується, від ключа, який використовується для підтвердження її автентичності. Цей недолік відсутній в схемах автентифікації суб'єкта за його індивідуальними біометричними параметрами, що і зумовлює зростання їх популярності. За виглядом результату прийнятого рішення системи автентифікації суб'єкта за голосом розділяють на системи верифікації та ідентифікації. Система верифікації суб'єкта за голосом розраховує оцінку ідентичності як міру близькості моделі фонограми суб'єкта, який авторизується, із відповідною еталонною моделлю голосу, зареєстрованою у системі. Якщо значення оцінки ідентичності перевищує поріг, то суб'єкт отримує доступ. Достовірність таких систем можна оцінити за емпіричними визначеними значеннями похибок першого та другого роду, а варіювати співвідношенням цих значень можна змінюючи поріг прийняття рішень. Відмінністю системи ідентифікації суб'єкта за голосом від системи верифікації того ж призначення полягає в тім, що наперед не відомо з якою еталонною моделлю голосу порівнювати модель емпіричної фонограми. Відповідно, порівняння здійснюється

попарно із всіма еталонними моделями голосів, а отриманий вектор оцінок ідентичності порівнюється з порогом і узагальнюється розв’язувальним правилом.

Відома акустична модель фонації виділяє у складі артикуляційного апарату людини такі елементи як мовленнєве джерело, акустичний фільтр і модулятор. При моделюванні акустичного фільтра використовують два підходи. Перший описує індивідуальні характеристики мовленнєвого сигналу системою диференціальних рівнянь високих порядків, а другий розглядає процес фонації як продукт взаємодії передатної функції і генератора імпульсів. Передатна функція описує чотири формантні області і дозволяє розрахувати формантні характеристичні параметри. Генератор імпульсів описує роботу мовленнєвого джерела і дозволяє розрахувати характеристичні параметри основного тону. Перетворення Фур’є і лінійне передбачення параметризують мовленнєвий сигнал множиною основних спектральних компонентів, кепстральних параметрів і коефіцієнтів лінійного передбачення. Вживають і складніші методи узагальнення на основі прихованих марковських моделей, динамічного програмування, машинного навчання тощо. Втім, універсального набору характеристичних параметрів в задачі автентифікації суб’єкта за голосом досі немає.

На основі проведеного аналізу здійснено постановку проблеми, сформульовано мету та задачі досліджень.

У **другому розділі** пропонуються моделі індивідуальності голосу в мовленнєвому сигналі, створені з орієнтацією на розв’язання задачі автентифікації суб’єкта за голосом. Формалізовано базову й уточнену детерміновані моделі індивідуальності голосу в мовленнєвому сигналі. Пропонуються стохастичні інтерпретації синтезованих детермінованих моделей. Описуються ефективні методи представлення характеристичних параметрів моделей індивідуальності голосу в мовленнєвому сигналі у часовому і частотному вимірах. Представлений аналітичний опис рівня відношення «сигнал»/«шум» у формалізмі моделей індивідуальності голосу.

З теорії зв'язку відомо, що передача повідомлень здійснюється структурою у складі джерела інформації, модуляторів і переносників інформації. У цьому контексті передавач в мовній системі зв'язку можна описати представленою на слайді схемою. У мовній системі зв'язку використовуються щонайменш три типи звуків-переносників інформації, а саме, тональний – для дзвінких звуків, шумовий – для глухих звуків та імпульсний – для вибухових звуків. Тональний переносник можна описати як періодичне полігармонійне коливання, що створюється рухом голосових зв'язок. Шумовий переносник можна охарактеризувати як гаусівський стаціонарний процес. Імпульсний переносник характеризується різким збільшенням швидкості повітряного потоку з подальшим експоненційним спадом. Передача інформації супроводжується модуляцією параметрів кожного з цих переносників. Залежно від типу переносника, мовленнєвий процес забезпечується амплітудною і фазовою модуляціями та модуляцією форми спектру. Лише тональний переносник зазнає всіх типів модуляції, що робить його потенційно найінформативнішим.

Спираючись на положення акустичної теорії мовотворення сформулюємо концепцію математичної моделі структурного представлення спектра найінформативнішого – сонорного, звуку у вигляді імпульсу амплітудно-модульованого коливання з кількома несними частотами. Представлений на рис. 3 графік ілюструє спрощений опис спектральних компонент трьох формант вокалізованого мовленнєвого сигналу математичною моделлю індивідуальності голосу. Спираючись на результати аналізу передавача в мовній системі зв'язку припустимо, що на інформативні для автентифікації суб'єкта за голосом характеристичні параметри вкажуть екстремальні значення амплітудних характеристик мовленнєвого тракту, які проявляються на частоті основного тону і частотах його обертонів.

Апроксимуємо спектральну щільність потужності $S(\omega)$ набором постійних складових S_l у частоних смугах шириною B_l в околі несних частот f_l^u, якими для мовленнєвого сигналу є частота основного тону f_0 і частоти його обертонів f_l. Обчисливши зворотне перетворення Фур'є від відомої спектральної щільності потужності, отримаємо математичну модель індивідуальності голосу $u(t)$ у вигляді амплітудно-модульованого коливання утвореного сумою модулюючого $u_{мод}(t)$ і несного $u_{нес}(t)$ коливань. При чому, шукані характеристичні параметри U_l входять до несної компоненти. Теорема Вінера-Хічкіна зв'язує перетворенням Фур'є спектральну щільність потужності сигналу з його автокореляційною функцією. Дана обставина регламентує отримання персоніфікованого опису вокалізованого мовленнєвого сигналу в результаті мінімізації середньоквадратичного відхилення значень кореляційних коефіцієнтів нормованих автокореляційних функцій досліджуваного сигналу і його моделі у вигляді амплітудно-модульованого полігармонійного коливання.

Узагальнимо аналітично щойно обґрунтовану концепцію моделі індивідуальності голосу в мовленнєвому сигналі (ІГМС). Базова квазідетермінована модель ІГМС це: модуляція потоку повітря $s(t)=\cos(2\pi F_0 t+\Phi_0) \Rightarrow$ обвідна l-го обертону основного тону $U_l(t)=U_l(1+Ms(t)) \Rightarrow$ модуляція L несних гармонік $u(t)=\sum_{l=1}^{L}U_l(t)\cos(2\pi l f_0 t+\varphi_0)$:

$$u(t)=\left(1+M\cos(2\pi F_0 t+\Phi_0)\right)\sum_{l=0}^{L}U_l\cos(2\pi l t f_0+\varphi_0),\ t\in[0,\tau_i], \qquad (1)$$

де F_0 і Φ_0 - частота і початкова фаза модулювального сигналу; φ_0 і τ_i - початкова фаза і тривалість полігармонійного несного сигналу; M - глибина модуляції; характеристичні параметри моделі: U_l - амплітуда l-ї несної гармоніки, $f_0=\overline{f_0}$ - усереднена для часового інтервалу τ_i частота основного тону.

Охарактеризуємо емпіричний дискретизований центрований мовленнєвий сигнал y автокореляційною функцією (АКФ) $R_y(j)$ і нормованою автокореляційною функцією (НАКФ) r_j^y:

$$R_y(j)=\sum_{i=0}^{N-1}(x_i-\overline{x})(x_{i-j}-\overline{x})=\sum_{i=0}^{N-1}y_i y_{i-j},\ r_j^y=R_y(j)/R_y(0),\ j=\overline{0,J}. \qquad (2)$$

Охарактеризуємо АКФ $R_u(\tau)$ і НАКФ r_τ^u модель ІГМС u, яка описуватеме сигнал y:

$$R_u(\tau)=\sum_{l=1}^{L}\sum_{m=1}^{L}U_l U_m I(\tau,l,m),\ r_\tau^u=R_u(\tau)/E_u, \qquad (3)$$

де $E_u=B_u(0)$, $\tau=j\Delta$, $I(\tau,l,m)$ - множини функцій, яуі є білінійними формами кореляційного інтегралу $B_u(\tau)=\int_0^{\tau_i}u(t)u(t-\tau)dt$ для імпульсного сигналу, описуваного моделлю (1).

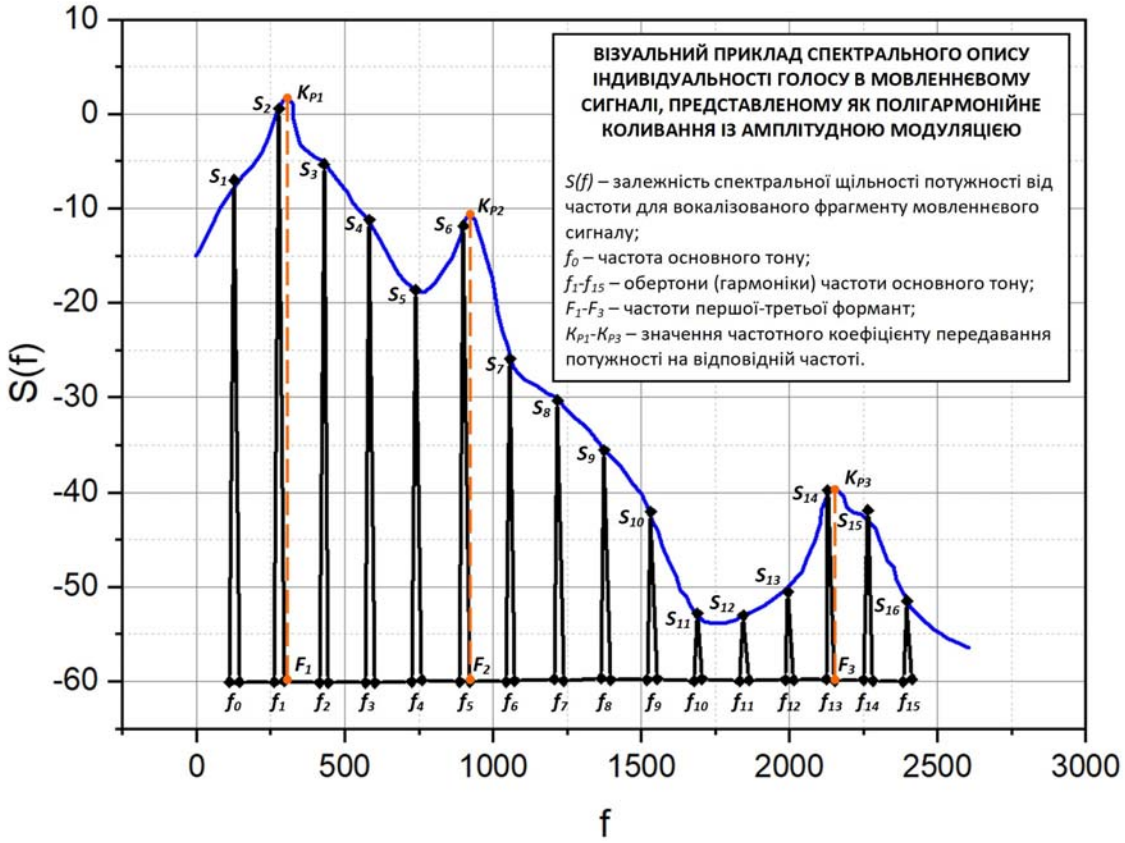

Рисунок 3 – Схематичний приклад детектування індивідуальності голосу при спектральному представленні мовленнєвого сигналу.

Критерій для обчислення U_l: $\varepsilon_b=\sum_{j=1}^{J}\left(r_j^u-r_j^y\right)^2\to\inf$, $l=\overline{1,L}$.

Для обчислення U_l приймаємо $\frac{\partial\varepsilon_b}{\partial U_l}=0\ \Rightarrow\ \left\{\sum_{j=1}^{J}\left(r_j^y-r_j^u\right)\frac{\partial r_j^u}{\partial U_l}=0,\ l=\overline{1,L}\right.$.

Критерії для оцінювання достатності значення J: $\beta=\left|\max\left(r_{j<J}^y\right)-r_{j=J}^y\right|$. Найкраще J при $\beta\to 0$.

Перетворення Фур'є зв'язує АКФ $R_u(\tau)$ і енергія E_u моделі ІГМС із спектральною щільністю потужності $W_u = \left|S(\omega)\right|^2$:

$$R_u(\tau) = \frac{U_0^2}{B_0}\operatorname{sinc}(\pi B_0 \tau) + 2\sum_{l=1}^{L}\frac{U_l^2}{B_l}\operatorname{sinc}(\pi B_0 \tau)\cos(2\pi l f_0 \tau),\ E_u = \frac{U_0^2}{B_0} + 2\sum_{l=1}^{L}\frac{U_l^2}{B_l} \Rightarrow$$
$$W_i = (S_i)^2 = \left(\frac{U_i}{B_i}\right)^2 = \left(\frac{U_i}{2f_i}\right)^2, \tag{4}$$

де B_i, $i = \overline{0,L}$ - частотні смуги, які накривають частоту основного тону f_0 і частоти її обертонів $f_1,\ldots,f_L$, відповідно.

Удосконалена версія базової квазідетермінованої моделі ІГМС є результатом представлення модулювального коливання рядом Фур'є:

$$u(t) = \sum_{k=0}^{K} M_k \cos(2\pi k F_0 t + \Phi_k)\sum_{l=0}^{L} U_l \cos(2\pi l f_0 t + \varphi_l), \tag{5}$$

де F_0 - найнижча частота модулювального коливання. Відповідно, множина характеристичних параметрів доповнюється значеннями глибин модуляції.

У стохастичних версіях базової і удосконаленої квазідетермінованих моделей ІГМС початкові фази модулювального і несного коливань - Φ_0 і φ_0, відповідно, вважаються взаємно некорельованими стохастичними величинами, рівномірно розподіленими на інтервалі $[0,2\pi]$ із щільностями імовірності $p_{\Phi_0} = 1/2\pi$ і $p_{\varphi_0} = 1/2\pi$.

На основі поєднання концепції передавача в мовній системі зв'язку із математичним апаратом стохастичних моделей індивідуальності голосу створено метод оцінювання рівня відношення «сигнал»/«шум» в емпіричному мовленнєвому сигналі. В запропонованому методі параметричний опис емпіричного мовленнєвого сигналу розглядається як сума параметричних описів еталонного мовленнєвого сигналу і шуму: $\xi(t) = u(t) + n(t)$, де $n(t)$ - стохастична складова, описувана моделлю «білого шуму», $u(t)$ - складова, описувана стохастичною моделлю ІГМС.

Визначимо аналітично математичне сподівання, дисперсію функцію кореляції, кореляційний коефіцієнт і спектральну щільність потужності для стаціонарного і ергодичного випадкового процесу $n(t)$: $m_n = 0$; $D_n^2 = N_0 f_h$; $R_n(\tau) = N_0 f_h \operatorname{sinc}(2\pi f_h \tau)$; $r_n(\tau) = \operatorname{sinc}(2\pi f_h \tau)$ $W_n(2\pi f) = N_0/2$, де $f \in [0, f_h]$, f_h – верхня частота смуги, $N_0 = const$ – одностороння спектральна щільність потужності.

Визначимо аналітично математичне сподівання, дисперсію функцію кореляції, кореляційний коефіцієнт і спектральну щільність потужності для стаціонарного і ергодичного випадкового процесу $u(t)$: $m_u = 0$;

$$D_u^2=\frac{1}{2}\left(1+\frac{M^2}{2}\right)\sum_{l=1}^{L}U_l^2;\qquad R_u(\tau)=\frac{1}{2}\left(1+\frac{M^2}{2}\cos(2\pi F_0\tau)\right)\sum_{l=1}^{L}U_l^2\cos(2\pi lF_0\tau);$$

$$r_u(\tau)=R_u(\tau)/D_u(\tau);\ W_u(2\pi f)=\frac{\tau}{2}\sum_{l=1}^{L}U_l^2\left(\mathrm{sinc}\left(2\pi\left(f+lf_0\right)\tau\right)+\mathrm{sinc}\left(2\pi\left(f-lf_0\right)\tau\right)+\right.$$

$$\frac{M^2}{4}\left(\mathrm{sinc}\left(2\pi\left(f+\left(lf_0+F_0\right)\right)\tau\right)+\right.+\mathrm{sinc}\left(2\pi\left(f-\left(lf_0+F_0\right)\right)\tau\right)+\mathrm{sinc}\left(2\pi\left(f+\left(lf_0-F_0\right)\right)\tau\right)+$$

$$\left.\left.+\mathrm{sinc}\left(2\pi\left(f-\left(lf_0-F_0\right)\right)\tau\right)\right)\right),\ \text{де}\ \tau=t_2-t_1>0.$$

Визначимо аналітично математичне сподівання, дисперсію функцію кореляції, кореляційний коефіцієнт і спектральну щільність потужності для стаціонарного і ергодичного випадкового процесу $\xi(t)$: $m_\xi=0$; $D_\xi^2=D_u^2+D_n^2$;

$$R_\xi(\tau)=R_u(\tau)+R_n(\tau);\qquad r_\xi(\tau)=r_u(\tau)+r_n(\tau);$$

$$W_\xi(2\pi f)=\begin{cases}W_u(2\pi f)+W_u(2\pi f),\ if\ \ f\in[0,f_h],\\ W_u(2\pi f),\ if\ \ f\notin[0,f_h].\end{cases}$$

Дисперсію центрованого емпіричного мовленнєвого сигналу опишемо виразом $D_y^2=R_y(0)\approx\frac{1}{N}\sum_{i=1}^{N}y_i^2=\left(D_u^{pr}\right)^2\{\le,=,\ge\}\left(D_u^{ps}\right)^2=\frac{1}{2}\left(1+\frac{M^2}{2}\right)\sum_{l=1}^{L}U_l^2$.

Порівнявши дисперсію центрованого емпіричного мовленнєвого сигналу із апостеріорною дисперсією, обчисленою на основі стохастичної моделі ІГМС можна обчислити дисперсію шуму та відповідно до її значення оцінити рівень відношення «сигнал»/«шум»:

$$\begin{gathered}D_\xi^2=\left(D_u^{ps}\right)^2+D_n^2\Rightarrow D_n^2=D_\xi^2-\left(D_u^{ps}\right)^2\Rightarrow\\ N_0=D_n^2/f_h\Rightarrow D_{SNR}^2=\left(D_u^{ps}\right)^2\Big/\left(D_\xi^2-\left(D_u^{ps}\right)^2\right).\end{gathered}\qquad(6)$$

При $D_{SNR}^2>>1$ присутньою в емпіричному мовленнєвому сигналі шумною складовою можна знехтувати, фонетичний вміст його можна вважати вокалізованим, а для опису індивідуальності голосу мовця в ньому варто використовувати квазідетерміновані моделі ІГМС. При $D_{SNR}^2\approx1$ в емпіричному мовленнєвому сигналі присутня помітна шумна складова, для опису індивідуальності голосу мовця в ньому варто використовувати стохастичні моделі ІГМС. При $D_{SNR}^2<<1$ шумна складова в емпіричному мовленнєвому сигналі домінує, отже, отримати адекватний опис індивідуальності голосу мовця в ньому в методології моделей ІГМС не вдасться.

Проілюструємо практичне застосування запропонованих моделей ІГМС, параметризувавши еталонний мовленнєвий сигнал, представлений на верхніх зображеннях на рис. 4. На лівому нижньому зображенні на рис. 4 наведено значення коефіцієнтів НАКФ еталонного сигналу і його опису базовою квазідетермінованою моделлю ІГМС. Абсолютна і відносна похибки представлення дорівнюють 0,5 і близько 5%, відповідно. На правому нижньому зображенні на рис. 4 наведено порівняння значень нормованої спектральної

щільності потужності еталонного сигналу і його опису базовою квазідетермінованою моделлюІГМС. Осциляцію і розмитість спектра в околі гармонік основного тону обумовлено його частотною модуляцією.

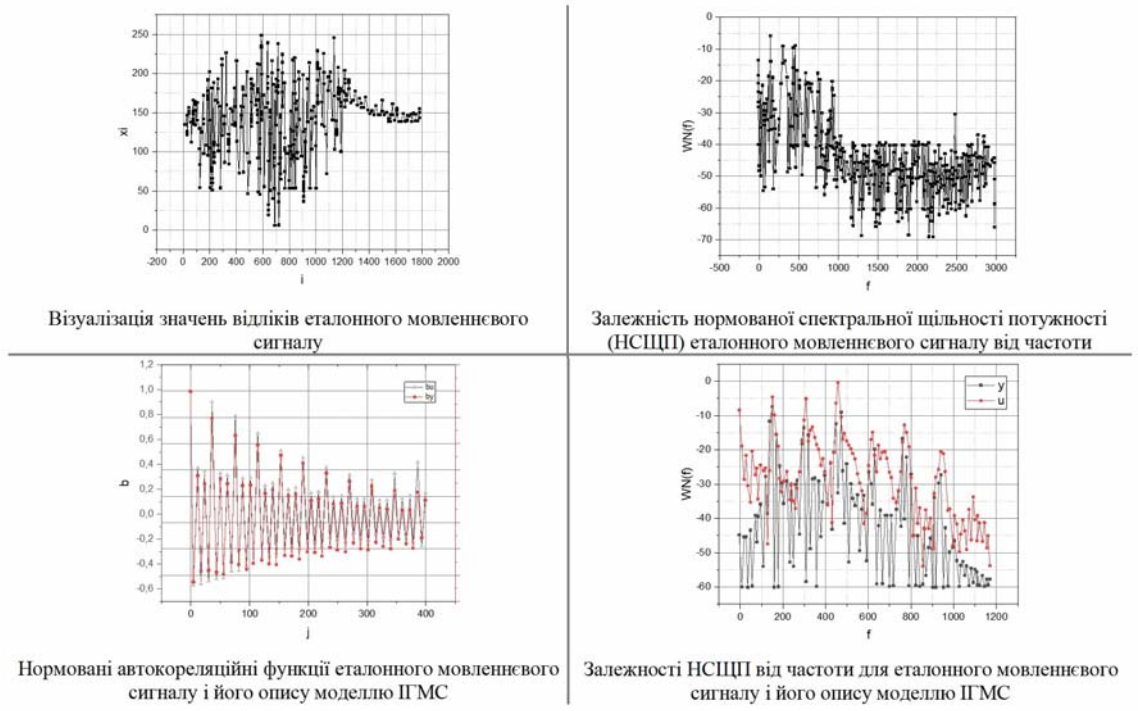

Рисунок 4 – Приклад опису емпіричного мовленнєвого сигналу моделлю ІГМС.

На рис. 5 наведено зображення, які додатково характеризують процес опису індивідуальності голосу в мовленнєвому сигналі в методології моделей ІГМС.

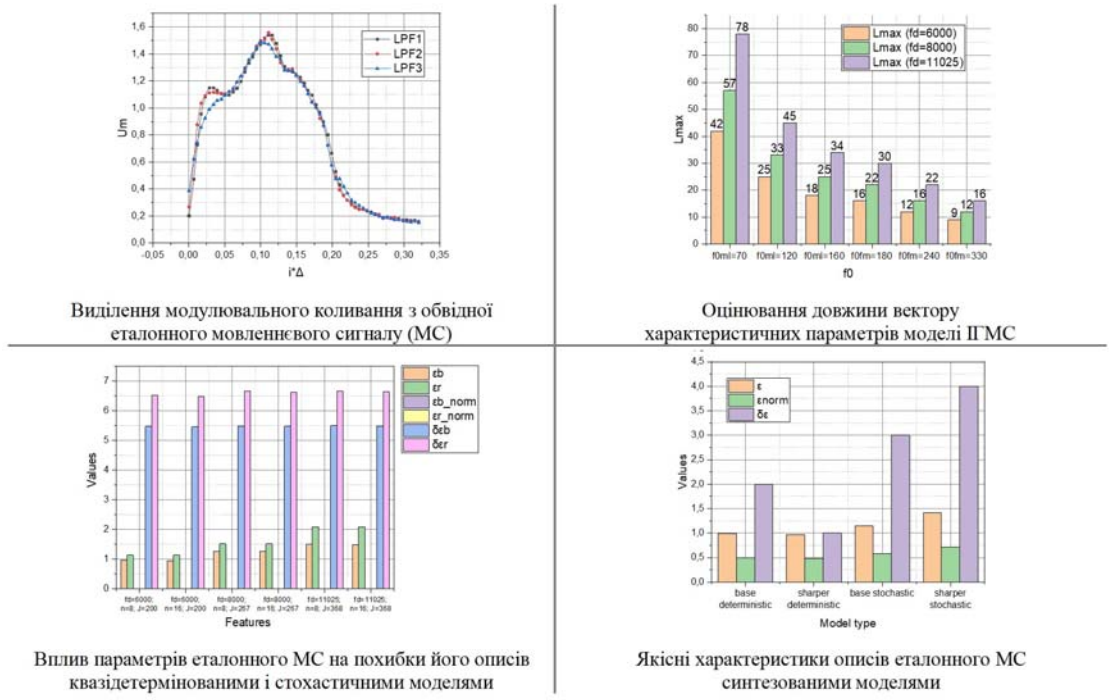

Рисунок 5 – Специфіка опису мовленнєвих сигналів моделями ІГМС.

На лівому верхньому зображенні на рис. 5 наведено результати виділення модулювального коливання із обвідної еталонного сигналу із застосуванням фільтрів низьких частот, синтезованих методом білінійного перетворення на основі фільтрів Батерворта 3-го, 2-го і 1-го порядків. Найякісніший результат отримано при застосуванні фільтра Батерворта 3-го порядку, що збігається з аналітичними викладками. На правому верхньому зображенні на рис. 5візуалізовано залежність максимальної кількості несних гармонік L_{max} у мовленнєвому сигналі від частоти дискретизації і типових значень частоти основного тону. Втім, висока достовірність опису індивідуальності голосу запропонованими моделями ІГМС досягається при L в діапазоні від 6 до 10. Оцінити вплив частоти дискретизації і розрядності квантування мовленнєвого сигналу на чутливість якісних характеристик його описів моделями ІГМС можна на лівому нижньому зображенні на рис. 5. На правому нижньому зображенні на рис. 5 візуалізовано значення абсолютної, нормованої абсолютної і відносної похибок описів індивідуальності голосу в еталонному сигналі створеними моделями.

Отже, в другому розділі дисертації аналітично формалізовано концепцію, коли представлений модулювальним і полігармонічним несним коливаннями мовленнєвий сигнал параметризується у просторі таких характеристичних параметрів, як усереднена частота основного тону і амплітуди несних гармонік, формалізованих в методології квазідетермінованих і стохастичних моделей індивідуальності голосу, що дозволяє отримати компактний, інформативний і адекватний параметричний опис індивідуальності сегментів мовленнєвих сигналів із високим і помірним рівнем вокалізації.

В **третьому розділі** в контексті задачі автентифікації суб'єкта за голосом систематизується процес встановлення адекватності емпіричних мовленнєвих сигналів і їх описів математичними моделями ІГМС, представленими в другому розділі. Також формалізується процес оцінювання порогу прийняття рішень в задачі автентифікації суб'єкта за голосом відповідно до рівня відношення «сигнал»/«шум» в аналізованому мовленнєвому сигналі.

Вкрай популярні зараз інтелектуальні методи прийняття рішень є вкрай ресурсозатратними. Цього недоліку позбавлена міра розрізнення, сформульована як сума зважених різниць між еталонним та емпіричним значеннями кожного характеристичного параметру опису мовленнєвого матеріалу моделлю ІГМС.

За умови фіксованого порогу D_0, можливі три підходи для розрахунку вагових коефіцієнтів міри розрізнення з орієнтацію на мінімізацію або похибки першого роду α або похибки другого роду β або півсуми цих похибок $(\alpha+\beta)/2$. Шукані значення вагових коефіцієнтів $\{w\}$ знаходяться в результаті розв'язання системи лінійних рівнянь, профілювання яких забезпечується використанням множини *H* або *I*.

Аналітично формалізуємо міру розрізнення між еталонним *et* і емпіричним *vs* представленнями мовленнєвих сигналів в параметричному просторі моделей ІГМС:

$$D=\sum_{l=1}^{L} w_l^U\left(U_l^{vs}-U_l^{et}\right)+w_{L+1}^{(f)}\left(f_0^{vs}-f_0^{et}\right), \qquad (7)$$

де $w^{(f)}$ – ваговий коефіцієнт частоти основного тону f_0, w_l^U – множина із L вагових коефіцієнтів при відповідних амплітудах несних гармонік.

Цільову функцію для задачі оптимізації значень ваг w_l сформулюємо на основі критерію D_Σ^α у вигляді

$$\min_{w_l}\left(D_\Sigma^\alpha\right)=\min_{w_l}\left(\sum_{p=1}^{P}\left(D_p^\alpha\right)^2\right)=\min_{w_l}\left(D_\Sigma^\alpha\right)=\min_{w_l}\left(\sum_{p=1}^{P}\left(\sum_{l=1}^{L+1}w_l\gamma_{l,p}\right)^2\right), \tag{8}$$

де D_p^α – міра розрізнення параметрів, екстрагованих із вхідної фонограми, із еталонними значеннями відповідних параметрів, збереженими у системі; P – кількість фонограм, вжитих для визначення еталонних значень параметрів w_l (не менше двох фонограм для кожного суб'єкта, якого автентифікуватиме навчена система), $\mathrm{H}=\{\gamma_{l,p}\}=\left\{\gamma_{1,p}\equiv\left(U_{1,p}^\alpha-U_1^{et}\right)^2,\ldots,\gamma_{L,p}\equiv\left(U_{L,p}^\alpha-U_L^{et}\right)^2,\quad \gamma_{L+1,p}\equiv\left(f_{0,p}^\alpha-f_0^{et}\right)^2\right\}$ – вектор оцінюваних характеристичних параметрів моделі ІГМС, а $\Omega=\{w_{L+1}\}=\left\{w_1=w_1^U,\ldots,w_L=w_L^U,w_{L+1}=w^{(f)}\right\}$ – вектор їх ваг, $p=\overline{1,P}$.

Виразимо $D_\Sigma^\alpha=\sum_{p=1}^{P}\left(\gamma_{1,p}+\sum_{l=2}^{L+1}w_l\left(\gamma_{l,p}-\gamma_{1,p}\right)\right)^2$, де $D_\Sigma^\alpha=\sum_{p=1}^{P}\left(D_p^\alpha\right)^2$. Прирівняємо до нуля похідні від D_Σ^α по w_l: $\frac{\partial D_\Sigma^\alpha}{\partial w_l}=0$. Розкриємо цю рівність у вигляді системи з L лінійних рівнянь:

$$\begin{cases}\sum_{l=2}^{L+1}\left(\sum_{p=1}^{P}\left(\gamma_{1,p}-\gamma_{2,p}\right)\left(\gamma_{1,p}-\gamma_{l,p}\right)\right)w_l=\sum_{p=1}^{P}\gamma_{1,p}\left(\gamma_{1,p}-\gamma_{2,p}\right),\\ \sum_{l=2}^{L+1}\left(\sum_{p=1}^{P}\left(\gamma_{1,p}-\gamma_{3,p}\right)\left(\gamma_{1,p}-\gamma_{l,p}\right)\right)w_l=\sum_{p=1}^{P}\gamma_{1,p}\left(\gamma_{1,p}-\gamma_{3,p}\right),\\ \ldots\\ \sum_{l=2}^{L+1}\left(\sum_{p=1}^{P}\left(\gamma_{1,p}-\gamma_{L+1,p}\right)\left(\gamma_{1,p}-\gamma_{l,p}\right)\right)w_l=\sum_{p=1}^{P}\gamma_{1,p}\left(\gamma_{1,p}-\gamma_{L+1,p}\right),\end{cases}, \tag{9}$$

розв'язавши яку відносно w_l отримаємо точку екстремуму, класифікувати яку можна за значенням другої похідної від D_Σ^α по w_l в цій точці:

$$\frac{\partial^2 D_\Sigma^\alpha}{\partial w_l^2}=\sum_{p=1}^{P}\left(\gamma_{1,p}-\gamma_{l,p}\right)^2>0. \tag{10}$$

Якщо нерівність (10) виконується, то точка, яка класифікується, є точкою мінімуму. Аналітичний розрахунок ваг w_l для міри D, представленої критерієм $\min_{w_l}\left(D_\Sigma^\alpha\right)$, зводиться до тривіального розв'язку системи лінійних рівнянь (9) відносно w_l. При чому розраховані значення ваг w_l забезпечують мінімальне

можливе значення похибки першого роду α при заданому порозі D_0 для досліджуваної конфігурації простору параметрів моделі ІГМС.

Припустимося аналогічних наведеним вище міркуванням для отримання аналітичних виразів для обчислення ваг w_l в контексті мінімізації критерію D_Σ^β:

$$\min_{w_l}\left(D_\Sigma^\beta\right)=\min_{w_l}\left(\sum_{m=1}^{M}\left(D_m^\beta\right)^2\right), \tag{11}$$

де D_m^β – міра близькості параметрів, екстрагованих із вхідної фонограми, із еталонними значеннями відповідних характеристичних параметрів, збережених у системі; M – кількість фонограм суб'єктів, мовленнєві матеріали яких не використовувалися на етапі навчання системи автентифікації. Позначимо $\mathrm{I}=\left\{\eta_{l,m}\right\}=\left\{\eta_{1,m}\equiv\left(U_{1,m}^\beta-U_1^{et}\right)^{-2},\ldots,\eta_{L,m}\equiv\left(U_{L,m}^\beta-U_L^{et}\right)^{-2},\ \eta_{L+1,m}\equiv\left(f_{0,p}^\beta-f_0^{et}\right)^{-2}\right\}$ – вектор оцінюваних характеристичних параметрів моделі ІГМС, і $\Omega=\left\{w_{L+1}\right\}=\left\{w_1=w_1^U,\ldots,w_L=w_L^U,w_{L+1}=w^f\right\}$ – вектор їхніх ваг, $m=\overline{1,M}$. Виразимо вагу w_1 із виразу для нормування ваг $\sum_{l=1}^{L+1}w_l=1$: $w_1=1-\sum_{l=2}^{L+1}\omega_l$ і підставимо у вираз для розрахунку критерію $D_\Sigma^\beta=\sum_{m=1}^{M}\left(D_m^\beta\right)^2$:

$$D_\Sigma^\beta=\sum_{m=1}^{M}\left(\eta_{1,m}+\sum_{l=2}^{L+1}w_l\left(\eta_{l,m}-\eta_{1,m}\right)\right)^2, \tag{12}$$

Прирівняємо до нуля похідні від D_Σ^β по w_l при $l=\overline{2,L+1}$: $\frac{\partial D_\Sigma^\beta}{\partial w_l}=0$, і розкриємо отриману рівність у вигляді системи з L лінійних рівнянь

$$\begin{cases}\sum_{l=2}^{L+1}\left(\sum_{m=1}^{M}\left(\eta_{1,m}-\eta_{2,m}\right)\left(\eta_{1,m}-\eta_{l,m}\right)\right)w_l=\sum_{m=1}^{M}\eta_{1,m}\left(\eta_{1,m}-\eta_{2,m}\right),\\ \sum_{l=2}^{L+1}\left(\sum_{m=1}^{M}\left(\eta_{1,m}-\eta_{3,m}\right)\left(\eta_{1,m}-\eta_{l,m}\right)\right)w_l=\sum_{m=1}^{M}\eta_{1,m}\left(\eta_{1,m}-\eta_{3,m}\right),\\ \ldots\\ \sum_{l=2}^{L+1}\left(\sum_{m=1}^{M}\left(\eta_{1,m}-\eta_{L+1,m}\right)\left(\eta_{1,m}-\eta_{l,m}\right)\right)w_l=\sum_{m=1}^{M}\eta_{1,m}\left(\eta_{1,m}-\eta_{L+1,m}\right),\end{cases} \tag{13}$$

розв'язавши яку відносно w_l, отримаємо точку екстремуму класифікувати яку можна за значенням другої похідної від D_Σ^β по w_l в цій точці:

$$\frac{\partial^2 D_\Sigma^\beta}{\partial w_l^2}=\sum_{m=1}^{M}\left(\eta_{1,m}-\eta_{l,m}\right)^2>0. \tag{14}$$

Якщо нерівність (14) виконується, то точка, яка класифікується, є мінімумом. Аналітичний розрахунок ваг w_l для міри D, представленої критерієм D_Σ^β, зводиться до розв'язку системи лінійних рівнянь (13) відносно w_l.

І, нарешті, отримаємо аналітичні вирази для обчислення ваг w_l в контексті мінімізації критерію $D_\Sigma^{\alpha+\beta} = D_\Sigma^{\alpha} + D_\Sigma^{\beta}$:

$$\min_{w_l}\left(D_\Sigma^{\alpha+\beta}\right) = \min_{w_l}\left(\sum_{p=1}^{P}\left(D_p^{\alpha}\right)^2 + \sum_{m=1}^{M}\left(D_m^{\beta}\right)^2\right). \tag{15}$$

Для вживання критерію $D_\Sigma^{\alpha+\beta}$ необхідно на етапі навчання системи проаналізувати не менше двох фонограм суб'єкта, який автентифікуватиметься. Автентифікація здійснюватиметься на основі результатів аналізу вхідної фонограми, яка не входила до навчальної вибірки. Прирівняємо до нуля похідні від $D_\Sigma^{\alpha+\beta}$ по ω_l при $l = \overline{2, L+1}$: $\dfrac{\partial D_\Sigma^{\alpha+\beta}}{\partial w_l} = 0$. Розкриємо отриманий вираз у вигляді системи з L лінійних рівнянь, Розв'язавши отриману систему лінійних рівнянь відносно w_l отримаємо точку екстремуму, класифікувати яку можна за значенням другої похідної від $D_\Sigma^{\alpha+\beta}$ по w_l у цій точці:

$$\frac{\partial^2 D_\Sigma^{\alpha+\beta}}{\partial w_l^2} = \sum_{p=1}^{P}\left(\gamma_{1,p} - \gamma_{l,p}\right)^2 \sum_{m=1}^{M}\left(\eta_{1,m} - \eta_{l,m}\right)^2 > 0. \tag{16}$$

Вище наведена нерівність завжди виконуватиметься, що гарантує знаходження значень w_l, які мінімізують значення критерію $D_\Sigma^{\alpha+\beta}$.

Поріг D_0 в критерії прийняття рішень щодо автентифікації суб'єкта за голосом доцільно обирати з врахуванням варіативності значення міри розрізнення $D(\lambda^{et},\lambda^{vs})$, яке враховує мінливість характеристичних параметрів еталонного голосу $\Delta\lambda^{et}$. В розділі наведені вирази для розрахунку порогу D_0 на основі мір розрізнення D і D', які враховують важливість ступеню розбіжності відповідних істотних параметрів моделі індивідуальності голосу.

Визначимо поріг D_0 у критерії прийняття рішень як значення міри розрізнення $D\left(\lambda^{et},\lambda^{vs}\right)$:

$$D_0\left(\Delta\lambda^{et}\right) = D\left(\lambda^{et},\lambda^{vs}\right)\Big|_{\lambda^{vs}=\lambda^{et}\pm\Delta\lambda^{et}} = D\left(\lambda^{et},\lambda^{et}\pm\Delta\lambda^{et}\right), \tag{17}$$

де $\lambda^{et} = \left(\lambda_1^{et},\lambda_2^{et},\ldots,\lambda_L^{et}\right)$, $\lambda^{vs} = \left(\lambda_1^{vs},\lambda_2^{vs},\ldots,\lambda_L^{vs}\right)$ - множини еталонних і емпіричні значень характеристичних параметрів моделі ІГМС, відповідно.

Для міри розрізнення $D = \sum_{l=1}^{L}\left(\dfrac{U_l^{vs}}{f_0^{vs}} - \dfrac{U_l^{et}}{f_0^{et}}\right)^2$ запишемо:

$$D_0 = 4\sum_{l=1}^{L}\left(\Delta f_0 U_l^{et} + \Delta U_l^{et} f_0^{et}\right)^2 \Big/ \left(\left(f_0^{et}\right)^2 - \left(\Delta f_0\right)^2\right)^2. \tag{18}$$

Довірчі інтервали варіації U_l і f_0: $\Delta U_l = \mu\sigma_{U_l^{et}}$, $\Delta f_0 = \mu\sigma_{f_0^{et}}$, де $\sigma_{U_l^{et}}$ і $\sigma_{f_0^{et}}$ - відповідне СКВ, $\mu \equiv \mu(P)$ – залежний від довірчої імовірності $P = \int_{-\mu\sigma}^{\mu\sigma} p(x)dx$ параметр, наприклад, при $P = 95\ \%$ $\mu = 2{,}005 \approx 2$, при $P = 99\ \%$ $\mu = 2{,}576 \approx 2{,}6$.

Введемо міру $D' = \left(\left(f_0^{et} - f_0^{vs}\right)^2 + v_1\right)\sum_{l=1}^{L}\left(\left(U_l^{et} - U_l^{vs}\right)^2 + v_2\right)\Big/\left(f_0^{et}\right)^2$, де $v_1 \equiv \Delta f_0$, $v_2 \equiv \Delta U_l$. Відцентрований невід'ємний варіант міри D':

$$D' = \left(\frac{f_0^{et} - f_0^{vs}}{f_0^{et}}\right)^2 \sum_{l=1}^{L}\left(U_l^{et} - U_l^{vs}\right)^2 + L\left(\Delta U_l^{et}\right)^2\left(\frac{f_0^{et} - f_0^{vs}}{f_0^{et}}\right)^2 + \\ + \left(\delta f_0^{et}\right)^2 \sum_{l=1}^{L}\left(U_l^{et} - U_l^{vs}\right)^2, \tag{19}$$

де $\delta f_0^{et} = \Delta f_0^{et} \big/ f_0^{et}$ – відносний інтервал варіації частоти основного тону.

Поріг D_0 у критерії прийняття рішень за значенням міри розрізнення D' опишемо таким виразом:

$$D_0 = \left(\frac{2\Delta f_0^{et}}{f_0^{et}}\right)^2 \sum_{l=1}^{L}\left(2U_l^{et}\right)^2 + L\left(\Delta U_l^{et}\right)^2\left(\frac{2\Delta f_0^{et}}{f_0^{et}}\right)^2 + \left(\delta f_0^{et}\right)^2 \sum_{l=1}^{L}\left(2U_l^{et}\right)^2 = \\ = 24L\left(\delta f_0^{et}\right)^2\left(\Delta U_l^{et}\right)^2. \tag{20}$$

Відзначимо, що міра D' є потенційно чутливішою, адже враховує відносний інтервал варіації частоти основного тону.

В **четвертому розділі** оцінюється вплив шумів акустичного оточення приймачів мовленнєвого сигналу на конфіденційність процесу автентифікації суб'єкта за голосом. Запропоновано моделі компенсування шумів в 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.

Представлений розділі 2 математичний апарат дозволяє визначити рівень відношення «сигнал»/«шум», при якому отримати адекватний опис мовленнєвого сигналу моделями ІГМС не вдасться. За такої обставини можливі два варіанти подальших дій – запропонувати суб'єкту повторно записати фонограму, або ж спробувати компенсувати шуми у фонограмі, застосовуючи математичний апарат сумішей гаусівських розподілів та машинного навчання. При узагальненні векторів характеристичних параметрів моделлю суміші гаусівських розподілів адитивні і мультиплікативні шуми впливають на значення дисперсій і на вектори середніх значень всіх компонентів моделі суміші, відповідно. Компенсувати цей вплив можна розв'язавши задачу мінімізації цільової функції *E(x|y)*, де *X* і *Y* є спектральним узагальненням вмісту еталонних баз фонограм без шуму та із шумом, відповідно. Графічну інтерпретацію такої концепції компенсування шумів в емпіричному мовленнєвому сигналі представлено на лівому зображенні на рис. 6. На правому зображенні на рис. 6 представлено концепцію агрегування спектрального узагальнення вмісту еталонних баз фонограм мовленнєвих сигналів без шуму та із шумом в єдину еталонну базу *Z*. Перевагою цієї концепції

є опис мовленнєвого матеріалу однією моделлю суміші $\lambda^{(Z)}$ і можливістю орієнтування цієї моделі суміші на компенсування конкретного типів шумів контролюючи вміст еталонної бази фонограм із шумом Y.

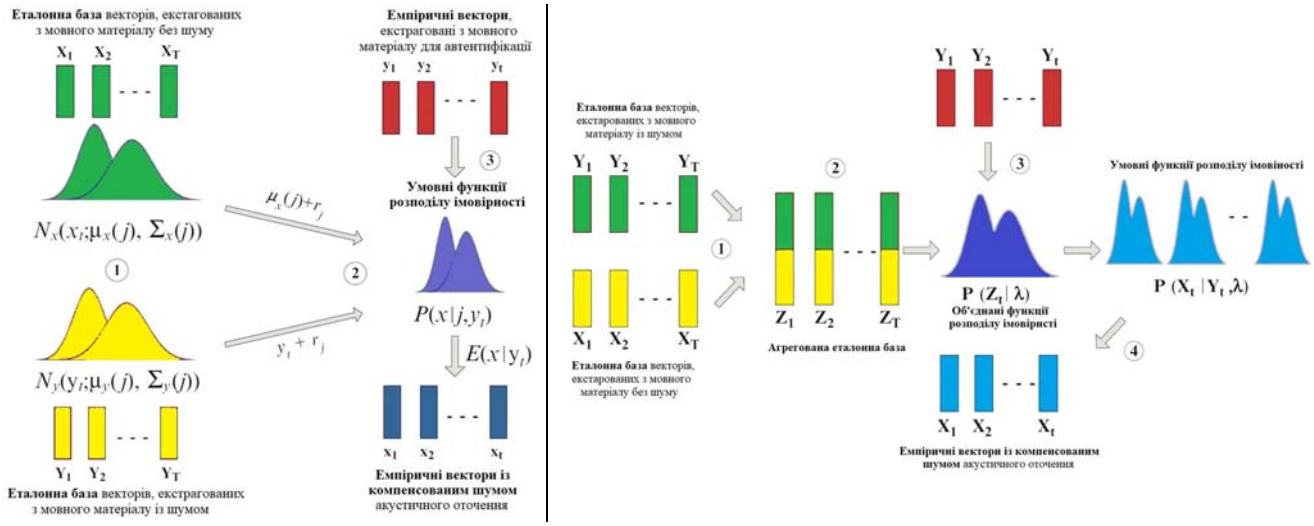

Рисунок 6 – Концепції стохастичної компенсація шумів в мовленнєвому сигналі.

На рис. 7 наведено результати застосування запропонованих концепцій компенсування шумів в мовленнєвому сигналі. На рисунках по вісі абсцис відкладено значення кепстрального коефіцієнта c_1, екстрагованого із мовленнєвого матеріалу без шуму, а по вісі ординат – значення цього ж коефіцієнта, екстрагованого з мовленнєвого матеріалу, до якого спочатку додали шум, а потім його компенсували.

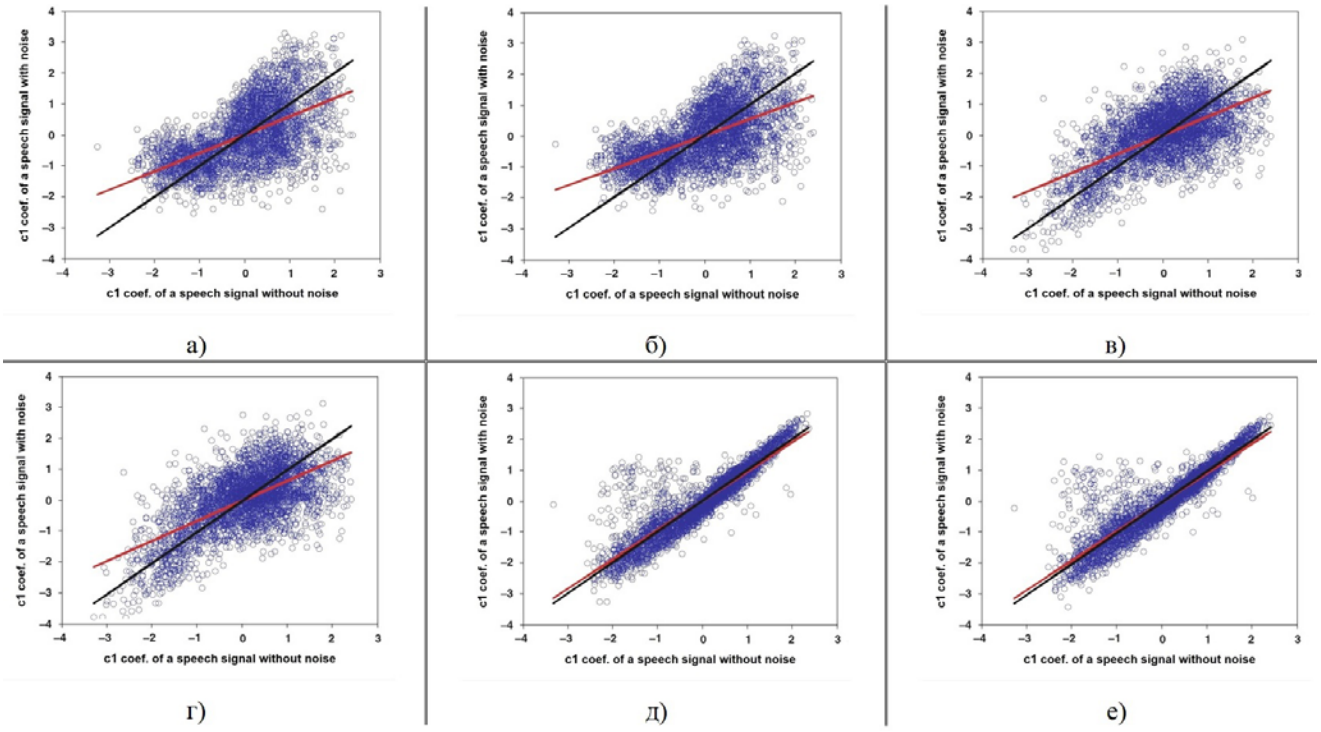

Рисунок 7 – Візуалізація результатів компенсування шумів в мовленнєвому сигналі за допомогою представлених на рис. 6 концепцій.

На рис. 7а представлено результати опрацювання мовленнєвого матеріалу з рівнем відношення «сигнал»/«шум» 0 дБ без компенсації шуму. Результати на рис. 7б і 7д демонструють продуктивність компенсування шуму при безпосередньому застосовуванні відповідних концепцій, представлених на рис. 6. Рисунок 7в характеризує адаптацію концепції, представленої на лівому зображенні на рис. 6, яка полягає у стохастичній інтерпретації ваг компонент моделей сумішей. Рисунок 7г характеризує адаптацію тієї ж концепції, яка полягає у профілюванні моделей сумішей для комплексного опису акустичного оточення суб'єкта. Рис. 7е характеризує адаптацію концепції, представленої на правому зображенні на рис. 6, яка полягає у врахуванні динамічних спектральних характеристик при формуванні еталонної бази *Z*. Порівняння решти рисунків з рис. 7а наочно демонструє продуктивність запропонованих концепцій для компенсації шумів в мовленнєвому матеріалі.

В роботі було проведено комплексне дослідження достовірності автентифікації суб'єкта машинами опорних супер- та *i*-векторів, результати якого представлені DET-кривими на нижньому зображенні на рис. 8. Мовленнєвий матеріал параметризувався у чотири набори характеристичних параметрів у складі векторів Мел-кепстральних коефіцієнтів, перцептивних коефіцієнтів лінійного передбачення, нормованих за потужністю кепстральних коефіцієнтів і амплітуд на частоті основного тону і частотах його обертонів. На рисунку ліворуч наведено алгоритм розрахунку значень перших трьох наборів характеристичних параметрів. Спочатку на основі даних параметризації мовленнєвого матеріалу із типізованим шумом контрольованої потужності були сформовані чотири 1024-компонентні універсальні фонові моделі. Далі універсальні фонові моделі адаптувалися до цільових суб'єктів *MAP*-методом, а отримані індивідуальні восьмикомпонентні моделі сумішей використовуватися машинами опорних векторів для прийняття рішень. Найдостовірнішу верифікацію показала одна з машин опорний *i*-векторів.

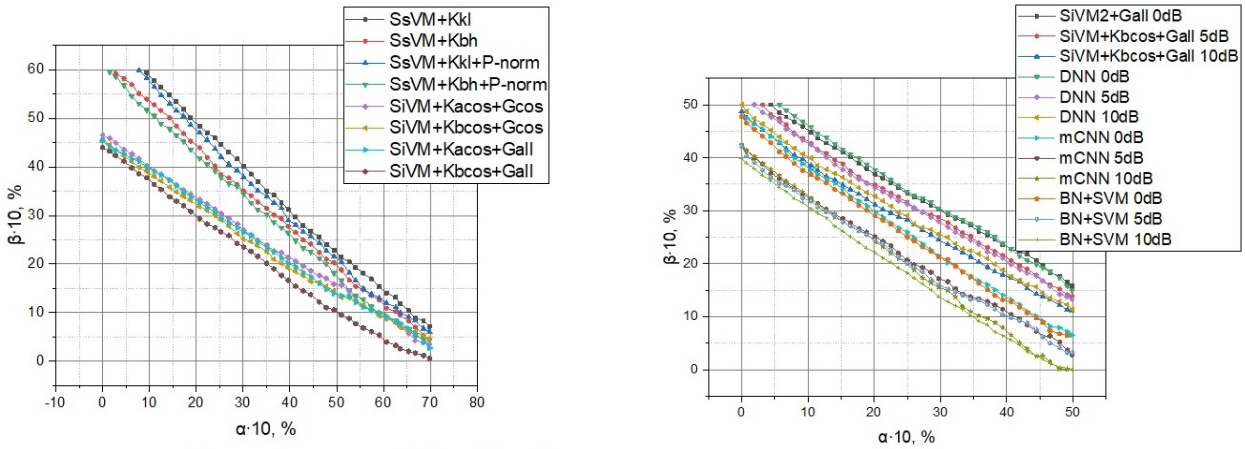

Рисунок 8 – Результати автентифікації суб'єкта за мовленнєвим сигналом із шумом запропонованими методами машинного навчання.

В розділі представлені результати адаптації глибоких нейромережевих класифікаторів для задачі автентифікації суб'єкта за голосом. Окремо досліджено застосування згорткової нейромережі для автентифікації суб'єкта за голосом. Цей

клас нейромереж працює із візуальними вхідними даними, що зумовлює представлення параметризованих фреймів мовленнєвих сигналів спектрограмами, компактно описати які дозволяє банк фільтрів Габора із частотами смуг, визначеними відповідно до положень теорії спектрально-темпоральних рецептивних полів. Функціональна схожість операцій, здійснюваних синтезованим банком фільтрів і вхідним шаром згорткової нейромережі, стала основою для створення модифікованої версії останньої. Інтеграція банку фільтрів з нейромережею забезпечується використанням у її вхідному шарі нейронів із лінійними функціями активації та встановленням параметра перекривання ядер рівним нулю.

На правому зображенні на рис. 8 наведені підсумкові результати крос-порівняння імовірнісних та нейромережевих класифікаторів в задачі автентифікації суб'єкта за мовленнєвим матеріалом із шумом. З наведених результатів видно, що для всіх типів і рівнів відношення «сигнал»/«шум» класифікатори в порядку зростання достовірності автентифікації розташувалися так: SiVM+Kbcos+Gall, DNN, mCNN, BN+SVM. Можна констатувати, що не зважаючи на очевидний ефект, який демонструє запропонований у розділі математичний апарат для компенсування шумів в мовленнєвому матеріалі, глибокі нейромережі краще ніж класифікатор SiVM+Kbcos приймають рішення при низьких рівнях відношення «сигнал»/«шум» у вхідному мовленнєвому сигналі. Втім, поєднання сильних сторін машин опорних векторів і нейромереж у класифікаторі BN+SVM дало очікуваний ефект, забезпечивши найвищу достовірність автентифікації серед конкурентів.

В **п'ятому розділі** відображено 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, доступності, цілісності, безвідмовності, готовності, обслуговуваності, інтенсивності відмов і напрацювань на відмову ІСКЗ. В отриманих моделях атрибутів 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-доступність та цілісність-функціональність, представлено відповідні моделі взаємозалежності цих інтегральних складових гарантоздатності із утворенням відповідних критеріїв.

В розділі представлено концепцію автентифікації суб'єктів-користувачів в процесі отримання доступу до мультисерверної ІСКЗ. Актори суб'єкт-системної взаємодії узагальнені множиною користувачів, множиною серверів та виділеним сервером-реєстраційним центром для обліку активних акторів без ведення верифікаційних таблиць. Інформаційний обмін між акторами відбувається у виділених сесіях, захист яких реалізовано на основі ключів із механізмом узгодження на основі односторонніх хеш-функцій та криптографії еліптичних кривих, яка на даний час забезпечує найкраще співвідношення надійності шифрування відносно до довжини ключа. Роботу із користувачами

персоніфіковано за допомогою індивідуальних карт доступу, які захищено на основі положень криптографічної теорії еліптичних кривих. На картах доступу, окрім ідентифікаційної інформації та паролю, зберігається індивідуальна біометрична інформація про особливості голосу користувача. Додаток для автентифікації, який встановлюється на обчислювальному засобі користувача, ініціюється двохступінчатою процедурою автентифікації (за умови наявності ідентифікаційної карти) – за введеним паролем та за результатами верифікації користувача за голосом. Запропоновану базову концепцію протестовано та обґрунтовано її відповідність стандарту ISO/IEC 27001:2013. Втім, досвід практичної експлуатації ІСКЗ виявив у базовій концепції ряд вразливостей, з метою позбавлення було формалізовано удосконалену концепцію, яка містить відповідні механізми захисту і також відповідає згаданому стандарту.

Для дослідження процесу доступу до ІСКЗ запропоновано марковську модель залежності функціональної спроможності ІСКЗ від впливу негативних факторів. Модель визначає множину станів ІСКЗ та дозволяє отримати аналітичні вирази для розрахунку імовірностей перебування ІСКЗ у відповідних станах у вибрані моменти часу зважаючи на імовірності появи негативних факторів та налаштування підсистеми розмежування доступу. Як похідний науковий результат отримано залежності перебування ІСКЗ в функціональному стані від імовірностей появи негативних факторів, здійснено оцінювання граничної тривалості функціонування ІСКЗ під впливом негативних факторів, досліджено швидкості зменшення імовірності перебування ІСКЗ у функціональному стані в залежності від параметрів налаштувань підсистеми розмежування доступу. Для практичного застосування моделі розроблено відповідну методику, яка дозволила, зокрема, підтвердити адекватність моделі використовуючи стандартні методи теорії планування експерименту, зокрема, за критерієм Фішера.

В розділі описано єдиний підхід для математичного моделювання інформаційних процесів ІСКЗ в рамках глобальної, дискреційної і локальної політик безпеки із прив’язкою до ієрархічної структури профільної системи із об’єктно-реляційною моделлю організації управління інформаційними ресурсами, що дозволяє виконувати аналіз і синтез сервісів підтримки ролей користувачів із можливістю їх інтеграції, індукування та сумісності в межах системної політики безпеки, контролювати цілісність інформації та автентичність статичного і динамічного доступу до неї. Синтезовано методи оптимізації роботи блоків оброблювання даних і розмежування доступу, які відповідають за контроль цілісності інформації та автентичність доступу до неї, відповідно. Формалізовано метод і критерій динамічного контролю цілісності інформації, який базується на математичному апараті напівмарковських мереж і комплексно стохастично описує дискретні стани контролю цілісності інформації на вибраних ієрархічних рівнях ІСКЗ під час неперервного дискреційного доступу. Метод дозволяє вибрати максимальні допустимі значення коефіцієнтів контролю цілісності інформації на рівнях ієрархічної структури ІСКЗ зважаючи на попередньо заданий обсяг контрольованої інформації, допустиму швидкість контролю її цілісності та максимальну тривалість перебування системи у відповідному стані. Формалізовано метод контролю доступу до інформаційних

процесів модельованої оцінною мережею Петрі ІСКЗ із ієрархічною структурою. Інформаційні процеси представлено відповідними контурами із інтегрованою множиною класифікаторів, які фіксують факти перевищення зваженими ступенями ідентичності суб'єкта-актора порогових значень, встановлених для відповідних класів інформаційних загроз, що ініціює описані у системній політиці безпеки реакції. На нижніх зображеннях на рис. 9 наведено залежність функціонального критерію контролю цілісності від відносної кількості контрольованої на цілісність інформації для процесів резервного копіювання та інформаційного пошуку. Функціональний критерій характеризує здатність інформаційної системи одночасно підтримувати всі функціональні сервіси та заданий рівень контролю цілісності даних при граничній середній тривалості процесу τ_m і граничній середній тривалості довільного стану напівмарковського процесу контролю цілісності K_{max}.

В розділі запропоновано комплекс керованих напівмарковських моделей, які описують динаміку процесу функціонування ІСКЗ як системи із багатьма станами, у напівмарковському описі якої узгоджуються стани, описувані різними розподілами, що дозволило формалізувати оцінювання максимуму функції правдоподібності та параметрів напівмарковського процесу, який описує експлуатації ІСКЗ, для різнотипних розподілів його станів, ідентифікувати функції марковського відновлення і напівмарковської перехідної матриці цього процесу, сформулювати вирази для: - розрахунку правдоподібності для нецензурованих і цензурованих визначених відрізків напівмарковських процесів із однією та багатьма траєкторіями розвитку процесу функціонування ІСКЗ; - оцінювання максимальної правдоподібності і оцінювання параметрів вихідного класу розподілів, базових для визначеного напівмарковського процесу; оцінювання таких атрибутів та індикаторів гарантоздатності ІСКЗ як готовність, безвідмовність, обслуговуваність, інтенсивність відмов і напрацювання на відмову. На правому верхньому зображенні на рис. 9 наведено залежності емпіричного та змодельованого рівня атрибуту безвідмовності від часу.

В розділі представлено математичну модель залежності втрат конфіденційності процесу автентифікації і показника готовності ІСКЗ. Модель формалізована як задача математичного програмування і дозволяє визначити процес оптимальної напівмарковської стратегії управління прийняттям рішень у марковському процесі надання доступу авторизованим суб'єктам в залежності від їх ролей. Прикладним результатом застосування цієї моделі є мінімізація втрат готовності ІСКЗ з врахуванням встановленного адміністратором порогового значення для параметра конфіденційності системи. Сформульовано методику застосування вищеописаної моделі зважаючи, що у системній політиці безпеки описано ситуації «критична помилка» і «підозра на помилку», які можуть ідентифікуватися відповідною підсистемою під час перебігу процесу надання доступу авторизованим суб'єктам. На лівому верхньому зображенні на рис. 9 представлено залежність середнього емпіричного значення атрибуту готовності d_e від граничного значення втрати конфіденційності α та задіяних в системі захисту типів класифікаторів. При значення α>7% конкуренція досліджуваних атрибутів припиняється.

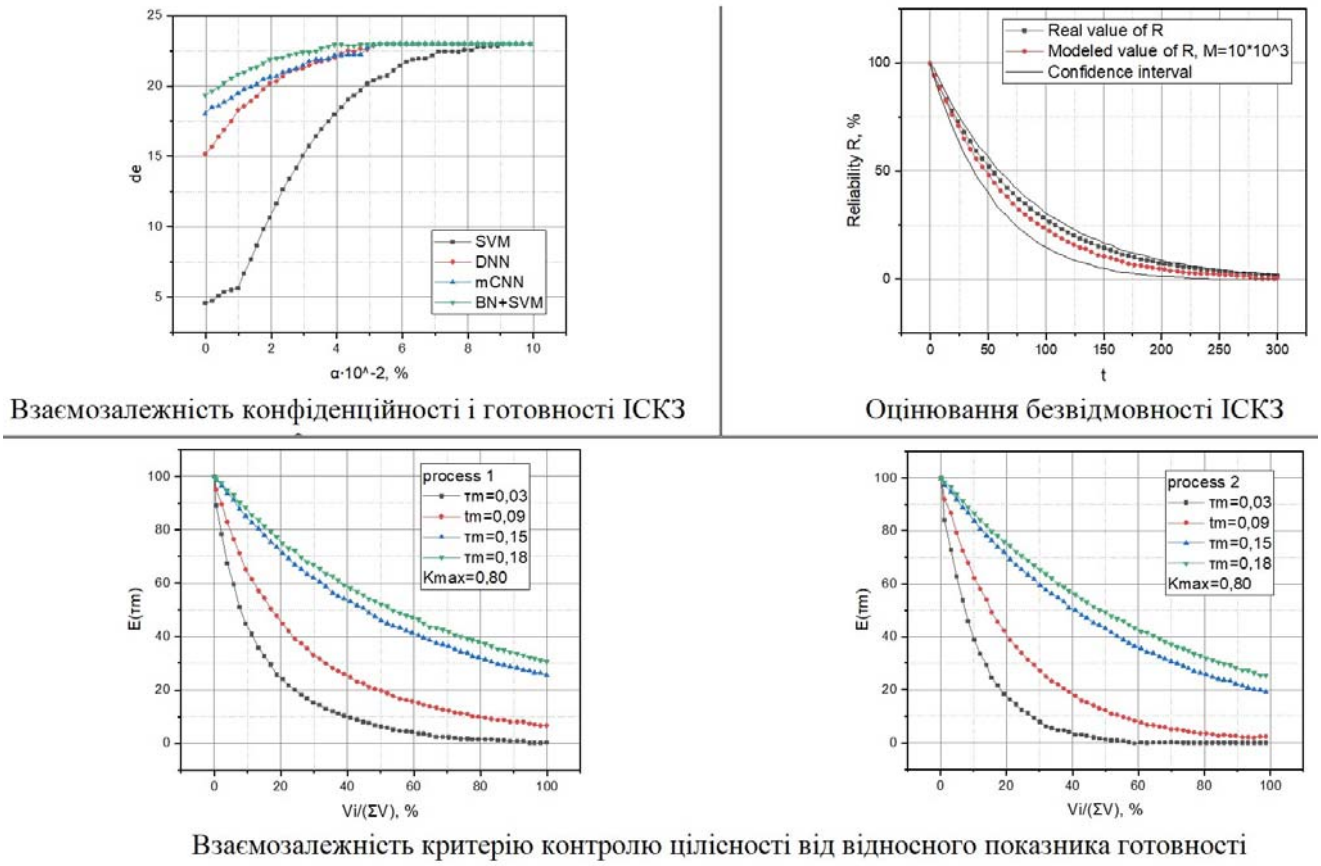

Рисунок 9 – Вибрані результати експериментів з оцінювання взаємозалежності атрибуту гарантоздатності ІСКЗ.

В загальному вигляді готовність ІСКЗ передбачає виділення авторизованому суб'єкту у відповідь на його вхідний запит ресурсів інформаційного середовища ІСКЗ, скінченний обсяг яких узагальнено поняттям «віртуальна машина». Архітектурна організація ІСКЗ передбачає, що віртуальні машини можуть створюватися: - у інформаційному середовищі сервера-реєстраційного центру; - у інформаційному середовищі серверів даних; - в обох цих інформаційних середовищах одночасно. Обмеження готовності пов'язано із відсутністю вільних ресурсів у ІСКЗ для створення нових віртуальних машин за запитом авторизованого суб'єкта, що призводитиме до тимчасового відхиленні нових вхідних запитів для здійснення сервісних операцій з вивільнення системних ресурсів. В розділі представлені математичні моделі управління готовністю ІСКЗ які враховують її топологічні особливості та перебіг її сервісних операцій при управлінні доступом авторизованих суб'єктів до інформаційного середовища системи і формалізують зв'язок множини сервісних операцій із множиною відповідей системи на запити авторизованих суб'єктів у вигляді керованого напівмарковського процесу із резервуванням ресурсів на заходи самоубезпечення, що дозволяє за допомогою апарату математичного програмування розраховувати оптимальну стратегію управління готовністю ІСКЗ із мінімізацією витрат на її функціонування та розрахувати стохастичну оцінку готовності системи. Представлені на рис. 10 ліворуч UML-діаграми характеризують напівмарковський процес переходу досліджуваної системи в

наступний стан в залежності від активної сервісної операції, привілей авторизованого суб'єкта та його потреб, виражених у бажаній кількості віртуальних машин. Праворуч на рис. 10 представлено аналітично обґрунтовану стратегію управління готовністю у вигляді залежності імовірності надання доступу $p(s,\alpha)$ від поточного стану системи s, коефіцієнта пріоритетності μ і персоніфікованої кількості віртуальних машин α.

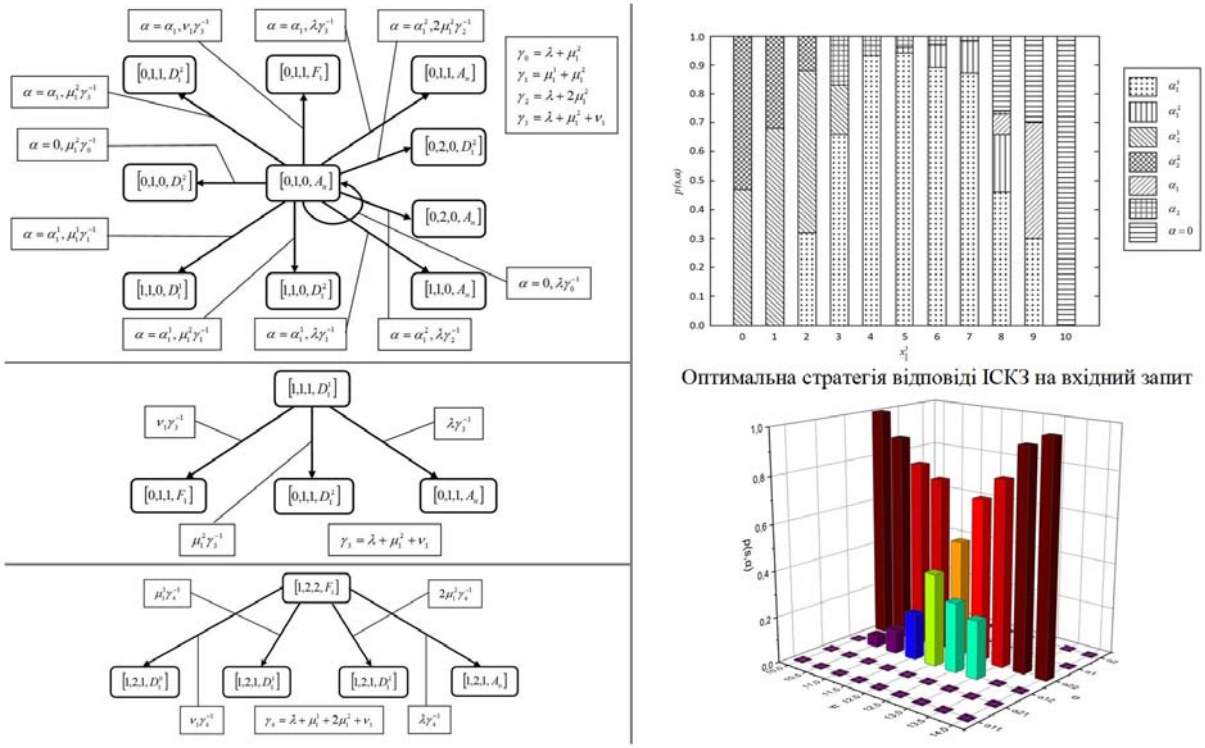

Рисунок 10 – Вибрані результати оцінювання атрибуту готовності ІСКЗ.

В розділі описані моделі функційної безпечності (ФБ) і живучості ІСКЗ у формалізмі марковських моделей. В моделі ФБ досліджувану ІСКЗ представлено структурованою множиною зв'язаних підсистем, кожна з яких характеризується інтенсивністю небезпечних збоїв і інтенсивністю відновлення ФБ. Модель дозволяє оцінити імовірність перебування ІСКЗ в кожному із множини станів, які описують доступні конфігурації збоїв підсистем ІСКЗ із урахуванням вищевказаних їх характеристик. Також сформульовано метод редукції структурної моделі ФБ ІСКЗ, який вводить індикатори вагомості, названі ступенями, для всіх станів останньої. Розрахувавши значення ступенів всіх станів моделі ФБ ІСКЗ можна спрощувати структуру вихідної моделі на етапі проектування, вилучаючи стани, ступінь яких менший вибраного порогового значення. Також створено модель живучості, яка дозволяє оцінити значення введеної таксономії атрибутів живучості для активного сеансу суб'єкт-системної взаємодії, під час якого можливе виникнення визначених типів збоїв. При створенні моделі живучості враховано архітектуру ІСКЗ та налаштування системної політики безпеки тощо. Адекватність запропонованих моделей і методу доведено результатами експериментів, у яких модельовані характеристики порівнювалися із емпіричними за значенням середньоквадратичного відхилення. Окремі результати цих експериментів

представлені на рис. 11. Зокрема, праворуч на рис. 11 представлено отриману для цільової інформаційної системи залежність імовірності відновлення активної віртуальної машини після збою від часу і вмісту кортежу, який описує збій, та залежність між емпіричним і модельованим значеннями накопичувальної середньої тривалості відновлення віртуальної машини після збою.

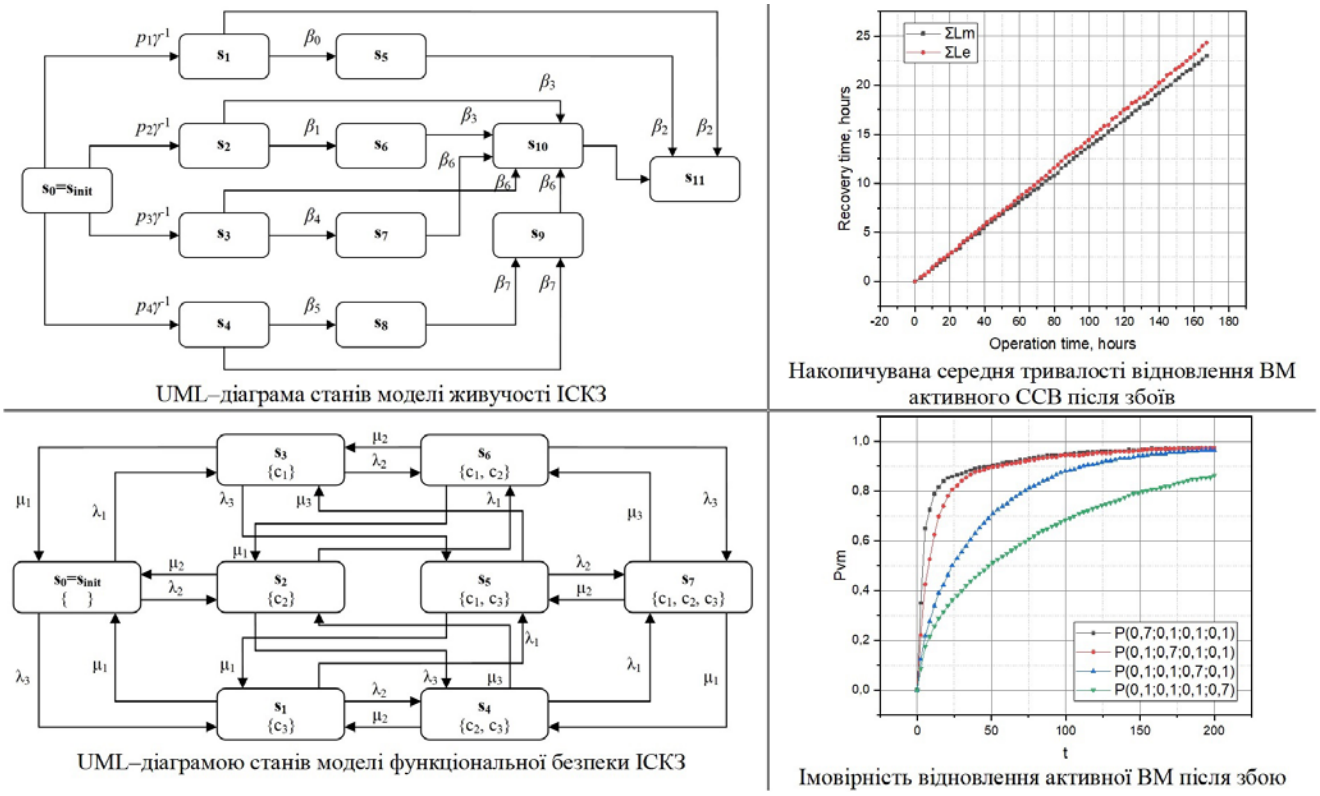

Рисунок 11 – Вибрані результати оцінювання атрибутів живучості та функційної безпечності ІСКЗ.

Загалом в розділі формалізовано систему марковських, напівмарковських і керованих напівмарковських моделей конфіденційності, цілісності, готовності, функційної безпечності, живучості та безвідмовності, що дозволяє поставити розв'язувану задачу математичного програмування для знаходження екстремального значення обраного атрибуту гарантоздатності та дослідити взаємозалежність «рівень конфіденційності»-«цілісність» та «рівень конфіденційності»-«готовність» для цільової екземпляру класу ІСКЗ.

В **шостому розділі** представлено аналітичні методи обчислення характеристичних параметрів моделей індивідуальності голосу для досліджуваних екземплярів мовленнєвих сигналів. Отримано адаптації цих методів залежно від того, відома чи не відома апріорна інформація щодо значень усталених параметрів моделей ІГМС для досліджуваного екземпляру мовленнєвого сигналу. Синтезовано інформаційну технологію автентифікації суб'єкта за індивідуальністю голосу в мовленнєвому сигналі та узагальнений метод і інформаційну технологію для оптимізації обраного атрибуту гарантоздатності цільової інформаційної системи критичного застосування.

Представлено орієнтований на прикладне застосування метод аналітичного розрахунку таких обов'язкових характеристичних параметрів моделей

індивідуальності голосу у мовленнєвому сигналі, як амплітуди несних гармонік. Метод у матричній формі однозначно узагальнює послідовність обчислювальних операцій для розрахунку амплітуд несних гармонік для фонограми емпіричного мовленнєвого сигналу, представленого послідовністю значень авто- або кореляційної функції в залежності від виду вживаної для його опису моделі ІГМС, її усталених параметрів і похибки. Досвід практичної експлуатації методу показав, що квазідетермінованим моделям ІГМС властива порівняно невисока обчислювальна складність і менша похибка опису досліджуваного мовленнєвого сигналу із високим ступенем вокалізації вмісту за рахунок врахування серед усталених параметрів моделей початкових фаз несного і модулювального коливань. Водночас, стохастичні моделі ІГМС дозволяють із прийнятною достовірністю описувати фрагменти мовленнєвих сигналів із низьким ступенем вокалізації вмісту та присутністю шумів. Також для аналізу описів, триманих за допомогою стохастичних моделей ІГМС, можна застосовувати потужний математичний апарат теорії імовірності і математичної статистики.

Для оцінювання одного із характеристичних параметрів моделей ІГМС – частоти основного тону, синтезовано аналітичні методи, які є удосконаленими версія класичних кореляційного і спектрального методів. В удосконалених методах узагальнюється інформація про значення коефіцієнта кореляції досліджуваного мовленнєвого сигналу для послідовності сусідніх інтервалів стаціонарності останнього, що разом із апріорно визначеним частотним діапазоном дозволяє зменшити кількість локальних мінімумів функції кореляції і, відповідно, збільшити імовірність визначення глобального мінімуму, позиція якого визначає оцінку основного тону. Спрямоване на підвищення достовірності і надійності оцінки частоти основного тону удосконалення кореляційного методу полягає в попередній фільтрації мовленнєвого сигналу із подальшим розрахунком характеристики, оберненої усередненому часовому інтервалу між першими (від двох до шести) сусідніми максимумами функції кореляції. Здійснене з тією ж метою удосконалення спектрального методу оцінювання частоти основного тону і обертонів мовленнєвого сигналу полягає в змістовному представленні досліджуваного мовленнєвого сигналу нормованою спектральною щільністю потужності, розрахованою за методикою кореляційних вікон. Досягнута достовірність оцінки частоти основного тону удосконаленими методами перевищує результати, продемонстровані методом на основі вейвлет-перетворення (на ~40%) і класичними амплітудним, кореляційним, спектральним методами (понад на порядок).

Дослідження взаємозв’язку між достовірністю оцінювання характеристичних параметрів моделі ІГМС і наявністю апріорної інформації про усталені параметри моделі дозволило формалізувати орієнтований на практичне застосування метод оцінювання частоти основного тону на основі визначення позиції глобального максимуму нормованого на максимальне значення логарифмічного функціоналу відношення правдоподібності оцінки частоти основного тону, апостеріорний розподіл якої для досліджуваного мовленнєвого сигналу визначався баєйсівським методом. Вихідною інформацією для методу є амплітуди і початкові фази несних гармонік. На значення визначеної за

допомогою представленого методу дисперсії оцінки частоти основного тону впливає рівень відношення «сигнал»/«шум», тривалість вокалізованого сегменту, кількість амплітуд несних гармонік тощо. Емпіричне оцінювання достовірності отримуваної за допомогою представленого методу оцінки частоти и основного тону показало результати, які збігаються із продемонстрованими удосконаленими версіями кореляційного і спектрального методів. Подальшим розвитком теоретичної бази методу оцінювання частоти основного тону на основі визначення позиції глобального максимуму нормованого на максимальне значення логарифмічного функціоналу відношення правдоподібності став метод визначення цієї ж характеристики в умовах відсутності апріорної інформації щодо значень усталених параметрів формалізованого моделлю ІГМС опорного сигналу. Емпіричне оцінювання достовірності отримуваної за допомогою представленого методу оцінки частоти и основного тону показало результати, які збігаються із продемонстрованими удосконаленими версіями кореляційного і спектрального методів. Втім, універсальність цього методу супроводжується найвищою серед представлених методів оцінювання частоти основного тону обчислювальною складністю.

На рис. 12 наведено структурну схему інформаційної технології автентифікації суб'єкта за індивідуальністю голосу.

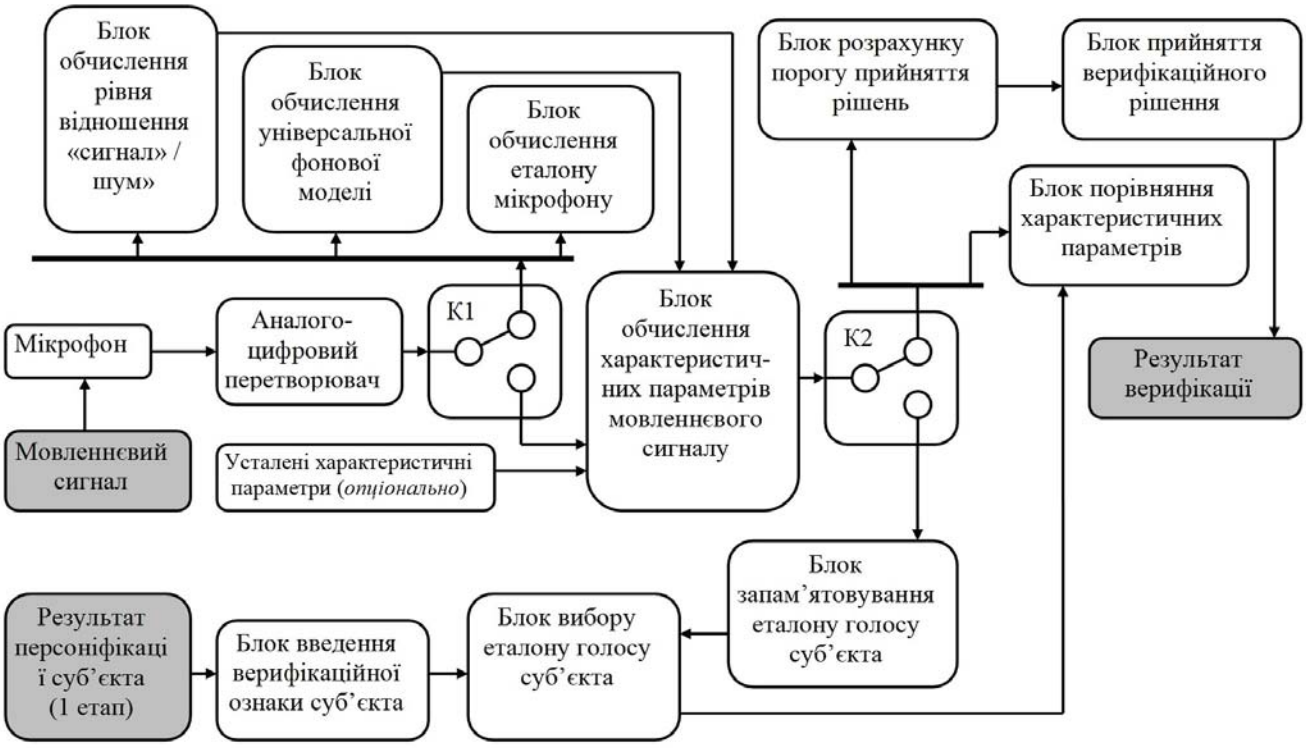

Рисунок 12 – Інформаційна технологія автентифікації суб'єкта за індивідуальністю голосу в мовленнєвому сигналі.

Комутатор *K1* переключає систему між режимом налаштування параметрів в режимом навчання або верифікації. В режимі навчання персоніфіковані фонограми парольних мовленнєвих сигналів потрапляють до блоку обчислення характеристичних параметрів, розрахована множина яких передається до блоку запам'ятовування еталону голосу. В режим верифікації система переводиться

переключенням комутатора *K2* в верхню позицію. Суб'єкт, який успішно подолав перший етап двохетапної схеми авторизації, виголошує у мікрофон запропоновану блоком запам'ятовування голосу парольну фразу. Далі у блоці порівняння характеристичних параметрів на основі значення міри розрізнення і порогу приймається верифікаційне рішення щодо надання доступу суб'єкту, який авторизується.

Представлена на рис. 13 UML-діаграма активності впорядковує процеси в інформаційній технології автентифікації суб'єкта за індивідуальністю голосу. Спочатку для нормованого мовленнєвого сигналу розраховуються значення кореляційних коефіцієнтів, які використовуються у блоці розрахунку частоти основного тону, та, разом із нею, передаються до блоку, де розраховуються амплітуди несних гармонік. Завершує процедуру параметризації сигналу блок ділення амплітуд несних гармонік на еталон АЧХ мікрофону. Верифікаційне рішення є результатом порівняння значення міри розрізнення із порогом.

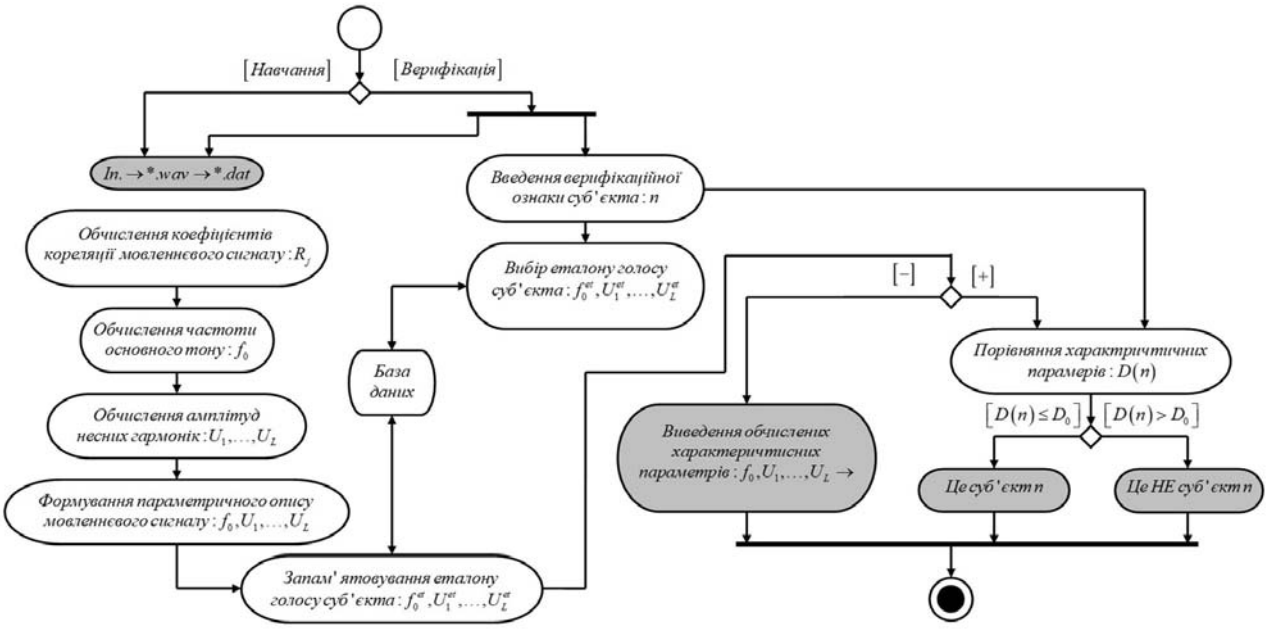

Рисунок 13 – Інформаційна технологія автентифікації суб'єкта за індивідуальністю голосу в мовленнєвому сигналі в динаміці.

Інформаційна технологія автентифікації суб'єкта за індивідуальністю голосу інтегрується в інформаційну технологію для підвищення обраного атрибуту гарантоздатності інформаційної системи критичного застосування, візуальна інтерпретація якої представлена на рис. 14. Якщо про підвищення атрибуту конфіденційність вже сказано, то концепції підвищення решти атрибутів базуються на профільних моделях марковського опису процесів в інформаційній системі критичного застосування. Конкуруючий щодо використання обчислювальних ресурсів характер атрибутів конфіденційності, цілісності та готовності описано відповідною моделлю. Враховуючи спільний математичний апарат, прикладне застосування створених профільних моделей реалізується через узагальнений метод підвищення обраного атрибуту гарантоздатності.

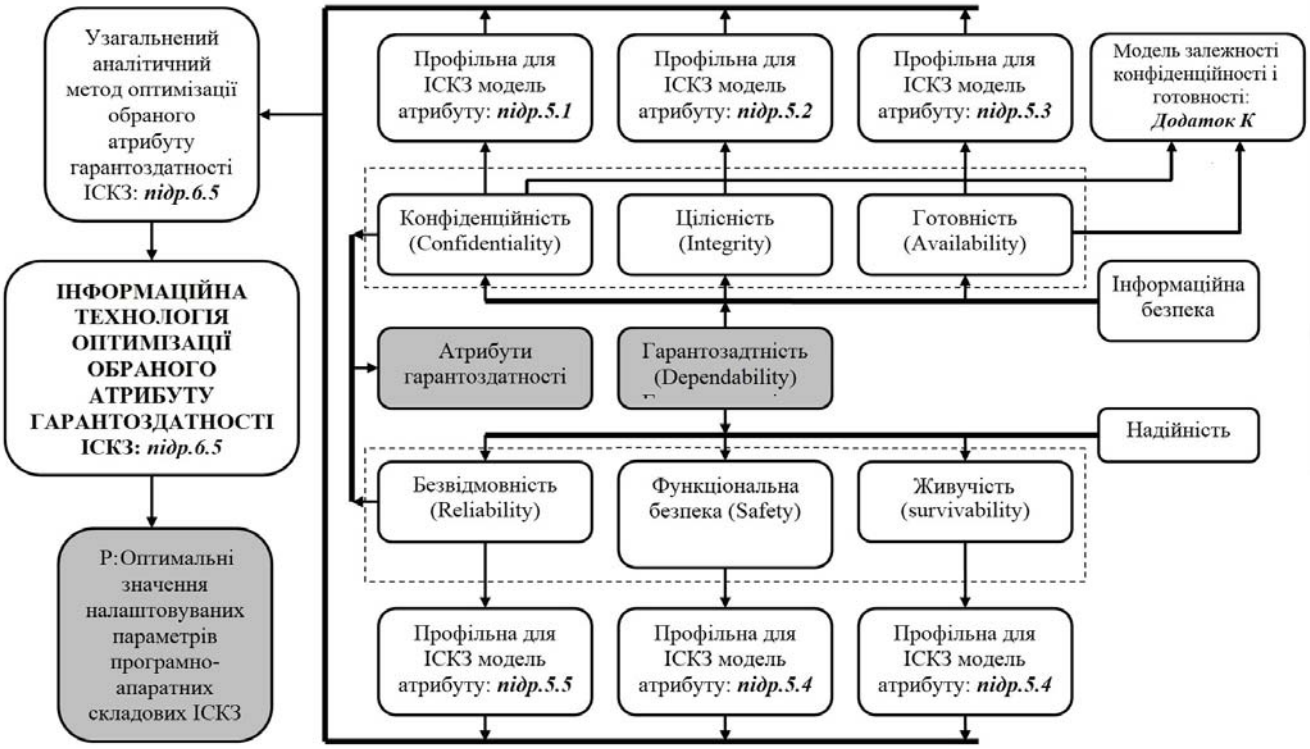

Рисунок 14 – Інформаційна технологія для підвищення обраного атрибуту гарантоздатності ІСКЗ.

На ліворуч на рис. 15 представлено узагальнену UML-діаграму активності інформаційної технології для підвищення обраного атрибуту гарантоздатності.

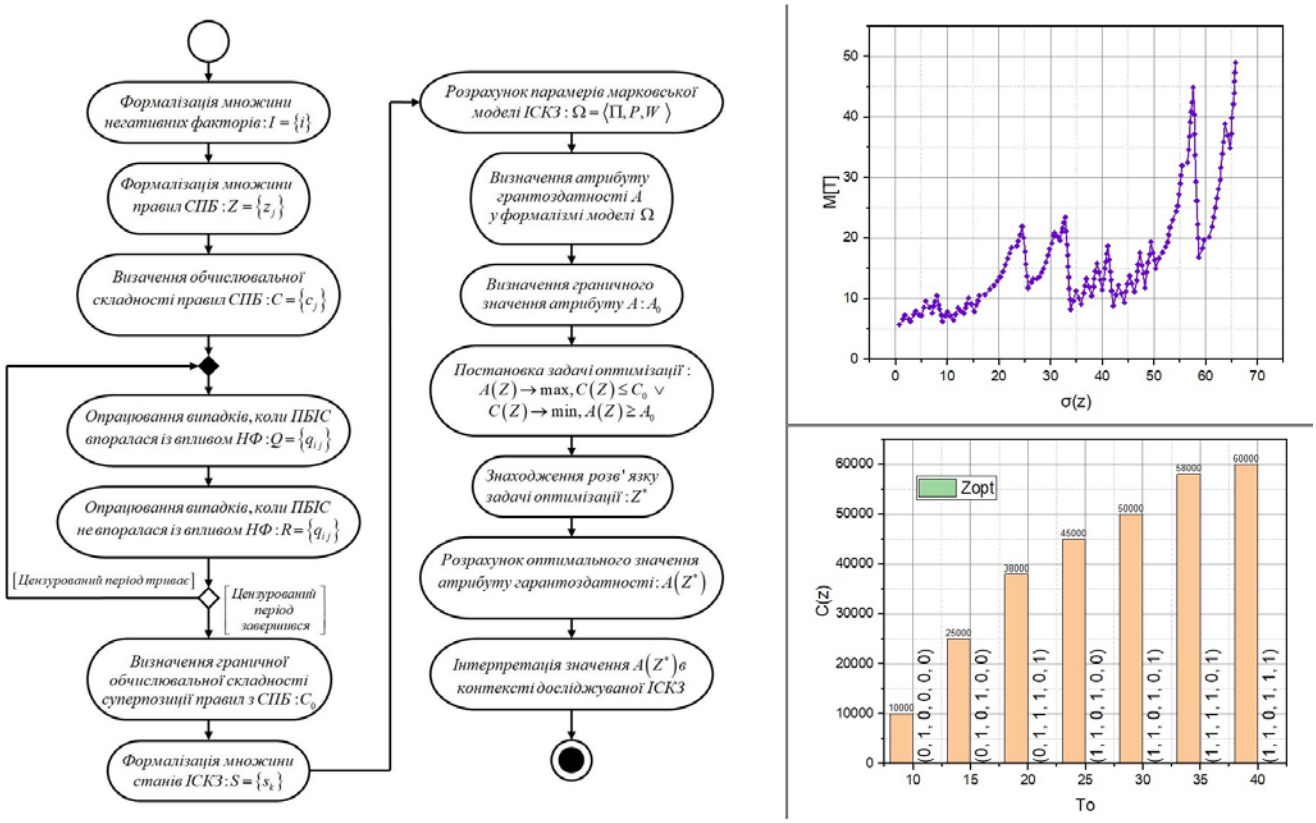

Рисунок 15 – Інформаційна технологія для підвищення обраного атрибуту гарантоздатності ІСКЗ в динаміці.

Праворуч наведені прикладні результати адаптації інформаційної технології для цільової інформаційної системи Ситуаційного центру Вінницької міської ради. Для протидії впливу негативних факторів сформульовано шість правил, які регламентують налаштування захисних механізмів, зокрема, для автентифікації суб'єкта за голосом. На верхньому зображенні візуалізовано залежність середнього часу до відмови від індексу суперпозиції правил, яку активує система захисту. На нижньому зображенні представлено склад і обчислювальну складність оптимальних суперпозицій правил як результатів розв'язків задач оптимізації типу *OT2* для цільової інформаційної системи при заданих значеннях часу до відмови. В розділі на прикладі ІСКЗ Ситуаційного центру департаменту інформаційних технологій Вінницької міської ради представлено повний цикл аналітичних операцій для реалізації інформаційної технології автентифікації суб'єкта за індивідуальністю голосу в мовленнєвому сигналі, яка визначає рівень конфіденційності цільової ІСКЗ, та для реалізації узагальненої інформаційної технології для оптимізації обраного атрибуту гарантоздатності цільової ІСКЗ.

Також в розділі представлені результати впровадження запропонованих інформаційних технологій в таких установах і підприємствах як Innovative Institute for Material Studies of Intel Research Practice (USA, військова сфера), ARS Online OÜ (a part of the Advertising Agencies Industry, Estonia, фінансова сфера), Відділ розпізнавання та синтезу звукових образів Міжнародного науково–навчального центру інформаційних технологій та систем НАН України та МОН України (м. Київ, науково-дослідна сфера), Хмельницьке міське комунальне підприємство «Хмельницькінфоцентр» (м. Хмельницький, урядова сфера), Львівське комунальне підприємство «Міський центр інформаційних технологій» (м. Львів, урядова сфера), Департамент інформаційних технологій ВінМР (Ситуаційний центр) (м. Вінниця, урядова сфера), КП «Вінницький інформаційний центр» (м. Вінниця, урядова сфера), ДОЗК Він. ОДА МОЗ України «Вінницький обласний центр медико–соціальної експертизи» (м. Вінниця, сфера охорони здоров'я), КНП ДОЗ Він. МР «Центр первинної медико-санітарної допомоги №3» (м. Вінниця, сфера охорони здоров'я), ТОВ «Агро-помсервіс» (м. Вінниця, комерційна сфера), ТОВ «Вінницяелектроконтакт» (м. Немирів, комерційна сфера). Впровадження якісно характеризувалися за значеннями таких показників як: – узагальнена характеристика конфіденційності P_α, P_β (усереднені імовірності виникнення похибок першого і другого роду в процесі автентифікації суб'єктів-користувачів інформаційної системи цільової установи за їх голосами за цензурований час експлуатації останньої); – узагальнена характеристика готовності A (відношення часу штатного функціонування інформаційної системи цільової установи до цього ж часу із додаванням часу, коли система перебувала в нефункціональному стані з причин, які стосуються атрибутів готовності та цілісності останньої); – узагальнена характеристика обслуговуваності S (відношення часу штатного функціонування інформаційної системи цільової установи до цього ж часу із додаванням часу, коли система перебувала в нефункціональному стані з причин збоїв, обумовлених відхиленням від оптимального графіку рекомендованого оновлення її апаратних компонентів, розробленого на основі оцінок атрибутів гарантоздатності,

розрахованих за методами, описаними в підрозділі 5.5). Значення цих якісних характеристик для цільових ІСКЗ потрапити в діапазони: P_{α} = [0,13%; 2,43%], P_{β} = [0,97%; 3,33%], A = [0,91; 1,00], S = [0,74; 0,97]. В наведених у дисертації актах результати впровадження оцінено позитивно.

ВИСНОВКИ

Представлені у дисертаційній роботі результати досліджень присвячено моделюванню системних інформаційних процесів життєвого циклу ІСКЗ із біометричною автентифікацією суб'єктів-користувачів, зокрема, за голосом, з обов'язковим забезпеченням позитивної динаміки значень атрибутів гарантоздатності такого класу систем. Зокрема, синтезовано комплекс нових математичних моделей, які забезпечують об’єктивну формальну оцінку довільного екземпляру класу інформаційних систем критичного застосування в таксономії атрибутів гарантоздатності, а також підвищують його конфіденційність організацією доступу за схемою двофакторної верифікації із автентифікацією суб’єкта-користувача за голосом як другого фактора.

Узагальнення отриманих в процесі досягнення мети дисертаційної роботи результатів, спрямованих на: забезпечення конфіденційності ІСКЗ представлено на рис. 6.17; оптимізацію обраного атрибуту гарантоздатності ІСКЗ представлено на рис. 6.18. Відмітимо головні з них:

– створено інформаційну технологію автентифікації суб’єкта за індивідуальністю голосу в мовленнєвому сигналі в якій, на відміну від існуючих, представлений модулювальним і полігармонічним несним коливаннями мовленнєвий сигнал параметризується у просторі таких характеристичних параметрів як усереднена частота основного тону і амплітуди несних гармонік, формалізованих у методології квазідетермінованих і стохастичних моделей індивідуальності голосу;

– створено інформаційну технологію і узагальнений аналітичний метод для оптимізації обраного атрибуту гарантоздатності цільової інформаційної системи критичного застосування, якої описано у формалізмі методології марковських, напівмарковських і керованих напівмарковських моделей конфіденційності, цілісності, готовності, функційної безпечності, живучості та безвідмовності;

– формалізовано метод оцінювання рівня відношення «сигнал»/«шум» у емпіричному мовленнєвому сигналі, який розглядається як сума модулювального та полігармонічного несного коливань і білого шуму, параметризованих у формалізмі уточненої квазідетермінованої моделі індивідуальності голосу;

– формалізовано метод розрахунку порогу прийняття рішень в задачі верифікації суб’єкта за голосом і міри відстані між зваженими характеристичними параметрами еталонного і досліджуваного мовленнєвих сигналів, параметризованих у формалізмі методології моделей індивідуальності голосу, де при оцінюванні довірчих інтервалів варіювання значень характеристичних параметрів мовленнєвих сигналів враховується рівень відношення «сигнал»/«шум»;

– удосконалено модель процесу автентифікації суб’єкта машиною опорних супер- та і-векторів за параметризованим представленням мовленнєвого

матеріалу із шумом, опрацьованого мультиваріантним методом компенсування шумів у парольному мовленнєвому сигналі з варіативним описом характеристичних параметрів моделлю сумішей гаусівських розподілів;

– удосконалено метод адаптації згорткової нейромережі для автентифікації суб'єкта за мовленнєвим матеріалом із шумом, в якому, на відміну від існуючих, перший, згортковий, шар інтегровано з банком фільтрів Габора із параметризацією вхідної спектрограми в формалізмі спектрально-темпоральних рецептивних полів.

Представлена в роботі узагальнена інформація щодо впровадження теоретичних і прикладних результатів дисертаційного дослідження підтверджує позитивну динаміку узагальнених характеристик конфіденційності, готовності та обслуговуваності інформаційних систем критичного застосування як вітчизняних, так і закордонних цільових установ , зокрема, Innovative Institute for Material Studies of Intel Research Practice (USA); ARS Online OÜ (a part of the Advertising Agencies Industry, Estonia); Polski Dom Nowych Mediów (Poland); відділі розпізнавання та синтезу звукових образів Міжнародного науково-навчального центру інформаційних технологій та систем НАН України та МОН України (м. Київ); хмельницькому міському комунальному підприємстві «Хмельницькінфоцентр» (м. Хмельницький); львівському комунальному підприємстві «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).

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

[1] В. В. Ковтун, М. М. Биков, та Н. Г. Савінова, «Надійний метод виділення складових сегментів у мовленнєвому сигналі.» *Наукові праці Вінницького національного технічного університету*, №1, 2007. [Електронний ресурс]. Доступно: https://trudy.vntu.edu.ua/ index.php/trudy/article/view/19/19. Дата звернення: Серпень 26, 2020.

[2] В. В. Ковтун, М. М. Биков, та Н. Г. Савінова, «Оцінювання впливу завад на достовірність роботи інформаційно-вимірювальної системи розпізнавання голосу.» *Наукові праці Вінницького національного технічного університету*, № 3, 2009. [Електронний ресурс]. Доступно: https://trudy.vntu.edu.ua/ index.php/trudy/article/view/149/148. Дата звернення: Серпень 26, 2020.

[3] В. В. Ковтун, М. М. Биков, та А. Раїмі, «Метод виділення основного тону на основі модифікованої математичної моделі слухової системи людини,» *Вісник Вінницького політехнічного інституту,* № 5, с. 130–135, 2011.

[4] В. В. Ковтун, М. М. Биков, та Н. Г. Савінова, «Оцінювання метрологічних характеристик інформаційно-вимірювальної системи автоматизованого розпізнавання голосів,» *Вісник Вінницького політехнічного інституту*, № 6, с. 189–193, 2011.

[5] В. В. Ковтун, М. М. Биков, та Н. Г. Савінова, «Аналіз стану проблеми розробки ефективних систем пошуку ключових слів,» *Вісник Вінницького політехнічного інституту*, № 1. с. 179–181, 2012.
[6] В. В. Ковтун, М. М. Биков, та К. Конате, «Метод підвищення ефективності роботи пам'яті в системах пошуку ключових слів у мовленнєвому сигналі,» *Вісник Вінницького політехнічного інституту*, № 2, с. 159–162, 2012.
[7] В. В. Ковтун, та М. М. Биков, «Оцінювання надійності автоматизованих систем розпізнавання мовців критичного застосування,» *Вісник Вінницького політехнічного інституту*, № 2, с. 70–76, 2017.
[8] В. В. Ковтун, та М. М. Биков, «Використання множини мікрофонів у автоматизованій системі розпізнавання мовця критичного застосування,» *Вісник Вінницького політехнічного інституту*, № 3, с. 84–91, 2017.
[9] В. В. Ковтун, М. М. Биков, та А. Д. Гафурова, «Дослідження комітету нейромереж у автоматизованій системі розпізнавання мовців критичного застосування,» *Вісник Хмельницького національного університету, серія: Технічні науки*, № 2(247), с. 144–150, 2017.
[10] В. В. Ковтун, М. М. Биков, А. О. Береза, та А. Д. Гафурова, «Оптимізація алфавіту інформативних ознак для автоматизованої системи розпізнавання мовців критичного застосування,» *Вісник Хмельницького національного університету, серія: Технічні науки*, № 3(249), с. 222–228, 2017.
[11] В. В. Ковтун, та М. М. Биков, «Метод представлення ознак у автоматизованій системі розпізнавання мовця критичного застосування,» *Вісник Хмельницького національного університету, серія: Технічні науки*, № 5(253), с. 112–120, 2017.
[12] В. В. Ковтун, та М. М. Биков, «Дослідження ефективності ознак розпізнавання мовців при використанні згортальних нейромереж,» *Оптико-електронні інформаційно-енергетичні технології*, № 2(32), с. 22–28, 2016.
[13] В. В. Ковтун, М. М. Биков, та О. О. Максимов, Детектування мовленнєвої активності в автоматизованій системі розпізнавання мовця критичного застосування. *Журнал інженерних наук*, Т. 4, № 1, 2017. [Електронний ресурс]. Режим доступу: http://jes.sumdu.edu.ua/wp-content/uploads/2017/11/JES_2017_01_H14-H20.pdf Дата звернення: Серпень 26, 2019.
[14] V. V. Kovtun et al, "Research of neural network classifier in speaker recognition module for automated system of critical use," *Proc. SPIE Photonics Applications in Astronomy, Communications, Industry, and High Energy Physics Experiments*, 1044521, August 7, 2017. doi:10.1117/12.2280930.
[15] В. В. Ковтун, та Т. В. Грищук, «Підвищення шумостійкості автоматизованої системи розпізнавання мовця критичного застосування,» *Вісник Вінницького політехнічного інституту*, № 1, с. 98–111, 2018.
[16] В. В. Ковтун В.В., О. В. Бісікало, та Т. В. Грищук, «Оптимізація класифікатора автоматизованої системи розпізнавання мовця критичного застосування,» *Радіоелектроніка, інформатика, управління*, № 2, с. 30–43, 2018. doi:10.15588/1607-3274-2018-2-4.

[17] В. В. Ковтун, та М. М. Биков, «Підвищення інформативності основного тону для розпізнаванні мовців згортальними нейромережами,» *Оптико-електронні інформаційно-енергетичні технології*, № 2(34). с. 44–51, 2017.
[18] В. В. Ковтун, «Оцінювання основного тону у автоматизованій системі розпізнавання мовця критичного застосування,» *Вісник Вінницького політехнічного інституту*, №4. с. 61-73, 2018.
[19] V. V. Kovtun et al, "Neural network modelling by rank configurations," *Proc. SPIE Photonics Applications in Astronomy, Communications, Industry, and High Energy Physics Experiments*, 1080821, 2018. doi: 10.1117/12.2501521.
[20] V. V. Kovtun, I. D. Ivasyuk, A. Kotyra, and A. Mussabekova, "The automated speaker recognition system of critical use," *Proc. SPIE Photonics Applications in Astronomy, Communications, Industry, and High Energy Physics Experiments*, 108082V, 2018. doi: 10.1117/12.2501688.
[21] В. В. Ковтун, «Концепція впровадження автоматизованої системи розпізнавання мовця у процес автентифікації для доступу до критичної системи,» *Вісник Вінницького політехнічного інституту*, № 5, с. 41–52, 2018. doi:10.31649/1997-9266-2018-140-5-41-52.
[22] V. V. Kovtun, O. V. Bisikalo, M. S. Yukhimchuk, and I. F. Voytyuk, "Analysis of the automated speaker recognition system of critical use operation results," *Radio Electronics, Computer Science, Control*, № 4, pp. 71–84, 2018. doi:10.15588/1607-3274-2018-4-7.
[23] В. В. Ковтун, Т. В. Грищук, та А. О. Береза, «Оцінювання надійності сеансу розпізнавання особи автоматизованою системою розпізнавання мовця критичного застосування,» *Вісник Хмельницького національного університету, серія: Технічні науки*, № 6(267, Т.1), с. 143–150, 2018. doi:10.31891/2307-5732-2018-267-6(1)-143-150.
[24] В. В. Ковтун, та А. Д. Гафурова, «Нейромережева адаптація PLDA для використання у автоматизованій системі розпізнавання мовця критичного застосування,» *Вісник Хмельницького національного університету, серія: Технічні науки*, № 1(269, Т.1), с. 172–178, 2019. doi:10.31891/2307-5732-2019-269-1-172-177.
[25] V. V. Kovtun, O. V. Bisikalo, and M. S. Yukhimchuk, "Modeling the security policy of the information system for critical use," *Radio Electronics, Computer Science, Control*, № 1, pp. 132–149, 2019. doi:10.15588/1607-3274-2019-1-13.
[26] В. В. Ковтун, «Моделювання залежності конфіденційності автентифікації і доступності у інформаційній системі критичного застосування,» *Вісник Вінницького політехнічного інституту*, № 6, с. 77–89, 2018. doi: 10.31649/1997-9266-2018-141-6-77-89.
[27] В. В. Ковтун, «Моделювання доступності інформаційної системи критичного застосування,» *Вісник Вінницького політехнічного інституту*, № 1, с. 41–57, 2019. doi:10.31649/1997-9266-2019-142-1-41-57.
[28] V. V. Kovtun, M. S. Yukhimchuk, P. Kisała, A. Abisheva, and S. Rakhmetullina, "Integration of hidden markov models in the automated speaker recognition system for critical use," *Przeglad Elektrotechniczny*, № 1, pp. 178–182, 2019. doi:10.15199/48.2019.04.32.

[29] В. В. Ковтун, «Напівмарковське оцінювання гарантоспроможності інформаційної системи критичного застосування,» *Вісник Вінницького політехнічного інституту*, № 2, с. 61–77, 2019. doi:10.31649/1997-9266-2019-143-2-61-77.
[30] V. V. Kovtun, O. V. Bisikalo, and V. V. Sholota, “The Information System for Critical Use Access Process Dependability Modeling,” *Proc. 9th International Conference on Advanced Computer Information Technologies (ACIT)*, 5–7 June 2019. doi:10.1109/ACITT.2019.8780013.
[31] В. В. Ковтун, *Моделі атрибутів гарантоздатності інформаційної системи критичного застосування із автентифікацією суб’єкта за голосом* : монографія, Вінниця : ВНТУ, 2020.
[32] V. V. Kovtun et al, “Improvement of the learning process of the automated speaker recognition system for critical use with HMM-DNN component,” *Proc. SPIE*, 11176, 1117620, November 6, 2019. doi: 10.1117/12.2536888.
[33] V. V. Kovtun et al, “Research of Pareto-Optimal Schemes of Control of Availability of the Information System for Critical Use,” *Proc. 1st International Workshop on Intelligent Information Technologies & Systems of Information Security (IntelITSIS 2020)*. CEUR-WS, Vol. 2623, pp. 174–193, 2020. urn:nbn:de:0074-2623-0.
[34] Oleg Bisikalo, Viacheslav Kovtun, Oksana Kovtun, and Volodimir Romanenko, “Research of safety and survivability models of the information system for critical use,” *Proc. IEEE 11th International Conference on Dependable Systems, Services and Technologies (DESSERT),* pp, 7-13, 14–18 May 2020. doi: 978-1-7281-9957-3/20.

АНОТАЦІЯ

Ковтун В. В. **Інформаційні технології для підвищення гарантоздатності інформаційних систем критичного застосування із автентифікацією суб’єкта за голосом. – Кваліфікаційна наукова праця на правах рукопису.**

Дисертація на здобуття наукового ступеня доктора технічних наук за спеціальністю 05.13.06 «Інформаційні технології». – Вінницький національний технічний університет, Вінниця, 2020.

Дисертаційна робота орієнтована на підвищення гарантоздатності інформаційної системи критичного застосування з автентифікацією суб’єкта за голосом шляхом розроблення і реалізації методів і засобів для оптимізації такого класу систем за обраним атрибутом гарантоздатності. В роботі вперше запропоновано: - методологію квазідетермінованих і стохастичних моделей індивідуальності голосу; - метод оцінювання рівня відношення «сигнал»/«шум» в емпіричному мовленнєвому сигналі; - метод обчислення міри відстані між зваженими характеристичними параметрами еталонного і емпіричного мовленнєвих коливань; - методи дослідження взаємозалежності «рівень конфіденційності»-«цілісність» та «рівень конфіденційності»-«готовність»; - інформаційну технологію автентифікації суб’єкта за індивідуальністю голосу в мовленнєвому сигналі; - інформаційну технологію для оптимізації обраного атрибуту гарантоздатності цільової інформаційної системи критичного застосування. В роботі удосконалено: - модель процесу автентифікації суб’єкта

машиною опорних супер- та і-векторів за параметризованим представленням мовленнєвого матеріалу із шумом; - метод адаптації згорткової нейромережі для автентифікації суб'єкта за мовленнєвим матеріалом із шумом.

Ключові слова: інформаційна система критичного застосування навантаження, автентифікація суб'єкта за голосом, гарантоздатність, конфіденційність, цілісність, готовність, безвідмовність, функційна безпечність, живучість.

АННОТАЦИЯ

Ковтун В. В. **Информационные технологии для повышения гарантоспособности информационных систем критического применения с аутентификацией субъекта по голосу. – Квалификационная научная работа на правах рукописи.**

Диссертация на соискание ученой степени доктора технических наук по специальности 05.13.06 «Информациолонные технологии». – Винницкий национальный технический университет, Винница, 2020.

Диссертационная работа ориентирована на повышение гарантоспособности информационной системы критического применения с аутентификацией субъекта по голосу путем разработки и реализации методов и средств для оптимизации такого класса систем относительно выбранного атрибута гарантоспособности.

В работе впервые предложен(а): - информационная технология аутентификации субъекта на основе индивидуальных особенностей его голоса в которой, в отличие от существующих, представленный модулирующим и полигармоническим несущим колебаниями речевой сигнал параметризируется в пространстве характеристических параметров, формализованных в методологии квазидетерминированных и стохастических моделей индивидуальности голоса; - метод оценки уровня отношение «сигнал»/«шум» в эмпирическом речевом сигнале, в котором, в отличие от существующих, последний рассматривается как сумма модулирующего и полигармонического несущего колебаний и белого шума, параметризованных в формализме уточненной квазидетерминированной модели индивидуальности голоса; - метод вычисления расстояния между взвешенными характеристическими параметрами эталонного и эмпирического речевых сигналов, параметризованных, в отличие от существующих, в формализме моделей индивидуальности голоса, где при оценке доверительных интервалов варьирования значений характеристических параметров учитывается уровень отношения «сигнал»/«шум»; - информационную технологию для оптимизации выбранного атрибута гарантоспособности целевой информационной системы критического применения, для описания которой, в отличие от существующих, создана методология марковских, полумарковских и управляемых полумарковских моделей конфиденциальности, целостности, готовности, функциональной безопасности, живучести и безотказности; - методы исследования взаимозависимости «уровень конфиденциальности»-«целостность» и «уровень конфиденциальности»-«готовность». Усовершенствован(а): - модель

процесса аутентификации субъекта машиной опорных супер- и i-векторов на основе параметризованного представления речевого материала с шумом, обработанного, в отличие от существующих, мультивариантным методом компенсации шумов в парольной речевом сигнале с вариативным описанием характеристических параметров модели смесей гауссовских распределений; - метод структурного проектирования сверточной нейросети для аутентификации субъекта на основе речевого материала с шумом, в котором, в отличие от существующих, в первый, сверточный, слой интегрирован с банком фильтров Габора для параметризации входной спектрограммы каждого фрейма парольного речевого сигнала в формализме тории спектрально-темпоральных рецептивных полей.

Практическое значение диссертационного исследования обеспечивается: - методикой оптимизации набора характеристических параметров для аутентификации субъекта на основе индивидуальных особенностей его голоса; - методикой определения порога принятия решений в задаче аутентификации субъекта на основе речевого материала с шумом; - методикой регуляризации глубокой нейросети для принятия решений в задаче аутентификации субъекта на основе речевого материала с шумом; - концепцией двухфакторной аутентификации субъекта-пользователя с его верификацией на основе индивидуальных особенностей голоса в качестве второго фактора; - методикой определения политики безопасности программной составляющей информационной системы критического применения; - методикой оптимального резервирования вычислительных ресурсов на этапе проектирования информационной системы критического применения с учетом предварительно заданного уровня ее готовности; - методикой оценки характеристических параметров при описании речевых сигналов моделями индивидуальности голоса; - методикой и алгоритмами для оценки частоты основного тона на основе моделей индивидуальности голоса; - методикой и алгоритмами для оценки частоты основного тона, сформулированными в контексте наличия/отсутствия априорной информации о значениях предварительно определяемых параметров моделей индивидуальности голоса; - методикой редукции структурной модели функциональной безопасности информационной системы критического применения; - методикой и алгоритмом для оптимизации целевой информационной системы критического применения относительно выбранного атрибута гарантоспособности; - методикой выделения модулирующего колебания в речевом сигнале; - методикой верификации математической модели индивидуальности голоса на основе значения критерия, который учитывает коэффициент множественной корреляции; - методиками выбора типа и настроек классификаторов в зависимости от уровня отношение «сигнал»/«шум» в эмпирическом речевом сигнале; - методикой бустинга процесса обучения профильных классификаторов; - методикой оптимизации зависимости конфиденциальности процесса аутентификации и готовности информационной системе критического применения.

Ключевые слова: информационная система критического применения, аутентификация субъекта на основе индивидуальных особенностей его голоса,

гарантоспособность, конфиденциальности, целостности, готовности, функциональной безопасности, живучести и безотказности.

ABSTRACT

***Viacheslav Kovtun*. Information technologies for increasing the dependability of the information systems for critical use with person authentication by voice. – Qualified scientific work on the right of the manuscript.**

Thesis for a scientific degree of Doctor of Engineering in the specialty 05.13.06 «Information technologies». – Vinnytsia National Technical University, Vinnytsia, 2020.

The dissertation thesis is focused on increasing the dependability of an information system for critical use with person authentication by voice by developing and implementing methods and means for optimizing this class of information systems with respect to the selected attribute of dependability.

In the thesis for the first time: - the information technology of person-user authentication by voice in a speech signal is proposed in which, unlike existing, the speech signal presented by modulating and polyharmonic carrier fluctuations is parametrized in space of such characteristic parameters as average pitch frequency and amplitudes of carrier fluctuations in the methodology of quasi-deterministic and stochastic models of voice individuality; - A method for estimating the level of the signal-to-noise ratio in an empirical speech signal is proposed in which, unlike the existing ones, the last is considered as the sum of modulating and polyharmonic carrier fluctuations and white noise parameterized in the formalism of a refined quasi-deterministic voice individuality model; - A method for calculating the measure of the distance between the weighted characteristic parameters of the reference and empirical speech oscillations, parameterized, unlike the existing ones, in the formalism of the methodology of voice individuality models, where when estimating the confidence intervals for varying the values of the characteristic parameters of individuality of speech signals, the level of the signal-to-noise ratio is taken into account; - The information technology for optimization of the chosen attribute of dependability of a target information system for critical use is offered, for the description of which, unlike existing, the methodology of Markov, semi-Markov and managed semi-Markov models of confidentiality, integrity, availability, functional security, survivability, reliability are synthesized; - Methods of research of interdependence "level of confidentiality-to-integrity" and "level of confidentiality-to-readiness" are proposed in which, unlike existing ones, for competing attributes of dependability capacity presented in formalism of profile semi-Markov mathematical models, one-criterion optimization tasks are carried out are offered. Also improved: - The model of the process of person-user authentication by the machine of reference super- and i-vectors according to the parameterized representation of speech material with noise is processed; - Method of adaptation of an convolutional neural network for person-user authentication by speech material with noise.

Key words: information system for critical use, person authentication by voice, dependability, confidentiality, integrity, availability, safety, survivability, reliability.

Підписано до друку 01.02.2021 р. Формат 21х29.7 1/4.
Наклад 100 прим. Зам. № 2021-_____.
Віддруковано в комп'ютерному інформаційно-видавничому центрі
Вінницького національного технічного університету.
м. Вінниця, вул. Хмельницьке шосе, 95. Тел.: 65-18-06
Суб’єкт видавничої справи
серія ДК №3516 від 01.07.2009 р.