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

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 і β

EM-метод – метод максимізації правдоподібності

ERB – еквівалент-прямокутна шкала пропускання

FAR, β – імовірність хибного допуску

FRR, – 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.

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 А. 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 withhigh-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, *ЕМ-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.