Вінницький національний технічний університет
Міністерство освіти і науки України

Кваліфікаційна наукова
праця на правах рукопису

КОВТУН В'ЯЧЕСЛАВ ВАСИЛЬОВИЧ

УДК 681.327.12

ДИСЕРТАЦІЯ

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

05.13.06 — інформаційні технології
Технічні науки

Подається на здобуття вченого ступеня доктора технічних наук

Дисертація містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело
_____ В. В. Ковтун

Науковий консультант Бісікало Олег Володимирович
доктор технічних наук, професор

Вінниця – 2020

АНОТАЦІЯ

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

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

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, 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. У актуальних вітчизняних і закордонних наукових роботах 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 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. 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 безпечгності, 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 має бути 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 відомих негативних факторів; – одночасно 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.

Наукова новизна отриманих результатів

Вперше: – Запропоновано 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, що дозволяє отримати компактний, інформативний і адекватний параметричний опис індивідуальності сегментів мовленнєвих сигналів із високим і помірним рівнем вокалізації; – Запропоновано метод оцінювання рівня відношення «сигнал»/«шум» у емпіричному мовленнєвому сигналі, в якому, на відміну від існуючих, останній розглядається як сума модулювального та полігармонічного несного коливань і білого шуму, параметризованих у формалізмі уточненої квазідетермінованої моделі індивідуальності голосу, що, на відміну від існуючих, дозволяє визначати рівень шуму як у вокалізованих, так і у невокалізованих сегментах мовленнєвих сигналів; – Запропоновано метод обчислення міри відстані між зваженими характеристичними параметрами еталонного і емпіричного мовленнєвих коливань, параметризованих, на відміну від існуючих, у формалізмі методології моделей індивідуальності голосу, де при оцінюванні довірчих інтервалів варіювання значень характеристичних параметрів мовленнєвих сигналів враховується рівень відношення «сигнал»/«шум», що дозволяє визначити поріг прийняття рішень в задачі верифікації суб’єкта за голосом; – Запропоновано інформаційну технологію для оптимізації обраного атрибуту гарантоздатності цільової інформаційної системи критичного застосування, для опису якої, на відміну від існуючих, синтезовано методологію марковських, напівмарковських і керованих напівмарковських моделей конфіденційності, цілісності, готовності, функційної безпечгності, живучості та безвідмовності, що дозволяє поставити розв’язувану задачу математичного програмування для знаходження екстремального значення обраного атрибуту гарантоздатності для цільової ІСКЗ; – Запропоновано методи дослідження взаємозалежності «рівень конфіденційності»-«цілісність» та «рівень конфіденційності»-«готовність», у

яких, на відміну від існуючих, для конкуруючих атрибутів гарантоздатності, представлених у формалізмі профільних напівмарковських математичних моделей, здійснено постановку однокритеріальних задач оптимізації цільової ІСКЗ, що дозволяє знайти для останньої екстремальне значення одного з атрибутів при заданих порогових значеннях решти.

Удосконалено: – Модель процесу автентифікації суб'єкта машиною опорних супер- та і-векторів за параметризованим представленням мовленнєвого матеріалу із шумом, опрацьованого, на відміну від існуючих, мультиваріантним методом компенсування шумів у парольному мовленнєвому сигналі з варіативним описом характеристичних параметрів моделлю сумішей гаусівських розподілів, що дозволило підвищити конфіденційність процесу автентифікації, готовність цільової інформаційної системи і оптимізувати процес навчання імовірнісного класифікатора; – Метод структурного синтезу згорткової нейромережі для автентифікації суб'єкта за мовленнєвим матеріалом із шумом, в якій, на відміну від існуючих, у перший, згортковий, шар інтегровано фільтри Габора із параметризацією вхідної спектрограми в формалізмі спектрально-темпоральних рецептивних полів, що дозволяє максимізувати інформативність інтерпретації вхідної спектрограми нейромережею автоматично, в процесі її навчання, та, за рахунок введення bottleneck-шару, отримати новий набір характеристичних параметрів для опису індивідуальності мовленнєвого матеріалу із шумом.

У **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. Як виявилось, найпомітніше на конфіденційність ІСКЗ впливає надійність процесу

розмежування доступу, що зумовило доцільність досліджень, спрямованих на підвищення надійності двохфакторної схеми верифікації для доступу до цільової інформаційної системи за рахунок інтеграції процесу біометричної автентифікації суб'єкта-користувача за голосом. Це зумовило відповідну орієнтацію наступних розділів.

У **другому розділі** пропонуються моделі індивідуальності голосу в мовленнєвому сигналі для 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 у контексті вирішуваної задачі. Формалізується бікомпонентна модель класифікації фрагментів мовленнєвих сигналів відповідно до їх інформативності для автентифікації суб'єкта за голосом.

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

В **четвертому розділі** оцінюється вплив шумів акустичного оточення приймачів мовленнєвого сигналу на конфіденційність процесу автентифікації суб'єкта за голосом. Запропоновано моделі компенсування шумів у мовленнєвих сигналах, які стали основою для синтезу імовірнісних моделей процесу автентифікації суб'єкта за мовленнєвим матеріалом із шумом, практичним

наслідком яких стало удосконалення відповідних методів прийняття рішень. Враховуючи значну ресурсовитратність процесу класифікації як неодмінної складової процесу автентифікації суб'єкта за голосом, проведено дослідження з оптимізації методів прийняття рішень щодо особи суб'єкта, зокрема методами машинного навчання.

У **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, готовності, 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-готовність та цілісність-готовність, представлено відповідні моделі взаємозалежності цих інтегральних складових гарантоздатності із утворенням відповідних критеріїв.

У **шостому розділі** представлено аналітичні методи обчислення характеристичних параметрів моделей індивідуальності голосу для досліджуваних екземплярів мовленнєвих сигналів. Отримано адаптації цих методів залежно від того, відомі значення усталених параметрів моделей індивідуальності голосу для досліджуваного екземпляру мовленнєвого сигналу, чи ні. 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.

Практичне значення отриманих результатів втілено у: методику оптимізації набору характеристичних параметрів для автентифікації суб'єкта за

голосом; методику визначення порогу прийняття рішень при автентифікації суб'єкта за мовленнєвим матеріалом із шумом; методику регуляризації глибокої нейромережі для прийняття рішень в задачі автентифікації суб'єкт за мовленнєвим сигналом із сумом; концепцію двохфакторної автентифікації суб'єкта-користувача із верифікацією за індивідуальними особливостями його голосу в якості другого фактору; методику формування політики безпеки програмної складової інформаційної системи критичного застосування; методику оптимального резервування обчислювальних ресурсів на етапі проектування системи з врахуванням заданого рівня її готовності; методику оцінювання характеристичних параметрів при описі мовленнєвих сигналів моделями ІГМС; методики і алгоритми для оцінювання частоти основного тону на основі моделей ІГМС; методики і алгоритми для оцінювання частоти основного тону, сформульовані в контексті апріорної інформації щодо усталених параметрів моделей ІГМС; методику редукції структурної моделі функційної безпечгності ІСКЗ; методику і алгоритм для оптимізації обраного атрибуту гарантоздатності цільової ІСКЗ; методику виділення модулювального коливання у мовленнєвому сигналі; методику верифікації математичної моделі ІГМС за значенням критерію, який засновано на коефіцієнті множинної кореляції; методики вибору типу і налаштувань класифікаторів в залежності від рівня відношення «сигнал»/«шум» в емпіричному мовленнєвому сигналі; методику бустінгу процесу навчання профільних класифікаторів; методику прийняття рішень в задачі класифікації суб'єкта за голосом на основі методу найкращих оцінок; методику синтезу профільної універсальної фонової моделі; методику оптимізації залежності конфіденційності процесу автентифікації і готовності інформаційній системі критичного застосування.

***Ключові слова*:** інформаційна система критичного застосування, гарантоздатність, атрибут, індивідуальність голосу у мовленнєвому сигналі, автентифікація суб'єкта за голосом, конфіденційність, цілісність, готовність.

SUMMARY

Kovtun V. V. Information technologies for increasing the dependability of the information systems for critical use with person authentication by voice. – Qualifying scientific work as a manuscript.

Dissertation for the degree of doctor of technical sciences on speciality 05.13.06 “Information technologies” – Vinnytsia National Technical University. Vinnytsia, 2020.

Among the existing classes of automated systems, the so-called critical systems, which operate with high reliability and functional safety, occupy a special place. Such systems function with the predicted level of the mentioned attributes during the operational life cycle due to the mechanisms put in at the design stage to counteract the impact of certain classes of negative factors. If an emergency take place with a critical system, it can cause significant material, reputational, and most importantly, human loss. Communication of critical systems with information space is provided by the specialized software – information systems for critical use (ISCU). The prime characteristic feature of ISCU is the predictability of the functioning results in the conditions of influence of both known and unknown negative factors. In current domestic and foreign scientific works authored by such scientists as Laprie J.-C. Laprie, A. Avizienis, B. Randell, A. Romanovsky, J. Knight, M. Al-Kuwaiti, V. Kharchenko, W. Zamojski, D. Nicol, J. Dugan, J. Arlat, G. Tesler A. Fedukhin, V. Ignatov, I. Shubinsky, R. Tsarev, S. Maharjan, F. Zahedi, O. Dolinina, J. Lungo, B. Littlewood and normative documents 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, depending on the industry to which the critical system belongs, the corresponding taxonomy of qualitative indicators – attributes of the functioning of the target systems is introduced. These taxonomies define, in particular, metrics for evaluating information system components. However, the existing works do not consider in a complex all the principles of increasing the dependability of information systems for critical use, in particular, for the most important attributes – confidentiality, integrity, availability, functional security, survivability, reliability. No single system approach has been proposed to estimate these

attributes of dependability, which is a necessary condition for the functioning of information systems for critical use as a class. Thus, to solve the **actual scientific and applied problem** of ensuring the dependability of information systems for critical use it is necessary to resolve the objective contradiction between: - the existence of distributed structured information systems for critical use, the key feature of which should be predictable operational behavior; - the availability of technologies that provide interaction between sets of persons-users, system services and information resources, but do not guarantee the full functioning of the ISCU in the face of known negative factors; - simultaneously increasing requirements for the level of confidentiality, integrity and availability of ISCUs on the one hand, and the impossibility of their simultaneous provision due to the objective limitation of system computing resources and the existence of criminals developed technologies to neutralize standard methods of persons-users authentication, on the other hand.

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, which allows to obtain a compact, informative and adequate parametric description of the individuality of segments of speech signals with a high and moderate level of vocalization; - 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, which allows to determine the noise level in both vocalized and non-vocalized segments of speech signals; - 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, which allows to determine the threshold of decision-making in the task of person-user verification by voice; - 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. which allows to setup a mathematical programming task to find the extreme value of the selected attribute of dependability for the target ISCU; - 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, which allows to find the extreme value of one selected attribute at a given threshold values of the rest ones.

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, in which, unlike the existing ones, by the multivariate method of noise compensation in the password speech signal with variable description of characteristic parameters increase the confidentiality of the authentication process, the readiness of the target information system and optimize the training process of the probability classifier; - Method of adaptation of an convolutional neural network for person-user authentication by speech material with noise, in which, unlike existing ones, the bank of Gabor filters with parameterization of input spectrogram in formalism of spectral-temporal receptive fields are integrated with the first, convolutional, layer, which allows to maximize informativeness of an input spectrogram by the neural network automatically, during the process of its training, and, due to the introduction of the bottleneck-layer, to obtain a new set of characteristic parameters to describe the person-user voise individuality of speech material with noise.

The **first chapter** presents the results of an analysis of the theoretical validity of the process of the estimation of the dependability of the ISCU with person authentication by voice as a complex phenomenon. An overview of theoretical works in the evaluation of the dependability of information systems is carried out. The descriptive taxonomy and the structure of the ISCU as a subclass of information systems designed to provide critical systems information support are analyzed. The review of technologies of increasing the confidentiality of information systems by biometric authentication methods, in particular, by voice, is conducted. As it turned out, the ISCU's confidentiality was most noticeably affected by the reliability of the access delimitation process, which led to the feasibility of studies aimed at enhancing the reliability of the two-factor verification scheme for accessing the target information system by integrating the biometric authentication process of the person by voice as a second factor. This led to the appropriate orientation of the following chapters.

The **second chapter** introduces voice personality models in the speech signal to solve the person’s voice authentication task. Formalized basic and refined deterministic models of voice personality in speech signal. Stochastic interpretations of synthesized deterministic models are proposed. Effective methods for representing the characteristic features of models of voice personality in a speech signal in time and frequency dimensions in the context of a solved problem are described. Formulate a bicomponent model for classifying speech fragments according to their informative content for person authentication by voice.

In the **third chapter**, the process of establishing the adequacy of the empirical speech signals and their description by the mathematical models presented in the second section are systematized in the context of the task of person authentication by voice. The method of verification of mathematical models of voice personality in a speech signal by the value of the selected criterion is synthesized. The process of estimating the decision threshold in the task of person authentication by voice is formalized in accordance with the signal-to-noise ratio of the analyzed speech signal. The empirical verification of the obtained theoretical results of modeling the personality of the voice

in the speech signal with the generalization of the results and their analysis is carried out.

The **fourth chapter** assesses the effect of the acoustic noise of the speaker's surround on the privacy of the process of person authentication by voice. Models of noise compensation in speech signals have been proposed, which became the basis for the synthesis of probabilistic models of the subject's authentication process for speech material with noise, the practical consequence of which was the improvement of appropriate decision-making methods. Considering the considerable resource consumption of the classification process as an indispensable component of the process of person authentication by voice, research has been conducted to optimize decision-making task in persons authentication by voice, in particular, by machine learning technologies.

The **fifth chapter** reflects the structural and functional features of an information system for critical use with person authentication by voice in an adequate dependability model as an integral characteristic that enables the estimation of confidentiality, accessibility, integrity, reliability, availability, serviceability, failure rate and mean time before failure of such information systems. The obtained models of the dependability attributes take into account the architectural features of the target system's information environment, the importance of its information resources, the specifics of the authentication process and the formation of a system security policy etc. Considering the competing nature of the pairs of attributes: confidentiality and accessibility, integrity and functionality, the corresponding models of interdependence of these integral dependability components with formation of corresponding criteria are presented.

The sixth chapter presents analytical methods for calculating the characteristic parameters of voice individuality models for the studied specimens of speech signals. Adaptations of these methods are obtained depending on whether the values of the established parameters of the models of voice individuality for the studied instance of the speech signal are known or not. The information technology of person authentication according to the individuality of the voice in the speech signal and the

generalized method and information technology for optimization of the selected attribute of dependability of the target information system for critical use are synthesized.

The **practical significance of the obtained results** is embodied in: the method of optimizing the set of characteristic parameters for the person-user authentication by voice; the method of determining the threshold of decision-making in the person-user authentication by the speech material with noise; the technique of regularization of the deep neural network for decision-making in the task of person-user authentication by the speech signal with noise; the concept of two-factor person-user authentication with verification of the individual characteristics of his voice as a second factor; methods of forming the security policy of the software component of the information system for critical use; the method of optimal redundancy of computing resources at the design stage of the system taking into account the specified level of its availability; methods of estimating characteristic parameters when describing speech signals by models of voice individuality in speech signal (VISS); techniques and algorithms for estimating the pitch frequency based on models of VISS; techniques and algorithms for estimating the pitch frequency, formulated in the context of a priori information on the established parameters of the models of VISS; methods of reduction of the structural model of functional safety of ISCU; methodology and algorithm for optimizing the selected attribute of dependability of the target ISCU; the method of selection of modulating oscillations in the speech signal; the method of verification of the mathematical model of VISS by the value of the criterion, which is based on the coefficient of multiple correlation; methods of selecting the type and settings of classifiers depending on the level of the signal-to-noise ratio in the empirical speech signal; methods of boosting the process of training profile classifiers; the method of decision-making in the task of lassification of the person-user by voice based on the method of best estimates; methods of synthesis of profile universal background model; methods of optimizing the dependence of the confidentiality of the authentication process and the availability of the information system for critical use.

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

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.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ І ПОЗНАЧЕНЬ ……..... 23
ВСТУП ……..... 24
РОЗДІЛ 1 АНАЛІЗ СТАНУ ПРОЦЕСУ ЗАБЕЗПЕЧЕННЯ ГАРАНТОЗДАТНОСТІ ІНФОРМАЦІЙНОЇ СИСТЕМИ КРИТИЧНОГО ЗАСТОСУВАННЯ ІЗ АВТЕНТИФІКАЦІЄЮ СУБ'ЄКТА ЗА ГОЛОСОМ ….. 36
1.1 Аналіз процесу забезпечення гарантоздатності інформаційної системи критичного застосування ……..... 36
1.2 Аналіз процесу автентифікації суб'єкта за голосом ……. 58
1.3 Вибір напряму, мети та постановка завдань дослідження …… 80
Висновки до першого розділу ……. 84
РОЗДІЛ 2 КВАЗІДЕТЕРМІНОВАНІ І СТОХАСТИЧНІ МОДЕЛІ ІНДИВІДУАЛЬНОСТІ ГОЛОСУ …..... 87
2.1 Базова квазідетермінована модель індивідуальності голосу ……. 87
2.2 Уточнена квазідетермінована модель індивідуальності голосу ……... 96
2.3 Стохастична інтерпретація базової і уточненої моделей індивідуальності голосу ……. 102
2.4 Опис рівня відношення «сигнал»/«шум» у формалізмі моделей індивідуальності голосу …….. 114
Висновки до другого розділу …… 123
РОЗДІЛ 3 ЗАСТОСУВАННЯ МОДЕЛЕЙ ІНДИВІДУАЛЬНОСТІ ГОЛОСУ ДЛЯ АВТЕНТИФІКАЦІЇ СУБ'ЄКТА …….. 126
3.1 Технологія автентифікації суб'єкта за голосом у формалізмі моделей індивідуальності голосу 126
3.2 Оцінювання адекватності запропонованих моделей індивідуальності голосу ……... 141
Висновки до третього розділу …….. 164
РОЗДІЛ 4 ДОСЛІДЖЕННЯ ПРОЦЕСУ АВТЕНТИФІКАЦІЇ СУБ'ЄКТА ЗА МОВЛЕННЄВИМ СИГНАЛОМ ІЗ ШУМОМ …..……..... 166

4.1 Компенсація шумів у фонограмі мовленнєвого сигналу в контексті задачі автентифікації суб'єкта за голосом …… 166
4.2 Моделі і методи процесу класифікації в задачі автентифікації суб'єкта за мовленнєвим сигналом із шумом ……..... 188
Висновки до четвертого розділу …….. 209
РОЗДІЛ 5 МОДЕЛІ І МЕТОДИ ЗАБЕЗПЕЧЕННЯ ГАРАНТОЗДАТНОСТІ ІНФОРМАЦІЙНОЇ СИСТЕМИ КРИТИЧНОГО ЗАСТОСУВАННЯ ІЗ АВТЕНТИФІКАЦІЄЮ СУБ'ЄКТА ЗА ГОЛОСОМ …… 213
5.1 Концепція забезпечення конфіденційності сеансу суб'єкт-системної інформаційної взаємодії ……..... 213
5.2 Модель цілісності інформаційної системи критичного застосування, забезпечуваної системною політикою безпеки …… 235
5.3 Модель готовності інформаційної системи критичного застосування …… 263
5.4 Моделі функційної безпечності і живучості інформаційної системи критичного застосування 284
5.5 Напівмарковська модель безвідмовності інформаційної системи критичного застосування …… 295
Висновки до п'ятого розділу …… 317
РОЗДІЛ 6 ПРИКЛАДНЕ УЗАГАЛЬНЕННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ДЛЯ ПІДВИЩЕННЯ ГАРАНТОЗДАТНОСТІ ІНФОРМАЦІЙНОЇ СИСТЕМИ КРИТИЧНОГО ЗАСТОСУВАННЯ ІЗ АВТЕНТИФІКАЦІЄЮ СУБ'ЄКТА ЗА ГОЛОСОМ …… 322
6.1 Методика аналітичного розрахунку характеристичних параметрів при описі мовленнєвих сигналів моделями ІГМС ……..... 322
6.2 Методика оцінювання частоти основного тону на основі моделей ІГМС ……. 329
6.3 Методики оцінювання частоти основного тону, сформульовані в контексті апріорної інформації щодо усталених параметрів моделей ІГМС ……. 340

6.4 Реалізація інформаційної технології автентифікації суб'єкта за індивідуальністю голосу в мовленнєвому сигналі 348
6.5 Узагальнена методика та інформаційна технологія для підвищення обраного атрибуту гарантоздатності ІСКЗ ……... 358
6.6 Узагальнення досвіду впровадження результатів дисертаційного дослідження ……. 372
Висновки до шостого розділу ……. 380
ВИСНОВКИ ……. 384
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ ……... 387
ДОДАТКИ …… 416
Додаток А Способи математичної формалізації інформаційних процесів у ІСКЗ ……..... 417
Додаток Б Аналіз моделей мовленнєвих сигналів у контексті задачі автентифікації суб'єкта за голосом ……... 426
Додаток В Спектральне представлення характеристичних параметрів моделей індивідуальності голосу …….. 442
Додаток Д Синтез і дослідження бікомпонентної моделі фонетичної динаміки мовленнєвого сигналу …… 450
Додаток Е Методика оцінювання адекватності математичних моделей ІГМС емпіричним даним ……... 462
Додаток Ж Імовірнісні моделі процесу автентифікації суб'єкта за мовленнєвим сигналом із шумом ……..... 471
Додаток З Формалізація методу найкращих оцінок ……..... 509
Додаток К Модель залежності конфіденційності та готовності інформаційній системі критичного застосування ……..... 517
Додаток Л Графічна інтерпретація пунктів наукової новизни …….. 530
Додаток М Акти впровадження результатів дисертаційного дослідження …... 536
Додаток Н Список опублікованих праць за темою дисертації ……... 564

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ І ПОЗНАЧЕНЬ

АС – суб’єкт автентифікації

АСГ – автентифікація суб’єкта за голосом

АСММШ – автентифікація суб’єкта за мовленнєвим матеріалом із шумом

БОД – блок оброблювання даних

БРД – блок розмежування доступу

ВМ – віртуальна машина

ВМП – відновлюваний марковський процес

ДЧВ – дисперсія часу до відмови

ІГМС – індивідуальність голосу в мовленнєвому сигналі

ІС – інформаційна система

ІСКЗ – інформаційна система критичного застосування

ІнР – інформаційні ресурси

ІнС – інформаційне середовище

ІП – інформаційний процес

КНМП – керований напівмарковський процес

КП – критична помилка

КФР – кумулятивна функція розподілу

НМП – напівмарковський процес

НФ – негативний фактор

ОМП – оцінна мережа Петрі

ПА – процес автентифікації

ПБ – політика безпеки

ПБІС – підсистема безпеки інформаційної системи

ПЗНД – підсистема захисту від несанкціонованого доступу

ПКЦІ – підсистема контролю цілісності інформації

ПММ – прихована марковська модель

ПП – підозра на помилку

ПРД – підсистема розмежування доступу

СГР – суміш гаусівських розподілів

СД – сервер даних

СІБ – система інформаційної безпеки

СК – системний контур

СПБ – системна політика безпеки

СТРП – спектрально-темпоральні рецептивні поля

ССВ – суб’єкт-системна взаємодія

СУБД – система управління базами даних

СРЦ – сервер-реєстраційний центр

СЧВ – середній час до відмови

ФБ – функціональна безпека

АА – додаток для автентифікації

DET-крива – крива компромісного визначення похибки

EER-коефіцієнт – точка рівності похибок α і β

EM-метод – метод максимізації правдоподібності

ERB – еквівалент-прямокутна шкала пропускання

FAR, β – імовірність хибного допуску

FRR, α – імовірність хибного недопуску

MAP-метод – метод максимальної апостеріорної адаптації

MFCC – Мел-частотні кепстральні коефіцієнти

PNC – перцептивні коефіцієнти лінійного передбачення

PNCC – нормовані за потужністю кепстральні коефіцієнти

SNR – рівень відношення «сигнал»/«шум»

ВСТУП

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 має бути 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 відомих негативних факторів;

– одночасно 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 безпечностю, 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 оптимізації взаємозалежності готовності і цілісності системи як відповідної задачі математичного програмування;

– формалізувати методи оптимізації індикаторів функційної безпечності і живучості інформаційної системи критичного застосування із постановкою відповідних задачі математичного програмування;

– синтезувати 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.

Системне уявлення щодо представлених у дисертаційній роботі результатів дають рис. 6.17, 6.18.

Наукова новизна отриманих результатів.

Вперше:

– запропоновано інформаційну технологію автентифікації суб’єкта за індивідуальністю голосу, відмінністю якої є те, що мовленнєвий сигнал представляється сумаою 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 в:

– методику оптимізації набору характеристичних параметрів для автентифікації суб’єкта за голосом (підр. 3.2);

– методику визначення порогу прийняття рішень при автентифікації суб’єкта за мовленнєвим матеріалом із шумом (підр. 3.2);

– методику регуляризації глибокої нейромережі для прийняття рішень в задачі автентифікації суб’єкт за мовленнєвим сигналом із сумом (підр. 4.2);

– концепцію двохфакторної автентифікації суб’єкта-користувача із верифікацією за індивідуальними особливостями його голосу в якості другого фактору (підр. 5.1);

– методику формування політики безпеки програмної складової інформаційної системи критичного застосування (підр. 5.2);

– методику оптимального резервування обчислювальних ресурсів на етапі проектування системи з врахуванням заданого рівня її готовності (підр. 5.3);

– методику оцінювання характеристичних параметрів при описі мовленнєвих сигналів моделями ІГМС (підр. 6.1);

– методики і алгоритми для оцінювання частоти основного тону на основі моделей індивідуальності голосу в мовленнєвому сигналі (ІГМС) (підр. 6.2);

– методики і алгоритми для оцінювання частоти основного тону, сформульовані в контексті апріорної інформації щодо усталених параметрів моделей ІГМС (підр. 6.3);

– методику редукції структурної моделі функційної безпечності ІСКЗ (підр. 6.4);

– методику і алгоритм для оптимізації цільової ІСКЗ за значенням обраного атрибуту гарантоздатності (підр. 6.5);

– методику виділення модулювального коливання у мовленнєвому сигналі (додаток В);

– методику верифікації математичної моделі ІГМС за значенням критерію, який засновано на коефіцієнті множинної кореляції (додаток Е);

– методики вибору типу і налаштувань класифікаторів в залежності від рівня відношення «сигнал»/«шум» в емпіричному мовленнєвому сигналі (додаток Ж);

– методику бустінгу процесу навчання профільних класифікаторів (додаток Ж);

– методику прийняття рішень в задачі класифікації суб’єкта за голосом на основі методу найкращих оцінок (додаток Ж);

– методику синтезу профільної універсальної фонової моделі (додаток З);

– методику оптимізації залежності конфіденційності процесу автентифікації і готовності інформаційній системі критичного застосування (додаток К).

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], [83], [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], [49], [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: [30] – метод виділення складових сегментів у мовленнєвому сигналі; [31] – модель і метод оцінювання впливу завад на достовірність роботи інформаційно-вимірювальної системи розпізнавання голосу; [32] – метод виділення основного тону на основі модифікованої математичної моделі слухової системи людини; [33] – метод оцінювання метрологічних характеристик інформаційно-вимірювальної системи автоматизованого розпізнавання голосів; [34] – узагальнення стану проблеми розробки ефективних систем пошуку ключових слів; [35] – метод пошуку ключових слів у мовленнєвому сигналі; [36] – модель і метод оцінювання надійності автоматизованих систем розпізнавання мовців критичного застосування; [37] – модель і метод узагальнення інформації множини мікрофонів у автоматизованій системі розпізнавання мовця критичного застосування; [38] – метод синтезу і навчання комітету нейромереж у автоматизованій системі розпізнавання мовців критичного застосування; [39] – метод оптимізації алфавіту інформативних ознак для автоматизованої системи розпізнавання мовців критичного застосування; [40] – метод представлення ознак у автоматизованій системі розпізнавання мовця критичного застосування; [41] – методика дослідження ефективності ознак розпізнавання мовців при використанні згорткових нейромережі і її прикладна реалізація; [42] – метод детектування

мовленнєвої активності в автоматизованій системі розпізнавання мовця критичного застосування; [43] – модель нейромережевого класифікатора для модуля розпізнавання мовця у складі автоматизованої системи критичного застосування; [44] – метод підвищення шумостійкості автоматизованої системи розпізнавання мовця критичного застосування; [45] – метод оптимального синтезу нейромережевого класифікатора автоматизованої системи розпізнавання мовця критичного застосування; [46] – метод підвищення інформативності основного тону для розпізнаванні мовців згортковими нейромережами; [48] – алгоритм і постановка експерименту з прикладного моделювання рангових конфігурацій; [49] – базова модель автоматизованої системи розпізнавання мовця критичного застосування; [51] – метод застосування СТРП-ознак в задачі автентифікації мовця; [52] – метод оцінювання надійності сеансу розпізнавання особи автоматизованою системою розпізнавання мовця критичного застосування; [53] – метод адаптації PLDA для прийняття рішень у автоматизованій системі розпізнавання мовця критичного застосування із нейромережевим класифікатором; [54] – модель оцінювання цілісності інформаційної системи критичного застосування і метод синтезу оптимальної системної політики безпеки; [57] – модель компенсування шумів у фонограмі мовленнєвого сигналу; [59] – модель готовності інформаційної системи критичного застосування і метод її прикладного застосування; [82] – модель безвідмовності інформаційної системи критичного застосування і метод її прикладного застосування; [83] – метод оптимізації безвідмовності інформаційної системи критичного застосування; [84] – моделі функційної безпечності і 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.

РОЗДІЛ 1
АНАЛІЗ СТАНУ ПРОЦЕСУ ЗАБЕЗПЕЧЕННЯ ГАРАНТОЗДАТНОСТІ ІНФОРМАЦІЙНОЇ СИСТЕМИ КРИТИЧНОГО ЗАСТОСУВАННЯ ІЗ АВТЕНТИФІКАЦІЄЮ СУБ'ЄКТА ЗА ГОЛОСОМ

1.1 Аналіз процесу забезпечення гарантоздатності інформаційної системи критичного застосування

Серед існуючих класів автоматизованих систем окреме місце займають так звані критичні системи [1–10], функціонування яких характеризується специфічними вимогами щодо визначення атрибутів гарантоздатності та умовою щодо збереження прогнозованого тренду варіації цих атрибутів під час життєвого циклу експлуатації за рахунок закладених на етапі проектування механізмів протидії впливу визначених класів НФ [114–116]. Питання оцінювання якісних характеристик інформаційних систем у метриці гарантоздатності розкриємо на основі матеріалу інформаційних джерел [60-113].

У своєму вихідному варіанті [26] гарантоздатність (англ. dependability) [60] утворилася як результат синтезу елементів теорії надійність [61–78] і теорії безпеки і ризику [79–86] у прикладному їх застосування для оцінювання функціональної якості досліджуваної системи. Декомпозицією поняття гарантоздатність є ідентифікація для досліджуваної системи елементів множин атрибутів, загроз і засобів. Множина атрибутів включає методи оцінювання надійності, ремонтопридатності, конфіденційності, готовності і цілісності досліджуваної системи. Ідентифікація множини загроз передбачає визначення типів несправностей, помилок і збоїв, які можуть виникнути під час життєвого циклу досліджуваної системи. Множина засобів включає методи: – запобігання загрозам; – забезпечення відмовостійкості; – усунення наслідків, спричинених впливом загроз; – прогнозування впливу загроз тощо.

Інтегральними характеристиками елементів цих множин є:

– безвідмовність [87], як властивість досліджуваної системи зберігати функціональний стан протягом обмеженого, неперервного інтервалу часу;

– готовність [88, 89] як здатність досліджуваної системи, забезпеченої необхідними зовнішніми ресурсами, у заданий момент та протягом фіксованого інтервалу часу виконувати передбачені специфікацією функції при дотриманні визначених умов експлуатації і регламенту технічного обслуговування;

– живучість [90–94], як властивість досліджуваної системи зберігати або відновлювати функціональний стан у визначеному обсязі при санкціонованій або несанкціонованій зміні умов експлуатації або структури апаратної чи інформаційної складових;

– обслуговуваність [21, 95], як властивість досліджуваної системи підлягати регламентованим процесам технічного обслуговування та ремонту;

– цілісність [96–109], як властивість досліджуваної системи зберігати визначений рівень структурної сталості при функціонуванні в умовах зовнішніх випадкових або детермінованих спотворень або руйнівних впливів;

– конфіденційність [96–109], як властивість досліджуваної системи самоубезпечуватися від несанкціонованого використання або структурних змін;

– функційна безпечність [110–112], як здатність досліджуваної системи не завдавати небезпечних (катастрофічних) впливів на людину або навколишнє середовище у відповідь на дію факторів із визначеної на етапі проектування множини загроз.

Оцінювання ***безвідмовності*** досліджуваної системи передбачає визначення таких параметрів як:

– імовірність безвідмовного функціонування $R(t)$ – імовірність того, що до настання моменту часу t досліджувана система не перейде у нефункціональний стан;

– середня тривалість безвідмовного функціонування $\overline{T}$ – математичне сподівання тривалості часу перебування системи у функціональному стані аж до моменту її першого переходу у нефункціональний стан;

– коефіцієнт потоку відмов $\omega(t)$ – добуток кількості переходів досліджуваної системи у нефункціональний стан із поверненням у функціональний стан за часовий інтервал тривалістю t і оберненого значення t^{-1}.

Методики розрахунку цих параметрів змінюються, якщо досліджуваній системі властива ***відмовостійкість***, яка для досліджуваної системи оцінюватиметься виразом [17]

$$P_{ts} = c^{s}\left(1 - F\left(f, q, s\right)\right), \tag{1.1}$$

де $F(f,q,s)$ – функція імовірності переходу системи в нефункціональний стан; s – кількість резервних модулів, які можна ввімкнути для переведення системи із нефункціонального стану у функціональний (потребує витрат на резервування на етапі проектування); q – кількість однотипних модулів, які функціонують паралельно для запобігання переходу системи у нефункціональний стан (потребує витрат на резервування як на етапі проектування, так і на етапі експлуатації); c – ступінь компенсування наслідків відмови (імовірність того, що система зможе із нефункціонального стану відновити функціональний стан у повному або обмеженому обсязі); f – гранично допустима для модуля кількість переходів із функціонального стану у нефункціональний і навпаки.

Якщо досліджувана система – електротехнічна, то, відповідно до актуальних міжнародних стандартів [351], імовірнісна функція $F(f,q,s)$ з виразу (1.1) є дифузійним монотонним (DN) розподілом [17]:

$$F\left(f, q, s\right) = DN\left(x, \nu, f, q, s\right), \tag{1.2}$$

де x – відносна тривалість безвідмовного функціонування: $x = \overline{T}^{-1}$; ν – коефіцієнт варіації розподілу. Згідно з тими ж стандартами, значення елементів множини $P_{ts} = \{q, c, f, s\}$ за замовчуванням визначено як $\{1,1,0,0\}$, відповідно. Зростання значень елементів множини P_{ts} спричиняє зростання імовірності P_{ts} та зростання витрат на експлуатацію досліджуваної системи.

Також вклад апаратної складової у безвідмовність досліджуваної системи враховують параметром N_s – обсяг апаратних ресурсів, які необхідно

акумулювати у досліджуваній системі для досягнення останньою заданого рівня безвідмовності. Відповідно, якщо на етапі проектування є різні варіанти реалізації досліджуваної системи, то їх варто порівняти, визначивши для кожного із них вартість, яку необхідно витратити для досягнення вибраного порогового значення характеристики R_{ts}.

Множина параметрів такої вкрай важливої для систем критичного застосування інтегральної характеристики як ***готовність*** включає коефіцієнт готовності і коефіцієнт оперативної готовності тощо.

Коефіцієнт готовності характеризує імовірність перебування досліджуваної системи в функціональному стані [17]:

$$K_f = T_f \left(T_f + T_{rf} \right)^{-1}, \tag{1.3}$$

де T_f – середня тривалість перебування системи в функціональному стані; T_{rf} – тривалість відновлення системою функціонального стану після переходів у нефункціональний стан, спричинених впливом НФ.

Коефіцієнт оперативної готовності характеризує імовірність перебування досліджуваної системи у функціональному стані у конкретний момент часу [16–18]:

$$K_{of} = K_f R(t), \tag{1.4}$$

де $R(t)$ – імовірність перебування досліджуваної системи у функціональному стані у момент часу t.

До параметрів ***живучості***, як властивості досліджуваної системи зберігати повну або часткову функціональність при експлуатації в умовах, які не передбачено на етапі проектування, відносять виживаність, запас живучості і коефіцієнти живучості та деградації.

Коефіцієнт живучості показує співвідношення кількості функціональних станів до всієї можливої кількості станів, у яких може перебувати досліджувана система, [17]:

$$K_G = M \left(C_l^i \right)^{-1}, \tag{1.5}$$

де M – кількість функціональних станів; C_l^i - загальна кількість сатанів системи; i – кратність відмови; l – кількість функціональних одиниць живучості досліджуваної системи.

Коефіцієнт деградації [17] показує співвідношення кількості нефункціональних станів до всієї можливої кількості станів, у яких може перебувати досліджувана система,

$$K_D = N\left(C_l^i\right)^{-1}, \tag{1.6}$$

де N – кількість нефункціональних станів досліджуваної системи.

Виживаність [16–18] – це властивість досліджуваної системи перебувати у функціональному стані під впливом n-кратного НФ:

$$R(n) = 1 - Q(n) = P\left(F = A_n^{-1}\right), \tag{1.7}$$

де F – бінарна функція роботоздатності рівна одиниці, якщо система роботоздатна, або нулю – у протилежному випадку; A_n – подія, яка відбувається у наслідок впливу n-кратного НФ.

Запас живучості $d = C - 1$ є зменшеною на одиницю критичною кількістю дефектів C, яка характеризує граничну кількість дефектів, по перевищенню якої досліджувана система перейде у нефункціональний стан.

Також інтегральною характеристикою гарантоздатності є ***обслуговуваність***, яка узагальнено описує складність регламентного обслуговування досліджуваної системи для підтримки її у функціональному стані. До параметрів обслуговуваності відносять:

– тривалість технічного обслуговування T_{to} – середній час, що має витрачатися на обслуговування досліджуваної системи згідно з технічною документацією;

– трудомісткість технічного обслуговування $T_{tz}(i)$ – середні трудовитрати на проведення i-го типу технічного обслуговування досліджуваної системи;

– вартість технічного обслуговування $C_{to}(i)$ – середня вартість проведення i-го типу технічного обслуговування досліджуваної системи;

– тривалість відновлення T_{rn} – середня тривалість часу, яка витрачається на переведення досліджуваної системи з нефункціонального стану у функціональний;

– обчислюваний за певний визначений період експлуатації досліджуваної системи коефіцієнт технічного використання $K_{tu} = T_u \left(T_u + T_r + T_{to}\right)^{-1}$, де T_u – тривалість перебування системи у функціональному стані; T_r – тривалість перебування системи у нефункціональному стані з причини ремонту; T_{to} – тривалість перебування системи у нефункціональному стані з причини технічного обслуговування.

Функційна безпечність як інтегральна характеристика гарантоздатності досліджуваної системи описується:

– імовірністю безпечного функціонування $R_{op}(t) = 1 - F_{op}(t)$ – імовірність того, що за час функціонування досліджуваної системи, рівний t, не трапиться критично небезпечна ситуація, тобто випадок, наслідки якого є критично небезпечними для навколишнього середовища, інфраструктури, життя людей тощо. Визначена імовірнісна функція $F_{op}(t)$ описує розподіл тривалості функціонування системи до настання критично небезпечної ситуації;

– імовірність критично небезпечної ситуації $Q_{op}(t) = 1 - R_{op}(t)$ – імовірність того, що за період функціонування досліджуваної системи, рівний t, трапиться критично небезпечна ситуація;

– відносна середня тривалість функціонування із урахуванням настання критично небезпечних ситуацій T_{cs} – відношення тривалості функціонування досліджуваної системи до математичного сподівання кількості зафіксованих за цей часовий період випадків настання критично небезпечних ситуацій;

– коефіцієнт безпечності $K_{fs} = T_{cs}\left(T_{cs} + T_{rcs}\right)$ – імовірність того, що у довільний момент часу функціонування досліджуваної системи не станеться критично небезпечна ситуація, якщо у цей час система використовується за призначенням. Параметр T_{rcs} описує середню тривалість відновлення

функціонального стану досліджуваної системи після настання критично небезпечної ситуації.

Цілісність є властивістю досліджуваної системи зберігати структурну сталість незважаючи на вплив випадкових чи навмисних спотворювальних чи руйнівних факторів. Параметрами цієї інтегральної характеристики є рівні цілісності апаратної й інформаційної системних складових.

Рівень цілісності апаратної складової L_a це властивість досліджуваної системи унеможливити несанкціоновані структурні зміни своєї апаратної складової.

Рівень цілісності інформаційного середовища L_{is} – властивість досліджуваної системи унеможливити несанкціоновані структурні зміни свого ІнС.

Рівень цілісності інформаційних ресурсів L_{is} – властивість досліджуваної системи унеможливити несанкціоновані структурні зміни своїх ІнР.

Конфіденційність, як властивість досліджуваної системи запобігати несанкціонованому використанню власних апаратних і інформаційних ресурсів, параметризується імовірністю загроз, рівнем готовності, рівнем секретності тощо.

Імовірність загроз P_{th} – це імовірність виникнення ситуації порушення конфіденційності досліджуваної системи.

Рівень готовності L_d – це властивість досліджуваної системи нейтралізувати за відповідний проміжок часу формалізовані типи загроз, спрямовані на отримання несанкціонованого доступу до власного ІнС.

Рівень секретності L_s – це властивість досліджуваної системи протидіяти формалізованим типам загроз, спрямованим на отримання несанкціонованого доступу до власних ІнР.

Якщо досліджувана система – інформаційна, то в актуальних стандартах [29, 104–106] параметри її цілісності оцінюються узагальненням значень бінарних критеріїв, які репрезентують відповідні параметри інтегральної складової.

Зокрема, такий параметр як рівень цілісності ІнС L_{is} декомпозується на два параметри – цілісність обчислювальних ресурсів L_{CR} і цілісність програмних ресурсів L_{PR}.

Цілісність обчислювальних ресурсів L_{CR} репрезентується такими бінарними критеріями: правильність експлуатації; безпека експлуатації; здатність перевіряти і зберігати дані; здатність захисту від суттєвих втрат конфіденційності в разі успішної реалізації загроз; здатність відновлювати конфіденційність після успішної реалізації збоїв і загроз; наявність захисту від порушень авторського права; наявність функцій відновлення конфіденційності; наявність функцій контролю конфіденційності; наявність захисту конфіденційності при функціонуванні у локальній мережі; наявність захисту конфіденційності при функціонуванні в середовищі мережі Internet; наявність функцій ідентифікації і автентифікації; наявність сервісів моніторингу та оповіщення; наявність сервісів оброблювання помилок. Як видно, більша частина критеріїв орієнтована на оцінювання конфіденційності. На оцінювання цілісності і готовності орієнтовано приблизно однакову кількість критеріїв.

Такий параметр як цілісність програмних ресурсів L_{PR} репрезентується такими бінарними критеріями: наявність функцій відновлення виконуваного процесу в разі збою операційної системи, процесора, зовнішніх пристроїв; наявність сервісів відновлення процесу в разі збоїв обладнання; наявність можливості повторного старту процесу з точки зупину; наявність автоматичного резервування ресурсів для збереження поточного стану процесу; наявність сервісів забезпечення стійкості при: виявленні помилок у вхідних даних, виявленні помилок користувача, відсутності необхідних даних; наявність сервісів забезпечення сумісності із апаратними засобами; наявність сервісів забезпечення сумісності із системними програмними засобами; наявність сервісів забезпечення сумісності із іншими програмними засобами, включаючи обмін даними; наявність сервісів оброблювання помилкових ситуацій.

Параметр рівень цілісності ІнР L_{is} репрезентується такими бінарними критеріями: достовірність; точність; якість; своєчасність; правильність; наявність сервісу контролю правильності введеної / виведеної інформації; наявність інформації про сервіси зберігання даних; наявність тестів для контролю допустимих значень вхідних / вихідних даних; наявність сервісів контролю повноти вхідних / вихідних даних; наявність сервісів контролю коректності вхідних / вихідних даних; наявність сервісів контролю несуперечливості вхідних / вихідних даних; наявність сервісів контролю дотримання діапазонів даними і адресами; наявність сервісів оброблювання граничних значень; наявність інформації про здатність відновлювання після помилок.

Як вже зазначалося наведені критерії – бінарні, що спрощує облік відповідних характеристик, але суттєво нівелює їх інформативність.

Окрім цілісності, процес оцінювання конфіденційності також репрезентується множинами бінарних критеріїв, які узагальнюють оцінки відповідних параметрів.

Параметр конфіденційності – імовірність загроз P_{th} репрезентується такими бінарними критеріями: правильність експлуатації обчислювальних ресурсів; безпека експлуатації обчислювальних ресурсів; здатність перевіряти і зберігати дані; здатність запобігати суттєвих наслідків для конфіденційності з причини виникнення помилок; здатність відновлювати конфіденційність після збоїв і помилок; наявність захисту від порушень авторського права; наявність функцій відновлення конфіденційності; наявність функцій контролю конфіденційності; наявність захисту конфіденційності при роботі у локальній мережі; наявність захисту конфіденційності при роботі у середовищі Internet; наявність функцій ідентифікації і автентифікації; наявність сервісів моніторингу та оповіщення; наявність сервісів оброблювання помилок.

Рівень готовності L_d , як параметр конфіденційності, репрезентується такими бінарними критеріями: наявність документа, що регламентує доступ до секретної інформації; наявність документа, що регламентує доступ до технічних засобів; наявність паролів доступу до ІнР; наявність фізичного захисту технічних

ресурсів; наявність захисту технічних ресурсів програмними засобами; наявність у персоналу дозволу на роботу із секретними технічними і / або ІнР; наявність сервісів відновлення виконуваного процесу після збоїв операційної системи, процесора, зовнішніх пристроїв; наявність сервісів забезпечення стійкості функціонування при наявності помилок у вхідних даних, помилок користувача, відсутності необхідних даних; наявність сервісів забезпечення сумісності із апаратними засобами; наявність сервісів забезпечення сумісності із системними програмними засобами; наявність сервісів забезпечення сумісності з іншими програмними засобами, включаючи обмін даними; наявність сервісів опрацювання помилкових ситуацій. Можна помітити, що майже половина критеріїв тотожна введеним для регламентування цілісності програмних ресурсів L_{PR}. Таке дублювання характеризує неточність у семантичній інтерпретації термінів «цілісність» і «конфіденційність».

Рівень секретності L_s, як параметр конфіденційності, репрезентується такими бінарними критеріями: наявність документа, що регламентує доступ до секретної інформації за рівнями секретності; наявність документа, що регламентує доступ до технічних засобів за рівнями секретності; наявність паролів доступу до ІнР; наявність фізичного захисту технічних ресурсів; наявність захисту технічних ресурсів програмними засобами; наявність у персоналу дозволу на роботу із секретними технічними і / або інформаційними ресурсами; наявність сервісів контролю правильність введеної / виведеної інформації; наявність сервісів контролю процесів збереження даних; наявність тестів контролю допустимих значень вхідних / вихідних даних; наявність сервісів контролю повноти вхідних / вихідних даних; наявність сервісів контролю коректності вхідних / вихідних даних; наявність сервісів контролю несуперечності вхідних / вихідних даних; наявність сервісів контролю дотримання діапазонів даними і адресами; наявність сервісів оброблювання граничних значень; наявність сервісів для відновлення інформації після помилок. Видно, що більше половини критеріїв тотожна введеним для регламентування рівня цілісності ІнР L_{is}.

Узагальнюючи наведену інформацію слід відзначити, що таксономії гарантоздатності властива суттєва надлишковість, спричинена відсутністю єдиного цільового міжнародного стандарту. Ця обставина зумовлює неоднозначність у параметризації інтегральних характеристик гарантоздатності. Також слід відмітити загальність критеріїв оцінювання гарантоздатності ІС. Враховуючи темпи розвитку галузі інформаційних технологій такі вади можуть стати причинами значних втрат, що обумовлює актуальність наукової формалізації процесу оцінювання атрибутів гарантоздатності ІСКЗ у парадигмі класичної теорії надійності, ризиків та інформаційної безпеки.

При проектуванні критичних систем віддають перевагу перевіреним та знаним методам та технологіям перед новітніми розробками, які не пройшли всебічної емпіричної перевірки. Впровадження ресурсовитратних технологій, використання яких у поточних автоматизованих системах є нерентабельним, допускається при створенні критичних систем, якщо це зробить процес їх функціонування прогнозованішим, надійнішим, безпечнішим.

Актуальна класифікація критичних систем розділяє їх за реакцією на виникнення надзвичайних ситуацій та за галуззю експлуатації.

За реакцією на виникнення надзвичайних ситуацій критичні системи розділяють на: критичні системи, які мають продовжувати функціонувати в умовах впливу НФ та при виникненні відмов та збоїв, наприклад, літак повинен продовжувати летіти; критичні системи, які повинні обов’язково безпечно переходити у нефункціональний стан, наприклад, потрібно загальмувати потяг, щоб не допустити значних матеріальних чи людських втрат.

За галуззю експлуатації критичні системи розділяють на:

– життєво-критичні системи (safety critical) – це автоматизовані системи, неконтрольований перехід у нефункціональний стан яких може призвести до загибелі людей, завдати суттєвих збитків навколишньому середовищу та інфраструктурі, наприклад, автоматизовані системи управління хімічними виробництвами, літаками, потягами, атомними електростанціями тощо;

– критичні системи гарантованого функціонування (mission critical) – це автоматизовані системи, які створюються з метою обов’язкового завершення визначеної множини операцій, наприклад, системи навігації, системи управління видачею багажу в аеропортах;

– критичні бізнес-системи (business critical) – це автоматизовані системи, створені з метою запобігання значним матеріальним або репутаційним втратам, що зазвичай забезпечується автоматичним вчасним припиненням виконання певних процесів, наприклад, банківські системи роботи із клієнтами, системи інтернет-трейдінгу, ERP-системи тощо;

– критичні системи (інформаційної) безпеки (security critical) – це автоматизовані системи, спроектовані для унеможливлення втрати секретної інформації та запобігання отриманню несанкціонованого доступу до неї.

Впровадження обчислювальної техніки у сферу критичних систем призвело до створення класу ІСКЗ [50, 54–56, 58, 59]. Цим ІС, враховуючи об’єкт їх застосування, властива підвищена привабливість з боку криміногенних і терористських угруповань, що зумовлює системний, професійний підхід спроб несанкціонованого доступу до функцій ІнС чи конфіденційних ІнР тощо. Ця обставина зумовлює первинність задач інформаційної безпеки процесів і даних у ІСКЗ перед підтримкою дій суб’єктів-користувачів, тим більше, що як показує досвід світових лідерів у створенні систем інформаційної безпеки – CISCO, FORTINET, PALOALTO networks, IBM, найрозповсюдженішим типом загроз для ІС є саме загрози отримання несанкціонованого доступу до даних та ІП, для оброблювання даних ініційованих [117, 118].

Захист інформації у ІС забезпечується профільною системою – системою інформаційної безпеки, яка є конгломератом об’єкта захисту і суб’єктів захисту, представлених відповідними техніками захисту інформації, діяльності яких регламентовано відповідними правовими, організаційно-розпорядчими і нормативними документами в сфері захисту інформації. Задачами СІБ є:

– підтримування безпеки апаратних засобів ІС шляхом регламентних перевірок сталості їх структури;

– підтримування безпеки ІнС шляхом регламентних перевірок відсутності незадекларованих функціональних можливостей;

– підтримування криптографічної безпеки ІнР ІС – даних;

– нормативний і функціональний апаратно-програмний захист ІС від несанкціонованого доступу.

У СІБ обов’язково виділяють підсистему захисту від несанкціонованого доступу, яка за способом реалізації може бути автономною або інтегрованою. Автономні ПЗНД зазвичай уніфікуються для всіх рівнів ІС і сценаріїв суб’єкт-системної взаємодії. Вони:

– запобігають появі умов, сприятливих для виникнення загроз несанкціонованого доступу;

– запобігають виникненню загроз несанкціонованого доступу;

– здійснюють пошук і виявлення джерел профільних загроз;

– виявляють, локалізують і нейтралізують впливи профільних загроз;

– відновлюють стан ІнС та ІнР ІС після впливів профільних загроз.

Втім, автономність ПЗНД, підвищуючи рівень безпеки підсистеми як такої, неодмінно знижує доступний їй рівень контролю інформаційних ресурсів і процесів. Певною мірою цей недолік можна компенсувати адекватно підібравши модель організації даних, яка програмно забезпечуватиметься впровадженням відповідної системи управління базами даних. Сучасні тенденції в організації мережевих обчислювальних процесів зумовлюють орієнтування на об’єктно-реляційну модель організації даних у перспективних ІС. Втім, при виборі конкретної СУБД варто враховувати:

– ефективність механізмів обмежень цілісності й організації бізнес-правил;

– надійність вбудованих механізмів доступу до даних;

– варіативність та надійність механізмів формулювання привілей для доступу, перегляду і маніпулювання даними і структурам даних.

Дотримання цих критеріїв дозволить аргументувати вибір СУБД з позицій забезпечення цілісності, конфіденційності і готовності ІнР ІСКЗ. Зауважимо, що

формально обмеження цілісності і бізнес-правила втілюються в пов'язаний із деякою базою даних логічний вираз, результатом обчислення якого завжди буде «true». Відмінність полягає в тому, що бізнес-правила формулюються природною мовою, що і зумовлює зростаючу популярність цього підходу до забезпечення аспекту цілісності даних. Практично обмеження цілісності реалізують на рівні мови СУБД у формі сервісів контролю операцій оновлення.

Аспект готовності на рівні СУБД забезпечується:

– оптимальністю автоматично генерованих стратегій, створюваних для розв'язання поставлених користувачем задач;

– розмежуванням класів ролей користувачів за рівнями доступних системних ресурсів для реалізації визначених множин функцій;

– ефективністю взаємовідображення фізичного і логічного рівнів оперування ІнР;

– варіативністю структур збереження даних у зовнішній пам'яті, а також варіативністю процедур доступу до цих структур.

Загальновизнану методику оцінювання аспекту конфіденційності СУБД втілено у «кольорові» стандарти Міністерства оборони США [119], зокрема, у «Orange Book» і «Lavender Book», де у першій сформульовано критерії забезпечення конфіденційності надійного апаратного забезпечення комп'ютерних систем, а у другій – наведено інтерпретацію цих критеріїв стосовно СУБД. Прикладним результатом цих стандартів є класифікація рівнів конфіденційності СУБД (за зростанням): Cl, C2, Bl, B2, B3, A. За цією класифікацією більшість комерційних СУБД із дискреційним доступом відповідають рівню конфіденційності C2, лише поодинокі представники [120] – рівню Bl, тоді як для відповідності СУБД рівню A слід математично довести, що втілюваний механізм захисту адекватний сформульованим атрибутам конфіденційності.

Окрім цілісності, готовності і конфіденційності визначною характеристикою ІС є надійність, яку у термінах, орієнтованих на інформаційні технології, описано у міжнародних стандартах [104–106]. Втім, у цих стандартах сформульовано лише каталог вимог безпеки і загальну систему понять, у термінах

яких має відбуватися оцінювання надійності ІС. Традиційної для наукового підходу функціональної моделі із визначеною множною атрибутів і формалізованим критерієм там немає. Передбачається, що ці складові мають формулюватися на етапі синтезу технічного завдання на створення ІС у формі профілів захисту і задач безпеки, де перші є універсальними [120–125], а другі – формулюються у співпраці із замовниками. Згідно з цими документами, надійність захисту ІС забезпечується системною політикою безпеки, реалізованою у відповідних системних сервісах із регламентованим переліком функцій. По суті СПБ є набором правил, які реалізують управління, захист і розподіл ІнР.

Універсальність профілів захисту забезпечується результатами досліджень прецедентів успішної реалізації загроз інформаційній безпеці профільних ІС із виділенням недоліків процесів функціонування ІС або засобів її убезпечення, представлених СІБ. Рекомендації щодо запобігання типовим вадам засобів захисту ІС викладено у профільних міжнародних стандартах [104–106]. Проте, темп оновлення їх вмісту явно не встигає за кількісною і якісною еволюцією типів загроз, спричинених експансивним розвитком інформаційних технологій. Запобігти виявленню вад процесів функціонування ІС можна або на етапі проектування, вживши засобів математичного моделювання із оцінюванням адекватності результату поставленим задачам, або на основі емпіричного досвіду експлуатації ІС, здійснюючи причинно-наслідковий аналіз збоїв, втім цей варіант для ІСКЗ є мало прийнятним. Отже, фактично єдиним прийнятним способом убезпечення ІСКЗ є забезпечення надійності інтегрованих ІП точковими засобами інформаційної безпеки, які задовольняють актуальні профільні стандарти. Втім, системний підхід до математичного моделювання надійності ІП супроводжується необхідністю узгодження результатів динамічного, локального, дискретного моделювання їх невразливості із результатами статичного, глобального, неперервного моделювання процесів функціонування інтегрованих захисних механізмів. Додатковим ускладненням є неоднозначна інтерпретація поняття

готовності і конфіденційності.

Готовність ІС забезпечується адаптивністю її захисних механізмів, що, перш за все, проявляється у варіативності механізмів розмежування доступу до інформації. Єдиною моделлю СПБ, яка задовольняє сформульовані вимоги варіативності, є дискреційна модель політики безпеки [126–129], яка, втім, є потенційно вразливою при теоретичному і практичному втіленні. Невразливим, як відомо, вважається мандатний метод розмежування доступу [127, 130], теоретично представлений моделлю кінцевих станів [131–133]. Втім, невразливість моделі кінцевих станів досягається саме низькою варіативністю механізмів розмежування доступу. Об’єднати високу конфіденційність моделі кінцевих станів із високою доступністю дискреційної моделі у межах єдиної СПБ у парадигмі традиційної аналітичної теорії неможливо, якщо розглядати процеси захисту інформації і процеси її оброблювання незалежно. Пошук теоретичних підходів для цього триває.

Згідно з положеннями теорії захисту інформації [134–144], захист ІП забезпечується відповідною політикою безпеки, синтез якої включає такі взаємозалежні задачі: формулювання, реалізація і дослідження ПБ. Формалізація ПБ для досліджуваного ІП починається з опису множини його станів, характеризованих рівнем безпеки. Така ПБ є глобальною і визначає так званий синтаксис доступу. Якщо правила переходів між станами ІП також формалізовано, то отриманий результат є локальною ПБ, яка визначає семантику доступу. Якщо локальну ПБ формалізовано, то СПБ є динамічною, якщо ні – статичною. Якщо множина станів ІП скінченна, то ПБ узагальнюється у вигляді моделі кінцевих станів, безпечність якої теоретично гарантується теоремою безпеки [145]: якщо у початковий момент часу глобальна ПБ для ІП виконується, а подальша зміна його станів здійснюється відповідно до положень локальної ПБ, то в будь-який наступний момент часу глобальна ПБ також виконуватиметься. Це означає, що вразити безпеку ІП може лише вплив непередбачуваних зовнішніх факторів.

Потреби захисту інформації завжди задовольняються за рахунок ресурсів, які можна було б направити на підтримку функціонального призначення ІСКЗ, адже їх реалізовано на спільній апаратній платформі. Беручи до уваги критичне застосування ІСКЗ, на етапі її проектування слід обов'язково запланувати надлишок обчислювальних ресурсів, які за потреби можна направити на убезпечення ІП, генеруючи відповідні управляючі впливи. Обсяг зарезервованих апаратних ресурсів у ІСКЗ на даний час визначається довільно і становить 5–300 % від запланованої їх кількості на підтримку базових функцій створюваної системи. Профільної математичної моделі для оцінювання обсягів резервування немає.

Необхідність управління процесом убезпечення ІСКЗ загалом та інтегрованих її процесів зокрема, спричиняє актуальність відповідних досліджень, реалізовуваних, зазвичай, у парадигмі теорії управління складними системами [146–156]. За метою управління схему його реалізації класифікують як: програмне управління, автоуправління, оптимальне управління, спостереження тощо. Задача управління ІП в ІСКЗ є багатокритеріальною задачею оптимального управління, метою якого є підтримування екстремального значення комплексного критерію функціональної якості ІСКЗ за рахунок маніпулювання значеннями керованих параметрів у відповідь на вхідні впливи. Загальновизнаного формалізованого критерію функціональної якості ІСКЗ на даний час немає – форма і вміст критерію визначається в залежності від умов експлуатації ІС, її цільового призначення, і головне – бажаного рівня інформаційної безпеки, адже саме цей показник може знизити безпосередні показники функціональної якості ІСКЗ. Це дозволяє описати задачу управляння захистом ІП у ІСКЗ як задачу пошуку такого набору значень керованих параметрів, при якому для даного моменту часу рівень надійності ІП є максимальним за умови, що кількість витрачених на заходи убезпечення ресурсів не перевищує граничний. Дослідження [51, 54] залежності значення критерію функціональної якості ІСКЗ від запровадженого рівня інформаційної безпеки показали, що найбільше падіння функціональної якості ІСКЗ спричиняє діяльність додатків розмежування доступу і контролю цілісності

ІнР, що визначає першочергову важливість заходів з оптимізації якості процесу функціонування цих системних сервісів. При цьому під якістю програмного сервісу [157–160] розумітимемо зважене кількісне представлення таких його характеристик як:

– функціональність – сукупність властивостей, визначена вмістом і конкретними особливостями множини функцій СІБ ІСКЗ, здатної задовольнити документально і де-факто задані вимоги щодо захисту інформації від несанкціонованого доступу тощо;

– надійність – сукупність властивостей, що характеризують здатність СІБ протягом визначеного інтервалу часу зберігати заданий рівень придатності при експлуатації ІСКЗ у регламентованих умовах;

– зручність використання – сукупність властивостей СІБ, що характеризує зусилля, необхідні для підтримування її функцій, представлені у формі кількісних оцінок або індивідуальних оцінок, даних суб’єктами-користувачами;

– ефективність – сукупність властивостей СІБ, що характеризує залежність аспектів рівня її придатності від характеру і часу використання системних (матеріальних, апаратних, програмних, людських) ресурсів і послуг у відповідному обсязі та за визначених умов експлуатації ІСКЗ;

– супроводжуваність – сукупність властивостей СІБ, що характеризує зусилля, потрібні для її модифікації;

– мобільність – сукупність властивостей СІБ, що характеризує її адаптивність до зміни умов експлуатації ІСКЗ.

Втім, варто відзначити орієнтацію цієї таксономії на оцінювання інформаційної безпеки ІСКЗ на етапі проектування, тоді як результати її функціонування, здебільшого, враховуються лише у двох останніх сукупностях властивостей.

Процес комплексного забезпечення надійності ІП у ІСКЗ можна розглянути і як окремий випадок процесу моделювання інформаційної технології, яку створено для розв’язання таких задач як:

– адекватний опис інформаційної технології формальною моделлю, яка визначеною множиною правил перетворень для контактних точок інтерфейсу ІСКЗ описує взаємодію суб'єктів-користувачів із рівнем фактично реалізованої системи;

– відтворення у синтезованих моделях певних властивостей інформаційної технології – структурних властивостей, властивостей забезпечення надійності ІП як потоків даних, властивостей забезпечення цілісності ІП тощо;

– узагальнена математична формалізації процесу проектування інформаційної технології у парадигмі відповідної математичної теорії, зокрема, теорії автоматів [161–164], теорії графів [165–168], теорії формальних мов [169–171], теорії алгоритмів [172–175], теорії імовірності і математичної статистики [176–180] тощо.

Здійснений якісний і структурний аналіз ІСКЗ дозволяє стверджувати доцільність ґрунтовнішої формалізації процесів синтезу її СПБ, оцінювання атрибутів гарантоздатності і їх взаємозв'язку, що можна забезпечити лише результатами математичного моделювання у відповідній парадигмі, вибір якої потребує додаткового аналізу.

Вибір теорії графів для моделювання надійності ІП у ІСКЗ припустимий лише на початковому етапі проектування, адже властива цій теорії загальність не дозволить адекватно описати нюанси функціонування СІБ. Теорія абстрактних автоматів фактично створена для опису процесів переходу між станами із урахуванням перехідних функцій. Абстрактний автомат можна описати і орієнтованим графом, вершини якого відповідають станам автомата, а дуги – переходам із визначеними перехідними функціями.

Втім, для опису перебігу ІП у ІСКЗ краще підходить проблемно-орієнтований клас орієнтованих графів – мережі Петрі [181–185], спеціально створені для узагальненого опису паралельних процесів. Основними складовими елементами мереж Петрі є події і умови, між якими допустимі зв'язки виду: умова може бути передумовою однієї або множини подій; умова може бути постумовою однієї або множини подій. Графічно події зображуються відрізками, умови –

колами, зв'язки – стрілками. Подія реалізовується, якщо виконано всі передумови і не виконано жодної постумови. Після реалізації події всі її передумови стають невиконаними, а всі постумови – виконаними. Факт реалізації події залежить від маркування і змінює його. Представивши ІС мережею Петрі можна досліджувати її еквівалентність, структуру, поведінку, цілісність, живучість, досяжність тощо.

Еволюційним розвитком математичного апарату мереж Петрі став підклас оцінних (обмежених) мереж Петрі [185–188]. Оцінна мережа Петрі – це двочастковий орієнтований граф, утворений із вершин двох типів – позицій і переходів, з'єднаних дугами, при чому кожна дуга може з'єднувати тільки перехід із позицією або позицію із переходом. На відміну від мереж Петрі, у ОМП:

– допускають існування декількох типів позицій;

– на з'єднання позицій і переходів накладено додаткові обмеження;

– динамічні елементи мережі – об'єкти можуть характеризуватися множиною атрибутів;

– із кожним переходом можна асоціювати операцію часової затримки і операцію перетворення атрибутів об'єктів;

– позиції дозволу організовують процеси умовного розгалуження і переключення при переміщенні об'єктів відповідно до значень їх атрибутів.

У ОМП допускають існування простих позицій (круг), позицій-черг (овал) і позицій дозволу (квадрат). Переходи у ОМП зображають відрізком лінії. Позиції і переходи з'єднуються дугами, при чому у кожну позицію може входити і виходити лише одна дуга. Формально описати ОМП можна кортежем $E = \langle S, T, I, J, M \rangle$, де S – скінченна непуста множина позицій, утворена неперетинними множинами простих позицій Q, позицій черг $\widetilde{Q}$ і позицій дозволу P: $S = Q \cup \widetilde{Q} \cup P$; T – скінченна непуста множина переходів; $I : T \to 2^S$ – вхідна функція, яка для кожного переходу визначає множину вхідних позицій, тобто позицій, дуги із яких направлено до переходу; $J : T \to 2^S$ – вихідна функція, яка для кожного переходу визначає множину вихідних позицій, тобто позицій, на

яких закінчуються дуги, які почалися на переході; $M : S = \{0,1,2,\ldots\}$ – функція розмітки, яка визначає маркування позицій.

Дуга із з'єднуваними нею позицією і переходом є структурною зв'язкою, а сукупність, утворена переходом t і множиною всіх структурних зв'язок, де перехід t задіяний, називають елементарною мережею E_t. В кожній елементарній мережі може бути лише одна позиція дозволу, причому така позиція має бути вхідною. Позиція дозволу виконує функцію управління на початку фази реалізації переходу і характеризується скінченною множиною станів і видом операції дозволу. Результат операції дозволу визначається атрибутами об'єктів, які знаходяться в позиціях тієї ж елементарної мережі, що і позиція дозволу, а також від атрибутів об'єктів в позиціях інших елементарних мереж. У позиціях дозволу ОМП можна реалізовувати і випадкові переходи, тоді перехід характеризується значеннями імовірності реалізації відповідних вихідних позицій. Позиція, яка містить об'єкт є маркованою – $M(p)$, де M – кількість об'єктів, що перебувають на позиції p. Проста позиція може містити один об'єкт, позиція-черга – довільну їх кількість. Динаміка ОМП описується переміщенням об'єктів із одних позицій в інші із зміною відповідних маркувань.

Наведений опис дозволяє стверджувати потенційну ефективність апарату ОМП для структурного опису ІП ІСКЗ та синтезу її СПБ. Оцінювання атрибутів гарантоздатності ІСКЗ і їх взаємозв'язку потребує узгодження стохастичних величин із різними законами розподілу, та врахуванням ступінчастого характеру системних ІП. Ці особливості можна врахувати здійснюючи відповідне математичне моделювання у парадигмі напівмарковських процесів [189–192].

Узагальнимо матеріал підрозділу однозначно сформулювавши таксономію гарантоздатності, яку застосовуватимемо для оцінювання якості функціонування ІСКЗ, представивши першу на рис. 1.1. При цьому матеріал Додатку А містить додаткову інформацію щодо математичної формалізації інформаційних процесів у ІСКЗ.

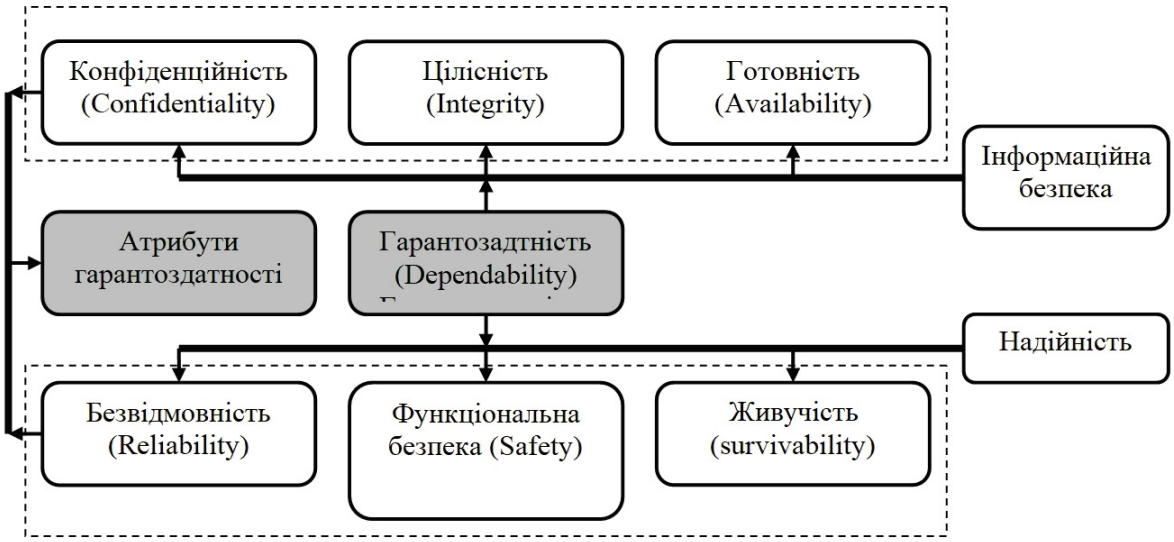


Рисунок 1.1 – Таксономія гарантоздатності для оцінювання ІСКЗ.

Також узагальнимо матеріал підрозділу визначивши ІСКЗ як підклас ІС, специфікою якого є:

– інформаційні ресурси, керовані об’єктно-реляційною СУБД, яка здійснює контроль їх цілісності;

– інформаційне середовище, яке реалізує тільки визначену на етапі проектування множину функцій, включаючи підтримку інтерфейсу суб’єкт-системної взаємодії. Реалізація відповідних функцій відбувається у виділених інформаційних процесах із інтегрованим контролем цілісності і конфіденційності;

– систему інформаційної безпеки, яка управляє рівнем конфіденційності із врахуванням поточної ресурсовитратності функціонального стану ІСКЗ відповідно до правил системної політики безпеки;

– керовану системою інформаційної безпеки підсистему захисту від несанкціонованого доступу, яка здійснює автентифікацію суб’єктів-користувачів, управляє процесом надання доступу відповідно до ролей користувачів, передбачених у системі, та поточного рівня готовності.

Визначною ознакою ІСКЗ є достовірна прогнозованість всіх ІП, забезпечувана адекватними профільними математичними моделями із

можливістю розрахунку атрибутів гарантоздатності як системи загалом, так і її складових зокрема.

1.2 Аналіз процесу автентифікації суб'єкта за голосом

Ключову роль у забезпеченні конфіденційності ІСКЗ відіграє підсистема захисту від несанкціонованого доступу, основною функцією якої є автентифікація особи суб'єкта, який ініціював сеанс суб'єкт-системної взаємодії. Процес автентифікації [103, 107, 114, 194], який полягає у встановленні достовірності суб'єкта-користувача або суб'єкта-програмного додатка як результату аналізу значень його істотних характеристичних параметрів, має два різновиди – верифікацію та ідентифікацію. Верифікація – бінарний процес, результатом якого є або ототожнення особи суб'єкта із деяким еталоном, або ні, а ідентифікації – мультиваріантний процес, який полягає у попарному порівнянні параметричного опису суб'єкта, що ідентифікується, та елементів множини еталонів із формуванням кількісної оцінки як результату кожної операції порівняння. Втім коректність обох варіантів процесу автентифікації забезпечується адекватністю математичної моделі, яка функціонально узагальнює параметричний опис суб'єкта, який формується на основі множини довільних, але достатньо репрезентативних індивідуальних ознак: програмного чи апаратного ключа, біометричних ознак тощо.

За природою походження індивідуальні ознаки для автентифікації розділяють на оптичні, магнітні, радіочастотні і біометричні [195].

Оптичні ознаки утворюються в результаті аналізу інтерпретації зображення видимих символів – штрих-коду, «капчі» тощо. Репрезентативність такої ознаки є низькою і на даний час дозволяє достовірно вирішувати лише задачу верифікації типу «людина»-«комп'ютер».

Магнітний сценарій процесу автентифікації полягає у аналізі записаних на магнітну стрічку символів. Цей спосіб є надійнішим від попереднього, адже потребує фізичної наявності відповідної магнітної карти із парольною інформацією, проте арсенал «кардерів» [196] дозволяє з легкістю зробити

копію оригінальної карти. Саме тому на практиці цей варіант реалізації процесу автентифікації додатково підсилюється символьним паролем.

Радіочастотний варіант процесу автентифікації передбачає радіочастотний обмін автентифікаційними даними із транспондером – RFID-міткою. Завдяки вживаним методам кодування недоліком цього варіанту автентифікації є лише відокремленість ключа доступу від особи суб’єкта. Фізично підробити RFID-мітку набагато складніше, порівняно із магнітними картами.

Біометричний варіант автентифікації полягає в інтерпретації результатів цільового аналізу оцифрованого представлення певної унікальної характеристики людини: ДНК, рисунку відбитків пальців або сітківки ока, голосу тощо. Перелік біометричних ознак весь час доповнюється, наприклад, нещодавно TD Bank і MasterCard сумісно із компанією Nymi розробили і тепер успішно впроваджують індивідуальні браслети для безконтактних платежів із технологією автентифікації користувачів за серцевим ритмом HeartID. Перевагою біометричних ознак є потенційна невідокремність від фізичного носія-людини, неможливість втрати, зручність використання (для більшості ознак) тощо. Недоліком, який поки що знижує частоту застосування біометричних ознак у процесі автентифікації, є властива біологічним сигналам комплексність та інформативність, що обумовлює необхідність застосування складних методів екстрагування репрезентативних цифрових представлень біометричних індивідуальних ознак та потужних методів аналізу для безпосередньої реалізації процедури автентифікації на їх основі. Втім, на рис. 1.2 візуалізовано дані прогнозу, зробленого у 2016 р. міжнародною консалтинговою компаніє J’son&Partners. Згідно із цим прогнозом, об’єм світового ринку біометричних систем безпеки до 2022 р. має скласти вражаючі 40,20 млрд. дол. США із середнім за рік темпом зростання у 18,6 %.

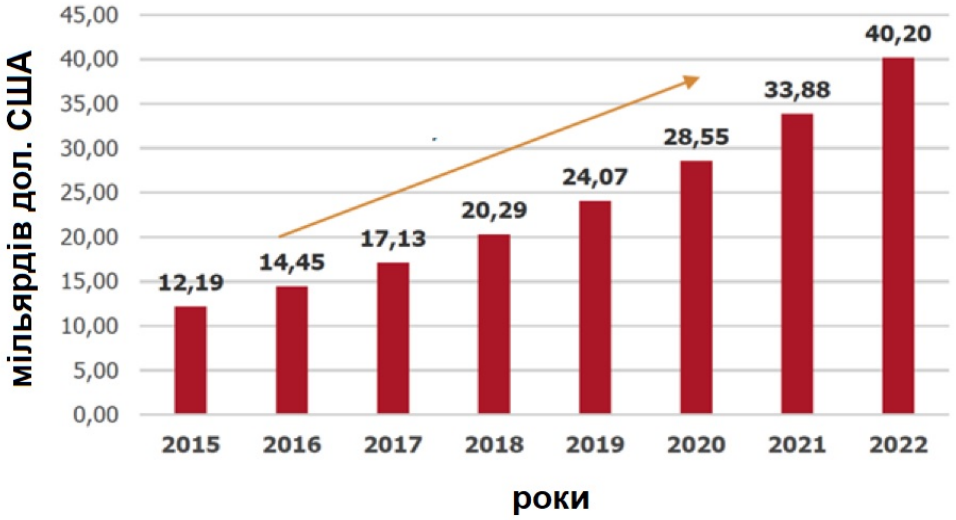


Рисунок 1.2 – Прогноз зростання об’єму світового ринку біометричних систем безпеки, зроблений J’son&Partners Consulting.

Цікавим є і прогноз сегментації цього ринку на 2022 р. за типами біометричних індивідуальних ознак, результати якого представлено на рис. 1.3.

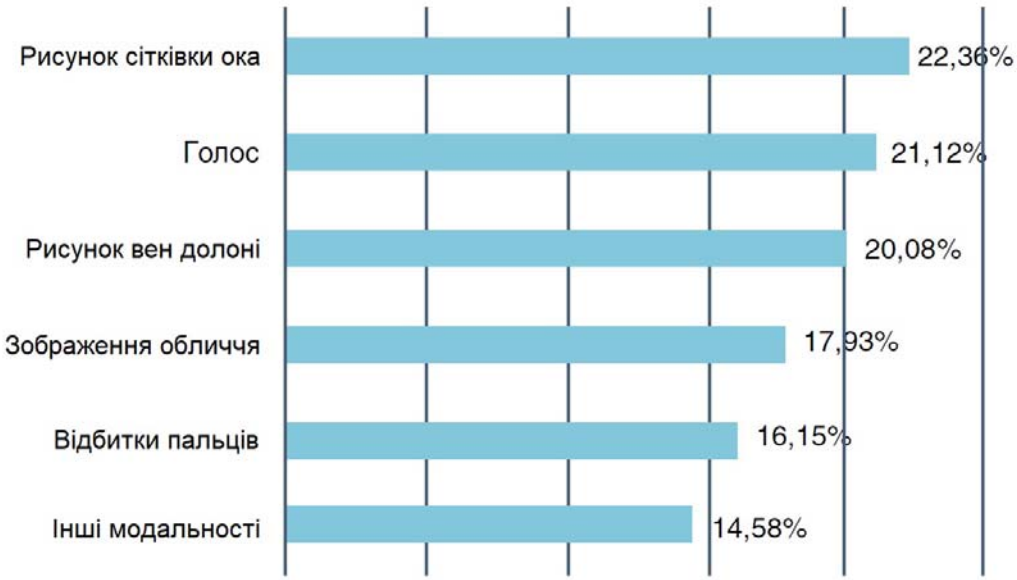


Рисунок 1.3 – Прогноз сегментації світового ринку біометричних систем безпеки у 2022 р. за типом біометричної ознаки, зроблений J’son&Partners Consulting.

Зауважимо, що у 2018 р. цей прогноз пройшов валідацію консалтинговою компанією Yole Development із визнанням його коректності. Як видно з рис. 1.3,

найстрімкіше зростання (на понад 20 %) спостерігатиметься серед систем безпеки із використанням найскладніших для інтерпретації біометричних індивідуальних ознак – рисунку сітківки ока, голосу, рисунку вен долоні тощо. На думку автора, цю обставину пов'язано із вражаючою динамікою зростання обчислювальної потужності мобільних платформ, вживаних у смартфонах, які стають невід'ємним атрибутом сучасної людини у корпоративному і соціальному секторах, зокрема.

Окрім державного сектора, розвиток і впровадження біометричних технологій автентифікації, зокрема, за голосом, помітний у банківському секторі. Вже зараз у call-центрах двох найкрупніших банків Сінгапуру (DBS і OCBC) використовують системи біометричної ідентифікації клієнтів за голосом. Міжнародний фінансовий конгломерат CityGroup запустив систему двофакторної біометричної автентифікації за голосом в азіатському регіоні для клієнтської аудиторії, яка налічує понад 1 млн. осіб. Англійський банк Barclays також використовує у своїй роботі голосову біометрію. У банку Banco Santander Mexico впроваджують біометричну автентифікацію за голосом для 1,5 млн. аудиторії клієнтів. Окрім комерційного застосування, біометричні системи АСГ використовують і в криміналістичній сфері для протидії терористичній загрозі та спостереження за мовленнєвими контактами підозрюваних.

Деталізуємо сучасні тенденції, щодо систем АСГ. За виглядом результату прийнятого рішення системи АСГ розділяють на системи верифікації суб'єкта і системи ідентифікації суб'єкта. Відповідні структурні схеми систем наведено на рис. 1.4 і 1.5.

Система верифікації суб'єкта за голосом розраховує оцінку ідентичності – міру близькості моделі фонограми суб'єкта, який автентифікується, із відповідною еталонною моделлю голосу зареєстрованого суб'єкта. Якщо значення оцінки ідентичності перевищує встановлений адміністратором поріг, то суб'єкт, який автентифікується, отримує доступ, якщо ж оцінка ідентичності є меншою або рівною пороговому значенню, то запит на доступ суб'єкта, який автентифікується, відхиляється.

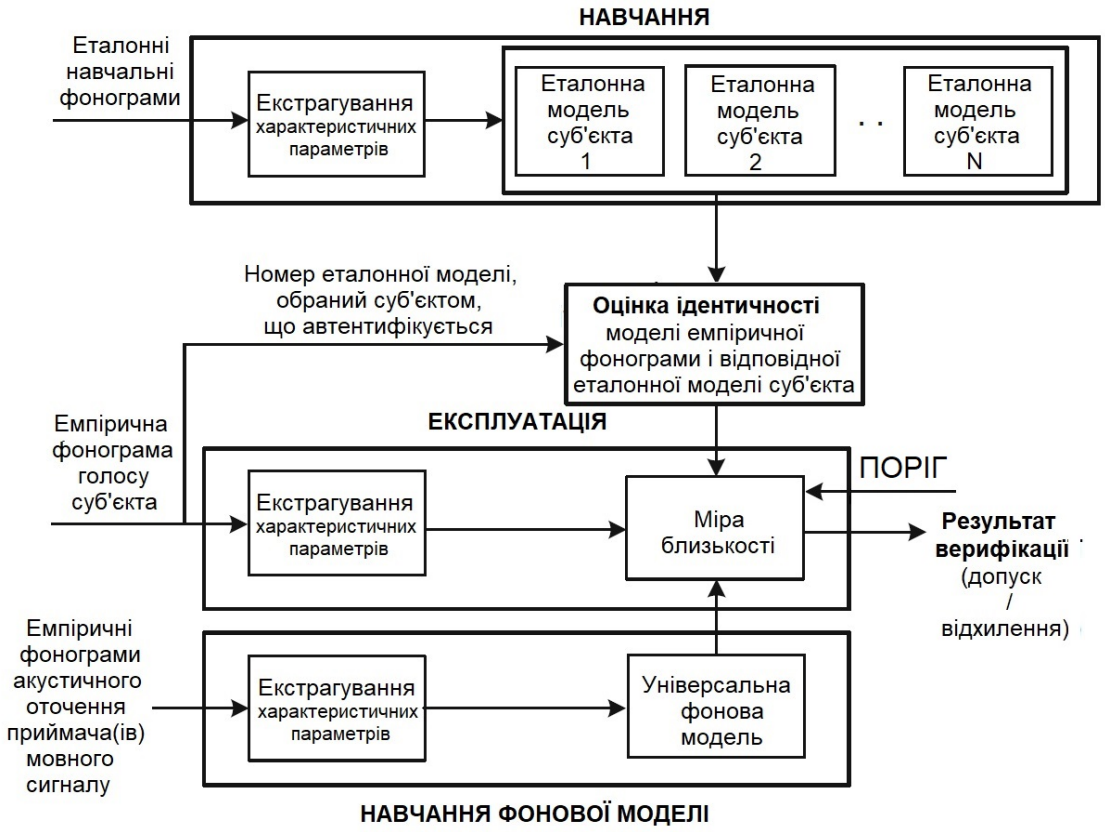


Рисунок 1.4 – Структурна схема системи верифікації суб’єкта за голосом.

У процесі порівняння оцінки ідентичності із порогом враховується вплив акустичного оточення приймача(ів) мовленнєвого сигналу на емпіричний мовленнєвий сигнал, представлений вхідною фонограмою з метою зменшення імовірності визнання «суб’єкта» – «антагоністом». Тут варто відзначити, що фундаментальними якісними характеристиками функціонування систем АСГ є:

– α – імовірність похибки першого роду, або похибка помилкового недопуску, є імовірнісною оцінкою ситуації недопуску системою санкціонованого суб’єкта (визнання «суб’єкта» – «антагоністом»);

– β – імовірність похибки другого роду, або похибка помилкового допуску, є імовірнісною оцінкою ситуації допуску системою несанкціонованого суб’єкта (визнання «антагоніста» – «суб’єктом»).

Варіювати співвідношенням значень похибок можна змінюючи значення порогу прийняття рішень. Також варто відзначити, що кожна із цих похибок

окремо не дає цілісної оцінки якості функціонування системи автентифікації – слід враховувати обидва типи похибок у вигляді, наприклад, квадрату їх півсуми.

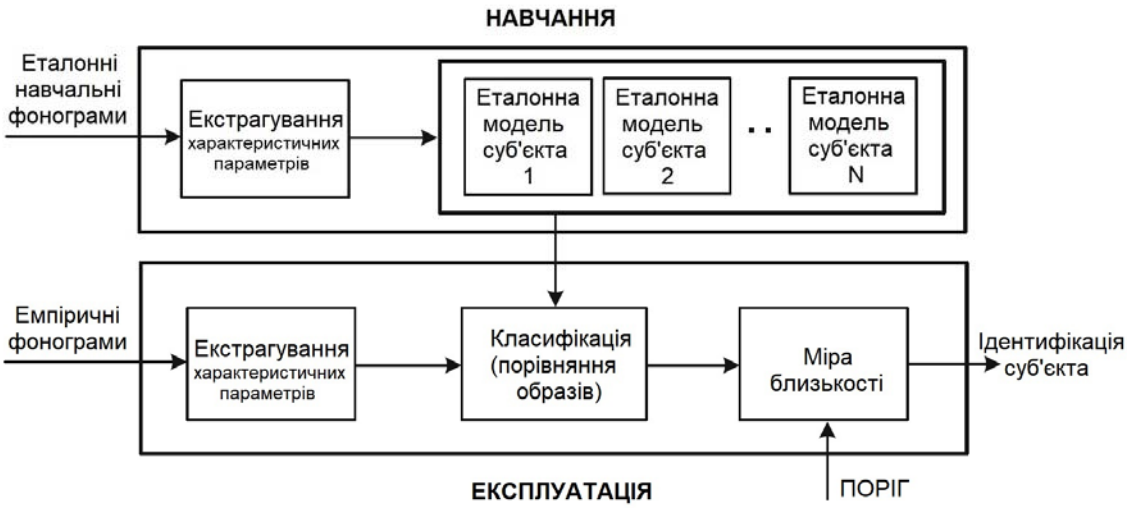


Рисунок 1.5 – Структурна схема системи ідентифікації суб’єкта за голосом.

Відмінністю системи ідентифікації суб’єкта за голосом від системи верифікації того ж призначення полягає в тому, що наперед не відомо з якою еталонною моделлю суб’єкта порівнювати модель емпіричної фонограми. Відповідно, порівняння здійснюється попарно із всіма еталонними моделями суб’єктів. Кількісним результатом процесу попарних порівнянь є вектор оцінок ідентичності, значення якого порівнюються із пороговим за допомогою вибраної міри близькості. Якщо значення елемента вектора оцінок ідентичності виявилося меншим або рівним пороговому, то суб’єкт, що ідентифікується, однозначно не асоціюється системою автентифікації із особою суб’єкта, якому належить відповідна еталонна модель голосу. Окремим випадком є ситуація, коли жоден з елементів вектора оцінок ідентичності не перевищив порогового значення – це означає, що суб’єкт, який ідентифікується, не зареєстрований у системі. Серед елементів вектора оцінок ідентичності, які перевищили поріг, за допомогою розв’язувального правила вибирається найбільша, а номер еталонної моделі суб’єкта, що їй відповідає, і є результатом ідентифікації.

Якщо провести аналогію із сферою інформаційної безпеки, то система верифікації суб'єкта за голосом органічно інтегрується у двофакторну схему автентифікації, де в якості першого фактора виступає оптична, магнітна, радіочастотна система або ж система класичної авторизації виду «логін»-«пароль», а другим фактором – біометрична система верифікації суб'єкта за голосом. Отже, перший фактор дозволяє суб'єкту, який автентифікується, аргументовано ототожнити себе із конкретною особою суб'єкта, зареєстрованого у системі, а другий, біометричний – підвищує конфіденційність процесу автентифікації. Система ідентифікації суб'єкта за голосом підходить для організації однофакторної схеми автентифікації, яка потенційно є менш безпечною.

За форматом вхідної фонограми системи АСГ розділяють на текстозалежні і текстонезалежні. У перших змістовний склад фонограми нормується, а у других – ні, тобто автентифікація суб'єкта здійснюється за фонограмою із мовленнєвим сигналом довільного лінгвістичного змісту. Системи, що відносяться до першого типу, є простішими як структурно, так і в експлуатації, але вони мають і вужчу сферу застосування. Для навчання таких систем необхідно набагато менше мовленнєвого матеріалу. У структуру текстонезалежних систем АСГ доводиться вводити підсистему лінгвістичного аналізу мовленнєвого сигналу, фактично – систему розпізнавання мови, адже для того, щоб коректно порівняти емпіричну і еталонну моделі голосу необхідно спочатку встановити тотожність лінгвістичного вмісту фонограм, з яких вони екстраговані. Окрім складнішої структури текстонезалежних систем, складнішою є і процес їх навчання, адже система, фактично, повинна вивчити ту мову, якою говоритиме цільовий суб'єкт. Ця обставина обумовлює як ускладнення вбудованого класифікатора, так і наявності відповідної еталонної навчальної бази фонограм мовленнєвих сигналів – спеціалізованого мовленнєвого корпусу. Відмітимо, що на даний час для української мови розроблено два офіційних мовленнєвих корпуси – Корпус текстів української мови розроблений співробітниками лабораторії комп'ютерної лінгвістики Інституту філології Київського національного університету імені Тараса Шевченка [197] і Генеральний регіонально анотований корпус української

мови [198]. Втім, це корпуси лінгвістичного застосування, тобто їх вміст не розмічено для застосування у задачах АСГ або розпізнавання мови. Є англомовні спеціалізовані корпуси [200, 201]: TIMIT, SWITCHBOARD, YOHO, KING, NOIZEUS, POLYCOST та ін. Всі ці корпуси мають свої індивідуальні властивості, але спільним є великий обсяг даних для аналізу (для деяких із згаданих корпусів – сотні гігабайт).

За ступенем залучення людини у процес прийняття рішень системи АСГ розділяють на автоматичні і автоматизовані. У перших, відповідно, всі інтегровані у процес АСГ підпроцеси реалізуються автоматично, без залучення людини. У других – людина, зазвичай, залучається після утворення моделі емпіричної фонограми для здійснення її цільового аналізу. В таких системах застосовують специфічні засоби візуалізації характеристичних параметрів моделі індивідуальності мовленнєвих сигналів, зручні для людини-експерта.

Структурні схеми системи верифікації та ідентифікації суб’єкта за голосом, наведені на рис. 1.4, 1.5, дозволять узагальнити структуру системи АСГ у формі послідовно з’єднаних блоків: параметризації мовленнєвого сигналу; синтезу еталонної моделі голосу; прийняття рішень. Проаналізуємо наукове підґрунтя кожного з них.

Еволюція сформувала артикуляційний апарат людини з орієнтацію на передавання, перш за все, семантичної інформації у формі продукту акту мовленнєвої комунікації – мовленнєвого сигналу. Втім, властива біологічним системам висока індивідуальність проявила себе і у варіативності мовленнєвих сигналів. Мозок людини, аналізуючи мовленнєвий сигнал, детермінує цю варіативність, що дозволяє нам ідентифікувати особу, якій аналізований мовленнєвий сигнал належить. Адекватна математична модель цього процесу дозволяє здійснювати АСГ використовуючи для цього значення певних характеристичних параметрів, екстрагованих із мовленнєвого сигналу. Відома акустична модель фонації [202–205] виділяє у складі артикуляційного апарату людини такі елементи як мовленнєве джерело (голосові зв’язки), акустичний фільтр (резонатори артикуляційного тракту), модулятор (губи). Кожен із цих

елементів привносить у мовленнєвий сигнал індивідуальну компоненту, описати яку можна із різною достовірністю. В контексті задачі АСГ, основним характеристичним параметром мовленнєвого джерела є період (частота) основного тону і похідні характеристики [207, 208]. Ці параметри характеризуються високою індивідуальністю, але низькою завадостійкістю.

При описі акустичного фільтра використовують два підходи – перший описує індивідуальні характеристики мовленнєвого сигналу як результат зміни форми резонаторів в наслідок функціонування активних артикуляційних органів у акті фонації, а другий аналізує безпосередньо мовленнєвий сигнал як продукт функціонування артикуляційного тракту в парадигмі теорії акустики [209–211] методами цифрового оброблювання сигналів [212, 213]. Аналітично перший підхід втілюється у систему диференціальних рівнянь високих порядків, яку часто просто неможливо розв’язати безпосередньо. Ця обставина зумовлює спрощення рівнянь у складі системи аж поки її розв’язок не стане досяжним. Наслідком спрощення є зниження достовірності опису індивідуальних характеристик мовленнєвого сигналу підсумковою моделлю. Втім, навіть при синтезі вихідної системи рівнянь припускаються суттєвих узагальнень, ніяк не відповідних об’єкту моделювання, наприклад, резонаторам артикуляційного тракту не властива осьова симетрія.

У другому підході аналізується форма акустичної хвилі, як продукту процесу фонації. Сам процес фонації розглядається як продукт функціонального синтезу двох компонентів – передатної функції і генератора імпульсів, де перша представляє систему резонаторів артикуляційного тракту, а другий – мовленнєве джерело. Передатна функція адекватно описує чотири формантні області [205], що дозволяє розрахувати значення таких індивідуальних параметрів мовленнєвого сигналу як середню частоту, частотний діапазон і енергію кожної форманти, їх траєкторії, обвідну спектра і похідні параметри. Генератор імпульсів описує роботу мовленнєвого джерела і дозволяє оцінити значення параметрів основного тону. Передатна функція описує статичні властивості процесу фонації, а генератор імпульсів – динамічні. Також артикуляційну динаміку мовленнєвого

сигналу можна описати методами спектрально-темпорального аналізу [214–217], але варто зважати на те, що адекватність такого опису визначатиметься ступенем досягнутої синхронності відтворення впливу активних органів артикуляційного апарату на значення параметрів спектрального представлення мовленнєвого сигналу.

Якщо вдатися до формального аналізу мовленнєвого сигналу, то адекватний цільовий його опис можна отримати на основі перетворення Фур'є [218] і лінійного передбачення [218] у вигляді множин основних спектральних компонентів, кепстральних параметрів, коефіцієнтів лінійного передбачення, зокрема, перцептивних коефіцієнтів лінійного передбачення [218]. Враховуючи, що мовленнєвий процес є вкрай динамічним, всі вищезгадані підходи до його параметризації залишаються адекватними, якщо описують короткотривалі, 10–30 мс, фрагменти мовленнєвого сигналу – інтервали стаціонарності [218].

Найпростішим способом аналізу більш тривалих фрагментів мовленнєвих сигналів є просте усереднення множин значень згаданих вище характеристичних параметрів. Вживають і більш складні методи узагальнення на основі прихованих марковських моделей [189–192], динамічного програмування [219–221], машинного навчання [222–226] тощо. Доцільність довготривалого аналізу обґрунтовується тим, що більшість шумів акустичного оточення, присутніх у фонограмі мовленнєвого сигналу, є короткочасними, отже, при коректному узагальненні множини характеристичних параметрів ступінь впливу шумів на результат автентифікації можна зменшити.

Інший підхід до пошуку індивідуальних параметрів мовленнєвого сигналу полягає в аналізі процесу їхнього сприйняття слуховою системою людини, якій властива здатність як розпізнавання мови, так і розпізнавання мовця тощо. Модель слухового сприйняття [208, 214, 216] дозволяє зменшити обчислювальну складність задачі параметризації мовленнєвого сигналів для подальшої АСГ обмежившись отриманням миттєвих розподілів спектра мовленнєвого сигналу і окремих фонем. На досягнення тієї ж мети спрямований і гомоморфний метод [218]. Він дозволяє представити короткочасний фрагмент мовленнєвого сигналу

компактною множиною кепстральних коефіцієнтів, які апроксимують формантний розріз із високою спектральною роздільною здатністю, представляючи таким чином найбільш інформативну для слухового сприйняття частину спектра. Кепстральний опис мовленнєвого сигналу є також основою кепстрального методу екстрагування частоти основного тону [207, 208]. Втім для опису цієї індивідуальної ознаки відомі і такі класичні методи як метод Голда-Рабінера [227] і кореляційний метод [228]. Якщо галузеве призначення системи автентифікації дозволяє аналізувати тривалі мовленнєві сигнали у яких проявляється індивідуальність вимови відповідного фонетичного вмісту, то для опису таких мовленнєвих сигналів використовують середньозважений спектр. Ключовим параметром при цьому стає висота голосу, яку, наприклад, оцінюють усередненим значенням частоти основного тону на визначеному фрагменті мовленнєвого сигналу.

Також відмітимо, що універсального набору характеристичних параметрів для опису мовленнєвих сигналів у задачі АСГ немає – в залежності від галузі застосування створюваної системи оптимальна множина характеристичних параметрів утворюється емпірично. Визначна важливість інформативності параметричного представлення мовленнєвих сигналів в контексті задачі автентифікації суб’єкта за голосом зумовила проведення поглибленого аналізу актуальних математичних моделей мовленнєвих сигналів, результатом якого стала концепція параметризації мовленнєвих сигналів, наведена на рис. 1.6. Теоретичний матеріал, покладений в основу наведеної на рис. 1.6 концепції викладено в Додатку Б.

Після параметризації мовленнєвого сигналу у парадигмі обраного математичного апарату актуальною стає задача прийняття рішень за результатами порівняння вектора характеристичних параметрів, екстрагованих із емпіричного мовленнєвого сигналу, представленого суб’єктом для автентифікації, та еталонними наборами характеристичних параметрів, які зберігаються у системі автентифікації для зареєстрованих суб’єктів.

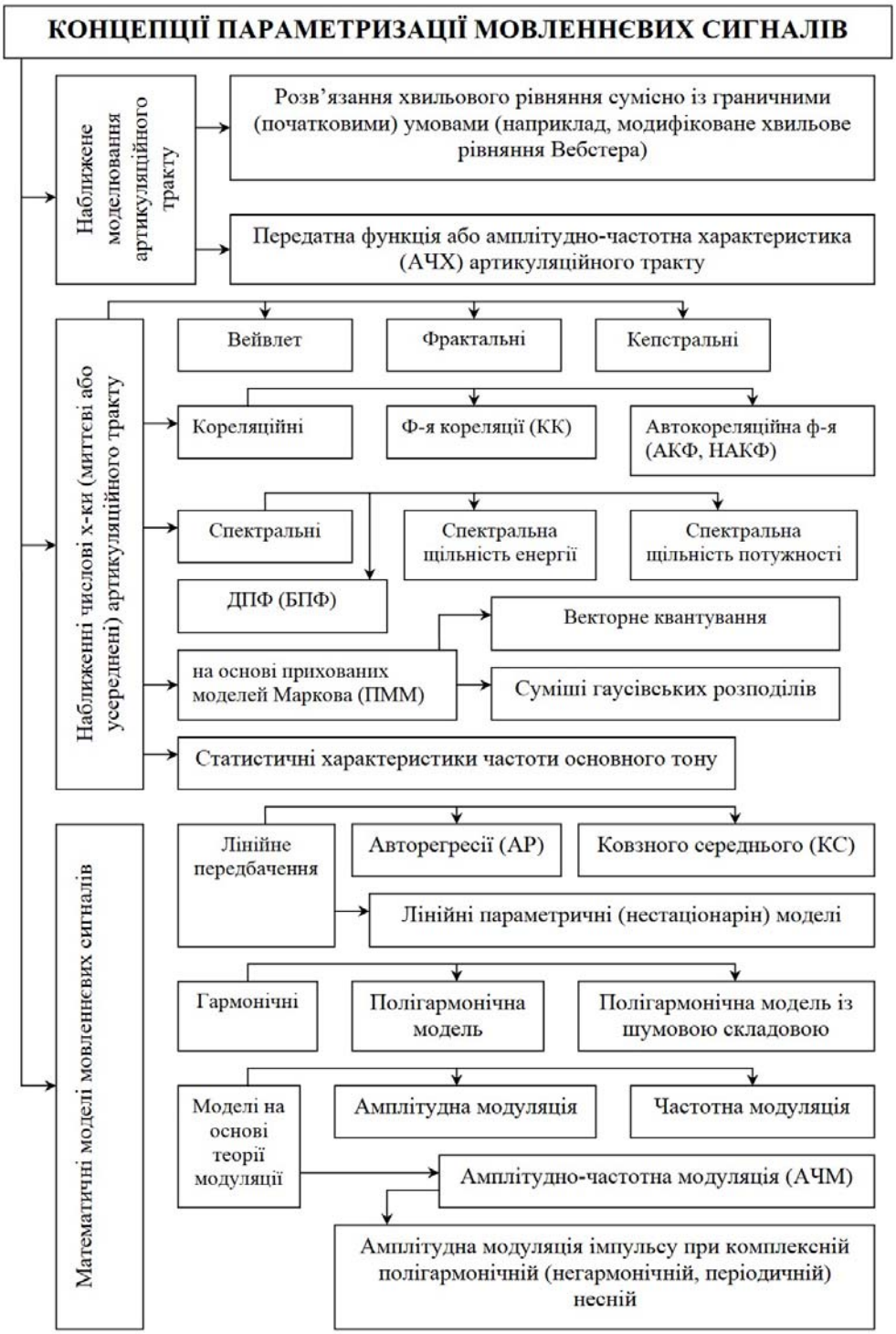


Рисунок 1.6 – Концепція параметризації індивідуальних характеристик голосу у мовленнєвому сигналі.

У задачі верифікації рішення приймається відносно порогового значення, встановленого відповідно до заданих рівнів імовірностей похибок першого і другого роду. Ці рівні залежать від застосування системи. Якщо обсяг навчальної

бази невеликий, то природно всі параметри розподілу похибок визначити неможливо. В такому випадку для цільового суб'єкта розраховується оцінка математичного сподівання похибок. Дисперсія, відповідно, розраховується для певної групи суб'єктів і є інтегральною якісною характеристикою системи – саме відштовхуючись від її значення доцільно обирати значення порогу прийняття рішень. Втім, якщо обсяг навчальної бази фонограм для цільового суб'єкта є статично репрезентативним, то дисперсію можна розраховувати для суб'єкта персонально, відповідно встановлюючи, і індивідуальний поріг. Також зауважимо, що відбір даних для розрахунку групової дисперсії можна здійснювати обираючи фонограми, наприклад, за типом або рівнем відношення «сигнал»/«шум», отримуючи таким чином множину значень порогу прийняття рішень, адаптованих до диференціальних умов експлуатації системи автентифікації. При розрахунку математичного сподівання і дисперсії вважають, що закон розподілу похибок наближається до нормального.

У задачі ідентифікації рішення приймають за спрощеною схемою – без оцінювання параметрів розподілу похибок для цільового суб'єкта. Значення порогу прийняття рішень встановлюють відповідно до значення критерію мінімізації похибок для навчальної бази фонограм. Також у задачі ідентифікації допускається варіювання метрикою параметричного простору [229–232] – не обмежуючись евклідовою, використовують метрики Чебишева, Хеммінга, кореляційної функції тощо.

Як видно з рис. 1.4, 1.5, система АСГ функціонує в двох режимах – навчання і експлуатації. У режимі навчання суб'єкт реєструється у системі для чого, зазвичай, йому необхідно кілька разів вимовити генеровану системою автентифікації парольну фразу тривалістю 3–5 секунд. Утворені у такий спосіб фонограми сегментуються на усереднені відрізки, які параметризуються, а отримані в результаті вектори характеристичних параметрів усереднюються, утворюючи еталон голосу відповідного суб'єкта. Еталон голосу зберігається в системі автентифікації в безпосередньому вигляді, втім, допускається застосування до еталону процедур стиснення без втрати інформації. На стадії

сегментації мовленнєвих сигналів на усереднені відрізки допустимою є процедура передопрацювання, під час якої із сегмента фонограми вирізаються фрагменти-«паузи», компенсуються або фільтруються шуми, енергетичні сплески тощо. Враховуючи, що вміст парольної фрази вибирається адміністратором, продуктивним є здійснювати сегментацію на усереднені відрізки не довільно, а з урахуванням семантики парольної фрази, виділяючи в окремі фрагменти записи фонем базової мови. В залежності від обраної конфігурації параметричного простору отримані усереднені відрізки описуються інтегральними характеристичними параметрам або додатково сегментуються на короткочасні фрейми, які описуються відповідними наборами характеристичних параметрів, при чому для уникнення крайових ефектів, властивих спектральному представленню вмісту фреймів, допускається перекриття границь останніх на 25–50 % їх тривалості.

В режимі експлуатації системи верифікації суб'єкта за голосом відбувається порівняння представленої суб'єктом, який автентифікується, фонограми із записом вимовленої парольної фрази або її частини з еталоном на основі обчислених відстаней D_j, $j=\overline{1,M}$, у N-вимірному параметричному просторі, де M – кількість векторів характеристичних параметрів, які описують порівнювані об'єкти. Якщо, наприклад, значення $d=\sum_{j=1}^{M} D_j$ не перевищує значення встановленого порогу D_0, то результатом верифікації буде надання доступу суб'єкту, який автентифікується. Якщо у системі автентифікації аналізується індивідуальність вимови окремих фонем, то рішення приймається на основі аналізу розташування максимумів взаємокореляційних функцій характеристичних параметрів, що представляють емпіричний і еталонний сигнали, відповідно.

Звичайно, стабільність значень характеристичних параметрів є суттєво відносною, що визначається багатьма факторами – станом здоров'я суб'єкта, його емоціональним станом, акустичним оточенням і схемою розташування приймача(ів) мовленнєвого сигналу тощо. Вплив цих факторів настільки розмиває межі кластерів, які відповідають цільовим суб'єктам, у параметричному просторі,

що при достатньо великій кількості зареєстрованих у системі автентифікації суб'єктів, кластери можуть перекриватися. Запобігти цьому не змінюючи правил експлуатації системи, тривалості та вмісту парольної фрази, конфігурації параметричного простору до певної міри можна застосовуючи нормалізацію. При цьому слід враховувати, що процедура нормалізації, притягуючи до центра найближчого кластера емпіричний образ, деформує границі решти кластерів, не змінюючи відносні ступені їх перекриття, тобто застосування нормалізації не призводить до зменшення імовірностей виникнення похибок першого і другого роду.

При формалізованому методі прийняття рішень, відомій конфігурації і метриці параметричного простору та ідентифікованому імовірнісному розподілі характеристичних параметрів, процес вибору порогу ідентифікації формалізується у задачу оптимізації. Якщо необхідно максимально запобігти ситуації отримання доступу несанкціонованими суб'єктами – слід мінімізувати імовірність похибки другого роду, максимізуючи при цьому імовірність виникнення похибки першого роду. Зростання імовірність похибки першого роду, спричиняє, відповідно, зростання кількості випадків недопуску санкціонованих суб'єктів, зменшуючи таким чином готовність ІС, доступ до якої захищено системою автентифікації. Втім, така схема дозволяє підтримувати конфіденційність процесу автентифікації за встановленому адміністратором рівні.

Завершуючи огляд теоретичної забезпеченості процесу автентифікації суб'єкта за голосом, доцільно прослідкувати еволюцію наукової думки, що втілилася в описані вище результати. На десятиліття раніше перших спроб програмного розпізнавання мови, у 1960-х роках, зафіксовано перші спроби програмної АСГ (англ., «Speaker Recognition»). Одним із піонерів напрямку був С. Прузанський з компанії Bell Labs, який порівнював цифрові спектрограми, отримані за допомогою банку фільтрів. До удосконалення методики С. Прузанського долучилися колективи на чолі із М. Метьюзом і К. Лі, який, зокрема, застосував у процесі порівняння лінійні дискримінатори. Вкладом Г. Доддінгтона з кампанії Texas Instruments в еволюцію АСГ стало застосування формантного

аналізу для параметризації мовленнєвих сигналів. Також важливу проблему варіативності характеристик мовленнєвого сигналу одного мовця досліджували наукові колективи, очолювані В. Ендресом і С. Фуруі.

У 1970-х роках проводилися дослідження з усереднення довготривалих фрагментів мовленнєвих сигналів у формі статистичних чи прогностичних характеристичних параметрів, придатних для застосування у задачі текстонезалежної АСГ. Досліджували, зокрема, усереднену автокореляцію (П. Брікер), миттєві матриці коваріації спектрів (К. Лі), гістограми спектра та частоти основного тону (Б. Бік), коефіцієнти лінійного передбачення (М. Самбур) та параметри довготривалого усереднення спектра (С. Фуруі). Властива текстонезалежним системам АСГ ресурсовитратність зумовила розвиток текстозалежних систем цього класу та пов’язаних із ними методів нормалізації тривалості фонетичних одиниць мовленнєвих сигналів у часовому вимірі. Дослідженнями у цьому напрямку займалися наукові колективи Б. Атала, С. Фуруі, А. Розенберга тощо. Компанія-новатор Texas Instruments першою запровадила у експлуатацію високонадійну текстозалежну систему АСГ, у якій особа суб’єкта розпізнавалася на основі результатів спектрального аналізу фонограми парольної фрази з чотирьох слів, які система пропонувала для виголошення, вибираючи з-поміж 16 доступних односкладових слів. За шість років експлуатації система здійснила мільйони сеансів розпізнавання сотень мовців. Колектив С. Фуруі з компанії Bell Labs створив експериментальну систему АСГ, мовленнєві сигнали в яку надходили телефонними каналами зв’язку. Мовленнєві сигнали параметризувалися комбінацією кепстральних, Δ- і ΔΔ-кепстральних коефіцієнтів. Активна піврічна експлуатація системи 120 мовцями дозволила виявити необхідність періодичного оновлення еталонів фонограм мовців та уточнення порогів прийняття рішень. Ці ж дослідження дозволили С. Фуруі та Б. Аталу формалізувати метод спектрального вирівнювання, призначений для зменшення лінійних канальних ефектів та довготривалої спектральній варіативності, які проявилися при передаванні мовленнєвих сигналів телефонними каналами зв’язку.

Цей метод, заснований на кепстральному представленні мовленнєвих сигналів, дозволив суттєво підвищити надійність процесу текстозалежного АСГ.

У 1980-х роках розпочався дрейф методології АСГ від методів, заснованих на класичній теорії розпізнавання образів, до методів, заснованих на теорії імовірності та математичної статистики і теорії математичного моделювання. Отримані у цей період наукові результати, удосконалені в 1990-х роках, знаходять своє впровадження і в актуальних сьогодні системах АСГ. Безсумнівно, в 1980-х роках на розвиток систем АСГ найбільше вплинула теорія прихованих моделей Маркова. Слід відзначити, що провісником цієї теорії була теорія динамічного згортання часу (DTW), запропонована колективом на чолі із Т. Вінцюком [160, 233]. Водночас не можна не згадати, що піонером напряму досліджень щодо можливості автентифікації мовця за індивідуальністю голосу серед радянських вчених є Г. Рамішвілі [162]. У першій половині 1980-х ця теорія здебільшого адаптувалася до задач АСГ науковими колективами компаній IBM, Dragon Systems, а також Інституту аналізу оборони (IDA, США), а в другій половині 1980-х розпочалося її практичне впровадження у системи АСГ. ПММ застосовувалися як для АСГ так і для програмного розпізнавання мови. У парадигмі цього математичного апарату будувалися надійні моделі мовленнєвих подій на основі результатів параметризації нетривалих навчальних фонограм із записами мовленнєвих сигналів. У побудованій на основі ПММ системі текстозалежного АСГ моделі мовців синтезувалися для кожної семантичної одиниці фонограми, включаючи і модель для пауз у мовленнєвому сигналі. Значний вклад в адаптацію і впровадження апарату ПММ у процес АСГ внесли колективи, керовані Л. Рабінером, Д. Фергюсоном, Д. Найком. У задачі текстонезалежного АСГ почали застосовувати параметричні та непараметричні імовірнісні моделі. Прикладне застосування непараметричних імовірнісних моделей втілилося у запропонований А. Розенбергом метод векторного квантування, який дозволяв знайти проекцію векторів характеристичних параметрів, екстрагованих із короткотривалих фрагментів фонограми мовленнєвого сигналу, на простір меншої розмірності, отримуючи компактну

кодову книгу для характеристики мовця. М. Сугіяма і Д. Фергюсон запропонували матричний квантувач для опису послідовності короткотривалих фреймів. В якості параметричної імовірнісної моделі для задачі текстонезалежного АСГ застосовували апарат ПММ, зокрема, А. Поріц синтезував ергодичні ПММ з п’ятьма станами для опису парольних висловлювань, а Н. Тішбі розширив цю концепцію до ергодичної авторегресійної ПММ з вісьмома станами, представленої неперервними функціями щільності імовірності, які описували кожен стан моделлю суміші з кількістю компонент від двох до восьми, що дозволило підвищити спектральну роздільну здатність вихідної ергодичної ПММ. Ця ж концепція надихнула Р. Роуза і Р. Рейнольдса на дослідження завадостійкості ПММ із одним станом, яку згодом розвинули у модель СГР і активно використовують у системах АСГ досі.

У 1990-х роках увагу дослідників привернула задача підвищення шумостійкості систем АСГ. Зокрема, колектив на чолі із Т. Мацуі порівняв у задачі текстонезалежного АСГ метод векторної квантифікації із методами, заснованими на моделюванні мовленнєвих сигналів дискретними і неперервними ергодичними ПММ. Результати порівняння показали зіставну шумостійкість неперервних ергодичних ПММ і векторного квантування за умови репрезентативної навчальної вибірки, у той час як дискретні ергодичні ПММ показали суттєво гірші результати. Подальші дослідження проводилися із неперервними ергодичними ПММ, у яких змінювали кількість станів і компонент сумішей. Виявилося, що достовірність розпізнавання мовців здебільшого визначалася кількістю компонент СГР, а не кількістю станів ПММ, що емпірично доводило більшу інформативність фонетичної складової парольного сигналу над когнітивною для задачі АСГ. Цей же колектив дослідив можливість синхронного опису миттєвих і перехідних характеристичних параметрів мовленнєвого сигналу, представлених кепстральними коефіцієнтами і частотою основного тону, відповідно, у кодовій книзі векторного квантувача. Результатом дослідження стала нова міра для оцінювання варіативності характеристик мовленнєвих сигналів різних суб’єктів, придатна і для оцінювання дрейфу значень характеристик мовленнєвих сигналів із часом. Дослідження

емпірично довели, що сумісне використання спектральних характеристик і частоти основного тону у задачі АСГ дозволяє суттєвого підвищити достовірність автентифікації, порівняно із експериментами, де ці характеристичні параметри використовувалися окремо. Колектив, очолюваний Р. Роузом, спробував описати мовленнєві сигнали, записані в умовах шумного акустичного оточення, комбінованою ПММ, утвореною індукуванням параметрів ПММ, яка моделювала мовленнєвий сигнал без шуму, із параметрами ПММ, яка моделювала шум акустичного оточення суб'єкта-мовця. Згодом колектив, очолюваний Т. Матцуі поглибив дослідження комбінованої ПММ, створивши множину ПММ, кожна з яких моделювала певний рівень потужності шумів акустичного оточення мовця. Аналіз множини значень правдоподібностей результатів попарного порівняння ПММ, яка моделювала емпіричний мовленнєвий сигнал із шумом, із кожною комбінованою ПММ дозволив ідентифікувати рівень відношення «сигнал»/«шум» для емпіричного мовленнєвого сигналу. Також продовжувалися дослідження варіативності характеристик мовленнєвих сигналів із часом, зокрема, А. Хіггінс запропонував обчислювально ефективний «когортний» метод нормалізації мовленнєвих сигналів, заснований на апостеріорній імовірності і рівні правдоподібності.

У 2000-х роках питання нормалізації мовленнєвих сигналів у задачі АСГ продовжило розвиток. Зокрема, колектив Ф. Бімбота запропонував плеяду score-методів нормалізації, у яких характеристики мовленнєвого сигналу нормалізувалися шляхом віднімання математичного сподівання та ділення результатів на показник дисперсії, де обидва показники оцінювалися на основі розподілу параметрів мовленнєвих сигналів «псевдо порушника». Розвинулися технології адаптації і компенсації для підвищення достовірності систем АСГ на основі СГР-представлення мовленнєвих сигналів. Наприклад, колектив на чолі із М. Маклареном запропонував технології компенсування при формуванні супервекторів для машини опорних секторів, які дозволили знизити вплив варіативності мовленнєвих сигналів між сеансами розпізнавання і прогнозувати потенційну ненадійність сеансів розпізнавання. Дослідження А. Петрі формалізувалися у модель самоадаптації системи АСГ до шумів у мовленнєвих сигналів на основі імовірнісного оброблювання матеріалів

навчальної вибірки фонограм. Суттєве зростання обчислювальної потужності комп'ютерної техніки дозволило практично реалізувати комбіновані, аудіо-візуальні, системи АСГ, у яких паралельно аналізується мовленнєвий сигнал і динаміка руху губ суб'єкта-мовця. Такі системи спонукали дослідження процесу прийняття рішень ансамблем класифікаторів. Зокрема, досліджувалися системи із мажоритарним голосуванням при синтезі вердикту щодо особи суб'єкта-мовця, який автентифікувався, а вердикт для ансамблю класифікаторів із імовірнісними виходами отримувався як результат лінійного або мультиплікативного комбінування. Окрім того, розвинувся напрямок систем АСГ із каскадами класифікаторів, у яких значення на виходах ансамблю первинних класифікаторів об'єднувалися у вектори, які згодом аналізувалися класифікаторами вищого рівня, зазвичай, машинами опорних векторів, бінарними деревами рішень, нейромережевими класифікаторами тощо. Колектив, очолюваний К. Легетером, запропонував метод лінійної регресії максимуму правдоподібності для самоадаптації ПММ-моделей у задачі АСГ з метою підвищення надійності процесу автентифікації. Цей метод виявився ефективнішим за попередні, тому активно впроваджується у системи АСГ і зараз.

У 2010-х роках тенденції, закладені у 2000-ні роки збереглися. Втім, активно впроваджуються технології машинного навчання у системи АСГ. Зокрема, глибокі та згорткові нейромережі використовуються як для прийняття рішень, так і адаптації й нормалізації мовленнєвих сигналів. Окрім того, навчені нейромережі із «bottleneck» шаром самі стають джерелом характеристичних параметрів для автентифікації суб'єкта-мовця. Дослідження галузі «Speaker Recognition» продовжують наукові установи, зокрема, Massachusetts Institute of Technology (США), John Hopkins University (США), Carnegie Mellon University (США), Cambridge University (В. Британія), Kyoto University (Японія), LIMSI-CNRS (Франція), Fondazione Bruno Kessel (Італія), RWTH (Німеччина), École de Technologie Supériure (Канада), МНЦІТС НАНУ та МОНУ (Україна), СПИИРАН (РФ), та комерційні компанії, зокрема, Alfabet/Google (США), Nuance Communications (США), AT&T (США), IBM (США), Microsoft (США), Facebook (США), Vocapia (Франція), Acapela Group (Франція), Loquendo (Італія), Sedat85

(Італія), Samsung (Корея). Також слід відмітити тенденцію до проведення челенджів з метою відкритого порівняння якісних характеристик актуальних систем автентифікації суб'єкта за голосом. Зокрема, для задачі «automatic speaker verification» найрепрезентативнішими є Automatic Speaker Verification Spoofing and Countermeasures Challenge (ASVSCC) (archive.signalprocessingsociety.org/technical-committees/list/sl-tc/spl-nl/2015-11/2015-11-ASVspoof/), Voxsrc: The first voxceleb speaker recognition challenge (https://arxiv.org/abs/1912.02522) і Mobile Biometry (MOBIO) Face and Speaker Verification Evaluation (idiap.ch/webarchives/sites/www.mobioproject.org/icpr-2010.html). У цих проектах досліджувалися десятки систем автоматичної верифікації суб'єктів за голосом, які показали результати, наведені на рис. 1.7. Ці дані можуть стати орієнтиром для оцінювання перспективності представлених в дисертаційній роботі наукових і прикладних результатів щодо автентифікації суб'єкта за голосом.

Отже, актуальність забезпечення високої достовірності процесу автентифікації суб'єкта-користувача підсистемою захисту від несанкціонованого доступу у складі ІСКЗ обумовлює пошук надійних схем автентифікації. Тенденції розвитку систем інформаційної безпеки дозволяють передбачити перспективність двофакторної схеми верифікації для управління доступом до ІСКЗ, де першим фактором виступатиме традиційна процедура верифікації із використанням індивідуальних карт доступу із магнітною або радіочастотною схемою інформаційного обміну та авторизацією виду «логін»/«пароль», а другим фактором – процедура верифікації суб'єкта-користувача за голосом. При цьому необхідно розв'язати задачі ідентифікації оптимальної конфігурації простору стійких до шуму характеристичних параметрів для опису фонограм мовленнєвих сигналів, способу прийняття рішень щодо результату верифікації та встановлення рівня порогу прийняття рішень. Враховуючи критичне застосування цільової ІС надійність результату верифікації превалює над готовністю системи, що обумовлює потребу в ідентифікації зв'язку між відношенням «сигнал»/«шум» у вхідній фонограмі та порогом прийняття рішень.

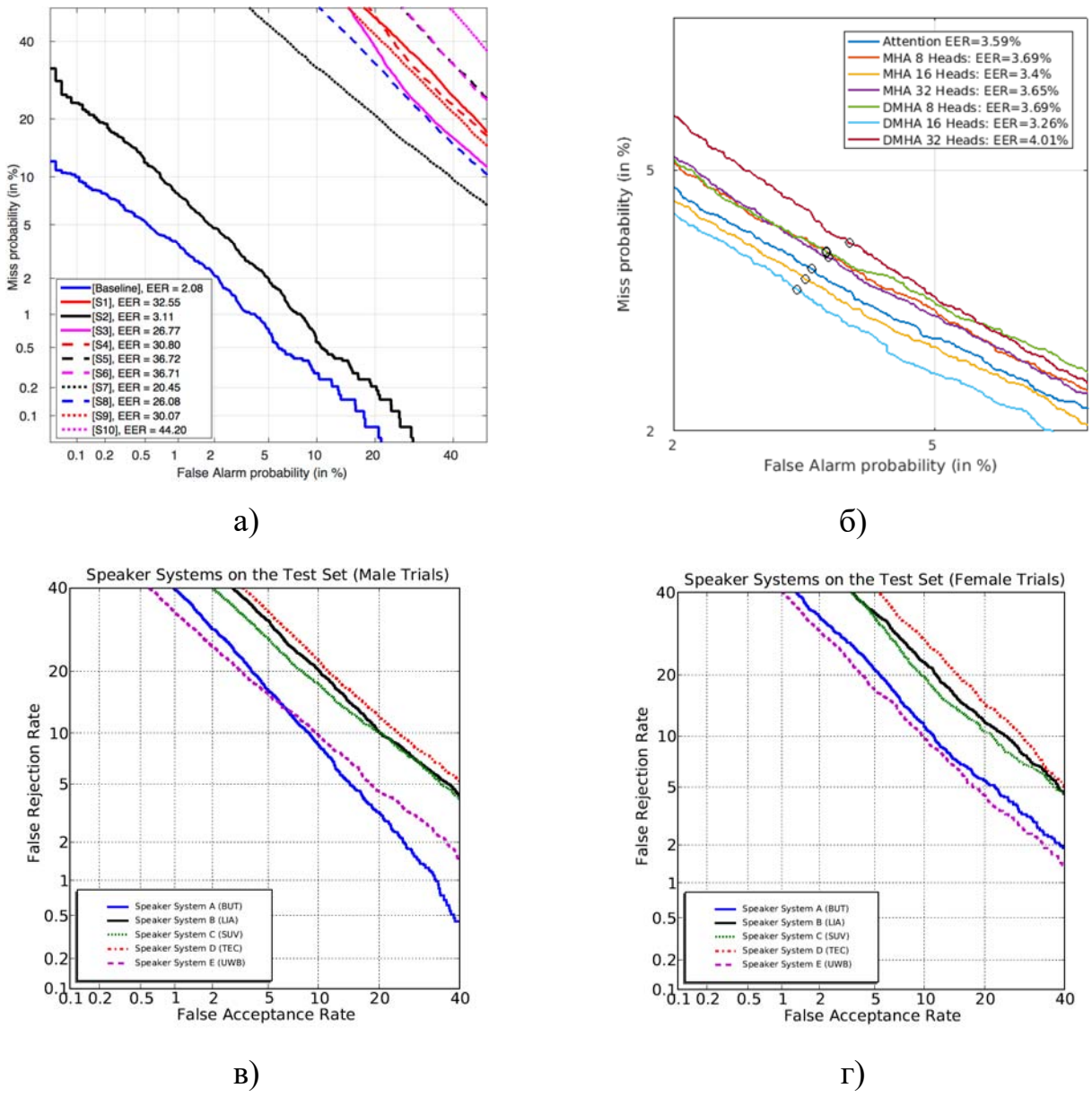


Рисунок 1.7 – Якісні результати систем автоматичної верифікації суб’єктів за голосом, представлені на челенджі: а) ASVSCC, б) Voxsrc, в) MOBIO male, г) MOBIO female.

Втім, доцільним є і отримання адекватних моделей компенсації шумів у вхідному мовленнєвому сигналі із врахуванням впливу результату компенсації на достовірність автентифікації, адже компенсація шумів дозволить експлуатувати систему автентифікації у реальному акустичному оточенні приймачів мовленнєвих сигналів, зменшивши кількість сеансів повторного запиту мовленнєвого матеріалу з причини неприйнятно високого вмісту шумів, тобто

суттєво зменшити втрати готовності. Також доцільним є впровадження перспективних завадостійких класифікаторів для прийняття рішень у системі АСГ, оптимізувавши їх для зменшення ресурсовитратності процесу навчання.

1.3 Вибір напряму, мети та постановка завдань дослідження

В Законах України «Про основи національної безпеки», «Про оборону України», «Про інформацію», «Про телекомунікації”, “Про захист інформації в інформаційно-телекомунікаційних системах», «Про основні засади забезпечення кібербезпеки України» присутні нові для нашої держави, але досить тривіальні для закордону, терміни «критичний об’єкт» і «критична інфраструктура». Визначення цих термінах у законодавчих актах відрізняється. Найбільш повно термін «об’єкт критичної інфраструктури» розкрито в Постанові Кабінету Міністрів № 563 від 23.08.2016 як «підприємства та установи (незалежно від форми власності) таких галузей, як енергетика, хімічна промисловість, транспорт, банки та фінанси, інформаційні технології та телекомунікації (електронні комунікації), продовольство, охорона здоров’я, комунальне господарство, що є стратегічно важливими для функціонування економіки і безпеки держави, суспільства та населення». Сучасні реалії декларують невід’ємність існування об’єкту критичної інфраструктури та його інформаційної системи. Втім, законодавчого визначення такої спеціалізованої інформаційної системи навіть на рівні простого переліку структурних і функціональних особливостей досі немає. Дана обставина зумовила концентрацію наукових розробок, втілених у дисертаційну роботу, навколо «інформаційної системи критичного застосування», визначеної як підклас інформаційних систем у підрозділі 1.1. Аналіз наукових робіт, присвячених спеціалізованим інформаційним системам, дозволив узагальнити ІСКЗ як сукупність інформаційних ресурсів, керованих об’єктно-реляційною СУБД, яка здійснює контроль їх цілісності; інформаційного середовища, яке реалізує тільки визначену на етапі проектування множину функцій, реалізація яких, включаючи підтримку інтерфейсу суб’єкт-системної взаємодії, відбувається у виділених інформаційних процесах із інтегрованим

контролем цілісності та конфіденційності останніх; підсистеми інформаційної безпеки, яка, відповідно до правил технічного рівня системної політики безпеки, управляє рівнем конфіденційності із врахуванням поточної ресурсовитратності функціонального стану ІСКЗ; керовану підсистемою інформаційної безпеки підсистему захисту від несанкціонованого доступу, яка здійснює автентифікацію суб’єктів-користувачів, управляє процесом надання доступу відповідно до ролей користувачів, передбачених у системі, та поточного обсягу вільних обчислювальних ресурсів ІСКЗ. Технічне спрямування наукових розробок зумовило пошук цілісної метрики, в якій можна було б якісно та кількісно охарактеризувати як ІСКЗ загалом, так і її складових окремо. Аналіз результатів інформаційного пошуку, представлених в підрозділ 1.1, показав, що єдиною метрикою, що повно характеризує ІСКЗ, є метрика гарантоздатності, яка складається з таких атрибутів як конфіденційність, цілісність, готовність, функційна безпечність, живучість, безвідмовність. Необхідність у прогнозованості процесу експлуатації ІСКЗ із урахування її структурної специфіки та конкурентної природи атрибутів гарантоздатності зумовлює потребу в створенні системного теоретично-прикладного комплексу для вирішення актуальної ***науково-прикладної проблеми*** забезпечення гарантоздатності інформаційних систем критичного застосування, здатного розв’язати об'єктивне протиріччя між:

– існуванням розподілених структурованих інформаційних систем критичного застосування, визначною рисою яких має бути 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 відомих негативних факторів;

– одночасно 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 в зловмисників напрацьованих технологій нейтралізації стандартних методів автентифікації суб’єктів-користувачів, з іншого боку.

Забезпечити підвищення конфіденційності ІСКЗ, враховуючи останню обставину, вдається можливим лише вдавшись до нетипових технологій автентифікації суб’єктів-користувачів, найперспективнішими з яких, як показав аналіз результатів інформаційного пошуку, наведених у підрозділі 1.2, є методи і технології біометричної автентифікації. Матеріали досліджень, узагальнені на рис. 1.3 зумовили орієнтацію саме на автентифікацію суб’єктів за індивідуальними особливостями голосів, як найперспективнішу на даний момент.

Отже, **метою** дисертаційної роботи полягає у підвищенні гарантоздатності інформаційної системи критичного застосування шляхом розроблення і реалізації методів і засобів для оптимізації останньої 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 оптимізації взаємозалежності готовності і цілісності системи як відповідної задачі математичного програмування;

– формалізувати методи оптимізації індикаторів функційної безпечності і живучості інформаційної системи критичного застосування із постановкою відповідних задачі математичного програмування;

– синтезувати 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.

Висновки до першого розділу

1. Концентратором теоретичних і практичних новацій у галузі гарантоздатних систем в Україні є регулярна міжнародна науково-технічна конференція «Dependeble systems, services&technologies» (DESSERT). Багаторічний досвід і представлені на конференції результати узагальнено у перспективній програмі дій у галузі гарантоздатності, у якій визнано перспективними дослідження, спрямовані на розробку і розвиток методологічних засад, методів аналізу і синтезу гарантоздатних комп’ютеризованих систем для різних галузей застосування, а також, інформаційних технологій, які забезпечують процеси створення, верифікації і експлуатації таких систем. Найперспективнішими напрямками досліджень визнано, зокрема: Методологічні аспекти теорії і практики гарантоздатних (надійних і безпечних) систем; Методологія і принципи гарантоздатності як комплексної властивості комп’ютерних і телекомунікаційних систем і мереж; Формальні методи розробки систем із високими вимогами щодо безпеки; Аналіз і оцінка гарантоздатності. Критерії і метрики її оцінки; Взаємозв'язок критеріїв і показників оцінки гарантоздатності; Засоби і методики оцінки гарантоздатності; Моніторинг і оцінка гарантоздатності композитних веб-сервісів, інфраструктур; Розвиток імовірнісних моделей і методів оцінки гарантоздатності програмного забезпечення. Аналіз інформаційних ресурсів виявив, що дослідження за загаданими напрямками ведуться у контексті прикладного застосування у галузях атомної енергетики, авіаційної і ракетно-космічної техніки, систем спеціального призначення тощо із акцентуванням уваги на апаратній складовій таких критичних систем. Втім, сучасні тенденції, закладені у платформу Індустрія 4.0 і спрямовані на інформаційну інтеграцію кіберфізичних систем обумовлюють актуальність адекватного формального опису процесів життєдіяльності саме інформаційної складової критичних систем – ІСКЗ, у таксономії атрибутів гарантоздатності, що і обмовило спрямування досліджень, результати яких представлено у дисертації.

2. Узагальнюючи теоретичні і прикладні дані щодо математичного моделювання інформаційних систем, формалізуємо ІСКЗ як підклас ІС. У складі

типового екземпляру ІСКЗ виділимо: Інформаційні ресурси, керовані об'єктно-реляційною СУБД, яка здійснює контроль їх цілісності; Інформаційне середовище, яке реалізує тільки визначену на етапі проектування множину функцій, включаючи підтримку інтерфейсу суб'єкт-системної взаємодії. Реалізація відповідних функцій відбувається у виділених інформаційних процесах із інтегрованим контролем цілісності і конфіденційності; Систему інформаційної безпеки, яка управляє рівнем конфіденційності із врахуванням поточної ресурсовитратності функціонального стану ІСКЗ відповідно до правил системної політики безпеки; Керовану системою інформаційної безпеки підсистему захисту від несанкціонованого доступу, яка здійснює автентифікацію суб'єктів-користувачів, управляє процесом надання доступу відповідно до ролей користувачів, передбачених у системі, та поточного рівня готовності. Визначною ознакою ІСКЗ є достовірна прогнозованість всіх ІП, забезпечувана адекватними профільними математичними моделями із можливістю розрахунку атрибутів гарантоздатності як системи загалом, так і її складових зокрема.

3. Перспективним напрямком підвищення конфіденційності інформаційних систем та готовності їх підсистем розмежування доступу є інтеграція біометричних технологій верифікації у процес автентифікації суб'єктів–користувачів. З-поміж технологій біометричної автентифікації суб'єкта, системи автентифікації суб'єкта за голосом вирізняються низькою собівартістю, зручністю апаратної реалізації, комфортною доступністю біометричної ознаки. Водночас, на надійність автентифікації за голосом помітно впливає: природна варіативність голосу; апаратні спотворення; фонові шуми; надлишковість і загальність характеристичних параметрів існуючих математичних моделей мовленнєвих сигналів в контексті опису індивідуальності голосу; недосконалість критеріїв співставлення емпіричного і еталонного параметричних описів мовленнєвих сигналів при класифікації.

4. Серед актуальних математичних підходів найбільш компактний і аналітично коректний опис мовленнєвих сигналів забезпечує акустична теорія фонації, що робить цей математичний апарат перспективним для синтезу

інформативного параметричного опису індивідуальності голосу у мовленнєвому сигналі, яка найбільш проявляється на вокалізованих його сегментах. Особливої уваги варті полігармонічні моделі, здатні компактно описати періодичний характер вокалізованих сегментів мовленнєвого сигналу із урахуванням амплітудної і частотної варіативності відповідною амплітудною і частотною модуляцією. Цю інформацію узагальнено у наведеній на рис. 1.6 концепції параметризації індивідуальних характеристик голосу у мовленнєвому сигналі.

Основні результати розділу опубліковано в [30, 31, 33, 34, 36, 41, 43, 49, 50, 51, 52, 54, 60].

РОЗДІЛ 2
КВАЗІДЕТЕРМІНОВАНІ І СТОХАСТИЧНІ МОДЕЛІ ІНДИВІДУАЛЬНОСТІ ГОЛОСУ

2.1 Базова квазідетермінована модель індивідуальності голосу

Як свідчать інформаційні джерела [242–249], актуальним методам опису мовленнєвих сигналів властива низка недоліків, зокрема, можливість оцінювання від двох до п'яти формантних частот [247–249] та ігнорування впливу передатної (амплітудно-частотної) характеристики мовленнєвого тракту на індивідуальність мовленнєвих сигналів. Такі обмеження дозволяють суттєво спростити модель параметризації мовленнєвого сигналу, що, водночас, дозволяє розв'язувати задачі синтезування мовленнєвих сигналів [262, 264, 265] та розпізнавання мови [266, 267] із прийнятною достовірністю. Втім, такий спрощений опис мовленнєвих сигналів спричиняє втрати інформації, необхідної для АСГ, що обумовлює актуальність викладених далі досліджень.

Згідно із [207, 208, 247, 249], генерування мовленнєвого сигналу ініціюється проходженням струменя повітря з легенів мовленнєвим джерелом, яке породжує імпульси несних гармонічних коливань із частотою $f_l = lf_0$, де l – номер імпульсу, $f_0 = \overline{f_0}$ – середнє значення частоти основного тону [207, 208], які потрапляють у ротову і носову порожнини, що функціонують як резонатори, підсилюючи частоти вхідних імпульсів, які дорівнюють їх власним частотам $f_l = f_p^{(m_1,m_2,m_3)}$, і модулюються губами з частотою модулювального коливання F_0. Результат функціонування артикуляційного тракту людини у процесі модуляції L несних мовленнєвих імпульсів опишемо у формалізмі моделі спектрально-темпоральних рецептивних полів [214–217], представивши останню у вигляді

$$u(t) = \sum_{l=1}^{L} U_l(t)\cos(2\pi l t f_0 + \varphi_0) = \qquad (2.1)$$

$$=\left(1+M\cos\left(2\pi F_0 t+\Gamma_0\right)\right)\sum_{l=0}^{L}U_l\cos\left(2\pi l t f_0+\varphi_0\right),$$

де $t\in\left[0,\tau_i\right]$; φ_0 і τ_i – вихідна фаза і тривалість несного імпульсу, відповідно; $U_l(t)=U_l(1+Ms(t))$ і U_l – обвідна і амплітуда l-го імпульсу, відповідно; M – глибина модуляції; $s(t)=\cos\left(2\pi t F_0+\Gamma_0\right)$ – модулювальний сигнал із вихідною фазою модуляції Γ_0 і частотою модуляції F_0.

Модель (2.1) комплексно описує результат функціонування артикуляційного тракту людини, зокрема, присутні у (2.1) параметри несного імпульсу, обвідної і модулювального імпульсу характеризують, відповідно, вплив мовленнєвого джерела, резонаторів артикуляційного тракту і губ суб'єкта на індивідуальність утворюваного мовленнєвого сигналу. Враховуючи, що низькочастотна складова мовленнєвого сигналу U_0 зазнає суттєвого пригнічення у резонаторах артикуляційного тракту [249] та при $\phi_0=0$, $M=1$, $\Gamma_0=\pi$ вираз (2.1) набуває спрощеного вигляду

$$u(t)=2\left(\sin\left(\pi t F_0\right)\right)^2\sum_{l=1}^{L}U_l\cos\left(2\pi l t f_0\right). \tag{2.2}$$

Якщо сфокусувати модель (2.2) на описі індивідуальності голосних і сонарних приголосних звуків у мовленнєвому сигналі, які здебільшого утворюються завдяки функціонуванню мовленнєвого джерела [202–205], то характеристичними параметрами моделі виявляються частота основного тону і амплітуди несних імпульсів, описувані, відповідно, параметрами f_0 і U_l. Автоматизовану ідентифікацію значень цих керованих змінних можна забезпечити чисельними методами, орієнтованими на пошук глобальних максимумів багатоекстремальної функції обвідної мовленнєвого сигналу, при чому адекватність моделі (2.2) прямо визначатиметься точністю роботи обраного числового методу. Окрім цього на достовірність ідентифікації значень параметрів U_l впливає ширина частотної смуги в якій аналізується мовленнєвий сигнал, а достовірність ідентифікації параметра f_0 ускладнюється тим, що здебільшого глобальний максимум у амплітудному спектрі реєструється не на частоті основного тону, а на одній з її гармонік-обертонів

[207, 208]. Враховуючі ці обставини математично оцінювати адекватність опису дискретизованого мовленнєвого сигналу із відліками x_i, $i=\overline{0,N}$, моделлю (2.2), представленою відліками u_i, пропонується за результатами зіставлення значень відповідних нормованих автокореляційних функцій:

$$bu_j = Bu_j\left(Bu_0\right)^{-1} = B_u\left(j\right)\left(Eu\right)^{-1} = \left(Eu\right)^{-1}\sum_{i=0}^{N-1} u_i u_{i-j}\ ; \tag{2.3}$$

$$bx_j = Bx_j\left(Bx_0\right)^{-1} = B_x\left(j\right)\left(Ex\right)^{-1} = \left(Ex\right)^{-1}\sum_{i=0}^{N-1} x_i x_{i-j}\ , \tag{2.4}$$

де $j=\overline{0,J}$; Eu і Ex – потужність сигналу моделі і потужність мовленнєвого сигналу, відповідно; $Bu_j \equiv B_u\left(j\right)$ і $Bx_j \equiv B_x\left(j\right)$ – автокореляційні функції дискретного сигналу моделі $u_i \equiv u\left(i\Delta\right)$ і мовленнєвого сигналу $x_i \equiv x\left(i\Delta\right)$, відповідно; Δ – період дискретизації.

Функції (2.3), (2.4) дозволяють оцінити кореляційні залежності у сигналах в часовому вимірі і враховують структурні особливості об’єкта моделювання, адже автокореляційну функцію зв’язано зі щільністю потужності спектра оберненим перетворенням Фур’є. Для зменшення впливу аналого-цифрового перетворення на вміст мовленнєвого сигналу пропонується значення x_i у виразі (2.3) центрувати:

$$y_i = x_i - \bar{x} = x_i - N^{-1}\sum_{i=0}^{N-1} x_i\ ,\ i=\overline{0,N-1}. \tag{2.5}$$

Мірою близькості значень функцій (2.3) і (2.4) слугуватиме евклідова нев’язка, розраховувана за виразом:

$$\varepsilon_b = \sum_{j=1}^{J}\left(b_j^u - b_j^y\right)^2, \tag{2.6}$$

де b_j^y і b_j^u – нормовані автокореляційні функції досліджуваного центрованого мовленнєвого сигналу (2.4) і результату його опису математичною моделлю (2.2), відповідно. Отже, при $\varepsilon_b \to 0$ модель (2.2) найкращим чином описує ІГМС $y\left(t\right)$.

Аналітичний вираз для опису нормованої автокореляційної функції моделі (2.1) на часовому інтервалі $[0,\tau_i]$ матиме вигляд

$$b^u(\tau)=B_u(\tau)(B_u(0))^{-1}=B_u(\tau)(E_u)^{-1}, \tag{2.7}$$

де автокореляційна функція $B_u(\tau)$ імпульсного сигналу описується виразом

$$B_u(\tau)=\int_0^{\tau_i}u(t)u(t-\tau)dt. \tag{2.8}$$

Здійснимо оцінювання компонент B_u і E_u нормованої автокореляційної функції $b^u(\tau)$ для моделі (2.1) при $0\le\tau\le\tau_i$, $\varphi_0=0$, $\Gamma_0=\pi$ на основі запропонованого в [271, 272] методу оптимального оброблювання сигналу складного джерела з метою оцінювання його характеристичних параметрів:

$$B_u=\sum_{l=1}^{L}\sum_{m=1}^{L}U_lU_m\Bigg(I_1^u(\tau,l,m)+0,5M\sum_{i=2}^{5}I_i^u(\tau,l,m)+0,25M^2\sum_{i=6}^{9}I_i^u(\tau,l,m); \tag{2.9}$$

$$E_u=0,5\tau_u\sum_{l=1}^{L}\sum_{m=1}^{L}U_lU_m\Big(\big(1+0,5M^2\big)I_1^e(\tau,l,m)-MI_2^e(\tau,l,m)+0,25M^2I_3^e(\tau,l,m)\Big), \tag{2.10}$$

де множини функцій $\{I_i^u\}$, $i=\overline{1,9}$, і $\{I_j^e\}$, $j=\overline{1,3}$, є білінійними формами кореляційного інтегралу (2.8) для імпульсного сигналу, описуваного моделлю (2.1). Аналітичний вигляд цих функцій такий:

$$I_1^u=0,5(\tau_i-\tau)(\mathrm{sinc}(\pi(l+m)f_0(\tau_i-\tau))\cos(\pi(l-m)f_0\tau)+$$
$$+\mathrm{sinc}(\pi(l-m)f_0(\tau_i-\tau))\cos(\pi(l+m)f_0\tau));$$

$$I_2^u=-0,5(\tau_i-\tau)(\mathrm{sinc}(\pi((l+m)f_0+F_0)(\tau_i-\tau))\cos(\pi((l-m)f_0-F_0)\tau)+$$
$$+\mathrm{sinc}(\pi((l-m)f_0-F_0)(\tau_i-\tau))\cos(\pi((l+m)f_0+F_0)\tau));$$

$$I_3^u=-0,5(\tau_i-\tau)(\mathrm{sinc}(\pi((l+m)f_0-F_0)(\tau_i-\tau))\cos(\pi((l-m)f_0+F_0)\tau)+$$
$$+\mathrm{sinc}(\pi((l-m)f_0+F_0)(\tau_i-\tau))\cos(\pi((l+m)f_0-F_0)\tau));$$

$$I_4^u=-0,5(\tau_i-\tau)(\mathrm{sinc}(\pi((l+m)f_0+F_0)(\tau_i-\tau))\cos(\pi((l-m)f_0+F_0)\tau)+$$
$$+\mathrm{sinc}(\pi((l-m)f_0+F_0)(\tau_i-\tau))\cos(\pi((l+m)f_0+F_0)\tau));$$

$$I_5^u=-0,5(\tau_i-\tau)(\mathrm{sinc}(\pi((l+m)f_0-F_0)(\tau_i-\tau))\cos(\pi((l-m)f_0-F_0)\tau)+$$
$$+\mathrm{sinc}(\pi((l-m)f_0-F_0)(\tau_i-\tau))\cos(\pi((l+m)f_0-F_0)\tau));$$

$$I_6^u = 0{,}5(\tau_i - \tau)(\mathrm{sinc}(\pi((l+m)f_0 + 2F_0)(\tau_i - \tau))\cos(\pi(l-m)f_0\tau) +$$
$$+ \mathrm{sinc}(\pi(l-m)f_0(\tau_i - \tau))\cos(\pi((l+m)f_0 + 2F_0)\tau));$$
$$I_7^u = 0{,}5(\tau_i - \tau)(\mathrm{sinc}(\pi(l+m)f_0(\tau_i - \tau))\cos(\pi((l-m)f_0 + 2F_0)\tau) +$$
$$+ \mathrm{sinc}(\pi((l-m)f_0 + 2F_0)(\tau_i - \tau))\cos(\pi(l+m)f_0\tau));$$
$$I_8^u = 0{,}5(\tau_i - \tau)(\mathrm{sinc}(\pi(l+m)f_0(\tau_i - \tau))\cos(\pi((l-m)f_0 - 2F_0)\tau) +$$
$$+ \mathrm{sinc}(\pi((l-m)f_0 - 2F_0)(\tau_i - \tau))\cos(\pi(l+m)f_0\tau));$$
$$I_9^u = 0{,}5(\tau_i - \tau)(\mathrm{sinc}(\pi((l+m)f_0 - 2F_0)(\tau_i - \tau))\cos(\pi(l-m)f_0\tau) +$$
$$+ \mathrm{sinc}(\pi(l-m)f_0(\tau_i - \tau))\cos(\pi((l+m)f_0 - 2F_0)\tau));$$
$$I_1^e = \mathrm{sinc}(\pi(l+m)f_0\tau_i) + \mathrm{sinc}(\pi(l-m)f_0\tau_i);$$
$$I_2^e = \mathrm{sinc}(\pi((l+m)f_0 + F_0)\tau_i) + \mathrm{sinc}(\pi((l+m)f_0 - F_0)\tau_i) +$$
$$+ \mathrm{sinc}(\pi((l-m)f_0 + F_0)\tau_i) + \mathrm{sinc}(\pi((l-m)f_0 - F_0)\tau_i);$$
$$I_3^e = \mathrm{sinc}(\pi((l+m)f_0 + 2F_0)\tau_i) + \mathrm{sinc}(\pi((l+m)f_0 - 2F_0)\tau_i) +$$
$$+ \mathrm{sinc}(\pi((l-m)f_0 + 2F_0)\tau_i) + \mathrm{sinc}(\pi((l-m)f_0 - 2F_0)\tau_i),$$

де $\mathrm{sinc}(x)$ – функція ненормованого кардинального синусу від аргументу x.

Значення амплітуд U_l у виразах (2.9), (2.10), які мінімізуватимуть значення критерію (2.6) для синтезовуваної моделі (2.1), можна отримати, розв'язавши систему рівнянь $\sum_{j=1}^{J}\left(b_j^y - b_j^u\right)\frac{\partial b_j^u}{\partial U_l} = 0$, яку в дискретному вигляді можна представити як

$$\sum_{j=1}^{J}\left(b_j^u\left(\sum_{k=1}^{L}\sum_{m=1}^{L}U_kU_mI(0,k,m) - \sum_{k=1}^{L}\sum_{m=1}^{L}U_kU_mI(j\Delta,k,m)\right)\times\right.$$
$$\times\left(\left(\sum_{m=1}^{L}U_m(I(j\Delta,l,m) + I(j\Delta,m,l))\right)\left(\sum_{k=1}^{L}\sum_{m=1}^{L}U_kU_mI(0,k,m)\right)\times\right. \qquad (2.11)$$
$$\times\left(\sum_{k=1}^{L}\sum_{m=1}^{L}U_kU_mI(j\Delta,k,m)\right)^{-2} - \left(\sum_{m=1}^{L}U_m(I(0,l,m) + I(0,m,l))\right)\times$$

$$\times\left(\sum_{k=1}^{L}\sum_{m=1}^{L}U_kU_mI(j\Delta,k,m)\right)\left(\sum_{k=1}^{L}\sum_{m=1}^{L}U_kU_mI(j\Delta,k,m)\right)^{-2}\Bigg)\times$$

$$\times\left(\sum_{k=1}^{L}\sum_{m=1}^{L}U_kU_mI(j\Delta,k,m)\right)^{-1}\Bigg)=0,\ l=\overline{0,L}.$$

У лівій частині рівнянь системи (2.11) містяться поліноми четвертого ступеня відносно змінних U_l. Згідно із [273] однозначного розв'язку системи таких нелінійних рівнянь не існує. Ця обставина змушує припуститися спрощення базових для системи (2.11) функцій (2.9) і (2.10). Якщо припустити, що мовленнєвий сигнал аналізуватиметься на інтервалах $\tau_i > 0.1$ с, то вірним стає твердження, що $f_0\tau_i >> 1$ [228], враховуючи яке остаточне значення функції (2.9) визначатиметься доданками $I^u(\tau, l, m)$ для яких $l = m$, що дозволяє позбутися додаткового підсумовування по m:

$$\begin{gathered}B_u(\tau)=2^{-1}(\tau_i-\tau)\sum_{l=1}^{L}\Big(U_l^2(\mathrm{sinc}(2\pi l(\tau_i-\tau)f_0)+\cos(2\pi l\tau f_0)-\\ -M(\mathrm{sinc}(\pi(2lf_0+F_0)(\tau_i-\tau))+\mathrm{sinc}(\pi(2lf_0-F_0)(\tau_i-\tau)))+\\ +0{,}25M^2(\mathrm{sinc}(\pi(2lf_0+2F_0)(\tau_i-\tau))+\mathrm{sinc}(\pi(2lf_0-2F_0)(\tau_i-\tau))+\\ +\cos(\pi(2lf_0+2F_0)\tau)+\cos(\pi(2lf_0-2F_0)\tau)++2\mathrm{sinc}(2\pi l(\tau_i-\tau)f_0)\times\\ \times\cos(2\pi F_0\tau)+2\mathrm{sinc}(2\pi(\tau_i-\tau)F_0)\cos(2\pi lf_0\tau))))).\end{gathered}\tag{2.12}$$

Якщо доповнити наведені вище міркуванням припущенням, що для однотипних за вмістом і суб'єктом мовленнєвих сигналів їх енергія для достатньо малих інтервалів аналізу $0 \le \tau \le \tau_i$ є сталою: $E_u \to E_y = \mathrm{const}$, то функція (2.10) набуде вигляду:

$$\begin{gathered}E_u=B_u(0)=2^{-1}\tau_i\sum_{l=1}^{L}\Big(U_l^2\big(\big(1+2^{-1}M^2\big)\big(\mathrm{sinc}\big(2\pi l\tau_i f_0\big)+1\big)-\\ -M(\mathrm{sinc}(\pi(2lf_0+F_0)\tau_i)+\mathrm{sinc}(\pi(2lf_0-F_0)\tau_i))+\\ +0{,}25M^2(\mathrm{sinc}(\pi(2lf_0+2F_0)\tau_i)+\mathrm{sinc}(\pi(2lf_0-2F_0)\tau_i)+\\ +\mathrm{sinc}(2\pi\tau_iF_0)))).\end{gathered}\tag{2.13}$$

Підставивши у систему (2.11) функції (2.12), (2.13) отримаємо систему лінійних рівнянь:

$$U_l^2 = E_u\left(\sum_{j=1}^{J} b_j^y S_{j,p}\right)\left(\sum_{j=1}^{J} S_{j,p} S_{j,l}\right)^{-1}, \tag{2.14}$$

де $l, p = \overline{1,L}$, а параметри $S_{n,m}$, $n \in \overline{1,J}$, $m \in \overline{1,L}$, розраховуються за виразом

$$\begin{aligned} S_{n,m} = {} & 2^{-1}(\tau_i - n\Delta)(\mathrm{sinc}(2\pi m(\tau_i - n\Delta)f_0) + \cos(2\pi mn\Delta f_0) - \\ & - M(\mathrm{sinc}(\pi(2mf_0 + F_0)(\tau_i - n\Delta)) + \mathrm{sinc}(\pi(2mf_0 - F_0)(\tau_i - n\Delta))) + \\ & + 0{,}25M^2(\mathrm{sinc}(\pi(2mf_0 + 2F_0)(\tau_i - n\Delta)) + \\ & + \mathrm{sinc}(\pi(2mf_0 - 2F_0)(\tau_i - n\Delta)) + \\ & + \cos(\pi(2mf_0 + 2F_0)n\Delta) + \cos(\pi(2mf_0 - 2F_0)n\Delta) + \\ & + 2\mathrm{sinc}(2\pi m(\tau_i - n\Delta)f_0)\cos(2\pi F_0 n\Delta) + \\ & + 2\mathrm{sinc}(2\pi(\tau_i - n\Delta)F_0)\cos(2\pi mf_0 n\Delta))). \end{aligned} \tag{2.15}$$

Відзначимо, що достовірність моделі (2.1), характеристичні параметри якої розраховуються із урахуванням критерію (2.6), залежить від кількості відліків J для яких розраховуються значення функцій (2.3), (2.4). Для оцінювання достатності значення J, пов'язаного із значенням інтервалу аналізу τ_i відношенням $\tau_i = J\Delta$, запропонуємо такі критерії:

1. α-критерій $(\alpha \to 1)$, значення якого дорівнює відношенню значення потужності сигналу за умови усічення функції (2.4) вище J-го відліку $E_{Jy} = (2\pi)^{-1}\int_{-\infty}^{\infty} W_y(\omega)d\omega$ до значення потужності сигналу $E = E_{Jy} + E_{J\Delta} = (2\pi)^{-1}\int_{-\infty}^{\infty} W(\omega)d\omega$: $\alpha = E_{Jy}E^{-1}$;

2. β-критерій $(\beta \to 0)$, абсолютне значення якого дорівнює відношенню значення функції (2.4) на J-му відліку b_J^y до максимального зареєстрованого значення цієї функції для попередніх відліків $\max(b_{j<J}^y) = 1$: $\beta = \left|\max(b_{j<J}^y) - b_{j=J}^y\right|$;

3. δ-критерій $\left(\delta^{-1} \to 0\right)$, який характеризує значущість потужності похибки усічення $E_{J\Delta} = (2\pi)^{-1} \int\limits_{-\infty}^{\infty} W_{\Delta}(\omega) d\omega$ відносно до значення потужності сигналу E: $\delta = EE_{J\Delta}^{-1}$. α - і δ-критерії пов'язані залежністю $\delta = 1(1-\alpha)^{-1}$.

Вживані у сформульованих вище критеріях значення спектральних щільностей відповідних потужностей $W(\omega)$, $W_y(\omega)$ і $W_{\Delta}(\omega)$ пов'яжемо із автокореляційною функцією $B(\tau)$ так:

$$W(\omega) = W_y(\omega) + W_{\Delta}(\omega) = \int\limits_{-\infty}^{\infty} B(\tau) e^{-i\omega\tau} d\tau = 2\int\limits_{0}^{\infty} B(\tau)\cos(\omega\tau) d\tau; \tag{2.16}$$

$$W_y(\omega) = \int\limits_{-\tau_J}^{\tau_J} B(\tau) e^{-i\omega\tau} d\tau = 2\int\limits_{0}^{\tau_J} B(\tau)\cos(\omega\tau) d\tau; \tag{2.17}$$

$$W_{\Delta}(\omega) = \int\limits_{-\infty}^{\tau_J} B(\tau) e^{-i\omega\tau} d\tau = \int\limits_{\tau_J}^{\infty} B(\tau) e^{-i\omega\tau} d\tau = 2\int\limits_{\tau_J}^{\infty} B(\tau)\cos(\omega\tau) d\tau. \tag{2.18}$$

На практиці, в залежності від описуваного мовленнєвого сигналу, варто обирати такий критерій із трьох сформульованих вище, який мінімізує значення нев'язки (2.6) при мінімальному значенні J. Наведемо приклад порядку розрахунку потужності мовленнєвого сигналу y при відомих значеннях його частоти дискретизації f_d, верхньої частоти спектра $f_h = 0{,}5 f_d$ і заданому рівні δ-критерію.

Потужність сигналу із верхньою частотою $\omega_h = 2\pi f_h$ у спектрі із парною спектральною щільністю потужності $\left(W(\omega) = W(-\omega)\right)$ при усіченні нормованої автокореляційної функції опишемо виразом

$$E_{J\Delta} = (2\pi)^{-1} \int\limits_{-\infty}^{\infty} W_{\Delta}(\omega) d\omega = (2\pi)^{-1} \int\limits_{-\omega_h}^{\omega_h} W_{\Delta}(\omega) d\omega = (\pi)^{-1} \int\limits_{0}^{\omega_h} W_{\Delta}(\omega) d\omega =$$

$$= \pi^{-1} \int\limits_{0}^{\omega_h} 2\int\limits_{0}^{\tau_J} B(\tau)\cos(\omega\tau) d\tau d\omega = 2\pi^{-1} \int\limits_{0}^{\tau_J} B(\tau) \int\limits_{0}^{\omega_h} \cos(\omega\tau) d\omega d\tau = \tag{2.19}$$

$$= 2\pi^{-1} \int\limits_{0}^{\tau_J} B(\tau)\sin(\omega_h\tau)\tau^{-1} d\tau = 2\omega_h \pi^{-1} \int\limits_{0}^{\tau_J} B(\tau)\operatorname{sinc}(\omega_h\tau) d\tau =$$

$$= 4 f_h \int_0^{\tau_J} B(\tau) \operatorname{sinc}(2\pi f_h \tau) d\tau .$$

Якщо $\tau_J = J\Delta \to \infty$, то $E_{J\Delta} \to E$, отже, $E = 4 f_h \int_0^{\tau_J} B(\tau) \operatorname{sinc}(2\pi f_h \tau) d\tau$, звідки $\int_0^{\tau_J} B(\tau) \operatorname{sinc}(2\pi f_h \tau) d\tau = E(4 f_h)^{-1}$, тобто δ-критерій можна описати виразом

$$\delta = E(E_{J\Delta})^{-1} = 4 f_h \int_0^{\infty} B(\tau) \operatorname{sinc}(2\pi f_h \tau) d\tau \left(4 f_h \int_{\tau_J}^{\infty} B(\tau) \operatorname{sinc}(2\pi f_h \tau) d\tau \right)^{-1} =$$
$$= \int_0^{\infty} B(\tau) \operatorname{sinc}(2\pi f_h \tau) d\tau \left(\int_{\tau_J}^{\infty} B(\tau) \operatorname{sinc}(2\pi f_h \tau) d\tau \right)^{-1} . \qquad (2.20)$$

Перетворивши вираз (2.20), можна для відомих параметрів f_h і $B(\tau)$ розраховувати τ_J при заданому рівні δ.

Вживане у (2.20) невідоме апріорно значення $B(\tau)$ можна оцінити апостеріорно, на основі відліків мовленнєвого сигналу y_i, використовуючи співвідношення $B_y(j) \equiv B_j^y = \sum_{i=0}^{N-1} y_i y_{i-j}$, $j = \overline{0, J}$. Зауважимо, що для точнішого розрахунку (2.20) можна не обмежуватися лише відомими значеннями функції $B(\tau)$ у точках $j = \overline{1, J}$, а апроксимувати ці дані, наприклад, тригонометричним поліномом з метою ідентифікації аналітичного вигляду функції $B(\tau)$.

Отже, наведений вище матеріал комплексно формалізує вклад основних складових елементів артикуляційного тракту у індивідуальність голосу суб’єкта. Модель дозволяє описати ІГМС множиною таких характеристичних параметрів як частота основного тону, амплітуди несних гармонік та щільність потужності на інтервалах сигналу із присутніми несними імпульсами. Модель формалізовано у вигляді автокреляційних функцій, кількість вагомих доданків яких можна обмежувати, застосовуючи один із сформульованих критеріїв, що дозволяє зменшити кількість обчислень без втрати моделлю адекватності.

2.2 Уточнена квазідетермінована модель індивідуальності голосу в мовленнєвому сигналі

У математичній моделі (2.1) множник $1+M\cos(2\pi F_0 t+\Gamma_0)$ описує вплив модулятора на ІГМС. Втім, припускаючи періодичну природу цих коливань, вплив модулятора $u_m(t)$ і мовленнєвого джерела $u_n(t)$ на індивідуальність голосу в досліджуваному мовленнєвому сигналі можна описати із використанням рядів Фур'є:

$$u_m(t)=\sum_{k=0}^{K} M_k \cos(\Omega_k t+\Gamma_k); \tag{2.21}$$

$$u_n(t)=\sum_{l=0}^{L} U_l \cos(\omega_l t+\varphi_l), \tag{2.22}$$

де $t\in[0,\tau_i]$; K і L – кількості модулювальних і несних гармонік, відповідно; M_k, $\Omega_k=2\pi F_k^m$, Γ_k – глибина модуляції, кутова частота, початкова фаза k-ї гармоніки модулювального коливання, відповідно; а U_l, ω_l, φ_l – амплітуда, кутова частота, початкова фаза l-ї гармоніки несного коливання, відповідно.

Вирази (2.21) і (2.22) можна узагальнити в уточнену модель ІГМС, формалізовану виразом

$$u_a(t)=u_m(t)u_n(t)=\sum_{k=0}^{K} M_k \cos(\Omega_k t+\Gamma_k)\sum_{l=0}^{L} U_l \cos(\omega_l t+\varphi_l). \tag{2.23}$$

Підставивши вираз (2.23) у модель (2.1) отримаємо

$$u(t)=\sum_{k=0}^{K} M_k \cos(2\pi k F_0 t+\Gamma_k)\sum_{l=0}^{L} U_l \cos(2\pi l f_0 t+\varphi_l), \tag{2.24}$$

де $t\in[0,\tau_i]$; F_0 – найнижча частота модулювального коливання; f_0 – частота основного тону.

Проведемо адаптацію моделі (2.24) до практичного застосування за процедурою, описаною вище для моделі (2.1). За аналогією з (2.9), (2.10), отримаємо аналітичні вирази для автокореляційної функції $B_u(\tau)$ і потужності E_u сигналу, описуваного моделлю (2.24):

$$B_u(\tau)=0{,}25\sum_{k=0}^{K}\sum_{l=1}^{L}\sum_{n=0}^{K}\sum_{m=1}^{L}M_kM_nU_lU_m\left(\sum_{i=1}^{4}I_i(\tau,k,l,n,m)\right); \qquad (2.25)$$

$$\begin{aligned}
E_u=8^{-1}\tau_i\sum_{k=0}^{K}\sum_{l=1}^{L}\sum_{n=0}^{N}\sum_{m=1}^{M}M_kM_nU_lU_m\big(&\mathrm{sinc}(\pi((l+m)f_0+(k+n)F_0)\tau_i+\\
&+0{,}5(\varphi_l+\varphi_m+\Gamma_k+\Gamma_n))\cos(0{,}5(\varphi_l-\varphi_m+\Gamma_k-\Gamma_n))+\\
&+\mathrm{sinc}(\pi((l-m)f_0+(k-n)F_0)\tau_i+0{,}5(\varphi_l-\varphi_m+\Gamma_k-\Gamma_n))\times\\
&\times\cos(0{,}5(\varphi_l+\varphi_m+\Gamma_k+\Gamma_n))+\mathrm{sinc}(\pi((l+m)f_0+(k-n)F_0)\tau_i+\\
&+0{,}5(\varphi_l+\varphi_m+\Gamma_k-\Gamma_n))\cos(0{,}5(\varphi_l-\varphi_m+\Gamma_k+\Gamma_n))+\\
&+\mathrm{sinc}(\pi((l-m)f_0+(k+n)F_0)\tau_i+0.5(\varphi_l-\varphi_m+\Gamma_k+\Gamma_n))\times\\
&\times\cos(0{,}5(\varphi_l+\varphi_m+\Gamma_k-\Gamma_n))+s\mathrm{inc}(\pi((l+m)f_0+(n-k)F_0)\tau_i+\\
&+0{,}5(\varphi_l+\varphi_m-\Gamma_k+\Gamma_n))\cos(0{,}5(\varphi_l-\varphi_m-\Gamma_k-\Gamma_n))+\\
&+\mathrm{sinc}(\pi((l-m)f_0+(-k-n)F_0)\tau_i+0{,}5(\varphi_l-\varphi_m-\Gamma_k-\Gamma_n))\times\\
&\times\cos(0{,}5(\phi_l+\phi_m-\Gamma_k+\Gamma_n))+s\mathrm{inc}(\pi((l+m)f_0+(-n-k)F_0)\tau_i+\\
&+0{,}5(\phi_l+\phi_m-\Gamma_k-\Gamma_n))\cos(0{,}5(\phi_l-\phi_m-\Gamma_k+\Gamma_n))+\\
&+\mathrm{sinc}(\pi((l-m)f_0+(n-k)F_0)\tau_i+0{,}5(\phi_l-\phi_m-\Gamma_k+\Gamma_n))\times\\
&\times\cos(0{,}5(\phi_l+\phi_m-\Gamma_k-\Gamma_n))),
\end{aligned} \qquad (2.26)$$

де доданки $I_1(\ldots)-I_4(\ldots)$ розрахуємо за виразами:

$$\begin{aligned}
I_1(\tau,k,l,n,m)=0{,}5(\tau_i-\tau)\big(&\mathrm{sinc}(\pi((l+m)f_0+(k+n)F_0)(\tau_i-\tau)+\\
&+0{,}5(\varphi_l+\varphi_m+\Gamma_k+\Gamma_n))\cdot\cos(\pi((l-m)f_0+(k-n)F_0)\tau+\\
&+0{,}5(\varphi_l-\varphi_m+\Gamma_k-\Gamma_n))+\mathrm{sinc}(\pi((l-m)f_0+(k-n)F_0)(\tau_i-\tau)+\\
&+0{,}5(\varphi_l-\varphi_m+\Gamma_k-\Gamma_n))\cdot\cos(\pi((l+m)f_0+(k+n)F_0)\tau+0{,}5(\phi_l+\phi_m+\Gamma_k+\Gamma_n))\big),
\end{aligned}$$

$$\begin{aligned}
I_2(\tau,k,l,n,m)=0{,}5(\tau_i-\tau)\big(&\mathrm{sinc}(\pi((l+m)f_0+(k-n)F_0)(\tau_i-\tau)+\\
&+0{,}5(\varphi_l+\varphi_m+\Gamma_k-\Gamma_n))\cdot\cos(\pi((l-m)f_0+(k+n)F_0)\tau+\\
&+0{,}5(\varphi_l-\varphi_m+\Gamma_k+\Gamma_n))+\mathrm{sinc}(\pi((l-m)f_0+(k+n)F_0)(\tau_i-\tau)+\\
&+0{,}5(\varphi_l-\varphi_m+\Gamma_k+\Gamma_n))\cdot\cos(\pi((l+m)f_0+(k-n)F_0)\tau+0{,}5(\phi_l+\phi_m+\Gamma_k-\Gamma_n))\big);
\end{aligned}$$

$$I_3(\tau,k,l,n,m)=0{,}5(\tau_i-\tau)(\mathrm{sinc}\,(\pi((l+m)f_0+(n-k)F_0)(\tau_i-\tau)+$$
$$+0{,}5(\varphi_l+\varphi_m+\Gamma_n-\Gamma_k))\cdot\cos(\pi((l-m)f_0+(-n-k)F_0)\tau+$$
$$+0{,}5(\varphi_l-\varphi_m-\Gamma_n-\Gamma_k))+\mathrm{sinc}(\pi((l-m)f_0+(-n-k)F_0)(\tau_i-\tau)+$$
$$+0{,}5(\varphi_l-\varphi_m-\Gamma_k-\Gamma_n))\cdot\cos(\pi((l+m)f_0+(n-k)F_0)\tau+0{,}5(\phi_l+\phi_m+\Gamma_n-\Gamma_k)))),$$

$$I_4(\tau,k,l,n,m)=0{,}5(\tau_i-\tau)(\mathrm{sinc}(\pi((l+m)f_0+(-n-k)F_0)(\tau_i-\tau)+$$
$$+0{,}5(\varphi_l+\varphi_m-\Gamma_n-\Gamma_k))\cdot\cos(\pi((l-m)f_0+(n-k)F_0)\tau+$$
$$+0{,}5(\varphi_l-\varphi_m+\Gamma_n-\Gamma_k))+\mathrm{sinc}(\pi((l-m)f_0+(n-k)F_0)(\tau_i-\tau)+$$
$$+0{,}5(\varphi_l-\varphi_m-\Gamma_k+\Gamma_n))\cdot\cos(\pi((l+m)f_0+(-n-k)F_0)\tau+0{,}5(\phi_l+\phi_m-\Gamma_n-\Gamma_k)))).$$

Якщо початкові фази не враховувати, то вирази (2.25), (2.26) спрощуються:

$$I_1(\tau,k,l,n,m)=0{,}5(\tau_i-\tau)\Big(\mathrm{sinc}\big(\pi((l+m)f_0+(k+n)F_0)(\tau_i-\tau)\big)\times$$
$$\times\cos\big(\pi((l-m)f_0+(k-n)F_0)\tau\big)+\mathrm{sinc}\big(\pi((l-m)f_0+(k-n)F_0)(\tau_i-\tau)\big)\times$$
$$\times\cos\big(\pi((l+m)f_0+(k+n)F_0)\tau\big)\Big);$$

$$I_2(\tau,k,l,n,m)=0{,}5(\tau_i-\tau)\Big(\mathrm{sinc}\big(\pi((l+m)f_0+(k-n)F_0)(\tau_i-\tau)\big)\times$$
$$\times\cos\big(\pi((l-m)f_0+(k+n)F_0)\tau\big)+\mathrm{sinc}\big(\pi((l-m)f_0+(k+n)F_0)(\tau_i-\tau)\big)\times$$
$$\times\cos\big(\pi((l+m)f_0+(k-n)F_0)\tau\big)\Big);$$

$$I_3(\tau,k,l,n,m)=0{,}5(\tau_i-\tau)\Big(\mathrm{sinc}\big(\pi((l+m)f_0+(n-k)F_0)(\tau_i-\tau)\big)\times$$
$$\times\cos\big(\pi((l-m)f_0+(-k-n)F_0)\tau\big)+\mathrm{sinc}\big(\pi((l-m)f_0+(-k-n)F_0)(\tau_i-\tau)\big)\times$$
$$\times\cos\big(\pi((l+m)f_0+(n-k)F_0)\tau\big)\Big);$$

$$I_4(\tau,k,l,n,m)=0{,}5(\tau_i-\tau)\Big(\mathrm{sinc}\big(\pi((l+m)f_0+(-k-n)F_0)(\tau_i-\tau)\big)\times$$
$$\times\cos\big(\pi((l-m)f_0+(k-n)F_0)\tau\big)+\mathrm{sinc}\big(\pi((l-m)f_0+(n-k)F_0)(\tau_i-\tau)\big)\times$$
$$\times\cos\big(\pi((l+m)f_0+(-k-n)F_0)\tau\big)\Big);$$

$$E_u=8^{-1}\tau_i\sum_{k=0}^{K}\sum_{l=1}^{L}\sum_{n=0}^{N}\sum_{m=1}^{M}M_kM_nU_lU_m(\mathrm{sinc}(\pi((l+m)f_0+(k+n)F_0)\tau_i)+$$

$$+\operatorname{sinc}\left(\pi\left((l-m)f_0+(k-n)F_0\right)\tau_i\right)+\operatorname{sinc}\left(\pi\left((l+m)f_0+(k-n)F_0\right)\tau_i\right)+$$
$$+\operatorname{sinc}\left(\pi\left((l-m)f_0+(k+n)F_0\right)\tau_i\right)+\operatorname{sinc}\left(\pi\left((l+m)f_0+(n-k)F_0\right)\tau_i\right)+$$
$$+\operatorname{sinc}\left(\pi\left((l-m)f_0+(-k-n)F_0\right)\tau_i\right)+\operatorname{sinc}\left(\pi\left((l+m)f_0+(-k-n)F_0\right)\tau_i\right)+$$
$$+\operatorname{sinc}\left(\pi\left((l-m)f_0+(n-k)F_0\right)\tau_i\right).$$

Якщо параметри M_k, Ω_k, Γ_k моделі (2.24) відомі, то значення амплітуд U_l, які мінімізують значення критерію (2.6), можна отримати розв'язавши систему з L нелінійних рівнянь виду (2.11), отриману на основі рівнянь (2.25), (2.26). Проте, як і при аналізі моделі (2.1), отримана для моделі (2.24) система нелінійних рівнянь (2.11) не має однозначного розв'язку. Отже, для спрощення (2.24) припустимо, що $f_0\tau_i >> 1$ і значення потужностей мовленнєвих сигналів із однотипним вмістом і суб'єктом є сталою величиною $E_u = const$. Також врахуємо, що значення нормованої автокореляційної функції (2.25) здебільшого утворюється вкладом доданків, для яких $k = n$ і $l = m$. Враховуючи сформульовані припущення, отримаємо на основі (2.26) і (2.74) придатні для практичного застосування вирази для обчислення автокореляційної функції $B_u(\tau)$ і потужності E_u мовленнєвого сигналу, описуваного моделлю (2.24):

$$B_u(\tau)=8^{-1}(\tau_i-\tau)\sum_{l=1}^{L}U_l^2\times$$
$$\times\sum_{k=0}^{K}M_k^2\left(\operatorname{sinc}\left(2\pi(lf_0+kF_0)(\tau_i-\tau)+(\varphi_l+\Gamma_k)\right)+\right.$$
$$+\operatorname{sinc}\left(2\pi(lf_0-kF_0)(\tau_i-\tau)+(\varphi_l-\Gamma_k)\right)+2\operatorname{sinc}\left(2\pi lf_0(\tau_i-\tau)+\varphi_l\right)\times \tag{2.27}$$
$$\times\cos\left(2\pi kF_0\tau+\Gamma_k\right)+2\operatorname{sinc}\left(2\pi lF_0(\tau_i-\tau)+\Gamma_k\right)\times$$
$$\times\cos\left(2\pi kf_0\tau+\varphi_l\right)+\cos\left(2\pi(lf_0+kF_0)\tau+\varphi_l+\Gamma_k\right)+$$
$$\left.+\cos\left(2\pi(lf_0-kF_0)\tau+\varphi_l-\Gamma_k\right)\right);$$

$$E_u=B_u(0)=8^{-1}\tau_i\sum_{l=1}^{L}U_l^2\sum_{k=0}^{K}M_k^2\left(\operatorname{sinc}\left(2\pi(lf_0+kF_0)\tau_i+\varphi_l+\Gamma_k\right)+\right.$$
$$+\operatorname{sinc}\left(2\pi(lf_0-kF_0)\tau_i+\varphi_l-\Gamma_k\right)+2\operatorname{sinc}\left(2\pi lf_0\tau_i\right)\cos\left(\Gamma_k\right)+ \tag{2.28}$$
$$\left.+2\operatorname{sinc}\left(2\pi kF_0\tau_i\right)\cos\left(\varphi_l\right)+2\cos\left(\varphi_l\right)\cos\left(\Gamma_k\right)\right).$$

Підставивши у систему (2.11) функції (2.27), (2.28), отримаємо систему лінійних рівнянь, структурно аналогічну (2.15), елементи $S_{i,j}$ якої опишемо виразом

$$\begin{aligned} S_{i,j} = 8^{-1}(\tau_i - i\Delta)\sum_{k=0}^{K} M_k^2 \big(\mathrm{sinc}\big(2\pi(jf_0 + kF_0)(\tau_i - i\Delta) + \varphi_j + \Gamma_k\big) + \\ + \mathrm{sinc}\big(2\pi(jf_0 - kF_0)(\tau_i - i\Delta) + \varphi_j - \Gamma_k\big) + 2\mathrm{sinc}\big(2\pi jf_0(\tau_i - i\Delta) + \varphi_j\big)\times \\ \times\cos\big(2\pi kF_0 i\Delta + \Gamma_k\big) + 2\mathrm{sinc}\big(2\pi kF_0(\tau_i - i\Delta) + \Gamma_k\big)\cos\big(2\pi jf_0 i\Delta + \varphi_j\big) + \\ + \cos\big(2\pi(jf_0 + kF_0)i\Delta + \varphi_j + \Gamma_k\big) + \cos\big(2\pi(jf_0 - kF_0)i\Delta + \phi_j - \Gamma_k\big). \end{aligned} \tag{2.29}$$

Втім, для практичного застосування придатний і ще більш спрощений варіант (2.24), у якому $\varphi_l = \Gamma_k = 0$,

$$u(t) = \sum_{k=0}^{K} M_k \cos(2\pi kF_0 t)\sum_{l=0}^{L} U_l \cos(2\pi lf_0 t),$$

де $t \in [0, \tau_i]$, а елементи $S_{i,j}$ з (2.29) описуються виразом

$$\begin{aligned} S_{i,j} = 8^{-1}(\tau_i - i\Delta)\sum_{k=0}^{K} M_k^2 \big(\mathrm{sinc}\big(2\pi(jf_0 + kF_0)(\tau_i - i\Delta)\big) + \\ + \mathrm{sinc}\big(2\pi(jf_0 - kF_0)(\tau_i - i\Delta)\big) + 2\mathrm{sinc}\big(2\pi jf_0(\tau_i - i\Delta)\big)\times \\ \times\cos(2\pi kF_0 i\Delta) + 2\mathrm{sinc}\big(2\pi kF_0(\tau_i - i\Delta)\big)\cos(2\pi jf_0 i\Delta) + \\ + \cos\big(2\pi(jf_0 + kF_0)i\Delta\big) + \cos\big(2\pi(jf_0 - kF_0)i\Delta\big). \end{aligned}$$

Розв’язавши (2.29) можна отримати всі необхідні параметри моделі (2.24) для опису індивідуальності голосу в емпіричному мовленнєвому сигналі, адекватного задачі АСГ. Модель (2.24) доповнює опис ІГМС моделлю (2.1), дозволяючи враховувати характеристичні параметри як несних, так і модулювальних коливань у мовленнєвому сигналі, індивідуальність голосу в якому забезпечується вкладом мовленнєвого джерела і модулятора тощо. Зокрема, коефіцієнти несних коливань U_l і φ_l дозволяють врахувати спотворення гармонічних коливань, утворених мовленнєвим джерелом, після проходження останніх резонаторами артикуляційного тракту, а коефіцієнти модулювальних коливань M_k і Γ_k дозволяють врахувати затухання обвідної нормованої автокореляційної функції мовленнєвого сигналу, спричинене роботою модулятора артикуляційного тракту у процесі фонації. Інфо-

рмативною для автентифікації суб'єкта, ІГМС якого описано моделлю (2.24), буде множина з $K+L+2$ векторів характеристичних параметрів $\{U_1,\ldots,U_L,M_0,\ldots,M_K,f_0\}$.

Відзначимо, що в усіх запропонованих моделях ІГМС – (2.1), (2.24), базовим параметром для формування описів виступає частота основного тону $\omega_0 = 2\pi f_0$ яка, проте, не є константою для суб'єкта, голос якого аналізується, а змінюється у часі: $\omega_0(t) = 2\pi f_0(t) = \omega_0 + Cu_{ot}(t)$, де $\omega_0 = const$; C – ваговий коефіцієнт; $u_{ot}(t)$ – квазіперіодична функція коливань основного тону, розкладання якої у ряд Фур'є описується виразом

$$u_{ot}(t) = \sum_{p=0}^{\infty} \Delta\omega_p \cos\left(\Omega_p^{ot} t + \Gamma_p^{ot}\right),$$

де $\Delta\omega_p$ – зміщення частоти основного тону для p-ї гармоніки ряду.

Миттєву частоту $\omega(t)$ мовленнєвого сигналу зв'язано із повною його фазою $\phi(t)$ відношенням $\omega(t) = \dfrac{d\phi(t)}{dt}$ звідки $\phi(t) = \int\limits_{-\infty}^{t} \omega(t)dt + const$. Введемо у цей вираз частоту основного тону $\omega_0(t) = \omega_0 + \sum\limits_{p=1}^{P} \Delta\omega_p \cos\left(\Omega_p^{ot} t + \Gamma_p^{ot}\right)$:

$$\phi(t) = \omega_0 t + \sum_{p=1}^{P} \Delta\omega_p \left(\Omega_p^{ot}\right)^{-1} \sin\left(\Omega_p^{ot} t + \Gamma_p^{ot}\right). \tag{2.30}$$

На основі виразу (2.30) сформулюємо частотно-модульоване представлення частоти основного тону рядом Фур'є

$$u_{\omega m}(t) = U_0 \cos\left(\omega_0 t + \sum_{p=1}^{P} m_p \sin\left(\Omega_p^{ot} t + \Gamma_p^{ot}\right) + \varphi_0\right), \tag{2.31}$$

де $m_p = \Delta\omega_p \left(\Omega_p^{ot}\right)^{-1}$.

Перевизначимо моделі (2.1) і (2.24) із урахуванням квазігармонічності частоти основного тону $\omega_l(t) = l\omega_0(t)$ і, приймаючи $u_n(t) = u_n(u_{ot}(t), t)$,

$$u_{a\omega}(t) = \sum_{k=0}^{K} M_k \cos\left(\Omega_k t + \Gamma_k\right) \times \tag{2.32}$$

$$\times\sum_{l=1}^{L} U_l \cos\left(l\omega_0 t + l\sum_{p=1}^{P} m_p \sin\left(\Omega_p^{ot} t + \Gamma_p^{ot}\right) + \phi_l \right),\ t \in [0, \tau_i].$$

Модель (2.32) є потенційно прецизійнішою за моделі (2.1) і (2.24), адже системно узагальнює вплив мовленнєвого джерела, резонаторів артикуляційного тракту і модулятора на ІГМС із урахуванням мінливості частоти основного тону в часі. Втім, ідентифікація аналітичних виразів для автокореляційних функцій і спектральної щільності для моделі (2.32) є суттєво трудомісткішою процедурою, хоч і передбачає виконання аналогічних, здійснених для формалізації моделей (2.1) і (2.24), математичних операцій. В результаті опису ІГМС моделлю (2.32) вектор характеристичних параметрів для АСГ матиме структуру $\{U_1,\ldots,U_L,M_0,\ldots,M_K,\omega_0,m_1,\ldots,m_p\}$.

2.3 Стохастична інтерпретація базової і уточненої моделей індивідуальності голосу

Аналізу мовленнєвих сигналів у часовому вимірі передує їх розбиття на короткочасні часові інтервали – інтервали стаціонарності тривалістю, здебільшого, 10–30 мс. Вважається [249], що значення характеристичних параметрів мовленнєвого сигналу на цих інтервалах квазідетерміновані. Втім, існують характеристичні параметри [247–249] для АСГ пошук і виділення яких обумовлює потребу в узагальнені інформації на суттєво триваліших фрагментах мовленнєвого сигналу ніж інтервал стаціонарності. При параметризації триваліших від інтервалу стаціонарності фрагментів мовленнєвого сигналу останній, із урахуванням окремих припущень [256], інтерпретують як стаціонарний випадковий процес, який характеризується усередненими у часі статистичними характеристиками, зокрема – функцією одновимірної середньої щільності імовірності $p(x)$ [248, 249] для апроксимації якої застосовують різні моделі, зокрема, Лапласа [249], гама-розподілу [249], синтез-розподілу [256] тощо:

$$p(x) = 1/\sqrt{2}\sigma_x \cdot \exp\left(-\sqrt{2}|x|/\sigma_x\right); \tag{2.33}$$

$$p(x)=\left(\sqrt{3}\left(8\pi\sigma_x|x|\right)^{-1}\right)^{0.5}\exp\left(-\sqrt{3}|x|\left(2\sigma_x\right)^{-1}\right); \tag{2.34}$$

$$\begin{aligned} p(x)=&\left(\eta k_\alpha\left(2\mathrm{H}(\alpha)x_{ef}\right)^{-1}\right)\left(k_\alpha|x|x_{ef}^{-1}\right)^{\alpha-1}\exp\left(-k_\alpha|x|x_{ef}^{-1}\right)+\\ &+(1-\eta)\left(\sqrt{2}\pi x_{ef}\varepsilon\right)^{-1}\exp\left(-\left(2\varepsilon^2x_{ef}^2\right)^{-1}x^2\right), \end{aligned} \tag{2.35}$$

де σ_x – дисперсія сигналу x; α, $0<\alpha<1$, $k_\alpha=\sqrt{\alpha(\alpha+1)}$ – характеристичний коефіцієнт мікрофону; $\mathrm{H}(\alpha)$ – гама-функція; η, $0\le\eta\le1$ – характеристичний коефіцієнт завантаженості каналу передавання сигналу; ε, $0\le\varepsilon\le1$ – характеристичний коефіцієнт, що описує функцію $p(x)$ для пауз мовленнєвого сигналу. Функції (2.33)–(2.35) наведено у порядку зростання прецизійності і обчислювальної складності.

В дослідженнях [249, 256] формалізовано функції для апроксимації двовимірної щільності імовірності мовленнєвого сигналу в неперервному та дискретному часі – $p(x_1,x_2,\tau)$ і $p(x_1,x_2,\Delta t)$, відповідно. Зокрема, апроксимація нормованої за дисперсією спектральної щільності потужності мовленнєвого сигналу в просторі додатних частот описується виразом

$$S(f)=\alpha\left(\left(\alpha^2+4\pi^2(f+f_0)^2\right)^{-1}+\left(\alpha^2+4\pi^2(f-f_0)^2\right)^{-1}\right), \tag{2.36}$$

де f_0 – частота основного тону; α – коефіцієнт згасання сигналу, який характеризує ефективну ширину мовленнєвого спектра. Достовірніші результати дає застосування апроксимувальної функції (2.36) частоти першої форманти F_1 замість f_0. Функції (2.36) відповідає індекс корельованості мовленнєвого сигналу

$$r(\tau)=\exp\left(-\alpha|\tau|\right)\cos\left(2\pi f_0\tau\right). \tag{2.37}$$

У формалізмі цифрового оброблювання сигналів, зокрема, в області оптимальної нелінійної фільтрації [256, 258], неперервний мовленнєвий сигнал $\lambda(t)$ характеризується полікомпонентним вектором $\Lambda^T=\left[\lambda(t)\equiv\lambda_1(t),\lambda_2(t),\ldots,\lambda_n(t)\right]$, зв’язок компонент якого описується системою стохастичних диференціальних рі-

внянь першого порядку. Наприклад, для першої компоненти $\lambda_1(t)$ неперервного марковського процесу $\lambda(t)$ згадану систему представимо так:

$$\begin{cases} \dfrac{d\lambda(t)}{dt} = -\alpha\lambda(t) - \alpha_1\lambda_1(t) + \alpha_1 n_\lambda(t); \\ \dfrac{d\lambda_1(t)}{dt} = -\alpha_1\lambda_1(t) + \alpha_1 n_\lambda(t), \end{cases} \tag{2.38}$$

де $n_\lambda(t)$ – стаціонарний гаусів білий шум; α, α_1 – сталі коефіцієнти. Показники $S(f)$ і $r(\tau)$ стохастичного процесу виду (2.38) опишемо відповідними виразами:

$$S(f) = \left(8\pi^2(\alpha+\alpha_1)f^2\right)\left(\left(\alpha^2 + 4\pi^2 f^2\right)\left(\alpha_1^2 + 4\pi^2 f^2\right)\right)^{-1}; \tag{2.39}$$

$$r(\tau) = (\alpha - \alpha_1)^{-1}\left(\alpha\exp(-\alpha|\tau|) - \alpha_1\exp(-\alpha_1|\tau|)\right). \tag{2.40}$$

Якщо модель (2.38) адекватно описує емпіричний мовленнєвий сигнал, то спектральна щільність (2.39) наближається до описуваного спектра, що дозволяє визнати коректною рівність $\alpha = \alpha_1$, яка дозволяє спростити вирази (2.38), (2.39) до вигляду:

$$S(f) = \left(16\pi^2\alpha f^2\right)\left(\alpha^2 + 4\pi^2 f^2\right)^{-2}; \tag{2.41}$$

$$r(\tau) = (1 - \alpha|\tau|)\exp(-\alpha|\tau|), \tag{2.42}$$

де α – зріз енергетичного спектра мовленнєвого сигналу на рівні половини його максимального значення.

Враховуючи орієнтацію на задачу АСГ, вираз (2.38) доцільно адаптувати для апроксимації мовленнєвого сигналу стохастичним процесом, який описує енергетичний спектр сигналу у вузькому околі обраної центральної частоти [274], наприклад, частоти основного тону f_0 або частоти першої форманти F_1:

$$\begin{cases} \dfrac{d\lambda(t)}{dt} = \lambda_1(t); \\ \dfrac{d\lambda_1(t)}{dt} = -2\alpha\lambda_1(t) - 4\pi^2 f_0^2\lambda(t) + 4\pi^2 f_0^2 n_\lambda(t), \end{cases} \tag{2.43}$$

Показники $S(f)$ і $r(\tau)$ для стохастичного процесу (2.43) опишемо відповідними виразами:

$$S(f)=4\alpha\left(\alpha^2+4\pi^2 f_0^2\right)\times\left(\left(\alpha^2+4\pi^2(f+f_0)^2\right)\left(\alpha^2+4\pi^2(f-f_0)^2\right)\right)^{-1}; \qquad (2.44)$$

$$r(\tau)=\exp(-\alpha|\tau|)\left(\cos(2\pi f_0\tau)+\alpha|\tau|\operatorname{sinc}(2\pi f_0|\tau|)\right). \qquad (2.45)$$

Порівнявши модель (2.38)–(2.40) із моделлю (2.43)–(2.45) можна стверджувати, що спеціалізацією останньої є прицезійний аналіз мовленнєвих сигналів. Втім, результати емпіричних досліджень [260] показують незадовільну якість опису ІГМС для задачі АСГ як у формалізмі моделі (2.38)–(2.40), так і у формалізмі моделі (2.43)–(2.45). Якісніших результатів дає застосування математичного апарату лінійного передбачення. У роботі [260] відзначається, що авторегресійна модель p-го порядку є дискретним аналогом стохастичного опису мовленнєвого сигналу в неперервному часі диференційним рівнянням того ж порядку. В цьому контексті стохастичні описи мовленнєвого сигналу (2.38), (2.43) в неперервному часі можна асоціювати із процесами авторегресії другого порідку в дискретному часі, зокрема, нормований спектр процесу авторегресії і кореляційний коефіцієнт описуються відповідними виразами [260]:

$$S(f)=\Delta\left(\left(1-\sum_{i=1}^{p}\varphi_i\cos(2\pi i f\Delta)\right)^2+\left(\sum_{i=1}^{p}\varphi_i\sin(2\pi i f\Delta)\right)^2\right),$$

$$r_k=\varphi_1 r_{k-1}+\varphi_2 r_{k-2}+\ldots+\varphi_p r_{k-p},$$

де ϕ_j – j-й коефіцієнт лінійного передбачення, зв'язаний із частковою кореляційною функцією ψ_{kk} [227]: $\phi_j=\psi_{pj}$, $j=\overline{1,p}$; p – порядок моделі; $\Delta=f_d^{-1}$ і f_d – період і частота дискретизації відповідно; f – центральна частота; k – порядок процесу авторегресії.

Втім, багатоекстремальний характер енергетичного спектра мовленнєвого сигналу із високою крутизною спектральної характеристики в околі спектральних екстремумів зумовлює адекватність лише авторегресійних моделей високого порядку $(p\geq 30)$, вживаних для його опису. Авторегресійним моделям таких високих порядків властива значна обчислювальна складність і утворення накопичувальної методичної похибки на етапі синтезу, що обмежує їх практичну цінність.

Цей факт, а також те, що існуючі стохастичні моделі опису мовленнєвих сигналів, синтезовано у парадигмі теорії цифрового оброблювання сигналів із орієнтацією на застосування у системах синтезу і розпізнавання мови, не дозволяють адекватно описати стохастичні складові мовленнєвого сигналу в контексті задачі АСГ у парадигмі акустичної теорії фонації, зумовили проведення досліджень, результати яких наведено далі.

Вважатимемо початкові фази φ_0 і Γ_0 у моделі (2.1) випадковими величинами:

$$u(t) = \left(1 + M\cos\left(2\pi F_0 t + \Gamma_0\right)\right)\sum_{l=1}^{L} U_l \cos\left(2\pi l f_0 t + \varphi_0\right), \tag{2.46}$$

де $t \in [0, \tau_i]$; τ_i – тривалість імпульсу; M – глибина модуляції; F_0 і Γ_0 – частота і початкова фаза модулювального коливання, відповідно; U_l і φ_0 – амплітуда і початкова фаза l-ї гармоніки несного коливання, відповідно; f_0 – частота основного тону. Незалежні випадкові величини φ_0 і Γ_0 рівномірно розподілені на інтервалі $[0, 2\pi]$ із щільностями імовірностей $p_{\varphi_0} = p_{\Gamma_0} = (2\pi)^{-1}$. Аналіз випадкового процесу (2.46) з позиції [237–240] дозволяє вважати його квазідетермінованим. Дослідимо чи є цей процес стаціонарним. Отримаємо аналітичний вигляд математичного сподівання випадкового процесу (2.46)

$$\begin{aligned}
m_u(t) &= \overline{u(t)} = \overline{\left(1 + M\cos\left(2\pi F_0 t + \Gamma_0\right)\right)\sum_{l=1}^{L} U_l \cos\left(2\pi l f_0 t + \varphi_0\right)} = \\
&= \sum_{l=1}^{L} U_l \overline{\left(\cos\left(2\pi l f_0 t + \varphi_0\right) + M\cos\left(2\pi F_0 t + \Gamma_0\right)\cos\left(2\pi l f_0 t + \varphi_0\right)\right)} = \\
&= \sum_{l=1}^{L} U_l \Big(0{,}5M\Big(\overline{\cos\left(\Gamma_0 + \varphi_0 + 2\pi\left(F_0 + l f_0\right)t\right)} + \\
&\quad + \overline{\cos\left(\Gamma_0 - \varphi_0 + 2\pi\left(F_0 - l f_0\right)t\right)}\Big)\Big) + \\
&\quad + \overline{\cos\left(2\pi l f_0 t + \varphi_0\right)}\Big) = \sum_{l=1}^{L} U_l \Bigg((2\pi)^{-1}\int_0^{2\pi} \cos\left(2\pi l f_0 t + \varphi_0\right) d\varphi_0 + \\
&\quad + 0{,}5M\Bigg((2\pi)^{-1}\int_0^{2\pi} \cos\left(2\pi\left(F_0 + l f_0\right)t + \Gamma_0 + \varphi_0\right) d\left(\Gamma_0 + \varphi_0\right) +
\end{aligned} \tag{2.47}$$

$$+(2\pi)^{-1}\int_0^{2\pi}\cos(2\pi(F_0-lf_0)t+\Gamma_0-\varphi_0)d(\Gamma_0-\varphi_0)\Bigg)\Bigg)=$$

$$=\sum_{l=1}^{L}U_l(0+0{,}5M(0+0))=0\,.$$

Дисперсія випадкового процесу (2.46) описуватиметься виразом

$$D_u(t)\equiv\sigma^2_{u(t)}=\overline{(u(t)-m_u(t))^2}=$$

$$=\overline{\left((1+M\cos(2\pi F_0t+\Gamma_0))\sum_{l=1}^{L}U_l\cos(2\pi lf_0t+\varphi_0)\right)^2}=$$

$$=\overline{(1+M\cos(2\pi F_0t+\Gamma_0))^2\times}$$ (2.48)

$$\overline{\times\sum_{l=1}^{L}\sum_{m=1}^{L}U_lU_m\cos(2\pi lf_0t+\varphi_0)\cos(2\pi mf_0t+\varphi_0)}=\left(0{,}5+0{,}25M^2\right)\sum_{l=1}^{L}U_l^2\,,$$

а його функція кореляції – виразом

$$R_u(t_1,t_2)=\overline{(u(t_1)-m_u(t_1))(u(t_2)-m_u(t_2))}=$$

$$=\overline{(1+M\cos(2\pi F_0t_1+\Gamma_0))\sum_{l=1}^{L}U_l\cos(2\pi lf_0t_1+\varphi_0)\times}$$

$$\overline{\times(1+M\cos(2\pi F_0t_2+\Gamma_0))\sum_{l=1}^{L}U_l\cos(2\pi lf_0t_2+\varphi_0)}=$$

$$=\overline{(1+M\cos(2\pi F_0t_1+\Gamma_0))(1+M\cos(2\pi F_0t_2+\Gamma_0))\times}$$ (2.49)

$$\overline{\times\sum_{l=1}^{L}\sum_{m=1}^{L}U_lU_m\cos(2\pi lf_0t_1+\varphi_0)\cos(2\pi mf_0t_2+\varphi_0)}=$$

$$=\left(0{,}5+0{,}25M^2\cos(2\pi F_0(t_2-t_1))\right)\sum_{l=1}^{L}U_l^2\cos(2\pi lf_0(t_2-t_1)).$$

Якщо ввести позначення $\tau=|t_2-t_1|$, то вираз (2.49) можна записати компактніше:

$$R_u(\tau)=\left(0{,}5+0{,}25M^2\cos(2\pi F_0\tau)\right)\sum_{l=1}^{L}U_l^2\cos(2\pi lf_0\tau)\,. \qquad (2.50)$$

Із виразів (2.47) і (2.48) видно, що математичне сподівання і дисперсія випадкового процесу (2.46) не залежать від часу, а його функція кореляції залежить від

τ, тобто в цілому процес (2.46) є стаціонарним, адже виконуються відповідні умови [237–240].

Перейдемо від аналітичного опису стаціонарного випадкового процесу (2.46) у вигляді характеристик (2.47)–(2.49) до його ергодичного представлення, замінивши в отриманих миттєвих функціях операції статистичного усереднення на операції усереднення в часі [207, 208]. Враховуючи ергодичність випадкового процесу (2.46), операцію усереднення виконуватимемо над однією реалізацією $u(t)$ тривалістю T. Адаптуємо вирази (2.47)–(2.49) для опису ергодичного випадкового процесу $\langle u \rangle(t)$:

$$m_{\langle u \rangle}(t) = \lim_{T \to \infty} T^{-1} \int_0^T u(t) dt; \tag{2.51}$$

$$\begin{aligned} D_{\langle u \rangle}(t) &= \left\langle (u(t) - m_u)^2 \right\rangle = \lim_{T \to \infty} T^{-1} \int_0^T (u(t) - m_u)^2 dt = \\ &= \left\langle (u(t))^2 \right\rangle - m_u^2; \end{aligned} \tag{2.52}$$

$$\begin{aligned} R_{\langle u \rangle}(\tau) &= \langle (u(t) - m_u)(u(t+\tau) - m_u) \rangle = \langle u(t) u(t+\tau) \rangle - m_u^2 = \\ &= \lim_{T \to \infty} T^{-1} \int_0^T u(t) u(t+\tau) dt - m_u^2. \end{aligned} \tag{2.53}$$

Узагальнимо (2.51)–(2.53), сформулювавши умову ергодичності для стаціонарного процесу (2.46) згідно із [237],

$$\lim_{T \to \infty} T^{-1} \int_0^T R_u(\tau) d\tau = 0. \tag{2.54}$$

Пересвідчимося, що модульований полігармонічний квазідетермінований випадковий процес виду (2.46) задовольняє умову (2.54):

$$\begin{aligned} &\lim_{T \to \infty} T^{-1} \int_0^T \left(0{,}5 + 0{,}25 M^2 \cos(2\pi F_0 \tau)\right) \sum_{l=1}^{L} U_l^2 \cos(2\pi l f_0 \tau) d\tau = \\ &= \lim_{T \to \infty} 0{,}5 T^{-1} \sum_{l=1}^{L} U_l^2 \int_0^T \cos(2\pi l f_0 \tau) d\tau + \lim_{T \to \infty} 0{,}25 \frac{M^2}{T} \sum_{l=1}^{L} U_l^2 \int_0^T \cos(2\pi F_0 \tau) \times \\ &\times \cos(2\pi l f_0 \tau) d\tau = \lim_{T \to \infty} 0{,}5 \sum_{l=1}^{L} U_l^2 \operatorname{sinc}(2\pi l f_0 T) + \lim_{T \to \infty} 0{,}125 T^{-1} \sum_{l=1}^{L} U_l^2 \times \end{aligned} \tag{2.55}$$

$$\times\left(\operatorname{sinc}\left(2\pi l\left(f_0+F_0\right)T\right)+\operatorname{sinc}\left(2\pi l\left(f_0-F_0\right)T\right)\right)=0.$$

де $\lim\limits_{x\to\infty}\operatorname{sinc}(x)=\lim\limits_{x\to\infty}x^{-1}\operatorname{sinc}(x)=0$.

Рівність виразу (2.55) не порушується, тобто умова (2.54) для випадкового процесу (2.46) виконується, що доводить його ергодичність.

Опишемо процес розрахунку параметрів U_l випадкового процесу (2.46) для заданого значення параметра f_0: $f_0=const$. Критерієм близькості опису мовленнєвого сигналу випадковим процесам (2.46) слугуватимуть значення кореляційних коефіцієнтів, отримуваних в результаті добутку функції кореляції R_j із дисперсією випадкового сигналу D,

$$r_j=R_jD. \tag{2.56}$$

Критерій (2.56) характеризує випадковий сигнал як у часовому вимірі (за ступенем кореляційного зв'язку між відліками описуваного випадкового сигналу та відліками його копії, зміщеної у часі на j відліків), так і у частотному вимірі, адже функція кореляції описує спектр сигналу за властивостями оберненого перетворення Фур'є. Мірою близькості описуваного центрованого мовленнєвого сигналу $y(t)$, відліки якого визначаються виразом (2.5), і його моделі $u(t)$, формалізованої виразом (2.46), стане евклідова нев'язка між кореляційними коефіцієнтами описуваного мовленнєвого сигналу r_j^y і кореляційними коефіцієнтами його моделі r_j^u:

$$\varepsilon_r=\sum_{j=1}^{J}\left(r_j^u-r_j^y\right)^2\to 0. \tag{2.57}$$

Формалізуємо вираз, необхідний для розрахунків кореляційних коефіцієнтів r_j^y,

$$\begin{gathered} r_j^y=R_{y_j}\left(R_{y_0}\right)^{-1}=R_y(j)D^{-1}=D(N-1)^{-1}\sum_{i=0}^{N-1-j}\left(y_i-\overline{y}\right)\left(y_{i+j}-\overline{y}\right)\approx \\ \approx DN^{-1}\sum_{i=0}^{N-1-j}y_iy_{i+j},\ j=\overline{0,J},\ \overline{y}=N^{-1}\sum_{i=0}^{N-1}y_i=0, \end{gathered} \tag{2.58}$$

де J – кількість кореляційних коефіцієнтів.

Формалізуємо вираз, необхідний для розрахунків кореляційних коефіцієнтів r_j^u, врахувавши вирази (2.47) і (2.49):

$$r_j^u = r^u(j\Delta) = r^u(\tau) = R_u(\tau)(R_u(0))^{-1} = R_u(\tau)D^{-1} =$$
$$= \left(1 + 0{,}5M^2\cos(2\pi F_0\tau)\right)\sum_{l=1}^{L} U_l^2\cos(2\pi f_0\tau)\left(\left(1 + 0{,}5M^2\right)\sum_{l=1}^{L} U_l^2\right)^{-1}. \quad (2.59)$$

Розрахуємо значення параметрів U_l моделі (2.46), застосувавши метод найменших квадратів для мінімізації значення критерію (2.57), прирівнявши до нуля похідні від ε_r за кожним із коефіцієнтів U_l при $l = \overline{1,L}$

$$\sum_{j=1}^{J}\left(r_j^u - r_j^y\right)^2 \frac{\partial r_j^u}{\partial U_l} = 0. \quad (2.60)$$

Вираз (2.60) описує систему з L нелінійних рівнянь відносно керованих змінних U_l при $l = \overline{1,L}$. Однозначного розв'язку такої системи не існує [273], отже, введемо ряд припущень з метою лінеаризації рівнянь системи (2.60). Вважатимемо, зокрема, що дисперсія всіх однотипних щодо особи суб'єкта і парольної фрази мовленнєвих сигналів є константою $D = const$. Врахування цього припущення дозволяє перетворити систему нелінійних рівняння виду (2.60) на систему лінійних рівнянь виду (2.15), коефіцієнти $A_{p,l}$ і B_p якої розраховуватимемо за виразами:

$$A_{p,l} = D^{-1}\sum_{j=1}^{J} S_{j,p}S_{j,l}; \quad (2.61)$$

$$B_p = \sum_{j=1}^{J} S_{j,p}r_j^u; \quad (2.62)$$

$$S_{j,l} = \left(0{,}5 + 0{,}25M^2\cos(2\pi F_0 j\Delta)\right)\cos(2\pi l f_0 j\Delta), \quad (2.63)$$

де $l, p = \overline{1,L}$, $V_l = U_l^2$.

Зауважимо, що модель (2.46) виступає стохастичним аналогом квазідетермінованої у часі моделі (2.1). Врахувавши цю обставину, синтезуємо стохастичний аналог уточненої параметричної моделі ІГМС (2.24), застосувавши вживані для аналізу моделі (2.46) процедури. Вважатимемо, що у виразах (2.21) і (2.22), які описують, відповідно, модулювальні і несні коливання у складі моделі (2.24),

початкові фази Γ_k і φ_l – взаємно некорельовані випадкові величини рівномірно розподілені на інтервалі $[0,2\pi]$ із щільностями імовірностей $p_{\varphi_l} = p_{\Gamma_k} = 0.5\pi^{-1}$, відповідно. Вважатимемо кількість модулювальних і несних гармонік у мовленнєвому сигналі скінченною і рівною $K+1$ і L, відповідно. Отже, стохастичний аналог моделі (2.22) із урахуванням наведених вище вихідних положень опишемо виразом

$$u(t) = \sum_{k=0}^{K} M_k \cos(2\pi k F_0 t + \Gamma_k) \sum_{l=1}^{L} U_l \cos(2\pi l f_0 t + \varphi_l), \tag{2.64}$$

де $t \in [0, \tau_i]$.

Отримаємо вирази для обчислення математичного сподівання, дисперсії і функції кореляції випадкового процесу (2.64) при $t \in [0, \tau_i]$ по аналогії із процесом синтезу виразів (2.47)-(2.49):

$$\begin{gathered} m_u(t) = \overline{u(t)} = \overline{\sum_{k=0}^{K} M_k \cos(2\pi k F_0 t + \Gamma_k) \sum_{l=1}^{L} U_l \cos(2\pi l f_0 t + \varphi_l)} = \\ = \sum_{k=1}^{K} \sum_{l=1}^{L} M_k U_l \overline{(\cos(2\pi k F_0 t + \Gamma_k)\cos(2\pi l f_0 t + \varphi_l))} = \sum_{k=1}^{K} \sum_{l=1}^{L} 0{,}5 M_k U_l \times \\ \times \overline{(\cos(2\pi(kF_0 + lf_0)t + \Gamma_k + \varphi_l) + \cos(2\pi(kF_0 - lf_0)t + \Gamma_k - \varphi_l))} = 0; \end{gathered} \tag{2.65}$$

$$\begin{gathered} D_u(t) \equiv \sigma_{u(t)}^2 = \overline{(u(t) - m_u(t))^2} = \\ = \overline{\left(\sum_{k=0}^{K} M_k \cos(2\pi k F_0 t + \Gamma_k) \sum_{l=1}^{L} U_l \cos(2\pi l f_0 t + \varphi_l) \right)^2} = \\ = \overline{\sum_{k=0}^{K} \sum_{n=0}^{K} \sum_{l=1}^{L} \sum_{m=1}^{L} M_k M_n U_l U_m \cos(2\pi k F_0 t + \Gamma_k) \cos(2\pi n F_0 t + \Gamma_n) \times} \\ \overline{\times \cos(2\pi l f_0 t + \varphi_l) \cos(2\pi m f_0 t + \varphi_m)} = 0.25 \sum_{k=0}^{K} M_k^2 \sum_{l=1}^{L} U_k^2; \end{gathered} \tag{2.66}$$

$$\begin{gathered} R_u(t_1, t_2) = \overline{(u(t_1) - m_u(t_1))(u(t_2) - m_u(t_2))} = \\ = \overline{\sum_{k=0}^{K} M_k \cos(2\pi k F_0 t_1 + \Gamma_k) \sum_{l=1}^{L} U_l \cos(2\pi l f_0 t_1 + \varphi_l) \times} \end{gathered} \tag{2.67}$$

$$\times \sum_{k=0}^{K} M_k \cos(2\pi k F_0 t_2 + \Gamma_k) \sum_{l=1}^{L} U_l \cos(2\pi l f_0 t_2 + \varphi_l) =$$

$$= \overline{\sum_{k=0}^{K} \sum_{n=0}^{K} \sum_{l=1}^{L} \sum_{m=1}^{L} M_k M_n U_l U_m \cos(2\pi k F_0 t_1 + \Gamma_k) \times}$$

$$\overline{\times \cos(2\pi n F_0 t_1 + \Gamma_n) \cos(2\pi l f_0 t_2 + \varphi_l) \cos(2\pi m f_0 t_2 + \varphi_m)} =$$

$$= 0{,}25 \sum_{k=0}^{K} M_k^2 \cos(2\pi k F_0 (t_2 - t_1)) \sum_{l=1}^{L} U_l^2 \cos(2\pi l f_0 (t_2 - t_1)).$$

Ввівши у вираз (2.67) змінну $\tau = |t_2 - t_1|$ отримаємо його компактніший запис

$$R_u(\tau) = 0{,}25 \sum_{k=0}^{K} M_k^2 \cos(2\pi k F_0 \tau) \sum_{l=1}^{L} U_l^2 \cos(2\pi l f_0 \tau). \tag{2.68}$$

Аналіз виразів (2.65)–(2.67) щодо дотримання умов стаціонарності [237] дозволяє вважати випадковий процес (2.64) стаціонарним. Доведемо, що для стаціонарного випадкового процесу (2.64) виконуються умови ергодичності [237]. Підставимо вираз (2.68) у праву частину умови (2.54):

$$\begin{aligned} &\lim_{T\to\infty} 0{,}25 \sum_{k=0}^{K} M_k^2 \cos(2\pi k F_0 \tau) \sum_{l=1}^{L} U_l^2 \cos(2\pi l f_0 \tau) = \\ &= \lim_{T\to\infty} 0{,}25 T^{-1} \sum_{k=0}^{K} M_k^2 \sum_{l=1}^{L} U_l^2 \int_0^T \cos(2\pi k F_0 \tau) \cos(2\pi l f_0 \tau) d\tau = \\ &= \lim_{T\to\infty} 0{,}125 \sum_{k=0}^{K} M_k^2 \sum_{l=1}^{L} U_l^2 (\operatorname{sinc}(2\pi (k F_0 + l f_0) T) + \\ &\quad + \operatorname{sinc}(2\pi (l f_0 - k F_0) T)) = 0. \end{aligned} \tag{2.69}$$

Оскільки рівність (2.69) не порушується, стаціонарний випадковий процес (2.64) є і ергодичним.

Розрахуємо значення параметрів U_l моделі (2.64), мінімізувавши значення критерію (2.57) методом найменших квадратів, прирівнявши до нуля похідні від ε_r за кожним із коефіцієнтів U_l як у виразі (2.60), відліки кореляційних коефіцієнтів $r^m(\tau)$ у якому визначатимемо за модифікованим виразом (2.59):

$$r^m(\tau) = \left(\sum_{k=0}^{K} M_k^2 \cos(2\pi k F_0 \tau) \sum_{l=1}^{L} U_l^2 \cos(2\pi l f_0 \tau) \right) \left(\sum_{k=0}^{K} M_k^2 \sum_{l=1}^{L} U_l^2 \right)^{-1}. \tag{2.70}$$

Істотні значення параметрів M_k, $\Omega_k = 2\pi F_k^m$ моделі (2.64) розрахуємо за методом представлення спектральних характеристик мовленнєвих сигналів в контексті уточненої моделі ІГМС, яку описано у підрозділі 2.3. В результаті отримаємо систему з L нелінійних рівнянь відносно керованих змінних U_l, $l = \overline{1,L}$, однозначного розв'язку якої не існує [273]. Врахувавши аналогічні вжитим для системи (2.60) припущення, перейдемо до системи лінійних рівнянь виду (2.15), коефіцієнти $A_{p,l}$ і B_p якої розрахуємо за виразами (2.61) і (2.62), у яких параметри $S_{j,l}$ розрахуємо за виразом

$$S_{j,l} = 0{,}25\sum_{k=0}^{K} M_k \cos(\Omega_k j\Delta)\cos(2\pi l f_0 j\Delta), \tag{2.71}$$

де $l, p = \overline{1,L}$, $V_l = U_l^2$.

Нормовану відносно максимального значення спектральну щільність потужності для моделі (2.64) можна розрахувати за виразом

$$W_N^m(f) = W_u(f)(\max(W_u(f)))^{-1}, \tag{2.72}$$

де спектральна щільність потужності $W_u(f)$ розраховується за теоремою Вінера–Хінчина [208, 249] на основі функції кореляції (2.67):

$$\begin{aligned} W_u(f) &= \int_{-\infty}^{\infty} R_u(\tau)\exp(-j2\pi f\tau)d\tau = 2\int_{0}^{\infty} R_u(\tau)\cos(2\pi f\tau)d\tau = \\ &= 0{,}125\tau_i \sum_{k=0}^{K} M_k^2 \sum_{l=1}^{L} U_l^2 (\operatorname{sinc}(2\pi(f + lf_0 + kF_0)\tau_i) + \\ &+ \operatorname{sinc}(2\pi(f - lf_0 - kF_0)\tau_i) + \operatorname{sinc}(2\pi(f + lf_0 - kF_0)\tau_i) + \\ &+ \operatorname{sinc}(2\pi(f - lf_0 + kF_0)\tau_i)). \end{aligned} \tag{2.73}$$

Таким чином, всі істотні параметри, необхідні для опису ІГМС стохастичною моделлю (2.64) ідентифіковано. Зауважимо, що варіюючи значеннями коефіцієнтів M_k моделі (2.64) можна адаптувати останню до присутнього в досліджуваному мовленнєвому сигналі рівня затухання обвідної кореляційних коефіцієнтів спектра, а варіюючи значенням коефіцієнтів U_l можна адаптувати модель (2.64) до фактичного вигляду несних коливань, присутніх у досліджуваному мовленнє-

вому сигналі в наслідок функціонування мовленнєвого джерела. Вектор характеристичних параметрів для АСГ у контексті застосування моделі (2.64) для параметризації мовленнєвих сигналів складатиметься із $K+L+2$ коефіцієнтів: $\left(f_0, U_1, \ldots, U_L, M_0, \ldots, M_K\right)$. Звичайно, повно досліджувати мовленнєвий сигнал можна лише за наявності моделей методів для представлення його характеристичних параметрів як у часовому, так і у частотному просторах. Якщо матеріал підрозділів 2.1–2.3 здебільшого орієнтовано на часовий, то матеріал додатку В – на частотний простір, що дозволяє, зокрема, перейти до адекватного опису шумних компонентів мовленнєвого сигналу в формалізмі моделей ІГМС.

2.4 Опис рівня відношення «сигнал»/«шум» у формалізмі моделей індивідуальності голосу

Стохастична модель (2.64) має універсальний характер, проте, для адекватного опису шумних фрагментів мовленнєвих сигналів необхідно враховувати настільки значну кількість амплітуд U_l, що обчислювальна складність розрахунків стає неприйнятною. Отже, доповнимо опис мовленнєвого сигналу, як сукупності несних і модулювальних коливань, ввівши у модель (2.64) «білий шум» [237] для опису фрагментів мовленнєвих сигналів із глухими приголосними звуками. Ідентифікацію таких фрагментів мовленнєвих сигналів здійснюватимемо, аналізуючи кореляційні функції (2.67). У дослідженнях [248] пропонується відносити вміст досліджуваного фрагмента мовленнєвого сигналу до приголосних звуків, якщо значення кореляційного коефіцієнта, що його описують, перевищують границю Бартлета [260, 277] $\pm 3\sigma_r = \pm 3\sqrt{N^{-1}\left(1+2\sum_{j=1}^{H}\left(r_j^y\right)^2\right)}$, де N – загальна кількість відліків у досліджуваному фрагменті мовленнєвого сигналу, $H = 0{,}25N$. Нехай, починаючи з деякого відліку $J_{\overline{|3\sigma_r|}}$, значення мовленнєвого сигналу y виходять за границі $\pm 3\sigma_r$, при чому

$$J_{\overline{|3\sigma_r|}} < J_0, \tag{2.74}$$

де J_0 – кількість значень кореляційного коефіцієнта, що описує період основного тону $T_0 = f_0^{-1} = J_0\Delta = J_0 f_d^{-1}$, де f_d – частота дискретизації. Враховуючи, що $J_0 = f_d f_0^{-1}$, розвинемо запис виразу (2.74) до вигляду

$$J_{\overline{|3\sigma_r|}} < J_0 = f_d f_0^{-1} = f_d f_{0\max}^{-1} \approx 3{,}3 \cdot 10^{-3} f_d\,, \tag{2.75}$$

де $f_{0\max} = 330$ Гц [248].

Для типових значень $f_d = \{6 \cdot 10^3; 8 \cdot 10^3; 11{,}025 \cdot 10^3\}$ Гц значення $J_{\overline{|3\sigma_r|}}$ згідно з (2.75) утворюють множину $\{18{,}2; 24{,}2; 33{,}4\}$. Отже, якщо для фрагмента мовленнєвого сигналу, оцифрованого із частотою дискретизації f_d, значення $\left|J_{\overline{|3\sigma_r|}}\right|$ кореляційного коефіцієнта знаходяться в межах Бартлета $\pm 3\sigma_r$, то аналізований фрагмент мовленнєвого сигналу містить приголосний звук. Такий фрагмент мовленнєвого сигналу описуватимемо моделлю білого шуму $n(t)$, обмеженого частотною смугою $[0, f_h]$ із спектральною щільністю потужності $0{,}5N_0$. Зважатимемо, що f_h – верхня частота смуги, а $N_0 = const$ – одностороння спектральна щільність потужності. Такі статистичні характеристики центрованого випадкового процесу $n(t)$, як математичне сподівання $m_n(t)$, дисперсія $D_n(t)$, функція кореляції $r_n(\tau)$ і спектральна щільність потужності $W_n(2\pi f)$при $f \in [0, f_h]$, опишемо відповідними виразами [248]:

$$m_n(t) = 0\,; \tag{2.76}$$

$$D_n(t) = N_0 f_h\,; \tag{2.77}$$

$$R_n(\tau) = \mathrm{sinc}(2\pi f_h \tau); \tag{2.78}$$

$$W_n(2\pi f) = 0{,}5N_0\,. \tag{2.79}$$

Скомбінувавши випадковий процес $n(t)$ і випадковий процес $u(t)$, описуваний виразом (2.64), отримаємо орієнтовану на практичне застосування стохастичну модель ІГМС:

$$\xi(t) = u(t) + n(t). \tag{2.80}$$

Отримаємо аналітичні вирази моментних функцій $m_\xi(t)$, $D_\xi(t)$, $R_\xi(t)$, $W_\xi(t)$ для опису моделлю (2.80) ІГМС на інтервалі спостереження τ_i, із припущенням, що випадкові процеси $u(t)$ і $n(t)$ – некорельовані:

$$m_\xi(t) = m_u(t) + m_n(t) = 0; \tag{2.81}$$

$$D_\xi(t) = D_u(t) + D_n(t); \tag{2.82}$$

$$R_\xi(\tau) = R_u(\tau) + R_n(\tau); \tag{2.83}$$

$$W_\xi(2\pi f) = \begin{cases} W_u(2\pi f) + W_u(2\pi f), \; if \;\; f \in [0, f_h], \\ W_u(2\pi f), \; if \;\; f \notin [0, f_h], \end{cases} \tag{2.84}$$

де функції $m_n(t)$, $D_n(t)$, $R_n(\tau)$ і $W_n(2\pi f)$ описуються виразами (2.76)–(2.79), відповідно, а функції $m_u(t)$, $D_u(t)$, $R_u(\tau)$ і $W_u(2\pi f)$ описуються виразами (2.65), (2.66), (2.68), (2.73), відповідно. Зауважимо, що функції $m_u(t)$, $D_u(t)$, $R_u(\tau)$ і $W_u(2\pi f)$ можна представляти і на основі моделі (2.46) – тоді вони описуватимуться виразами (2.47), (2.48), (2.50), (2.73), відповідно.

Розрахуємо параметри квазідетермінованої складової $u(t)$ моделі (2.80), для чого припустимо, що дисперсія однотипних за суб'єктом і вмістом мовленнєвих сигналів є сталою – $D_u(t) = const$, і дорівнює дисперсії вихідного центрованого мовленнєвого сигналу $D_y(t)$, тобто

$$D_u(t) = D_y(t) = R_y(0) = (N-1)^{-1} \sum_{i=1}^{N} y_i^2 \approx N^{-1} \sum_{i=1}^{N} y_i^2, \tag{2.85}$$

де y_i – відліки вихідного мовленнєвого сигналу y, $i = \overline{1, N}$.

Розрахувавши за виразами (2.61), (2.62), (2.71) параметри f_0, $U_l = \sqrt{V_l}$, M_k моделі (2.64), можна за виразом (2.66) розрахувати апостеріорну дисперсію моделі (2.64)

$$D_u^{ps}(t) = 0{,}25 \sum_{k=0}^{K} M_k^2 \sum_{l=1}^{L} U_k^2. \tag{2.86}$$

Також припускатимемо, що дисперсія моделі (2.80) $D_{\xi}(t)$ дорівнює дисперсії вихідного центрованого мовленнєвого сигналу $D_y(t)$. Із урахуванням (2.86), вираз (2.82) можна представити як

$$D_{\xi}(t) = D_u^{ps}(t) + D_n(t), \tag{2.87}$$

звідки

$$D_n(t) = D_{\xi}(t) - D_u^{ps}(t). \tag{2.88}$$

Розрахувавши за виразом (2.88) дисперсію $D_n(t)$ можна на основі виразу (2.77) розрахувати спектральна щільність потужності N_0:

$$N_0 = D_n(t) f_h^{-1}. \tag{2.89}$$

Скориставшись виразами (2.86) і (2.88), можна фактично оцінити співвідношення квазідетермінованої періодичної і шумової складових в описуваному моделлю (2.80) мовленнєвому сигналі:

$$D_z(t) = D_u^{ps}(t)(D_n(t))^{-1} = D_u^{ps}(t)\left(D_{\xi}(t) - D_u^{ps}(t)\right)^{-1}. \tag{2.90}$$

Дисперсія $D_z(t)$ за своїм фізичним змістом еквівалентна відношенню «сигнал»/«шум» для вихідного мовленнєвого сигналу y, індивідуальність голосу в якому описується моделлю (2.80). На основі величини дисперсії $D_z(t)$ можна приймати рішення щодо вибору моделі для опису фрагмента вихідного мовленнєвого сигналу, зокрема:

- при $D_z(t) >> 1$ в описуваному фрагменті мовленнєвого сигналу переважає вокалізована складова і адекватний опис його для АСГ можна отримати застосувавши квазідетерміновані, (2.1), (2.24), (В.8), або стохастичні, (2.46), (2.64), моделі;

- при $D_z(t) << 1$ в описуваному фрагменті мовленнєвого сигналу переважає шумна складова і адекватний опис його для АСГ можна отримати застосувавши модель білого шуму $n(t)$ із параметрами (2.76)–(2.79);

- при $D_z(t) \approx 1$ в описуваному фрагменті мовленнєвого сигналу в зіставній мірі присутня як вокалізована, так і шумна складові і адекватний опис його для АСГ можна отримати застосувавши модель (2.80).

Зрештою, опис шумних фрагментів мовленнєвого сигналу моделлю білого шуму є очевидним, але не єдиним варіантом. Зокрема, шумні фрагменти мовленнєвого сигналу можна описати моделлю авторегресії. На відміну від моделі білого шуму $n(t)$, у якій мовленнєвий сигнал характеризується єдиним параметром N_0, у моделі авторегресії для опису шумного фрагмента мовленнєвого сигналу застосовується множина коефіцієнтів ϕ_i, $i = \overline{1, p}$, кількість яких p обмежується лише заданою похибкою опису і обчислювальною складністю задачі розрахунку цих коефіцієнтів.

Представимо модель ІГМС (2.80) у дискретній формі із періодом дискретизації Δ:

$$\xi_i = u_i + n_i, \tag{2.91}$$

де $\xi_i = \xi(t)|_{t=i\Delta} = \xi(i\Delta)$; $u_i = u(t)|_{t=i\Delta} = u(i\Delta)$, а складову n_i, яка є дискретною формою стаціонарного випадкового процесу $n(t)$, опишемо моделлю авторегресії такого виду:

$$n_i = \sum_{p=1}^{P} \phi_p n_{i-p} + b a_i, \tag{2.92}$$

де a_i – сигнал білого гаусівського шуму для збудження системи; P – порядок моделі авторегресії; ϕ_p – коефіцієнти лінійного передбачення; b – константа.

Для розрахунку параметрів b і ϕ_p моделі (2.92) скористаємося виразами [256]:

$$\phi_j = \psi_{pj}; \tag{2.93}$$

$$b = D_n = R_0 - \sum_{i=1}^{p} \phi_i R_i, \tag{2.94}$$

де $j = \overline{1, p}$; R_i – відліки функції кореляції мовленнєвого сигналу; ψ_{pj} – часткова кореляційна функція, що розраховується за виразами Дарбіна [257],

$$\psi_{p+1,j} = \psi_{pj} - \psi_{p+1,p+1}\psi_{p,p-j+1}; \tag{2.95}$$

$$\psi_{p+1,p+1} = \left(r_{pj} - \sum_{j=1}^{p} \psi_{pj} r_{p+1-j} \right)\left(1 - \sum_{j=1}^{p} \psi_{pj} r_j \right)^{-1}, \tag{2.96}$$

і пов'язана із значеннями кореляційного коефіцієнта r_j процесу авторегресії рівнянням Юла–Уокера [257] виду

$$r_j = \psi_{k,l} r_{j-1} + \ldots + \psi_{k,k-1} r_{j-k+1} + \psi_{k,k} r_{j-k}, \tag{2.97}$$

де $k = \overline{1,P}$ – порядок процесу авторегресії.

Для розрахунку параметрів моделі (2.92) слід віднайти значення кореляційного коефіцієнта $r_n(j\Delta)$ випадкового процесу $n(t)$ з моделі (2.90). Враховуючи некорельованість компонентів змішаного випадкового процесу $\xi(\tau) = \xi(j\Delta)$, функції кореляції для неперервної $R_\xi(\tau)$ і дискретної $R_\xi(j\Delta)$ його форм опишемо, відповідно, виразами:

$$R_\xi(\tau) = R_u(\tau) + R_n(\tau); \tag{2.98}$$

$$R_\xi(j\Delta) = R_u(j\Delta) + R_n(j\Delta). \tag{2.99}$$

Відповідно, коефіцієнти функції (2.99) можна описати виразами

$$r_\xi(j\Delta) = R_\xi(j\Delta) D_\xi^{-1}; \tag{2.100}$$

$$r_u(j\Delta) = R_u(j\Delta) D_u^{-1}; \tag{2.101}$$

$$r_n(j\Delta) = R_n(j\Delta) D_n^{-1}, \tag{2.102}$$

зважаючи, що $D_\xi = R_\xi(0) = R_u(0) + R_n(0) R_\xi(0) = D_u + D_n$.

Врахувавши вирази (2.100)–(2.102) і вираз (2.90), який описує дисперсію відношення «сигнал»/«шум» D_z, отримаємо вираз для розрахунку значень кореляційного коефіцієнта моделі (2.80):

$$r_\xi(\tau) = r_u(\tau) D_z (D_z + 1)^{-1} + r_n(\tau)(D_z + 1)^{-1}, \tag{2.103}$$

на основі якого отримаємо вирази для розрахунку кореляційних коефіцієнтів $n(\tau) = n(j\Delta)$:

$$r_n(\tau) = r_\xi(\tau) D_z (D_z + 1)^{-1} - r_u(\tau) D_z, \tag{2.104}$$

$$r_n(j\Delta) = r_\xi(j\Delta) D_z (D_z + 1)^{-1} - r_u(j\Delta) D_z. \tag{2.105}$$

Визначені за допомогою (2.105) значення кореляційного коефіцієнта $r_n(j\Delta)$ дозволяють розрахувати параметри моделі (2.92) за виразами (2.93), (2.94). Окремим наслідком аналізу моделі (2.92) із урахуванням (2.80) є висновок, що вклад шумної компоненти в описуваний моделлю (2.58) мовленнєвий сигнал можна встановити за значенням дисперсії відношення «сигнал»/«шум» D_z.

При адаптації до практичного застосування всіх запропонованих моделей ІГМС, в тому числі, квазідетермінованих – (2.1), (2.24), (2.101), і стохастичних – (2.46), (2.64), вважалося, що потужності модельованих фрагментів сигналів однотипних за суб'єктом і вмістом є сталою величиною. Втім, у загальному випадку мовленнєвий сигнал не є стаціонарним і ергодичним випадковим процесом [256]. Для наближення реальних характеристик мовленнєвих сигналів до згаданих вище в практиці цифрового оброблювання сигналів вдаються до попередньої фільтрації мовленнєвого сигналу з метою вирівнювання його спектра. Формалізуємо цю операцію в контексті опису шумних фрагментів мовленнєвого сигналу моделлю авторегресії.

Дискретизуємо мовленнєвий сигнал $x(t)$ із частотою f_d і до отриманих в результаті відліків x_i, $i = \overline{1, N}$, застосуємо нелінійну операцію

$$y_i = \ln(x_i). \tag{2.106}$$

Для оцінювання нестаціонарності в мовленнєвому сигналі розрахуємо коефіцієнти кореляції за виразом

$$r_j = R_j R_0^{-1} = (N-1)^{-1} \sum_{i=1}^{N-j} (y_i - \overline{y})(y_{i+j} - \overline{y}) R_0^{-1}, \tag{2.107}$$

де $j = \overline{0, L}$; $L < N$; $\overline{y} = N^{-1} \sum_{i=1}^{N} y_i$.

Функція (2.107) є квазіперіодичною згасаючою функцією, значення якої, починаючи з відліку j^+, входять у границі довірчого інтервалу $\pm 3\sigma_r$, обрахованого за методом Бартлета [260, 277] при

$$\sigma_r = \sqrt{N^{-1}\left(1 + 2\sum_{j=1}^{L} r_j^2\right)}. \qquad (2.108)$$

Індикатором нестаціонарної складової в мовленнєвому сигналі є вихід значень кореляційних коефіцієнтів, розрахованих за виразом (2.107), за межі довірчого інтервалу $\pm 3\sigma_r$. Для фільтрації цієї нестаціонарної складової використаємо режекторний фільтр Чебишева другого роду восьмого порядку [237], утворений каскадним з'єднанням чотирьох фільтрів Чебишева другого роду другого порядку.

Опишемо отриманий після фільтрації стаціонарний сигнал моделлю авторегресії, для визначення порядку якої розрахуємо часткову кореляційну функцію [278] відфільтрованого сигналу

$$\psi_{11} = r_{f_1};\ \psi_{ll} = \left(r_{f_l} - \sum_{j=1}^{l-1} \psi_{l-1,j} r_{f_{l-j}}\right)\left(1 - \sum_{j=1}^{l-1} \psi_{l-1,j} r_{f_j}\right), \qquad (2.109)$$

де $l = \overline{2,L}$; $j = \overline{1,l-1}$; r_f – значення кореляційного коефіцієнта мовленнєвого сигналу $y(t)$, відфільтрованого на частоті f, а

$$\psi_{lj} = \psi_{l-1,j} - \psi_{ll}\psi_{l-1,l-j}. \qquad (2.110)$$

Шуканий порядок моделі авторегресії дорівнює номеру відліку часткової кореляційної функції, починаючи з якого значення останньої знаходяться у межах інтервалу Бартлета $\pm 3\sigma_1$:

$$A\phi = x, \qquad (2.111)$$

де $\sigma_1 = N^{-0,5}$, A – матриця розмірністю $i \times j$, $i, j = \overline{1,p}$, утворена елементами $A_{ij} = R_{f_{|i-j|}}$, а x і ϕ – вектор-стовпці з елементів $x_i = R_{f_i}$ і ϕ_i відповідно.

Достовірність авторегресійної моделі (2.111) оцінюватимемо за величиною залишкової похибки між значенням модельованого сигналу і виходом авторегресійної моделі для l-го відліку

$$a_l = \left(w_l - \overline{w}\right) - \sum_{i=1}^{p} \phi_i \left(w_{l-i} - \overline{w}\right), \qquad (2.112)$$

де w_l – відліки сигналу після фільтрації; $\overline{w}$ – його математичне сподівання.

Адекватність отриманої авторегресійної моделі (2.111) оцінюватимемо за критерієм Пірсона [260]

$$\chi^2 = N \sum_{j=1}^{S} r_a^2(j), \tag{2.113}$$

де $r_a(j)$ – залишкові похибки значень кореляційного коефіцієнта. Кількість ступенів свободи критерію Пірсона $\nu = S - p$, де S – кількість врахованих залишкових похибок значень кореляційного коефіцієнта.

Можна аналітично порівняти ефективність опису шумової складової мовленнєвого сигналу значеннями часткового кореляційного коефіцієнта із передфільтрацією і, наприклад, коефіцієнтами лінійного передбачення. Так для вихідного фрагмента мовленнєвого сигналу тривалістю 0,2 с аналізованого на частоті основного тону f_0 і на частоті першої її гармоніки $f_1 = 2f_0$ порівнянні значення критерію Пірсона $\chi^2 \approx 59$ при однаковому рівні значимості $\alpha = 0{,}001$ можна отримати, описавши сигнал або 140 коефіцієнтами лінійного передбачення (при цьому фрагмент мовленнєвого сигналу розбивався на інтервали стаціонарності тривалістю по 20 мс), або 13 значеннями часткового кореляційного коефіцієнта, до яких ще варто додати 16 параметричних коефіцієнтів, що описують вжиті на етапі передфільтрації частотні фільтри (по 8 коефіцієнтів на фільтр для кожної із двох аналізованих частот). Таким чином, з позиції компактифікації розмірності простору характеристичних параметрів для опису індивідуальності голосу суб’єкта, моделювання шумних фрагментів мовленнєвих сигналів значеннями часткового кореляційного коефіцієнта із передфільтрацією виявляється в понад 5 разів ефективнішим, порівняно із традиційно вживаним підходом на основі коефіцієнтів лінійного передбачення. Матеріал підрозділу став основою для синтезу представленої в додатку Д бікомпонентної моделі ІГМС, яка на основі моделей (2.1), (2.24), (2.46), (2.64) і виразу (2.90) дозволяє визначити переходи між вокалізованими і шумними сегментами мовленнєвого сигналу.

Висновки до другого розділу

1. Для опису спектральної щільності потужності вокалізованих сегментів мовленнєвого сигналу синтезовано комплекс квазідетермінованих імпульсних модуляційних полігармонічних математичних моделей, параметричний простір яких утворений усередненою частотою основного тону, амплітудами несних гармонік і, зокрема, глибинами модулювальних гармонік. Враховуючи, що спектральна щільність потужності описуваного мовленнєвого сигналу зв'язана через обернене перетворення Фур'є із його автокореляційною функцією, аналізуючи достатню кількість відліків останньої можна отримати значення характеристичних параметрів моделей, які адекватно описують вихідний мовленнєвий сигнал. Згадана достатність визначається запропонованими критеріями, у яких аналізується ступінь ослаблення автокореляційної функції аналізованого сигналу відносно найбільшого її значення припускаючи, що потужності однотипних за вмістом і суб'єктом вокалізованих сегментів стала.

2. Фізична відповідність моделі описуваному сигналу, забезпечувана введенням у модель амплітудної модуляції із полігармонічним представленням модулювального коливання, сприяє зростанню достовірності першої із зростанням кількості обчислюваних амплітуд несних гармонік, обмеженого відношенням верхньої частоти у спектрі мовленнєвого сигналу до частоти основного тону. Математично формалізовано процес ідентифікації модулювального коливання полігармонічної математичної моделі в результаті пропускання обвідної аналізованого мовленнєвого сигналу відповідним фільтром нижніх частот.

3. Аналізуючи описи мовленнєвих сигналів базовою полігармонічною математичною моделлю індивідуальності голосу із апроксимацією спектра вокалізованого мовленнєвого сигналу фрагментами постійної спектральної потужності в околі частоти основного тону і її гармонік і удосконаленим варіантом цієї моделі із додатковим врахуванням модулювальних і несних складових досліджуваних сигналів можна зробити висновок, що середньоквадратична помилка удосконаленої моделі в понад два рази менша аналогічної характеристики базової моделі для однакових емпіричних мовленнєвих сигналів, у той час як факторний аналіз показав, що для адекватного опису фрагмента емпіричного вокалізованого мовленнє-

вого сигналу достатньо значень усередненої частоти основного тону і амплітуд перших десяти несних гармонік.

4. Випадкову складову мовленнєвого сигналу описано такими стохастичними характеристичними параметрами полігармонічної математичної моделі як початкові фази модулювального і несного коливань. Розрахунок параметричного опису емпіричного мовленнєвого сигналу у формалізмі стохастичного варіанту відповідної полігармонічної моделі відбувається на основі значень відліків його автокореляційної функції, достатня кількість яких визначається з умови входження останньої у довірчі границі нульових значень, визначені за методом Бартлета [260]. Аналітичний розрахунок характеристичних параметрів квазідетермінованих варіантів базової і удосконаленої медалей індивідуальності голосу в мовленнєвому сигналі можливий виключно за умови рівності дисперсій потужностей однакових за вмістом і суб'єктом вокалізованих фрагментів мовленнєвих сигналів. Достовірність синтезованих амплітудно модульованих квазідетермінованих полігармонічних моделей зростає із зростанням кількості враховуваних амплітуд несних гармонік, яка обмежена відношенням верхньої частоти спектра сигналу до частоти основного тону. Інформація про номер відліку автокореляційної функції аналізованого мовленнєвого сигналу, починаючи з якого її значення заходять у довірчі границі нульових значень, визначені за методом Бартлета, дозволяє визначити межу між вокалізованим і невокалізованим фрагментами у сигналі.

5. Ступінь вокалізації фрагмента мовленнєвого сигналу охарактеризована значенням відношення «сигнал»/«шум», для аналітичного опису якого у квазідетерміновані полігармонічні моделі вводиться адитивна компонента із обмеженим за смугою частот білим шумом. Суму інформативної компоненти, описаної квазідетермінованим стохастичним процесом із випадковими початковими фазами полігармонічних модулювальних і несних коливань, і шумової компоненти, описаної моделлю авторегресії, узагальнено у бікомпонентну математичну модель мовленнєвого сигналу, ступінь вокалізації характеризується значенням відношення «сигнал»/«шум». Отриманій моделі властива універсальність, яка дозволяє описувати як вокалізовані, так і невокалізовані фрагменти мовленнєвих сигналів корис-

туючись потужним математичним апаратом теорії імовірності і математичної статистики, і, зокрема, аналітично оцінити відношення енергії шуму до енергії інформативної складової мовленнєвого сигналу.

6. Вцілому у підрозділі реалізовано 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 у 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

Основні результати розділу опубліковано в [30, 32, 35, 37, 39, 40, 41, 42, 46, 47, 49, 60].

РОЗДІЛ 3
ЗАСТОСУВАННЯ МОДЕЛЕЙ ІНДИВІДУАЛЬНОСТІ ГОЛОСУ ДЛЯ АВТЕНТИФІКАЦІЇ СУБ'ЄКТА

3.1 Технологія автентифікації суб'єкта за голосом у формалізмі моделей індивідуальності голосу

Задача оцінювання адекватності моделі ІГМС емпіричним даним має нерозривний семантичний зв'язок із задачею АСГ, яка передбачає: екстрагування із вхідної фонограми мовленнєвого сигналу характеристичних параметрів; розрахунок відхилення екстрагованих значень характеристичних параметрів від відповідних еталонних значень на основі вибраної міри; порівняння розрахованих відхилень із відповідними пороговими значеннями за обраним критерієм; формулювання результату верифікації згідно з обраним розв'язувальним правилом на основі результатів порівнянь. Представлене у додатку Е узагальнення інформаційних джерел [241–248] дозволило синтезувати методику верифікації математичної моделі за значенням критерію, який засновано на коефіцієнті множинної кореляції (Е.17), яка найкраще підходить для встановлення адекватності моделей ІГМС, представлених у розділі 2. Втім, питання цільового використання такого параметричного опису індивідуальності голосу в задачі АСГ потребує додаткового дослідження.

У контексті моделей (2.1), (2.24), (2.46), (2.64), параметричний простір суб'єкта, особа якого автентифікується за голосом, включатиме: частоти основного тону f_0 і $l=\overline{1,L}$ її гармонік $f_l \approx (l+1)f_0$, які описують вплив особливостей мовленнєвого джерела і, опосередковано, резонаторів артикуляційного тракту суб'єкта на ІГМС; амплітуди несних гармонік $U_l \approx U_l^{sc} K_l^{at}$, де параметр U_l^{sc} описує амплітудні складові спектра сигналу мовленнєвого джерела, а параметр K_l^{at} описує амплітудно-частотну характеристику артикуляційного тракту $K_l^{at} \equiv \left| K^{at}(2\pi f_l) \right|$ на частотах відповідних гармонік.

Адаптуємо описані у додатку Е міри для розділення класів суб'єктів, що автентифікуються за їх голосами, у параметричному просторі, конфігурацію якого було щойно описано.

Представимо міру (Е.1) у вигляді

$$D = \sum_{l=1}^{L} \left(\lambda_l^{vs} - \lambda_l^{et} \right)^2 , \tag{3.1}$$

де λ_l^{vs} – значення l-го характеристичного параметра математичної моделі ІГМС, екстраговане із фонограми суб'єкта, який автентифікується; λ_l^{et} – еталонне значення l-го характеристичного параметра математичної моделі ІГМС для відповідного суб'єкта; L – кількість характеристичних параметрів, значення яких враховується для АСГ.

Враховуючи (3.1), зведемо міру (Е.4) до вигляду

$$D = \sum_{l=1}^{L} w_l \left(\lambda_l^{vs} - \lambda_l^{et} \right)^2 , \tag{3.2}$$

де w_l – вага інформативності l-го характеристичного параметра математичної моделі ІГМС для задачі АСГ.

Враховуючи (3.1), зведемо міру (Е.9) до вигляду

$$D = \sum_{l=1}^{L} \left| \lambda_l^{vs} - \lambda_l^{et} \right| . \tag{3.3}$$

Врахуємо (3.1)–(3.3) при приведенні виразу (Е.11) до вигляду

$$D_n = \left(\lambda^{vs} - \overline{\lambda_n^{et}} \right) W_n^{-1} \left(\lambda^{vs} - \overline{\lambda_n^{et}} \right)^T , \tag{3.4}$$

де $\overline{\lambda_n^{et}} = \left(\overline{\lambda_{1,n}^{et}}, \overline{\lambda_{2,n}^{et}}, \ldots, \overline{\lambda_{l,n}^{et}}, \ldots, \overline{\lambda_{L,n}^{et}} \right)$ – усереднений вектор еталонних значень характеристичних параметрів моделі ІГМС n-го суб'єкта, $\lambda^{vs} = \left(\lambda_1^{vs}, \lambda_2^{vs}, \ldots, \lambda_L^{vs} \right)$ – вектор характеристичних параметрів моделі фонограми суб'єкта, який автентифікується; W_n – коваріаційна матриця, елементи якої описуються виразом

$$\{W_n\}_{i,j} = M^{-1} \sum_{m=1}^{M_n} \lambda_{i,n,m}^{et} \lambda_{j,n,m}^{et} - \left(\overline{\lambda_n^{et}} \right) \left(\overline{\lambda_n^{et}} \right)^T ,$$

де $i, j = \overline{1, L}$, $\overline{\lambda_{l,n}^{et}} = M_n^{-1} \sum_{m=1}^{M_n} \lambda_{l,n,m}^{et}$, l – індекс характеристичного параметра моделі ІГМС; m – індекс фонограми у навчальній базі мовленнєвих сигналів n-го суб'єкта; M_n – обсяг (кількість фонограм) навчальної бази n-го суб'єкта (для статистичної репрезентативності має містити не менше 20 реалізацій).

Якщо в якості характеристичних параметрів λ_l для автентифікації особи суб'єкта використовуються коефіцієнти лінійного передбачення ϕ_l, то міру (3.4) можна адаптувати до вигляду

$$D = \left(\phi^{vs} - \phi^{et}\right)\left(NR\left(\phi^{vs} R\left(\phi^{vs}\right)^T\right)\right)\left(\phi^{vs} - \phi^{et}\right)^T , \tag{3.5}$$

де $\phi^{et} = \left(1, \phi_1^{et}, \phi_2^{et}, \ldots, \phi_L^{et}\right)$ – вектор усереднених еталонних значень кореляційних коефіцієнтів для відповідного суб'єкта, $\phi^{vs} = \left(1, \phi_1^{vs}, \phi_2^{vs}, \ldots, \phi_L^{vs}\right)$ – вектор значень кореляційних коефіцієнтів, екстрагованих із фонограми мовленнєвого сигналу суб'єкта, який автентифікується; N – кількість відліків фонограми; R – відповідна аналізованій фонограмі кореляційна матриця розмірністю $(L+1)\times(L+1)$, елементи якої описуються виразом $R_{i,j} = R_{|i-j|} = R(j)$, де $R(j)$ – відповідна аналізованій фонограмі функція кореляції.

Варто відзначити, що міра (3.5) є коректною за умови стаціонарності коефіцієнтів лінійного передбачення для однотипних звуків у довільному сегментів мовленнєвого сигналу. Якщо розглядати мовленнєвий сигнал як нестаціонарний випадковий процес, що більше відповідає реальності, то міру (3.5) можна представити у вигляді

$$D = \left(\phi^{vs} - \overline{\phi^{et}}\right)\left(C^{-1}\right)\left(\phi^{vs} - \overline{\phi^{et}}\right)^T , \tag{3.6}$$

де $\overline{\phi^{et}} = \left(1, \overline{\phi_1^{et}}, \overline{\phi_2^{et}}, \ldots, \overline{\phi_L^{et}}\right)$ – вектор усереднених за навчальною базою значень коефіцієнтів лінійного передбачення для відповідного суб'єкта; $C = S + N^{-1} R^{-1}\left(\phi^{vs} R\left(\phi^{vs}\right)^T\right)$ – повна коваріаційна матриця вхідного мовленнєвого сигналу. Значення параметрів $\overline{\phi^{et}} = M^{-1} \sum_{m=1}^{M} \phi_{l,m}^{et}$ і

$S = \{S\}_{i,j} = M^{-1} \sum_{m=1}^{M} \phi_{i,m}^{et} \cdot \phi_{j,m}^{et} - \overline{\phi_i^{et}} \cdot \overline{\phi_j^{et}}$ необхідно оцінювати для кожної фонограми навчальної вибірки, враховуючи, що $l, i, j = \overline{1, L}$, а $\phi_{l,m}^{et}$ – l-й коефіцієнт лінійного передбачення, екстрагований із m-ї фонограми із навчальної вибірки відповідного суб'єкта. Обсяг начальної вибірки M має бути статистично репрезентативним.

Практично вживатимемо спрощений варіант міри (3.6):

$$D = \lg\left(\varphi^{et} R\left(\varphi^{et}\right)^T \Big/ \varphi^{vs} R\left(\varphi^{vs}\right)^T\right), \tag{3.7}$$

який, втім, може набувати від'ємних значень і суттєво зменшує інформативність значень характеристичних параметрів моделі ІГМС [51]. Параметри φ^{et} і $\left(\varphi^{et}\right)$ також згадувалися у описі до виразу (3.5).

Для прийняття рішень в задачі АСГ можна рекомендувати міри (3.1)–(3.3), обчислене значення яких D порівнюється із пороговим значенням D_0:

$$D \le D_0 . \tag{3.8}$$

Якщо нерівність (3.8) виконується, то суб'єкт вважається успішно автентифікованим (при повній ідентичності значень відповідних елементів векторів λ^{vs} і λ^{et} значення міри D дорівнює нулю). Для систем АСГ значення порогу D_0 можна вважати компромісом між очікуваними похибками першого і другого роду [247, 248].

Виділимо з плеяди описаних вище мір міру (3.2), у якій за рахунок вживання ваг ω_l можна оптимізувати процес АСГ, впроваджуючи факторний аналіз до моделі ІГМС [49]. Обґрунтуємо методику розрахунку ваг параметрів моделі ІГМС в аналітичному вигляді, для чого визначимося із критерієм оптимальності таких систем.

Вважатимемо, що система АСГ працює найкраще при мінімальних значеннях імовірностей виникнення похибок першого і другого роду – α і β відповідно, або при прямуванні до нуля середньої імовірності їх виникнення:

$$P_e = 0{,}5(\alpha + \beta) \to 0 , \tag{3.9}$$

або при $\alpha = \beta$ (так звана EER [247]):

$$P_{eer} = P_e\Big|_{\alpha=\beta} \equiv P_{\alpha\beta} = \alpha = \beta . \tag{3.10}$$

На основі (3.9), (3.10) зробимо такі постановки задачі аналітичного розрахунку ваг міри близькості (3.2) в контексті АСГ:

1. Мінімізація імовірності похибки першого роду α при фіксованому значенні порогу D_0 у вигляді критерію D_Σ^α.

2. Мінімізація імовірності похибки другого роду β при фіксованому значенні порогу D_0 у вигляді критерію D_Σ^β.

3. Мінімізація середньої імовірності похибки P_e при фіксованому значенні порогу D_0 у вигляді критерію $D_\Sigma^{\alpha+\beta} = D_\Sigma^\alpha + D_\Sigma^\beta$.

Впровадження міри (3.2) для оцінювання ваг характеристичних параметрів опишемо аналітично виразом

$$D = \sum_{l=1}^{L} w_l^U \left(U_l^{vs} - U_l^{et} \right) + w_{L+1}^{(f)} \left(f_0^{vs} - f_0^{et} \right), \tag{3.11}$$

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

$$\min_{w_l}\left(D_\Sigma^\alpha \right) = \min_{w_l}\left(\sum_{p=1}^{P} \left(D_p^\alpha \right)^2 \right), \tag{3.12}$$

де D_p^α – міра близькості 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).

Узгодимо вирази (3.11), (3.12) у вигляді виразу

$$\min_{w_l}\left(D_{\Sigma}^{\alpha}\right)=\min_{w_l}\left(\sum_{p=1}^{P}\left(\sum_{l=1}^{L+1}w_l\gamma_{l,p}\right)^2\right), \tag{3.13}$$

де $\mathrm{H}=\{\gamma_{l,p}\}=\left\{\gamma_{1,p}\equiv\left(U_{1,p}^{\alpha}-U_1^{et}\right)^2,\ldots,\gamma_{L,p}\equiv\left(U_{L,p}^{\alpha}-U_L^{et}\right)^2,\ \gamma_{L+1,p}\equiv\left(f_{0,p}^{\alpha}-f_0^{et}\right)^2\right\}$ – вектор оцінюваних характеристичних параметрів моделі (3.11), 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, $p=\overline{1,P}$. Для розрахунку оптимальних щодо критерію (3.13) ваг w_l необхідно прирівняти до нуля похідні від D_{Σ}^{α} по w_l і розв'язати отриману систему лінійних рівнянь відносно w_l. Якщо обмеження на значення ваг w_l відсутні, то в результаті розв'язку ми отримаємо тривіальний результат – при $\gamma_{l,p}>0$ $w_l=0$, адже мінімальне значення критерію $D_{\Sigma}^{\alpha}=0$ отримується при значеннях ваг $w_l=0$. Природно, що практичної цінності такий результат не має, адже, при $D_0\to 0$ і $\alpha\to 0$ значення $\beta\to 1$, що неприпустимо. Втім, розвинемо цю ідею. Виразимо вагу w_1 із виразу для нормування ваг $\sum_{l=1}^{L+1}w_l=1$:

$$w_1=1-\sum_{l=2}^{L+1}w_l \tag{3.14}$$

і підставимо у вираз для розрахунку критерію $D_{\Sigma}^{\alpha}=\sum_{p=1}^{P}\left(D_p^{\alpha}\right)^2$:

$$D_{\Sigma}^{\alpha}=\sum_{p=1}^{P}\left(\gamma_{1,p}+\sum_{l=2}^{L+1}w_l\left(\gamma_{l,p}-\gamma_{1,p}\right)\right)^2. \tag{3.15}$$

Прирівняємо до нуля похідні від D_{Σ}^{α} по w_l, аналітично описані виразом (3.15) при $l=\overline{2,L+1}$,

$$\frac{\partial D_{\Sigma}^{\alpha}}{\partial w_l}=0. \tag{3.16}$$

Розкриємо вираз (3.16) у вигляді системи з L лінійних рівнянь:

$$\begin{cases} \sum_{l=2}^{L+1}\left(\sum_{p=1}^{P}\left(\gamma_{1,p}-\gamma_{2,p}\right)\left(\gamma_{1,p}-\gamma_{l,p}\right)\right)w_l=\sum_{p=1}^{P}\gamma_{1,p}\left(\gamma_{1,p}-\gamma_{2,p}\right), \\ \sum_{l=2}^{L+1}\left(\sum_{p=1}^{P}\left(\gamma_{1,p}-\gamma_{3,p}\right)\left(\gamma_{1,p}-\gamma_{l,p}\right)\right)w_l=\sum_{p=1}^{P}\gamma_{1,p}\left(\gamma_{1,p}-\gamma_{3,p}\right), \\ \ldots \\ \sum_{l=2}^{L+1}\left(\sum_{p=1}^{P}\left(\gamma_{1,p}-\gamma_{L+1,p}\right)\left(\gamma_{1,p}-\gamma_{l,p}\right)\right)w_l=\sum_{p=1}^{P}\gamma_{1,p}\left(\gamma_{1,p}-\gamma_{L+1,p}\right), \end{cases} \tag{3.17}$$

розв’язавши яку відносно w_l отримаємо точку екстремуму, класифікувати яку можна за значенням другої похідної від (3.15) по w_l у цій точці:

$$\frac{\partial^2 D_{\Sigma}^{\alpha}}{\partial w_l^2}=\sum_{p=1}^{P}\left(\gamma_{1,p}-\gamma_{l,p}\right)^2>0. \tag{3.18}$$

Якщо нерівність (3.18) виконується, то точка, яка класифікується, є точкою мінімуму. Аналітичний розрахунок ваг w_l для міри D, представленої критерієм (3.12), зводиться до тривіального розв’язку системи (3.17) 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.

Для зручності застосування чисельних методів для розв’язування системи (3.17) представимо останню у матричному вигляді

$$Aw=B, \tag{3.19}$$

де w – вектор-стовпець розмірністю $L\times 1$ з елементів w_l, $l=\overline{2,L+1}$; B – вектор-стовпець розмірністю $L\times 1$ з елементів $b_j=\sum_{p=1}^{P}\gamma_{1,p}\left(\gamma_{1,p}-\gamma_{j,p}\right)$, $j=\overline{2,L+1}$; A – матриця розмірністю $L\times L$ з елементів $a_{j,l}=\sum_{p=1}^{P}\left(\gamma_{1,p}-\gamma_{j,p}\right)\left(\gamma_{1,p}-\gamma_{l,p}\right)$, $j,l=\overline{2,L+1}$.

Аналітично розв’язок (3.19) опишемо виразом

$$w=A^{-1}B. \tag{3.20}$$

Відзначимо, що при малій розбіжності значень характеристичних параметрів математичної моделі, екстрагованих із різних фонограм одного і того ж суб'єкта, або при явній перевазі значень одних параметрів над іншими між рядками невиродженої матриці A може виникнути квазіперіодичність, в наслідок чого визначник ΔA набуватиме замалого значення, що призводитиме до значної похибки при розрахунку значень матриці A, і, відповідно, значень вектор-стовпця w. Позбавитися описаних обчислювальних ускладнень можна, зокрема, якщо у виразі (3.20) перейти від оберненої матриці A^{-1} до псевдооберненої матриці $A^{+}\big|_{\Delta A \neq 0}$ по Муру–Петроузу [283], що забезпечить мінімальність нев'язки і максимальність евклідової норми розв'язання системи (3.19). Емпірично було виявлено значення елементів перевірних нульових матриць $F = AA^{-1}A - A = 0$ і $G = AA^{+}A - A = 0$ для різних порядків матриці A:

- при розмірності 2×2 матриці A – $\max\left(f_{j,l}\right) \approx 10^{-4}$, $\max\left(g_{j,l}\right) \approx 10^{-8}$;
- при розмірності 3×3 матриці A – $\max\left(f_{j,l}\right) \approx 10^{-4}$, $\max\left(g_{j,l}\right) \approx 10^{-4}$;
- при розмірності 4×4 матриці A – $\max\left(f_{j,l}\right) \approx 10^{-2}$, $\max\left(g_{j,l}\right) \approx 10^{-4}$;
- при розмірності 5×5 матриці A – $\max\left(f_{j,l}\right) \approx 10^{-4}$, $\max\left(g_{j,l}\right) \approx 10^{-4}$;
- при розмірності 6×6 матриці A – $\max\left(f_{j,l}\right) \approx 10^{16}$, $\max\left(g_{j,l}\right) \approx 10^{-5}$.

Псевдообернена матриця A^{+} розраховувалася за методом Гревіля [283]. Отже, якщо значення визначника невиродженої матриці A є достатньо малим, рекомендується перейти від виразу (3.19) до виразу

$$w = A^{+}B, \tag{3.21}$$

що дозволить зменшити методичну похибку розрахунків.

Припустимося аналогічних наведеним вище міркуванням для отримання аналітичних виразів для обчислення ваг w_l в контексті мінімізації критерію D_{Σ}^{β}

$$\min_{w_l}\left(D_{\Sigma}^{\beta}\right) = \min_{w_l}\left(\sum_{m=1}^{M}\left(D_{m}^{\beta}\right)^{2}\right), \tag{3.22}$$

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 $\mathrm{I} = \{\eta_{l,m}\} = \left\{\eta_{1,m} \equiv \left(U_{1,m}^{\beta} - U_1^{et}\right)^{-2}, \ldots, \eta_{L,m} \equiv \left(U_{L,m}^{\beta} - U_L^{et}\right)^{-2},\right.$ $\left.\eta_{L+1,m} \equiv \left(f_{0,p}^{\beta} - f_0^{et}\right)^{-2}\right\}$ – вектор оцінюваних характеристичних параметрів моделі (3.11), і $\Omega = \{w_{L+1}\} = \left\{w_1 = w_1^U, \ldots, w_L = w_L^U, w_{L+1} = w^f\right\}$ – 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 $D_{\Sigma}^{\beta} = \sum_{m=1}^{M} \left(D_m^{\beta}\right)^2$:

$$D_{\Sigma}^{\beta} = \sum_{m=1}^{M} \left(\eta_{1,m} + \sum_{l=2}^{L+1} w_l \left(\eta_{l,m} - \eta_{1,m} \right) \right)^2 . \tag{3.23}$$

Прирівняємо до нуля похідні від D_{Σ}^{β} по w_l, описані виразом (3.23), при $l = \overline{2, L+1}$:

$$\frac{\partial D_{\Sigma}^{\beta}}{\partial w_l} = 0 . \tag{3.24}$$

Розкриємо (3.24) у вигляді системи з L лінійних рівнянь

$$\begin{cases} \sum_{l=2}^{L+1} \left(\sum_{m=1}^{M} \left(\eta_{1,m} - \eta_{2,m}\right)\left(\eta_{1,m} - \eta_{l,m}\right) \right) w_l = \sum_{m=1}^{M} \eta_{1,m} \left(\eta_{1,m} - \eta_{2,m}\right), \\ \sum_{l=2}^{L+1} \left(\sum_{m=1}^{M} \left(\eta_{1,m} - \eta_{3,m}\right)\left(\eta_{1,m} - \eta_{l,m}\right) \right) w_l = \sum_{m=1}^{M} \eta_{1,m} \left(\eta_{1,m} - \eta_{3,m}\right), \\ \ldots \\ \sum_{l=2}^{L+1} \left(\sum_{m=1}^{M} \left(\eta_{1,m} - \eta_{L+1,m}\right)\left(\eta_{1,m} - \eta_{l,m}\right) \right) w_l = \sum_{m=1}^{M} \eta_{1,m} \left(\eta_{1,m} - \eta_{L+1,m}\right), \end{cases} \tag{3.25}$$

розв'язавши яку відносно w_l, отримаємо точку екстремуму класифікувати яку можна за значенням другої похідної від (3.23) по w_l у цій точці:

$$\frac{\partial^2 D_\Sigma^\beta}{\partial w_l^2} = \sum_{m=1}^{M} \left(\eta_{1,m} - \eta_{l,m}\right)^2 > 0 . \qquad (3.26)$$

Якщо нерівність (3.26) виконується, то точка, яка класифікується, є мінімумом. Аналітичний розрахунок ваг w_l для міри D, представленої критерієм (3.22), зводиться до розв'язку системи (3.25) відносно w_l, матрична форма запису якої аналогічна (3.19), де B – вектор-стовпець розмірністю $L \times 1$ з елементів $b_j = \sum_{m=1}^{M} \eta_{1,m}\left(\eta_{1,m} - \eta_{j,m}\right)$, $j = \overline{2, L+1}$; A – матриця розмірністю $L \times L$ з елементів $a_{j,l} = \sum_{m=1}^{M} \left(\eta_{1,m} - \eta_{j,m}\right)\left(\eta_{1,m} - \eta_{l,m}\right)$, $j,l = \overline{2, L+1}$. Розв'язок системи (3.25) в матричній формі аналогічний виразу (3.20).

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

$$\min_{w_l}\left(D_\Sigma^{\alpha+\beta}\right) = \min_{w_l}\left(\sum_{p=1}^{P}\left(D_p^\alpha\right)^2 + \sum_{m=1}^{M}\left(D_m^\beta\right)^2\right). \qquad (3.27)$$

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 $l = \overline{2, L+1}$:

$$\frac{\partial D_\Sigma^{\alpha+\beta}}{\partial w_l} = 0 . \qquad (3.28)$$

Розкриємо вираз (3.28) у вигляді системи з L лінійних рівнянь, матричний запис якої збігається із (3.19), в якій B – вектор-стовпець розмірністю $L \times 1$ з елементів $b_j = \sum_{p=1}^{P} \gamma_{1,p}\left(\gamma_{1,p} - \gamma_{j,p}\right) + \sum_{m=1}^{M} \eta_{1,m}\left(\eta_{1,m} - \eta_{j,m}\right)$, $j = \overline{2, L+1}$; A – матриця розмірністю $L \times L$ з елементів $a_{j,l} = \sum_{p=1}^{P} \left(\gamma_{1,p} - \gamma_{j,p}\right)\left(\gamma_{1,p} - \gamma_{l,p}\right) + \sum_{m=1}^{M} \left(\eta_{1,m} - \eta_{j,m}\right)\left(\eta_{1,m} - \eta_{l,m}\right)$, $j,l = \overline{2, L+1}$.

Розв'язавши систему, перетворену до вигляду (3.20), відносно ω_l отримаємо точку екстремуму, класифікувати яку можна за значенням другої похідної від $D_{\Sigma}^{\alpha+\beta}$ по ω_l у цій точці:

$$\frac{\partial^2 D_{\Sigma}^{\alpha+\beta}}{\partial w_l^2} = \sum_{p=1}^{P}\left(\gamma_{1,p} - \gamma_{l,p}\right)^2 \sum_{m=1}^{M}\left(\eta_{1,m} - \eta_{l,m}\right)^2 > 0\,. \tag{3.29}$$

Нерівність (3.29) завжди виконуватиметься, що гарантує знаходження значень ω_l, які мінімізують значення критерію $D_{\Sigma}^{\alpha+\beta}$.

Зауважимо, що на практиці значення ваг w_l і критеріїв D можуть бути і від'ємними, тому при порівнянні значення критерію D з порогом D_0 значення першого слід брати за модулем, причому найкращим буде значення критерію $|D| \to 0$. Окрім умови нормованості, при розрахунку значень w_l, які мінімізують значення критеріїв $D_{\Sigma} = \left\{D_{\Sigma}^{\alpha}, D_{\Sigma}^{\beta}, D_{\Sigma}^{\alpha+\beta}\right\}$ в задачу оптимізації можна ввести додаткове обмеження на додатність значень w_l: $0 \le w_l \le 1$. В такому випадку задачу оптимізації можна класифікувати як задачу нелінійного (квадратичного) програмування, розв'язати яку можна відомими методами математичного програмування [284–286].

Також відзначимо, що мовленнєві сигнали, описувані моделями (2.1), (2.24), (2.46), (2.64), параметризуються взаємно некорельованими характеристиками f_0 і U_l, що дозволяє окрім очевидної міри (3.11) запропонувати відносну міру

$$D' = \sum_{l=1}^{L}\left(U_l^{vs}\left(f_0^{vs}\right)^{-1} - U_l^{et}\left(f_0^{et}\right)^{-1}\right)^2, \tag{3.30}$$

позбавлену ваг. Чутливість міри (3.30) забезпечується динамічною природою амплітуд U_l, а нормованість – відносною стабільністю частоти основного тону f_0. Втім, проаналізуємо самостійність міри D' від міри D, розкривши вираз (3.11) для обчислення останньої у вигляді

$$D = \sum_{l=1}^{L} w_l \cdot \Delta U_l^2 + w_{L+1} \cdot \Delta f_0^2\,, \tag{3.31}$$

де $\Delta U_l = U_l^{vs} - U_l^{et}$; $\Delta f_0 = f_0^{vs} - f_0^{et}$.

У контексті (3.31), міру (3.30) можна описати виразом

$$D' = \sum_{l=1}^{L}\left(\left(\Delta U_l f_0^{et} - \Delta f_0 U_l^{et}\right)\left(f_0^{et}\left(\Delta f_0 + f_0^{et}\right)\right)^{-1}\right) =$$

$$= \Delta U_l^2 \sum_{l=1}^{L}\left(\Delta f_0 + f_0^{et}\right)^{-2} + \Delta f_0^2 \sum_{l=1}^{L}\left(U_l^{et}\right)^2\left(\left(f_0^{et}\right)^2\left(\Delta f_0 + f_0^{et}\right)^2\right)^{-1} - \tag{3.32}$$

$$- \Delta U_l \cdot \Delta f_0 \sum_{l=1}^{L} 2U_l^{et}\left(\left(f_0^{et}\right)\left(\Delta f_0 + f_0^{et}\right)^2\right)^{-1}.$$

Вирази (3.31) і (3.32), вочевидь, не збігаються, що підтверджує самостійність міри D' від D, а залежність значення міри (3.32) не тільки від сталих значень U_l^{et} і f_0^{et}, а і від відносних значень ΔU_l і Δf_0 не дозволяє ввести еквівалент ваг ω_l в явному вигляді. Представлення міри (3.30) у вигляді (3.32) дозволило з'ясувати, що $D' = 0$ при

$$\Delta U_l \left(U_l^{et}\right)^{-1} = \Delta f_0 \left(f_0^{et}\right)^{-1}, \tag{3.33}$$

де $l = \overline{1, L}$, що є недоліком. Проте, описану ситуацію можна звести до малоімовірної збільшивши кількість несних гармонік L, амплітуди яких враховуються в якості характеристичних параметрів індивідуальності мовленнєвого сигналу.

Представимо значення порогу D_0 як функцію від варіації значень характеристичних параметрів $\lambda^{vs} = \left(\lambda_1^{vs}, \lambda_2^{vs}, \ldots, \lambda_L^{vs}\right)$, екстрагованих із фонограми, представленої суб'єктом для автентифікації, відносно еталонних значень характеристичних параметрів $\lambda^{et} = \left(\lambda_1^{et}, \lambda_2^{et}, \ldots, \lambda_L^{et}\right)$, отриманих узагальненням результатів параметризації фонограм навчальної вибірки,

$$D_0(\Delta\lambda) = D\left(\lambda^{vs}, \lambda^{et}\right) = D\left(\lambda^{et} \pm \Delta\lambda, \lambda^{et}\right), \tag{3.34}$$

де $\Delta\lambda = \left(\Delta\lambda_1 = \left|\lambda_1^{et} - \lambda_1^{vs}\right|, \ldots, \Delta\lambda_{L+1} = \left|\lambda_L^{et} - \lambda_L^{vs}\right|\right)$ – вектор, який описує згадану вище варіативність аналітично. Із урахуванням варіації $\pm\Delta\lambda$ вираз (3.34) можна перетворити до вигляду

$$D_0(\Delta\lambda) = D\left(\lambda^{et} - \Delta\lambda, \lambda^{et} + \Delta\lambda\right). \tag{3.35}$$

Врахувавши вираз (3.35), опишемо аналітично процес розрахунку порогу D_0 на основі міри (3.30) у вигляді

$$D_0 = \sum_{l=1}^{L}\left(\left(U_l^{et} + \Delta U_l\right)\left(f_0^{et} - \Delta f_0\right)^{-1} - \left(U_l^{et} - \Delta U_l\right)\left(f_0^{et} + \Delta f_0\right)^{-1}\right) = \\ = 4\left(\left(f_0^{et}\right)^2 - \left(\Delta f_0\right)^2\right)^{-2} \sum_{l=1}^{L}\left(\Delta f_0 U_l^{et} + \Delta U_l^{et} f_0^{et}\right)^2. \quad (3.36)$$

Значення вектора $\Delta\lambda$ фактично утворюють довірчі інтервали для відповідних характеристичних параметрів індивідуальності мовленнєвого сигналу, зокрема, для U_l і f_0 їх можна описати виразами

$$\Delta U_l = \mu\sigma_{U_l^{et}},\ \Delta f_0 = \mu\sigma_{f_0^{et}}, \quad (3.37)$$

де $\sigma_{U_l^{et}}$ і $\sigma_{f_0^{et}}$ – середньоквадратичні відхилення відповідних параметрів; $\mu \equiv \mu(P)$ – параметр [281], залежний від довірчої імовірності $P = \int_{-\mu\sigma}^{\mu\sigma} p(x)dx$, де $p(x)$ – щільність імовірності нормального розподілу, так при $P = 95\,\%$ $\mu = 2{,}005 \approx 2$, при $P = 99\,\%$ $\mu = 2{,}576 \approx 2{,}6$.

Врахувавши (3.34), удосконалимо міру (3.30) з метою позбавлення недоліку (3.33):

$$D' = \left(f_0^{et}\right)^{-2} \sum_{l=1}^{L}\left(\left(f_0^{et} - f_0^{vs}\right)^2 + v_1\right)\left(\left(U_l^{et} - U_l^{vs}\right)^2 + v_2\right) = \\ = \left(\left(f_0^{et} - f_0^{vs}\right)^2 + v_1\right)\left(f_0^{et}\right)^{-2} \sum_{l=1}^{L}\left(\left(U_l^{et} - U_l^{vs}\right)^2 + v_2\right), \quad (3.38)$$

де v_1 – константа ступеня розбіжності значень параметрів f_0^{et} і f_0^{vs}, v_2 – константа ступеня розбіжності значень параметрів U_l^{et} і U_l^{vs}, $l = \overline{1, L}$. Природнім буде обирати значення констант v_1 і v_2 пропорційно значенням інтервалів Δf_0 і ΔU_l, визначених у (3.37), що дозволить привести міру (3.38) до вигляду

$$D' = \left(\left(f_0^{et} - f_0^{vs}\right)^2 + \Delta f_0^2\right)\left(f_0^{et}\right)^{-2} \sum_{l=1}^{L}\left(\left(U_l^{et} - U_l^{vs}\right)^2 + \Delta U_l^2\right). \quad (3.39)$$

Значення міри (3.39) завжди більше нуля, навіть при виконанні умови (3.33)

$$D'\big|_{(5,74)} = \Delta f_0^2 \left(f_0^{et}\right)^{-2} \sum_{l=1}^{L} \Delta U_l^2 \ . \tag{3.40}$$

Перетворимо міру (3.39) так, щоб при виконанні умови (3.33) значення міри дорівнювало нулю, враховуючи, що $\Delta U_l = const$,

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

$$- \Delta f_0^2 \left(f_0^{et}\right)^{-2} L \Delta U_l^2 = \left(\left(f_0^{et} - f_0^{vs}\right) \left(f_0^{et}\right)^{-1} \right)^2 \sum_{l=1}^{L} \left(U_l^{et} - U_l^{vs}\right)^2 + \tag{3.41}$$

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

де $\delta f_0^2 = \Delta f_0 \left(f_0^{et}\right)^{-1}$ – відносний інтервал варіації частоти основного тону.

Значення порогу D_0 для міри (3.41) визначимо з урахуванням (3.33):

$$D_0 = \left(2\Delta f_0 \left(f_0^{et}\right)^{-1} \right)^2 \sum_{l=1}^{L} \left(2\Delta U_l\right)^2 + L \Delta U_l^2 \left(2\Delta f_0 \left(f_0^{et}\right)^{-1} \right)^2 +$$

$$+ \delta f_0^2 \sum_{l=1}^{L} \left(2\Delta U_l\right)^2 = 24 L \delta f_0^2 \Delta U_l^2 . \tag{3.42}$$

Проведемо оцінювання залежності значень довірчих інтервалів параметрів ΔU_l δf_0 від достовірності методів розрахунку значень характеристичних параметрів f_0 і U_l. Наприклад, оцінюватимемо достовірність параметра f_0^{et}, обчисленого при невідомих початкових характеристиках несних гармонік за методом максимальної правдоподібності із середньоквадратичним відхиленням

$$\sigma_{f_0^{et}} = \sqrt{3 L_{f_0} \left(\pi^2 D_z T^2 \sum_{l=1}^{L_{f_0}} l^2 \right)^{-1}} , \tag{3.43}$$

де D_z – коефіцієнт рівня відношення «сигнал»/«шум», значення якого визначається за виразом (2.90); T – тривалість спостереження аналізованого сигналу; L_{f_0} – кількість амплітуд гармонік для обчислення частоти основного тону.

Скористаємося виразами (3.37) для визначення відносного розкиду значення частоти основного тону δf_0 при заданому значенні довірчої імовірності P:

$$\delta f_0 = \sqrt{\mu L_{f_0}\left(\pi^2 D_z \tau_i^2 \left(f_0^{et}\right)^2 \sum_{l=1}^{L_{f_0}} l^2\right)^{-1}}\,. \qquad (3.44)$$

Враховуючи вираз (3.37), сформулюємо вираз для обчислення значення абсолютного розкиду амплітуд гармонік ΔU_l для несних гармонік U_l^{et}, значення яких розраховано за методом найменших квадратів із середньоквадратичним відхиленням (Д.44):

$$\Delta U_l = \sqrt{\mu^2 \varepsilon\left(\widehat{V}\right)\left\{S^T S\right\}_{l,l}\left(4(J-L)\widehat{U}_l^2\right)^{-1}}\,. \qquad (3.45)$$

Опишемо аналітично поріг (3.42) для міри (3.39), характеристичні параметри для якої розраховувалися на основі виразів (3.44) і (3.45):

$$D_0 = 6\mu^4 L L_{f_0} \varepsilon\left(\widehat{V}\right)\left\{S^T S\right\}_{l,l}\left(\pi^2 D_z \tau_i^2 (J-L)\left(\widehat{U}_l f_0^{et}\right)^2 \sum_{l=1}^{L_{f_0}} l^2\right)^{-1}. \qquad (3.46)$$

Встановивши значення параметрів $f_d = 8000$ Гц; $L_{f_0} = 3$; $J = 200$; $L = 10$; $P = \{95\,\%, 99\,\%, 99{,}5\,\%, 99{,}7\,\%\}$, обчислимо значення порогу D_0 за виразом (3.46) для чоловічих і жіночих голосів при тривалості фонограм $T_f = \{0{,}1, 0{,}5, 1\}$ с, представивши результат у вигляді табл. 3.1.

Результати емпіричних досліджень з автентифікації 40 суб’єктів за їх мовленнєвими матеріалами, представленими у базі NOIZEUS (дві фонограми для навчання системи і п’ять фонограм для її тестування для кожного суб’єкта), описуваними множинами характеристичних параметрів $\{f_0, U_1, \ldots, U_{10}\}$, із використанням мір (3.30) – D_1' і (3.41) – D_2', такі: усереднені імовірності похибок першого роду – $\overline{\alpha}_{D_1'} = 0{,}8\%$, $\overline{\alpha}_{D_2'} = 0{,}4\%$; усереднені імовірності похибок другого роду – $\overline{\beta}_{D_1'} = 0{,}9\%$, $\overline{\beta}_{D_2'} = 0{,}6\%$; середня імовірність похибки – $\overline{P}_e^{D_1'} \le 0{,}5\%$ $\overline{P}_e^{D_2'} \le 0{,}5\%$.

Таблиця 3.1

Емпірично визначені рекомендовані значення порогу D_0

Тривалість	Поріг D_0

фонограми	$P = 95\%$	$P = 99\%$	$P = 99{,}5\%$	$P = 99{,}7\%$
Чоловічі голоси				
0,1 с	$2{,}281 \cdot 10^{-2}$	$1{,}825 \cdot 10^{-2}$	$1{,}294 \cdot 10^{-2}$	$4{,}750 \cdot 10^{-3}$
0,5 с	$1{,}684 \cdot 10^{-2}$	$1{,}347 \cdot 10^{-2}$	$9{,}555 \cdot 10^{-3}$	$3{,}507 \cdot 10^{-3}$
1 с	$1{,}509 \cdot 10^{-2}$	$1{,}207 \cdot 10^{-2}$	$8{,}560 \cdot 10^{-3}$	$3{,}142 \cdot 10^{-3}$
Жіночі голоси				
0,1 с	$1{,}634 \cdot 10^{-2}$	$1{,}307 \cdot 10^{-2}$	$9{,}272 \cdot 10^{-3}$	$3{,}404 \cdot 10^{-3}$
0,5 с	$1{,}260 \cdot 10^{-2}$	$1{,}008 \cdot 10^{-2}$	$7{,}149 \cdot 10^{-3}$	$2{,}624 \cdot 10^{-3}$
1 с	$8{,}145 \cdot 10^{-3}$	$6{,}517 \cdot 10^{-3}$	$4{,}622 \cdot 10^{-3}$	$1{,}696 \cdot 10^{-3}$

Також виявилося, що для апріорного оцінювання результатів автентифікації в якості похибки першого роду можна використовувати величину $\alpha = 1 - P$, де P – довірча імовірність, враховувана при обчисленні порогу D_0. Тоді в значенні порогу D_0 враховуватимуться варіації характеристичних параметрів голосу цільового суб'єкта, а імовірність його не автентифікувати дорівнюватиме α. Значення похибки другого роду β визначається, здебільшого, рівнем відношення «сигнал»/«шум» і обсягом навчальної вибірки. Зауважимо, що при відомій достовірній оцінці рівня відношення «сигнал»/«шум» значення β при фіксованому значенні α можна обчислити за критерієм Неймана–Пірсона [281], при чому максимальна потужність критерію дорівнюватиме $1 - \beta$.

3.2 Оцінювання адекватності запропонованих Моделей індивідуальності голосу

У розділі 2 теоретично обґрунтовано чотири основних моделі ІГМС для АСГ, зокрема, базову й уточнену квазідетерміновані моделі та базову й уточнену стохастичні моделі, які формалізовано виразами (2.1), (2.24), (2.46) і (2.64), відповідно. У підрозділі 3.1 сформульовано методику оцінювання адекватності моделей ІГМС для АСГ вхідним даним. Узагальнимо згадані теоретичні результати

здійснивши емпіричне оцінювання адекватності запропонованих моделей ІГМС для АСГ.

Перед порівнянням якісних характеристик оцінюваних моделей уніфікуємо формат їх вхідних даних. В якості вхідних даних використаємо еталонний мовленнєвий сигнал – прийменник «on», фонограму із записом виголошення якого взято із безкоштовної бази Школи інжинірингу та комп'ютерних наук Еріка Джонсона при Університеті Техасу (Даллас, США) NOIZEUS [282], матеріали якої використовуються науковцями для дослідження алгоритмів покращення звуку. Еталонний мовленнєвий сигнал, значення x_i якого візуалізовано на рис. 3.1, оцифровано із частотою дискретизації $f_d = 6000$ Гц і 8-ми бітною розрядністю квантування.

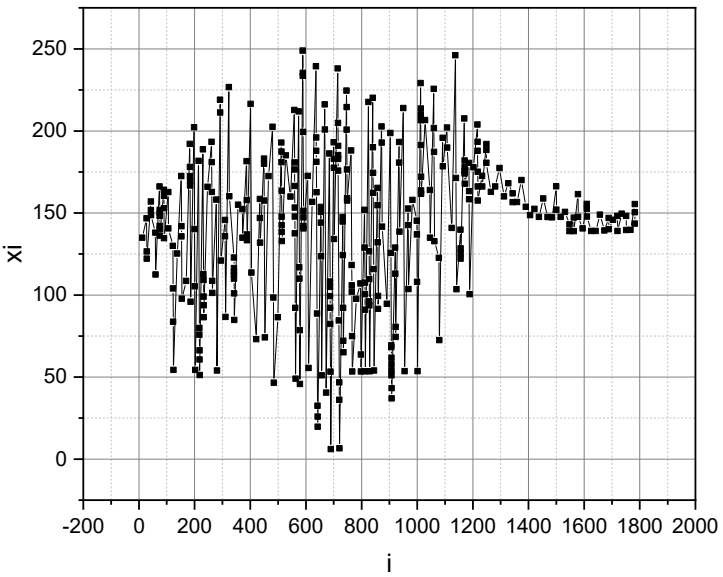


Рисунок 3.1 – Візуалізація значень відліків еталонного мовленнєвого сигналу.

Також уніфікуємо значення основних вихідних коефіцієнтів τ_i, φ_0, Γ_0, F_0, M, вживаних у більшості досліджуваних моделях. При тривалості оцифрованої із частотою дискретизації $f_d = 6000$ Гц фонограми $\tau_i = 300$ мс, кількість відліків сигналу $N = 1800$. Кількість істотних відліків нормованої автокореляційної функції $J = 200$. Враховуючи, що початкові фази фонем виголошеної злитої мови практично не розпізнаються слуховою системою людини [45, 214–217], приймемо значення початкових фаз рівними $\varphi_0 = 0$, $\Gamma_0 = \pi$, відповідно. Приймемо період

модулювального коливання T_{F_0} рівним тривалості виголошення однієї фонеми, значення якої знаходиться у діапазоні $50 \div 300$ мс [248]. Відповідно, значення частоти модулювального коливання знаходиться у діапазоні $F_0 = 3{,}3 \div 20$ Гц. Враховуючи однотипність аналітичного апарату досліджуваних моделей із математичним апаратом Фур'є, оцінюватимемо частоту основного тону не за миттєвими зрізами спектра τ_1, а за усередненими за інтервал τ_i значеннями спектра: $f_0 = \overline{f_0^{\tau_i}} = \tau_i^{-1} \int_0^{\tau_i} f_0(t)dt$, де $f_0(t)$ – функція, яка описує зміну значення частоти основного тону у часі [262]. Такий вибір пояснюється специфікою масштабування перетворення Фур'є – чим коротший сигнал у часовому вимірі, тим ширший його спектр у частотному вимірі. На рис. 3.2 видно, що результати оцінювання частоти основного тону за миттєвими зрізами $\tau_1 = 85$ мс суттєво відрізняються від результатів оцінювання цього параметра за усередненими значеннями τ_i – у першому варіанті з'являються хибні локальні максимуми.

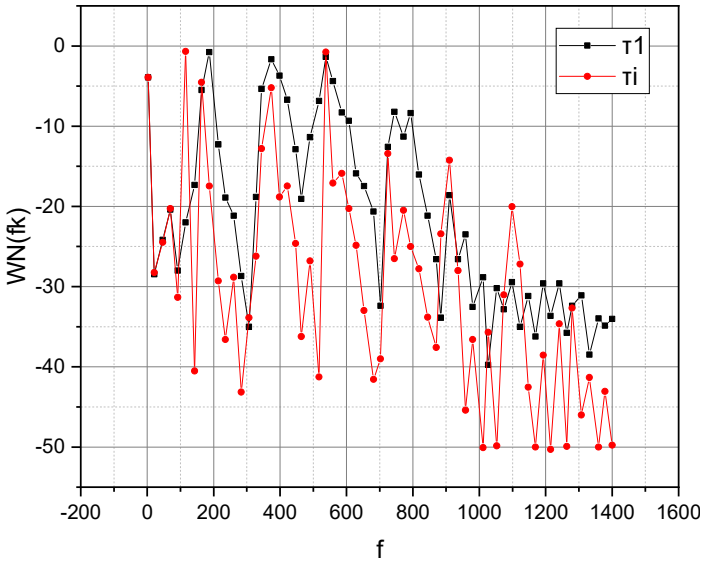


Рисунок 3.2 – Оцінювання частоти основного тону за положеннями максимумів функції нормованої спектральної щільності потужності еталонного мовленнєвого сигналу.

По осі ординат графіка, наведеного на рис. 3.2, відкладено шкалу значень нормованої спектральної щільності потужності еталонного мовленнєвого сигналу, аналітичний опис якої визначається виразом

$$W_N(f_k) \equiv W_n\left(kf_d N^{-1}\right) = W_k\left(\max(W_k)\right)^{-1}, \qquad (3.47)$$

де $k = \overline{0, N-1}$, $f \in [0{,}0{,}5 f_d]$, $W_n\left(kf_d N^{-1}\right) = W_k = \left|\dot{C}_k\right|^2$ – коефіцієнти спектральної щільності потужності; $\dot{C}_k$ – коефіцієнти дискретного перетворення Фур'є.

Опишемо еталонний мовленнєвий сигнал базовою квазідетермінованою моделлю (2.1) при значеннях вихідних коефіцієнтів $f_d = 6000$ Гц, $\tau_i = 300$ мс, $L = 6$, $M = 1$, $F_0 = 10$ Гц, $\varphi_0 = 0$, $\Gamma_0 = \pi$, $J = 200$, $E_u = 1$. В результаті отримаємо, відповідно, значення сімох характеристичних параметрів моделі (2.1): $f_0 = 155{,}2$ Гц, $U_1 = 0{,}819$, $U_2 = 0{,}784$, $U_3 = 1{,}457$, $U_4 = 0{,}315$, $U_5 = 0{,}327$, $U_6 = 0{,}142$. Розраховане за виразом $\varepsilon_b = \sum_{j=1}^{J}\left(b_j^u - b_j^y\right)^2$ значення абсолютної похибки опису дорівнює $0{,}994$.

Значення абсолютної похибки, нормованої за кількістю відліків кореляційної функції J, $\varepsilon_b^{norm} = J^{-1}\sum_{j=1}^{J}\left(b_j^u - b_j^y\right)^2$ дорівнює $0{,}497$. Значення відносної похибки моделі $\delta\varepsilon_b = \sum_{j=1}^{J}\left(b_j^u - b_j^y\right)^2\left(\sum_{j=1}^{J}\left(b_j^y\right)^2\right)^{-1} \cdot 100\ \%$ дорівнює $5{,}688\%$. На рис. 3.3 візуалізовано нормовану автокореляційну функцію b_j^y центрованого еталонного мовленнєвого сигналу і значення нормованої автокореляційної функції b_j^u його опису моделлю (2.1), відповідно.

Перспектива застосування значень характеристичних параметрів моделі (2.1) для АСГ визначає доцільність ідентифікації залежності між похибкою моделі ε_b і кількістю її характеристичних параметрів, що описують індивідуальність мовленнєвого сигналу. Емпірично ідентифікований вигляд такої залежності наведено на рис. 3.4.

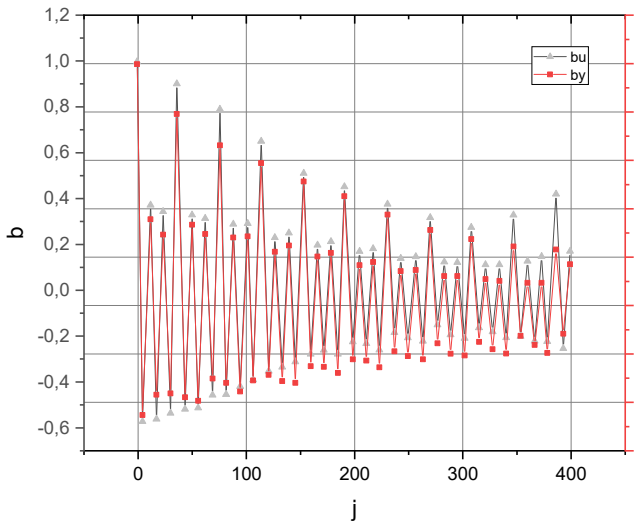


Рисунок 3.3 – Значення нормованих автокореляційних функцій центрованого еталонного мовленнєвого сигналу і його опису моделлю (2.1).

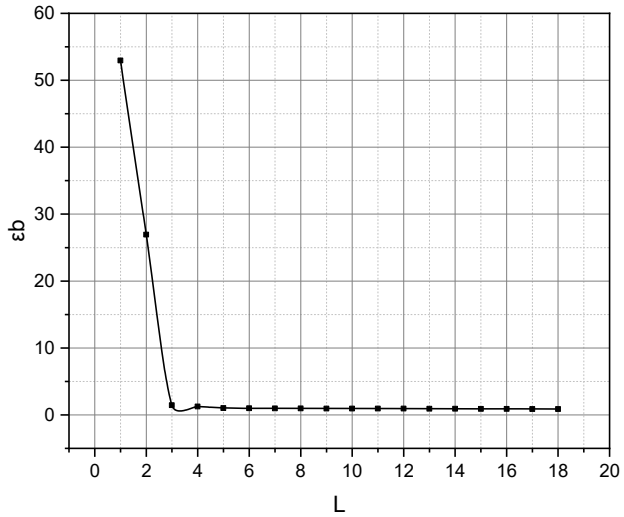


Рисунок 3.4 – Залежність абсолютної похибки моделі від кількості її характеристичних параметрів.

Зрештою, максимальна кількість гармонік несного коливання мовленнєвого сигналу, які містяться у визначеному діапазоні частот $[0, 0{,}5 f_d]$, є скінченною і може бути розрахована аналітично за виразом $L_{\max} = \lfloor 0{,}5 f_d f_0^{-1} \rfloor$.

На рис. 3.5 візуалізовано залежність $L_{\max}$ від значень частоти дискретизації мовленнєвого сигналу f_d і типових значень частоти основного тону для суб'єктів-чоловіків – $f_0^{ml} = \{f_0^{ml}{}_{\min}, f_0^{ml}{}_{avg}, f_0^{ml}{}_{\max}\}$, і суб'єктів-жінок – $f_0^{fm} = \{f_0^{fm}{}_{\min}, f_0^{fm}{}_{avg}, f_0^{fm}{}_{\max}\}$, відповідно. Зауважимо, що при розрахунку характеристичних параметрів U_l за виразом (2.15) значення $U_l^2 \in \Re$, отже слід враховувати, що

$$U_l = \begin{cases} \sqrt{U_l^2}, \, if \; U_l^2 \geq 0, \\ \dot{U}_l = i\sqrt{\left|U_l^2\right|} = \sqrt{\left|U_l^2\right|} \exp(0.5\pi i), \, if \; U_l^2 < 0. \end{cases}$$

Параметри $\dot{U}_l$ є комплексними амплітудами із вихідними фазами $\varphi_l = 0{,}5\pi$ і значеннями амплітуд несних гармонік, рівними $\sqrt{\left|U_l^2\right|}$. Емпірично встановлено,

що поява комплексних амплітуд $\dot{U}_l$ імовірна при $l \geq 7$, тоді як згідно з результатами, наведеними на рис. 3.4, високий рівень достовірності опису ІГМС моделлю (2.1) досягається вже при $L = 6 \div 10$.

Також викликає дослідницький інтерес задача оцінювання впливу характеристики модулювального коливання на похибку опису еталонного мовленнєвого сигналу моделлю (2.1). Емпірично ідентифіковано вид залежності між цими параметрами, яку візуалізовано на рис. 3.6.

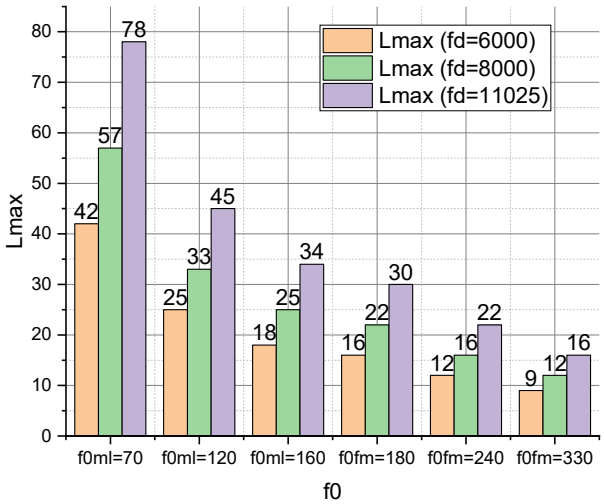


Рисунок 3.5 – Оцінювання довжини вектору характеристичних параметрів моделі ІГМС.

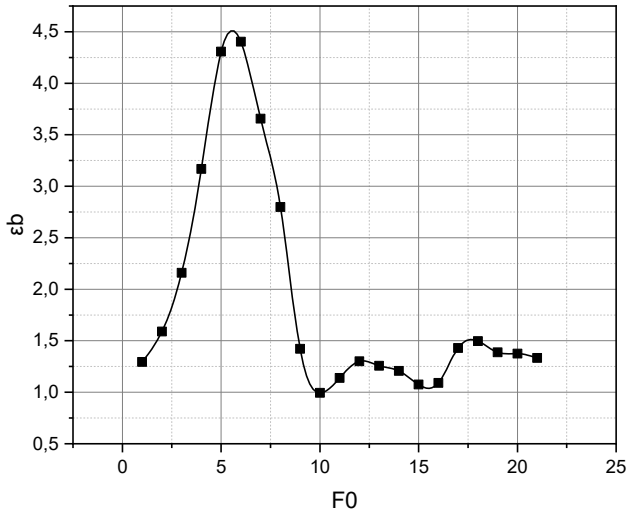


Рисунок 3.6 – Вплив модулювального коливання на похибку опису еталонного мовленнєвого моделлю (2.1)

Результати, наведені на рис. 3.6 емпірично підтверджують коректність вживання значення $F_0 = 10$ Гц при описі ІГМС моделлю (2.1). Форма модульованого коливання, описуваного моделлю (2.1), визначається результатом згортки несного і модулювального коливань. При $M = 0$ форма модульованого коливання визначається виключно формою несного коливання. Дослідимо доцільність врахування модулювального коливання при описі індивідуальності голосу в мовленнєвому сигналі моделлю (2.1). На рис. 3.7 наведено нормовані автокореляційні функції центрованого еталонного мовленнєвого сигналу b_j^y і b_j^u – його опису моделлю (2.1) при $M = 0$.

Абсолютна, нормована абсолютна і відносна похибки опису індивідуальності голосу в еталонному мовленнєвому сигналі моделлю (2.1), отриманого без урахування модулювальної компоненти, виявилися рівними $\varepsilon_b = 5{,}613$, $\varepsilon_b^{norm} = 0{,}028$ і $\delta\varepsilon_b = 32{,}119\,\%$ відповідно. Отже, нехтування модулювальною компонентою при описі індивідуальності голосу в еталонному мовленнєвому сигналі моделлю (2.1) в понад шість разів погіршує достовірність отриманого результату.

Оцінимо достовірність опису індивідуальності голосу в еталонному мовленнєвому сигналі моделлю (2.1) в частотному вимірі. На рис. 3.8 наведено залежність нормованої спектральної щільності потужності еталонного мовленнєвого сигналу $W_N(f)$, розрахованої за виразом (3.47), від частоти, значення якої змінювалося в діапазоні $f \in [0,\, 0{,}5 f_d]$.

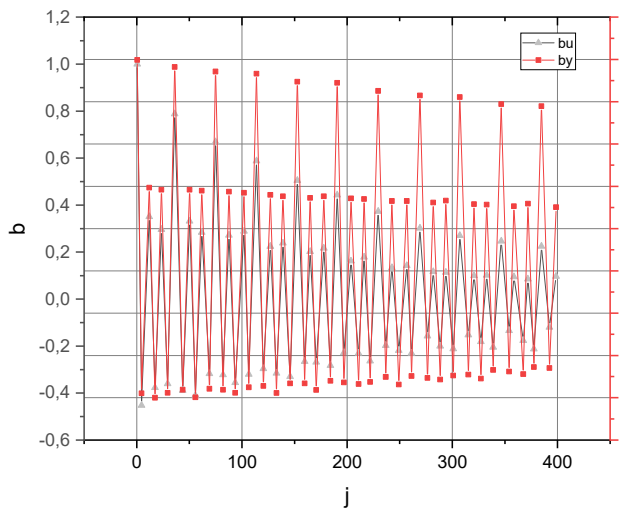


Рисунок 3.7 – Нормовані автокореляційні функції центрованого еталонного мовленнєвого сигналу і його моделі виду (2.1) без урахування модулювальної компоненти.

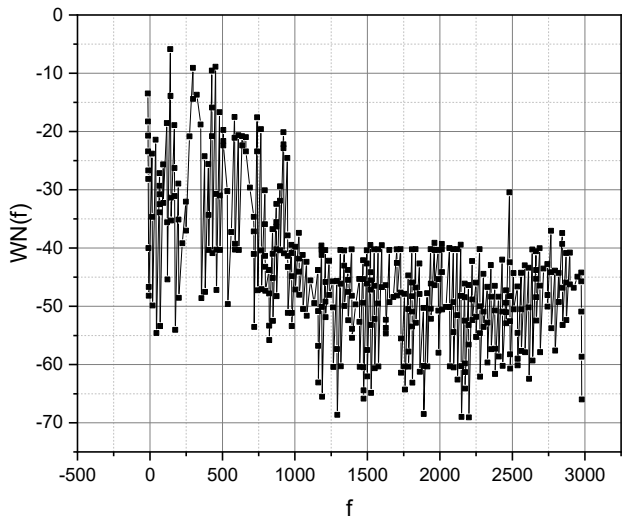


Рисунок 3.8 – Залежність нормованої спектральної щільності потужності еталонного мовленнєвого сигналу від частоти.

Максимуми функції, наведеної на рис. 3.8, відповідають наявності гармонік, кратних частості основного тону в еталонному мовленнєвому сигналі. На шостій

гармоніці значення $W_N(f)$ дорівнює $-20{,}2$ дБ, а при $f \geq 970$ Гц значення $W_N(f)$ не перевищує величини -35 дБ.

На рис. 3.9 візуалізовано залежності функцій нормованих спектральних щільностей потужностей $W_N(f)$ і $W_N^u(f)$ від частоти f. Описана виразом (3.47) функція $W_N(f)$ характеризує еталонний мовленнєвий сигнал, а функція $W_N^u(f)$ – його опис моделлю (2.1). Аналітичний вигляд функції $W_N^u(f)$ опишемо виразом

$$W_N^u(f) = (S_u(f))^2 \left(\max\left((S_u(f))^2\right)\right)^{-1}, \tag{3.48}$$

де спектральна щільність потужності моделі (2.1) обчислюється за виразом

$$\begin{aligned} S_u(f) = 0{,}5\tau_i \sum_{l=1}^{L} U_l \big(&\mathrm{sinc}(\pi(f + lf_0)\tau_i) + \mathrm{sinc}(\pi(f - lf_0)\tau_i) - \\ &- 0{,}5M\big(\mathrm{sinc}(\pi(f + lf_0 + F_0)\tau_i) + \mathrm{sinc}(\pi(f - lf_0 - F_0)\tau_i) + \\ &+ \mathrm{sinc}(\pi(f + lf_0 - F_0)\tau_i) + \mathrm{sinc}(\pi(f - lf_0 + F_0)\tau_i)\big)\big). \end{aligned} \tag{3.49}$$

Аналіз наведених на рис. 3.9 графіків дозволяє стверджувати збіжність максимумів функцій $W_N(f)$ і $W_N^u(f)$, тобто модель (2.1) адекватно описує частоту основного тону і її гармоніки в частотному вимірі. Певну осциляцію і розмитість спектра в околі гармонік основного тону обумовлено частотною модуляцією основного тону в мовленнєвому сигналі. Це є природним [287].

Переконавшись у доцільності урахування модулювальної компоненти при моделюванні ІГМС, розширимо експеримент дослідженням результатів опису індивідуальності голосу в еталонному мовленнєвому сигналі уточненою квазідетермінованою моделлю (2.24), коефіцієнти M_k і Γ_k якої дозволяють урахувати затухання обвідної нормованої автокореляційної функції досліджуваного мовленнєвого сигналу, а коефіцієнти U_l і φ_l – адекватно описувати складний характер мовленнєвих коливань, породжених артикуляційним апаратом людини. На рис. 3.10 візуалізовано нормовані автокореляційні функції еталонного мовленнєвого сигналу і його опису моделлю (2.24) при $J = 600$.

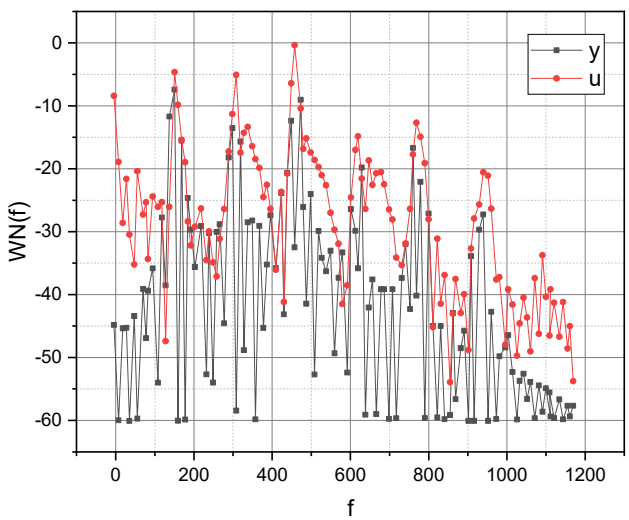


Рисунок 3.9 – Залежності нормованої спектральної щільності потужності від частоти для еталонного мовленнєвого сигналу і його опису моделлю (2.1).

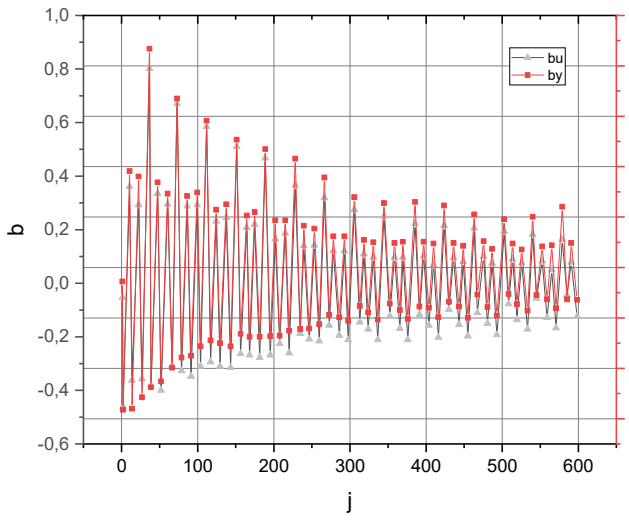


Рисунок 3.10 – Нормовані автокореляційні функції центрованого еталонного мовленнєвого сигналу і його опису моделлю (2.24).

При значеннях вхідних параметрів $\tau_i = 0{,}3$, $N = 1800$, $L = 6$, $F_0 = 10$ Гц, $\Gamma_k = 0$, $\varphi_l = 0$, $E_u = 1$, $J = 600$, $M_0 = 1$, $M_1 = 1$, $M_2 = 0{,}6$, $M_3 = 0{,}5$, $M_4 = 0{,}5$, $M_5 = 0{,}5$, модель (2.24) описала індивідуальність голосу в еталонному мовленнєвому сигналі такими значеннями характеристичних параметрів: $f_0 = 155{,}2$ Гц, $U_1 = 0{,}832$, $U_2 = 0{,}791$, $U_1 = 1.456$, $U_4 = 0{,}274$, $U_5 = 0{,}276$, $U_6 = 0{,}185$. Абсолютна, нормована абсолютна і відносна похибки опису склали величини $\varepsilon_b = 0{,}971$, $\varepsilon_b^{norm} = 0{,}486$ і $\delta\varepsilon_b = 5{,}558\%$, відповідно. Обчислення спектральних компонент моделі (2.24) здійснювалося на основі наведених у підрозділі 2.4 аналітичних виразів, зокрема, для еталонного мовленнєвого сигналу $(f_d = 6000$ Гц, $\tau_i = 0{,}3)$ допустиме значення частоти зрізання фільтра низьких частот перебуває у діапазоні $f_z = 15 \div 30$ Гц (далі у розрахунках $f_z = 20$ Гц). На рис. 3.11 наведено результати виділення модулювального коливання із обвідної еталонного мовленнєвого сигналу із застосуванням різних фільтрів низьких частот: фільтра низьких частот Батерворта 3-го порядку $(LPF1)$, фільтра низьких частот

Батерворта 2-го порядку $(LPF2)$, потрійної фільтрації фільтром низьких частот 1-го порядку $(LPF3)$.

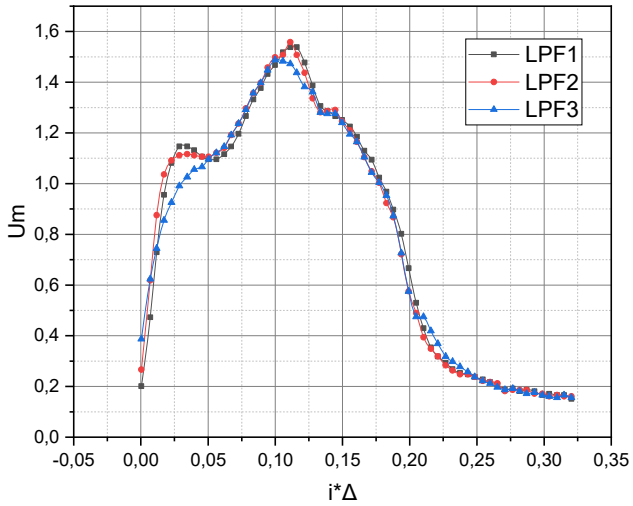


Рисунок 3.11– Виділення модулювального коливання з обвідної еталонного мовленнєвого сигналу з застосуванням різних фільтрів.

Найякісніший результат отримано при вживанні фільтра $LPF1$, що збігається з аналітичними викладками. Фільтри $LPF3$ недостатньо ослаблюють високочастотні складові несного коливання в мовленнєвому сигналі в смузі затримування, що спричиняє накладання періодичних осциляцій із частотами ω_l на модулювальне коливання. Фільтри $LPF2$ надто сильно ослаблюють інформативні для виділення модулювального коливання гармоніки Ω_k в смузі пропускання.

Оцінимо емпірично адекватність стохастичних інтерпретацій моделей ІГМС для АСГ. Втім, оцінимо спочатку ефективність опису індивідуальності голосу в мовленнєвому сигналі стохастичними моделями, які формалізовано виразами (2.36)–(2.37), (2.38)–(2.40) і (2.43)–(2.45). Розрахуємо значення нормованої спектральної щільність потужності $S(f)$ і кореляційного коефіцієнта $r(\tau)$ еталонного мовленнєвого сигналу при таких вихідних параметрах: $f_d = 6000$ Гц, $f_0 = 400$ Гц, $\Delta = f_0^{-1} = 1{,}67 \cdot 10^{-4}$ с, $\tau = \tau_j \equiv j\Delta$, $J = 100$, $\alpha = 1000$ с$^{-1}$, $\alpha_1 = 2\pi f_0 = 2513$ с$^{-1}$. Результати розрахунків представлено залежностями 5 на рис. 3.12 і 3.13, відповідно.

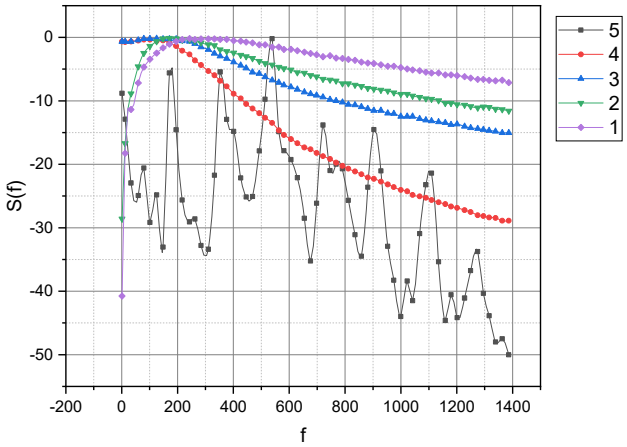


Рисунок 3.12 – Нормована спектральна щільність потужності еталонного мовленнєвого сигналу і відповідних стохастичних моделей.

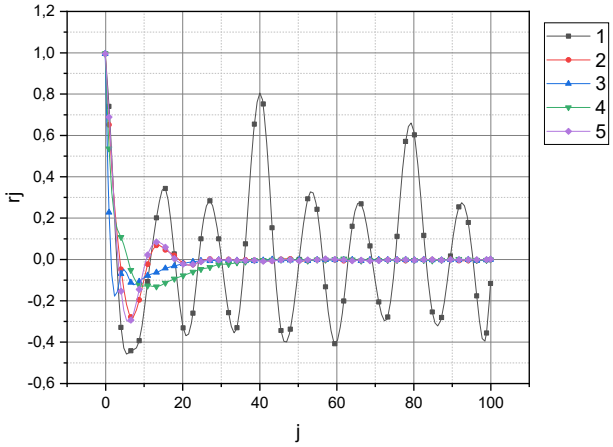


Рисунок 3.13 – Коефіцієнт кореляції еталонного мовленнєвого сигналу і відповідних стохастичних моделей.

Результати моделювання функції $S(f)$ наведено на рис. 3.12, де значення залежності 1 розраховано за виразом (2.39), значення залежності 2 – за виразом (2.41), значення залежності 3 – за виразом (2.36), значення залежності 4 – за виразом (2.44). Результати моделювання функції $r(\tau)$ наведено на рис. 3.13, де значення залежності 1 розраховано за виразом (2.40), значення залежності 2 – за виразом (2.42), значення залежності 3 – за виразом (2.37), значення залежності 4 – за виразом (2.45).

Порівнюючи наведені на рис. 3.12, 3.13 емпіричні результати очевидно, що стохастична модель (2.43)–(2.45) описує ІГМС достовірніше за моделі (2.36)–(2.37) і (2.38)–(2.40). Втім, очевидним є і те, що достовірність опису ІГМС мовленнєвих сигналів згаданими апроксимувальними залежностями є недостатньою. Потенційно підвищити достовірність згаданих вище стохастичних моделей можна вживши математичний апарат лінійного передбачення, згаданий у підрозділі 2.1, адже, згідно з [260], модель авторегресії порядку p є дискретним аналогом стохастичного диференціального рівняння порядку p, що описує спектральні і кореляційні характеристики мовленнєвого сигналу в неперервному часі.

Відповідно, дискретними аналогами стохастичних виразів (2.38) і (2.43) є процеси авторегресії другого порядку. Нормований спектр процесу авторегресії визначається виразом (Б.16), а кореляційний коефіцієнт – виразом (Б.9). У загальному випадку кореляційний коефіцієнт стаціонарного процесу авторегресії можна представити сукупністю згасних експонент і синусоїд [260]. На основі емпіричних досліджень з'ясувалося, що для достатньо достовірного опису усередненого спектра і функції кореляції мовленнєвого сигналу останній слід описувати авторегресійною моделлю порядку $p \geq 30$, оскільки для опису кожного екстремуму в спектрі мовленнєвого сигналу необхідно використовувати два полюси частотної характеристики моделі, тобто два коефіцієнти моделі авторегресії. Отже, для опису 10 максимумів у спектрі мовленнєвого сигналу необхідно 20 коефіцієнтів, при чому спектр такої авторегресійної моделі матиме пологі межі в околі максимумів, що не властиве реальному спектру мовленнєвого сигналу. Отже, для збільшення крутизни спектральної характеристики в околі її максимумів порядок авторегресійної моделі слід збільшувати на $10-20$ коефіцієнтів. Відмітимо, що використання авторегресійних моделей таких високих порядків хоч і дозволяє підвищити достовірність опису кореляційних і спектральних характеристик мовленнєвих сигналів, але супроводжується зростанням обчислювальної складності задачі розрахунку значень коефіцієнтів моделі і призводить, відповідно, до накопичення методичної похибки. На рис. 3.14 наведено результати опису нормованої спектральної щільності потужності еталонного мовленнєвого сигналу (залежність 1) моделями авторегресії 20-, 30-, 40-го порядків (залежності 2, 3, 4, відповідно).

Для еталонного мовленнєвого сигналу частинна кореляційна функція (Б.11), (Б.12) заходила у довірчі межі Бартлета [260, 277] $\pm 3\sigma_r$ при порядку моделі $p \geq 40$.

Зрештою, перш ніж перейти до експериментів із отримання значень характеристичних параметрів, які описують індивідуальність голосу в еталонному мовленнєвому сигналі в парадигмі базової і уточненої стохастичних моделей (2.46) і (2.64), відповідно, слід визначити кількість кореляційних коефіцієнтів J, достат-

ню для забезпечення адекватності такого опису. Результати такого дослідження візуалізовано на рис. 3.15.

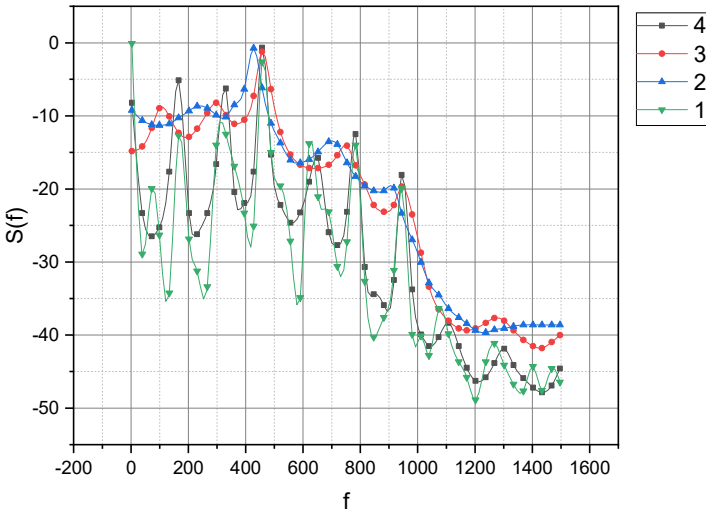


Рисунок 3.14 – Нормована спектральна щільність потужності еталонного мовленнєвого сигналу і відповідних авторегресійних моделей.

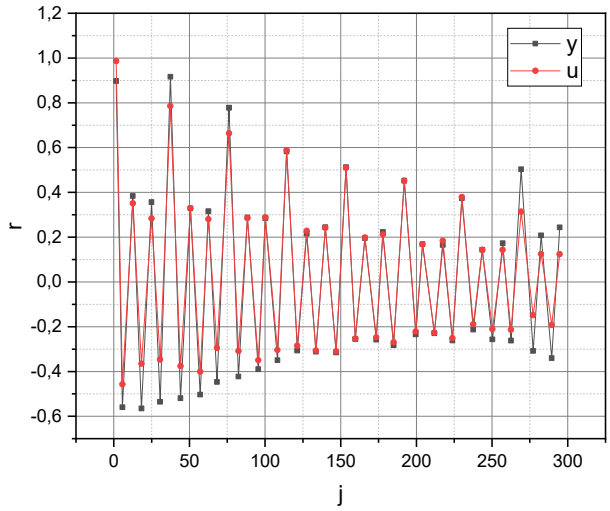


Рисунок 3.15 – Коефіцієнт кореляції еталонного мовленнєвого сигналу і його опис базовою стохастичною моделлю.

На рис. 3.15 кривою $r_y(j)$ описано динаміку зміни значень кореляційного коефіцієнта r_y, який описує еталонний мовленнєвий сигнал. Можна візуально переконатися, що відліки квазіперіодичної згасної функції $r_y(j)$ і відліки функції $r_u(j)$, розраховані на основі стохастичної моделі (2.46), заходять у межі довірчого інтервалу Бартлета $\pm 3\sigma_r$ при $J \geq 200$, де середньоквадратичне відхилення значень кореляційного коефіцієнта r_u розраховується за виразом [260]

$$\sigma_r = \sqrt{N^{-1}\left(1 + \sum_{j=1}^{H}\left(r_j^u\right)^2\right)}, \tag{3.50}$$

де N – кількість відліків аналізованого вхідного сигналу; $H \leq 0{,}25N$ – кількість аналізованих значень кореляційного коефіцієнта. Також відзначимо – якщо функція $r_u(j)$ є згасною і заходить у межі Бартлета, то аналізований мовленнєвий сигнал можна розглядати як стаціонарний випадковий процес. Якщо частота дис-

кретизації аналізованого мовленнєвого сигналу $f_d \neq 6000$ Гц, то величину параметра J можна оцінити за виразом (Е.18).

Отже, для еталонного мовленнєвого сигналу при вихідних значеннях $f_d = 6000$ Гц, $\tau_i = 300$ мс, $\sigma_u^2 = \tau_i^{-1} = 3{,}333$ с$^{-1}$, $L = 6$, $M = 1$, $F_0 = 10$ Гц, $J = 200$ розраховано, відповідно, сім характеристичних параметрів базової стохастичної моделі (2.46): $f_0 = 155{,}2$ Гц, $U_1 = 0{,}821$, $U_2 = 0{,}793$, $U_3 = 1{,}457$, $U_4 = 0{,}328$, $U_5 = 0{,}342$, $U_6 = 0{,}158$, при абсолютній похибці моделі $\varepsilon_r = 1{,}154$, нормованій за кількістю відліків кореляційної функції J абсолютній похибці $\varepsilon_r^{norm} = 0{,}577$ і відносній похибці $\delta\varepsilon_r = 6{,}605\%$.

Враховуючи, що якісні показники опису еталонного мовленнєвого сигналу моделлю (2.46) виявилися нижчими від аналогічних показників квазідетермінованих моделей (2.1) і (2.24), проведемо дослідження з ідентифікації залежності, формалізованої виразом (3.47), похибки ε_r опису індивідуальності голосу в еталонному мовленнєвому сигналі моделлю (2.46) від кількості характеристичних параметрів моделі L. Результат дослідження представлено графіком на рис. 3.16. Як видно з результатів, наведених на рис. 3.16, при $L \geq 6$ похибка моделі (2.46) фактично не змінюється. Також ідентифіковано характер впливу значення частоти модулювального коливання F_0 на величину похибки ε_r моделі (2.46) у вигляді графіка, зображеного на рис. 3.17.

Як видно із результатів, наведених на рис. 3.17, при $F_0 = 15$ Гц похибка моделі (2.46) є найменшою. Форма модульованого коливання, описуваного моделлю (2.46), визначається результатом згортки несного і модулювального коливань. При $M = 0$ форма модульованого коливання визначається виключно формою несного коливання.

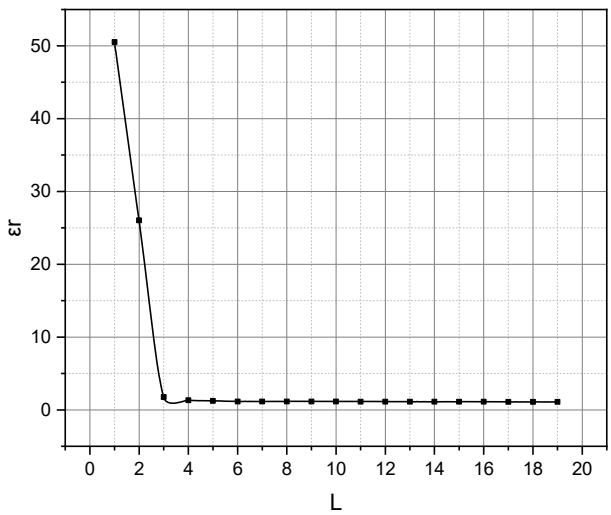


Рисунок 3.16 – Залежність абсолютної похибки базової стохастичної моделі від кількості її характеристичних параметрів.

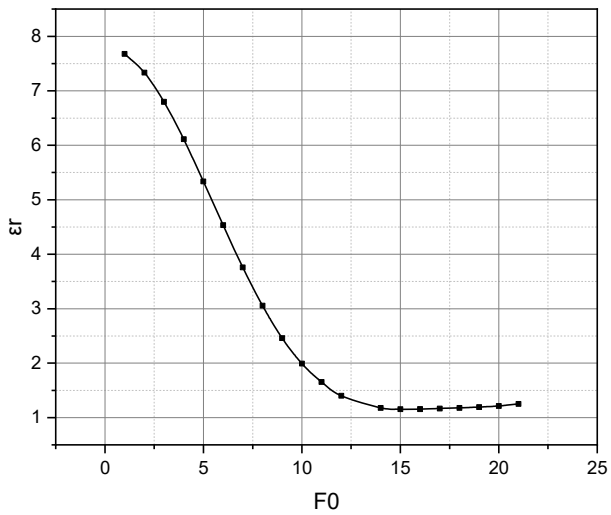


Рисунок 3.17 – Оцінювання впливу модулювальногоколивання на похибку опису еталонного мовленнєвого сигналу моделлю (2.46).

Проведемо дослідження, аналогічне проведеному для моделі (2.1), результати якого було представлено на рис. 3.7. На рис. 3.18 наведено нормовані автокореляційні функції центрованого еталонного сигналу r_j^y і r_j^u – його опису моделлю (2.46) при $M = 0$.

Навіть візуально можна помітити зростання похибки моделі, порівняно із результатами, візуалізованими на рис. 3.15. Аналітичні значення абсолютної, нормованої і відносної похибок моделі (2.46) без урахування модулювальної компоненти $(M = 0)$ склали $\varepsilon_r = 7{,}844$, $\varepsilon_r^{norm} = 3{,}923$ і $\delta\varepsilon_r = 44{,}89\%$ відповідно, що в понад 7 разів перевищує значення відповідних якісних характеристик, які показала модель (2.46) при $M > 0$.

Дослідимо адекватність опису ІГМС моделлю (2.46) в частотному вимірі, для чого проведемо експеримент, методично аналогічний здійсненим для квазідетермінованих моделей. На рис. 3.19 наведено залежність нормованої спектральної щільності потужності еталонного мовленнєвого сигналу $W_N(f)$, розрахованої за виразом (3.47), від частоти, значення якої змінювалося у діапазоні $f \in [0, 0{,}5 f_d]$.

При обчисленнях у виразі (3.47) використовуватимемо кореляційне вікно Тьюкі [253]:

$$W_k = \begin{cases} 0{,}5 + \left(1 + \cos\left(\pi k M^{-1}\right)\right), \; if \; |k| \le M, \\ 0, \; if \; |k| > M, \end{cases} \tag{3.51}$$

де M – точка відсікання, значення якої пов'язане із шириною спектрального вікна b залежністю $b = b_N f_d M^{-1}$, де $b_N = 1{,}333$ – нормована ширина частотної смуги. Для наведених на рис. 3.19 результатів $M = 1600$, а $b = 5$ Гц, відповідно.

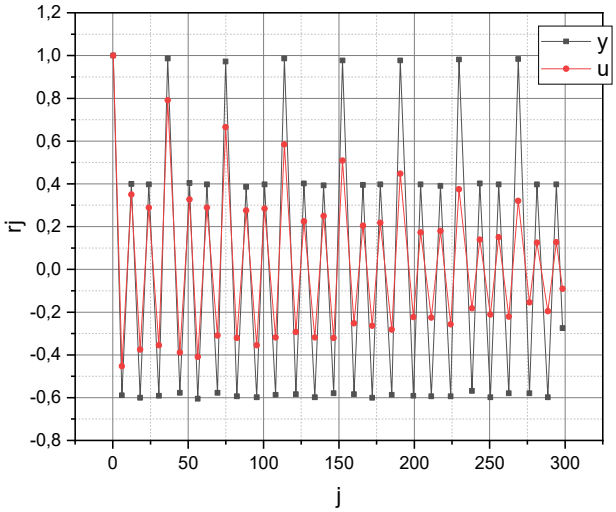


Рисунок 3.18 – Коефіцієнти кореляції центрованого еталонного сигналу і його опису базовою стохастичною моделлю без урахування модулювальної компоненти.

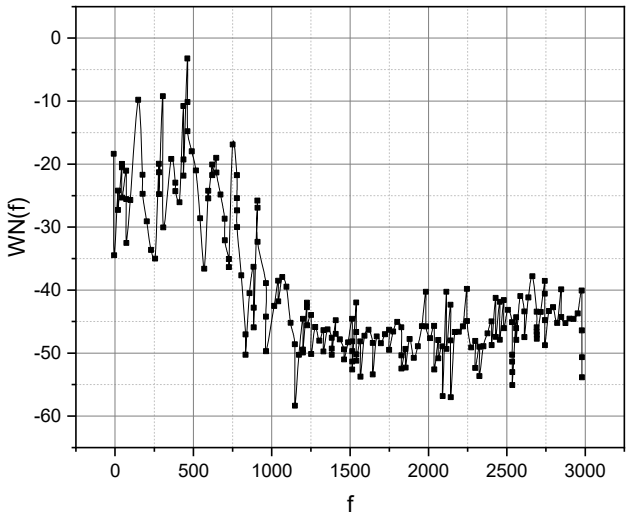


Рисунок 3.19 – Залежність нормованої спектральної щільності потужності еталонного мовленнєвого сигналу від частоти.

Максимуми функції $W_N(f)$, зображеної на рис. 3.19, детектують гармонічні складові в еталонному мовленнєвому сигналі, тобто гармоніки, кратні частоті основного тону.

На рис. 3.20 візуалізовано залежності функцій $W_N(f)$ і $W_N^u(f)$ від частоти f. Значення функції $W_N(f)$, яка характеризує еталонний мовленнєвий сигнал, обчислювалися за виразом (3.47) із урахуванням (3.51). Значення функції $W_N^u(f)$,

яка характеризує нормовану спектральну щільність потужності опису еталонного мовленнєвого сигналу моделлю (2.46), обчислювалися за виразом

$$W_N^u(f) = W_u(f)(\max(W_u(f)))^{-1}, \tag{3.52}$$

де спектральна щільність потужності сигналу $W_u(f)$, згідно з теоремою Вінера–Хінчина [237], обчислювалася за виразом

$$W_u(f) = \int_{-\infty}^{\infty} R_u(\tau)\exp(-j2\pi f\tau)d\tau = 2\int_{0}^{\infty} R_u(\tau)\cos(2\pi f\tau)d\tau . \tag{3.53}$$

Урахувавши функцію кореляції (2.50), вираз (3.53) можна привести до вигляду

$$\begin{aligned} W_u(f) = 0{,}5\tau_i \sum_{l=1}^{L} U_l^2 (&\mathrm{sinc}(2\pi(f + lf_0)\tau_i) + \mathrm{sinc}(2\pi(f - lf_0)\tau_i) + \\ -0{,}25M^2(&\mathrm{sinc}(2\pi(f + lf_0 + F_0)\tau_i) + \mathrm{sinc}(2\pi(f - lf_0 - F_0)\tau_i) + \\ &+ \mathrm{sinc}(2\pi(f + lf_0 - F_0)\tau_i) + \mathrm{sinc}(2\pi(f - lf_0 + F_0)\tau_i))). \end{aligned} \tag{3.54}$$

Аналіз наведених на рис. 3.20 графіків дозволяє стверджувати збіжність максимумів функцій $W_N(f)$ і $W_N^u(f)$, тобто модель (2.46) адекватно описує частоту основного тону і її гармоніки в частотному вимірі.

Дослідимо адекватність уточненої стохастичної моделі (2.64), здійснивши експерименти методично тотожні здійсненим при аналізі адекватності моделі (2.46). Визначимо кількість кореляційних коефіцієнтів J, достатню для забезпечення адекватності опису u еталонного мовленнєвого сигналу y моделлю (2.64). Результати дослідження візуалізовано на рис. 3.21.

На рис. 3.21 залежністю $r_y(j)$ описано динаміку зміни значень кореляційного коефіцієнта r_y, який характеризує еталонний мовленнєвий сигнал. Можна візуально переконатися, що відліки r_j^y квазіперіодичної згасної функції $r_y(j)$ і відліки r_j^u функції $r_u(j)$, розраховані згідно моделі (2.64), заходять у межі довірчого інтервалу Бартлета $\pm 3\sigma_r$ при $J \geq 600$, де середньоквадратичне відхилення значень кореляційних коефіцієнтів розраховується за виразом (3.50) при $N = 1800$ і $H = 0{,}25N$.

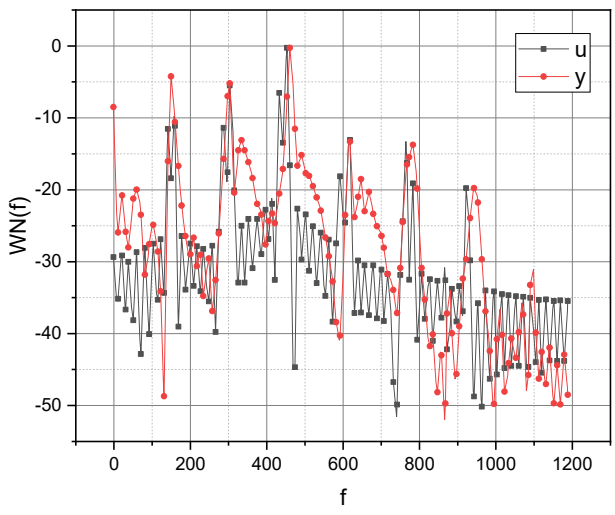


Рисунок 3.20 – Залежності нормованої спектральної щільності потужності від частоти для еталонного мовленнєвого сигналу і його опису моделлю (2.46).

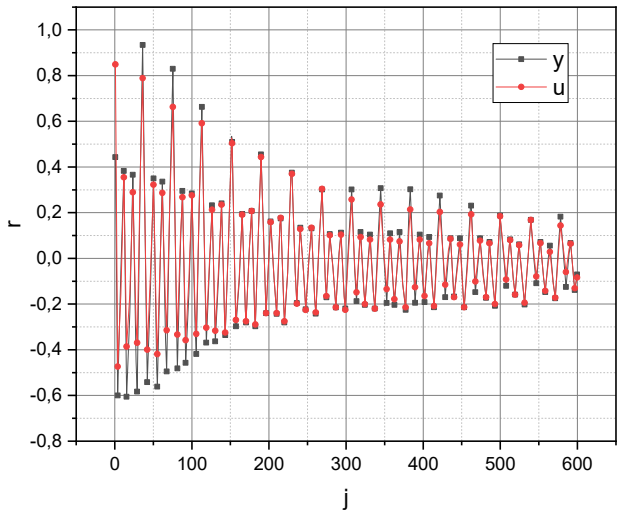


Рисунок 3.21 – Коефіцієнти кореляції еталонного мовленнєвого сигналу і його опису уточненою стохастичною моделлю.

Для еталонного мовленнєвого сигналу і значень вихідних коефіцієнтів $f_d = 6000$ Гц, $\tau_i = 300$ мс, $\sigma_u^2 = \tau_i^{-1} = 3{,}333$ с$^{-1}$, $L = 6$, $F_0 = 10$ Гц, $J = 600$, $M_0 = 1$, $M_1 = 0{,}7$, $M_2 = 0{,}7$, $M_3 = 0{,}5$, $M_4 = 0{,}4$, $M_5 = 0{,}5$ розраховано, відповідно, сім характеристичних параметрів уточненої стохастичної моделі (2.64): $f_0 = 155{,}2$ Гц, $U_1 = 0{,}830$, $U_2 = 0{,}786$, $U_3 = 1{,}456$, $U_4 = 0{,}272$, $U_5 = 0{,}282$, $U_6 = 0{,}173$. Абсолютна похибка моделі $\varepsilon_r = 1{,}422$, нормована за кількістю відліків кореляційної функції J абсолютної похибки моделі $\varepsilon_r^{norm} = 0{,}711$, відносна похибка моделі $\delta\varepsilon_r = 8{,}140\%$.

Зауважимо, що значення функції $W_N^u(f)$ для моделі (2.64) обчислюються за виразом (3.52), а спектральна щільність потужності сигналу $W_u(f)$, згідно з теоремою Вінера–Хінчина, розраховується за модифікованим виразом (3.54)

$$W_u(f) = 0{,}125\tau_i \sum_{k=0}^{K} M_k^2 \sum_{l=1}^{L} U_l^2 \left(\mathrm{sinc}\left(2\pi\left(f + lf_0 + kF_0\right)\tau_i\right) + \right.$$
$$\left. + \mathrm{sinc}\left(2\pi\left(f - lf_0 - kF_0\right)\tau_i\right) + \mathrm{sinc}\left(2\pi\left(f + lf_0 - kF_0\right)\tau_i\right) + \right. \qquad (3.55)$$

$$+\operatorname{sinc}\left(2\pi\left(f-lf_0+kF_0\right)\tau_i\right)\Big).$$

Узагальнимо емпіричні дослідження адекватності запропонованих стохастичних моделей мовленнєвого сигналу для АСГ конкретизувавши процедуру розрахунку статистичних характеристик еталонного мовленнєвого сигналу. Спочатку до оцифрованих із частотою дискретизації $f_d = 6000$ Гц відліків еталонного мовленнєвого сигналу x_i, $i=\overline{1,N}$, застосуємо нелінійну операцію $y_i = \ln\left(x_i\right)$. Сигнал y_i аналізується щодо можливої нестаціонарності за обчисленими значеннями кореляційного коефіцієнта $r_j = R_j R_0^{-1}$, де функція кореляції $R_j = \left(N-1\right)^{-1}\sum\limits_{i=1}^{N-j}\left(y_i-\bar{y}\right)\left(y_{i+j}-\bar{y}\right)$, а $\bar{y} = N^{-1}\sum\limits_{i=1}^{N} y_i$, $j=\overline{0,L}$, а L – кількість відліків функції кореляції. Динамку значень кореляційного коефіцієнта $r_j\left(j\right)$ описано відповідним графіком, наведеним на рис. 3.22.

Функція $r_j\left(j\right)$ має згасний характер і приблизно з 200-го відліку заходить у межі довірчого інтервалу нульових значень, отриманих за методом Бартлета, $\pm\sigma_r = \sqrt{N^{-1}\left(1+2\sum\limits_{j=1}^{L} r_j^2\right)} = \pm 0{,}213$. Також помітно, що зображена на рис. 3.22 функція $r_j\left(j\right)$ нестаціонарна, тобто містить квазіперіодичну компоненту, позбавитися якої можна відфільтрувавши вихідний сигнал з метою вирівнювання його спектра.

Для фільтрації застосуємо фільтр Чебишева другого роду восьмого порядку, утворений каскадним з’єднанням чотирьох фільтрів Чебишева другого роду другого порядку. Фільтрацію здійснюватимемо на частоті основного тону f_0 і частоті першої її гармоніки $f_1 = 2f_0$. Саму частоту основного тону оцінюватимемо кореляційним методом за визначенням періоду пульсації значень квазіперіодичного кореляційного коефіцієнта: $f_0 = f_d N_p^{-1}$, де N_p – кількість відліків функції $r_j\left(j\right)$, через які пульсація повторюється. Для заглушення на частотах f_0 і f_1 вживатимемо смуги режекції $\Pi_0 = 36$ Гц і $\Pi_1 = 20$ Гц відповідно. Підтвердження коректт-

ності оцінки основного тону отримаємо проаналізувавши нормовану функцію спектральної щільності потужності сигналу y_i, обчислену за виразом

$$S(f) = 2 f_d^{-1}\left(1 + 2\sum_{k=1}^{M-1} r_k W_k \cos\left(2\pi f f_d^{-1} k\right)\right),$$

де M – точка відсікання кореляційного вікна Тьюкі W_k, описаного виразом (3.51). На зображеному на рис. 3.23 графіку, функції $S(f)$ гармоніки основного тону відфільтрованого сигналу y_i^f можна ідентифікувати за положенням максимумів.

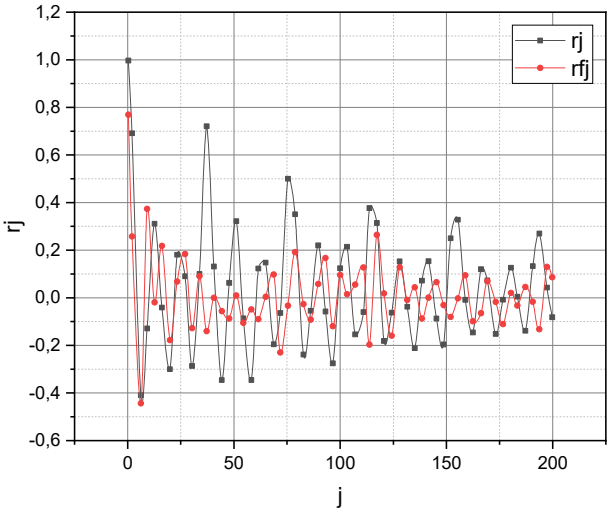


Рисунок 3.22 – Значення коефіцієнта кореляції еталонного мовленнєвого сигналу до і після його фільтрації.

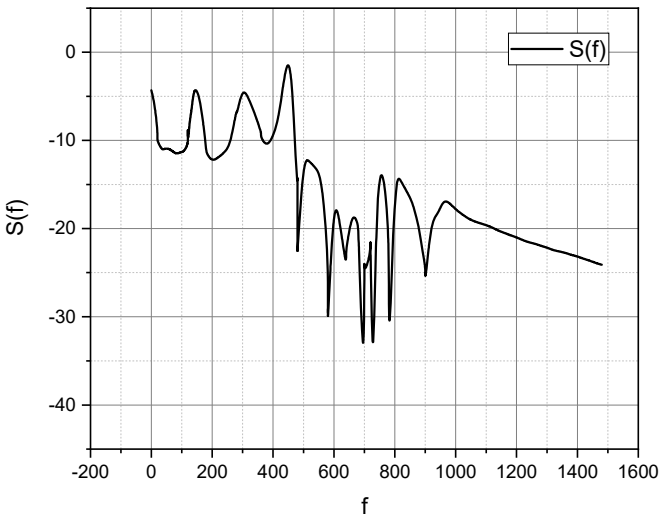


Рисунок 3.23 – Нормована спектральна щільність потужності (в дБ) відфільтрованого сигналу y_i^f.

Застосувавши алгоритм обчислення значень функції $r_j(j)$ до відліків відфільтрованого сигналу y_i^f обчислимо значення функції $r_j^f(j)$, графік якої візуалізовано на рис. 3.22. Сигнал, описаний функцією $r_j^f(j)$, має згасний характер, заходить у межі довірчого інтервалу нульових значень, отриманих за методом Бартлета, і є стаціонарним і ергодичним.

Стаціонарний сигнал y_i^f опишемо моделлю авторегресії, порядок якої визначимо розрахувавши частинну кореляційну функцію [256]:

$$\psi_{11} = r_1^f \,,\; \psi_{ll} = \left(r_1^f - \sum_{j=1}^{l-1} \psi_{l-1,j} r_{l-j}^f \right) \left(1 - \sum_{j=1}^{l-1} \psi_{l-1,j} r_j^f \right),$$

$$\psi_{lj} = \psi_{l-1,j} - \psi_{ll} \psi_{l-1,l-j} \,,\; l = \overline{2,L} \,,\; j = \overline{1,l-1} \,,$$

де r^f – кореляційний коефіцієнт відфільтрованого сигналу y^f. Графік функції $\psi(l)$ для сигналу y^f наведено на рис. 3.24. Границі Бартлета для нього: $\pm 3\sigma_1 = \pm N^{-0,5} = \pm 0,072$. Шуканому значенню порядку моделі авторегресії p відповідає номер відліку функції $\psi(l)$, починаючи з якого значення частинного кореляційного коефіцієнта залишається у межах $\pm 3\sigma_1$.

Саму модель авторегресії опишемо в матричній формі виразом

$$A\phi = x \,, \tag{3.56}$$

де матриця A містить елементи $A_{ij} = R^{f_{|i-j|}}$; вектор-стовпець оцінок параметрів моделі авторегресії ϕ – керовані змінні моделі ϕ_i; вектор x – елементи $x_i = R^{f_i}$; $i, j = \overline{1,p}$. Ідентифікацію моделі (3.56) здійснимо за величиною остаточних похибок між еталонним сигналом і моделлю

$$\alpha_l = \left(y_l^f - \bar{y}^f \right) - \sum_{i=1}^{p} \phi_i \left(y_{l-i}^f - \bar{y}^f \right),$$

де $\bar{y}^f = N^{-1} \sum_{i=1}^{N} y_i^f$; $l = \overline{1,N}$; N – кількість відліків сигналу y^f.

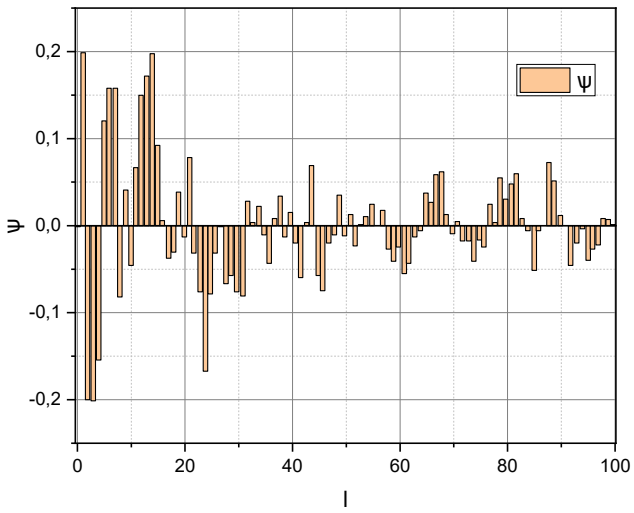


Рисунок 3.24 – Частинна кореляційна функція сигналу y^f.

Адекватність моделі встановимо скориставшись критерієм Пірсона χ^2 [260], для чого обчислимо статистику остаточних похибок кореляційного коефіцієнта $r_\alpha(j)$ за виразом (2.113):

$$\chi^2 = N \sum_{j=1}^{S} r_\alpha^2(j),$$

значення якої порівняємо із табличним значенням критерію, врахувавши кількість ступенів свободи $\nu = S - p$ та рівень значимості $\alpha = 10^{-3}$. За результатами оцінювання виявилося, що модель авторегресії виду (3.56) адекватно описує еталонний мовленнєвий сигнал при порядку моделі $p \geq 14$, а найкраще – при значенні $p = 31$.

Нарешті, оцінимо вплив таких ключових параметрів еталонного мовленнєвого сигналу як частота дискретизації $f_d = \{6000, 8000, 11025\}$ Гц і розрядність квантування $n = \{8, 16\}$ біт на чутливість якісних характеристик його описів квазідетермінованими і стохастичними моделями. При цьому необхідну для адекватного опису кількість коефіцієнтів кореляції J визначатимемо за виразом (Е.18). Кількість характеристичних параметрів моделей $L = 10$.

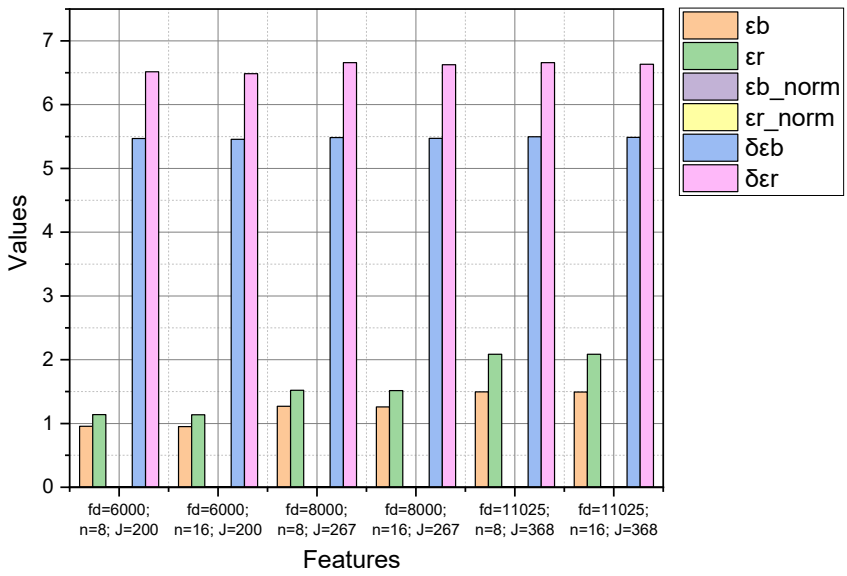


Рисунок 3.25 – Вплив параметрів еталонного мовленнєвого сигналу на похибки його описів квазідетермінованими і стохастичними моделями.

Результати, наведені на рис. 3.25, фіксують зростання достовірності опису вхідного мовленнєвого сигналу із зростанням розрядності квантування n, що можна пояснити зменшенням дисперсії похибки квантування сигналу. Зростання частоти дискретизації f_d еталонного мовленнєвого сигналу супроводжується зростанням абсолютних і відносних похибок моделей і незначним спаданням нормованих за значенням параметра J абсолютних похибок моделей. Це можна пояснити тим, що всі L значень характеристичних параметрів, обчислюваних моделями при формуванні описів еталонного мовленнєвого сигналу, входять у частотний діапазон із верхньою межею $0{,}5 f_d$, тобто при формуванні описів враховується вся істотна частина спектра. Втім, збільшуючи кількість обчислюваних характеристичних параметрів моделей L доцільно збільшувати і частоту дискретизації вхідного сигналу f_d, щоб уникнути втрат інформації.

Отже, узагальнимо результати, представлені у підрозділі, діаграмою, наведеною на рис. 3.26.

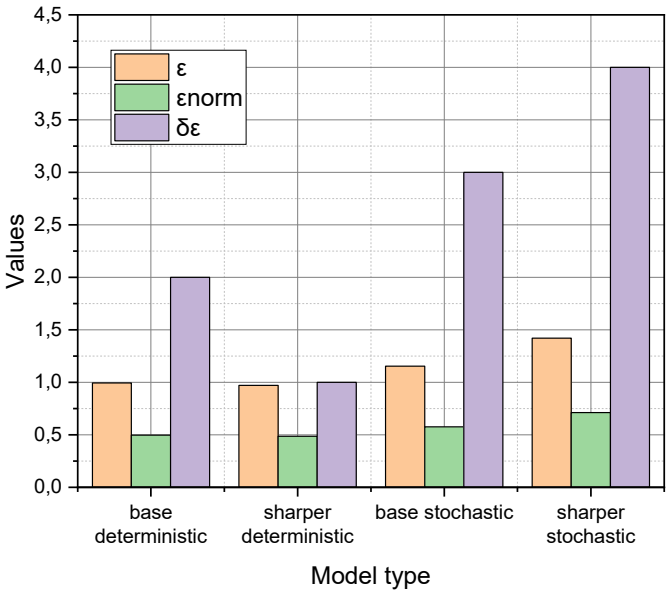


Рисунок 3.26 – Якісні характеристики описів еталонного мовленнєвого сигналу синтезованими моделями.

На діаграмі візуалізовано значення абсолютної, нормованої абсолютної і відносної похибок описів індивідуальності голосу в еталонному мовленнєвому

сигналі базовою і уточненою квазідетермінованими та базовою і уточненою стохастичними моделями, (2.1), (2.24), (2.46) і (2.64), відповідно. Усі моделі показали адекватний опис індивідуальності голосу в еталонному мовленнєвому сигналі, але квазідетерміновані моделі виявилися достовірнішими, зокрема, уточнена квазідетермінована модель (2.24) показала найвищу достовірність з-поміж досліджених.

Такий результат можна пояснити, зокрема, малою тривалістю еталонного мовленнєвого сигналу – $\tau_i = 300$ мс. Мала тривалість парольного сигналу робить процедуру АСГ комфортнішою, проте не дозволяє набрати достатньо інформації для розкриття потенціалу стохастичних моделей ІГМС. Втім, при критичному застосуванні синтезованих теоретичних результатів прогнозованість результату автентифікації превалюватиме над комфортністю цієї процедури, що дає можливість орієнтувати параметри процедури автентифікації на розкриття потенціалу стохастичних моделей (2.46) і (2.64).

Висновки до третього розділу

1. Дослідження залежності достовірності автентифікації суб’єктів за голосами, параметризованими запропонованими полігармонічними математичними моделями, від частоти дискретизації і глибини квантування відповідних фонограм показало, що зростання частоти дискретизації понад 8000 Гц, а розрядності понад 16 біт не покращує результат автентифікації.

2. Формалізовано методику аналітичного розрахунку вагових коефіцієнтів міри роздільності для еталонного і оцінюваного образів мовленнєвих сигналів у параметричному просторі полігармонічних моделей як задачі оптимізації зваженої суми квадратів відхилень у постановках, орієнтованих на: мінімізацію похибки першого роду, мінімізації похибки другого роду, максимізації достовірності автентифікації тощо.

3. Формалізовано процес обчислення початкового порогового значення міри роздільності для критерію прийняття рішень щодо результату автентифікації суб’єкта за мовленнєвим сигналом із урахуванням довірчих інтервалів варіації йо-

го відображення у параметричному просторі амплітудно модульованих полігармонічних математичних моделей.

4. Матеріали інформаційних джерел, тематично пов’язаних із даним підрозділом, узагальнено в наведеній у додатку Е універсальній методиці перевірки адекватності математичної моделі мовленнєвого сигналу за критерієм відповідності на основі коефіцієнта множинної кореляції, у якому порівнюється коефіцієнти кореляції емпіричного мовленнєвого сигналу і його амплітудно модульованої математичної моделі, зокрема, квазідетермінованої.

5. Акцентуємо увагу, що у підрозділі формалізовано метод обчислення міри відстані між зваженими характеристичними параметрами еталонного і емпіричного мовленнєвих коливань, параметризованих, на відміну від існуючих, у формалізмі методології моделей індивідуальності голосу, де при оцінюванні довірчих інтервалів варіювання значень характеристичних параметрів мовленнєвих сигналів враховується рівень відношення «сигнал»/«шум», що дозволяє визначити поріг прийняття рішень в задачі верифікації суб’єкта за голосом.

Основні результати розділу опубліковано в [36, 39, 40, 41, 45, 46, 49, 50, 51, 52, 60].

РОЗДІЛ 4
ДОСЛІДЖЕННЯ ПРОЦЕСУ АВТЕНТИФІКАЦІЇ СУБ'ЄКТА ЗА МОВЛЕННЄВИМ СИГНАЛОМ ІЗ ШУМОМ

4.1 Компенсація шумів у фонограмі мовленнєвого сигналу в контексті задачі автентифікації суб'єкта за голосом

Якість вибраної множини характеристичних параметрів для опису мовленнєвого сигналу для АСГ можна оцінити за значенням інтегрального критерію, складеного із достовірності, завадостійкості і обчислювальної складності отриманої моделі. Причому одночасно досягти екстремальних значень бодай двох згаданих складових складно, бо висока дискримінаційність характеристичного параметра зазвичай супроводжується його низькою завадостійкістю або значною обчислювальною складністю розрахунку. Традиційно позбавитися шумів акустичного оточення, присутніх у фонограмі мовленнєвого сигналу можна застосувавши фільтрацію [212, 213, 247, 248], тип якої залежить від рівня відношення «сигнал»/«шум» і типу самих шумів тощо. Втім, фільтрація привносить у мовленнєвий сигнал нелінійні спотворення і дозволяє ефективно позбавитися лише стохастичних, явно помітних на тлі корисного сигналу, шумів. Також неоднозначність застосування фільтрації у контексті задачі АСГ полягає у тому, що досить часто сигнал шуму накладається на мовленнєвий сигнал у частотному діапазоні, де очікується присутність характеристичного параметра голосу суб'єкта, отже, доцільно не вилучати, а компенсувати вплив шуму, щоб згодом описати вміст цього частотного діапазону значеннями відповідного спектрального характеристичного параметра.

Експлуатація приймачів сигналу в реальному акустичному оточенні зазвичай супроводжується привнесенням у фонограму мовленнєвого сигналу, зокрема, низькочастотних шумів, що може призвести до неадекватності результату процедури екстрагування такого характеристичного параметра як частота основного тону. Запропонований у підрозділі 2.6 математичний апарат дозволяє визначити рівень відношення «сигнал»/«шум» при якому отримати адекватний опис мовленнєвого сиг-

налу в множині математичних моделей (2.1), (2.24), (2.46) і (2.64) не вдасться. За такої обставини можливі два варіанти продовження перебігу сеансу АСГ – запропонувати суб'єкту повторно записати фонограму із мовленнєвим сигналом, сподіваючись отримати результат із вищим рівнем відношення «сигнал»/«шум», або ж спробувати компенсувати шуми у фонограмі мовленнєвого сигналу, контролюючи достовірність отриманого результату за допомогою відповідного математичного апарату. Отже, синтезуємо математичний апарат для компенсації шумів акустичного оточення приймачів сигналу в фонограмі із застосуванням методів машинного навчання і моделей СГР.

При спектральному представленні мовленнєвого сигналу спотворення значень відповідних характеристичних параметрів під впливом шумів моделюється операціями додавання або множення корисного мовленнєвого сигналу із стохастичним сигналом шуму [248]. Якщо характеристичні параметри узагальнено моделлю СГР [247, 248, 288–293], то 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

$$\hat{x}_t = E\left(x|y_t\right) = \int_X xp\left(x|y_t\right)dx, \tag{4.1}$$

де x і y_t – вектори характеристичних параметрів, які описують фонограми еталонного мовленнєвого сигналу без шуму і емпіричного мовленнєвого сигналу із шумом, відповідно; $\hat{x}_t$ – підсумковий вектор характеристичних параметрів, у значеннях якого вплив шумів, присутніх у значеннях вектора y_t, компенсовано; $p\left(x|y_t\right)$ – умовна функція розподілу імовірних значень вектора x для заданих значень вектора y_t.

Нехай сформовано бази фонограм із мовленнєвим матеріалом, записаним без шуму, і мовленнєвим матеріалом, записаним із шумом, з яких екстраговано вектори спектральних характеристичних параметрів, організовані, відповідно, в еталонну базу векторів без шуму X і еталонну базу векторів із шумом Y. Опишемо вміст еталонних баз $X = \{x_t\}$ і $Y = \{y_t\}$, $t = \overline{1,T}$, відповідними моделями СГР

$$p(x_t) = \sum_{j=1}^{M} w_x(j) N_x(x_t, \mu_x(j), \Sigma_x(j)), \tag{4.2}$$

$$p(y_t) = \sum_{j=1}^{M} w_y(j) N_y(y_t, \mu_y(j), \Sigma_y(j)), \tag{4.3}$$

де $w(j)$, $\mu(j)$, $\Sigma(j)$ – вага, вектор середніх значень і коваріаційна матриця j-ї компоненти відповідної моделі суміші, що узагальнює M компонентів. Умовні функції розподілів імовірності $p(x|j, y_t)$ можна отримати апроксимувавши вміст еталонних баз X або Y значеннями адитивних і мультиплікативних факторів r_j і R_j, відповідно, отриманих в результаті максимізації відповідних функцій правдоподібності значень вектора x для заданих значень вектора y_t. При ідентифікованих умовних функціях $p(x|j, y_t)$ отримати значення вектора $\hat{x}_t$ для емпіричного вектора характеристичних параметрів можна за критерієм (4.1). Узагальнену схему щойно описаного стохастичного методу компенсації шумів у емпіричному мовленнєвому матеріалі наведено на рис. 4.1. Формалізуємо його перебіг в залежності від способу отримання умовних функцій розподілу імовірності $p(x|j, y_t)$.

Представимо модель суміші (4.3), яка описує еталонну базу мовленнєвого матеріалу із шумом $Y = \{y_t\}$, $t = \overline{1,T}$, на основі моделі суміші (4.2) із введеними векторами компенсувальних факторів r_j і R_j, узагальнених множиною $\phi = \{r_j, R_j\}$, $j = \overline{1,M}$:

$$p(y) = \sum_{j=1}^{M} w_y(j) N_y(y, \mu_x(j) + r_j, \Sigma_x(j) + R_j). \tag{4.4}$$

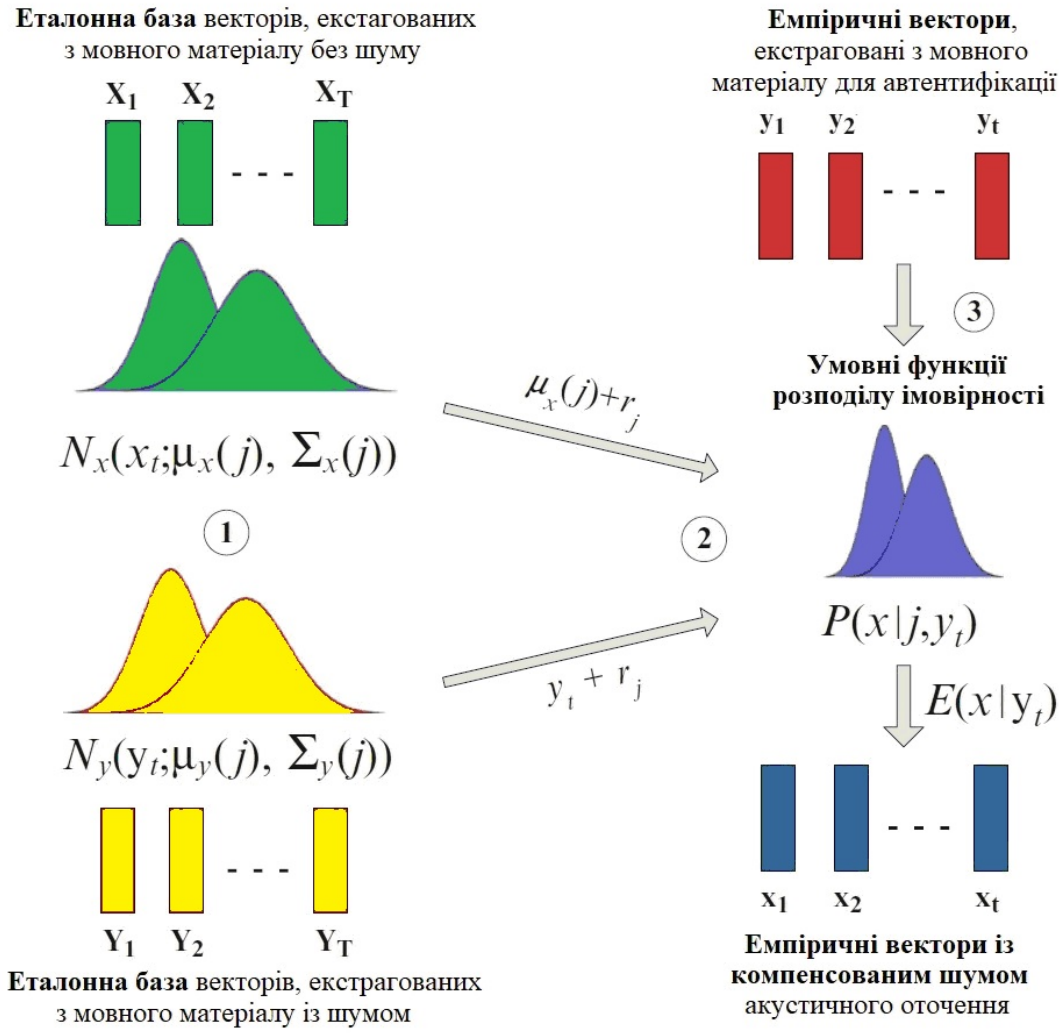


Рисунок 4.1 – Стохастична компенсація шумів у параметризованому емпіричному мовленнєвому сигналі з незалежним моделюванням еталонного мовленнєвого матеріалу

Модель суміші (4.4) використаємо для оцінювання значень множини ϕ скориставшись методом максимізації функції правдоподібності [288, 289, 294–297]. У загальному вигляді цей метод дозволяє ідентифікувати невідомі параметри деякої статистичної моделі в результаті ітераційного розв’язку задачі максимізації

$$\phi = \arg\max_{\phi} Q(\phi,\phi) = \arg\max_{\phi\in X} \sum_{z} p\left(z|X,\phi\right)\log\left(p\left(z,X|\phi\right)\right). \tag{4.5}$$

Використовувану у виразі (4.5) функцію правдоподібності опишемо виразом

$$Q(\phi,\phi') = \sum_{z} p\left(z|X,\phi'\right)\log\left(p\left(z,X|\phi\right)\right), \tag{4.6}$$

де z – множина невідомих параметрів моделі СГР, яка описує визначену параметризовану навчальну базу X; ϕ' – множина аргументів функції, значення яких оцінюється на поточній ітерації; ϕ – множина аргументів функції, значення яких оцінювалося на попередній ітерації. Сформулюємо логарифмічну функцію правдоподібності для моделі суміші, описаної виразом (4.4)

$$L(Y)=\log\prod_{t=1}^{T}p(y_t)=\sum_{t=1}^{T}\log\sum_{j=1}^{M}w_y(j)N_y\left(y_t,\mu_y(j),\Sigma_y(j)\right)=$$
$$=\sum_{t=1}^{T}\log\sum_{j=1}^{M}w_y(j)N_y\left(y_t,\mu_x(j)+r_j,\Sigma_x(j)+R_j\right). \tag{4.7}$$

Підставимо аналітичну форму функції правдоподібності (4.7) у вираз (4.6), позначивши невідомі параметри моделі суміші для емпіричного вектора y_t змінними $s_t(j)$,

$$Q=Q(\phi,\phi')=\sum_{t=1}^{T}\sum_{j=1}^{M}p\left(s_t(j)\middle|y_t,\phi\right)\log\left(p\left(y_t,s_t(j)\middle|\phi'\right)\right)=$$
$$=\sum_{t=1}^{T}\sum_{j=1}^{M}p\left(s_t(j)\middle|y_t,\phi\right)\Big(-0{,}5D\log\left|R_j+\Sigma_x(j)\right|-$$
$$-0{,}5\left(y_t-\mu_x(j)-\hat{r}_j\right)^T\left(\Sigma_x(j)+R_j\right)^{-1}\left(y_t-\mu_x(j)-\hat{r}_j\right)\Big)+K, \tag{4.8}$$

де D – розмірність простору характеристичних параметрів; K – незалежна константа.

Задачу оптимізації (4.5) для функції правдоподібності (4.8), враховуючи структуру множини ϕ, можна розв’язувати відносно вектора адитивних компенсувальних факторів r_j або відносно вектора мультиплікативних компенсувальних факторів R_j у формі $\frac{\partial Q}{\partial \hat{r}_j}=0$ або $\frac{\partial Q}{\partial \hat{R}_j}=0$, відповідно. Зокрема, аналітичний вираз

$$\frac{\partial Q}{\partial \hat{r}_j}=\sum_{t=1}^{T}p\left(s_t(j)\middle|y_t,\phi\right)\left(\Sigma_x(j)+R_j\right)^{-1}\left(y_t-\mu_x(j)-\hat{r}_j\right)=0$$

можна спрости до вигляду

$$\sum_{t=1}^{T} p\left(s_t(j)\middle|y_t,\phi\right)\left(y_t-\mu_x(j)-\hat{r}_j\right)=0,$$

з якого виразити значення адитивних компенсувальних факторів

$$\hat{r}_j=\sum_{t=1}^{T} p\left(s_y(j)\middle|y_t,\phi\right)\left(y_t-\mu_x(j)\right)\left(\sum_{t=1}^{T} p\left(s_y(j)\middle|y_t,\phi\right)\right)^{-1}. \tag{4.9}$$

Аналогічно, з аналітичного виразу $\frac{\partial Q}{\partial \hat{R}_j}=0$, після відповідних перетворень, отримаємо вираз для розрахунку значень загорткових компенсувальних факторів $\hat{R}_j$:

$$\hat{R}_j=\sum_{t=1}^{T} p\left(s_y(j)\middle|y_t,\phi\right)\left(\left(y_t-\mu_x(j)-\hat{r}_j\right)\left(y_t-\mu_x(j)-\hat{r}_j\right)^T-\Sigma_x(j)\right)\times$$
$$\times\left(\sum_{t=1}^{T} p\left(s_y(j)\middle|y_t,\phi\right)\right)^{-1}. \tag{4.10}$$

Присутня у виразах (4.9), (4.10) функція $p\left(s_y(j)\middle|y_t,\phi\right)$ – це апостеріорна імовірність, яка характеризує невідомі компоненти $s_y(j)$ моделі суміші для емпіричного вектора y_t. Якщо взяти до уваги, що відповідно до вихідного положення (4.4) відмінність між моделями сумішей (4.2) і (4.3) визначається значеннями невідомих компонентів $s_y(j)$, які характеризуються ймовірностями $p\left(s_y(j)\middle|y_t,\phi\right)$, то можна записати

$$p\left(s_y(j)\middle|y_t,\phi\right)=p\left(s_y(j)\right)p\left(y_t\middle|s_y(j),\phi\right)\left(\sum_{k=1}^{M} p\left(s_y(k)\right)p\left(y_t\middle|s_y(k),\phi\right)\right)^{-1}=$$
$$=p\left(s_x(j)\right)p\left(x_t\middle|s_x(j)\right)\left(\sum_{k=1}^{M} p\left(s_x(k)\right)p\left(y_t\middle|s_x(k)\right)\right)^{-1}= \tag{4.11}$$
$$=w_x(j)N_x\left(x_t,\mu_x(j),\Sigma_x(j)\right)\left(\sum_{j=1}^{M} w_x(j)N_x\left(x_t,\mu_x(j),\Sigma_x(j)\right)\right).$$

Врахувавши вираз (4.11), вирази (4.9), (4.10) можна спростити до вигляду

$$\hat{r}_j=\sum_{t=1}^{T} p\left(s_x(j)\middle|x_t\right)\left(y_t-x_t\right)\left(\sum_{t=1}^{T} p\left(s_x(j)\middle|x_t\right)\right)^{-1}, \tag{4.12}$$

$$\hat{R}_j = \sum_{t=1}^{T} p\left(s_x(j)\middle|x_t\right)\left(\left(y_t - x_t - \hat{r}_j\right)\left(y_t - x_t - \hat{r}_j\right)^T - \Sigma_x(j)\right)\times$$
$$\times\left(\sum_{t=1}^{T} p\left(s_x(j)\middle|x_t\right)\right)^{-1}, \tag{4.13}$$

відповідно. Підставивши вирази (4.12) і (4.13) у вираз (4.1) отримаємо значення вектора характеристичних параметрів $\hat{x}_t$, у яких присутній у значеннях емпіричного вектора характеристичних параметрів y_t шум компенсовано:

$$\hat{x}_t = E\left(x\middle|y_t\right) = \int_x x p\left(x\middle|y_t\right)dx = \int_x \left(y_t - r(x)\right)p\left(x\middle|y_t\right)dx =$$
$$= \int_x y_t p\left(x\middle|y_t\right)dx - \int_x r(x)p\left(x\middle|y_t\right)dx = y_t \int_x p\left(x\middle|y_t\right)dx -$$
$$- \int_x \sum_{j=1}^{M} r(x)p\left(x, j\middle|y_t\right)dx = y_t - \sum_{j=1}^{M} p\left(j\middle|y_t\right)\int_x r(x)p\left(x\middle|j, y_t\right)dx = \tag{4.14}$$
$$= y_t - \sum_{j=1}^{M} p\left(j\middle|y_t\right)r_j \int_x p\left(x\middle|j, y_t\right)dx = y_t - \sum_{j=1}^{M} p\left(j\middle|y_t\right)r_j .$$

Узагальнена у вигляді виразу (4.14) процедура оцінювання значень $\hat{x}_t\left(p\left(j\middle|y_t\right), r_j\right)$ залишається адекватною поки рівність (4.11) виконується. Втім, із спаданням значення рівня відношення «сигнал»/«шум», варіативність значень умовних функцій $p\left(s_y(j)\middle|y_t, \phi\right)$ зростає настільки, що вважати вагу $w_y(j)$ j-ї компоненти моделі суміші (4.4) детермінованою величиною стає неможливо. Отже, адекватно описати мовленнєвий матеріал із низьким значенням рівня відношення «сигнал»/«шум» може модель СГР виду

$$p(y_t) = \sum_{j=1}^{M} p(j)p\left(y_t\middle|j\right), \tag{4.15}$$

де $p(j)$ – стохастичний еквівалент ваги $w_y(j)$ j-ї компоненти моделі суміші, а $p\left(y_t\middle|j\right)$ – параметрична характеристика моделі суміші (4.3), тобто множина $N_y\left(y_t, \mu_y(j), \Sigma_y(j)\right)$.

Представимо модель суміші (4.3), яка описує еталонну базу мовленнєвого матеріалу із шумом $Y = \{y_t\}$, $t = \overline{1,T}$, на основі моделі суміші (4.2) із урахуванням

виразу (4.15) та введенням узагальненої множини компенсувальних факторів $\phi = \{r_j, \Gamma_j\},\ j = \overline{1, M}$:

$$p(x|y_t) = \sum_{j=1}^{M} w_y(j) p(x|j, y_t). \tag{4.16}$$

де умовна функція розподілу

$$p(x|j, y_t) = N_y(x, y_t + r_j, \Gamma_j). \tag{4.17}$$

Сформулюємо логарифмічну функцію правдоподібності для виразу (4.16):

$$\begin{aligned} L(X) &= \sum_{t=1}^{T} \log(p(x_t)) = \sum_{t=1}^{T} \log \sum_{j=1}^{M} w_x(j) N_x(x_t, \mu_x(j), \Sigma_x(j)) = \\ &= \sum_{t=1}^{T} \log \sum_{j=1}^{M} w_y(j) N_y(x_t, y_t + r_j, \Gamma_j). \end{aligned} \tag{4.18}$$

Підставимо аналітичну форму функції правдоподібності (4.18) у вираз (4.6), позначивши невідомі параметри моделі суміші для вектора даних y_t змінними $s_t(j)$:

$$\begin{aligned} Q = Q(\phi, \phi') &= \sum_{t=1}^{T} \sum_{j=1}^{M} p(s_t(j)|y_t, \phi) \log(p(x_t, s_t(j)|\phi')) = \\ &= \sum_{t=1}^{T} \sum_{j=1}^{M} p(s_t(j)|y_t, \phi)\Big(-0{,}5 D \log|\Gamma_j| - \\ &- 0{,}5(x_t - y_t - \hat{r}_j)^T \Gamma_j^{-1} (x_t - y_t - \hat{r}_j)\Big) + K\ . \end{aligned} \tag{4.19}$$

Задачу оптимізації (4.5) для функції правдоподібності (4.18), враховуючи структуру множини ϕ, можна розв'язувати відносно вектора адитивних компенсувальних факторів r_j або відносно вектора мультиплікативних компенсувальних факторів Γ_j у формі $\frac{\partial Q}{\partial \hat{r}_j} = 0$ або $\frac{\partial Q}{\partial \hat{\Gamma}_j} = 0$, відповідно. Зокрема, аналітичний вираз $\frac{\partial Q}{\partial \hat{r}_j} = \sum_{t=1}^{T} p(s_t(j)|y_t, \phi) \Gamma_j^{-1} (x_t - y_t - \hat{r}_j) = 0$ можна спрости до вигляду $\sum_{t=1}^{T} p(s_t(j)|y_t, \phi)(x_t - y_t - \hat{r}_j) = 0$, з якого можна визначити значення адитивних компенсувальних факторів

$$\hat{r}_j = \sum_{t=1}^{T} p\left(s_t(j)\middle|y_t,\phi\right)(x_t - y_t)\left(\sum_{t=1}^{T} p\left(s_t(j)\middle|y_t,\phi\right)\right)^{-1}. \tag{4.20}$$

Подальше спрощення виразу (4.20) допускає опускання ϕ і введення заміни $j = s_t(j)$. В результаті отримаємо вираз

$$\hat{r}_j = \sum_{t=1}^{T} p\left(j\middle|y_t\right)(x_t - y_t)\left(\sum_{t=1}^{T} p\left(j\middle|y_t\right)\right)^{-1}. \tag{4.21}$$

Аналогічно з аналітичного виразу $\frac{\partial Q}{\partial \hat{\Gamma}_j} = 0$ після відповідних перетворень отримаємо вираз для розрахунку значень мультиплікативних факторів

$$\hat{\Gamma}_j = \sum_{t=1}^{T} p\left(j\middle|y_t\right)\left((x_t - y_t)(x_t - y_t)^T - \hat{r}_j \hat{r}_j^T\right)\left(\sum_{t=1}^{T} p\left(j\middle|y_t\right)\right)^{-1}, \tag{4.22}$$

де апостеріорну імовірність j-ї компоненти моделі суміші для емпіричного вектора y_t опишемо виразом

$$p\left(j\middle|y_t\right) = p(j)p\left(y_t\middle|j\right)\left(\sum_{j=1}^{M} p(j)p\left(y_t\middle|j\right)\right). \tag{4.23}$$

Підставивши вирази (4.21) і (4.22) у вираз (4.1) отримаємо значення вектора характеристичних параметрів $\hat{x}_t$, в яких присутній у значеннях емпіричного вектора характеристичних параметрів y_t шум компенсовано:

$$\begin{aligned}
\hat{x}_t &= E\left(x\middle|y_t\right) = \int_x x p\left(x\middle|y_t\right)dx = \int_x \sum_{j=1}^{M} x p\left(j\middle|y_t\right) p\left(x\middle|j, y_t\right)dx = \\
&= \sum_{j=1}^{M} p\left(j\middle|y_t\right)\int_x x p\left(j\middle|y_t\right) p\left(x\middle|j, y_t\right)dx = \sum_{j=1}^{M} p\left(j\middle|y_t\right)\left(y_t + r_j\right) = \\
&= \sum_{j=1}^{M} p\left(j\middle|y_t\right)y_t + \sum_{j=1}^{M} p\left(j\middle|y_t\right)r_j = y_t + \sum_{j=1}^{M} p\left(j\middle|y_t\right)r_j .
\end{aligned} \tag{4.24}$$

Припущення (4.11) і (4.15) дозволили отримати аналітичні вирази (4.14) і (4.24) для розрахунку значень вектора (4.1) із акцентуванням уваги на моделюванні СГР еталонної бази X для мовленнєвого матеріалу без шуму і еталонної бази Y для мовленнєвого матеріалу із шумом, відповідно. Проте, на практиці рідко зустрічається ситуація, коли вміст еталонних баз X і Y відповідає лише одній з

умов (4.11) і (4.15). Розіб'ємо мовленнєвий матеріал еталонної бази Y на сегменти відповідно до характеристики акустичного оточення приймачів мовленнєвого сигналу e так, щоб для кожного сегменту Y_e умова (4.15) виконувалася. Опишемо Y_e-й сегмент еталонної бази Y незалежною моделлю СГР

$$p_e(y_t) = \sum_{s_y^e=1}^{M} p\left(y_t \middle| s_y^e\right) p\left(s_y^e\right), \tag{4.25}$$

де s_y^e – невідома складова моделі суміші, навченої на сегменті Y_e, із апріорною імовірністю і умовною функцією щільності імовірності описаними, відповідно, виразами:

$$\begin{gathered} p\left(s_y^e\right) = w_y^e, \\ p\left(y_t \middle| s_y^e\right) = N\left(y_t, \mu\left(s_y^e\right), \Sigma\left(s_y^e\right)\right). \end{gathered} \tag{4.26}$$

Еталонну базу X для мовленнєвого матеріалу без шуму, вміст якої задовольняє умову (4.11), опишемо однією моделлю суміші, ідентичною (4.2):

$$p(x_t) = \sum_{s_x=1}^{M} p(x_t | s_x) p(s_x) = \sum_{j=1}^{M} w_x(j) N(x_t, \mu_x(j), \Sigma_x(j)). \tag{4.27}$$

Формалізуємо зв'язок між моделями сумішей $p_e(y)$, які описують еталонні бази $Y_e \in Y$, і моделлю суміші $p(x)$, яка описує еталонну базу X, за значеннями компенсувальних векторів $r\left(s_x, s_y^e\right)$ у формі моделі суміші

$$p\left(x \middle| y_t, s_y^e, s_x\right) = N\left(x \middle| y_t - \sum_e p(e|y_t) r\left(s_x, s_y^e\right), \Sigma\left(s_x, s_y^e\right)\right), \tag{4.28}$$

де $p(e|y_t)$ – апостеріорна імовірність, що характеризує акустичне середовище e для емпіричного вектора характеристичних параметрів y_t, значення якої обчислюється в результаті роботи рекурсійного алгоритму, формалізованого виразом

$$p(e|y_t) = \beta p(e|y_{t-1}) + (1-\beta) p_e(y_{t-1}) \left(\sum_e p_e(y_{t-1}) \right)^{-1}, \tag{4.29}$$

де $0 \le \beta \le 1$ – константа, а $p(e|y_0)$ – узагальнена характеристика для всієї еталонної бази Y. Сформулюємо логарифмічну функцію правдоподібності для виразу (4.29):

$$L(Y_e) = \sum_{t_e=1}^{T_e} \log \sum_{s_y^e=1}^{M} p(s_y^e) N_y\left(y_{t_e}, \mu(s_y^e) + r(s_x, s_y^e), \Sigma(s_x, s_y^e)\right), \tag{4.30}$$

де $Y_e = \{y_{t_e}\}_{t_e=1}^{T_e}$ і $X_e = \{x_{t_e}\}_{t_e=1}^{T_e}$ – відповідні еталонні навчальні бази.

Підставивши функцію правдоподібності (4.30) у вираз (4.6), формалізуємо розв'язок отриманої задачі оптимізації:

$$r(s_x, s_y^e) = \sum_{t_e=1}^{T_e} p(s_x|x_{t_e}) p(s_y^e|y_{t_e})(y_{t_e} - x_{t_e}) \left(\sum_{t_e=1}^{T_e} p(s_x|x_{t_e}) p(s_y^e|y_{t_e}) \right)^{-1}, \tag{4.31}$$

де $p(s_x|x_{t_e})$ і $p(s_y^e|y_{t_e})$ – апостеріорні імовірності моделей сумішей s_x і s_y^e, відповідно, які описують емпіричні вектори $x_{t_e} \in X_e$ і $y_{t_e} \in Y_e$. На основі виразів (4.25) і (4.27) отримаємо вирази для розрахунку $p(s_x|x_{t_e})$ і $p(s_y^e|y_{t_e})$:

$$p(s_x|x_{t_e}) = p(x_{t_e}|s_x) p(s_x) \left(\sum_{s_x=1}^{M} (x_{t_e}|s_x) p(s_x) \right)^{-1}, \tag{4.32}$$

$$p(s_y^e|y_{t_e}) = p(y_t|s_y^e) p(s_y^e) \left(\sum_{s_y^e=1}^{M} p(y_t|s_y^e) p(s_y^e) \right)^{-1}. \tag{4.33}$$

Підставивши вираз (4.31) у вираз (4.1) отримаємо значення вектора характеристичних параметрів $\hat{x}_t$, у яких вплив присутнього у значеннях емпіричного вектора характеристичних параметрів y_t шуму компенсовано,

$$\begin{aligned} \hat{x}_t &= E(x|y_t) = \int_x x p(x|y_t) dx = \int_x \sum_e \sum_{s_y^e=1}^{M} \sum_{s_x=1}^{M} x p(x|y_t, s_y^e, s_x, e) dx = \\ &= y_t - \int_x \sum_e \sum_{s_y^e=1}^{M} \sum_{s_x=1}^{M} r(s_y^e, s_x) p(x|y_t, s_y^e, s_x, e) dx = \\ &= y_t - \sum_e \sum_{s_y^e=1}^{M} \sum_{s_x=1}^{M} r(s_y^e, s_x) p(e|y_t) p(x|y_t, s_y^e, s_x, e), \end{aligned} \tag{4.34}$$

де $p\left(s_x \middle| s_y^e, y_t, e\right)$ – крос-імовірнісна модель відхилення гаусівської компоненти s_x, що описує вектор x_t, від гаусівської компоненти s_y^e, що описує вектор y_t. Для спрощення кількісне значення $p\left(s_x \middle| s_y^e, y_t, e\right)$ вважатимемо рівним відношенню кількості випадків, коли s_x і s_y^e збігаються до загальної кількості випадків обчислення s_y^e:

$$p\left(s_x \middle| s_y^e, y_t, e\right) = \sum_{t_e=1}^{T_e} p\left(s_x \middle| x_{t_e}\right) p\left(s_y^e \middle| y_{t_e}\right) p\left(s_x\right) p\left(s_y^e\right) \times$$
$$\times \left(\sum_{t_e=1}^{T_e} \sum_{s_x=1}^{M} p\left(s_x \middle| x_{t_e}\right) p\left(s_y^e \middle| y_{t_e}\right) p\left(s_x\right) p\left(s_y^e\right) \right)^{-1}. \quad (4.35)$$

Антитезою реалізованої у виразі (4.28) концепції сегментації матеріалу еталонних баз для компенсування шумів акустичного оточення у фонограмі мовленнєвого сигналу із низьким значенням рівня відношення «сигнал»/«шум» є концепція інтеграції еталонної бази спектральних характеристичних параметрів, екстрагованих із фонограм мовленнєвого матеріалу без шуму, із еталонною базою спектральних характеристичних параметрів, екстрагованих з фонограм мовленнєвого матеріалу із шумом, у єдину агреговану еталонну базу. Такий підхід дозволяє не тільки скоротити обсяг задіяних обчислювальних ресурсів, адже мовленнєвий матеріал утвореної агрегованої еталонної бази описуватиметься однією моделлю СГР замість двох або більшої кількості моделей сумішей, як це було реалізовано у виразах (4.14), (4.24), (4.34), а й орієнтувати отриману модель суміші на компенсування конкретного типу шуму, контролюючи вміст еталонної бази із результатами параметризації мовленнєвого матеріалу із шумом. Візуально процес компенсування шумів у емпіричному мовленнєвому сигналі моделлю СГР, навченою на вмісті агрегованої еталонної бази, зображено на рис. 4.2.

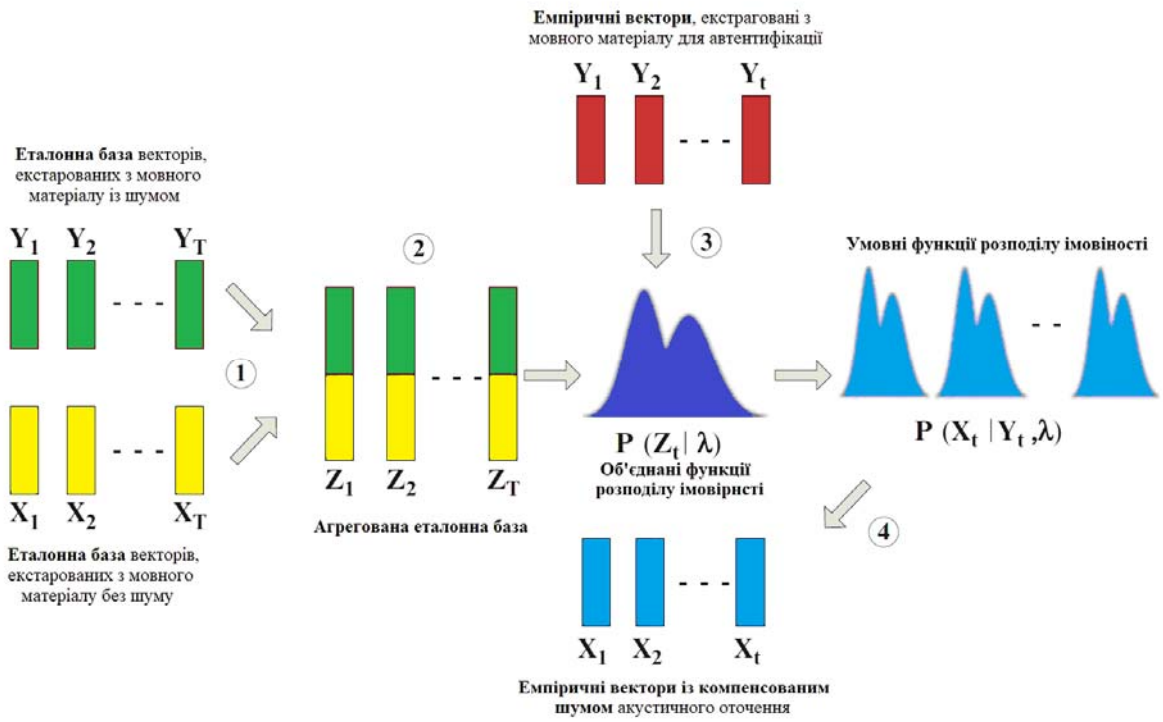


Рисунок 4.2 – Стохастична компенсація шумів у емпіричному мовленнєвому сигналі моделлю суміші, навченою на агрегованій еталонній базі

Сформуємо з кожної пари d-вимірних векторів характеристичних параметрів x_t і y_t, $t=\overline{1,T}$, взятих з еталонних баз X і Y, відповідно, об'єднаний вектор характеристичних параметрів z_t розмірністю $2\times d$ виду $z_t=\left[y_t^T, x_t^T\right]^T$, утворюючи таким чином агреговану еталонну базу $Z=\{z_t\}$, $t=\overline{1,T}$, для опису вмісту якої синтезуємо модель СГР $\lambda^{(Z)}$, формалізовану виразом

$$\begin{aligned}
\lambda^{(Z)} &= E\left[x|y_t\right] = \int_x x p(x|y_t)dx = \int_x (y_t - r(x))p(x|y_t)dx = \\
&= \int_x y_t p(x|y_t)dx - \int_x r(x)p(x|y_t)dx = y_t \int_x p(x|y_t)dx - \\
&- \int_x \sum_{j=1}^{M} r(x)p(x,j|y_t)dx = y_t - \sum_{j=1}^{M} p(j|y_t)\int_x r(x)p(x|j,y_t)dx = \\
&= y_t - \sum_{j=1}^{M} p(j|y_t) r_j \int_x p(x|j,y_t)dx = y_t - \sum_{j=1}^{M} p(j|y_t) r_j,
\end{aligned} \tag{4.36}$$

структуру вектора середніх значень $\mu_z(j)$ і коваріаційної матриці $\Sigma_z(j)$ j-ї компоненти якої опишемо виразами

$$\mu_z(j)=\begin{pmatrix}\mu_y(j)\\ \mu_x(j)\end{pmatrix},$$
$$\Sigma_z(j)=\begin{pmatrix}\Sigma_{yy}(j) & \Sigma_{yx}(j)\\ \Sigma_{xy}(j) & \Sigma_{xx}(j)\end{pmatrix}. \tag{4.37}$$

Вектори $\mu_x(j)$, $\mu_y(j)$ і коваріаційні матриці $\Sigma_{xx}(j)$, $\Sigma_{yy}(j)$ вже використовувалися для синтезу моделей сумішей (4.2), (4.3), відповідно, а крос-коваріаційні матриці $\Sigma_{xy}(j)$, $\Sigma_{yx}(j)$, які описують зв'язок вмісту еталонних баз X і Y, вживаються вперше.

Навчатимемо модель суміші (4.36) методом максимізації правдоподібності. Синтезуємо аналітичний вираз для опису умовних функцій розподілу імовірностей $p(x_t|y_t)$, які, враховуючи структуру агрегованої еталонної бази Z, векторів $\mu_z(j)$ і матриць $\Sigma_z(j)$, є окремими моделями сумішей, вагами яких є апостеріорні імовірності всіх компонентів, залежних від y:

$$p\left(x_t\middle|y_t,\lambda^{(Z)}\right)=\sum_{j=1}^{M}p\left(j\middle|y_t,\lambda^{(Z)}\right)p\left(x_t\middle|y_t,j,\lambda^{(Z)}\right), \tag{4.38}$$

де моделі сумішей $p\left(j\middle|y_t,\lambda^{(Z)}\right)$ і $p\left(x_t\middle|y_t,j,\lambda^{(Z)}\right)$ описуються виразами

$$p\left(j\middle|y_t,\lambda^{(Z)}\right)=w_y(j)N\left(y_t,\mu_y(j),\Sigma_{yy}(j)\right)\times$$
$$\times\left(\sum_{j=1}^{M}w_y(j)N\left(y_t,\mu_y(j),\Sigma_{yy}(j)\right)\right)^{-1}, \tag{4.39}$$

$$p\left(x_t\middle|y_t,j,\lambda^{(Z)}\right)=N\left(x_t,E_x(j,t),D_x(j)\right). \tag{4.40}$$

Вектор середніх значень $E_x(j,t)$ і коваріаційну матрицю $D_x(j)$ для j-ї компоненти умовної функції розподілу імовірності (4.38) опишемо виразами

$$E_x(j,t)=\mu_x(j)+\Sigma_{xy}(j)\left(\Sigma_{yy}(j)\right)^{-1}\left(y_t-\mu_y(j)\right), \tag{4.41}$$

$$D_x(j) = \Sigma_{xx}(j) + \Sigma_{xy}(j)\left(\Sigma_{yy}(j)\right)^{-1}\Sigma_{yx}(j). \tag{4.42}$$

Застосувавши критерій мінімізації середньоквадратичної похибки (4.1) формалізуємо розрахунок значень вектора характеристичних параметрів $\hat{x}_t$ у якому, присутній у значеннях емпіричного вектора характеристичних параметрів y_t шум, компенсовано:

$$\begin{aligned} \hat{x}_t &= E\left(x_t \middle| y_t\right) = \int_X x_t p\left(x_t \middle| y_t, \lambda^{(Z)}\right) dx_t = \\ &= \int_X \sum_{j=1}^{M} x_t p\left(j \middle| y_t, \lambda^{(Z)}\right) p\left(x_t \middle| y_t, j, \lambda^{(Z)}\right) dx_t = \sum_{j=1}^{M} p\left(j \middle| y_t, \lambda^{(Z)}\right) E_x(j,t). \end{aligned} \tag{4.43}$$

Процес синтезу виразу (4.43) описано компактно, адже він структурно ідентичний процесу синтезу виразу (4.24), у якому тільки необхідно було додатково врахувати структурні особливості агрегованої еталонної бази Z.

Як було описано вище, вміст агрегованої еталонної бази Z утворювався безпосереднім попарним об'єднанням векторів характеристичних параметрів x_t і y_t, $t = \overline{1,T}$, з еталонних баз X і Y, відповідно, у двохвимірний вектор $z_t = \left[y_t^T, x_t^T\right]^T$, $t = \overline{1,T}$. Хоч матеріал еталонних баз X і Y є незалежним, з'являється ненульова імовірність виникнення кореляції між об'єднаними векторами z_t, яка згодом підсилюватиметься у процесі розрахунку параметрів (4.37), і, в свою чергу, призведе до того, що навчена модель суміші (4.38), задіяна у процесі компенсування шумів у емпіричному мовленнєвому сигналі у виразі (4.43), привноситиме у вихідний вектор характеристичних параметрів $\hat{x}_t$ динамічні спотворення і занадто згладжуватиме спектр підсумкового сигналу. Для унеможливлення описаної ситуації необхідно забезпечити як незалежність всіх компонент $2d$ вектора z_t, так і самих векторів z_t у масштабі всієї агрегованої еталонної бази Z. Враховуючи спектральну природу характеристичних параметрів, об'єднаних у вектори x_t і y_t, пропонується при формуванні об'єднаних векторів z_t додатково враховувати динамічні спектральні характеристики [247, 248]. В такому разі мовленнєвий матеріал без шуму і мовленнєвий матеріал із шумом, накопичені для на-

вчання моделі суміші, опишемо відповідними множинами матриць характеристичних параметрів $X=\left\{X_t^T\right\}^T$ і $Y=\left\{Y_t^T\right\}^T$, $t=\overline{1,T}$, де матриці $X_t=\left(x_t^T,\Delta x_t^T,\Delta^2 x_t^T\right)$ і $Y_t=\left(y_t^T,\Delta y_t^T,\Delta^2 y_t^T\right)$ містять безпосередні, дельта і дельта-дельта значення спектральних характеристичних параметрів, розрахованих для t-х фреймів відповідних мовленнєвих сигналів.

Нехай модель суміші $\lambda^{(Z)}$ об'єднаних умовних функцій щільностей імовірностей $p\left(Z_t\middle|\lambda^{(Z)}\right)$ навчено за даними з динамічної агрегованої еталонної бази $Z_t=\left[Y_t^T,X_t^T\right]$, $t=\overline{0,T}$. Оцінити зв'язок між матрицями динамічних характеристичних параметрів з еталонних баз X і Y можна розв'язавши задачу максимізації функції правдоподібності

$$\begin{aligned} p\left(X\middle|Y,\lambda^{(Z)}\right)&=\sum_j p\left(j\middle|Y,\lambda^{(Z)}\right)p\left(X\middle|Y,j,\lambda^{(Z)}\right)= \\ &=\prod_{t=1}^{T}\sum_{j=1}^{M} p\left(j\middle|Y_t,\lambda^{(Z)}\right)p\left(X_t\middle|Y_t,j,\lambda^{(Z)}\right), \end{aligned} \tag{4.44}$$

де $j=\{j_t\}$, $t=\overline{1,T}$ – множина компонентів моделі суміші. Вагу $p\left(j\middle|Y_t,\lambda^{(Z)}\right)$ і умовну функцію розподілу імовірності $p\left(X_t\middle|Y_t,j,\lambda^{(Z)}\right)$ кожної j-ї компоненти суміші (4.44), що описує фрейм t, можна формалізувати виразами

$$p\left(j\middle|Y_t,\lambda^{(Z)}\right)=w_j^Y N\left(Y_t,\mu_j^Y,\Sigma_j^{YY}\right)\left(\sum_{j=1}^{M} w_j^Y N\left(Y_t,\mu_j^Y,\Sigma_j^{YY}\right)\right), \tag{4.45}$$

$$p\left(X_t\middle|Y_t,j,\lambda^{(Z)}\right)=N\left(X_t,E_{j,t}^X,D_j^X\right), \tag{4.46}$$

де вектор середніх значень і коваріаційну матрицю j-ї компоненти суміші (4.46) для фрейма t опишемо виразами

$$E_{j,t}^X=\mu_j^X+\Sigma_j^{XY}\left(\Sigma_j^{YY}\right)^{-1}\left(Y_t-\mu_j^Y\right), \tag{4.47}$$

$$D_j^X=\Sigma_j^{XX}-\Sigma_j^{XY}\left(\Sigma_j^{YY}\right)^{-1}\Sigma_j^{YX}. \tag{4.48}$$

Враховуючи структуру матриць динамічних характеристичних параметрів X та Y, задачу розрахунку матриці $\hat{X}$, в елементах якої компенсовано вплив шумів акустичного оточення, присутніх у відповідних елементах емпіричної матриці динамічних характеристичних параметрів Y, розв'язуватимемо у два етапи. Спочатку перейдемо від емпіричної матриці динамічних характеристичних параметрів Y до статичних значень і знайдемо статичні значення вектора $\hat{x}$, які максимізують функцію правдоподібності (4.44). На другому етапі для ідентифікованого вектора $\hat{x}$ розрахуємо вектори його дельта і дельта-дельта значень, які узагальнимо в динамічній матриці оцінок $\hat{X}$, яку і порівнюватимемо із еталонною базою матриць динамічних характеристичних параметрів X. Аналітично перший і другий етапи опишемо виразами

$$\hat{x} = \arg\max_{x} p\left(X \middle| Y, \lambda^{(Z)}\right), \tag{4.49}$$

$$\hat{X} = W\hat{x}, \tag{4.50}$$

де $\hat{x} = \left(\hat{x}_1^T, \hat{x}_2^T, \ldots, \hat{x}_T^T\right)$ – вектор статичних значень для $\hat{X}$, а трансформувальна матриця W розмірністю $3dT \times dT$ має структуру

$$W = \{W_t\}^T \otimes I_{d\times d}, \tag{4.51}$$

$$W_t = \left(w_t^{(0)}, w_t^{(1)}, w_t^{(2)}\right), \tag{4.52}$$

$$w_t^{(0)} = \left(\overset{1-ŭ}{0}, \ldots, 0, \overset{\left(t-L_-^{(n)}\right)-ŭ}{w^{(n)}\left(-L_-^{(n)}\right)}, \ldots, \overset{\left(t+L_+^{(n)}\right)-ŭ}{w^{(n)}\left(L_+^{(n)}\right)}, \ldots, \overset{t-ŭ}{w^{(n)}(0)}, \ldots, \overset{T-ŭ}{0} \right)^T, \tag{4.53}$$

де $t = \overline{1,T}$, $n = \overline{0,2}$, $w^{(n)}(\tau)$ – ваги, необхідні для обчислення динамічного значення відповідного спектрального характеристичного параметра Δ^n для моменту часу $(t+\tau)$ у межах t-го фрейма, $\tau \in \left[-L_-^{(n)}, L_+^{(n)}\right]$, $L_-^{(0)} = L_+^{(0)} = 0$, $w^{(0)}(0) = 1$,

$$\Delta^1 x_t = \sum_{\tau=-L_-^{(1)}}^{L_+^{(1)}} w^{(1)}(\tau) x_{t+\tau}, \tag{4.54}$$

$$\Delta^2 x_t = \sum_{\tau=-L_-^{(2)}}^{L_+^{(2)}} w^{(2)}(\tau) x_{t+\tau}. \tag{4.55}$$

Підставивши аналітичну форму функції правдоподібності (4.49) у вираз (4.6) отримаємо цільову функцію із керованими змінними $\hat{x}$:

$$
\begin{aligned}
Q\left(X,\hat{X}\right) &= \sum_{j} p\left(j\middle|Y,X,\lambda^{(Z)}\right)\log\left(p\left(\hat{X},j\middle|Y,\lambda^{(Z)}\right)\right)= \\
&= \sum_{t=1}^{T}\sum_{j=1}^{M} p\left(j\middle|Y_t,X_t,\lambda^{(Z)}\right)\log\left(p\left(\hat{X}_t,j\middle|Y_t,\lambda^{(Z)}\right)\right)= \\
&= \sum_{t=1}^{T}\sum_{j=1}^{M}\lambda_{j,t}\left(0{,}5\hat{X}_t^T\left(D_j^X\right)^{-1}\hat{X}_t+\hat{X}_t^T\left(D_j^X\right)^{-1}E_{j,t}^X\right)+K= \\
&= \sum_{t=1}^{T}\left(-0{,}5\sum_{j=1}^{M}\lambda_{j,t}\hat{X}_t^T\left(D_j^X\right)^{-1}\hat{X}_t+\sum_{j=1}^{M}\lambda_{j,t}\hat{X}_t^T\left(D_j^X\right)^{-1}E_{j,t}^X\right)+K= \\
&= \sum_{t=1}^{T}\left(-0{,}5\hat{X}_t^T\overline{\left(D_j^X\right)^{-1}}\hat{X}_t+\hat{X}_t^T\overline{\left(D_j^X\right)^{-1}E_{j,t}^X}\right)+K= \\
&= -0{,}5\hat{X}^T\overline{\left(D^X\right)^{-1}}\hat{X}+\hat{X}^T\overline{\left(D^X\right)^{-1}E^X}+K= \\
&= -0{,}5\hat{x}^TW^T\overline{\left(D^X\right)^{-1}}\hat{x}W+\hat{x}^TW^T\overline{\left(D^X\right)^{-1}E^X}+K\,.
\end{aligned}
\tag{4.56}
$$

Підставивши вираз (4.56) у вираз (4.1) отримаємо шуканий вектор характеристичних параметрів $\hat{x}$ для емпіричного вектора характеристичних параметрів y_t, значення якого екстраговано із мовленнєвого матеріалу із шумом:

$$
\frac{\partial Q\left(X,\hat{X}\right)}{\partial\hat{x}} = -W^T\overline{\left(D^X\right)^{-1}}\hat{x}W+W^T\overline{\left(D^X\right)^{-1}E^X}\,. \tag{4.57}
$$

Прирівняємо вираз (4.57) до нуля і виразимо

$$
\hat{x} = \left(W^T\overline{\left(D^X\right)^{-1}}\hat{x}W\right)^{-1}W^T\overline{\left(D^X\right)^{-1}E^X}\,. \tag{4.58}
$$

де $\overline{\left(D^X\right)^{-1}}$ і $\overline{\left(D^X\right)^{-1}E^X}$ – складена $3dT\times 3dT$-розмірна матриця і складений $3dT\times 1$-розмірний вектор, структуру яких описано виразами

$$
\overline{\left(D^X\right)^{-1}} = diag\left(\overline{\left(D_1^X\right)^{-1}},\overline{\left(D_2^X\right)^{-1}},\ldots,\overline{\left(D_t^X\right)^{-1}},\ldots,\overline{\left(D_T^X\right)^{-1}}\right); \tag{4.59}
$$

$$
\overline{\left(D^X\right)^{-1}E^X} = \left(\overline{\left(D_1^X\right)^{-1}E_1^X}^T,\ldots,\overline{\left(D_t^X\right)^{-1}E_t^X}^T,\ldots,\overline{\left(D_T^X\right)^{-1}E_T^X}^T\right)^T, \tag{4.60}
$$

відповідно, а їх елементи розраховуються за виразами

$$\overline{\left(D_t^X\right)^{-1}} = \sum_{j=1}^{M} \lambda_{j,t} \left(D_j^X\right)^{-1}; \tag{4.61}$$

$$\overline{\left(D_t^X\right)^{-1} E_t^X} = \sum_{j=1}^{M} \lambda_{j,t} \left(D_j^X\right)^{-1} E_{j,t}^X; \tag{4.62}$$

$$\lambda_{j,t} = p\left(j \middle| Y_t, X_t, \lambda^{(Z)}\right). \tag{4.63}$$

Розв'язком виразу (4.58) буде вектор значень $dT \times 1$.

Проведемо дослідження ефективності процедури компенсації шумів акустичного оточення у запропонованому суб'єктом для сеансу автентифікації мовленнєвому матеріалі, здійснюваної за методами, узагальненими виразами (4.14), (4.24), (4.34), (4.43), (4.58) тощо. Дослідження проводитимемо із мовленнєвим матеріалом з бази NOIZEUS [282], наповнивши еталонну і емпіричну бази відповідного суб'єкта мовленнєвим матеріалом тривалістю 120 с і 12 с, відповідно, який розбито на фрейми тривалістю 20 мс із перекриттям у 10 мс. У базі NOIZEUS є записи шумів акустичного оточення типу «Car», «Street», «Airport», «Train station» тощо, які можна підмішувати до мовленнєвого матеріалу без шуму, отримуючи мовленнєвий матеріал із необхідним рівним відношення «сигнал»/«шум». Для експериментів використовувався мовленнєвий матеріал із SNR=0 дБ. Кожен фрейм описувався 39-розмірним вектором спектральних характеристичних параметрів, який включав 13 Мел-частотних кепстральних коефіцієнтів $C = \{c_1, c_2, \ldots, c_{13}\}$, 13 дельта $\Delta = \{\Delta_1, \Delta_2, \ldots, \Delta_{13}\}$ і 13 дельта-дельта коефіцієнтів $\Delta^2 = \left\{\Delta_1^2, \Delta_2^2, \ldots, \Delta_{13}^2\right\}$ тощо. При виборі кількості обчислюваних кепстральних коефіцієнтів враховувалося, що коефіцієнт із порядковим номером 0 характеризує потужність всього частотного діапазону аналізованого сигналу у фреймі, що робить його інформативним лише для сегментації вмісту фрейма на класи «сигнал» або «пауза», а коефіцієнт із порядковим номером 1 характеризує баланс між потужностями низько- і високочастотної складової аналізованого сигналу у фреймі. Решта кепстральних коефіцієнтів деталізують спектральний опис сигналу. Перші і другі похідні від відповідних кепстральних коефіцієнтів – дельта- і дельта-дельта-коефіцієнти, призначені для врахування динамічних властивостей аналізованого сигналу.

До векторів характеристичних параметрів послідовно застосовувалися процедури віднімання кепстрального середнього [248] і нормалізації спектральної дисперсії [248]. Всі функції розподілів центрувалися відніманням середнього і приводилися до одиничної дисперсії. Для забезпечення відтворюваності отриманих результатів використано 1024-компонентну універсальну фонову модель [298, 299], навчену на мовленнєвому матеріалі тривалістю дванадцять годин. Восьмикомпонентні моделі СГР суб'єктів отримано в результаті адаптації універсальної фонової моделі на основі мовленнєвого матеріалу з еталонних баз відповідних суб'єктів, тобто для кожного суб'єкта сформовано по дві моделі сумішей – на основі мовленнєвого матеріалу без шуму і на основі мовленнєвого матеріалу із шумом, відповідно.

На рис. 4.3 представлено гістограми значень найінформативнішого, першого, кепстрального коефіцієнта c_1 із параметричних векторів, які описують мовленнєві сигнали:

- із еталонної бази (без шуму);
- із емпіричної бази із SNR = 0 дБ;
- шуми в яких компенсовано за методами, узагальненими виразами (4.14), (4.24), (4.34), (4.43), (4.58), відповідно.

Якість компенсації визначається площею перетину оцінюваної гістограми із першою гістограмою. За цим критерієм очевидно, що найкращі результати показують методи, узагальнені виразами (4.43), (4.58).

Результати, представлені на рис. 4.3, підтверджуються результатами, представленими на рис. 4.4, де по осі абсцис відкладено значення коефіцієнта c_1, екстрагованого із екземпляра мовленнєвого сигналу без шуму, а по осі ординат – значення коефіцієнта c_1, екстрагованого із екземпляра мовленнєвого сигналу: а) із шумом при SNR = 0 дБ; б), в), г), д), е) – шум у якому компенсовано за методом, узагальненим виразом (4.14), (4.24), (4.34), (4.43), (4.58), відповідно. Чорною лінією на рис. 4.4 позначено випадки $x = y$, а червоною – випадки найменшої розбіжності значень. Вочевидь, можна стверджувати ефективність запропонованої процедури компенсації шумів акустичного оточення в емпіричному мовленнєвому

сигналі. Також очевидно, що найкращі результати показують методи, узагальнені виразами (4.43), (4.58). Втім, ці методи є і найбільш ресурсозатратними.

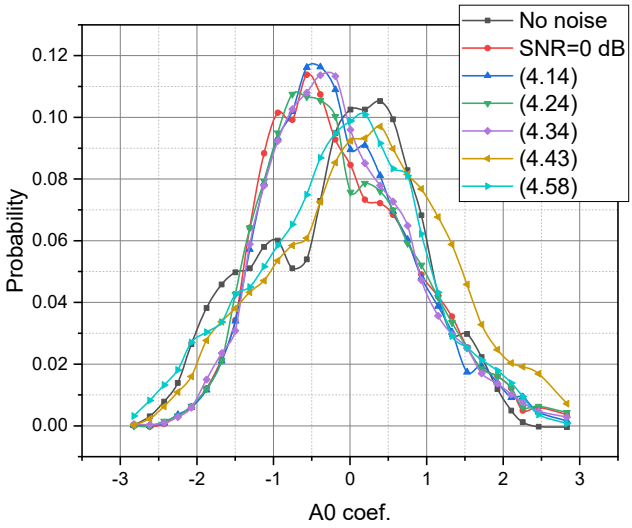
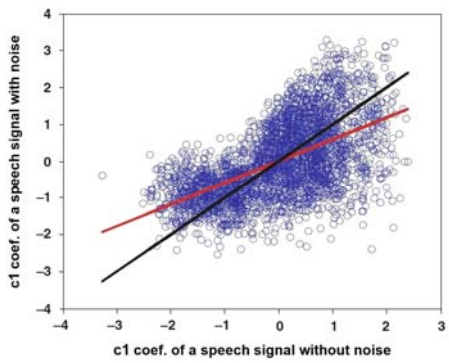
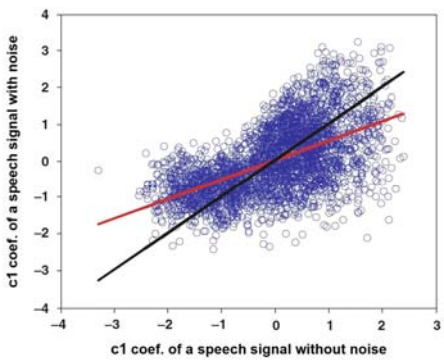


Рисунок 4.3 – Гістограми розподілу значень кепстрального коефіцієнта c_1, екстрагованих із мовленнєвих матеріалів, шум у яких компенсовано відповідним методом.

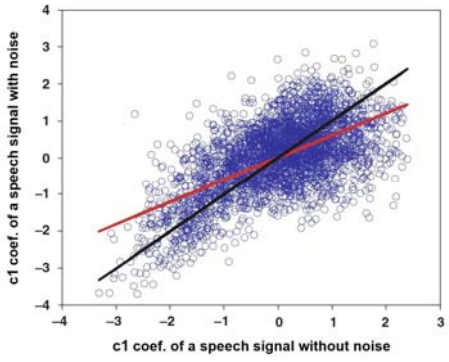
Прикладне застосування і емпіричне доведення адекватності представленого у підрозділі матеріалу наведено у додатку Ж, де вичерпно описано теоретичні і практичні аспекти моделювання процесу АСММШ (рис. Ж.1, Ж.2, Ж.3) у формалізмі породжувальних і дискримінаційних імовірнісних моделей [300–317]. Наведені на рис. Ж.7 результати підтверджують доцільність та дієвість запропонованого в підрозділі 4.1 математичного апарату для компенсації шумів у мовленнєвому сигналі, який використовується для автентифікації суб’єкта. Компенсування спричиняє помітний вплив на достовірність автентифікації при рівні відношення «сигнал»/«шум» 5 і 10 дБ. Також помітно, що вдається успішно компенсувати всі чотири типи шумів, а найефективніше – шум типу «Car», який найбільше впливав на достовірність моделі автентифікації в дослідженні, представленому на рис. Ж.6.



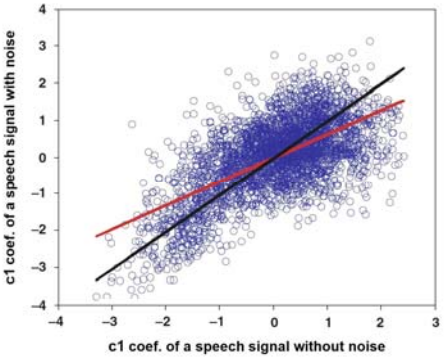
а)



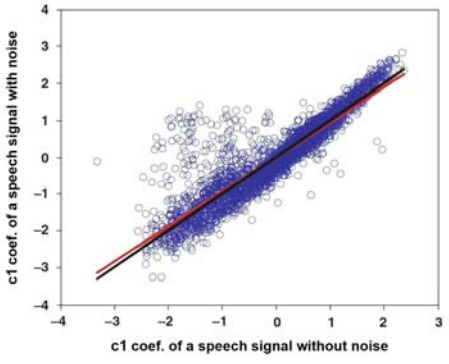
б)



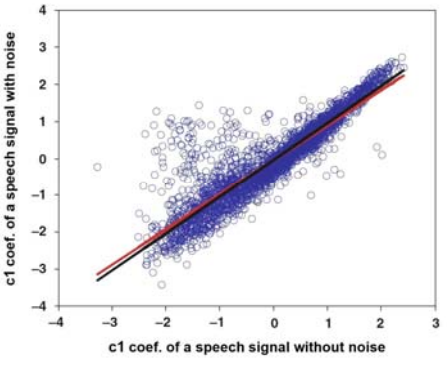
в)



г)



д)



е)

Рисунок 4.4 – Діаграми розсіювання значень кепстрального коефіцієнта c_1, екстрагованих із (вісь абсцис) мовленнєвого матеріалу без шуму та із (вісь ординат) мовленнєвого матеріалу із SNR=0 дБ, шум у якому було компенсовано методом: а) без компенсації, б) (4.14), в) (4.24), г) (4.34), д) (4.43), е) (4.58)

Представлені на рис. Ж.13 результати підтверджують помітний вплив порогу прийняття рішень у класифікаторі машини опорних супервекторів та тривалості

парольного мовленнєвого сигналу на достовірність моделі процесу АСММШ, що іще раз підтверджує актуальність наукових результатів, представлених в підрозділі 3.2. Наведені на рис. Ж.12 результати експериментів із представленою у додатку Ж технологією бустінгу вмісту еталонної бази фонограм показали, що остання дозволяє адаптувати класифікатори комплексної моделі АСММШ до протидії періодичним низькочастотним шумам, знижуючи імовірності виникнення похибок першого або другого роду на $\pm 0{,}5 \div 1{,}5\,\%$ і $\pm 0{,}5 \div 2\,\%$, відповідно. Нарешті, на основі комплексного дослідження, результати якого візуалізовано на рис. Ж.12, визначено найкращу конфігурацію імовірнісного класифікатора для АСММШ: SiVM+Kbcos+Gall.

4.2 Моделі і методи процесу класифікації в задачі автентифікації суб'єкта за мовленнєвим сигналом із шумом

Як відзначалося у додатку Ж, достовірність практичних результатів моделювання процесу автентифікації суб'єкта машиною опорних векторів на основі моделі СГР для представлення параметризованого мовленнєвого сигналу із шумом, значно залежить від обсягу еталонної навчальної бази. Необхідно проаналізувати справді великі обсяги мовленнєвого матеріалу, щоб машина опорних векторів якісно вирізняла в супер- або *i*-векторах необхідну для автентифікації суб'єкта інформацію. Недоліки процедури векторного квантування при опрацюванні великих обсягів інформації зумовлюють пошук альтернативних методів класифікації в задачі АСГ, зокрема, нейромережевих.

Прецеденти використання глибоких нейромереж як для параметризації мовленнєвих сигналів [222–225], так і для класифікації [241–248] в задачі АСГ, відомі. Навчена глибока нейромережа може описати представлений на вхідний шар вектор характеристичних параметрів вектором апостеріорних імовірностей, який є аналогом *i*-вектора і може згодом використовуватися для класифікації [241–248]. Також відома практика синтезу глибокої нейромережі, в якій кількість нейронів на останньому прихованому шарі є суттєво меншою порівняно із кількістю нейронів на решті прихованих шарів. Після навчання такої нейромережі

ваги нейронів останнього прихованого шару використовують як характеристичні параметри для подальшої класифікації [247, 248]. В залежності від вмісту навчальної бази, можна закласти у такі характеристичні параметри стійкість до вибраних ефектів, які спостерігаються в мовленнєвих сигналах. Зокрема, міні-пакетний стохастичний метод градієнтного спуску [225, 226] дозволяє за рахунок попереднього розбиття еталонної навчальної бази на сегменти-«пакети» профілювати початкові приховані шари глибокої нейромережі для виділення характеристичних параметрів низького рівня, які згодом узагальнюються останнім прихованим шаром у характеристичні параметри високого рівня, імітуючи когнітивну діяльність кори головного мозку людини. Архітектура глибоких нейромереж, які використовуються для класифікації, передбачає наявність порівняно невеликої кількості прихованих шарів і дискретного вихідного шару, кількість нейронів на якому дорівнює кількості класів, які має вирізняти класифікатор. В задачі АСГ нейромережевий класифікатор перед винесенням остаточного вердикту узагальнює кілька послідовно поданих на його вхідний шар векторів характеристичних параметрів, екстрагованих із відповідних фреймів мовленнєвого сигналу. При такій організації процесу класифікації глибоку нейромережу доповнюють шаром, який здійснює усереднення проміжних результатів класифікації для винесення підсумкового вердикту.

Втім, недоліком глибоких нейромереж є грандіозна кількість параметрів, які слід налаштовувати в процесі навчання. Ця обставина обумовлює суворість вимог до репрезентативності вмісту і обсягу еталонної навчальної бази. Спробою компенсування цього недоліку став синтез цілої низки методів редукування [222–226], призначених для структурної та параметричної оптимізації глибоких нейромереж. Вирізняють спрямоване на управління вагами міжнейронних зв’язків, параметричне редукування на основі похідної від скаляризації технології регуляризації [225], зокрема, L_1- і L_2-регуляризацію. Також глибоким нейромережам властиве явище перенавчання, яке проявляється в суттєво нижчій усередненій достовірності класифікації для тестувальної бази, порівняно з усередненою достовірністю класифікації для еталонної бази. Основною причиною перенавчання є недбалість при формуванні еталонної бази, яка проявляється в невиявленій взаємокореляції між її екзем-

плярами, якої потім немає між екземплярами тестувальної бази. Для запобігання перенавчання вживають різних методів, як класичних [225], наприклад, байєсвіського порівняння моделей [225], так і емпіричних, наприклад, множення сигналу на виході нейронів прихованого шару на сигнал білого шуму [225] тощо. Всі ці операції, відповідно, подовжують процес підготовки нейромережі для експлуатації.

Отже, проведемо дослідження достовірності процесу класифікації в задачі АСГ при використанні глибокого нейромережевого класифікатора. Як і в попередньому підрозділі, для досліджень використаємо мовленнєвий матеріал бази NOIZEUS, на основі якого утворимо бази мовленнєвих матеріалів з різним типом та рівнем акустичних шумів. Параметризація мовленнєвого матеріалу здійснювалася аналогічно описаному у додатку Ж і включала представлення фреймів мовленнєвого сигналу векторами чотирьох наборів характеристичних параметрів.

Для синтезу глибокої нейромережі скористаємося безкоштовним стандартизованим фреймворком CogNitive ToolKit (CNTK) [318] від Microsoft, який дозволяє навчати створені нейромережі швидше ніж безкоштовні аналоги типу Caffe, Theano, TensorFlow тощо. У бібліотеках CNTK є все необхідне для синтезу і навчання всіх актуальних класів нейромереж. Фреймворк забезпечує сумісність вбудованих бібліотек із програмними середовищами C++ і Python, дозволяє навчати створені нейромережі використовуючи центральний процесор, графічний адаптер, кластер графічних адаптерів, організованих із програмною підтримкою пакету інструкцій NVIDIA CUDA, тощо.

При конструюванні класифікатора передбачимо, що для урахування динамічних складових сегментованого мовленнєвого сигналу доцільно здійснювати його аналіз порціями з 10 послідовних фреймів із подальшим зміщенням на один фрейм, тому кількість нейронів на вхідному шарі нейромережевого класифікатора дорівнюватиме збільшеній у десять разів кількості елементів у векторі характеристичних параметрів, екстрагованих із одного фрейма мовленнєвого сигналу. Відповідно, під кожен набір характеристичних параметрів необхідно синтезувати індивідуальну нейромережу. В базовій архітектурі створюваних нейромереж передбачено наявність трьох прихованих шарів із тисячею нейронів на кожному.

У нейронах вхідного шару використовувалася лінійна функція активації, в нейронах прихованих шарів – сигмоїдна, а у нейронах вихідного шару – softmax-функція. Рішення щодо початкової оптимізації кількості нейронів на прихованих шарах приймалося на основі результатів емпіричних досліджень для першого набору характеристичних параметрів, вектори якого є найдовшими. Класифікатор навчався стохастичним методом градієнтного спуску [225] із коефіцієнтом швидкості навчання нейромережі 0,001. Результат дослідження наведено на рис. 4.5, з яких видно, що збільшення кількості нейронів на прихованому шарі понад 1000 екземплярів не дає зростання достовірності класифікації.

Досить значна різниця між достовірністю опису тестувальних і еталонних даних, виявлена на рис. 4.5, свідчити про недостатній обсяг еталонної бази для навчання нейромережі із вибраною конфігурацію. Одним із варіантів підвищення достовірності класифікації, не змінюючи еталонну базу, є застосування оберненого редукування [225] до прихованих шарів нейромережі, результати якого наведено на рис. 4.6.

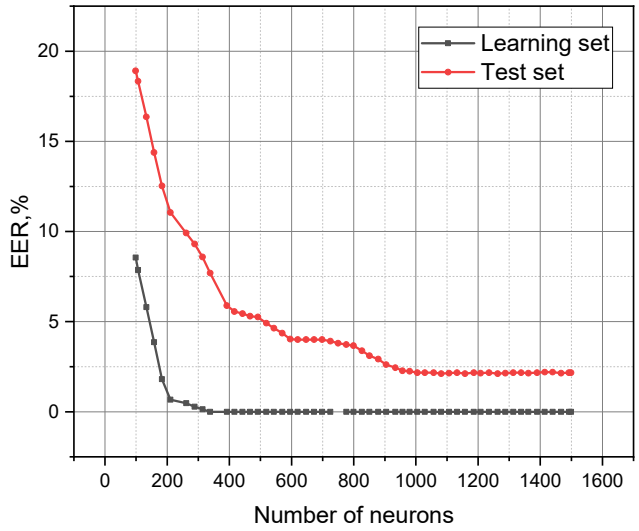


Рисунок 4.5 – Оцінювання впливу на якість класифікації кількості нейронів на прихованих шарах

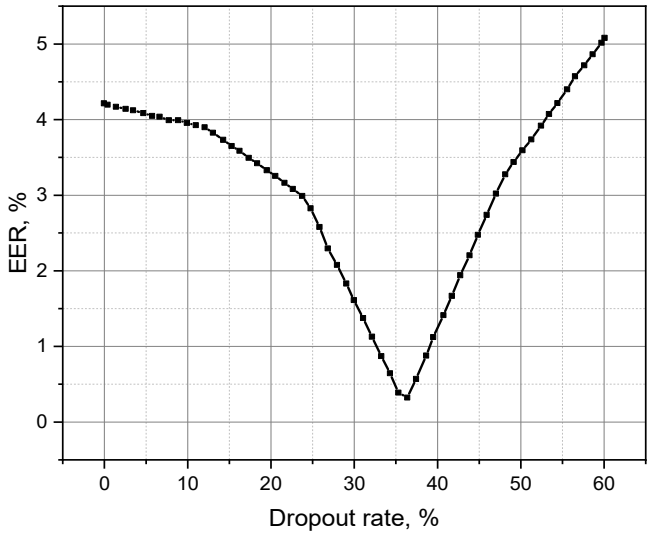


Рисунок 4.6 – Застосування оберненого редукування до базової конфігурації глибокої нейромережі

Результати, наведені на рис. 4.6 свідчать про те, що для оптимального опису вмісту еталонної бази кількість нейронів на прихованих шарах слід зменшити на 36 %, тобто на 360 екземплярів, відповідно. Це суттєво зменшить ресурсозатрат-

ність процесу навчання, адже конфігурація вихідної нейромережі описувалася множиною із понад 2,5 млн параметрів. Втім, обернене редукування є лише першим етапом оптимізації структури глибокої нейромережі.

Застосуємо до глибокої нейромережі L_2 регуляризацію [225], результативність якої в залежності від рівня представленого в мовленнєвому матеріалі шуму показано відповідними діаграмами на рис. 4.7.

З отриманих результатів видно, що зменшення кількості міжнейронних зв'язків у 10 разів спричиняє помітне падіння достовірності автентифікації, тому подальші дослідження проводитимемо із базовою глибокою нейромережею, в якій врахуємо лише результати оберненого редукування.

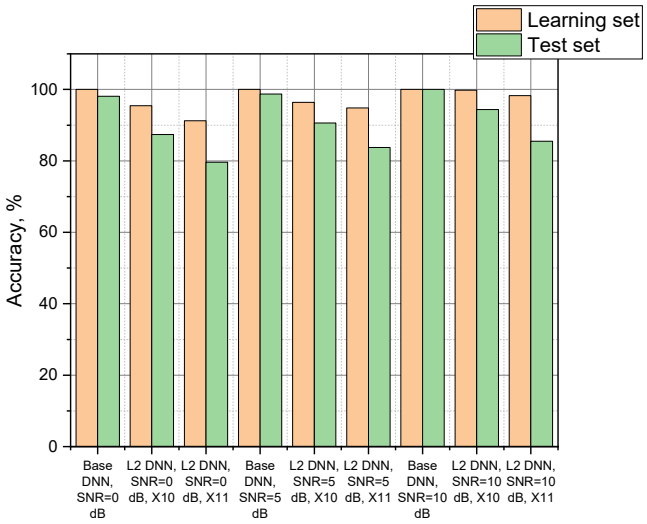


Рисунок 4.7 – Залежність достовірності автентифікації від коефіцієнта L_2-регуляризації нейромережевого класифікатора і SNR вхідного мовленнєвого матеріалу

Втім, спробуємо здійснити регуляризацію глибокої мережі відштовхуючись від її цільового призначення та враховуючи, що перший і другий приховані шари узагальнюють вхідні значенням на низькому рівні, а останній прихований шар – на високому. Узагальнимо ваги міжнейронних зв'язків між вхідним і першим прихованим шарами множиною $IH1$, між першим і другим прихованими шарами – множиною $H12$, між другим і третім прихованими шарами – множиною $H23$, між третім прихованим і вихідним шарами – множиною $H3O$. Ініціалізуємо для кожної мно-

жини відповідний фактор важливості узагальнивши їх вихідні значення множиною $T = \{t_{IH1}, t_{H12}, t_{H23}, t_{H3O}\} = \{0{,}10; 0{,}15; 0{,}15; 0{,}40; 0{,}2\}$ та встановимо коефіцієнт зміни фактора важливості $\Delta t = 0{,}05$.

Здійснимо навчання нейромережі. Далі в порядку $H23 \to H12 \to IH1 \to H3O$ виконуватимемо таки дії:

1) розраховуємо $\overline{\Delta}$ – середнє відхилення значень міжнейронних зв'язків між відповідними шарами до і після навчання;

2) розраховуємо значення порогу зрізання θ як результат добутку параметра $\overline{\Delta}$ із відповідним фактором важливості з множини факторів T;

3) в аналізованій множині міжнейронних зв'язків прирівнюємо до нуля значення всіх елементів, поточне значення яких менше порогу зрізання θ;

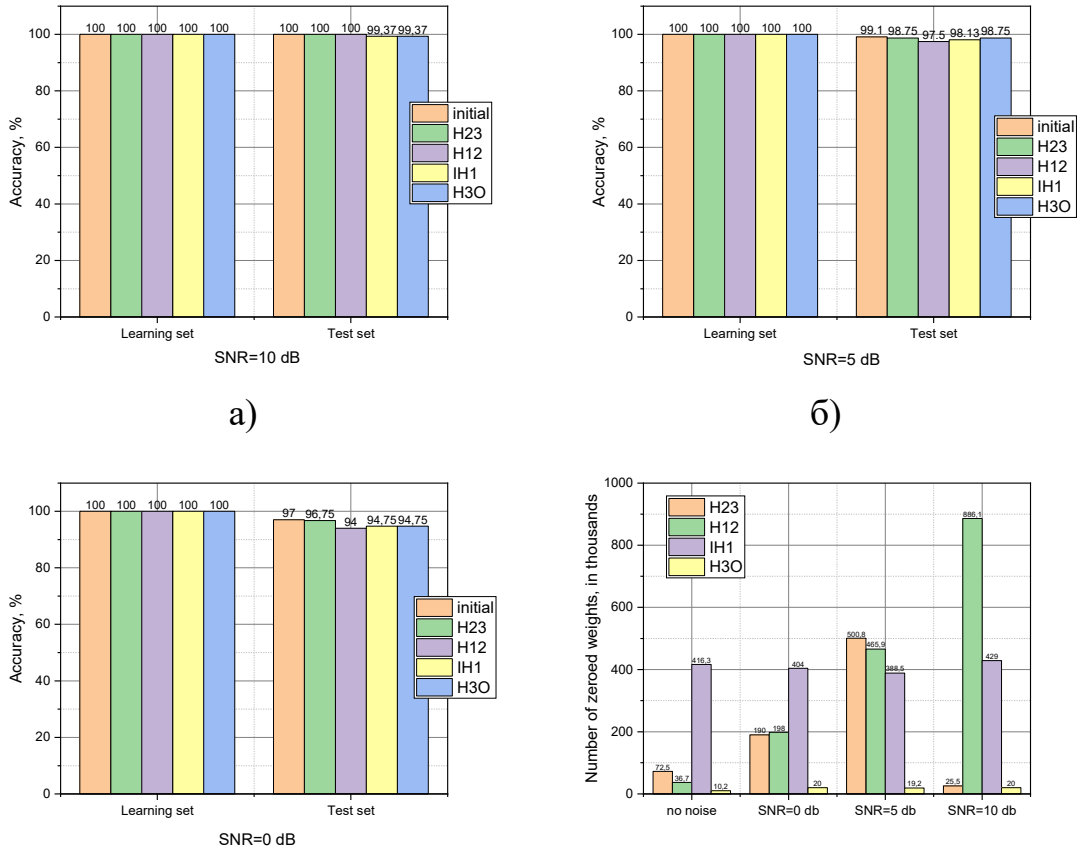
4) контролюємо вплив здійснених змін на достовірність процесу класифікації і якщо падіння достовірності перевищило допустиме значення, то відновлюємо вихідні значення в аналізованій множині міжнейронних зв'язків, зменшуємо відповідний фактор важливості з множини T на значення Δt та повертаємося до п. 1. Якщо ж падіння достовірності процесу класифікації виявилося прийнятним, або поточне значення фактора важливості виявилося рівним нулю, то переходимо до аналізу наступної множини ваг міжнейронних зв'язків з послідовності $H23 \to H12 \to IH1 \to H3O$;

5) процес закінчується, коли всю послідовність $H23 \to H12 \to IH1 \to H3O$ пройдено.

Доведемо емпірично адекватність запропонованої методики регуляризації, в якому враховано специфіку розв'язання задачі АСГ глибоким нейромережевим класифікатором. Результати досліджень наведено на рис. 4.8.

Результати, представлені на рис. 4.8а–4.21в, описують залежність достовірності автентифікації суб'єкта за мовленнєвим матеріалом із рівнем відношення «сигнал»/«шум» 10, 5, 0 дБ, відповідно, глибоким нейромережевим класифікатором, ваги міжнейронних зв'язків якого після навчання модифікувалися за авторською процедурою регуляризації. Видно, що регуляризація ваг зв'язків між другим і третім прихованими шарами фактично не впливає на достовірність

класифікації, що можна пояснити ефективністю проміжного узагальнення характеристичних параметрів на другому шарі. Найпомітніше падіння спостерігається після регуляризації ваг між вхідним і першим прихованим шарами, адже характеристичні параметри ще фактично не узагальнювалися нейромережею.



а) б)

в) г)

Рисунок 4.8 – Вплив запропонованої методики регуляризації на перебір процесу класифікації у задачі АСГ глибоким нейромережевим класифікатором

Зауважимо, що запропонована процедура дозволяє здійснювати регуляризацію множин міжнейронних ваг незалежно, тому можна одностайно рекомендувати запроваджувати цю процедуру до множини $H23$, а до множин $H12$, $H3O$ – за потребою. Зиск від запропонованої процедури регуляризації можна оцінити за результатами, представленими на рис. 4.8г. Видно, що з позиції зменшення ресурсозатратності:

- здійснювати регуляризацію множини $H3O$ недоцільно;

- доцільність регуляризації множини $H23$ зростає із спаданням рівня відношення «сигнал»/«шум»;
- стабільний ефект дає регуляризація множини $IH1$, що в зіставленні з інформацією на рис. 4.8а–4.21в, вказує на неоднорідність інформативності елементів вектора характеристичних параметрів для першого набору;
- доцільність регуляризації множини $H12$ зростає із зростанням рівня відношення «сигнал»/«шум».

Отже, запропонована процедура регуляризації дозволяє оптимізувати ваги міжнейронних зв'язків, зменшивши їх кількість на 15–20 % при незначному падінні достовірності класифікації. В цілому глибока нейромережа показала зіставні результати із результатами, продемонстрованими у додатку Ж машиною опорних векторів.

Продемонстровані на рис. 4.8 якісні характеристики глибокої нейромережі зумовлюють доцільність дослідження використання в якості класифікатора в процесі АСММШ також і згорткової глибокої нейромережі [319–321]. Цей клас нейромереж працює із візуальними вхідними даними, що зумовлює спектральне представлення аналізованих фреймів мовленнєвих сигналів у просторі відповідних наборів характеристичних параметрів, описаних у додатку Ж. Хоча згорткова нейромережа і не потребує ретельного оброблювання вхідного зображення, все ж від його інформативності залежить як архітектура нейромережі, так і достовірність класифікації. Спектрограму можна вважати зображенням із структурною надлишковістю квазіперіодичного походження, тому для її компактнішого представлення доцільно використати банк фільтрів Габора [45]. Смугові фільтри Габора переважно використовують у задачах визначення крайових ефектів зображень. Вони дозволяють охарактеризувати діапазон частот сигналу у визначеному часовому проміжку x і напрямку y. Імпульсна передатна характеристика фільтра Габора є добутком гаусівської і гармонічної функцій:

$$Gb[x,y] = K\left(2\pi\sigma_x\right)^{-0,5}\exp\left(-x^2\left(2\pi\sigma_x\right)^{-1}\right)\left(2\pi\sigma_y\right)^{-0,5}\times \qquad (4.64)$$

$$\times \exp\left(-y^2\left(2\pi\sigma_y\right)^{-1}\right)\cos\left(2\pi f_0 x+\phi\right),$$

де f_0 і φ – частота і фаза, відповідно. В процесі фільтрації відбувається згортка у часовому просторі вхідного сигналу, в якості якого може виступати будь-яке зображення im, наприклад, одна із спектрограм з рис. Ж.5, і фільтра Габора Gb. При переході від часового простору до частотного операцію згортки замінюють множенням: $F(im\cdot Gb)=F(im)\cdot F(Gb)$, де $F(\ldots)$ – перетворення Фур'є. $F(Gb)$ – це гаусівський сигнал, екстремальне значення якого розташоване на центральній частоті фільтра f_0. Множення у частотному просторі підсилює амплітуди близьких до центральної частоти фільтра частот вхідного сигналу на тлі затухання амплітуд решти частот. Ефективність фільтрів Габора здебільшого визначається значеннями параметрів висоти σ_x ї ширини σ_y гаусівської компоненти виразу (4.64). Емпірично виявлено, що оптимальна чіткість фільтра при оброблюванні зображень спектрограм досягається при $\sigma_x=\left(2\pi f_0\right)^{-0,5}$ і $\sigma_y=1,5\sigma_x$.

Результати фізіологічних експериментів показали, що нейрони у первинній слуховій корі головного мозку ссавців чутливі до певних спектрально-темпоральних структур, названих спектрально-темпоральними рецептивними полями [214–217], які є функціональними дескрипторами лінійного оброблювання змінних акустичних спектрів слуховою системою. Отриману на основі результатів цих досліджень спектрально-темпоральну модель сприйняття звукових сигналів використовують при розпізнаванні мови і автентифікації суб'єктів за голосом. Дослідження [45, 51] дозволили ідентифікувати характеристики банку фільтрів із спектральною, темпоральною та спектрально-темпоральною модуляціями, які у першому наближенні описують шаблони збудження нейронів для типових спектрально-темпоральних складових вхідних сигналів. Зокрема, рецептивні поля аналітично описано множиною одиночних пульсацій із синусоїдально-модульованими спектральними профілями у частотно-часовому просторі:

$$O\left[n_t,k\right]=\Delta A\sin\left(2\pi\omega_{n_t}n_t+2\pi\omega_k k+\Phi\right). \tag{4.65}$$

Екстремальні значення функції $O[n_t,k]$ характеризуються значеннями темпоральної і спектральної циклічних частот ω_n і ω_k, відповідно, на різних амплітудних рівнях ΔA. На основі виразу (4.65), опис вхідного сигналу в спектрально-темпоральних полях формалізуємо процесом фільтрації виду

$$O[n_t,k] = STRF[n_t,k] * x[n_t,k], \tag{4.66}$$

тобто у довільний момент часу n_t і на частоті k реакція нейронів $O[n_t,k]$ описується згорткою СТРП-фільтра із динамічним спектром вхідного сигналу в околі моменту часу і частоти $x[n_t,k]$. За своїм функціональним призначенням СТРП-фільтр є близьким до фільтра Габора, що дозволяє, врахувавши вираз (4.64), описати перший виразом

$$STRF[n_t,k] \cong Gb[n_t,k] = s[n_t,k] \cdot h[n_t,k], \tag{4.67}$$

де $s[n_t,k] = \exp(i\omega_n n + i\omega_k k)$ – комплексна синусоїда з темпоральною циклічною частотою ω_n і спектральною циклічною частотою ω_k, а $h[n_t,k] = 0{,}25\left(1-\cos\left(2\pi n_t\left(W_{n_t}+1\right)^{-1}\right)\right)\left(1-\cos\left(2\pi k\left(W_k+1\right)^{-1}\right)\right)$ – віконна функція Хенінга, в якій параметри W_n і W_k визначаються як $W_{n_t} = 3{,}5\pi\left|\omega_{n_t}\right|^{-1}$ і $W_k = 3{,}5\pi\left|\omega_k\right|^{-1}$, відповідно.

Згідно з виразом (4.67), при заданих значеннях спектральної і темпоральної циклічної частоти інтенсивність і нахил функції Габора визначатиметься кількістю гармонік у вхідному сигналі. Синтезований для досліджень банк фільтрів Габора включає 59 фільтрів, налаштованих на різні темпоральні та спектральні циклічні частоти (темпоральні циклічні частоти ω_n, Гц: 0; 1,9; 3,9; 6,2; 9,9; 15,7; 25; спектральні циклічні частоти ω_k, циклів/октаву: –0,25; –0,1224; –0,0424; –0,0293; 0; 0,0293; 0,0424; 0,1224; 0,25, що візуалізовано на рис. 4.9 [51].

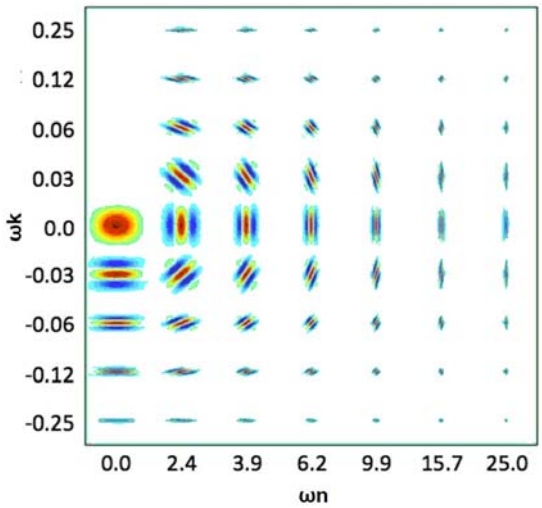


Рисунок 4.9 – Частотна роздільна здатність синтезованого банку фільтрів Габора.

Візуальний приклад оброблювання синтезованим банком фільтрів Габора спектрограми вхідного мовленнєвого сигналу наведено на рис. 4.10. Фільтри із високою циклічною частотою (вузькі фільтри) опрацьовують швидкозмінювані області спектрограми, а фільтри із низькою циклічною частотою (широкі фільтри) – стабільніші її області, відповідно. На виході банку вузьких та широких фільтрів Габора із відповідними центральними спектральними циклічними частотами утворюється динамічний параметричний опис спектрограми вхідного мовленнєвого сигналу.

Для зменшення імовірності виникнення ефекту перенавчання, властивого згортковій, як і будь якій іншій глибокій нейромережі, скористаємося розрідженим методом головних компонентів [225] при формуванні еталонної навчальної бази СТРП-характеристичних параметрів. Цільову функція методу із L_1-штрафною нормою опишемо виразом

$$\max v^T \Sigma_x v - \rho\left(\|v\|_1^2\right), \tag{4.68}$$

де $\|v\|_2 = 1$; ρ – невід'ємний параметр управління розрідженістю головного вектора; Σ_x – емпірична коваріаційна матриця, розрахована за результатами спостережень $\{x_i\}$; v – головний вектор.

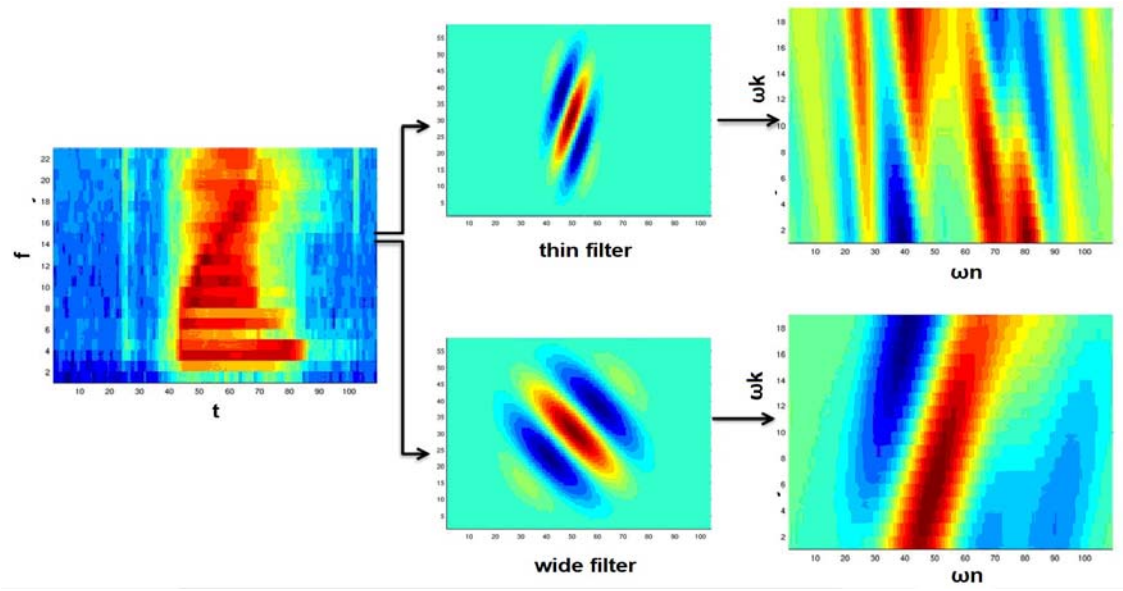


Рисунок 4.10 – СТРП-представлення спектрограми мовленнєвого сигналу: вище: результат функціонування вузького фільтра ($\omega_n = 6{,}2$ Гц, $\omega_k = 0{,}03$ ц./о.); нижче: результат функціонування широкого фільтра ($\omega_n = 2{,}4$ Гц, $\omega_k = 0{,}03$ ц./о.)

Застосувавши сингулярне перетворення, представимо вираз (4.68) у вигляді

$$\max Tr\left(\Sigma_x, vv^T\right) - \rho\left(I^T \left| vv^T \right| I\right), \tag{4.69}$$

де $\|v\|_2 = 1$, а L_1-штрафна норма описується виразом

$$\rho\left(I^T \left| vv^T \right| I\right) = \min_U Tr\left(Uvv^T\right), \tag{4.70}$$

де $-\rho \le U_{ij} \le \rho$. Узагальнимо представлення цільової функції (4.68), врахувавши вирази (4.69), (4.70),

$$\max \min Tr\left(\left(\Sigma_x + U\right)vv^T\right), \tag{4.71}$$

де $\|v\|_2 = 1$; $-\rho \le U_{ij} \le \rho$. Нарешті, зорієнтуємо вираз (4.71) на кінцевий результат:

$$\max \min v^T\left(\Sigma_x + U\right)v, \tag{4.72}$$

або

$$\min_U \lambda_{\max}\left(\Sigma_x + U\right), \tag{4.73}$$

де $\|v\|_2 = 1$; $-\rho \le U_{ij} \le \rho$; $\lambda_{\max}\left(\sum_x + U\right)$ – максимальне власне значення комплексної матриці $\left(\sum_x + U\right)$. З виразу (4.73) видно, що задача факторного аналізу зводиться до пошуку мінімального з найбільших власних значень коваріаційної матриці сигналу із доданою матрицею шуму. Для розв'язання такої задачі оптимізації скористаємося методом розширення лагранжіана [322] і обмежимося обчисленням лише головного розрідженого власного вектора, нульовим значенням у якому відповідатимуть елементи СТРП-характеристичних параметрів, які варто прибрати із еталонної навчальної бази.

В описаній виразом (4.66) операції згортки задіяно СТРП-фільтр із параметрами ω_n і ω_k. Однотипну по суті операцію здійснює і перший, згортковий, шар згорткової нейромережі. Ця обставина зумовила інтеграцію описаних виразом (4.67) СТРП-фільтрів у топологію згорткової нейромережі із заміною ядер згортки відповідними СТРП-фільтрами із керованими параметрами ω_n і ω_k. Архітектуру модифікованої таким чином нейромережі представлено на рис. 4.11.

Доцільність інтеграції банку СТРП-фільтрів у нейромережу пояснюється можливістю автоматичного налаштування параметрів фільтрів у процесі її навчання. Технологічно описану модифікацію забезпечено використанням на першому, згортковому, шарі нейромережі нейронів із лінійними функціями активації та встановленням параметра перекривання ядер рівним нулю. Після таких модифікацій згортковий шар стає передатною функцією банку СТРП-фільтрів, параметри ω_n і ω_k яких обчислюються за виразами $2K_m + 1$ і $2N_m + 1$, відповідно, де m – номер фільтра в банку. Аналітично описати процес інтеграції банку СТРП-фільтрів у згорткову нейромережу можна виразом

$$W_m = h_m[n_t, k] = lin\left(\sum_{i=-N_m}^{N_m} \sum_{j=-K_m}^{K_m} Gb_m(-i,-j) \cdot x(n_t + i, k + j)\right) = \\ = Gb_m[n_t, k] * x[n_t, k], \tag{4.74}$$

де W_m – вхідні ваги нейромережі, функція $h_m[n_t, k]$ описує нейрон, який сприймає сигнал з виходу m-го СТРП-фільтра, рецептивне поле якого з матрицею

з $2K_m+1$ смуг по вертикалі на $2N_m+1$ відліків по горизонталі сприймає відповідну смугу спектрограми поточного фрейма $x(n,k)$.

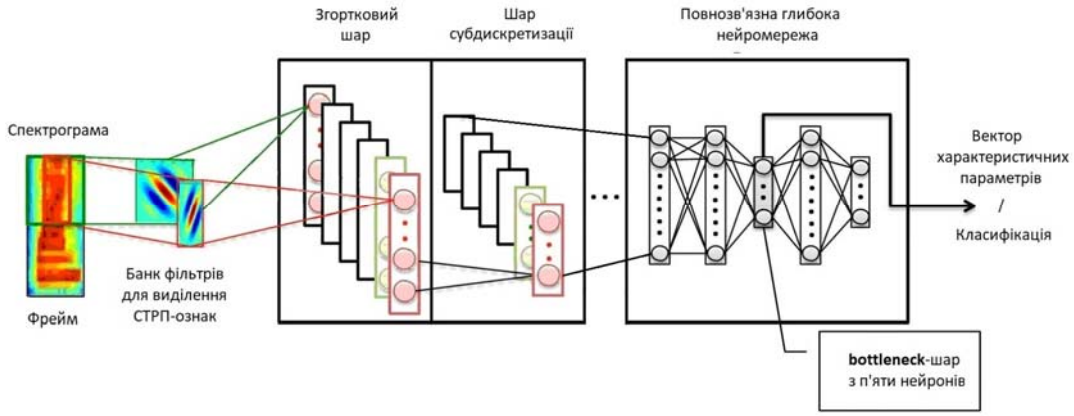


Рисунок 4.11 – Модифікована згорткова нейромережа з СТРП-вхідним шаром і можливістю екстрагування характеристичних параметрів.

Як видно з рис. 4.11, в топології модифікованої згорткової нейромережі передостаннім прихованим шаром повнозв’язного фрагмента є bottleneck-шар, кількість нейронів у складі якого суттєво менша від кількості нейронів на решті прихованих шарів глибокої нейромережі. Після навчання нейромережі для автентифікації цільового суб’єкта значення ваг bottleneck-шару можна використовувати в якості вектора характеристичних параметрів, утворивши таким чином п’ятий набір характеристичних параметрів.

Як і попередню, модифіковану згорткову нейромережу реалізовано в фреймворку CNTK. Повнозв’язний фрагмент синтезованої нейромережі включав три прихованих шари із 1000-ю нейронів на кожному і третій за порядком bottleneck-шар із 25-ма нейронами. Загальна кількість керованих параметрів нейромережі склала величину понад 3,5 мільйони. Для прискорення навчання нейромережі початкові значення керованих параметри отримано за допомогою переднавчання із використанням обмежених машин Больцмана [323–326], а подальше навчання відбувалося за алгоритмом зворотного поширення похибки із коефіцієнтом швид-

кості навчання рівним 0,008 і використанням значення перехресної ентропії в якості функції втрат.

При синтезі згорткового шару передбачалося, що він передаватиме інформацію з виходів 120 СТРП-фільтрів, кожен з яких накривав 9 частотних смуг і 15 послідовних відліків у зображенні вхідної спектрограми, при цьому розмірність ядер СТРП-фільтрів знаходилася у діапазоні $7 \div 99 \times 7 \div 40$, відліків/смуг, для часового і частотного просторів, відповідно.

Отже, узагальнимо дослідження нейромережевих класифікаторів здійснивши комплексний експеримент, у якому порівняємо їх результативність із відповідними показниками, продемонстрованими машинами опорних векторів у додатку Ж. Для експериментів скористаємося все тими ж наборами множин фонограм, утвореними на основі бази NOIZEUS: «без шуму», «шум Car, SNR=0 дБ», «шум Car, SNR=5 дБ», «шум Car, SNR=10 дБ», …, «шум Train station, SNR=0 дБ», «шум Train station, SNR=5 дБ», «шум Train station, SNR=10 дБ». Весь мовленнєвий матеріал сегментовано на фрейми тривалістю 20 мс із перекриттям у 10 мс. Порівнюватимемо достовірність процесу автентифікації суб’єкта за мовленнєвим матеріалом із рівнем відношення «сигнал»/«шум» 0, 5, 10 дБ:

- SiVM+Kbcos+Gall: машиною опорних *i*-векторів із функцією-ядром $K_{B\cos}$ і розв’язувальним правилом G_{all}, яка виявилася кращою з-поміж претендентів, результати дослідження яких продемонстровано на рис. Ж.10;
- DNN: глибокою нейромережею, результати проміжного дослідження якої наведено на рис. 4.8;
- mCNN: модифікованою згортковою нейромережею із СТРП-вхідним шаром, архітектуру якої зображено на рисунку 4.11;
- BN+SVM: машиною опорних векторів SiVM+Kbcos+Gall, на вхід якої замість *i*-векторів подаватимуться вектори з п’ятого набору характеристичних параметрів, які є вагами bottleneck-шару модифікованої згорткової нейромережі.

На рис. 4.12а, б, в, г до мовленнєвого матеріалу без шуму підмішувалися шуми типу «Car», «Street», «Airport», «Train station», відповідно.

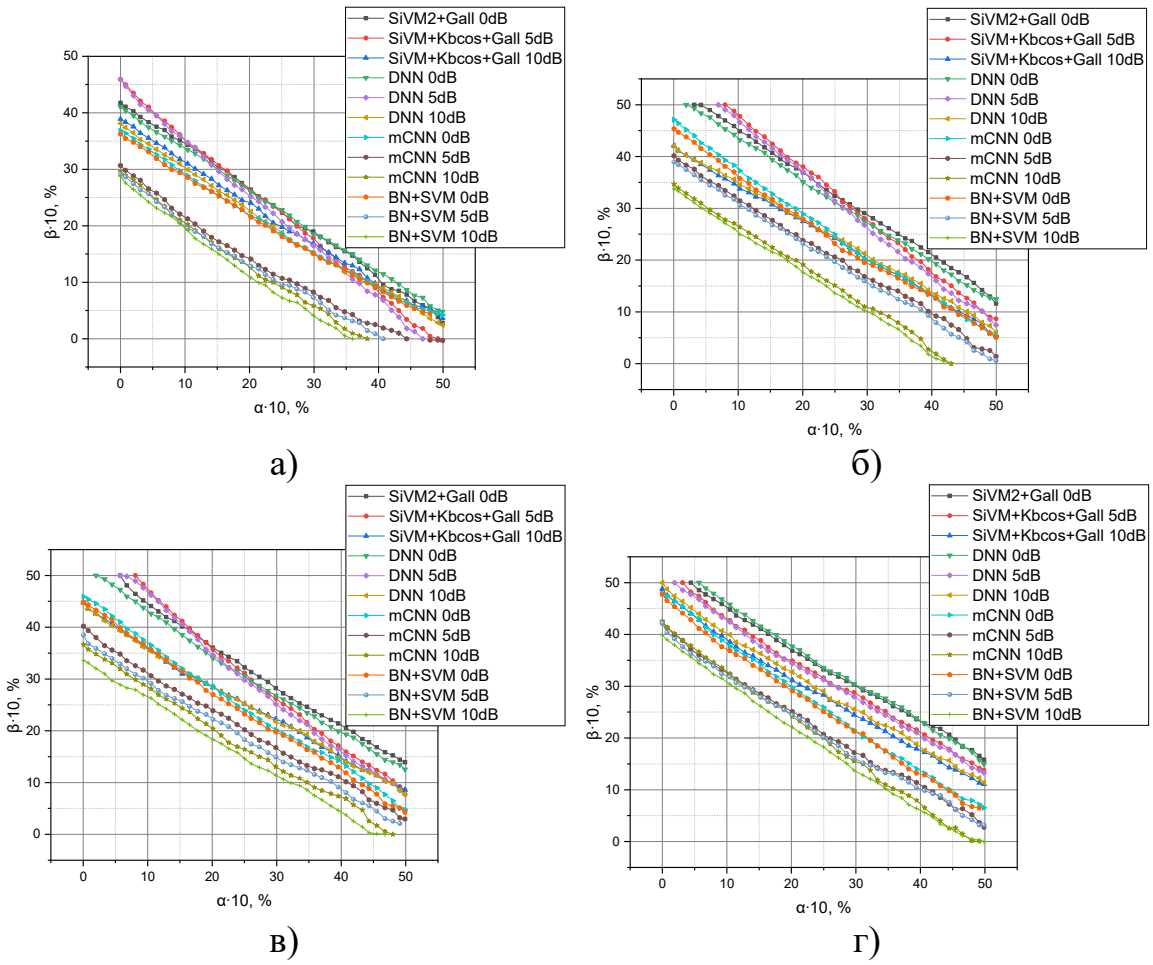


Рисунок 4.12 – Достовірність класифікації в задачі АСММШ, продемонстрована машинами опорних векторів і глибокими нейромережами.

Слід відзначити, що це дослідження є найбільш ґрунтовним серед проведених. Машина опорних векторів SiVM+Kbcos+Gall приймає рішення на основі аналізу вхідних *i*-векторів, утворених як результат опису параметризованих четвертим набором характеристичних параметрів емпіричних мовленнєвих сигналів відповідними моделями СГР, утворених адаптацією універсальної фонової моделі до цільових суб’єктів. Глибокі нейромережі DNN і mCNN приймають рішення на основі опису параметризованих третім набором характеристичних параметрів емпіричних мовленнєвих сигналів у вигляді векторів значень і спектрограм, відповідно. Ці класифікатори синтезують характеристичні параметри високого рівня самі в процесі навчання. Машина опорних векторів BN+SVM приймає рішення на основі опису параметризованих п’ятим набором характеристичних параметрів емпіричних мовленнєвих сигналів. Цей набір є продуктом bottleneck-шару модифіко-

ваної згорткової нейромережі. Фактично в класифікаторі BN+SVM поєднано властиву машинам опорних векторів швидкість, однозначність і математичну строгість прийнятого рішення із властивою нейромережам нечутливістю до шумів у вхідному сигналі і здатністю самостійно синтезувати характеристичні параметри високого рівня в процесі навчання.

З наведених на рис. 4.12 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 підрозділі 4.1 математичний апарат для компенсування шумів у 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.

За рекомендацією колективу відділу розпізнавання та синтезу звукових образів Міжнародного науково-навчального центру інформаційних технологій та систем НАНУ та МОНУ застосуємо описані в розділах 2–4 моделі і методи в класичній задачі «text-dependent speaker verification», яка найбільш близька семантично до задачі АСГ. Центральним питанням у такому дослідженні є вибір відомого загальнодоступного і репрезентативного мовленнєвого корпусу. В результаті інформаційного пошуку знайдено два мовленнєвих корпуси, які задовольняють ці критерії – RedDots dataset і CSTR VCTK Corpus.

Перший із згаданих корпусів є основним результатом міжнародного проекту RedDots, здійснюваного під патронажем Міжнародної асоціації мовленнєвої комунікації INTERSPEECH. Метою проекту, доступного за URL https://sites.google.com/site/thereddotsproject/, є розпізнавання мовців за дискретизованим засобами мобільної комунікації короткотривалим мовленнєвим сигналом із високою фонетичною варіативністю. Англомовний корпус RedDots dataset сформовано на основі мовленнєвого матеріалу, отриманого від 62 мовців (49 – чоло-

вічої, 13 – жіночої статі) з 21 країни світу. За сценарієм проекту зареєстрований мовець кожен тиждень протягом року виголошував запропоновану організаторами проекту короткотривалу контрольну фразу, з’єднавшись власним засобом мобільної комунікації із сайтом RedDots. Запис фонограм із дискретизованим мовленнєвим сигналом здійснювався на сервері проекту. Кожна фонограма сегментувалася на відрізки тривалістю 3 с, із яких згодом комбінувалися чотири бази мовленнєвих записів, з яких для тестування систем текстозалежної верифікації мовців призначено першу, яка містить записи із однаковим фонетичним вмістом для всіх мовців. Фонограми зберігаються у файлах формату PCM (моно, частота дискретизації – 16 кГц, розрядність квантування – 16 біт).

Корпус CSTR VCTK, вільно доступний за URL https://datashare.is.ed.ac.uk/handle/10283/2651 , сформовано колективом дослідницького центру мовленнєвих технологій Університету Единбургу під час роботи над фреймворком для клонуванням голосу Voice Cloning Toolkit. При формуванні англомовного корпусу CSTR 109 мовців із різних місцевостей Великобританії зачитували до 400 речень, вибраних із газет видавництва Herald&Times Group. Всі записи здійснювалися єдиним всеспрямованим мікрофоном DPA 4035 із частотою дискретизації 96 кГц і розрядністю квантування 24 біти та зберігалися у файли формату WAV (моно, частота дискретизації – 48 кГц, розрядність квантування – 16 біт). Файли в корпусі впорядковано на ідентифікаторами мовця і речення, що дозволяє використовувати корпус, зокрема, для тестування систем текстозалежної верифікації мовців.

Зауважимо, що виголошення мовленнєвого матеріалу, фонограми із записом якого увійшли у згадані вище корпуси, відбувалося в умовах мінімізації шумів оточення джерела мовленнєвого сигналу. Для спрощення відтворюваності результатів здійснюваного експерименту використовуватимемо вміст корпусів безпосередньо, без додавання шумів, розбиваючи доступний для кожного мовця мовленнєвий матеріал у пропорції 70 % / 30 % на навчальну і тестувальну вибірки, відповідно.

Технологічно здійснюваний експеримент близький із описаним у додатку Ж. Весь мовленнєвий матеріал корпусів RedDots і CSTR сегментуємо на фрейми тривалістю 20 мс із перекриттям у 10 мс. Кожен фрейм мовленнєвого матеріалу опишемо трьома наборами векторів характеристичних параметрів у парадигмі уточненої детермінованої моделі ІГМС, описаної у підрозділі 2.3. Кожен фрейм мовленнєвого сигналу описуватиметься:

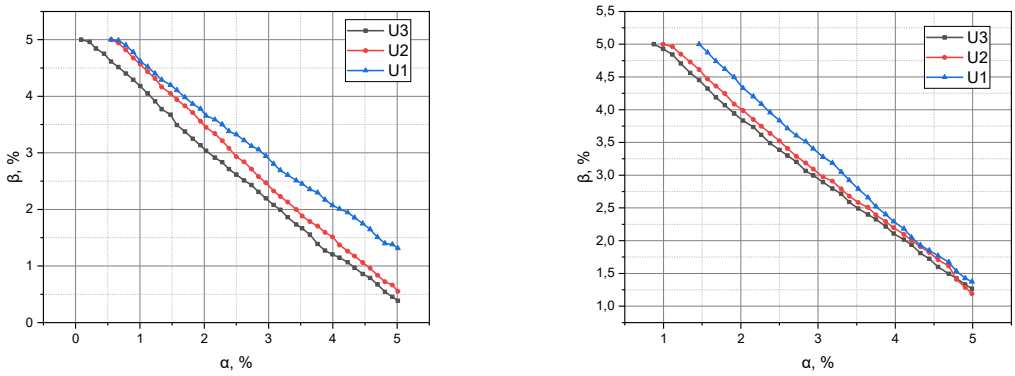
- у першому наборі – 7-розмірним вектором, який включатиме 7 значень енергії сигналу на частоті основного тону і шести її гармоніках: $U_1 = \{u_0, u_1, \ldots, u_6\}$;
- у другому наборі – 10-розмірним вектором, який включатиме 10 значень енергії сигналу на частоті основного тону і дев'яти її гармоніках: $U_2 = \{u_0, u_1, \ldots, u_9\}$;
- у третьому наборі – 14-розмірним вектором, який включатиме 14 значень енергії сигналу на частоті основного тону і дванадцяти її гармоніках: $U_3 = \{u_0, u_1, \ldots, u_{12}\}$.

Якщо в описуваному фреймі з причини фонетичного наповнення чи обмеженої тривалості необхідна кількість гармонік основного тону не спостерігатиметься, то значення відповідних елементів вектора характеристичних параметрів заповнюватиметься нулями.

Для вмісту кожного корпусу окремо сформуємо три 1024-компонентні універсальні фонові моделі, навчені протягом 200 ітерацій ЕМ-методу на всьому матеріалі відповідних навчальних вибірок, всі фрейми яких параметризовано одним із трьох наборів характеристичних параметрів. Далі навчені універсальні фонові моделі адаптуватимемо до цільових мовців МАР-методом для утворення індивідуальних 8-ми компонентних моделей СГР. Відповідно до обраного набору характеристичних параметрів, для кожного цільового мовця з відповідного корпусу створено по три адаптованих моделі суміші. Проведемо дослідження із моделлю процесу верифікації, представленою на рис. 1.3, для вибору оптимального набору характеристичних параметрів, використавши мовленнєвий матеріал корпусів RedDots і CSTR, та скориставшись для прийняття рішень машиною опорних *i*-

векторів із функцією-ядром $K_{B\cos}$ і розв'язувальним правилом G_{all}, яка виявилася кращою з-поміж претендентів, результати дослідження яких продемонстровано на рис. Ж.10. Результат дослідження представимо відповідними DET-кривими на рис. 4.13, де результати на рис. 4.13а характеризуватимуть матеріали корпусу RedDots, а результати на рис. 4.13б – матеріали корпусу CSTR.

Результати, представлені на рис. 4.13 дозволяють стверджувати, що при сталій структурі системи верифікації мовців, достовірність верифікації зростає із збільшенням кількості елементів у векторах характеристичних параметрів, що описують фрейми мовленнєвих сигналів. Водночас видно, що розрив не надто суттєвий, що можна пояснити розрідженістю векторів характеристичних параметрів, адже основний тон здебільшого спостерігається у вокалізованих відрізках фонограми мовленнєвого сигналу, тоді як мовленнєвий матеріал корпусів не оптимізовано щодо цього критерію. Варто відзначити, що на відміну від мовленнєвого матеріалу корпусу RedDots, мовленнєвий матеріал корпусу CSTR записувався в лабораторних умовах, тобто за умов фактичної відсутності шумів навколишнього оточення, в той же час, обсяги корпусу CSTR як за кількістю мовців, так і за загальною тривалістю їх мовленнєвих матеріалів, майже вдвічі перевищують аналогічні показники корпусу RedDots. Враховуючи ці обставини відзначимо, що досліджувана система показала нижчий рівень показників якості верифікації для матеріалів корпусу CSTR, тобто запропонований метод параметризації мовленнєвих сигналів зазнає меншої вразливості від незначних шумів у мовленнєвому сигналі, тоді як при суттєвому зростанні кількості мовців, що верифікуються, до вибору фонетичного складу парольної фрази слід підходити раціонально. В цілому, продемонстровані на рис. 4.13 результати дозволяють однозначно визнати досліджувану систему верифікації мовців функціональною із потенціалом для можливого удосконалення.



а) б)

Рисунок 4.13 – Результативність авторської концепції розв’язання задачі «text-dependent speaker verification» при описі вмісту корпусів RedDots і CSTR уточненою моделлю ІГМС.

Як вже неодноразово зазначалося, недоліком всіх вже описаних у додатку Ж і підрозділі 4.2 класифікаторів є суттєва ресурсозатратність процесу навчання. Описані у додатку Ж процеси бустінгу еталонних навчальних даних та синтезу проекційної функції-ядра машини опорних векторів дозволили в поєднанні запропоновувати математичний апарат для синтезу простого класифікатора найкращих оцінок. Під терміном «найкраща оцінка» розумітимемо ідентифіковану дискримінантну функцію, яка найкраще описує вміст даної еталонної навчальної бази. Відповідно, можна представити навчання як ітеративний процес ідентифікації таких функцій. На кожній ітерації з множини конкуруючих варіантів обирається дискримінантна функція, яка забезпечує найкраще розділення класів, а вміст еталонної бази зрізується, тобто з неї вилучаються елементи, які обрана функція найкращої оцінки класифікувала вірно. Ітеративний процес продовжується, якщо після поточної операції зрізання отримано не пусту еталонну базу, обсяг якої перевищує встановлене гранично допустиме обмеження. Детальне дослідження методу найкращих оцінок в контексті прийняття рішень в задачі АСММШ представлено у додатку З.

Висновки до четвертого розділу

1. У найперспективніших на даний час системах автентифікації суб'єкта за голосом використовується математичний апарат сумішей гаусівських розподілів із їх узагальненням у вигляді універсальної фонової моделі. В процесі експлуатації таких систем проявися факт відчутного зниження достовірності автентифікації суб'єктів за мовленнєвим матеріалом із шумом, здебільшого, адитивним. Втім, математичному апарату сумішей гаусівських розподілів у контексті їх застосування в задачах машинного навчання поряд із суттєвою ресурсозатратністю властива гнучкість, що обумовило проведення досліджень у напрямку пошуку ефективних методів компенсування шумів у мовленнєвому сигналі, вживаному для автентифікації суб'єкта за голосом.

2. В основу досліджень покладено дві базових концепції. Перша полягає у формалізації процесу адаптації моделі суміші гаусівських розподілів, навченої на параметризованому мовленнєвому матеріалі без шуму, до впливу детермінованих за видом і енергією шумів. Друга передбачає пошук у моделях сумішей, навчених на параметризованих базах фонограм із мовленнєвим матеріалом без шуму та із шумом, спільних ознак, які характеризують індивідуальність голосу, але не зазнають впливу шумів – так званих, ознак високого рівня.

3. При спектральному представленні мовленнєвого сигналу спотворення значень відповідних характеристичних параметрів під впливом шумів моделюється операціями додавання або множення корисного мовленнєвого сигналу із стохастичним сигналом шуму. Якщо характеристичні параметри узагальнено моделлю СГР, то адитивні і мультиплікативні шуми обумовлюють, відповідно, варіативність значень дисперсій і векторів середніх значень всіх компонентів моделі суміші. Параметризувавши цю варіативність множиною відповідних компенсувальних змінних, їх значення можна ідентифікувати розв'язавши задачу мінімізації критерію середньоквадратичної похибки методом максимізації функції правдоподібності.

4. Виявилося, що при високому рівні відношення «сигнал»/«шум» у емпіричному мовленнєвому сигналі компенсувальні змінні можна вважати детермінова-

ними, а їх значення характеризуються усередненою оцінкою близькості значень параметрів моделей СГР, які окремо описують вміст еталонних баз параметризованих фонограм мовленнєвих сигналів із шумом та без шуму, відповідно. При низькому рівні відношення «сигнал»/«шум» адекватно компенсувати шуми у емпіричному мовленнєвому сигналі вдалося лише визнавши компенсувальні змінні стохастичними із відповідним перетворенням методу оцінювання їх значень. Враховуючи потенційний детермінований характер шумів, формалізовано метод оцінювання компенсувальних змінних за умови, що вміст еталонної бази фонограм із шумом додатково сегментовано за видами шумів.

5. Аналітично описано концепцію інтеграції еталонної бази спектральних характеристичних параметрів, екстрагованих із фонограм мовленнєвого матеріалу без шуму, із еталонною базою спектральних характеристичних параметрів, екстрагованих з фонограм мовленнєвого матеріалу із шумом, у єдину агреговану еталонну базу. Перевагою такого підходу стало автоматичне оцінювання значень компенсувальних змінних в процесі параметричного синтезу відповідної моделі суміші. Така концепція дозволяє не тільки скоротити обсяг задіяних обчислювальних ресурсів, адже мовленнєвий матеріал утвореної агрегованої еталонної бази описується однією, хоч і комплексною, моделлю СГР, а й орієнтувати отриману модель суміші на компенсування конкретного виду шуму, контролюючи вміст еталонної бази із параметризованим мовленнєвим матеріалом із шумом.

6. При великому обсязі навчальних даних ненульовою є імовірність виникнення кореляції між об’єднаними векторами характеристичних параметрів у агрегованій еталонній базі. Якщо описана ситуація реалізується, то навчена на таких даних модель суміші одночасно із компенсуванням цільових типів шумів у емпіричному мовленнєвому сигналі привноситиме у його результуючий параметричний опис динамічні спотворення і занадто згладжуватиме спектр підсумкового сигналу. Враховуючи спектральну природу характеристичних параметрів, об’єднуваних у вектори при формуванні агрегувальної еталонної бази, формалізовано процес їх доповнення динамічними спектральними характеристиками, збільшуючи таким чином роздільну здатність параметричного опису.

7. Формалізовано теоретичні і практичні аспекти математичного моделювання процесу автентифікації суб’єкта за мовленнєвим матеріалом із шумом у парадигмі породжувальних і дискримінаційних імовірнісних моделей. Підтверджено помітний вплив порогу прийняття рішень у класифікаторі машини опорних супервекторів та тривалості парольного мовленнєвого сигналу на достовірність цільової моделі. Емпірично доведено, що збільшення тривалості парольного мовленнєвого сигналу понад 2 хв. не веде до помітного зростання достовірності цільової моделі, але при зростанні цієї тривалості від 2 с до 2 хв. імовірності похибок першого і другого роду спадають приблизно на один відсоток, відповідно. Втім, використання таких тривалих парольних мовленнєвим сигналів на практиці спричинятиме суб’єктам суттєвий дискомфорт.

8. Формалізовано моделі процесу класифікації в задачі автентифікації суб’єкта за мовленнєвим матеріалом із шумом у парадигмі машинного навчання. Синтезовано процедуру регуляризації профільного глибокого нейромережевого класифікатора, яка дозволяє оптимізувати ваги міжнейронних зв’язків, зменшивши їх кількість на 15–20 % при незначному падінні достовірності класифікації. Описано технологію бустінгу орієнтовану на ансамбль імовірнісних класифікаторів для профільної задачі класифікації. Формалізовано процес інтеграції банку оптичних фільтрів, синтезованих на основі положень теорії спектрально-темпоральних рецептивних полів, у згортковий глибокий нейромережевий класифікатор із bottleneck-шаром. Передбачено автоматичне налаштування параметрів фільтрів в процесі навчання нейромережі.

9. Враховуючи значну ресурсозатратність процесу навчання імовірнісних і нейромережевих класифікаторів, на основі описаного процесу бустінгу еталонних навчальних даних та синтезу проекційної функції-ядра машини опорних векторів запропоновано математичний апарат для синтезу простого класифікатора найкращих оцінок. Під терміном «найкраща оцінка» розуміється ідентифікована дискримінантна функція, яка найкраще описує вміст даної еталонної навчальної бази. Відповідно, навчання такого класифікатора є ітеративним процесом ідентифікації таких функцій. На кожній ітерації з множини конкуруючих варіантів обирається

дискримінантна функція, яка забезпечує найкраще розділення класів, а вміст еталонної бази зрізується, тобто з неї вилучаються елементи, які обрана функція найкращої оцінки класифікувала вірно.

10. Відзначимо, що матеріал підрозділу 4.1 і додатку Ж аналітично формалізує і емпірично верифікує модель процесу автентифікації суб'єкта машиною опорних супер- та і-векторів за параметризованим представленням мовленнєвого матеріалу із шумом, опрацьованого, на відміну від існуючих, мультиваріантним методом компенсування шумів у парольному мовленнєвому сигналі з варіативним описом характеристичних параметрів моделлю сумішей гаусівських розподілів, що дозволило підвищити конфіденційність процесу автентифікації, готовність цільової інформаційної системи і оптимізувати процес навчання імовірнісного класифікатора.

– У підрозділі 4.2 представлено концепцію удосконалення топології згорткової нейромережі для автентифікації суб'єкта за мовленнєвим матеріалом із шумом, в якій, на відміну від існуючих, у перший, згортковий, шар інтегровано фільтри Габора із параметризацією вхідної спектрограми в формалізмі спектрально-темпоральних рецептивних полів, що дозволяє максимізувати інформативність інтерпретації вхідної спектрограми нейромережею автоматично, в процесі її навчання, та, за рахунок введення bottleneck-шару, отримати новий набір характеристичних параметрів для опису індивідуальності мовленнєвого матеріалу із шумом.

Основні результати розділу опубліковано в [38, 40, 43, 44, 45, 48, 49, 50, 51, 52, 53, 57, 60, 82].

РОЗДІЛ 5
МОДЕЛІ І МЕТОДИ ЗАБЕЗПЕЧЕННЯ ГАРАНТОЗДАТНОСТІ ІНФОРМАЦІЙНОЇ СИСТЕМИ КРИТИЧНОГО ЗАСТОСУВАННЯ ІЗ АВТЕНТИФІКАЦІЄЮ СУБ'ЄКТА ЗА ГОЛОСОМ

5.1 Концепція забезпечення конфіденційності сеансу суб'єкт-системної інформаційної взаємодії

Швидкий розвиток мережевих технологій загалом та технологій розподілених обчислень зокрема спричинив зміни в архітектурі ІСКЗ у напрямку переходу від односерверної до мультисерверної їх організації. Мультисерверним ІСКЗ [54, 55, 58, 59] властива значно більша обчислювальна потужність та комунікаційні можливості, стійкість до перевантаження, підтримка сучасних протоколів віддаленого резервування інформації тощо. Втім, еволюція цих ІС у напрямку мультисерверної архітектури привела до ускладнення задачі забезпечення конфіденційності сеансу суб'єкт-системної інформаційної взаємодії. У односерверних ІСКЗ конфіденційність сеансу суб'єкт-системної інформаційної взаємодії визначається надійністю процесу взаємної автентифікації суб'єктів-користувачів і ІС, представленої сервером. У мультисерверних ІСКЗ ця задача набуває комплексності, спричиненої, зокрема, необхідністю взаємної автентифікації апаратних елементів мультисерверної інфраструктури в складі системи. Ця обставина зумовила неможливість або недоцільність адаптації створених для односерверних ІСКЗ відповідних концепцій [327–329] для виконання цільових операцій у мультисерверних ІСКЗ, адже навіть у першому наближенні суб'єкта необхідно було б незалежно реєструватись на кожному з серверів у складі ІС і, відповідно, проходити незалежні процедури взаємної автентифікації із ними для здійснення інформаційного обміну. Питання ж внутрішньої безпеки міжсерверної взаємодії в таких концепціях не розглядається взагалі. Отже, в останні роки відповідно до вимог актуальних стандартів безпеки ІС [334] було запропоновано багато концепцій забезпечення конфіденційності сеансу суб'єкт-системної інформаційної взаємодії для мультисерверних ІС. Якість цих концепцій визначається обчислювальною складністю і на-

дійністю використаного процесу взаємної автентифікації в мультисерверному інформаційному просторі. Зокрема, відомі концепції з використанням верифікаційних таблиць [327–329], із апаратним захистом на основі карт доступу [327], на основі індивідуальних біометричних характеристик людини [328], із використанням нейронних мереж з динамічним ідентифікатором [327], із використанням цифрового підпису або хеш-функцій [327–329]. Проте, цим концепціям властива або вразливість до певних типів атак, або висока обчислювальна складність або суттєвий дискомфорт процесу автентифікації суб'єкта-користувача, що обумовлює доцільність проведених досліджень.

Нехай у сеансі суб'єкт-системної взаємодії мультисерверної ІКСЗ бере участь множина об'єктів, яка містить підмножини суб'єктів-користувачів і серверів та виділений сервер-реєстраційний центр для обліку об'єктів без ведення верифікаційних таблиць. Інформаційний обмін під час сеансу суб'єкт-системній взаємодії пропонується організувати у вигляді захищених сесій на основі ключів із механізмом узгодження на основі односторонніх хеш-функцій та криптографії еліптичних кривих [330–332], яка на даний час забезпечує найкраще співвідношення надійності шифрування по відношенню до довжини ключа серед існуючих криптосистем. Роботу із суб'єктами-користувачами пропонується персоніфікувати застосувавши захищені на основі положень криптографічної теорії еліптичних кривих індивідуальні карти доступу на яких, окрім ідентифікаційної інформації та пароля, зберігатиметься індивідуальна біометрична інформація голосу суб'єкта. Додаток для доступу до ІнС ІСКЗ, який встановлюватиметься на віддалених терміналах, ініціюватиметься двофакторною процедурою автентифікації суб'єкта-користувача (за умови наявності ідентифікаційної карти) – за індивідуальними особливостями його голосу та за введеним паролем, що поряд із зручністю забезпечуватиме надійність процесу автентифікації.

Для включення в склад ІСКЗ сервер S_j має пройти процедуру реєстрації на сервер-реєстраційному центрі RC, яка включає таку послідовність дій:

1. $S_j \to RC: SID_j$. Сервер S_j, використовуючи захищене з'єднання, передає в центр RC свій унікальний ідентифікатор SID_j;

2. $RC \to S_j : h(SID_j \| y)$. В центрі RC обчислюється секретний ключ $R_j = h(SID_j \| y)$ для сервера S_j, де y – частина секретного ключа RC для реєстрації сервера; $h(\ )$ – одностороння хеш-функція [330–332]; а $\|$ – операція конкатенації. Центр RC надсилає секретний ключ R_j захищеним каналом зв'язку серверу S_j для зберігання.

Аналогічно суб'єкт-користувач U_i також має зареєструватися на сервері RC, виконавши таку послідовність дій:

1. $U \to RC : \{ID, B, h(PW \| B)\}$. Суб'єкт U_i використовує встановлений на віддаленому терміналі додаток для автентифікації AA для утворення еталону свого голосу B_i, вибору та введення унікального ідентифікатора ID_i та пароля PW_i. Додаток AA обчислює значення $h(PW_i \| B_i)$ та, використовуючи захищене з'єднання, передає в центр RC повідомлення $\{ID_i, B_i, h(PW_i \| B_i)\}$;

2. $RC \to U : \{IC(Z, B, h(\ ), d(\ ), \tau)\}$. В центрі RC обчислюються секретні ключі $R_i = h(ID_i \| x)$ та $Z_i = R_i \oplus h(PW_i \| B_i)$ для суб'єкта U_i, де x – частина секретного ключа RC для реєстрації суб'єкта; $d(\ )$ – симетрична параметрична функція [330–332]; τ_i – поріг надійності для процесу автентифікації особи i-го суб'єкта за голосом, який визначається центром RC на основі аналізу наданого i-м суб'єктом узагальненого еталону голосу B_i за методом [43, 45, 48, 49]; $\oplus$ – операція XOR. Далі масив інформації $\{Z_i, B_i, h(\ ), d(, \tau_i)\}$ записується на індивідуальну карту суб'єкта IC, яку передають суб'єкту із гарантуванням безпеки цієї операції.

Сеансу доступу суб'єкта U_i до ІнС сервера S_j, який є складовою ІСКЗ, має передувати процес взаємної автентифікації, в якій братимуть учать суб'єкт U_i,

сервер S_j та центр RC тощо. Цей процес включатиме таку послідовність операцій:

1. $U \to S_j : \{ID, X, C_1\}$. Якщо суб'єкт U_i бажає синхронізувати ключ сесії із сервером S_j, він має ініціювати індивідуальну карту IC, відкрити додаток AA та сформувати, використовуючи його можливості, фонограму із записом власного голосу B_i' для подальшого аналізу. Далі додаток AA порівнює значення характеристичних параметрів голосу, екстраговані з фонограми B_i', із збереженими на IC, і якщо $d(B_i, B_i') \geq \tau_i$, то процес біометричної автентифікації вважається невдалим і описані вище дії потрібно повторювати. Якщо ж $d(B_i, B_i') < \tau_i$, то процес біометричної АСГ вважається успішно завершеним і додаток AA надає суб'єкту U_i можливість ввести свій код ID_i і пароль PW_i, а згодом випадковим чином генерує ціле число $\alpha \in [1, q-1]$, розраховує значення $R_i = Z_i \oplus h(PW_i \| B_i)$, $X = \alpha \times P$ і $C_1 = h(h(ID_i \| x) \| \alpha \times P) = h(R_i \| X)$ та надсилає повідомлення M_1 із параметрами $\{ID_i, X, C_1\}$ серверу S_j. У наведених вище виразах P є вихідною точкою з множини точок $E(F_p)$ над скінченним полем F_p, де $E(F_p) = \{(x, y) : x, y \in F_p$ задовольняє $y^2 = x^3 + ax + b\} \cup \{O\})$; E – несуперсингулярна еліптична крива над скінченним полем F_p – $E : y^2 = (x^3 + ax + b) \bmod p$, де p – велике (1024–2048 біт) просте число; $\alpha, \beta \in [1, p-1]$ – випадково обрані цілі числа, які задовольняють нерівність $(4a^3 + 27b) \bmod p \neq 0$. Ці положення відповідають теорії еліптичної криптографії і детальніше описані у [330–332];

2. $S_j \to RC : \{ID, X, C_1, SID_j, Y, C_2\}$. Отримавши описане у п.1 повідомлення M_1 сервер S_j генерує випадкове ціле число $\beta \in [1, q-1]$, розраховує значення $Y = \beta \times P$ і параметр $C_2 = h(h(SID_j \| y) \| \beta P) = h(R_j \| Y)$ та надсилає повідомлення M_2 із параметрами $\{ID_i, X, C_1, SID_j, Y, C_2\}$ центру RC;

3. $RC \to S_j : \{C_3, C_4\}$. На основі даних з повідомлення M_2 центр RC розраховує значення $C_1' = h(h(ID_i \| x) \| \alpha P) = h(h(ID_i \| x) \| X)$ та $C_2' = h(h(SID_j \| y) \| \beta P) = h(h(SID_j \| y) \| Y)$ і перевіряє, чи виконуються обидві рівності $C_1 = C_1'$ та $C_2 = C_2'$. Якщо ні, то центр RC ініціює переривання сесії, а якщо виконуються, то обчислює параметри $V = h(h(SID_j \| y) \| Y \| X)$, $W = h(h(ID_i \| x) \| SID_j \| X \| Y)$ та коефіцієнти $C_3 = V \oplus W$ і $C_4 = h(V \| W)$ на їх основі, які включаються у вміст повідомлення $M_3 = \{C_3, C_4\}$, що надсилається серверу S_j. Параметр W є одноразовим секретним ключем для сесії між суб'єктом U_i та сервером S_j;

4. $S_j \to U : \{Y, C_5\}$. Сервер S_j обчислює параметри $V' = h(R_j \| Y \| X)$, $W' = V' \oplus C_3$ і $C_4' = h(V' \| W')$ та перевіряє, чи виконується рівність $C_4 = C_4'$. Якщо рівність не виконується, то сервер S_j перериває сесію, а якщо виконується, то сервер S_j обчислює ключ сесії $SK_j = \beta \times X = \alpha\beta \times P$ і значення параметра $C_5 = h(ID_i \| SID_j \| W' \| SK_j)$, яке, на додачу до значення Y, надсилає повідомленням $M_4 = \{Y, C_5\}$ суб'єкту U_i;

5. $U_i \to S_j : \{C_6\}$. Додаток AA , отримавши повідомлення M_4 , обчислює значення $W'' = h(R_i \| SID_j \| X \| Y)$, $SK_i = \alpha \times Y = \alpha\beta \times P$ і параметр $C_5' = h(ID_i \| SID_j \| W'' \| SK_i)$ на їх основі, та аналізує, чи виконується рівність $C_5 = C_5'$. Якщо рівність не виконується, то додаток AA ініціює переривання сесії, а якщо виконується, то розраховує значення $C_6 = h(W'' \| SK_i \| Y)$ і надсилає його серверу S_j у вмісті повідомлення $M_5 = \{C_6\}$;

6. Сервер S_j розраховує значення $C_6' = h(W' \| SK_j \| Y)$ та аналізує, чи виконується рівність $C_6 = C_6'$. Якщо рівність не виконується, то сервер S_j ініціює переривання сесії, а якщо виконується, то процес автентифікації суб'єкта U_i для доступу до ІнС сервера S_j, який є складовою ІСКЗ, вважається успішно завершеним.

Під час встановленої сесії суб'єкт U_i і сервер S_j використовують секретний ключ $SK = \alpha\beta P$.

Якщо суб'єкт U_i бажає змінити пароль чи оновити еталон голосу, який використовується у процесі автентифікації, йому слід виконати таку послідовність дій:

1. $U \to IC : \{B^*\}$. суб'єкт U_i ініціює свою індивідуальну карту IC, запускає додаток AA та утворює користуючись його можливостями фонограму власного голосу B_i^* для подальшого аналізу;

2. $d(B, B^*) < \tau \xrightarrow{+} IC : \{B^* \to B\}$. Додаток AA здійснює порівняння наданої фонограми B_i^* із еталоном голосу суб'єкта B_i і якщо нерівність $d(B_i, B_i^*) < \tau_i$ виконується, то суб'єкту U_i надається можливість замінити B_i на B_i^* із збереженням змін на індивідуальній карті IC. Якщо згадана вище нерівність не виконується, то процес оновлення інформації на карті IC припиняється;

3. $U \to IC\{PW^*\}$. Якщо п. 2 цієї послідовності дій завершився коректно, то додаток AA пропонує суб'єкту U_i оновити свій пароль, для чого необхідно ввести поточний пароль PW_i та бажаний новий пароль PW_i^*;

4. $PW \overset{?}{=} PW \xrightarrow{+} IC : \{PW^*, Z^*\} \to \{PW, Z\}$. Якщо, відповідно до п. 3 цієї послідовності дій, суб'єкт U_i невірно ввів свій поточний пароль PW_i, то додаток AA припиняє процес оновлення особових даних. Якщо ж поточний пароль PW_i введено вірно, то додаток AA обчислює значення $Z_i^* = Z_i \oplus h(PW_i \| B_i) \oplus h(PW_i^* \| B_i^*)$ та замінює значення Z_i та PW_i на картці IC суб'єкта U_i новими значеннями Z_i^* та PW_i^* відповідно.

Згідно із актуальним стандартом безпеки інформаційних систем ISO/IEC 27001:2013 [334] у надійному процесі взаємної автентифікації необхідно передбачити захист від таких типів атак: атаки із вгадуванням пароля, атаки із відтворен-

ням запису пароля, атаки із використанням викрадених засобів верифікації, атаки із використанням викрадених ідентифікаційних карт, атаки на основі авторизованих аккаунтів суб'єктів (інсайдерів), спуфінг-атаки, атаки із підбором пароля, атаки із спробою підробки ключа сесії, атаки на основі частини відомих ключів сесій, атаки на основі ключів сесій довготривалого використання, атаки на основі одноразових паролів, атаки в процесі оновлення пароля, атаки із перевантаженням апаратних засобів тощо.

Вище запропоновану базову концепцію організації сеансу суб'єкт-серверної взаємодії захищено від атак із вгадуванням пароля в усіх режимах роботи (он-, оффлайн, та в процесі обміну повідомленнями між складовими елементами системи тощо). Працюючи в режимі он-лайн центр RC однозначно автентифікує суб'єкта U після виконання третього етапу відповідної послідовності дій. Оффлайн атака із вгадуванням пароля також не спрацює, оскільки на додачу до пароля PW для автентифікації суб'єкта U використовується параметризоване порівняння фонограми голосу суб'єкта із еталоном голосу B, і лише при співпадінні значень цих параметрів в межах порогу τ обчислюється ключ суб'єкта R на основі значення параметра Z. Використання односторонніх хеш-функцій та випадкових значень в процесі інформаційного обміну у вигляді повідомлень $M_1 - M_6$ захищає інформаційну систему від втрати секретних ключів RC та x при перехоплені цих повідомлень. У запропонованій базовій концепції передбачено захист від атак із відтворенням запису пароля, оскільки весь інформаційний обмін персоніфікується за рахунок ключів x та y і ключів сесій SK, які передаються у хешованих повідомленнях M_4 та M_5 і розшифровуються лише при знаних випадкових числах α і β. Атаки із використанням викрадених засобів верифікації, атаки із використанням викрадених ідентифікаційних карт та інсайдерські атаки не вражають ІС, оскільки на серверах S та у реєстраційному центрі RC, згідно запропонованої базової концепції, не зберігається необхідна для верифікації суб'єкта інформація (PW, B) у явному вигляді. Втім, навіть маючи індивідуальну карту суб'єкта IC та знаючи його пароль PW антагоністу доведеться проходити процедуру голосової

верифікації. Аналогічно у системі реалізовано захист від спуфінг-атак із спробами антагоніста видати себе за сервер S, центр RC або суб'єкта U, адже, значення $h(ID_i \| x)$, $h(SID_j \| y)$ і W, відповідно, забезпечують взаємну автентифікацію цих складових елементів системи. Захист від атак із підбором пароля забезпечується надійністю обраного методу хешування на основі еліптичних кривих та постійній взаємній перевірці компонентами системи автентичності одне одного на основі інформації із повідомлень $M_1 - M_6$. Захист від атак із спробою підробки ключа сесії забезпечуються унікальністю ключів кожної із сесій, повторюваність яких виключається способом їх формування на основі параметра W із використанням випадкових чисел α і β, а застосування процедури хешування унеможливлює присутність повторюваних послідовностей у ключах сесій обраної довжини. Захист ІС від атаки на основі ключів сесій довготривалого використання базується на проблемі дискретного логарифмування еліптичних кривих [330–332] яка полягає у складності задачі обчислення секретного ключа α на основі відомої точки публічного ключа $Q = \alpha P$ та проблемі протоколу Діффі–Геллмана на еліптичних кривих [330–332], яка полягає в складності пошуку $\alpha\beta P$ для відомих точок αP та βP. Тобто, навіть отримавши ключі довготривалого використання x та y, пароль суб'єкта PW і параметри еталону голосу B антагоніст не розрахує ключ сесій $SK = \alpha\beta P$ без відомих значень α і β. Так само, навіть взнавши αP і βP антагоніст не обчислить ключ сесій SK. Одноразові паролі в запропонованій концепції не передбачено. Стійкість системи до атак у процесі оновлення пароля забезпечується надійністю процесу АСГ B та необхідністю розрахунку параметра Z із знанням попередньої індивідуальної інформації. Атаки із перевантаженням апаратних засобів не можуть вразити запропоновану базову концепцію через те, що процес автентифікації не може значно завантажити канали зв'язку, а кількість суб'єктів, які можуть спробувати одночасно отримати доступ до ІСКЗ можна однозначно обмежити кількістю віддалених терміналів із встановленими додатками для автентифікації. Таким чином, запропонована базова концепція забезпечення конфіденційності сеансу суб'єкт-системної інформаційної взаємодії відповідає

всім вимогам до безпеки такого класу процесів, викладеним у актуальному стандарті ISO/IEC 27001:2013.

Досвід практичної експлуатації ІСКЗ із використанням базової концепції забезпечення конфіденційності сеансу суб'єкт-системної інформаційної взаємодії виявив ряд її вразливостей. Не зважаючи на те, що згідно із базовою концепцією суб'єкт U при реєстрації не надсилає свої індивідуальні дані в центр RC у відкритому вигляді, антагоніст все ж може їх отримати виконавши такі дії: маючи доступ до ресурсів центру RC та не захищеного хешуванням значення B_i антагоніст може змінювати пароль PW_i' і обчислювати значення $h' = h(PW_i' \| B_i)$ доти, поки воно не зрівняється із надісланим суб'єктом значенням $h(PW_i \| B_i)$, що означатиме, що $PW_i' = PW_i$. Схожою за сутністю є і друга вразливість, пов'язана із несанкціонованим доступом до карти IC та додатку AA. Припустимо, антагоністу вдалося екстрагувати секретну інформацію $\{Z_i, B_i, h(\ ), d(\ ), \tau_i\}$ з карти IC суб'єкта U_i та перехопити повідомлення $M_1 = \{ID_i, X, C_1\}$, яке додаток AA надсилатиме від імені суб'єкта U_i на сервер S_j. В такому разі антагоніст може підбирати значення пароля PW_i^* поки рівність $C_1 = C_1^* = h(Z_i \oplus h(PW_i^* \| B_i) \| X)$ не виконається, тобто PW_i^* не співпаде із PW_i. І, нарешті, третя вразливість проявляється, якщо антагоніст отримав доступ до додатку AA та сервера S_j. Нехай антагоніст U_A хоче, щоб сервер S_j автентифікував його як суб'єкта U_i. Для цього U_A на загальних підставах реєструється згідно з базовою послідовністю дій і отримує свої секретні дані $Z_A = R_A \oplus h(PW_A \| B_A) = h(ID_A \| x) \oplus h(PW_A \| B_A)$, на основі яких він, знаючи згенероване на його терміналі α, обчислює значення $R_A = Z_A \oplus h(PW_A \| B_A)$, $X = \alpha P$, $C_1 = h(R_A \| X)$, які надсилає серверу S_j у вигляді повідомлення $M_1 = \{ID_i, X, C_1\}$. Отримавши повідомлення M_1, сервер S_j генерує випадкове ціле β та, обчисливши $Y = \beta P$ і $C_2 = h(R_j \| Y)$, надсилає повідомлення $M_2 = \{ID_i, X, C_1, SID_j, Y, C_2\}$ у центр RC, яке антагоніст U_A перехоплює і замінює повідомленням $M_2' = \{ID_A, X, C_1, SID_j, Y, C_2\}$. На основі отриманого повідом-

лення M_2', центр RC перевіряє чи виконуються рівності $C_1 = h(h(ID_A \| x) \| X)$, $C_2 = h(h(SID_j \| y) \| Y)$, і якщо вони виконуються, то надсилає серверу S_j повідомлення $M_3 = \{C_3, C_4\}$. Отримавши повідомлення M_3, сервер S_j перевіряє чи виконується рівність $C_4 = h(h(R_j \| Y \| X) \| h(R_j \| Y \| X) \oplus C_3)$, і якщо так, то обчисливши ключ сесії $SK_j = \beta X = \alpha\beta P$ і $C_5 = h(ID_i \| SID_j \| W \| SK_j)$ надсилає повідомлення $M_4 = \{Y, C_5\}$ антагоністу U_A. Отримавши M_4, антагоніст U_A досягає рівності $C_5 = h(ID_i \| SID_j \| h(R_i \| SID_j \| X \| Y) \| \alpha\beta P)$ після чого, обчисливши $C_6 = h(h(R_i \| SID_j \| X \| Y) \| SK_i \| Y)$, надсилає його повідомленням $M_5 = \{C_6\}$ серверу S_j, який, перевіривши виконання рівності $C_6 = h(h(R_j \| Y \| X) \oplus C_3 \| SK_j \| Y)$, автентифікує антагоніста U_A як суб'єкта U_i.

Звичайно, в процесі реальної експлуатації ІСКЗ імовірність появи описаних вище вразливостей вкрай низька, але, враховуючи критичне застосування ІС, нехтувати нею не варто, тому створимо удосконалену концепцію забезпечення конфіденційності сеансу суб'єкт-системної інформаційної взаємодії.

Аналіз процедури реєстрації сервера S_j у центрі RC, яку описано в базовій концепції, показав, що запропонована послідовності дій не містить вразливостей, отже, залишимо її без змін. А от процес реєстрації суб'єкта U_i, як виявилося, необхідно допрацювати. Удосконалений процес реєстрації суб'єкта U_i опишемо такою послідовність дій:

1. $U \to RC : \{ID, B, h(PW \| B \| b)\}$. Суб'єкт U_i використовує додаток AA для утворення еталону свого голосу B_i, вибору та введення унікального ідентифікатора ID_i та пароля PW_i. Після чого додаток AA генерує випадкове ціле число b_i, обчислює значення $h(PW_i \| B_i \| b_i)$ та, використовуючи захищене з'єднання, передає в центр RC повідомлення $\{ID_i, B_i, h(PW_i \| B_i \| b_i)\}$;

2. $RC \to U : \{IC(Z, B, h(\ ), d(\ ), \tau)\}$. У центрі RC обчислюються секретні ключі $R_i = h(ID_i \| x) \times P$ та $Z_i = R_i \oplus h(PW_i \| B_i \| b_i)$ і масив інформації $\{Z_i, B_i, h(\ ), d(, \tau_i)\}$ записується на карту IC, яку передають суб'єкту U_i із гарантуванням безпеки цієї операції;

3. $AA \to U : \{IC(b)\}$. Додаток AA завершує процес реєстрації суб'єкта U_i дописавши на карту IC значення $\{b_i\}$.

Зазнає удосконалення і процес взаємної автентифікації суб'єкта U_i і сервера S_j:

1. $U \to S_j : \{ID, X, C_1\}$. Суб'єкт U_i ініціює свою карту IC і додаток AA та формує використовуючи його можливості фонограму із записом власного голосу B_i' для подальшого аналізу. Далі додаток AA порівнює значення характеристичних параметрів, екстрагованих із фонограми B_i', із збереженими на карті IC, і якщо $d(B_i, B_i') \geq \tau_i$, то процес біометричної автентифікації вважається невдалим і описані вище дії потрібно повторювати. Якщо ж $d(B_i, B_i') < \tau_i$, то додаток AA надає суб'єкту можливість ввести свій код ID_i і пароль PW_i, а згодом випадковим чином генерує ціле число $\alpha \in [1, q-1]$, розраховує значення $R_i = Z_i \oplus h(PW_i \| B_i \| b_i)$, $X = \alpha \times P$, $X' = \alpha \times R_i$, $C_1 = h\left(h\left(ID_i \| x\right) \| \alpha \times P \| \alpha \times R_i\right) = h\left(R_i \| X \| X'\right)$ та надсилає повідомлення M_1 із параметрами $\{ID_i, X, C_1\}$ серверу S_j;

2. $S_j \to RC : \{ID, X, C_1, SID_j, Y, C_2\}$. Отримавши описане у п. 1 повідомлення M_1, сервер S_j генерує випадкове ціле число $\beta \in [1, q-1]$, розраховує значення $Y = \beta \times P$ і $C_2 = h(ID_i \| X \| C_1 \| R_j \| Y)$ та надсилає повідомлення M_2 із параметрами $\{ID_i, X, C_1, SID_j, Y, C_2\}$ центру RC;

3. $RC \to S_j : \{C_3, C_4\}$. На основі даних з повідомлення M_2, центр RC розраховує значення $C_1' = h(ID_i \| X \| h(ID_i \| x) \times X)$ та $C_2' = h(ID_i \| X \| C_1 \| h(SID_j \| y) \| Y)$ і перевіряє, чи виконуються обидві рівності $C_1 = C_1'$ та $C_2 = C_2'$. Якщо ні, то центр RC

ініціює переривання сесії, а якщо виконуються, то обчислює параметри $V = h\left(h\left(SID_j \| y\right) \| Y \| X\right)$, $W = h\left(h\left(ID_i \| x\right) \times X \| SID_j \| X \| Y\right)$ та коефіцієнти $C_3 = V \oplus W$ і $C_4 = h\left(V \| W \| ID_i\right)$ на їх основі, які включаються у вміст повідомлення $M_3 = \{C_3, C_4\}$, яке надсилає серверу S_j;

4. $S_j \to U : \{Y, C_5\}$. Сервер S_j обчислює параметри $V' = h\left(R_j \| Y \| X\right)$, $W' = V' \oplus C_3$ і $C_4' = h\left(V' \| W' \| ID_i\right)$ та перевіряє, чи виконується рівність $C_4 = C_4'$. Якщо рівність не виконується, то сервер S_j перериває сесію, а якщо виконується, то сервер S_j обчислює ключ сесії $SK_j = \beta \times X = \alpha\beta \times P$ і значення параметра $C_5 = h\left(ID_i \| SID_j \| W' \| SK_j\right)$, та надсилає повідомлення $M_4 = \{Y, C_5\}$ додатку AA;

5. $U_i \to S_j : \{C_6\}$. Додаток AA, отримавши повідомлення M_4, обчислює значення $W'' = h\left(SID_j \| X \| Y \| X'\right)$, $SK_i = \alpha \times Y = \alpha\beta \times P$ і параметр $C_5' = h\left(ID_i \| SID_j \| W'' \| SK_i\right)$, аналізує, чи виконується рівність $C_5 = C_5'$. Якщо рівність не виконується, то додаток AA ініціює переривання сесії, а якщо виконується, то розраховується значення $C_6 = h\left(W'' \| SK_i \| Y\right)$ і надсилається серверу S_j у складі повідомлення $M_5 = \{C_6\}$.

6. Сервер S_j розраховує значення $C_6' = h\left(W' \| SK_j \| Y\right)$ та аналізує, чи виконується рівність $C_6 = C_6'$. Якщо рівність не виконується, то сервер S_j ініціює переривання сесії, а якщо виконується, то процес взаємної автентифікації суб'єкта U_i і сервера S_j вважається успішно завершеним і між ними встановлюється сесія для обміну інформацією із ключем сесії $SK = \alpha\beta P$.

Незначних змін для позбавлення виявленої вразливості зазнав процес оновлення еталону голосу B_i та пароля PW_i суб'єкта U_i:

1. $U \to IC : \{B^*\}$. Суб'єкт U_i ініціює свою карту IC, запускає додаток AA та утворює, користуючись його можливостями, фонограму власного голосу B_i^* для подальшого аналізу;

2. $d\left(B,B^*\right)<\tau \xrightarrow{+} IC:\left\{B^* \to B\right\}$. Додаток AA здійснює порівняння наданої фонограми B_i^* із еталоном голосу суб'єкта B_i і якщо нерівність $d\left(B_i,B_i^*\right)<\tau_i$ виконується, то суб'єкту U_i надається можливість замінити B_i на B_i^* із збереженням змін на індивідуальній карті IC. Якщо згадана вище нерівність не виконується, то процес оновлення інформації на картці IC припиняється;

3. $U \to IC\left\{PW^*\right\}$. Якщо п. 2 цієї послідовності дій завершився коректно, то додаток AA пропонує суб'єкту U_i оновити свій пароль, для чого пропонується ввести поточний пароль PW_i та бажаний новий пароль PW_i^*.

4. $PW \overset{?}{=} PW \xrightarrow{+} IC:\left\{PW^*,Z^*\right\} \to \left\{PW,Z\right\}$. Якщо, відповідно до п. 3 цієї послідовності дій, суб'єкт U_i невірно ввів свій поточний пароль PW_i, то додаток AA припиняє процес оновлення особових даних. Якщо ж поточний пароль PW_i введено вірно, то додаток AA обчислює значення $Z_i^* = Z_i \oplus h\left(PW_i \| B_i \| b_i\right) \oplus h\left(PW_i^* \| B_i^* \| b_i\right)$ та замінює значення Z_i та PW_i на картці IC суб'єкта U_i новими значеннями Z_i^* та PW_i^*, відповідно.

Введення додаткового випадкового цілого числа b_i, яке використовується у процесі взаємної автентифікації за участю додатка AA і сервера S_j, але в явному вигляді невідоме центру RC, дозволяє стверджувати, що удосконалену концепцію убезпечено від першої із виявлених вразливостей базової концепції. Тепер антагоністу, щоб видати себе за суб'єкта U_i перед сервером S_j, необхідно згенерувати вірне повідомлення

$$M_1 = \left\{ID_i, X, C_1\right\} = \left\{ID_i, \alpha \times P, h\left(ID_i \| \alpha \times P \| X'\right)\right\} =$$
$$= \left\{ID_i, \alpha \times P, h\left(ID_i \| \alpha \times P \| \alpha \times h\left(ID_i \| x\right) \times P\right)\right\},$$

яке включає значення $h\left(ID_i \| x\right) \times P$, підробити яке без доступу до сервера S_j і центра RC неможливо. Складніше протидіяти ситуації, коли антагоніст отримав доступ до карти IC і дешифрував записану на ній інформацію $\left\{Z_i, B_i, h(\ ), d(\ ), \tau_i\right\}$.

У такому разі антагоніст зможе обчислити значення X, але обчислити вірне значення $X' = \alpha \times R_i = \alpha \times Z_i \oplus h(PW_i \| B_i \| b_i)$ для розрахунку параметра C_1 не маючи пароля PW_i він не зможе. Якщо антагоніст захоче видати себе за сервер S_j перед суб'єктом U_i, йому необхідно підробити повідомлення $M_4 = \{Y, C_5\}$ маючи інформацію із повідомлення $M_1 = \{ID_i, X, C_1\}$, для чого необхідно обчислити значення $h(ID_i \| x) \times X$, що можливе лише при відомому секретному ключі x, який зберігається лише у центрі RC. Якщо антагоніст спробує перехопити повідомлення M_1, надіслане суб'єктом U_i, з метою видати себе за нього перед сервером S_j, то він не зможе вірно обчислити ключ $SK_i = \alpha\beta \times P$, адже не знатиме значення випадкового цілого α, і, відповідно, не зможе надіслати серверу S_j вірного повідомлення $M_5 = \{C_6\}$. Взагалі інформаційний обмін у процесі взаємної автентифікації за удосконаленою концепцією повністю регламентований множиною повідомлень $M = \{M_1, M_2, \ldots, M_5\}$ із вбудованими автентифікаційними кодами $C = \{C_1, C_2, \ldots, C_6\}$ і для вдалого втручання у цей процес антагоністу фактично слід мати доступ до карти IC, додатку AA (секретний код R_i), сервера S_j (секретний код R_j) і центру RC (секретні коди x та y). Але навіть якщо антагоніст знає всі ці параметри і здатний підробляти інформаційні повідомлення, то при обчисленні ключа сесії $SK_j = \alpha\beta \times P$ він стикнеться із ECDLP-проблемою [330–332]. Таким чином, удосконалена концепції забезпечення конфіденційності сеансу суб'єкт-системної інформаційної взаємодії має всі переваги базової концепції і захищена від виявлених експлуатаційних вразливостей стійкістю математичного апарату еліптичної криптографії та надійністю процесу АСГ.

Оцінювання обчислювальної складності запропонованих концепцій організації сеансу суб'єкт-системної інформаційної взаємодії виконаємо підрахувавши кількість операцій масштабованого множення T_m та обчислення хеш-функції T_h у процесах автентифікації суб'єкта U_i, сервера S_j, центра RC та в процесі їх взаємної автентифікації тощо. Ці операції є найбільш обчислювально складними і

тривалістю виконання решти обчислень, зазначених в описаних вище концепціях, можна знехтувати. Результати оцінювання представлено на рис. 5.1, де BC та MC є абревіатурами базової та удосконаленої концепцій, відповідно.

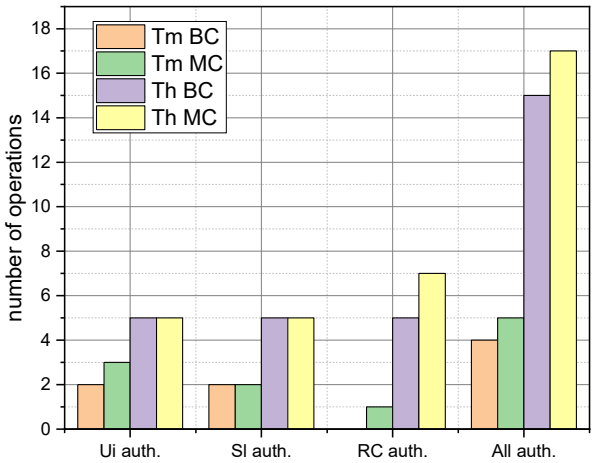


Рисунок 5.1 – Оцінювання обчислювальної складності базової і удосконаленої концепцій організації сеансу суб’єкт-системної взаємодії

Як видно з рис. 5.1, удосконалена концепція забезпечення конфіденційності сеансу суб’єкт-системної інформаційної взаємодії в цілому є більш обчислювано складною (на 10–15 %) порівняно із базовою концепцію. Але зважаючи на те, що удосконалену концепцію позбавлено виявлених у процесі експлуатації базової концепції вразливостей та врахувавши орієнтацію запропонованих концепцій для забезпечення конфіденційності сеансів суб’єкт-системної взаємодії в ІСКЗ, саме використання удосконаленої концепції є рекомендованим.

Розглядаючи питання забезпечення конфіденційності сеансу суб’єкт-системної інформаційної взаємодії доцільним є отримати математичний апарат який би дозволив у парадигмі теорії надійності оцінити вплив на сеанс експлуатації ІСКЗ некорельованих НФ, що можуть спричинити передчасне припинення активного сеансу. Припустимо, що формалізовано множину з n незалежних зовнішніх НФ, вплив яких на ІСКЗ може спричинити несанкціоноване переривання активного сеансу її експлуатації. Появу цих НФ опишемо імовірностями $q_1, q_2, \ldots, q_n$, $\sum_{i=1}^{n} q_i < 1$. Вважатимемо, що НФ впливають на ІСКЗ по одному і на-

ступний НФ впливатиме на систему після того, як СПБ знешкодила вплив попереднього. Тоді у будь-який дискретний момент часу t ІСКЗ перебуває у одному із z_i станів, де $i=\overline{1,n}$ – тип НФ, а стан z_0 є станом штатного перебігу сеансу експлуатації ІСКЗ (функціональним станом). В наслідок діяльності СПБ у момент часу $t+1$ система із стану z_i може перейти у стан z_0 із імовірністю u_i (вплив НФ на систему нейтралізовано), або ж система може перейти у стан z_{n+1} з імовірністю $\overline{u_i}=1-u_i$, де z_{n+1} – стан, коли сеанс експлуатації передчасно перервано (нефункціональний стан), у який ІСКЗ переходить у наслідок надзвичайної ситуації, спричиненої впливом i-го НФ, нейтралізувати вплив якого СПБ виявилася нездатною. Базовим математичним апаратом для опису процесу перебігу сеансу експлуатації ІСКЗ із імовірним впливом НФ можне бути марковська мережа, переходи між станами якої описано матрицею

$$\Pi=\begin{pmatrix} q_0 & q_1 & q_2 & \dots & q_n & 0 \\ u_1 & 0 & 0 & \dots & 0 & \overline{u_1} \\ u_2 & 0 & 0 & \dots & 0 & \overline{u_2} \\ & & & \dots & & \\ u_n & 0 & 0 & \dots & 0 & \overline{u_n} \\ 0 & 0 & 0 & \dots & 0 & 1 \end{pmatrix},$$

де $q_0=1-\sum_{i=1}^{n} q_i$. Тоді імовірність того, що ІСКЗ у момент часу t перебуває у стані z_i опишемо виразом $g_i(t)=\sum_{j=0}^{n+1} g_j(t-1)\Pi_{ji}$ або

$$g(t)=g(t-1)\Pi=g(0)\Pi^t, \tag{5.1}$$

де $g(t)=(g_0(t),g_1(t),\dots,g_{n+1}(t))$.

Нехай у початковий момент часу $t=0$ ІСКЗ перебуває у стані z_0, тобто $g(0)=(1,0,\dots,0)$. Тоді імовірність перебування ІСКЗ у стані z_0 у момент часу t представимо як

$$g_0(t)=w^{-1}\left((0{,}5(q_0+w))^{t+1}-(0{,}5(q_0-w))^{t+1}\right), \tag{5.2}$$

де $w=\sqrt{q_0^2+4\sum_{i=1}^{n}u_iq_i}\geq 0$ – керований комплексний параметр, який характеризує налаштування СПБ. Отримаємо аналітичні вирази для оцінювання імовірностей перебування ІСКЗ в решті можливих станів у момент часу t. Якщо $g(t+1)=g(t)\Pi$, то

$$g_0(t+1)=g_0(t)q_0+\sum_{i=1}^{n}g_i(t)u_i, \tag{5.3}$$

де $g_i(t)=g_0(t-1)q_i$. Тоді $g_i(t+1)=g_0(t)q_i$, а

$$g_{n+1}(t+1)=\sum_{i=1}^{n}g_i(t)\overline{u_i}+g_{n+1}(t). \tag{5.4}$$

За аналогією із (5.2), розкриємо вираз (5.3) так:

$$g_0(t+1)=q_0w^{-1}\left(\left(0{,}5(q_0+w)\right)^{t+1}-\left(0{,}5(q_0-w)\right)^{t+1}\right)+$$

$$+w^{-1}\left(\left(0{,}5(q_0+w)\right)^{t}-\left(0{,}5(q_0-w)\right)^{t}\right)\sum_{i=1}^{n}q_iu_i=$$

$$=w^{-1}\left(\left(0{,}5(q_0+w)\right)^{t+2}-\left(0{,}5(q_0-w)\right)^{t+2}\right),$$

а вираз (5.4), із урахуванням того, що $g_0(t)+\sum_{i=1}^{n}g_i(t)+g_{n+1}(t)=1$, так:

$$g_{n+1}(t+1)=g_0(t)\left(1-\sum_{i=1}^{n}q_i\right)+\sum_{i=1}^{n}g_i(t)+g_{n+1}(t)-g_0(t+1)=$$

$$=1-g_0(t)\sum_{i=1}^{n}q_i-g_0(t+1).$$

Ситуацію відсутності у СПБ захисту від i-го НФ опишемо виразом $u_i=0$, тоді $w=q_0$, і, відповідно, $g_0(t)=q_0^t$, $g_i(t)=q_0^{t-1}q_i$, $g_{n+1}(t)=1-q_0^{t-1}$. Ці вирази є основою для отримання граничних виразів для розрахунку імовірностей перебування ІСКЗ у станах z_i у момент часу t:

$$\begin{gathered}\lim_{t\to\infty}g_0(t)=\ldots=\lim_{t\to\infty}g_n(t)=0,\\ \lim_{t\to\infty}g_{n+1}(t)=1,\end{gathered} \tag{5.5}$$

які, втім, актуальні і тоді, коли окремі $u_i>0$.

Отже, з виразу (5.5) очевидно, що при $t \to \infty$ ІСКЗ перебуватиме у стані z_{n+1}.

Також, при $t \to \infty$, маємо $\lim\limits_{t\to\infty}\left|(q_0 - w)(q_0 + w)^{-1}\right|^t = 0$, на основі чого отримаємо

$$g_0(t) \approx \hat{g}_0(t) = w^{-1}\left(0{,}5(q_0 + w)\right)^{t+1}, \tag{5.6}$$

звідки

$$t > \log_{0{,}5(q_0 - w)} \Delta w - 1, \tag{5.7}$$

де $\Delta > \left|g_0(t) - \hat{g}_0(t)\right|$.

Вираз (5.6) дозволяє розрахувати імовірність того, що ІСКЗ перебуває в функціональному стані в момент часу t, а вираз (5.7) – оцінити тривалість перебування ІСКЗ у функціональному стані в залежності від значення характеристичного параметра СПБ w.

Отримане у вигляді (5.5) математичне підтвердження того факту, що при $t \to \infty$ ІСКЗ перебуватиме в стані z_{n+1}, робить актуальною задачу оцінювання тривалості перебування ІСКЗ у функціональному стані z_0 при управлінні значеннями $w = f_0(U)$, для чого проаналізуємо швидкість спадання функції залежності $g_0(t) = f(w,t)$ (5.6) на інтервалі часу $[0,t]$, де t розраховано за виразом (5.7). Введемо коефіцієнт затухання ϕ такий, що $g_0(0) = 2g_0(\phi)$. На основі (5.6) отримаємо вираз для розрахунку ϕ виду

$$\phi = \log_{0{,}5(q_0 + w)}(0{,}5w) - 1, \tag{5.8}$$

який розкриємо врахувавши функціональну залежність w і U:

$$0{,}5w \le \left(0{,}5(q_0 + w)\right)^{t_a + 1}, \tag{5.9}$$

де t_a – фіксований момент часу, такий, що $\phi \ge t_a$.

Розв’язком (5.9) відносно w буде нерівність

$$w \ge 2\alpha - q_0, \tag{5.10}$$

де $\alpha \in [q_0, 1]$ – дійсний корінь рівняння

$$w^{t_a + 1} - w + 0{,}5q_0 = 0. \tag{5.11}$$

Нерівність (5.10), із урахуванням (5.2), дозволяє визначити область допустимих значень $U = \{u_1, u_2, \ldots, u_n\}$, при яких ІСКЗ у момент часу $t_a \le \phi$ перебуватиме у стані z_0, системою обмежень

$$\begin{cases} \sum_{i=1}^{n} q_i u_i \ge \alpha(\alpha - q_0), \\ u_i \le 1, \end{cases} \tag{5.12}$$

де $i = \overline{1,n}$.

Подальше дослідження виразу (5.2) дозволяє передбачити існування залежності між імовірністю перебування ІСКЗ у функціональному стані $g_0(t)$ і ймовірностями впливу на систему відповідних НФ, формалізованих множиною $Q = \{q_1, q_2, \ldots, q_n\}$. Узагальнимо множини $Q = \{q_1, q_2, \ldots, q_n\}$ і $U = \{u_1, u_2, \ldots, u_n\}$, де u_i – імовірність того, що СПБ нейтралізує вплив q_i, індукуючими параметрами $q = \sum_{i=1}^{n} q_i$ і $u = q^{-1} \sum_{i=1}^{n} q_i u_i$, відповідно. Аналіз результату узагальнення матриці (5.1) для параметрів q і u дозволяє стверджувати поліноміальний характер залежності $g_0(t) = f(q)$ виду

$$g_0(t) = c_t q^t + c_{t-1} q^{t-1} + \ldots + c_1 q + c_0, \tag{5.13}$$

коефіцієнти c_k, $k = \overline{0,t}$ якої, із урахуванням виразу (5.2), можна отримати як $c_k = (-1)^k \sum_{l=0}^{\min(t-k,k)} C_{t-l}^k C_k^l (-u)^l$. Вираз (5.13) можна деталізувати до рівня q_i / u_i у вигляді

$$g_0(t) = \sum_{k=1}^{t} \sum_{l=1}^{\min(t-k,k)} (-1)^{l+k} C_{t-l}^k C_k^l \left(\sum_{i=1}^{n} q_i u_i \right)^l \left(\sum_{j=1}^{n} q_j \right)^{k-l}. \tag{5.14}$$

Підставивши у вираз (5.14) мінімальне та максимальне допустимі значення параметра q_i, $0 \le q_i \le 1$, отримаємо шукані залежності $g_0(t) = f(q_i)$:

$$g_0(t)\big|_{q_i=0} = 1, \tag{5.15}$$

$$g_0(t)\Big|_{q_i=1} = \begin{cases} 0, if\ t - \text{natural odd number}, \\ \left(\sum_{i=1}^{n} q_i u_i\right)^{0.5t}, \ if\ t - \text{natural even number}. \end{cases}$$

Аналіз виразів (5.15) дозволяє стверджувати, що імовірність перебування у стані z_0 ІСКЗ, яка експлуатується в реальних умовах, у парні моменти часу дорівнює нулю, а в непарні моменти часу відмінна від нуля і зменшується із зростанням параметра t, але швидкість спадання значення $g_0(t)$ тим повільніша, чим більше значення u_i, яке характеризує здатність СПБ протидіяти впливу i-го НФ.

На рис. 5.2а наведено результати обчислювального експерименту з оцінювання залежності імовірності перебування ІСКЗ у функціональному стані g_0 від часу t, який пройшов з моменту початку сеансу експлуатації системи, і двох варіантів налаштування СПБ для протидії одному НФ.

Результати отримано на основі виразу (5.2). Видно, що імовірність g_0 спадає із зростанням тривалості сеансу експлуатації t, що дозволяє зробити висновок, що ІСКЗ перейде в нефункціональний стан при $t \to \infty$ незалежно від налаштувань СПБ. Проте, отриманий математичний апарат дозволяє оцінити імовірності перебування ІСКЗ у функціональному стані g_0 від імовірності появи НФ q при заданому рівні надійності u правила СПБ, орієнтованого на протидію цьому НФ. На рис. 5.2б наведено криві, отримані на основі виразу (5.14), з яких видно, що при $u = 0{,}5$ для парних значень параметра t функція $g_0 = f(q)$ має явно виражений екстремум, а для непарних значень параметра t – є спадною, що підтверджується виразом (5.15) і доводить адекватність виразу (5.14). Вирази (5.10), (5.12) дозволяють оцінити імовірності перебування ІСКЗ у функціональному стані в момент часу t_α від імовірності появи НФ та налаштувань СПБ. Візуально оцінити такі залежності при впливі на ІСКЗ одного і двох НФ можна за результатами, наведеними на рис. 5.2в і 5.2г, відповідно. Практична цінність отриманих теоретичних результатів розкривається далі.

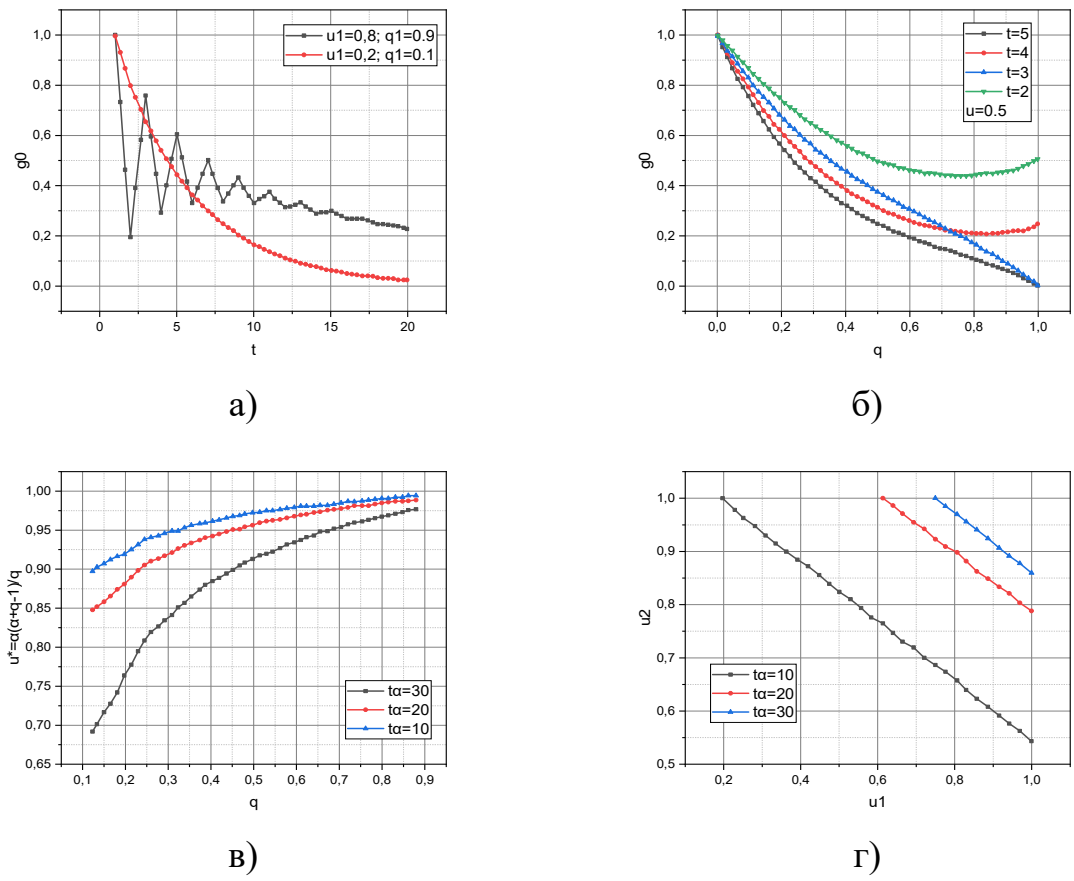


Рисунок 5.2 – Емпіричні дослідження із математичним апаратом для моделювання перебігу сеансу експлуатації ІСКЗ

Сформулюємо методику прикладного застосування створеної моделі перебігу сеансу експлуатації ІСКЗ та проведемо її аналіз. Нехай $u_{i,k}$ – імовірність того, що СПБ нейтралізує вплив на ІСКЗ i-го НФ застосувавши k-те правило, $1 \le k \le m$. Тоді ситуацію, коли СПБ застосовує для нейтралізації i-го НФ декілька правил опишемо виразом

$$u_i(W) = \sum_{l=1}^{m} (-1)^{l-1} \sum_{k_1 < k_2 < \ldots < k_l} (u_{i,k_1} x_{k_1})(u_{i,k_2} x_{k_2}) \cdots (u_{i,k_l} x_{k_l}), \tag{5.16}$$

де $W = \{w_1, w_2, \ldots, w_m\} \in \{0,1\}^m$ – множина бінарних змінних, які фіксують ініціацію w_i правила СПБ. Із виразу (5.16) очевидно, що значення параметра $u_i(X)$ характеризує надлишковість СПБ. Актуальною для досягнення обчислювальної ефективності СПБ задачею є мінімізація цієї надлишковості за рахунок управління кількістю правил для знешкодження i-го НФ для заданого значення параметра

$u_i(X)$. На основі цього твердження сформулюємо задачу оптимізації надлишковості СПБ у вигляді

$$C(W) = \sum_{k=1}^{m} c_k w_k \to \min, \tag{5.17}$$

де c_k – обчислювальна складність активації k-го правила СПБ для нейтралізації i-го НФ, а

$$W = \left\{ w \in \{0,1\}^m : \sum_{i=1}^{n} q_i u_i(w) \geq \alpha(\alpha - q_0) \right\} \tag{5.18}$$

є множиною, яка описує реакцію СПБ, де $q_0 = 1 - \sum_{i=1}^{n} q_i$, а параметр α розраховується із виразом (5.10). Цільова функція (5.17) і обмеження (5.18) утворюють задачу нелінійного бульового програмування, для розв'язання яких розроблено низку методів [284–286, 333], проте, універсального методу не існує.

Наведемо приклад розв'язання прикладної задачі, описаної виразами (5.16)–(5.18). Нехай на ІСКЗ можуть впливати два НФ, імовірності появи яких $Q = \{0{,}23, 0{,}59, 0{,}18\}$. Для протидії цим НФ у СПБ сформульовано $m = 5$ правил, обчислювальну складність активації яких описано множиною $C = \{6, 7, 4, 2, 4\}$, а матриця $\Pi = \begin{pmatrix} 0{,}96 & 0{,}50 & 0{,}47 & 0{,}50 & 0{,}07 \\ 0{,}66 & 0{,}43 & 0{,}60 & 0{,}69 & 0{,}92 \end{pmatrix}$ містить імовірності $u_{i,k}$ знешкодження i-го НФ в наслідок активації k-го правила СПБ, $i = \overline{1,2}$, $k = \overline{1,m}$. Знайдемо оптимальну конфігурацію W станом на моменти часу $t_\alpha = 10$ і $t_\alpha = 100$ з початку сеансу експлуатації ІСКЗ.

При $t_\alpha = 10$ із виразу (5.11) знайдемо α: $\alpha = 0{,}988 \in [0{,}23{,}1]$, тоді із виразу (5.18) отримаємо $W = \{w \in \{0,1\}^5 : 0{,}59u_1(w) + 0{,}18u_2(w) \geq 0{,}749\}$. Скориставшись методом [286] отримаємо розв'язок цієї задачі оптимізації: $W^* = \{1, 0, 1, 1, 0\}$, $C(W^*) = 12$. Отже, на момент часу $t_\alpha = 10$ з початку сеансу експлуатації ІСКЗ її перебування

у функціональному стані при появі описаних вище НФ забезпечуватиметься першим, третім і четвертим правилами СПБ для чого буде вжито 12 одиниць обчислювальної потужності.

При $t_a = 100$ із виразу (5.11) знайдемо α: $\alpha = 0{,}999 \in [0{,}23, 1]$, тоді із виразу (5.18) отримаємо

$$W = \left\{ w \in \{0, 1\}^5 : 0{,}59 u_1(w) + 0{,}18 u_2(w) \geq 0{,}772 \right\}.$$

Вже раніше використовуваний метод [286] показав, що при таких обмеженнях задача оптимізації не має розв'язку. Це означає, що $t_a = 100 > \phi$,

що входить у протиріччя із вмістом виразу (5.8), де параметр ϕ – граничний час перебування ІСКЗ у функціональному стані із урахуванням вихідних умов.

5.2 Модель цілісності інформаційної системи критичного застосування, забезпечуваної системною політикою безпеки

Інформаційна система є структурним і функціональним комплексом технічних, програмних та інших засобів, утвореним для підтримки одного чи кількох видів ІП та надання інформаційних послуг. Актуальним ІС притаманна ієрархічність, децентралізованість, функціональна розподіленість, паралельне виконання користувацьких задач тощо. Такі системи функціонують в умовах активного інформаційного обміну під впливом випадкових та негативних факторів із високою вартістю наслідків можливих порушень чи помилок у своїй роботі. Структура таких систем утворюється відповідно до мети функціонування і характеризується високою складністю та елементною насиченістю на програмному та апаратному рівнях, що відбиваються на складності управляючих алгоритмів та механізмів комутації елементів системи.

Критичне застосування ІС, обумовлене важливістю ІнР такої системи, потребує комплексного підходу до реалізації її безпеки, включаючи захист каналів зв'язку, захист процесу автентифікації суб'єктів-користувачів і сервісів, захист віддалених елементів системи, цілісний захисту всієї системи та створення алгоритмів поведінки системи при виявленні інформаційних загроз. Відповідно, під-

система захисту такої ІС має включати механізми захисту компонентів ІнС (ІС як такої), механізми мінімізації ризиків для компонентів ІнС і ІнР (даних, присутніх у ІС), комплекс процедурних, логічних і фізичних заходів, спрямованих на протидію загрозам ІнР і компонентам ІнС. Оскільки захищеність інформаційного ресурсу передбачає і неможливість його втрати внаслідок відмов компонентів ІнС, задачу убезпечення ІнР декомпозують на задачу забезпечення надійності апаратної платформи, яка гарантує безперервність функціонування ІнС, і задачу протидії та запобіганню загрозам ІнР. Вимоги для забезпечення безпечного функціонування ІС втілюються у СПБ. Дотримання СПБ гарантує, що при виникненні передбачених проблемних ситуацій внаслідок впливів негативних факторів відповідних типів, система буде здатна виконувати своє цільове призначення у повному обсязі.

Наведена вище інформація дозволяє стверджувати неможливість побудови адекватної математичної моделі для вичерпного опису функціонування ІС. Втім, критичне застосування ІС звужує як характеристики ІнС, так і обсяг і характер ІнР, які знаходяться в такій ІС. Ця обставина дозволяє відмовитися від надмірної деталізації і звузити об’єкт моделювання до процесу формування політики безпеки ІСКЗ, адекватний проблемний опис якого є досяжним за умови раціонального вибору математичного апарату.

Представимо узагальнену математичну модель ІС кортежем $\langle A, C, R, F, t \rangle$, де A – множина адміністраторів системи; C – множина суб’єктів-користувачів; R – множина ролей, кожна з яких визначає межі можливостей, виділених адміністраторами для відповідних класів суб’єктів; F – множина функцій, які забезпечують виконуваність визначених ролей; t – час. Під СПБ розумітимемо комплекс методів, який регулює управління, захист і розподіл інформації. Джерелом небезпеки, в такому разі, буде непередбачуваний результат перетину множини ролей і функцій для певного суб’єкта з причини недосконалості обраної СПБ: $R \cap F \forall c \in C$. Отже, надійною вважатиметься лише така СПБ, яка строго формалізована у парадигмі адекватного математичного апарату та описує дозволені процеси формування і взаємодії елементів множин із згаданого вище кортежу, контролює повно-

ту та прогнозованості результатів цієї взаємодії, виявляє та ідентифікує недозволені процеси і чітко регламентує відповідну реакцію системи для таких випадків.

На міжнародному рівні поняття інформаційної безпеки загалом регламентується стандартом ISO/IEC 27001:2013, у додатках якого описано комплекс профільних заходів. Безпосередньо питанням інформаційної безпеки присвячено 14 розділів додатку А стандарту. Загалом у стандарті перелічено 114 аспектів для убезпечення ІнС і ІнР системи, які узагальнено описують механізми інформаційної безпеки, в основному без вказівок щодо застосування конкретних технологій, що обумовлено швидкою їх еволюцією. Згідно зі стандартом ISO/IEC 27001:2013, захищена ІС має успішно протидіяти визначеним на етапі її проектування типам атак при заданих зовнішніх щодо системи експлуатаційних умовах. Зазвичай для досягнення такого результату у ПБІС включають механізми, що реалізують лише частину із сформульованих у стандарті ISO/IEC 27001:2013 114 аспектів. Такий спосіб створення ПБІС є значно швидшим, дешевшим і здебільшого задовольняє стандарт ISO/IEC 27001:2013, але не гарантує відсутності вразливостей, пов’язаних із відсутністю системного підходу при реалізації підсистеми. Інформаційний пошук не виявив робіт, де на належному рівні формалізації описано концепцію організації СПБ ІСКЗ, що обумовлює актуальність представлених далі досліджень.

Звичайно, дослідження питання безпеки ІСКЗ варто розпочати із визначення її як об’єкта. ІСКЗ є окремим випадком ІС, до складу якої, згідно зі стандартом ISO/IEC 2382:2015, входять системи збереження, пошуку і оброблювання інформації та відповідні організаційні ресурси, що забезпечують і розповсюджують інформацію. В широкому сенсі невід’ємними компонентами ІС є дані, технічне (в т. ч. комунікаційне) і програмне забезпечення, персонал і організаційні заходи. ІСКЗ, відповідно, це ІС, яка оперує настільки важливими даними, що отримання несанкціонованого доступу до них може спричинити значні матеріальні або людські втрати. Для системного представлення ІС можна скористатися ієрархічною мережевою моделлю OSI [335, 336], яка, проте, акцентує увагу на комунікаційній складовій, тоді як програмна складова представляється лише прикладним рівнем. У

табл. 5.1 прикладний рівень моделі OSI розкрито для системного представлення ІСКЗ як комплексної інформаційної структури із виділеними підрівнями, розташованими у строгій ієрархії.

Таблиця 5.1

Ієрархічна структурна організація ІСКЗ

Структурний блок:	Функція структурного блока		Ієрархічний рівень ІСКЗ
адміністрування	Встановлення привілей для множини ролей суб'єктів-користувачів		**L1 Адміністративний**
Автентифікації	Прийняття рішення щодо встановлення відповідності між особою суб'єкта-користувача та вибраною ним роллю за результатами процесу автентифікації. Забезпечує конфіденційність ІСКЗ		**L2 Автентифікаційний**
віртуалізації	Створення для автентифікованого суб'єкта-користувача віртуального інформаційного середовища відповідно до його ролі. Забезпечує цілісність інформаційного середовища ІСКЗ		**L3 Інтеграційний**
системної маршрутизації	Ініціює диспетчер програм ІСКЗ, який, відповідно до ролі авторизованого інтегратора, запускає системні прикладні програми, утиліти та сервіси доступу до ресурсів ІСКЗ		**L4 Диспетчерський**
мережевої навігації	Забезпечує ініціацію та підтримку інформаційного обміну із відповідними серверами ІСКЗ згідно з запитом на пошук інформації, згенерованого індивідуальним інформаційним середовищем суб'єкта		**L5 Навігаційний**
трансферу даних	Керуючись концепцією сеансу суб'єкт-системної взаємодії організовує доступ авторизованого засобу навігації до двох типів серверів ІСКЗ:		**L6 Серверний**
	Сервер реєстрації	***Ординарний сервер даних***	
менеджменту об'єктів	Підтримує конфіденційність, цілісність, готовність даних та процесів ІСКЗ на низькому рівні	Забезпечує адекватну реакцію на авторизований запит до цільових інформаційних ресурсів	**L7 Прикладний**
менеджменту ресурсів	Забезпечує доступ авторизованого інтерпретатора до менеджера ресурсів сервера. Підтримує функціонування ядра СУБД ІСКЗ		**L8 Менеджерський**
ресурсів	Забезпечує доступ авторизованого менеджера ресурсів до баз даних сервера серед яких, відповідно до типу сервера, виділяють:		**L9 Інформаційний**
	БД авторизації доступу, БД підсистеми комунікації, БД обліку інформації, БД архівації	БД авторизації доступу, БД профільних даних	

Подальшу формалізацію опису ІСКЗ, спираючись на представлену у табл. 5.1 її ієрархічну структуру, пропонується здійснювати на основі математичної моделі циркуляції інформації [45] в якій, за рахунок стандартизації інтерфейсів спряження прикладних процесів і комплексів сервісів із декомпозицією за рівнями доступу до ресурсів ІСКЗ, поєднується невразливість із варіативністю за кожним із аспектів захищеності даних: конфіденційністю, готовністю та цілісністю. Під варіативністю захисних механізмів в контексті конфіденційності і готовності розумітимемо раціональність процесу розмежування доступу до інформації із ав-

тентифікацією суб'єктів інформаційної взаємодії, а під невразливістю – адекватність моделі СПБ, що застосовується у ІСКЗ.

Необхідним при моделюванні СПБ є створення глобальної (синтаксичної) моделі, яка описує бажані властивості блока оброблювання даних ІСКЗ, а достатнім – створення локальної (семантичної) моделі, яка описує правила переходу між усталеними станами цієї підсистеми. За наявності локальної моделі ПБ остання є динамічною, а за відсутності локальної моделі – статичною. Динамічну модель ПБ із скінченною множиною станів називатимемо моделлю кінцевих станів. Основна теорема безпеки [145] теоретично обґрунтовує принципову безпеку моделі кінцевих станів БОД ІСКЗ: якщо у початковий момент часу глобальна ПБ виконується і всі переходи між станами БОД ІСКЗ задовольняють локальну модель ПБ, то у будь-який наступний момент часу глобальна модель ПБ також виконуватиметься, тобто вразливості ІСКЗ з'являються на етапі експлуатації, а не закладені безпосередньо в адекватну модель СПБ. Другою невід'ємною складовою гарантування безпеки ІСКЗ є блок розмежування доступу, який в контексті глобальної ПБ найкраще описується дискреційною моделлю, яка регламентує процес доступу суб'єктів-користувачів до ресурсів ІСКЗ у рамках визначених ролей, не враховуючи стани БОД ІСКЗ та переходи між ними. Втім, на відміну від моделі кінцевих станів, дискреційна модель є потенційно небезпечною. Убезпечити процеси дискреційного доступу можна запускаючи кожен з них у виділеному контрольованому та незалежному процесі із однозначно визначеною послідовністю переходів між кінцевими станами. В такій концепції довільний процес дискреційного доступу, керований положеннями глобальної ПБ, матиме відповідну алгоритмічну послідовність авторизованих доступів компонентів вищого рівня до ресурсів компонентів поточного або нижчого рівня, об'єднаних у чітку вертикальну ієрархію рівнів ІСКЗ, із параметрами, встановленими правилами локальної ПБ.

Щоб передати специфіку глобальної та локальної ПБ при організації дискреційного доступу до ресурсів ІСКЗ, у структуру якої входять БОД і БРД із описаними вище функціями і характеристиками, скористаємося математичним апаратом оцінних мереж Петрі [181–188]. У рамках концепції ОМП певний структуро-

ваний процес у ІСКЗ представляється базовим елементом – модулем порядку j рівня l_h, який є результатом групування відповідно до сенсу процесу кількох сусідніх рівнів ІСКЗ із номерами $l = \overline{l_l, l_h}$, де $l_l = l_h - j + 1$ – номер нижнього рівня цього шару ІСКЗ. Структура ОМП блочна. Її динаміка визначається переміщенням по заданих процедурах (перетворення, доступу та часової затримки) суб'єктів, які групуються у транзакти. Кожен модуль ОМП містить набір пар протилежних вхідних (простих) і вихідних (доступу) позицій, які характеризуються унікальними механізмами автентифікації. Кількість позицій доступу в модулі дорівнює кількості механізмів автентифікації.

Для ідентифікації модулів і контурів ОМП ІСКЗ введемо систему індексів, засновану на належності модулів рівням ІСКЗ та внутрішній нумерації модулів у контурах. Визначатимемо індекс j-го прядку як послідовність $i_1, i_2, \ldots, i_j$. Модулі l-го рівня ідентифікуються індексами порядку $(L - l)$, $l = \overline{1, L}$, де L – кількість рівнів ІСКЗ. Всі модулі деякого контуру поділяються на верхні та нижні за належністю верхнім та нижнім рівням ІСКЗ, відповідно. Довільний контур ОМП з індексом I містить єдиний верхній модуль з індексом I та $K[I]$ нижніх модулів з номерами $j = \overline{1, K[I]}$, відповідно, що еквівалентно виразу $I.j$. Відповідно, вважатимемо індекс J підіндексом індексу I – $J \subset I \equiv I \supset J$, якщо $I = J.i_1.i_2.\ldots.i_k$, а випадок $((J \subset I) \vee (J = I))$ позначатимемо $J \subseteq I \equiv I \supseteq J$. Логічна змінна $r = r(I, \alpha)$ описуватиме допустимість процедури автентифікації типу α у модулі із індексом I. Із кожною позицією доступу асоційовано процедуру часової затримки і процедуру перетворення. Із кожною позицією доступу асоційовано відповідну процедуру, яка фактично є операцією умовного розгалуження із відповідним маркуванням БРД ІСКЗ аналізованого суб'єкта в залежності від значень його ознак-атрибутів. Кожен суб'єкт може переміщуватися по позиціях однієї процедури автентифікації, яку проіндексовано в множині процедур автентифікації відповідної транзакції. Переміщення суб'єкта може відбуватися або із вхідної позиції модуля в протилежну їй вихідну, або у вхідну позицію тієї ж процедури автентифікації іншого модуля того ж контуру із спуском на один рівень ієрархії ІСКЗ, або у вхідну позицію

тієї ж процедури автентифікації модуля L-го рівня ієрархії ІСКЗ. Одночасно (паралельно) у системі можуть опрацьовуватися багато суб'єктів, при чому процедура доступу може бути відстрочена процедурою часової затримки, яка є властивою відповідному модулю, по завершенню якої виконується переміщення із можливим поглинанням або розмноженням представлення суб'єкта, до атрибутів якого застосовуватиметься процедура перетворення.

Узагальнимо описане вище, представивши модуль ОМП кортежем

$$u = \langle I, q, p \rangle \in U_l, \tag{5.19}$$

де $I = I(u) = i_1.i_2.i_3.\ldots.i_{L-1}$, $q = q[I,\alpha] \in Q_l$, $p = p[I,\alpha] \in P_l$, $|Q_l| = |P_l| \neq 0$, а множини модулів U_l, простих позицій Q_l і позицій доступу P_l рівня l є основою для синтезу множин модулів U, простих позицій Q, позицій доступу P у масштабі всієї ОМП ІСКЗ: $Q = \bigcup_{l=1}^{L} Q_l \neq \emptyset$, $|Q| < \infty$, $Q_k \cap Q_l \neq \emptyset$; $P = \bigcup_{l=1}^{L} P_l \neq \emptyset$, $|P| < \infty$, $P_k \cap P_l \neq \emptyset$; $U = \bigcup_{l=1}^{L} U_l \neq \emptyset$, $|U| < \infty$, $U_k \cap U_l \neq \emptyset$. На основі (5.19), узагальнимо структуру ОМП кортежем

$$E = \langle N, K, r, M_{in}, M_{out} \rangle, \tag{5.20}$$

де $K = K[I]$, $r = r[I,\alpha]$, $M_{in} = M_{in}[I,\alpha]$, $M_{out} = M_{out}[I,\alpha]$. Також введемо поняття множини позицій (шарів) ОМП S, $S = Q \cup P \neq \emptyset$, $Q \cap P \neq \emptyset$, $|S| < \infty$, $|Q| = |P|$, яка узагальнює множини простих позицій Q та позицій доступу P. Шар $S_{l_l \ldots l_h}$ рівня l_h із нижнім рівнем l_l – це частина ОМП $B_0 = S_{1\ldots L}$ порядку $j = l_h - l_l + 1$, яка відноситься до шару ОМП порядку j рівня l_h і містить лише модулі цього шару ОМП і дуги, що їх з'єднують. Для шару першого порядку $S_{l_h \ldots l_h} = U_{l_h}$. Шари ОМП $S_{l_{li} \ldots l_{hi}}$ і $S_{l_{lj} \ldots l_{hj}}$ перетинаються, якщо в них є хоча б один спільний рівень ОМП $(\max(l_{li}, l_{lj}) \leq \min(l_{hi}, l_{hj}))$, у протилежному випадку ці шари не перетинаються. Якщо шари перетинаються, то для них можна визначити операції об'єднання і перетину. Об'єднанням шарів ОМП $S_{l_{li} \ldots l_{hi}}$ і $S_{l_{lj} \ldots l_{hj}}$ буде шар

$S_{l_l \ldots l_h} = S_{l_{li} \ldots l_{hi}} \cup S_{l_{lj} \ldots l_{hj}}$, де $l_l = \min(l_{li}, l_{lj})$, $l_h = \max(l_{hi}, l_{hj})$, а перетином цих шарів буде шар $S_{l_l \ldots l_h} = S_{l_{li} \ldots l_{hi}} \cap S_{l_{lj} \ldots l_{hj}}$.

Описане вище дозволяє ввести ще один рівень узагальнення при моделюванні ІСКЗ оцінною мережею Петрі, який називатимемо системним контуром $B_{l_l \ldots l_h}$ рівня l_h із нижнім рівнем l_l та індексом I, який є частиною всієї ОМП ІСКЗ $B_0 = B_{1 \ldots L}(0)$ порядку $j = l_h - l_l + 1$, яку вписано у шар $S_{l_l \ldots l_h}$, індекси модулів у складі якої задовольняють $J \subseteq I$. Порядок СК показує кількість рівнів ОМП, на яких розташовано модулі, що входять до його складу, а рівень СК вказує на найвищий рівень ОМП у його складі. СК B накриває множину рівнів ОМП, серед яких є найвищий, найнижчий і проміжні рівні, на кожному з яких розташовується модулі, для ідентифікації яких введемо змінні $Q_l(B)$, $P_l(B)$, $U_l(B)$, які позначають множину простих позицій, множину позицій доступу і множину модулів на l-му рівні СК, відповідно. Узагальнивши введені позначення для всіх рівнів СК, отримаємо відповідні системні множини $Q(B) = \bigcup_{l=l_l}^{l_h} Q_l(B)$, $P(B) = \bigcup_{l=l_l}^{l_h} P_l(B)$, $U(B) = \bigcup_{l=l_l}^{l_h} U_l(B)$. Проаналізуємо операції із системними контурами, взявши за аналоги описані вище операції із шарами ОМП ІСКЗ. Так системні контури перетинаються, якщо мають хоча б один спільний модуль, тобто два системні контури ОМП ІСКЗ перетинаються, якщо верхній модуль одного із них входить до складу іншого. Таке твердження має ряд наслідків, а саме: системні контури, вписані в один і той самий шар не перетинаються; системні контури однакового рівня, але різного порядку або не перетинаються, або мають спільний верхній модуль і СК вищого порядку включає в себе СК нижчого порядку; якщо системні контури із однаковим нижнім рівнем перетинаються, то вони мають різний порядок і СК вищого порядку включає в себе СК нижчого порядку. Зрештою, результатом перетину системних контурів буде СК, до складу якого входять всі спільні модулі вихідних системних контурів: нехай $B_{l_l \ldots l_h}(I) = B_{l_{li} \ldots l_{hi}}(I_i) \cap B_{l_{lj} \ldots l_{hj}}(I_j)$,

$l_h = \min(l_{hi}, l_{hj})$, $l_l = \max(l_{li}, l_{lj})$, тоді якщо $l_h = l_{hi}$, то $I = I_i$, або якщо $l_h = l_{hj}$, то $I = I_j$. Така інтерпретації операцій із системними контурами ОМП ІСКЗ узгоджується із процесом формалізації її глобальної ПБ. Якщо розуміти глобальну ПБ ІСКЗ як систему привілеїв дискреційного доступу до конфіденційних даних із комплексним розгалуженим процесом автентифікації, то її математичною моделлю на рівні СК $B = B_{l_l \ldots l_h}(I_0)$ буде підмножина позицій доступу $\Omega_G(B)$ нижнього рівня СК: $\Omega_G(B) \subseteq P_{l_l}(B)$. Відповідно, всі позиції доступу нижнього рівня маркуватимуться за відповідністю глобальній ПБ ІСКЗ: $(\forall p = p[I,\alpha] \in P_{l_l}(B) \setminus \Omega_G(B))(M_{out}[I,\alpha] = 0)$, що унеможливлює нелегальний дискреційний доступ до ресурсів нижнього рівня без порушення маркування: $(\exists p = p[I,\alpha] \in P_{l_l}(B) \setminus \Omega_G(B))(M_{out}[I,\alpha] = 1)$.

Для інтеграції дискреційної моделі автентифікації в створювану модель СПБ ІСКЗ в контексті описаного вище підходу до формування її глобальної ПБ, введемо поняття дискреційної ПБ ІСКЗ, яка визначатиме привілеї дискреційного доступу суб'єктів до вибраного рівня ІСКЗ за результатами комплексного розгалуженого процесу автентифікації. За аналогією з описаним вище, представимо дискреційну ПБ l-го рівня для СК $B = B_{l_l \ldots l_h}(I_0)$ підмножиною позицій доступу $\Omega_{Dl}(B)$ до l-го рівня СК: $\Omega_{Dl}(B) \subseteq P_l(B)$, $l_l \le l \le l_h$. Виконання дискреційної ПБ $\Omega_{Dl}(B)$ на l-му рівні СК B означатиме відповідне маркування всіх позицій доступу на цьому рівні: $(\forall p = p[I,\alpha] \in P_l(B) \setminus \Omega_{Dl}(B))(M_{out}[I,\alpha] = 0)$, а спроба порушення ПБ маркуватиметься як $(\exists p = p[I,\alpha] \in P_l(B) \setminus \Omega_{Dl}(B))(M_{out}[I,\alpha] = 1)$.

На відміну від глобальної ПБ, локальна ПБ ІСКЗ описуватиме взаємодію суб'єктів як проекцію на концепцію ієрархічного представлення ІСКЗ із реалізацією правила «керуючий-керований» для пар суб'єктів, розташованих на сусідніх рівнях ієрархії системи. Відповідно до цього правила, суб'єкти поточного рівня ієрархії є керованими суб'єктами вищого сусіднього рівня ієрархії ІСКЗ. Локальна ПБ $\Omega_{Ll}(B)$ для l-го рівня в СК $B = B_{l_l \ldots l_h}(I_0)$ описуватиметься множиною

$\Omega_{Ll}(B)=\left\{\langle I(u),\alpha,r[I(u),\alpha]\rangle \middle| u\in U_l(B),\alpha=\overline{1,N}\right\}$, $l_l\le l\le l_h$ і визначатиме ознаки результатів автентифікації в модулях цього рівня, які входять у СК. Відповідно, підмножина позицій доступу, дозволених локальною ПБ на l-му рівні у СК B, описується підмножиною $\left\{p=p[I(u),\alpha]\in P_l(B) \middle| u\in U_l(B),\alpha=\overline{1,N},\langle I(u),\alpha,1\rangle\in\Omega_{ll}(B)\right\}$ і дозволяє описати прецеденти дотримання та порушення локальної ПБ виразами

$$\left(\forall p=p\left[I(u),\alpha\right]\in P_l(B) \middle| u\in U_l(B),\alpha=\overline{1,N},\left\langle I(u),\alpha,0\right\rangle\in\Omega_{Ll}(B)\right)\times$$
$$\times\left(M_{out}\left[I,\alpha\right]=0\right)$$

та

$$\left(\exists p=p\left[I(u),\alpha\right]\in P_l(B) \middle| u\in U_l(B),\alpha=\overline{1,N},\left\langle I(u),\alpha,0\right\rangle\in\Omega_{Ll}(B)\right)\times$$
$$\times\left(M_{out}\left[I,\alpha\right]=1\right),$$

відповідно. Деталізація процесу формування локальної ПБ ІСКЗ потребує диференціації правил безпечного управління взаємодією суб’єктів із урахуванням їх ієрархії на рівні контуру ОМП. Єдиний верхній модуль довільного контуру ОМП ІСКЗ із індексом I асоціюється із управляючим суб’єктом, а його нижні модулі (із номерами $\overline{1,K[I]}$ у масштабі контуру, або із номерами $\overline{I.1,I.K[I]}$ у масштабі всієї ОМП ІСКЗ), асоціюються із фактично або потенційно керованими суб’єктами. Розвинемо цю концепцію у поняття ПБ для контуру в складі ІСКЗ, яка встановлює ознаки допустимості процесів автентифікації в усіх модулях контуру. Для формалізації ПБ для контуру опишемо механізм узгодження ознак допустимості процесів автентифікації і відповідних множин позицій доступу між верхнім модулем та всіма нижніми модулями контуру. Виходячи із факту однотипності процесів автентифікації для управляючого і керованого суб’єктів можна стверджувати, що допустимість процесів автентифікації для керованого суб’єкта потребує допустимості тих же процесів автентифікації і для керуючого суб’єкта, і навпаки. Цей тезис дозволяє сформулювати правила узгодження ознак допустимості процесів автентифікації в ПБ для контуру:

$$\left(\exists j \in \overline{1,K(I)}\right)\left(r[I.j,\alpha]=1\right) \Rightarrow \left(r[I,\alpha]=1\right), \tag{5.21}$$

$$\left(r[I,\alpha]=0\right) \Rightarrow \left(\forall j \in \overline{1,K[I]}\right)\left(r[I.j,\alpha]=0\right), \tag{5.22}$$

де $\alpha = \overline{1,N}$, $I = I(u)$, $u \in U \setminus U_1$.

Врахуємо концепцію ПБ для контуру при формуванні локальної ПБ для СК $B = B_{l_l \ldots l_h}(I_0)$:

$$\Omega_L(B) = \bigcup_{l=l_l}^{l_h} \Omega_{Ll}(B) = \left\{ \left\langle I(u), \alpha, r[I(u),\alpha] \right\rangle \middle| u \in U(B), \alpha = \overline{1,N} \right\}, \tag{5.23}$$

де всі ознаки $r[I(u),\alpha]$ по всіх контурах взаємоузгоджені за правилами (5.21), (5.22). Розширимо застосування правил (5.21), (5.22) на процес формалізації локальної ПБ для СК $B = B_{l_l \ldots l_h}(I_0)$:

$$\begin{gathered}\left(r[I,\alpha]=1\right) \Rightarrow \left(\forall J \subset I \middle| p[J,\alpha] \in P(B)\right)\left(r[J,\alpha]=1\right), \\ u \in U(B) \setminus U_{l_h}(B),\end{gathered} \tag{5.24}$$

$$\begin{gathered}\left(r[I,\alpha]=0\right) \Rightarrow \left(\forall J \subset I \middle| p[J,\alpha] \in P(B)\right)\left(r[J,\alpha]=0\right), \\ u \in U(B) \setminus U_{l_l}(B),\end{gathered} \tag{5.25}$$

де $\alpha = \overline{1,N}$, $I = I(u)$.

Нарешті, на основі правил (5.21)–(5.25), формалізуємо процес узгодження привілей дискреційного доступу для всієї ПБ ІСКЗ, об’єднавши рівневі дискреційні ПБ для всіх рівнів ІСКЗ із їх узгодженням на основі ПБ для контурів:

$$\Omega_{DP}(B) = \bigcup_{l=l_l}^{l_h} \Omega_{Dl}(B) \subseteq P(B), \tag{5.26}$$

де $B = B_{l_l \ldots l_h}(I_0)$, множини $\Omega_{Dl}(B)$ узгоджено за правилами (5.21), (5.22), а процеси узгодження позицій доступу та ознак допустимості процесів автентифікації еквівалентні. Еквівалентність (5.21), (5.22) визначає аналітичний вигляд правила узгодження позицій доступу при визначенні ПБ для контурів ОМП:

$$\left(\exists j \in \overline{1,K}\right)\left(p[I.j,\alpha] \in \Omega_{DP}\right) \Rightarrow \left(p[I,\alpha] \in \Omega_{DP}\right), \tag{5.27}$$

$$\left(p[I,\alpha] \notin \Omega_{DP}\right) \Rightarrow \left(\forall j \in \overline{1,K[I]}\right)\left(p[I.j,\alpha] \notin \Omega_{DP}\right), \tag{5.28}$$

при $\alpha = \overline{1,N}$, $I = I(u)$, $u \in U \setminus U_1$.

Узагальнивши сформульовані для різних рівнів ІСКЗ правила (5.27) і (5.28), отримаємо правила узгодження позицій доступу в дискреційній ПБ для СК $B = B_{l_l \ldots l_h}(I_0)$:

$$\begin{gathered}(p[I,\alpha] \in \Omega_{DP}(B)) \Rightarrow (\forall J \subset I | p[J,\alpha] \in P(B))(p[J,\alpha] \in \Omega_{DP}(B)), \\ u \in U(B) \setminus U_{l_h}(B),\end{gathered} \tag{5.29}$$

$$\begin{gathered}(p[I,\alpha] \notin \Omega_{DP}(B)) \Rightarrow (\forall J \supset I | p[J,\alpha] \in P(B))(p[J,\alpha] \notin \Omega_{DP}(B)), \\ u \in U(B) \setminus U_{l_l}(B),\end{gathered} \tag{5.30}$$

при $\alpha = \overline{1,N}$, $I = I(u)$.

Отже, дискреційну ПБ ОМП ІСКЗ можна визначати множиною позицій доступу відповідно до правил (5.29), (5.30), але такому представленню властива інформаційна збитковість, якої позбавлене глобалізоване системне представлення дискреційної ПБ:

$$\begin{gathered}\Omega_{DG}(B) \subseteq \Omega_{Dp}(B) \Rightarrow (p[I,\alpha] \in \Omega_{DG}(B)) \Leftrightarrow \\ \Leftrightarrow ((p[I,\alpha] \in \Omega_{Dp}(B)) \wedge (\forall J \supset I | p[J,\alpha] \in P(B))(p[J,\alpha] \notin \Omega_{Dp}(B))),\end{gathered} \tag{5.31}$$

де $\alpha = \overline{1,N}$, $I = I(u)$, $u \in U(B)$. Існує і зворотна можливість – ідентифікувати множину $\Omega_{DP}(B)$ за визначеною множиною $\Omega_{DG}(B)$:

$$\begin{gathered}(p[I,\alpha] \in \Omega_{DP}(B)) \Leftrightarrow \\ \Leftrightarrow ((\exists J \supseteq I | p[J,\alpha] \in P(B))(p[J,\alpha] \in \Omega_{DG}(B))).\end{gathered} \tag{5.32}$$

Як наслідок, для однотипного процесу автентифікації індекс однієї з двох позицій доступу p' і p'' з глобалізованої множини позицій доступу $\Omega_{DG}(B)$ не може бути підіндексом іншої:

$$\begin{gathered}(p' = p[I',\alpha] \in \Omega_{DG}(B) \wedge p'' = p[I'',\alpha] \in \Omega_{DG}(B)) \Rightarrow \\ \Rightarrow (I' \not\subset I'' \wedge I'' \not\subset I').\end{gathered} \tag{5.33}$$

Формалізуємо множину $\Omega_{Dp}(B)$ для цієї ж ПБ на основі виразу (5.32) із урахуванням виразу (5.33). Включимо в множину $\Omega_{Dp}(B)$ кожен елемент з $\Omega_{DG}(B)$ і всі типи процесів автентифікації, індекси яких є його підіндексами:

$$\left(\forall p = p[I,\alpha] \in P(B) \setminus \Omega_{Dp}(B)\right)\left(M_{out}[I,\alpha] = 0\right), \tag{5.34}$$

що робить всі позиції доступу, які не марковані цією ПБ, недоступними, а спроба їх ініціації приведе до відповідного маркування:

$$\left(\exists p = p[I,\alpha] \in P(B) \setminus \Omega_{Dp}(B)\right)\left(M_{out}[I,\alpha] = 1\right). \tag{5.35}$$

На рівні БОД ІСКЗ виконання дискреційної ПБ гарантується дотриманням у СК B ОМП локальної ПБ $\Omega_L(B)$ і дискреційної ПБ $\Omega_{Dp}(B)$, формалізованих виразами (5.23) і (5.26), відповідно, і виконанням правила

$$\left(\forall p = p[I,\alpha] \in P(B)\right)\left(\left(p \in \Omega_{Dp}(B)\right) \Leftrightarrow \left(r[I,\alpha] = 1\right)\right).$$

Відповідно, якщо в певний момент часу визначена для деякого СК ОМП ІСКЗ дискреційна ПБ виконується та всі переміщення суб'єктів у цьому СК задовольняють визначеній у СК локальній ПБ, то в будь-який подальший момент часу дискреційна ПБ у СК також виконуватиметься. Виконаємо маркування доступних у рамках вибраної локальної ПБ позицій у СК $B = B_{l_l \ldots l_h}(I_0)$:

$$\begin{aligned} &\left(\forall p = p[I,\alpha] \in P_{l_h}(B)\right)\left(\left(M_{in}[I,\alpha] = 1\right) \wedge \left(M_{out}[I,\alpha] = 0\right)\right) \wedge \\ &\wedge \left(\forall p = p[I,\alpha] \in P(B) \setminus P_{l_h}(B)\right)\left(M_{in}[I,\alpha] = M_{out}[I,\alpha] = 0\right). \end{aligned} \tag{5.36}$$

Називатимемо маркування (5.36) базовим. На його основі отримаємо індуковане дискреційною ПБ маркування

$$\begin{aligned} &\left(\forall p = p[I,\alpha] \in \Omega_{DG}(B)\right)\left(\left(M_{in}[I,\alpha] = 0\right) \wedge \left(M_{out}[I,\alpha] = 1\right)\right) \wedge \\ &\wedge \left(\forall p = p[I,\alpha] \in P(B) \setminus \Omega_{DG}(B)\right)\left(M_{in}[I,\alpha] = M_{out}[I,\alpha] = 0\right), \end{aligned} \tag{5.37}$$

Вираз (5.37) описує процес дискреційного доступу до ресурсів нижнього рівня ієрархії ІСКЗ із привілеями, максимально допустимими визначною в СК дискреційною ПБ. Врахувавши вирази (5.36) і (5.37), вважатимемо, що глобальна ПБ $\Omega_G(B)$ у СК B індукується визначеною для цього ж СК дискреційною ПБ $\Omega_{GD}(B)$, якщо $\Omega_G(B) = \Omega_{GD}(B)$. Підмножина $\Omega_G(B) \subset P(B)$ задовольняє вираз (5.33), адже всі її елементи належать нижньому рівню ієрархії ІСКЗ, тому у довільному СК будь-яка глобальна ПБ індукується єдиною дискреційною ПБ, яка, в свою чергу, індукується локальною ПБ. Таким чином, для довільної, заданої виразом (5.33) для СК ОМП, глобальної ПБ можна визначити процедури доступу

(5.29) і перетворення (5.30) для цього СК так, що індуковане цією глобальною ПБ маркування СК (5.37) може бути отримано із базового маркування (5.36) в рамках локальної ПБ, яка індукувала цю глобальну ПБ.

Описані вище вирази математично коректно та цілісно описують взаємодію всіх рівнів ПБ в ієрархічній ІСКЗ із ПОД і ПРД складовими, але, враховуючи комплексний характер ІСКЗ, актуальним є питання узгодження ПБ системних контурів у масштабах всієї ІСКЗ. Для дослідження цього питання визначимо поняття слабкої і сильної сумісності (несумісності) ПБ. Слабкою сумісністю (несумісністю) ПБ Ω_i та Ω_j вважатимемо відсутність (існування) безпосередніх протиріч між ними і позначатимемо $\Omega_i \sim \Omega_j$ ($\Omega_i \not\sim \Omega_j$). Сильною сумісністю (несумісністю) ПБ Ω_i та Ω_j вважатимемо відсутність (існування) протиріч при їх розповсюдженні на всю ОМП ІСКЗ і позначатимемо $\Omega_i \approx \Omega_j$ ($\Omega_i \not\approx \Omega_j$). Також вважатимемо дві довільні ПБ однотипними, якщо вони стосуються одного рівня ОМП-представлення ІСКЗ (обидві глобальні, обидві локальні і т. д.), або різнотипними у протилежних випадках.

Аналітично опишемо поняття сумісності (несумісності) однотипних ПБ:

$$\begin{gathered}(\Omega_G(B_i) \sim \Omega_G(B_j)) \Leftrightarrow (\Omega_G(B_i) \cap P_N(B_j) = \Omega_G(B_j) \cap P_N(B_i)),\\ (\Omega_G(B_i) \not\sim \Omega_G(B_j)) \Leftrightarrow (\Omega_G(B_i) \cap P_N(B_j) \neq \Omega_G(B_j) \cap P_N(B_i)).\end{gathered} \tag{5.38}$$

$$\begin{gathered}(\Omega_{Dl}(B_i) \sim \Omega_{Dl}(B_j)) \Leftrightarrow (\Omega_{Dl}(B_i) \cap P_N(B_j) = \Omega_{Dl}(B_j) \cap P_N(B_i)),\\ (\Omega_{Dl}(B_i) \not\sim \Omega_{Dl}(B_j)) \Leftrightarrow (\Omega_{Dl}(B_i) \cap P_N(B_j) \neq \Omega_{Dl}(B_j) \cap P_N(B_i)).\end{gathered} \tag{5.39}$$

$$\begin{gathered}(\Omega_{Ll}(B_i) \sim \Omega_{Ll}(B_j)) \Leftrightarrow (|\Omega_{Ll}(B_i) \cap \Omega_{Ll}(B_j)| = N|U_l(B_i) \cap U_l(B_j)|),\\ (\Omega_{Ll}(B_i) \not\sim \Omega_{Ll}(B_j)) \Leftrightarrow (|\Omega_{Ll}(B_i) \cap \Omega_{Ll}(B_j)| < N|U_l(B_i) \cap U_l(B_j)|).\end{gathered} \tag{5.40}$$

$$\begin{gathered}(\Omega_L(B_i) \sim \Omega_L(B_j)) \Leftrightarrow (|\Omega_L(B_i) \cap \Omega_L(B_j)| = N|U_l(B_i) \cap U(B_j)|),\\ (\Omega_{Ll}(B_i) \not\sim \Omega_{Ll}(B_j)) \Leftrightarrow (|\Omega_L(B_i) \cap \Omega_L(B_j)| < N|U(B_i) \cap U(B_j)|).\end{gathered} \tag{5.41}$$

$$\begin{gathered}(\Omega_{Dp}(B_i) \sim \Omega_{Dp}(B_j)) \Leftrightarrow (\Omega_{Dp}(B_i) \cap P(B_j) = \Omega_{Dp}(B_j) \cap P(B_i)),\\ (\Omega_{Dp}(B_i) \not\sim \Omega_{Dp}(B_j)) \Leftrightarrow (\Omega_{Dp}(B_i) \cap P(B_j) \neq \Omega_{Dp}(B_j) \cap P(B_i)).\end{gathered} \tag{5.42}$$

Із виразів (5.38)–(5.42) видно, що слабка сумісність (несумісність) однотипних ПБ у одному і тому ж системному контурі трактується як їх рівність (нерівність):

$$\begin{gathered}\left(\left(\Omega(B_i)\sim\Omega(B_j)\right)\wedge\left(B_i=B_j\right)\right)\Leftrightarrow\left(\Omega(B_i)=\Omega(B_j)\right),\\ \left(\left(\Omega(B_i)\not\sim\Omega(B_j)\right)\vee\left(B_i\neq B_j\right)\right)\Leftrightarrow\left(\Omega(B_i)\neq\Omega(B_j)\right).\end{gathered}\tag{5.43}$$

Сильну сумісність однотипних ПБ $\Omega(B_i)$ та $\Omega(B_j)$ у системних контурах B_i та B_j, відповідно, розумітимемо як їх одночасну слабку сумісність із певною єдиною ПБ всієї ОМП B_0 того ж типу:

$$\begin{gathered}\left(\Omega(B_i)\approx\Omega(B_j)\right)\Leftrightarrow\left(\left(\exists\Omega(B_0)\right)\left(\left(\Omega(B_i)\sim\Omega(B_0)\right)\wedge\left(\Omega(B_j)\sim\Omega(B_0)\right)\right)\right),\\ \left(\Omega(B_i)\not\approx\Omega(B_j)\right)\Leftrightarrow\left(\left(\forall\Omega(B_0)\right)\left(\left(\Omega(B_i)\not\sim\Omega(B_0)\right)\vee\left(\Omega(B_j)\not\sim\Omega(B_0)\right)\right)\right).\end{gathered}\tag{5.44}$$

Із виразу (5.44) видно, що сильна сумісність (несумісність) однотипних ПБ у одному і тому ж системному контурі трактується як їх рівність (нерівність):

$$\begin{gathered}\left(\left(\Omega(B_i)\sim\Omega(B_j)\right)\wedge\left(B_i=B_j\right)\right)\Leftrightarrow\left(\left(\Omega(B_i)\approx\Omega(B_j)\right)\wedge\left(B_i=B_j\right)\right)\Leftrightarrow\\ \Leftrightarrow\left(\Omega(B_i)=\Omega(B_j)\right).\\ \left(\left(\Omega(B_i)\not\sim\Omega(B_j)\right)\vee\left(B_i=B_j\right)\right)\Leftrightarrow\left(\left(\Omega(B_i)\not\approx\Omega(B_j)\right)\vee\left(B_i=B_j\right)\right)\Leftrightarrow\\ \Leftrightarrow\left(\Omega(B_i)\neq\Omega(B_j)\right).\end{gathered}\tag{5.45}$$

На основі вже сформульованого, аналітично опишемо поняття сумісності (несумісності) різнотипних ПБ. Опишемо слабку сумісність (несумісність) визначеної на l-му рівні у системному контурі B_i дискреційної ПБ $\Omega_{Dl}(B_i)$ із визначеною для СК B_j дискреційною ПБ $\Omega_{Dp}(B_j)$ виразами:

$$\begin{gathered}\left(\Omega_{Dl}(B_i)\sim\Omega_{Dp}(B_j)\right)\Leftrightarrow\left(\Omega_{Dl}(B_i)\cap P(B_j)=\Omega_{Dp}(B_j)\cap P_l(B_i)\right),\\ \left(\Omega_{Dl}(B_i)\not\sim\Omega_{Dp}(B_j)\right)\Leftrightarrow\left(\Omega_{Dl}(B_i)\cap P(B_j)\neq\Omega_{Dp}(B_j)\cap P_l(B_i)\right).\end{gathered}\tag{5.46}$$

Слабку сумісність (несумісність) дискреційних ПБ для різних рівнів системи формалізуємо як похідну форму слабкої сумісності (несумісності) однотипних дискреційних ПБ:

$$\left(\Omega_{Dl_i}(B_i)\sim\Omega_{Dl_j}(B_j)\right)\Leftrightarrow\tag{5.47}$$

$$\Leftrightarrow \left(\left(\exists \Omega_{Dp}(B_i) \middle| \Omega_{Dl_i}(B_i) \sim \Omega_{Dp}(B_i)\right) \times \right.$$

$$\left. \times \left(\exists \Omega_{Dp}(B_j) \middle| \Omega_{Dl_j}(B_j) \sim \Omega_{Dp}(B_j)\right)\left(\Omega_{Dp}(B_i) \sim \Omega_{Dp}(B_j)\right)\right),$$

$$\left(\Omega_{Dl_i}(B_i) \nsim \Omega_{Dl_j}(B_j)\right) \Leftrightarrow$$

$$\Leftrightarrow \left(\left(\forall \Omega_{Dp}(B_i) \middle| \Omega_{Dl_i}(B_i) \sim \Omega_{Dp}(B_i)\right) \times \right.$$

$$\left. \times \left(\forall \Omega_{Dp}(B_j) \middle| \Omega_{Dl_j}(B_j) \sim \Omega_{Dp}(B_j)\right)\left(\Omega_{Dp}(B_i) \nsim \Omega_{Dp}(B_j)\right)\right).$$

Аналогічно, опишемо слабку сумісність (несумісність) визначеної на l-му рівні в системному контурі B_i локальної ПБ $\Omega_{Ll}(B_i)$ із локальною ПБ $\Omega_L(B_j)$ у СК B_j виразами

$$\begin{aligned} &\left(\Omega_{Ll}(B_i) \sim \Omega_L(B_j)\right) \Leftrightarrow \left(\left|\Omega_{Ll}(B_i) \cap \Omega_L(B_j)\right| = N \left|U_l(B_i) \cap U(B_j)\right|\right), \\ &\left(\Omega_{Ll}(B_i) \nsim \Omega_L(B_j)\right) \Leftrightarrow \left(\left|\Omega_{Ll}(B_i) \cap \Omega_L(B_j)\right| < N \left|U_l(B_i) \cap U(B_j)\right|\right). \end{aligned} \tag{5.48}$$

Слабку сумісність (несумісність) локальних ПБ різних рівнів формалізуємо як похідну форму слабкої сумісності (несумісності) однотипних локальних ПБ:

$$\begin{aligned} &\left(\Omega_{Ll_i}(B_i) \sim \Omega_{Ll_j}(B_j)\right) \Leftrightarrow \\ &\Leftrightarrow \left(\left(\exists \Omega_L(B_i) \middle| \Omega_{Ll_i}(B_i) \sim \Omega_L(B_i)\right) \times \right. \\ &\left. \times \left(\exists \Omega_L(B_j) \middle| \Omega_{Ll_j}(B_j) \sim \Omega_L(B_j)\right)\left(\Omega_L(B_i) \sim \Omega_L(B_j)\right)\right), \\ &\left(\Omega_{Ll_i}(B_i) \nsim \Omega_{Ll_j}(B_j)\right) \Leftrightarrow \\ &\Leftrightarrow \left(\left(\forall \Omega_L(B_i) \middle| \Omega_{Ll_i}(B_i) \sim \Omega_L(B_i)\right) \times \right. \\ &\left. \times \left(\forall \Omega_L(B_j) \middle| \Omega_{Ll_j}(B_j) \sim \Omega_L(B_j)\right)\left(\Omega_L(B_i) \nsim \Omega_L(B_j)\right)\right). \end{aligned} \tag{5.49}$$

Взаємну слабку сумісність (несумісність) локальної, дискреційної і глобальної ПБ у певному СК формалізуємо як результат індукування локальної ПБ дискреційною ПБ і, в свою чергу, глобальною ПБ:

$$\begin{aligned} &\left(\Omega_L(B_i) \sim \Omega_{Dp}(B_j)\right) \Leftrightarrow \\ &\Leftrightarrow \left(\left(\exists \Omega_{Dp}(B_i) \middle| \Omega_L(B_i) \sim \Omega_{Dp}(B_i)\right)\left(\Omega_{Dp}(B_i) \sim \Omega_{Dp}(B_j)\right)\right), \end{aligned} \tag{5.50}$$

$$\left(\Omega_L(B_i) \not\sim \Omega_{Dp}(B_j)\right) \Leftrightarrow$$
$$\Leftrightarrow \left(\left(\forall \Omega_{Dp}(B_i) \middle| \Omega_L(B_i) \sim \Omega_{Dp}(B_i)\right)\left(\Omega_{Dp}(B_i) \not\sim \Omega_{Dp}(B_j)\right)\right).$$
$$\left(\Omega_L(B_i) \sim \Omega_G(B_j)\right) \Leftrightarrow$$
$$\Leftrightarrow \left(\left(\exists \Omega_G(B_i) \middle| \Omega_L(B_i) \sim \Omega_G(B_i)\right)\left(\Omega_G(B_i) \sim \Omega_G(B_j)\right)\right),$$
$$\left(\Omega_L(B_i) \not\sim \Omega_G(B_j)\right) \Leftrightarrow \tag{5.51}$$
$$\Leftrightarrow \left(\left(\forall \Omega_G(B_i) \middle| \Omega_L(B_i) \sim \Omega_G(B_i)\right)\left(\Omega_G(B_i) \not\sim \Omega_G(B_j)\right)\right).$$
$$\left(\Omega_{Dp}(B_i) \sim \Omega_G(B_j)\right) \Leftrightarrow$$
$$\Leftrightarrow \left(\left(\exists \Omega_G(B_i) \middle| \Omega_{Dp}(B_i) \sim \Omega_G(B_i)\right)\left(\Omega_G(B_i) \sim \Omega_G(B_j)\right)\right),$$
$$\left(\Omega_{Dp}(B_i) \not\sim \Omega_G(B_j)\right) \Leftrightarrow \tag{5.52}$$
$$\Leftrightarrow \left(\left(\forall \Omega_G(B_i) \middle| \Omega_{Dp}(B_i) \sim \Omega_G(B_i)\right)\left(\Omega_G(B_i) \not\sim \Omega_G(B_j)\right)\right).$$

Слабку сумісність (несумісність) локальної і дискреційної ПБ, визначених на довільному рівні системи, формалізуємо як слабку сумісність (несумісність) певної локальної ПБ із певною дискреційною ПБ, визначених на цьому рівні системи, із якими вихідні ПБ слабко сумісні (несумісні):

$$\left(\Omega_{Ll_i}(B_i) \sim \Omega_{Dl_j}(B_j)\right) \Leftrightarrow$$
$$\Leftrightarrow \left(\left(\exists \Omega_L(B_i) \middle| \Omega_{Ll_i}(B_i) \sim \Omega_L(B_i)\right) \times\right.$$
$$\left.\times \left(\exists \Omega_{Dp}(B_j) \middle| \Omega_{Dl_j}(B_j) \sim \Omega_{Dp}(B_j)\right)\left(\Omega_L(B_i) \sim \Omega_{Dp}(B_j)\right)\right),$$
$$\left(\Omega_{Ll_i}(B_i) \not\sim \Omega_{Dl_j}(B_j)\right) \Leftrightarrow \tag{5.53}$$
$$\Leftrightarrow \left(\left(\forall \Omega_L(B_i) \middle| \Omega_{Ll_i}(B_i) \sim \Omega_L(B_i)\right) \times\right.$$
$$\left.\times \left(\forall \Omega_{Dp}(B_j) \middle| \Omega_{Dl_j}(B_j) \sim \Omega_{Dp}(B_j)\right)\left(\Omega_L(B_i) \not\sim \Omega_{Dp}(B_j)\right)\right).$$

Слабку сумісність (несумісність) локальної ПБ, визначеної для певного рівня системи, і дискреційної ПБ розглядатимемо як слабку сумісність (несумісність) цієї дискреційної ПБ із певною локальною ПБ, із якою вихідна локальна ПБ, визначена для певного рівня системи, слабко сумісна (несумісна):

$$\begin{gathered}\left(\Omega_{Ll}(B_i)\sim\Omega_{Dp}(B_j)\right)\Leftrightarrow\\ \Leftrightarrow\left(\left(\exists\Omega_L(B_i)\middle|\Omega_{Ll}(B_i)\sim\Omega_L(B_i)\right)\left(\Omega_L(B_i)\sim\Omega_{Dp}(B_j)\right)\right),\\ \left(\Omega_{Ll}(B_i)\nsim\Omega_{Dp}(B_j)\right)\Leftrightarrow\\ \Leftrightarrow\left(\left(\forall\Omega_L(B_i)\middle|\Omega_{Ll}(B_i)\sim\Omega_L(B_i)\right)\left(\Omega_L(B_i)\nsim\Omega_{Dp}(B_j)\right)\right).\end{gathered}\tag{5.54}$$

Аналогічно, слабку сумісність (несумісність) локальної ПБ, визначену для певного рівня системи, і глобальної ПБ розглядатимемо як слабку сумісність (несумісність) цієї глобальної ПБ із певною локальною ПБ, із якою вихідна локальна ПБ, визначена для певного рівня системи, слабко сумісна (несумісна):

$$\begin{gathered}\left(\Omega_{Ll}(B_i)\sim\Omega_G(B_j)\right)\Leftrightarrow\\ \Leftrightarrow\left(\left(\exists\Omega_L(B_i)\middle|\Omega_{Ll}(B_i)\sim\Omega_L(B_i)\right)\left(\Omega_L(B_i)\sim\Omega_G(B_j)\right)\right),\\ \left(\Omega_{Ll}(B_i)\nsim\Omega_G(B_j)\right)\Leftrightarrow\\ \Leftrightarrow\left(\left(\forall\Omega_L(B_i)\middle|\Omega_{Ll}(B_i)\sim\Omega_L(B_i)\right)\left(\Omega_L(B_i)\nsim\Omega_G(B_j)\right)\right).\end{gathered}\tag{5.55}$$

Слабку сумісність (несумісність) дискреційної ПБ, визначеної для певного рівня системи, і локальної ПБ розглядатимемо як слабку сумісність (несумісність) даної локальної ПБ із певною дискреційною ПБ, із якою вихідна дискреційна ПБ, визначена для певного рівня системи, слабко сумісна (несумісна):

$$\begin{gathered}\left(\Omega_{Dl}(B_i)\sim\Omega_L(B_j)\right)\Leftrightarrow\\ \Leftrightarrow\left(\left(\exists\Omega_{Dp}(B_i)\middle|\Omega_{Dl}(B_i)\sim\Omega_{Dp}(B_i)\right)\left(\Omega_{Dp}(B_i)\sim\Omega_L(B_j)\right)\right),\\ \left(\Omega_{Dl}(B_i)\nsim\Omega_L(B_j)\right)\Leftrightarrow\\ \Leftrightarrow\left(\left(\forall\Omega_{Dp}(B_i)\middle|\Omega_{Dl}(B_i)\sim\Omega_{Dp}(B_i)\right)\left(\Omega_{Dp}(B_i)\nsim\Omega_L(B_j)\right)\right).\end{gathered}\tag{5.56}$$

Аналогічно, слабку сумісність (несумісність) дискреційної ПБ, визначену для певного рівня системи, і глобальної ПБ розглядатимемо як слабку сумісність (несумісність) даної глобальної ПБ із певною дискреційною ПБ, з якою вихідна рівнева дискреційна ПБ, визначена для певного рівня системи, слабко сумісна (несумісна):

$$\left(\Omega_{Dl}(B_i)\sim\Omega_G(B_j)\right)\Leftrightarrow\tag{5.57}$$

$$\Leftrightarrow \left(\left(\exists \Omega_{Dp}(B_i) \middle| \Omega_{Dl}(B_i) \sim \Omega_{Dp}(B_i)\right)\left(\Omega_{Dp}(B_i) \sim \Omega_G(B_j)\right)\right),$$

$$\left(\Omega_{Dl}(B_i) \nsim \Omega_G(B_j)\right) \Leftrightarrow$$

$$\Leftrightarrow \left(\left(\forall \Omega_{Dp}(B_i) \middle| \Omega_{Dl}(B_i) \sim \Omega_{Dp}(B_i)\right)\left(\Omega_{Dp}(B_i) \nsim \Omega_G(B_j)\right)\right).$$

Під сильною сумісністю (несумісністю) визначених для різних системних контурів різнотипних ПБ розумітимемо слабку сумісність (несумісність) деяких однотипних ПБ, визначених для всієї ІСКЗ, які слабко сумісні (несумісні) із вихідними ПБ для відповідних системних контурів (5.44) є частинним випадком щойно описаної ситуації):

$$\begin{gathered}
\left(\Omega_i(B_i) \approx \Omega_j(B_j)\right) \Leftrightarrow \\
\Leftrightarrow \left(\left(\exists \Omega_i(B_0) \middle| \Omega_i(B_i) \sim \Omega_i(B_0)\right) \times \right. \\
\left. \times \left(\exists \Omega_j(B_0) \middle| \Omega_j(B_j) \sim \Omega_j(B_0)\right)\left(\Omega_i(B_0) \sim \Omega_j(B_j)\right)\right), \\
\left(\Omega_i(B_i) \not\approx \Omega_j(B_j)\right) \Leftrightarrow \\
\Leftrightarrow \left(\left(\forall \Omega_i(B_0) \middle| \Omega_i(B_i) \sim \Omega_i(B_0)\right) \times \right. \\
\left. \times \left(\forall \Omega_j(B_0) \middle| \Omega_j(B_j) \sim \Omega_j(B_0)\right)\left(\Omega_i(B_0) \nsim \Omega_j(B_j)\right)\right).
\end{gathered} \tag{5.58}$$

Формалізуємо слабку і сильну сумісності двох різнотипних ПБ Ω_i та Ω_j, визначених для системних контурів B_i та B_j із індексами $I_i = I(B_i)$ та $I_j = I(B_j)$, відповідно. Якщо ці системні контури перетинатимуться, то слабка і сильна сумісність їх ПБ тотожна еквівалентності:

$$\left(\Omega_i(B_i) \sim \Omega_j(B_j)\right) \Leftrightarrow \left(\Omega_i(B_i) \approx \Omega_j(B_j)\right),$$

а якщо ці системні контури ще й збігаються ($B_i = B_j = B$ і ПБ однотипні), то слабка і сильна сумісність їх ПБ тотожна рівності:

$$\left(\Omega_i(B) \sim \Omega_j(B)\right) \Leftrightarrow \left(\Omega_i(B) \approx \Omega_j(B)\right) \Leftrightarrow \left(\Omega_i(B) = \Omega_j(B)\right).$$

Якщо системні контури не перетинаються, але індекс одного з них є підіндексом іншого $I_j \subset I_i$, то їх ПБ обов'язково слабко, але не обов'язково сильно, сумісні. Якщо індекс жодного із СК не є підіндексом іншого $\left(I_i \not\subset I_j\right) \wedge \left(I_j \not\subset I_i\right)$, то їх ПБ обов'язково сильно, і, відповідно, слабко, сумісні. Для наочності отримані

вирази для забезпечення слабкої і сильної сумісностей (несумісностей) різнотипних ПБ зведено в табл. 5.2.

Таблиця 5.2

Вирази для забезпечення слабкої і сильної сумісності (несумісності) різнотипних ПБ, визначених для системних контурів у складі ІСКЗ

Тип ПБ	Глобальна	Рівнева дискреційна	Рівнева локальна	Локальна	Дискреційна
Глобальна	(5.38), (5.44)	(5.57), (5.58)	(5.55), (5.58)	(5.51), (5.58)	(5.52), (5.58)
Рівнева дискреційна		(5.39), (5.47), (5.44), (5.58)	(5.53), (5.58)	(5.56), (5.58)	(5.46), (5.58)
Рівнева локальна			(5.40), (5.49), (5.44), (5.58)	(5.48), (5.58)	(5.54), (5.58)
Локальна				(5.41), (5.44)	(5.50), (5.58)
Дискреційна					(5.42), (5.44)

Підсумовуючи сказане, вважатимемо, що для СК B у складі ІСКЗ визначено СПБ $\Omega(B)=\langle\Omega_G(B),\Omega_{Dp}(B),\Omega_{Dg}(B),\Omega_L(B)\rangle$, якщо для СК визначено ПБ всіх типів ($\Omega_G(B),\Omega_L(B)$ – глобальну і локальну ПБ, відповідно, які забезпечують функціонування БОД ІСКЗ, $\Omega_{Dp}(B)$ і $\Omega_{Dg}(B)$ – рівневу і глобалізовану дискреційну ПБ, які забезпечують функціонування БРД ІСКЗ) і всі ці ПБ хоча б слабко сумісні. При такому представленні дискреційна ПБ індукована локальною, а глобальна – локальною і дискреційною. Враховуючи, що модельована оцінною мережею Петрі ІСКЗ є композицією системних контурів, можна розширити сформульовану вище концепцію визначення СПБ для СК до масштабів всієї ІСКЗ із збереженням коректності та сумісності математичних представлень та можливістю формального синтезу захищеної ієрархічної ІСКЗ із будь-яким рівнем складності із дотриманням стандарту ISO/IEC 27001:2013.

В запропонованій в табл. 5.1 ієрархічній структурі ІСКЗ за практичну реалізацію обраної моделі СПБ відповідають БОД та БРМ, емпіричні дослідження яких дозволять пересвідчитися у адекватності отриманих вище математичних моделей.

Зробимо постановку експериментів для оцінювання процесів функціонування цих структурних елементів. БОД реалізує процеси ефективного оброблювання інформації в ІСКЗ відповідно до дій сегрегованих за ролями суб'єктів-користувачів. Інформаційна безпека цих процесів забезпечується роботою підсистеми контролю цілісності інформації, яку розміщено на сервер-реєстраційному центрі, і структурно віднесено до прикладного рівня ієрархії ІСКЗ. Під цілісністю інформації розумітимемо якісний стан ІнС та ІнР ІСКЗ. Відповідно контроль цілісності інформації передбачає регламентоване функціонування сервісів її визначення, збереження і відновлення. Втім, контроль цілісності інформації, як і будь-який процес, потребує ресурсів, обсяг яких зростатиме із часом експлуатації системи. Враховуючи критичне застосування описуваної ІС необхідно створити механізм контролю цілісності її інформації, який функціонуватиме в реальному часі, віддаючи пріоритет по використанню ресурсів функціональному призначенню ІСКЗ, забезпечуючи, водночас, високий рівень інформаційної безпеки. Враховуючи сказане, визначимо оптимальний сценарій роботи ПКЦІ $a \in A$ як результат розв'язання задачі математичного програмування із цільовою функцією $E_f(a) \to \max$ при обмежені $E_s(a) \geq E_{s\min}$, де E_f – здатність ІСКЗ виконувати функціональні обов'язки підтримуючи цілісність даних; E_s – здатність ІСКЗ підтримувати заданий показник якості функціонування без проведення контролю цілісності інформації; $E_{s\min}$ – експлуатаційна константа, яка задається адміністратором. Стверджуючи, що ступінь повноти процесу контролю цілісності інформації є оберненим до його тривалості, представимо процес контролю цілісності в часі як:

$$E_f = P(K_{dm} > K_{dm\min}) = 1 - P(\tau_{dm} \leq \tau_{\min f}) = 1 - E(\tau_{mf}),$$

$$E_s = P(K_{dm} \leq K_{dm\max}) = 1 - P(\tau_{dm} \leq \tau_{\max s}) = 1 - E(\tau_{ms}),$$

де $\tau_{dm} = v_{dm} c^{-1}$ і $K_{dm} = v_{dm} V_{dm}^{-1} = c\,\tau_{dm} V_{dm}^{-1}$ – випадкові параметри, які характеризують тривалості і коефіцієнт процесу контролю цілісності інформації під час сеансу дискреційного доступу m, відповідно V_{dm} – параметр, який характеризує обсяг інформації, цілісність якої необхідно контролювати; v_{dm} – випадковий па-

раметр, значення якого характеризує обсяг інформації, цілісність якої проконтрольовано упродовж сеансу дискреційного доступу m; c – швидкість контролю цілісності інформації; $K_{dm\min}$, $K_{dm\max}$, $\tau_{\min f}$, $\tau_{\max s}$ – граничні значення відповідних параметрів. Узагальнимо E_f та E_s у вигляді динамічного критерію ефективності ПКЦІ ІСКЗ:

$$E(\tau_m) = P(\tau_{dm} \le \tau_{\max}(\tau_m)), \tag{5.59}$$

де функція $\tau_{\max}(\tau_m)$ – експоненційно розподілена із середнім $\overline{\tau_m}$.

Зважаючи на критерій (5.59), випадковий процес контролю цілісності інформації в ІСКЗ у часі характеризується послідовністю станів випадкової тривалості з різними законами розподілу імовірності, тобто є типовим напівмарковським процесом [189–192], який характеризується матрицею $H(\tau) = \left\| H_{ij}(\tau) \right\|$, довільний елемент якої $H_{ij}(\tau)$ описує імовірність того, що модельований процес, потрапивши у стан i, перейде у визначений архітектурою ОМП стан j за час, менший від τ, $i = \overline{1, n-1}$, $j = i+1$, $n = l_{\max} + 1$, $1 \le l_{\max} \le L$, де L – кількість рівнів ІСКЗ. Отже $i = \overline{1, l_{\max}}$ – кількість станів; V_i – обсяг інформації, цілісність якої контролюється, при перебуванні ІСКЗ у стані i; $F_b(\tau)$ – базовий закон розподілу із параметрами

$$\xi = \{P_0, P_1, a, b, d\},$$

$$P_0 \ge 0,\ P_1 \ge 0,\ P_0 + P_1 \le 1,\ 0 \le a \le b \le 1,\ 0 \le d \le \infty,$$

$$(P_0 + P_1 \ne 1) \wedge (a = b = 1) \wedge (d = \infty),$$

$$(P_0 + P_1 \ne 1) \wedge (a = b = d = 0)$$

і щільністю

$$f_b(\tau) = P_0 \delta(\tau) + P_1 \delta(\tau - 1) + f_l(0, a, 0, f_b(a), \tau) +$$
$$+ f_l(a, b, f_b(a), f_b(b), \tau) + f_l(b, 1, f_b(b), 0, \tau)$$

при

$$d < \infty \Rightarrow f_b(b) = d f_b(a),\ d = \infty \Rightarrow f_b(a) = 0,$$

$$f_l(x_1, x_2, y_1, y_2, x) = \begin{cases} 0, if\ x \in [0; x_1] \cup [x_2; \infty], \\ (y_2 - y_1)(x - x_1)(x_2 - x_1)^{-1} + y_1, if\ x \in [x_1; x_2], \end{cases}$$

є вхідними параметрами для генерування управлінського рішення, яке полягає у виборі для кожного із $i=\overline{1,l_{\max}}$ станів значень $K_{\max i}$ і параметрів базового розподілу імовірності. Управлінські впливи встановлюються через задавання величин $K_i = K_{\max i}\xi_i$.

Для оцінювання критерію динамічної ефективності ПКЦІ ІСКЗ спочатку для кожного стану $i=\overline{1,l_{\max}}$ на основі значень $\xi=\{P_0,P_1,a,b,d\}$ обчислюємо значення щільності базового розподілу імовірності

$$f_b(a)=\begin{cases} 0, if\ (d=\infty)\vee(a=b=d=0), \\ 2(1-P_0-P_1)(b-ad+d)^{-1}, if\ else; \end{cases}$$
$$f_b(b)=\begin{cases} 2(1-P_0-P_1)(1-a)^{-1}, if\ d=\infty, \\ df_b(a), if\ else. \end{cases} \tag{5.60}$$

Далі, при обчисленій величині $T_i = K_{\max i}V_i c^{-1}$ – максимальній тривалості перебування НМП у стані i, обчислюємо значення $v = T_i t_m^{-1} = K_{\max i}V_i(c\tau_m)^{-1}$ і перетворення Лапласа–Стілтьєса функції базового розподілу імовірності

$$\varphi_{bi}\left(T_i\tau_m^{-1}\right)=P_0+P_1e^{-v}+\varphi_{bl}(v)+\varphi_{bs}(v)+\varphi_{bn}(v), \tag{5.61}$$

де

$$\varphi_{bn}(v)=\begin{cases} 0, if\ b=1, \\ vf_b(b)\left(2e^{-bv}-e^{-v}\right)\left(v(1-b)\right)^{-1}, if\ b<1; \end{cases}$$

$$\varphi_{bl}(v)=\begin{cases} 0, if\ a=0, \\ vf_b(a)\left(1-e^{-av}\right)\left(av-e^{-av}\right)^{-1}, if\ a>0; \end{cases}$$

$$\varphi_{bs}(v)=\begin{cases} 0, if\ a=b, \\ v\left(f_b(b)-f_b(a)\right)\left(e^{-av}-e^{-bv}\right)\times \\ \times\left(v(b-a)+f_b(a)e^{-av}-f_b(b)e^{-bv}\right)^{-1}, if\ a<b, \end{cases}$$

і представляємо критерій (5.59) у прикладному вигляді

$$E(\tau_m)=\prod_{i=1}^{l_{\max}}\varphi_{bi}\left(T_i\tau_m^{-1}\right). \tag{5.62}$$

Отже, вирази (5.37)–(5.51) формалізують асоційований із ОМП-представленням СПБ ІСКЗ, адаптований для практичного застосування, метод

оцінювання процесу функціонування ПКЦІ на основі динамічного критерію контролю цілісності інформації (5.62). Критерій (5.62) базується на математичному апараті напівмарковських мереж для комплексного стохастичного опису дискретних станів контролю цілісності інформації на вибраних ієрархічних рівнях ІСКЗ упродовж неперервного сеансу дискреційного доступу. Метод дозволяє вибрати максимальні допустимі значення коефіцієнтів контролю цілісності інформації на рівнях ІСКЗ, при яких максимізується значення критерію (5.62), врахувавши попередньо задані значення обсягу контрольованої інформації, швидкості контролю її цілісності та максимальної тривалості перебування системи у відповідному стані.

Узагальнимо модель СПБ ІСКЗ з позиції роботи БРМ кортежем

$$\langle A, C, R, G \rangle, \tag{5.63}$$

де A – множина адміністраторів системи; C – множина суб'єктів-користувачів; R – множина ролей, кожна з яких визначає межі можливостей, виділених адміністраторами для відповідних класів користувачів; G – ОМП-представлення програмно-технічної складової ІСКЗ. Перша позиція кортежу (5.63) відповідає адміністративному рівню з табл. 5.1, друга – ідентифікаційному, третя – інтеграційному, а четверта – решті підрівнів. Множина G є сукупністю підмножин

$$G = \{G_E, G_R \cup G_A \cup G_M, G_I\}, \tag{5.64}$$

де G_E – множина суб'єктів-системних контурів ІСКЗ, описуваних наборами вершин графу ОМП; G_R – множина дуг графу стану ОМП ІСКЗ, які описують ролі суб'єктів-користувачів; G_A – множина дуг графу стану ОМП ІСКЗ, які описують дії активних суб'єктів-користувачів в межах визначених для них ролей; G_M – множина дуг графу стану ОМП ІСКЗ, які описують ІП між суб'єктами ІСКЗ; G_I – функція ієрархічної структури ІСКЗ.

Зважаючи на (5.63), (5.64), виділимо в ОМП ІСКЗ множину суб'єктів, які є потенційними цілями для негативних впливів, $Q = \{q_1, \ldots, q_n\}$, яка в системному масштабі утворюється в результаті об'єднання неперетинних множин класів ін-

формаційних загроз $Z = \{z_1, \ldots, z_m\}$. Множина суб'єктів $D = \{d_1, \ldots, d_m\} \in Q$, класифікованих за типами інформаційних загроз, є множиною прецедентів, яка використовуватиметься для навчання БРД.

Навчена БРД представляється в кожному системному контурі ОМП структури ІСКЗ множиною класифікаторів, які визначають зважені ступені ідентичності атрибутів аналізованого суб'єкта q_i, $1 \le i \le n$, класам інформаційних загроз z_j, $j = \overline{1,m}$, і порівнюють ці ступені із відповідними пороговими значеннями. Ситуації перевищення ступенями ідентичності порогових значень кваліфікуються як факти виявлення відповідних інформаційних загроз, що ініціює реакцію системи, описану у СПБ. При описаному механізмі функціонування ефективність БРД визначатиметься типом використовуваних класифікаторів, репрезентативністю множини прецедентів, використовуваних для їх навчання, адекватністю значень множини ваг класів інформаційних загроз та адекватністю значень множини порогових значень для спрацювання БРД тощо.

Налаштуємо роботу БОД та БРД ІСКЗ, організованої за сформульованою в табл. 5.1 структурою, так, щоб оптимізувати значення критеріїв (5.62) та (5.63), відповідно. Аналітичний вигляд виразу (5.61) дозволяє передбачити, що найбільш відчутну динаміку значення критерію (5.62) можна буде спостерігати при значній сегрегації обсягів контрольованої на цілісність інформації на різних рівнях ієрархії ІСКЗ. Втім, як і для більшості потужних ІС, понад 99 % всіх даних ІСКЗ розташовано на першому (інформаційному) рівні. Зокрема, у досліджуваній ІС обсяг архіву даних-фонограм складає 10 Тб, а обсяг решти програмного забезпечення, разом із серверною операційною системою та всім спеціалізованим програним забезпеченням ІСКЗ – близько 70 Гб. У такій ситуації найбільший дисбаланс щодо обсягів контрольованої на цілісність інформації на рівнях ІСКЗ може спостерігатися при ініціації потужних процесів маніпулювання інформацією, найбільш типовими із яких є: 1) ініційований адміністратором процес резервного копіювання даних, 2) ініційований авторизованим суб'єктом-користувачем процес пошуку інформації по всій базі даних ІСКЗ. Проаналізуємо відносні обсяги контрольованої

на цілісність інформації на рівнях ієрархії ІСКЗ для цих двох процесів, представивши результат аналізу на рис. 5.3.

На основі представлених на рис. 5.3 даних про відносні обсяги контрольованої на відповідних рівнях ІСКЗ інформації, виявимо залежність значення динамічного критерію ефективності ПКЦІ ІСКЗ (5.62) від значень параметрів тривалості та коефіцієнта процесу контролю цілісності інформації під час активних сеансів дискреційних доступів. Результати проведеного дослідження представлено на рис. 5.4.

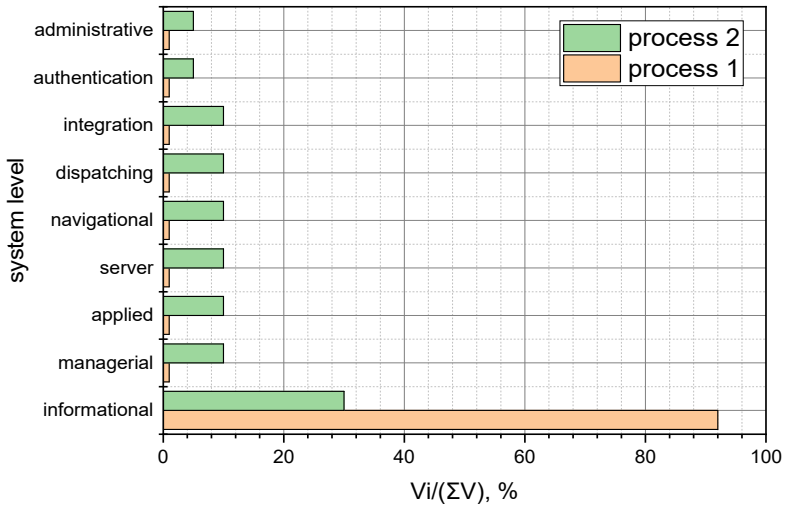
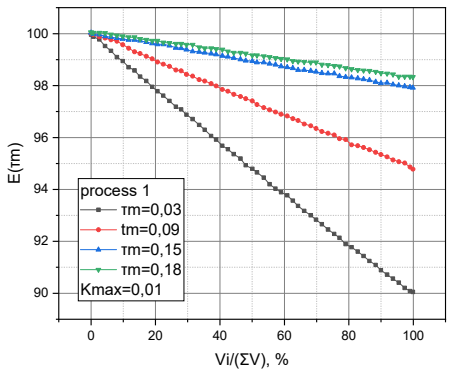
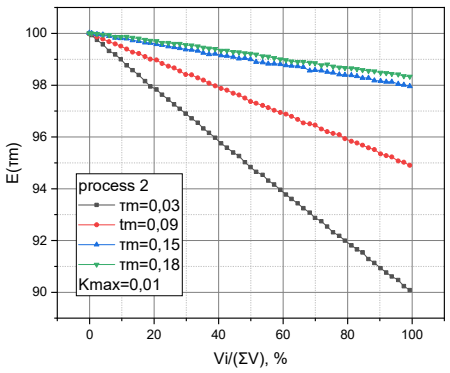


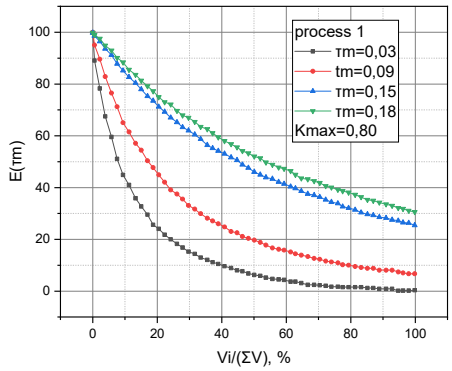
Рисунок 5.3 – Відносні обсяги контрольованої на цілісність інформації на рівнях ієрархії ІСКЗ для процесів 1 і 2



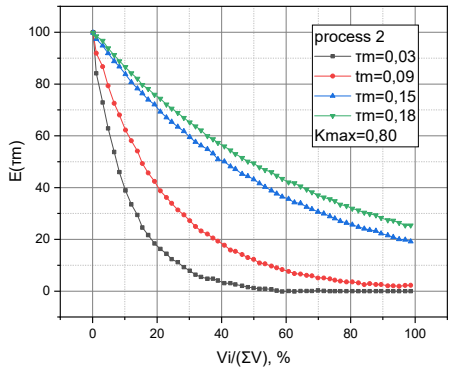
а)



б)



в)



г)

Рисунок 5.4 – Залежність функціонального критерію (5.62) від вхідних параметрів

Робота БРД описаної вище ІСКЗ полягає у виявленні та вірній класифікації атак, метою яких є або отримання несанкціонованого доступу до ІнР ІСКЗ, або порушення цілісності її інформації. Для перевірки адекватності роботи БРД та реакції СПБ ІСКЗ на виявлені загрози сформуємо базу прецедентів типізованих атак, спрямованих на перевірку адекватності: глобальної ПБ (атаки на вміст ролей користувачів, 5 видів атак); локальної ПБ (атаки на процеси взаємодії апаратних та програмних складових ІСКЗ, в т.ч. на різних рівнях її ієрархії, 12 видів атак); дискреційної ПБ (атаки зі спробою автентифікації антагоністів за паролем, ідентифікаційною карткою, індивідуальними параметрами голосу та із комбінацією перерахованих атрибутів тощо, 6 видів атак).

Підсумкова кількість типів атак склала 23. Кількість функцій ІСКЗ, що описували відповідні системні контури різного порядку, і підтримували розв’язання задач збирання, реєстрації, збереження, оброблювання, актуалізації та представлення суб’єктам-користувачам інформаційних ресурсів системи, склала 41. Кількість ознак, значення яких оцінювалися класифікаторами для ідентифікації типів атак, становила 9. Кількість реалізацій атак склала 100 разів для кожного із типів, значення ознак 40 % із яких було використано для навчання БРМ. Реакцію БРМ на імітовані атаки узагальнено в множині рекомендованих значень вагових коефіцієнтів для класифікаторів, які відповідають за виявлення атак на глобальну, ло-

кальну та дискреційну ПБ, відповідно: $(0{,}15; 0{,}22; 0{,}63)$. Поріг чутливості класифікаторів для виявлення факту атаки, враховуючи критичне застосування ІС, встановлювався рівним 0,1. Аналіз результатів експериментів дозволив виділити низку закономірностей в роботі БОД та БРМ ІСКЗ, зокрема:

– вплив параметра $K_{\max i}$ i-го рівня ІСКЗ на значення критерію $E(\tau_m)$ прямо залежить від обсягів інформації V_i, цілісність якої контролюється на цьому рівні, і обернено – від всієї кількості інформації $\sum V$, цілісність якої контролюється у системі під час активного сеансу дискреційного доступу;

– при близьких значеннях V_i, помітних змін значення критерію $E(\tau_m)$ можна досягти варіюванням значень $K_{\max i}$ на відповідних рівнях ІСКЗ;

– змінюючи в одному напрямку значення τ_m і значення параметра $K_{\max i}$ можна покращити динаміку зміни значення критерію $E(\tau_m)$;

– при близьких до нуля значеннях параметрів $K_{\max i}$ ПКЦІ ІСКЗ перестає виконувати свої функції, а при близьких до одиниці значеннях $K_{\max i}$ ефективність ПКЦІ ІСКЗ цілком визначається значенням параметра τ_m;

– зміна рівневих параметрів $K_{\max i}$ призводить до синхронної зміни математичного сподівання часу реалізації контролю цілісності інформації в ІСКЗ, впливаючи, відповідно, на процес функціонування ПКЦІ ІСКЗ;

– реалізація ПРД у вигляді набору класифікаторів дозволяє виявити подальший напрямок підвищення ефективності процесу функціонування цієї підсистеми, застосовуючи методи машинного навчання, створені для ансамблів

розв’язувальних правил.

5.3 Модель готовності інформаційної системи критичного застосування

Безпека ІС великою мірою визначається її архітектурою. Сучасні ІС будуються як на основі централізованої клієнт-серверної архітектури [337–342], так і на основі однорангової розподіленої децентралізованої хмарної архітектури, у якій, окрім ефективної організації доступу до ІнР, закладено підтримку GRID-технологій, хмарних обчислень і пірінгових мереж тощо. Кожен архітектурний підхід має свої переваги і недоліки [337–339], які варто розглядати, перш за все, з позиції галузевого призначення ІС. Критичне застосування ІС зумовлює специфічні вимоги до реалізації заходів інформаційної безпеки, зокрема, у забезпеченні готовності ІнР системи для автентифікованих суб’єктів, вважаючи фактор вартості функціонування ІСКЗ другорядним. Враховуючи сказане, актуальною задачею є синтез моделі готовності розподіленої ІСКЗ із урахуванням її топології і вбудованих сервісів. При чому, в залежності від обраної базової архітектури системи, доведеться досліджувати питання невизначеності елементів або сегментів її топології, не повної достовірності інформації про системні апаратні і програмні ресурси, мінливості поведінки системи в залежності від ступеня її завантаженості та від ступеня небезпеки дій автентифікованих суб’єктів тощо.

Аналіз інформаційних джерел дозволив виявити підходи, які використовуються для моделювання готовності актуальних мережевих ІС. Найчастіше оцінювання готовності мережевої ІС здійснюється формально, обмежуючись розрахунком коефіцієнта готовності [337, 338] у вигляді відношення середньої тривалості роботи системи без відмов у доступі до суми цього ж показника із середньою тривалістю робіт, виконуваних для відновлення готовності системи. Простота такого підходу нівелюється його загальністю, що дозволяє рекомендувати його використання лише на першому етапі дослідження готовності ІС. Втім, застосовують і стохастичний підхід для оцінювання готовності та безвідмовності мережевих ІС [343], при якому викорис-

товують структурні схеми надійності, дерева відмов, марковські мережі і мережі Петрі. В роботах [337, 338, 343] запропоновано марковські моделі для оцінювання готовності мережевих ІС із урахуванням ієрархічної структури їх топології. В дослідженнях [337, 343] проводився аналіз і моделювання надійності мережевих інформаційних і GRID-систем та їх сервісів у парадигмі марковських процесів і систем масового обслуговування [344–347]. Втім, всі згадані дослідження стосуються мережевих ІС без урахування можливості їх критичного застосування, що обумовлює неадекватність цих моделей для опису ІСКЗ через не врахування специфічних сервісів останньої та необхідності підтримування високого рівня конфіденційності і готовності навіть при значних витратах ресурсів на функціонування системи.

Нехай ІСКЗ реалізовано на основі запропонованої автором у підрозділі 5.1 архітектури. Під готовністю такої ІСКЗ розумітимемо властивість системи надавати автентифікованим суб'єктам доступ до системних ІнР за правилами, сформульованими у СПБ, за умови, що тривалість очікування доступу не перевищить заданого значення t_d. Оцінювати готовність ІСКЗ в такому разі будемо за значенням параметра p_i, $0 \le p_i \le 1$, який описуватиме імовірність того, що i-й автентифікований суб'єкт отримав доступ до ІСКЗ очікуючи менше τ_d. Значення параметра p_i залежатиме від: комплексного параметра a_{ir}, який узагальнює інформацію про архітектурні особливостей ІС, що визначають розташування системних ІнР; комплексного параметра a_{is}, який узагальнює інформацію про обсяги ресурсів ІнС ІСКЗ, доступні для реалізації дій автентифікованих суб'єктів; комплексного параметру a_{pb}, який узагальнює інформацію про правила використання ІнС ІСКЗ відповідно до повноважень автентифікованих суб'єктів, які звертаються до системи; комплексного параметра a_{so}, який узагальнює інформацію про порядок активації і регламент проведення необхідних для функціонування ІСКЗ сервісних операцій; часу t_z, коли надійшов запит від автентифікованого суб'єкта. Згадані вище параметри можна узагальнити у вигляді моделі

$p_i = f(a_{ir}, a_{is}, a_{pb}, a_{so}, t_z)$, на основі якої можна поставити, наприклад, задачу оптимізації готовності ІСКЗ виду $p_i = f(a_{ir}, a_{is}, a_{pb}, a_{so}, t_z) \to \max$ при обмеженнях $\tau_{oz} \le \tau_d$, $o_{ISCU} \le o_d$, де τ_{oz} – тривалість очікування автентифікованим суб'єктом на отримання доступу; o_{ISCU}, o_d – фактичні і граничні витрати на функціонування ІСКЗ, відповідно. Постановку задачі оптимізації, звичайно, можна змінювати, але покладена в її основу математична модель готовності ІСКЗ залишатиметься сталою.

У загальному випадку комунікація ІСКЗ із суб'єктами, які бажають скористатися її ІнР, описується двома концепціями: концепцією автентифікації суб'єкта для отримання доступу до ІСКЗ і концепцією підтримки ІнС ІСКЗ дій автентифікованих суб'єктів в рамках їх ролей, описаних у СПБ. Теорія випадкових процесів дозволяє описати першу концепцію Пуассонівським процесом із інтенсивністю λ, а другу – експоненційним розподілом із масштабним коефіцієнтом μ_i^j, де $i \in \{1,2,\ldots,W\}$ – індекси суб'єктів, а $j \in \{1,2,\ldots,T\}$ – індекси віртуальних машин, які створюються для підтримки дій i-го суб'єкта у ІнС ІСКЗ. Далі використовуватимемо узагальнююче поняття ВМ для опису визначеної адміністратором кількості обчислювальних ресурсів, обсягу пам'яті і ширини каналу зв'язку, що одноразово виділяються в ІнС ІСКЗ для підтримки дій суб'єкта. Значення W і T задаються на етапі проектування ІСКЗ і описують, відповідно, максимальну кількість АС, роботу яких може підтримувати ІСКЗ у певний момент часу, і максимальну кількість ВМ, які може створювати ІСКЗ для підтримки дій одного суб'єкта, відповідно. Зауважимо, що ІСКЗ розгортається на мультисерверній платформі, яка включає сервер-реєстраційний центр і множину пов'язаних із ним серверів даних. Обслуговування запиту АС починається із виділення ресурсів СРЦ із подальшим підключенням ресурсів СД за потребою. Делеговані СД ІП також характеризуватимемо експоненційними розподілами із масштабними коефіцієнтами ν_i. Введемо змінні x_i^j і y_i, які описуватимуть кількість активних інформаційних потоків між i-м АС і j-м ВМ, які обслуговують його запити на

стороні СРЦ, та ВМ, які обслуговують запити i-го АС на стороні СД, відповідно. Ці змінні дозволяють оцінити підсумкову кількість інформаційних потоків у суб'єкт-системній взаємодії у вигляді відношень $\sum_{j=1}^{T}\sum_{i=1}^{W} ix_i^j + \sum_{i=1}^{W} iy_i \le B$ і $\sum_{j=1}^{T}\sum_{i=1}^{W} ix_i^j \le M$, де змінна B задає проектну межу кількості інформаційних потоків у ІнС ІСКЗ, а змінна M описує проектну межу кількості ВМ у ІнС СРЦ.

Функціонування ІСКЗ у контексті оцінювання її готовності для АС описуватимемо простором станів $s = \lfloor x_1^1, \ldots, x_W^T, y_1, \ldots, y_W, e(s) \rfloor \in S$, де характеристична змінна $e(s) = \{A_n, D_i^j, F_i\}$ описує визначену множину системних операцій, що можуть виконуватися в ІнС ІСКЗ у довільний момент часу її життєвого циклу. Зокрема, виділимо операцію готовності до прийняття вхідного запиту A_n, при якій у системи достатньо ресурсів та активовано відповідні функції її ІнС для підтримки дій АС; операцію очищення СРЦ D_i^j, при якій прийняття вхідних запитів неможливе і здійснюється вивільнення зарезервованих для дій i-го АС j ВМ у ІнС СРЦ; операцію очищення СД F_i при якій прийняття вхідних запитів неможливе і здійснюється вивільнення зарезервованих за i-м АС ресурсів ІнС СД.

На вхідний запит від АС ІСКЗ, що перебуває в стані s, в ІнС якої в цей момент часу виконується операція $e(s)$, може відповісти одним із можливих варіантів надання сервісу, описаних множиною $A = \bigcup_{s \in S} A_s : \{-1; 0; \alpha_i^j; \alpha_i\}$, де -1 – ситуація відхилення вхідного запиту з причини виконання однієї із операцій очищення; 0 – відхилення запиту з іншої причини; α_i^j – задовольняється вхідний запит від i-го АС із виділенням для його потреб j ВМ в ІнС СРЦ; α_i – задовольняється вхідний запит від i-го АС із виділенням для його потреб ресурсів СД. Охарактеризуємо аналітично виразом (5.65) функцію $\gamma(s, \alpha)$ швидкості зміни стану системи, яка перебуваючи у стані s із активною операцією $e(s)$, реагує дією α у відповідь на вхідний запит АС. У виразі

(5.65) параметр λ описує інтенсивність надходження вхідних запитів, багаточлен $\sum_{j=1}^{T}\sum_{i=1}^{W} x_i^j \mu_i^j + \sum_{i=1}^{W} y_i \nu_i$ – ступінь завантаженості ІнС ІСКЗ вцілому, а його одночлен $\sum_{i=1}^{W} y_i \nu_i$ – ступінь завантаженості СД ІСКЗ, зокрема.

$$\gamma(s,\alpha)=\begin{cases} \lambda+\sum_{j=1}^{T}\sum_{i=1}^{W} x_i^j \mu_i^j+\sum_{i=1}^{W} y_i \nu_i, e(s)=A_n \wedge \alpha=0, \\ \lambda+\sum_{j=1}^{T}\sum_{i=1}^{W} x_i^j \mu_i^j+\sum_{i=1}^{W} y_i \nu_i+\mu_\omega^t, e(s)=A_n \wedge \alpha=\alpha_\omega^t, \\ \lambda+\sum_{j=1}^{T}\sum_{i=1}^{W} x_i^j \mu_i^j+\sum_{i=1}^{W} y_i \nu_i+\nu_\omega, e(s)=A_n \wedge \alpha=\alpha_\omega, \\ \lambda+\sum_{j=1}^{T}\sum_{i=1}^{W} x_i^j \mu_i^j+\sum_{i=1}^{W} y_i \nu_i-\mu_\omega^t, e(s)=D_\omega^t \wedge \alpha=-1, \\ \lambda+\sum_{j=1}^{T}\sum_{i=1}^{W} x_i^j \mu_i^j+\sum_{i=1}^{W} y_i \nu_i-\nu_\omega, e(s)=F_\omega \wedge \alpha=-1, \end{cases} \tag{5.65}$$

При надходженні вхідного запиту ІСКЗ, що перебуває у стані його очікування $(e(s)=A_n)$, може: відхилити вхідний запит $(\alpha=0)$, не змінюючи при цьому завантаженість ІС; прийняти вхідний запит завантаживши при цьому СРЦ на величину α_ω^t; прийняти вхідний запит завантаживши при цьому СД на величину α_ω. Дії α_ω^t або α_ω виконуються зі швидкістю μ_ω^t або ν_ω, відповідно. Під час виконання системою операцій очищення $e(s)=D_\omega^t$ або $e(s)=F_\omega$, в результаті яких вивільниться D_ω^t ресурсів СРЦ або F_ω ресурсів СД, відповідно, вхідні запити від АС не приймаються $(\alpha=-1)$ з технічних причин, що знижує результуючу швидкість прийняття вхідного запиту на величину μ_ω^t або ν_ω, відповідно. Зауважимо, що обернений до $\gamma(s,\alpha)$ параметр $\tau(s,\alpha)=\gamma(s,\alpha)^{-1}$ описує очікувану тривалість перебування суб'єкт-серверної взаємодії в стані s.

Простір станів готовності ІСКЗ представимо зваженою графоподібною структурою, в якій стани $s \in S$ утворюють вершини графа, зв'язки між ними показують допустимі переходи між станами відповідно до логіки функціону-

вання ІСКЗ у вигляді (5.65), а ваги зв'язків містять імовірності переходу із вихідного стану s у стан k, $s,k \in S$, в наслідок відповіді α на вхідний запит АС. Деталізуємо опис динаміки системи формалізувавши імовірності переходу системи із стану s, у якому виконується операція $e(s)$, у стан k в результаті відповіді α на вхідний запит АС.

Імовірність переходу системи $p(k|s,\alpha)$ зі стану $s = \left[x_1^1,\ldots,x_1^T,\ldots,x_W^1,\ldots x_W^T, y_1,\ldots,y_W, A_n\right]$ у стан k в наслідок відповіді α на вхідний запит від АС опишемо як

$$p(k|s,\alpha) = \begin{cases} \lambda\gamma(s,\alpha)^{-1}, e(k) = A_n, \\ \mu_i^j\left(x_i^j + 1\right)\gamma(s,\alpha)^{-1}, e(k) = D_i^j \wedge \alpha = \alpha_i^j, \\ \mu_i^j x_i^j \gamma(s,\alpha)^{-1}, e(k) = D_i^j \wedge \alpha \neq \alpha_i^j, \\ \nu_i(y_i + 1)\gamma(s,\alpha)^{-1}, e(k) = F_i \wedge \alpha = \alpha_i, \\ \nu_i y_i \gamma(s,\alpha)^{-1}, e(k) = F_i \wedge \alpha \neq \alpha_i. \end{cases} \tag{5.66}$$

Імовірність переходу системи $p(k|s,\alpha)$ зі стану $s = \left[x_1^1,\ldots,x_1^T,\ldots,x_S^1,\ldots x_S^T, y_1,\ldots,y_W, D_\omega^t\right]$ у стан k в наслідок відповіді α на вхідний запит від АС опишемо як

$$p(k|s,\alpha) = \begin{cases} \lambda\gamma(s,\alpha)^{-1}, e(k) = A_n, \\ \mu_i^j\left(x_i^j - 1\right)\gamma(s,\alpha)^{-1}, e(k) = D_i^j \wedge D_i^j = D_\omega^e, \\ \mu_i^j x_i^j \gamma(s,\alpha)^{-1}, e(k) = D_i^j \wedge D_i^j \neq D_\omega^e, \\ \nu_i y_i \gamma(s,\alpha)^{-1}, e(k) = F_i. \end{cases} \tag{5.67}$$

Імовірність переходу системи $p(k|s,\alpha)$ зі стану $s = \left[x_1^1,\ldots,x_1^T,\ldots,x_W^1,\ldots x_W^T, y_1,\ldots,y_W, F_\omega\right]$ у стан k в наслідок відповіді α на вхідний запит від АС опишемо як

$$p(k|s,\alpha) = \begin{cases} \lambda\gamma(s,\alpha)^{-1}, e(k) = A_n, \\ \mu_i^j x_i^j \gamma(s,\alpha)^{-1}, e(k) = D_i^j, \\ \nu_i(y_i - 1)\gamma(s,\alpha)^{-1}, e(k) = F_i \wedge F_i = F_\omega, \\ \nu_i y_i \gamma(s,\alpha)^{-1}, e(k) = F_i \wedge F_i \neq F_\omega. \end{cases} \tag{5.68}$$

Вирази (5.65)–(5.68) є основою для синтезу керованого напівмарковського процесу [189–192], який описуватиме готовність ІСКЗ для АС з урахуванням архітектурних особливостей першої. Для наочності отримаємо графічне представлення КНМП готовності ІСКЗ у вигляді UML-діаграм станів. Нехай $W = 1$, $T = 2$, $s = \left[x_1^1, x_1^2, y_1, e(s)\right]$, $e(s) = \left\{A_n, D_i^j, F_i\right\}$. На рис. 5.5–5.7 наведено діаграми переходу ІСКЗ із вихідних станів $\left[0, 1, 0, A_n\right]$, $\left[1, 1, 1, D_1^1\right]$ і $\left[1, 2, 1, F_1\right]$ у допустимі згідно з виразами (5.65)–(5.68) наступні стани в залежності від відповіді α на вхідні запити АС.

З метою управління готовністю ІСКЗ доповнимо опис стану ІСКЗ у наведеній вище моделі (5.65)–(5.68) дійсною управляючою функцією $r(s,\alpha)$, значення якої описує перевагу від вибору системою, яка перебуває у стані s, дії α у відповідь на вхідний запит від АС. Значення дійсної функції $r(s,\alpha)$ розраховуватимемо як різницю показника $k(s,\alpha)$, як міри доцільності ініціації системної операції $e(s)$, і добутку вартості її реалізації $o(s,\alpha)$ і її тривалості $\tau(s,\alpha)$:

$$r(s,\alpha) = k(s,\alpha) - \tau(s,\alpha) \cdot o(s,\alpha). \tag{5.69}$$

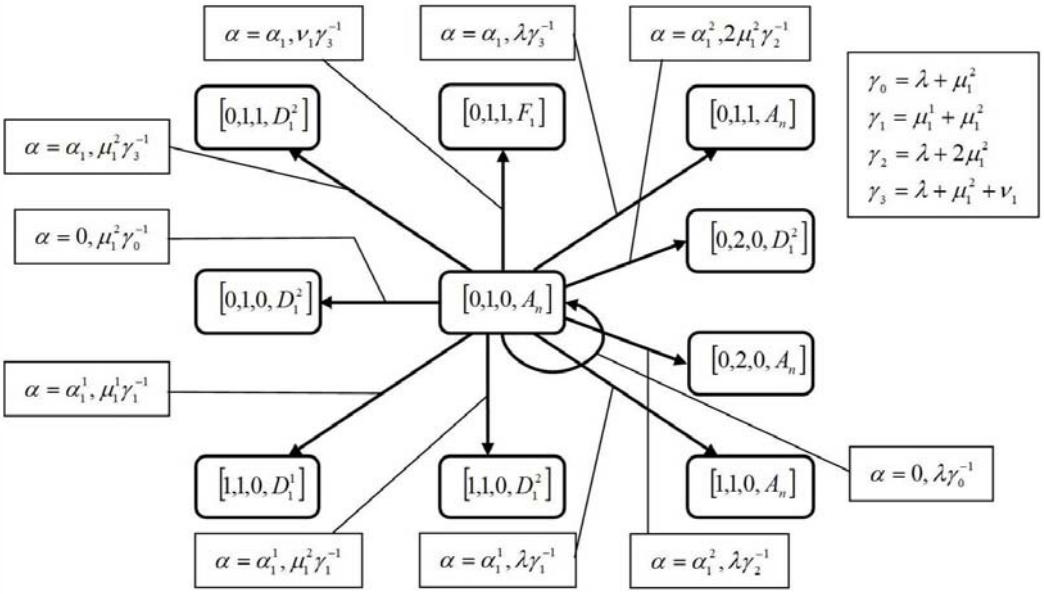


Рисунок 5.5 – UML-діаграма переходу ІСКЗ із стану $[0,1,0,A_n]$ у допустимі наступні стани в залежності від відповіді α на вхідні запити АС

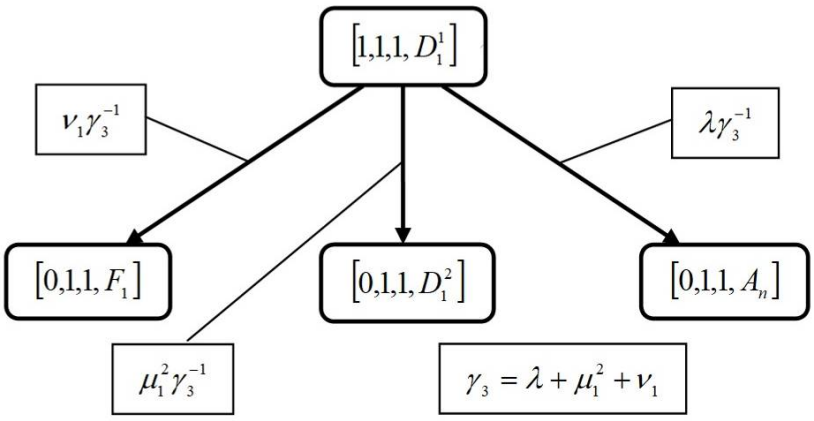


Рисунок 5.6 – UML-діаграма переходу ІСКЗ із стану $[1,1,1,D_1^1]$ у допустимі наступні стани в залежності від відповіді α на вхідні запити АС

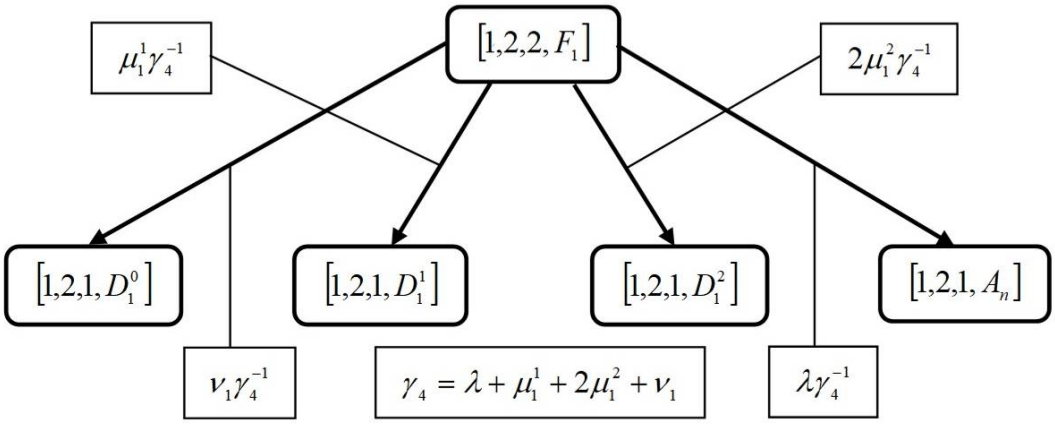


Рисунок 5.7 – UML-діаграма переходу ІСКЗ із стану $[1,2,1,F_1]$ у допустимі наступні стани в залежності від відповіді α на вхідні запити АС

Значення показника доцільності системних операції $k(s,\alpha)$ в контексті ІСКЗ можна розкрити як

$$k(s,\alpha)=\begin{cases} E_\alpha - C_t\left(\mu_i^j\right)^{-1}, \alpha=\alpha_i^j, \\ E_\alpha - C_t\left(\nu_i\right)^{-1}, \alpha=\alpha_i, \\ -E_r, \alpha=0, \\ 0, \alpha=-1, \end{cases} \tag{5.70}$$

де E_α – накопичувальний показник готовності ІСКЗ, який зростає при задоволенні вхідних запитів; E_r – накопичувальний показник неготовності ІСКЗ, який зростає при відхиленні вхідних запитів; C_t – вартість одиниці машинного часу, витраченого на операції очищення D_i^j або F_i. Показник $o(s,\alpha)$ вводиться в управляючу функцію $r(s,\alpha)$ для нормування вартості обчислювальних та комунікаційних ресурсів використовуваних у суб'єкт-системній взаємодії у вигляді

$$o(s,\alpha)=c_b\left(\sum_{j=1}^{T}\sum_{i=1}^{W} ix_i^j + \sum_{i=1}^{W} iy_i\right)+c_e\sum_{j=1}^{T}\sum_{i=1}^{W} ix_i^j ,$$

де c_b – норма вартості комунікаційних ресурсів, а c_e – норма вартості обчислювальних ресурсів, відповідно.

Користуючись можливостями КНМП сформулюємо на основі (5.69) задачу оптимізації готовності ІСКЗ із цільовою функцією

$$\Phi(s,\alpha)=\sum_{s\in S}\sum_{\alpha\in \mathrm{A}_s}\left(r(s,\alpha)z(s,\alpha)\right)\to \max \tag{5.71}$$

і системою обмежень

$$\begin{cases} \sum\limits_{s\in S}\sum\limits_{\alpha\in \mathrm{A}_s}\left(\tau(s,\alpha)z(s,\alpha)\right)=1, \\ \sum\limits_{\alpha\in \mathrm{A}_k} z(k,\alpha)-\sum\limits_{s\in S}\sum\limits_{\alpha\in \mathrm{A}_s}\left(p(k|s,\alpha)z(s,\alpha)\right)=0, \\ \sum\limits_{s\in S}\sum\limits_{\alpha=0}\tau(s,\alpha)z(s,\alpha)\le P_b, \end{cases} \tag{5.72}$$

де $s,k\in S$, $\alpha\in A_s$, $z(s,\alpha)$ – оптимальна стратегія реагування ІСКЗ на вхідні запити для кожного стану s. Перше обмеження у системі (5.72) описує аналізований фрагмент життєвого циклу ІСКЗ сумою оцінок тривалостей станів s, в яких перебуватиме система, реагуючи діями α на вхідні запити АС. Друге обмеження вводиться для балансу вхідних і вихідних зв'язків від-

повідних станів моделі. Третє обмеження визначає імовірність гарантованої готовності ІСКЗ, для чого суми добутків характеристичних $\tau(s,\alpha)$ і оптимізовуваних $z(s,\alpha)$ параметрів ІСКЗ обмежено пороговим значенням імовірності відхилення запиту АС P_b.

Аналіз сформульованої у вигляді (5.71), (5.72) задачі оптимізації дозволяє її класифікувати як задачу лінійного програмування, для розв'язання якої існує універсальний симплекс-метод [184, 185]. Результатом розв'язку такої задачі для конкретної ІСКЗ буде оптимальна стратегія параметризації складових її елементів у вигляді множини оптимальних параметрів $z(s,\alpha)\in Z$, на основі яких можна розрахувати стохастичні оцінки оптимального вибору реакції α у відповідь на вхідний запит від АС до системи, що перебуває у стані s:

$$p(s,\alpha)=z(s,\alpha)\left(\sum_{\alpha'\in \mathrm{A}_s} z(s,\alpha')\right). \tag{5.73}$$

Орієнтація на критичне застосування описуваної ІС робить доцільним доповнення отриманої у вигляді (5.65)–(5.68) моделі її готовності урахуванням необхідності резервування ресурсів на заходи убезпечення системного ІнС від дій АС. В такому разі інтенсивність вхідних запитів на виділення ν ВМ $(1\le \nu \le T)$ від i-го АС, рівень загрози безпеці ІСКЗ від дій якого описується дискретним параметром r, $(1\le r\le R)$, опишемо величиною $\lambda_{i,r,\nu}$. ІСКЗ, відповідно, виділить для задоволення вхідного запиту i-го АС $j+f$ ВМ, де $j\le \nu$ ВМ використовуватимуться АС, а f ВМ резервуватимуться на заходи убезпечення системного ІнС від дій АС. Заходи ІнС ІСКЗ по підтримуванню дій i-го АС у рамках прийнятого запиту описуватимуться експоненційним розподілом із масштабним коефіцієнтом μ_i (для j ВМ – $j\mu_i$, відповідно). Керованими параметрами x_i^j і x_i^f опишемо кількість ВМ, виділених на підтримку дій i-го АС у рамках прийнятого запиту, і кількість ВМ, зарезервованих на заходи убезпечення системного ІнС від дій i-го АС, відповідно. За-

уважимо, що сумарна кількість задіяних у суб'єкт-системній взаємодії ВМ у будь-який момент часу не повинна перевищувати встановленого на етапі проектування системи значення M :

$$\sum_{i=1}^{W}\sum_{j=1}^{T} jx_i^j + \sum_{i=1}^{W}\sum_{j=1}^{T}(j+f)x_i^f \le M .$$

Функціонування ІСКЗ в контексті оцінювання її готовності для АС із резервуванням ресурсів на убезпечення системного ІнС від дій останнього описуватимемо простором станів $s = \lfloor x_1, \ldots, x_T, x_1^f, \ldots, x_T^f, e(s) \rfloor \in S$, де характеристична змінна $e(s) \in \{A_{r,\nu}, D_j, D_j^f\}$ описує визначену множину системних операцій, що можуть виконуватися в ІнС ІСКЗ у довільний момент часу її життєвого циклу. Зокрема, виділимо: операцію готовності до прийняття вхідного запиту $A_{r,\nu}$ на виділення ν ВМ для потреб АС, рівень небезпечності якого не перевищує r; операцію очищення ІнС D_j, при якій очищуються виділені для потреб АС ресурси, задіяні під j ВМ; операцію очищення зарезервованих ресурсів ІнС D_j^f, при якій очищуються ресурси, виділені під f ВМ, які здійснювали заходи з убезпечення системного ІнС від дій АС, здійснюваних у виділених останньому j ВМ. На вхідний запит від АС ІСКЗ, що перебуває у стані s, в ІнС якої в цей момент часу виконується операція $e(s)$, може відповісти одним із можливих варіантів надання сервісу, описаних множиною $A = \bigcup_{s \in S} A_s : \{-1; 0; \alpha_i^j; \alpha_i\}$, де -1 – ситуація відхилення вхідного запиту з причини виконання однієї із операцій очищення; 0 – відхилення запиту з іншої причини; α_i^j – задовольняється вхідний запит від i-го АС із виділенням для його потреб j ВМ в ІнС СРЦ; α_i – задовольняється вхідний запит від i-го АС із виділенням f ВМ для реалізації заходів по убезпеченню системного ІнС від здійснюваних суб'єктом дій. Аналогічно (5.65), охарактеризуємо функцією $\gamma(s, \alpha)$ швидкість зміни стану системи s із активною операцією $e(s)$, що супроводжується відповіддю α на вхідний запит АС. У виразі (5.74) пара-

метр ω описує фактичну кількість ВМ, виділених ІСКЗ для підтримки дій АС, у межах виконуваного запиту

$$\gamma(s,\alpha)=\begin{cases}\sum_{i=1}^{R}\sum_{j=1}^{M}\lambda_{i,j}+\sum_{i=1}^{W}\sum_{j=1}^{T}j\left(x_i^j+x_i^f\right)\mu_i, e(s)=A_{r,\nu}, \alpha=0,\\ \sum_{i=1}^{R}\sum_{j=1}^{M}\lambda_{i,j}+\sum_{i=1}^{W}\sum_{j=1}^{T}j\left(x_i^j+x_i^f\right)\mu_i+\omega\mu_i, e(s)=A_{r,\nu}, \alpha=\alpha_i^{\omega}\vee a_i^f,\\ \sum_{i=1}^{R}\sum_{j=1}^{M}\lambda_{i,j}+\sum_{i=1}^{W}\sum_{j=1}^{T}j\left(x_i^j+x_i^f\right)\mu_i-\omega\mu_i, e(s)=D_{\omega}\vee D_{\omega}^f,\end{cases} \tag{5.74}$$

Деталізуємо опис динаміки системи, поведінка якої описується виразом (5.74), формалізувавши імовірності її переходу із стану s, у якому виконується операція $e(s)$, у стан k в результаті відповіді α на вхідний запит АС. За аналогією з (5.66), імовірність переходу системи $p(k|s,\alpha)$ зі стану $s=\left\lfloor x_1,\ldots,x_T,x_1^f,\ldots,x_T^f,A_{r,\nu}\right\rfloor$ у стан k в наслідок відповіді α на вхідний запит від АС опишемо як

$$p(k|s,\alpha)=\begin{cases}\lambda_{r,\nu}\gamma(s,\alpha)^{-1}, e(k)=A_{r,\nu},\\ \mu_i j\left(x_i^j+1\right)\gamma(s,\alpha)^{-1}, e(k)=D_j\wedge\alpha=\alpha_i^j,\\ \mu_i j x_i^j\gamma(s,\alpha)^{-1}, e(k)=D_j\wedge\alpha\neq\alpha_i^j,\\ \mu_i j\left(x_i^f+1\right)\gamma(s,\alpha)^{-1}, e(k)=D_j^f\wedge\alpha=\alpha_i^f,\\ \mu_i j x_i^f\gamma(s,\alpha)^{-1}, e(k)=D_j^f\wedge\alpha\neq\alpha_i^f.\end{cases} \tag{5.75}$$

Імовірність переходу системи $p(k|s,\alpha)$ зі стану $s=\left\lfloor x_1,\ldots,x_T,x_1^f,\ldots,x_T^f,D_{\omega}\right\rfloor$ у стан k у наслідок відповіді α на вхідний запит від АС опишемо як

$$p(k|s,\alpha)=\begin{cases}\lambda_{r,\nu}\gamma(s,\alpha)^{-1}, e(k)=A_{r,\nu},\\ \mu_i j\left(x_i^j-1\right)\gamma(s,\alpha)^{-1}, e(k)=D_j\wedge j=\omega,\\ \mu_i j x_i^j\gamma(s,\alpha)^{-1}, e(k)=D_j\wedge j\neq\omega,\\ \mu_i j x_i^f\gamma(s,\alpha)^{-1}, e(k)=D_j^f.\end{cases} \tag{5.76}$$

Імовірність переходу системи $p(k|s,\alpha)$ зі стану $s=\left\lfloor x_1,\ldots,x_T,x_1^f,\ldots,x_T^f,D_{\omega}^f\right\rfloor$ у стан k у наслідок відповіді α на вхідний запит від АС опишемо як

$$p(k|s,\alpha)=\begin{cases}\lambda_{r,\nu}\gamma(s,\alpha)^{-1}, e(k)=A_{r,\nu},\\ \mu_i j\left(x_i^f-1\right)\gamma(s,\alpha)^{-1}, e(k)=D_j^f \wedge j=\omega,\\ \mu_i j x_i^f \gamma(s,\alpha)^{-1}, e(k)=D_j^f \wedge j\neq\omega,\\ \mu_i j x_i^f \gamma(s,\alpha)^{-1}, e(k)=D_j.\end{cases} \quad (5.77)$$

Вирази (5.76), (5.77) сформульовано із урахуванням того, що всі вхідні запити від АС, що надходять до ІСКЗ, яка виконує одну з операцій очищення ІнС D_ω або D_ω^f, автоматично відхилятимуться доки ці сервісні операції не завершаться.

Скориставшись виразами (5.74)–(5.77) синтезуємо КНМП, який описуватиме готовність ІСКЗ для АС із резервуванням ресурсів на убезпечення системного ІнС від дій останніх. Нехай $W=2$, $T=3$, $f=1$, вихідний стан системи

$$s=\left[x_1,x_2,x_3,x_1^1,x_2^1,x_3^1,e(s)\right]=\left[0,1,0,0,1,0,A_{r,2}\right],$$

тоді UML-діаграму станів, яка ілюструє процес переходу зі стану s у стани $k=\{[0,2,0,0,2,0,e(s)],[0,1,0,0,1,0,e(s)],[0,1,0,0,1,1,e(s)]\}$ на основі моделі (5.74)–(5.77), візуалізуємо на рис. 5.8.

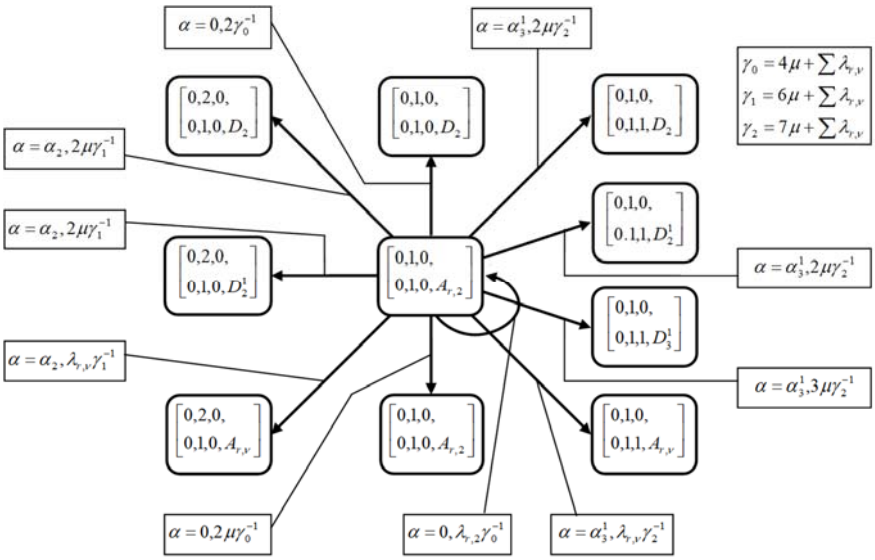


Рисунок 5.8 – UML-діаграму переходу ІСКЗ із стану s у стани $k=\{[0,2,0,0,2,0,e(s)],[0,1,0,0,1,0,e(s)],[0,1,0,0,1,1,e(s)]\}$ згідно з моделлю (5.74)–(5.77).

Задачу управління готовністю ІСКЗ із резервування ресурсів на заходи убезпечення системного ІнС від дій АС сформулюємо аналогічно (5.69), конкретизувавши спосіб визначення показника доцільності системних операції $k(s,\alpha)$:

$$k(s,\alpha)=\begin{cases} E_\alpha - rE_tR^{-1} - C_t(j\mu_i)^{-1}, e(s)=A_{r,\nu} \vee \alpha=\alpha_i^j, \\ E_\alpha + rE_sR^{-1} - C_t(j\mu_i)^{-1}, e(s)=A_{r,\nu} \vee \alpha=\alpha_i^f, \\ E_r r^{-1}, e(s)=A_{r,\nu} \vee \alpha=0, \\ 0, \alpha=-1, \end{cases} \tag{5.78}$$

де E_s – накопичувальний показник, що враховує додаткове резервування ВМ для убезпечення ІнС ІСКЗ від дій АС, тоді як E_t – накопичувальний показник, що враховує кількість виділених АС ВМ, дії в яких не контролюються ІС.

Зростання показника E_s відбивається на зниженні готовності ІСКЗ, адже її ресурси додатково витрачатимуться на задачі самоубезпечення, що, втім, веде до зростання безпеки ІСКЗ. Показник E_t виступає антагоністом показникові E_s. Загалом, ситуації, коли дії АС супроводжуються зростанням показника E_s або E_t, є нетиповими, непередбаченими у СПБ, і є результатом втручання адміністратора в перебіг процесу доступу АС до ІнС ІСКЗ. Показник для нормування вартості обчислювальних та комунікаційних ресурсів $o(s,\alpha)$ представимо як

$$o(s,\alpha)=c_{vm}\left(\sum_{i=1}^{W}\sum_{j=1}^{T} jx_i^j + \sum_{i=1}^{W}\sum_{j=1}^{T}(j+f)x_i^f\right),$$

де c_{vm} – норма вартості використання ресурсів однієї ВМ.

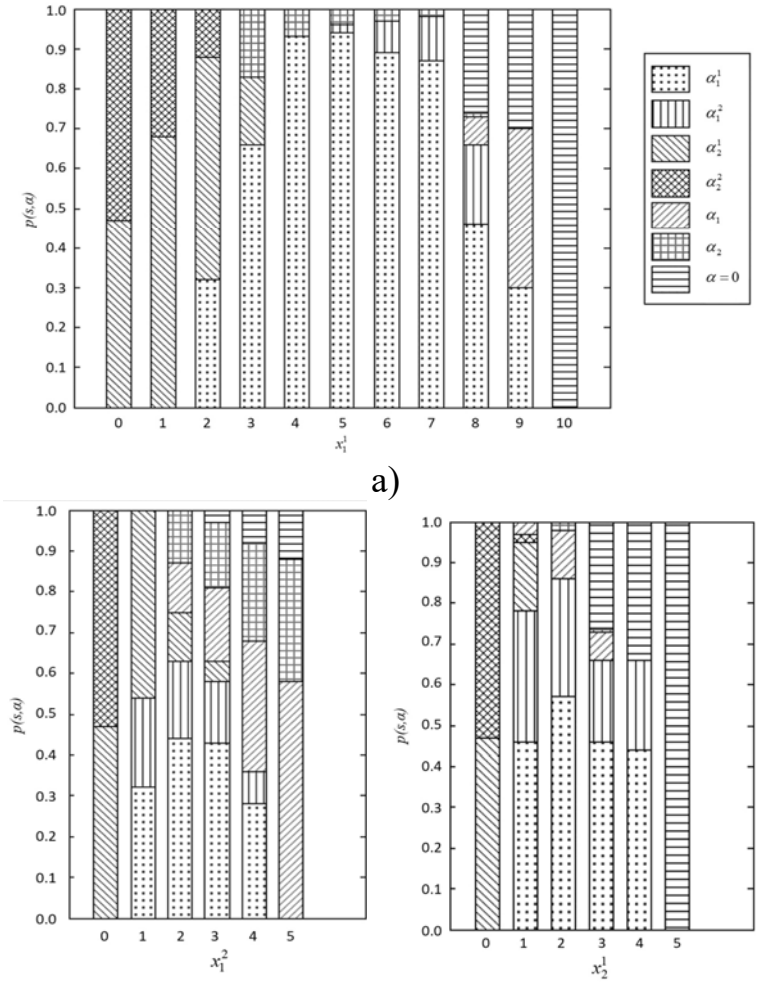
Описані вище адаптації, спрямовані на урахування при оцінюванні готовності ІСКЗ необхідності резервування ресурсів на її самоубезпечення, можна без додаткових модифікацій узагальнити у вигляді задачі оптимізації з цільовою функцією $\Phi(s,\alpha)$, аналогічною (5.71), і системою обмежень, аналогічною (5.72). Результатом розв’язання такої задачі для конкретної ІСКЗ буде

стратегія управління доступом до її ІнС із оптимізацією внутрішньосистемних сервісних операцій, отримувана у вигляді множини оптимальних параметрів $z(s,\alpha)\in Z$, на основі яких формуватимуться оптимальні з позиції СПБ відповіді α від ІСКЗ, що перебуває в стані s, на вхідні запити АС. Стохастичну оцінку отриманої оптимальної стратегії управління доступом Z можна розрахувати на основі (5.73).

Обчислимо оптимальну стратегію управління доступом до ІСКЗ розв'язавши задачу оптимізації (5.71), (5.72) у програмному середовищі Matlab за допомогою функції *linprog*, яка входить до Optimization Toolbox, із такими значеннями вихідних параметрів: ІСКЗ дозволяє створювати не більше 2-х ВМ у ІнС СРЦ і 2-х ВМ у ІнС СД для одного прийнятого від АС вхідного запиту (сесії), шаблон формату стану має вигляд $s=\left[x_1^1,x_1^2,x_2^1,x_2^2,y_1,y_2,e(s)\right]$, стохастичні параметри інтенсивностей запитів $\left[\lambda,\mu_1^1,\mu_1^2,\mu_2^1,\mu_2^2,\nu_1,\nu_2\right]$ встановимо рівними $[12;3;4;5;6;3{,}5;5{,}5]$, обмеження на кількість інформаційних потоків $[M,B]$ встановимо рівними $[10,10]$, коефіцієнти для задачі оптимізації готовності ІСКЗ $\left[E_\alpha,E_r,C_t,P_b\right]$ встановимо рівними $\left[6,3,1,5\cdot10^{-3}\right]$. Підставивши вказані вище значення у вирази (5.71), (5.72), ми отримали оптимальні значення налаштувань СПБ у вигляді множини Z, які у формі діаграм представлено на рис. 5.9 для різних варіантів вихідного стану ІСКЗ s враховуючи, що $\sum\alpha=1, x_1^1=\overline{0{,}10}$, $x_1^2,x_2^1,x_2^2=\overline{0,5}$.

Інтерпретуємо результати, наведені на рис. 5.9а. Нехай, наприклад, $x_1^1=3$ і $y_1=3$ тобто в даний момент часу ІСКЗ підтримує три активних сесії 1-го АС, кожна з яких використовує 1 ВМ у ІнС СРЦ і 1 ВМ у ІнС СД. Враховуючи, що за умовою експерименту максимальна кількість ВМ, яку можна створити в ІнС СРЦ, $M=10$ і максимальна кількість ВМ, яку можна створити у ІнС СД, $B=10$, то обчислювані ресурси СРЦ і СД завантажено на 30 % і 30 %, відповідно. Для поточного стану s здійснювана ІСКЗ внутрішня операція $e(s)=A_n$, тобто система очікує на вхідний запит. Відповідно до розра-

хованої оптимальної СПБ, відповідь системи на вхідний запит буде α_1^1 (виділення 1 ВМ у ІнС СРЦ і 1 ВМ у ІнС СД) із імовірністю 65 %, α_2^1 (виділення 2 ВМ у ІнС СРЦ і 1 ВМ у ІнС СД) із імовірністю 20 %, α_2 (виділення 2 ВМ у ІнС СРЦ) із імовірністю 15 %, тобто СПБ ІСКЗ віддає перевагу збалансованому помірному завантаженню ресурсів СРЦ і СД.



а)

б) в)

Рисунок 5.9 – Оптимальна стратегія відповіді ІСКЗ на вхідний запит АС, якщо: а) стан $s = [x_1^1, 0, 0, 0, y_1 = x_1^1, 0, A_n]$, б) стан $s = [0, x_1^2, 0, 0, y_1 = 2x_1^2, 0, A_n]$, в) стан $s = [0, x_1^2, 0, 0, y_1 = 0{,}5x_1^2, 0, A_n]$

За аналогією, при $x_1^1 = 9$ і $y_1 = 9$ відповідь СПБ на вхідний запит буде: $\alpha_0 = 30\,\%$ (відхилення запиту), $\alpha_1^1 = 30\,\%$ (виділення 1 ВМ у ІнС СРЦ і 1 ВМ

у ІнС СД, при чому ресурси ІСКЗ будуть повністю завантажено), $\alpha_1 = 40\,\%$ (виділення 1 ВМ у ІнС СРЦ). При $x_1^1 = 10$ відповідь СПБ на вхідний запит буде $\alpha_0 = 100\,\%$.

Для візуалізації отриманої в результаті розв'язання задачі (5.71), (5.72), оптимальної СПБ для управління доступом до ІСКЗ приведемо систему в стан $s = [0, 0, 0, 0, 0, 0, A_n]$ (без урахування інформації про попередні стани), тоді узагальнену оптимальну стратегію управління доступом у вигляді значень імовірностей $p(s, \alpha)$, похідних від керованих змінних задачі оптимізації (5.71), (5.72) $z(s, \alpha) \in Z$, які описують варіант відповіді системи α на вхідні запити, які надходять від АС із різною інтенсивністю μ, зображено на рис. 5.10.

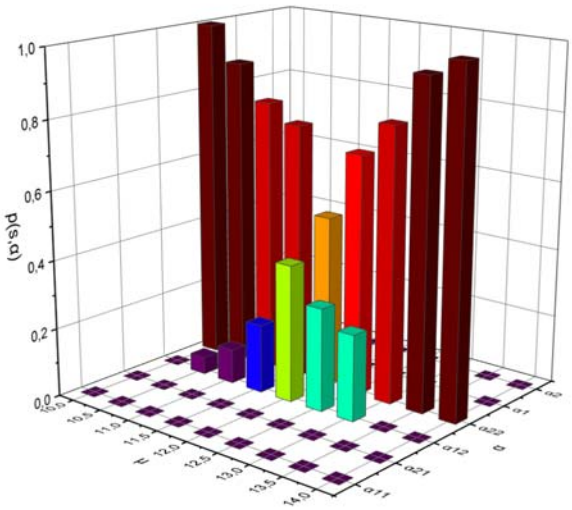


Рисунок 5.10 – Візуалізація оптимальної стратегії відповіді ІСКЗ, яка перебуває у стані $s = [0, 0, 0, 0, 0, 0, A_n]$, на вхідний запит від АС

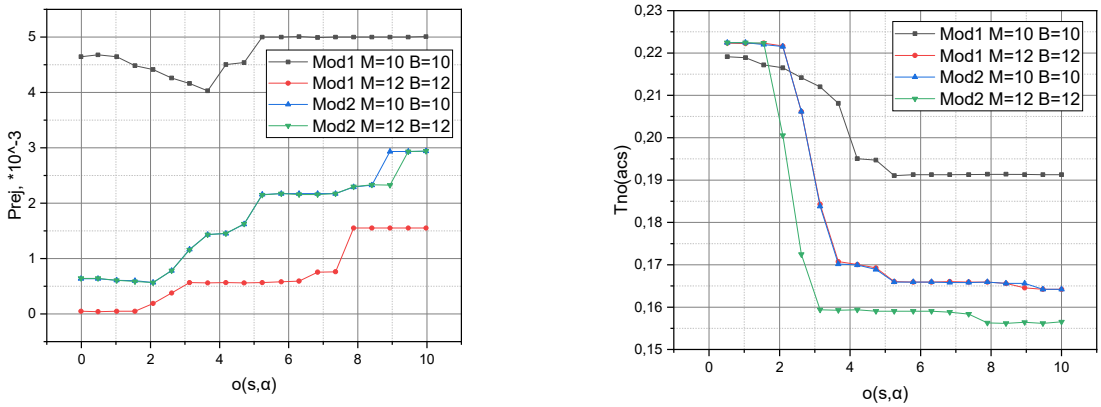
Наведенні на рис. 5.10 результати показують, що в оптимальній стратегії управління доступом ІСКЗ при низькій і високій інтенсивності надходження вхідних запитів спостерігається тенденція до рівномірного завантаження ІнС СРЦ і ІнС СД. При середній інтенсивності надходження вхідних запитів ІнС СРЦ завантажується більше, що призводить до зростання вартості функціонування системи за одиницю часу але дозволяє підтримувати сто-

хастичну оцінку готовності системи в заданих виразом (5.72) межах, тому що обчислювальна потужність, а отже, і швидкість реагування апаратної платформи СРЦ вища за аналогічну характеристику СД.

Оцінимо залежність готовності ІСКЗ від витрат на функціонування системи $o(s,\alpha)$. Враховуючи, що показник $o(s,\alpha)$ для базової моделі готовності ІСКЗ (далі – Mod_1) і для моделі готовності ІСКЗ із резервуванням ресурсів на убезпечення системного ІнС від дій АС (далі – Mod_2) розраховується по різному, введемо узагальнені показники для оцінювання готовності. Використовуватимемо узагальнений показник імовірності відхилення вхідного запиту $P_{rej} = N_{rej} N_{all}^{-1}$, де N_{rej} – кількість відхилених ІСКЗ вхідних запитів, а N_{all} – загальна кількість вхідних запитів за період спостережень T_s, і показник середньої тривалості сервісних операцій $T_{\overline{acs}} = T_s \left(N_{all} - N_{rej}\right)^{-1}$, який є узагальненням показника $\tau(s,\alpha)$ для періоду спостережень T_s. Емпіричні значення залежності цих показників від узагальненої вартості використання ІСКЗ за одиницю часу $o(s,\alpha)$ для різних стратегій завантаження ІнС СРЦ і ІнС СД, кожна з яких задовольняє сформульовану в (5.72) умову $\sum_{s \in S} \sum_{\alpha=0} \tau(s,\alpha) z(s,\alpha) \le P_b$, наведено на рис. 5.11.

Наведені на рис. 5.11 результати одержано при $P_b = 5 \cdot 10^{-3}$. Як видно із рис. 5.11а, узагальнена імовірність відхилення вхідного запиту P_{rej} зростає із зростанням узагальненої вартості використання системи за одиницю часу $o(s,\alpha)$ для всіх стратегій управління доступом до ІСКЗ. Втім, найкраща динаміка залежності спостерігається для стратегій, значення параметрів яких наближені до оптимальної. В цілому ж характер залежності P_{rej} від $o(s,\alpha)$ можна пояснити тим, що зростання $o(s,\alpha)$ пов’язане зі зростанням кількості активних ВМ, що, природно, призводить до зростання кількості відхилень вхідних запитів. Наведені на рис. 5.11б результати показують, що для всіх стратегій управління доступом до ІСКЗ значення середньої тривалості серві-

сних операцій становить скінченну величину, значення якої лише частково залежить від витрат на функціонування системи, а загалом визначається обраною стратегією управління доступом, що підтверджує актуальність отриманих моделей.



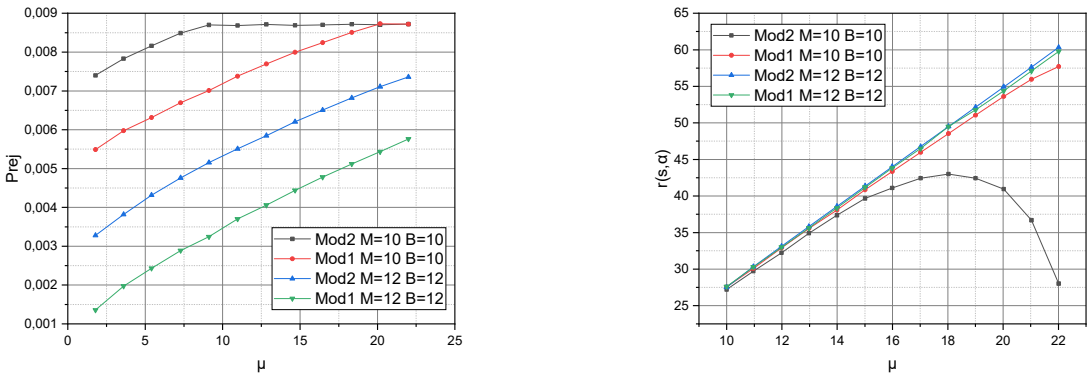
а) б)

Рисунок 5.11 – Визначена із урахуванням відповідної стратегії готовності ІСКЗ залежність узагальненої вартості використання системи за одиницю часу $o(s,\alpha)$ від: а) узагальненого показника імовірності відхилення вхідного запиту P_{rej}, б) середньої тривалості сервісних операцій $T_{\overline{acs}}$.

Окремої уваги варте порівняння моделі готовності ІСКЗ із резервуванням ресурсів на убезпечення системного ІнС від дій АС Mod_2 із базовою моделлю готовності ІСКЗ Mod_1 за такими критеріями як узагальнена імовірність відхилення вхідного запиту P_{rej} і значення функції якості реакції ІСКЗ на вхідний запит $r(s,\alpha)$, яке розраховується за виразом (5.69) із сегрегацією правила обчислення показника $k(s,\alpha)$ за видом моделі готовності. Дослідження моделі Mod_2 проводилося в умовах надходження вхідних запитів від АС, кожному із яких було присвоєно відповідний рівень загрози безпеці ІСКЗ у вигляді параметра r, значення якого вибиралися із множини значень $\{\text{low}, \text{medium}, \text{high}\} = \{0{,}2;\ 0{,}5;\ 0{,}8\}$, відповідно. Правила виділення ВМ на убезпечення системного ІнС в залежності від значення параметра r для i-го АС

формулювалися так: $r_i = low \to x_i^j = 1, 2, 3 \to x_i^f = 0, 0, 1$, $r_i = medium \to x_i^j = 1, 2, 3 \to x_i^f = 0, 1, 2$, $r_i = high \to x_i^j = 1, 2, 3 \to x_i^f = 1, 2, 2$. Обмеження $x_i^j \le 3$, $f_i^j \le 2$, $M = \{10, 12\}$, $B = \{10, 12\}$ стосувалися обох досліджуваних моделей. Для проведеного дослідження імовірність того, що вхідний запит надійшов від АС із рівнем $r = \{\text{low}, \text{medium}, \text{high}\}$ становила $\{0{,}2; 0{,}3; 0{,}5\}$, відповідно.

Наведені на рис. 5.12а результати показують, що імовірність відхилення вхідного запиту більшою мірою залежить від кількості доступних для створення ВМ апаратних ресурсів у системі, встановлюваних параметрами $[M, B]$, та інтенсивності надходження вхідних запитів. Виділення системних ресурсів на заходи убезпечення не призводять до перевищення глобального обмеження на імовірність відхилення вхідних запитів $P_b = 5 \cdot 10^{-3}$ із зростанням інтенсивності їх надходження, що говорить про ефективність оптимальних налаштувань СПБ для обох розглянутих моделей готовності ІСКЗ.



а) б)

Рисунок 5.12 – Порівняння моделей готовності Mod_2 і Mod_1 за критерієм:

а) узагальненої імовірності відхилення вхідного запиту P_{rej};

б) значенням функції якості реакції ІСКЗ $r(s, \alpha)$ на вхідний запит.

Втім для СПБ, сформульованої на основі моделі Mod_2, узагальнена імовірність відхилення вхідних запитів виявляється вищою за значення цього ж по-

казника для СПБ, сформульованої на основі моделі Mod_1. Особливо цікаві результати наведено на рис. 5.12б. Виявилося, що якість реакції ІСКЗ, яка визначається моделлю Mod_2, при значенні параметрів $[M, B] = [10, 10]$ починає стрімко знижуватися із зростанням інтенсивності вхідних запитів,

але при збільшенні значень параметрів $[M, B]$ до $[12, 12]$ ситуація покращується до зіставних із моделлю Mod_1 результатів. Таку реакцію можна пояснити вибраними правилами виділення ВМ на убезпечення системного ІнС, при яких для АС із $r = 0{,}8$ співвідношення кількості ВМ, виділених на підтримку дій АС, до кількості ВМ, виділених на заходи убезпечення, становить $\approx 3:2$. В результаті, якщо інтенсивність запитів від «ненадійних» АС домінує у множині вхідних запитів, системі не вистачає до $20\,\%$ апаратних ресурсів для ефективного функціонування. Цю обставину необхідно враховувати при проектуванні ІСКЗ. Також відзначимо, Модель залежності конфіденційності процесу автентифікації і готовності інформаційній системі критичного застосування наведено у додатку К.

5.4 Моделі функційної безпечності і живучості інформаційної системи критичного застосування

В умовах впровадження Індустрії 4.0 та Інтернету речей питання гарантоздатності інформаційно–технологічних систем стає одним із важливіших, адже тотальний доступ до єдиного інформаційного простору може стати каналом розповсюдження наслідків збоїв у одній і з систем на інші із надзвичайною швидкістю і непередбачуваними наслідками.

Зосередимося на двох атрибутах гарантоздатності – функційній безпечності (ФБ) і живучості. Питанням ФБ присвячено низку профільних міжнародних стандартів: IEC 61508, IEC 61511, IEC 62061, ISO 26262, EN 50129, IEC 62304 тощо. Зокрема, згідно IEC 61508, ФБ – складова загальної безпеки, зумовлена використанням керованого обладнання та систем управління, і залежна від правильності функціонування систем, які стосуються безпеки, та інших засобів зниження ризику. Втім, якщо об’єктом застосування згаданих стандартів є інформаційна система (ІС) як така, то як ФБ так і її атрибути або безпосередньо пов’язують із надійністю апаратної платформи ІС, або тісно переплітають із інформаційною безпекою. Ця обставина робіть актуальною задачу синтезу гнучкої, універсальної моделі ФБ інформаційно–технологічної системи як

комплексного явища, здатної для застосування на етапі проектування останньої. В широкому сенсі живучість – це фундаментальна властивість, яка дозволяє ІС реалізувати її функціональне призначення попри вплив негативних факторів. У контексті теорії інформаційної безпеки живучість – це властивість ІС зберігати цілісність застосовуючи вбудовані механізми адаптації навіть за рахунок зміни функціонального призначення. Якщо досліджувана ІС орієнтована на критичне застосування, то живучість пропонується розглядати як властивість ІСКЗ зберігати цілісність та функціональне призначення в умовах впливу негативних факторів, за рахунок адаптаційних механізмів, закладених на етапі проектування в захисні механізми ІС, правила налаштування яких визначено у її політиці безпеки. Якщо в наслідок збою ІСКЗ не в змозі зберегти цілісність або функціональне призначення, то система повинна перейти у нефункціональний стан зберігаючи ФБ. Саме ця обставина обумовила комплексне досліджень ФБ і живучості для класу ІСКЗ.

Вхідними даними для моделі ФБ ІСКЗ є множина первинних структурних або динамічних моделей варіантів реалізації інформаційної системи, яка проектується, формалізованих у єдиній парадигмі, наприклад, мереж Петрі або марковських моделей тощо. Структурною основою такої моделі є орієнтований граф, вершини якого відповідають станам, у яких перебуває як модельована система в цілому, так і її компоненти зокрема, а дуги демонструють допустимість і напрям переходів між станами. Саме така первинна інформація доступна на етапі проектування ІСКЗ.

Припустимо, що досліджувана ІСКЗ є результатом інтеграції атомарних модулів, узагальнених множиною $C = \{c_1, c_2, \ldots, c_N\}$, де довільний модуль c_i, $i \in \overline{1, N}$, характеризується інтенсивністю небезпечних збоїв λ_i і інтенсивністю відновлення ФБ μ_i, що входять у множини Λ і M, відповідно. Імовірності перебування модуля c_i у функціональному або нефункціональному станах у момент часу t із урахуванням множин Λ і M опишемо, відповідно, виразами:

$$P_i^f(t) = (\lambda_i + \mu_i)^{-1}\left(\mu_i + \lambda_i e^{-(\lambda_i+\mu_i)t}\right), \tag{5.79}$$

$$P_i^{\bar{f}}(t) = (\lambda_i + \mu_i)^{-1}\left(\lambda_i - \lambda_i e^{-(\lambda_i+\mu_i)t}\right). \tag{5.80}$$

Якщо базова структурна модель ФБ ІСКЗ представлена марковським ланцюгом, то імовірності $P_i^f(t)$ і $P_i^{\bar{f}}(t)$ можна розрахувати безпосередньо, розв'язавши систему диференційних рівнянь виду:

$$\begin{cases} \dfrac{\partial P_i^f(t)}{\partial t} = -\lambda_i P_i^f(t) + \mu_i P_i^{\bar{f}}(t), \\ \dfrac{\partial P_i^{\bar{f}}(t)}{\partial t} = \lambda_i P_i^f(t) - \mu_i P_i^{\bar{f}}(t). \end{cases} \tag{5.81}$$

Отже, при безпосередній формалізації моделі ФБ ІСКЗ у парадигмі марковських моделей [348, 349] для кожного модуля необхідно буде знайти чисельний розв'язок систем диференційних рівнянь виду (5.81), а також описати взаємодію модулів у межах ІСКЗ. Вочевидь, кількість обчислень із збільшенням кількості модулів стрімко зростатиме, що обмовляю актуальність пошуку детермінованого методу структурної редукції моделі ФБ ІСКЗ.

Охарактеризуємо довільний стан $s_j \in S$ графу моделі ФБ ІСКЗ ступенем $R(s_j)$, $0 \le R(s_j) \le 1$, при чому $s_j \ne s_{init}$, де $s_0 = s_{init}$ – функціональний стан ІСКЗ, вага якого $R(s_{init}) = 1$. Визначивши q_{ij} – кількість переходів зі стану i у стан j, обчислимо ступінь $R(s_j)$ за виразом

$$R(s_j) = \max_{s_i \in S_p}\left(R(s_i) q_{ij}\left(\sum_{k \in K} q_{ik}\right)^{-1}\right), \tag{5.82}$$

де множина S_p містить допустимі стани, які передують s_j, а множина K містить індекси всіх допустимих станів–нащадків стану s_i.

Врахувавши вираз (5.82), опишемо процес ініціалізації множини $G = (\Sigma, \Omega) \in C$, де C – множина переходів вихідного орієнтованого графу, множина Σ містить ідентифікатори всіх станів, ступені $R(\Sigma)$ яких не менші

порогового значення τ, а Ω – множина переходів між станами, які увійшли до множини Σ.

Прийнявши вихідні припущення: $C \leftarrow \{s_{init}\}$, $R(s_{init}) = 1$, $\Sigma \leftarrow \emptyset$, $\Omega \leftarrow \emptyset$, формалізуємо простір станів базової моделі ФБ досліджуваної ІСКЗ.

Поки виконуються умови $C \neq \emptyset$ і $\max\{R(s_k), s_k \in C\} \geq \tau$ будемо ітеративно:

- вибирати з–поміж ще не досліджених станів стан s_i із найбільшою вагою: $s_i = \arg\max\{R(s_k), s_k \in C\}$, $C \leftarrow C \setminus \{s_i\}$, $\Sigma \leftarrow \Sigma \cup \{s_i\}$;
- обчислювати кількість допустимих переходів зі стану s_i у стани s_k, $k \in K$: $D = \sum_{k \in K} q_{ik}$;
- розраховувати для всіх станів s_j, досяжних зі стану s_i, ступені $R(s_j)$ виходячи з міркувань: якщо умова $s_j \notin \Sigma$ виконується, то обчислюємо величину $R = R(s_i) q_{ij} D^{-1}$ та перевіряємо, чи виконується умова $s_j \in C$. Якщо так, то ступінь $R(s_j) = \max\{R(s_j), R\}$, а якщо ні, то вважаємо ступінь $R(s_j) = R$ і додаємо стан s_j у множину C: $C \leftarrow C \cup \{s_j\}$;
- нарощувати множину переходів Ω, враховуючи попередньо прийняте рішення щодо стану s_j і його ступеню $R(s_j)$: $\Omega = \Omega \cup \{(s_i, q_{ij}, s_j)\}$.

Визначена в результаті вищеописаних дій множина $G = (\Sigma, \Omega)$ містить інформацію щодо вагомих станів і переходів між ними. Залишилося спростити множину C, виключивши з неї інформацію стосовно станів, які не увійшли до множини Σ: для кожного елементу $t = (s_i, q_{ij}, s_j)$ множини Ω перевіряємо умову $s_j \notin \Sigma$ і якщо вона виконується, то $\Omega \leftarrow \Omega \setminus \{t\}$.

Як зазначалося у статтях [50, 55, 56, 58], інтерфейс суб’єкт–системної взаємодії (ССВ) ІСКЗ реалізовано у інформаційному середовищі (ІнС) сервера–реєстраційного центру (СРЦ), із можливістю віддаленого управління ІнС множини серверів даних (СД). Управління ССВ на рівні ІСКЗ здійснює керована

системною політикою безпеки (СПБ) підсистема розмежування доступу (ПРД). Для підтримки дій авторизованого суб'єкта (АС) створюються віртуальні машини (ВМ) у ІнС СРЦ та, за рішенням ПРД, у ІнС СД, кількість і позиціонування яких визначається в залежності від розташування необхідних АС інформаційних ресурсів (ІнР), характеру операцій над ними, привілей АС тощо. Також, одночасно із виділенням ВМ для задоволення потреб АС, ПРД виділяє ВМ на заходи самоубезпечення ІСКЗ, кількість яких залежить від рівня потенційної небезпечності АС. Формалізуємо модель делегування частки цих ВМ на забезпечення живучості ІСКЗ, врахувавши, що кількість і розташування цих ВМ визначатиметься потребами забезпечення живучості, а не розташуванням чи кількістю ВМ, виділених для підтримки дій АС.

Позначимо імовірність передчасного переривання активного сеансу ССВ з причини: – впливу сервісних операцій ІС на активні ВМ: p_1, [у.о.]; – недопустимих операцій всередині активних ВМ: p_2, [у.о.]; – втручання ПРД, зумовленого конфліктом правил СПБ: p_3, [у.о.]; – збою ПРД: p_4, [у.о.] Зважатимемо, що $\sum_{i=1}^{4} p_i = 1$. Також позначатимемо середню тривалість повноцінного відновлення активного сеансу ССВ після: – переключення з активної ВМ на резервну в наслідок виконання сервісних операцій у першій: β_0^{-1}, [с]; – переключення з активної ВМ на резервну в наслідок критичного збою у першій: β_1^{-1}, [с]; – перезавантаження активної ВМ: β_2^{-1}, [с]; – збою у активній ВМ: β_3^{-1}, [с]; – здійснення сервісних операцій у ПРД: β_4^{-1}, [с]; – збою у ПРД: β_5^{-1}, [с]; – перезавантаження ПРД: β_6^{-1}, [с]; – функціонального збою СРЦ: β_7^{-1}, [с]. Передбачається, що: – ІнР ІСКЗ зберігаються на дискових масивах типу RAID1; – ІнС ІСКЗ і ІнС ВМ оперативно оновлюють відповідні журнали реєстрації.

Модель живучості ІСКЗ будуватимемо для достатньо тривалого часового інтервалу $\gamma^{-1} >> \max(\beta_i)$, $i = \overline{1,7}$, у формалізмі неперервних марковських ланцюгів. Відповідно, синтезовану модель візуалізовано UML–діаграмою станів

на рисунку 5.13. Вихідним станом $s_0 = s_{init}$ моделі є стан збою ССВ, тривалість якого прямує до нуля – $\gamma^{-1} \to 0$. Стани s_1, s_2, s_3, s_4 характеризують, відповідно, збій сеансу ССВ з причини: – перезавантаження активної ВМ; – непередбаченого сценарію функціонування ІнС СРЦ; – перезавантаження ПРД; – непередбаченого сценарію функціонування ПРД. Стани s_5, s_6, s_7, s_8 характеризують відновлення за допомогою резервних ВМ сеансу ССВ, збій якого викликано, відповідно: – перезавантаженням активної ВМ; – критичного збою активної ВМ; – перезавантаженням активної ВМ з ініціативи ПРД; – критичного збою ПРД. Стан s_9 описує ситуацію, коли ПРД здатна відновити функціональність після перезавантаження. Стан s_{10} описує ситуацію, коли функціональність ВМ відновлено, і вона очікує від ПРД команди на активацію. Стан s_{11} описує ситуацію відновлення ССВ після збою.

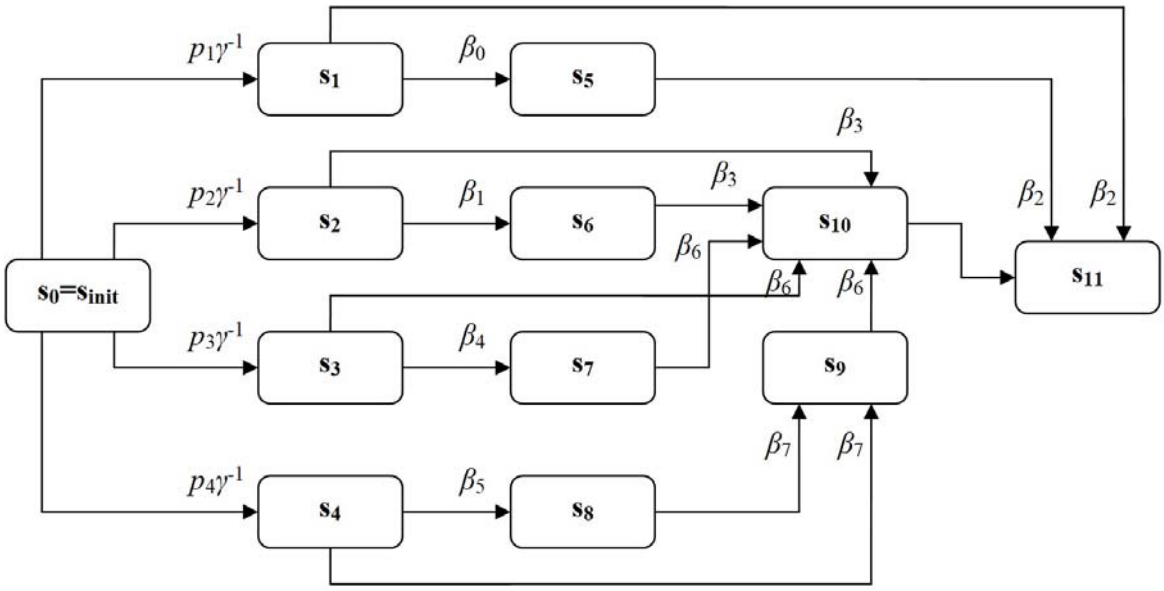


Рисунок 5.13 – UML–діаграма станів моделі живучості ІСКЗ.

Формалізуємо перехідні імовірності $\pi_i(t)$, $i = \overline{1,11}$, для синтезованої марковської моделі живучості ІСКЗ, враховуючи, що $\sum_{i=1}^{11} \pi_i(t) = 1$. Нехай вихідні значення імовірностей станів моделі такі: $\pi_i(0) = p_i$, $i = \overline{1,4}$; $\pi_i(0) = 0$, $i = \overline{5,11}$.

Тоді імовірності $\pi_i(t)$, $i=\overline{1,11}$, для довільного моменту часу t опишемо виразами:

$$\pi_i(t)=\pi_i(0)\exp(-X_i t),\ i=\overline{1,4},$$
$$\pi_5(t)=\pi_1(0)\left(\exp(-\beta_2 t)-\exp(-X_1 t)\right),$$
$$\pi_6(t)=\pi_2(0)\left(\exp(-\beta_3 t)-\exp(-X_2 t)\right),$$
$$\pi_7(t)=\pi_3(0)\left(\exp(-\beta_6 t)-\exp(-X_3 t)\right),$$
$$\pi_8(t)=\pi_4(0)\left(\exp(-\beta_7 t)-\exp(-X_4 t)\right),$$
$$\pi_9(t)=\beta_7 X_5^{-1}\pi_4(0)\left(\exp(-\beta_6 t)-\exp(-\beta_7 t)\right), \tag{5.83}$$
$$\begin{gathered}\pi_{10}(t)=\beta_3 X_6^{-1}\pi_2(0)\left(\exp(-\beta_2 t)-\exp(-\beta_3 t)\right)+\\ +\beta_6\left(X_5\pi_3(0)+\beta_7\pi_4(0)\right)\left(X_5X_6\right)^{-1}\cdot\\ \cdot\left(\exp(-\beta_2 t)-\exp(-\beta_6 t)\right)-\beta_6\beta_7\pi_4(0)\left(X_5X_6\right)^{-1}\cdot\\ \cdot\left(\exp(-\beta_2 t)-\exp(-\beta_7 t)\right),\end{gathered}$$
$$\pi_{11}(t)=1-\sum_{i=1}^{10}\pi_i(t),$$

де $X_1=\beta_0+\beta_2$, $X_2=\beta_1+\beta_3$, $X_4=\beta_4+\beta_6$, $X_4=\beta_5+\beta_7$, $X_5=\beta_7-\beta_6$, $X_6=\beta_3-\beta_2$. Присвоїмо кожному стану моделі ваговий коефіцієнт ω_i, $i=\overline{1,11}$. При $\omega_i=1$, $i=\overline{1,4}$; $\omega_i=0$, $i=\overline{5,11}$, тривалість перебування ІСКЗ у нефункціональному стані з причини збою у процесі сеансу ССВ $\overline{F}(t)$ опишемо виразом

$$\overline{F}(t)=\sum_{i-1}^{11}\int_0^t \pi_i(x)\,dx. \tag{5.84}$$

Враховуючи вираз (5.84), усереднений накопичений ефект від перебування системи у стані i тривалістю τ при збої сеансу ССВ опишемо виразом

$$L_i(\tau)=\int_0^\tau \omega_i\pi_i(x)\,dx,\ i\in[1,11]. \tag{5.85}$$

Комбінуючи характеристики (5.84), (5.85) формалізуємо ряд індикаторів живучості ІСКЗ:

1. Імовірність відновлення активної ВМ після збою:

$$P_{VM} = \sum_{i=5}^{11} \pi_i(t); \tag{5.86}$$

2. Імовірність відновлення сеансу ССВ після збою:

$$P_s = \pi_{11}(t); \tag{5.87}$$

3. Середня тривалість відновлення активної ВМ після збою:

$$L_{VM} = \int_0^t \sum_{i=1}^{4} L_i(x)\,dx; \tag{5.88}$$

4. Середня тривалість відновлення сеансу ССВ після збою:

$$L_S = \int_0^t \sum_{i=1}^{10} L_i(x)\,dx. \tag{5.89}$$

Проведемо дослідження адекватності методу редукції структурної моделі ФБ ІСКЗ, порівнявши результати роботи методу із результатами моделювання ФБ ІСКЗ у формалізмі марковських моделей. Нехай кількість модулів деякої ІСКЗ $N = 3$, тоді представлений на рисунку 5.14 UML–діаграмою станів повний орієнтований граф цієї системи, описаної множиною $C = \{c_1, c_2, c_3\}$, включатиме $M = 2^3 = 8$ станів, узагальнених множиною $S = \{s_j\}$, $j = \overline{1, M}$. Нехай вихідний склад множин Λ і M такий: $\Lambda = \{\lambda_1, \lambda_2 = 2\lambda_1, \lambda_3 = 3\lambda_1\}$, $\mathrm{M} = \{\mu_1 = \mu_2 = \mu_3 = 10^2\lambda_1\}$, тоді із урахуванням (5.81) при $t \to \infty$ імовірності перебування ІСКЗ у кожному із станів множини S опишемо, відповідно, виразами: $P_{s_0} = P_{s_{init}} = \mu_1\mu_2\mu_3\Pi$, $P_{s_1} = \mu_1\mu_2\lambda_3\Pi$, $P_{s_2} = \mu_1\lambda_2\mu_3\Pi$, $P_{s_3} = \lambda_1\mu_2\mu_3\Pi$, $P_{s_4} = \mu_1\lambda_2\lambda_3\Pi$, $P_{s_5} = \lambda_1\mu_2\lambda_3\Pi$, $P_{s_6} = \lambda_1\lambda_2\mu_3\Pi$, $P_{s_7} = \lambda_1\lambda_2\lambda_3\Pi$, де $\Pi = (\lambda_1 + \mu_1)^{-1}(\lambda_2 + \mu_2)^{-1}(\lambda_3 + \mu_3)^{-1}$.

Припустимо, що $\lambda_1 = 6^{-1}$, тоді, урахувавши структуру системи, представлену на рисунку 5.14, та вираз (5.82), розрахуємо ступені $R(s_j)$, $j = \overline{0,7}$: $R(s_0) = R(s_{init}) = 1$, $R(s_1) = 3/6 = 0.5$, $R(s_2) = 2/6 \approx 0.33$, $R(s_3) = 1/6 \approx 0.17$,

$R(s_4) = 2/103\,R(s_1) \approx 9.71 \cdot 10^{-3}$, $R(s_5) = 1/103\,R(s_1) \approx 4.85 \cdot 10^{-3}$,

$R(s_6) = 1/104\,R(s_2) \approx 3.21 \cdot 10^{-3}$, $R(s_7) = 1/201\,R(s_4) \approx 4.83 \cdot 10^{-5}$.

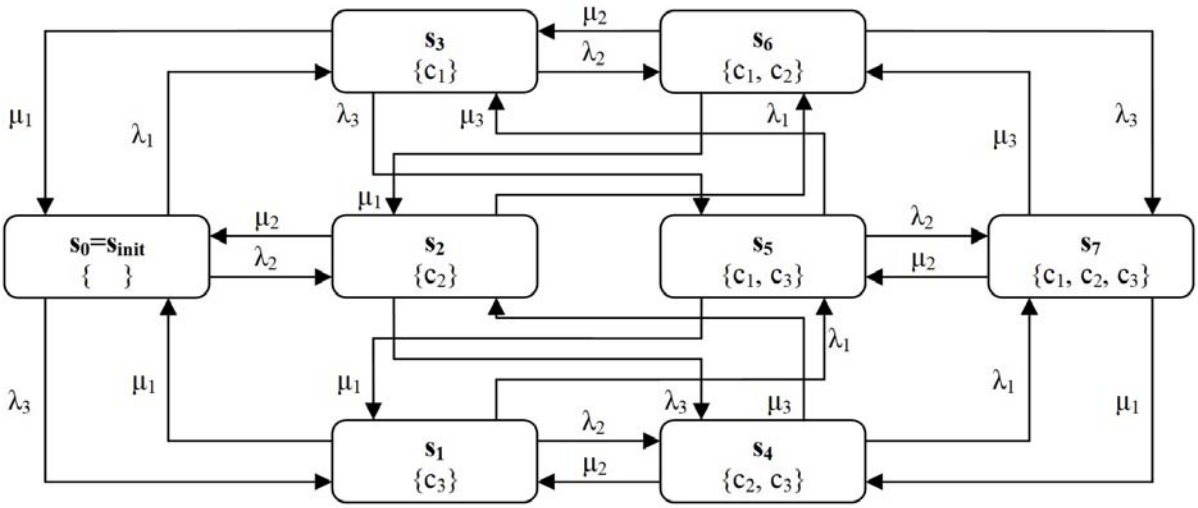


Рисунок 5.14 – UML–діаграмою станів повного орієнтованого графу моделі ФБ досліджуваної системи.

Для обраної конфігурації множин Λ і M при значенні $\lambda_1 = 6^{-1}$ розрахуємо імовірності P_{s_j}, $j = \overline{0,7}$: $P_{s_0} = P_{s_{init}} \approx 0.942$, $P_{s_1} \approx 2.82 \cdot 10^{-2}$, $P_{s_2} \approx 1.88 \cdot 10^{-2}$, $P_{s_3} \approx 9.42 \cdot 10^{-3}$, $P_{s_4} \approx 5.65 \cdot 10^{-4}$, $P_{s_5} \approx 2.82 \cdot 10^{-4}$, $P_{s_6} \approx 1.88 \cdot 10^{-4}$, $P_{s_7} \approx 5.65 \cdot 10^{-6}$. Впорядкувавши за спаданням розраховані значення імовірностей P_{s_j} і ступенів $R(s_j)$ та проаналізувавши динаміку їх спадання можна зробити висновок, що порядок розташування станів s_j за значенням згаданих характеристик співпадає, як співпадає і динаміка спадання значень цих характеристик. Отже, значення ступеню $R(s_j)$, як і імовірність P_{s_j}, є об'єктивною кількісною оцінкою імовірності переходу досліджуваної системи у стан s_j, у той час, як метод розрахунку ступеню $R(s_j)$ алгебраїчно простіший і не потребує розв'язання систем диференційних рівнянь, на відміну від методу розрахунку імовірностей P_{s_j}. Відповідно, за значеннями ступенів $R(s_j)$ можна виключати малоімовірні стани, чисельно обґрунтовуючи ризик вчинених дій.

Проведемо обчислювальний експеримент залежності індикатора моделі живучості ІСКЗ – імовірності відновлення активної ВМ після збою P_{VM} від значень імовірностей передчасного переривання активного сеансу ССВ з причини: – впливу сервісних операцій ІС на активні ВМ p_1; – недопустимих операцій всередині активних ВМ p_2; – втручання ПРД, зумовленого конфліктом правил СПБ p_3; – збою ПРД p_4. Експеримент проводитимемо для чотирьох наборів значень множини $P(p_1, p_2, p_3, p_4)$: $(0.7, 0.1, 0.1, 0.1)$, $(0.1, 0.7, 0.1, 0.1)$, $(0.1, 0.1, 0.7, 0.1)$, $(0.1, 0.1, 0.1, 0.7)$. Всі дослідження проводитимемо із ІСКЗ – ситуаційним центром Вінницької міської ради, значення параметрів β_i^{-1}, $i = 0,7$, якої визначені емпірично і представлені у множині $\mathrm{B} = \left(3, 2\beta_0, 60, 3.6 \cdot 10^3, 60, 2\beta_4, 180, 8.64 \cdot 10^4\right)$. Скориставшись моделлю (5.84) обчислимо значення індикатора P_{VM} при вищезгаданих вихідних значеннях, представивши результат на рисунку 5.15.

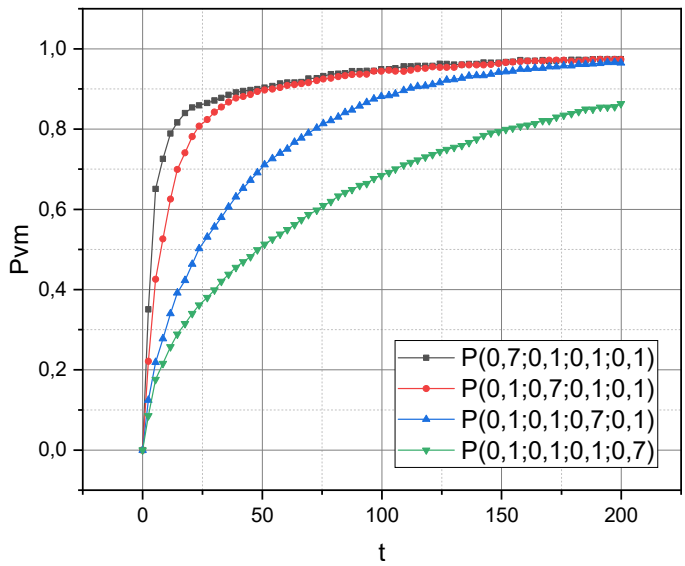


Рисунок 5.15 – Залежність імовірності відновлення активної ВМ після збою P_{VM} конфігурації множини P.

З рисунку 5.15 видно, що за вагомістю впливу на значення індикатора P_{VM} імовірнісні параметри можна впорядкувати так: p_4, p_3, p_2, p_1. Вид всіх

емпіричних залежностей характерний для експоненційного розподілу. Можна констатувати, що координація функціонування активних ВМ з боку ПРД дозволяє суттєво підвищити живучість сеансу ССВ. Втім, сама ПРД, як видно з результатів, отриманих для четвертого набору параметрів P, є критичним параметром ІСКЗ, що обумовлює доцільність заходів, спрямованих на запобігання ситуацій виникнення збоїв у цій підсистемі.

Пересвідчимося у адекватності запропонованої моделі живучості порівнявши емпіричні і модельовані значення накопичувальної середньої тривалості відновлення ВМ активного ССВ після збоїв ΣL_{VM}^{e} і ΣL_{VM}^{m}, відповідно. Значення ΣL_{VM}^{e} отримувалися в результаті контрольованого експерименту, при якому чотири типи збоїв, описаних при введенні параметрів p_1, p_2, p_3, p_4, ініціювалися у пропорцій $4:3:2:1$ за годину експлуатації активного сеансу ССВ, який загалом тривав 168 годин. Порядок ініціації збоїв кожного типу вибирався випадково. Значення ΣL_{VM}^{m} розраховувалися на основі моделі (5.84) і виразів (5.85), (5.88) для вищезгаданих значень B і $P=(0,4,0.3,0.2,0.1)$. Результати порівняння із фіксацією значень ΣL_{VM}^{e} і ΣL_{VM}^{m} по годинам наведено на рисунку 5.16.

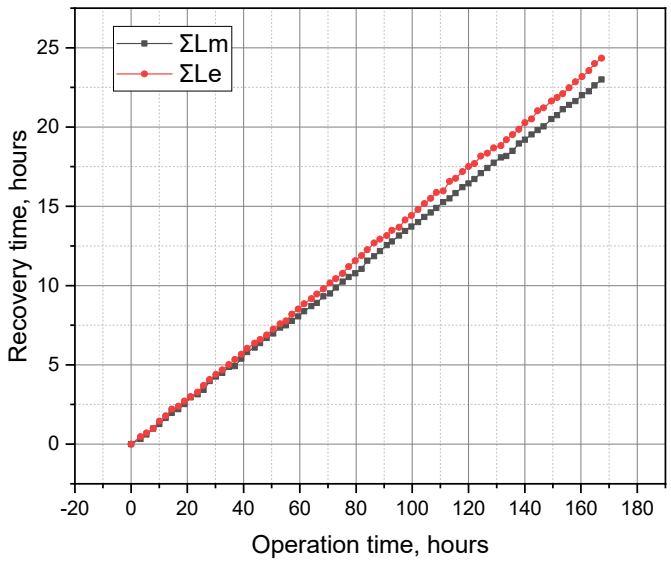


Рисунок 5.16 – Залежність між емпіричними і модельованими значеннями накопичувальної середньої тривалості відновлення ВМ активного ССВ після збоїв.

Лінійний характер залежностей, наведених на рисунку 5.16 можна пояснити тим, що проведений експеримент був контрольований, всі причини збоїв були детерміновані, отже, у СПБ і ПРД було закладено відповідні захисні механізми. Середньоквадратичне відхилення значень ΣL_{VM}^{e} і ΣL_{VM}^{m} становить приблизно 6%. Воно, здебільшого, обумовлене часовою затримкою на прийняття ПРД рішень щодо перезавантаження ВМ, у якій відбулася недопустима операція.

У підрозділі синтезовано моделі функційної безпечності і живучості ІСКЗ у формалізмі марковських моделей. У моделі ФБ досліджуваної ІСКЗ представлено структурованою множиною зв'язаних підсистем, кожна з яких характеризується інтенсивністю небезпечних збоїв і інтенсивністю відновлення ФБ. Модель дозволяє оцінити імовірність перебування ІСКЗ у кожному із множини станів, які описують 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 системи, 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 детермінованих збоїв. При синтезі моделі живучості враховано архітектуру ІСКЗ, функції ПРД, налаштування СПБ тощо. Адекватність запропонованих моделей і методу доведено результатами експериментів, у яких модельовані характеристики порівнювалися із емпіричними за значенням середньоквадратичного відхилення.

5.5 Напівмарковська модель безвідмовності інформаційної системи критичного застосування

Інформаційну систему критичного застосування можна класифікувати як комплексну розгалужену ІС, яка працює в мережевому клієнт-серверному середовищі, апаратна частина якої, в першому наближенні, включає множину обчислювальних машин класу «сервер» і «клієнт», засобів і каналів зв'язку, периферійних

засобів введення-виведення інформації тощо. Відзначимо, що для оцінювання гарантоздатності апаратної складової ІСКЗ можна застосовувати відомі апробовані коректні методи [11–29], тоді як оцінювання гарантоздатності інформаційної її складової вимагає додаткових досліджень, пов'язаних із специфікою оцінювання таких індикаторів гарантоздатності як безвідмовність, готовність, обслуговуваність, інтенсивність відмов та інтерпретацією поняття функціонального стану ІСКЗ тощо. Зокрема, така складова інформаційної гарантоздатності ІСКЗ як конфіденційність забезпечується ПРД, представленою ансамблем класифікаторів, які автентифікують суб'єкта-користувача в тому числі і за голосом. Звичайно, рішення окремих класифікаторів у ансамблі може не збігатися. Ця обставина, причини її виникнення та необхідність її врахування обумовлює віднесення ІСКЗ до класу систем із багатьма станами [189–192], що додатково ускладнює процес моделювання її інформаційної гарантоздатності.

Однозначним показником функціональної якості ІСКЗ можна вважати зафіксовану протягом встановленого періоду експлуатації системи кількість збоїв у її роботі. Існує низка моделей, в яких по різному інтерпретується цей показник при оцінюванні гарантоздатності досліджуваної системи. Виділимо, зокрема, моделі, які аналізують час між збоями в роботі системи; моделі, які аналізують кількість збоїв у роботі системи за фіксований час її експлуатації; моделі, що аналізують реакцію системи на спровоковані збої в її роботі; моделі, що аналізують реакцію системи на заздалегідь підготовлений комплекс тестових вхідних даних.

Моделі першого типу [5, 63, 64] використовують математичний апарат аналізу часових рядів для ідентифікації параметрів статистичного розподілу, який найкращим чином описує інтервали між збоями у роботі досліджуваної системи. Адекватність таких моделей істотно залежить від репрезентативності емпіричних даних про експлуатацію модельованої системи. Також при побудові цього типу моделей враховується лише факт збою без аналізу причинно-наслідкових зв'язків його виникнення, що у випадку моделювання систем із самонавчанням стає додатковим джерелом похибок.

Моделі другого типу [66, 67] аналізують дані про кількість збоїв на визначеному часовому інтервалі експлуатації досліджуваної системи. При цьому припускається, що кількість збоїв у часі описується певним стохастичним процесом із неперервною або дискретною функцією інтенсивності, оцінюваною емпірично. Більшість моделей цього типу базуються на розподілі Пуассона і відрізняються, здебільшого, способом обчислення параметрів цього розподілу. Недоліки моделей цього типу аналогічні сформульованим для моделей першого типу.

В моделях третього типу [65–67] за допомогою методів комбінаторики та максимальної правдоподібності оцінюється як інформація про кількість зафіксованих у процесі експлуатації досліджуваної системи збоїв із невідомими джерелами походження, так і інформація про кількість збоїв, спровокованих відомою послідовністю дій, захист від яких повинен був бути закладений у СПБ. Ці моделі дають в тому числі і причино-наслідкову оцінку збоїв у процесі функціонування досліджуваної системи. Цей підхід до моделювання дає системну оцінку гарантоздатності, але частина експериментів, результати яких враховуються, все ж залишаються неконтрольованими, що знижує достовірність оцінювання.

Моделі четвертого типу [66, 67] синтезують на основі результатів контрольованих експериментів, коли збої у роботі системи виникають, здебільшого, з причини виходу значень параметрів-атрибутів за межі, встановлені на етапі проектування досліджуваної системи. Враховуючи, що причини збоїв зазвичай взаємопов’язані, моделі цього типу будують на основі апарату ланцюгів Маркова [189–192] що дозволяє врахувати мультипоточність у роботі досліджуваної системи і неоднорідність процесу відновлення її функціонального стану після збоїв. Поведінку реальних комплексних ІС якісніше описують напівмарковські моделі, адже процес відновлення функціонального стану системи може описуватися не тільки експоненційною функцією розподілу. Структурні особливості досліджуваної системи при цьому підході до моделювання можна врахувати введенням графу потоку управління, в якому процес передавання управління між структурними елементами системи описується марковським ланцюгом або кількома – для систем із багатьма станами. Згадані моделі гарантоздатності відносяться до парамет-

ричного класу, тоді як існують і непараметричні моделі [66, 67], побудовані, наприклад, на основі штучних нейромереж [70], які дозволяють апроксимувати довільні нелінійні неперервні функції із необхідною точністю. Втім, при синтезі таких моделей не враховуються структурні особливості досліджуваної системи, а якість отримуваних моделей значно залежить від типу, топології, налаштувань і організації процесу навчання використовуваних нейромереж.

Враховуючи сказане, оптимальним з позиції врахування архітектурних особливостей ІСКЗ та специфіки перебігу процесу її функціонування виявляється синтез відповідного математичного апарату для оцінювання гарантоздатності в парадигмі напівмарковських моделей із багатьма станами. Динаміку функціонування такої системи в імовірнісному просторі (Ω, F, P) [289] можна описати послідовністю станів, узагальнених множиною $E = \{1, 2, \ldots, N\}$, де стан із номером «1» характеризує ситуацію, коли ІСКЗ показує найменшу продуктивність роботи, а стан «N», відповідно, виступає антагоністом стану «1». Описуючи ІСКЗ напівмарковською моделлю, враховуватимемо, що тривалість перебування системи в певному стані визначається видом розподілу, що його характеризує. Ця обставина обумовлює доцільність дослідження впливу виду розподілу на динаміку створюваної напівмарковської моделі, а представлення досліджуваної системи керованим напівмарковським процесом дозволяє ідентифікувати значення керованих параметрів, при яких інтегральна оцінка її гарантоздатності буде максимальною.

Нехай простір станів ІСКЗ скінченний і описується множиною $E = \{1, \ldots, N\}$, $N < \infty$, а поведінка системи у часі описується стохастичним процесом $Z = (Z_t)_{t \in \Re_+}$. Опишемо множиною $S = (S_n)_{n \in \aleph}$ моменти часу, коли ІСКЗ змінює свій стан із збереженням функціональності; множиною $J = (J_n)_{n \in \aleph}$ – відповідні переходам S номери кінцевих станів, у які переходила система; множиною $X = (X_n)_{n \in \aleph} = (S_n - S_{n-1})_{n \in \aleph}$ – тривалість перебування ІСКЗ у $J = (J_n)_{n \in \aleph}$ станах (для вихідного стану $X_0 = S_0 = 0$). Використовуючи ці позначення життєвий цикл ІСКЗ можна описати відновлюваним марковським процесом $(J, S) = (J_n, S_n)_{n \in \aleph}$,

для всіх елементів якого виконується рівність $\mathrm{P}\left(J_{n+1}=j, S_{n+1}-S_n \le t \middle| J_0,\ldots,J_n; S_1,\ldots,S_n\right)=$

$=\mathrm{P}\left(J_{n+1}=j, S_{n+1}-S_n \le t \middle| J_n\right)$, де $j \in E$, $t \in \Re_+$. Для оцінювання динаміки ІСКЗ, описуваної (J,S), на часовому інтервалі $(0,t]$ використаємо модель напівмарковського процесу $Z=(Z_t)_{t\in\Re_+}$, для якого $Z_t = J_{N(t)} \Leftrightarrow J_n = Z_{S_n}$, де $t \in \Re_+$, а результат підрахунку кількості переходів ІСКЗ із стану в стан на часовому інтервалі $(0,t]$ отримаємо за правилом

$$N(t)=\max\{n \in N | S_n \le t\}. \tag{5.90}$$

Вважатимемо ВМП і НМП регулярними, тобто $\mathrm{P}_i(N(t)<\infty)=1 \forall (t>0) \wedge (i \in E)$ і $\hat{\alpha}_{ij}(L_l,M)=N_{i,0}^{(L_l)}L_l^{-1}$, а їх вбудовані марковські ланцюги – нерозкладними і позитивно рекурентними. Загалом, напівмарковську модель ІСКЗ характеризуватимемо вихідним розподілом $\alpha=(\alpha_1,\ldots,\alpha_j,\ldots,\alpha_N), \alpha_j=\mathrm{P}(J_0=j), j \in E$ і напівмарковським ядром $q_{ij}(t)=P(J_n=j, X_n=t | J_{n-1}=i)$, кумулятивна форма якого описується виразом $Q_{ij}(t)=P(J_n=j, X_n \le t | J_{n-1}=i)=\sum_{l=0}^{t} q_{ij}(l)$. Вбудовані марковські ланцюги $(J_n)_{n\in\aleph}$ характеризуватимемо перехідними імовірностями $p_{ij}=\mathrm{P}(J_n=j | J_{n-1}=i)=\lim_{t\to\infty} Q_{ij}(t)$ і умовними функціями розподілу середньої тривалості стану

$$W_{ij}(t)=\mathrm{P}(S_n-S_{n-1} \le t | J_{n-1}=i, J_{n-1}=j)=\mathrm{P}(X_n \le t | J_{n-1}=i, J_{n-1}=j),$$

відношення між якими опишемо виразом $Q_{ij}(t)=p_{ij}W_{ij}(t)$. Умовний розподіл для X_n опишемо виразом

$$f_{ij}(t)=P(X_n=t | J_{n-1}=i, J_n=j)=\begin{cases} q_{ij}(t)(p_{ij})^{-1}, if\ p_{ij} \ne 0, \\ 1_{\{t=\infty\}}, if\ p_{ij}=0, \end{cases},$$

кумулятивною формою якого буде вираз $F_{ij}(t)=P(X_n \le t | J_{n-1}=i, J_n=j)$. Розподіл значення часу перебування системи у стані i опишемо виразом $h_i(t)=P(X_n=t | J_{n-1}=i)=\sum_{j\in E} q_{ij}(t)$, кумулятивною формою якого буде вираз

$H_i(t) = P(X_n \le t | J_{n-1} = i) = \sum_{l=0}^{t} h_i(l)$, а середній час перебування системи у стані i опишемо виразом $m_i = E(S_1 | J_0 = i) = \sum_{t \ge 0} (1 - H_i(t))$. Передбачається, що час перебування ІСКЗ у стані i відмінний від нуля, тобто для будь якого стану j виконується рівність $f_{ij}(0) = q_{ij}(0) = h_i(0) = 0$. Введемо параметр T_{ij} для опису тривалості перебування ІСКЗ у стані i, який завершується рішенням щодо переходу системи в стан j. Для оцінювання T_{ij} введемо неперервну кумулятивну функцію розподілу $F_{ij}(t, \theta_{ij})$ із щільністю $f_{ij}(t, \theta_{ij})$, де θ_{ij} – залучений у базовий розподіл m-вимірний характеристичний вектор-параметр, який описує внутрішні налаштування ІСКЗ. Вибір стану j в який перейде ІСКЗ зі стану i відбувається за правилом $j = \arg\min_{l \in E}(T_{il})$, де l – множина індексів станів, у які ІСКЗ може перейти зі стану i.

Узагальнимо сказане вище представивши ядро НМП як

$$Q_{ij}(t) = \mathrm{P}\left(\min_l T_{il} \le t \,\&\, j = \arg\min_{l \in E}(T_{il}) \middle| J_{n-1} = i \right) =$$

$$= \mathrm{P}\left(\min_l T_{il} \le t, T_{ij} \le T_{il}, \forall l \middle| J_{n-1} = i \right) =$$

$$= \mathrm{P}\left(\min_l T_{il} \le t \middle| J_{n-1} = i, J_n = j \right) \mathrm{P}(T_{ij} \le T_{il}, \forall l | J_{n-1} = i) = p_{ij} W_i(t),$$

де $p_{ij} = \mathrm{P}(J_n = j | J_{n-1} = i) = \mathrm{P}(T_{ij} \le T_{il}, \forall l | J_{n-1} = i)$, а для опису тривалості перебування ІСКЗ у стані i використаємо незалежну від j і неперервну КФР виду

$$W_i(t) = W_{ij}(t) = \mathrm{P}(S_n - S_{n-1} \le t | J_{n-1} = i, J_n = j) =$$

$$= \mathrm{P}\left(\min_l T_{il} \le t \middle| J_{n-1} = i, J_n = j \right) = \mathrm{P}\left(\min_l T_{il} \le t \middle| J_{n-1} = i \right).$$

Узагальнивши $Q_{ij}(t)$ для всіх j отримаємо рівність $\sum_j Q_{ij}(t) = W_i(t)$.

Отже, динаміку модельованої НМП ІСКЗ можна описати параметрами p_{ij}, $W_i(t, \theta)$ і $Q_{ij}(t, \theta)$, значення яких залежать від часу t і значень характеристичного вектор-параметра ІСКЗ θ. Формалізуємо оцінки цих характеристик для можливих

видів розподілів $F_{ij}(t,\theta_{ij})$, $i,j=1,\ldots,N$, які є функціонально близькими, але відрізняються параметрично, тобто, типовий представник такого класу функцій розподілу задовольняє рівність

$$F_{ij}(t,\theta_{ij})=F(t,\alpha)=1-(1-F(t,1))^{\alpha}, \tag{5.91}$$

де α – узагальнений параметр функції розподілу. До розподілів, які задовольняють рівність (5.91), відносять [289] дискретний геометричний розподіл і низку неперервних розподілів, зокрема, експоненційний розподіл, розподіл Вейбула, розподіл Релея, зрізаний експоненційний розподіл Ерланга, розподіл Парето тощо.

Перевизначимо із урахуванням (5.91) основні функціональні компоненти НМП, який описує функціонування ІСКЗ, зокрема, функцію розподілу $F(t)=F(t,1)$, її щільність $f(t)=f(t,1)$, ядро НМП

$$Q_{ij}(t,\alpha_{ik})=Q_{ij}(t)=\alpha_{ij}\left(1-(1-F(t))^{\sum_{k\in E}\alpha_{ik}}\right)\left(\sum_{k\in E}\alpha^{ik}\right)^{-1}, \tag{5.92}$$

$k=1,\ldots,N$, матрицю імовірностей переходів між станами

$$p_{ij}=\alpha_{ij}\left(\sum_{k\in E}\alpha_{ik}\right)^{-1} \tag{5.93}$$

і КФР

$$W_i(t)=1-(1-F(t))^{\sum_{j=1}^{N}\alpha_{ij}}, \tag{5.94}$$

щільність якої визначатимемо за виразом

$$f_i(t)=f(t)\left(\sum_{j=1}^{N}\alpha_{ij}(1-F(t))^{\sum_{j=1}^{N}\alpha_{ij}}\right)(1-F(t))^{-1}.$$

Очікуване значення мінімуму функції розподілу $F(t)$, що характеризує динаміку НМП, який описує функціонування ІСКЗ, опишемо виразом

$$\mathrm{E}(X_{(1)})=\left(\sum_{j=1}^{N}\alpha_{ij}\right)\int_0^{\infty}t(1-F(t))^{\sum_{j=1}^{N}\alpha_{ij}-1}f(t)dt.$$

Враховуючи, що стани НМП, який описує функціонування ІСКЗ, можуть характеризуватися різними розподілами формалізуємо процес оцінювання параметрів α_{ij} для довільної пари станів $i,j=1,\ldots,N$ в залежності від виду розподілу

випадкових величин. Обчислимо у вигляді функції $N_i(t)$ кількість випадків, коли ІСКЗ за час, менший від $t \in \Re_+$, переходила у стан i:

$$N_i(t) = \sum_{n=0}^{N(t)-1} 1_{\{J_n = i\}} = \sum_{n=0}^{\infty} 1_{\{J_n = i, S_{n+1} \le t\}}, \tag{5.95}$$

де $1_{\{J_n = i, S_{n+1} \le t\}} = \begin{cases} 1, \, if \, (J_n = i) \wedge (S_{n+1} \le t), \\ 0, \, else \end{cases}$.

Обчислимо у вигляді функції $N_{ij}(t)$ кількість випадків, коли ІСКЗ за час, менший від $t \in \Re_+$, переходила зі стану i у стан j:

$$N_{ij}(t) = \sum_{n=0}^{N(t)} 1_{\{J_{n-1} = i, J_n = j\}} = \sum_{n=1}^{\infty} 1_{\{J_{n-1} = i, J_n = j, S_n \le t\}}, \tag{5.96}$$

де $1_{\{J_{n-1} = i, J_n = j, S_n \le t\}} = \begin{cases} 1, if \, (J_{n-1} = i) \wedge (J_n = j) \wedge (S_n \le t), \\ 0, else \end{cases}$.

Обчислимо у вигляді функції $N_{ij}(t, M)$ кількість випадків, коли ІСКЗ за час, менший від $t = M$, переходила зі стану i в стан j за умови, що тривалість стану i дорівнює k, $1 \le k \le M$:

$$N_{ij}(t, M) = \sum_{n=0}^{N(t)} 1_{\{J_{n-1} = i, J_n = j, X_n = k\}}. \tag{5.97}$$

У виразах (5.95)–(5.97) $N(t)$ – формалізована виразом (5.90) функція, яка описує процес підрахунку кількості переходів системи із стану в стан. Використовуючи функції $N_i(M)$, $N_{ij}(M)$ і $N_{ij}(t, M)$ обчислимо емпіричні оцінки НМП, який описує життєвий цикл ІСКЗ:

$$\hat{p}_{ij}(M) = N_{ij}(M)(N_i(M))^{-1}, \tag{5.98}$$

$$\hat{F}_{ij}(t, M) = N_{ij}(t, M)(N_{ij}(M))^{-1}, \tag{5.99}$$

$$\hat{q}_{ij}(t, M) = N_{ij}(t, M)(N_i(M))^{-1}. \tag{5.100}$$

Відзначимо, що оцінки (5.98)–(5.100) мають асимптотичний характер і за значенням наближаються до оцінок максимуму правдоподібності, описуваних множиною функцій правдоподібності L. Перевірку коректності цього твердження буде проведено далі.

Сформулюємо вираз для оцінювання правдоподібності траєкторії перебігу станів ІСКЗ $\{j_0, x_1, j_1, x_2, \ldots, j_{N(M)}\}$ на інтервалі спостереження $t = M$:

$$L = \alpha_{j_0} p_{j_0 j_1} f_{j_0}(x_1) \ldots p_{j_{N(M)-1}, j_{N(M)}} f_{j_{N(M)-1}}(x_{N(M)}) =$$

$$= \alpha_{j_0} \left(\prod_{i,j \in E} p_{ij}^{N_{ij}(M)} \right) \left(\prod_{i \in E} \prod_{k=1}^{N_i(M)} f_i\left(x_i^{(1,k)}\right) \right), \tag{5.101}$$

де $x_i^{(1,k)}$ – тривалість перебування ІСКЗ у стані i, в який система потрапила k-й раз за час спостереження $t = M$, $k = 1, \ldots, N_i(M)$.

На основі (5.101) отримаємо вираз для оцінювання максимальної правдоподібності перебігу станів ІСКЗ, якщо імовірні значення характеристик НМП (5.92)–(5.95) описуються законами розподілів, які задовольняють умову (5.91):

$$L = \alpha_{j_0} \left(\prod_{i,j \in E} \alpha_{ij}^{N_{ij}(M)} \right) \prod_{i,k} \left(\left(1 - F\left(x_i^{(1,k)}\right)\right)^{\sum_{j \in E} \alpha_{ij}} \left(1 - F\left(x_i^{(1,k)}\right)\right)^{-1} f\left(x_i^{(1,k)}\right) \right),$$

Взявши похідну від логарифмічної функції правдоподібності по α_{ij}, $i, j \in E$, отримаємо оцінки α_{ij} виду:

$$\hat{\alpha}_{ij}(M) = -N_{ij}(M) \left(\sum_{k=1}^{N_i(M)} \log\left(1 - F\left(X_i^{(1,k)}\right)\right) \right)^{-1}. \tag{5.102}$$

Отримаємо вираз для функції правдоподібності якщо час спостереження $t = M$ цензурований. В такому випадку перебіг станів ІСКЗ опишемо послідовністю $\{j_0, x_1, j_1, x_2, \ldots, j_{N(M)}, u_M\}$, де $u_M = M - S_{N(M)}$ – тривалість останнього стану системи за цензурований час спостереження $t = M$. На основі наведеного вище, вираз для обчислення функції правдоподібності набуде вигляду

$$L = \alpha_{j_0} p_{j_0 j_1} f_{j_0}(x_1) \ldots p_{j_{N(M)-1}, j_{N(M)}} f_{j_{N(M)-1}}(x_{N(M)}) \times$$

$$\times \mathrm{P}\left(X_{j_{N(M)}} > u_M\right) = \alpha_{j_0} \left(\prod_{i,j \in E} p_{ij}^{N_{ij}(M)} \right) \times \tag{5.103}$$

$$\times \left(\prod_{i \in E} \prod_{k=1}^{N_i(M)} f_i\left(x_i^{(1,k)}\right) \right) \times \left(1 - W_{j_{N(M)}}(u_M)\right).$$

У випадку розподілу параметрів НМП згідно із (5.91) функцію правдоподібності (5.103) опишемо виразом

$$L=\alpha_{j_0}\left(\prod_{i,j\in E}\alpha_{ij}^{N_{ij}(M)}\right)\prod_{i,k}\left(\left(1-F\left(x_i^{(1,k)}\right)\right)^{\sum_{j\in E}\alpha_{ij}}\times\right.$$

$$\left.\times\left(1-F\left(x_i^{(1,k)}\right)\right)^{-1}f\left(x_i^{(1,k)}\right)\right)\times\left(1-F\left(u_M\right)\right)^{\sum_{j\in E}\alpha_{ij}},$$

взявши похідну від якого по α_{ij}, $i,j\in E$, отримаємо оцінки α_{ij} виду:

$$\hat{\alpha}_{ij}(M)=-N_{ij}(M)\left(B_i(M)+C(M)\right)^{-1}=$$

$$=-N_{ij}(M)\left(\sum_{k=1}^{N_i(M)}\log\left(1-F\left(X_i^{(1,k)}\right)+\log\left(1-F\left(U_M\right)\right)\right)\right)^{-1}. \tag{5.104}$$

За аналогією із (5.101)–(5.104) отримаємо вирази для визначення функцій правдоподібності в яких враховуватимуться L_l траєкторій розвитку НМП, що описує функціонування ІСКЗ. За аналогією із (5.101), функцію правдоподібності для нецензурованого процесу виду $\left\{j_0^{(l)},x_1^{(l)},j_1^{(l)},x_2^{(l)},\ldots,j_{N^l(M)}^{(l)}\right\}$, який може розвиватися за $l=1,\ldots,L_l$ траєкторіями, опишемо виразом

$$L=\prod_{l=1}^{L_l}\alpha_{j_0}^{(l)}p_{j_0^{(l)}j_1^{(l)}}f_{j_0^{(l)}}\left(x_1^{(l)}\right)\ldots f_{j_{N^l(M)-1}^{(l)}}\left(x_{N^l(M)}^{(l)}\right)=$$

$$=\left(\prod_{i\in E}\alpha_i^{N_{i,0}^{(L_l)}}\right)\left(\prod_{i,j\in E}p_{ij}^{\sum_{l=1}^{L_l}N_{ij}^{(l)}(M)}\right)\left(\prod_{l=1}^{L_l}\prod_{i\in E}\prod_{k=1}^{N_i^{(l)}(M)}f_i\left(x_i^{(l,k)}\right)\right), \tag{5.105}$$

де $N_i^{(l)}(M)$ – кількість випадків, коли система переходила в стан i для l-ї траєкторії за час спостереження $t=M$, $N_{ij}^{(l)}(M)$ – кількість випадків, коли система переходила зі стану i в стан j для l-ї траєкторії за час спостереження $t=M$, $x_i^{(l,k)}$ – тривалість перебування ІСКЗ у стані i під час k-го переходу в цей стан для l-ї траєкторії, $l=1,\ldots,L_l$, $k=1,\ldots,N_i^{(l)}(M)$, $N_{i,0}^{(L_l)}=\sum_{l=1}^{L_l}1_{\left\{J_0^{(l)}=i\right\}}$, $N_{ij}(L_l,M)=\sum_{l=1}^{L_l}N_{ij}^{(l)}(M)$. При $L_l=1$ вираз (5.105) збігається із виразом (5.101).

При врахуванні умови (5.91) функція правдоподібності (5.105) набуває вигляду

$$L=\prod_{i\in E}\alpha_i^{N_{i,0}^{(L_l)}}\left(\prod_{l=1}^{L_l}\prod_{i,j\in E}\alpha_{ij}^{N_{ij}^{(l)}(M)}\right)\times$$

$$\times\prod_{l,i,k}\left(\left(1-F\left(x_i^{(l,k)}\right)\right)^{\sum_{j\in E}\alpha_{ij}}\left(1-F\left(x_i^{(l,k)}\right)\right)^{-1}f\left(x_i^{(l,k)}\right)\right),$$

врахувавши яку отримаємо вираз для оцінювання параметрів α_{ij} аналізованого НМП відповідного типу:

$$\hat{\alpha}_{ij}\left(L_l,M\right)=-\left(\sum_{l=1}^{L_l}\sum_{k=1}^{N_i^{(l)}(M)}\log\left(1-F\left(X_i^{(l,k)}\right)\right)\right)^{-1}N_{ij}\left(L_l,M\right), \tag{5.106}$$

взявши похідну від якого і врахувавши, що $\sum_{i\in E}\alpha_i$, отримаємо вираз для максимальної оцінки правдоподібності вихідного розподілу

$$\hat{\alpha}_{ij}\left(L_l,M\right)=N_{i,0}^{(L_l)}L_l^{-1}. \tag{5.107}$$

За аналогією з (5.103) функцію правдоподібності для цензурованого процесу виду $\left\{j_0^{(l)},x_1^{(l)},j_1^{(l)},x_2^{(l)},\ldots,j_{N^l(M)}^{(l)},u_M^{(l)}\right\}$, який може розвиватися за $l=1,\ldots,L_l$ траєкторіями, опишемо виразом

$$L=\left(\prod_{i\in E}\alpha_i^{N_{i,0}^{(L_l)}}\right)\left(\prod_{i,j\in E}p_{ij}^{\sum_{l=1}^{L_l}N_{ij}^{(l)}(M)}\right)\times$$
$$\times\left(\prod_{l=1}^{L_l}\prod_{i\in E}\prod_{k=1}^{N_i^{(l)}(M)}f_i\left(x_i^{(l,k)}\right)\right)\left(\prod_{i\in E}\prod_{k=1}^{N_{i,M}(L_l)}\left(1-W_i\left(u_i^{(k)}\right)\right)\right), \tag{5.108}$$

де $u_M^{(l)}=M-S_{N^l(M)}$ – цензурований час спостереження l-ї траєкторії життєвого циклу ІСКЗ; $u_i^{(k)}$ – цензурована тривалість перебування системи в стані i впродовж k-го переходу в цей стан, $k=1,\ldots,N_{i,M}\left(L_l\right)$; $N_{i,M}\left(L_l\right)=\sum_{l=1}^{L_l}1_{\left\{J_{N^l(M)}^{(l)}=i\right\}}$ – кількість випадків, коли система переходила в стан i, який був останнім станом для цензурованого часу спостереження $t=M$ для всіх $L_l=\sum_{i\in E}N_{i,M}\left(L_l\right)$ траєкторій.

Якщо в момент часу M ІСКЗ, життєвий цикл якої розвивається за l-ю траєкторією, здійснює перехід між станами, то значення відповідного параметра $u_M^{(l)} = 0$, а його внесок у значення функції правдоподібності дорівнюватиме одиниці. Отже, якщо цензурування не впроваджується, то вираз (5.108) збігається із (5.105).

При врахуванні умови (5.91) функція правдоподібності (5.108) набуде вигляду

$$L = \left(\prod_{i \in E} \alpha_i^{N_{i,0}^{(L_l)}} \right) \left(\prod_{l=1}^{L_l} \prod_{i,j \in E} \alpha_{ij}^{N_{ij}^{(l)}(M)} \right) \left(\prod_{i \in E} \prod_{k=1}^{N_{i,M}(L_l)} \left(1 - F\left(u_i^{(k)}\right)\right)^{\sum_{j \in E} \alpha_{ij}} \right) \times$$
$$\times \prod_{i,i,k} \left(\left(f\left(x_i^{(l,k)}\right) \left(1 - F\left(x_i^{(l,k)}\right)^{-1}\right) \right) \left(1 - F\left(x_i^{(l,k)}\right)\right)^{\sum_{j=E} \alpha_{ij}} \right). \tag{5.109}$$

На основі (5.109) отримаємо вирази для оцінювання параметрів α_{ij} і α_i для НМП із L_l траєкторіями розвитку:

$$\hat{\alpha}_{ij}(L_l, M) = -N_{ij}(L_l, M)\left(B_i(L_l, M) + C(L_l, M)\right)^{-1} =$$
$$= -N_{ij}(L_l, M) \left(\sum_{l=1}^{L_l} \sum_{k=1}^{N_i^{(l)}(M)} \log\left(1 - F\left(X_i^{(l,k)}\right)\right) + \sum_{k=1}^{N_{i,M}(M)} \log\left(1 - F\left(U_i^{(k)}\right)\right) \right)^{-1}, \tag{5.110}$$

$$\hat{\alpha}_i(L_l, M) = N_{i,0}^{(L_l)} L_l^{-1}. \tag{5.111}$$

Користуючись викладеним вище, в залежності від інформації про життєвий цикл ІСКЗ для оцінювання α_{ij} обираємо однин із виразів (5.102), (5.104) або (5.110), здійснюючи згодом оцінювання таких визначальних характеристик НМП як p_{ij}, W_i, Q_{ij} використовуючи вирази

$$\hat{p}_{ij}(M) = \hat{\alpha}_{ij}(L_l, M) \left(\sum_{l \in E} \hat{\alpha}_{il}(L_l, M) \right)^{-1} = N_{ij}(M)\left(N_i(M)\right)^{-1}, \tag{5.112}$$

$$\hat{W}_i(t, M) = 1 - \left(1 - F(t)\right)^{\sum_{j \in E} \hat{\alpha}_{ij}(L_l, M)}, \tag{5.113}$$

$$\hat{Q}_{ij}(t, M) = \hat{\alpha}_{ij}(L_l, M) \left(1 - \left(1 - F(t)\right)^{\sum_{k \in E} \hat{\alpha}_{ik}(L_l, M)}\right) \left(\sum_{k \in E} \hat{\alpha}_{ik}(L_l, M) \right)^{-1}, \tag{5.114}$$

відповідно. Скористаємося виразами (5.102), (5.104), (5.110) і формалізуємо оцінки значень $\alpha_{ij}(L_l, M)$ для розподілів, які задовольняють правило (5.91). Для

розподілу Вейбула маємо $F(x,\alpha_{ij})=1-e^{-\alpha_{ij}x^c}$, $F(x,1)=1-e^{-x^c}$, $f(x,1)=cx^{c-1}e^{-x^c}$, де c – параметр розподілу. Для цього розподілу оцінка значень $\alpha_{ij}(L_l,M)$ для нецензурованого процесу набуде вигляду

$$\hat{\alpha}_{ij}(L_l,M)=N_{ij}(L_l,M)\left(\sum_{l=1}^{L_l}\sum_{k=1}^{N_i^{(l)}(M)}\left(X_i^{(l,k)}\right)^c\right)^{-1}, \tag{5.115}$$

а для цензурованого:

$$\hat{\alpha}_{ij}(L_l,M)=N_{ij}(L_l,M)\left(\sum_{l=1}^{L_l}\sum_{k=1}^{N_i^{(l)}(M)}\left(X_i^{(l,k)}\right)^c+\sum_{k=1}^{N_{i,M}(L_l)}\left(U_i^{(k)}\right)^c\right)^{-1}. \tag{5.116}$$

Максимум функції правдоподібності розподілу Вейбула, залежний від значення параметра c, отримуємо в результаті розв’язання рівняння

$$\frac{\partial \log L}{\partial c}=\sum_{l,i,j}\left(N_{ij}^{(l)}(M)\left(x_i^{(l,k)}\right)^{-1}\right)\times$$

$$\times m_i=E\left(S_1\middle|J_0=i\right)=\int_0^\infty\left(1-W_i(t)\right)dt=\int_0^\infty\left(1-F(t)\right)\sum_{j=1}^{N}\alpha_{ij}\,dt.$$

Оцінки значень $\alpha_{ij}(L_l,M)$ для експоненційного розподілу і розподілу Релея знаходяться як частинний випадок розподілу Вейбула, а от для розподілу Парето матимемо $F(x,\alpha_{ij})=1-\left(cx^{-1}\right)^{\alpha_{ij}}$, $F(x,1)=1-cx^{-1}$, $f(x,1)=cx^{-2}$. Для розподілу Парето оцінка значень $\alpha_{ij}(L_l,M)$ для нецензурованого процесу розраховуватиметься за виразом

$$\hat{\alpha}_{ij}(L_l,M)=N_{ij}(L_l,M)\left(\sum_{l=1}^{L_l}\sum_{k=1}^{N_i^{(l)}(M)}\log\left(cX_i^{-(l,k)}\right)\right)^{-1}, \tag{5.117}$$

а для цензурованого:

$$\hat{\alpha}_{ij}(L_l,M)=N_{ij}(L_l,M)\times$$

$$\times\left(\sum_{l=1}^{L_l}\sum_{k=1}^{N_i^{(l)}(M)}\log\left(cX_i^{-(l,k)}\right)+\sum_{k=1}^{N_{i,M}(L_l)}\log\left(cU_i^{-(k)}\right)\right)^{-1}. \tag{5.118}$$

Максимум функції правдоподібності розподілу Парето, залежний від значення параметра c, отримуємо в результаті розв'язання задачі оптимізації

$$\hat{c} = \min_{i,l,k} X_i^{(l,k)}.$$

Функція марковського відновлення $\Psi_{ij}(t)$ [189–192], $i, j \in E$, $t \geq 0$, повертає очікувану кількість $N_j(t)$ переходів системи в стан j за час спостережень не більший від t за умови, що вихідним станом системи в момент часу $t = 0$ був стан i. В контексті наведених вище аналітичних виразів формалізуємо функцію $\Psi_{ij}(t)$ виразом

$$\Psi_{ij}(t) = E_i\left[N_j(t)\right] = \sum_{n=1}^{\infty} Q_{ij}^{(n)}(t) = \sum_{n=1}^{\infty} \sum_{k \in E} \int_0^t Q_{ik}(s) Q_{kj}^{(n-1)}(t-s)ds, \tag{5.119}$$

перетворивши який із урахуванням (5.92) отримаємо

$$\Psi_{ij}(t) = \sum_{n=1}^{\infty} \sum_{k \in E} \int_0^t \left(\alpha_{ik} \left(1 - (1 - F(s))_{k \in E}^{\sum \alpha_{ik}}\right) \left(\sum_{k \in E} \alpha_{ik} \right)^{-1} \right) Q_{kj}^{(n-1)}(t-s)ds,$$

де $Q_{ij}^{(n)}$ – згортка n-го порядку Q самої з собою, отримувана за правилом [189]

$$Q_{ij}^{(n)}(t) = \begin{cases} \sum_{k \in E} \int_0^t Q_{ik}(s) Q_{kj}^{(n-1)}(t-s)ds, & n \geq 2, \\ Q_{ij}(t), & n = 1, \\ \delta_{ij} 1\{t \geq 0\}, & n = 0. \end{cases}$$

Згідно із [189–192], вираз для визначення напівмарковської перехідної матриці набуде вигляду

$$P_{ij}(t) = P(Z_t = j | Z_0 = i) = I_N - diag\left(\sum_j Q_{ij}(t); i \in E \right) + (Q * P)(t),$$

де I_N – матриця ідентичності розмірністю $N \times N$, $(Q * P)(t) = (Q * P)_{ij}(t) = \sum_{k \in E} \int_0^t Q_{ik}(s) P_{kj}(t-s)ds$ – результат згортки $P(t) = P_{ij}(t)$ і $Q(t) = Q_{ij}(t)$.

Якщо визначено діагональну матрицю вигляду

$$W(t) = diag(W_i(t); i \in E) = diag\left(\sum_j Q_{ij}(t); i \in E\right) = diag(Q \cdot 1_N)(t),$$

(i,i)-й елемент якої еквівалентний $W_i(t) = \sum_{j \in E} Q_{ij}(t)$, а $1_N = \underbrace{(1,\ldots,1)}_{N}^T$ є операцією транспонування відповідного вектора, то значення $P_{ij}(t)$ знайдемо в результаті розв'язання рівняння

$$P(t) = \left((I_N - Q)^{(-1)} * (I_N - W)\right)(t) = (\Psi * (I_N - W))(t). \quad (5.120)$$

Оцінки функцій $P_{ij}(t)$ і $\Psi_{ij}(t)$ опишемо, відповідно, виразами

$$\hat{P}_{ij}(t,M) = \left(\hat{\Psi}_{ij} * \left(1 - \sum_{k \in E} \hat{Q}_{jk}\right)\right)(t,M), \quad (5.121)$$

$$\hat{\Psi}_{ij}(t,M) = \sum_{n=1}^{\infty} \hat{Q}_{ij}^{(n)}(t,M) = \sum_{n=1}^{\infty} \sum_{k \in E} \int_0^t \hat{Q}_{ik}(s,M) \hat{Q}_{kj}^{(n-1)}(t-s,M) ds, \quad (5.122)$$

у яких $\hat{Q}_{ij}(t,M)$ визначаються на основі оцінок α_{ij}, які, в залежності від обраного виду розподілу, описуються одним із рівнянь (5.102), (5.104), (5.106), (5.110), відповідно.

Узагальнимо наведену вище інформацію, отримавши вирази для оцінювання гарантоздатності ІСКЗ, модельованої НМП, із урахуванням специфічних особливостей такої моделі. В якості атрибутів гарантоздатності використаємо безвідмовність, готовність, обслуговуваність, інтенсивність відмов і наробок на відмову системи тощо.

Припустимо, що простір станів ІСКЗ E складається з двох підпросторів U і D таких, що $E = U \cup D$, $E = U \cap D = \phi$, де $U = \{1,\ldots,n\}$ містить стани ІСКЗ, визнані функціональними, а $D = \{n+1,\ldots,N\}$ – нефункціональні стани ІСКЗ. Сегрегуємо матричну форму представлення характеристичних параметрів НМП із урахуванням факту існування підпросторів U і D:

$$p = \begin{array}{c} \begin{array}{cc} U & D \end{array} \\ \begin{bmatrix} p_{UU} & p_{UD} \\ p_{DU} & p_{DD} \end{bmatrix} \end{array} \begin{array}{c} \\ U \\ D \end{array};$$

$$Q(t)=\begin{array}{cc} & \begin{array}{cc} U & D \end{array} \\ & \begin{bmatrix} Q_{UU}(t) & Q_{UD}(t) \\ Q_{DU}(t) & Q_{DD}(t) \end{bmatrix} \begin{array}{c} U \\ D \end{array} \end{array};$$

$$W(t)=\begin{array}{cc} & \begin{array}{cc} U & D \end{array} \\ & \begin{bmatrix} W_U(t) & 0 \\ 0 & W_D(t) \end{bmatrix} \begin{array}{c} U \\ D \end{array} \end{array},$$

$$\alpha = \begin{array}{c} \begin{array}{cc} U & D \end{array} \\ \begin{bmatrix} \alpha_U & \alpha_D \end{bmatrix} \end{array},$$

де $W_U(t)=diag(W_i(t);i\in U)$; $W_D(t)=diag(W_i(t);i\in D)$; $\alpha_U=(\alpha_i;i\in U)$; $\alpha_D=(\alpha_i;i\in D)$.

Функцію $\Psi(t)$ і рівняння $P(t)$ марковського відновлення із врахуванням U і D опишемо виразами

$$\Psi_{UU}(t)=(I_n-Q_{UU})^{(-1)}(t); \tag{5.123}$$

$$P_{UU}(t)=(\Psi_{UU}*(I_n-W_U))(t), \tag{5.124}$$

на основі яких отримаємо $(Q_{UU})_{ij}(t)=\alpha_{ij}\left(1-(1-F(t))_{k\in E}^{\sum\alpha_{ik}}\right)\left(\sum_{k\in E}\alpha_{ik}\right)^{-1}$.

Опишемо безвідмовність ІСКЗ у часі функцією $R(t)=P(T_D>t)=P(Z_s\in U,s\le t)$, яка дозволяє встановити імовірності того, що система перебуватиме у функціональному стані в час $s\le t$, де $T_D=\inf\{t|Z_t\in D\}$ – життєвий цикл ІСКЗ, який включає часовий проміжок від початку функціонування системи $t=0$ до першого зареєстрованого часу переходу системи в один із станів з підпростору D. Враховуючи (5.123), (5.124), сформулюємо оцінку безвідмовності ІСКЗ для $t>0$ у вигляді

$$\hat{R}(t,M)=\hat{\alpha}_U(M)\hat{P}_{UU}(t,M)1_n, \tag{5.125}$$

де $\hat{\alpha}_U(M)$ і $\hat{P}_{UU}(t,M)$ – оцінки $\alpha_U(M)$ і $P_{UU}(t,M)$, відповідно. Функція безвідмовності з урахуванням (5.125) набуде вигляду

$$R(t)=\alpha_U P_{UU}(t)1_n. \tag{5.126}$$

За аналогією з (5.98)–(5.100), для скінченного цілого t запропонована в формі виразу (5.125) оцінка безвідмовності описаної напівмарковською моделлю

ІСКЗ є строго сумісною $\left(\left|\hat{R}(t,M)-R(t)\right|\underset{M\to\infty}{\to}0\right)$ і асимптотично нормальною $\left(\sqrt{M}\left|\hat{R}(t,M)-R(t)\right|\underset{M\to\infty}{\to}\aleph\left(0,\sigma_R^2(t)\right)\right)$.

Асимптотичну дисперсію опишемо виразом

$$\sigma_R^2(t)=\sum_{i=1}^{s}\mu_{ii}\left\{\sum_{j=1}^{s}\left(D_{ij}^U-1_{\{i\in U\}}\sum_{l\in U}\alpha(l)\Psi_{li}\right)^2*q_{ij}(t)-\right.$$
$$\left.-\left(\sum_{j=1}^{s}\left(D_{ij}^U*q_{ij}-1_{\{i\in U\}}\sum_{l\in U}\alpha(l)\psi_{li}*Q_{ij}\right)\right)^2(t)\right\}, \tag{5.127}$$

де $D_{ij}^U=\sum_{n\in U}\sum_{r\in U}\alpha(n)\psi_{ni}*\left(I(t)-diag\left(Q_{ij}(t)\cdot 1_{\{i=j\}}\right)\right)_{rr}$; $\Psi(t)=\sum_{n=0}^{t}Q^{(n)}(t)$; $\psi(t)=\sum_{n=0}^{t}q^{(n)}(t)$; $*$ – операція згортки; μ_{ii} – середня тривалість рекурсії для стану i марковського ланцюга Z, $i,j\in E$, $t\in\aleph$.

У дискретному сенсі під готовністю ІСКЗ $A(t)$ розумітимемо імовірність надання доступу до ІнР системи автентифікованому суб'єкту в момент його звернення в час t:

$$A(t)=P(Z_t\in U). \tag{5.128}$$

Оцінювання готовності ІСКЗ, модельованої НМП, у момент часу $t>0$ здійснюватимемо за виразом

$$\hat{A}(t,M)=\hat{\alpha}(M)\hat{P}(t,M)1_{N;n}, \tag{5.129}$$

де $\hat{P}(t,M)$ є оцінкою $P(t)$; $\hat{\alpha}(M)$ є оцінкою α; а $1_{N;n}=\left(\underbrace{1,\ldots,1}_{n},\underbrace{0,\ldots,0}_{N-n}\right)^T$. За аналогією з отриманням (5.126), вирази (5.128) і (5.129) можна узагальнити у формі

$$A(t)=\alpha P(t)1_{N;n}. \tag{5.130}$$

Під обслуговуваністю ІСКЗ $M(t)$ розумітимемо імовірність переходу ІСКЗ із нефункціонального стану у функціональний до настання моменту часу t:

$$M(t) = P(T_U \le t) = 1 - P(Z_s \in S, s \le t), \tag{5.131}$$

де $T_U = \inf\{t | Z_t \in U\}$ – тривалість перебування системи у нефункціонального стані. Оцінювання обслуговуваності ІСКЗ, модельованої НМП, у момент часу $t > 0$, здійснюватимемо за виразом

$$\hat{M}(t, M) = 1 - \hat{\alpha}_D(M)\hat{P}_{DD}(t, M)1_{N-n}, \tag{5.132}$$

де $\hat{\alpha}_D(M)$ є оцінкою α_D; $\hat{P}_{DD}(t, M)$ є оцінкою $P_{DD}(t, M)$.

Визначимо інтенсивність відмов ІСКЗ $\lambda(t)$ як умовну імовірність того, що система перейде в нефункціональний стан в момент часу $t = M$, якому передуватиме період безвідмовної роботи системи тривалістю $[0, t)$. Зв'яжемо характеристику $\lambda(t)$ із безвідмовністю $R(t)$ виразом

$$\lambda(t) = P(T_D = t | T_D \ge t) = \begin{cases} 1 - R(t)(R(t < M))^{-1}, if\ R(t < M) \ne 0, \\ 0, else \end{cases} =$$

$$= \begin{cases} 1 - \alpha_U P_{UU}(t) 1_n \left(\alpha_U P_{UU}(t < M) 1_n\right)^{-1}, if\ R(t < M) \ne 0, \\ 0, else, \end{cases} \tag{5.133}$$

$$\lambda(0) = 1 - R(0).$$

Оцінку інтенсивності відмов ІСКЗ $\lambda(t)$, визначеної виразом (5.133), обчислимо як

$$\hat{\lambda}(t, M) = \begin{cases} 1 - \hat{R}(t, M)\left(\hat{R}(t < M, M)\right)^{-1}, if\ \left(\hat{R}(t < M, M) \ne 0\right) \wedge (k \ge 1), \\ 0, if\ \left(\hat{R}(t < M, M) = 0\right) \wedge (k \ge 1), \end{cases}$$

$$\hat{\lambda}(0, M) = 1 - \hat{R}(0, M).$$

Під наробком на відмову MTF розумітимемо середній час поки ІСКЗ не перейде в будь-який стан із підпростору D: $MTF = E(T_D)$. Загалом, визначимо вектор $m = (m_1, \ldots, m_N)^T$, $i = \overline{1, N}$, де m_i – тривалість перебування ІСКЗ в i-му стані, тоді середню тривалість перебування ІСКЗ у i-му стані опишемо як

$$m_i = E(S_1 | J_0 = i) = \int_0^\infty (1 - W_i(t))dt = \int_0^\infty (1 - F(t))^{\sum_{j=1}^{N} \alpha_{ij}} dt.$$

Для оцінювання m_i запропонуємо два варіанти формалізації:

$$\hat{m}_i^{(1)} = \int_0^\infty \left(1 - \hat{W}_i(t, M)\right) dt = \int_0^\infty \left(1 - F(t)\right)^{\sum_{j=1}^{N} \hat{\alpha}_{ij}(M)} dt\,;$$

$$m_i^{(2)}(M) = \sum_{k=1}^{N_i(M)} X_i^{(k)} \left(N_i(M)\right)^{-1},$$

де оцінки α_{ij} для $\hat{m}_i^{(1)}$ в залежності від виду розподілу визначаються за одним із виразів (5.102), (5.104), (5.106) або (5.110).

На основі $\hat{m}_i^{(1)}$ і $\hat{m}_i^{(2)}$ отримаємо вирази для оцінювання MTF:

$$\hat{MTF}^{(1)}(M) = \hat{m}_U^{(1)}(M)\hat{\alpha}_U(M)\left(I_n - \hat{p}_{UU}(M)\right)^{-1};$$

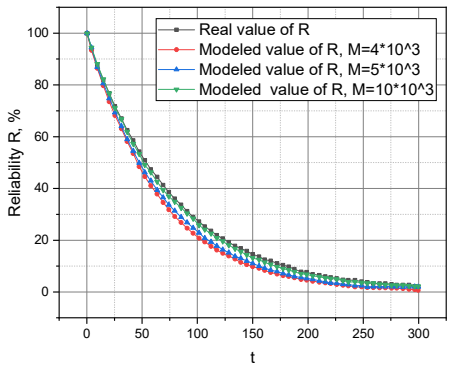
$$\hat{MTF}^{(2)}(M) = \hat{m}_U^{(2)}(M)\hat{\alpha}_U(M)\left(I_n - \hat{p}_{UU}(M)\right)^{-1},$$

де $\hat{\alpha}_U$ і $\hat{p}_{UU}(M)$ є оцінками α_U і $p_{UU}(M)$, відповідно.

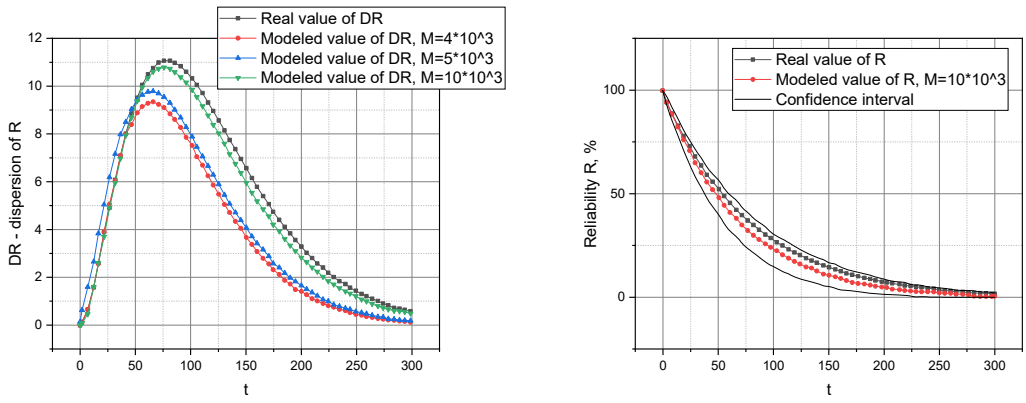
Нехай існує ІСКЗ, описана керованою напівмарковською моделлю, із множиною допустимих станів $E = \{1, 2, 3\}$, яка включає підмножину функціональних станів $U = \{1, 2\}$ і підмножину нефункціональних станів $D = \{3\}$. Вихідні характеристики НМП, який описує життєвий цикл ІСКЗ, такі: вихідний розподіл $\alpha = (1,\ 0,\ 0)$, матриця перехідних імовірностей $p_{ij} = \begin{pmatrix} 0 & 1 & 0 \\ 0{,}95 & 0 & 0{,}05 \\ 1 & 0 & 0 \end{pmatrix}$, умовні розподіли для відповідних часових інтервалів життєвого циклу ІСКЗ описуються матрицею $F_{ij}(t) = \begin{pmatrix} 0 & F_{12}(t) & 0 \\ F_{21}(t) & 0 & F_{23}(t) \\ F_{31}(t) & 0 & 0 \end{pmatrix}$, де F_{12} – геометричний розподіл із параметром $p = 0{,}8$, а $F_{21} = W_{q_1,c_1}$, $F_{23} = W_{q_2,c_2}$ і $F_{31} = W_{q_3,c_3}$ – розподіли Вейбула для яких $q_1 = 0{,}3$, $q_2 = 0{,}5$, $q_3 = 0{,}6$, $c_1 = 0{,}5$, $c_2 = 0{,}7$, $c_3 = 0{,}9$, відповідно, при аналітичному вигляді розподілу $W_{q,c} = q^{(t-1)^c} - q^{t^c}$ і $W_{q,c}(0) = 0$. Використовуючи дані матриці p_{ij} і $F_{ij}(t)$, розрахуємо для напівмарковського ланцюга довжиною M значення $N_i(M)$, $N_{ij}(M)$ і $N_{ij}(t, M)$ за виразами (5.95), (5.96) і (5.97), відповідно, викорис-

товуючи які обчислимо емпіричні оцінки $\hat{p}_{ij}(M)$, $\hat{F}_{ij}(t,M)^{-1}$, $\hat{q}_{ij}(t,M)$ за виразами (5.98)–(5.100), відповідно. Далі, використовуючи вираз (5.125), здійснимо оцінювання безвідмовності ІСКЗ $\hat{R}(t,M)$ і, обчисливши оцінки $\hat{Q}(t,M)$, $\hat{\psi}(t,M)$, $\hat{\Psi}(t,M)$, розрахуємо оцінку $\hat{\sigma}_R^2(t,M)$ асимптотичної дисперсії (5.127), що дозволяє отримати асимптотичний довірчий інтервал безвідмовності ІСКЗ.

Числові значення оцінок безвідмовності, розраховані за сформульованою вище методикою для різних значень t і M, візуалізовано на рис. 5.17а, з якого видно, що змодельована оцінка безвідмовності наближається до дійсного значення цієї характеристики із зростанням M. На рис. 5.17б представлено залежність оцінки асимптотичної дисперсії безвідмовності $\hat{\sigma}_R^2(t,M)$ від значень t і M, з якої також простежується тенденція до наближення змодельованих значень оцінок до реальних значень дисперсії із зростанням M. Наведені на рис. 5.17в результати показують, що довірчий інтервал безвідмовності накриває дійсне і розраховане на основі запропонованого математичного апарату значення цієї характеристики, що підтверджує адекватність синтезованих математичних моделей.



а)



б) в)

Рисунок 5.17 – Емпіричне доведення адекватності запропонованого математичного апарату оцінювання безвідмовності ІСКЗ:
а) порівняння дійсної і змодельованих оцінок безвідмовності ІСКЗ; б) порівняння дійсної і змодельованих дисперсій оцінок безвідмовності ІСКЗ;
в) оцінювання входження дійсної і емпіричної оцінок безвідмовності ІСКЗ у довірчий інтервал.

Узагальнимо емпіричну частину підрозділу оцінюванням адекватності запропонованих моделей у парадигмі класичної теорії планування експерименту. Сформуємо визначені множини вхідних впливів, поява яких може спричинити перехід ІСКЗ у нефункціональний стан: $X^k = \{x_1^k, x_2^k, \ldots, x_n^k\}$ і $X^{\bar{k}} = \{x_1^{\bar{k}}, x_2^{\bar{k}}, \ldots, x_m^{\bar{k}}\}$. Реакцію ІСКЗ на вхідні впливи, включені в множину X^k, описано у СПБ, отже, система має успішно протидіяти їм залишаючись у функціональному стані. Вхідні впливи, включені у множину $X^{\bar{k}}$, структурно ідентичні описаним у множині X^k, але відрізняються від них за значеннями, які можуть перевищувати граничні, встановлені на етапі проектування системи, величини для відповідних вхідних параметрів. Реакцією ІСКЗ на вхідний вплив із множини $X^{\bar{k}}$ може стати перехід системи у нефункціональний стан.

Кількості елементів множин X^k і $X^{\bar{k}}$ становлять $n = 200$ і $m = 700$, відповідно. Далі проведемо експерименти з фіксацією реакції ІСКЗ на вхідні впливи з множини X^k у матрицю $Y_e^k = \left(y_{ij}^k\right)$, $i = \overline{1,n}$, де $y_{ij}^k = \{res_{ij}^k, t_{ij}^k\}$ – множина, в якій

res_{ij}^{k} – результат j-ї спроби переведення ІСКЗ у нефункціональний стан з причини негативного впливу x_j^k, t_{ij}^k – час, витрачений СПБ на протидію відповідному негативному впливу. Також зафіксуємо емпіричну реакцію ІСКЗ на вхідні впливи з множини $X^{\bar{k}}$ у матрицю $Y_e^{\bar{k}} = \left(y_{ij}^{\bar{k}}\right)$, $i = \overline{1,m}$, де $y_{ij}^{\bar{k}} = \left\{res_{ij}^{\bar{k}}, t_{ij}^{\bar{k}}\right\}$ – множина, в якій $res_{ij}^{\bar{k}}$ – результат j-ї спроби переведення ІСКЗ у нефункціональний стан з причини негативного впливу $x_j^{\bar{k}}$, $t_{ij}^{\bar{k}}$ – час, витрачений СПБ на відновлення функціонального стану ІСКЗ, якщо вхідний вплив $x_j^{\bar{k}}$ перевів її у нефункціональний стан. Розрахуємо для i-го вхідного впливу дисперсію переходу ІСКЗ у нефункціональний стан: $s_i^2 = M^{-1}\sum_{j=1}^{M}\left(y_{ij} - y'_{ij}\right)^2$, де y_{ij} – визначений у СПБ стан, у який ІСКЗ повинна перейти в наслідок i-го вхідного впливу; y'_{ij} – фактичний стан, в який ІСКЗ перейшла в наслідок i-го вхідного впливу. Розрахуємо середнє значення дисперсії для всіх вхідних впливів: $s^2 = N^{-1}\sum_{i=1}^{N} s_i^2$. Оцінювання фактичних відхилень s_i^2 від s^2 за критерієм Фішера показало, що всі відхилення не перевищують таблич-них значень, що підтверджує адекватність запропонованого в підрозділі математичного апарату для оцінювання гарантоздатності ІСКЗ.

Висновки до п’ятого розділу

1. Представлено концепцію автентифікації суб’єктів-користувачів в процесі отримання доступу до мультисерверної інформаційної системи критичного застосування. 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 співвідношен-

ня 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 яких синтезовано удосконалену концепцію, яка містить відповідні механізми захисту і також відповідає згаданому стандарту.

2. Для оцінювання надійності процесу доступу до ІСКЗ запропоновано марковську модель залежності функціональної спроможності ІСКЗ від впливу негативних факторів, у якій визначено множину станів ІСКЗ та отримано 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.

3. Запроваджено єдиний підхід для математичного моделювання інформаційних процесів у 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 функцій 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 суперблоками 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.

4. 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 здійснен-

ня сервісних операцій з вивільнення системних ресурсів. Синтезовані математичні моделі управління готовністю ІСКЗ які враховують топологічні особливості ІСКЗ, 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 дозволило за допомогою апарату математичного програмування отримати оптимальну стратегію управління готовністю ІСКЗ із мінімізацією витрат на її функціонування та отримати стохастичну оцінку готовності системи на будь-якому етапі її життєвого циклу.

5. Розвитком матеріалу підрозділів 5.1, 5.3 стала наведена у додатку К математична модель залежності втрат конфіденційності процесу автентифікації і показника готовності ІСКЗ, у якій у формі задачі математичного програмування представлено процес синтезу оптимальної напівмарковської стратегії управління прийняттям рішень у марковському процесі автентифікації суб’єктів, які бажають отримати доступ до ресурсів ІСКЗ, що дозволяє мінімізувати втрати готовності ІСКЗ за рахунок встановлення адміністратором порогового значення для параметра конфіденційності системи. Сформульовано методику застосування вищеописаної моделі вважаючи, що у системній політиці безпеки описано ситуації «критична помилка» і «підозра на помилку», які можуть ідентифікуватися відповідною підсистемою під час перебігу процесу автентифікації.

6. Синтезовано моделі функційної безпечності і живучості ІСКЗ у формалізмі марковських моделей. У 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 у 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 системи, 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 детермінованих збоїв. При синтезі моделі живучості враховано архітектуру ІСКЗ, функції ПБІС, налаштування СПБ тощо. Адекватність запропонованих моделей і методу доведено результатами експериментів, у яких модельовані характеристики порівнювалися із емпіричними за значенням середньоквадратичного відхилення.

7. Синтезовано комплекс керованих напівмарковських моделей, які описують динаміку процесу функціонування ІСКЗ як систему із багатьма станами, у напівмарковському описі якої узгоджуються стани, описувані різними розподілами, що дозволило формалізувати оцінювання максимуму функції правдоподібності і параметрів напівмарковського процесу, який описує життєвий цикл 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, які моделюють життєвий цикл 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.

8. Загалом в розділі формалізовано методологію 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.

Основні результати розділу опубліковано в [36, 43, 49, 50, 51, 55, 56, 58, 59, 60, 83, 84].

РОЗДІЛ 6
ПРИКЛАДНЕ УЗАГАЛЬНЕННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ДЛЯ ПІДВИЩЕННЯ ГАРАНТОЗДАТНОСТІ ІНФОРМАЦІЙНОЇ СИСТЕМИ КРИТИЧНОГО ЗАСТОСУВАННЯ ІЗ АВТЕНТИФІКАЦІЄЮ СУБ'ЄКТА ЗА ГОЛОСОМ

6.1 Методика аналітичного розрахунку характеристичних параметрів при описі мовленнєвих сигналів моделями ІГМС

Формалізуємо аналітично процес розрахунку характеристичних параметрів моделей ІГМС виду (2.1), (2.24), (2.46) і (2.64), заданих як явні функції від часу. Нехай для фонограми досліджуваного мовленнєвого сигналу обчислено J відліків функції кореляції K_j. Також для обраної моделі ІГМС обчислена авто– або кореляційна функція $Ka(\tau)$, аналітично представлена відповідним з виразів (2.9), (2.27), (2.50), (2.68) у формі

$$Ka(\tau)=\sum_{l=0}^{L}U_l^2 S_l(\tau), \tag{6.1}$$

де U_l – амплітуда l–ї несної гармоніки в математичній моделі, $S_l(\tau)$ – функція, значення якої залежить від номера несної гармоніки l, часового інтервалу τ і решти параметрів обраної математичної моделі (наприклад, частоти основного тону мовленнєвого сигналу, частоти модулювального коливання, тривалості мовленнєвого повідомлення – див. підрозділ 3.3). За визначенням $Ka(\tau)$, кореляційні коефіцієнти (відліки нормованої автокореляційної функції) математичної моделі опишемо виразом

$$Ra_j=\frac{Ka(j\Delta)}{Ka(0)}\equiv\frac{Ka_j}{Ka_0}. \tag{6.2}$$

Застосуємо метод найменших квадратів для розрахунку значень характеристичних параметрів U_l, $l=\overline{1,L}$, обраної математичної моделі ІГМС при яких мінімізується значення середньоквадратичної помилки

$$\varepsilon = \sum_{j=1}^{J} \left(Ra_j - R_j \right)^2 . \tag{6.3}$$

Для квазідетермінованих моделей (2.1), (2.24) нормовані автокореляційні функції досліджуваного центрованого мовленнєвого сигналу y і моделі u такі: $R_j = b_j^y = B_j^y / B_0^y = B_j^y / E^y$, $Ra_j = b_j^u = B_j^u / B_0^u = B_j^u / E^u$, де B_j і E – автокореляційна функція і енергія, відповідно. Для стохастичних моделей (2.46), (2.64) функції кореляції досліджуваного центрованого мовленнєвого сигналу y і моделі u такі: $R_j = r_j^y = R_j^y / R_0^y = R_j^y / \left(\sigma^y \right)^2$, $Ra_j = r_j^u = R_j^u / R_0^u = R_j^u / \left(\sigma^u \right)^2$, де σ^2 – дисперсія.

Прирівняємо до нуля перші похідні $\varepsilon R \equiv \varepsilon R \left(U_0, U_1, \ldots, U_L \right)$ (6.3) за кожним коефіцієнтом U_l, $l = \overline{0, L}$, отримуючи систему з $L+1$ рівнянь:

$$\sum_{j=1}^{J} \left(R_j - Ra_j \right) \frac{\partial Ra_j}{\partial U_l} = 0 . \tag{6.4}$$

Система (6.4) складається з поліномів четвертого ступеню і, відповідно, однозначного розв’язку не має. Припускаємо, що енергія (для квазідетермінованих) або дисперсія (для стохастичних моделей) однотипних за вмістом і суб’єктом мовленнєвих сигналів є сталою величиною: $Ka_0 = const$. Використаємо заміну

$$V_l = U_l^2 \tag{6.5}$$

та позначимо

$$S_{jl} = S_j \left(j\Delta \right), \; Ka_j = Ka \left(j\Delta \right). \tag{6.6}$$

Перетворимо вирази (6.1) і (6.4) з врахуванням виразів (6.5), (6.6). Отримаємо, відповідно:

$$Ka_j = \sum_{l=0}^{L} V_l S_{jl} , \; j = \overline{1, J} . \tag{6.7}$$

$$\sum_{j=1}^{J} \left(R_j - Ra_j \right) \frac{\partial Ra_j}{\partial V_l} = 0 , \; l = \overline{0, L} . \tag{6.8}$$

Обчисливши похідні у виразі (6.9) отримаємо систему лінійних рівнянь:

$$\frac{1}{Ka_0}\sum_{l=0}^{L}\left(\sum_{j=1}^{J}S_{jp}S_{jl}\right)V_l=\sum_{j=1}^{J}S_{j0}R_j\,,\ p=\overline{0,L}. \tag{6.9}$$

Продовжимо компактифікацію системи (6.9) ввівши такі заміни:

$$A_{pl}=\frac{1}{Ka_0}\sum_{j=1}^{J}S_{jp}S_{jl}\,,\ p,l=\overline{0,L}, \tag{6.10}$$

$$B_p=\sum_{j=1}^{J}S_{jp}R_j\,,\ p=\overline{0,L}. \tag{6.11}$$

Врахувавши (6.10), (6.11) отримаємо спрощену форму системи (6.9):

$$\sum_{l=0}^{L}A_{pl}V_l=B_p\,,\ p=\overline{0,L}. \tag{6.12}$$

Розв'язок системи лінійних рівнянь (6.12) відносно V_l тривіальний. Для спрощення програмної реалізації формалізуємо вищенаведену аналітичну послідовність обчислень у матричній формі. Так вираз (6.7) запишемо як

$$Ka=SV\,, \tag{6.13}$$

де Ka – вектор–стовпець розмірністю $J\times 1$ з елементів Ka_j, S – матриця розмірністю $J\times(L+1)$ з елементів S_{jl}, де V – вектор–стовпець розмірністю $(L+1)\times 1$ з елементів V_l. Похибку обраховуваної моделі у матричній формі представимо виразом

$$\begin{aligned}\varepsilon(V)&=(Ka-K)^T(Ka-K)=(K-Ka)^T(K-Ka)=\\&=(K-SV)^T(K-SV),\end{aligned} \tag{6.14}$$

де K – вектор–стовпець розмірністю $J\times 1$ з елементів K_j, $(A)^T$ – операція транспонування матриці A.

Застосуємо операцію скалярно–матричного диференціювання до необхідної умови існування мінімуму задачі оптимізації (6.14):

$$\partial\varepsilon(V)/\partial V=0, \tag{6.15}$$

отримавши в результаті рівняння

$$2S^T(K-SV)=0. \tag{6.16}$$

На основі рівняння (6.16) отримаємо нормальну систему метода найменших квадратів у матричній формі:

$$S^T SV = S^T K, \tag{6.17}$$

з якої виразимо вектор оцінок характеристичний параметрів досліджуваної моделі:

$$V = \left(S^T S\right)^{-1} S^T K. \tag{6.18}$$

Компактніший вигляд (6.18) отримаємо замінивши $S^T S = A$, $S^T K = B$:

$$AV = B, \tag{6.19}$$

де A – квадратна матриця розмірністю $\left(L+1\right)\times\left(L+1\right)$ з елементів (6.10), B – вектор–стовпець розмірністю $\left(L+1\right)\times 1$ з елементів (6.11). Розв'язок (6.19) відносно V опишемо виразом

$$V = A^{-1}B, \tag{6.20}$$

з якого, врахувавши вираз (6.5), отримаємо значення шуканих характеристичних параметрів:

$$U_l = \sqrt{V_l}\,.\ l = \overline{0,L}\,. \tag{6.21}$$

Також відзначимо, що при використанні параметрів R_j вираз (6.18) за умови, що $K_0 = Ka_0$, можна представити у вигляді

$$V = Ka_0\left(S^T S\right)^{-1} S^T R, \tag{6.22}$$

де R – вектор–стовпець розмірністю $J\times 1$ з елементів R_j.

Відзначимо, що вищенаведена методика розрахунку характеристичних параметрів моделей (2.1), (2.24), (2.46), (2.64) у формі послідовності аналітичних виразів (6.1)–(6.22) характеризується універсальністю щодо виду обраної моделі ІГМС. Фактично, від виду моделі залежить лише функціональна залежність авто– або кореляційної функції (6.1) $S_l\left(\tau\right)$, тобто змінюватимуться лише параметри S_{jl} і Ka_0.

Розглянемо окремі випадки розв'язання (6.21) в залежності від виду обраної моделі ІГМС. *Базова квазідетермінована модель ІГМС (2.1)* в окремому випадку,

при $\varphi_0 = 1$, $M = 1$, $\Gamma_0 = \pi$, спрощується до вигляду (2.2). Втім, присутність добутків $U_l U_m$ в автокореляційній функції (2.9) робить її невідповідною формі (6.1), що унеможливлює подальше використання розв'язку системи (6.19) у вигляді (6.20). Але, при виконанні умови $f_0 \tau_i >> 1$, в ітогове значення автокореляційній функції (2.9) істотний вклад вносять лише доданки із U_l^2, що дозволяє спростити аналітичний вигляд функції (2.9) до вигляду (2.12). В такому випадку елементи матриці S для виразу (6.18) можна розрахувати за виразом (2.15). Для прикладного застосування допускається рівність значень енергій: $Ka_0 \equiv E^u = E^y \equiv B_0^y$. В автокореляційній функції (2.25), використовуваній в *уточненій квазідетермінованій моделі ІГМС (2.24)*, також присутні добутки $U_l U_m$, що також унеможливлює подальше використання розв'язку системи (6.19) у вигляді (6.20). Втім, за умови, що $f_0 \tau_i >> 1$ та ще ряду описаних у підрозділі 2.3 припущень, автокореляційна функція (2.25) набуває спрощеного вигляду (2.47) для якого елементи матриці S для виразу (6.18) можна розрахувати за виразом (2.29). Для прикладного застосування також допускається рівність значень енергій: $Ka_0 \equiv E^u = E^y \equiv B_0^y$. Для *базової стохастичної моделі ІГМС (2.46)* функція кореляції $Ka(\tau)$ визначається за виразом (2.50). Елементи матриці S для виразу (6.18) для цієї моделі можна розрахувати за виразом (2.63). Для прикладного застосування також допускається рівність значень дисперсій: $Ka_0 \equiv \left(\sigma^u\right)^2 = \left(\sigma^y\right)^2 \equiv R_0^y$. Для *удосконаленої стохастичної моделі ІГМС (2.64)* функція кореляції $Ka(\tau)$ визначається за виразом (2.68). Елементи матриці S для виразу (6.18) для цієї моделі можна розрахувати за виразом (2.71). Для прикладного застосування також допускається рівність значень дисперсій: $Ka_0 \equiv \left(\sigma^u\right)^2 = \left(\sigma^y\right)^2 \equiv R_0^y$.

Отже, для досліджуваного мовленнєвого сигналу при заданій оцінці частоти основного тону $\widehat{f}_0$ і заданих значеннях фіксованих параметрах моделі ІГМС характеристичні параметри останньої можна обчислити за виразом (6.21).

Наприклад, при застосуванні вищенаведеної методики для аналізу описів фонограми мовленнєвого сигналу, візуалізованого на рисунку 3.1, базовою квазідетермінованої і базовою стохастичною моделями ІГМС (2.1) і (2.46), відповідно, при значеннях усталених параметрів моделей $f_d = 6000$ Гц, $\tau = 0{,}3$ с, $L = 6$, $M = 1$, $F_0 = 15$ Гц, $J = 200$, виявилося, що відносні похибки описів дорівнюють $\delta\varepsilon_{(2.23)} = 5{,}688\%$ і $\delta\varepsilon_{(2.68)} = 6{,}605\%$, відповідно. Отримані результати можна покращувати варіюючи значеннями усталених параметрів моделей, що, проте, не відміняє потенційно вищу прицезійність базової квазідетермінованої моделі ІГМС, що було емпірично доведено у підрозділі 3.3.

Обчислимо дисперсію оцінок амплітуд несних гармонік $\widehat{U}_l$, отриманих як результат застосування методу найменших квадратів. Матрицю розсіювання для оцінок характеристичних параметрів, отриманих методом найменших квадратів, формалізуємо виразом

$$\Pi\left(\widehat{V}\right) = \sigma^2 \left(S^T S\right)^{-1} = \frac{1}{J-L}\left(K - S\widehat{V}\right)^T \left(K - S\widehat{V}\right)\left(S^T S\right)^{-1}, \tag{6.23}$$

де $\widehat{V}$ – оцінки параметрів V, σ^2 – незміщена оцінка для дисперсії спостережень:

$$\sigma^2 = \frac{1}{J-L}\left(K - S\widehat{V}\right)^T \left(K - S\widehat{V}\right), \tag{6.24}$$

де J – кількість спостережень, L – кількість оцінюваних параметрів.

Визначимо дисперсії $D\left(\widehat{V}\right)$ оцінок параметрів $\widehat{V}_l$ як відповідні елементи $\left\{\Pi\left(\widehat{V}\right)\right\}_{ll}$ матриці розсіювання (6.23):

$$D\left(\widehat{V}\right) = \left\{\Pi\left(\widehat{V}\right)\right\}_{ll} = \frac{1}{J-L}\varepsilon\left(\widehat{V}\right)\left\{\left(S^T S\right)^{-1}\right\}_{ll}. \tag{6.25}$$

Середньоквадратичне відхилення оцінок параметрів $\widehat{V}_l$ визначимо як

$$\sigma_{\widehat{V}_l} = \sqrt{\frac{1}{J-L}\varepsilon\left(\widehat{V}\right)\left\{\left(S^T S\right)^{-1}\right\}_{ll}}. \tag{6.26}$$

Абсолютні похибки оцінок параметрів $\widehat{V}_l$ для довірчої імовірності $P = 99,7\%$ (довірчі інтервали $\pm 3\sigma_{\widehat{V}_l}$) визначимо як

$$\Delta_{\widehat{V}_l} \approx 3\sigma_{\widehat{V}_l}. \tag{6.27}$$

Абсолютні похибки оцінок параметрів $\widehat{U}_l$ при довірчих інтервалах $\pm 3\sigma_{\widehat{V}_l}$ для оцінок параметрів $\widehat{V}_l$ визначимо як $\widehat{U}_l \pm \Delta_{\widehat{U}_l} = \sqrt{\widehat{V}_l \pm \Delta_{\widehat{V}_l}}$, звідки

$$\Delta_{\widehat{U}_l} = \sqrt{\widehat{V}_l \pm \Delta_{\widehat{V}_l}} - \widehat{U}_l. \tag{6.28}$$

Якщо розкласти перший доданок (6.28) у біноміальний ряд і обмежитися першими двома членами розкладу (адже $\widehat{V}_l >> \Delta_{\widehat{V}_l}$), то отримаємо

$$\Delta_{\widehat{U}_l} \approx \frac{\Delta_{\widehat{V}_l}}{2\widehat{U}_l}. \tag{6.29}$$

Підставимо вирази (6.26), (6.27) у вираз (6.29):

$$\Delta_{\widehat{U}_l} \approx \frac{\Delta_{\widehat{V}_l}}{2\widehat{U}_l} = \frac{3\sigma_{\widehat{V}_l}}{2\widehat{U}_l} = \frac{3}{2\widehat{U}_l}\sqrt{\frac{1}{J-L}\varepsilon\left(\widehat{V}\right)\left\{\left(S^T S\right)^{-1}\right\}_{ll}}. \tag{6.30}$$

Врахувавши (6.30) опишемо відносні похибки оцінок параметрів $\widehat{U}_l$:

$$\delta_{\widehat{U}_l} = \frac{\Delta_{\widehat{U}_l}}{\widehat{U}_l} \cdot 100\%. \tag{6.31}$$

Аналіз виразів (6.31), (6.31) переконує, що найбільше на значення похибки $\varepsilon(V)$ впливає саме вид математичної моделі ІГМС, який вибирається для опису досліджуваного мовленнєвого сигналу. Наприклад, при описі візуалізованого на рисунку 3.1 мовленнєвого сигналу моделлю (2.46) із значеннями усталених параметрів $f_d = 6000$ Гц, $\tau = 0,3$ с, $L = 6$, $M = 1$, $F_0 = 15$ Гц, $\sigma_u^2 = 23,218$, $J = 200$ в результаті роботи методу найменших квадратів отримано значення амплітуд несних гармонік $U_1 = 2,249$; $U_2 = 2,173$; $U_3 = 3,994$; $U_4 = 0,900$; $U_5 = 0,937$; $U_6 = 0,433$ при $f_0 = 155,2$ Гц і $\varepsilon_{(2.68)} = 1,154$. Скориставшись виразами (6.30), (6.31) розрахуємо відносні похибки оцінок параметрів $\widehat{U}_l$, $l = \overline{1,6}$: $\delta_{\widehat{U}_1} = \pm 0,433\%$; $\delta_{\widehat{U}_2} = \pm 0,464\%$; $\delta_{\widehat{U}_3} = \pm 0,137\%$; $\delta_{\widehat{U}_4} = \pm 2,707\%$; $\delta_{\widehat{U}_5} = \pm 2,495\%$; $\delta_{\widehat{U}_6} = \pm 11,662\%$.

Розраховані значення відносних похибок дозволяють із довірчою імовірністю $P = 99{,}7\%$ побачити як оцінки $\widehat{U}_l$ групуються відносно значень характеристичних параметрів U_l. Отриманий розкид значень можна пояснити природною варіативністю голосу.

Резюмуючи вміст підрозділу відзначимо, що квазідетермінованим моделям ІГМС виду (2.1), (2.24) властива порівняно невисока обчислювальна складність і менша похибка $\varepsilon\delta$ опису досліджуваного мовленнєвого сигналу із високим ступенем вокалізованості вмісту за рахунок врахування серед усталених параметрів моделей початкових фаз несного і модулювального коливань. Водночас, стохастичні моделі ІГМС виду (2.46), (2.64) 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.

6.2 Методики оцінювання частоти основного тону на основі моделей ІГМС

Удосконалимо кореляційний метод [227, 231] оцінювання частоти основного тону з метою підвищення достовірності і надійності останнього. Удосконалення полягає у попередній фільтрації мовленнєвого сигналу із подальшим розрахунком характеристики, оберненої усередненому часовому інтервалу між першими (від двох до шісти) сусідніми максимумами функції кореляції. Частоту основного тону мовленнєвого сигналу можна оцінити за значенням періоду пульсації квазіперіодичного кореляційного коефіцієнта з відліками $r_k \equiv R(k)/R(0) = r(k\Delta) = r(\tau_k) = r(\tau)\big|_{\tau=\tau_k}$ для центрованого мовленнєвого сигналу (рисунок 3.18). Для визначення оцінки частоти основного тону пропонується такий алгоритм:

1. Здійснюється фільтрація мовленнєвого сигналу смуговим фільтром із смугою пропускання 70–330 Гц;

2. Для відфільтрованого сигналу розраховується множина кореляційних коефіцієнтів $R = \{r_j\}$, $j = \overline{1, J}$, за виразом, який залежить від обраної моделі ІГМС;

3. Приймаємо $j = 1$; ініціалізуємо одновимірний масив цілих чисел $J\_\max$; задаємо цілочисельне значення $P \geq 2$, яке визначає кількість локальних максимумів кореляційної функції, які бажано знайти;

4. Допоки $length(J\_\max) \leq P$ або $j \leq J$, нарощуючи значення j $(j++)$:

4.1 Шукаємо локальне мінімальне значення кореляційного коефіцієнту. Якщо таке знайдено, то присвоюємо бульовій змінній $loc\_\min$ значення $true$ і фіксуємо індекс кореляційного коефіцієнту з локальним мінімальним значенням у цілочисельній змінній $j\_loc\_\min$;

4.2 Шукаємо локальне максимальне значення кореляційного коефіцієнту. Якщо таке знайдено, то фіксуємо його індекс у цілочисельній змінній $j\_loc\_\max$. Якщо значення бульової змінної $loc\_\min = true$ і $j\_loc\_\max > j\_loc\_\min$, то індекс $j\_loc\_\max$ заносимо у останню вільну комірку одновимірного масиву $J\_\max$, змінюємо значення змінної $loc\_\min$ на $false$ і переходимо до п. 4.1;

5. Знаходимо кількість відліків кореляційної функції між двома сусідніми локальними максимумами опрацьовуючи дані масиву $J\_\max$: $\Delta J\_\max[i] = J\_\max[i+1] - J\_\max[i]$, $i = \overline{1, p-1}$, де $p \leq P$ – фактична кількість знайдених локальних максимумів функції кореляції.

6. Знаходимо середнє значення відліків кореляційної функції, через яке спостерігаються локальні максимуми останньої: $AVG\_J = \frac{1}{p-1}\sum_{i=1}^{p-1} \Delta J\_\max[i]$;

7. Розраховуємо усереднене значення частоти основного тону: $f_0 = f_d / AVG\_J$, де f_d – частота дискретизації досліджуваного мовленнєвого сигналу.

Експериментальні дослідження показали, що задана максимальна кількість локальних максимумів функції кореляції знаходиться за тим меншу проаналізовану кількість її відліків, чим вища ступінь вокалізації досліджуваного мовленнєвого сигналу. Цей факт також можна використовувати як об'єктивну характеристику фонетичного вмісту досліджуваного мовленнєвого сигналу.

Формалізуємо удосконалений спектральний метод оцінювання частоти основного тону і обертонів мовленнєвого сигналу. Удосконалення полягає у змістовному представленні досліджуваного мовленнєвого сигналу нормованою спектральною щільністю потужності $W_N(f)$, розрахованої за методикою кореляційних вікон на основі виразу (3.51). Наприклад, як це показано на рисунку 3.19, де у смузі частот до 1 кГц явно видимі шість перших обертонів основного тону в досліджуваному мовленнєвому сигналі. Удосконалена методика включає таку послідовність операцій:

1. Для визначення оцінки частоти основного тону $\widehat{f}_0$ у частотному діапазоні $f_0^m \pm B_0/2$ знаходиться максимум нормованої спектральної щільності потужності враховуючи, що $f_0^m = 200$ Гц – центральна частота смуги, де відбувається пошук максимуму; $B_0 = 260$ Гц – смуга частот в околі f_0^m. Значення f_0^m, B_0 обираються дослідником з допустимого діапазону спостереження цієї індивідуальної характеристики голосу: $\left[f_0^l = 70 \div f_0^h = 330\right]$, Гц. Якщо в досліджуваному частотному діапазоні виявляється кілька локальних максимумів нормованої спектральної щільності потужності, то за оцінку частоти основного тону приймаємо частоту, на яку вказує найбільший максимум.

2. Для визначення оцінки частоти першого обертону $\widehat{f}_1$ у частотному діапазоні $f_1^m \pm B_1/2\Bbbk$ знаходиться максимум нормованої спектральної щільності потужності враховуючи, що $f_1^m \approx 2\widehat{f}_0$ Гц, $B_1 = 50$ Гц . Звуження частотного діапазону має за мету уникнення ситуації повторного зарахування виявленого у п.1 максимуму.

3. Повторюємо аналогічні описаним у п.1 і 2 операції, визначаючи обертони $\widehat{f}_n$, $n = 2,3,\ldots$, досліджуючи частотні діапазони $f_n^m \pm B_n/2$ де $f_n^m \approx (n+1)\widehat{f}_0$ (Гц), $B_n = 50$ Гц.

Квазіперіодичність $\widehat{f}_n \approx (n+1)\widehat{f}_0$ можна пояснити варіативністю артикуляційних органів людини в процесі генерування вокалізованих звуків.

Спільною характеристикою актуальних методів екстрагування основного тону з мовленнєвого є їх автоматизованість, а не автоматичність. Необхідність втручання експерта проявляється щонайменш на двох етапах: визнання досліджуваного мовленнєвого фрагменту вокалізованим; налаштування усталених параметрів методики екстрагування основного тону. Представлені у розділі 2 математичні моделі ІГМС можуть стати основою для синтезу суто автоматичної методики екстрагування основного тону, що аналітично і експериментально обґрунтуємо далі.

В якості базового елементу використаємо характерний для моделей ІГМС підхід визнання оцінкою частоти основного тону значення частоти при якому спостерігається найменше значення нев'язки (2.6) (для квазідетермінованих моделей ІГМС) або (2.57) (для стохастичних моделей ІГМС). Отже, оцінку частоти основного тону визначимо виразом

$$\widehat{f}_0 = \arg\left\{\inf_f \left(\varepsilon_r(f)\right)\right\}, \tag{6.32}$$

де f_0, $\widehat{f}_0$ – істинне значення частоти основного тону та його оцінка, f – змінюване значення частоти, $\varepsilon_r(f) = \sum_{j=1}^{J}\left(r_j^u(f) - r_j^y(f_0)\right)^2$ – нев'язка виду (2.57). Відзначимо, що формалізувати аналітично оцінку $\widehat{f}_0$ як результат мінімізації $\varepsilon_r(f)$ не оптимально. Це пояснюється тим, що кореляційний коефіцієнт моделі ІГМС $r_j^u(f)$, який входить у $\varepsilon_r(f)$, є періодичною функцією від аргументу f. Отже, задача мінімізації $\varepsilon_r(f)$ із цільовою функцією

$$\frac{\partial \varepsilon_r(f)}{\partial f} = \sum_{j=1}^{J} 2\left(r_j^u(f) - r_j^y(f_0)\right)\frac{\partial r_j^u(f)}{\partial f} = 0. \qquad (6.33)$$

відносно аргументу f матиме велику кількість розв'язків f_q. Останні відповідатимуть як екстремумам, так і точкам перегину. Для локальних мінімумів $f_q^{\min} = \arg\left\{\min_f\left(\varepsilon_r(f)\right)\right\}$ з множини розв'язків $\{f_q\}$ виконуватиметься умова

$$\left.\frac{\partial^2 \varepsilon_r(f)}{\partial f^2}\right|_{f_q} > 0. \qquad (6.34)$$

Наприклад, для візуалізованого на рисунку 3.1 мовленнєвого сигналу, оцифрованого із частотою дискретизації $f_d = 6000$ Гц і тривалістю $\tau_i = 300$ мс при $J = 200$ в залежності від досліджуваного інтервалу $\tau < \tau_i$ кількість локальних мінімумів $f_q^{\min}$ варіювалася в діапазоні $[10, 40]$. Таким чином, із зростанням кількості усталених характеристик досліджуваного мовленнєвого сигналу обчислювальна складність задачі знаходження глобального мінімуму на тлі множинних локальних мінімумів зростає стрімко нелінійно. Втім, якщо змінювати значення f у виразі (6.32) із кроком $\Delta f > 1$ обчислювальна складність задачі знаходження глобального мінімуму зменшується.

Результати розв'язання задачі (6.32) в залежності від виду моделі ІГМС, яка визначає аналітичний вигляд виразу для обчислення залежних від частоти значень кореляційних коефіцієнтів $r_j^u(f)$, показали, що не врахування модуляції при обчисленні $r_j^u(f)$ не впливає на достовірність оцінки частоти основного тону за виразом (6.32) (це природно, адже модуляція проявляється у семантичній складовій мовленнєвого сигналу, тоді як основний тон – визначна характеристика мовного джерела). Дана обставина також спрощує обчислювальну складність задачі оцінювання частоти основного тону (6.32) обмежуючи коло доцільних для застосування моделей ІГМС до базових – (2.1) або (2.46), відповідно. Отже, для обчислення значень кореляційних коефіцієнтів $r_j^u(f)$ скористаємося спрощеним виразом:

$$r_j^u = \sum_{l=1}^{L} U_l^2 \cos\left(2\pi l f_0 j\Delta\right) \Big/ \sum_{l=1}^{L} U_l^2 . \qquad (6.35)$$

Для застосування виразу (6.37) необхідна апріорна інформація про значення амплітуд несних гармонік U_l, яку, наприклад, можна отримати попередньо проаналізувавши амплітудний спектр досліджуваного мовленнєвого сигналу. За відсутності апріорної інформації щодо значень U_l приймемо

$$U_l = U = const . \qquad (6.36)$$

Звичайно, на практиці вираз (6.36) не виконується, проте, допустимість такого припущення проаналізуємо далі. З врахуванням (6.36) вираз (6.37) набуде вигляду

$$r_j^u = \sum_{l=1}^{L} \cos\left(2\pi l f_0 j\Delta\right) \Big/ L . \qquad (6.37)$$

Проведемо емпіричне дослідження оцінювання частоти основного тону за виразом (6.32), у якому значення кореляційних коефіцієнтів $r_j^u\left(f\right)$ обчислювалися згідно виразу (6.37) за умови, що $L = 3$. Для забезпечення порівняльної бази сформуємо множину еталонних сигналів виду

$$u_i^{et} = \sum_{l=0}^{L^{et}} U_l^{et} \cos\left(2\pi l f_0^{et} j\Delta\right), \qquad (6.38)$$

де $f_0^{et} = \left[70, 75, \cdots, 330\right]$ – усереднений частотний діапазон присутності основного тону. Відповідно, в еталонну множину увійшли 53 сигнали виду (6.38). Кореляційні коефіцієнти $r_j^y\left(f_0\right)$ у виразі (6.32) розраховувалися саме для цих еталонних сигналів. Результати експерименту узагальнимо рисунком 6.1 у формі залежності відносної похибки $\delta\widehat{f}_0 = 100 \cdot \widehat{f}_0 - f_0^{et} \big/ f_0^{et}$ оцінювання частоти основного тону за виразом (6.32) від істинного значення f_0^{et}.

З рисунку 6.1 видно, що відносна похибка оцінювання частоти основного тону із використанням базової квазідетермінованої моделі ІГМС при $L = 3$ і врахуванням припущення (6.36) не перевищує 0,28%. Подальші дослідження, спрямовані на виявлення залежності похибки оцінювання від кількості

характеристичних параметрів L моделі ІГМС показали, що збільшення L дозволяє знизити $\delta\widehat{f}_0$ менше ніж на 0,1% (при $L=7$) при суттєвому зростанні обчислювальної складності.

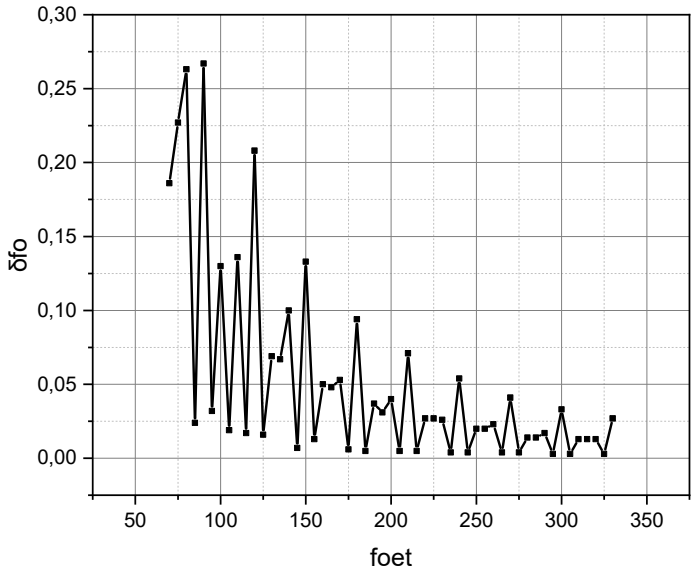


Рисунок 6.1 – Відносна похибка оцінювання частоти основного тону із використанням моделей ІГМС

Досягнута достовірність оцінки частоти основного тону перевищує результати, продемонстровані методом на основі вейвлет–перетворення [261] (на ~40%) і класичними амплітудним [227, 231], кореляційним [227, 231], спектральним [227, 231] методами (понад на порядок). На рисунку 6.2 наведено UML–діаграму активності для вищеописаного методу. Окрім множини кореляційних коефіцієнтів $R^y=\left\{r_j^y\right\}$, $j=\overline{1,J}$, обчислених для центрованого мовленнєвого сигналу y, вхідними параметрами методу є: f_d – частота дискретизації y, f_l – нижня межа досліджуваного частотного діапазону, f_h – верхня межа досліджуваного частотного діапазону, L – кількість характеристичних параметрів моделі ІГМС (за умовчанням $L=3$). Вихідним параметром методики є $\widehat{f}_0$ – оцінка частоти основного тону для мовленнєвого сигналу y.

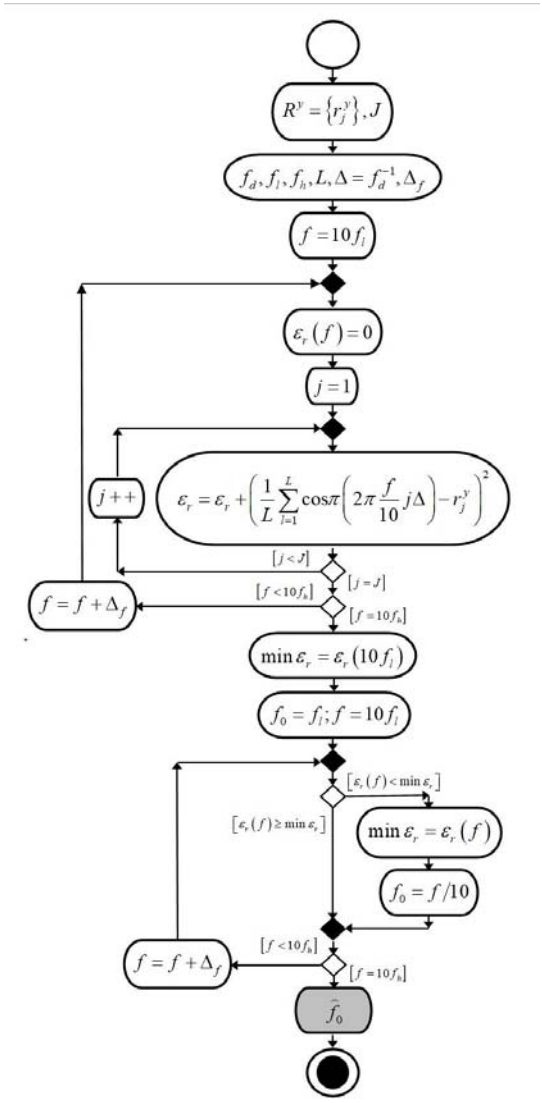


Рисунок 6.2 – UML–діаграма активності автоматизованої методики оцінювання частоти основного тону на основі моделі ІГМС

Відповідно до виразів (2.74), (2.75), досліджуючи ступінь затухання значення коефіцієнта кореляції $r(\tau)$ відносно нульових границь Бартлета можна зробити висновок щодо вокалізованості досліджуваного мовленнєвого сигналу. Враховуючи статистичний характер спостережень, кількісною оцінкою ступеню затухання слугуватиме значенням його умовної дисперсії як характеристики, що дозволяє врахувати усереднення стохастичної величини за її значеннями. Аналітичний матеріал для розрахунку дисперсії оцінки частоти основного тону отримаємо на основі мінімуму нев’язки між кореляційними коефіцієнтами емпіричного мовленнєвого сигналу і його представленням моделлю ІГМС.

Аналітично визначимо зміщення, розсіювання і дисперсію оцінки частоти основного тону як:

$$b\left(\hat{f}_0 \middle| f_0\right) = \left\langle \hat{f}_0 - f_0 \right\rangle, \tag{6.39}$$

$$V\left(\hat{f}_0 \middle| f_0\right) = \left\langle \left(\hat{f}_0 - f_0\right)^2 \right\rangle, \tag{6.40}$$

$$D\left(\hat{f}_0 \middle| f_0\right) = \left\langle \left(\hat{f}_0 - \left\langle \hat{f}_0 \right\rangle\right)^2 \right\rangle, \tag{6.41}$$

де $\langle\ \rangle$ – операція усереднення стохастичної компоненти за її значеннями. Наведені вище результати експериментів із множиною еталонних сигналів (6.38) довели, що зміщення оцінки частоти основного тону для різних значень L практично дорівнює нулю, тобто $\left\langle \hat{f}_0 \right\rangle \approx f_0$. Отже, розсіювання і дисперсія оцінки частоти основного тону практично рівні:

$$D\left(\hat{f}_0 \middle| f_0\right) \approx \left\langle \left(\hat{f}_0 - f_0\right)^2 \right\rangle. \tag{6.42}$$

Розкладемо нев'язку $\varepsilon(f)$ оцінки частоти основного тону в ряд Тейлора в околі істинного значення частоти основного тону f_0 і скористаємося двома першими членами отриманого розкладу:

$$\varepsilon(f)\Big|_{f=f_0} \approx \varepsilon(f_0) + (f - f_0)\frac{d\varepsilon(f)}{df}\Bigg|_{f=f_0} + \frac{1}{2}(f - f_0)^2 \frac{d^2\varepsilon(f)}{df^2}\Bigg|_{f=f_0}. \tag{6.43}$$

Для глобального мінімуму оцінки f_0 виконується умова

$$\frac{d\varepsilon(f)}{df}\Bigg|_{f=f_0} = 0. \tag{6.44}$$

Врахувавши вирази (6.42), (6.43), аналітично визначимо квадрат відхилення оцінки частоти основного тону від істинного значення:

$$\left(f - \hat{f}_0\right)^2 = 2\left(\varepsilon(f)\Big|_{f=f_0} - \varepsilon(f_0)\right) \Bigg/ \frac{d^2\varepsilon(f)}{df^2}\Bigg|_{f=f_0}. \tag{6.45}$$

Результати вищенаведених досліджень показали, що величина $\varepsilon(f)\big|_{f=f_0}$ змінюється зі зміною значення свого аргументу на крок $\pm\Delta_f$ відносно істинного значення f_0, що, з врахуванням виразів (6.42) і (6.45), дозволяє записати:

$$D^{\pm}\left(\hat{f}_0\middle|f_0\right)=2\left(\varepsilon\left(f_0\pm\Delta_f\right)-\varepsilon\left(f_0\right)\right)\Bigg/\left\langle\left.\frac{d^2\varepsilon(f)}{df^2}\right|_{f=f_0}\right\rangle. \tag{6.46}$$

Для розрахунку значення (6.46) представимо кореляційний коефіцієнт r_j^y мовленнєвого сигналу сумою квазідетермінованої $r_u\left(j\Delta,f_0\right)$ і стохастичної $r_n\left(j\Delta\right)$компонент,як це робилося у виразах (2.98), (2.103):

$$\begin{aligned} r_j^y \equiv r_j^y\left(f_0\right)\equiv r^y\left(j\Delta,f_0\right)=r_u\left(j\Delta,f_0\right)\frac{\sigma_u^2}{\sigma^2}+r_n\left(j\Delta\right)\frac{\sigma_n^2}{\sigma^2}= \\ =r_u\left(j\Delta\right)D_z^2\Big/\left(D_z^2+1\right)+r_n\left(j\Delta\right)\Big/\left(D_z^2+1\right), \end{aligned} \tag{6.47}$$

де $D_z=\sigma_u^2\big/\sigma_n^2$ – дисперсія рівня відношення «сигнал»/«шум».

Підставимо визначену виразом (6.32) величину $\varepsilon(f)$ у вираз (6.47) і виконавши операція диференціювання отримаємо вираз для обчислення другої похідної нев’язки в точці істинного значення частоти основного тону за умови $D_z>>1$:

$$\left\langle\left.\frac{d^2\varepsilon(f)}{df^2}\right|_{f=f_0}\right\rangle\approx 2\sum_{j=1}^{J}\left(\left.\frac{dr_j^u(f)}{df}\right|_{f=f_0}\right)^2. \tag{6.48}$$

Підставивши вираз (6.48) у вираз (6.46) отримаємо вираз для розрахунку умовної дисперсії оцінки частоти основного тону:

$$D^{\pm}\left(\hat{f}_0\middle|f_0\right)=\frac{\sum_{j=1}^{J}\left(r_j^y-r_j^u\left(f_0\pm\Delta_f\right)\right)^2-\sum_{j=1}^{J}\left(r_j^y-r_j^u\left(f_0\right)\right)^2}{\sum_{j=1}^{J}\left(\left.\frac{dr_j^u(f)}{df}\right|_{f=f_0}\right)^2}. \tag{6.49}$$

Аналіз (6.49) дозволяє стверджувати, що для підвищення достовірності оцінки частоти основного тону необхідно так обирати вид і усталені параметри моделі ІГМС u, щоб розраховуваний на її основі коефіцієнт кореляції $r_j^u\left(f\right)$:

- прямував до значення коефіцієнта кореляції r_j^y досліджуваного центрованого мовленнєвого сигналу y;
- швидко змінював своє значення в околі значення частоти основного тону f_0.

Підставимо вираз (6.49) у вираз (6.37) і отримаємо вираз

$$D^{\pm}\left(\hat{f}_0\middle|f_0\right)=\left(\sum_{j=1}^{J}\left(r_j^y-\frac{1}{L}\sum_{l=1}^{L}\cos\left(2\pi l\left(f_0\pm\Delta_f\right)j\Delta\right)\right)^2-\right.$$
$$\left.-\sum_{j=1}^{J}\left(r_j^y-\frac{1}{L}\sum_{l=1}^{L}\cos\left(2\pi l f_0 j\Delta\right)\right)^2\right)\left(\sum_{j=1}^{J}\left(\frac{1}{L}\sum_{l=1}^{L}\left(2\pi l j\Delta\right)\sin\left(2\pi l f_0 j\Delta\right)\right)^2\right)^{-1}, \tag{6.50}$$

на основі якого аналітично сформулюємо усереднене середньоквадратичне відхилення оцінки частоти основного тону:

$$\bar{\sigma}\equiv\bar{\sigma}\left(\hat{f}_0\middle|f_0\right)=\sqrt{\bar{D}\left(\hat{f}_0\middle|f_0\right)}=\sqrt{\frac{1}{2}\left(D^{+}\left(\hat{f}_0\middle|f_0\right)+D^{-}\left(\hat{f}_0\middle|f_0\right)\right)}. \tag{6.51}$$

Відзначимо, що для візуалізованого на рисунку (3.1) мовленнєвого сигналу y, оцифрованого із $f_d=6000$ Гц, в результаті вищеописаного експерименту знайдено оцінку частоти основного тону $\hat{f}_0=155{,}2$ Гц. Скориставшись моделлю ІГМС можна оцінити максимальну кількість несних гармонік у досліджуваному мовленнєвому сигналі як $L_{\max}=\left\lfloor f_h=0.5f_d/\hat{f}_0\right\rfloor=19$. Використаємо вираз (6.51) для емпіричного дослідження залежності значення усередненого середньоквадратичного відхилення оцінки частоти основного тону у сигналі y від кількості враховуваних у його описі моделлю ІГМС характеристичних параметрів L.

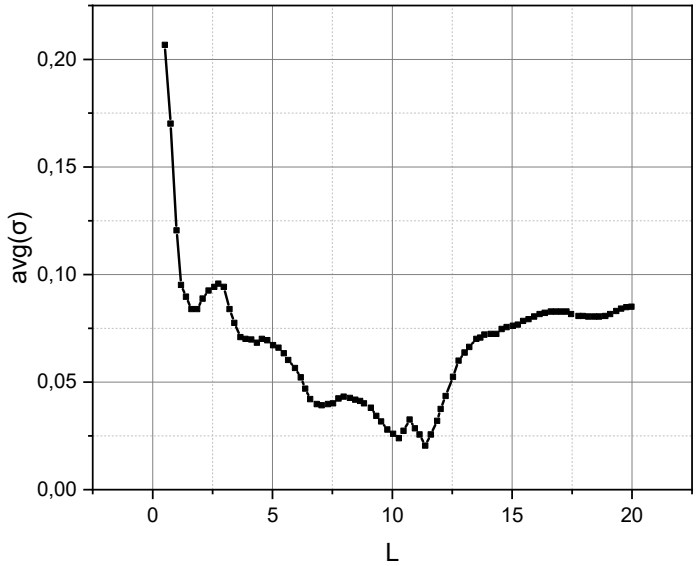


Рисунок 6.3 – Залежність усередненого середньоквадратичного відхилення оцінки частоти основного тону від кількості характеристичних параметрів моделі ІГМС.

З результатів, наведених на рисунку 6.3 видно, що найдостовірнішу оцінку частоти основного тону запропонована методика показує при кількості характеристичних параметрів моделі ІГМС $10 \le L \le 13$. Проте, ще раз відзначимо, що із збільшенням характеристичних параметрів моделі ІГМС складність розрахунків оцінки частоти основного тону запропонованою методикою зростає стрімко нелінійно.

6.3 Методики оцінювання частоти основного тону, сформульовані в контексті апріорної інформації щодо усталених параметрів моделей ІГМС

Якщо на виході цільової математичної моделі є достатньо адекватної інформації, щоб отримати апостеріорний розподіл оцінюваного параметру, то спираючись на таку математичну модель можна синтезувати оптимальні методики і алгоритми відповідного призначення. Нехай задача дослідження полягає в оцінюванні значення характеристичного параметру f_0 у квазідетермінованому мовленнєвому сигналі $u(t, f_0)$ із шумом $n(t)$. В умовах апріорної невизначеності оцінюваного параметру доцільним є застосування методу максимальної правдоподібності [352] як оптимального методу оцінки.

Формалізуємо оцінювання частоти основного тону f_0 методом максимальної правдоподібності спираючись на математичну модель мовленнєвого сигналу:

$$\xi(t, f_0) = u(t, f_0) + n(t), \tag{6.52}$$

де квазідетермінований сигнал $u(t, f_0)$ представлено моделлю ІГМС виду (2.1) або (2.24), а $n(t)$ – гасівський випадковий процес із нульовим середнім значенням і функцією кореляції виду

$$R(t_1, t_2) = N_0 \delta(t_1 - t_2)/2, \tag{6.53}$$

де N_0 – однобічна спектральна щільність потужності шуму, $\delta(\ )$ – δ– функція Дірака. Оскільки невідомий параметр f_0 визначається в результаті опрацювання реалізації випадкового сигналу (6.52), то, відповідно до положень математичної статистики, оцінка f_0 також є стохастичною величиною. Отже, найповніша інформація щодо значень параметр f_0 міститься у апостеріорній щільності імовірності $W_{ps}(f) = W\left(f \middle| \xi(t, f_0)\right)$, тобто щільності імовірності параметру f за умови реалізації $\xi(t, f_0)$. Визначимо апріорну щільність імовірності $W_{pr}(f)$ на основі апостеріорної $W_{ps}(f)$:

$$W_{ps}(f) = K W_{pr}(f) \Lambda(f), \tag{6.54}$$

де $\Lambda(f)$ – функціонал відношення правдоподібності f, K – нормувальний коефіцієнт. Отримати оцінку параметру f за апостеріорним розподілом можна баєйсівським методом, який мінімізує усереднені втрати від неточного визначення оцінюваного параметру. Якщо розподіл $W_{pr}(f)$ невідомий, то оцінку можна отримати на основі інформації про максимум $\Lambda(f)$. Для сигналу (6.52), функція кореляції шуму в якому описується (6.52), з врахуванням [270, 352], логарифмічний функціонал відношення правдоподібності для параметру f визначимо виразом:

$$M(f) = \frac{2}{N_0} \int_0^T \xi(t, f_0) u(t, f) dt - \frac{1}{N_0} \int_0^T u^2(t, f) dt, \tag{6.55}$$

де T – цензурований період спостереження.

н.

На основі (6.55) оцінка максимальної правдоподібності параметру f визначається виразом

$$\widehat{f}_0 = \arg\sup M\left(f\right). \tag{6.56}$$

Виділимо з виразу (6.55) перший доданок, залежний від $\xi\left(t, f_0\right)$:

$$M_0\left(f\right) = \frac{2}{N_0}\int_0^T \xi\left(t, f_0\right) u\left(t, f\right) dt. \tag{6.57}$$

У попередньому підрозділі емпірично встановлено, що впливом модулювального коливання на достовірність оцінки частоти основного тону можна знехтувати, тому опорний сигнал $u\left(t, f_0\right)$ визначимо у формалізмі моделі ІГМС виду (2.1):

$$u\left(t, f\right) = \sum_{l=1}^{L} U_l \cos\left(2\pi l f t + \varphi_l\right). \tag{6.58}$$

Нехай, наприклад, в результаті попереднього спектрального аналізу значення амплітуд U_l і початкових фаз φ_l визначено апріорі. Тоді UML–діаграму активності розрахунку оцінки частоти основного тону (6.56) для вхідного мовленнєвого сигналу (6.52) на основі логарифмічного функціоналу відношення правдоподібності (6.55) представимо на рисунку 6.4. Блок *Інт./Сум.* на діаграмі 6.4 реалізує операцію обчислення інтегралу Рімана–Стілтьєса для вхідного сигналу. Якщо вхідний сигнал аналоговий: $\xi\left(t, f_0\right)$, то реалізується операція інтегрування: $\int_0^T \Xi\left(t\right) dt$. Якщо вхідний сигнал дискретний: $\xi\left(i\Delta, f_0\right) = \xi_i\left(f_0\right)$, то реалізується операція підсумовування: $\Delta\sum_{i=0}^{N-1} \Xi\left(i\Delta\right)$. У першому випадку сигнал $u\left(t, f\right)$ визначимо виразом (6.58), у другому приймаємо $u_i\left(f\right) \equiv u\left(i\Delta, f\right)$.

На рисунку 6.5 представлено залежність нормованого на максимальне значення логарифмічного функціоналу відношення правдоподібності $M_n\left(f\right)$ від

частоти f для мовленнєвого сигналу, візуалізованого на рисунку 3.1. При обчисленні значень $M_n(f)$ опорний сигнал $u(t,f)$ виду (6.58) генерувався при $L=3$ і апріорних значеннях $U_l=1$, $\varphi_l=0$, $l=\overline{1,L}$.

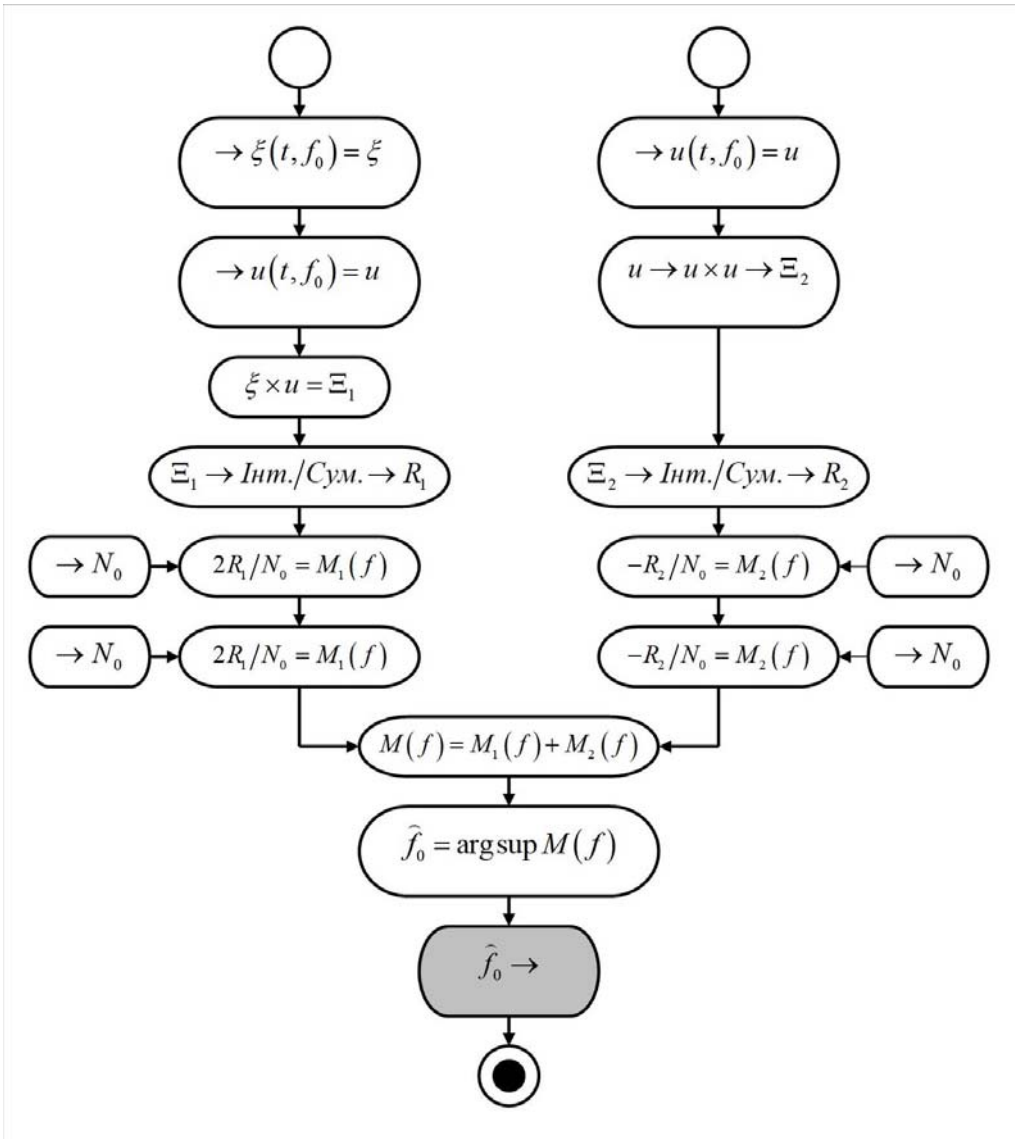


Рисунок 6.4 – UML–діаграму активності розрахунку оцінки частоти основного тону при визначених апріорно усталених параметрах моделі ІГМС

Як видно з рисунку 6.5, глобальний максимум значення $M_n(f)$ однозначно спостерігається при $f=f_0=155$ Гц, що повністю співпадає із результатами обчислення частоти основного тону для цього сигналу, представленими у попередньому підрозділі.

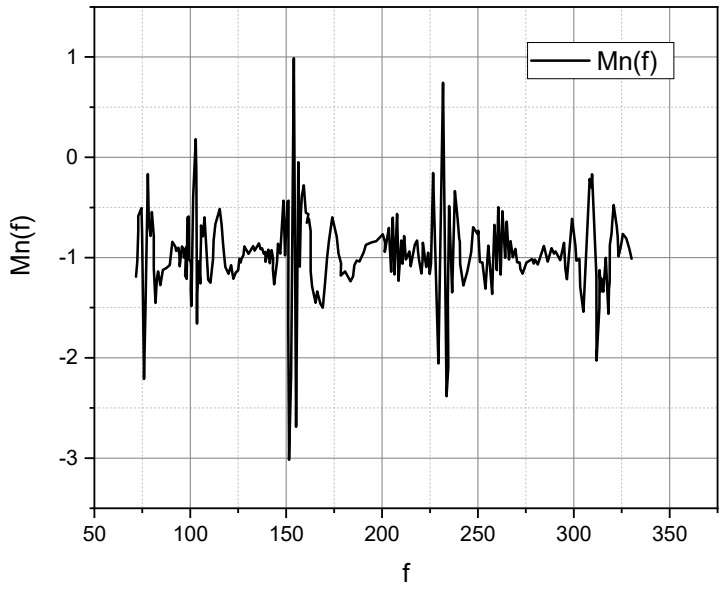


Рисунок 6.5 – Залежність нормованого на максимальне значення логарифмічного функціоналу відношення правдоподібності від частоти для сигналу, візуалізованого на рисунку 3.1.

Узагальнена виразом (6.56) методика знаходження оцінки частоти основного тону за позицією максимуму логарифмічного функціоналу відношення правдоподібності (6.57) передбачає наявність апріорної інформації щодо значень усталених параметрів опорного сигналу $u(t, f_0)$, як це видно з виразу (6.58). Припустимо, що апріорна інформація щодо значень U_l, φ_l, $l = \overline{1, L}$, відсутня. Фактично, це означає, що кількість характеристичних параметрів моделі ІГМС виду (2.1) зросла на $2L$. Врахуємо це представивши модель (6.58) у вигляді

$$u(t, f_0) = \sum_{l=1}^{L} \left(x_l \cos(2\pi l f_0 t) + y_l \sin(2\pi l f_0 t) \right), \tag{6.59}$$

де $x_l = U_l \cos(-\varphi_l)$, $y_l = U_l \sin(-\varphi_l)$.

Врахуємо вираз (6.59) при визначенні логарифмічного функціоналу відношення правдоподібності $M(f)$ для параметру f у виразі (6.55):

$$M(f) = \frac{N_0}{2T} \left(\sum_{l=1}^{L} \left(X_l(f) \right)^2 + \sum_{l=1}^{L} \left(Y_l(f) \right)^2 \right). \tag{6.60}$$

Доданки $X_l(f)$ і $Y_l(f)$ визначимо виразами

$$X_l(f)=\frac{2}{N_0}\int_0^T \xi(t,f_0)\cos(2\pi lft)dt,$$
$$Y_l(f)=\frac{2}{N_0}\int_0^T \xi(t,f_0)\sin(2\pi lft)dt. \quad (6.61)$$

Оцінити ступінь збіжності частоти f_{ij} гармонік несного коливання, кожна з яких визначається параметрами U_i, φ_j, $i,j=\overline{1,L}$, із сигналом основного тону із частотою f_0 можна за значеннями нормованої взаємної функції невизначеності [270], представленої виразом

$$\Psi_{ij}(f_1,f_2)=\sqrt{\left(S_{ij}^x(f_1,f_2)^2+\left(S_{ij}^y(f_1,f_2)^2\right)\right)},\ i,j=\overline{1,L}. \quad (6.62)$$

де значення сигнальних функцій $S_{ij}^x(f_1,f_2)$ і $S_{ij}^x(f_1,f_2)$ характеризують, відповідно, доданки $X_l(f)$ і $Y_l(f)$ з виразу (6.60). Враховуючи кореляційну природу інтегралів (6.61), нам треба знайти гармоніки, для яких виконується умова

$$\Psi_{ij}(f_0,f_0)<<1,\ i\neq j,\ i,j=\overline{1,L}. \quad (6.63)$$

Узагальнені аналітичні вирази для розрахунку сигнальних функцій виду $S_{ij}^x(f_1,f_2)$ і $S_{ij}^x(f_1,f_2)$ для матриці взаємної функції невизначеності $\Psi_{ij}(f_1,f_2)$, $i,j=\overline{1,L}$, виведено у [271]. Адаптуємо їх для задачі оцінки частоти основного тону сингалу (6.58):

$$S_{ij}^x(f_1,f_2)\approx\frac{\cos\left(2\pi(jf_2-if_1)T\right)-1}{2\pi(jf_2-if_1)T},$$
$$S_{ij}^y(f_1,f_2)\approx\frac{\sin\left(2\pi(jf_2-if_1)T\right)-1}{2\pi(jf_2-if_1)T}. \quad (6.64)$$

Підставимо вирази (6.64) у вираз (6.62) і отримаємо

$$\Psi_{ij}(f_1,f_2)=\frac{\sin\left(\pi(jf_2-if_1)T\right)}{\pi(jf_2-if_1)T}=\mathrm{sinc}\left(\pi(jf_2-if_1)T\right). \quad (6.65)$$

Перепишемо умову (6.63) з врахуванням виразу (6.65):

$$\Psi_{ij}\left(f_0,f_0\right)=\frac{\sin\left(\pi\left(j-i\right)f_0T\right)}{\pi\left(j-i\right)f_0T}=\mathrm{sinc}\left(\pi\left(j-i\right)f_0T\right). \qquad (6.66)$$

Враховуючи, що нерівність $\left|\mathrm{sinc}(\pi x)\right|<0{,}1<<1$ виконується при $x\geq 2{,}69$, умова (6.63) для визначеної виразом (6.66) функції $\Psi_{ij}\left(f_0,f_0\right)$ виконуватеметься при $f_0T=T/T_0\geq 2{,}69\vee i\neq j$. Для виконання умови (6.63) необхідно, щоб цензурована тривалість спостереження T досліджуваного сигналу перевищувала значення періоду основного тону в $2{,}69$ рази. Так як діапазон частот, де спостерігається основний тон обмежено: $\left[f_0^l=70, f_0^h=330\right]$, (Гц), то діапазон значень періоду основного тону буде $\left[T_0^l=3{,}3, T_0^h=14{,}3\right]$, (мс). Вибираючи цензурований період $T=2{,}69T_0^h\approx 38{,}5$ мс ми гарантуватимемо присутність несних гармонік у досліджуваному сигналі. Узагальнимо сказане представивши на рисунку 6.6. UML–діаграму активності для методики розрахунку оцінки частоти основного тону (6.56) для вхідного мовленнєвого сигналу (6.52) на основі логарифмічного функціоналу відношення правдоподібності (6.60).

Блок *Інт./Сум.* на діаграмі 6.6 реалізує операцію обчислення інтегралу Рімана–Стілтьєса для вхідного сигналу. Якщо вхідний сигнал аналоговий: $\xi\left(t,f_0\right)$, то реалізується операція інтегрування: $\int_0^T \Xi\left(t\right)dt$. Якщо вхідний сигнал дискретний: $\xi\left(i\Delta,f_0\right)=\xi_i\left(f_0\right)$, то реалізується операція підсумовування: $\Delta\sum_{i=0}^{N-1}\Xi\left(i\Delta\right)$. У першому випадку сигнал $u\left(t,f\right)$ має вигляд (6.58), у другому приймаємо $u_i\left(f\right)\equiv u\left(i\Delta,f\right)$. Аналітичний вигляд неперервних опорних сигналів, згаданих на діаграмі такий: $u_{x_1}\left(t,f\right)=\cos\left(2\pi ft\right)$, …, $u_{x_L}\left(t,f\right)=\cos\left(2\pi Lft\right)$; $u_{y_1}\left(t,f\right)=\sin\left(2\pi ft\right)$, …, $u_{y_L}\left(t,f\right)=\sin\left(2\pi Lft\right)$. Дискретне їх представлення таке: $u_{x_1}\left(i\Delta,f\right)=\cos\left(2\pi fi\Delta\right)$, …, $u_{x_L}\left(i\Delta,f\right)=\cos\left(2\pi Lfi\Delta\right)$; $u_{y_1}\left(i\Delta,f\right)=\sin\left(2\pi fi\Delta\right)$, …, $u_{y_L}\left(i\Delta,f\right)=\sin\left(2\pi Lfi\Delta\right)$. На рисунку 6.7 представлено залежність нормованого на максимальне значення логарифмічного функціоналу відношення

правдоподібності $M_n(f)$ від частоти f мовленнєвого сигналу, візуалізованого на рисунку 3.1. При обчисленні значень $M_n(f)$ опорний сигнал $u(t,f)$ виду (6.58) генерувався при $L=3$. Апріорна інформація про значення U_l, φ_l, $l=\overline{1,L}$, була відсутня.

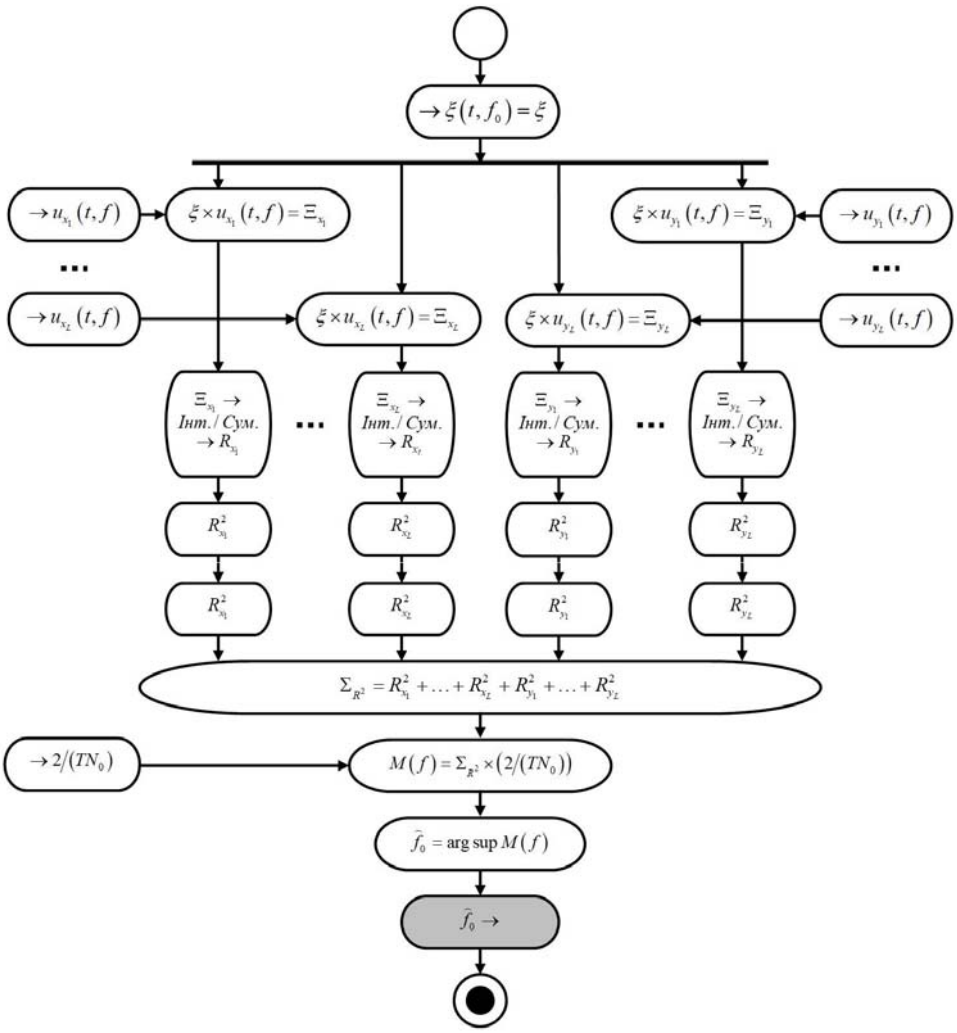


Рисунок 6.6 – UML–діаграму активності методики розрахунку оцінки частоти основного тону при невизначених усталених параметрах моделі ІГМС.

Як видно з рисунку 6.7, глобальний максимум значення $M_n(f)$, однозначно спостерігається при $f=f_0=155$ Гц, що повністю співпадає із результатами оцінювання частоти основного тону для цього ж сигналу, представленими на рисунку 6.5, де нормоване значення логарифмічного функціоналу відношення правдоподібності $M_n(f)$ розраховувалося за виразом (6.57).

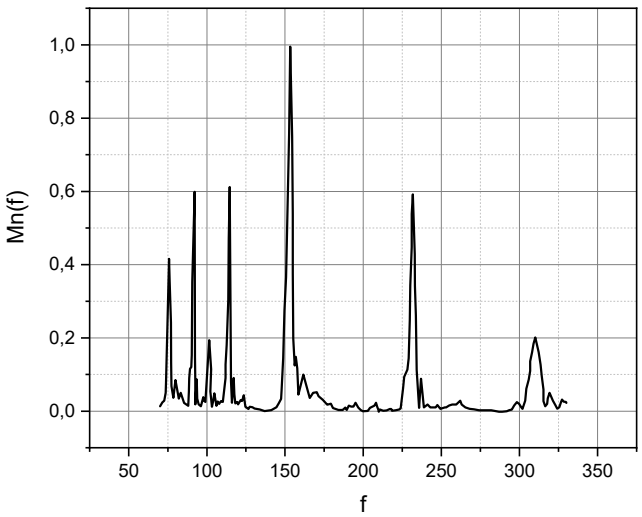


Рисунок 6.7 – Залежність нормованого на максимальне значення логарифмічного функціоналу відношення правдоподібності (6.60) від частоти для сигналу, візуалізованого на рисунку 3.1.

Отже, у підрозділі формалізовано і апробовано методики знаходження оцінки частоти основного тону за позицією максимуму логарифмічного функціоналу відношення правдоподібності (6.57) або (6.60), залежно від того є апріорна інформації щодо значень усталених параметрів формалізованого моделлю ІГМС опорного сигналу $u(t, f_0)$ чи така інформація відсутня. Тестування запропонованих методик у порівнянні із запропонованими у попередньому підрозділі удосконаленими кореляційними і спектральним методами оцінки частоти основного тону на єдиному емпіричному мовленнєвому сигналі, візуалізованому на рисунку 3.1, довела адекватність і достовірність представлених у підрозділі методик. Втім, запропонованим методикам властива обчислювальна складність, яка із зростанням кількості враховуваних характеристичних параметрів моделі ІГМС зростає стрімко нелінійно.

6.4 Реалізація інформаційної технології автентифікації суб’єкта за індивідуальністю голосу в мовленнєвому сигналі

Актуальним сьогодні програмним і апаратним засобам АСГ [241–249] властиве обмеження надійності з причини помилок, які виникають на етапі

параметризації мовленнєвого сигналу і відбиваються на достовірності значень характеристичних параметрів за якими здійснюється розпізнавання особи. Зокрема, типовими є:

- помилки у визначенні глобального максимуму спектру потужності з причини наявності на інтервалі пошуку локальних екстремумів;
- помилки у виборі виду і параметрів функції нормалізації, на значення якої на етапі попереднього оброблення кожного фрейму мовленнєвого сигналу множать спектр потужності останнього;
- помилки емпіричного вибору вагових коефіцієнтів ступеню впливу кожного характеристичного параметру на значення міри роздільності порівнюваних емпіричного і еталонного образів мовленнєвого сигналу;
- велика кількість характеристичних параметрів, незалежність і значимість яких втрачається;
- характеристика індивідуальності джерела мовленнєвого сигналу усередненими параметрами основного тону, ігноруючи гармонійні властивості цієї характеристики;
- ігнорування семантичної складової мовленнєвого сигналу;
- низька надійність АСГ в умовах шумного акустичного оточення;
- зростання похибки першого роду, пов’язане із варіативністю вимови однакових за вмістом і особою суб’єкта мовленнєвих сигналів.

Запропоновані у дисертаційній роботі теоретичні і прикладні наукові результати орієнтовані на усунення вищеописаних помилок з метою підвищення надійності АСГ за рахунок достовірного параметричного представлення оцінки основного тону і її гармонік, розрахунок якої здійснюється із автоматичною або автоматизованою адаптацією параметрів вживаної моделі ІГМС до рівня відношення «сигнал»/«шум» в емпіричному мовленнєвому сигналі. Зокрема, апаратно–орієнтоване підвищення завадостійкості АСГ досягається діленням значень розрахованих характеристичних параметрів моделі ІГМС на еталон АЧХ мікрофону. Згаданий еталон пов’язано оберненою квадратичною залежністю із частотним коефіцієнтом передавання потужності мікрофона. Цей частотний

коефіцієнт є узагальненням результатів експерименту з посегментного ділення значень спектральної щільності потужності фонограми тестового мовленнєвого сигналу, отриманої за допомогою оцінюваного мікрофону, на відповідні значення спектральної щільності потужності фонограми цього ж сигналу, отриманої за допомогою еталонного мікрофону із рівномірною АЧХ. Описану процедуру візуалізовано на рисунку 6.8. Програмно–орієнтоване підвищення завадостійкості АСГ досягається нормалізацією значень розрахованих характеристичних параметрів моделі ІГМС із залученням даних спеціалізованої універсальної фонової моделі, отриманої в результаті узагальнення методом максимальної правдоподібності параметризованих фонограм мовленнєвого матеріалу різних мовців, записаних в лабораторних умовах із контрольованим рівнем відношення «сигнал»/«шум», що описано у розділі 4.

Рисунок 6.8 – Структурна схема процедури визначення еталону АЧХ мікрофону.

Представлені у дисертаційні роботі методи параметризації мовленнєвого сигналу спираються на математичні моделі ІГМС, синтез яких характеризується повнотою і коректністю математичних операцій, здійснюваних в парадигмі

математичного апарату теорії імовірності і математичної статистики та цифрового оброблення сигналів, а адекватність доведена емпірично із застосуванням математичного апарату теорії планування експерименту і математичної статистики. Застосування моделей ІГМС дозволяє описати сегментовану фонограму досліджуваного мовленнєвого сигналу множиною таких характеристичних параметрів, як значення частоти основного тону і амплітуди несних гармонік на частоті основного тону і її обертонів. Оцінка частоти основного тону і амплітуд несних гармонік обчислюється в результаті мінімізації нев'язки між коефіцієнтами кореляції досліджуваного сигналу і моделі. Методики розрахунку цих оцінок заснований на методі найменших квадратів. Процедура формування множини характеристичних параметрів моделі ІГМС для досліджуваного мовленнєвого сигналу візуалізована на рисунку 6.9.

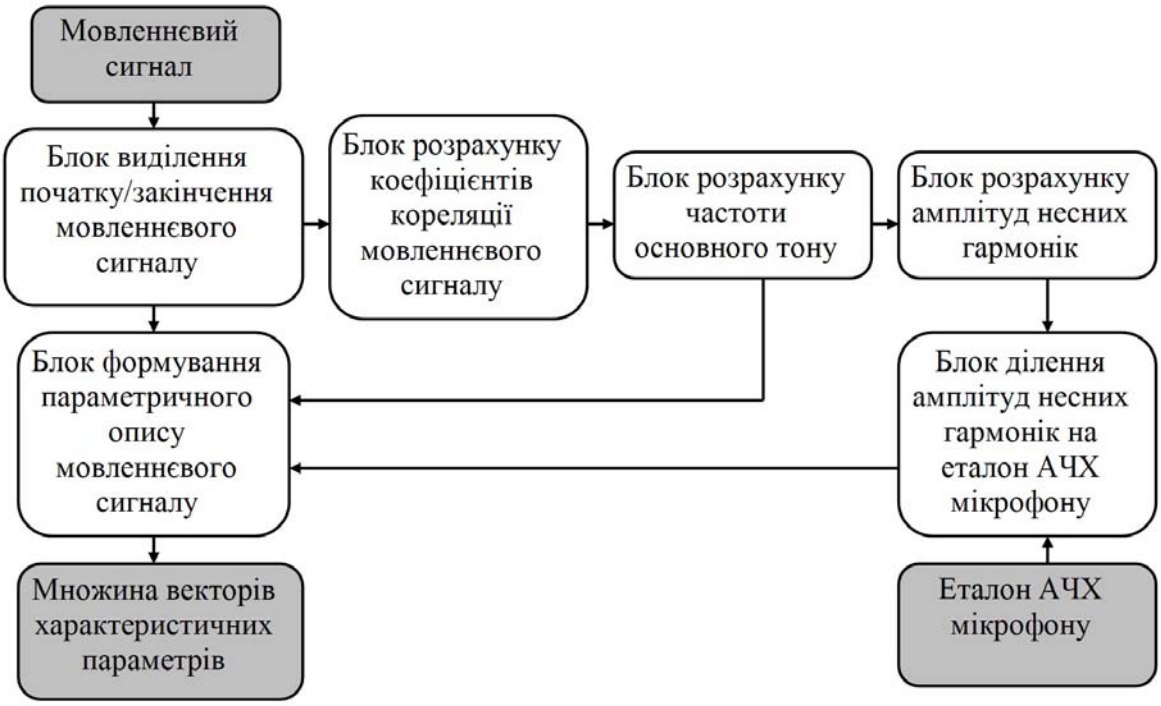


Рисунок 6.9 – Структурна схема процедури параметризації мовленнєвого сигналу в формалізмі моделей ІГМС.

Порівняння характеристичних параметрів емпіричного мовленнєвого сигналу із попередньо розрахованими еталонними здійснюється за величиною

міри розрізнення (3.43), а поріг прийняття рішень (3.46) обчислюється з врахуванням рівня відношення «сигнал»/«шум» в емпіричному мовленнєвому сигналі. На рисунку 6.10 представлено структурну схему інформаційної технології автентифікації суб'єкта на основі ІГМС.

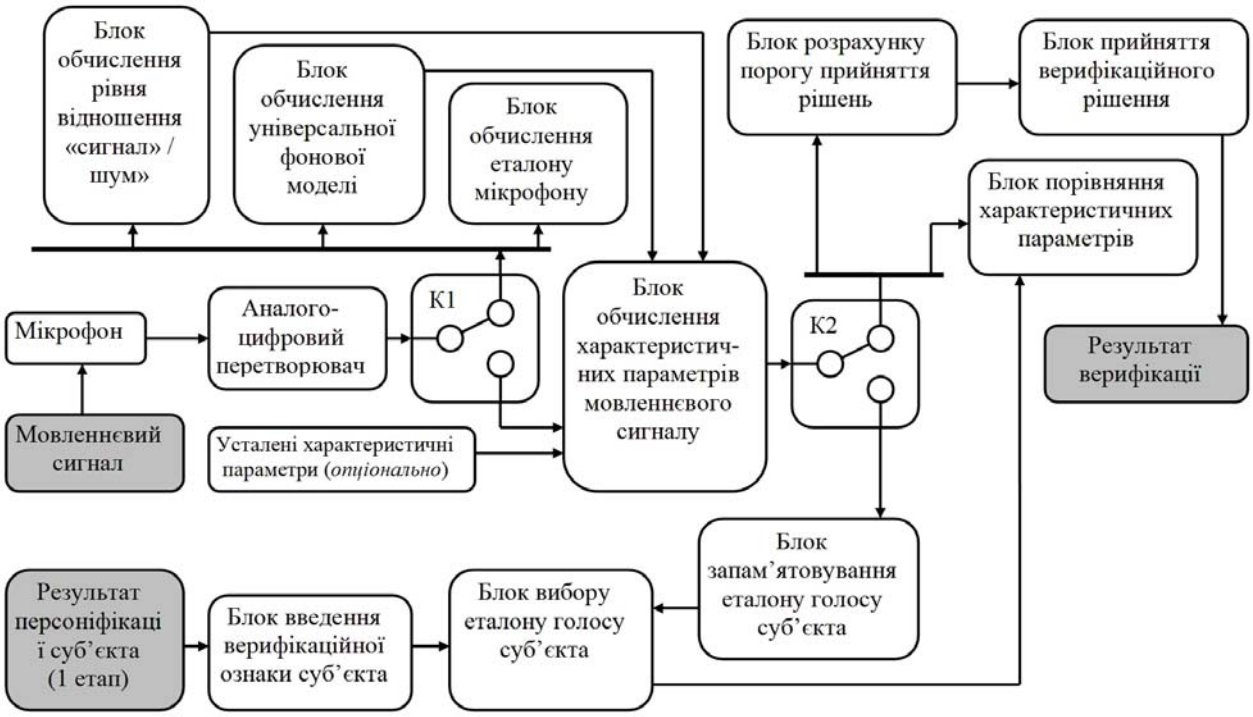


Рисунок 6.10 – Структурна схема інформаційної технології автентифікації суб'єкта на основі ІГМС.

Представлені на рисунку 6.10 комутатор К1 переключає систему в режим налаштування параметрів (вверх) чи в режим верифікації/навчання (вниз). Отже, система АСГ може функціонувати в режимах навчання, верифікації і налаштування параметрів. В режимі навчання персоніфіковані фонограми парольних мовленнєвих сигналів, утворені в результаті послідовного функціонування мікрофону і аналого–цифрового перетворювача, потрапляють до блоку обчислення характеристичних параметрів мовленнєвого сигналу, обчислена множина яких передається до блоку запам'ятовування еталону голосу суб'єкта, адже в режимі навчання комутатор К2 замкнено у нижній позиції. Для кожного суб'єкта і парольного мовленнєвого сигналу створюється унікальний еталон.

Реалізація описаної у підрозділі 5.1 концепції двохетапної схеми верифікації передбачає, що на першому етапі суб’єкт, який автентифікується, персоніфікується за схемою «логін»/«пароль». Лише після успішного подолання першого етапу суб’єкт, який автентифікується, допускається до другого етапу – верифікації за індивідуальними характеристиками голосу. Зв'язок першого і другого етапу схеми верифікації здійснює блок введення верифікаційної ознаки суб’єкта, який передає ідентифікатор суб’єкта блоку вибору еталону голосу суб’єкта для встановлення зв’язку «ідентифікатор суб’єкта»–«ідентифікатор еталону голосу суб’єкта»–«ідентифікатор семантики парольної фрази». Далі ця інформація як множина кортежів ідентифікаторів передається блоку запам’ятовування голосу суб’єкта. В режим верифікації система переводиться переключенням комутатора К2 в верхню позицію. Суб’єкт, який успішно подолав перший етап схеми автентифікації, виголошує у мікрофон запропоновану системою верифікації парольну фразу, семантичний зміст якої сформовано системою з врахуванням інформації від блоку запам’ятовування голосу суб’єкта. Виголошений у мікрофон парольний мовленнєвий сигнал зазнає аналого–цифрового перетворення і параметризується у блоці обчислення характеристичних параметрів мовленнєвого сигналу, сутність операцій здійснюваних у якому розкрито структурною схемою на рисунку 6.9. Процедура обчислення кореляційних коефіцієнтів у відповідному блоці з рисунку 6.9 відбувається за виразом (2.7) для квазідетермінованого варіанту моделі ІГМС чи за виразом (2.58) для стохастичного варіанту моделі ІГМС. Розраховані значення кореляційних коефіцієнтів використовуються у блоці розрахунку частоти основного тону, який реалізує описану в підрозділі 6.3 методику знаходження оцінки частоти основного тону за позицією максимуму логарифмічного функціоналу відношення правдоподібності (6.57) або (6.60), залежно від того є апріорна інформації щодо значень усталених параметрів формалізованого моделлю ІГМС опорного сигналу $u(t, f_0)$ (автоматизований варіант) чи така інформація відсутня (автоматичний варіант). Розраховані оцінка частоти основного тону і значення кореляційних коефіцієнтів передаються блоку

розрахунку амплітуд несних гармонік де реалізується методика характеристичних параметрів при описі мовленнєвих сигналів моделями ІГМС, представлена у підрозділі 6.1, а саме, на основі розрахованих елементів матриць (6.10), (6.11) розраховується вираз (6.21). Використовувана для розрахунку елементів матриць (6.10), (6.11) характеристична матриця (6.18) розраховується залежно від обраної моделі ІГМС (2.1), (2.24), (2.46), (2.64) за виразами (2.15), (2.29), (2.63), (2.71), відповідно. Завершує процедуру параметризації мовленнєвого сигналу блок ділення амплітуд несних гармонік на еталон АЧХ мікрофону: $U_l^{norm} = \widehat{U}_l \Big/ \sqrt{K_P(\omega_l)}$, де $\widehat{U}_l$, U_l^{norm} – вихідне і нормоване значенням l–ї несної гармоніки, $l = \overline{1,L}$, $\omega_l = 2\pi l f_0$, $K_P(\omega) = \left|K(j\omega)\right|^2$ – частотний коефіцієнт передавання потужності мікрофону. Отже, кожен вектор множини характеристичних параметрів містить $V_i^P = \left\{f_0, U_l^{norm}\right\}$, $l = \overline{1,L}$, де i – індекс сегменту–фрейму, f_0 – частота основного тону, U_l^{norm} – нормована амплітуда l–ї несної гармоніки. Кількість векторів дорівнює кількості сегментів–фреймів на які розбивається досліджуваний мовленнєвий сигнал. Спираючись на результати досліджень, представлених у підрозділі 6.3, при частоті дискретизації вхідного мовленнєвого сигналу $f_d = 6000$ Гц для гарантованого обчислення всіх складових V_i^P тривалість фрейму обираємо $T = 40$ мс. В режимі верифікації комутатор К2 замикається у верхньому положенні, а у блоці порівняння характеристичних параметрів для персоніфікованого суб’єкта, який верифікуються, здійснюється порівняння множини векторів характеристичних параметрів, екстрагованих з парольного мовленнєвого сигналу, із множини векторів характеристичних параметрів, яка є еталоную для особи, з якою прагне себе ототожнити суб’єкт, який верифікуються. Результат порівняння згаданих множин втілюється у значення міри розрізнення (3.43), яке додатково порівнюється з порогом прийняття рішень D_0, який обчислюється за виразом (3.46). Відзначимо, що при обчисленні значення порогу, згідно матеріалу підрозділу 3.2, враховується рівень відношення «сигнал»/«шум» (2.90) у емпіричному мовленнєвому сигналі і один із

обраних варіантів орієнтації міри розрізнення на: мінімізацію похибки першого роду α, мінімізацію похибки другого роду β, мінімізацію усередненої похибки $(\alpha+\beta)/2$. Переведення комутатора К1 у верхнє положення переводить систему АСГ в режим налаштування усталених параметрів, в якому можна вручну задати значення усталених параметрів моделей ІГМС (2.1), (2.24), (2.46) і (2.64) та ініціювати процедуру визначення еталону АЧХ мікрофону, представлену на рисунку 6.8. Якщо функції перших двох блоків були щойно описані, то блок розрахунку середнього значення спектральної щільності потужності реалізує посегментне обчислення відповідного параметру за виразами (Б.1), (Б.2) для емпіричного мовленнєвого сигналу s^{emp}, семантика якого співпадає із семантикою еталонного мовленнєвого сигналу s^{et} записаного мікрофоном з рівномірною АЧХ в лабораторних умовах. Далі у блоці ділення реалізується відповідна операція: $K_P(\omega)=S_N^{emp}(\omega)/S_N^{et}(\omega)$, де $S_N^{emp}(\omega)$, $S_N^{et}(\omega)$ – нормована спектральної щільності потужності емпіричного і еталонного мовленнєвих сигналів, відповідно. Значення еталону АЧХ мікрофону розраховується за виразом $\left|K(j\omega)\right|=\sqrt{K_P(\omega)}$. Подальше застосування цього параметру таке: якщо ідентифікатор особи, яка верифікуються співпадає із ідентифікатором особи, для якої обчислено еталон АЧХ мікрофону, то обчислені з емпіричного мовленнєвого сигналу амплітуди несних гармонік діляться на відповідні компоненти АЧХ мікрофону. Таким чином ми позбавляємося впливу мікрофону на значення відповідних характеристичних параметрів.

Узагальнимо вищесказане синтезувавши UML-діаграму активності інформаційну технологію АСГ у методології ІГМС, представленої профільними математичними моделями з розділу 2, та методами і методиками на їх основі в розділах 3, 4, 6. Відповідний результат наведений на рисунку 6.11. Індивідуальність голосу в представленій інформаційній технології визначається такими характеристичними параметрами, як частота основного тону f_0 і амплітуди несних гармонік U_l, $l=\overline{1,L}$.

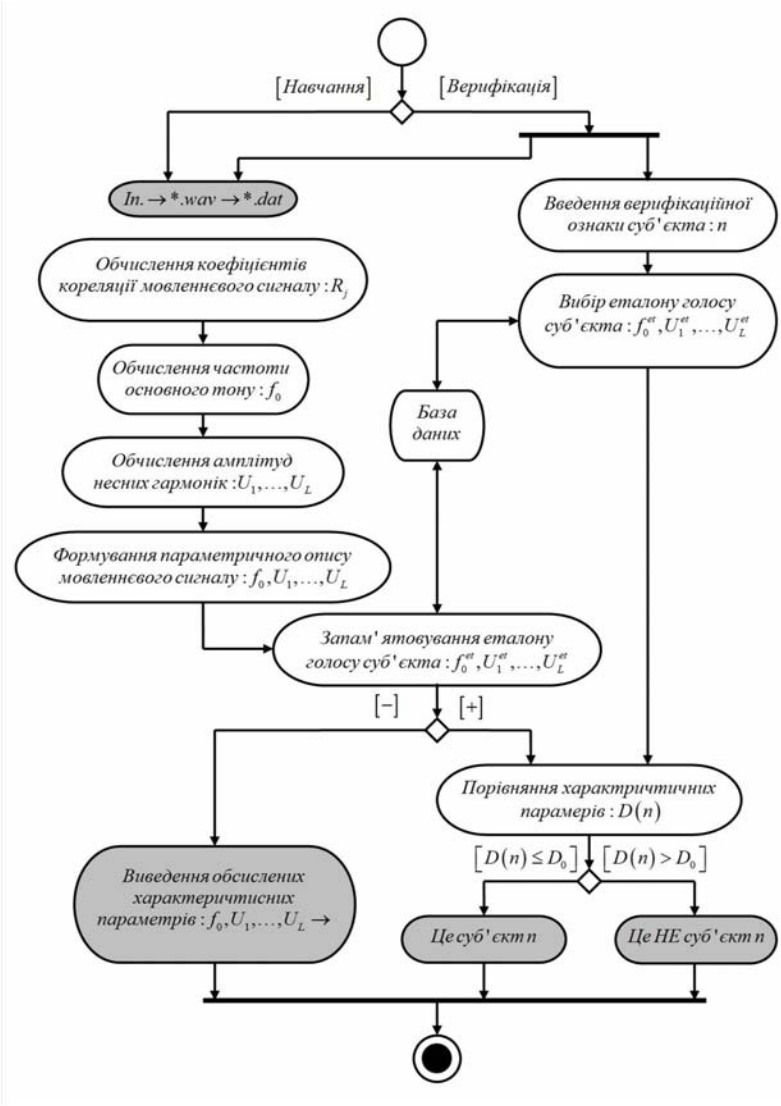
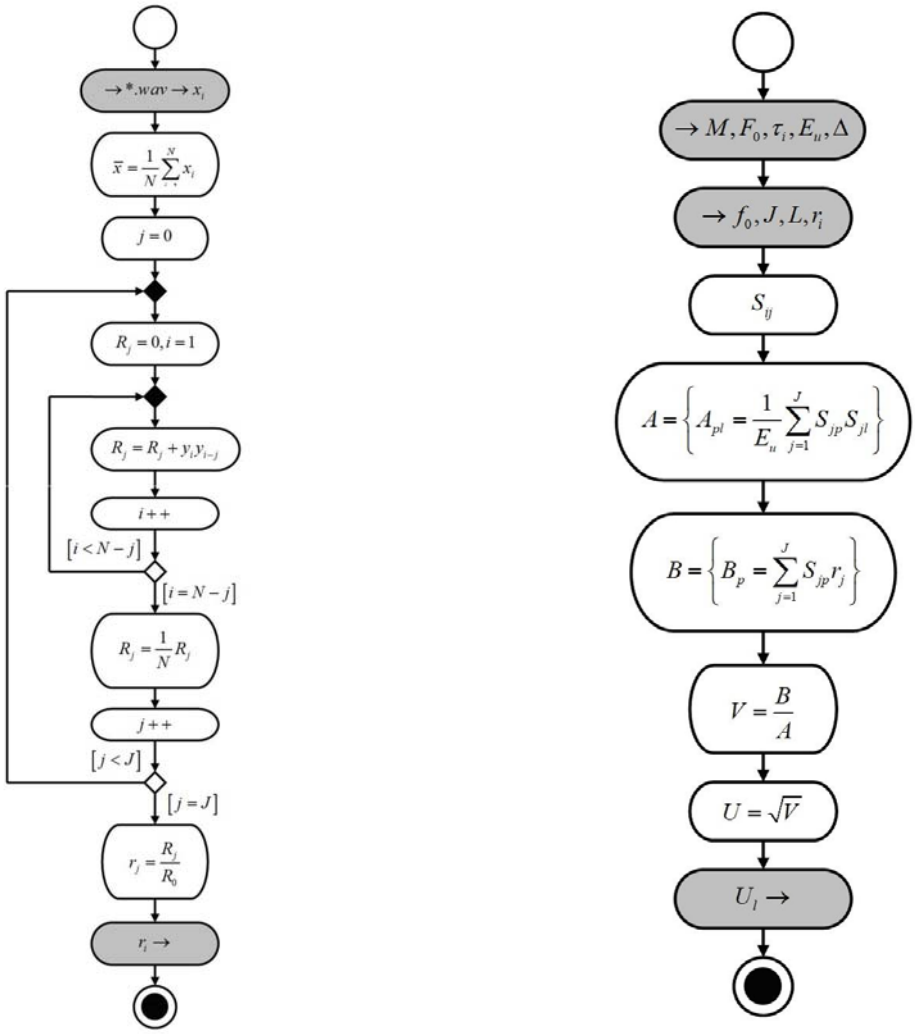


Рисунок 6.11 – UML-діаграма активності інформаційна технологія АСГ у методології ІГМС.

Спрощення прикладної реалізації представленої на рисунку 6.11 інформаційної технології забезпечується профільними базовими UML–діаграмами активності для: обчислення коефіцієнтів кореляції мовленнєвого сигналу (блок розрахунку коефіцієнтів кореляції мовленнєвого сигналу на рисунках 6.8, 6.9) – рисунок 6.12а; розрахунку значення частоти основного тону (блок розрахунку частоти основного тону на рисунку 6.9) – рисунки 6.2, 6.4, 6.6; розрахунку значень амплітуд несних гармонік (блок розрахунку амплітуд несних гармонік на рисунку 6.9) – рисунок 6.12б. Представлена у формі UML–діаграми активності на рисунку 6.11 інформаційна технологія деталізована представленою на рисунку 6.10 струкруною схемою із відповідним описом.



а) б)

Рисунок 6.12 – Базові UML–діаграми активності: а) блоку розрахунку коефіцієнтів кореляції мовленнєвого сигналу, б) блоку розрахунку амплітуд несних гармонік.

Вхідними параметрами для блоку розрахунку амплітуд несних гармонік окрім характеристичного параметру f_0 – частоти основного тону, є усталені параметри M – глибина модуляції, F_0 – основна частота модулювального коливання, τ_i – тривалість імпульсу, E_u – енергія моделі ІГМС (2.13), Δ – період дискретизації. Метод розрахунку елементів характеристичної матриці S залежить виду обраної моделі ІГМС, що описано у підрозділах 2.2–2.4. Численні експерименти, узагальнені результати яких наведено, зокрема, у підрозділі 3.3, дозволили визначити рекомендовані значення усталених параметрів. При

тривалості оцифрованої із частотою дискретизації $f_d = 6000$ Гц фонограми $\tau_i = 300$ мс, кількість відліків сигналу $N = 1800$. Кількість істотних відліків нормованої автокореляційної функції $J = 200$. Враховуючи, що початкові фази фонем виголошеної злитої мови практично не розпізнаються слуховою системою людини [45, 214–217], значення приймаємо $\varphi_0 = 0$, $\Gamma_0 = \pi$. Період модулювального коливання T_{F_0} приймаємо рівним тривалості виголошення однієї фонеми, яке знаходиться у діапазоні $50 \div 300$ мс [248]. Відповідно, значення частоти модулювального коливання обирається в діапазоні $F_0 = 3{,}3 \div 20$ Гц. Для енергії моделі допустиме вихідне значення $E_u = 1$. Якщо тривалість парольного мовленнєвого сигналу перевищує 0,5 с, то система автоматично розбиває фонограму на фрейми тривалістю 400 мс із можливим перекриванням фреймів у часі. При цьому верифікаційне рішення приймається для кожного фрейму окремо, а узагальнене рішення формулюється як $\left\{\overline{D} \geq \overline{D_0} : true, \overline{D} < \overline{D_0} : false\right\}$, де $\overline{D} = \frac{1}{S}\sum_{s=1}^{S} D_s$, $\overline{D_0} = \frac{1}{S}\sum_{s=1}^{S} D_{0s}$ – середньозважене значення міри і порогу, відповідно, S – кількість фреймів. Також можливий інший варіант визначення цих характеристик: $\overline{D} = \sum_{s=1}^{S} \rho_s D_s$, $\overline{D_0} = \sum_{s=1}^{S} \rho_s D_{0s}$, де ρ_s – вага значимості фрейму s, для визначення якої можна адаптувати метод розрахунку ваг W характеристичних параметрів моделі ІГМС, описаний у підрозділі 3.2.

Отже, описовий характер даного підрозділу мав за мету орієнтувати представлені у роботі наукові результати на практичне впровадження і узагальнюють вклад синтезованих моделей і методів для АСГ у підвищення такого атрибуту гарантоздатності як конфіденційність для класу ІСКЗ.

6.5 Узагальнена методика та інформаційна технологія для підвищення обраного атрибуту гарантоздатності ІСКЗ

Наведені в розділі 5 наукові результати вичерпно характеризують у формалізмі моделей Маркова процес визначення і оптимізації таких атрибутів

гарантоздатності як готовність, цілісність, безвідмовність, готовність, обслуговуваність, інтенсивність відмов і наробок на відмову тощо для класу інформаційних систем критичного застосування. Втім, досвід впровадження виявив доцільність узагальнення і прикладної орієнтації запропонованих у розділі 5 моделей і методів у вигляді профільної інформаційної технології для оптимізації обраного атрибуту гарантоздатності ІСКЗ, яка експлуатується в агресивному кіберфізичному просторі. Для наочності синтез узагальненої методики та інформаційної технології реалізуватимемо в контексті одного із зазначених атрибутів гарантоздатності, наприклад, *часу до відмови*. Основою для формалізації стануть математичні моделі оцінювання атрибутів гарантоздатності, наведені у підрозділі 5.5, методи організації системної політики безпеки, наведені у підрозділі 5.2, та концепція суб'єкт-системної взаємодії, наведена у підрозділі 5.1.

Узагальнимо ідентифікатором s_0 стан ІСКЗ, перебуваючи в якому остання повністю реалізує своє функціональне призначення. Якщо у дискретний момент часу t на систему із імовірністю q_i здійснюється вплив i–го детермінованого негативного фактору (НФ), $i=\overline{1,n}$, то система переходить у відповідний стан s_i, з якого у дискретний момент часу $t+1$ може перейти в один із станів з множини $\{s_0, s_{n+1}\}$, де стан s_{n+1} характеризує ситуацію, коли НФ вражає систему і остання припиняє своє функціонування реалізуючи відповідний протокол функціональної безпеки. Протидіяти впливу НФ має підсистема безпеки інформаційної системи (ПБІС) використовуючи узагальнені у системній політиці безпеки (СПБ) правила в яких вказано налаштування відповідних захисних механізмів. Відповідно, ПБІС або із імовірністю r_i нейтралізує вплив i–го НФ і у момент часу $t+1$ ІСКЗ переходить у стан s_0, або із імовірністю $\overline{r}_i = 1 - r_i$ не впорається із НФ і у момент часу $t+1$ ІСКЗ переходить у стан s_{n+1}. Як зазначалося у підрозділі 5.1, описаний перебіг подій, що характеризує життєвий цикл ІСКЗ, найкраще моделюється дискретним марковським ланцюгом із перехідною матрицею

$$\Pi = \left\{ \pi_{ij} \right\} = \begin{pmatrix} q_0 & q_1 & q_2 & \dots & q_n & 0 \\ r_1 & 0 & 0 & \dots & 0 & \overline{r_1} \\ r_2 & 0 & 0 & \dots & 0 & \overline{r_2} \\ \dots & \dots & \dots & \dots & \dots & \dots \\ r_n & 0 & 0 & \dots & 0 & \overline{r_n} \\ 0 & 0 & 0 & \dots & 0 & 1 \end{pmatrix}, \tag{6.67}$$

де $i, j = \overline{1, n+1}$, $q_0 = 1 - \sum_{i=1}^{n} q_i$. Імовірність перебування ІСКЗ у стані s_i у момент часу t із урахуванням (6.67) опишемо стохастичною величиною $p_i(t)$, $i = \overline{0, n+1}$, яка розраховується за виразом

$$p_i(t) = \sum_{j=0}^{n+1} \pi_{ji} p_j(t-1), \tag{6.68}$$

де визначена у матриці (6.67) стохастична величина π_{ij} характеризує імовірність переходу ІСКЗ із стану s_j у стан s_i. Вважатимемо, що у початковий момент $t = 0$ цензурованого часу експлуатації ІСКЗ остання перебувала у стані s_0:

$$\left\{ p_0(0) = 1, p_1(0) = 0, p_2(0) = 0, \dots, p_{n+1}(0) = 0 \right\}. \tag{6.69}$$

Узагальнимо вирази (6.68)–(6.69) формалізувавши імовірність перебування ІСКЗ у стані s_0 в момент часу $t > 0$ виразом

$$p_0(t) = w^{-1} \left(\left(0.5(q_0 + w) \right)^{t+1} - \left(0.5(q_0 - w) \right)^{t+1} \right), \tag{6.70}$$

де додатній параметр w характеризує задіяну ПБІС суперпозицію правил СПБ:

$$w^2 = q_0^2 + 4 \sum_{i=1}^{n} q_i r_i . \tag{6.71}$$

Аналітично формалізуємо полярні ситуації, імовірні для класу ІСКЗ. Нехай вплив НФ на досліджувану систему відсутній: $q_i \big|_{i=1}^{n} = 0$, тоді $q_0 = w = 1$ і, згідно виразу (6.70), маємо $p_0(t) = 1$, тобто ІСКЗ перманентно перебуватиме у стані s_0. Антагоністичною описаній буде ситуація, коли ПБІС не функціонує: $r_i \big|_{i=1}^{n} = 0$, тоді

$q_0 = w$ і, згідно виразу (6.70), маємо $p_0(t) = q_0^t$, тобто імовірність, що ІСКЗ перебуває у стані s_0 швидко спадає із зростанням значення t. Якщо НФ інтенсивно впливають на ІСКЗ (аналог DoS–атаки): $q_0 \to 0$, то $w \approx \sqrt{4\sum_{i=1}^{n} q_i r_i}$ і, згідно виразу (6.70), маємо $p_0(t) \approx 0.5\left(1+(-1)^t\right)\left(\sum_{i=1}^{n} q_i r_i\right)^{0.5t}$, тобто ІСКЗ перманентно перебуватиме у одному зі станів з множини $\{s_i\}\big|_{i=1}^{n}$ і навіть не перебуваючи у стані s_{n+1} не реалізовуватиме своє функціональне призначення.

Формалізуємо математичний апарат для визначення часу до відмови ІСКЗ, життєвий цикл якої описаний моделлю (6.70). Ідентифікуємо час до відмови як дискретний цілочисельний стохастичний параметр T, значення якого описує час за який досліджувана ІСКЗ перейде в стан s_{n+1}. Визначимо закон розподілу параметру T на основі виразу (6.70). Нехай параметр $P(T)$ описує імовірність переходу ІСКЗ у стан s_{n+1} рівно у момент часу T. З матриці (6.67) очевидно, що досліджувана система може опинитися у момент часу T у стані s_{n+1} лише якщо у момент часу $t = T-2$ вона перебувала у стані s_0, що характеризується імовірністю $p_0(T-2)$. З врахуванням цього, на основі виразу (6.70) визначимо параметр $P(T)$ як $P(T) = p_0(T-2)\sum_{i=1}^{n} q_i \overline{r}_i$, а закон розподілу цієї стохастичної величини опишемо виразом

$$P(T) = \begin{cases} w^{-1}\sum_{i=1}^{n} q_i \overline{r}_i \left(\left(\frac{q_0+w}{2}\right)^{T-1} - \left(\frac{q_0-w}{2}\right)^{T-1}\right), якщо\, T \geq 2, \\ 0, якщо\, T < 2. \end{cases} \tag{6.72}$$

Скористаємося виразом (6.72) для аналітичної формалізації моменту k–го порядку стохастичної величини T:

$$\mu_k[T] = \sum_{T=0}^{\infty} T^k P(T) = w^{-1}\sum_{i=1}^{n} q_i \overline{r}_i \left(\sum_{T=2}^{\infty} T^k \left(\frac{q_0+w}{2}\right)^{T-1} - \left(\sum_{T=2}^{\infty} T^k \left(\frac{q_0-w}{2}\right)^{T-1}\right)\right) = \tag{6.73}$$

$$= w^{-1}\sum_{i=1}^{n} q_i \overline{r}_i \left(2\left(q_0 + w\right)^{-1} \sum_{T=0}^{\infty} T^k \left(\frac{q_0 + w}{2} \right)^T - 2\left(q_0 - w\right)^{-1} \sum_{T=0}^{\infty} T^k \left(\frac{q_0 - w}{2} \right)^T \right).$$

Враховуючи, що $\left|q_0 \pm w\right| < 2$, ряди у виразі (6.73) збіжні. Це дозволяє застосувати до виразу (6.73) відому властивість [272]:

$$\sum_{n=0}^{\infty} n^k x^n = S_k\left(x\right) \equiv \left(x \frac{d}{dx} \right)^k \frac{1}{1-x} \tag{6.74}$$

з метою отримання компактнішої його форми:

$$\mu_k\left[T\right] = w^{-1}\sum_{i=1}^{n} q_i \overline{r}_i \left(2\left(q_0 + w\right)^{-1} S_k\left(\frac{q_0 + w}{2} \right) - 2\left(q_0 - w\right)^{-1} S_k\left(\frac{q_0 - w}{2} \right) \right). \tag{6.75}$$

Момент 1–го порядку стохастичної величини є її математичним сподіванням. Застосуємо це твердження до стохастичного параметру T, підставивши останній у вираз (6.75), і врахувавши, що $S_1\left(x\right) = x\left(1-x\right)^{-2}$ [272]:

$$M\left[T\right] = \left(1 + \sum_{i=1}^{n} q_i \right) \left(\sum_{i=1}^{n} q_i \overline{r}_i \right)^{-1}. \tag{6.76}$$

Дисперсія $D\left[x\right]$ стохастичної величини x визначається за її моментом 2–го порядку за виразом $D\left[x\right] = \mu_2\left[x\right] - \left(\mu_1\left[x\right]\right)^2$. Застосуємо це твердження до стохастичного параметру T, підставивши останній у вираз (6.75), і врахувавши вираз (6.76), а також те, що $S_2\left(x\right) = x\left(1+x\right)\left(1-x\right)^{-3}$ [272]:

$$D\left[T\right] = \left(1 + \sum_{i=1}^{n} q_i + \sum_{i=1}^{n} q_i r_i \left(3 + \sum_{j=1}^{n} q_j \right) \right) \left(\sum_{i=1}^{n} q_i \overline{r}_i \right)^{-2}. \tag{6.77}$$

Як зазначалося у підрозділі 5.5, формалізована виразом (6.76) величина $M\left[T\right]$ у таксономії гарантоздатності визначається як середній час до відмови (СЧВ), а формалізована виразом (6.77) величина $D\left[T\right]$ визначається як дисперсія часу до відмови (ДЧВ). Виразимо у метриці параметрів $M\left[T\right]$, $D\left[T\right]$ описані вище ситуації, коли: [1] – вплив НФ на досліджувану систему відсутній: $q_i\big|_{i=1}^{n} = 0$;

[2] – ПБІС не функціонує: $r_i\big|_{i=1}^{n}=0$; [3] – НФ інтенсивно впливають на ІСКЗ (аналог DoS–атаки): $q_0\to 0$, $\sum_{i=1}^{n}q_i\approx 1$:

$$[1]: M[T]=\frac{1-q_0}{1-q_0},\quad D[T]=\frac{q_0}{(1-q_0)^2};$$

$$[2]: M[T]=1+\left(\sum_{i=1}^{n}q_i\right)^{-1},\quad D[T]=\left(\sum_{i=1}^{n}q_i\right)^{-1}\left(\left(\sum_{i=1}^{n}q_i\right)^{-1}-1\right);$$

$$[3]: M[T]\approx 2\left(1-\sum_{i=1}^{n}q_ir_i\right)^{-1}\quad D[T]\approx 4\left(1-\sum_{i=1}^{n}q_ir_i\right)^{-2}\sum_{i=1}^{n}q_ir_i\,.$$

Вирази (6.72), (6.75), (6.77), (6.78) характеризуються універсальністю в межах класу ІСКЗ і є базовими для продовження синтезу.

Представимо в метриці $\langle M[T],D[T]\rangle$ природну для агресивного кіберфізичного простору ситуацію, коли на ІСКЗ одночасно впливає більше одного незалежного НФ. Для аналітичного опису такої ситуації розвинемо вихідні положення, наведені на початку підрозділу. Формалізуємо вплив НФ на ІСКЗ у дискретний момент часу t множиною $x=\{x_i\}$, де $i=\overline{1,n}$ – ідентифікатор НФ, x_i – бінарна змінна, яка приймає значення «1», якщо i–й НФ впливає на ІСКЗ у момент часу t, або «0» у протилежному випадку. Отже, якщо ІСКЗ яка на перебуває в стані s_0 у момент часу t реалізується множинний вплив НФ, факт чого визначається множиною x, то у момент часу $t+1$ досліджувана система перейде у стан $s_{\sigma(x)}$, де $\sigma(x)=\sum_{i=1}^{n}2^{n-i}x_i$ – представлення множини бінарних значень $x\in[0,1]^n$ у десятковій системі числення. Вважаючи НФ незалежними, імовірність переходу ІСКЗ із стану s_0 у стан $s_{\sigma(x)}$ аналітично опишемо виразом

$$Q_{\sigma(x)}=\prod_{i=1}^{n}\left(x_iq_i+(1-x_i)(1-q_i)\right). \tag{6.78}$$

Якщо у момент часу t ІСКЗ перебуває у стані $s_{\sigma(x)}$, $x\neq 0$, то в залежності від ефективності функціонування ПБІС у момент часу $t+1$ досліджувана система

або з імовірністю $R_{\sigma(x)}$ перейде у стан s_0 (вплив всіх НФ нейтралізовано), або з імовірністю $\overline{R}_{\sigma(x)}$ перейде у стан s_{2^n} (вплив хоча б одного з активних НФ нейтралізувати не вдалося). Аналітично таке розгалуження опишемо відповідними виразами:

$$\begin{aligned} R_{\sigma(x)} &= \prod_{i=1}^{n}\left(x_i\left(r_i-1\right)+1\right), \\ \overline{R}_{\sigma(x)} &= 1-R_{\sigma(x)}. \end{aligned} \tag{6.79}$$

Враховуючи сказане, матриця переходів (6.67) еволюціонує до вигляду

$$\Pi = \begin{pmatrix} Q_0 & Q_1 & Q_2 & \dots & Q_{2^n} & 0 \\ R_1 & 0 & 0 & \dots & 0 & \overline{R}_1 \\ R_2 & 0 & 0 & \dots & 0 & \overline{R}_2 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ R_{2^n} & 0 & 0 & \dots & 0 & \overline{R}_{2^n} \\ 0 & 0 & 0 & \dots & 0 & 1 \end{pmatrix}. \tag{6.80}$$

Зауважимо, що еволюція матриці (6.67) до вигляду (6.80) забезпечувалася множиною формальних замін вигляду

$$\left\{n \to 2^n, q_i \to Q_i, r_i \to R_i\right\}. \tag{6.81}$$

Ця обставина дозволяє нам отримати оновлені з урахуванням (6.80) аналітичні вирази для стохастичного параметру T і його моментів підставивши (6.81) у вирази (6.72) і (6.75). Відповідно, врахувавши (6.81), вирази (6.76) і (6.77), які формалізують СЧВ і ДЧВ, приведемо до вигляду

$$M\left[T\right] = \frac{1+\sum\limits_{x\neq 0} Q_{\sigma(x)}}{\sum\limits_{x\neq 0} Q_{\sigma(x)}\left(1-R_{\sigma(x)}\right)}, \tag{6.82}$$

$$D\left[T\right] = \frac{1-\sum\limits_{x\neq 0} Q_{\sigma(x)} + \sum\limits_{x\neq 0} Q_{\sigma(x)} R_{\sigma(x)}\left(3+\sum\limits_{x'\neq 0} Q_{\sigma(x')}\right)}{\left(\sum\limits_{x\neq 0} Q_{\sigma(x)}\left(1-R_{\sigma(x)}\right)\right)^2}. \tag{6.83}$$

Підсумовування у виразах (6.82), (6.83) здійснюється за всіма непустими множинами x і x' з $\{0,1\}^n$.

Розвиток наведеного теоретичного матеріалу до інформаційної технології зумовлює додаткову формалізацію процесу налаштування засобів управління конфіденційністю ІСКЗ. Нехай у СПБ досліджуваної системи синтезовано m правил для протидії НФ. Орієнтуючись на клас ІСКЗ, ПБІС реалізує комплексний захист із можливістю одночасної активації кількох правил. Отже, задіювана ПБІС суперпозиція правил визначатиметься множиною бінарних значень $z=\{z_j\}\in\{0,1\}^m$, $j=\overline{1,m}$, де бінарна змінна z_j приймає або значення «1» якщо j–та правило активоване, або «0» – у протилежному випадку. Опишемо імовірність нейтралізації впливу на досліджувану ІСКЗ i–го НФ в результаті активації k–го правила стохастичною змінною $r_{i,k}$. Сценарій комплексного захисту передбачає, що для нейтралізації впливу i–го НФ ПБІС може активувати більше одного правила. Опишемо імовірність нейтралізації впливу i–го НФ хоча б одним правилом таким виразом:

$$r_i(z)=\sum_{j=1}^{m}(-1)^j\sum_{k_1<k_2<\ldots k_j}\left(r_{i,k_1}z_{k_1}\right)\left(r_{i,k_2}z_{k_2}\right)\ldots\left(r_{i,k_j}z_{k_j}\right). \tag{6.84}$$

Підставивши вираз (6.84) у (6.79) формалізуємо імовірність нейтралізації впливу описаного множиною x комплексного НФ на ІСКЗ, ПБІС якої у відповідь активує описану множиною z суперпозицію правил:

$$R_{\sigma(x)}=\prod_{i=1}^{n}\left(\left(1-x_i\right)r_i(z)+1\right). \tag{6.85}$$

Враховуючи (6.85) у виразі (6.82) отримуємо аналітичну форму середнього часу до відмови комплексно захищеної ІСКЗ, яка експлуатується в умовах агресивного кіберфізичного простору:

$$M[T](z)=\frac{1+\sum\limits_{x\neq 0}Q_{\sigma(x)}}{\sum\limits_{x\neq 0}Q_{\sigma(x)}\left(1-R_{\sigma(x)}(z)\right)}. \tag{6.86}$$

Природно, максимальний рівень конфіденційності ІСКЗ забезпечить постійна активація всіх правил, але обсяг обчислювальних ресурсів будь–якої інформаційної системи обмежений і нераціональне їх використання, як доведено у підрозділах 5.2, 5.4, негативно впливає на значення таких атрибутів гарантоздатності, як готовність та цілісність. Це твердження є вихідним для постановки задачі пошуку оптимальної суперпозиції правил, для постановки якої опишемо обчислювальну складність j–ї правила змінною c_j. Відповідно, обчислювальну складність суперпозиції правил опишемо виразом

$$C(z) = \sum_{j=1}^{m} c_j z_j \,. \tag{6.87}$$

Прикладний сенс мають два варіанти постановки задачі оптимізації на основі цільової функції (6.87) і виразу (6.86):

$$OT1: \quad M[T](z) \to \max \quad C(z) \le C_0 \,, \tag{6.88}$$

$$OT2: \quad C(z) \to \min \quad M[T](z) \ge T_0 \,, \tag{6.89}$$

де C_0 – константа, яка характеризує граничну обчислювальну складність суперпозиції правил, T_0 – константа, яка характеризує бажаний час до відмови досліджуваної системи. Задачі оптимізації виду (6.88), (6.89) класифікуються як нелінійні задачі цілочисельного програмування. Для розв’язання таких задач оптимізації використовують комбінаторні методи, зокрема, метод послідовного аналізу варіантів [284], та, при $m \le 20$, метод повного перебору. Впорядкуємо вищенаведений матеріал у вигляді узагальненої інформаційної технології оптимізації значення обраного атрибуту гарантоздатності цільової ІСКЗ. Візуальне представлення синтезованої інформаційної технології у вигляді UML–діаграми активності наведено на рисунку 6.14.

В якості прикладу, представимо процес застосування синтезованої інформаційної технології для оптимізації часу до відмови однієї з ІСКЗ, де впроваджувалися результати дисертаційного дослідження, а саме, ІСКЗ Ситуаційного центру департаменту інформаційних технологій Вінницької міської ради. Ситуаційний центр функціонує з 2018 р. Основна його функція –

відеофіксація подій у місті узагальнюючи вхідні відеопотоки від понад 550 відеокамер з подальшим збереження цієї інформації в розгалуженій реляційній базі даних. Персоніфікований доступ до бази даних центру надається співробітникам Вінницької міської ради, Національної поліції України, Служби безпеки України, ряду муніципальних підприємств тощо.

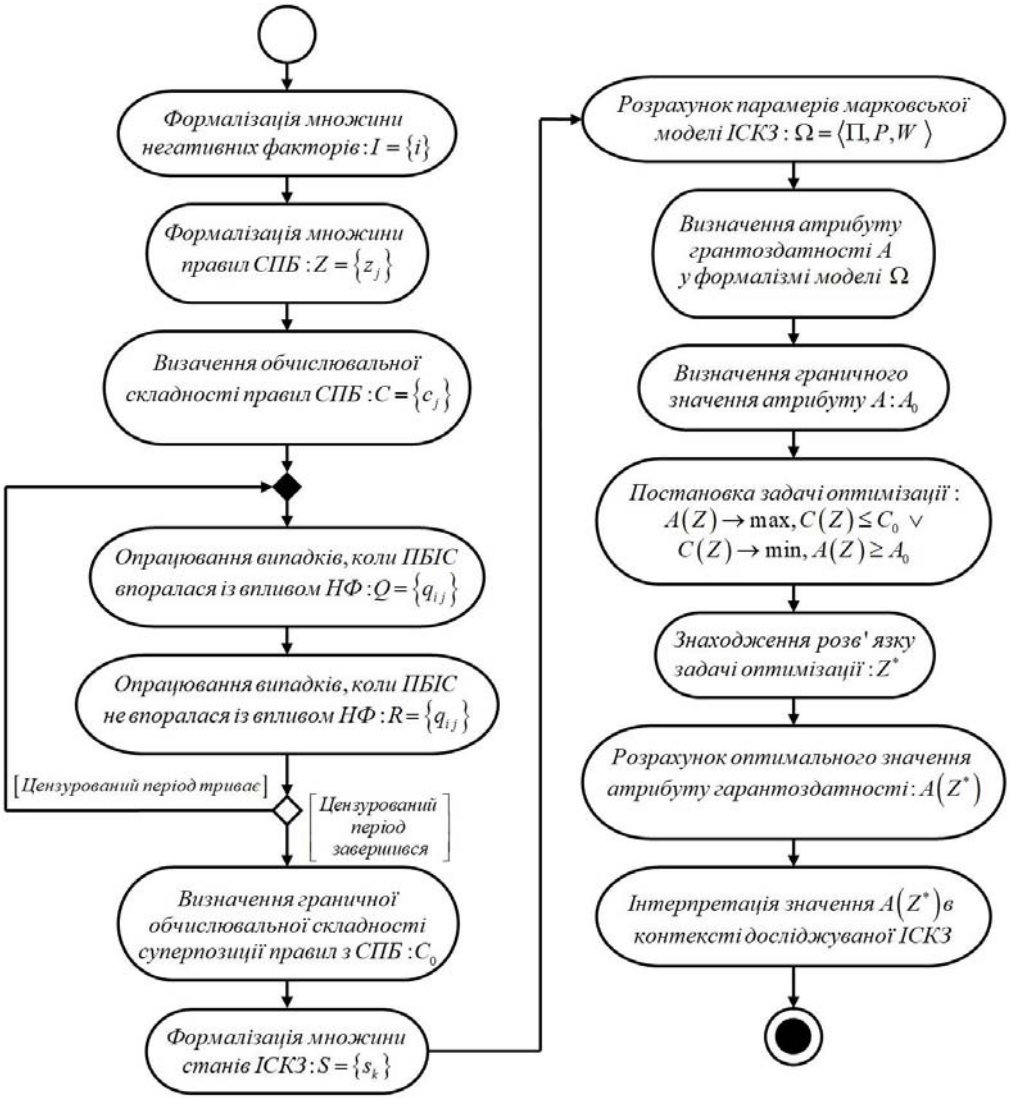


Рисунок 6.14 – Узагальнена інформаційна технологія оптимізації обраного атрибуту гарантоздатності досліджуваної ІСКЗ.

Центральним питанням при постановці експериментів, які стосуються питань функціонування інформаційних систем в умовах потенційних кіберзагроз, є вибір актуальних для цільової ІСКЗ типів НФ і оцінювання імовірностей їх

впливів на досліджувану систему за визначений інтервал часу. Повний список актуальних кіберзагроз для функціонуючих у кіберфізичному просторі інформаційних систем представлено у галузевому стандарті The Common Vulnerability Scoring System (CVSSv3.1) і спеціалізованій базі даних відкритого міжнародній проекту Open Web Application Security Project (OWASP). Зокрема, на ресурсі owasp.org щороку публікується впорядкований за ступенем небезпеки перелік актуальних НФ, який для 2020 р. включає: A1: Injection; A2: Broken Authentication; A3: Sensitive Data Exposure; A4: XML External Entities (XXE); A5: Broken Access Control; A6: Security Misconfiguration; A7: Cross–Site Scripting (XSS); A8: Insecure Deserialization; A9: Using Components with Known Vulnerabilities; A10: Insufficient Logging & Monitoring. Аналіз експлуатаційної інформації цільової ІСКЗ за цензурований період часу з 01.01.2020 р. по 01.06.2020 р. показав факти виявлення НФ, які належать до типів A1–A8, а аналіз цієї інформації дозволив розрахувати $q_1, q_2, \ldots q_8$ – імовірності впливу відповідних типів НФ на цільову ІСКЗ:

$$\{0.02, 0.01, 0.03, 0.03, 0.02, 0.04, 0.05, 0.02\}. \qquad (6.90)$$

Для протидії впливу згаданих типів НФ у СПБ цільової ІСКЗ реалізовано шість правил, які відрізняються налаштуваннями таких захисних механізмів як: програма антивірусного захисту, програмний брандмауер, програмні засоби захисту від несанкціонованого доступу із автентифікацією суб'єкта за голосом, програмні засоби розмежування доступу, засоби довіреного завантаження, засоби криптографічного захисту. Обчислювальна складність кожного z_j, $j = \overline{1,6}$, правила захисту представлена відповідним елементом множини: $\{20 \cdot 10^3, 10 \cdot 10^3, 8 \cdot 10^3, 15 \cdot 10^3, 10 \cdot 10^3, 5 \cdot 10^3\}$. Відповідно, аналітичний вигляд суперпозиції правил з СПБ вигляду (6.70) для цільової ІСКЗ представимо виразом

$$C(z) = 20 \cdot 10^3 z_1 + 10 \cdot 10^3 z_2 + 8 \cdot 10^3 z_3 + 15 \cdot 10^3 z_4 + 10 \cdot 10^3 z_5 + 5 \cdot 10^3 z_6. \qquad (6.91)$$

Аналіз експлуатаційної інформації цільової ІСКЗ за цензурований період часу дозволив розрахувати імовірності нейтралізації відповідних типів НФ

наявними правилами з СПБ. Результати розрахунку представлені у вигляді матриці

$$\left\| r_{i,k} \right\| = \begin{pmatrix} 0.8 & 0.5 & 0.25 & 0.5 & 0 & 0 \\ 0 & 0 & 0.5 & 0 & 0.9 & 0 \\ 0 & 0 & 0 & 0.8 & 0.2 & 0 \\ 0 & 0.7 & 0 & 0 & 0 & 0.5 \\ 0 & 0.8 & 0 & 0 & 0 & 0.5 \\ 0 & 0.8 & 0 & 0 & 0 & 0.5 \\ 0.9 & 0.5 & 0 & 0 & 0 & 0 \\ 0.2 & 0 & 0.2 & 0.5 & 0.1 & 0 \end{pmatrix}, \tag{6.92}$$

де $i = \overline{1,8}$ – індекси актуальних типів НФ, $k = \overline{1,6}$ – індекси актуальних захисних механізмів. Наявність у i–му рідку матриці (6.92) більше одного ненульового значення означає, що для нейтралізації впливу i–го НФ ПБІС активує відповідні захисні механізми, реалізуючи сценарій комбінованого захисту. Продемонструємо розв'язання для цільової ІСКЗ задачі оптимізації типу $OT2$ (6.89). Підставимо елементи матриці (6.92) у вираз (6.84) і отримаємо набір поліномів $r_i(z)$, $i = \overline{1,8}$, від бінарних змінних z_j, $j = \overline{1,6}$:

$$\begin{gathered} r_1(z) = 0.8z_1 + 0.5z_2 + 0.25z_3 + 0.5z_4 - 0.4z_1z_2 - 0.2z_1z_3 - \\ -0.4z_1z_4 - 0.125z_2z_3 - 0.25z_2z_4 - 0.125z_3z_4 + 0.1z_1z_2z_3 + \\ +0.2z_1z_2z_4 + 0.1z_1z_3z_4 + 0.0625z_2z_3z_4 - 0.05z_1z_2z_3z_4, \end{gathered}$$

$$r_2(z) = 0.5z_3 + 0.9z_5 - 0.45z_3z_5,\ r_3(z) = 0.8z_4 + 0.2z_5 - 0.16z_4z_5,$$

$$r_4(z) = 0.7z_2 + 0.5z_6 - 0.35z_2z_6,\ r_5(z) = 0.8z_2 + 0.5z_6 - 0.4z_2z_6,$$

$$r_6(z) = 0.8z_2 + 0.5z_6 - 0.4z_2z_6,\ r_7(z) = 0.9z_1 + 0.5z_2 - 0.45z_1z_2,$$

$$\begin{gathered} r_8(z) = 0.2z_1 + 0.2z_3 + 0.5z_4 + 0.1z_5 - 0.04z_1z_3 - 0.1z_1z_4 - \\ -0.02z_1z_5 - 0.02z_3z_5 - 0.1z_3z_4 - 0.05z_4z_5 + 0.02z_1z_3z_4 + \\ +0.04z_1z_3z_5 + 0.01z_1z_4z_5 + 0.01z_3z_4z_5 - 0.002z_1z_3z_4z_5. \end{gathered}$$

Підставляємо набір поліномів $r_i(z)$, $i = \overline{1,8}$, у вираз (6.85), отримуючи набір поліномів $R_{\sigma(x)}(z)$, які характеризують імовірності нейтралізації можливих комбінацій НФ, представлених множиною x, суперпозицією правил,

представлених множиною z. Підставляємо емпіричні дані (6.90) у вираз (6.78) і отримуємо вираз для розрахунку імовірності переходу цільової ІСКЗ із стану s_0 у стан $s_{\sigma(x)}$:

$$Q_{\sigma(x)} = (x_1 - 0.98)(x_2 - 0.99)(x_3 - 0.97)(x_4 - 0.97)\times$$
$$\times(x_5 - 0.98)(x_6 - 0.96)(x_7 - 0.95)(x_8 - 0.98).$$

Підставляємо набір поліномів $R_{\sigma(x)}(z)$ і поліном $Q_{\sigma(x)}(z)$ у вираз (6.82) і після підсумовування за всіма $x \in \{0,1\}^{n=8}$ отримуємо аналітичний вираз для розрахунку СЧВ цільової ІСКЗ у вигляді $M[T](z) = V(z)$, де $V(z)$ – результуючий поліном, спосіб отримання якого тривіальний, тому, зважаючи на його довжину, не наводиться. Далі на рисунку 6.15 візуалізовано залежність СЧВ цільової ІСКЗ від індексу суперпозиції правил $\sigma(z)$.

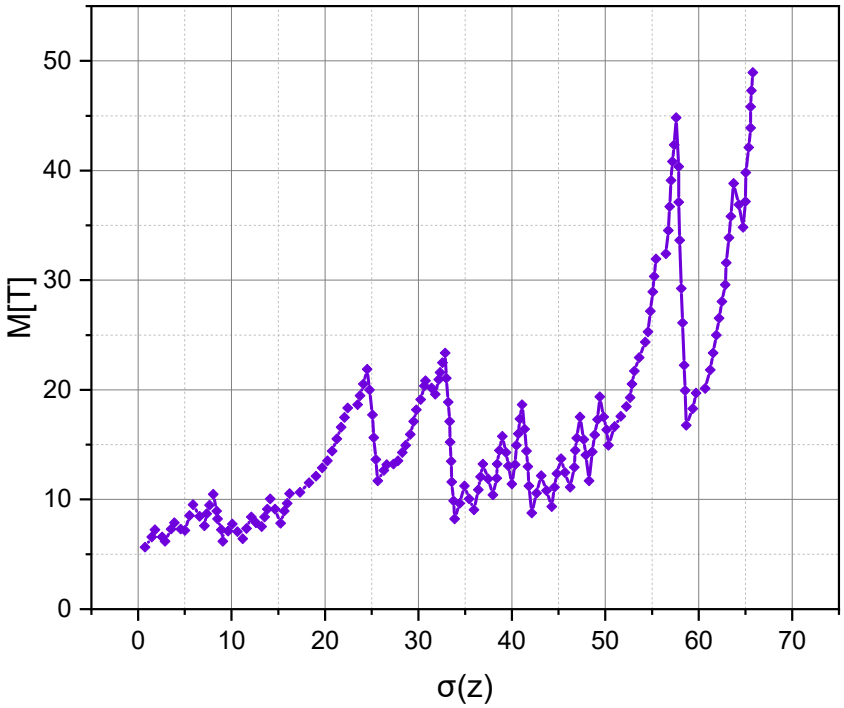


Рисунок 6.15 – Залежність СЧВ цільової ІСКЗ від індексу суперпозиції правил.

З наведеної на рисунку 6.15 результатів видно, що СЧВ цільової ІСКЗ, вплив на яку кіберфізичного простору визначається (6.90), (6.92), при нефункціонуючій ПБІС ($\sigma(z) = 0$) дорівнює 5.9891, а при активації всіх правил

($\sigma(z) = 2^{m=6} = 64$) дорівнює 48.8869. Отже, активація всіх правил подовжує СЧВ цільової ІСКЗ на понад 817%. Результати розв'язання для цільової ІСКЗ задачі оптимізації типу $OT2$ (6.89) для граничних значень $T_0 = \{10,15,20,25,30,35,40\}$, $5.98 < T_0 < 48.88$, візуалізовано на рисунку 6.16 Зауважимо, що кількість комбінацій варіантів реалізації z для цільової ІСКЗ невелика ($\sigma(z) = 2^{m=6} = 64$). Це допускає розв'язання задачі оптимізації методом повного перебору, але не технологічність такого підходу зумовили створення профільного програмного додатку для розв'язання задач оптимізації типів (6.88), (6.89) методом послідовного аналізу варіантів.

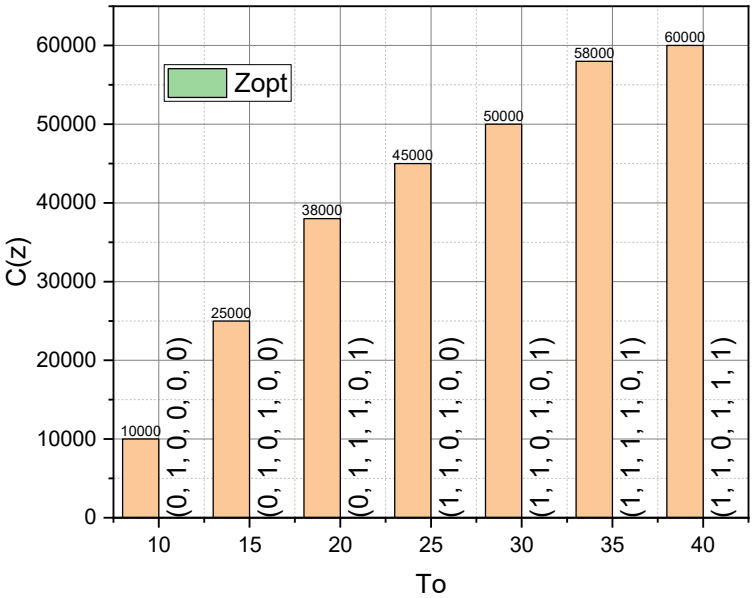


Рисунок 6.16 – Результати розв'язання для цільової ІСКЗ задачі оптимізації типу $OT2$ для різних граничних значень T_0.

На рисунку 6.16 для кожного розглянутого граничного значення T_0 наведено оптимальну суперпозицію правил у вигляді множин бінарних значень z_j, $j = \overline{1,6}$, і її обчислювальну складність. Результати роботи авторського програмного додатку повністю співпали із результатами, отриманими методом повного перебору. З наведених на рисунку 6.16 емпіричних результатів прослідкується очевидна тенденція – із зростанням граничного значення СЧВ зменшується виродженість оптимальної суперпозиції правил з СПБ і зростає її

обчислювальна складність. Втім, доцільність створеного математичного апарату теж очевидна – з його допомогою, наприклад, для цільової ІСКЗ, розрахованої на експлуатацію із СЧВ рівним 25 знайдено оптимальну суперпозицію правил з обчислювальною складністю $45 \cdot 10^3$, що на 44% менше за обчислювальну складність активації всіх правил, визначених у СПБ. Зауважимо, що продемонстрований приклад є ординарним тоді, як представлений в розділі 5.5 математичний апарат дозволяє формалізувати обраний атрибут гарантоздатності цільової ІСКЗ, у якій переходи між станами описуються різними законами розподілу. Втім, ця обставина не впливає на коректність наведеної на рисунку 6.14 інформаційної технології, приклади застосування якої для оптимізації цілісності, готовності, функційної безпечності і живучості для цієї ж ІСКЗ Ситуаційного центру департаменту інформаційних технологій Вінницької міської ради представлено в підрозділах 5.2, 5.3, 5.4.

6.6 Узагальнення досвіду впровадження результатів дисертаційного дослідження

Розвиток і впровадження ІСКЗ ускладнюється підвищеною увагою до них з боку зловмисників, що призводить до паралельного розвитку як методів забезпечення належного рівня безвідмовності, конфіденційності, цілісності таких систем, так і детермінованих негативних факторів, що впливають на ІСКЗ. У дисертаційній роботі представлено наукові і практичні результати, які сприяють досягненню визначальної переваги у перманентному інструментальному протистоянні «захист vs напад» за рахунок вирішення актуальної науково–технічної проблеми інтеграції методів автентифікації суб’єктів–користувачів за голосами у системні інформаційні процеси життєвого циклу ІСКЗ з обов’язковим забезпеченням позитивної динаміки значень атрибутів гарантоздатності такого класу систем. Структурне узагальнення та цільове спрямування представлених у роботі результатів, спрямованих на забезпечення конфіденційності ІСКЗ, представлено на рисунку 6.17. Структурне узагальнення та цільове спрямування

представлених у роботі результатів, спрямованих на оптимізацію решти атрибутів гарантоздатності ІСКЗ, представлено на рисунку 6.18.

Процес впровадження результатів дисертаційного дослідження структурувався з метою посилення конфіденційності, готовності та обслуговуваності інформаційної системи цільової установи.

Посилення конфіденційності досягається впровадженням двохетапної схеми автентифікації суб'єкта–користувача для доступу до критично важливих інформаційних ресурсів цільової установи. На першому етапі цієї схеми, формалізованої у підрозділі 5.1, користувач персоніфікувався за схемою авторизації виду «логін»–«пароль», а на другому етапі – верифікувався за результатами аналізу фонограми із виголошеною парольною фразою тривалістю 10 с, змістовний склад якої генерується автоматично і випадково на основі заданого репрезентативного словника, який містить близько 1000 іменників, дієслів і прикметників. Перед початком експлуатації система верифікації навчалася на фонограмах цільових користувачів тривалістю близько 30 с. Коло осіб, які мали доступ до критично важливих даних цільової установи сегментувалося на три категорії ролей відповідно до привілей, відображених у системній політиці безпеки. Зокрема роль «користувач» обмежувалася лише функцією перегляду критично важливих даних, до привілей ролі «модератор» включалися функції перегляду, додавання і редагування критично важливих даних, а до привілей ролі «адміністратор», на додачу до перелічених сервісів, додавалися функції реєстрації нових користувачів із відповідними ролями, а також, редагування і видалення аккаунтів, віднесених до ролей типів «користувач» і «модератор» тощо.

Процедура верифікації передбачала або підтвердження особи користувача, який автентифікується, або ні із занесенням відповідного запису в системний журнал подій, дані з якого забезпечують можливість розрахунку, зокрема, таких характеристик як імовірність виникнення похибок першого і другого роду за цензурований період експлуатації двохетапної схеми автентифікації, інтегрованої у інформаційну систему цільової установи.

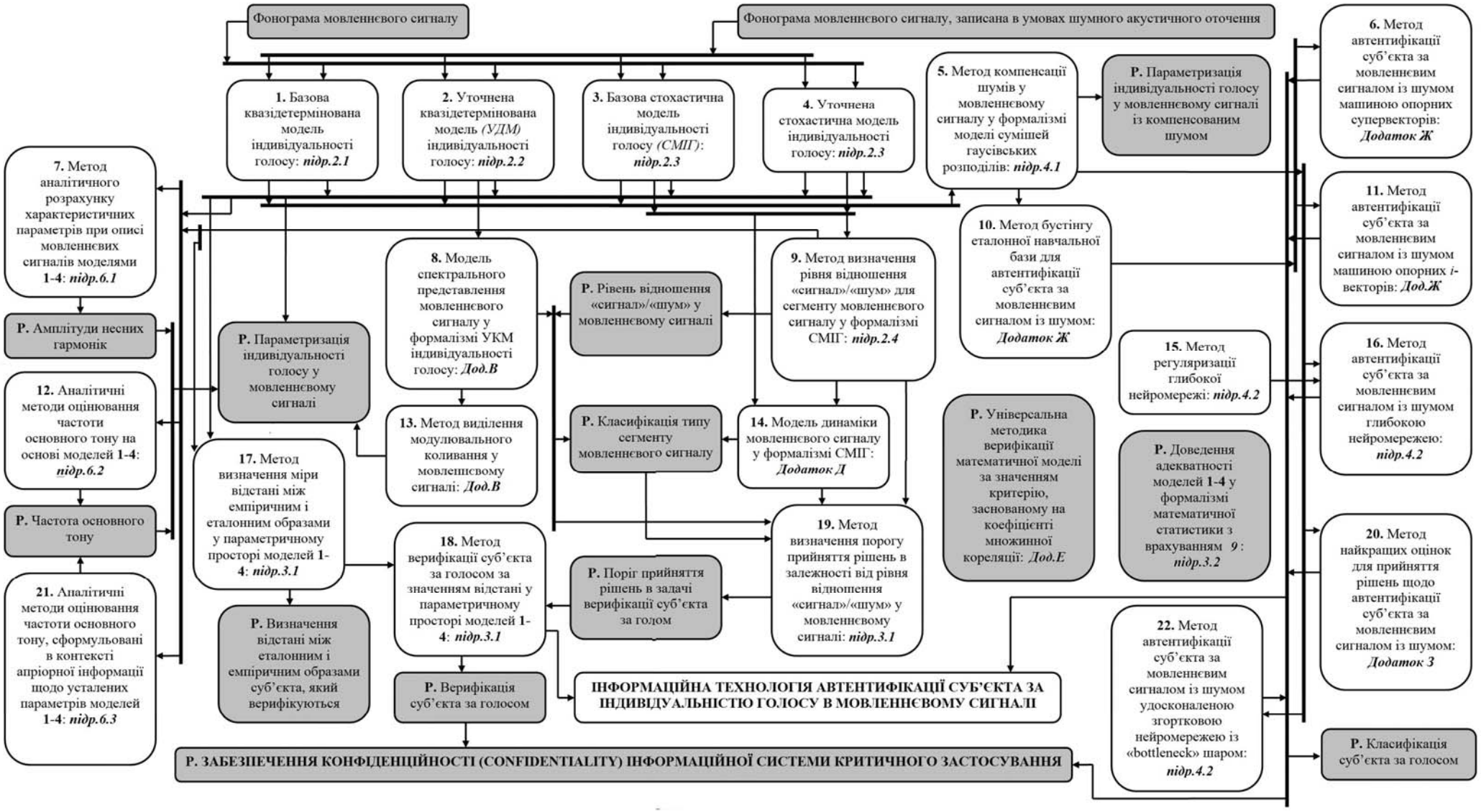


Рисунок 6.17 – Узагальнення представлених у роботі результатів, спрямованих на забезпечення конфіденційності ІСКЗ.

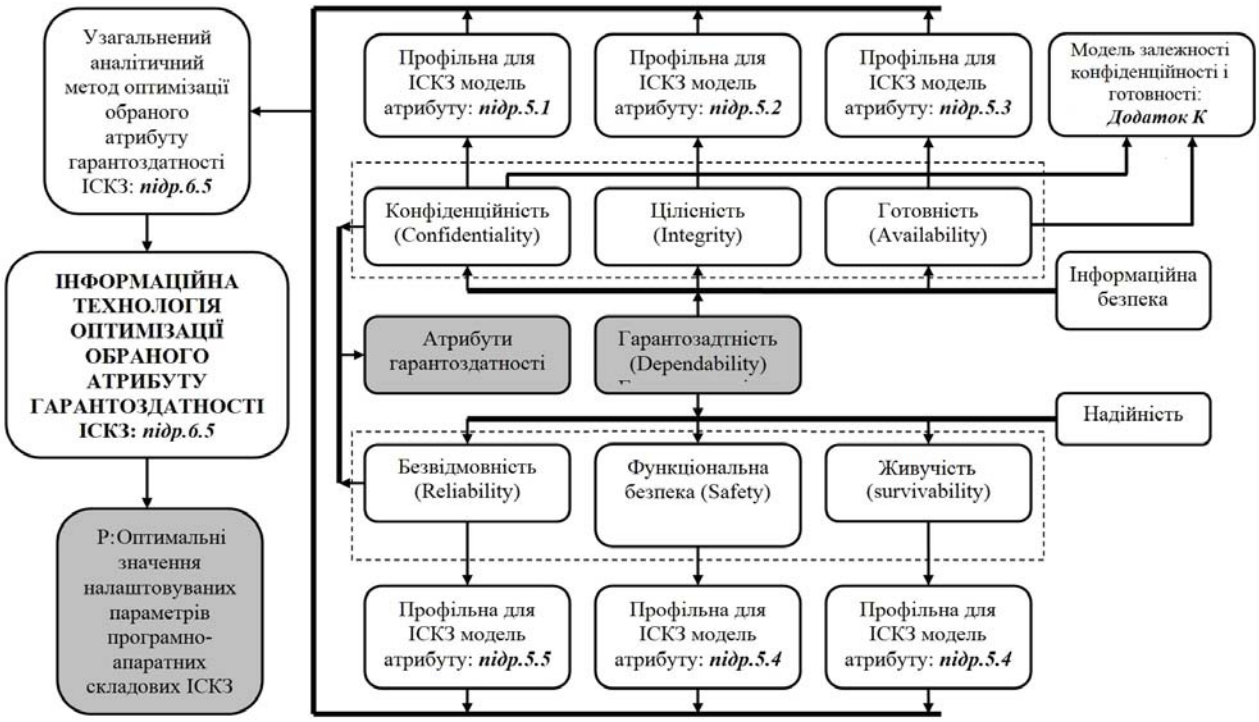


Рисунок 6.18 – Узагальнення представлених у роботі результатів, спрямованих на оптимізацію обраного атрибуту гарантоздатності ІСКЗ.

Посилення готовності інформаційної системи цільової установи досягається оптимізацією налаштувань правил QoS технології в операційному середовищі роутерів внутрішньої комп’ютерної мережі. Параметри налаштувань розраховувалися за методами, описаними у підрозділах 5.1–5.4, для чотирьох типів аккаунтів: «адміністратор», «модератор», «користувач», «не авторизований», де перші три типи аккаунтів мають привілеї доступу до критично важливих даних, а четвертий тип – ні. Налаштування здійснюються для забезпечення першочергового доступу до інформаційної системи авторизованим користувачам, аккаунти яких належали до перших двох типів. Зафіксовані за цензурований період експлуатації модифікованої інформаційної системи установи у системному журналі подій факти несанкціонованого переривання сеансів доступу до критично важливих даних для авторизованих користувачів із ролями перших трьох типів, а також, факти відхилення запиту на реалізацію вибраної авторизованим користувачем функції, дозволеної у рамах його ролі, є підставою

для кількісного оцінювання атрибуту готовності. Додаткову інформацію щодо ефективності здійснених модифікацій дає періодичне стресове тестування доступності критичних даних цільової інформаційної системи в умовах емульованої розподіленої DoS–атаки на сегмент внутрішньої комп'ютерної мережі, де відповідні інформаційні ресурси зберігаються.

Посилення обслуговуваності інформаційної системи установи втілюється у розроблений графік рекомендованого оновлення її апаратних компонентів, у якому враховано оцінки базових параметрів гарантоздатності, розраховані на основі методів, описаних у підрозділі 5.6. Розрахунок відповідних атрибутів гарантоздатності здійснюється за результатами математичного моделювання процесу функціонування цільової інформаційної системи як керованого напівмарковського процесу.

Впровадження результатів дисертаційного дослідження у цільових установах розпочинався презентацією, під час якої демонструвався найнаочніший прикладний результат – автентифікація суб'єкта за голосом. Методику демонстрації достовірності цього процесу, який узагальнює представлені у розділах 2–4 наукові результати, сформульовано відповідно до рекомендацій колективу відділу розпізнавання та синтезу звукових образів Міжнародного науково–навчального центру інформаційних технологій та систем НАНУ та МОНУ (м. Київ) на чолі із М. М. Сажком, який здійснив рецензування матеріалів монографії [60]. Детально методику і аналіз результатів її застосування описано у підрозділі 4.3. Враховуючи семантичну близькість задачі автентифікації суб'єкта за голосом і класичної задачі «text–dependent speaker verification», оцінювання достовірності результатів роботи програмного забезпечення, реалізованого на основі авторських моделей і методів, здійснено за результатами його тестування на матеріалах спеціалізованих, вільно доступних, репрезентативних за вмістом мовленнєвих корпусів RedDots dataset і CSTR VCTK Corpus. Перший із згаданих корпусів, доступний за URL https://sites.google.com/site/thereddotsproject/, є основним результатом міжнародного проекту RedDots, здійснюваного під патронажем Міжнародної асоціації мовленнєвої комунікації INTERSPEECH з

метою отримання репрезентативних матеріалів для тестування систем розпізнавання мовців за дискретизованим засобами мобільної комунікації короткотривалим мовленнєвим сигналом із високою фонетичною варіативністю. Корпус CSTR VCTK, доступний за URL https://datashare.is.ed.ac.uk/handle/10283/2651, сформовано колективом дослідницького центру мовленнєвих технологій Університету Единбургу під час роботи над фреймворком для клонуванням голосу Voice Cloning Toolkit. У проведеному експерименті кожен фрейм дискретизованого мовленнєвого сигналу описувався трьома наборами векторів характеристичних параметрів, значення яких отримувалися у парадигмі уточненої детермінованої моделі ІГМС, представленої у підрозділі 2.3. Для вмісту кожного корпусу окремо формувалися три 1024–компонентні універсальні фонові моделі, навчені протягом 200 ітерацій ЕМ–методу на всьому матеріалі відповідних навчальних вибірок, всі фрейми яких параметризувалися одним із трьох згаданих наборів характеристичних параметрів. Далі навчені універсальні фонові моделі адаптувалися до цільових мовців МАР–методом для утворення індивідуальних 8–ми компонентних моделей сумішей гаусівських розподілів. Відповідно до обраного набору характеристичних параметрів, для кожного цільового мовця з відповідного корпусу створювалося по три адаптованих моделі суміші. Дослідження проводилися із моделлю процесу верифікації, представленою на рис. 1.3, у якій для прийняття рішень використовувалася машина опорних *i*–векторів із функцією–ядром $K_{B\cos}$ і розв'язувальним правилом G_{all}, яка виявилася кращою з–поміж претендентів, результати дослідження яких продемонстровано на рис. 4.14. Результат дослідження представлено відповідними DET–кривими на рис. 4.26, де результати на рис. 4.26а отримано на основі матеріалів корпусу RedDots, а результати на рис. 4.26б – на основі матеріалів корпусу VCTK. В залежності від набору характеристичних параметрів, оцінювана система автентифікації суб'єктів за голосами продемонструвала достовірність верифікації в діапазоні 93,75–95% для корпусу RedDots і 93,5–94,25% для корпусу VCTK, відповідно. В цілому, продемонстровані на рис. 4.26 результати дозволяють однозначно визнати

систему верифікації мовців, побудовану на основі авторських наукових результатів, функціональною із потенціалом для можливого удосконалення.

Зауважимо, що адекватність представлених у розділі 2 моделей індивідуальності голосу у мовленнєвому сигналі емпірично доведено із визначенням відповідних абсолютних, нормованих абсолютних і відносних похибок. Методику відповідних експериментів формалізовано у підрозділі 3.1, а їх узагальнені результати представлено на рис. 3.26.

Станом на березень 2020 р. результати дисертаційної роботи впроваджені у: 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).

У наведених в додатку М актах результати впровадження оцінено позитивно. Найважливішу інформацію, на підставі якої формувалися відповідні акти узагальнено в таблиці 6.1 де:

- узагальненою характеристикою конфіденційності виступають усереднені імовірності виникнення похибок першого і другого роду у процесі автентифікації суб’єктів–користувачів інформаційної системи цільової установи за їх голосами за цензурований час експлуатації останньої;
- узагальненою характеристикою готовності виступає відношення часу штатного функціонування інформаційної системи цільової установи до цього ж часу із додаванням часу, коли система перебувала у нефункціональному стані з причин, які стосуються атрибутів готовності і цілісності останньої;
- узагальненою характеристикою обслуговуваності виступає відношення часу штатного функціонування інформаційної системи цільової установи до цього ж часу із додаванням часу, коли система перебувала у 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 у підрозділі 5.5.

Таблиця 6.1

Основна інформація щодо впровадження результатів дисертаційного дослідження у цільових установах

№	Назва цільової установи	Цензурований час впровадження	Узагальнена х–ка конфіденційності, %	Узагальнена х–ка готовності, %	Узагальнена х–ка обслуговуваності, %
1	**2**	**3**	**4**	**5**	**6**
1	Innovative Institute for Material Studies of Intel Research Practice (USA)	01.01.2020 р. – 01.06.2020 р.	P_α = 1,31; P_β = 2,88.	1,00	0,96
2	ARS Online OÜ (a part of the Advertising Agencies Industry, Estonia)	31.01.2020 р. – 1.06.2020 р.	P_α = 1,30; P_β = 2,90.	1,00	0,96
3	Polski Dom Nowych Mediów (Poland)	01.01.2019 р. – 01.06.2020 р.	P_α = 1,31; P_β = 2,95.	1,00	0,94
4	Відділ розпізнавання та синтезу звукових образів Міжнародного науково–навчального центру інформаційних технологій та систем НАН України та МОН України	01.10.2019 р. – 31.12.2019 р.	P_α = 2,47; P_β = 3,11.	-	-
5	Хмельницьке міське комунальне підприємство «Хмельницькінфоцентр»	11.02.2019 р. – 30.06.2020 р.	P_α = 1,41; P_β = 1,13.	1,00	-
6	Львівське комунальне підприємство «Міський центр інформаційних технологій»	04.03.2019 р. – 30.12.2019 р.	P_α = 1,03; P_β = 0,97.	0,96	0,96
7	Департамент інформаційних технологій ВінМР (Ситуаційний центр м. Вінниці)	01.11.2019 р. – 31.01.2020 р.	P_α = 1,37; P_β = 3,11.	0,93	0,88
8	КП «Вінницький інформаційний центр»	01.11.2019 р. – 31.01.2020 р.	P_α = 0,76; P_β = 2,84.	0,98	0,94
9	ДОЗК Він. ОДА МОЗ України «Вінницький обласний центр медико–соціальної експертизи»	01.03.2019 р. – 31.01.2020 р.	P_α = 0,13; P_β = 1,09.	0,99	0,97
10	КНП ДОЗ Він. МР «Центр первинної медико–санітарної допомоги №3»	01.03.2019 р. – 31.01.2020 р.	P_α = 1,22; P_β = 3,33.	0,91	0,74
11	ТОВ «Агро-помсервіс»	01.01.2019 р. – 01.06.2020 р.	P_α = 1,32; P_β = 2,02.	1,00	0,98
12	ТОВ «Вінницяелектроконтакт»	01.01.2019 р. – 01.06.2020 р.	P_α = 1,30; P_β = 2,75.	1,00	0,74

З наведених у таблиці 6.1 результатів можна зробити такі висновки:

- у всіх цільових установах імовірність виникнення похибок другого роду перевищувала імовірність виникнення похибок першого роду, що обмовлено

відповідним вибором значення порогу прийняття рішень, розрахованого за методом, описаним у підрозділі 3.2. Враховуючи критичну важливість даних цільових інформаційний систем, відповідні значення порогів вибрано з орієнтацією на мінімізацію ситуації допуску несанкціонованого суб'єкта–користувача, навіть зважаючи на одночасне зростання імовірності недопуску санкціонованого користувача;

- якщо ранжувати цільові установи за зростанням кількості суб'єктів–користувачів, санкціонованих для доступу до критично важливих інформаційних ресурсів, то отримаємо ряд виду 3, 4, 2, 1. Простежується залежність між кількості суб'єктів–користувачів у цільовій установі і значенням узагальненої характеристики конфіденційності, що говорить про потенціал до оптимізації параметричного простору і моделі прийняття рішень процесу автентифікації суб'єктів за голосом;

- якщо ранжувати цільові установи за зростанням усередненого віку апаратної компоненти їх інформаційних систем, то отримаємо ряд виду 3, 2, 1, 4. Простежується залежність між віком апаратної складової інформаційної системи цільової установи і відповідними значеннями узагальнених характеристик готовності і обслуговуваності, що іще раз акцентує увагу на необхідності своєчасного оновлення апаратної компоненти і необхідності резервування апаратних ресурсів на етапі проектування системи, обсяг якого можна оцінити за методом, описаним у підрозділі 5.3.

Окремо відзначимо, що всі обчислювальні експерименти, результати яких наведено у фінальних частинах підрозділів 5.1–5.5, отримано на основі даних впровадження результатів дисертаційної роботи у департаменті інформаційних технологій Вінницької міської ради.

Висновки до шостого розділу

1. 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 виду (2.1), (2.24) 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 виду (2.46), (2.64) 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.

2. 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 у попередній фільтрації мовленнєвого сигналу із подальшим розрахунком характеристики, оберненої усередненому часовому інтервалу між першими (від двох до шісти) сусідніми максимумами функції кореляції. Здійснене з тією ж метою удосконалення спектрального методу оцінювання частоти основного тону і обертонів мовленнєвого сигналу полягає у змістовному представленні

досліджуваного мовленнєвого сигналу нормованою спектральною щільністю потужності , розрахованої за методикою кореляційних вікон на основі виразу (3.51). 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).

3. 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.

4. 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.

5. Синтезовано і продемонстровано на прикладі повний цикл аналітичних операцій для реалізації інформаційної технології автентифікації суб’єкта за індивідуальністю голосу в мовленнєвому сигналі, яка визначає рівень конфіденційності цільової інформаційної системи критичного застосування, та для реалізації узагальненої інформаційної технології для оптимізації обраного атрибуту гарантоздатності цільової ІСКЗ.

Основні результати розділу опубліковано в [83, 84].

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:

– Синтезовано інформаційну технологію автентифікації суб’єкта за індивідуальністю голосу в мовленнєвому сигналі (рис. 6.11) 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 представленій в розділі 2 методології квазідетермінованих і стохастичних моделей індивідуальності голосу. Останні дозволяють отримати компактний, інформативний і адекватний параметричний опис індивідуальності сегментів мовленнєвих сигналів із високим і помірним рівнем вокалізації.

– Синтезовано інформаційну технологію (рис. 6.14) і узагальнений аналітичний метод для оптимізації обраного атрибуту гарантоздатності цільової інформаційної системи критичного застосування, якої описано у фор-

малізмі 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, що дозволяє визначати рівень шуму як у вокалізованих, так і у невокалізованих сегментах мовленнєвих сигналів.

– 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, що дозволило підвищити конфіденційність процесу автентифікації, готовність цільової інформаційної системи і оптимізувати процес навчання імовірнісного класифікатора.

– 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, що дозволяє максимізувати інформативність інтерпретації вхідної спектрограми нейромережею автоматично, в про-

цесі її навчання, та, за рахунок введення bottleneck-шару, отримати новий набір характеристичних параметрів для опису індивідуальності мовленнєвого матеріалу із шумом.

Представлена в таблиці 6.1 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 ВИКОРИСТАНИХ ДЖЕРЕЛ

[1] L. F. Robert, and R. A. R Norma, *Critical Systems Thinking: Current Research and Practice.* Germany: Springer Science & Business Media, 2007.

[2] V. P. Nandish, *Critical Systems Analysis and Design: A Personal Framework Approach.* USA, NY: Psychology Press, 2005.

[3] C. Dale, and T. Anderson, "Safety-Critical Systems: Problems, Process and Practice," in *Proceedings of the Seventeenth Safety-Critical Systems Symposium*, Brighton, UK, 3–5 February 2009. Springer Science & Business Media, 2009.

[4] M. Bozzano, and A. Villafiorita, *Design and Safety Assessment of Critical Systems*. Boca Raton, USA: CRC Press, 2010.

[5] M. Rausand, *Reliability of Safety-Critical Systems: Theory and Applications.* Hoboken, USA: John Wiley & Sons, 2014.

[6] S. Gnesi, and T. Margaria, *Formal Methods for Industrial Critical Systems: A Survey of Applications*. Hoboken, USA: John Wiley & Sons, 2012.

[7] P. Millot, *Risk Management in Life-Critical Systems.* Hoboken, USA: John Wiley & Sons, 2014.

[8] W. Ding, *Using Model Checking to Generate Test Cases for Critical Systems*. USA: George Mason University, 2000.

[9] C. Brooke, *Critical Management Perspectives on Information Systems*. London, UK: Routledge, 2009.

[10] R. Wallace, *Information Theory Models of Instabilities in Critical Systems.* World Scientific, 2016.

[11] В. С. Харченко, «Гарантоздатність комп'ютерних систем: проблеми і результати,» *Авіаційнокосмічна техніка і технологія*, № 7(23), с. 352–376, 2005.

[12] В. С. Харченко, «Гарантоспособность и гарантоспособные системы: элементы методологии,» *Радіоелектронні і комп'ютерні системи*, № 5(17), с. 7–19, 2006.

[13] В. С. Харченко, «Гарантоздатність комп’ютерних систем: проблеми, напрямки досліджень, результати,» *Радіоелектронні і комп’ютерні системи*, № 5(17), с. 105–109, 2006.

[14] В. С. Харченко, «Гарантоздатність комп’ютерних систем: межа універсальності в контексті інформаційно-технічного стану,» *Радіоелектронні і комп’ютерні системи*, № 8, с. 8–16, 2007.

[15] В. Глухов, «Оцінювання гарантоздатності криптографічних комп’ютерних систем,» *Вісник Національного університету "Львівська політехніка"*, № 616: *Комп’ютерні науки та інформаційні технології*, с. 66–72, 2008.

[16] А. В. Федухин, и В. П. Пасько, «К вопросу о количественных характеристиках безотказности избыточных компьютерных систем,» *Математические машины и системы*, № 1, с. 180–188, 2012.

[17] А. В. Федухин, и Г. Н. В. Сеспедес, «Атрибуты и метрики гарантоспособных компьютерных систем,» *Математические машины и системы*, № 2, с. 195–201, 2013.

[18] А. В. Федухин, и Б. Г. Мудла, «Гарантоспособность компьютерных систем – мода или объективная необходимость,» *Математические машины и системы*, № 4, с. 179–188, 2014.

[19] В. Г. Сербін, та А. І. Сухомлин, «Визначення і формалізація основних показників гарантоздатності живучих комп’ютерних систем керування на основі ймовірнісно-фізичного підходу для їх проектної оцінки і прогнозування,» *Математические машины и системы*, № 4, с. 182–189, 2012.

[20] Г. С. Теслер, «Концепция построения гарантоспособных вычислительных систем,» *Математические машины и системы*, № 1, с. 134–145, 2006.

[21] Г. С. Теслер, «Решение проблемы гарантоспособности компьютерных систем в аспекте базисов компьютерной науки,» *Математические машины и системы*, № 4, с. 171–189, 2008.

[22] Б. Г. Мудла, Т. І .Єфімова, та Р. М. Рудько, «Гарантоздатність як фундаментальний узагальнюючий та інтегруючий підхід,» *Математические машины и системы*, № 2, с. 148–165, 2010.

[23] Р. Ю. Царев, Д. В. Капулин, Д. В. Машурова, Я. А. Тынченко, и Д. Н. Ковтанюк, «Многоатрибутивное формирование гарантоспособных систем управления и обработки информации,» С*ибирский журнал науки и технологий*, № 5(45), с. 106–110, 2012.

[24] И. Б. Шубинский, А. М. Замышляев, и Л. Р. Папич, «Адаптивная гарантоспособность информационных систем управления,» *Надежность*, № 4(18). с. 3–9. doi:10.21683/1729-2646-2018-18-4-3-9.

[25] W. Hasselbring, *Dependability Engineering*. Berlin, Germany: GITO mbH Verlag, 2006.

[26] F. J. Redmill, *Dependability of Critical Computer Systems*. USA, NY: Springer Science & Business Media, 1989.

[27] S. Bernardi, J. Merseguer, and D. Corina Petriu, *Model-Driven Dependability Assessment of Software Systems*. USA, NY: Springer Science & Business Media, 2013.

[28] M. Tokoro, *Open Systems Dependability: Dependability Engineering for Ever-Changing Systems*. USA, NY: CRC Press, 2012.

[29] IEC-TC56: Dependability Standards and Supporting Standards [Online]. Available: http://www2.fiu.edu/~revellk/pad3003/Neave.pdf. Accessed on: August 26, 2020.

[30] 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.

[31] 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.

[32] 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.

[33] 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.

[34] 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.

[35] 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.

[36] В. В. Ковтун, та М. М. Биков, «Оцінювання надійності автоматизованих систем розпізнавання мовців критичного застосування,» *Вісник Вінницького політехнічного інституту*, № 2, с. 70–76, 2017.

[37] 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.

[38] 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.

[39] 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.

[40] 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.

[41] 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.

[42] 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]. Доступно: http://jes.sumdu.edu.ua/wp-content/uploads/2017/11/JES_2017_01_H14-H20.pdf Дата звернення: Серпень 26, 2020.

[43] 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.

[44] В. В. Ковтун, та Т. В. Грищук, «Підвищення шумостійкості автоматизованої системи розпізнавання мовця критичного застосування,» *Вісник Вінницького політехнічного інституту*, № 1, с. 98–111, 2018.

[45] 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.

[46] 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.

[47] В. В. Ковтун, «Оцінювання основного тону у автоматизованій системі розпізнавання мовця критичного застосування,» *Вісник Вінницького політехнічного інституту*, №4. с. 61-73, 2018.

[48] 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.

[49] 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.

[50] 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.

[51] 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.

[52] 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.

[53] 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.

[54] 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.

[55] 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.

[56] 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.

[57] 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.

[58] 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.

[59] 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.

[60] В. В. Ковтун, *Моделі атрибутів гарантоздатності інформаційної системи критичного застосування із автентифікацією суб’єкта за голосом* : монографія, Вінниця : ВНТУ, 2020.

[61] A. Avizienis, J.-C. Laprie, B. Randell and C. Landwehr, “Basic concepts and taxonomy of dependable and secure computing,” *IEEE Transactions on Dependable and Secure Computing*, Vol. 1, No. 1, pp. 11– 33, 2004. doi: 10.1109/TDSC.2004.2.

[62] J. Arlat, A. Costes, Y. Crouzet, J.-C. Laprie and D. Powell, “Fault injection and dependability evaluation of fault-tolerant systems,” *IEEE Transactions on Computers*, Vol. 42, No. 8, pp. 913–923, 1993. doi: 10.1109/12.238482.

[63] J. Arlat et al., “Fault injection for dependability validation: a methodology and some applications,” *IEEE Transactions on Software Engineering*, Vol. 16, No. 2, pp. 166-182, 1990. doi: 10.1109/32.44380..

[64] J.-C. Laprie, “Dependability Evaluation of Software Systems in Operation,” *IEEE Transactions on Software Engineering*, Vol. SE-10, No. 6, pp. 701–714, 1984. doi: 10.1109/TSE.1984.5010299..

[65] Л A. Avižienis, “The architecture of a resilience infrastructure for computing and communication systems,” *43rd Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*, Budapest, pp. 1-2, 2013. doi: 10.1109/DSN.2013.6575340.

[66] E. Bauer, *Design for reliability: information and computer-based systems*. USA: IEEE Press + Wiley, 2010.

[67] A. Avizienis, “A fault tolerance infrastructure for dependable computing with high-performance COTS components,” *International Conference on Dependable Systems and Networks. DSN*, New York, NY, USA, pp. 492-500, 2000. doi: 10.1109/ICDSN.2000.857581.

[68] О. Г. Додонов, М. Г. Кузнєцова, и О. С. Горбачик, *Живучість складних систем: аналіз та моделювання*. К.: НТУУ КПІ, 2009.

[69] B. Randell, “Dependability-a unifying concept,” *Computer Security, Dependability, and Assurance: From Needs to Solutions (Cat. No.98EX358)*, York, UK & Williamsburg, VA, USA, pp. 16-25, 1998. doi: 10.1109/CSDA.1998.798354..

[70] В. П. Тарасенко, А. Ю. Маламан, Ю. П. Черніченко, та В. І. Корнійчук, *Надійність комп’ютерних систем*. К.: Корнійчук, 2007.

[71] B. Randell, “Dependable pervasive systems,” *23rd IEEE International Symposium on Reliable Distributed Systems*, Florianpolis, Brazil, pp. 2-, 2004 doi: 10.1109/RELDIS.2004.1352998.

[72] В. М. Дубовой, *Моделювання систем контролю та керування*. Вінниця: ВНТУ, 2005.

[73] A. Gorbenko, A. Romanovsky and V. Kharchenko, “How to Enhance UDDI with Dependability Capabilities,” 32nd Annual IEEE International Computer Software and Applications Conference, Turku, pp. 1023-1028, 2008. doi: 10.1109/COMPSAC.2008.33.

[74] Y. Chen and A. Romanovsky, “Improving the Dependability of Web Services Integration,” *IT Professional*, Vol. 10, No. 3, pp. 29-35, 2008. doi: 10.1109/MITP.2008.49..

[75] R. de Lemos, C. Gacek and A. Romanovsky, “Workshop on Architecting Dependable Systems (WADS),” *International Conference on Dependable Systems and Networks (DSN'06)*, Philadelphia, PA, pp. 592-592, 2006. doi: 10.1109/DSN.2006.78..

[76] И. А. Рябинин, *Надежность и безопасность структурно-сложных систем*. СПб: Политехника, 2000.

[77] Z. Andrews, J. Fitzgerald, R. Payne and A. Romanovsky, “Fault modelling for systems of systems,” *IEEE Eleventh International Symposium on Autonomous Decentralized Systems (ISADS)*, Mexico City, Mexico, pp. 1-8, 2013. doi: 10.1109/ISADS.2013.6513445.

[78] A. Romanovsky and I. Smith, “Dependable on-line upgrading of distributed systems,” 26th Annual International Computer Software and Applications, Oxford, UK, pp. 975-976, 2002. doi: 10.1109/CMPSAC.2002.1045132..

[79] Э. Дж. Хенли, и Х. Кумамото, *Надежность технических систем и оценка риска*. М.: Машиностроение, 1984.

[80] С. П. Тимошенков, Б. М. Симонов, В. Н. Горошко, *Надежность технических систем и техногенный риск*. М.: Юрайт, 2018.

[81] Н. А. Северцев, и В. Н. Темнов, *Метрологическое обеспечение безопасности сложных технических систем*. М.: Курс: Инфра-М, 2015.

[82] 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.

[83] 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.

[84] 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.

[85] В. А. Зорин, *Основы работоспособности технических систем*. М.: Академия, 2009.

[86] А. В. Гуськов, и К. Е. Милевский, *Надежность технических систем и техногенный риск*. Новосибирск: НГТУ, 2007.

[87] Л. Н. Александровская, А. П. Афанасьев, и А. А. Лисов, *Современные методы обеспечения безотказности сложных технических систем*. М.: Логос, 2001.

[88] Д. К. Потресов, и Д. В. Скоморохов, «Факторы надежности информационных систем высокой готовности,» *Горный информационно-аналитический бюллетень (научно-технический журнал)*, № 5, с. 134–139, 2013.

[89] В. В. Гришин, «Модель готовности сложной технической системы управления,» *Информационно-управляющие системы*, № 6, с. 8–11, 2004.

[90] А. О. Недосекин, В. В. Виноградов, и З. И. Абдулаева, *Методы и модели оценки функциональной живучести структурно-сложных технических систем*. СпБ: Изд-во Политехнического университета, 2018.

[91] А. Г. Додонов, и Д. В. Флейтман, «Технологические аспекты обеспечения живучести информационных систем,» *Известия Южного федерального университета. Технические науки*, № 4(48), с. 5–7, 2005.

[92] А. И. Елисеев, Ю. В. Минин, и Г. Г. Ягудаев, «Графовая модель показателей частных характеристик живучести сетевых информационных структур,» *Вестник Воронежского института МВД России*, № 1, с. 73–78, 2013.

[93] А. Г. Додонов, Е. С. Горбачик, и М. Г. Кузнецова, «Живучесть компьютерных систем и безопасность информационной инфраструктуры,» *Известия Южного федерального университета. Технические науки*, № 1(76), с. 203–207, 2007.

[94] Д. К. Потресов, и Д. В. Скоморохов, «Факторы надежности информационных систем высокой готовности,» *Горный информационно-аналитический бюллетень (научно-технический журнал)*, № 5, с. 134–139, 2013.

[95] G. B. Digo, and N. B. Digo, “Approximation of domains of serviceability and attainability of control system on the basis of the inductive approach,” *Reliability: Theory & Applications*, vol. 6, no. 2(21), pp. 41-46, 2011.

[96] A. I. Awad, and M. Fairhurst, *Information Security. Foundations, technologies and applications*. USA: The Institution of Engineering and Technology, 2018.

[97] M. Bishop, *Computer Security: Art and Science*. 2nd ed. USA: Addison-Wesley Professional, 2018.

[98] В. В. Бондарев, *Введение в информационную безопасность автоматизированных систем*. М.: МГТУ им. Н. Э. Баумана, 2016.

[99] В. И. Ярочкин, *Информационная безопасность*. Учебник для вузов. 2-е издание. М.: Академический Проект, Гаудеамус, 2004.

[100] В. Ф. Шаньгин, *Информационная безопасность*. М.: ДМК Пресс, 2014.

[101] С. А. Филин, *Информационная безопасность*. М.: Альфа-Пресс, 2006.

[102] О. О. Шумейко, *Інформаційна безпека*. Дніпродзержинськ: Дніпродзержинський державний технічний університет, 2012.

[103] О. Б. Проценко, та К. В. Меркулова, *Кібербезпека у системі національної безпеки України: пріоритетні напрями розвитку*. Маріуполь: Маріупольський державний університет, 2018.

[104] Ю. Н. Сычев, *Стандарты информационной безопасности. Защита и обработка конфиденциальных документов*. М.: РЭУ им. Г. В. Плеханова, 2017.

[105] А. А. Парошин, *Информационная безопасность: стандартизированные термины и понятия*. Владивосток: Дальневосточный университет, 2010.

[106] В. П. Кириленко, и Г. В. Алексеев, *Международное право и информационная безопасность государства*. СПб: СПбГИКиТ, 2016.

[107] А. А. Афанасьев, Л. Т. Веденьев, А. А. Воронцов и др., *Аутентификация. Теория и практика. Обеспечение безопасного доступа к информационным ресурсам*. М.: Горячая линия-Телеком, 2009.

[108] О. Р. Лапонина, *Криптографические основы безопасности*, 2-е изд. М.: Национальный Открытый Университет ИНТУИТ, 2016.

[109] С. Бармен, *Разработка правил информационной безопасности*. М.: Вильямс, 2002.

[110] M. Rausand, *Reliability of Safety-Critical Systems: Theory and Applications*. New Jersey: Wiley, Hoboken, 2014.

[111] E. Griffor, *Handbook of System Safety and Security. Cyber Risk and Risk Management, Cyber Security, Threat Analysis, Functional Safety, Software Systems, and Cyber Physical Systems*. Amsterdam: Syngress, 2017.

[112] В. В. Липаев, *Надежность и функциональная безопасность комплексов программ реального времени*. Саратов: Вузовское образование, 2015.

[113] В. В. Белозеров, А. Ю. Любавский, и С. Н. Олейников, *Модели диагностики надежности и безопасности СВТ и АСУ объектов техносферы*. М.: Издательский дом Академия Естествознания, 2015. doi:10.17513/np.133.

[114] H. Pham, *Safety and Risk Modeling and Its Applications*. USA: Springer, 2011.

[115] D. Antonucci, *The Cyber Risk Handbook: Creating and Measuring Effective Cybersecurity Capabilities*. USA: Wiley, 2017.

[116] А. П. Курило, Н. Г. Милославская, М. Ю. Сенаторов, и А. И. Толстой, *Управление рисками информационной безопасности*, 2-е изд., испр. М.: Горячая линия-Телеком, 2014.

[117] G. C. Wilshusen, *Cybersecurity: Continued Efforts Are Needed to Protect Information Systems Form Evolving Threats: Congressional Statement for the Record*. USA: DIANE Publishing, 2010.

[118] K. A. Wager, F. W. Lee, and J. P. Glaser, *Managing Health Care Information Systems: A Practical Approach for Health Care Executives*. USA: John Wiley & Sons, 2005.

[119] Rainbow Books. *Wikipedia* : web-site. [Online]. Available: https://en.wikipedia.org/wiki/Rainbow_Books Accessed on: August 26, 2020.

[120] S. Sumathi, and S. Esakkirajan, *Fundamentals of Relational Database Management Systems*. USA: Springer Science & Business Media, 2007.

[121] В. А. Сердюк, *Организация и технологии защиты информации : обнаружение и предотвращение информационных атак в автоматизированных системах предприятий*. М.: Издательский дом Высшей школы экономики, 2011.

[122] Ю. Н. Загинайлов, *Теория информационной безопасности и методология защиты информации*. Барнаул: Directmedia, 2015.

[123] Н. В. Скабцов, *Аудит безопасности информационных систем*. СПб: Питер, 2017.

[124] T. R. Peltier, *Information Security Policies and Procedures: A Practitioner's Reference, Second Edition*. USA: CRC Press, 2004.

[125] J. L. Bayuk, J. Healey, and P. Rohmeyer, *Cyber Security Policy Guidebook*. USA: Wiley, 2012.

[126] В И. Шестухина, *Теоретические основы компьютерной безопасности*. Учебное пособие. Хабаровск: ДВГУПС, 2008.

[127] А. В. Овчинников, и В. Г. Семин, *Обеспечение информационной безопасности автоматизированных систем транснациональных корпораций (АСТК)*. Учеб. пособие. М.: РУДН, 2008.

[128] А. Ю. Щеглов, *Модели, методы и средства контроля доступа к ресурсам вычислительных систем*. СПб: Университет ИТМО, 2014.

[129] С. В. Белим, и С. В. Усов, «Объектно-ориентированный подход в построении дискреционной политики безопасности,» *Математические структуры и моделирование*, № 2(20), с. 153–159, 2009.

[130] В. Ю. Мельников, и Е. К. Пугачев, *Методы защиты операционных систем и данных*. М.: МГТУ им. Баумана, 2017.

[131] В. В. Гуренко, и Б. И. Бычков, «Анализ структур данных для представления базовых моделей конечных автоматов,» *Машиностроение и компьютерные технологии*, № 2, с. 150–168, 2015.

[132] И. А. Гудкова, и Н. Д. Масловская, «Вероятностная модель для анализа задержки доступа к инфраструктуре облачных вычислений с системой мониторинга,» *T-Comm - Телекоммуникации и Транспорт*, № 6, с. 13–15, 2014.

[133] Е. А. Рогозин, и А. Д. Попов, «Модель функционирования типовой системы защиты информации от несанкционированного доступа в автоматизированных информационных системах ОВД,» *Вестник Воронежского института МВД России*, № 4, с. 122–131, 2016.

[134] A. Acquisti, S. Gritzalis, C. Lambrinoudakis, S. Di Vimercati at al., *Digital Privacy. Theory, Technologies, and Practices*. Germany: Auerbach Publications, 2008.

[135] В. Ф. Шаньгин, *Защита компьютерной информации. Эффективные методы и средства*. М.: ДМК Пресс, 2010.

[136] В. А. Хорошко, и А. А. Чекатков, *Методы и средства защиты информации*. К.: Юниор, 2003.

[137] В. И. Петренко, *Теоретические основы защиты информации*. Ставрополь: СКФУ, 2015.

[138] С. Е. Остапов, С. П. Євсеєв, и О. Г. Король, *Технології захисту інформації*. Харків: ХНЕУ, 2013.

[139] А. А. Малюк, *Теория защиты информации*. М.: Горячая линия – Телеком, 2012.

[140] С. В. Ленков, Д. А. Перегудов, и В. А. Хорошко, *Методы и средства защиты информации*. Том 2. Информационная безопасность. К.: Арий, 2008.

[141] С. В. Войцеховский, А. С. Марковский, и В. А. Палагушин, *Защита информации в автоматизированных системах*. СПб.: Питер, 2005.

[142] Б. Ю. Анин, *Защита компьютерной информации*. СПб: БХВ-Петербург, 2000.

[143] R. Zeidman, *The Software IP Detective's Handbook: Measurement, Comparison, and Infringement Detection*. UK: Pearson Education, 2011.

[144] А. Ю. Зубов, *Математика кодов аутентификации*. М.: Гелиос АРВ, 2007.

[145] Основная теорема безопасности Белла-Лападулы. *Википедия* [Электронный ресурс]. Доступ: https://ru.wikipedia.org/wiki/Модель_Белла_—_Лападулы Дата обращения: Авг. 26, 2020.

[146] В. С. Симанков, и Е. В. Луценко, *Адаптивное управление сложными системами на основе теории распознавания образов*. Краснодар: ТУ КубГТУ, 1999.

[147] И. В. Мирошник, *Теория автоматического управления. Линейные системы*. СПб: Питер, 2005.

[148] В. Н. Афанасьев, *Управление неопределенными системами*. М.: РУДН, 2008.

[149] И. В. Мирошник, В. О. Никифоров, и А. Л. Фрадков, *Нелинейное и адаптивное управление сложными динамическими системами*. СПб: Наука, 2000.

[150] Y. Haimes, *Modeling and Managing Interdependent Complex Systems of Systems*. USA: Wiley-IEEE Press, 2019.

[151] E. E. N. Macau, *A Mathematical Modeling Approach from Nonlinear Dynamics to Complex Systems*. USA: Springer, 2019.

[152] Q. Zhu, and A. T. Taher Azar, *Complex System Modelling and Control Through Intelligent Soft Computations*. USA: Springer, 2015.

[153] A. Ioannou Petros, and A. Pitsillides, *Modeling and Control of Complex Systems*. USA: CRC Press, Taylor & Francis Group, 2008.

[154] J. Lü, X. Yu, G. Chen, and W. Yu, *Complex Systems and Networks: Dynamics, Controls and Applications*. Berlin, Heidelberg: Springer-Verlag, 2016.

[155] T. R. J. Bossomaier, and D. G. Green, *Complex Systems*. UK: Cambridge University Press, 2000.

[156] M. Davoodi, N. Meskin, and K. Khorasani, *Integrated Fault Diagnosis and Control Design of Linear Complex Systems*. New York: The Institution of Engineering and Technology, 2017.

[157] G. G. Schulmeyer at al., *Handbook of Software Quality Assurance*. Fourth Edition. USA: Artech House, 2007.

[158] D. Galin, *Software Quality: Concepts and Practice*. USA: Wiley, 2018.

[159] Б В. Черников, *Управление качеством программного обеспечения*. М.: Форум, 2012

[160] Т. К. Винцюк, *Анализ, распознавание и интерпретация речевых сигналов*. Киев: Наук. думка, 1987.

[161] J. A. Anderson, *Automata Theory with Modern Applications*. UK: Cambridge University Press, 2006.

[162] Г. С. Рамишвили, *Речевой сигнал и индивидуальность голоса*. Тбилиси: Мецниереба, 1976.

[163] J.-É. Pin, *Mathematical Foundations of Automata Theory*. Paris: Jean-Eric Pin, 2016.

[164] Д. Хопкрофт, Р. Мотвани, и Дж. Ульман, *Введение в теорию автоматов, языков и вычислений*. 2-е изд. М.: Вильямс, 2002.

[165] A. Bondy, and U. S. R. Murty, *Graph Theory*. USA: Springer, 2008.

[166] L. Novak, and A. Gibbons, *Hybrid Graph Theory and Network Analysis*. UK: Cambridge University Press, 1999.

[167] Д. В. Карпов, *Теория графов*. СПБ: Санкт-Петербургское отделение Мат. института им. В. А. Стеклова РАН, 2017.

[168] Н. П. Хоменко, *Топологические аспекты теории графов*. К.: Издание Института математики АН УССР, 1971.

[169] А. Е. Пентус, и М. Р. Пентус, *Математическая теория формальных языков*. М.: Интернет-университет информационных технологий; БИНОМ. Лаборатория знаний, 2006.

[170] G. Bel-Enguix, and M. D. Jiménez-López, *New Developments in Formal Languages and Applications*. USA: Springer, 2008.

[171] S. C. Reghizzi, *Formal Languages and Compilation*. USA: Springer, 2009.

[172] D. H. Greene, and D. E. Knuth, *Mathematics for the Analysis of Algorithms*. Germany: Birkhauser, 2008.

[173] L. Parida, *Pattern Discovery in Bioinformatics. Theory & Algorithms*. USA: Chapman & Hall / CRC Press, 2008.

[174] В. Н. Крупский, и В. Е. Плиско, *Теория алгоритмов*. М.: Академия, 2009.

[175] В. И. Игошин, *Математическая логика и теория алгоритмов*. 2-е изд. М.: Академия, 2008.

[176] P. Gatti, *Probability theory and mathematical statistics for engineers*. Londonand New-York: Spon Press. 2005.

[177] A. A. Borovkov, *Probability Theory*. USA: Springer, 2013.

[178] W. Linde, *Probability Theory: A First Course in Probability Theory and Statistics*. Germany: Walter de Gruyter GmbH, 2016.

[179] Н. Г. Тактаров, *Теория вероятностей и математическая статистика: Краткий курс с примерами и решениями*. М.: УРСС, 2010.

[180] В. Н. Тарасов, и Н. Ф. Бахарева, *Теория вероятностей, математическая статистика и случайные процессы*. 3-е изд. Самара: Изд-во ПГУТИ, 2017.

[181] W. Penczek, and A. Półrola, *Advances in Verification of Time Petri Nets and Timed Automata. A Temporal Logic Approach*. USA: Springer, 2006.

[182] N. Wu, and M. Zhou, *System Modeling and Control with Resource-Oriented Petri Nets*. USA: CRC Press, 2006.

[183] K. Jensen, *Coloured Petri Nets*. USA: Springer, 2009.

[184] T. Aized, *Advances in Petri Net: Theory and Applications*. Pakistan: InTechOpen, 2010.

[185] Дж. Питерсон, *Теория сетей Петри и моделирование систем*. М.: Мир, 1984.

[186] MengChu Zhou, *Petri Nets in Flexible and Agile Automation*. USA: Springer Science & Business Media, 2012.

[187] E. Badouel, L. Bernardinello, and P. Darondeau, *Petri Net Synthesis*. USA: Springer, 2015.

[188] E. Best, R. Devillers, and M. Koutny, *Petri Net Algebra*. USA: Springer Science & Business Media, 2001.

[189] J. Janssen, *Semi-Markov Models: Theory and Applications*. USA: Springer, 2013.

[190] B. Harlamov, *Continuous Semi-Markov Processes*. USA: Wiley, 2008.

[191] V. S. Barbu, and N. Limnios, *Semi-Markov Chains and Hidden Semi-Markov Models toward Applications: Their use in Reliability and DNA Analysis*. USA: Springer, 2008.

[192] S.-Z. Yu, *Hidden Semi-Markov Models: Theory, Algorithms and Applications*. Amsterdam: Elsevier, 2016.

[193] Теорема Радона-Нікодима *Вікіпедія* [Електронний ресурс]. Доступно: https://uk.wikipedia.org/wiki/Теорема_Радона_—_Нікодима Дата обращения: серпень, 26, 2020.

[194] О. Ю. Мєшков, О. О. Новіков, та В. О Новіков, *Аналіз голосових сигналів людини та аутентифікація особистості за голосом*. Херсон: ФОП Вишемирський В. С., 2018.

[195] М. Н. Григорьев, и С. А. Уваров, *Логистика*. 4-е изд. М.: Юрайт, 2019.

[196] Кардинґ *Вікіпедія* [Електронний ресурс]. Доступно: https://uk.wikipedia.org/wiki/Кардинґ Дата звернення: серпень, 26, 2020.

[197] Корпус української мови MOVA.info [Електронний ресурс]. Доступо: http://www.mova.info/carticle.aspx?l1=210&DID=5347 Дата звернення: серпень, 26, 2020.

[198] Генеральний регіонально анотований корпус української мови [Электронный ресурс]. Доступно: http://uacorpus.org/ Дата звернення: серпень, 26, 2020..

[199] А. Н. Продеус, «Речевые корпуса: создание и проблемы,» *Электротехнические и компьютерные системы*, № 9(85), с. 118–126, 2013.

[200] A. Bouziane, H. Kadi, S. Hourri, and J Kharroubi, “An open and free speech corpus for speaker recognition: The FSCSR speech corpus,” *Proc. 11th*

International Conference on Intelligent Systems: Theories and Applications (SITA), pp. 1–5, 2016. doi: 10.1109/SITA.2016.7772320.

[201] J. P. Campbell, and D. A. Reynolds, “Corpora for the evaluation of speaker recognition systems,” *IEEE International Conference on Acoustics, Speech, and Signal Processing. Proceedings. ICASSP99 (Cat. No.99CH36258)*, pp. 829–832, 1999. doi:10.1109/icassp.1999.759799.

[202] M. Tatham, and K. Morton, *Speech Production and Perception*. UK: Palgrave, 2006.

[203] W. J. Hardcastle, and A. Marchal, *Speech Production and Speech Modelling*. Netherlands: Kluwer, 1990.

[204] S. E. Levinson, *Mathematical Models for Speech Technology*. USA: John Wiley & Sons, 2005.

[205] Jay Timothy, *Why We Curse: A Neuro-Psycho-Social Theory of Speech*. Netherlands: John Benjamins Publishing, 2000.

[206] L. Deng, *Dynamic Speech Models. Theory, Algorithms, and Applications*. California: Morgan & Claypool, 2006.

[207] W. Hess, *Pitch Determination of Speech Signals. Algorithms and Devices*. USA: Springer, 1983.

[208] S. Seneff, *Pitch and Spectral Analysis of Speech Based on an Auditory Synchrony Model*. Barcelona: Universitat Politècnica de Catalunya, 1985.

[209] D. M. Howard, and J. A. S. Angus, *Acoustics and Psychoacoustics. Fourth edition*. Massachusetts: Focal Press, 2010.

[210] H. Fastl, and E. Zwicker, *Psychoacoustics. Facts and Models*. Germany: Springer-Verlag, 2007.

[211] Я. А. Альтман и др., *Слуховая система. Основы современной физиологии*. Л.: Наука, 1990.

[212] А. Б. Сергиенко, *Цифровая обработка сигналов*. СПБ: БХВ-Петербург, 2011.

[213] А. И. Солонина, *Цифровая обработка сигналов. Моделирование в MATLAB*. СПб: БХВ-Петербург, 2008.

[214] F. E. Theunissen, K. Sen, and A. J. Doupe, “Spectral-Temporal Receptive Fields of Nonlinear Auditory Neurons Obtained Using Natural Sounds,” *Journal of Neuroscience*, № 20(6), pp. 2315–2331, 2000. doi:10.1523/JNEUROSCI.20-06-02315.2000.

[215] S. Handel, *Perceptual Coherence: Hearing and Seeing*. UK: Oxford University Press, 2006.

[216] M. S. Malmierca, and D. R. F. Irvine, *Auditory Spectral Processing*. Texas: Gulf Professional Publishing, 2005.

[217] L. Zhao, and L. Zhaoping, “Understanding Auditory Spectro-Temporal Receptive Fields and Their Changes with Input Statistics by Efficient Coding Principles,” *PLoS Computational Biology*, № 7(8), e1002123, 2011. doi:10.1371/journal.pcbi.1002123.

[218] J. Benesty, M. M. Sondhi, and Y. Huang, *Springer Handbook of Speech Processing*. USA: Springer, 2008.

[219] Р. Габасов, и Ф. М. Кириллова, *Основы динамического программирования*. Минск: Изд-во БГУ, 1975.

[220] Р. Арис, *Дискретное динамическое программирование*. М.: Мир, 1969.

[221] Дж. Хедли, *Нелинейное и динамическое программирование*. М.: Мир, 1967.

[222] Х. Бринк, Дж. Ричардс, и М. Феверолф, *Машинное обучение*. СПБ: Питер, 2017.

[223] В. В. Вьюгин, *Математические основы теории машинного обучения и прогнозирования*. М.: МЦНМО, 2013.

[224] Гифт Ной, *Прагматичный ИИ. Машинное обучение и облачные технологии*. СПБ: Питер, 2019.

[225] Ф. Шолле, *Глубокое обучение на Python*. СПБ: Питер, 2018.

[226] Э. Траск, *Грокаем глубокое обучение*. СПБ: Питер, 2019.

[227] Л. Р. Рабинер, и Р. В. Шафер, *Цифровая обработка речевых сигналов*. М.: Радио и связь, 1981.

[228] М. А. Сапожков, и В. Г. Михайлов, *Вокодерная связь*. М.: Радио и связь, 1983.

[229] К. Фукунага, *Введение в статистическую теорию распознавания образов*. М.: Наука, 1979.

[230] Э. А. Патрик, *Основы теории распознавания образов*. М.: Советское радио, 1980.

[231] Дж. Ту, и Р. Гонсалес, *Принципы распознавания образов*. М.: Мир, 1978.

[232] Р. Дуда, и П. Харт, *Распознавание образов и анализ сцен*. М.: Мир, 1976.

[233] Т. К. Вінцюк, М. М. Сажок, Р. А. Селюх, Д. Я. Федорин, О. А. Юхименко, и В. В. Робейко, «Автоматичне розпізнавання, розуміння та синтез мовленнєвих сигналів в Україні,» *Управляющие системы и машины*, № 6. с. 7–24, 2018.

[234] В. В. Булатов, *Введение в математические методы моделирования сложных систем*. М.: ОнтоПринт, 2018.

[235] И. В. Кузьмин, *Основы моделирования сложных систем*. К.: Вища школа, 1980.

[236] В. П. Тарасик, *Математическое моделирование технических систем*. Минск: Дизайн-ПРО, 2004.

[237] А. А. Харкевич, *Основы радиотехники*. 3-е издание, стереотипное. М.: Физматлит, 2007.

[238] М. В. Амалицкий, *Основы радиотехники*. 3-е издание. М.: Связьиздат, 1959.

[239] В. И. Тихонов, *Статистическая радиотехника*. М.: Рипол Классик, 2013.

[240] Л. Е. Варакин, *Теория сложных сигналов*. М.: Рипол Классик, 1970.

[241] T. Herbig, F. Gerl, and W. Minker, *Self-Learning Speaker Identification. A System for Enhanced Speech Recognition*. USA: Springer, 2011.

[242] F. E. El-Samie, *Information Security for Automatic Speaker Identification*. USA: Springer, 2011.

[243] T. B. Alderman, *Forensic Speaker Identification: A Likelihood Ratio-based Approach Using Vowel Formants*. EU: Lincom Europa, 2005.

[244] L. F. Gallardo, *Human and Automatic Speaker Recognition over Telecommunication Channels*. USA: Springer, 2014.

[245] J. Keshet, S. Bengio, *Automatic Speech and Speaker Recognition. Large Margin and Kernel Methods*. USA: Wiley, 2009.

[246] D. D. Zhang, *Automated Biometrics. Technologies and Systems*. Netherlands: Kluwer, 2000.

[247] P. Rose, *Forensic Speaker Identification*. UK: Taylor & Francis, 2002.

[248] A. Neustein, and H. A. Patil, *Forensic Speaker Recognition. Law Enforcement and Counter-Terrorism*. USA: Springer, 2012.

[249] H. Beigi, *Fundamentals of Speaker Recognition*. USA: Springer, 2011.

[250] В. В. Волгин, и Р. Н. Каримов, *Оценка корреляционных функций в промышленных системах управления*. М.: Энергия, 1979.

[251] Е. Н. Львовский, *Статистические методы построения эмпирических функций*. М.: Высшая школа, 1988.

[252] Ю. И. Алимов, *Измерение спектров и статистических вероятностей*. Свердловск: Изд-во Уральского политехнического ин-та, 1986.

[253] Г. Дженкинс, *Спектральный анализ и его приложения*. М.: Мир,1971.

[254] К. Раушер, Ф. Йанссен, и Р. Минихольд, *Основы спектрального анализа*. М.: Горячая линия-Телеком, 2006.

[255] А. М. Крот, и Е. Б. Минервина, *Быстрые алгоритмы и программы спектральной обработки сигналов и изображений*. Минск: Навука і тэхніка, 1995.

[256] М. В. Назаров, и Ю. Н. Прохоров, *Методы цифровой обработки и передачи речевых сигналов*. М.: Радио и связь, 1985.

[257] Д. Маркел, и А. Х. Грей, *Линейное предсказание речи*. М.: Связь, 1980.

[258] О. И. Шелухин, и Н. Ф. Лукьянцев, *Цифровая обработка и передача речи*. М.: Радио и связь, 2000.

[259] Н. К. Обжелян, и В. Н. Трунин-Донской, *Машины, которые говорят и слушают*. Кишинёв: Штиинца, 1987.

[260] Дж. Бокс, и Г. Дженкинс, *Анализ временных рядов прогноз и управление*. Кн.1. М.: Мир, 1974.

[261] С. Малла, *Вейвлеты в обработке сигналов*. М.: Мир, 2005.

[262] А. В. Фролов, и Г. В. Фролов, *Синтез и распознавание речи. Современные решения*. М.: Связь, 2003.

[263] Ю. Ю. Громов, О. Г. Иванова, В. О. Драчев, и В. В. Алексеев, *Фрактальный анализ и процессы в компьютерных сетях*. Тамбов: ТГТУ, 2012.

[264] В. Н. Сорокин, *Синтез речи*. М.: Наука, 1992.

[265] Дж. Л. Фланаган, *Анализ, синтез и восприятие речи*. М.: Связь, 1968.

[266] N. R. Shabtai, *Advances in Speech Recognition*. Pakistan: InTech, 2010.

[267] A. J. Rubio Ayuso, and J. M. Lopez Soler, *Speech Recognition and Coding. New Advances and Trends*. USA: Springer, 1995.

[268] F. Mihelič, and J. Žibert, *Speech Recognition. Technologies and Applications*. Pakistan: InTech, 2008.

[269] Z.-H. Tan, and B. Lindberg, *Automatic Speech Recognition on Mobile Devices and over Communication Networks*. USA: Springer, 2008.

[270] С. Е. Фалькович, и Э. И. Хомяков, *Статистическая теория измерительных радиосистем*. М.: Радио и связь, 1981.

[271] А. Н. Лукин, *Радиофизические методы измерения параметров сложных источников излучения* : дис. докт. физ.-мат. наук : 01.04.03 / Воронеж, 1998.

[272] Г. Корн, *Справочник по математике для научных работников и инженеров*. М.: Наука, 1973.

[273] И. Н. Бронштейн, и К. А. Семендяев, *Справочник по математике для инженеров и учащихся втузов*. 10-е издание. М.: Наука, 1964.

[274] В. И. Тихонов, и Н. К. Кульман, *Нелинейная фильтрация и квазикогерентный прием сигналов*. М.: Советское радио, 1975.

[275] Э. С. Айфичер, и Б. У. Джервис, *Цифровая обработка сигналов: практический подход*. М.: Вильямс, 2004.

[276] Преобразование Гильберта *Википедия* [Электронный ресурс]. Доступно: https://ru.wikipedia.org/wiki/Преобразование _Гильберта Дата обращения: Авг. 26, 2020.

[277] Критерий Бартлетта *Википедия* [Электронный ресурс]. Доступно: https://ru.wikipedia.org/wiki/Критерий_Бартлетта Дата обращения: Авг. 26, 2020.

[278] Ю. Н. Прохоров, *Статистические модели и рекуррентное предсказание речевых сигналов*. М.: Радио и связь, 1984.

[279] Ю. Г. Сосулин, *Теория обнаружения и оценивания стохастических сигналов*. М.: Сов. радио, 1978.

[280] И. Д. Мандель, *Кластерный анализ*. М.: Финансы и статистика, 1988.

[281] М. Кендалл, и А. Стьюарт, *Статистические выводы и связи*. М.: Наука, 1973.

[282] NOIZEUS: Noisy speech corpus – Univ. Texas-Dallas [Online]. Available: https://ecs.utdallas.edu/loizou/speech/noizeus/ Accessed on: August 26, 2020.

[283] Ф. Р. Гантмахер, *Теория матриц*. М.: ФИЗМАТЛИТ, 2004. 560 с.

[284] В. Н. Тарасов, и Н. Ф. Бахарева, *Математическое программирование. Теория, алгоритмы, программы*. Самара: Гольфстрим, 2007.

[285] А. М. Загребаев и др., *Методы математического программирования в задачах оптимизации сложных технических систем*. М.: МИФИ, 2007.

[286] А. В. Кузнецов, В. А. Сакович, и Н. И. Холод, *Высшая математика. Математическое программирование*. 4-е изд., стер. СПб: Лань, 2013.

[287] Е. Янке, Ф. Эмде, и Ф. Лёш, *Специальные функции*. М.: Наука, 1977.

[288] В. Ю. Королёв, *EM-алгоритм, его модификации и применение к задаче разделения смесей вероятностных распределений*. М.: ИПИ РАН, 2007.

[289] Р. Н. Вадзинский, *Справочник по вероятностным распределениям*. М.: Наука, 2001.

[290] M. N. Stuttle, *A Gaussian Mixture Model Spectral Representation for Speech Recognition*. UK: Cambridge University, 2003.

[291] A. Salazar, *On Statistical Pattern Recognition in Independent Component Analysis Mixture Modelling*. USA: Springer, 2013.

[292] Unsupervised Machine Learning in Python. Master Data Science and Machine Learning with Cluster Analysis, Gaussian Mixture Models, and Principal Components Analysis. LazyProgrammer, 2016. 66 p. [Online]. Available: https://lazyprogrammer.me/ Accessed on: August 26, 2020.

[293] А. В. Аграновский, и Д. А. Леднов, *Теоретические аспекты алгоритмов обработки и классификации речевых сигналов*. М.: Радио и связь, 2004.

[294] M. R. Gupta, and Y. Chen, *Theory and Use of the EM Algorithm*. Boston: NOWPress, 2011.

[295] Ch. D. Manning, P. Raghavan, and H. Schütze, *Introduction to Information Retrieval*. UK: Cambridge University Press, 2008.

[296] Р. В. Шамин, *Практическое руководство по методам машинного обучения*. М.: Lector.ru, 2019.

[297] S. J. Godsill, and P. J. W. Rayner, *Digital Audio Restoration - a Statistical Model Based Approach*. USA: Springer, 1998.

[298] B. Xiang, *Acoustic modeling for efficient speaker verification*. UK: Cornell University, 2003.

[299] M. A. Pathak, *Privacy-Preserving Machine Learning for Speech Processing*. USA: Springer Science & Business Media, 2012.

[300] В. М. Буре, Е. М. Парилина, и А. А Седаков, *Теория вероятностей и вероятностные модели*. СПб: Лань, 2018.

[301] А. Б. Мерков, *Распознавание образов. Построение и обучение вероятностных моделей*. М.: Ленанд, 2014.

[302] В. Г. Лисиенко, и др., *Моделирование сложных вероятностных систем*. Екатеринбург: УРФУ, 2011.

[303] В. В. Губарев, *Вероятностные модели*. Часть 1. Новосибирск: Новосибирский электротехн. ин-т, 1992.

[304] В. В. Губарев, *Вероятностные модели*. Часть 2. Новосибирск: Новосибирский электротехн. ин-т, 1992.

[305] М. А. Федоткин, *Построение вероятностных моделей*. Нижний Новгород: Нижегородский госуниверситет, 2012.

[306] Р. Е. Саркисян, *Системный анализ и принятие решений*. Часть 3. Вероятностные модели и методы. Неформальные правила решения. Диалоговые модели многокритериальной оптимизации. М.: МИИТ, 2009.

[307] П. И. Тутубалин, и В. С. Моисеев, *Вероятностные модели обеспечения информационной безопасности автоматизированных систем обработки информации и управления*. Казань: РИЦ Школа, 2008.

[308] Т. Сегаран, *Программируем коллективный разум*. СПб: Символ-Плюс, 2008.

[309] S. Abe, *Support Vector Machines for Pattern Classification*. USA: Springer, 2010.

[310] I. Steinwart, and A. Christmann, *Support Vector Machines*. USA: Springer, 2008.

[311] Y. Ma, and G. Guo, *Support Vector Machines Applications*. USA: Springer, 2014.

[312] C. Campbell, and Y. Ying, *Learning with Support Vector Machines*. California: Morgan & Claypool, 2011.

[313] Теорема Мерсера *MachineLearning.ru* [Электронный ресурс]. Доступно: http://www.machinelearning.ru/wiki/index.php?title= Теорема_Мерсера Дата обращения: Авг. 26, 2020.

[314] Розходження Кульбака-Лейблера *Вікіпедія* [Електронний ресурс]. Доступно: https://uk.wikipedia.org/wiki/Розходження_Кульбака_—_Лейблера Дата звернення: серпень, 26, 2020.

[315] Бхаттачариа расстояние - Bhattacharyya distance *qwerty.wiki* [Электронный ресурс]. Доступно: https://ru.qwerty.wiki/wiki/Bhattacharyya_distance Дата обращения: Авг. 26, 2020.

[316] N. Dehak, R. Dehak, P. Kenny, N. Brummer, P. Ouellet, and P. Dumouchel, “Support Vector Machines versus Fast Scoring in the Low-

Dimensional Total Variability Space for Speaker Verication," *InterSpeech*, pp. 1559–1562, 2009.

[317] Алгоритм Баума-Велша *Википедия* [Электронный ресурс]. Доступно: https://ru.wikipedia.org/wiki/Алгоритм_Баума_—_Велша Дата обращения: Авг. 26, 2020.

[318] The Microsoft Cognitive Toolkit - Cognitive Toolkit - CNTK Microsoft Azure [Электронный ресурс]. Доступно: https://docs.microsoft.com/en-us/cognitive-toolkit/ Дата обращения: Авг. 26, 2020.

[319] L. Lu, Y. Zheng, G. Carneiro, and L. Yang, *Deep Learning and Convolutional Neural Networks for Medical Image Computing: Precision Medicine, High Performance and Large-Scale Datasets*. USA: Springer International Publishing, 2017.

[320] M. Sewak, Md. R. Karim, and P. Pujari. Practical Convolutional Neural Networks. Packt Publishing, 2018.

[321] A. Menshawy, *Deep Learning By Example: A Hands-on Guide to Implementing Advanced Machine Learning Algorithms and Neural Networks*. UK: Packt, 2018.

[322] H. Zou, T. Hastie, and R. Tibshirani, "Sparse Principal Component Analysis," *Journal of Computational and Graphical Statistics*, № 15(2), pp. 265–286, 2006. doi:10.1198/106186006x113430.

[323] U. Khan, P. Safari, and J. Hernando, "Restricted Boltzmann Machine Vectors for Speaker Clustering and Tracking Tasks in TV Broadcast Shows," *Applied Sciences*, № 9(13). pp. 2761, 2019. doi:10.3390/app9132761.

[324] N. Zhang, S Ding., J. Zhang, and Y. Xue. "An overview on Restricted Boltzmann Machines." *Neurocomputing*. no. 275, pp. 1186–1199, 2018. doi:10.1016/j.neucom.2017.09.065.

[325] Y. Zhang, X. Gao, X. Peng, J. Ye, and X. Li, "Attention-Based Recurrent Temporal Restricted Boltzmann Machine for Radar High Resolution Range Profile Sequence Recognition," *Sensors*, no. 18(5), pp. 1585, 2018. doi:10.3390/s18051585.

[326] S. K. Kim, L. C. McAfee, P. L. McMahon, and K. A. Olukotun, “A highly scalable Restricted Boltzmann Machine FPGA implementation,” *2009 International Conference on Field Programmable Logic and Applications*, pp. 367–372, 2009. doi:10.1109/fpl.2009.5272262.

[327] C. Vielhauer, *Biometric User Authentication for IT Security. From Fundamentals to Handwriting*. USA: Springer, 2006.

[328] D. R. Kisku, P. Gupta, and J. K. Sing, *Advances in Biometrics for Secure Human Authentication and Recognition*. USA: CRC Press, 2014.

[329] S. O. Thian, C. Tee, and S. M. Shohel, *Security and Authentication*. USA, NY: Nova Science Publishers, Inc., 2017.

[330] I. F. Blake, G. Seroussi, and N. P. Smart, *Advances in Elliptic Curve Cryptography*. UK: Cambridge University Press, 2005.

[331] J. H. Silverman, *The Arithmetic of Elliptic Curves*. 2nd Edition. USA: Springer Science & Business Media, 2009.

[332] Darrel R. Hankerson, Alfred J. Menezes, and Scott A. Vanstone, *Guide to Elliptic Curve Cryptography*. USA: Springer, 2004.

[333] К. Хоггер, *Введение в логическое программирование*. М.: Мир, 1988.

[334] K. Scarfone, D. Benigni, and T. Grance. Cyber Security Standards. [Online]. Available: https://ws680.nist.gov/publication/get_pdf.cfm?pub_id=152153 Accessed on: August 26, 2020.

[335] M. M. Alani, *Guide to OSI and TCP/IP Models*. USA: Springer, 2014.

[336] McM. Troy, *Cisco Networking Essentials. Textbook*, Second Edition. USA: Wiley, 2015.

[337] P. Bernus, K. Mertins, and G. Schmidt, *Handbook on Architectures of Information Systems*. USA: Springer, 2006.

[338] Á. Rocha et al., *Advances in Information Systems and Technologies*. USA: Springer, 2013.

[339] Christos Kalloniatis, *Modern Information Systems*. Pakistan: InTech, 2012.

[340] K. Klinger, *Enterprise Information Systems: Concepts, Methodologies, Tools and Applications*. France: Information Science Reference, 2011.

[341] R. Pooley et al., *Information Systems Development: Reflections, Challenges and New Directions*. USA: Springer, 2013.

[342] A. Gunasekaran, *Modeling and Analysis of Enterprise Information Systems*. France: IGI Global, 2007.

[343] B. S. Dhillon, *Robot System Reliability and Safety: A Modern Approach*. USA: CRC Press, 2015.

[344] А. П. Кирпичников, *Методы прикладной теории массового обслуживания*. М.: УРСС, 2018.

[345] В. Ф. Матвеев, и В. Г. Ушаков, *Системы массового обслуживания*. М.: Изд-во МГУ, 1984.

[346] А. А. Назаров, и А. Ф. Терпугов, *Теория массового обслуживания*. Томск: Изд-во НТЛ, 2004.

[347] Л. Клейнрок, *Теория массового обслуживания*. М.: Машиностроение, 1979.

[348] Р. Г. Асадуллаев, *Нечеткая логика и нейронные сети*. Белгород: БелГУ, 2017.

[349] В. В. Круглов, М. И. Дли, и Р. Ю. Голунов, *Нечеткая логика и искусственные нейронные сети*. М.: ФИЗМАТЛИТ, 2001.

[350] М. В. Назаров, и Ю. Н. Прохоров, *Методы цифровой обработки и передачи речевых сигналов*. М.: Радио и связь, 1985

[351] Н. Н. Иванов, «Вероятностная модель диффузионного распределения для оценки надежности радиоэлектронных приборов,» *Информационно-управляющие системы*, № 4 (59), с. 64–69, 2012.

[352] Е. И. Куликов, и А. П. Трифонов, *Оценка параметров сигнала на фоне помех*. М.: Советское радио, 1978.

ДОДАТКИ

Додаток А

Способи математичної формалізації інформаційних процесів у ІСКЗ

Якщо поєднати властивості марковських процесів і процесів відновлення, то отримаємо напівмарковський процес – випадковий процес, який переходить із одного стану в інший відповідно до заданих розподілів імовірностей, із випадковою величиною часу перебування процесу у довільному стані, розподіл якої залежить як від поточного стану, так і від стану, в який буде здійснено наступний перехід. Процес відновлення, марковський ланцюг із дискретним часом, однорідний марковський процес із неперервним часом – це окремі випадки НМП. Так, процес відновлення є НМП із одним станом, марковський ланцюг із дискретним часом – НМП, тривалість перебування у кожному із станів для якого дорівнює одиниці, а однорідний марковський процес із неперервним часом є НМП, тривалість перебування у відповідному стані для якого описується експоненційним розподілом, параметри якого визначаються номером стану.

Аналітично НМП описується двовимірним марковським ланцюгом (ξ_n, θ_n), де $0 \le n \le \infty$, $\xi_n \in E = \{1,2,...,N\}$, $\theta_n \in [0;\infty)$, при чому розподіл $P\{\theta_0 = 0\} = 1$, $p_i = P\{\xi_0 = i\} \ge 0$. Марковський ланцюг визначається перехідними імовірностями, які називають напівмарковським ядром:

$$\begin{aligned} &P\{\xi_{n+1} = j, \theta_{n+1} < t | \xi_n = i, \theta_n < \tau\} = \\ &= P\{\xi_{n+1} = j, \theta_{n+1} < t | \xi_n = i\} = Q_{ij}(t). \end{aligned} \tag{A.1}$$

Якщо ця перехідна імовірність не залежить від n (номера стану), то марковський ланцюг називають однорідним. Напівмарковське ядро описує імовірність того, що НМП перейде у стан j за час переходу менший від t за умови, що процес перебуває у стані i. Напівмарковському ядру $P\{\xi_{n+1} = j, \theta_{n+1} < t | \xi_n = i\} = Q_{ij}(t)$ притаманний ряд властивостей [192]:

– $Q_{ij}(t) \ge 0$;

– $p_{ij} = \lim\limits_{t \to \infty} Q_{ij}(t) = P\{\xi_{n+1} = j | \xi_n = i\}$;

– $\sum_{j\in E} P\{\xi_{n+1}=j,\theta_{n+1}<t\}=\sum_{j\in E} Q_{ij}(t)=P\{\theta_{n+1}<t|\xi_n=i\}$;

– $F_{ij}(t)=P\{\theta_{n+1}<t|\xi_n=i,\xi_{n+1}=j\}=p_{ij}^{-1}Q_{ij}(t)$,

де $i,j\in E=\{1,2,...,N\}$, $p_{ij}\neq 0$, $\sum_{j\in E} p_{ij}=1$, $Q_{ij}(t)$ – неспадна функція, аналогічна $F_{ij}(t)$. Імовірності переходів визначаються стохастичною матрицею $P=\|p_{ij}\|$ розмірністю $N\times N$, яка визначає вкладений марковський ланцюг, де p_{ij} – імовірність переходу із стану i у стан j.

Для визначення НМП необхідно:

– визначити марковські моменти;

– визначити стан процесу

– обчислити напівмарковське ядро $Q_{ij}(t)$

– перевірити властивості синтезованого напівмарковського ядра.

Керований напівмарковський процес визначається тривимірним марковським ланцюгом (ξ_n,θ_n,u_n), де $0\le n\le\infty$, $\xi_n\in E=\{1,2,...,N\}$, $\theta_n\in[0;\infty)$, $u_n\in U_i$ – управління; $B\in\boldsymbol{B}$, $\boldsymbol{B}$ – σ-алгебра підмножин множини U, при чому розподіл $P\{\theta_0=0\}=1$, $p_i=P\{\xi_0=i\}\ge 0$. Тоді, у свою чергу, марковський ланцюг визначається перехідними імовірностями у формі напівмарковського ядра $\hat{Q}_{ij}(t,B)$:

$$\begin{aligned}&P\{\xi_{n+1}=j,\theta_{n+1}<t,u_{n+1}\in B|\xi_n=i,\theta_n<\tau,u_n\in A\}=\\&=P\{\xi_{n+1}=j,\theta_{n+1}<t,u_{n+1}\in B|\xi_n=i\}=\hat{Q}_{ij}(t,B).\end{aligned}\qquad(A.2)$$

Вважатимемо, що ця перехідна імовірність не залежить від номера стану n, що передбачає однорідність марковського ланцюга. Напівмарковське ядро $\hat{Q}_{ij}(t,B)$ характеризується такими властивостями [192]:

– $p_{ij}(B)=\lim_{t\to\infty}\hat{Q}_{ij}(t,B)=P\{\xi_{n+1}=j,u_{n+1}\in B|\xi_n=i\}$;

– $p_{ij}(B)=\lim_{t\to\infty}\hat{Q}_{ij}(t,B)=P\{\xi_{n+1}=j,u_{n+1}\in B|\xi_n=i\}=p_{ij}$;

– $\sum_{j\in E} P\{\xi_{n+1}=j,\theta_{n+1}<t,u_{n+1}\in B|\xi_n=i\}=\sum_{j\in E}\widehat{Q}_{ij}(t,B)=$

$=P\{\xi_{n+1}\in E,\theta_{n+1}<t,u_{n+1}\in B|\xi_n=i\}=P\{\theta_{n+1}<t,u_{n+1}\in B|\xi_n=i\};$

– $\lim_{t\to\infty}\sum_{j\in E}\widehat{Q}_{ij}(t,B)=P\{u_{n+1}\in B|\xi_n=i\}=G_i(B);$

– $\widehat{Q}_{ij}(t,B)\geq G_i(B)$,

де $i,j\in E=\{1,2,...,N\}$, $p_{ij}\neq 0$, $\sum_{j\in E}p_{ij}=1$, $\widehat{Q}_{ij}(t,B)\geq 0$ – неспадна функція; $G_i(B)$ – множина імовірнісних мір. Напівмарковське ядро $\widehat{Q}_{ij}(t,B)$ породжує умовну міру у просторі управління. Згідно з теоремою Радона–Нікодима [193], якщо нерівність $\widehat{Q}_{ij}(t,B)\geq G_i(B)$ виконується, то існує така функція $Q_{ij}(t,U)$, що задовольняє рівність $\widehat{Q}_{ij}(t,B)=\int_{u\in B}Q_{ij}(t,u)G_i(dU)$, яка і є напівмарковським ядром КНМП $Q_{ij}(t,U)=P\{\xi_{n+1}=j,\theta_{n+1}<t|\xi_n=i,u_n=u\}$, яке описує умовну імовірність того, що КНМП перейде у стан j за час переходу, менший від t, за умови, що процес перебував у стані i та в цьому стані було прийнято управляюче рішення $u\in U$. При цьому зважатимемо, що

$$p_{ij}(u)=P\{\xi_{n+1}=j|\xi_n=i,u_n=u\},$$
$$F_{ij}(t,u)=P\{\theta_{n+1}<t|\xi_n=i,\xi_{n+1}=j,u_{n+1}=u\}=p_{ij}^{-1}(u)Q_{ij}(t,u). \tag{A.3}$$

Визначити КНМП можна задавши ядро $\widehat{Q}_{ij}(t,B)$ або задавши набір матриць $Q_{ij}(t,U)$ і вектори набору імовірнісних мір. Так, керований напівмарковський процес $X(t)$ визначається як $X(t)=(\xi(t),u(t))$, де $\xi(t)=\xi_{\nu(t)-1}$, $u(t)=u_{\nu(t)}$, а процес $\nu(t)=\inf\left(n:\sum_{k\leq n}\theta_k\right)$, $\theta_0=0$ називають зчитуючим процесом. Процес $\xi(t)$ збігається із стандартним НМП, а управляюча компонента $u(t)$ визначає траєкторію прийняття рішень. Компоненти КНМП $\xi(t)$, $u(t)$ і зчитуючий процес $\nu(t)$ характеризуються ступінчатими траєкторіями із синхронізованими моментами

розривів. При фіксованій стратегії управління імовірнісні характеристики НМП визначаються рівністю

$$Q_{ij}(t) = Q_{ij}(t, U_i) = \int_{U_i} Q_{ij}(t,u) G_i(du),$$

а множина імовірнісних мір $G_i(B)$ визначає однорідну рандомізовану марковську стратегії управління. Послідовність формалізації КНМП така:

– визначення марковських моментів;

– визначення стану процесу;

– визначення множини управління;

– визначення напівмарковського ядра, для чого визначають вектор управління $G_i(B)$ і напівмарковське ядро $Q_{ij}(t,U)$;

– перевірка властивостей синтезованого напівмарковського ядра.

Об'єктивність управління визначається обраною траєкторією процесу, оцінювання якої здійснюється за значенням функціоналу, який характеризує траєкторію чи її фрагмент. Траєкторії КНМП із скінченною множиною станів є ступінчатими функціями, які визначенні на довільному інтервалі $(0,T)$:

– послідовністю моментів переходів $t_0 = 0 < t_1 < t_2 < ... < t_n \le T < t_{n+1}$;

– послідовністю, яка визначає стан процесу у моменти t_k, $i_0, i_1, i_2, ..., i_{n+1}$, $i_k \in E$, $0 \le k \le n+1$;

– послідовністю управлінських впливів $u_0, u_1, u_2, ..., u_{n+1}$, $\xi(t_k) = i_k$,

де $n(T)$ – кількість переходів на інтервалі $(0,T)$, $\sum_{s=0}^{n(T)} t_s < T < \sum_{s=0}^{n(T)+1} t_s$.

Якщо визначено числові функції $R_{ij}(t,u)$, $i, j \in E$, то для визначеної траєкторії значення функціоналу опишемо виразом

$$\sum_{k=0}^{n(T)-1} R_{i_k i_{k+1}}(t_{k+1}, u_{k+1}) + R_{i_{n(T)} i_{n(T)+1}}\left(t_{n(T)+1}, T - \sum_{k=0}^{n(T)} t_k, u_{n+1}\right).$$

Функція $R_{ij}(t,\tau,u)$ є математичним сподіванням накопиченого ефекту за час τ за умови, що процес перебуває у стані i, наступним буде стан j, час переходу не перевищить t, у момент переходу із стану i прийнято рішення u.

Функція $R_{ij}(t,u)$ є математичним сподіванням накопиченого ефекту за весь період t, за умови, що процес перебуває у стані i, наступним буде стан j, у момент переходу із стану i прийнято рішення u.

Функціонал накопичення $MS(T)$ визначається як математичне сподівання накопиченого ефекту на інтервалі часу $(0,T)$.

Якщо процес стартує із стану i, $P\{\xi(0)=i\}=1$, то значення функціоналу накопичення залежатиме від i. Нехай $MS_i(t)$ – умовне математичне сподівання накопиченого ефекту за період $(0,t)$, за умови, що процес $\xi(t)$ стартує із стану i при $t=0$. Тоді, згідно з визначенням повного математичного сподівання, отримаємо систему інтегральних рівнянь відносно шуканих функцій $S_i(t)=MS_i(t)$:

$$S_i(t)=s_i(t)+\sum_{j\in E}\int_0^t S_i(t-x)dQ_{ij}(x),$$

$$s_i(t)=\sum_{j\in E}\int_{u\in U_i}\left\{\int_0^t R_{ij}(x,u)dQ_{ij}(x,u)+\int_t^\infty R_{ij}(x,t,u)dQ_{i,j}(x,u)\right\}G_i(du),$$

розв’язком якої буде множина значень виду

$$s_i=\lim_{t\to\infty}s_i(t)=\sum_{j\in E}\int_{u\in U_i}\int_0^\infty R_{ij}(x,u)dQ_{ij}(x,u)G_i(du) \qquad (A.4)$$

– математичне сподівання накопиченого ефекту за час перебування процесу в стані i. Вважатимемо ці значення скінченними. Якщо довго спостерігати процес $\xi(t)$, то накопичений ефект необмежено зростатиме, тому якість функціонування досліджуваної системи описуватимемо питомим накопиченим ефектом: $\lim\limits_{t\to\infty}\left(t^{-1}S_i(t)\right)$, якщо така границя існує.

Інколи замість функціоналу накопченого ефекту доцільніше використовувати функціонал досяжності. З цією метою множину станів E розбивають на дві не пересічені множини E_0 і $E_1: E=E_0\cup E_1$, $E_0E_1=\varnothing$. Для кожної траєкторії КНМП $\xi(t)$ поставимо у відповідність час η до першого випадку переходу траєкторії у стан з підмножини E_1. Позначимо

$\Phi_i(x) = P\{\tau < x | \xi(0) = i\}$, $i \in E_1$, тоді функціонал $\Phi_i(t)$ можна вважати окремим випадком функціоналу $S_i(t)$ для модифікованого КНМП, множина станів E_0 якого є поглинальними станами і рівність $R_{ij}(t,u) = 0$ виконується для $i \in E_0$. Відповідно до формули повної імовірності, інтегральне рівняння умовних розподілів $\Phi_i(t)$ формалізуємо як

$$\Phi_i(t) = \sum_{j \in E_0} Q_{ij}(t) + \sum_{j \in E_1} \int_0^t \Phi_j(t-x) dQ_{ij}(x),$$

тоді математичне сподівання часу непевного перебування процесу у стані i визначимо як

$$m_i = \lim_{t \to \infty} m_i(t) = \sum_{j \in E} \int_0^\infty x dQ_{ij}(x) = \int_0^\infty \left(1 - \sum_{j \in E} Q_{ij}(x)\right) dx. \quad (A.5)$$

Для розрахунку функціоналу досяжності необхідно розраховувати функціонал КНМП до моменту його переходу у стан із підмножини станів відмови.

На певному рівні абстракції ІСКЗ можна представити системою масового обслуговування, структура якої включає в себе множину обслуговуючих елементів, які називають каналами обслуговування. Систему масового обслуговування призначено для обслуговування відповідного потоку вимог, які спрямовані до системи. Метою теорії масового обслуговування є вироблення рекомендацій щодо забезпечення високої ефективності функціонування досліджуваної системи. Розв’язком задачі теорії масового обслуговування є ідентифікована залежність ефективності функціонування досліджуваної системи від її організації. Метрика ефективності функціонування може бути різна, визначена відповідно до цільового призначення досліджуваної системи. Синтез математичних моделей масового обслуговування супроводжується введенням поняття стратегія, під якою розуміють правила прийняття конкретних управлінських рішень. Для керованого випадкового процесу це синтез оптимальної стратегії управління із кількісною характеристикою якості управління, пов’язаною із конкретною траєкторією розвитку досліджуваного

процесу. Таким чином, кожній траєкторії необхідно поставити у відповідність значення, яке характеризує якість управління, тобто розрахувати певний функціонал. Те, що досліджуваний процес розвиватиметься за певною траєкторією, описується відповідною імовірністю, отже, значення обчислюваного функціоналу буде випадковою величиною. Безпосередньо порівнювати функції розподілу випадкових величин неможливо, але можна порівнювати, наприклад, значення відповідних математичних сподівань.

Якщо ІСКЗ як об'єкт управління представити КНМП, то тренд траєкторій його розвитку можна оцінити за розрахованими значеннями обраних функціоналів. Визначимо імовірнісні характеристики НМП

$$Q_{ij}(t) = Q_{ij}(t, U_i) = \int_{U_i} Q_{ij}(t,u) G_i(du), \tag{A.6}$$

де напівмарковське ядро $Q_{ij}(t,u)$ описує імовірність того, що напівмарковський процес перейде у стан j і тривалість переходу не перевищить t за умови, що вихідним станом процесу був стан i та на цьому стані було прийнято управлінське рішення u; $G_i(u)$ – розподіл, який регламентує правило вибору управлінського рішення для станів $i, j \in E$. Далі необхідно визначити перехідні імовірності вкладеного марковського ланцюга

$$p_{ij} = Q_{ij}(\infty) = Q_{ij}(\infty, U_i); \tag{A.7}$$

обчислити нормований розв'язок π_k системи алгебраїчних рівнянь

$$\left\{ \sum_{j \in E} \pi_j p_{jk} \right., \tag{A.8}$$

де $\sum_{k \in E} \pi_k = 1$;

обчислити умовні математичні сподівання тривалості невизначеного перебування процесу у стані i

$$m_i = \int_{x \in (0,\infty)} \left(1 - \sum_{j \in E} Q_{ij}(x) \right) dx; \tag{A.9}$$

обчислити умовні математичні сподівання накопиченого ефекту від управління за весь період перебування системи у стані i

$$s_i = \sum_{j \in E} \int_0^{\infty} R_{ij}(x) dx Q_{ij}(x); \qquad (A.10)$$

де функція $R_{ij}(t)$ – умовне математичне очікування накопиченого ефекту за умови, що система перебуває у стані i і через час, не більший від t, здійснить перехід у стан j. Функціонал якості управління обчислюватиметься за виразом

$$S = \sum_{k \in E} s_k \pi_k \left(\sum_{k \in E} m_k \pi_k \right)^{-1}. \qquad (A.11)$$

Зазвичай з об'єктивних причин всі характеристики конкретного процесу невідомі, але відомі характеристики множини процесів, до якої можна віднести досліджуваний процес. Тоді, якщо відомі:

– оцінка математичного сподівання $\bar{x}$, то приймаємо $\mu = \bar{x}$, де μ – математичне сподівання ξ, та визначаємо $F(x) \in \Omega(\mu)$ – множину функцій розподілів із математичним сподіванням μ;

– довірчий інтервал для математичного сподівання $\mu \in (\alpha, \beta)$ тоді визначаємо $F(x) \in \Omega(\mu, \mu \in (\alpha, \beta))$;

– оцінки значень функції розподілу $F(x)$ в окремих точках: $y_0 = 0 < y_1 < y_2 < ..... < y_n < y_{n+1} = \infty$, тоді визначаємо $F(y_i) = \pi_i$, де $\pi_0 = 0 \le \pi_1 \le \pi_2 \le \ldots < \pi_i < \ldots \le \pi_n \le \pi_{n+1} = 1$.

Вважатимемо, що $F \in \Omega(n, \vec{y}, \vec{\pi})$ – множина функцій розподілів, які у точках $\vec{y}$ приймають значення $\vec{\pi}$. Для описаної множини імовірних процесів ставимо відповідну задачу управління, наприклад, мінімаксну. З множини процесів вибираємо такий, якому відповідає найменше значення функціоналу. Вирішуємо для цього процесу задачу пошуку оптимальної стратегії управління, мінімізуючи значення функціоналу. Вважається якщо розповсюдити отриману стратегію оптимального управляння на всі процеси у складі вихідної множини, то найгірших наслідків все одно вдасться уникнути. Якщо ж таке рішення неприйнятне, доведеться звужувати множину процесів, збільшуючи таким чином ступінь інформованості про цільовий процес, досягаючи в решті решт

прийнятного результату. Звичайно наведена інформація носить загальний характер і її доведеться суттєво конкретизувати для опису ІСКЗ із урахуванням її структури та тієї обставини, що тривалості перебування системи у певному стані можуть описуватися різними законами розподілів.

Додаток Б

Аналіз моделей мовленнєвих сигналів у контексті задачі автентифікації суб'єкта за голосом

Математичне моделювання мовленнєвих сигналів ставить за мету отримання аналітичного опису їх характеристичних параметрів, вагомих в контексті задачі, для розв'язання якої модель створюється. На цей клас моделей розповсюджуються звичайні вимоги щодо математичних моделей [234–236] – адекватність, простота, мінімальність методичної похибки тощо. В контексті задачі аналізу мовленнєвих сигналів перша вимога задовольняється побудовою нових моделей у парадигмі акустичної теорії фонації [202–206]. Для задоволення другої вимоги періодичну компоненту мовленнєвого сигналу описують гармонічною функцією, застосовуючи при цьому потужний математичний апарат теорії радіотехніки [237–240]. Частину мовленнєвого сигналу, адекватно описати яку гармонічною функцією не вдається, вважають шумовою його компонентою. Результати досліджень процесу фонації [202–208] дозволяють констатувати, що періодична компонента утворюється як результат функціонування мовленнєвого джерела і модулятора, тоді як шумова – як результат проходження струменя повітря резонаторами артикуляційного тракту. Втім, задача віднесення аналізованого фрагмента мовленнєвого сигналу до періодичної чи шумової компоненти також має науковий інтерес.

Систематизуємо актуальні моделі опису мовленнєвих сигналів виділивши такі їх класи [205–208]:

1. Лінійні стаціонарні моделі із локально-сталими параметрами (авторегресії, ковзного середнього, комбіновані).

2. Лінійні параметричні моделі (авторегресії проінтегрованого ковзного середнього і похідні від них).

3. Нелінійні стаціонарні моделі (із вживанням нелінійної апроксимації).

4. Нелінійні параметричні моделі (комплексні нелінійні регресійні моделі).

Серед моделей, що описують мовленнєвий сигнал у часовому вимірі, виділимо:

1. Лінійній моделі, засновані на описі фрагментів мовленнєвих сигналів методом лінійного передбачення.

2. Диференційні моделі роботи артикуляційного тракту в процесі фонації на фізичному рівні (акустичні моделі фонації).

3. Гармонійні моделі, засновані на частотному описі мовленнєвих сигналів.

4. Модуляційні моделі, які представляють мовленнєвий сигнал безпосередньою функціональною залежністю від часу.

Звичайно, модель мовленнєвого сигналу є аналітичною залежністю обраних для представлення останнього з характеристичних параметрів, визначених відповідно до вживаного математичного апарату. Перелічимо найуживаніші з таких характеристичних параметрів [241–249]: середнє значення частоти основного тону і її гармонік (обертонів); середнє або нормоване середнє значення спектральної щільності енергії/потужності; коефіцієнти дискретного перетворення Фур’є; середнє або нормоване середнє значення спектральної щільності потужності; кепстральні характеристики; кореляційні характеристики; характеристики лінійного передбачення; відносний або нормований час детектування сигналу у смугах спектра; медіанне значення сигналу у смугах спектра; значення відносної потужності сигналу у смугах спектра; характеристики обвідної спектра; значення коефіцієнтів кореляції обвідних у смугах спектра; параметри гістограм розподілу періодів або частот основного тону; енергія і частота перетину сигналом нульового рівня; параметри миттєвих спектрів; амплітудні характеристики основного тону і його гармонік. Для характеристики зв’язності відліків мовленнєвого сигналу у часовому вимірі вживають коефіцієнт або функцію кореляції (автокореляції). Розподіл енергії

мовленнєвого сигналу за частотою оцінюють, аналізуючи його амплітудний спектр. Навіть наведений стислий перелік характеристичних параметрів виявляється достатньо значним, отже, проаналізуємо далі моделі параметризації мовленнєвих сигналів із вживанням згаданих вище характеристик з метою виявлення найінформативніших для розв'язання задачі АСГ.

Параметризація мовленнєвих сигналів для задачі АСГ здійснюється методами амплітудної (часової) селекції, спектрального (частотного) аналізу, кореляційного аналізу, кепстрального аналізу, вейвлет-аналізу та ін. Така широка палітра методів пояснюється низкою труднощів в оцінюванні індивідуальних ознак для АСГ, які полягають, зокрема, в обчислювальній складності, низькій точності, низькій завадостійкості і лише частковій автоматизації алгоритмів виділення характеристичних параметрів. Проаналізуємо детальніше згадані методи параметризації мовленнєвих сигналів в контексті специфіки їх застосування для задачі АСГ.

Амплітудна селекція для моделювання ІГМС. При амплітудній селекції мовленнєвого сигналу вважається [247–249], що на вокалізованих його відрізках при низькому рівні шумів форма мовленнєвого коливання є квазіперіодичною. Це дозволяє вважати тривалість часового інтервалу між глобальними максимумами мовленнєвого сигналу індивідуальною ознакою для автентифікації особи суб'єкта – періодом основного тону T_0. Вразливість таких методів пов'язана з природою мовленнєвого сигналу, в якому міститься значна кількість локальних максимумів, які слід заглушувати, застосовуючи до аналізованого мовленнєвого сигналу процедуру попереднього оброблювання, яка здебільшого включає фільтрацію, нелінійне перетворення, диференціювання тощо [249]. Втім, виставлення зависокого порогу спрацювання у детекторі глобальних максимумів призводить до зростання імовірності пропуску реального, пов'язаного із роботою мовленнєвого джерела, максимуму. Отже, методам параметризації мовленнєвих сигналів на

основі алгоритмів амплітудної селекції властиві всі згадані вище недоліки, що дозволяє передбачити лише лабораторне їх застосування.

Кореляційний аналіз для моделювання ІГМС. Ідея детектування періодів пульсацій у квазіперіодичних мовленнєвих коливаннях лежіть і в основі кореляційного їх аналізу. Відмінність від амплітудної селекції полягає у тому, що досліджується не форма чи потужність мовленнєвого коливання, а автокореляційна чи кореляційна його функції або нормовані їхні характеристики [248, 249]. Аналогічно, періодом основного тону вважають інтервали між першим максимумом кореляційної функції (відлік $j = 0$) і другим її максимумом, який відстоїть від першого на $j = J_0 = T_0 \Delta^{-1}$ відліків, де Δ – період дискретизації. Також за значеннями кореляційних функцій можна проводити сегментацію мовленнєвого сигналу на фрагменти класів «сигнал», «шум», «пауза» тощо. До переваг кореляційних методів можна віднести вищу стійкість до завад, поява яких носить епізодичний, а не періодичний характер. Також перевагою кореляційного аналізу над амплітудною селекцією є те, що для другої властивий вплив фазових взаємовідносин у мовленнєвому сигналі на період між глобальними максимумами, а кореляційний аналіз позбавлено цих впливів, що робить максимуми кореляційних функцій мовленнєвих сигналів виразнішими, втім, проблема детектування локальних максимумів залишається, що також вирішується попереднім оброблюванням мовленнєвих сигналів, підвищуючи і так значну обчислювальну складність кореляційного аналізу. Також кореляційним методам властивий зв’язок достовірності оцінювання інформативних ознак із кроком кореляційної функції, у свою чергу, залежного від частоти дискретизації. Наприклад, якщо мовленнєвий сигнал із істинним значенням частоти основного тону $f_0 = 250$ Гц оцифровано із частотою дискретизації $f_d = 8000$ Гц, то періодичність кореляційної функції, спричинена основним тоном, проявлятиметься через $j = T_0 \Delta^{-1} = f_d f_0^{-1} = 32$ відліки, отже, при відхиленні отриманої в результаті роботи алгоритму

оцінки частоти основного тону від істинного її значення на ± 1 відлік кореляційної функції відносна похибка вимірювань f_0 складатиме $\pm 3{,}23\,\%$, тобто є досить значною.

Спектральний аналіз для моделювання ІГМС. У акустичній теорії фонації вважається, що спектр мовленнєвого сигналу є результатом добутку спектра передатної характеристики артикуляційного тракту і спектра функції збудження. Вважається [249], що спектр функції збудження не несе інформативних ознак для АСГ, тому його впливу можна позбавитися здійснивши усереднення спектра вихідного мовленнєвого сигналу за значеннями у точках, зібраних у вибрану оптимальну множину, розмірність якої знаходиться у прямій залежності із тоном аналізованого сигналу.

В теорії цифрового оброблювання сигналів [212, 213] виділяють такі види спектрального його представлення як: ряди Фур'є, вживані для опису неперервних періодичних функцій; перетворення Фур'є, вживане для опису неперервних аперіодичних функцій; дискретне або швидке перетворення Фур'є, вживане для опису скінченного дискретного ряду, утвореного в результаті дискретизації сигналу.

Для обчислення спектра застосовують квазідетермінований і стохастичний підходи, а для його характеристики вживають короткочасні (миттєві) і усереднені компоненти. Перші обчислюються для фрагментів сигналу тривалістю 5–30 мс, які називають фреймами [249], а другі – для всієї аналізованої тривалості сигналу. Квазідетермінований підхід до обчислення спектра зумовлює його характеристику у вигляді ряду Фур'є, спектральної щільності, спектральної щільності потужності, одностороннього дискретного перетворення Фур'є, швидкого перетворення Фур'є тощо [212, 213]. Стохастичний підхід до обчислення спектра зумовлює його характеристику у вигляді одно- чи двосторонньої спектральної щільності потужності, двосторонньої спектральної щільності потужності, нормованої за дисперсією чи за максимумом тощо [241–249]. Вибір між квазідетермінованим чи стохастичним підходом до обчислення спектра

здійснюється в залежності від бажаного представлення аналізованого сигналу.

Безпосередньому оцінюванню значень спектра відповідає велика похибка [249], для зменшення якої оцінювання проводять у часових, спектральних або кореляційних вікнах-фреймах, характер яких визначається їх ваговими функціями. Наприклад, однією з головних статистичних характеристик мовленнєвого сигналу вважається косинус-перетворення Фур'є вибіркової функції кореляції – вибірковий спектр потужності $W_{\xi}(2\pi f)$ [250–252]. Адекватна оцінка мовленнєвого сигналу за цією ознакою зазвичай здійснюється у взаємозалежних спектральних або кореляційних фреймах [248, 249]:

$$W_{\xi}(2\pi f) = 2\Delta\left(R_0 + 2\sum_{k=1}^{M-1} R_k W(k)\cos(2\pi f \Delta k)\right), \qquad (Б.1)$$

де $\Delta = f_d^{-1}$ – період дискретизації мовленнєвого сигналу $x(t)$; $M = b_{norm}(b\Delta)^{-1}$ – точка відсікання кореляційного фрейма $W(k)$; b – ширина спектрального фрейма; b_{norm} – нормована ширина істотної для спектрального фрейма частотної смуги; R_k – функція кореляції відліків x_i дискретизованого сигналу $x(t)$.

Нормований за дисперсією варіант характеристики (Б.1) описується виразом

$$S(f) = W_{\xi}(2\pi f)R_0^{-1} = 2\Delta\left(1 + 2\sum_{k=1}^{M-1} r_k W(k)\cos(2\pi f \Delta k)\right), \qquad (Б.2)$$

де r_k – коефіцієнти кореляції відліків x_i.

У емпіричних дослідженнях мовленнєвих сигналів найуживанішими є кореляційні фрейми Бартлета, Тьюкі, Парзена тощо [253]. Зрештою, вибір виду фрейма є результатом компромісу між бажаною роздільною здатністю у часовому або частотному вимірах [253–255].

Метою частотного аналізу мовленнєвих сигналів у контексті АСГ є виявлення і характеристика піків у спектрі сигналу на певних частотах,

зокрема, на частості основного тону $f_0 = T_0^{-1}$ і її гармоніках. Якщо обчислити швидке перетворення Фур'є $\dot{C}_k$ послідовності відліків мовленнєвого сигналу x_i із достатньо малим кроком дискретизації за частотою, то першому глобальному максимуму спектра відповідатиме оцінка частоти основного тону $\hat{f}_0$. В подальшому глобальні максимуми детектуватимуться в околі $\hat{f}_0$ і відповідатимуть гармонікам частоти основного тону. Існують алгоритми [249], у яких пошук екстремуму здійснюють не у спектрі, а серед значень нелінійної функції від нього, яка є сумою стиснених за частотою логарифмів спектра потужності. Перевагою такого представлення є те, що потужності гармонік періодичних компонент аналізованого сигналу, до яких відноситися частота основного тону, додаватимуться, утворюючи значні піки на відповідній частоті, тоді як неперіодичні складові сигналу такого підсилювання не зазнаватимуть. Втім, всім спектральним методам властива методична похибка, спричинена вживаним нелінійних перетворень.

Кепстральний аналіз для моделювання ІГМС. У моделях [247–249] короткочасні фрагменти мовленнєвого сигналу описують як результат згортки двох функцій – функції збудження артикуляційного тракту і його лінійної імпульсної характеристики із постійними параметрами. Ідентифікація параметрів цих функцій для різних мовленнєвих сигналів дозволяє вирішувати широке коло задач, але окремою задачею є їх сепаратний аналіз, для здійснення якого вживають положення гомоморфного аналізу, одним із видів якого є кепстральний аналіз [249].

Кепстр апроксимують оберненим дискретним перетворенням Фур'є від логарифму модуля дискретного перетворенням Фур'є послідовності відліків аналізованого фрагмента мовленнєвого сигналу тривалістю 10–20 мс:

$$\dot{c}_p(n) = N^{-1} \sum_{k=0}^{N-1} \log\left|\dot{X}(k)\right| \exp\left(j2\pi knN^{-1}\right),\ n = \overline{0, N-1} \qquad (Б.3)$$

Кепстральний аналіз має за мету виявлення максимумів на періодах повторення гармонічних складових мовленнєвих сигналів. Факт детектування та ступінь вираження таких максимумів залежать від формантної структури аналізованого мовленнєвого сигналу, виду і параметрів фрейма, вживаного для його зважування тощо.

Кепстральному аналізу мовленнєвих сигналів, в контексті виявлення характеристичних параметрів для АСГ, властива низка недоліків, зокрема, необхідність експертного втручання для встановлення порогу спрацьовування детектора періодичних компонент за значенням виявленого максимуму, робота методів у абстрактному масштабі часу, вживання фреймів і операцій згладжування, залежність достовірності детектування періодичних компонент від параметрів гребінки частотних фільтрів, що вживаються для параметризації мовленнєвого сигналу.

Лінійне передбачення для моделювання ІГМС. У парадигмі теорії лінійних динамічних систем мовленнєвий сигнал можна описати положеннями методу лінійного передбачення, а саме, у вигляді лінійних моделей із локально-сталими параметрами (авторегресійна, ковзного середнього, комбінована тощо) [241–249] або у вигляді лінійних параметричних нестаціонарних моделей (авторегресії проінтегрованого ковзного середнього тощо).

При описі мовленнєвого сигналу моделлю авторегресії перший вважається локально-стаціонарним процесом, генерованим артикуляційним трактом, який вважається лінійною системою. Отже, x_t – мовленнєвий сигнал у дискретному часі, утворюється на виході модельованого лінійним частотним фільтром артикуляційного тракту, збуджуваного послідовністю випадкових величин a_t, згенерованих відповідно до гаусівського закону розподілу при моделюванні невокалізованих фрагментів мовленнєвого сигналу або квазіперіодичних – у іншому випадку [256]:

$$a_t = \sum_m u_{t-t_m} + w_t, \qquad (Б.4)$$

де u_t - трикутний імпульс, t_m – часові координати імпульсу; w_t – випадкова некорельована послідовність слабкої інтенсивності.

В залежності від модельованих періодичних компонент вживають різні фільтри низьких частот [247–249], наприклад, для виділення частоти основного тону використовується фільтр низьких частот із частотою зрізання 800–900 Гц [249, 257]. Періодичність згенерованого за виразом (Б.4) сигналу задається періодом основного тону $T_0 = t_m - t_{m-1}$, а форма імпульсів найчастіше є трикутною.

Алгоритм лінійного передбачення використовується для визначення параметрів моделі, представлених значеннями коефіцієнтів ϕ_i:

$$\widetilde{x}_t = \sum_{i=0}^{\infty} \phi_i x_{t-i}, \qquad (Б.5)$$

де $\sum_{i=0}^{\infty} |\phi_i| < \infty$. Також параметризувати модель (Б.4) можна значеннями коефіцієнтів дробово-раціональної функції, зв'язаної із послідовністю ϕ_i z-перетворенням.

Вираз (Б.5) можна доповнити коефіцієнтом підсилення $b = const$:

$$x_t = \sum_{i=0}^{p} \phi_i x_{t-i} + b a_t. \qquad (Б.6)$$

Вираз (Б.6) є поданням мовленнєвого сигналу у класі дискретних процесів лінійної авторегресії. Похибку такого подання можна описати виразами

$$e_t = x_t - \widetilde{x}_t; \qquad (Б.7)$$

$$E(N) = \sum_{t=1}^{N} e_t^2 = \sum_{t=1}^{N} \left(x_t - \sum_{i=1}^{p} \phi_i x_{t-i} \right)^2, \qquad (Б.8)$$

де e_t – похибка передбачення; $E(N)$ – середньоквадратичне відхилення опису мовленнєвого сигналу; N – кількість відліків в межах фрейма аналізу [249].

З плеяди методів обчислення оцінок коефіцієнтів лінійного передбачення [249, 257–259] акцентуємо увагу на автокореляційному методі. Опишемо коефіцієнти кореляції процесу авторегресії виразом

$$r_k = \phi_1 r_{k-1} + \phi_2 r_{k-2} + \ldots + \phi_j r_{k-j} + \ldots + \phi_p r_{k-p}, \qquad (Б.9)$$

$k > 0$, $j = \overline{1, p}$, і, в залежності від співвідношень коефіцієнтів ϕ_j, представимо або сумою згасних експонент або сумою згасних синусоїд. Якщо значення чи оцінки кореляційних коефіцієнтів відомі, то сформулювавши p рівнянь для r_k, $k = \overline{1, p}$, можна розрахувати оцінки Юла–Уокера [257] для коефіцієнтів процесу авторегресії. Змістовно ці оцінки ґрунтуються на марковській інтерпретації процесу авторегресії, при якій коректно стверджувати, що навіть якщо кореляційний коефіцієнт r_k ненульовий для будь-яких значень порядку процесу авторегресії k, то цей коефіцієнт все ж можна представити множиною з p ненульових часткових кореляційних коефіцієнтів $\psi_{i,j}$. Враховуючи, що $\phi_k = 0$, $k > p$, згадане твердження дозволяє, послідовно змінюючи порядок процесу авторегресії $k = \overline{1, p+n}$, $n \geq 1$, сформувати систему рівнянь Юла–Уокера:

$$r_k = \psi_{k,1} r_{j-1} + \ldots + \psi_{k,k-1} r_{j-k+1} + \psi_{k,k} r_{j-k}, \qquad (Б.10)$$

де $j = \overline{1, k}$, розв'язавши яку можна знайти нульове значення $\psi_{k,k}$ і визначити таким чином порядок процесу авторегресії.

Аналітичний вигляд часткової кореляційної функції, яка описує залежність $\psi_{k,k}$ від k, можна отримати інтерпретуючи двовимірну умовну гаусівську щільність імовірності $W_2\left(x_t, x_{t-k} \middle| x_{t-1}, \ldots, x_{t-k+1}\right)$ у вигляді рекурентної формули Дарбіна [257]:

$$\psi_{p+1,j} = \psi_{p,j} - \psi_{p+1,p+1} \psi_{p,p-j+1}, \qquad (Б.11)$$

де $j = \overline{1, p}$,

$$\psi_{p+1,p+1} = \left(r_{p+1} - \sum_{j=1}^{p} \psi_{p,j} r_{p+1-j} \right) \left(1 - \sum_{j=1}^{p} \psi_{p,j} r_j \right)^{-1}. \qquad (Б.12)$$

На відміну від кореляційних коефіцієнтів r_k, для процесу авторегресії порядку p при $k > p$ часткова кореляційна функція $\psi_{k,k} = 0$ зв'язана із коефіцієнтами лінійного передбачення ϕ_j залежністю виду

$$\varphi_j = \psi_{p,j}, \tag{Б.13}$$

де $j = \overline{1, p}$, p – порядок моделі авторегресії.

Коефіцієнт підсилення b, вживаний у (Б.6), обчислюється за виразом [256]:

$$b = R_0 - \sum_{i=1}^{p} \phi_i R_i , \tag{Б.14}$$

де R_i – відліки функції кореляції мовленнєвого сигналу.

Спектральна щільність потужності (Б.1) для сигналу, що описується процесом авторегресії, обчислюється за виразом [260]:

$$W_\xi(2\pi f) = \Delta b \left(1 - \sum_{i=1}^{p} \phi_i \exp(-j2\pi f \Delta i)\right)^{-2}, \tag{Б.15}$$

а нормований за дисперсією варіант характеристики (Б.15) описується виразом, отриманим у базисі Лагерра [350]:

$$\begin{aligned} S(f) &= \Delta \left(1 - \sum_{i=1}^{p} \phi_i \exp(-j2\pi f \Delta i)\right)^{-2} = \\ &= \Delta \left(\left(1 - \sum_{i=1}^{p} \phi_i \cos(2\pi f \Delta i)\right)^2 + \left(1 - \sum_{i=1}^{p} \phi_i \sin(2\pi f \Delta i)\right)^2 \right). \end{aligned} \tag{Б.16}$$

Слід відзначити, що при зависокій частоті дискретизації f_d модельованого сигналу x_t умова стійкості авторегресійної моделі, отриманої в результаті роботи описаного вище авторегресійного методу, може порушуватися [257]. Умова дотримання стійкості $|\phi_j| = |\psi_{p,j}| < 1$ при $j = \overline{1, p}$.

Зазвичай коефіцієнти лінійного передбачення розраховуються для кожного фрагмента описуваного мовленнєвого сигналу тривалістю 20–30 мс [249], втім, у актуальному стандарті LPC-10 кожен фрейм мовленнєвого

сигналу тривалістю 15 мс описується 10-ма коефіцієнтами лінійного передбачення. Також слід відзначити, що немає прямого зв'язку між порядком і похибкою отриманого із використанням лінійного передбачення опису мовленнєвого сигналу. Як занадто низький, так і занадто високий порядок моделі може спричинити зростання похибки опису. У літературних джерелах [249] пропонують описувати кожні 20 мс вхідного сигналу 14 коефіцієнтами лінійного передбачення, що для фрагментів мовленнєвого сигналу тривалістю $\tau_i = \{0{,}1;\ 0{,}2;\ 0{,}4\}$ дає $\{70,\ 140,\ 280\}$ коефіцієнтів, відповідно.

Також для апроксимації мовленнєвих сигналів обмежено використовують лінійну непараметричну нестаціонарну модель авторегресії проінтегрованого ковзного середнього і похідні від неї [257–260]. Обмежене вживання цих моделей обумовлено їх аналітичною і обчислювальною складністю при порівнянній із лінійними моделями із локально-сталими параметрами достовірності опису мовленнєвих сигналів.

Вейвлет-аналіз для моделювання ІГМС. На відміну від спектрального аналізу вейвлет-перетворення, завдяки вживаним вейвлет-базисним функціям, дозволяє отримати двовимірне представлення аналізованого сигналу у площині частота-положення, де аналогом частоти виступає масштаб аргументу базисної функції, а положення визначається її зсувом. Таке представлення дозволяє довільно деталізувати представлення аналізованого сигналу, локалізуючи його особливості у часовому вимірі. Якщо при спектральному аналізі розкладання аналізованого сигналу здійснюється за нескінченними гармоніками базису Фур'є, то при вейвлет-аналізі розкладання здійснюється за зміщуваними у часі скінченними вейвлетами (тривалістю приблизно 5–40 мс) [261, 262], утворюючи таким чином суттєво комплексніший параметричний опис аналізованого сигналу.

У теорії цифрового оброблювання сигналів [262] їх вейвлет-аналіз найчастіше здійснюється із використанням вейвлету Морле

$$\psi(t) = \exp(j\xi t)\exp\left(-0{,}5t^2\right), \qquad (Б.17)$$

де ξ – центральна частота вейвлет-функції, яка визначає вибірковість базису. Практичне застосування базису (Б.17) описується виразом

$$W_f(a,b) = |a|^{-0,5} \times$$
$$\times \int_{-\infty}^{\infty} f(t)\exp\left(j\xi(t-b)a^{-1}\right)\exp\left(-(t-b)^2\left(2a^2\right)^{-1}\right)dt, \quad (Б.18)$$

де a – параметр, що визначає смугу пропускання вейвлет-функції [262].

Для гармонійних сигналів, виду, наприклад,

$$f(t) = A_0 \cos(\omega_0 t + \varphi_0), \quad (Б.19)$$

девіацією значення $|W_f(a,b)|$ із змінюванням b можна знехтувати [261], що дозволяє, приймаючи $b = 0$, спростити вираз (Б.18) до вигляду

$$|W_f(a)| = 2A_0(2\pi a)^{-0.5}\left(\exp\left(-0,5(\xi - a\omega_0)^2 - \varphi_0\right) + \right.$$
$$\left. + \exp\left(-0,5(\xi - a\omega_0)^2 + \varphi_0\right)\right). \quad (Б.20)$$

Із урахуванням того, що в області додатних значень a другим доданком у (Б.20) можна знехтувати, положення локального максимуму сигналу (Б.19), описуваного вейвлет-перетворенням (Б.20), можна формалізувати виразом

$$a = \left(\xi + \left(\xi^2 + 2\right)^{-0,5}\right)(2\omega_0)^{-1}. \quad (Б.21)$$

Якщо описується сигнал, складніший від (Б.19), то відбувається суперпозиція неперервних вейвлет-перетворень сигналів, що передбачає і суперпозицію частотних зрізів.

Отже, за відомим значенням максимуму $a_{\max}$ вейвлету Морле можна розрахувати при заданому значенні ξ частоту періодичної компоненти мовленнєвого сигналу

$$f_0 = 0,5\pi^{-1}\omega_0 = \left(\xi + \left(\xi^2 + 2\right)^{0.5}\right)(4\pi a_{\max}). \quad (Б.22)$$

До переваг вейвлет-аналізу мовленнєвих сигналів можна віднести високу достовірність опису останніх. До недоліків – необхідність

коригування фрейма перетворення для кожної оцінюваної частоти і значну обчислювальна складність аналізу, обмовлену аналітичною складністю алгоритму метода.

Фрактальний аналіз для моделювання ІГМС. Відносно новими є спроби опису мовленнєвого сигналу в часі у парадигмі теорії квазідетермінованого хаосу на основі математичного апарату фрактального аналізу [263]. В цих роботах мовленнєвий сигнал розглядається як динамічна система із структурованим набором режимів, переходи між якими відбуваються під впливом внутрішніх чи зовнішніх впливів. При такому підході робляться спроби використання в якості характеристичних параметрів для АСГ результатів представлення мовленнєвого сигналу у розмірності Хаусдорфа. Втім, поки що така параметризація дозволила досягти помітних якісних результатів лише у задачі розпізнавання мови.

Марковське моделювання ІГМС. Розглянемо певний процес як розподілений ланцюг станів $\{W\}^N = \{W_N, W_{N-1}, \ldots, W_1\}$, $\forall W \in \{w\}$ деякого джерела, яке генерує символи спостереження $\{X\}^M = \{X_M, X_{M-1}, \ldots, X_1\}$, $\forall X \in \{x\}$. Поставимо у відповідність кожному стану $W \in \{w\}$ одну чи кілька послідовностей виду $\{C\}^K = \{C_K, C_{K-1}, \ldots, C_1\}$, $\forall C \in \{c\}$ так, що $\{W\}^N \Rightarrow \{C\}^M = \{C_M, C_{M-1}, \ldots, C_1\}$, тобто послідовність $\{C\}^M$ є синхронною із $\{X\}^M$. Випадковий процес (джерело) є марковським [189–192] із порядком *m*, якщо він так породжує стохастичну послідовність $\{C\}^M$, що поточне значення послідовності C_t залежить лише від попередніх значень аж до моменту часу $t-m$: $P(C_t | C_{t-1}, C_{t-2}, \ldots, C_1) \equiv P(C_t | C_{t-1}, C_{t-2}, \ldots, C_{t-m})$. Відповідно, прихованою марковською моделлю є марковське джерело, яке репрезентує процес переходу між скінченним набором внутрішніх станів $\{c\}$, де при кожному переході в стан c_i утворюється символ спостереження відповідно до деякого розподілу імовірності $p(X | c_i)$, але послідовність внутрішніх станів

$\{C\}^M = \{C_M, C_{M-1}, \ldots, C_1\}$ залишається невідомою спостерігачеві. Науковою задачею є знаходження оптимальної конфігурації $\{C\}^M$ для опису $\{W\}^N$. Також відзначимо, що оцінювання параметрів прихованої марковської моделі не залежить від виду значень послідовності $\{X\}^M$ – дискретні значення із кодової книги утворюються векторним квантуванням [258], а послідовності векторів значень характеристичних параметрів – моделюванням розподілу імовірності утворення символу спостереження $p(X_i|C_i, W_i)$ сумішшю розподілів Гауса [249].

Якщо перейти від абстрактного опису теорії Маркова до її прикладної адаптації для розв'язання задачі АСГ, то під джерелом розумітимемо особу суб'єкта, фонограми генерованих артикуляційним трактом якого парольних мовленнєвих сигналів утворюватимуть елементи множини станів $\{w\}$ із відповідною транскрипцією $\{C\}^K$. Символи спостереження $X \in \{x\}$ є параметризованим представленням фонограм парольних мовленнєвих сигналів у просторі обраних характеристичних параметрів. Якщо значення X неперервні, то щільність імовірності $p(X|c_i)$ моделюється сумішшю розподілів Гауса, а компоненти вектора X вважаються незалежними величинами. Якщо ж значення X – дискретні мітки з кодової книги векторного квантування, то оцінки імовірності $p(X|c_i)$ отримуються за законом великих чисел. Векторне квантування дозволяє розбити акустичні вектори на класи за обраною мірою подібності, наприклад, евклідовою відстанню. Для синтезу стохастичного механізму АСГ, який оптимально здійснює перехід $\{X\}^M \Rightarrow \{W\}^N$, необхідно розв'язувати задачі акустичного і лінгвістичного моделювання, на якість розв'язку яких можуть впливати як методичні, так і стохастичні фактори.

В цілому, застосуванню марковських моделей для опису мовленнєвих сигналів сприяє: ефективність цього математичного апарату для опису сигналів як у часовому, так і у частотному вимірах; властива марковським

моделям гнучка топологія, яка дозволяє враховувати різні рівні абстракції при описі сигналів; велика база математично коректних алгоритмів для параметризації, навчання і оцінювання результатів моделювання.

Водночас, прикладне застосування марковських моделей для опису мовленнєвих сигналів ускладнюється слабкістю дискримінантних властивостей перших, адже на етапі навчання акустичні моделі утворюються на основі критерію максимуму правдоподібності, а не точнішого критерію максимуму апостеріорної імовірності. Можна відзначити також часткове сутнісне розходження суто стохастичних марковських моделей як предмета дослідження із об'єктом дослідження – мовленнєвим сигналом, який, відповідно до теорії фонації [216–218], можна вважати стохастичним лише наближено. Також мовленнєвий сигнал можна вважати стаціонарним лише на досить короткотривалих інтервалах, тоді як властива марковському стану стаціонарна статистика – розподіли емісійних імовірностей, що не залежать від часу. Марковську модель можна класифікувати як модель першого порядку – стан у момент часу t залежить лише від попереднього стану у момент часу $t-1$, що можна вважати вірним для мовленнєвого сигналу лише частково. Відзначимо також окремі недоліки процедури навчання, зокрема, оптимізація і навчання акустичної і лінгвістичної марковських моделей мовленнєвих сигналів здійснюється незалежно, а самі методи навчання – суттєво обчислювально затратні. Але найсуттєвішим недоліком є висока чутливість моделі до завад і спотворень у аналізованих мовленнєвих сигналах [247]. Всі ці недоліки не означають неадекватність марковських моделей опису мовленнєвих сигналів, але вважати такі моделі універсальними однозначно некоректно. Зрештою, ведуться дослідження у напрямку адаптації математичного апарату марковських мереж для опису мовленнєвого сигналу як результату когнітивної діяльності людини шляхом інтеграції марковських моделей із штучними нейромережами [222–226].

Додаток В

Спектральні компоненти уточненої квазідетермінованої моделі індивідуальності голосу

Еволюція моделі (2.1) до вигляду (2.24) супроводжувалася, зокрема, введенням в останню базису Фур'є, що допускає розширення вектора характеристичних параметрів для АСГ коефіцієнтами, які описують спектральну щільність потужності сигналів, генерованих моделлю (2.24), і дозволяє врахувати вклад резонаторів артикуляційного тракту у ІГМС.

Опишемо W_N^u – нормовану спектральну щільність потужності сигналу моделі (2.1), виразом

$$W_N^u = \left(S_u(f)\right)^2 \left(\left(\max S_u(f)\right)\right)^{-1}, \tag{В.1}$$

де спектральну щільність потужності $S_u(f)$ розрахуємо за виразом

$$\begin{aligned} S_u(f) = 2^{-1}\tau_i \sum_{l=1}^{L} U_l \big(&\mathrm{sinc}\big(\pi(f + lf_0)\tau_i\big) + \mathrm{sinc}\big(\pi(f - lf_0)\tau_i\big) - \\ &- 2^{-1} M \big(\mathrm{sinc}\big(\pi(f + lf_0 + F_0)\tau_i\big) + \mathrm{sinc}\big(\pi(f - lf_0 - F_0)\tau_i\big) + \\ &+ \mathrm{sinc}\big(\pi(f + lf_0 - F_0)\tau_i\big) + \mathrm{sinc}\big(\pi(f - lf_0 + F_0)\tau_i\big)\big)\big). \end{aligned} \tag{В.2}$$

Значення нормованої спектральної щільності потужності сигналу моделі (2.24) також розраховуватимемо за виразом (В.1), але спектральну щільність потужності в такому разі розраховуватимемо за виразом

$$\begin{aligned} S_u(f) = 4^{-1}\tau_i \sum_{k=1}^{K} M_k \big(&\mathrm{sinc}\big(\pi(f + lf_0 + kF_0)\tau_i\big) e^{-i(\varphi_l + \Gamma_k)} + \\ &+ \mathrm{sinc}\big(\pi(f - lf_0 - kF_0)\tau_i\big) e^{i(\varphi_l + \Gamma_k)} + \\ &+ \mathrm{sinc}\big(\pi(f + lf_0 - kF_0)\tau_i\big) e^{-i(\varphi_l - \Gamma_k)} + + \mathrm{sinc}\big(\pi(f - lf_0 + kF_0)\tau_i\big) e^{i(\varphi_l - \Gamma_k)}\big), \end{aligned} \tag{В.3}$$

у якому при $\varphi_l = \Gamma_k = 0$ експоненційні множники дорівнюватимуть одиниці:

$$\begin{aligned} S_u(f) = 4^{-1}\tau_i \sum_{k=1}^{K} M_k \big(&\mathrm{sinc}\big(\pi(f + lf_0 + kF_0)\tau_i\big) + \\ &+ \mathrm{sinc}\big(\pi(f - lf_0 - kF_0)\tau_i\big) + \mathrm{sinc}\big(\pi(f + lf_0 - kF_0)\tau_i\big) + \\ &+ \mathrm{sinc}\big(\pi(f - lf_0 + kF_0)\tau_i\big)\big). \end{aligned} \tag{В.4}$$

Відзначимо, що отримане у вигляді (В.1) спектральне представлення мовленнєвого сигналу характеризується загальністю і виявляється малоефективним для застосування у задачі АСГ. Втім, аналіз моделі (2.24) дозволив персоніфікувати опис мовленнєвого сигналу вектором характеристичних параметрів $\{U_1,\ldots,U_L,M_0,\ldots,M_K,f_0\}$ із індивідуальною інформацією про частоту основного тону та її гармоніки. Врахуємо цю інформацію, сегрегуючи отримане із використанням (В.1) спектральне представлення мовленнєвого сигналу. Апроксимуємо спектральну щільність потужності сигналу $S^u(\omega)=S^u u(2\pi f)$ множиною сталих складових S_l, $l=\overline{0,L}$, у частотних смугах шириною Δ_l^f в околі несної частоти f_l^n, роль якої в мовленнєвому сигналі відіграє частота основного тону f_0 і її гармоніки $f_1,f_2,\ldots,f_{L-1}$:

$$S^u(\omega)=S^u(2\pi f)=\begin{cases} S_0, if\ f\in\left[0,f_0^n+0{,}5\Delta_0^f\right), \\ S_1, if\ f\in\left[f_1^n-0{,}5\Delta_1^f,f_1^n+0{,}5\Delta_1^f\right), \\ \ldots \\ S_L, if\ f\in\left[f_L^n-0{,}5\Delta_L^f,f_L^n+0{,}5\Delta_L^f\right]. \end{cases} \tag{В.5}$$

Обернене перетворення Фур'є від (В.5) дає аналітичний вигляд мовленнєвого сигналу в спектральній його проекції

$$u(t)=\sum_{l=0}^{L}U_l\operatorname{sinc}(2\pi F_l t)\cos\left(2\pi f_l^n t\right), \tag{В.6}$$

де $F_l=0{,}5\Delta_l^f$; $U_l=S_l^u\Delta_l^f=2S_l^u F_l$. Якщо прийняти $f_l^n=lf_0$; $\Delta_l^f=\Delta_0^f$; $l=\overline{0,L}$, то вираз (В.6) набуде спрощеного вигляду

$$u(t)=\operatorname{sinc}(2\pi F_0 t)\sum_{l=0}^{L}U_l\cos(2\pi f_0 t). \tag{В.7}$$

Аналізуючи модель (В.7) можна побачити, що вона структурно близька із моделлю (2.24), тобто узагальнює опис модулювального і несного коливань. Втім аналітичний вигляд цих коливань для моделі (В.7) інший:

$$u_m(t)=\operatorname{sinc}(2\pi F_0 t); \tag{В.8}$$

$$u_n(t) = \sum_{l=0}^{L} U_l \cos(2\pi f_0 t). \qquad (B.9)$$

Виявлена структурна подібність моделей (2.24) і (В.7) дозволяє вжити для аналізу моделі (В.7) синтезований для аналізу моделі (2.24) математичний апарат. Отже, амплітудні коефіцієнти U_l моделі (В.7) знайдемо, розв'язавши систему вигляду (2.11), отриману за описом нормованих автокореляційних функцій моделі (В.7) методом найменших квадратів із мінімізацією середньоквадратичної похибки за виразом (2.6). Необхідні для розрахунку параметри $B_u(\tau)$ і E_u для моделі (В.7) мають вигляд:

$$\begin{aligned} B_u(\tau) &= U_0^2 \left(\Delta_0^f\right)^{-1} \operatorname{sinc}\left(\pi \Delta_0^f \tau\right) + \\ &+ 2\sum_{l=1}^{L} U_l^2 \left(\Delta_l^f\right)^{-1} \operatorname{sinc}\left(\pi \Delta_l^f \tau\right) \cos\left(2\pi l \Delta_l^f \tau\right) = \\ &= \left(2F_0\right)^{-1} \operatorname{sinc}\left(2\pi F_0 \tau\right) U_0^2 + \\ &+ \left(F_0\right)^{-1} \operatorname{sinc}\left(2\pi F_0 \tau\right) \sum_{l=1}^{L} U_l^2 \cos\left(2\pi l f_0 \tau\right); \end{aligned} \qquad (B.10)$$

$$E_u = \left(\Delta_0^f\right)^{-1} U_0^2 + 2\sum_{l=1}^{L} \left(\Delta_l^f\right)^{-1} U_l^2 = \left(2F_0\right)^{-1} U_0^2 + F_0^{-1} \sum_{l=1}^{L} U_l^2 . \qquad (B.11)$$

Зауважимо, що вирази для розрахунку цих параметрів отримано в результаті оберненого перетворення Фур'є спектральної щільності потужності $W^u(\omega) = \left|S^u(\omega)\right|^2$:

$$W_l = S_l^2 = \left(U_l \left(\Delta_l^f\right)^{-1}\right)^2 = \left(0.5 U_l F_l^{-1}\right)^2 .$$

Для спрощення розрахунків не враховуватимемо низькочастотну складову сигналу (В.7) при $l = 0$ і покладатимемо потужність однотипних за вмістом та суб'єктом, що їх виголосив, мовленнєвих сигналів сталою величиною. Ці припущення роблять рівняння системи (2.14), утворені для моделі (В.7) із урахуванням (В.10) і (В.11), лінійними, що дозволяє однозначно розрахувати

значення коефіцієнтів U_l^2. Необхідну для розв'язку відносно U_l системи лінійних рівнянь виду (2.14) множину коефіцієнтів S_{ij} знайдемо, використовуючи вираз

$$S_{ij} = F_0^{-1}\mathrm{sinc}(2\pi F_0 i\Delta)\sum_{j=1}^{L}\cos(2\pi j f_0 i\Delta). \qquad (B.12)$$

Дослідження інформативності спектрального представлення мовленнєвого сигналу для задачі АСГ, втілене у модель (2.32), можна розвинути в формалізацію зв'язку таких характеристик мовленнєвого сигналу як обвідна енергії спектра і параметри модулювальних коливань, утворюваних голосовим джерелом, функціонування якого описуватиметься моделлю (2.24). Позначивши $\Omega_k = 2\pi k F_0$ і $\omega_l = 2\pi l f_0$, перепишемо аналітичну форму моделі (2.24):

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

Обвідну сигналу $u(t)$ можна описати виразом

$$U(t) = \sqrt{u^2(t) + v^2(t)}, \qquad (B.13)$$

де $v^2(t)$ – сигнал, спряжений із $u(t)$ за Гілбертом [274, 275].

Властивості перетворення Гілберта дозволяють записати

$$U(t) = |u_m(t)|U_n(t), \qquad (B.14)$$

де $U_n(t)$ – обвідна несного коливання. Далі будемо розглядати додатно визначенні модулювальні коливання: $u_m(t) \geq 0$. Згідно із (2.24) несний сигнал опишемо виразом $u_n(t) = \sum_{l=1}^{L} U_l \cos(\omega_l t + \varphi_l)$, тоді спряжений із ним за Гілбертом сигнал опишемо виразом $v_n(t) = \sum_{l=1}^{L} U_l \sin(\omega_l t + \varphi_l)$. Згідно із (B.13) обвідну несного коливання опишемо виразом

$$U_n(t) = \sqrt{u_n^2(t) + v_n^2(t)} = \sqrt{\sum_{l,n=1}^{L} U_n U_l \cos((\omega_n - \omega_l)t + \varphi_n - \varphi_l)}. \qquad (B.15)$$

Враховуючи (B.14) і (B.15), опишемо обвідну мовленнєвого сигналу виразом

$$U(t)=u_m(t)\sqrt{u_n^2(t)+v_n^2(t)}=\sqrt{\sum_{l,n=1}^{L}U_nU_l\cos((\omega_n-\omega_l)t+\varphi_n-\varphi_l)}=$$
$$=\sum_{k=0}^{K}M_k\cos(\Omega_k t+\Gamma_k)\sqrt{\sum_{l,n=1}^{L}U_nU_l\cos((\omega_n-\omega_l)t+\varphi_n-\varphi_l)}. \quad (B.16)$$

Виділимо модулювальне коливання із моделі обвідної (B.15), врахувавши (B.16)

$$U_n(t)=$$
$$=\sqrt{\left(1-\sum_{\substack{l,n=1,\\ n\neq l}}^{L}U_nU_l\cos((\omega_n-\omega_l)t+\varphi_n-\varphi_l)\right)}. \quad (B.17)$$

Розкладемо функцію (B.17) у ряд Тейлора і, обмежуючись двома першими членами ряду, отримаємо

$$U_n(t)\approx\sqrt{\sum_{l=1}^{L}U_l^2}\times$$
$$\times\left(1+\left(2\sum_{l=1}^{L}U_l^2\right)^{-1}\sum_{\substack{l,n=1,\\ n\neq l}}^{L}U_nU_l\cos((\omega_n-\omega_l)t+\varphi_n-\varphi_l)\right). \quad (B.18)$$

Враховуючи (B.18), вираз (B.16) представимо у вигляді

$$U(t)=u_m(t)\times$$
$$\times\left(\sqrt{\sum_{l=1}^{L}U_l^2}+\left(2\sum_{l=1}^{L}U_l^2\right)^{-1}\sum_{\substack{l,n=1,\\ n\neq l}}^{L}U_nU_l\cos((\omega_n-\omega_l)t+\varphi_n-\varphi_l)\right). \quad (B.19)$$

Із виразу (B.19) видно, що в обвідній мовленнєвого сигналу містяться як високочастотні, так і низькочастотні коливання, які пропорційні модулювальним коливанням.

Пропустимо обвідну (B.19) крізь фільтр низьких частот із частотним передатним коефіцієнтом $K(j\omega)$ і в результаті отримаємо

$$u_{LPF}(t)\approx u_m(t)\sqrt{\sum_{l=1}^{L}U_l^2}\left|K(j\omega)\right|_{\omega<\omega_z}+{}_m(t)\left(\sum_{l=1}^{L}U_l^2\right)^{-0,5}\times \quad (B.20)$$

$$\times \sum_{\substack{l,n=1,\\ n\neq l}}^{L} U_n U_l \cos\left(\left(\omega_n-\omega_l\right)t+\varphi_n-\varphi_l+\arg\left(K\left(j\omega\right)\right)\right)\left|K\left(j\omega\right)\right|_{\omega<\omega_z},$$

де ω_z – частота зрізання фільтра.

Вважатимемо, що при $\min\left(\omega_n-\omega_l\right)>\omega_z$ амплітудно-частотна характеристика фільтра $\left|K\left(j\omega\right)\right|\approx 0$, а при $\max\left(\Omega_k\right)<\omega_z$ – $\left|K\left(j\omega\right)\right|\approx 1$, тоді вираз (В.20) можна спростити

$$u_{LPF}\left(t\right)\approx u_m\left(t\right)\sqrt{\sum_{l=1}^{L} U_l^2}\,. \qquad \text{(В.21)}$$

Інтерпретувати (В.21) можна так: сигнал обвідної на виході фільтра низьких частот пропорційний модулювальному коливанню. Враховуючи, що потужність сигналу $u\left(t\right)$ $E=0{,}5\tau_i\sum_{l=1}^{L}U_l^2$, а його середня потужність $\overline{P}=E\tau_i^{-1}=0{,}5\sum_{l=1}^{L}U_l^2$, вираз (В.21) можна перетворити до вигляду

$$u_m\left(t\right)=\left(2\overline{P}\right)^{-0.5}u_{LPF}\left(t\right). \qquad \text{(В.22)}$$

Інтерпретувати (В.22) можна так: модулювальний сигнал можна виділити із мовленнєвого сигналу, пропустивши обвідну останнього крізь фільтр низьких частот.

Конкретизуємо описані вище процедури для мовленнєвого сигналу $u\left(t\right)$ тривалістю τ_i, оцифрованого із частотою дискретизації $\Delta=f_d^{-1}$ у масив $Y=\left(y_1,\ldots,y_i,\ldots,y_{N-1}\right)$, де $y_i=x_i-\overline{x}$, $N=\tau_i\Delta^{-1}$. Обчислюватимемо обвідну сигналу $u\left(t\right)$, виходячи із положення перетворення Гілберта: $\dot{Z}\left(\omega\right)=\begin{cases}2\dot{U}\left(\omega\right), if\ \omega\geq 0,\\ 0, if\ \omega<0,\end{cases}$ де $\dot{U}\left(\omega\right)$ – спектральна щільність мовленнєвого сигналу $u\left(t\right)$, а $\dot{Z}\left(\omega\right)$ – спектральна щільність аналітичного сигналу $z\left(t\right)$. Спектр мовленнєвого сигналу $u\left(t\right)$, представленого масивом Y, розрахуємо за алгоритмом швидкого перетворення Фур'є, результатом роботи якого буде множина коефіцієнтів $\dot{C}u_k$, $k=\overline{0,N-1}$, пропорційна множині коефіцієнтів аналітичного сигналу $\dot{C}z_k$: $\dot{C}z_k=2\dot{C}u_k$. Застосувавши алгоритм оберненого

перетворення Фур'є до коефіцієнтів $\dot{C}z_k$, отримаємо множину відліків аналітичного сигналу $\dot{Z} = (\dot{z}_1, \ldots, \dot{z}_i, \ldots, \dot{z}_N)$, які описують обвідну мовленнєвого сигналу $u(t)$

$$U_i = |\dot{z}_i| = \sqrt{\dot{u}_i^2 + \dot{v}_i^2}\,. \qquad \text{(B.23)}$$

Для подальшого оброблювання обвідної застосуємо фільтр низьких частот Батерворта третього порядку [247], якому властива рівномірна амплітудно-частотна характеристика $A(\omega) = |K(j\omega)|$ у смузі пропускання і достатнє ослаблення сигналу у смузі затримування. Фільтрація відбуватиметься за алгоритмом

$$w_i = \sum_{j=0}^{p_{LPF}} a_j U_{i-j} + \sum_{m=0}^{p_{LPF}} a_m U_{i-m}\,, \qquad \text{(B.24)}$$

де w_i – відлік сигналу на виході фільтра; p_{LPF} – порядок фільтра (у нашому випадку $p_{LPF} = 3$); $\{a_0, \ldots, a_{p_{LPF}}, b_0, \ldots, b_{p_{LPF}}\}$ – множина коефіцієнтів фільтра, які розраховуються за виразами:

$$a_0 = \omega_z^3 B^{-1},\ a_1 = 3a_0,\ \ a_2 = 3a_0,\ a_3 = a_0;$$

$$b_1 = \left(24\Delta^{-3} + 48\omega_z\Delta^{-2} - 4\omega_z^2\Delta^{-1} - 3\omega_z^2\right)B^{-1};$$

$$b_2 = \left(-24\Delta^{-3} + 8\omega_z\Delta^{-2} + 4\omega_z^2\Delta^{-1} - 3\omega_z^2\right)B^{-1};$$

$$b_3 = \left(8\Delta^{-3} - 8\omega_z\Delta^{-2} + 4\omega_z^2\Delta^{-1} - \omega_z^2\right)B^{-1};$$

$$B = 8\Delta^{-3} + 8\omega_z\Delta^{-2} + 4\omega_z^2\Delta^{-1} + \omega_z^2.$$

Зауважимо, що фільтрація супроводжується фазовими затримками, тобто сигнал на виході фільтра є зміщеним у часі відносно вихідного сигналу на часовий інтервал [247, 248] $\tau(\omega) = -\dfrac{d\Gamma(\omega)}{d\omega}$, де $\Gamma(\omega) = \arg(K(j\omega))$ – фазо-частотна характеристика рекурсивного цифрового фільтра [248].

Значення середньої потужності мовленнєвого сигналу $\overline{P}$ можна розрахувати за виразом

$$\overline{P} = N^{-1} \sum_{i=1}^{N} y_i^2 \,, \tag{B.25}$$

що дозволяє перетворити вираз (B.22) до вигляду

$$u_{mi} = \left(2\overline{P}^2\right)^{-0.5} w_i \,. \tag{B.26}$$

Аналіз (B.26) дозволяє стверджувати: якщо модулювальне коливання, описуване виразом (B.22), є періодичною функцією з періодом розкладання $T_\Omega = \tau_i$ і основною частотою $\Omega_1 = 2\pi F_0 = 2\pi T_\Omega^{-1}$ при частоті кратних гармонік $\Omega_k = 2\pi k F_0 = 2\pi k T_\Omega^{-1}$, то прицезійніший опис модулювального коливання рядом Фур'є досягається при урахуванні $K = 5 \div 10$ членів ряду. Це твердження дозволяє сформулювати такий вираз для оцінювання частоти зрізання синтезовуваного фільтра:

$$f_z = F_K = KF_0 = KT_\Omega^{-1} = K\tau_i^{-1} \,. \tag{B.27}$$

Резюмуючи сказане констатуємо, що виділити модулювальне коливання $u_m(t)$ можна:

1) підібравши аналітичний вигляд опису модулювального коливання $u_m(t)$ у моделі ІГМС $u(t)$ так, щоб мінімізувати похибку $\|u(t) - y(t)\|$;

2) пропустивши мовленнєвий сигнал $u(t)$ крізь елемент із нелінійною характеристикою, наприклад, $u_{ne}(t) = (u(t))^2$, відфільтрувавши згодом отриманий сигнал фільтром низьких частот із частотою зрізання $f_z > F_K$;

3) обчисливши його обвідну $U(t)$, яку згодом відфільтрувати фільтром низьких частот із частотою зрізання $f_z > F_K$.

Для першого варіанта при безпосередній реалізації не існує однозначного розв'язку, другий варіант привносить у модулювальний сигнал нелінійні спотворення, позбавитися яких згодом неможливо. Лише третій варіант поєднує достатню для АСГ прицезійність оцінювання модулювальних коливань із прийнятною обчислювальною складністю виконуваних при його отриманні обчислювальних операцій.

Додаток Д

Синтез і дослідження бікомпонентної моделі фонетичної динаміки мовленнєвого сигналу

У моделі (2.80) мовленнєвий сигнал $\xi(t)$ розглядається як стохастичний бікомпонентний процес у складі періодичної компоненти $u(t)$, описуваної квазідетермінованою або стохастичною моделлю з-поміж моделей (2.1), (2.24), (2.46), (2.64), і стохастичної компоненти $n(t)$, вживаної для опису шумних фрагментів. Запропонований у підрозділі 2.6 спосіб вибору моделі для опису фрагментів вихідного мовленнєвого сигналу на основі значення дисперсії відношення «сигнал»/«шум» $D_z(t)$ (2.90) є порівняно простим, проте не формалізує динаміку процесу переходу між компонентами моделі (2.80). Прогнозуючи присутність у досліджуваному на часовому інтервалі $\tau = t_2 - t_1$, $t_2 > t_1$, випадковому мовленнєвому сигналі $\xi(t)$ квазідетермінованої компоненти, використаємо в якості його узагальненої характеристики автокореляційну функцію

$$B_\xi(\tau) = \int_{-\infty}^{\infty} \xi(t)\xi(t-\tau)dt\,. \qquad (Д.1)$$

Вважаючи, що у випадковому мовленнєвому сигналі $\xi(t)$ міститься як квазіквазідетермінована періодична компонента $u(t)$, так і обмежений певною частотною смугою білий шум $n(t)$, конкретизуємо вираз (Д.1) для центрованих процесів $u(t)$ і $n(t)$ тривалістю τ_i, враховуючи їх стаціонарність і ергодичність,

$$B_\xi(\tau) = \tau_i\left(R_u(\tau) + R_n(\tau) + R_{un}(\tau) + R_{nu}(\tau)\right), \qquad (Д.2)$$

де функції кореляції $R_u(\tau)$, $R_n(\tau)$ і взаємні функції кореляції $R_{un}(\tau)$, $R_{nu}(\tau)$ випадкових сигналів $u(t)$ і $n(t)$ описуються відповідними виразами:

$$R_u(\tau) = \lim_{\tau_i \to \infty} \tau_i^{-1} \int_0^{\tau_i} u(t)u(t-\tau)dt \approx \tau_i^{-1} \int_0^{\tau_i} u(t)u(t-\tau)dt\,; \qquad (Д.3)$$

$$R_n(\tau) = \lim_{\tau_i \to \infty} \tau_i^{-1} \int_0^{\tau_i} n(t)n(t-\tau)dt \approx \tau_i^{-1} \int_0^{\tau_i} n(t)n(t-\tau)dt\,; \qquad (Д.4)$$

$$R_{un}(\tau)=\lim_{\tau_i\to\infty}\tau_i^{-1}\int_0^{\tau_i}u(t)n(t-\tau)dt\approx\tau_i^{-1}\int_0^{\tau_i}u(t)n(t-\tau)dt\,; \qquad (Д.5)$$

$$R_{nu}(\tau)=\lim_{\tau_i\to\infty}\tau_i^{-1}\int_0^{\tau_i}n(t)u(t-\tau)dt\approx\tau_i^{-1}\int_0^{\tau_i}n(t)u(t-\tau)dt\,. \qquad (Д.6)$$

Вважаючи випадкові сигнали $u(t)$ і $n(t)$ взаємно некорельованими $(R_{un}(\tau)=R_{nu}(\tau)=0)$, вираз (Д.2) можна спростити:

$$B_\xi(\tau)=\tau_i(R_u(\tau)+R_n(\tau)). \qquad (Д.7)$$

Оскільки $u(t)$ – квазідетермінований сигнал, то бікомпонентний випадковий процес $\xi(t)$ не є стохастичним і залежить від часу:

$$m_\xi(t)=\overline{\xi(t)}=\overline{u(t)+n(t)}=u(t)+\overline{n(t)}. \qquad (Д.8)$$

Якщо компоненту $n(t)$ вважати центрованою $(\overline{n(t)}=0)$, то вираз (Д.8) спрощується:

$$m_\xi(t)=u(t),$$

а функції кореляції випадкових сигналів $\xi(t)$ і $n(t)$ співпадатимуть:

$$R_\xi(t_1,t_2)=\overline{(\xi(t_1)-m_\xi(t_1))(\xi(t_2)-m_\xi(t_2))}=$$
$$=\overline{(u(t_1)+n(t_1)-u(t_1)+\overline{n(t_1)})(u(t_2)+n(t_2)-u(t_2)+\overline{n(t_2)})}= \qquad (Д.9)$$
$$=\overline{(n(t_1)-m_n(t_1))(n(t_2)-m_n(t_2))}=R_n(t_1,t_2).$$

Якщо врахувати, що $n(t)$ – стаціонарний ергодичний центрований випадковий процес, то $R_\xi(\tau)=R_n(\tau)$, де $R_n(\tau)$ розраховується за виразом (Д.4). Відповідно, при $n(t)\to 0$, $R_\xi(\tau)=R_n(\tau)=0$, тобто на інтервалі τ випадковий сигнал $\xi(t)$ утворюється виключно квазідетермінованою компонентою $u(t)$, відліки якої не мають статистичного зв’язку.

Опишемо нестаціонарний бікомпонентний випадковий процес $\xi(t)$ виразом

$$B_\xi(\tau)=B_u(\tau)+\tau_iR_n(\tau)+B_{un}(\tau)+B_{nu}(\tau), \qquad (Д.10)$$

де автокореляційну функцію $B_u(\tau)$ і взаємокореляційні функції $B_{un}(\tau)$, $B_{nu}(\tau)$ опишемо відповідними виразами:

$$B_u(\tau)=\int_{-\infty}^{\infty}u(t)u(t-\tau)dt\,; \qquad (Д.11)$$

$$B_{un}(\tau)=\int_{-\infty}^{\infty}u(t)n(t-\tau)dt\,; \qquad (Д.12)$$

$$B_{nu}(\tau)=\int_{-\infty}^{\infty}n(t)u(t-\tau)dt\,. \qquad (Д.13)$$

Вважатимемо компоненти $u(t)$ і $n(t)$ некорельованими, тоді

$$B_{un}(\tau)=\int_{0}^{\tau_i}u(t)n(t-\tau)dt=\tau_i\left(\tau_i^{-1}\int_{0}^{\tau_i}u(t)n(t-\tau)dt\right)=$$

$$=\tau_i\langle u(t)n(t-\tau)\rangle=\tau_i\overline{u(t)n(t-\tau)}=\tau_i u(t)\overline{n(t-\tau)}=0\,;$$

$$B_{nu}(\tau)=\tau_i\langle n(t)u(t-\tau)\rangle=\tau_i\overline{n(t)u(t-\tau)}=\tau_i\overline{n(t)}u(t-\tau)=0,$$

де $\langle u(t)n(t-\tau)\rangle$, $\langle n(t)u(t-\tau)\rangle$ – стаціонарні ергодичні центровані випадкові процеси. Зрештою, вираз (Д.10) спрощується до вигляду

$$B_\xi(\tau)=B_u(\tau)+\tau_i R_n(\tau). \qquad (Д.14)$$

Формалізуємо перехід від бікомпонентної моделі $\xi(t)$ до квазіквазідетермінованої моделі. Згідно із (Д.7), такий перехід можливий у двох випадках – коли $n(t)\to 0$ або коли $u(t)\to 0$. Проаналізуємо ці варіанти почергово. Нехай $n(t)\to 0$, що у контексті (2.90) відповідає варіанту коли $D_z>>1$ або $D_z=R_u(0)(R_n(0))^{-1}=D_u(D_n)^{-1}>>1$, тобто $\xi(t)\approx u(t)$ і вираз (Д.7) збігається до вигляду

$$B_\xi(\tau)=\tau_i R_u(\tau). \qquad (Д.15)$$

Якщо ж $u(t)\to 0$, що в контексті (2.90) відповідає варіанту коли $D_z<<1$, тобто $\xi(t)\approx n(t)$, то вираз (Д.7) збігається до вигляду

$$B_\xi(\tau)=\tau_i R_n(\tau). \qquad (Д.16)$$

Формалізуємо перехід від бікомпонентної моделі $\xi(t)$ до квазідетермінованої моделі. Згідно із (Д.7) такий перехід можливий у двох випадках – коли $n(t)\to 0$ або коли $u(t)\to 0$. Проаналізуємо ці варіанти почергово.

Нехай $n(t) \to 0$, що у контексті (2.90) відповідає варіанту коли $D_z >> 1$, тобто $\xi(t) \approx u(t)$ і вираз (Д.14) збігається до $B_\xi(\tau) = B_u(\tau)$. Якщо ж $u(t) \to 0$, що у контексті (2.90) відповідає варіанту коли $D_z << 1$, тобто $\xi(t) \approx n(t)$ і вираз (Д.14) збігається до (Д.16).

У загальному випадку бікомпонентну модель можна описати функцією $\xi(\varphi(t), t)$, де $\varphi(t)$ – вектор випадкових процесів, окремим випадком якої буде квазіквазідетермінована функція $\xi(\varphi(t), t) = \xi(\varphi, t)$, яку можна інтерпретувати як квазідетерміновану функцію $\xi(t)$ із стохастичною векторною складовою φ. Наприклад, у квазіквазідетермінованій функції $\xi(\varphi, t) = A\sin(\omega t + \varphi)$ в залежності від постановки задачі стохастичними складовими можуть бути: амплітуда A, частота ω, початкова фаза φ тощо. Перехід від стохастичної до квазідетермнованої моделі можливий при заданні початкових умов для випадкової величини, наприклад, $\varphi(t_0) = \varphi_0$. Зважаючи, що одновимірна щільність імовірності випадкової величини φ_0 не залежить від часу, запишемо $p_0(\varphi_0, t) = p(\varphi_0)$. Якщо початкове значення випадкової величини є квазідетермінованим – $\varphi(t_0) = \varphi_0^{\det}$, то щільність імовірності такої випадкової величини опишемо дельта-функцією [279] $p(\varphi_0) = \delta\left(\varphi_0 - \varphi_0^{\det}\right)$. Подальшим кроком стане перехід від випадкової величини до квазідетермінованого, залежного від часу, сигналу $u\left(\varphi_0^{\det}, t\right) \equiv u^{\det}(t)$.

Застосуємо викладені положення до бікомпонентної моделі (2.64), яку у загальному вигляді можна класифікувати як стохастичну модель, до складу якої входять випадкові величини – початкові фази φ_l і Γ_k, із одновимірними щільностями імовірностей $f_0(\varphi_l, t) = p_0(\varphi_l, t)$ і $f_1(\Gamma_k, t) = p_0(\Gamma_k, t)$, відповідно. Якщо ці випадкові величини взаємно некорельовані і рівномірно розподілені на інтервалі $[0, 2\pi]$, то можна стверджувати, що $p_0(\varphi_l, t) = p_0(\varphi_l) = 0{,}5\pi^{-1}$ і $p_0(\Gamma_k, t) = p_0(\Gamma_k) = 0{,}5\pi^{-1}$, тобто модель (2.64) є квазіквазідетермінованою. В свою

чергу, квазіквазідетерміновану модель (2.64) можна звести до квазідетермінованої моделі (2.24), якщо виконаються умови $p_0(\varphi_l)=\delta\left(\varphi-\varphi_\partial^{\det}\right)$ і $p_0(\Gamma_k)=\delta\left(\Gamma-\Gamma_k^{\det}\right)$.

Формалізуємо зв'язок автокореляційної функції $B_\xi(\tau)$ випадкового сигналу $\xi_0(t)$ і кореляційної функції $R_u(\tau)$ квазіквазідетермінованого сигналу $u(t)$, нехтуючи шумною компонентною. Узагальнюючи вирази (Д.3), (Д.11), (Д.15) на основі [212, 213], можна описати зв'язок між $B_\xi(\tau)$ і $R_u(\tau)$ виразом

$$R_u(\tau)=\lim_{\tau_i\to\infty}\left(\tau_i^{-1}B_\xi(\tau)\right), \tag{Д.17}$$

який для практичного застосування можна спростити до вигляду

$$R_u(\tau)=\tau_i^{-1}B_\xi(\tau), \tag{Д.18}$$

тобто відношення автокореляційної функції $B_\xi(\tau)$ випадкового сигналу $\xi_0(t)$ і кореляційної функції $R_u(\tau)$ квазіквазідетермінованого сигналу $u(t)$ збігається до сталої величини τ_i^{-1} [237]. Відповідно, нормовану автокореляційну функцію $r_u(\tau)$ центрованого сигналу $\xi_0(t)$ можна описати кореляційними коефіцієнтами $b_\xi(\tau)$ квазідермінованого випадкового процесу $u(t)$ як

$$r_u(\tau)=b_\xi(\tau), \tag{Д.19}$$

де

$$r_u(\tau)=R_u(\tau)(R_u(0))^{-1}=R_u(\tau)D_u^{-1}; \tag{Д.20}$$

$$b_\xi(\tau)=B_\xi(\tau)\left(B_\xi(0)\right)^{-1}=B_\xi(\tau)E_\xi^{-1}, \tag{Д.21}$$

а D_u – дисперсія сигналу $u(t)$; E_ξ – потужність сигналу $\xi_0(t)$.

Продовжимо аналіз зв'язку сигналів $\xi_0(t)$ і $u(t)$ у дискретному їх представленні відліками $\xi_n=\xi(t_n)=\xi(n\Delta)$ і $u_n=u(t_n)=u(n\Delta)$, отриманими із частотою дискретизації Δ^{-1}. Автокореляційну $B_\xi(j)$, і нормовану автокореляційну $b_\xi(j)$ функції випадкового дискретного сигналу ξ_n отримаємо на основі виразу (Д.1) при $j=\overline{0,J}$:

$$B_{\xi}(j)=\sum_{n=-\infty}^{\infty}\xi_n\xi_{n-j}=\sum_{n=1}^{N-j}\xi_n\xi_{n+j}\,; \qquad (Д.22)$$

$$b_{\xi}(j)=B_{\xi}(j)\left(B_{\xi}(0)\right)^{-1}=B_{\xi}(j)E_{\xi}^{-1}, \qquad (Д.23)$$

де N – кількість відліків.

Кореляційну функцію ергодичного стаціонарного дискретного випадкового сигналу u_n згідно із [253] при $j=\overline{0,J}$ опишемо виразом

$$R_u(j)=\lim N^{-1}\sum_{n=1}^{N-j}(u_n-m_u)(u_{n+j}-m_u), \qquad (Д.24)$$

де $m_u=\lim\limits_{N\to\infty}N^{-1}\sum\limits_{n=1}^{N}u_n$ – математичне сподівання.

Оцінки кореляційної функції (Д.24) для центрованого ергодичного стаціонарного дискретного випадкового сигналу u^c опишемо виразом

$$R_{u^c}(j)=(N-1)^{-1}\sum_{n=1}^{N-j}u_n^c u_{n+j}^c\approx N^{-1}\sum_{n=1}^{N-j}u_n^c u_{n+j}^c\,, \qquad (Д.25)$$

а вираз для обчислення кореляційних коефіцієнтів матиме вигляд

$$r_{u^c}(j)=R_{u^c}(j)\left(R_{u^c}(0)\right)^{-1}=R_{u^c}(j)D_{u^c}^{-1}. \qquad (Д.26)$$

За аналогією із (Д.17), опишемо зв’язок функції $R_{u^c}(j)$ і $B_{\xi}(j)$ залежністю

$$R_{u^c}(j)=\lim_{N\to\infty}\left(N^{-1}B_{\xi}(j)\right)\approx N^{-1}B_{\xi}(j), \qquad (Д.27)$$

на основі якої можна стверджувати, що

$$r_{u^c}(j)=b_{\xi}(j). \qquad (Д.28)$$

Отже, результати проведеного вище аналізу бікомпонентної моделі (Д.1) без урахування її шумної складової показують, що характеристики стохастичної і квазідетермінованої її складових параметрично тотожні, отже, можуть бути обчислені із використанням ідентичного математичного апарату. Скориставшись цим висновком сформулюємо орієнтовану на практичне застосування процедуру розрахунку характеристичних параметрів моделей (2.1), (2.24), (2.46), (2.64) тощо.

Нехай в результаті кореляційного аналізу емпіричних мовленнєвих сигналів розраховано K_j, $j=\overline{1,J}$, коефіцієнтів функції кореляції. Відповідно,

автокореляційну або кореляційну функцію математичної моделі ІГМС $K_a(\tau)$ визначено одним із виразів (2.9), (2.25), (2.49), (2.67) та узагальнено у вигляді

$$K_a(\tau) = \sum_{l=0}^{L} U_l^2 S_l(\tau), \qquad (Д.29)$$

де U_l^2 – амплітуди несних гармонік моделі; $S_l(\tau)$ – параметричні функції моделі, значення яких визначається номером несної гармоніки l, тривалістю інтервалу спостереження τ і видом математичної моделі. На основі (Д.29) отримаємо нормовану автокореляційну функцію математичної моделі:

$$R_{a_j} = K_a(j\Delta)(K_a(0))^{-1} = K_{a\,j}(K_{a0})^{-1}. \qquad (Д.30)$$

Обчислимо значення параметрів U_l, застосувавши метод найменших квадратів для мінімізації похибки моделі

$$\varepsilon = \sum_{j=1}^{J} \left(R_{a_j} - R_j\right)^2. \qquad (Д.31)$$

Для квазідетермінованої математичної моделі відповідні параметри (Д.31) опишемо виразами $R_j = b_j^y = B_j^y\left(B_0^y\right) = B_j^y\left(E^y\right)^{-1}$, $R_{a_j} = b_j^u = B_j^u\left(B_0^u\right) = B_j^u\left(E^u\right)^{-1}$, де y – центрований емпіричний сигнал, а u – математична модель, що його описує.

Для квазіквазідетермінованої математичної моделі відповідні параметри (Д.31) опишемо виразами $R_j = r_j^y = R_j^y\left(R_0^y\right) = R_j^y\left(D_y\right)^{-1}$, $R_{a_j} = r_j^u = R_j^u\left(R_0^u\right) = R_j^u\left(D_u\right)^{-1}$, де R_j^y і D_y – функція кореляції і дисперсія центрованого емпіричного сигналу y, відповідно; R_j^u і D_u - функція кореляції і дисперсія математичної моделі u, що описує y, відповідно.

Візьмемо частинні похідні від (Д.31) за всіма коефіцієнтами U_l, $l = \overline{0, L}$, почергово, прирівнявши кожен із отриманих аналітичних виразів до нуля:

$$\sum_{j=1}^{J} \left|R_{a_j} - R_j\right| \frac{\partial R_{a_j}}{\partial U_l} = 0, \qquad (Д.32)$$

отримавши в результаті систему нелінійних рівнянь – степеневих поліномів четвертого степеня, яка не має однозначного розв’язку [273].

Для спрощення отриманої системи припустимо, що такі характеристики мовленнєвого матеріалу, вживаного для АСГ, як потужність (у випадку квазідетермінованої моделі) та дисперсія (у випадку квазіквазідетермінованої моделі) є сталими величинами $K_{a_0} = const$. Врахувавши це припущення приведемо систему (Д.32) до системи лінійних рівнянь виду:

$$\sum_{j=1}^{J} \left| R_{a_j} - R_j \right| \frac{\partial R_{a_j}}{\partial V_l} = 0, \qquad (Д.33)$$

де $V_l = U_l^2$, у якій, із урахуванням (Д.30),

$$K_{a_j} = \sum_{l=0}^{L} V_l S_{jl}, \qquad (Д.34)$$

де $K_{a_j} = K_a(j\Delta)$, $S_{jl} = S_l(j\Delta)$.

Узагальнимо всі ці операції, перетворивши (Д.33) до вигляду

$$\left(K_{a_0}\right)^{-1} \sum_{l=0}^{L} \left(\sum_{j=1}^{J} S_{jp} S_{jl} \right) V_l = \sum_{j=1}^{J} S_{j0} R_j, \qquad (Д.35)$$

де $p = \overline{0, L}$.

Введемо заміни $A_{p,l} = \left(K_{a_0}\right)^{-1} \sum_{l=0}^{L} \left(\sum_{j=1}^{J} S_{jp} S_{jl} \right)$, $B_p = \sum_{j=1}^{J} S_{j0} R_j$ і отримаємо компактний запис (Д.35):

$$\sum_{l=0}^{L} A_{p,l} V_l = B_p. \qquad (Д.36)$$

Значення керованих змінних V_l у системі (Д.36) можна розрахувати однозначно, застосувавши відомі методи розв’язання систем лінійних алгебраїчних рівнянь [273].

Представимо вираз (Д.34) у матричному вигляді:

$$K_a = SV, \qquad (Д.37)$$

де K_a і V – вектор-стовпці з елементів K_{a_j} і V_l розмірністю $J \times 1$ і $(L+1) \times 1$, відповідно, а S – матриця з елементів S_{jl} розмірністю $J \times (L+1)$.

Похибку моделі в контексті формалізації кореляційних функцій у матричному вигляді опишемо як

$$\varepsilon(V) = (K_a - K)^T (K_a - K) = (K - K_a)^T (K - K_a) = \\ = (K - SV)^T (K - SV), \tag{Д.38}$$

де T – операція транспонування, а K – вектор-стовпець з елементів K_j розмірністю $J \times 1$.

Представимо умову (Д.33) у матричному вигляді виразом

$$\frac{\partial \varepsilon}{\partial V} = 0, \tag{Д.39}$$

підставивши у який вираз (Д.38) і здійснивши операцію скалярно-матричного диференціювання [237], отримаємо вираз

$$2S^T (K - SV) = 0,$$

звідки

$$S^T SV = S^T K \Rightarrow V = \left(S^T S\right)^{-1} S^T K. \tag{Д.40}$$

Зауважимо, що вираз (Д.40) із урахуванням (Д.30) можна записати і відносно вектор-стовпця R з елементів R_j розмірністю $J \times 1$:

$$V = K_{a_0} \left(S^T S\right)^{-1} S^T R, \tag{Д.41}$$

де $K_0 = K_{a_0}$.

В залежності від вибору моделі індивідуальності ІГМС змінюватимуться лише окремі параметри виразів (Д.29) і (Д.31). У виразі (Д.29) змінюватиметься аналітичний вигляд характеристичної функції $S_l(\tau)$, що відбиватиметься на значеннях параметрів S_{jl} і K_{a_j}, вживаних у виразах (Д.34), (Д.35). У виразі (Д.31) змінюватиметься інтерпретація параметрів R_{a_j} і R_j. Згадані зміни не спричиняють змін у перебігу процесу розрахунку параметрів $U_l = \sqrt{V_l}$, узагальненого виразами (Д.40), (Д.41).

У виразі (Д.31) для обчислення значень параметрів U_l застосовується метод найменших квадратів. Оцінки $\widehat{V}_l$ параметрів U_l, обчислених за методом найменших квадратів, є незміщеними і ефективними оцінками лінійної моделі в класі лінійних функцій від даних, що спостерігаються [253]. Це твердження обґрунтовується виразом (Д.37), в якому вектор-стовпці шуканих параметрів V і спостережень K пов'язні лінійною залежністю, втіленою в ідентифіковану матрицю характеристичних коефіцієнтів S. Опишемо матрицю розсіювання $\Pi(\widehat{V})$ вектор-стовпця оцінок V, який містить значення $\widehat{V}_l$, виразом

$$\Pi(\widehat{V}) = D\left(S^T S\right)^{-1} = (J-L)^{-1}(K-SV)^T(K-SV)\left(S^T S\right)^{-1}, \qquad (Д.42)$$

де $D = (J-L)^{-1}(K-SV)^T(K-SV)$ – незміщена дисперсія спостережень.

Представимо дисперсію $D(\widehat{V})$ і середньоквадратичне відхилення $\sigma_{\widehat{V}_l}$ множиною елементів матриці оцінок $\{\Pi(\widehat{V})\}_{l,l}$ для матриці розсіювання (Д.42):

$$D(\widehat{V}_l) = \{\Pi(\widehat{V})\}_{l.l} = (J-L)^{-1}\varepsilon(\widehat{V})\left\{\left(S^T S\right)^{-1}\right\}_{l,l}; \qquad (Д.43)$$

$$\sigma_{\widehat{V}_l} = \sqrt{D(\widehat{V}_l)} = \sqrt{(J-L)^{-1}\varepsilon(\widehat{V})\left\{\left(S^T S\right)^{-1}\right\}}. \qquad (Д.44)$$

Абсолютні похибки $\Delta_{\widehat{U}_l}$ оцінок параметрів $\widehat{U}_l$ із урахуванням довірчих інтервалів $\pm 3\sigma_{\widehat{V}_l}$ для параметрів $\widehat{V}_l$ опишемо виразом

$$\widehat{U}_l \pm \Delta_{\widehat{U}_l} = \sqrt{\widehat{V}_l \pm \Delta_{\widehat{V}_l}}, \qquad (Д.45)$$

де $\Delta_{\widehat{V}_l} \approx 3\sigma_{\widehat{V}_l}$.

Розкладемо $\sqrt{\widehat{V}_l \pm \Delta_{\widehat{V}_l}}$ у біноміальний ряд [272], врахувавши, що $\widehat{V}_l >> \Delta_{\widehat{V}_l}$. Тоді, обмежившись першими двома членами ряду, виразимо з перетвореного виразу (Д.45) оцінки

$$\Delta_{\widehat{U}_l} = 0{,}5\Delta_{\widehat{V}_l}\widehat{U}_l^{-1}. \qquad (Д.46)$$

Отримаємо аналітичний вираз для обчислення абсолютної похибки $\Delta_{\widehat{U}_l}$, підставивши (Д.44) у (Д.46) і врахувавши, що $\Delta_{\widehat{V}_l} \approx 3\sigma_{\widehat{V}_l}$:

$$\Delta_{\widehat{U}_l} = 1.5\widehat{U}_l^{-1}\sqrt{(J-L)^{-1}\varepsilon(\widehat{V})\left\{\left(S^T S\right)^{-1}\right\}}. \qquad (Д.47)$$

Відповідно, відносну похибку $\delta_{\widehat{U}_l}$ оцінок $\widehat{U}_l$ опишемо виразом

$$\delta_{\widehat{U}_l} = \Delta_{\widehat{U}_l} U_l^{-1} \cdot 100\,\%. \qquad (Д.48)$$

Аналізуючи (Д.47) і (Д.48) можна зробити висновок, що для зменшення похибок $\Delta_{\widehat{U}_l}$ і $\delta_{\widehat{U}_l}$ необхідно зменшувати похибку математичної моделі опису ІГМС $\varepsilon(\widehat{V})$. Наприклад, результатом опису фонограми зі словом «сон» математичною моделлю (2.46) із параметрами $f_d = 8000$ Гц; $\tau_i = 0{,}3$ с; $L = 6$; $M = 1$; $F_0 = 15$ Гц; $D_u = 22$; $J = 200$ є множина параметрів $f_0 = 155{,}2$ Гц, $U_1 = 2{,}173$, $U_2 = 2{,}173$, $U_3 = 3{,}994$, $U_4 = 0{,}900$, $U_5 = 0{,}937$, при цьому $\varepsilon_r = 1{,}154$, $\delta_{\widehat{U}_1} = \pm 0{,}433\%$, $\delta_{\widehat{U}_2} = \pm 0{,}464\%$, $\delta_{\widehat{U}_3} = \pm 0{,}137\%$, $\delta_{\widehat{U}_4} = \pm 2{,}707\%$, $\delta_{\widehat{U}_5} = \pm 2{,}495\%$, тобто оцінки $\widehat{U}_1 - \widehat{U}_5$ амплітуд гармонік основного тону не виходять за межі довірчих інтервалів із довірчою імовірністю $99{,}7\%$.

Отже, синтезовано бікомпонентну математичну модель ІГМС, представленою сумою квазіквазідетермінованого випадкового процесу із випадковими вихідними фазами модулювального і полігармонійного несного коливань і процесу авторегресії. Модель дозволяє враховувати рівень відношення «сигнал-шум» у досліджуваному сигналі, що є особливо важливим, враховуючи критичне застосування описуваної ІС із АСГ.

З позиції прикладного застосування можна відзначити, що квазідетермінованим моделям властива висока достовірність опису ІГМС із вокалізованим вмістом, при чому універсальну модель (2.1) можна застосовувати і у задачі текстонезалежної АСГ, а модель (2.24) є точнішою від моделі (2.1) завдяки урахуванню діяльності модулятора у процесі фонації і урахуванню початкових фаз несних і модулювальних коливань в описі мовленнєвого сигналу.

Прикладне застосування стохастичних моделей виду (2.46), (2.64) дозволяє адекватно описувати ІГМС із довільним ступенем вокалізованості і застосовувати для оброблювання емпіричних результатів широкий спектр методів теорії імовірності і математичної статистики.

Додаток Е

Методика оцінювання адекватності математичних моделей ІГМС емпіричним даним

Адекватна математична модель дозволяє описати ІГМС значеннями характеристичних параметрів, обраних у контексті її застосування, із достовірністю, встановленою за допомогою обраного критерію відповідності. Доведення адекватності моделі відбувається за результатами процедури верифікації [248], під час якої реальні емпіричні дані порівнюються із генерованими оцінюваною моделлю. Результати порівняння узагальнюються мірою близькості, значення якої аналізується правилом розв'язування у складі обраного критерію відповідності із винесенням вердикту щодо адекватності оцінюваної моделі. Питання вибору міри близькості в контексті задачі АСГ розглядається в низці публікацій [241–248] в яких, проте, не здійснено систематизацію мір близькості і критеріїв.

Нехай математична модель ІГМС генерує параметричний опис досліджуваного мовленнєвого сигналу у змінному часу. Перелічимо міри близькості, які доцільно вживати при оцінюванні адекватності моделі у такому трактуванні.

1. Сума квадратів похибок (квадрат евклідової метрики, квадрат довжини вектора похибок) між векторами емпіричних характеристичних параметрів $r^e = \left(r_1^e, r_2^e, \ldots, r_J^e\right)$ і характеристичними параметрами з виходу оцінюваної моделі $r^m = \left(r_1^m, r_2^m, \ldots, r_J^m\right)$:

$$\varepsilon = \sum_{j=1}^{J} \left(r_j^e - r_j^m\right)^2 ; \tag{E.1}$$

$$\varepsilon = \sqrt{\sum_{j=1}^{J} \left(r_j^e - r_j^m\right)^2} , \tag{E.2}$$

де $j = \overline{1, J}$ – індекс часового проміжку, а вираз (Е.2) є варіацією міри (Е.1) у випадку використання евклідової відстані в якості міри близькості. Оцінювана модель описує ІГМС найкраще при $\varepsilon \to \infty$. До переваг цієї міри віднесемо

простоту, додатність, а до недоліків – абсолютне, а не відносне значення міри, зростання значення міри із зростанням J, і те, що вклад кожної j-ї операції порівняння в підсумкову похибку є однаковим.

2. Сума квадратів похибок, поділена на кількість операцій порівняння,

$$\varepsilon = J^{-1} \sum_{j=1}^{J} \left(r_j^e - r_j^m \right)^2 , \tag{E.3}$$

яка, на відміну від (E.1), із зростанням J може залишатися без змін, або зменшуватися – заходити у межі довірчого інтервалу.

3. Зважена сума квадратів похибок

$$\varepsilon = \sum_{j=1}^{J} \omega_j \left(r_j^e - r_j^m \right)^2 , \tag{E.4}$$

де ω_j, $0 \le \omega_j \le 1$ – ваговий коефіцієнт, який дозволяє встановити важливість вкладу j-ї операції порівняння в підсумкове значення міри. Зазвичай вагові коефіцієнти нормують: $\sum_{j=1}^{J} \omega_j = 1$.

4. Зважена сума квадратів похибок, нормована за кількістю операцій порівняння,

$$\varepsilon = J^{-1} \sum_{j=1}^{J} \omega_j \left(r_j^e - r_j^m \right)^2 . \tag{E.5}$$

5. Нормована сума квадратів похибок у евклідовій метриці

$$\varepsilon = \sum_{j=1}^{J} \left(r_j^e - r_j^m \right)^2 \left(\sum_{j=1}^{J} \left(r_j^e \right)^2 \right)^{-1} . \tag{E.6}$$

Метрика (E.6) є відносною, тобто її значення є безрозмірним.

6. Зважена нормована сума квадратів похибок

$$\varepsilon = \sum_{j=1}^{J} \omega_j \left(r_j^e - r_j^m \right)^2 \left(\sum_{j=1}^{J} \left(r_j^e \right)^2 \right)^{-1} . \tag{E.7}$$

7. Відносна евклідова метрика між порівнюваними векторами

$$\varepsilon = \sqrt{\sum_{j=1}^{J}\left(r_j^e - r_j^m\right)^2 \left(\sum_{j=1}^{J}\left(r_j^e\right)^2\right)^{-1}}\ . \qquad (E.8)$$

Порівняно із мірою (E.1), задачі обчислення значень мір (E.4), (E.5), (E.7), (E.8) є суттєво ресурсозатратнішими.

8. Сума абсолютних значень різниць порівнюваних параметрів

$$\varepsilon = \sum_{j=1}^{J}\left|r_j^e - r_j^m\right|. \qquad (E.9)$$

Ця міра, у порівнянні із (E.1), є простішою для безпосереднього розрахунку, проте, викликає обчислювальні ускладнення у випадку її застосування в аналітичних розрахунках, де здійснюється математична операція обчислення похідних.

9. Узагальнена степенева відстань Мінковського [280]

$$\varepsilon = \sqrt[p]{\sum_{j=1}^{J}\left(r_j^e - r_j^m\right)^p}\ , \qquad (E.10)$$

де p – константа покажчика степеня в мірі близькості.

10. Відстань Махаланобіса [272, 273]:

$$\varepsilon = \left(r^e - r^m\right) W_o \left(r^e - r^m\right)^T, \qquad (E.11)$$

де W_o – матриця, обернена до коваріаційної [280]. Ця міра дозволяє оцінювати кореляційні зв’язки між порівнюваними параметрами, що можна використати, наприклад, для об’єктивного визначення значень вагових коефіцієнтів $w_j = W_j \Big/ \prod_{j=1}^{J} W_j$, де $W_j \equiv W_{j,j}$ – елементи діагональної коваріаційної матриці W. До недоліків цієї міри можна віднести: найбільшу з-поміж згаданих мір кількість обчислень; якщо порівнювані параметри в цілому виявляються близькими за значеннями, матриця W^{-1} вироджується; вплив на поточне j-те порівняння характеристичних параметрів решти реалізацій операцій порівняння, здійснюване через вживання в (E.11) оберненої до коваріаційної матриці W^{-1}.

Вплив другого і третього з перелічених недоліків на репрезентативність міри (Е.11) зменшується із зростанням J.

11. Коефіцієнт множинної кореляції

$$\rho = \sum_{j=1}^{J}\left(r_j^e - \overline{r}^e\right)\left(r_j^m - \overline{r}^m\right) \Bigg/ \sqrt{\left(\sum_{j=1}^{J}\left(r_j^e - \overline{r}^e\right)^2 \sum_{j=1}^{J}\left(r_j^m - \overline{r}^m\right)^2\right)}, \qquad (E.12)$$

де $\overline{r}^e = J^{-1}\sum_{j=1}^{J} r_j^e$, $\overline{r}^m = J^{-1}\sum_{j=1}^{J} r_j^m$ – відповідні математичні сподівання. При $|\rho| \to 1$ оцінювана математична модель описує емпіричні дані найкраще.

12. Коефіцієнт детермінації [281]

$$R^2 = \left(\sum_{j=1}^{J}\left(r_j^e - \overline{r}^e\right)\left(r_j^m - \overline{r}^m\right)\right)^2 \Bigg/ \left(\sum_{j=1}^{J}\left(r_j^e - \overline{r}^e\right)^2 \sum_{j=1}^{J}\left(r_j^m - \overline{r}^m\right)^2\right), \qquad (E.13)$$

значення якого знаходиться у межах $0 \le R^2 \le 1$. При $R^2 \to 1$ оцінювана математична модель описує емпіричні дані найкраще.

13. F-коефіцієнт [281]

$$F = R^2\left(\left(J-2\right)\left(1-R^2\right)\right)^{-1} = \left(\left(1-R^2\right)^{-1} - 1\right) \Big/ \left(J-2\right). \qquad (E.14)$$

При $F \to \infty$ оцінювана математична модель описує емпіричні дані найкраще.

На практиці [248] найчастіше вживають міри (Е.1), (Е.6), (Е.12). Міру (Е.1) використовують для отримання аналітичних виразів оцінок параметрів математичної моделі, міру (Е.6) – для порівняння відносних похибок різних математичних моделей, а міру (Е.12) – для статистично обґрунтованого, уточненого кількісного визначення ступеню адекватності оцінюваної моделі емпіричним даним із застосуванням критеріїв, похідних від критерію множинної кореляції.

Отже, обравши одну з мір близькості з множини $\left\{\varepsilon, \rho, R^2, F\right\}$ і встановивши порогові значення мір $\left\{D_0^{\varepsilon}, D_0^{\rho}, D_0^{R^2}, D_0^{F}\right\}$, при не перевищенні яких оцінювана модель вважається адекватною емпіричним даним, можна сформулювати правило

розв'язування – оцінювана модель є адекватною емпіричним даним, якщо $\varepsilon \le D_0^{\varepsilon} \vee \rho \ge D_0^{\rho} \vee R^2 \ge D_0^{R^2} \vee F \ge D_0^{F}$.

Якщо відхилення розрахованих і емпіричних значень характеристичних параметрів не перевищують границь відповідних довірчих інтервалів [281], вважається, що відхилення носять стохастичний характер і оцінювану модель можна визнати адекватною. Класично задачу визначення границь довірчих інтервалів розв'язують за допомогою теорії планування експерименту із застосуванням об'єктивно-статистичних критеріїв перевірки гіпотез, зокрема, критерію Стьюдента [281] і критерію, заснованому на коефіцієнті множинної кореляції [281].

Критерій Стьюдента дозволяє встановити значимість T_j – відхилення значень характеристичних параметрів, отриманих на виході оцінюваної моделі, $r_j^m = M^{-1}\sum_{m=1}^{M} r_{j,m}^m$ від емпіричних значень характеристичних параметрів $r_j^e = M^{-1}\sum_{m=1}^{M} r_{j,m}^e$:

$$T_j = \sqrt{M}\left(\overline{r}_j^e - \overline{r}_j^m\right)\Big/\left(\sigma_j^e\right), \qquad \text{(E.15)}$$

де M – кількість фонограм із записами однакового за вмістом і суб'єктом мовленнєвого матеріалу; $\sigma_j^e = \sqrt{(M-1)^{-1}\sum_{m=1}^{M}\left(r_{j,m}^e - \overline{r}_j^e\right)^2}$ – виправлена дисперсія для кожного j-го характеристичного параметра мовленнєвого сигналу; $r_{j,m}^e$ і $r_{j,m}^m$ – значення характеристичного параметра в m-й фонограмі з емпіричних даних і оцінюваної моделі, відповідно. Значення T_j, обчислене за виразом (E.15), порівнюються із табличним значенням $t_j(\alpha, k)$ для j-го характеристичного параметра, де α – рівень значимості або імовірність похибки першого роду (зазвичай α приймають рівним 1% або 5%), а $k = M - 1$ – кількість ступенів свободи. Якщо за результатами порівняння нерівність

$$\left|T_j\right| < t_j(\alpha, k), \qquad (E.16)$$

виконується, то оцінювану модель вважають адекватною емпіричним даним із імовірністю похибки першого роду рівною α. Якщо нерівність (Е.16) не виконується, то оцінювану модель вважають неадекватною емпіричним даним. Недоліком критерію (Е.15) при застосуванні для оцінювання моделей ІГМС є необхідність опрацьовування статистично репрезентативної кількості виголошень M, що супроводжується значними обчислювальними затратами і спричиняє незручності для залучених до експериментів суб'єктів.

Для встановлення факту кореляційного зв'язку між емпіричним r_j^e і розрахованим за оцінюваною моделлю r_j^m значеннями j-го характеристичного параметра використовують критерій, заснований на коефіцієнті множинної кореляції T [281]:

$$\left|T\right| = \left|\rho\sqrt{J-2}\Big/\sqrt{1-\rho^2}\right| \geq t(\alpha, k), \qquad (E.17)$$

де ρ – коефіцієнт множинної кореляції, що розраховується за виразом (Е.12); $t(\alpha, k)$ – критична точка розподілу Стьюдента; J – кількість реалізацій операції порівняння емпіричних і розрахованих значень j-го характеристичного параметра; $k = J - 2$ – кількість ступенів свободи. Якщо нерівність (Е.17) виконується, то можна стверджувати, що із імовірністю $P = 1 - \alpha$ між вживаними для розрахунку (Е.17) емпіричними і розрахованими даними існує тісний кореляційний зв'язок, що є ознакою адекватності оцінюваної моделі.

Узагальнимо наведений матеріал сформулювавши порядок оцінювання адекватності математичної моделі ІГМС. Зокрема, спочатку здійснюється якісний аналіз мовленнєвого сигналу, за результатами якого обираються характеристичні параметри r_j (для моделей (2.1), (2.24), (2.46), (2.64) це коефіцієнти кореляції). Далі розраховуються параметри математичної моделі ІГМС на основі методу найменших квадратів із мінімізацією міри (Е.1).

Верифікацію математичної моделі ІГМС пропонується розпочати перевіркою факту нормальності розподілу значень коефіцієнта кореляції

емпіричних даних, що вживатимуться в критерії (Е.17). В якості емпіричних даних використовуватимемо, наприклад, фонограми із спеціалізованої бази даних Школи інжинірингу та комп'ютерних наук Еріка Джонсона при Університеті Техасу (Даллас, США) NOIZEUS [282], яку використовують, зокрема, для дослідження алгоритмів покращення звуку. Результати здійснюваної на основі критерію Пірсона χ^2 [272, 273] процедури перевірки виду розподілу коефіцієнтів кореляції, екстрагованих із фонограм при $f_d = 8000$ Гц і $J = 200$, дозволяють із імовірністю $P = 1 - \alpha = 100 - 5 \cdot 10^{-4} = 99{,}9995$ % підтвердити нормальність розподілу досліджуваних емпіричних даних, що доводить їх статистичну репрезентативність. Зауважимо, що значення кількості відліків коефіцієнтів кореляції J вибрано так, щоб для всіх аналізованих фонограм всі значення коефіцієнтів кореляції були в межах довірчого інтервалу Бартлета [260, 277] $\pm\sigma_r$, де $\sigma_r = \sqrt{\frac{1}{N}\left(1 + 2\sum_{j=1}^{\lceil 0.25N \rceil}\left(r_j^e\right)^2\right)}$ – стандартна похибка для коефіцієнтів кореляції [281]; N – кількість відліків фонограми мовленнєвого сигналу. У разі, якщо аналізуватиметься мовленнєвий матеріал, дискретизовано із частотою $f_d' \neq f_d$, для визначення допустимого значення J' можна скористатися емпірично виведеним аналітичним виразом

$$J' = \lceil J f_d' / f_d \rceil. \qquad (E.18)$$

Сформулюємо універсальну методику верифікації математичної моделі за значенням критерію, який засновано на коефіцієнті множинної кореляції (Е.17):

1. Вибираємо необхідне значення рівня значимості α.
2. Формуємо набір пар значень кореляційних коефіцієнтів $R^{(em)} = \left(r_1^e, r_1^m; r_2^e, r_2^m; \ldots; r_J^e, r_J^m\right)$, $j = \overline{1, J}$, де r_j^e - значення j-го кореляційного коефіцієнту, обчисленого з емпіричних даних, r_j^m - значення j-го кореляційного коефіцієнту, обчисленого в результаті опису емпіричних даних математичною моделлю, яка верифікується.
3. За виразом (Е.12) обчислюємо коефіцієнт множинної кореляції ρ.

4. За виразом (Е.17) обчислюємо значення критерію T.

5. При кількості ступенів свободи $k = J - 2$ обчислюємо критичну точку розподілу Стьюдента $t(\alpha, k)$;

6. Якщо для попередньо обчислених значень нерівність (Е.17) виконується, то можна стверджувати, що із імовірністю $P = 1 - \alpha$ між обчисленими за емпіричними даними значеннями кореляційного коефіцієнта r_j^e і розрахованими на основі оцінюваної математичної моделі значеннями кореляційного коефіцієнта r_j^m існує тісний кореляційний зв'язок, тобто оцінювана модель є адекватною емпіричним даним.

Міри близькості (Е.1)–(Е.17) зручно вживати для верифікації математичних моделей ІГМС, описаних функціональною залежністю від часу. Саме такий вигляд мають запропоновані в розділі 2 моделі (2.1), (2.24), (2.46), (2.64). Отже, верифікацію цих моделей за описаною вище методикою пропонується супроводжувати обчисленням: абсолютної похибки ε_b (Е.1), розраховуваної за виразом $\varepsilon_b = \sum_{j=1}^{J} \left(b_j^e - b_j^m\right)^2$; нормованої за значенням J абсолютної похибки ε_b^{norm} (Е.3), розраховуваної за виразом $\varepsilon_b^{norm} = \left(\sum_{j=1}^{J} \left(b_j^e - b_j^m\right)^2 \right) \Big/ J$; відносної похибки $\delta\varepsilon_b$ (Е.6), розраховуваної за виразом $\delta\varepsilon_b = 100 \cdot \sum_{j=1}^{J} \left(b_j^e - b_j^m\right)^2 \Big/ \left(\sum_{j=1}^{J} \left(b_j^e\right)^2 \right)$.

Також можна передбачити зростання якісних характеристик оцінюваних моделей із зростанням розрядності квантування вхідного мовленнєвого сигналу, пов'язане із зменшенням дисперсії рівномірно розподіленої похибки квантування, аналітичний вигляд якої описується виразом

$$\sigma_q^2 = 1/12 \cdot \left(\Delta u\right)^2, \qquad \text{(Е.19)}$$

де $\Delta u = u_{\max} / 2^n$ – крок квантування; $u_{\max}$ – найбільше значення аналогового вхідного сигналу на вході аналого-цифрового перетворювача.

Відносну до амплітуди описуваного сигналу похибку квантування можна описати виразом

$$\delta_q = \pm 1{,}5\sigma_q u_{\max}^{-1} \cdot 100\% = \pm 2^{-n}\sqrt{3} \cdot 100\%, \qquad (E.20)$$

де $\pm\sigma_q$ – довірчий інтервал, що відповідає довірчій імовірності $P = 99{,}7\%$. Значення похибки (Е.20) для $n = \{8, 16\}$ біт становлять $\delta_q = \{\pm 6{,}760 \cdot 10^{-1}\%, \pm 2{,}642 \cdot 10^{-1}\%\}$, відповідно, що не має вирішального впливу на достовірність оцінюваних моделей, втім дозволяє незначно, але прогнозовано її підвищити.

Додаток Ж

Імовірнісні моделі процесу автентифікації суб'єкта за мовленнєвим сигналом із шумом

Запропонований у підрозділі 4.1 математичний апарат для компенсування шумів акустичного оточення в мовленнєвому сигналі для АСГ можна розширити в спеціалізовану модель процесу автентифікації, формалізовану в парадигмі моделей СГР [289–293], спрямованих на пошук мультивимірних нормальних розподілів імовірностей, які найкраще кластеризують параметризований вміст еталонної бази фонограм мовленнєвих сигналів із шумом. Така система машинного навчання належатиме до класу імовірнісних моделей [300–307], процедура навчання яких є високоскладною задачею, ефективний розв'язок якої можливий за умови чіткої формалізації процесів параметризації вмісту еталонної бази, факторного аналізу результатів параметризації, кластеризації параметричного простору, синтезу розв'язувального правила, оптимізації процесу навчання системи тощо. Результати розв'язку цих задач взаємопов'язані і комплексно впливають на підсумкову достовірність процесу автентифікації. Отже, формалізуємо імовірнісну модель процесу автентифікації суб'єкта за мовленнєвим сигналом, записаним в умовах шумного акустичного оточення приймачів сигналу.

Представимо мовленнєвий матеріал суб'єкта Ω, описаний вектором характеристичних параметрів x_t, $t=\overline{1,D}$, зваженою сумою M гаусівських щільностей імовірностей:

$$P(x_t|\Omega)=\sum_{i=1}^{M} w_i P_i(x_t), \qquad (Ж.1)$$

де w_i – вага i-ї компоненти моделі суміші із щільністю імовірності $P_i(x_t)$, яка для D-розмірного вектора характеристичних параметрів x_t розраховується за виразом

$$P_i(x_t)=\frac{1}{(2\pi)^{0,5D}\sqrt{|\Sigma_i|}}\exp\left(-0,5(x_t-\mu_i)^T\Sigma_i^{-1}(x_t-\mu_i)\right), \qquad (Ж.2)$$

де μ_i і Σ_i – вектор математичного сподівання і коваріаційна матриця i-ї компоненти моделі суміші, відповідно, а значення ваг є нормованим – $\sum_{i=1}^{M} w_i = 1$. Множина значень ваг, векторів середніх значень і коваріаційних матриць цілком визначає модель суміші (Ж.1) у вигляді множини параметрів

$$\Omega = \{w_i, \mu_i, \Sigma_i\},\ \overline{i = 1, M}, \tag{Ж.3}$$

які виступають керованими змінними в задачі максимізації функції правдоподібності

$$P(X|\Omega) = \prod_{t=1}^{T} P(x_t|\Omega) \tag{Ж.4}$$

моделі суміші, яка описує еталонну навчальну базу векторів характеристичних параметрів $X = \{x_t\},\ t = \overline{1, T}$. Вираз (Ж.4) можна представити у логарифмічній формі на основі виразу (Ж.1):

$$\log(P(X|\Omega)) = \sum_{t=1}^{T} \log\left(\sum_{i=1}^{M} w_i P_i(x_t)\right). \tag{Ж.5}$$

Функції (Ж.4) і (Ж.5) є суттєво нелінійними, що унеможливлює безпосередній розв’язок задачі їх максимізації. Втім, розроблено наближені ітеративні методи розв’язання задачі максимізації таких функцій, найпопулярнішим з яких є ЕМ-метод [288], який передбачає ітеративне кероване оновлення значень параметрів моделі суміші (Ж.3) доти, поки відхилення значень функції правдоподібності (Ж.4) або (Ж.5) не стане меншим або рівним заданому пороговому значенню або ж кількість ітерацій процесу оновлення параметрів (Ж.3) не перевищить заданої максимально допустимої їх кількості. Вихідні значення параметрів (Ж.3) отримуються в результаті узагальнення даних еталонної навчальної бази X методом векторного квантування [248] або ж методом K-середніх [301]. Кожна ітерація розпочинається розрахунком апостеріорних імовірностей $\Pr(i|x_t)$ для всіх $i = \overline{1, M}$ компонентів моделі суміші за виразом

$$\Pr(i|x_t) = w_i P_i(x_t)\left(\sum_{j=1}^{M} w_j P_j(x_t)\right)^{-1}. \qquad (Ж.6)$$

Значення (Ж.6) використовуються для оновлення значень параметрів множини (Ж.3):

$$\overline{w}_i = T^{-1}\sum_{i=1}^{T}\Pr(i|x_t); \qquad (Ж.7)$$

$$\overline{\mu}_i = \sum_{i=1}^{T}\Pr(i|x_t)x_t\left(\sum_{i=1}^{T}\Pr(i|x_t)\right)^{-1}; \qquad (Ж.8)$$

$$\overline{\sigma}_i^2 = \sum_{i=1}^{T}\Pr(i|x_t)|x_t - \overline{\mu}_i|^2\left(\sum_{i=1}^{T}\Pr(i|x_t)\right)^{-1}. \qquad (Ж.9)$$

Якщо елементи векторів характеристичних параметрів $x_t \in X$ некорельовані, то допускається розрахунок лише діагональних значень коваріаційних матриць (Ж.9). Емпірично встановлено, що для отримання значень параметрів (Ж.3), при яких функція правдоподібності (Ж.4) або (Ж.5) потрапляє в окіл свого максимуму, достатньо десяти ітерацій процесу оновлення цих параметрів, здійснюваного за виразами (Ж.7)–(Ж.9).

Нехай синтезовано навчену індивідуальну модель суміші для кожного s-го суб'єкта з множини суб'єктів $\Omega = \{\Omega_s\}$, $s = \overline{1,S}$, мовленнєві матеріали яких були представлені у відповідній узагальненій еталонній навчальній базі. Тоді особа суб'єкта $\hat{s}$, який представив для сеансу автентифікації мовленнєвий сигнал, фонограми якого не було в еталонній базі, ототожнюється з особою одного із суб'єктів з множини Ω в результаті аналізу апостеріорних імовірностей $P(\Omega_S|X)$ за правилом Байєса [248, 301]:

$$\hat{s} = \max_{1\le s\le S} P(\Omega_S|X') = \max_{1\le s\le S}(P(X'))^{-1}P(\Omega_S)P(X'|\Omega_S), \qquad (Ж.10)$$

де $X' = \{x'_t\}$, $t = \overline{1,T}$ – вектори характеристичних параметрів, значення яких екстраговано із фонограми мовленнєвого сигналу, наданої суб'єктом, який автентифікується.

Враховуючи, що у певний момент часу будь-який суб'єкт з множини Ω може ініціювати сеанс автентифікації, а також статистичну незалежність цих процедур, розв'язувальне правило (Ж.10) можна перетворити до вигляду

$$\hat{s} = \max_{1 \le s \le S} \sum_{i=1}^{T} \log P\left(x_t' \middle| \Omega_S\right), \qquad (Ж.11)$$

де імовірності $P\left(x_t' \middle| \Omega_S\right)$ описується виразом (Ж.1). Для збільшення прицезійності сеансу автентифікації допускається порівняння значень апостеріорних імовірностей $P\left(\Omega_S \middle| X'\right)$ із заданим значенням порогу θ. Якщо нерівність $P\left(\Omega_S \middle| X\right) > \theta$ не виконується, то результати сеансу автентифікації не зараховуються.

Застосуємо представлені у підрозділі 4.1 теоретичні результати для синтезу спеціалізованої моделі СГР – універсальної фонової моделі, призначенням якої є оцінювання рівня шумів у вхідному мовленнєвому сигналі. В залежності від результатів оцінювання вплив шумів можна компенсувати або ж винести рішення про неприйнятно високий їх рівень для продовження сеансу автентифікації. Такі можливості є особливо актуальними, враховуючи критичне застосування ІС, що передбачає забезпечення гарантованого рівня надійності процесу автентифікації [43, 49]. Отже, універсальна фонова модель λ описує еталонну базу D-розмірних векторів характеристичних параметрів $y \in Y$, екстрагованих із мовленнєвого матеріалу, записаного в умовах реального акустичного оточення приймачів мовленнєвого сигналу, зваженою сумою M гаусівських розподілів:

$$p\left(y \middle| \lambda\right) = \sum_{i=1}^{M} w_i^{\lambda} p_i(y), \qquad (Ж.12)$$

де w_i^{λ} – ваги компонентів моделі суміші, а $p_i(y)$ – їх щільності імовірностей, описані виразом

$$p_i(y) = \left(\sqrt{\Sigma_i^{\lambda}} (2\pi)^{0.5D}\right)^{-1} \exp\left(-0.5\left(y - \mu_i^{\lambda}\right)^T \left(\Sigma_i^{\lambda}\right)^{-1} \left(y - \mu_i^{\lambda}\right)\right), \qquad (Ж.13)$$

де μ_i^λ і Σ_i^λ – вектор математичного сподівання і коваріаційна матриця i-ї компоненти фонової моделі, значення ваг компонентів якої нормовано $\sum_{i=1}^{M} w_i^\lambda = 1$. Окремо відзначимо, що у ІСКЗ використовується мультиканальна схема [37] отримання вхідної, в тому числі мовленнєвої, інформації, яка аналізується в процесі автентифікації суб'єкта. Для синтезу універсальної фонової моделі мовленнєвий матеріал необхідно позбавити складових, привнесених середовищем каналу передавання інформації. Якщо незалежний вхідний канал передавання мовленнєвої інформації описано відповідною моделлю суміші CH, то вибрати компоненту $c \in CH$, яка найкраще описує вектор характеристичних параметрів X^{CH}, екстрагований із переданого аналізованим каналом вхідного мовленнєвого сигналу, можна розв'язавши задачу оптимізації із цільовою функцією

$$c = \arg \max_{1 \le j \le M} \omega_j^{CH} p_j^{CH}\left(X^{CH}\right), \qquad (Ж.14)$$

де ω_j^{CH} і $p_j^{CH}\left(X^{CH}\right)$ – вага і щільність імовірності j-ї компоненти моделі суміші CH, утвореної множиною з M компонентів. Відобразимо вектор X^{CH}, описаний середнім значенням μ_c^{CH} і діагональною коваріаційною матрицею Σ_c^{CH} c-ї компоненти суміші CH: $X \sim N\left(\mu_c^{CH}, \Sigma_c^{CH}\right)$, у параметричному просторі універсальної фонової моделі λ:

$$Y = \left(X^{CH} - \mu_c^{CH}\right)\Sigma_c^\lambda \left(\Sigma_c^{CH}\right)^{-1} + \mu_c^\lambda, \qquad (Ж.15)$$

де $Y \sim N\left(\mu_c^\lambda, \Sigma_c^\lambda\right)$ – а-канальний узагальнений вектор характеристичних параметрів, який є проекцією вектора X^{CH} на параметричний простір універсальної фонової моделі.

Отже, модель СГР універсальної фонової моделі можна визначити множиною $\lambda = \left\{w_i^\lambda, \mu_i^\lambda, \Sigma_i^\lambda\right\}$, $i = \overline{1, M}$, значення параметрів якої ідентифікуються в результаті узагальнення даних еталонної навчальної бази методом максимізації правдоподібності, описаним виразами (Ж.4)–(Ж.9). Як свідчить саме визначення, безпосереднім призначенням універсальної фонової моделі є опис акустичного

оточення приймачів мовленнєвого сигналу, яке, відповідно, є універсальним для всіх суб'єктів. Втім, навчальна база для синтезу фонової моделі містить мовленнєвий матеріал усіх суб'єктів, що автентифікуватимуться, отже, суміш λ можна адаптувати для опису мовленнєвого матеріалу відповідного суб'єкта застосувавши MAP-метод [289–292]. Нехай мовленнєвий матеріал суб'єкта Ω представлено еталонною базою векторів характеристичних параметрів $X^t = \{x_t\}$, $t = \overline{1,T}$, $X^t << Y$. Кожному вектору x_t в універсальній фоновій моделі λ відповідає набір з M компонентів, які можна виділити в окрему модель суміші i, яка характеризується апостеріорною імовірністю

$$\Pr(i|x_t) = w_i p_i(x_t)\left(\sum_{j=1}^{M} w_j p_j(x_t)\right)^{-1}. \qquad (Ж.16)$$

Використовуючи вираз (Ж.16), формалізуємо аналітичні вирази для обчислення істотних статистик для i-ї моделі суміші з λ за даними навчальної бази X^t:

$$\begin{aligned} n_i &= \sum_{t=1}^{T} \Pr(i|x_t); \\ E_i(x) &= n_i^{-1} \sum_{t=1}^{T} \Pr(i|x_t) x_t; \\ E_i(x^2) &= n_i^{-1} \sum_{t=1}^{T} \Pr(i|x_t) x_t^2. \end{aligned} \qquad (Ж.17)$$

Значення істотних статистик (Ж.17) використаємо для переоцінювання параметрів λ:

$$\begin{aligned} \hat{w}_i &= \gamma\left(\alpha_i n_i T^{-1} + w_i^{\lambda}(1-\alpha_i)\right); \\ \hat{\mu}_i &= \alpha_i E_i(x) + \mu_i^{\lambda}(1-\alpha_i); \\ \hat{\sigma}_i^2 &= \alpha_i E_i(x^2) + \left(\left(\Sigma_i^{\lambda}\right)^2 + \left(\mu_i^{\lambda}\right)^2\right)(1-\alpha_i) - \hat{\mu}_i^2, \end{aligned} \qquad (Ж.18)$$

де $\lambda^{\Omega} = \left\{\hat{w}_i, \hat{\mu}_i, \hat{\sigma}_i^2\right\}_{i=1}^{M}$ – адаптована до суб'єкта Ω фонова модель суміші з вагою $\hat{w}_i$, вектором середніх значень $\hat{\mu}_i$ і коваріаційною матрицею $\hat{\sigma}_i^2$ i-ї компоненти; γ – масштабний параметр, значення якого гарантує, що рівність $\sum_{i=1}^{M} \hat{w}_i = 1$ виконуватиметься, а $\alpha_i = n_i(n_i + r)^{-1}$ – коефіцієнт адаптації, якій описує співвідношення між вихідним і переоціненим значеннями параметрів фонової моделі; r – сталий коефіцієнт ступеня переоцінювання.

Окремо варто звернути увагу на вибір коефіцієнта адаптації α, який використовується у виразах (Ж.18). За своїм фізичним змістом коефіцієнт α характеризує зв'язок між спектрами $S_A(f)$ і $S_B(f)$ для деякої частоти f, тобто $S_B(f) = S_A\left(f^{\alpha}\right)$. Аналітично функцію $S_A\left(f^{\alpha}\right)$ можна описати виразом

$$S_A\left(f^{\alpha}\right) = \begin{cases} \alpha f, if\ 0 \le f \le f_{\min}, \\ \alpha f_{\min} + \Delta f^{-1}(f - f_{\min})(f_{\max} - \alpha f_{\min}), if\ f_{\min} \le f \le f_{\max}, \end{cases} \quad (Ж.19)$$

де $f_{\min}$, $f_{\max}$ – нижня і верхня межі аналізованої частотної смуги спектра, $\Delta f = f_{\max} - f_{\min}$. Процес вибору значення коефіцієнту адаптації α можна представити у формі задачі оптимізації із цільовою функцією

$$\alpha^* = \arg\max p\left(X_S^{\alpha} | \lambda\right), \quad (Ж.20)$$

де λ – базова універсальна фонова модель, X_S^{α} – вектор характеристичних параметрів, екстрагований зі спектра $S_B(f)$ вихідного мовленнєвого сигналу, трансформованого згідно з (Ж.19), при заданому значенні α. Значення коефіцієнта α пропонується змінювати від $\alpha_{\min} = 0{,}80$ до $\alpha_{\max} = 1{,}20$ із кроком $0{,}02$. Оптимальне значення коефіцієнта адаптації α^*, використане в (Ж.18), максимізує швидкість адаптації базової універсальної фонової моделі λ до цільового суб'єкта Ω у формі моделі суміші λ^{Ω}, яку можна використовувати для автентифікації особи цього суб'єкта, замінивши модель суміші Ω_S у функції (Ж.10) або (Ж.11). Розв'язувальне правило для такого процесу автентифікації формалізуємо виразом

$$S(X_e) = \log p\left(X_e \middle| \lambda^{\Omega}\right) - \log p\left(X_e | \lambda\right) \geq \theta, \qquad (Ж.21)$$

де $p\left(X_e | \Lambda\right) = \sum_{k=1}^{K} \log\left(p\left(x_k | \Lambda\right)\right)$; $\Lambda = \left\{\lambda, \lambda^{\Omega}\right\}$; θ – порогове значення; $X_e = \left\{x_j^e\right\}$; $j = \overline{1, K}$ – результат параметризації вихідного мовленнєвого сигналу суб'єкта, який прагне автентифікуватися як Ω. На рис. Ж.1 візуалізовано процес автентифікації суб'єкта Ω за мовленнєвим сигналом, описаним моделлю СГР у вигляді (Ж.1), характеристики якої отримано в результаті адаптації універсальної фонової моделі (Ж.12) для опису мовленнєвого матеріалу цільового суб'єкта. Результат автентифікації утворюється за розв'язувальним правилом (Ж.21).

Результатом процесу адаптації універсальної фонової моделі є розбиття параметричного простору на кластер суб'єкта, який має право доступу до цільової ІСКЗ, і кластер його антагоніста, тобто, кластери «суб'єкт» і «антагоніст», відповідно. Під час сеансу автентифікації із вхідної фонограми мовленнєвого матеріалу екстрагуються значення характеристичних параметрів, які дозволяють розв'язувальному правилу здійснити класифікацію. Застосування адаптованої універсальної фонової моделі зумовлює опис такої системи машинного навчання в парадигмі породжувальних імовірнісних моделей [303, 304], навчання яких є задачею високої складності. Втім, можна перейти від породжувальної до дискримінаційної імовірнісної моделі [303, 304], навчити яку простіше. Враховуючи специфіку задачі АСГ, формалізуємо цей процес переходу застосувавши математичний апарат машин опорних векторів [223, 308–312], у якому за допомогою нелінійної функції-ядра вхідний вектор характеристичних параметрів відображається у мультивимірний параметричний простір, де класи «суб'єкт» і «антагоніст» розділено лінійно.

Коректність процесу навчання машини опорних векторів забезпечується чітким нормуванням вхідних даних, яке можна здійснити двома способами. Перший спосіб передбачає нормування вмісту мовленнєвого матеріалу на етапі його сегментації на фрейми. Далі, вектори характеристичних параметрів, екстраговані із фреймів вихідного мовленнєвого матеріалу, оцінюються

логарифмованими значеннями імовірностей правдоподібності адаптованої моделі суміші, які і використовуються в якості вхідних даних для функції-ядра машини опорних векторів. Другий спосіб передбачає цілісний параметричний опис мовленнєвого матеріалу, як джерела інформації про індивідуальні особливості голосу суб’єкта, акустичне оточення приймача сигналу, умови каналу передавання сигналу тощо, у формі супервекторів [308–312] у форматі: один супервектор – одна фонограма. Формалізуємо обидва цих способи нормування вихідної інформації для машини опорних векторів в контексті задачі автентифікації суб’єкта за фонограмою мовленнєвого сигналу з низьким рівнем відношення «сигнал»/«шум».

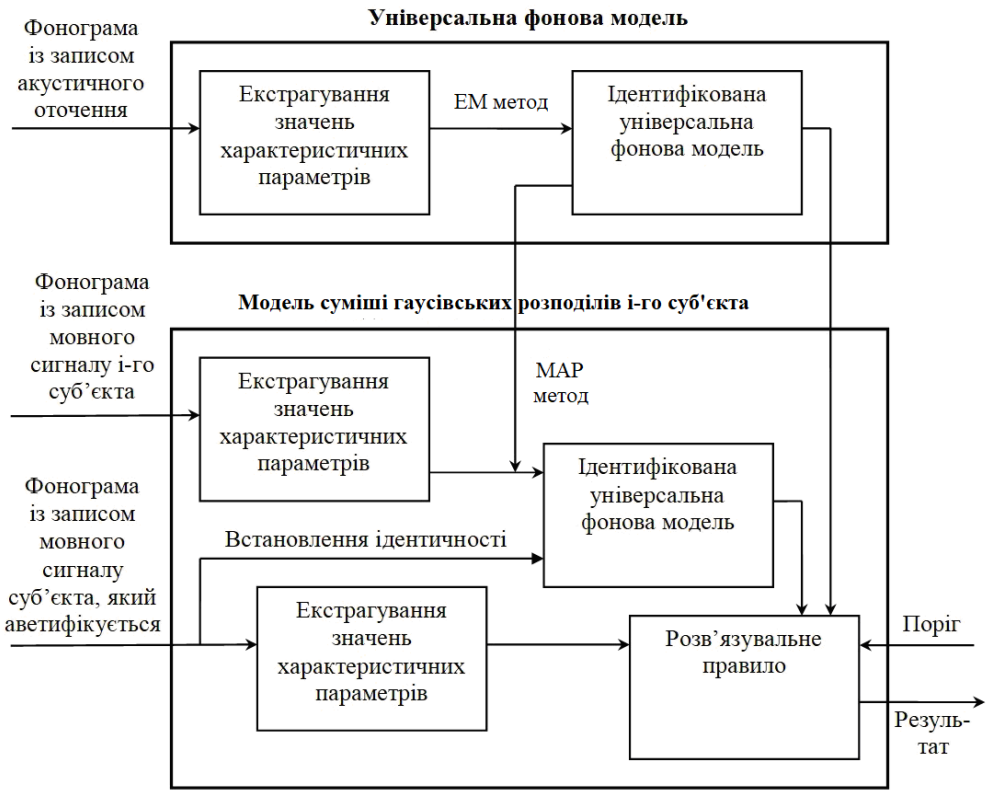


Рисунок Ж.1 – Процес автентифікації суб’єкта за мовленнєвим сигналом моделлю СГР, утвореною адаптацією універсальної фонової моделі

Метою процесу навчання машини опорних векторів є знаходження гіперплощини прийняття рішень, яка найкраще розділяє два класи – «суб’єкт» і

«антагоніст», для еталонної бази мічених опорних векторів, що можна описати виразом

$$y(x) = \sum_{i=1}^{L} \alpha_i t_i K(x_i, x) + d\,, \qquad (Ж.22)$$

де $\alpha_i > 0$ – множники Лагранжа; x_i – опорні вектори; $t_i \in \{-1,1\}$ – мітки векторів еталонної бази; K – функція-ядро; d – зміщення.

Значення бінарного вихідного вектора $y(x)$ утворюється як результат порівняння функціональної залежності значень вхідного вектора x, представленого функцією-ядром у формі опорного вектора x_i, із пороговим значенням. Функція-ядро має відповідати умовам Мерсера [313]:

$$K(x, y) = S(x)^T S(y), \qquad (Ж.23)$$

де $S(x)$ і $S(y)$ – проекції векторів x і y на простір високої розмірності.

Нехай на основі інформації з еталонної бази суб'єкта Ω характеристики універсальної фонової моделі λ адаптовано із утворенням моделі суміші

$$p(x) = \sum_{i=1}^{M} w_i N(x, m_i, \Sigma_i), \qquad (Ж.24)$$

де w_i, m_i, Σ_i – вага, вектор математичного сподівання і коваріаційна матриця i-ї компоненти моделі суміші, $i = \overline{1, M}$. Супервектор для машини опорних векторів утворюється конкатенацією всіх векторів середніх значень у складі моделі СГР (Ж.24), так M векторів середніх значень розмірністю D утворять супервектор розмірністю MD. Таким чином, інформація, якою оперує машина опорних векторів, безпосередньо визначається структурою і вмістом моделі суміші і опосередковано – результатами параметризації відповідного мовленнєвого матеріалу. Процес автентифікації суб'єкта машиною опорних супервекторів візуалізовано на рис. Ж.2.

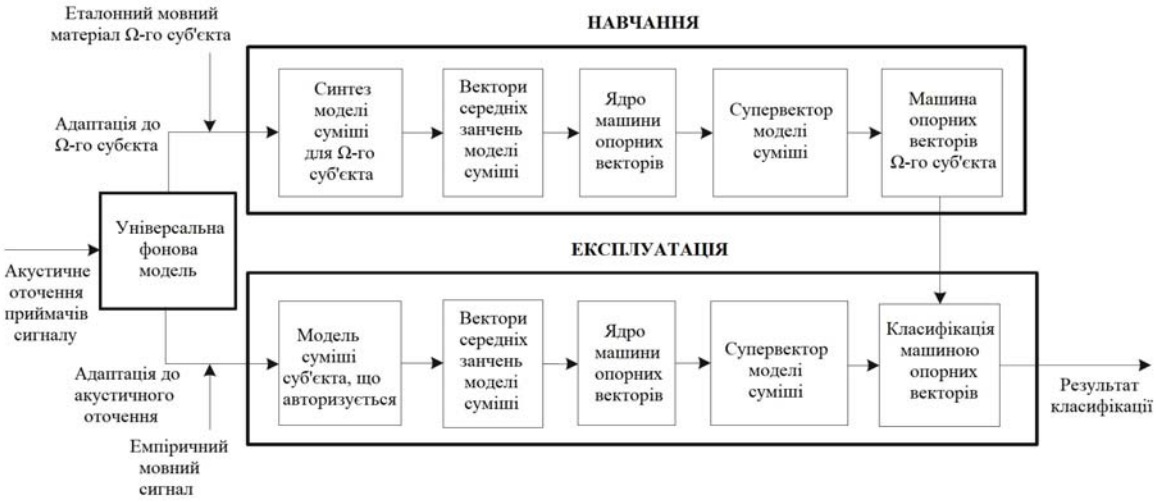


Рисунок Ж.2 – Процес автентифікації
суб’єкта машиною опорних супервекторів

Проаналізувавши вираз (Ж.23) можна стверджувати, що мірою близькості образів фонограм мовленнєвих сигналів a і b, описаних відповідними супервекторами $S(a)$ і $S(b)$, є значення функції-ядра $K(a,b)=S(a)^T S(b)$, яке також можна розглядати як відстань між відповідними точками в параметричному просторі супервекторів. У загальному вигляді відстань між розподілами імовірності p_a і p_b можна оцінити за виразом Кульбака–Лейблера [314]:

$$D_{KL}\left(p_a, p_b\right)=\int_X p_a\left(x\right)\log\left(p_a\left(x\right)\left(p_b\left(x\right)\right)^{-1}\right)dx. \qquad (Ж.25)$$

Функція (Ж.25) у безпосередньому вигляді не задовольняє умови, сформульовані теоремою Мерсера, але на основі виразу (Ж.25) у [248] представлено функцію-ядро у формі лінійної функціональної залежності між двома однотипно адаптованими моделями сумішей p_a і p_b, що описують мовленнєві сигнали a і b, відповідно:

$$K_{KL}=\sum_{i=1}^{M}\left(w_i^{0,5}m_i^a\left(\Sigma_i^\lambda\right)^{-0,5}\right)^T\left(w_i^{0,5}m_i^b\left(\Sigma_i^\lambda\right)^{-0,5}\right), \qquad (Ж.26)$$

де Σ_i^λ – коваріаційна матриця i-ї компоненти базової універсальної фонової моделі λ, m_i^a і m_i^b – вектори середніх значень i-х компонентів моделей сумішей p_a і p_b, відповідно. Враховуючи (Ж.26), вклад кожної i-ї компоненти моделі

суміші для довільного мовленнєвого сигналу c суб'єкта Ω у супервектор S^c можна описати виразом $s_i^c = w_i^{0,5} m_i^c \left(\Sigma_i^\lambda\right)^{-0,5}$, $i = \overline{1, M}$, $S^c = \left(s_1^T, s_2^T, \ldots, s_M^T\right)^T$.

Альтернативою відстані Кульбека–Лейбнера для оцінювання функціональної залежності між розподілами імовірності p_a і p_b є відстань Бхаттачаріа [315]:

$$D_{Bh}\left(p_a, p_b\right) = \int_X \sqrt{p_a\left(x\right) p_b\left(x\right)} dx, \qquad (Ж.27)$$

особливістю якої є врахування всіх характеристик порівнюваних моделей сумішей. Функцію-ядро на основі відстані (Ж.27) можна описати виразом

$$K_{Bh}\left(p_a, p_b\right) = \sum_{i=1}^{M} \left(m_i^b - m_i^a\right)^T \left(m_i^b - m_i^a\right)\left(0,5\left(\Sigma_i^b + \Sigma_i^a\right)\right)^{-0,5}. \qquad (Ж.28)$$

Враховуючи (Ж.28), вклад кожної i-ї компоненти моделі суміші для довільного мовленнєвого сигналу c суб'єкта Ω у супервектор S^c можна описати виразом $s_i^\lambda = \left(m_i^c - m_i^\lambda\right)\left(0,5\left(\Sigma_i^c + \Sigma_i^\lambda\right)\right)^{-0,5}$, $i = \overline{1, M}$, $S^c = \left(s_1^T, s_2^T, \ldots, s_M^T\right)^T$. Відстань (Ж.28) повніше від відстані (Ж.26) описує зв'язок між досліджуваними розподілами імовірності, але потребує суттєво більшої кількості обчислень і еталонних баз більшої розмірності для якісного навчання моделей сумішей.

При ідентифікованій функції-ядрі, формалізуємо процес класифікації машиною опорних векторів особи суб'єкта, який представив для сеансу автентифікації емпіричний мовленнєвий сигнал X^t, параметризований супервектором S^t,

$$G\left(X^t\right) = \sum_{i=1}^{L} \alpha_i t_i K\left(X^i, X^t\right) + d = S^t \left(\sum_{i=1}^{L} \alpha_i t_i S^i\right)^T + d, \qquad (Ж.29)$$

де X^i – послідовність еталонних вхідних векторів, які у формі відповідних супервекторів S^i використовувалися для навчання машини, а K – функція-ядро (Ж.26) або функція-ядро (Ж.28).

Повторивши міркування, втілені у вираз (Ж.27), можна зробити висновок, що методика отримання супервектора конкатенацією всіх векторів середніх

значень у складі відповідної моделі СГР призводить до відображення в його елементах окрім інформації, необхідної для АСГ, інформації про акустичне оточення приймача мовленнєвого сигналу і канал його передавання тощо. Ці дані, враховуючи цільове призначення описуваної моделі, є надлишковими і призводить до зниження ефективності навчання машини опорних векторів та, відповідно, якості класифікації (Ж.29). Сформулюємо процедуру підвищення інформативності супервекторів для задачі АСГ. Нехай еталонну інформацію цільового суб'єкта $\Omega_j \in \Omega = \{\Omega_j\}_{j=1}^{J}$ описано множиною супервекторів $S^{\Omega_j} = \{S_i^{\Omega_j}\}_{i=1}^{M}$. Розрахуємо усереднений по множині супервектор $\overline{S}^{\Omega_j}$, який поелементно віднімемо від кожного супервектора множини $\{S_i^{\Omega_j}\}_{i=1}^{M}$ отримавши в результаті множину $S_-^{\Omega_j}$, значення елементів якої мають меншу варіативність порівняно із множиною S^{Ω_j}. Здійснивши описані вище операції для всіх J суб'єктів, об'єднаємо всі отримані матриці $S_-^{\Omega_j}$, $j = \overline{1,J}$, в єдину матрицю S_-^{Ω} для якої розрахуємо внутрішньокласову коваріаційну матрицю $W = S_-^{\Omega}\left(S_-^{\Omega}\right)^T$ до якої застосуємо спектральне розкладення: $W = V\Lambda V^{-1}$, де V – матриця власних векторів матриці W; Λ – діагональна матриця власних значень матриці W. Сформуємо прямокутну матрицю v з k власних векторів матриці W, яким відповідають найбільші власні значення Λ, та отримаємо на основі матриці v матрицю-проекцію

$$P = I - vv^T, \tag{Ж.30}$$

де I – одинична матриця відповідної розмірності. Використаємо описану виразом (Ж.30) матрицю-проекцію P для синтезу проекційної функції-ядра

$$K_P(x, y) = (PS(x))^T (PS(y)), \tag{Ж.31}$$

де $S(x)$ і $S(y)$ – супервектори, які описують вектори вхідних параметрів x і y, відповідно. Застосування в розв'язувальному правилі (Ж.29) синтезованої в результаті спеціалізованої процедура підвищення інформативності супервекторів

функції-ядра (Ж.31) дозволяє зменшити опосередкований вплив явища перенавчання на якість класифікації, але не нівелює центрального недоліку, властивого машині опорних супервекторів – самої високої з-поміж розглянутих математичних методів ресурсозатратності. Звичайно, зважаючи на критичне застосування ІС із АСГ, цей недолік не є визначним, проте спроба знизити ресурсозатратність машини опорних векторів обумовлює проведення додаткових досліджень. Зокрема, використавши стохастичний варіант методу головних компонентів [247, 248] можна формалізувати процес відображення супервекторів у підпросторі малої розмірності виразом

$$M = m + Tw, \qquad (Ж.32)$$

де M – вектор середніх значень моделі суміші; m – супервектор універсальної фонової моделі, значення якого характеризують виключно акустичне оточення приймача сигналу, а не суб'єкта чи канал передавання мовленнєвої інформації; T – низькорангова прямокутна матриця у стовпцях якої містяться власні вектори коваріаційної матриці загальної мінливості із найбільшими власними значеннями; $w \sim N(0, I)$ – вектор ідентичності або *i*-вектор [249, 316], значення якого генеруються випадково, відповідно до нормального закону розподілу. Можна стверджувати, що значення M описуються нормальним законом розподілу із урахуванням середнього значення m і коваріаційної матриці TT^T – $M \sim N(m, TT^T)$. Опишемо процес утворення матриці T як результату керованого навчання на основі еталонної бази, яка містить S фонограм мовленнєвих сигналів, кожна з яких належить іншому суб'єкту. Сам процес навчання починається розрахунком для мовленнєвого сигналу (s), представленого множиною D-розмірних векторів характеристичних параметрів $\{y_1, y_2, \ldots, y_T\}$, T статистик Баума–Велша [248, 317]. Аналітично процес обчислення істотних статистик нульового, першого і другого порядків описується відповідними виразами

$$N_i(s) = \sum_{t=1}^{T} p(i|y_t, \lambda); \qquad (Ж.33)$$

$$F_i(s) = \sum_{t=1}^{T} p(i|y_t, \lambda)(y_t - m_i);$$

$$S_i(s) = diag\left(\sum_{t=1}^{T} p(i|y_t, \lambda)(y_t - m_i)(y_t - m_i)^T \right),$$

де $p(i|y_t, \lambda)$ – апостеріорна імовірність i-ї, $i = \overline{1, M}$, компоненти суміші універсальної фонової моделі λ, яка генерує y_t; m_i – вектор середніх значень i-ї компоненти. Представимо статистики (Ж.33) у матричній формі:

$$N(s) = \begin{bmatrix} N_1(s)I & & \\ & \ddots & \\ & & N_M(s)I \end{bmatrix};$$

$$F(s) = \begin{bmatrix} F_1(s) \\ \vdots \\ F_M(s) \end{bmatrix};$$

$$S(s) = \begin{bmatrix} S_1(s)I & & \\ & \ddots & \\ & & S_M(s)I \end{bmatrix},$$

де $N(s)$, $S(s)$ – діагональні матриці розмірністю $MD \times MD$; $N(s)$ – супервектор розмірністю $MD \times 1$; I – одинична матриця розмірністю $D \times D$.

Ініціюємо матрицю T необхідної розмірності випадковими значеннями і розрахуємо значення відповідних статистик:

$$N_i = \sum_{s=1}^{S} N_i(s);$$

$$A_i = \sum_{s=1}^{S} N_i(s) l^{-1}(s);$$

$$l = \sum_{s=1}^{S} F(s)\left(l^{-1}(s) T^T \Sigma^{-1} F(s)\right)^T; \qquad (Ж.34)$$

$$N = \sum_{s=1}^{S} N(s),$$

де $l^{-1}(s)=\left(I+T^T\Sigma^{-1}N(s)T\right)^{-1}$, а Σ – блочна діагональна матриця, діагональні блоки якої включають коваріаційні матриці Σ_i, $i=\overline{1,M}$, відповідних компонентів універсальної фонової моделі.

На основі значень статистик (Ж.34) здійснюється переоцінювання значень матриці

$$T=\begin{bmatrix} T_1 \\ \vdots \\ T_M \end{bmatrix}=\begin{bmatrix} A_1^{-1}l_1 \\ \vdots \\ A_M^{-1}l_M \end{bmatrix}, \qquad (Ж.35)$$

де $l=\begin{bmatrix} l_1 \\ \vdots \\ l_M \end{bmatrix}$.

Операції обчислення статистик (Ж.34) і оновлення матриці T згідно із (Ж.35) здійснюються в 20-25 ітерацій. На кожній наступній ітерацій при обчисленні статистик (Ж.34) використовується матриця T, обчислена за виразом (Ж.35) на попередній ітерації. Зауважимо, що при недостатньо великій еталонній навчальній базі коваріаційну матрицю Σ універсальної фонової моделі, вживану в (Ж.34), можна переоцінювати за виразом

$$\Sigma=N^{-1}\left(\left(\sum_{s=1}^{S}S(s)\right)-diag\left(lT^T\right)\right). \qquad (Ж.36)$$

Відповідно, аналітично описана в (Ж.33) статистика $S(s)$ використовується тільки для розрахунку виразу (Ж.36) – якщо переоцінювання матриці Σ не здійснюється, то і обраховувати статистику $S(s)$ немає потреби. Якщо ж обрана для синтезу машини опорних векторів функція-ядро враховує Σ, то переоцінювання значень цієї матриці здійснюється за виразом (Ж.36) після оновлення матриці T згідно з виразом (Ж.35) доти, поки процес навчання матриці T триває.

Після завершення навчання матриці T можна обчислити значення *i*-вектора

$$w=\left(T^T\Sigma^{-1}F(s)\right)\left(I_{MD\times MD}+T^T\Sigma^{-1}N(s)T\right)^{-1}, \qquad (Ж.37)$$

де Σ і $N(s)$ – блочні діагональні матриці розмірністю $MD \times MD$, діагональні блоки яких включають коваріаційні матриці Σ_i всіх $i = \overline{1, M}$ компонентів моделі суміші λ і матриці ідентичності, зважені статистиками нульового порядку $N_i(s) I_{D \times D}$, $i = \overline{1, M}$, відповідно, а $F(s)$ – супервектор, утворений зсунутими відносно середнього значення статистиками першого порядку $F_i(s)$, $i = \overline{1, M}$.

Утворені як (Ж.37), *i*-вектори здатні описати фонограми мовленнєвих сигналів довільної тривалості. Як і супервектори, *i*-вектори можна використати для навчання машини опорних векторів, у складі якої можна використати функцію-ядро, описану одним з виразів (Ж.26), (Ж.28), (Ж.31) тощо. Втім, при оцінюванні відстані між *i*-векторами w_1 і w_2 доцільніше вживати косинусну функцію-ядро [248]

$$K_{\cos} = k(w_1, w_2) = \langle w_1, w_2 \rangle \left(\|w_1\|_F \|w_2\|_F \right)^{-1}, \tag{Ж.38}$$

де $\langle w_1, w_2 \rangle$ – скалярний добуток *i*-векторів w_1 і w_2, а $\|w_1\|_F$ і $\|w_2\|_F$ – їх норми Фребеніуса. Таке рішення обґрунтовано тим, що функція (Ж.38) описує лише косинус кута між *i*-векторами w_1 і w_2 не зважаючи на їх значення, які зазнають впливу шумів, присутніх у відповідних мовленнєвих сигналах.

Додатково оцінити інформацію про акустичне оточення приймачів мовленнєвих сигналів можна ідентифікувавши зв’язок між класами суб’єктів, які узагальнюють вміст їх еталонних баз у параметричному просторі *i*-векторів. Опишемо зв’язки всередині класів окремих суб’єктів W_S і зовнішні зв’язки між класами суб’єктів B_S у парадигмі лінійної алгебри виразом

$$A = B_S v = \lambda W_S v, \tag{Ж.39}$$

де коваріаційні матриці B_S і W_S описуються, відповідно, виразами

$$B_S = \sum_{s=1}^{S} (\mu_s - \mu)(\mu_s - \mu)^T; \tag{Ж.40}$$

$$W_S = \sum_{s=1}^{S} n_s^{-1} \sum_{i=1}^{n_s} (w_i - \mu)(w_i - \mu_s)^T, \tag{Ж.41}$$

де S – підсумкова кількість суб'єктів, чиї класи представлено в параметричному просторі *i*-векторів; n_s – кількість фонограм в еталонній базі суб'єкта s; $\mu_s = n_s^{-1}\sum_{i=1}^{n_s} w_i$ – усереднений *i*-вектор для всіх w_i, $i = \overline{1, n_s}$, *i*-векторів, які описують еталонну базу суб'єкта s; μ – усереднений для всіх S суб'єктів нуль-і-вектор. Кількість стовпців у матриці A можна підбирати емпірично. Ввівши матрицю A у косинусну функцію-ядро (Ж.38) отримаємо модифіковане ядро

$$K_{A\cos} = \left(\left(A^T w_1\right)^T \left(A^T w_2\right)\right)\left(\left\|A^T w_1\right\|\left\|A^T w_2\right\|\right)^{-1}. \qquad (Ж.42)$$

Окремо можна модифікувати косинусну функцію-ядро (Ж.38) для мінімізації похибок першого і другого роду врахувавши кореляційні зв'язки між значеннями *i*-векторів всередині класу відповідного суб'єкта, представлені матрицею (Ж.41),

$$K_{B\cos} = \left(\left(B^T w_1\right)^T \left(B^T w_2\right)\right)\left(\left\|B^T w_1\right\|\left\|B^T w_2\right\|\right)^{-1}, \qquad (Ж.43)$$

де B – отримується як результат розкладення Холецького оберненої матриці W_S:

$$W_S^{-1} = BB^T. \qquad (Ж.44)$$

Формалізуємо процес класифікації машиною опорних векторів із функцією-ядром, описаною одним із виразів (Ж.38), (Ж.42), (Ж.43), особи суб'єкта, який надав для сеансу автентифікації емпіричний мовленнєвий сигнал X^t, представлений і-вектором w^t,

$$G_{\cos} = \left\langle w^t, w^e \right\rangle \left(\left\|w^t\right\|\left\|w^e\right\|\right)^{-1}, \qquad (Ж.45)$$

де w^e – еталонний *i*-вектор для суб'єкта із особою якого прагне себе ототожнити суб'єкт, який автентифікується.

Якщо в розв'язувальному правилі необхідно врахувати ступінь близькості фонограми суб'єкта, який автентифікується, з усіма суб'єктами, еталонні

матеріали яких опрацьовувалися при синтезі індивідуальних машин опорних векторів, то варто модифікувати вираз (Ж.29) так:

$$G_{all} = \sum_{t=1}^{T} \alpha_t K\left(w^e, w^t\right) - \sum_{i=1}^{B} \alpha_i K\left(w^i, w^t\right) + d\,, \qquad (Ж.46)$$

де w^t – i-вектор, який описує фонограму мовленнєвого сигналу, запропоновану суб'єктом, який автентифікується; w^e – еталонний i-вектор відповідного суб'єкта; w^i – еталонний i-вектор відповідного акустичного оточення приймачів сигналу; α_t і α_i – ненульові множники Лагранжа; T і B – кількість i-векторів у відповідному класі; d – константа зсуву, а функція-ядро описується одним із виразів (Ж.38), (Ж.42), (Ж.43), відповідно. Структурну схему, яка описує весь перебіг процесу автентифікації суб'єкта машиною опорних i-векторів із $K_{A\cos} + K_{B\cos}$ нормалізацією за наданим під час сеансу автентифікації мовленнєвим матеріалом, представлено на рис. Ж.3.

Як уже згадувалося, достовірність моделей процесу АСММШ, візуально представлених на рис. Ж.1, Ж.2, Ж.3, визначається, зокрема, і якістю процесу навчання, яку можна підвищити застосувавши до вмісту еталонної навчальної бази таку технологію машинного навчання як бустінг [222–224].

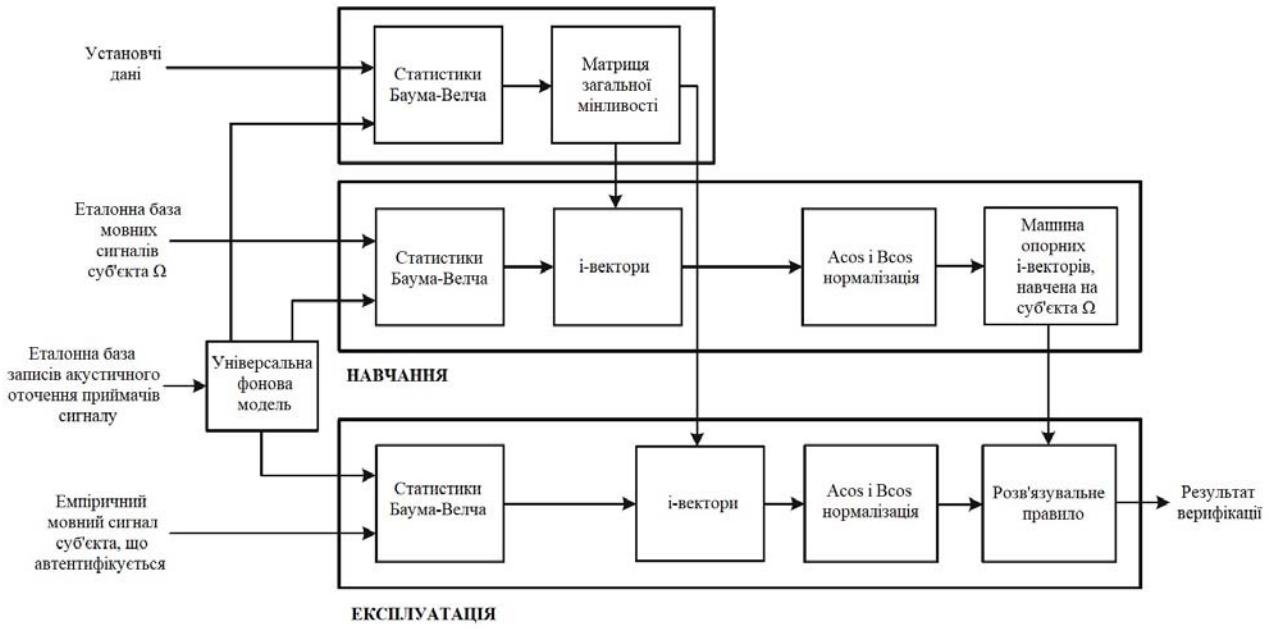


Рисунок Ж.3 – Процес автентифікації суб'єкта машиною опорних i-векторів

Бустінг – це ітеративний процес зважування невірно класифікованих на етапі тестування екземплярів еталонної бази. В контексті АСГ бустінг дозволяє отримати додаткову емпіричну інформацію. Якщо процедуру бустінгу реалізувати як процес контрольованого змішування елементів еталонної бази із фонограмами мовленнєвих сигналів без шуму із елементами еталонної бази фонограм шумів, структурованих за рівнем і типом, то можна чітко визначити область застосування досліджуваних цільових класифікаторів у складі комплексної моделі процесу автентифікації. Формалізуємо задачу ідентифікації складних для автентифікації елементів еталонної бази і задачу класифікації цих елементів за типом і рівнем присутніх у них шумів, розуміючи під елементом еталонної бази $E = \{(x_i, y_i)\}_{i=1}^{N}$ пару вхідних і вихідних значень (x_i, y_i), де x_i – еталонний вектор значень характеристичних параметрів, а $y_i \in \{-1,+1\}$. Всім елементам еталонної бази E присвоїмо початкові значення ваг: $D(i) = N^{-1} \forall i = \overline{1,N}$. Передбачається, що за вмістом еталонної бази E навчатиметься ансамбль класифікаторів $H = \{h_t\}_{t=1}^{T}$, утворений, наприклад, імовірнісними класифікаторами, візуалізованими на рис. Ж.1, Ж.2, Ж.3 тощо.

Формалізуємо задачу ідентифікації складних для автентифікації елементів еталонної бази. Впорядкуємо екземпляри еталонної бази E в порядку спадання їх підсумкових ваг D_i^{Σ}, значення яких узагальнює результати індивідуального навчання всіх T класифікаторів ансамблю H: $D_i^{\Sigma} = \sum_{t=1}^{T} D_t(i), \quad i = \overline{1,N}$. Вважатимемо перші N_{tTr} екземпляри впорядкованої еталонної бази E складними для автентифікації і виділимо їх у підмножину E^{Dif}, де $N_{tTr} = \varepsilon_t \times N$, а ε_t – зважена похибка класифікатора на t-й ітерації бустінгу. Проаналізуємо склад підмножини E^{Dif} виділивши у ній дві підмножини E_{all}^{Dif} і E_{tar}^{Dif}, де в множину E_{all}^{Dif} включимо екземпляри з множини E^{Dif}, які невірно класифікували всі класифікатори, а в множину E_{tar}^{Dif} включимо екземпляри з множини E^{Dif}, які

невірно класифікував класифікатор h_t. Кількість екземплярів у складі множин E_{all}^{Dif} і E_{tar}^{Dif} дорівнює N_{all} і N_{tar}, відповідно, при чому $N_{tTr} = N_{all} + N_{tar}$. Проаналізуємо склад екземплярів множин E_{all}^{Dif} і E_{tar}^{Dif}. Розіб'ємо вхідний вектор у складі кожного екземпляра множини E_{tar}^{Dif} довільним чином на P фрагментів, порядок яких перемішаємо R разів, зберігаючи кожну отриману варіацію в множину E_{tar}^{*}, в яку також перенесемо і вихідну множину E_{tar}^{Dif}. В результаті кількість елементів у множині E_{tar}^{*} дорівнюватиме $N_{tar}PR + N_{tar}$. За аналогією, розіб'ємо кожен екземпляр з множини E_{dif}^{Dif} довільним чином на P фрагментів, порядок яких перемішаємо, зберігаючи отриману варіацію в множину E_{all}^{*}, у яку також перенесемо і вихідну множину E_{all}^{Dif}. В результаті кількість елементів у множині E_{all}^{*} дорівнюватиме $N_{all}P + N_{all}$. Представимо елементи множин E_{tar}^{*} і E_{all}^{*} відповідними *i*-векторами.

Тепер опишемо процедуру ідентифікації ваг α_t для всіх класифікаторів у ансамблі H використовуючи тестувальну множину E_{all}^{*} і цільові тестувальні множини E_{tar}^{*}, відповідно. Повторюватимемо для кожного класифікатора $h_t \in H$ таку послідовність дій: навчаємо класифікатор h_t на еталонній базі E; формуємо для класифікатора h_t тестувальну множину E_{tar}^{*} і дані для тестувальної множини E_{all}^{*} за описаною вище методикою; ініціюємо перерахунок ваг $D_t(i)_{i=1}^{N}$ для тестувальної множини $E_{tar}^{*} + E_{all}^{*}$, $N = N_{tar}PR + N_{tar} + N_{all}P + N_{all}$; якщо умова $\varepsilon_t = \sum_{i=1}^{N} D_i(i) I(h_t(x_i) \neq y_i) < 0{,}5$ не виконується, то класифікатор h_t визнаємо неперспективним і з ансамблю класифікаторів H виключаємо: $t++$; $T--$, інакше – обчислюємо вагу класифікатора h_t: $\alpha_t = 0{,}5\log(1-\varepsilon_t)\varepsilon_t^{-1}$, та змінюємо ваги екземплярів у тестувальній множині $E_{tar}^{*} + E_{all}^{*}$:

$D_{t+1}(i) = Z_t^{-1} D_t(i) \exp(-\alpha_t h_t(x_i) y_i)$, де $Z_t = \sum_{i=1}^{N} D_t(i) \exp(-\alpha_t h_t(x_i) y_i)$. Після опрацювання всіх класифікаторів у ансамблі отримаємо фінальний його варіант із зваженими класифікаторами $H_{fin} = \sum_{t=1}^{T} \alpha_t h_t$. Зауважимо, що хоча описану технологію бустінгу орієнтовано на ансамбль імовірнісних класифікаторів, її також можна застосовувати і для підвищення ефективності навчання будь-яких класифікаторів у складі моделі процесу АСГ.

Проведемо емпіричні дослідження для доведення адекватності отриманих теоретичних результатів з моделювання процесу АСММШ, запропоновані в поточному додатку. Як і в підрозділах 3.2 і 4.1, дослідження проводитимемо із мовленнєвим матеріалом з бази NOIZEUS [282], в якій окрім мовленнєвого матеріалу без шуму, отриманого від різних суб'єктів, є фонограми шумів акустичного оточення типу «Car», «Street», «Airport», «Train station» тощо. Для проведення досліджень мовленнєвий матеріал без шуму відповідного суб'єкта змішуватимемо із фонограмою типізованого шуму, потужність якого підбиратимемо так, щоб рівень відношення «сигнал»/«шум» у підсумковому мовленнєвому матеріалі дорівнював 0, 5, 10 дБ, відповідно. Отже, для кожного цільового суб'єкта утворимо тринадцять множин фонограм: «без шуму», «шум Car, SNR=0 дБ», «шум Car, SNR=5 дБ», «шум Car, SNR=10 дБ», …, «шум Train station, SNR=0 дБ», «шум Train station, SNR=5 дБ», «шум Train station, SNR=10 дБ». Весь отриманий мовленнєвий матеріал сегментовано на фрейми тривалістю 20 мс із перекриттям у 10 мс. Для кожного суб'єкта сформовано індивідуальну еталонну і емпіричну бази, наповнені відповідним мовленнєвим матеріалом тривалістю 120 с і 12 с тощо.

Адекватність моделі процесу АСММШ визначається, зокрема, обраним методом параметризації мовленнєвого матеріалу. Кожен фрейм мовленнєвого матеріалу опишемо чотирма наборами векторів характеристичних параметрів на базі:

- Мел-частотних кепстральних коефіцієнтів (MFCC) (перший набір);

- перцептивних коефіцієнтів лінійного передбачення (PNC) [248] (другий набір);
- нормованих за потужністю кепстральних коефіцієнтів (PNCC) [248] (третій набір);
- значень енергії сигналу на частоті основного тону і її гармоніках, описаних уточненою детермінованою моделлю (2.24), визнаною найпрецизійнішою з поміж множини моделей (2.1), (2.24), (2.46), (2.64) за результатами досліджень, наведених у підрозділі 3.2 (четвертий набір).

Розрахунок значень характеристичних параметрів у складі першого і другого наборів базується на спектральному представленні пропущеної банком трикутних смугових фільтрів послідовності фреймів аналізованого мовленнєвого сигналу:

$$MF[m,l]=\sum_{k=0}^{0,5K-1}\left|x\left[m,e^{j\omega_k}\right]h_l\left[e^{j\omega_k}\right]\right|^2, \qquad (Ж.47)$$

де $x[\ldots]$ – короткочасний спектр аналізованого мовленнєвого сигналу; $h_l[\ldots]$ – віконна функція згладжування; k – номер частотної вибірки; $\omega_k = 2\pi k/f_d$ – циклічна частота; f_d – частота дискретизації; m, l – номери фрейма та частотної смуги в банку фільтрів тощо. Представлення (Ж.47) є основою для екстрагування із m-го фрейма мовленнєвим сигналу множини Мел-кепстральних коефіцієнтів і перцептивних коефіцієнтів лінійного передбачення, де перші розраховуються за виразом

$$MFCC[n]=L^{-1}\sum_{l=1}^{L}\log\left(MF[m,l]\cos\left[2\pi L^{-1}(l+0,5)n\right]\right), \qquad (Ж.48)$$

а другі, на основі коефіцієнтів лінійного передбачення $b(i)$ – за рекурсійним виразом

$$PLP[n]=-b(n)+n^{-1}\sum_{i=1}^{n-1}(n-i)b(i)PLP[n-i], \qquad (Ж.49)$$

де n – номер коефіцієнта лінійного передбачення; L – кількість фільтрів у банку. Описані процеси візуалізовано в лівій гілці процесу параметризації мовленнєвого сигналу, представленого на рис. Ж.4.

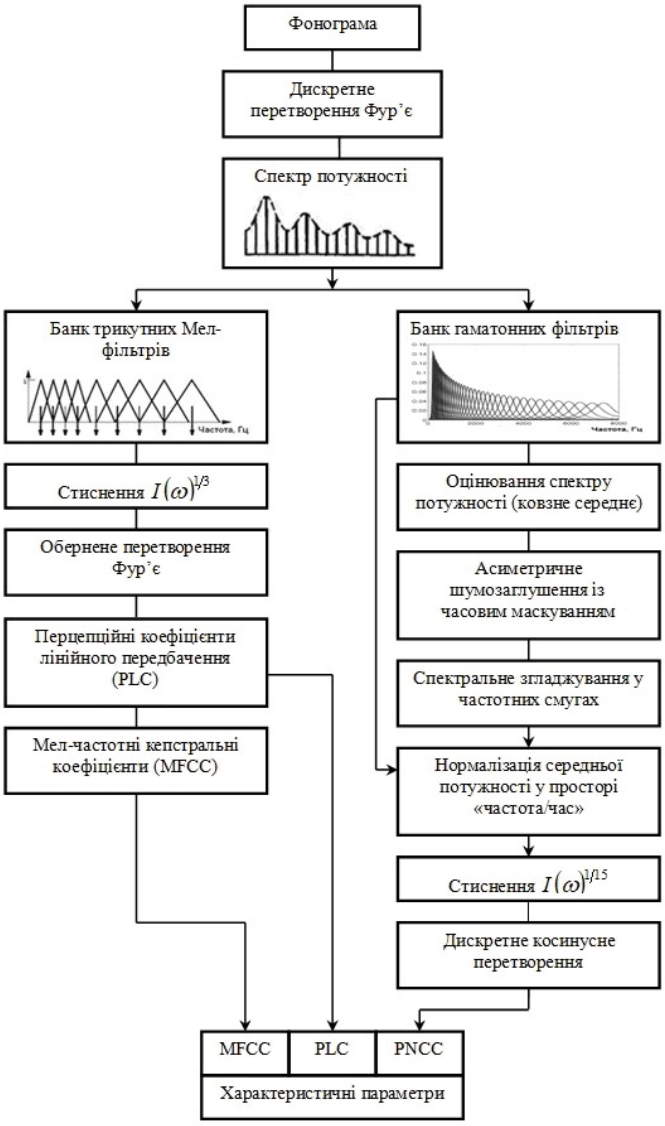


Рисунок Ж.4 – Параметризація мовленнєвого сигналу у форматі 1–3 наборів характеристичних параметрів

До переваг першого і другого наборів характеристичних параметрів можна віднести стійкість до лінійних спектральних спотворень і акцентування уваги на інформативнішій для АСГ (низькочастотній) частині спектра, що підтверджується моделями слухового сприйняття людини [208, 209]. Недолік такої параметризації мовленнєвих сигналів полягає в усередненні спектральних характеристик на виході банку фільтрів.

Третій набір характеристичних параметрів є множиною нормалізованих за потужністю кепстральних коефіцієнтів, фізичний зміст яких описано моделлю реакції слухового нерва людини при сприйнятті мовленнєвих сигналів у шумному

акустичному оточенні [45]. В значення цих коефіцієнтів закладено механізм компенсації шуму, заснований на оцінюванні усередненої протягом кількох послідовних фреймів короткочасної потужності спектра, утвореного на виході банку гаматонних фільтрів [248]. Таким чином, істотна частина спектра мовленнєвого сигналу утворюється як результат динамічного процесу віднімання оцінки порогового рівня шуму від короткочасної оцінки потужності спектра:

$$Q_{out}[m,l]=\begin{cases}\lambda_a Q_{out}[m-1,l]+(1-\lambda_a)Q_{in}[m,l], if\ Q_{in}[m,l]\geq Q_{out}[m-1,l],\\ \lambda_b Q_{out}[m-1,l]+(1-\lambda_b)Q_{in}[m-1,l], if\ Q_{in}[m,l]<Q_{out}[m-1,l],\end{cases} \quad (Ж.50)$$

де $Q_{in}[m,l]$ – результат ковзного усереднення $MF[m,l]$ на інтервалі з M послідовних фреймів; $Q_{out}[m,l]$ – усереднена за часом спектральна потужність при коефіцієнтах забування $1>\lambda_a>\lambda_b>0$. Після визначення істотної частини спектра за виразом (Ж.50) проводиться компенсування впливу каналу передавання мовленнєвого сигналу на основі інформації про енергію сегментів фреймів, що відповідають паузам у мовленнєвому сигналі. Ідентифікація пауз здійснюється детектором мовленнєвої активності, де істотна частина мовленнєвого сигналу випрямляється ідеальним лінійним напівперіодним випрямлячем, після чого паралельно аналізується в двох каналах – у першому каналі, з метою оцінювання порогового рівня потужності тільки сегментів-«пауз», до випрямленого сигналу повторно застосовується операція віднімання (Ж.50), а в другому каналі здійснюється часове маскування випрямленого сигналу:

$$Q_{tm}[m,l]=\begin{cases}Q_0[m,l], if\ Q_0[m,l]\geq \lambda_t Q_P[m-1,l],\\ \mu_t Q_P[m-1,l], if\ Q_0[m,l]<\lambda_t Q_P[m-1,l],\end{cases} \quad (Ж.51)$$

де $Q_0[m,l]$ – сигнал після напівперіодного випрямлення; λ_t – коефіцієнт забування, а $Q_P[m,l]=\max(\lambda_t Q_P[m-1,l], Q_0[m,l])$ для кожної смуги l і фрейма m. Дані обох каналів узагальнюються пороговим енергетичним детектором, на виході якого отримується значення вектора нормованих за потужністю кепстральних коефіцієнтів:

$$PNCC_n[m,l]=\begin{cases}\max(Q_{tm}[m,l], Q_f[m,l]), for\ "signal",\\ Q_f[m,l], for\ "pause",\end{cases} \quad (Ж.52)$$

де n – кількість отримуваних коефіцієнтів; $Q_{tm}[m,l]$ – сигнал після процедури часового маскування; $Q_f[m,l]$ – значення обвідної після напівперіодного випрямлення. Описані процеси візуалізовано в правій гілці процесу параметризації мовленнєвого сигналу, представленого на рис. Ж.4.

Як вказано на рис. Ж.4, при розрахунку третього набору характеристичних параметрів застосовується банк смугових гаматонних фільтрів, центральні частоти яких розподілено в цільовому частотному діапазоні за ERB-шкалою [209–211]: конвертування даного у Гц-шкалі значення частоти f в значення в ERB-шкалі відбувається за виразом $ERB(f) = 21{,}41\log_{10}(1 + f/229)$. Таке представлення спектра відповідає положенням психоакустики [209–211] і адекватно відтворює такі властиві слуховій системі людини явища як псевдологарифмічне зростання ширини критичної смуги із зростанням частоти, розподіл інтервалів сприйняття частот за логарифмічним законом, нечутливість до биття і інтермодуляцій між сигналом і фоновим шумом тощо. На рис. Ж.5 можна візуально оцінити відмінність спектрограм, де мовленнєвий сигнал із різним рівнем відношення «сигнал»/«шум» описано Мел-частотними кепстральними коефіцієнтами і нормованими за потужністю кепстральними коефіцієнтами.

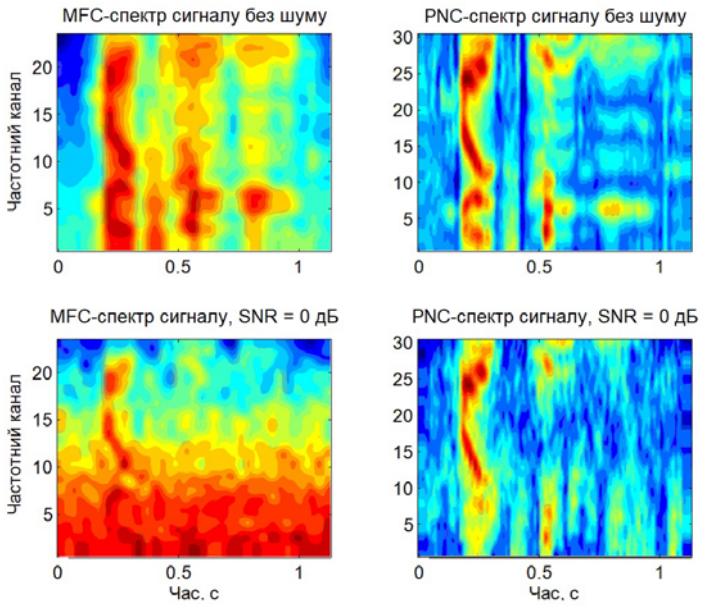


Рисунок Ж.5 – Візуалізація спектрів мовленнєвого сигналу без/з шумом, описаних першим і третім наборами характеристичних параметрів

Отже, кожен фрейм вхідного мовленнєвого сигналу описувався:

- в першому наборі характеристичних параметрів – 39-розмірним вектором, який включав 13 Мел-частотних кепстральних коефіцієнтів $C = \{c_1, c_2, \ldots, c_{13}\}$, 13 дельта $\Delta = \{\Delta_1, \Delta_2, \ldots, \Delta_{13}\}$ і 13 прискорених коефіцієнтів $\Delta^2 = \{\Delta_1^2, \Delta_2^2, \ldots, \Delta_{13}^2\}$ тощо;

- в другому наборі характеристичних параметрів – 14-розмірним вектором, який включав 14 перцептивних коефіцієнтів лінійного передбачення $L = \{l_1, l_2, \ldots, l_{14}\}$;

- в третьому наборі характеристичних параметрів – 39-розмірним вектором, який включав 13 нормованих за потужністю кепстральних коефіцієнтів $P = \{p_1, p_2, \ldots, p_{13}\}$, 13 дельта $\Delta = \{\Delta_1, \Delta_2, \ldots, \Delta_{13}\}$ і 13 прискорених коефіцієнтів $\Delta^2 = \{\Delta_1^2, \Delta_2^2, \ldots, \Delta_{13}^2\}$ тощо;

- в четвертому наборі характеристичних параметрів – 7-розмірним вектором, який включав 7 значень енергії сигналу на частоті основного тону і шести її гармоніках $U = \{u_0, u_1, \ldots, u_6\}$.

Досліджувані моделі АСММШ відносяться до класу біометричних моделей інформаційної безпеки, тому оцінювання їх достовірності необхідно здійснювати відповідно до міжнародного стандарту ISO/IEC 19795-1:2006 «Information technology – Biometric performance testing and reporting – Part 1: Principles and framework», який у 2016 р. було переатестовано. Відповідно до цього стандарту, кількісними характеристиками для оцінювання адекватності біометричної інформаційної моделі є:

- імовірність хибного недопуску (False Rejection Rate, FRR, α) – класифікація «суб'єкта» як «антагоніста» із визнанням сеансу автентифікації для доступу до середовища ІСКЗ проваленим;

- імовірність хибного допуску (False Acceptance Rate, FAR, β) – класифікація «антагоніста» як «суб'єкта» із наданням несанкціонованому суб'єкту відповідного рівня допуску до середовища ІСКЗ;

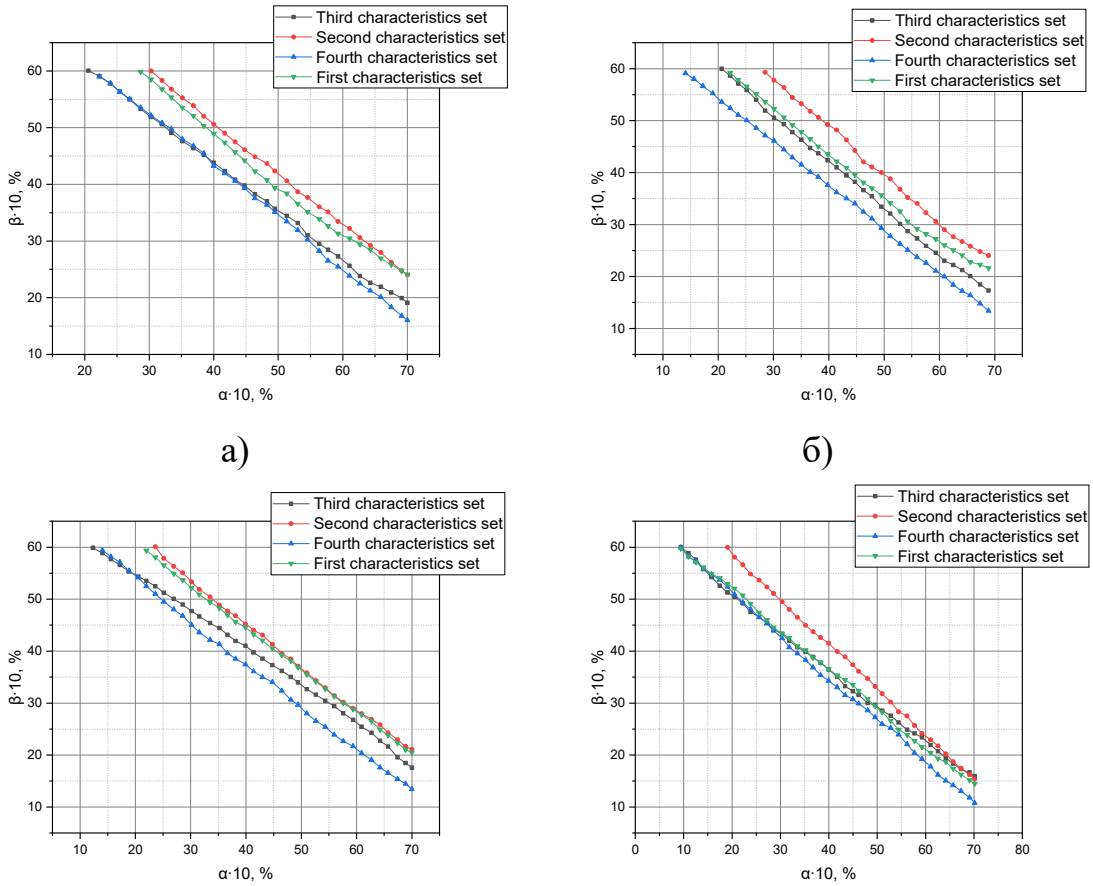
- EER-коефіцієнт – точка рівності похибок α і β (Equal Error Rate, EER);

- DET-крива – побудована у системі координат FRR (вісь абсцис) – FAR (вісь ординат), крива компромісного визначення похибки (Detection Error Trade-off curve, DET-curve).

При розрахунку цих характеристик враховуються лише результати і кількість завершених сеансів автентифікації, а сеанси автентифікації, які розв'язувальне правило, відповідно до встановленого адміністратором значення порогу чутливості θ, визнало некоректними, не враховуються. Цілісно достовірність оцінюваної моделі характеризують EER-коефіцієнт і DET-крива, причому, чим значення цих характеристик менші, тим оцінювана модель системи надійніша.

Отже, сформуємо чотири 1024-компонентні універсальні фонові моделі, навчені протягом 200 ітерацій EM-методом на всьому еталонному мовленнєвому матеріалі, утвореному на основі комбінування типізованих шумів різного рівня із фонограмами без шуму з бази NOIZEUS, всі фрейми якого параметризовано одним із чотирьох наборів характеристичних параметрів. Далі навчені універсальні фонові моделі адаптувалися до цільових суб'єктів MAP-методом для утворення індивідуальних восьми компонентних моделей СГР. Відповідно до обраного набору характеристичних параметрів, для кожного цільового суб'єкта створено по чотири адаптованих моделі суміші. Проведемо дослідження із моделлю процесу автентифікації, представленої на рис. Ж.1, для вибору оптимального набору характеристичних параметрів, використавши мовленнєвий матеріал із SNR=0 дБ для кожного з чотирьох типів шумів. Результат дослідження представимо відповідними DET-кривими на рис. Ж.6, де рис. Ж.6а описує достовірність оцінюваної моделі в умовах впливу шуму типу «Car», рис. Ж.6б описує достовірність оцінюваної моделі в умовах впливу шуму типу «Street», рис. Ж.6в описує достовірність оцінюваної моделі в умовах впливу шуму типу «Airport», рис. Ж.6г описує достовірність оцінюваної моделі в умовах впливу шуму типу «Train station». Відповідність між символьним номером у межах нумерованого рисунку і типом шуму виду: а) –

шуму типу «Car»; б) – шуму типу «Street»; в) – шуму типу «Airport»; г) – шуму типу «Train station», зберігатиметься і для наступних рисунків.



а) б) в) г)

Рисунок Ж.6 – Залежність достовірності породжувальної імовірнісної моделі процесу автентифікації від набору характеристичних параметрів і типу шуму в мовленнєвому матеріалі

Як видно з рис. Ж.6, вибір набору характеристичних параметрів дозволяє змінювати підсумкові імовірності похибок першого і другого роду в діапазоні ±1% для обох типів похибок, що є досить помітним результатом. Набори характеристичних параметрів розташувалися в такому порядку за зростанням інформативності для розв’язання задачі АСММШ: другий, перший, третій, четвертий. Це можна пояснити, зокрема, інтегрованими технологіями компенсування шумів у методах параметризації, які дозволили розрахувати значення третього і четвертого наборів характеристичних параметрів. Перевагою

першого і другого набору є їх універсальність і менша ресурсозатратність. У порядку зростання впливу на достовірність моделі процесу автентифікації типи шумів розташувалися так: «Train station», «Airport», «Street», «Car». Втім, для інших моделей ця залежність може змінитися. Представлені на рис. Ж.6 результати, продемонстровані із використанням першого набору характеристичних параметрів, потребують додаткового аналізу, адже цей набір складається з Мел-частотних кепстральних коефіцієнтів та перших і других їх похідних, які, де-факто, є найпопулярнішими у сфері аналізу мовленнєвих сигналів. Застосуємо доробки з підрозділу 4.1 для підвищення інформативності першого набору характеристичних параметрів. Проведемо дослідження достовірності породжувальної імовірнісної моделі процесу автентифікації суб’єкта за всім емпіричним мовленнєвим матеріалом, тобто для всіх типів і рівнів шумів, безпосередньо, та з їх компенсуванням. Отримані результати наведено на рис. Ж.7.

Наведені на рис. Ж.7 результати підтверджують доцільність та дієвість запропонованого в підрозділі 4.1 математичного апарату для компенсації шумів у мовленнєвому сигналі, який використовується для автентифікації суб’єкта. Компенсування спричиняє помітний вплив на достовірність автентифікації при рівні відношення «сигнал»/«шум» 5 і 10 дБ. Також помітно, що вдається успішно компенсувати всі чотири типи шумів, а найефективніше – шум типу «Car», який найбільше впливав на достовірність моделі автентифікації в дослідженні, представленому на рис. Ж.6.

Продемонстровані на рис. Ж.6, Ж.7 результати отримано із використанням адаптованої для автентифікації цільового суб’єкта універсальної фонової моделі із розв’язувальним правилом, формалізованим виразом (Ж.21). Адекватність такої моделі визначається репрезентативністю еталонної бази, а процес навчання є вкрай ресурсозатратним. Альтернативу цій породжувальній імовірнісній моделі складає комплекс дискримінаційних імовірнісних моделей, утворених у парадигмі машини опорних векторів. Порівняємо їх, представивши результати на рис. Ж.8.

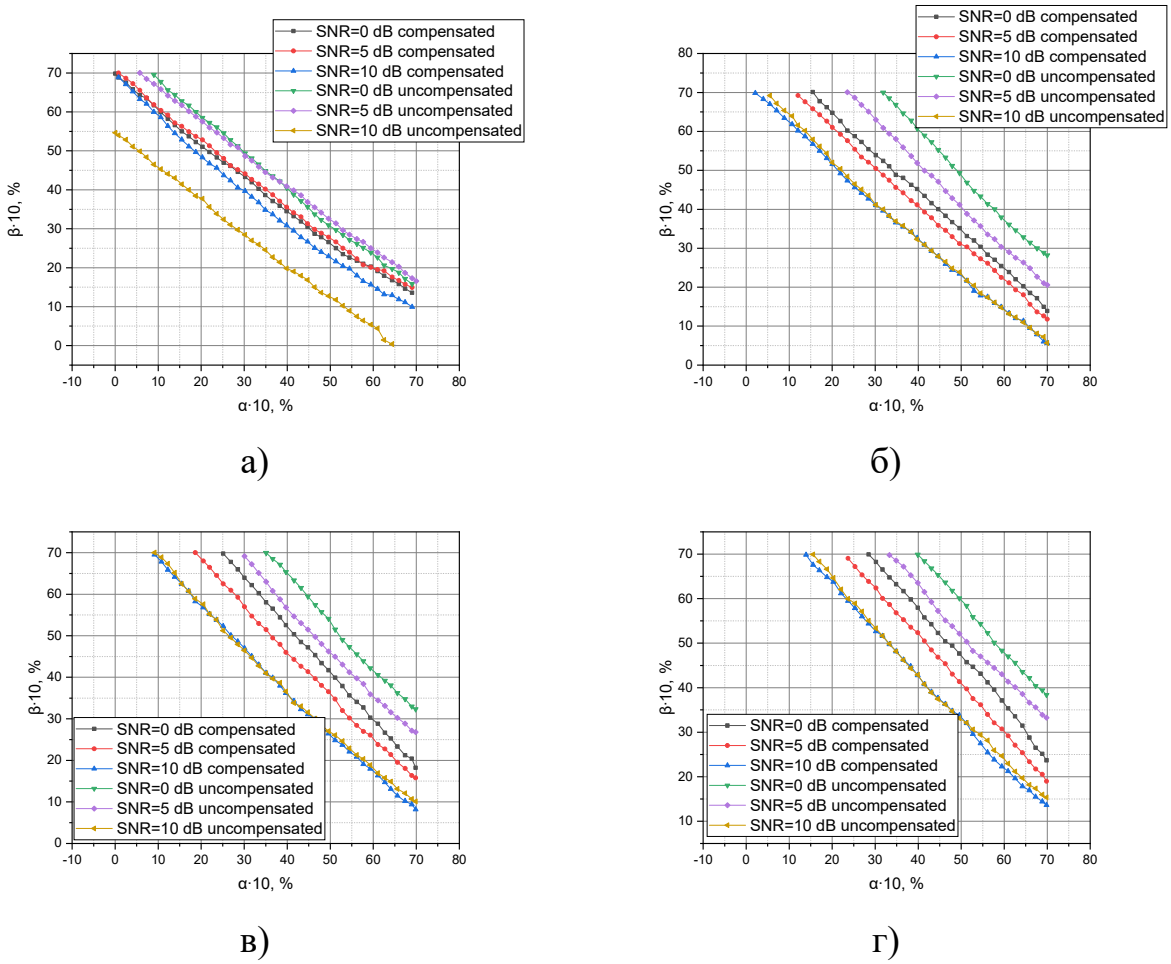


Рисунок Ж.7 – Дослідження впливу, запропонованого у підрозділі 4.1 методу компенсації шумів, на достовірність породжувальної імовірнісної моделі процесу автентифікації суб’єкта за мовленнєвим матеріалом, описаним першим набором характеристичних параметрів

На рис. Ж.8 наведено результати оцінювання достовірності автентифікації суб’єкта за мовленнєвим матеріалом із різним рівнем відношення «сигнал»/«шум» породжувальною імовірнісною моделлю (UBM+GMM) і найпростішими дискримінаційними імовірнісними моделями: SsVM+Kkl – із функцією-ядром K_{KL}, описаною виразом (Ж.26), та SsVM+Kbh – із функцією-ядром K_{Bh}, описаною виразом (Ж.28). Представлені емпіричні результати доводять, що для вживаної еталонної бази модель автентифікації суб’єкта машиною опорних векторів перевершує породжувальну модель автентифікації суб’єкта для всіх типів шуму і рівнів відношення «сигнал»/«шум», демонструючи імовірність похибки першого роду меншу на 1 %, а імовірність похибки другого роду – на

майже 3 %. За аналогією з аналізом рис. Ж.6, викликає інтерес детальніше дослідженні впливу типу шуму та рівня відношення «сигнал»/«шум» у мовленнєвому матеріалі на достовірність відповідних дискримінаційних імовірнісних моделей автентифікації суб’єкта. У зручній для сприйняття формі ці результати наведено на рис. Ж.9.

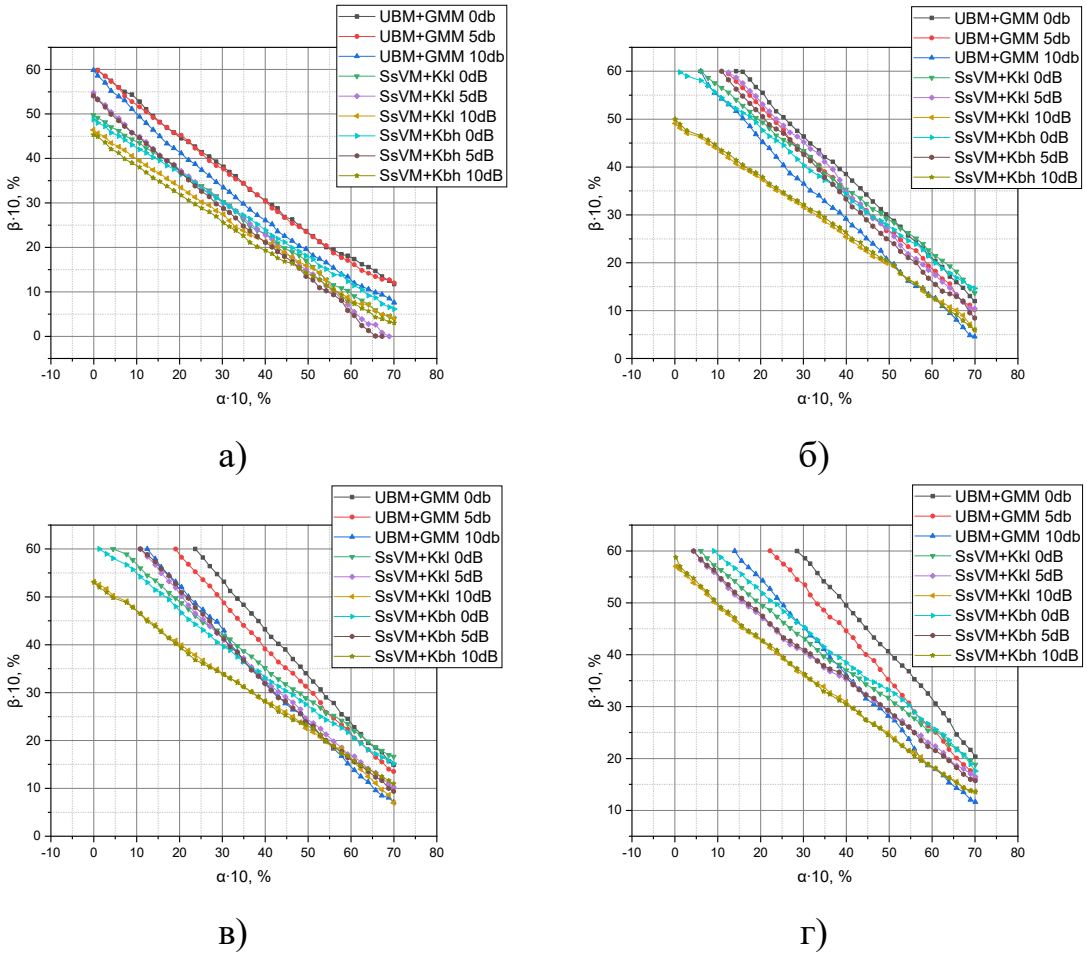
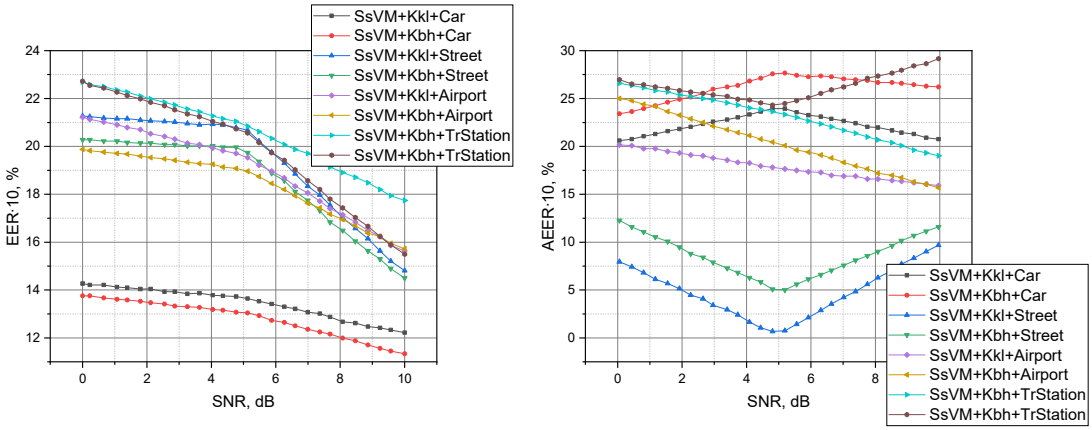


Рисунок Ж.8 – Оцінювання достовірності породжувальної і найпростіших дискримінаційних імовірнісних моделей автентифікації суб’єкта за мовленнєвим матеріалом із SNR=0, 5, 10 дБ

Як видно з рис. Ж.9, найпростіші дискримінаційні імовірнісні моделі найкраще функціонують саме в умовах впливу шуму типу «Car», тоді як у породжувальної імовірнісної моделі (Ж.21) саме із цим типом шуму виникли найбільші ускладнення. Решта типів шумів спричинили суттєвий вплив на достовірність оцінених дискримінаційних імовірнісних моделей, що обумовлює доцільність подальших досліджень.



а) б)

Рисунок Ж.9 – Оцінювання достовірності процесів автентифікації суб’єкта найпростішими дискримінаційними імовірнісними моделями

Порівняємо результати автентифікації суб’єктів за мовленнєвим сигналом із шумом машинами опорних супер- та *i*-векторів, формалізованих виразами (Ж.29) і (Ж.45), відповідно, представивши результати експерименту на рис. Ж.10. Всі дослідження проводилися із емпіричним мовленнєвим матеріалом із рівнем відношення «сигнал»/«шум» у 0 дБ. Досліджувалися машини опорних супервекторів: – із функцією-ядром K_{KL}, описаною виразом (Ж.26) – SsVM+Kkl; із функцією-ядром K_{Bh}, описаною виразом (Ж.28) – SsVM+Kbh; із функцією-ядром K_{KL} і нормалізацією супервектора матрицею-проекцією (Ж.30) – SsVM+Kkl+P-norm; із функцією-ядром K_{Bh} і нормалізацією супервектора матрицею-проекцією (Ж.30) – SsVM+Kbh+P-norm. Також досліджувалися машини опорних *i*-векторів: із функцією-ядром $K_{A\cos}$, описаною виразом (Ж.42) і розв’язувальним правилом $G_{\cos}$, описаним виразом (Ж.45) – SiVM+Kacos+Gcos; із функцією-ядром $K_{B\cos}$, описаною виразом (Ж.43) і розв’язувальним правилом $G_{\cos}$ – SiVM+Kbcos+Gcos; із функцією-ядром $K_{A\cos}$ і розв’язувальним правилом G_{all}, описаним виразом (Ж.46) – SiVM+Kacos+Gall; із функцією-ядром $K_{B\cos}$ і розв’язувальним правилом G_{all} – SiVM+Kbcos+Gall.

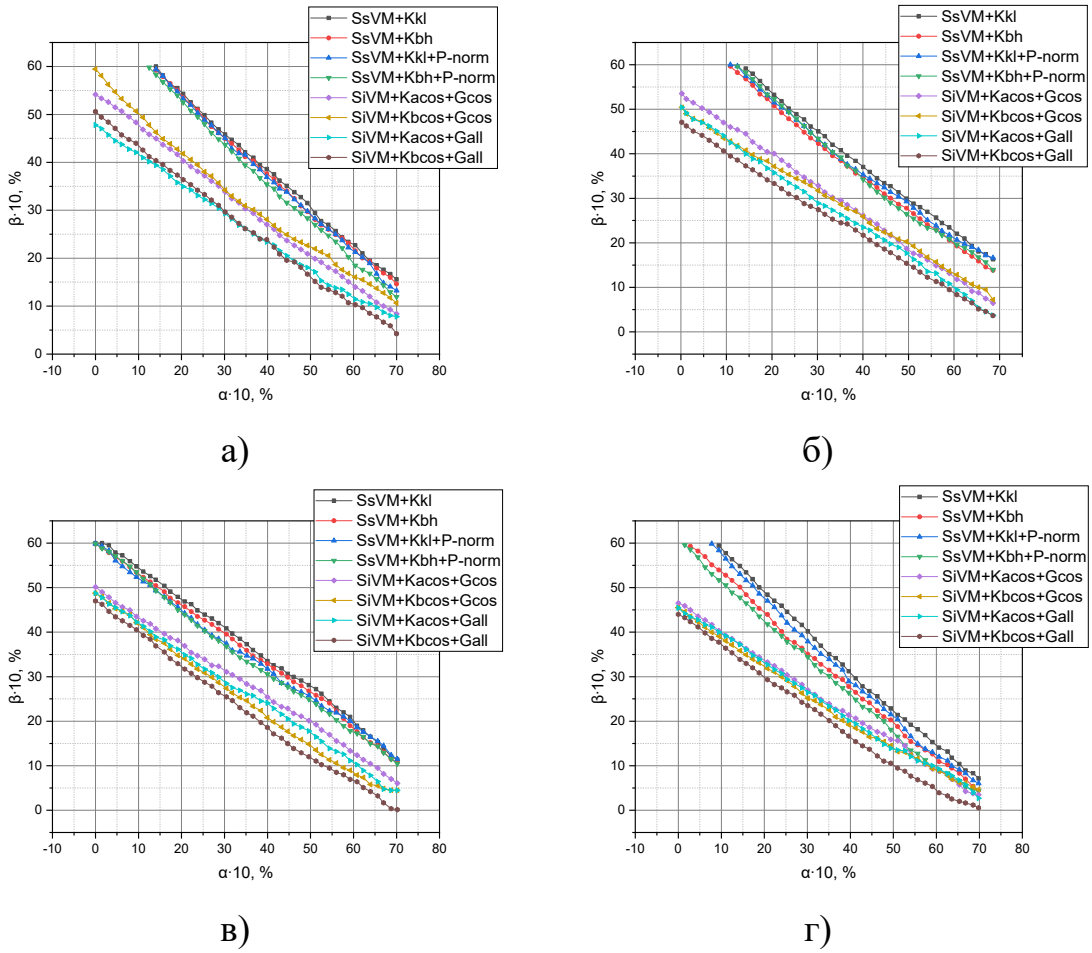
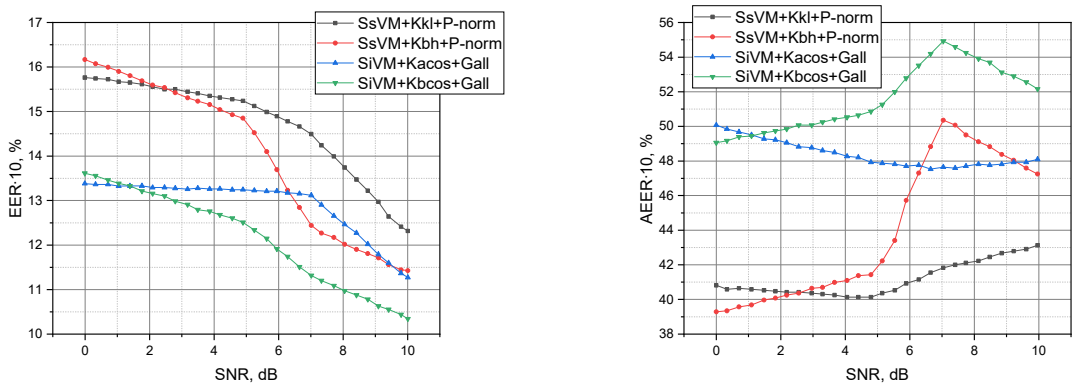


Рисунок Ж.10 – Порівняння достовірності автентифікації суб’єкта машинами опорних супер-та *i*-векторів за мовленнєвим сигналом із SNR=0 дБ

Результати, представлені на рис. Ж.10, дозволяють стверджувати, що опис характеристичних параметрів мовленнєвого матеріалу *i*-векторами виявився кращим при АСММШ. Взагалі, роздільність отриманих результатів дозволяє однозначно визнати модель SiVM+Kbcos+Gall кращою. Проте, для підтвердження отриманих результатів порівняємо моделі SsVM+Kkl+P-norm, SsVM+Kbh+P-norm, SiVM+Kacos+Gall і SiVM+Kbcos+Gall за значенням коефіцієнта EER (рис. Ж.11а) і його відносної інтерпретації AEER (див. рис. Ж.11б) при автентифікації суб’єкта за мовленнєвим матеріалом, рівень відношення «сигнал»/«шум» в якому ітеративно змінювався в діапазоні $0 \div 10$ дБ.



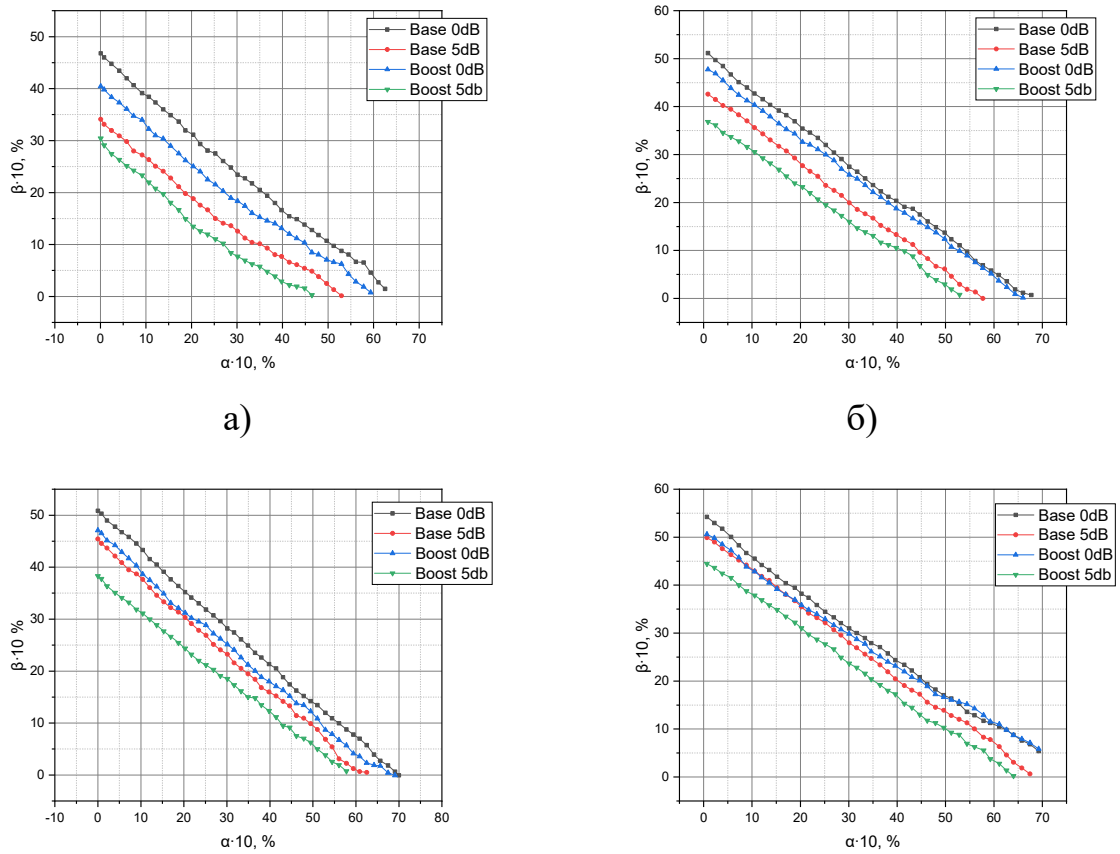
а) б)

Рисунок Ж.11 – Залежність коефіцієнтів EER і AEER від варіанта конфігурації машини опорних векторів

Наведені на рис. Ж.11 результати підтвердили результати з рис. Ж.10 і дозволяють однозначно визнати конфігурацію SiVM+Kbcos+Gall як таку, що дозволяє забезпечити вищу з-поміж порівняних конфігурацій машини опорних *i*-векторів достовірність АСММШ. Також відзначимо, що в експерименті використовувався шум типу «Train station», при якому роздільність варіантів конфігурацій машини опорних векторів була найгіршою (див. рис. Ж.10г).

Дослідимо емпірично вплив запропонованої технології бустінгу вмісту еталонної бази на достовірність комплексної моделі процесу АСММШ, у якій інтегровано моделі, представлені на рис. Ж.1, Ж.2, Ж.3. Відповідно, процес прийняття рішень у досліджуваній комплексній моделі підтримується ансамблем класифікаторів, описаних виразами (Ж.21), (Ж.29), (Ж.46) тощо. Результати експерименту представлено на рис. Ж.12, з яких видно, що застосування технології бустінгу дає помітний ефект, знижуючи імовірності виникнення похибок першого або другого роду на $\pm 0{,}5 \div 1{,}5\,\%$ і $\pm 0{,}5 \div 2\,\%$, відповідно. З результатів, наведених на рис. Ж.12а і б, очевидно, що бустінг дозволяє адаптувати класифікатори комплексної моделі до протидії періодичним низькочастотним шумам – саме їх більше за все в шумах типу «Car» і «Street». У той же час, зробити комплексну модель менш чутливою до шумів типу «Airport» і «Train station», як це видно з рис. Ж.12в і г, відповідно, вдається гірше, що можна

пояснити суттєво ширшим частотним діапазоном, який зазнає впливу шуму, а також суттєво вищою енергією самих шумів.



а) б)

в) г)

Рисунок Ж.12 – Результати використання запропонованого методу бустінгу

Завершуючи аналіз моделей процесу АСММШ на основі машини опорних супервекторів відзначимо, що процес навчання машини опорних супервекторів відбувається на незбалансованому еталонному матеріалі, тобто є суттєвий дисбаланс на користь кількості супервекторів, які описують акустичне оточення приймачів сигналу, перед кількістю супервекторів, які використовуються для персоніфікації голосу цільового суб’єкта, відповідно до встановлених міток.

Причина виникнення дисбалансу закладена в саму структуру моделі, представленої на рис. Ж.2 – при синтезі універсальної фонової моделі опрацьовується еталонний матеріал всіх суб’єктів. Така ситуація проявляється у

завищенні кількості випадків, коли розв’язувальне правило (Ж.29) не може віднести особу суб’єкта, який автентифікується, до жодного з двох класів.

Подолати цей недолік можна здійснивши більш прецизійне налаштування порогу прийняття рішень. Наступний недолік опосередковано пов’язаний із попереднім – процедура генерування супервекторів чутлива до тривалості мовленнєвих сигналів, що опрацьовуються. Невідповідність тривалості аналізованих мовленнєвих сигналів призводить до зниження якості адаптації універсальної фонової моделі до цільового суб’єкта, знижуючи таким чином достовірність моделі процесу автентифікації. Проаналізуємо вплив визначених недоліків емпірично, представивши отримані результати на рис. Ж.13.

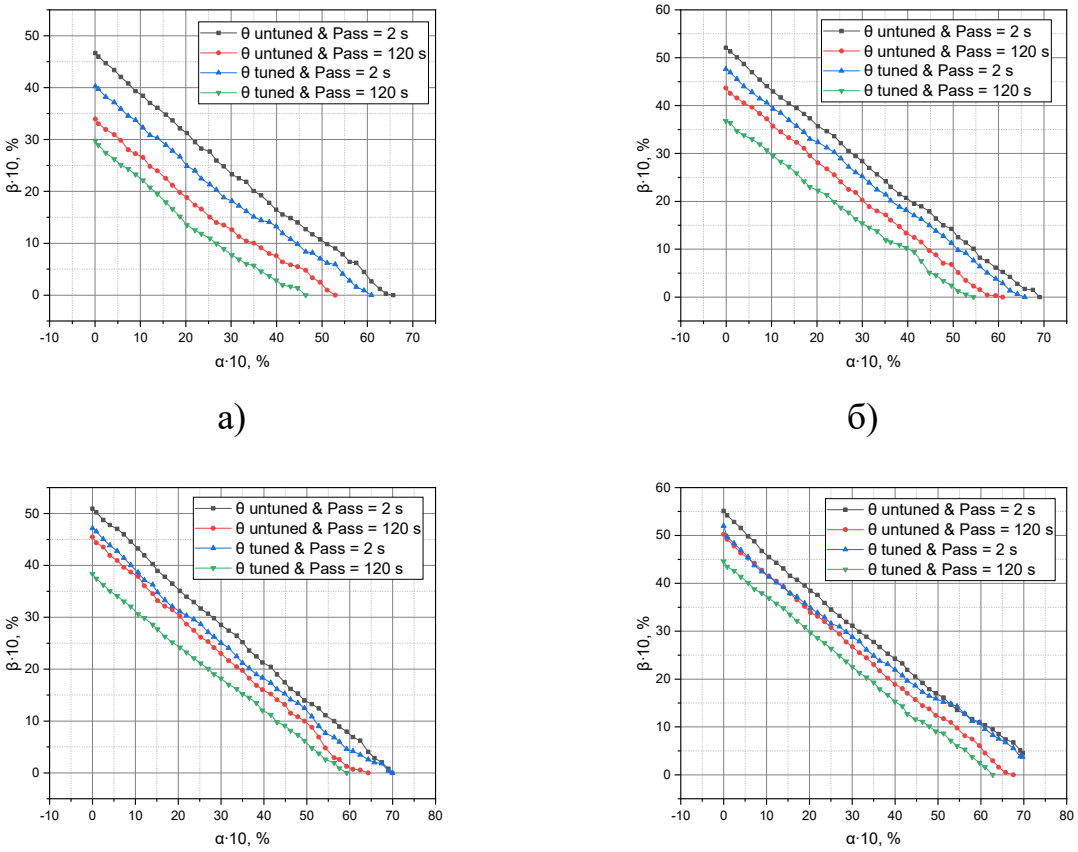


Рисунок Ж.13 – Вплив порогу прийняття рішень і тривалості парольного мовленнєвого сигналу на достовірність моделі процесу автентифікації суб’єкта машиною опорних супервекторів

Результати, представлені на рис. Ж.13, підтверджують помітний вплив порогу прийняття рішень у класифікаторі машини опорних супервекторів та тривалості парольного мовленнєвого сигналу на достовірність моделі процесу АСММШ. Емпірично доведено, що збільшення тривалості парольного мовленнєвого сигналу понад 2 хв. не веде до помітного зростання достовірності моделі, але при зростанні цієї тривалості від 2 с до 2 хв. імовірності похибок першого і другого роду спадають приблизно на один відсоток, відповідно. Втім, використання таких тривалих парольних мовленнєвим сигналів на практиці спричинятиме суб’єктам суттєвий дискомфорт. Також підтвердилася доцільність додаткового налаштування порогу прийняття рішень, але цей процес поки що є, в кращому випадку, автоматизованим.

Отже, у додатку вичерпно описано теоретичні і практичні аспекти моделювання процесу АСММШ у парадигмі породжувальних і дискримінаційних імовірнісних моделей. Емпіричні результати всебічно довели адекватність і достовірність отриманих моделей. Підводячи підсумок варто акцентувати увагу на тому, що навчання імовірнісних моделей потребує відповідної репрезентативної еталонної бази – мовленнєвого корпусу. Прикро, але коректно розміченого для задачі АСГ мовленнєвого корпусу із україномовними фонограмами досі не існує, що значно призупиняє інтеграцію отриманих результатів на регіональному рівні.

Додаток З

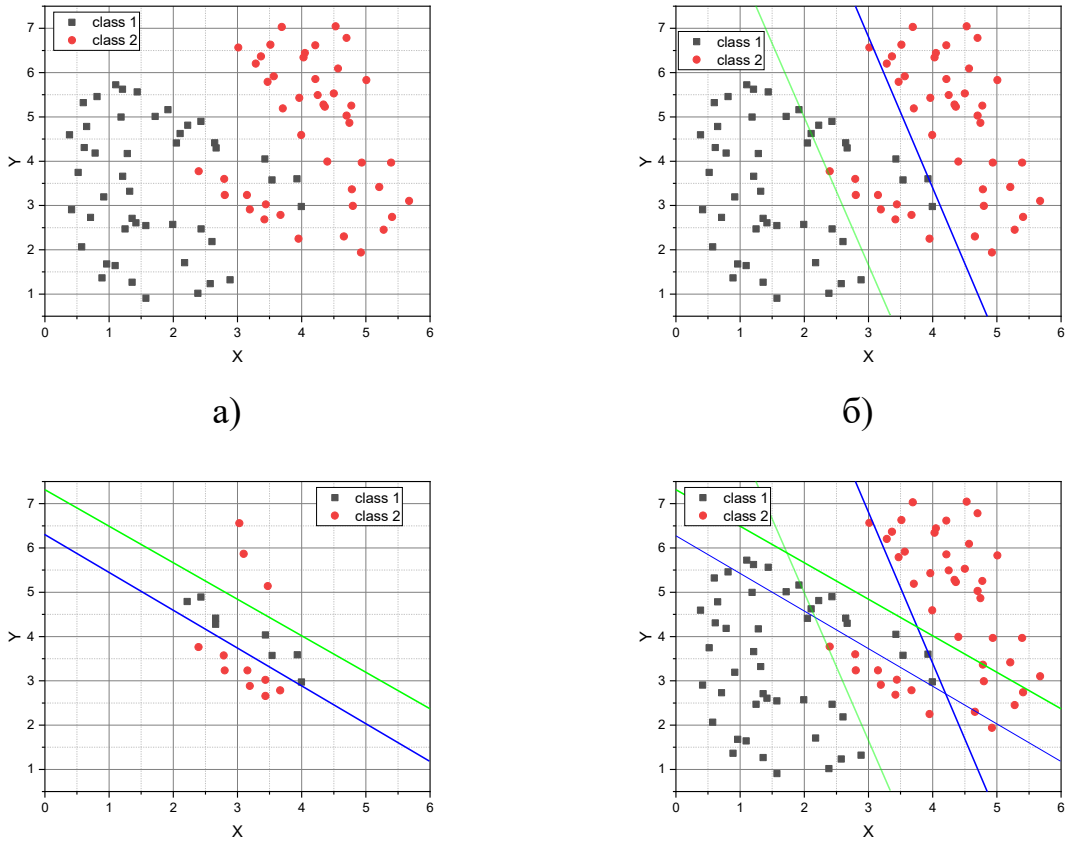
Формалізація методу найкращих оцінок

Описані у підрозділі 4.1 і додатку Ж процеси бустінгу еталонних навчальних даних та синтезу проекційної функції-ядра машини опорних векторів дозволили в поєднанні запропоновувати математичний апарат для синтезу простого класифікатора найкращих оцінок. Під терміном «найкраща оцінка» розумітимемо ідентифіковану дискримінантну функцію, яка найкраще описує вміст даної еталонної навчальної бази. Відповідно, можна представити навчання як ітеративний процес ідентифікації таких функцій. На кожній ітерації з множини конкуруючих варіантів обирається дискримінантна функція, яка забезпечує найкраще розділення класів, а вміст еталонної бази зрізується, тобто з неї вилучаються елементи, які обрана функція найкращої оцінки класифікувала вірно. Ітеративний процес продовжується, якщо після поточної операції зрізання отримано не пусту еталонну базу, обсяг якої перевищує встановлене гранично допустиме обмеження.

Проілюструємо на рис. З.1 описаний вище процес. Нехай у параметричному просторі представлено два класи (див. рис. З.1а). Скориставшись двома з описаних у додатку Ж класифікаторів лінійно розділимо класи в просторі ознак (зелена лінія характеризує перший класифікатор, а синя – другий) та визначимо похибку кожного з класифікаторів підрахувавши кількість невірно класифікованих точок у параметричному просторі (див. рис. З.1б). Визначившись із кращим з класифікаторів, сформулюємо на його основі функцію найкращих оцінок для першої ітерації та виконаємо процедуру зрізання, прибравши із простору характеристичних параметрів вірно класифіковані точки (див. рис. З.1в), розпочавши наступну ітерацію. На рис. З.1г наведено результати функціонування конкуруючих класифікаторів для першої і другої ітерацій методу найкращих оцінок із відображенням початкової конфігурації параметричного простору.

Центральним питанням, що вирішуватиметься на кожній ітерації функціонування методу, є вибір найкращої дискримінантної функції, який можна спростити ввівши у розв’язувальне правило поріг прийняття рішень. Нехай два

еталонних набори даних C_1 і C_2 описано моделлю СГР з двох компонентів із векторами середніх значень μ_1, μ_2 і коваріаційними матрицями Σ_1, Σ_2, відповідно.



а) б)

в) г)

Рисунок 3.1 – Приклад двох ітерацій методу найкращих оцінок.

Найпростіше розв’язувальне правило для класифікації за таких вихідних умов опишемо виразами

$$C_1 : L(x) \geq \theta, \tag{3.1}$$

$$C_2 : L(x) < \theta, \tag{3.2}$$

де x – вхідний вектор характеристичних параметрів розмірністю N, а θ – поріг прийняття рішень, залежний від вектора ваг компонент моделі суміші w, апріорної імовірності і детермінанта коваріаційних матриць тощо.

Формалізуємо дискримінантну функцію для описаного виразами (3.1), (3.2) процесу класифікації:

$$L(x) = x^T\left(\Sigma_1^{-1} - \Sigma_2^{-1}\right)x - 2\left(\mu_1^T\Sigma_1^{-1} - \mu_2^T\Sigma_2^{-1}\right)x = \sum_{i=1}^{N}\lambda_i\left|x^T w_i\right|^2 - 2w_0 x, \tag{3.3}$$

де $w_0 = \left(\mu_1^T\Sigma_1^{-1} - \mu_2^T\Sigma_2^{-1}\right)$, а λ_i і w_i – i-е власне значення та i-й власний вектор коваріаційної матриці $\Sigma_1^{-1} - \Sigma_2^{-1}$, відповідно. Аналіз виразу (3.3) дозволяє зробити низку висновків. Зокрема, якщо $\Sigma_1 = \Sigma_2$, то зменшуване в (3.3) дорівнює нулю і розв'язувальне правило збігається до лінійного дискримінанта Фішера: $L(x) = -2w_0 x$. Якщо $i = 1$, тобто використовується лише одне, екстремальне, власне значення λ_i, то результат операцій із матрицями в (3.3) втілиться в форму квадратної матриці. Також, враховуючи, що в зменшуваному у виразі (3.3) використовується операція піднесення до квадрату, то поріг θ можна апроксимувати двома порогами θ_1 і θ_2, утвореними як результат розв'язання відповідного квадратного рівняння.

Якщо класи C_1 і C_2 представлено множиною точок у N-вимірному параметричному просторі, то для найкращого розділення класів треба розв'язати задачу лінійного дискримінантного аналізу [248] на основі виразу (3.3) маючи за мету знаходження максимально допустимих значень вектора w. Аналітично розв'язок такої задачі для двох класів можна описати функцією-критерієм

$$J_s(w) = \left(w^T S_B w\right)\left(w^T S_W w\right)^{-1}, \tag{3.4}$$

де

$$S_B = (M_1 - M_2)(M_1 - M_2)^T; \tag{3.5}$$

$$S_W = \sum_{x\in X_1}(x - M_1)(x - M_1)^T + \sum_{x\in X_2}(x - M_2)(x - M_2)^T; \tag{3.6}$$

X_1 і X_2 – еталонні навчальні матриці першого і другого класів, відповідно, в яких у рядках представлено вектори характеристичних параметрів; M_1 і M_2 – вектори середніх значень для еталонних матриць X_1 і X_2, відповідно.

Фактично, вираз (3.6) у формі S_W описує лінійну комбінацію коваріаційних матриць першого і другого класів на основі еталонних матриць X_1 і X_2. Вочевидь, що при ненульовому векторі $(M_1 - M_2)$, вектор w, значення якого максимізують критерій (3.4), можна розрахувати з виразу

$$S_B w = \lambda S_W w, \tag{3.7}$$

який, при несингулярній матриці S_W, можна переписати так:

$$S_B S_W^{-1} w = \lambda w. \tag{3.8}$$

Якщо S_B – матриця першого рангу, а значення $S_B w$ прямують до $(M_1 - M_2)$, то вектор ваг можна отримати врахувавши єдине ненульове власне значення

$$w = \alpha S_W^{-1}(M_1 - M_2), \tag{3.9}$$

де α – константа нормалізації.

При мультикласовій класифікації вираз (3.5) набуває вигляду

$$S_B = \sum_{i=1}^{c} r_i (M_i - M)(M_i - M)^T, \tag{3.10}$$

де M_i – вектор середніх значень для класу i; r_i – кількість векторів у еталонній базі класу i; M – вектор середніх значень для всіх класів.

За аналогією з виразом (3.10), перетворимо вираз (3.6):

$$S_W = \sum_{i=1}^{c} \sum_{x \in X_i} (x - M_i)(x - M_i)^T.$$

Адаптовану для мільтикласової класифікації версію критерію (3.4) із урахуванням виразу (3.9), (3.10) опишемо виразом

$$J_s(w') = \left((w')^T S' w'\right)\left((w')^T w\right)^{-1}, \tag{3.11}$$

де $w' = w\sqrt{S_W}$, $S' = \left(S_W^{-0,5}\right)^T S_B S_W^{-0,5}$.

Максимізують критерій (3.11) значення вектора w, розраховані із урахуванням припущень, описаних при формалізації виразу (3.9):

$$w = w' S_W^{-0,5}. \tag{3.12}$$

Критерій (3.4), або його мультикласовий варіант (3.11), якісно розділяє класи, якщо вектор $(M_1 - M_2)$ є суттєво невиродженим. Якщо ж це не так, то налаштування значення порогу виконуватимемо відповідно до критерію

$$J_p = \left(E\left\{(X_l w)^T (X_l w)\right\}\right)\left(E\left\{(X_c w)^T (X_c w)\right\}\right)^{-1} = \\ = \left(w^T \Sigma_l w\right)\left(w^T \Sigma_c w\right)^{-1}, \tag{3.13}$$

де X_l – еталонна матриця для класу l, у рядках якої представлено відповідні вектори характеристичних параметрів; а X_c – еталонні матриці всіх інших класів, окрім класу l; Σ_l і Σ_c – відповідні коваріаційні матриці. На клас l з-поміж всіх c класів вказує найбільше власне значення з обчислених при сингулярному розкладенні еталонних матриць кожного класу окремо.

Вектор ваг w, значення якого максимізують функцію-критерій (3.13), можна розрахувати виходячи із виразу

$$\Sigma_l w = \lambda \Sigma_c w, \tag{3.14}$$

здійснивши аналітичні перетворення, аналогічні описаним у процесі формалізації виразу (3.9).

Коректність запропонованого у формі виразу (3.13) прецизійного класифікатора можна довести математично описавши його зв'язок із нейромережевим гаусівським класифікатором [291, 309], якщо дані еталонної бази описують гаусівським розподілом із нульовим вектором середніх значень. Нехай $w = \Sigma_c^{-0,5} V$, звідки $V = \Sigma_c^{0,5} w$, тоді представимо критерій (3.13) виразом

$$J_G = \left(V^T \left(\Sigma_c^{-0,5}\right)^T \Sigma_l \Sigma_c^{-0,5} V\right)\left(V^T V\right)^{-1},$$

який приведемо до компактнішого вигляду, ввівши заміну $S = \left(\Sigma_c^{-0,5}\right)^T \Sigma_l \Sigma_c^{-0,5}$:

$$J_G = \left(V^T S V\right)\left(V^T V\right)^{-1}. \tag{3.15}$$

Представимо сингулярне розкладення коваріаційної матриці S як $S = U \Lambda U^T$, де Λ – діагональна матриця власних значень. Критерій (3.15) досягає свого максимального значення при $V = U_1$, де $U_1 \in U$ – власний вектор, якому відповідає найбільше власне значення $\lambda_1 \in \Lambda$, тобто при

$$w = \Sigma_c^{-0,5} U_1 . \tag{3.16}$$

Функцію класифікації для ступеневої форми (3.16) можна описати виразом

$$C_l : \left| x^T \Sigma_c^{-0,5} U_1^T \right|^2 > \theta' , \tag{3.17}$$

$$C_c : \left| x^T \Sigma_c^{-0,5} U_1^T \right|^2 \le \theta' , \tag{3.18}$$

де θ' – відповідне порогове значення. Врахувавши вирази (3.17), (3.18), перетворимо дискримінантну функцію (3.3):

$$\begin{aligned} L(x) &= x^T \left(\Sigma_c^{-1} - \Sigma_l^{-1} \right) x = x^T \left(\Sigma_c^{-0,5} \right)^T \left(I - \left(\Sigma_c^{-0,5} \right)^T \Sigma_l^{-1} \Sigma_c^{0,5} \right) \Sigma_c^{-0,5} x = \\ &= x^T \left(\Sigma_c^{-0,5} \right)^T \left(I - S^{-1} \right) \Sigma_c^{-0,5} x = x^T \left(\Sigma_c^{-0,5} \right)^T \left(I - U \Lambda^{-1} U^T \right) \Sigma_c^{-0,5} x = \\ &= x^T \left(\Sigma_c^{-0,5} \right)^T U \left(I - \Lambda^{-1} \right) U^T \Sigma_c^{-0,5} x = \sum_{i=1}^{N} \left(1 - \left(\lambda_i' \right)^{-1} \right) \left| x^T \Sigma_c^{-0,5} U_i^T \right|^2 . \end{aligned} \tag{3.19}$$

При $i = 1$ аналітичний вигляд дискримінантної функції з виразу (3.19) збігається із наведеним у виразах (3.17) і (3.18) тощо. Також відзначимо, що при апроксимації квадратичної форми у (3.19) двома пороговими значеннями вирази (3.17) і (3.18) можна представити у формі:

$$C_l : \theta_1 \le x^T \Sigma_c^{-0,5} U_1 \le \theta_2 , \tag{3.20}$$

$$C_c : x^T \Sigma_c^{-0,5} U_1 < \theta_1 \vee x^T \Sigma_c^{-0,5} U_1 > \theta_2 . \tag{3.21}$$

Отже, на поточній ітерації методу найкращих оцінок конкуруватимуть проста і прецизійна детермінантні функції, описані виразами (3.3) і (3.19), відповідно. Рішення щодо вибору буде здійснюватися в результаті порівняння значень критеріїв (3.11) і (3.13), відповідно. На рис. 3.2 візуалізовано приклад перебігу такого процесу класифікації у двовимірному просторі характеристичних параметрів для двох класів.

Представлений на рис. 3.2 ітеративний процес класифікації методом найкращих оцінок тривав три ітерації. В результаті конкурентного відбору на всіх трьох ітераціях найкращі оцінки забезпечила проста дискримінантна функція (3.11). Безпосередньо класифікація здійснювалася із встановленням двох порогових значень, як це описано у виразах (3.20), (3.21).

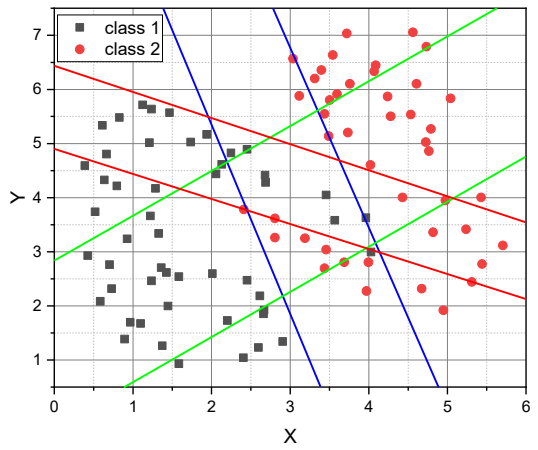
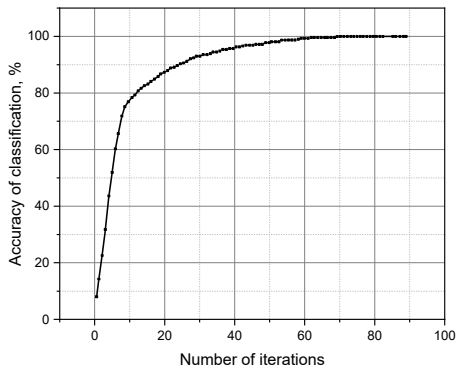
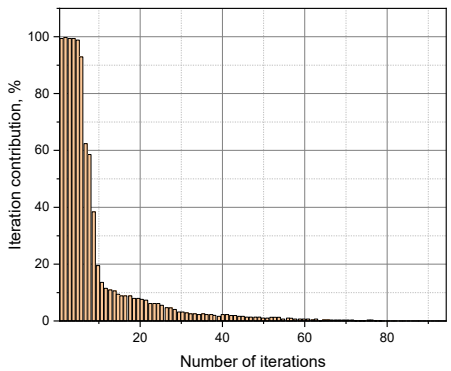


Рисунок 3.2 – Приклад реалізації ітеративного процесу класифікації за методом найкращих оцінок

На рис. 3.3 представлено результати опису методом найкращих оцінок вмісту еталонної навчальної бази, утвореної мовленнєвим матеріалом бази NOIZEUS, який було сегментовано на фрейми тривалістю 20 мс із перекриттям у 10 мс, і параметризовано четвертим набором характеристичних параметрів, описаним у підрозділі 4.2. Кожен фрейм, відповідно, описано значеннями енергії сигналу на частоті основного тону і шести її гармоніках. Такий вибір обумовлено, перш за все, компактністю цього набору характеристичних параметрів.



а)



б)

Рисунок 3.3 – Результати опису вмісту еталонної навчальної бази методом найкращих оцінок

Весь процес опису вмісту еталонної навчальної бази методом найкращих оцінок зайняв 96 ітерацій із встановленням 192 порогових значень. На рис З.3а представлено динаміку зростання адекватності опису вмісту еталонної навчальної бази в міру нарощування складності класифікатора. Зауважимо, що навчання продовжувалося до коректної класифікації всього вмісту еталонної бази. Втім, на практиці такого варто уникати, адже настільки прецизійне навчання є ознакою перенавчання [225], що потім негативно відіб'ється на достовірності процесу автентифікації. Тому на рис. З.3б показано динаміку відносної зміни значень розрахованих класифікатором порогів у міру нарощування його складності. Видно, що прийнятний опис вмісту еталонної бази був отриманий в діапазоні 40–60 ітерацій. Отже, математично коректний метод найкращих оцінок дозволяє отримати простий і ефективний класифікатор для розв'язання задачі верифікації. Недоліком методу є вимога, щоб дані еталонної бази описувалися гаусівським розподілом із нульовим вектором середніх значень.

Додаток К

Модель залежності конфіденційності та готовності інформаційній системі критичного застосування

Практичне впровадження ІС у прикладні галузі підтримки функціонування суспільних інститутів держави, сферу зберігання конфіденційної інформації привело до поступового виділення похідного класу інформаційних систем – інформаційних систем критичного застосування. Зокрема, зараз розглядаються проекти внесення змін у Закон України «Про основи національної безпеки України» з метою формулювання положень критичної інформаційної інфраструктури України та заходів її убезпечення. В наукових публікаціях в залежності від масштабу аналізу до ІСКЗ відносять моделі автоматизованих систем управління критично важливих об’єктів, моделі критичної інформаційної інфраструктуру держави, моделі прикладних ІС, ресурси яких мають значну цінність для визначеного кола зацікавлених суб’єктів тощо.

Критичне застосування ІС обумовлює жорсткі вимоги до забезпечення її інформаційної безпеки. В широкому сенсі під інформаційною безпекою розуміють систему заходів по запобіганню несанкціонованому доступу, використанню, розкриттю, спотворенню, зміні або знищенню інформації. Конкретніше визначення інформаційної безпеки втілено в домінуючу на даний момент тріаду CIA [96–101]: «конфіденційність», «цілісність», «готовність», що розуміють як збалансований захист конфіденційності, цілісності і ІС із підтримуванням визначеного рівня продуктивності її функціонування.

Зазвичай інформаційне убезпечення системи представляють багатоетапним процесом управління ризиками, в якому ідентифіковано архітектуру інформаційного простору системи, джерела загроз, вразливості, потенційні ступені впливу і можливості управління ризиками. Актуальні методики оцінювання ризиків інформаційної безпеки можна розділити на стандартизовані та наукові. Перші, здебільшого, базуються на якісному управлінні ризиками із застосуванням різноманітних таблиць зі шкалами значень ризиків. У світовій практиці найуживанішими є методики, наведені у стандартах ISO/IEC 27005:2011, NIST SP800-30, OCTAVE,

EBIOS тощо. Наприклад, у міжнародному стандарті ISO/IEC 31010 наведено понад 30 підходів для аналізу та оцінювання ризиків. До недоліків зазначених підходів можна віднести їх жорсткість, занадту комплексність і швидке застарівання. Наукові методики, здебільшого, базуються на різноманітних методах кількісного аналізу із застосуванням відповідного математичного апарату, а саме: теорії систем [150, 151], теорії імовірність і математичної статистики [179, 180], мереж Петрі [182, 183], теорії нечіткої логіки [348, 349], нейронних мереж [222, 223, 348, 349] тощо. Втім, спільним для всіх цих методів є універсальність, що веде до необхідності їх адаптації при спробах застосування для опису специфічних класів ІС, до яких відноситься й ІСКЗ. При чому часто адаптація можлива лише після створення проміжної моделі-інтерфейсу, яка може виявитися складнішою за саму модель оцінювання ризику. Також ці підходи розглядають процеси оцінювання ризиків конфіденційності і готовності як незалежні задачі. Отже, враховуючи згадані вище обставини, можна констатувати відсутність моделі оцінювання залежності конфіденційності і готовності ІСКЗ, а актуальність цієї задачі обумовлює доцільність її ідентифікації.

Практичну реалізацію процесу автентифікації в ІСКЗ покладено на підсистему розмежування доступу, яка автентифікує суб’єкта за: даними ідентифікаційної карти; паролем; біометричними характеристиками голосу. Для прийняття рішення за кожним із згаданих вище атрибутів у ПРД реалізовано ансамбль класифікаторів із можливістю ранжування генерованих ними рішень відповідно до обраної адміністратором стратегії управління, формалізованої в СПБ. Узагальнюючи ранжовані результати від кожного з класифікаторів ансамблю, ПРД приймає остаточне рішення щодо особи суб’єкта, який автентифікується. Такий підхід до організації процесу автентифікації робить його вкрай надійним, але входить у суперечність із CIA [98, 99]. Зокрема, в суперечність входять перший і третій компоненти тріади, адже, підвищення конфіденційності ускладнює процес автентифікації і робить його все тривалішим, що, відповідно, знижує готовність ІСКЗ, прямою характеристикою для визначення якої є час, за який суб’єкт отримує доступ до ІнР системи відповідно до його привілей і класу. Отже, виникає потреба у фо-

рмалізації математичного апарату який би дозволив ідентифікувати залежність між конфіденційністю комплексного ступінчатого процесу автентифікації, керованого ПРД, та готовністю ІнР ІСКЗ. Для отримання базової моделі під управлінням конфіденційністю розумітимемо можливість активації/деактивації окремих класифікаторів у ансамблі ПРД, а поняття готовності ототожнимо із тривалістю процесу автентифікації суб'єкта. Зрештою, необхідно мінімізувати втрати готовності ПА, конфіденційність якого не повинна знизитися нижче заданого адміністратором порогового рівня.

Отже, ПА в ІСКЗ має ступінчатий характер і включає каскад послідовно реалізованих незалежних процедур автентифікації особи суб'єкта, який отримує доступ, за різними атрибутами. Врахувавши це, в якості базового математичного апарату для моделювання надійності ПА використаємо напівмарковську модель прийняття рішень для керованого марковського процесу в неперервному часі із дискретною тривалістю окремих його етапів. Такий вибір базового математичного апарату походить з визначення НМП як випадкового процесу, що переходить з одного стану в інший відповідно до заданих розподілів імовірностей, а тривалість перебування процесу в довільному стані є випадковою величиною, розподіл якої залежить як від поточного стану, так і від стану, в який буде здійснено наступний перехід. Це визначення органічно корелює із описом ПА в ІСКЗ. Модель ПА в ІСКЗ має дозволити обрати оптимальну стратегію роботи ПРД, визначивши доцільність активації/деактивації окремих класифікаторів в ансамблі, що досягається застосуванням методу булевого програмування [284, 285, 333]. Нехай існує множина станів $i \in S = \{0,1,\ldots,N\}$, кожному з яких відповідає етап ПА, під час якого ПРД приймає одне із скінченної множини описаних у СПБ рішень $R_i = \{1,2,\ldots,r_i\}$. Імовірнісний закон

$$Y_{ij}^{r}(t) = P_{ij}^{(r)} F_{ij}^{(r)}(t) \tag{К.1}$$

описує прийняте ПРД рішення $r = R_i$ на $i \in S$ етапі ПА, де $P_{ij}^{(r)}$ – імовірність переходу ПА від етапу i до етапу j, а $F_{ij}^{(r)}(t)$ – функція розподілу тривалос-

ті перебування ПА на етапі i при прийнятті ПРД рішення r за умови, що етап j наслідуватиме i. Функції $F_{0j}^{(r)}(t)$ і $F_{j0}^{(r)}(t)$, $j \in \widetilde{S} = S/\{0\}$, $r \in R_j$, та їх перші похідні неперервні при $t > 0$ та експоненційно зростають. Вважатимемо, що коректному завершенню відповідного етапу ПА відповідатиме значення $i = 0$, а $i \neq 0$ відповідатиме факту реєстрації на цьому етапі ПА ситуації, описаної у СПБ. Нехай за одиницю часу перебігу i-го етапу ПА внаслідок прийняття ПРД рішення r витрачається $k_i^{(r)}$ умовних одиниць готовності (квантів машинного часу). Значення $\left|k_i^{(r)}\right|$ обмежені для всіх $i \in S$, $r \in R_i$, а імовірності $P_i^{(r)}$ задовольняють вираз $\sum_{j \in S} P_i^{(r)} = 1$, $P_{ij}^{(r)} \geq 0$, $i, j \in S$, $r \in R_i$. Отже, під час перебігу $i \in S$ етапу ПА, ПРД аналізує r_i варіантів із скінченної множини R_i, вибираючи варіант r, що еквівалентно ідентифікації всіх значень кортежу $\left\langle Y_{ij}^r(t), P_{ij}^{(r)}, F_{ij}^{(r)}(t), k_i^{(r)} \right\rangle$, $i, j \in S$. При $i = 0$, $j \in S, R_0 = \{0\}$ величина $P_{0j}^{(r)} \neq 0$ описує імовірність переходу ПА у стан j і визначається як емпірично встановлене відношення кількості порушень СПБ на етапі j до загальної кількості зареєстрованих порушень СПБ для всього ПА, а функція $F_{0j}^{(r)}(t)$ описує розподіл тривалості реакції ІСКЗ на виявлений ПРД факт порушення СПБ на етапі j. При $i = \overline{1, N}$, $\forall r \in R_i$, $P_{i0}^{(r)} = 1$, $P_{ij}^{(r)} = 0$, $j \neq 0$ функція $F_{i0}^{(r)}(t)$ описує розподіл тривалості реакції ІСКЗ на виявлений факт порушення СПБ, пов'язаний із прийнятим ПРД рішенням r на етапі i. За умови неперервності експлуатації ІСКЗ використовуватимемо експоненційну міру втрат готовності $\exp(-\alpha\tau)$, де α – норма втрат, а загальні втрати готовності для всього ПА опишемо виразом

$$\int_0^t k_i \exp(-\alpha\tau) d\tau = k_i \alpha^{-1}(1 - \exp(-\alpha\tau)). \qquad (К.2)$$

Якщо перебіг ПА від початкового етапу i_0 після n-го переходу досягає етапу i_n, який характеризується прийнятим ПРД рішенням u_n при тривалості етапу

τ_n, то оптимальні стратегії прийняття рішень для ПРД опишемо послідовністю імовірнісних мір $\beta_n(z_n)$, де $z_n = (i_0, u_0, \tau_0, \ldots, i_{n-1}, u_{n-1}, \tau_{n-1}, i_n)$ описує історію перебігу ПА з моменту його початку. Позначимо: $d_i^{(r)}$ – щільність міри стратегії β_n; $i_n = i$; $u_n = r$, $r \in R_i$; $g_i(t, \alpha, \beta)$ – загальні втрати готовності ІСКЗ, ПА якої керовано стратегією β із нормою переоцінювання α під час неперервного циклу експлуатації тривалістю t; $\upsilon_i(t, \alpha, \beta) = g_i(t, \alpha, \beta)/t$ – нормовані за тривалістю t втрати готовності ІСКЗ. Підсумкові ж обмеження щодо конфіденційності ІСКЗ із урахуванням стратегії управління перебігом ПА узагальнимо виразом

$$\sum_{j \in S} c_{rj} x_{rj} \geq b_r , \tag{К.3}$$

де $r \in R = \bigcup_{j \in S} R_j$; c_{rj} – втрати конфіденційності, пов'язані із прийняттям ПРД рішення r внаслідок реєстрації факту порушення СПБ на етапі j; b_r – задані адміністратором порогові значення припустимих втрат конфіденційності при реалізації рішення r; x_{rj} – булева змінна, яка приймає значення 1, якщо внаслідок прийнятого ПРД рішення r зафіксовано факт порушення СПБ на етапі j, або 0, якщо факту порушення СПБ не зафіксовано. Теорія математичного програмування [284, 285] дозволяє стверджувати – якщо система обмежень (К.3) сумісна, то існує невипадкова стаціонарна стратегія β^*, яка мінімізує нормовані загальні втрати готовності ПА $\upsilon(\alpha, \beta) = (\upsilon_0(\alpha, \beta), \upsilon_1(\alpha, \beta), \ldots, \upsilon_N(\alpha, \beta))$ при довільній стратегії β і нормі переоцінювання $\alpha > 0$. Вектор $\upsilon(\alpha, \beta)$ містить $\upsilon(\alpha, \beta) - (N+1) \times 1$ елементів, причому

$$\upsilon_i(\alpha, \beta) = \lim_{t \to \infty} \upsilon_i(t, \alpha, \beta), \; i \in S . \tag{К.4}$$

Отже, необхідно синтезувати α-оптимальну стаціонарну марковську стратегію β^*, яка мінімізуватиме нормовані загальні втрати готовності напівмарковського ПА $\upsilon(\alpha, \beta)$ при довільному початковому розподілі станів процесу

$$y = (y_0, y_1, \ldots, y_N), \; \sum_{i \in S} y_i = 1, \; i \in S . \tag{К.5}$$

Імовірність переходів напівмарковського ПА з етапу i на етап j із прийняттям ПРД рішення $r \in R_i$ описуватимемо матрицею $P^{(r)} = \left\{p_{ij}^{(r)}\right\}$, стохастичні елементи якої дозволяють, враховуючи вираз (К.1), визначити сумісну імовірність $Q_{ij}^{(r)}(t)$ того, що за час t ПА перейде з етапу i на етап j $(i \neq j)$ в наслідок прийняття ПРД рішення $r \in R_i$:

$$\begin{cases} Q_{ij}^{(r)}(0) = 0, \; if \;\; t = 0, \\ \sum\limits_{i,j \in S} Q_{ij}^{(r)}(t) = \sum\limits_{i,j \in S} p_{ij}^{(r)} = 1, \; if \;\; t > 0. \end{cases} \tag{К.6}$$

На основі матриці $Q^{(r)}(t) = \left\{Q_{ij}^{(r)}(t)\right\}$ перейдемо до функції розподілу тривалості перебування ПА на етапі i при прийнятті ПРД рішення $r \in R_i$:

$$H_i^{(r)} = \sum_{i,j \in S} Q_{ij}^{(r)}(t). \tag{К.7}$$

Отже, управління Z_t напівмарковським ПА, який перебуває у момент часу t на етапі i, описуватиметься кортежем $\left\langle N, y, Q_{ij}^{(r)}(t)\right\rangle$ при $i, j \in S$, $r \in R_i$. Спираючись на положення теорії відновлення [300] для одноелементних множин рішень R_i отримаємо такий вираз для визначення $\upsilon_i(t, \alpha, \beta)$:

$$\upsilon_i(t, \alpha, \beta) = (1 - H_i(t))(1 - \exp(-\alpha t))\alpha^{-1} k_i +$$

$$+ \sum_{j \in S} \int_0^y \left((1 - \exp(-\alpha t))\alpha^{-1} k_i + \upsilon_j(t - \tau)\exp(-\alpha t)\right) dQ_{ij}(\tau),$$

який, при переході до скінченних множин R_i та із урахуванням імовірностей $d_i^{(r)}$ прийняття ПРД рішення r на етапі i, перетворимо до вигляду

$$\upsilon_i(t, \alpha, \beta) = \sum_{r \in R_i} d_i^r \left((1 - H_i^{(r)}(t))(1 - \exp(-\alpha t))\alpha^{-1} k_i^{(r)}\right) +$$

$$+ \sum_{j \in S} \sum_{r \in R_i} \int_0^y d_i^r \left((1 - \exp(-\alpha t))\alpha^{-1} k_i^{(r)} + \upsilon_j(t - \tau)\exp(-\alpha t)\right) dQ_{ij}(\tau), \tag{К.8}$$

де $k_i^{(r)}$ – втрати готовності за одиницю часу перебування ПА на етапі i при прийнятті ПРД рішення $r \in R_i$; $\upsilon_j(t-\tau)$ – нормовані загальні втрати готовності із урахування переоцінювання (К.2) за умови, що історія перебігу ПА відома з моменту часу $t=0$ і розпочалася етапом j. Здійснимо подальше спрощення виразу (К.8), застосувавши перетворення Лапласа–Стілтьєса [347] до виразу (К.4) з метою переходу від $\upsilon_i(\alpha,\beta)$ до $\upsilon_i(\alpha)$. Аналіз виразу (К.7) дозволяє стверджувати, що $H_i^{(r)}(\infty)=1$, тоді перший доданок у виразі (К.8) при $t \to \infty$ дорівнює нулю, а застосувавши до решти частинне інтегрування і позначивши $L^*_{s=\alpha}\left\langle H_i^{(r)}(\tau)\right\rangle$ – перетворення Лапласа–Стілтьєса функції $H_i^{(r)}(\tau)$, отримаємо вираз:

$$F_j^{(r)}(t)=\sum_j \int_0^t (1-\exp(-\alpha t))dQ_{ij}^{(r)}(\tau)=$$

$$=(1-\exp(-\alpha t))\sum_j dQ_{ij}^{(r)}(\tau)\Big|_0^t-\sum_j \alpha\int_0^t \exp(-\alpha t)H_i(\tau)d\tau= \qquad (К.9)$$

$$=(1-\alpha)L_{s=\alpha}\left\langle H_i^{(r)}(\tau)\right\rangle=1-L^*_{s=\alpha}\left\langle H_i^{(r)}(\tau)\right\rangle=1-h_i^{(r)}(\alpha).$$

Об’явимо функцію $\Phi_i^{(r)}(t)=\int_0^r e^{-\alpha t}v_j(t-\tau)dQ_{ij}^{(r)}(t)$, яку при $t \to \infty$ представимо як $\Phi_i^{(r)}(t)=\int_0^\infty e^{-\alpha t}v_j(\alpha)dQ_{ij}^{(r)}(\tau)=v_j(\alpha)q_{ij}^{(r)}(\alpha)$, де $q_{ij}^{(r)}(\alpha)=L^*_{s=\alpha}\left\langle Q_i^{(r)}(\alpha)\right\rangle$. Застосуємо ці вирази для визначення $F_j^{(r)}(t)$ і $\Phi_i^{(r)}(t)$ у виразі (К.9) для його перетворення із вираженням функції $\upsilon_i(t)$ при $t \to \infty$:

$$\upsilon_i(t)=\varepsilon_i(\alpha)+\sum_{j\in S} q_{ij}^{(r)}(\alpha)v_j(\alpha), \qquad (К.10)$$

де

$$\varepsilon_i(\alpha)=\sum_{r\in R_i} d_i^{(r)}\left(\varepsilon_i^{(r)}(\alpha)\right),$$
$$\varepsilon_i^{(r)}(\alpha)=k_i^{(r)}\left(1-h_i^{(r)}(\alpha)\right)\alpha^{-1}, \qquad (К.11)$$

а між векторами $\mathrm{E}(\alpha)=(\varepsilon_0(\alpha),\varepsilon_1(\alpha),\ldots,\varepsilon_N(\alpha))^T$ і $V(\alpha)=(v_0(\alpha),v_1(\alpha),\ldots,v_N(\alpha))^T$ існує зв'язок виду

$$V(\alpha)=\{I-q(\alpha)\}^{-1}\mathrm{E}(\alpha), \tag{К.12}$$

де $q(\alpha)=\{q_{ij}(\alpha)\}=\left\{\sum\limits_{r\in R_i} d_i^{(r)}\left(q_{ij}^{(r)}(\alpha)\right)\right\}$, а I – одинична матриця розмірністю $N\times N$.

Позначивши $\{I-q(\alpha)\}^{-1}=\mu(\alpha)$, перейдемо до матричного запису виразу (К.12), увівши в нього вектор y, описаний у виразі (К.5):

$$y\upsilon(\alpha)=\sum_{i\in S}\sum_{j\in\widetilde{S}}\sum_{r\in R_i} y_i\mu_{ij}(\alpha)\varepsilon_j^{(r)}(\alpha)d_i^{(r)}.$$

Перепозначивши $x_{rj}=d_i^{(r)}$, $d_i^{(r)}\in\{0,1\}$, $\sum\limits_{j\in S} d_i^{(r)}=1$, сформулюємо у термінах математичного програмування цільову функцію і систему обмежень задачі оптимізації готовності ІСКЗ із напівмарковським представленням ПА та обмеженнями на втрати конфіденційності:

$$f(\alpha,X)=\sum_{i\in S}\sum_{j\in\widetilde{S}}\sum_{r\in R_i} y_i\mu_{ij}(\alpha,X)\varepsilon_j^{(r)}x_{rj}\to\min$$

$$\begin{cases}\sum\limits_{j\in\widetilde{S}} c_{rj}x_{rj}\ge b_r,\\ \sum\limits_{r\in R_i} x_{rj}=1,\end{cases} \tag{К.13}$$

де $i\in S$, $j\in\widetilde{S}$, $r\in R_i$. Задача оптимізації (К.13) є задачею математичного програмування із нелінійною цільовою функцією і лінійною системою обмежень, яку можна було б розв'язати стандартними методами нелінійного програмування [284, 285], але присутність у (К.13) булевих змінних обумовлює доцільність коментування процесу розв'язання. Позначимо область допустимих розв'язків системи обмежень задачі (К.13) як $Z=\{s_j\}$, $j=1,\ldots,N$, де s_j – множина номерів r, які задовольняють рівність $x_{rj}=1$. Знайшовши розв'язки m нерівностей $\sum\limits_{j\in\widetilde{S}} c_{rj}x_{rj}\ge b_r$, завершимо

процес знаходження Z за m кроків, розпочавши із початкового вектора $Z^{(0)}$, який містить всі значення $r = R_i$. Якщо на r-му кроці значення $r = r_1$ із вектора $Z^{(r-1)}$ співпаде із одним із розв'язків r-ї нерівності $\alpha_j \in \{0,1,\phi\}$ із (К.13), де ϕ – невизначений булевий параметр, то $s_j^{(r)}$ елемент Z визначатимемо аналізуючи такі варіанти: якщо $\alpha_j = 1$, то при $r_1 \in s_j^{(r-1)}$ вважаємо $s_j^{(r)} = \{r_1\}$; якщо $r_1 \overline{\in} s_j^{(r-1)}$, то вважаємо $s_j^{(r)} = \varnothing$; якщо $\alpha_j = 0$, то $s_j^{(r)} = s_j^{(r-1)} / \{r_1\}$; для всіх інших α_j вважаємо $s_j^{(r)} = s_j^{(r-1)}$. Отриманий на m-му кроці алгоритму вектор-розв'язок системи обмежень задачі (К.13) $Z^{(m)} = \{\alpha_1^{(m)}, \ldots, \alpha_N^{(m)}\}$ складається із $\alpha_j^{(m)}$, $j = 1, \ldots, N$, елементів, кожен з яких містить множину значень $\{r\}$, $r \in R = \{1, \ldots, m\}$. Підставивши отримані із вектора $Z^{(m)}$ значення $\alpha_j^{(m)}$, які належать області допустимих розв'язків системи обмежень задачі (К.13), у цільову функцію $f(\alpha, X)$, знаходимо елементи вектора X, що її мінімізують, і описують оптимальну стратегією налаштувань ПРД при заданих обмеженнях на втрати конфіденційності ІСКЗ.

Сформулюємо методику застосування описаної вище моделі вважаючи, що у СПБ описано два типи помилок ПА: критична помилка – коли ПРД, спираючись на результати роботи більшості класифікаторів ансамблю із урахуванням ваг їх рішень, визнає суб'єкта, який автентифікується, таким, що не має права доступу; підозра на помилку – коли ПРД, спираючись на результати роботи більшості класифікаторів ансамблю із урахуванням ваг їх рішень, визнає суб'єкта, який автентифікується, таким, що має право доступу, проте помітна кількість класифікаторів автентифікувала суб'єкта як антагоніста. Враховуючи критичне застосування ІС, у ситуації ПП доцільним є інформування адміністратора для винесення остаточного вердикту щодо надання суб'єкту доступу, але така дія значно подовжує тривалість ПА, знижуючи, відповідно, готовність ІСКЗ.

Нехай в СПБ у випадку реєстрації КП передбачено послідовність дій $R = \{r_1, r_2, r_3\}$, а у випадку реєстрації ПП – $R = \{r_1, r_4\}$, тоді у термінах описаної вище моделі $N = 2$, а $m = 4$. Зважатимемо, що ПРД має ступінчату, комплексну,

послідовно з'єднану блочну структуру. Кожен блок-ступінь ПРД включає відповідні підблоки виділення характеристичних параметрів і класифікації, об'єднані в ансамбль. Рішення, яке приймає класифікатор кожного із підблоків є незалежним. Нехай $F_j(t)$ – функція розподілу тривалості ПА між двома зареєстрованими ситуаціями КП або ПП, які опишемо змінною j. Тоді $G_j^{(k)}(t)$ – функція розподілу втрат готовності від реакції СПБ r на факт реєстрації ситуації j. Вважатимемо, що функції $F_j(t)$ та $G_j^{(k)}(t)$ описуватимуться екпоненційним законом із коефіцієнтами λ_j та $\mu_j^{(k)}$, відповідно:

$$F_j(t) = 1 - \exp(-\lambda_j t),$$
$$G_j^{(k)}(t) = 1 - \exp\left(-\mu_j^{(r)} t\right), \tag{К.14}$$

де $\lambda_j = T_{j1}^{-1}$, $\mu_j^{(r)} = T_{j2}^{-1}$, а T_{j1}^{-1} – величина, обернена до середньої тривалості перебігу ПА між двома зареєстрованими ситуаціями j, а T_{j2}^{-1} – величина, обернена до середньої кількості втрат готовності від реакції СПБ r на зареєстровану ситуацію j. Нехай $d_i^{(k)}$ – стаціонарна стратегія ПРД, яка контролює ПА, що перебуває на етапі i, приймаючи рішення k, яке описується імовірністю r: $d_i^{(k)} \in \{0,1\}$, $\sum\limits_{k \in K} d_i^{(r)} \in 1$, $i \in S$, тоді вирази (К.14) можна переписати:

$$F_j(t) = 1 - \exp(-\lambda t),$$
$$G_j^{(r)}(t) = 1 - \exp(-\mu t), \tag{К.15}$$

де $\lambda = \sum\limits_{j=1}^{N} \lambda_j$, $\mu = \sum\limits_{j}^{N} d_j^{(r)} \mu_j^{(r)}$. Нехай $i = 0$ означає штатний перебіг ПА, $i = 1$ означає реєстрацію КП, а $i = 2$ – реєстрацію ПП, тоді сформуємо множини $S = \{0, 1, 2\}$ і $\widetilde{S} = \{1, 2\}$ і, при вибраних значеннях T_{11}, T_{21}, $T_{12}^{(1)}$, $T_{22}^{(1)}$, $T_{12}^{(2)}$, $T_{12}^{(3)}$, $T_{22}^{(4)}$, на основі виразів (К.14) і (К.15) розрахуємо $F_0(t)$, $F(t)$, $F_1(t)$, $F_2(t)$, $G_1^{(1)}(t)$, $G_1^{(2)}(t)$, $G_1^{(3)}(t)$, $G_2^{(1)}(t)$ і $G_2^{(4)}(t)$. Нехай c_{kj} – норми втрат конфіденційності від ре-

алізації описаної у СПБ реакції k у відповідь на реєстрацію ситуації j, тоді для продовження розв'язування задамо вартісні коефіцієнти c_{11}, c_{12}, c_{21}, c_{31}, c_{42}. Вважатимемо, що на етапі $i=0$ прийнято рішення $r=0$ і задано імовірності $p_{00}^{(0)}$, $p_{01}^{(0)}$, $p_{02}^{(0)}$, $\sum_{i=0}^{2} p_{0i}^{(0)}=1$, тоді, підставивши розраховані вище значення T_{j1}, T_{j2}, $F_j(t)$, $G_j^{(k)}(t)$, $k=1,2,3$, у вираз (К.6) і (К.7), отримаємо аналітичний вигляд функцій $Q_{00}^{(0)}(t)$, $Q_{01}^{(0)}(t)$, $Q_{02}^{(0)}(t)$, $Q_{10}^{(1)}(t)$, $Q_{10}^{(2)}(t)$, $Q_{10}^{(3)}(t)$, $Q_{20}^{(1)}(t)$, $Q_{20}^{(4)}(t)$ (для описуваної постановки задачі $Q_{11}^{(k)}(t)=Q_{12}^{(k)}(t)=0$) і функцій $H_0^{(0)}(t)$, $H_1^{(0)}(t)$, $H_1^{(2)}(t)$, $H_1^{(3)}(t)$, $H_2^{(1)}(t)$, $H_2^{(4)}(t)$, відповідно. Далі, приймаючи $x_{00}=1$, $x_{kj}=d_j^{(k)}$, $r\in R_j$, $j\in\widetilde{S}$, на основі розрахованого вище отримаємо аналітичний вигляд матриці $q(\alpha,x)=\sum_{r\in R_j} x_{ki}q_{ij}^{(r)}$, $i,j\in S$. Розрахуємо визначник $D(\alpha,x)$ матриці $[I-q(\alpha,x)]$, використавши який при $[I-q(\alpha,x)]^{-1}=[\mu_{ij}(\alpha,x)]$ знайдемо $\mu_{00}(\alpha,x)$, $\mu_{01}(\alpha,x)$, $\mu_{02}(\alpha,x)$, $\mu_{10}(\alpha,x)$, $\mu_{11}(\alpha,x)$, $\mu_{12}(\alpha,x)$, $\mu_{20}(\alpha,x)$, $\mu_{21}(\alpha,x)$, $\mu_{22}(\alpha,x)$. На основі виразу (К.11), задавши $k_0^{(0)}$, $k_1^{(1)}$, $k_1^{(2)}$, $k_1^{(3)}$, $k_2^{(1)}$, $k_2^{(4)}$, знайдемо величини $\varepsilon_0^{(0)}$, $\varepsilon_1^{(1)}$, $\varepsilon_1^{(2)}$, $\varepsilon_1^{(3)}$, $\varepsilon_2^{(1)}$, $\varepsilon_2^{(4)}$. Знайдемо розв'язки $r_1=\{\{1:1,1:2,1:3\},\{2:1,2:2\},\{3:1,3:2\},\{4:1,4:2\}\}$ системи обмежень-нерівностей (К.13), враховуючи, що їх вільні члени b_k задовольняють умови $2c_1<b_1<c_{11}$, $b_2<c_{21}$, $b_3<c_{31}$, $b_4<c_{42}$. Знаючи r_1, на основі початкового вектора $Z^{(0)}=\{\{1,2,3\},\{1,4\}\}$, отримаємо п'ять пар функцій $Z_{1221}^{(4)}$ і $Z_{1222}^{(4)}$, $Z_{2121}^{(4)}$ і $Z_{2122}^{(4)}$, $Z_{2211}^{(4)}$ і $Z_{2212}^{(4)}$, $Z_{3121}^{(4)}$ і $Z_{3122}^{(4)}$, $Z_{3211}^{(4)}$ і $Z_{3212}^{(4)}$, де вектор-розв'язок x_j у кожній парі не містить пустої множини. В результаті, при відомому α та $y=(1,0,\ldots,0)$ розрахуємо допустимі значення цільової функції (К.13) $f_j(\alpha,x_j)$, $j=1,\ldots,5$, і виберемо з них найменше, якому відповідатиме вектор-розв'язок $x_j^*\in x_j$, який задає оптимальну стратегію роботи ПРД із урахуванням обмежень на втрати конфіденційності ПА.

Проведемо дослідження описаної в підрозділі 5.2 ІСКЗ, змінюючи налаштування її ПРД відповідно до наведеної вище моделі. Оптимізуємо стратегію управління ПРД, змінюючи порогове значення параметра втрат конфіденційності α в діапазоні $[1,2,\ldots,15]\cdot 10^{-2}$. Для кожного значення α виконаємо аналогічні описаним вище обчислення для оптимального управління ПА. Для кожної оптимальної стратегії управління ПА, отриманої для відповідного порогового значення α, визначимо середнє емпіричне значення параметра готовності $\overline{d}_e$, для чого узагальнимо дані про тривалість 100 ПА всіх суб'єктів, дані яких є в базі NOIZEUS. Отриману за результатами експериментів залежність втрат конфіденційності ПА і середнього емпіричного значення параметра готовності ІСКЗ для описаних у підрозділі 5.3 класифікаторів у складі ансамблю представлено на рис. К.1.

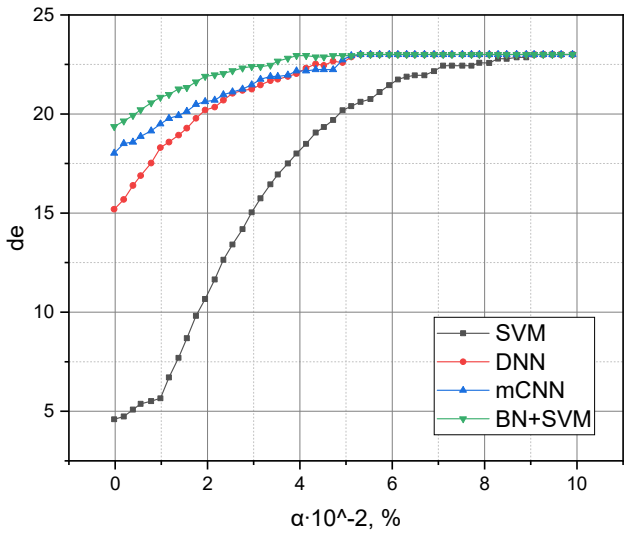


Рисунок К.1 – Залежність втрат конфіденційності ПА
і середнього емпіричного значення параметра готовності ІСКЗ
в залежності від типу класифікаторів, використаних ансамблі ПРД.

Наведені на рис. К.1 результати емпіричних досліджень залежності конфіденційності ПА і готовності ІСКЗ збігаються із розрахованими на основі запропонованої методики, що підтверджує адекватність представленої у підрозділі моделі, а також дозволяють зробити такі висновки: із зменшенням вимог щодо конфіденційності ПА готовність ІСКЗ зростає але, починаючи із значення $\alpha \approx 10\cdot 10^{-2}$ зростання готовності припиняється, що можна пояснити остаточною

адаптацією ПРД до процесу прийняття рішень для досліджуваного колективу суб'єктів; при малих значеннях α готовність ІСКЗ є порівняно низькою, що обмовлено реєстрацією великої кількості ПП та КП, на опрацювання яких витрачається час; класифікатори, основані на глибокій нейромережі (DNN) і машині опорних векторів, яка опрацьовує набори характеристичних параметрів, представлені адаптованими до цільових суб'єктів моделями сумішей гаусівських розподілів (SVM), забезпечують найнижчі показники готовності ІСКЗ при малих значеннях α, що обмовлено реєстрацією великої кількості КП у першому і великої кількості ПП у другому випадках; найкращі показники щодо готовності ІСКЗ при будь-яких значеннях α показали класифікатори, засновані на модифікованій згортковій нейромережі (mCNN) і машині опорних векторів, яка узагальнює BN-характеристичні параметри (BN+SVM). Отримані результати збігаються з представленими в підрозділі 5.3, адекватність яких доведено емпірично.

Додаток Л

Графічна інтерпретація пунктів наукової новизни

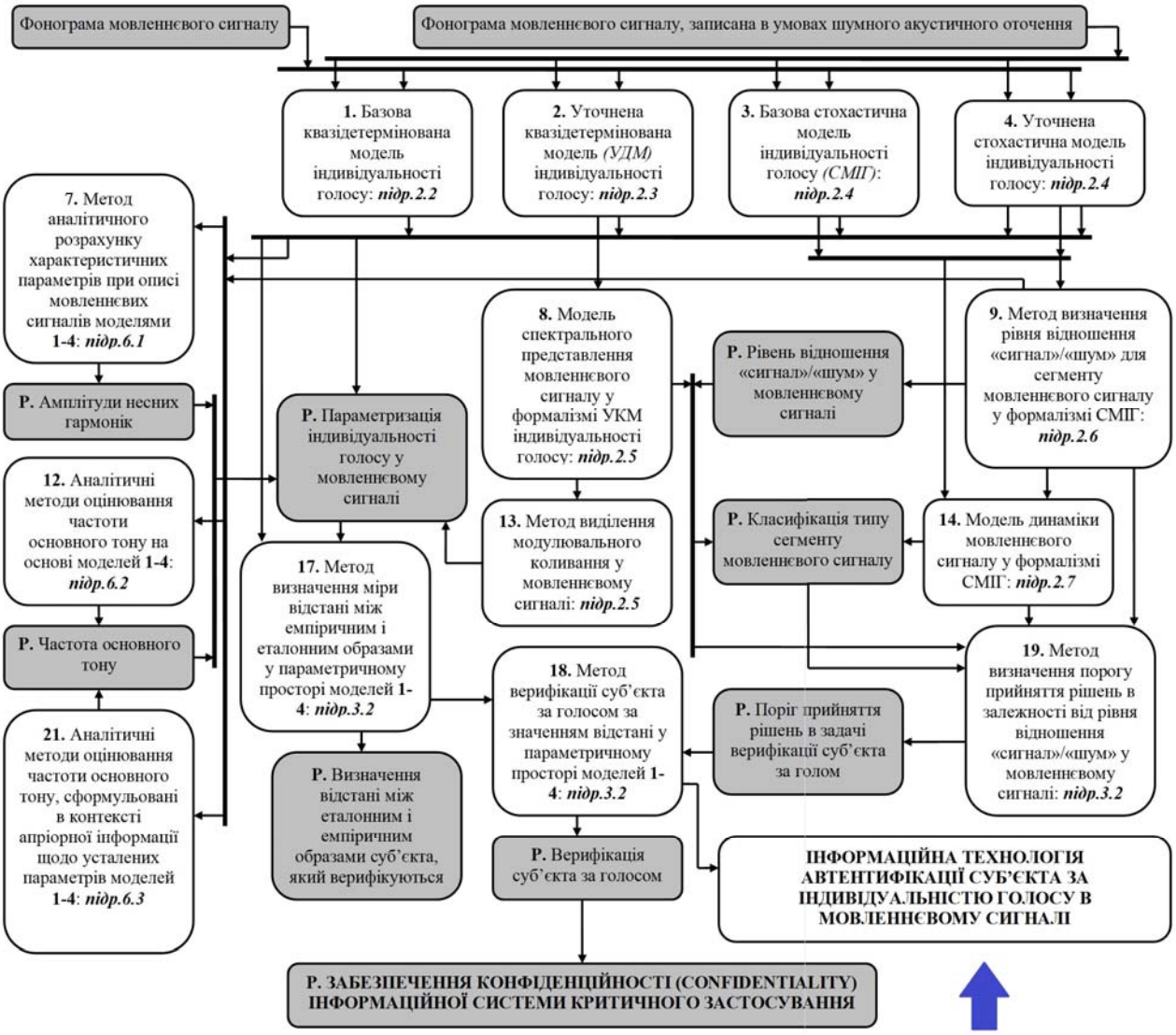


Рисунок Н.1 – Місце 1-го пункуту наукової новизни в інформаційній технології автентифікації суб'єкта за індивідуальністю голосу в мовленнєвому сигналі.

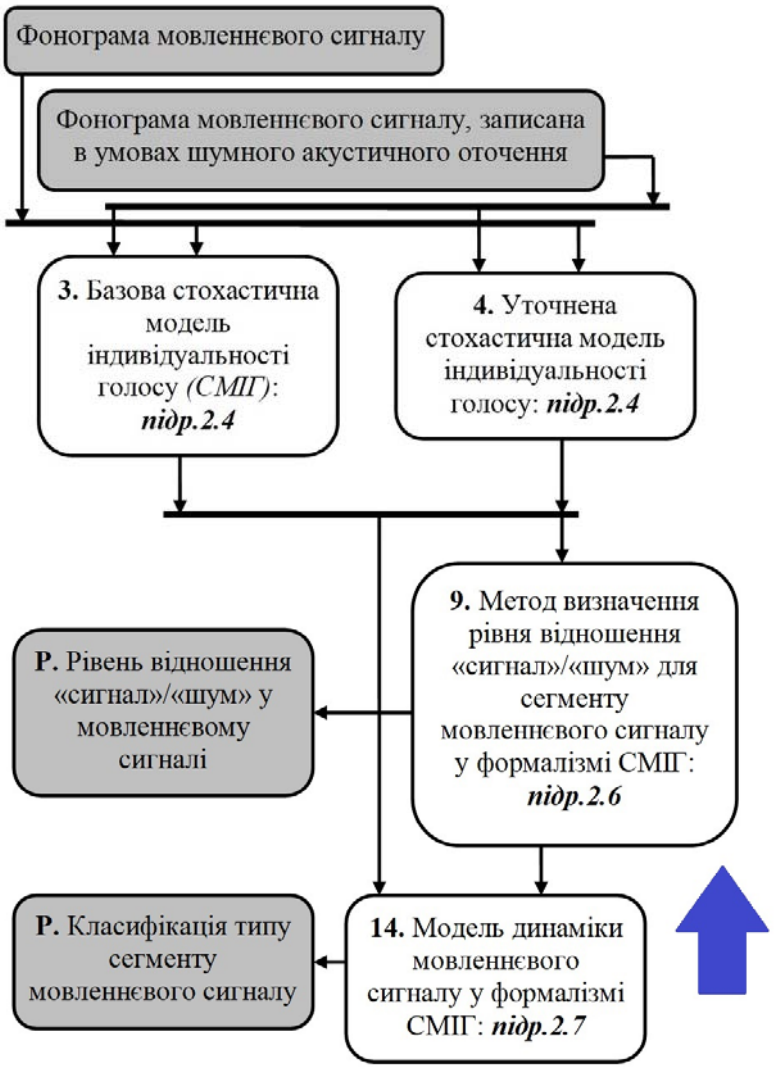


Рисунок Н.2 – Місце 2-го пункуту наукової новизни в інформаційній технології автентифікації суб’єкта за індивідуальністю голосу в мовленнєвому сигналі.

.

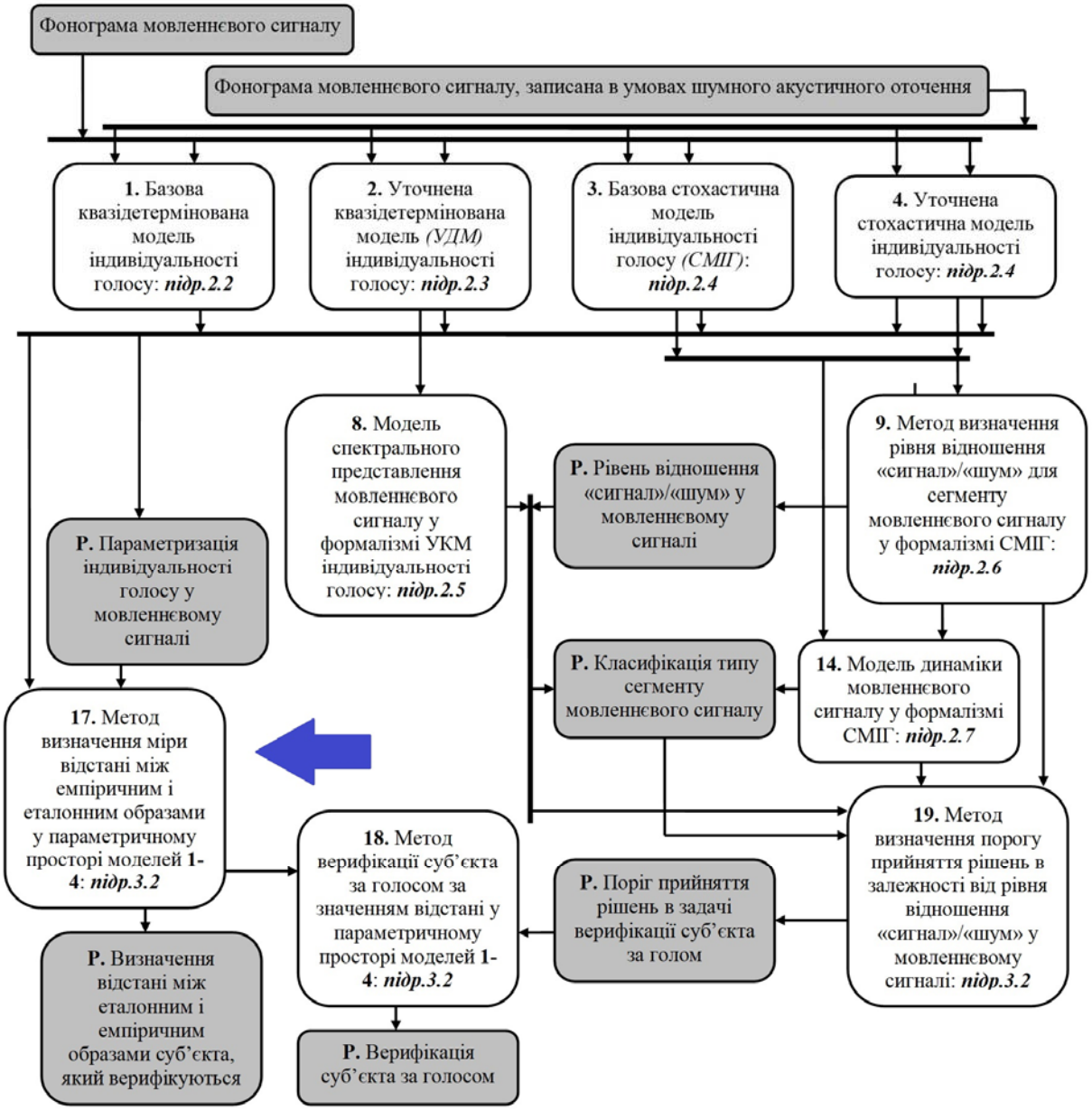


Рисунок Н.3 – Місце 3-го пункуту наукової новизни в інформаційній технології автентифікації суб'єкта за індивідуальністю голосу в мовленнєвому сигналі.

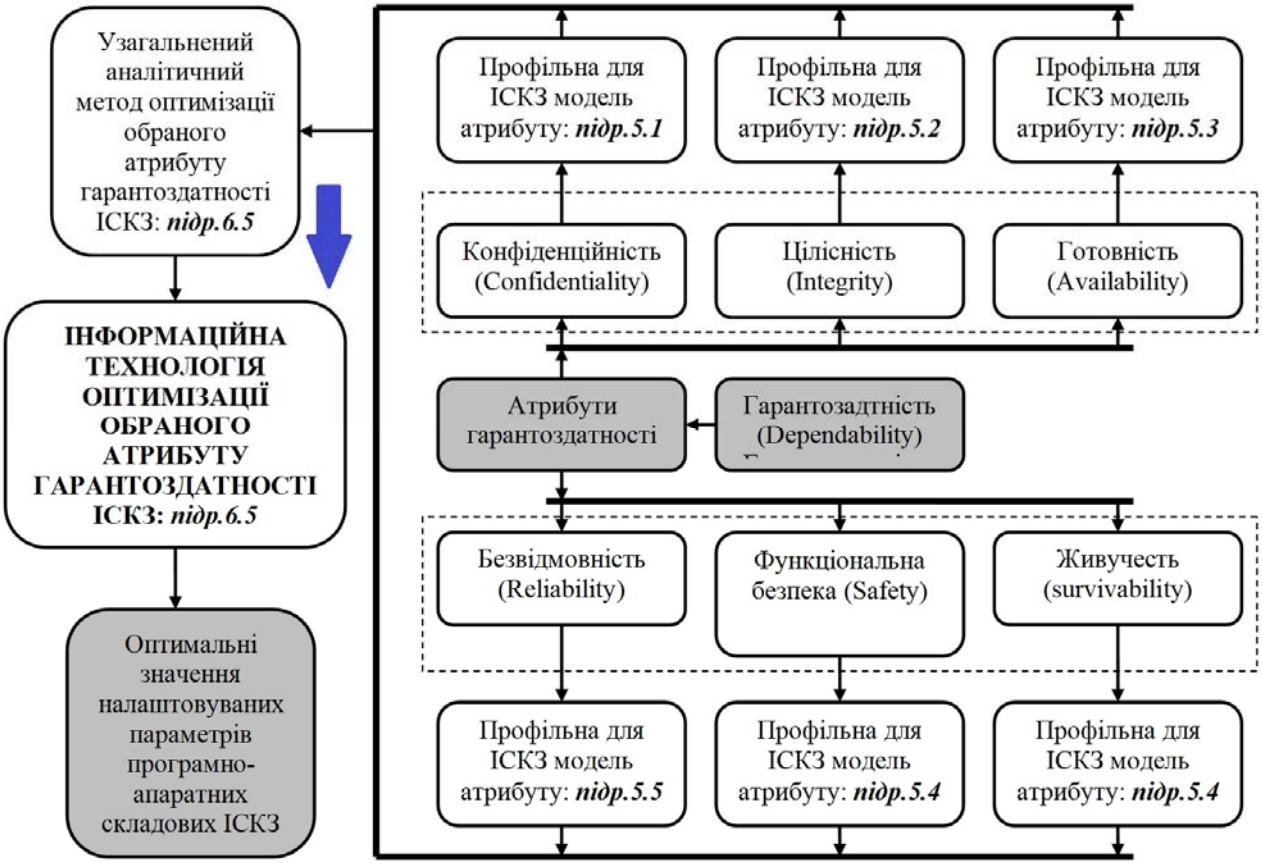


Рисунок Н.4 – Місце 4-го пункуту наукової новизни в інформаційній технології для підвищення обраного атрибуту гарантоздатності інформаційної системи критичного застосування.

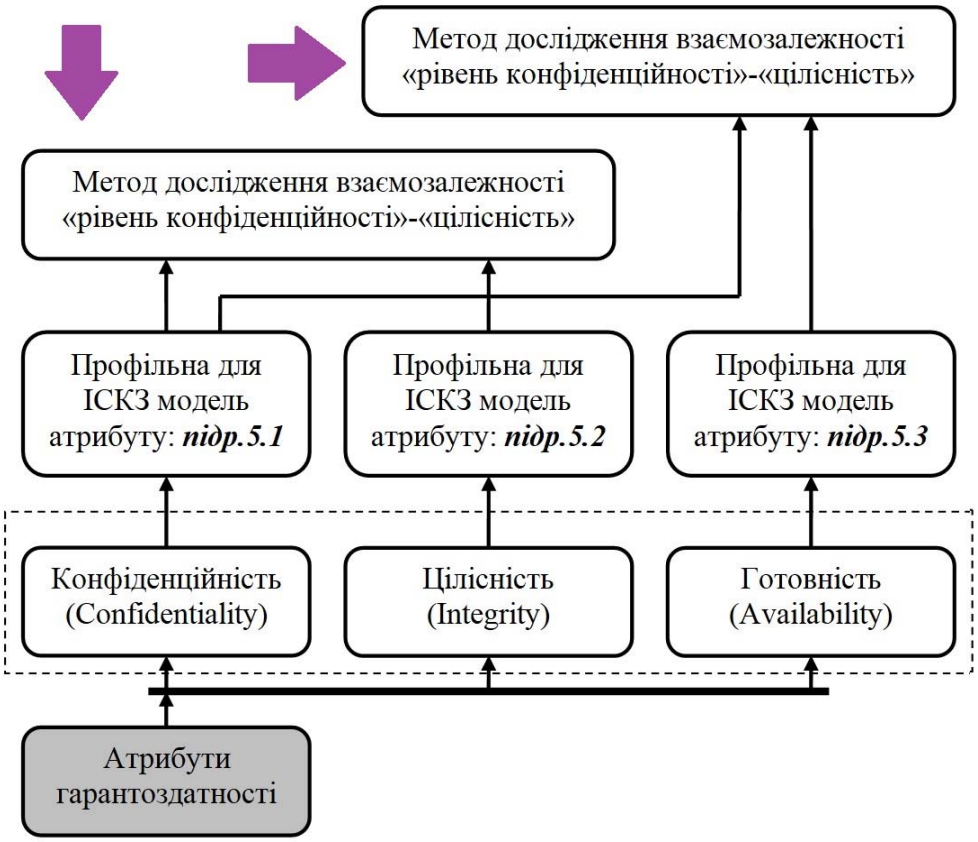


Рисунок Н.5 – Місце 5-го пункуту наукової новизни в інформаційній технології для підвищення обраного атрибуту гарантоздатності інформаційної системи критичного застосування.

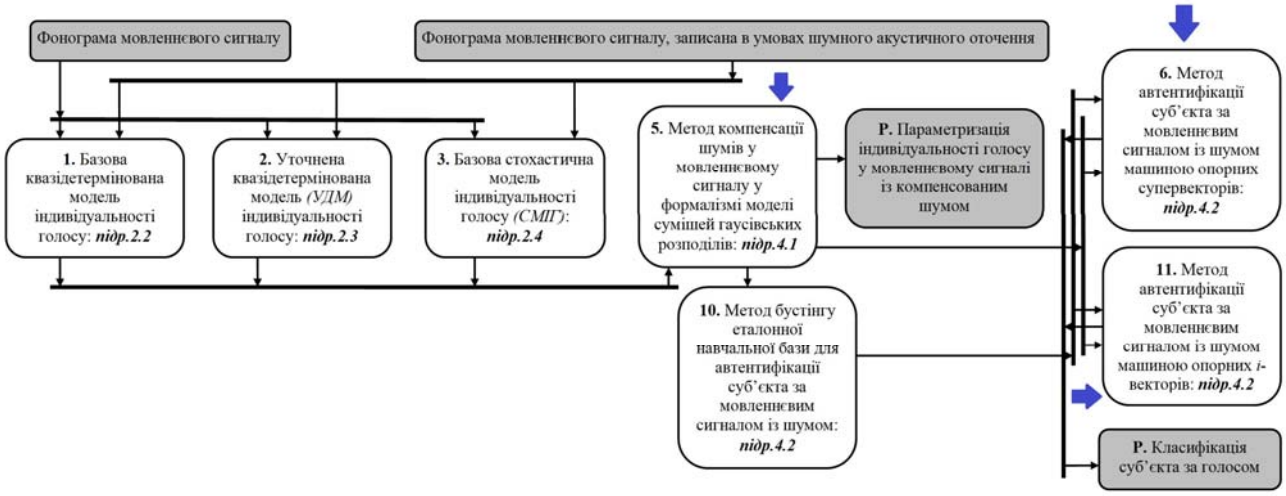


Рисунок Н.6 – Місце 6-го пункуту наукової новизни в інформаційній технології автентифікації суб'єкта за індивідуальністю голосу в мовленнєвому сигналі.

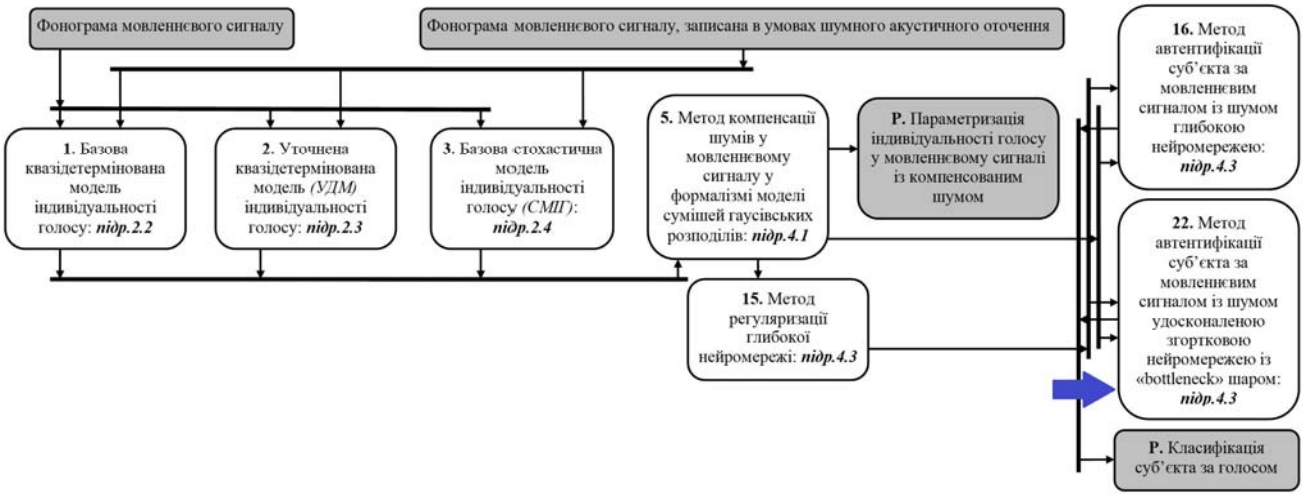


Рисунок Н.7 – Місце 7-го пункуту наукової новизни в інформаційній технології автентифікації суб'єкта за індивідуальністю голосу в мовленнєвому сигналі.

Додаток М

Акти впровадження результатів дисертаційного дослідження

«APPROVE»

Innovative Institute for
Material Studies, LLC
Intel Research Practice

Chairman

ACT OF IMPLEMENTATION OF RESULTS
of dissertation research of Kovtun Viacheslav Vasylovych
on the topic «Information technologies for optimization of
information system for critical use with person authentication
by voice according to the attributes of dependability»

The commission consists of:

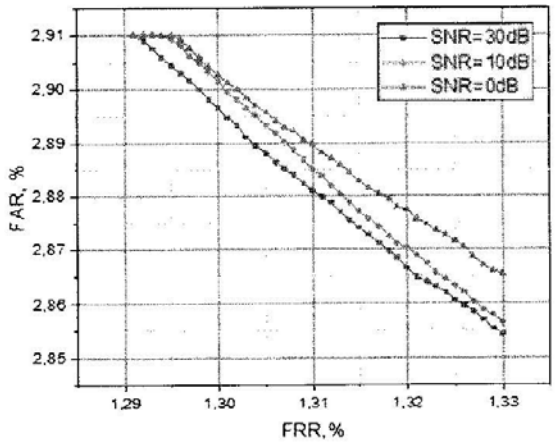
the chairman – Intel Technology Researcher – Roy Lee Wright;

the members: Senior Scientist - Pavlo Molchanov;

made this act stating that in the Innovative Institute for Material Studies, LLC, 415 Old Town Court, Alexandria, VA 22314, USA scientific and applied results obtained by Kovtun V.V. in the process of dissertation research were approbated. The results of the approbation are the strengthening of information security, functional ability and reliability of the prototype of information ecosystem for the Armored Eyewear OCELLUS (http://iims.us/armored-eyewear/) as a hierarchical composition of information platforms of the tactical and network levels. The information ecosystem was designed with the prospect of integration into the Multifunctional Information Distribution System used in NATO military units.

Strengthening of information security was achieved by the implementation of the author's scheme of person authentication via the phonogram of the spoken voice message lasting up to 10 s., encoded according to NATO standard STANAG-4591. The set of words that formed the passphrase was generated by the access control system randomly for each authentication session. The words were chosen from a pre-formed representative dictionary in terms of content and volume (about 1000 nouns, verbs and adjectives). Similarly, the process of training of the access control system with the authentication of the person by voice was organized, except the fact that the duration of the initial phrase reached 30 s. During the tests, 182 persons had access to the data reproduced by the interfaces of the information platforms of the tactical and network levels. 175 persons had "soldier" privileges that provided only the ability to view tactical information. 5 persons had "sarge" privileges that allowed them to view, add and edit tactical information. 2 persons had "commander" privileges which, in addition to the already mentioned services, allowed to initiate the procedure of personalization of new tactical interfaces and provided privileges for viewing, adding and editing

strategic information. During the censored period of operation of the described access control system from 01.01.2020 to 01.06.2020, more than 500 000 authentication sessions were performed. To evaluate the obtained empirical results, the metrics of qualitative indicators defined in the current international standard ISO/IEC 2382-37:2012 Information technology – Vocabulary – Part 37: Biometrics was used. In particular the average probability of error of the first kind (False Rejection Rate, FRR) was 1,31%, and the average probability of error of the second kind (False Acceptance Rate, FAR) was 2,88%. With a confidence level of 99% the ranges of true values of the probabilities of errors of the first and second kind have been determined, respectively: [1,30 ÷ 1,32], [2,86 ÷ 2,90], [%].The following image is the Detection error tradeoff (DET) curve constructed in the FRR-FAR coordinate system which details the above-described results of the censored operation of the studied system depending on the signal-to-noise ratio (SNR):



Additionally, the experiments were performed according to the procedure described in the monograph "The models of attributes of the dependability of the information system for critical use with the person authentication by voice" authored by Kovtun V.V. In particular, the procedure included tests of the operation of the information platform of the tactical level in a noisy acoustic environment of the person, which is authenticated by the individual features of the voice. The value of the signal-to-noise ratio in the test phonograms varied dynamically in the range [0 ÷ 30], [dB]. Noise phonograms were taken from the specialized database of the Eric Johnson School of Engineering and Computer Science at the University of Texas (Dallas, USA) NOIZEUS.

Strengthening of functional ability was achieved by optimizing the settings of the rules of QoS technology in the operating environment of routers of the information platform of the network level, which is the highest level of the synthesized information ecosystem. The network-level information platform provides information exchange and support for services on tactical-level

information platforms. The values of the parameters of the settings were calculated using the author's method described in the fifth section of the mentioned above monograph authored by Kovtun V.V. As a result, for all defined classes of accounts ("soldier", "sarge", "commander"), appropriate access schemes were created depending on the operational circumstances: "confrontation", "tactical game", "strategic game" and "test". Schemes differ in the privileges of providing access to the resources of the network-level information platform for certain classes of accounts. For the accounts of the first two classes in the synthesized schemes the priority in access to the general and tactical information is considered, and in the schemes for the accounts of the third class the top priority of access to tactical information and to strategic information in addition is realized. During the censored period of operation of the modified information platform of network level the facts of unauthorized interruption of access to critical data for authorized persons with accounts of authorized classes weren't registered even in periodically emulated distributed DoS-attacks on the network component of the information ecosystem.

Strengthening of the reliability of the synthesized information ecosystem is embodied in the form of a schedule of the recommended update of the hardware component of the information platforms of the tactical and network levels. In the formation of the schedule methods of estimation of such attributes of dependability as availability, mean time between failures (MTBF), maintainability, survival, functional safety, reliability, etc. calculated by the author's were taken into account. During the censored period theoretical estimates of these attributes deviated from the empirical values by no more than 4% with certain 95% confidence intervals for these characteristics.

This act is informative one and the information provided in it isn't a basis for receiving a monetary reward.

Chairman: signature Roy Lee Wright
full name.

Members: signature Pavlo Molchanov
full name.

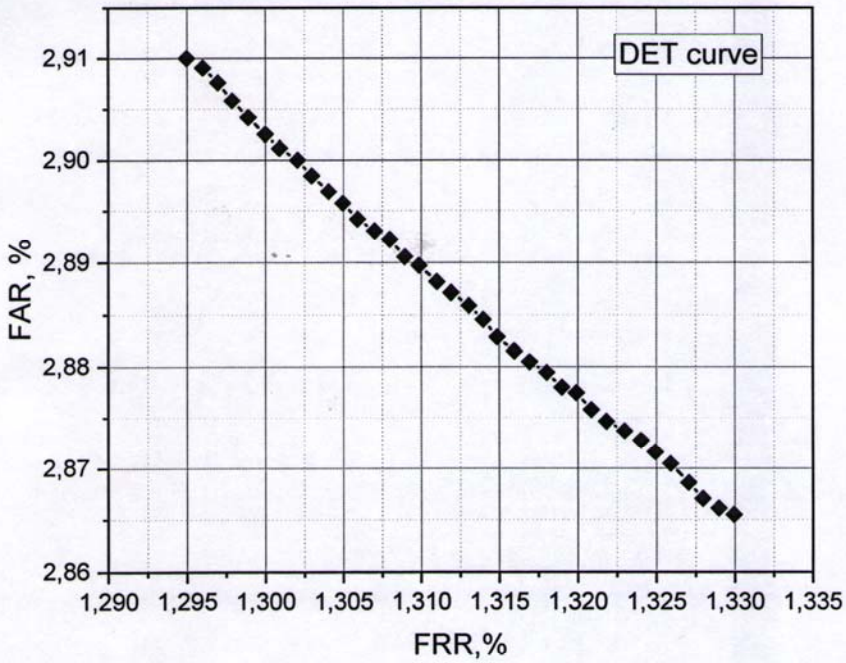
ARS Online OÜ (Limited Liability Company ARS Online)
Address: 10128, 24, Laulupeo str., Harju county, The city of Tallinn, Estonia,
phone: (372) 698 04 66
Registration # 12417225 IBAN # LV21PRTT0265021625100
SWIFT code: PRTTLV22 AS PRIVATBANK (Riga, Latvia)
Correspondent bank: AS PRIVATBANK, DNIPROPETROVSK, UKRAINE
a/c 16007000480001 SWIFT code: PBANUA2X

ACT OF THE RESULTS IMPLEMENTATION
of dissertation research of Kovtun Viacheslav Vasylovych
on the topic «Methodology of information technology synthesis
for optimization in taxonomy of the dependability of information
system of critical use with an authentication of person by voice»

Scientific and applied results obtained by Kovtun V.V. during the process of dissertation research were implemented. The applied results of the approbation are the strengthening of information security, functional ability and reliability of the information system of the institution that issued this act.

Strengthening of information security was reached by introducing a two- phase person authentication scheme for access to stored confidential data of the institution. At the first phase of the implemented scheme, the person was personified according to the authorization scheme of the type "login"–"pass". At the second phase of the implemented scheme the person was verified by the results of the analysis of a phonogram with a spoken password phrase lasting about 10 s. The password phrase content for person verification by voice was generated automatically and randomly on the basis of a given representative dictionary which contained about 1000 nouns, verbs and adjectives. Prior to exploitation the verification system was trained on phonograms with spoken materials of a target persons lasting about 2 minutes. To realize the author's security scheme the data of the institution's database (ID) were segmented into general and confidential parts. The last are the stored personal data of employees, the logistical information, the financial information, digitized versions of agreements with partners and statutory documents, etc. Personalized access to the general segment of the ID could be initiated via HTTPS from specialized smart computer devices with any MAC and IP address. Personalized access to the confidential segment of the ID could be initiated via HTTPS from specialized smart computer devices with MAC and IP addresses which were included in the protected pool of allowed addresses. The set of persons who had access to the confidential segment of the ID: 113 persons whose privileges were limited to viewing confidential information ("user" type); 24 persons whose privileges allowed adding, viewing and editing confidential information ("manager" type); 3 persons whose privileges in addition to the listed services also allowed to initiate the procedure of registration of new persons with privileges of access to confidential data ("administrator" type). The verification procedure involved either confirming the identity of the person being authenticated or not. During the censored period of operation of the information system of the institution with the above-

described protection scheme of the access procedure to the information environment from 01.01.2020 to 01.06.2020 more than 72000 authentication sessions were executed. To evaluate the obtained empirical results, the metrics of qualitative indicators defined in the current international standard ISO/IEC 2382-37:2012 Information technology – Vocabulary – Part 37: Biometrics was used. In particular the average probability of error of the first kind (False Rejection Rate, FRR) was 1,33%, and the average probability of error of the second kind (False Acceptance Rate, FAR) was 2,95%. With a confidence level of 99% the ranges of true values of the probabilities of errors of the first and second kind were determined, respectively: [1,31 ÷ 1,35], [2,93 ÷ 2,97], [%].The following image is the Detection error trade-off (DET) curve constructed in the FRR-FAR system of coordinate which details the above-described results of the censored operation of the implemented system:



Strengthening of the functional ability of the information system was reached by optimizing the parameters of the rules of QoS technology in the operating environment of routers of the internal computer network of the institution. The values of the parameters were calculated according to the method described in the fifth chapter of the V. V. Kovtun's monograph "The models of attributes of the dependability of the information system for critical use with the person authentication by voice" for four types of accounts: "user", " manager", "administrator", "guest". In addition the first three types of accounts had privileges of access to the confidential segment of the ID, and the fourth type – didn't. The parameters of the rules provided gave priority access to the information environment to authorized persons whose accounts belonged to the first three above described types. During the censored period of operation of the modified information system of the institution the facts of unresolved interruption of an

active sessions of access to confidential data for authenticated persons with accounts of authorized types were not recorded. Even in the conditions of periodically emulated distributed DoS-attacks on the segment of the internal computer network of the institution information system where confidential information was stored, no fact of unresolved interruption of active sessions was fixed.

Strengthening of the reliability of the synthesized information ecosystem is embodied in the form of a schedule of the recommended update of it's hardware component. In the formation of the schedule methods of estimation of such attributes of dependability as availability, mean time between failures (MTBF), maintainability, survival, functional safety, reliability, etc. calculated by the author's were taken into account. During the censored period theoretical estimates of these attributes deviated from the empirical values by no more than 6% with certain 95% confidence intervals for these characteristics.

This act is informative one and the information provided in it isn't a basis for receiving a monetary reward.

Director: _____ Pavol Lemko
signature

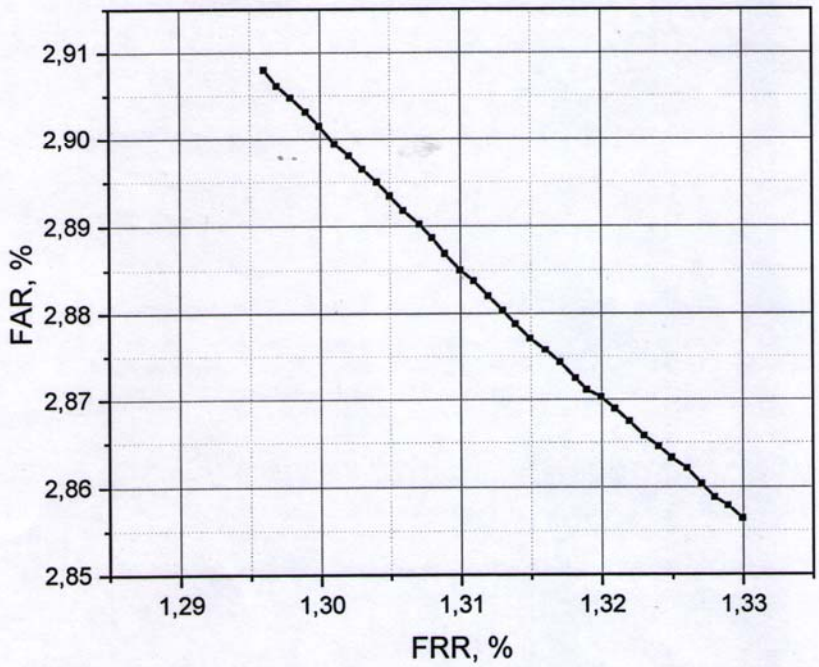
Polski Dom Nowych Mediów Sp. z.o.o
Address: 8 Zhitnia street, Kielce, Swietokrzyskie Voivodship, Poland, 25-018
a/c PL21 1750 1110 0000 0000 1042 9668 Bank Raiffeisen Bank Polska
Spółka SWIFT: PPABPLPKXXX Registration code: KRS 0000299955
NIP: 9591813046 Register Number: 260217436

ACT OF THE RESULTS IMPLEMENTATION
of dissertation research of Kovtun Viacheslav Vasylovych
on the topic «Methodology of information technology synthesis
for optimization in taxonomy of the dependability of information
system of critical use with an authentication of person by voice»

Scientific and applied results obtained by Kovtun V.V. in the process of dissertation research were approbated. The results of the approbation are the strengthening of information security, functional ability and reliability of the information system of the institution that issued this act.

Strengthening of information security was achieved by introducing a two-stage person authentication scheme for access to confidential data of the institution. At the first stage of this scheme, the person was personified according to the authorization scheme of the type "login"–"password". At the second stage of the implemented scheme the person was verified by the results of the analysis of a phonogram with a spoken password phrase lasting 10 s. The meaningful composition of the password phrase for voice verification was generated automatically and randomly on the basis of a given representative dictionary which contained about 1000 nouns, verbs and adjectives. Prior to operation the verification system was trained on phonograms with spoken language materials of target persons lasting about 2 minutes. To implement the author's security scheme the contents of the institution's database were segmented into general and confidential parts. The last is in particular stored personal data of employees, financial and logistical information, digitized versions of statutory documents and agreements with partners. Personalized access to the general segment of the institution's database could be initiated via HTTPS from a specialized devices with any MAC and IP address. Personalized access to the confidential segment of the institution's database could be initiated via HTTPS from a specialized device with MAC and IP addresses which were included in the protected pool of allowed addresses. The circle of persons who had access to the confidential segment of the institution's database included: 81 persons whose privileges were limited to viewing confidential data (type "user"); 11 persons whose privileges allowed viewing, adding and editing confidential data (type "moderator"); 2 persons whose privileges in addition to the listed services also allowed to initiate the procedure of registration of new persons with privileges of access to confidential data (type "administrator"). The verification procedure involved either confirming the identity of the person

being authenticated or not. During the censored period of operation of the information system of the institution with the above-described protection of the access procedure from 01/31/2020 to 01/06/2020 more than 50000 authentication sessions were performed. To evaluate the obtained empirical results, the metrics of qualitative indicators defined in the current international standard ISO/IEC 2382-37:2012 Information technology – Vocabulary – Part 37: Biometrics was used. In particular the average probability of error of the first kind (False Rejection Rate, FRR) was 1,30%, and the average probability of error of the second kind (False Acceptance Rate, FAR) was 2,90%. With a confidence level of 99% the ranges of true values of the probabilities of errors of the first and second kind were determined, respectively: [1,28 ÷ 1,32], [2,85 ÷ 2,95], [%].The following figure is the Detection error tradeoff (DET) curve constructed in the FRR-FAR coordinate system which details the above-described results of the censored operation of the studied system:



Strengthening of the functional ability of the information system was achieved by optimizing the settings of the rules of QoS technology in the operating environment of routers of the internal computer network of the institution. The settings were calculated according to the method described in the fifth section of the monograph "The models of attributes of the dependability of the information system for critical use with the person authentication by voice" authored by Kovtun V.V. for four types of accounts: "user", "moderator", "administrator", "unauthorized". Moreover the first three types of accounts had privileges of access to the confidential segment of the

database of the institution, and the fourth type didn't. The settings provided gave priority access to the information system to authorized persons whose accounts belonged to the first three types. During the censored period of operation of the modified information system of the institution the facts of unauthorized interruption of sessions of access to confidential data for authorized persons with accounts of authorized types were not recorded. Even in the conditions of periodically emulated distributed DoS-attacks on the segment of the internal computer network of the information system of the institution where confidential data was stored, no fact of unauthorized interruption of active sessions was recorded.

Strengthening of the reliability of the synthesized information ecosystem is embodied in the form of a schedule of the recommended update of it's hardware component. In the formation of the schedule methods of estimation of such attributes of dependability as availability, mean time between failures (MTBF), maintainability, survival, functional safety, reliability, etc. calculated by the author's were taken into account. During the censored period theoretical estimates of these attributes deviated from the empirical values by no more than 4% with certain 95% confidence intervals for these characteristics.

This act is not a basis for receiving a monetary reward or concluding additional agreements.

Director: _____ Beznar Dymitr
signature

Міністерство освіти і науки України
Міжнародний науково-навчальний центр
інформаційних технологій та систем
НАН України та МОН України

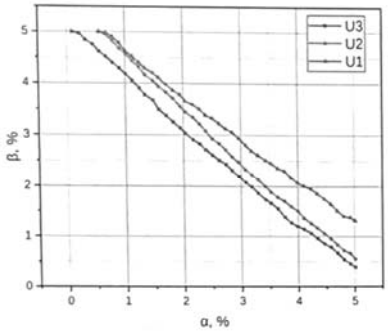
ВІДГУК ЩОДО АПРОБАЦІЇ РЕЗУЛЬТАТІВ
дисертаційної роботи Ковтуна В'ячеслава Васильовича
на тему «Інформаційні технології для підвищення гарантоздатності
інформаційних систем критичного застосування
із автентифікацією суб'єкта за голосом»

У відділі розпізнавання та синтезу звукових образів Міжнародного науково-навчального центру інформаційних технологій та систем НАН України та МОН України апробовано результати дисертаційного дослідження Ковтуна В. В. та тему ««Інформаційні технології для підвищення гарантоздатності інформаційних систем критичного застосування із автентифікацією суб'єкта за голосом». Апробація стосувалася результатів, узагальнених Ковтуном В. В. в монографії «Моделі атрибутів гарантоздатності інформаційної системи критичного застосування із автентифікацією суб'єкта за голосом», у процесі рецензування вмісту якої колектив відділу приймав участь з жовтня по грудень 2019 р. включно. Безпосередньо апробовано отриманий Ковтуном В. В. науковий результат – інформаційну технологію для підвищення конфіденційності цільової інформаційної системи за рахунок інтеграції двохетапної схеми автентифікації користувача для доступу до критично важливих даних, а також прикладний результат – авторське програмне забезпечення для верифікації суб'єкта за голосом у мовленнєвому сигналі з адитивними завадами.

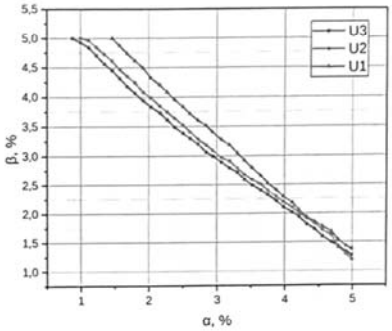
Апробована інформаційна технологія синтезована на основі: квазідетермінованих і стохастичних математичних моделей опису характеристичних параметрів індивідуальності голосу у мовленнєвому сигналі, досліджуваному як у часовому, так і у спектральному просторах; стохастичної математичної моделі параметризації мовленнєвого сигналу із шумом амплітудними значеннями гармонік частоти основного тону мовця; бікомпонентної моделі індивідуальності голосу в мовленнєвому сигналі; методу попереднього оцінювання порогу прийняття рішень в задачі автентифікації суб'єкта за голосом на основі моделювання відношення «сигнал/шум» у досліджуваному мовленнєвому сигналі; методу компенсації шумів у фонограмі мовленнєвого сигналу в контексті задачі автентифікації суб'єкта за голосом із застосуванням сумішей гаусівських розподілів; методів ефективної автентифікації суб'єкта за мовленнєвим матеріалом із шумом спеціалізованими імовірнісними та нейромережевими класифікаторами; моделей і методів оцінювання представлених у метриці гарантоздатності результатів процесу інтеграції механізмів біометричної автентифікації суб'єкта, зокрема, за голосом у цільову інформаційну систему критичного застосування. Аналітичне представлення згаданої інформаційної технології виконано на високому науковому рівні із застосуванням математичного апарату теорії імовірності та математичної статистики, теорії випадкових процесів, теорії математичного аналізу, теорії розпізнавання образів, теорії фонації, методів цифрового оброблення сигналів тощо. Представлені у складі інформаційної технології методи і алгоритми оцінки частоти основного тону і амплітуд формантних зон працюють коректно і дозволяють компактно описати індивідуальність голосу суб'єкта для подальшої верифікації його особи за цією біометричною ознакою.

Апробація авторського програмного забезпечення здійснювалася на етапі рецензування вищезгаданої монографії. За рекомендацією колективу відділу авторське програмне забезпечення було протестовано на матеріалах вільнодоступних мовленнєвих корпусів RedDots dataset і CSTR VCTK Corpus, репрезентативних для тестування систем класу «text-dependent speaker verification». Результати експериментів, описані у підрозділі

4.3 вищезгаданої монографії і узагальнені нижченаведеними DET-кривими (U_1-U_3 – варіанти параметризації індивідуальності голосу), дають змогу однозначно визнати програмне забезпечення для верифікації суб'єкта за голосом, створене на основі синтезованої Ковтуном В. В. профільної інформаційної технології, функціональним із потенціалом для удосконалення.



RedDots dataset



CSTR VCTK

В цілому, результати апробації довели аналітичну коректність і практичну цінність авторських наукових і прикладних наробок, які рекомендується застосовувати для підвищення безпеки процедури персоніфікованого доступу до конфіденційної інформації. Водночас, слід відзначити, що код написаного на мові програмування Python авторського програмного забезпечення для верифікації суб'єкта за голосом доцільно оптимізувати з метою зниження ресурсозатратності. Також, для спрощення інтеграції авторського програмного забезпечення в сучасні корпоративні програні продукти, перше варто представити в об'єктно-орієнтованій, а не структурно-процедурній моделі програмування. Відзначимо, що ці зауваження не впливають на демонстровану авторським програмним забезпеченням високу достовірність верифікації осіб за їх голосами.

Завідувач відділу розпізнавання
та синтезу звукових образів
Міжнародного науково-навчального
центру інформаційних технологій та
систем НАН України та МОН України

М. М. Сажок

КАНЦЕЛЯРІЯ
Сажка М.М.
ЗАСВІДЧУЮ
Зав. канц. 20.03.20
Андросова Г.М.

ЗАТВЕРДЖУЮ

ХМКП «Хмельницькінфоцентр»
назва установи

директор

С.В. МАТВІЙЧУК
П.І.Б. керівника

АКТ ВПРОВАДЖЕННЯ РЕЗУЛЬТАТІВ
дисертаційної роботи Ковтуна В'ячеслава Васильовича
для здобуття наукового ступеня доктора технічних наук

Комісія у складі:
Голова – **заступник директора, Андріїшина Валентина Володимирівна;**
посада, П.І.Б. голови комісії

Члени комісії:
головний інженер-програміст, Широкий Дмитро Вікторович;
інженер-програміст, Медведчук Максим Сергійович;

склала цей акт про те, що в **Хмельницькому міському комунальному підприємстві «Хмельницькінфоцентр»** впроваджено результати дисертаційного дослідження Ковтуна В. В. на тему «Методологія синтезу інформаційної технології для оптимізації інформаційної системи критичного застосування із автентифікацією суб'єкта за голосом у метриці гарантоздатності», здійсненого з метою набуття наукового ступеня доктора технічних наук. Досягнутим практичним результатом впровадження стало адекватне оцінювання надійності інформаційної системи установи та підвищення безпеки її конфіденційних ресурсів, про що докладніше викладено далі.

Практичним втіленням наукових результатів, впроваджуваних Ковтуном В. В., став інтегрований у інформаційну систему установи блок управління інформаційними процесами з такими функціями:

- підтримування процедури доступу до критично важливих даних із двохфакторною авторизацією користувача із послідовним аналізом введеного ним логіну, паролю і фонограми виголошеної парольної фрази, запропонованої блоком;
- налаштування системної політики безпеки інформаційної системи установи для максимізації її доступності для заданого адміністратором рівня конфіденційності;
- управління резервуванням обчислювальних ресурсів для забезпечення цілісності критично важливих даних, задіюваних у інформаційних процесах авторизованих користувачів із різним рівнем привілей;
- розрахунок оцінок готовності, наробки на відмову, обслуговуваності, живучості, функціональної безпеки, безвідмовності для актуальної

конфігурації інформаційної системи установи при заданих рівнях її доступності, цілісності і конфіденційності.

Коректність роботи блоку управління інформаційними процесами починаючи із моменту впровадження, 11.02.2019 р., з періодичністю чотири тижні перевірялася за результатами контрольованого експерименту, який полягав у розпізнаванні 50% довільно вибраних фонограм мовних сигналів, взятих із контрольної вибірки, у яку увійшли 40% мовних матеріалів із спеціалізованих мовних корпусів Centre for Speech Technology Research English Multi-speaker Corpus та RedDots, 60% мовного матеріалу яких було використано для навчання блоку, здійсненого на початку впровадження. Найнижча зафіксована усереднена достовірність розпізнавання мовців за результатами десяти контрольованих експериментів становить 97.46% із визначеними 99% довірчими інтервалами для значень цієї характеристики. Також виявилося, що при реальній експлуатації блоку процедуру його перенавчання необхідно повторювати раз на 2-3 тижні з причини зниження достовірності розпізнавання реальних користувачів.

Також у контрольований експеримент входив набір завдань, спрямованих на перевірку якості підтримуваних блоком управління інформаційними процесами сервісів забезпечення цілісності і доступності критично важливих даних. У набір завдань входили тести з примусовим передчасним завершенням процесів читання, запису, копіювання контрольних даних, які ініціювалися авторизованими акаунтами із різним рівнем привілей. Результати десяти проведених контрольованих експериментів показали відсутність втрати контрольних даних в результаті передчасного переривання операцій читання та копіювання, контрольованих впровадженим блоком. Втрати не збережених контрольних даних в наслідок передчасного переривання контрольованої впровадженим блоком операції запису виявилися пропорційними тривалості часу резервного зберігання, який встановлювався блоком обернено пропорційно рівню привілей досліджуваного акаунту. Відповідно до налаштувань, для акаунтів із найвищим рівнем привілей втрат контрольних даних вдалося уникнути.

В цілому, результати впровадження довели коректність і практичну цінність авторських наукових наробок.

Цей акт не є підставою для отримання грошової винагороди.

Голова комісії _____ В. В. Андріїшина
підпис П.І.Б.

Члени комісії: _____ Д. В. Широкий
підпис П.І.Б.

_____ М. С. Медведчук
підпис П.І.Б.

ЗАТВЕРДЖУЮ

Львівське комунальне
назва установи
підприємство "Міський
центр інформаційних технологій"

підпис П.І.Б. керівника

АКТ
впровадження результатів дисертаційної роботи
Ковтуна В'ячеслава Васильовича
для здобуття наукового ступеня доктора технічних наук

Комісія у складі:
Голова - Директор, Поліщук Володимир Борисович
посада, П.І.Б. голови комісії
;

Члени комісії: Заступник директора з розвитку,
посади, П.І.Б. членів комісії (2 особи)
Войціцький Олег Володимирович, завідувач сектору
ІТ-інфраструктури Батрак Андрій Романович;

склала цей акт про те, що в ЛКП "Міський центр
назва установи
інформаційних технологій"
впроваджено у використання результати реалізованого з метою набуття наукового ступеня доктора технічних наук дисертаційного дослідження Ковтуна В. В. на тему «Методологія синтезу інформаційної технології для оптимізації інформаційної системи критичного застосування із автентифікацією суб'єкта за голосом у метриці гарантоздатності». Моделі гарантоздатності інформаційної системи критичного застосування із автентифікацією суб'єкта за голосом». Впровадження стосувалося підвищення показників гарантоздатності інформаційної системи установи та удосконалення структури і організації підсистеми захисту останньої.

На початковому етапі впровадження, яке розпочалося 04.03.2019 р., автор розрахував показники готовності, наробки на відмову, обслуговуваності, живучості, функціональної безпеки, безвідмовності для вихідної конфігурації апаратного і програмного забезпечення інформаційної системи установи, на основі якого рекомендував наростити обчислювальну потужність інформаційної системи на 23%, адже аналіз логів мережевої її складової з початку 2019 р. зафіксував окремі неперіодичні факти відмови у наданні доступу авторизованим користувачам з причини перевантаження процесорів або пам'яті роутерів мережі. Втім, застосувавши авторський метод оптимізації політики безпеки, вдалося налаштувати QoS-правила роутерів інформаційної системи так, що проблем із доступністю

інформаційної системи на протязі всього цензурованого часу її експлуатації (по 30.12.2019 р. включно) зафіксовано не було ні авторизованими користувачами ні програмно. В результаті вдалося заощадити кошти на модернізацію обладнання.

Також процес авторизації користувачів для отримання доступу до критично важливих ресурсів інформаційної системи установи було посилено введенням авторської схеми двохфакторної верифікації із автентифікацією суб'єкта за голосом як другого фактору. Адекватність удосконаленого таким чином процесу авторизації окрім фактичними результатами експлуатації перевірялася раз на місяць за результатами контрольованого експерименту, який полягав у верифікації 50% довільно вибраних фонограм мовних сигналів, взятих із контрольної вибірки, у яку увійшли 40% мовних матеріалів із спеціалізованих мовних корпусів RedDots і Centre for Speech Technology Research English Multi-speaker Corpus, 60% мовного матеріалу яких було використано для навчання системи верифікації, здійсненого 04.03.2019 р. Найнижча зафіксована усереднена достовірність верифікації суб'єктів з мовних корпусів за результатами десяти контрольованих експериментів склала понад 98% із визначеними 99% довірчими інтервалами для значень цієї характеристики. Експлуатація системи показала, що для підтримування достовірності верифікації реальних суб'єктів-користувачів на високому рівні перенавчання системи необхідно повторювати з періодичністю у два тижні, що спричиняло певний дискомфорт, тому обмеження застування удосконаленої схеми верифікації лише для управління доступом до критично важливих ресурсів інформаційної системи установи виявилося раціональним.

Посилення надійності інформаційної системи установи втілено у формі графіку рекомендованого оновлення її апаратної компоненти, у якому враховано розраховані за авторськими методами оцінки таких параметрів як готовність, наробка на відмову, обслуговуваність, живучість, функціональна безпека, безвідмовність. За цензурований період теоретичні оцінки цих параметрів відхилялися від фактичних не більше ніж на 4% із визначеними 95% довірчими інтервалами для значень згаданих параметрів.

Цей акт не є підставою для отримання грошової винагороди.

Голова комісії _____ Поліщук В.Б.
підпис П.І.Б.

Члени комісії: _____ Бєторик А. Р.
підпис П.І.Б.

_____ Вобуцький О.В.
підпис П.І.Б.

ЗАТВЕРДЖУЮ
директор департаменту
інформаційних технологій
Вінницької міської ради

_____ В. Б. Романенко

АКТ
впровадження результатів дисертаційного дослідження
Ковтуна В'ячеслава Васильовича

Комісія у складі:

Голова - заступник директора департаменту інформаційних технологій Вінницької міської ради Щеглов Д. П.;

Члени комісії: начальник відділу програмного забезпечення департаменту інформаційних технологій Вінницької міської ради Рознюк О. О., начальник відділу інформатизації департаменту інформаційних технологій Вінницької міської ради Черненко Д. С.;

склала цей акт про те, що у департаменті інформаційних технологій Вінницької міської ради впроваджено, зокрема, такі результати дисертаційного дослідження Ковтуна В. В. на тему «Моделі гарантоздатності інформаційної системи критичного застосування із автентифікацією суб'єкта за голосом»:

- комплекс математичних моделей оцінювання атрибутів гарантоздатності (зокрема, готовності, наробки на відмову, обслуговуваності, живучості, функціональної безпеки, цілісності, доступності, конфіденційності, безвідмовності, інтенсивності відмов) для характеристики процесу функціонування досліджуваної інформаційної системи із біометричною автентифікацією суб'єкта;
- математична модель залежності конфіденційності процесу автентифікації суб'єкта і доступності досліджуваної інформаційної системи;
- математичні моделі управління доступністю досліджуваної інформаційної системи із біометричною автентифікацією суб'єкта;
- комплексні математичні моделі процесів оброблювання інформації та розмежування доступу до неї у досліджуваній інформаційній системі;
- базові і уточнені детерміновані і стохастичні математичні моделі індивідуальності голосу у мовленнєвому сигналі, описуваної усередненою частотою основного тону, амплітудами модулювального коливання і вибраною кількістю несних гармонік;
- бікомпонетна математична модель індивідуальності голосу у мовленнєвому сигналі;
- метод розрахунку вагових коефіцієнтів міри розрізнення між еталонним і емпіричним образами у параметричному просторі індивідуальності голосів;

- метод автентифікації суб'єкта за мовленнєвим сигналом із шумом згортковою нейромережею із авторською топологією;
- метод автентифікації суб'єкта машиною опорних векторів із авторським параметризованим представленням мовленнєвого матеріалу із шумом.

Впроваджені результати дозволили: оптимізувати топологію інформаційної системи департаменту; оптимізувати доступність інформаційної системи департаменту при заданому рівні її конфіденційності; підвищити конфіденційність інформаційної системи департаменту за рахунок введення двохфакторної схеми авторизації із автентифікацією суб'єкта за голосом; оптимізувати процес автентифікації суб'єкта за голосом до акустичного оточення терміналів доступу до інформаційної системи департаменту; оптимізувати обчислювальну складність процесу автентифікації суб'єкта за голосом відповідно до умов експлуатації системи і заданого рівня конфіденційності процесу авторизації; забезпечити цілісність інформаційних ресурсів при заданому рівні конфіденційності інформаційної системи департаменту за рахунок оптимізації процесу резервування; оптимізувати правила системної політики безпеки інформаційної системи департаменту. В цілому, впроваджені авторські результати дозволили підвищити конфіденційність, цілісність, доступність інформаційної системи департаменту із збереженням попереднього рівня готовності і безвідмовності останньої. З моменту впровадження результатів авторських досліджень ситуацій порушення конфіденційності або цілісності інформаційних ресурсів у інформаційній системі департаменту зафіксовано не було. Доступність інформаційній системі департаменту у моменти інтенсивного звернення користувачів зросла на величину близько 20%. Результати оцінювання атрибутів гарантоздатності враховуються при плануванні процесу оновлення апаратної складової інформаційної системи департаменту.

Голова комісії _____ Д. П. Щеглов

Члени комісії: _____ О. О. Рознюк

_____ Д. С. Черненко

«ЗАТВЕРДЖУЮ»

КП «Вінницький інформаційний центр»

підпис С. С. Бригадир
П.І.Б. директора

АКТ

впровадження результатів дисертаційного дослідження
Ковтуна В'ячеслава Васильовича
на тему «Моделі гарантоздатності інформаційної системи критичного застосування із автентифікацією суб'єкта за голосом»

Комісія у складі:
Голова - начальник відділу електрозв'язку - Ратушний Ю. Я.;
посада, П.І.Б. голови комісії

Члени комісії: технік із системного адміністрування - Олійник В. В.; начальник відділу інформаційних технологій - Найдамюк К. В.;
посади, П.І.Б. членів комісії (2 особи)

склала цей акт про те, що в КП «Вінницький інформаційний центр» впроваджено і використовуються наукові та прикладні результати дисертаційного дослідження Ковтуна В. В. з метою захисту доступу до критично важливих даних і організації процесів у середовищі інформаційної системи підприємства.

Перед безпосереднім впровадженням автор продемонстрував ефективність запропонованого програмного засобу для автентифікації суб'єкта за індивідуальними властивостями його голосу на матеріалах загальнодоступних мовленнєвих корпусів RedDots (https://sites.google.com/site/thereddotsproject/) і CSTR (https://datashare.is.ed.ac.uk/handle/10283/2651). Постановку експерименту автор виконав аналогічно до описаного у підрозділі 4.3 монографії «Моделі атрибутів гарантоздатності інформаційної системи критичного застосування із автентифікацією суб'єкта за голосом», виданої у ВНТУ у 2020 р. Результати демонстраційного експерименту співпали із візуалізованими на рисунку 4.26 вищезгаданої монографії.

Для перевірки якісних показників модернізованої із використанням пропозицій Ковтуна В. В. інформаційної системи підприємства з інтервалом у місяць здійснювалося тестування реакції системної політики безпеки на прецеденти із бази типізованих атак, спрямованих на перевірку адекватності: - глобальної політики безпеки (атаки на вміст ролей користувачів, 5 видів атак); - локальної політики безпеки (атаки на процеси взаємодії апаратних та програмних складових інформаційної системи, в т.ч. на різних рівнях її

ієрархії, 12 видів атак); - дискреційної політики безпеки (атаки зі спробою автентифікації несанкціонованих суб'єктів за паролем, індивідуальними параметрами голосу та із комбінацією перелічених варіантів тощо, 6 видів атак). Загальна кількість типів атак у базі складала 23. Кількість функцій інформаційної системи підприємства, що описувалися відповідними системними контурами різного порядку, і підтримували розв'язання задач збирання, реєстрації, збереження, оброблювання, актуалізації та представлення суб'єктам-користувачам критично важливих даних інформаційної системи, складала 41. Кількість ознак, значення яких оцінювалися класифікаторами для ідентифікації типів атак, становила 9. Кількість реалізацій атак за сеанс тестування складала 100 разів для кожного із типів, при цьому 40% значень ознак було використано для оптимізації системної політики безпеки. Поріг чутливості класифікаторів для виявлення факту атаки, враховуючи критичне застосування ІС, встановлювався рівним 0.005. На основі проведених експериментів виявилось, що модернізація інформаційної системи підприємства дозволила покращити значення оцінок готовності, наробки на відмову, обслуговуваності, живучості, функціональної безпеки, безвідмовності на 7-15% із визначеними 95% довірчими інтервалами для значень цих характеристик.

Загалом, модернізована із застосуванням авторських моделей і методів інформаційна система підприємства протягом 2019 р. успішно протидіяла спробам несанкціонованого доступу до критично важливих даних, підтримувала їх цілісність і доступність для авторизованих користувачів. Здійснене за авторським методом оцінювання надійності інформаційної системи підприємства дозволило оптимізувати процес оновлення матеріальної бази інформаційної системи і заощадити кошти.

Цей акт не є підставою для отримання грошової винагороди.

Голова комісії _____ Ратушний Ю.М.
підпис П.І.Б.

Члени комісії: _____ Майданюк К.В.
підпис П.І.Б.

_____ Осейчик В.В.
підпис П.І.Б.

МОЗ України
Департамент охорони здоров'я та курортів Вінницької ОДА
ВІННИЦЬКИЙ ОБЛАСНИЙ ЦЕНТР МЕДИКО-СОЦІАЛЬНОЇ ЕКСПЕРТИЗИ
Ідентифікаційний код 20097160
21029, м. Вінниця,
вул. Хмельницьке шосе, 92
тел. (0432) 69-70-41

ЗАТВЕРДЖУЮ
Вінницький Обласний
установа
Центр Медико-соціальної експертизи
Вінницька Міська МСЕК №2

підпис Антонюк Н. А.
П.І.Б. керівника

АКТ
впровадження результатів дисертаційного дослідження
Ковтуна В'ячеслава Васильовича
на тему
«Моделі гарантоздатності інформаційної системи критичного застосування із автентифікацією суб'єкта за голосом»

Комісія у складі:
Голова - Антонюк Н. А. Голова Вінницької Міської МСЕК №2
посада, П.І.Б. голови комісії
;

Члени комісії: Марусяк Д. А. - лікар-терапевт Вінницької Міської МСЕК №2; Лунина О. Ї. лікар-невропатолог Вінницької Міської МСЕК №2
посади, П.І.Б. членів комісії (2 особи)

склала цей акт про те, що в Вінницькій Міській Медико-соціально експертній комісії №2
назва установи

впроваджено наукові і прикладні результати дисертаційного дослідження Ковтуна В. В. на вищезгадану тему для оптимізації захисту інформації, організації сервісних процесів та оцінювання функціональних характеристик інформаційної системи установи із виділеними інформаційними ресурсами критичної важливості.

Впроваджені результати дозволили виявити і виправити недоліки у політиці безпеки інформаційної системи установи, налаштування якої не були розраховані на довготривалу експлуатацію системи в умовах інтенсивного звернення користувачів. Організоване за авторським методом оцінювання доступності інформаційної системи установи виявило її потенційну вразливість, пов'язану із недостатнім резервуванням апаратних ресурсів на заходи безпеки, оцінюване у 30-40%. Результати теоретичного оцінювання показників безвідмовності, готовності, обслуговуваності, інтенсивності відмов, наробки на відмову, функціональної безпеки, живучості не вийшли за межі довірчих інтервалів при порівнянні із фактичними показниками результатів експлуатації інформаційної системи

установи протягом 2019 р. Впровадження авторської технології двохетапної авторизації суб'єктів із урахуванням індивідуальних особливостей їх голосів зробив процедуру авторизації користувачів для доступу до критично важливих інформаційних ресурсів менш комфортною, але дозволив запобігти сіми спробам порушення конфіденційності інформаційної системи установи протягом 2019 р.

Даний акт не є підставою для взаємних фінансових розрахунків.

Голова комісії _____ Антонюк Н.І.
підпис П.І.Б.

Члени комісії: _____ Марусяк Д.А.
підпис П.І.Б.

_____ Луняка О.І.
підпис П.І.Б.

Департамент охорони здоров'я Вінницької міської ради
Комунальне некомерційне підприємство
«Центр первинної медико-санітарної допомоги №3 м. Вінниці»
Ідент. код 25502352
Хмельницьке шосе, 96
Тел.(факс):46-74-19
«____» _____ 20___ р.
№_____

ЗАТВЕРДЖУЮ

КНП ЦПМСД №3 м. Вінниці
назва установи

Департамент охорони здоров'я Вінницької міської ради Комунальне некомерційне підприємство «ЦЕНТР ПЕРВИННОЇ МЕДИКО-САНІТАРНОЇ ДОПОМОГИ №3 М. ВІННИЦІ» 25502352 Україна

підпис П.І.Б. керівника

АКТ

впровадження результатів дисертаційної роботи
Ковтуна В'ячеслава Васильовича
для здобуття наукового ступеня доктора технічних наук

Комісія у складі:
Голова - заступник медичного директора
посада, П.І.Б. голови комісії
КНП ЦПМСД №3 м. Вінниці Шкільова І.В.

Члени комісії: зав. амбулаторією Сотченко Г.В.
посади, П.І.Б. членів комісії (2 особи)
секретар ЛКК Загубіна О.В.;

склала цей акт про те, що в _____
назва установи

впроваджено у використання результати реалізованого з метою набуття наукового ступеня доктора технічних наук дисертаційного дослідження Ковтуна В. В. на тему «Моделі гарантоздатності інформаційної системи критичного застосування із автентифікацією суб'єкта за голосом». Впровадження стосувалося підвищення показників гарантоздатності інформаційної системи установи та удосконалення структури і організації підсистеми захисту останньої.

На початковому етапі впровадження, яке розпочалося 04.03.2019 р., автор розрахував показники готовності, наробки на відмову, обслуговуваності, живучості, функціональної безпеки, безвідмовності для вихідної конфігурації апаратного і програмного забезпечення інформаційної системи установи, на основі якого рекомендував наростити обчислювальну потужність інформаційної системи на 23%, адже аналіз логів мережевої її складової з початку 2019 р. зафіксував окремі неперіодичні факти відмови у наданні доступу авторизованим користувачам з причини перевантаження процесорів або пам'яті роутерів мережі. Втім, застосувавши авторський метод оптимізації політики безпеки, вдалося налаштувати QoS-правила роутерів інформаційної системи так, що проблем із доступністю інформаційної системи на протязі всього цензурованого часу її експлуатації (по 30.12.2019 р. включно) зафіксовано не було ні авторизованими

користувачами ні програмно. В результаті вдалося заощадити кошти на модернізацію обладнання.

Також процес авторизації користувачів для отримання доступу до критично важливих ресурсів інформаційної системи установи було посилено введенням авторської схеми двохфакторної верифікації із автентифікацією суб'єкта за голосом як другого фактору. Адекватність удосконаленого таким чином процесу авторизації окрім фактичними результатами експлуатації перевірялася раз на місяць за результатами контрольованого експерименту, який полягав у верифікації 50% довільно вибраних фонограм мовних сигналів, взятих із контрольної вибірки, у яку увійшли 40% мовних матеріалів із спеціалізованих мовних корпусів RedDots і Centre for Speech Technology Research English Multi-speaker Corpus, 60% мовного матеріалу яких було використано для навчання системи верифікації, здійсненого 04.03.2019 р. Найнижча зафіксована усереднена достовірність верифікації суб'єктів з мовних корпусів за результатами десяти контрольованих експериментів склала понад 98% із визначеними 99% довірчими інтервалами для значень цієї характеристики. Експлуатація системи показала, що для підтримування достовірності верифікації реальних суб'єктів-користувачів на високому рівні перенавчання системи необхідно повторювати з періодичністю у два тижні, що спричиняло певний дискомфорт, тому обмеження застування удосконаленої схеми верифікації лише для управління доступом до критично важливих ресурсів інформаційної системи установи виявилося раціональним.

Цей акт не є підставою для отримання грошової винагороди.

Голова комісії _____ підпис _____ П.І.Б.

Члени комісії: _____ підпис _____ П.І.Б.

_____ підпис _____ П.І.Б.

ЗАТВЕРДЖУЮ»
Директор товариства з обмеженою відповідальністю «АГРО-ПРОМСЕРВІС»
_____Піонткевич І. В.
_____ 20___ р.

АКТ ВПРОВАДЖЕННЯ РЕЗУЛЬТАТІВ
дисертаційної роботи Ковтуна В'ячеслава Васильовича
на тему «Методологія синтезу інформаційної технології для оптимізації у таксономії гарантоздатності інформаційної системи критичного застосування із автентифікацією суб'єкта за голосом»

Комісія у складі голови - директора ТОВ «АГРО-ПРОМСЕРВІС» Піонткевича І. В., та членів комісії - інженера Рильського І. А., та інженера Білого П. А., склала цей акт про те, що в ТОВ «АГРО-ПРОМСЕРВІС», Вінницька обл., м. Немирів, вул. Горького, 94, каб. 9, https://agropromservis.net.ua/, апробовано отримані Ковтуном В. В. в процесі дисертаційного дослідження практичні і наукові результати, зокрема, для посилення інформаційної безпеки, функціональної спроможності і надійності інформаційної системи установи.

Посилення інформаційної безпеки досягнуто реалізацією двохетапної схеми автентифікації користувача для захисту процедури персоніфікованого доступу до критично важливих даних. На першому етапі цієї схеми користувач автентифікується за співпадінням пари «логін»-«пароль», а на другому етапі – верифікується за результатами аналізу фонограми із виголошеною парольною фразою тривалістю 10-15 с. Набір слів, які утворювали парольну фразу, генерується системою управління доступом випадково для кожного сеансу автентифікації. Змістовно склад парольної фрази обиралися із попередньо сформованого репрезентативного за вмістом і обсягом словника (понад 1000 іменників, дієслів і прикметників). Аналогічно описаному організовано процес навчання системи управління процедури персоніфікованого доступу до критично важливих даних установи за виключенням того, що тривалість начальної фрази досягала 2 хв. У коло осіб, які мали доступ до критично важливих даних установи входило 41 особа привілеї яких обмежувалися лише переглядом даних (тип «користувач»), 7 осіб привілеї яких дозволяли перегляд, додавання і редагування даних (тип «модератор»), 2 особи привілеї яких на додачу до перелічених сервісів дозволяли також ініціювати процедуру реєстрації нових користувачів (тип «адміністратор»). Процедура верифікації передбачала або підтвердження особи користувача, який автентифікувався, або ні. За цензурований період експлуатації описаної системи управління доступом з 01.01.2020 р. по 01.06.2020 р. було здійснено понад 33000 сеансів автентифікації, за результатами яких усереднена імовірність виникнення похибки першого роду склала 1,32%, а усереднена імовірність виникнення похибки другого роду склала 2,02% із визначеними 99% довірчими інтервалами для значень цих характеристик. Детальніше процедуру організації двохетапної схеми

автентифікації користувача для захисту процедури персоніфікованого доступу до критично важливих даних описано у четвертому розділі монографії В.В. Ковтуна «Моделі атрибутів гарантоздатності інформаційної системи критичного застосування із автентифікацією суб'єкта за голосом».

Посилення функціональної спроможності було досягнуто оптимізацією налаштувань правил QoS технології у операційному середовищі роутерів інформаційної системи установи. Параметри налаштувань були розраховані за допомогою авторського методу, який описаний у п'ятому розділі вищезгаданої монографії, для чотирьох типів акаунтів: «користувач», «модератор», «адміністратор», «не авторизований», де перші три типи аккаунтів мають привілеї доступу до критично важливих даних, а четвертий тип – ні. Відповідно, здійснені налаштування забезпечили першочерговий доступ до інформаційної системи авторизованим користувачам, аккаунти яких належали до перших трьох типів. За цензурований період експлуатації модифікованої інформаційної системи установи фактів несанкціонованого переривання сеансів доступу до критично важливих даних для авторизованих користувачів із акаунтами санкціонованих типів зафіксовано не було навіть в умовах періодично емульованих розподілених DoS-атаках на мережеву компоненту інформаційної системи установи.

Посилення надійності інформаційної системи установи втілено у формі графіку рекомендованого оновлення її апаратної компоненти, у якому враховано розраховані за авторськими методами оцінки таких параметрів як готовність, наробка на відмову, обслуговуваність, живучість, функціональна безпека, безвідмовність. За цензурований період теоретичні оцінки цих параметрів відхилялися від фактичних не більше ніж на 3,5% із визначеними 95% довірчими інтервалами для значень згаданих параметрів.

Цей акт не є підставою для отримання грошової винагороди чи укладання додаткових угод.

Голова комісії _____ Піонткевич І. В.
підпис

Члени комісії: _____ Рильський І. А.
підпис

_____ Білий П. А.
підпис

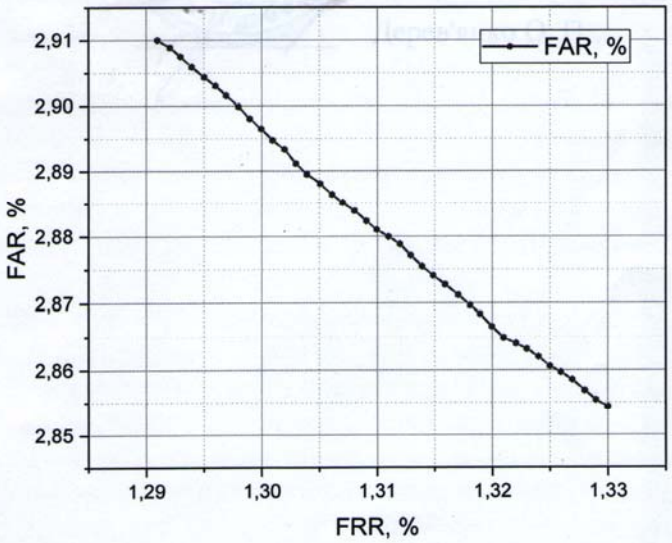
«ЗАТВЕРДЖУЮ»
Директор товариства з обмеженою відповідальністю «Вінницяелектроконтакт»
_____ Паламарчук В. М.
"____" _____ 2020 р.

АКТ ВПРОВАДЖЕННЯ РЕЗУЛЬТАТІВ
дисертаційної роботи Ковтуна В'ячеслава Васильовича
на тему «Методологія синтезу інформаційної технології для оптимізації у таксономії гарантоздатності інформаційної системи критичного застосування із автентифікацією суб'єкта за голосом»

Комісія у складі голови - директора ТОВ «Вінницяелектроконтакт» Паламарчука В. М., та членів комісії - заступника директора Довгалюка Р. А., та інженера Дерев'янко О. П., склала цей акт про те, що в ТОВ «Вінницяелектроконтакт», м. Вінниця, вул. Пірогова 151а, оф.21, https://www.elektrokontakt.com.ua, апробовано наукові і прикладні результати, отримані Ковтуном В. В. в процесі здійснення дисертаційного дослідження.

Результатами впровадження є посилення інформаційної безпеки, функціональної спроможності і надійності інформаційної системи установи. Посилення інформаційної безпеки досягнуто впровадженням двохетапної схеми автентифікації користувача для доступу до критично важливих даних установи. На першому етапі цієї схеми користувач персоніфікувався за схемою авторизації виду «логін»-«пароль». На другому етапі впровадженої схеми користувач верифікувався за результатами аналізу фонограми із виголошеною парольною фразою тривалістю 10 с. Змістовний склад парольної фрази для верифікації за голосом генерувався автоматично і випадково на основі заданого репрезентативного словника, який містить близько 1000 іменників, дієслів і прикметників. Перед початком експлуатації систему верифікації було навчено на фонограмах із мовними матеріалами цільових користувачів тривалістю близько 2 хв. Вміст бази даних установи було сегментовано на загальну і конфіденційну частини. В останній, зокрема, зберігалися персональні дані співробітників, фінансова інформація, логістична інформація, оцифровані версії уставних документів та договорів із партнерами. Персоніфікований доступ до загального сегменту бази даних установи міг ініціюватися за протоколом HTTPS зі спеціалізованого пристрою із довільною MAC- та IP-адресою. Персоніфікований доступ до конфіденційного сегменту бази даних установи міг ініціюватися за протоколом HTTPS зі спеціалізованого пристрою із MAC- та IP-адресою, які входили до пулу дозволених адрес. У коло осіб, які мали доступ до конфіденційного сегменту бази даних установи входило: 63 особа привілеї яких обмежувалися лише переглядом даних (тип «користувач»); 15 осіб привілеї яких дозволяли перегляд, додавання і редагування даних (тип

«менеджер»); 2 особи привілеї яких на додачу до перелічених сервісів дозволяли також ініціювати процедуру реєстрації нових користувачів із привілеями доступу до конфіденційних даних (тип «керівник»). Процедура верифікації передбачала або підтвердження особи користувача, який автентифікується, або ні. За цензурований період експлуатації інформаційної системи установи із вищеописаним захистом процедури доступу з 01.01.2019 р. по 01.06.2020 р. було здійснено понад 45000 сеансів автентифікації. Для оцінки отриманих емпіричних результатів використано метрику якісних показників, визначену у актуальному міжнародному стандарті ISO/IEC 2382-37:2012 Information technology – Vocabulary – Part 37: Biometrics. Зокрема, усереднена імовірність виникнення похибки першого роду (False Rejection Rate, FRR) склала 1,3%, а усереднена імовірність виникнення похибки другого роду (False Acceptance Rate, FAR) склала 2,75%. Із довірчою імовірність 99% визначено діапазони істинних значень імовірностей виникнення похибок першого і другого роду, відповідно: [1,30 ÷1,35], [2,60 ÷2,90], [%]. Далі наведено побудовану в системі координат FRR-FAR криву компромісного визначення похибки (Detection error tradeoff (DET) curve), яка деталізує вищеописані результати цензурованої експлуатації досліджуваної системи:



Посилення готовності інформаційної системи було досягнуто оптимізацією налаштувань правил QoS технології в операційному середовищі роутерів внутрішньої комп'ютерної мережі установи. Параметри налаштувань були розраховані за методом, описаним у розділі 5 монографії Ковтуна В. В., для чотирьох типів акаунтів: «користувач», «менеджер», «керівник», «гість», де перші три типи акаунтів мають привілеї доступу до конфіденційного сегменту бази даних установи, а четвертий тип – ні. Здійснені налаштування забезпечили першочерговий доступ до інформаційної системи авторизованим користувачам, акаунти яких належали до перших трьох типів. За цензурований період експлуатації модифікованої

інформаційної системи установи фактів несанкціонованого переривання сеансів доступу до критично важливих даних для авторизованих користувачів із акаунтами санкціонованих типів не зафіксовано (навіть в умовах періодично емульованих розподілених DoS-атаках на сегмент внутрішньої комп'ютерної мережі інформаційної системи установи, де зберігалися конфіденційні дані).

Для посилення обслуговуваності інформаційної системи установи розроблено графік рекомендованого оновлення її апаратних компонентів, у якому враховано оцінки базових параметрів гарантоздатності, розраховані на основі методів, описаних у 5-му розділі монографії Ковтуна В.В. За цензурований період теоретичні оцінки цих параметрів відхилялися від фактичних не більше ніж на 2% із визначеними 95% довірчими інтервалами для значень згаданих параметрів.

Цей акт не є підставою для отримання грошової винагороди чи укладання додаткових угод.

Голова комісії _____ Паламарчук В. М

Члени комісії: _____ Довгалюк Р. А.

_____ Дерев'янко О. П.

Додаток Н

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.