Аналіз, оцінка та усунення ризиків в біометричних системах голосової автентифікації

Analysis, Assessment, and Mitigation of Risks in Voice Biometric Authentication Systems

Дмитро Сабодашко
Corresponding author: доктор філософії, старший викладач кафедри захисту інформації, e-mail: dmytro.v.sabodashko@lpnu.ua, ORCID ID: 0000-0003-1675-0976

Христина Руда
доктор філософії, доцент кафедри захисту інформації, e-mail: khrystyna.s.ruda@lpnu.ua, ORCID ID: 0000-0001-8644-411X

Юлія Оліярник
студент кафедри захисту інформації, e-mail: khrystyna.s.ruda@lpnu.ua, ORCID ID: 0009-0005-1018-651X

Андрій Нестор
студент кафедри захисту інформації, e-mail: khrystyna.s.ruda@lpnu.ua, ORCID ID: 0009-0004-1601-9598

Національний університет "Львівська політехніка", м. Львів, Україна

Dmytro Sabodashko
Corresponding author: Doctor of Philosophy, Senior Lecturer of Department of Information Security, e-mail: dmytro.v.sabodashko@lpnu.ua, ORCID ID: 0000-0003-1675-0976

Khrystyna Ruda
Doctor of Philosophy, Associate Professor of Department of Information Security, e-mail: khrystyna.s.ruda@lpnu.ua, ORCID ID: 0000-0001-8644-411X

Yuliia Oliiarnyk
Student of the Department of Information Security, e-mail: khrystyna.s.ruda@lpnu.ua, ORCID ID: 0009-0005-1018-651X

Andrii Nestor
Student of the Department of Information Security, e-mail: khrystyna.s.ruda@lpnu.ua, ORCID ID: 0009-0004-1601-9598

Lviv Polytechnic National University, Lviv, Ukraine

Received: December 23, 2025 | Revised: December 30, 2025 | Accepted: December 31, 2025

DOI: https://doi.org/10.33445/sds.2025.15.6.27

Мета роботи. Розробка та обґрунтування формалізованої методики комплексного аналізу й кількісної оцінки критичності ризиків у біометричних системах голосової автентифікації з урахуванням архітектурних особливостей embedding-моделей і адаптивного характеру сучасних кіберзагроз.

Метод дослідження. У роботі використано комплекс аналітичних, кількісних та прикладних методів дослідження, спрямованих на формалізований аналіз і пріоритезацію ризиків у біометричних системах голосової автентифікації з урахуванням особливостей їх архітектури та сучасного загрозового ландшафту. Основним методом дослідження є кількісно-аналітична оцінка критичності ризиків, що базується на модифікованій моделі управління ризиками.

Результати дослідження. Визначено, що найбільш критичними для систем голосової автентифікації є атаки із застосуванням синтезованого та клонованого мовлення, які характеризуються високими значеннями ймовірності, впливу та адаптивності. Показано, що інтеграція модуля виявлення життєдіяльності на основі аналізу нелінійних спектрально-фазових характеристик аудіосигналу дозволяє суттєво знизити інтегральний показник критичності deepfake-атак і перевести їх із критичного рівня до помірного або прийнятного.

Теоретична цінність дослідження. Полягає в розвитку підходів до формалізованого аналізу кіберризиків у біометричних системах шляхом урахування адаптивності сучасних атак. Запропонована модель розширює класичні підходи до оцінки безпеки біометричних систем, виходячи за межі традиційних точнісних показників FAR і FRR.

Практична цінність дослідження. Полягає в можливості використання запропонованої методики для пріоритезації загроз на етапі проєктування та програмної реалізації систем голосової біометричної автентифікації. Отримані результати можуть бути використані розробниками для обґрунтованого вибору захисних механізмів, зокрема модулів liveness detection, з метою підвищення кіберстійкості систем. полягає у формуванні комплексного підходу до оцінки критичності ризиків у системах голосової автентифікації, що поєднує архітектурний аналіз, кількісне оцінювання та обґрунтування програмних контрзаходів. Запропонований підхід створює основу для систематизації ризиків і підвищення

Purpose. To develop and substantiate a formalized methodology for comprehensive analysis and quantitative assessment of risk criticality in voice biometric authentication systems, taking into account the architectural features of embedding models and the adaptive nature of modern cyber threats.

Method. The study employs a combination of analytical, quantitative, and applied research methods aimed at the formalized analysis and prioritization of risks in voice biometric authentication systems, considering their architectural characteristics and the contemporary threat landscape. The core research method is a quantitative–analytical assessment of risk criticality based on a modified risk management model.

Findings. It has been determined that the most critical threats to voice authentication systems are attacks involving synthesized and cloned speech, which are characterized by high levels of probability, impact, and adaptability. It is shown that the integration of a liveness detection module based on the analysis of nonlinear spectral–phase characteristics of the audio signal makes it possible to significantly reduce the integral risk criticality of deepfake attacks and to shift them from a critical level to a moderate or acceptable one.

Theoretical implications. The theoretical contribution lies in advancing approaches to the formalized analysis of cyber risks in biometric systems by incorporating the adaptive nature of modern attacks. The proposed model extends classical approaches to biometric security assessment beyond traditional accuracy metrics such as FAR and FRR.

Practical implications. The practical significance of the research consists in the possibility of using the proposed methodology for threat prioritization at the design and software implementation stages of voice biometric authentication systems. The obtained results can be applied by developers to justify the selection of protective mechanisms, in particular liveness detection modules, in order to enhance the cyber resilience of such systems.

Value. The study contributes by forming a comprehensive approach to assessing risk criticality in voice authentication systems that combines architectural analysis, quantitative evaluation, and the substantiation of software-based countermeasures. The proposed approach provides a foundation for systematic risk

обґрунтованості інженерних рішень у сфері голосової біометрії.

Майбутні дослідження: Подальші дослідження доцільно спрямувати на автоматизацію оцінювання коефіцієнта адаптивності загроз, розширення набору ознак для виявлення синтезованого мовлення, а також експериментальну валідацію запропонованої методики на реальних промислових системах голосової автентифікації.

Тип статті. Аналітично-прикладне дослідження.

Ключові слова: Біометрична Автентифікація, Голосова Автентифікація, Аналіз Ризиків, Кіберстійкість, Deepfake-Атаки, Liveness Detection, Embedding-Моделі.

structuring and for improving the soundness of engineering decisions in the field of voice biometrics.

Future research. Further research should focus on automating the assessment of the threat adaptability coefficient, expanding the set of features for detecting synthesized speech, and experimentally validating the proposed methodology on real industrial voice authentication systems.

Papertype. Analytical and applied study.

Key words: Biometric Authentication, Voice Authentication, Risk Analysis, Cyber Resilience, Deepfake Attacks, Liveness Detection, Embedding Models.

Вступ

Інтенсивний розвиток інфокомунікаційних технологій та широке впровадження автоматизованих систем контролю доступу зумовлюють зростання вимог до надійності та безпеки механізмів автентифікації користувачів. Традиційні методи ідентифікації, що базуються на використанні паролів або фізичних носіїв, характеризуються високим рівнем уразливості до компрометації, що стимулювало активний розвиток біометричних систем автентифікації [1].

Серед різновидів біометричних технологій особливе місце посідає голосова автентифікація, яка вирізняється зручністю використання, можливістю віддаленої ідентифікації та простотою інтеграції в мобільні, хмарні та IoT-системи [2]. Сучасні системи автоматичної верифікації диктора ґрунтуються на застосуванні векторних представлень голосу (embedding-моделей), зокрема архітектур x-vector та i-vector, що забезпечують високі показники точності в умовах контрольованого середовища [3].

Водночас стрімкий розвиток генеративних нейронних мереж та технологій синтезу і клонування мовлення суттєво ускладнив загрозовий ландшафт систем голосової автентифікації. Поява атак із використанням синтетичного мовлення та deepfake-технологій призводить до зростання ризику несанкціонованого доступу навіть за умови високих значень традиційних точнісних показників, таких як FAR та FRR [4]. Це свідчить про обмеженість підходів, орієнтованих виключно на оцінювання продуктивності системи без урахування її кіберстійкості до адаптивних загроз [5].

У зв’язку з цим актуальною науково-практичною задачею є розробка методів комплексного аналізу ризиків у біометричних системах голосової автентифікації, які враховують не лише ймовірність реалізації загрози та її вплив, але й динаміку розвитку сучасних атак [6]. Це зумовлює необхідність формування кількісної методики оцінки критичності ризиків, орієнтованої на архітектуру сучасних систем голосової біометрії та особливості їх програмної реалізації.

Теоретичні основи дослідження

Дослідження у сфері біометричних систем автентифікації традиційно зосереджуються на оцінюванні точності розпізнавання, що визначає базовий рівень надійності системи. Найпоширенішими показниками ефективності є коефіцієнти помилкового прийняття (False Acceptance Rate, FAR) та помилкової відмови (False Rejection Rate, FRR), які широко використовуються для порівняльного аналізу різних біометричних технологій [7]. Високі значення FAR асоціюються з підвищеним ризиком несанкціонованого доступу, тоді як зростання FRR негативно впливає на зручність та доступність системи для легітимних користувачів [8].

У низці наукових робіт запропоновано багатокритеріальні підходи до вибору оптимального біометричного методу, зокрема із застосуванням методу аналізу ієрархій. Такі підходи дозволяють поєднувати точнісні показники з додатковими критеріями, включаючи зручність використання та апаратні вимоги [9]. Водночас результати подібних досліджень

свідчать, що голосова автентифікація за усередненими значеннями FAR та FRR часто поступається фізіологічним біометричним методам, зокрема ідентифікації за райдужною оболонкою ока, що обмежує її застосування у високозахищених системах [10].

Разом із тим зазначені підходи мають суттєве методологічне обмеження, оскільки ґрунтуються на середніх емпіричних значеннях, отриманих у контрольованих експериментальних умовах. Така оцінка не враховує впливу цілеспрямованих та адаптивних атак, характерних для реальних сценаріїв експлуатації систем голосової автентифікації, унаслідок чого ризики, пов'язані з компрометацією біометричних механізмів, залишаються поза межами формалізованого аналізу [11].

Сучасні системи автоматичної верифікації диктора переважно базуються на embedding-моделях, таких як x-vector та i-vector, які забезпечують масштабованість і високу продуктивність [12]. Дослідження, присвячені аналізу таких архітектур, зосереджуються переважно на питаннях точності, обчислювальної складності та масштабованості. Водночас у цих роботах, як правило, відсутня формалізована методика оцінки ризиків, пов'язаних із властивостями embedding-простору, зокрема ризиків model inversion, model extraction або зміщення векторних представлень унаслідок адверсаріальних впливів [13].

Окрему групу досліджень становлять роботи, присвячені аналізу стійкості систем голосової автентифікації до спотворень аудіосигналу. У таких роботах розглядається вплив шумів, варіацій тембру та умов запису на якість розпізнавання диктора [14]. Хоча ці дослідження є важливими для забезпечення робастності системи, вони здебільшого орієнтовані на природні спотворення та не охоплюють умисні атаки, зокрема атаки із застосуванням синтезованого мовлення або технологій клонування голосу.

Стрімкий розвиток генеративних моделей мовлення призвів до появи нових класів загроз, які суттєво підвищують ризик несанкціонованого доступу до систем голосової автентифікації. Дослідження, присвячені спуфінг-атакам і deepfake-технологіям, підтверджують високу ефективність таких атак щодо сучасних ASV-систем [15]. Разом із тим у більшості робіт основна увага зосереджується на розробці окремих захисних механізмів без кількісного обґрунтування критичності відповідних ризиків та їх пріоритетності для програмної реалізації.

Таким чином, аналіз сучасних наукових публікацій засвідчує наявність методологічної прогалини, що полягає у відсутності комплексної кількісної системи оцінки критичності ризиків у біометричних системах голосової автентифікації. Існуючі підходи не забезпечують формалізованої пріоритезації загроз з урахуванням їх адаптивного характеру та специфіки сучасних embedding-архітектур, що ускладнює прийняття обґрунтованих рішень щодо вибору та реалізації захисних механізмів.

Постановка проблеми

Проведений аналіз сучасних наукових досліджень у сфері біометричних систем голосової автентифікації засвідчив, що існуючі підходи до оцінки безпеки таких систем є методологічно обмеженими. Переважна більшість робіт зосереджується на аналізі точнісних характеристик, зокрема показників FAR та FRR, або на використанні експертних багатокритеріальних методів, які не враховують специфіку та динаміку сучасних кіберзагроз.

Сучасні системи автоматичної верифікації диктора, побудовані на основі embedding-моделей голосу, характеризуються підвищеною складністю та масштабованістю, що водночас зумовлює появу нових класів ризиків. До таких ризиків належать атаки із застосуванням синтезованого та клонованого мовлення, адверсаріальні впливи на embedding-простір, а також атаки, спрямовані на компрометацію біометричних шаблонів. Зазначені загрози мають адаптивний характер і здатні еволюціонувати разом із розвитком методів захисту, що не відображається в межах традиційних статичних моделей оцінки безпеки.

Відсутність формалізованої кількісної методики оцінки критичності ризиків у біометричних системах голосової автентифікації унеможливлює обґрунтовану пріоритезацію загроз на етапі програмної реалізації. У результаті заходи захисту впроваджуються фрагментарно, без чіткого зв'язку між рівнем ризику та складністю відповідних програмних рішень, що негативно впливає на загальну кіберстійкість системи.

Таким чином, науково-практична проблема, що розглядається у статті, полягає у відсутності комплексного підходу до кількісного аналізу та пріоритезації ризиків у біометричних системах голосової автентифікації з урахуванням адаптивності сучасних атак і архітектурних особливостей embedding-моделей. Розв'язання цієї проблеми є необхідною передумовою для проєктування та програмної реалізації ефективних і стійких до сучасних загроз систем голосової біометрії.

Метою даної наукової статті є розробка та обґрунтування методики комплексного аналізу і кількісної оцінки критичності ризиків у біометричних системах голосової автентифікації з урахуванням адаптивності сучасних загроз і особливостей архітектур на основі embedding-моделей.

Для досягнення поставленої мети у роботі необхідно розв'язати такі завдання:

1. провести аналіз сучасних наукових підходів до оцінки безпеки біометричних систем голосової автентифікації та виявити їх методологічні обмеження;

2. здійснити класифікацію основних ризиків, характерних для систем голосової автентифікації, з урахуванням архітектурних рівнів їх реалізації;

3. розробити кількісну модель оцінки критичності ризиків, що поєднує показники ймовірності реалізації загрози, її впливу та адаптивності;

4. виконати оцінювання критичності основних ризиків для систем голосової автентифікації на основі запропонованої методики;

5. обґрунтувати програмні підходи до усунення або мінімізації найбільш критичних ризиків та оцінити їх вплив на рівень кіберстійкості системи.

Методологія дослідження

Методологія дослідження спрямована на формування формалізованого підходу до аналізу та пріоритезації ризиків у біометричних системах голосової автентифікації з урахуванням архітектурних особливостей сучасних ASV-систем і динамічного характеру сучасних кіберзагроз. На відміну від традиційних підходів, орієнтованих виключно на показники точності, запропонована методика забезпечує підтримку прийняття інженерних рішень на етапі програмної реалізації системи.

Для забезпечення системного аналізу ризики класифікуються відповідно до рівня їх впливу на архітектуру системи голосової автентифікації:

1. Ризики рівня вхідних даних, спрямовані на маніпуляцію аудіосигналом, що подається на вхід системи (replay-атаки, атаки із застосуванням синтезованого або клонованого голосу).

2. Ризики рівня моделі та алгоритмів, пов'язані з компрометацією embedding-моделей або механізмів прийняття рішень (adversarial examples, model inversion, data poisoning).

3. Ризики інфраструктурного рівня, що стосуються зберігання та передавання біометричних даних (перехоплення трафіку, витік embedding-шаблонів, компрометація серверної частини).

У межах даного дослідження основну увагу зосереджено на ризиках перших двох рівнів, оскільки вони є найбільш специфічними для програмної реалізації біометричних систем голосової автентифікації та безпосередньо впливають на їх кіберстійкість [16].

Для оцінки критичності ризиків використовується модифікована кількісно-якісна модель, що базується на класичному підході до управління ризиками. Базова оцінка ризику визначається як добуток ймовірності реалізації загрози та впливу її наслідків:

$$R_{\text{баз}} = P \cdot I, \quad (1)$$

де P — ймовірність реалізації ризику;
I – рівень впливу на систему у разі реалізації загрози.

Обидва параметри оцінюються за п’ятибальною порядковою шкалою, де 1 відповідає мінімальному, а 5 — максимальному рівню [17].

Однак використання статичної моделі $R_{\text{баз}}$ є недостатнім для адекватної оцінки сучасних загроз, що мають адаптивний характер і здатні еволюціонувати разом із розвитком захисних механізмів. З цією метою у методиці вводиться додатковий коефіцієнт адаптивності загрози A, який відображає динаміку розвитку атаки, складність її виявлення та потребу в постійному оновленні захисних механізмів [18].

Коефіцієнт A набуває таких значень:

- $A = 1$ — статичні ризики, які можуть бути усунені за допомогою фіксованих програмних або організаційних заходів;
- $A = 2$ — динамічні ризики, що характеризуються швидкою еволюцією та потребують інтеграції складних адаптивних захисних механізмів.

З урахуванням коефіцієнта адаптивності повна оцінка критичності ризику визначається як:

$$R = P \cdot I \cdot A. \quad (2)$$

Запропонована модель не претендує на абсолютну метричну точність, а використовується як інструмент формалізованої пріоритезації ризиків у процесі проєктування та програмної реалізації системи голосової автентифікації. Такий підхід відповідає практиці адаптації стандартів управління ризиками (зокрема ISO/IEC 27005 [19]) до специфіки прикладних кіберфізичних систем.

На основі отриманого значення R ризикам присвоюється рівень критичності:

- $R \leq 10$ — низький ризик (контрольований);
- $11 \leq R \leq 20$ — помірний ризик (потребує моніторингу);
- $21 \leq R \leq 40$ — високий ризик (потребує додаткових заходів безпеки);
- $R > 40$ — критичний ризик (необхідне негайне усунення).

Застосування цієї методики дозволяє забезпечити обґрунтовану пріоритезацію загроз та визначити напрями програмної реалізації захисних механізмів відповідно до реального рівня ризику.

Оцінка ризиків системи голосової автентифікації

Оцінка ризиків системи голосової автентифікації здійснювалась відповідно до запропонованої кількісно-якісної методики, що базується на моделі:

$$R = P \cdot I \cdot A.$$

Оцінювання параметрів P, I та A виконувалось за п’ятибальною порядковою шкалою з урахуванням доступності атакуючих інструментів, потенційних наслідків для конфіденційності, цілісності та доступності системи, а також здатності загрози еволюціонувати з часом. На основі отриманих значень визначався інтегральний показник критичності ризику R та відповідний рівень ризику.

Результати оцінювання основних ризиків, характерних для сучасних біометричних систем голосової автентифікації, наведено в таблиці 1. Для кожного ризику також наведено приклади основних заходів усунення або мінімізації та повторну оцінку критичності після впровадження відповідних захисних механізмів.

Таблиця 1 – Оцінка критичності ризиків у системі голосової автентифікації

№ з/п	Тип атаки / ризику	*P* (до)	*I* (до)	*A* (до)	*R* (до)	Основні заходи усунення	*P* (після)	*I* (після)	*R* (після)	Рівень ризику після
1	Replay-атака (відтворення голосу)	4	3	1	12	Challenge response, аналіз акустики, часові кореляції	2	2	4	Низький
2	Deepfake / синтез голосу (TTS)	5	5	2	50	Liveness Detection, CQCC, ensemble, challenge-response	2	2	8	Середній
3	Adversarial examples	3	4	2	24	Adversarial training, input sanitization, anomaly detection	2	3	12	Середній
4	Data poisoning	2	5	2	20	Контроль цілісності датасетів, підписані моделі	1	3	3	Низький
5	Model inversion / extraction	3	4	2	24	Differential privacy, обмеження API-відповідей	2	2	8	Середній
6	Витік embedding-шаблонів	3	5	1	15	Шифрування (AES-GCM), TEE/HSM, cancellable transforms	1	3	3	Низький
7	MITM / мережеві атаки	3	4	1	12	TLS 1.3, certificate pinning, перевірка таймштампів	1	3	3	Низький
8	Voice conversion	4	4	2	32	Liveness detection, спектрально-фазовий аналіз, рандомні команди	2	2	8	Середній
9	Фішинг / соціальна інженерія	4	3	1	12	Освітні заходи, перевірка контексту, поведінковий аналіз	2	2	4	Низький
10	Вразливості серверів / ескалація прав	3	5	1	15	Пентест, контроль оновлень, сегментація мережі	1	3	3	Низький

Аналіз результатів, наведених у таблиці 1, засвідчує, що найбільш критичними для системи голосової автентифікації є ризики, пов’язані з використанням синтезованого та клонованого голосу. Зокрема, deepfake-атаки та атаки на основі voice conversion характеризуються високими значеннями ймовірності реалізації та впливу, а також підвищеним коефіцієнтом адаптивності, що зумовлює їх високий інтегральний показник критичності.

Deepfake-атака має максимальне значення показника R, що свідчить про її критичний характер і необхідність негайного усунення на етапі програмної реалізації системи. Висока оцінка коефіцієнта адаптивності для цього типу загроз пояснюється стрімким розвитком генеративних моделей мовлення та постійним удосконаленням методів обходу традиційних механізмів захисту.

На відміну від цього, класичні replay-атаки та інфраструктурні загрози, такі як перехоплення трафіку або компрометація серверної частини, характеризуються нижчим рівнем критичності. Це зумовлено їх відносно статичним характером і наявністю добре відпрацьованих програмних та організаційних механізмів захисту, що дозволяють ефективно знижувати ймовірність та вплив таких ризиків.

Повторна оцінка ризиків після впровадження запропонованих заходів захисту демонструє суттєве зниження інтегрального показника критичності для всіх розглянутих загроз. Особливо помітний ефект спостерігається для deepfake-атак, для яких впровадження спеціалізованих механізмів виявлення життєдіяльності дозволяє перевести ризик із критичної зони до прийнятного або помірного рівня.

Отримані результати підтверджують доцільність використання запропонованої методики для формалізованої пріоритезації ризиків у біометричних системах голосової автентифікації та створюють підґрунтя для обґрунтування вибору програмних захисних механізмів.

Результати

За результатами застосування розробленої методики кількісної оцінки критичності ризиків встановлено, що для сучасних біометричних систем голосової автентифікації домінуючими загрозами є атаки із застосуванням синтезованого та клонованого мовлення, які поєднують високу ймовірність реалізації, значний вплив на безпеку системи та адаптивний характер.

Запропонована модель оцінювання дозволила формалізувати пріоритетність таких загроз і обґрунтувати доцільність їх усунення саме на етапі програмної реалізації системи. Зокрема, інтеграція спеціалізованих механізмів виявлення життєдіяльності як окремого архітектурного модуля забезпечує істотне зниження критичності deepfake-атак без погіршення функціональних характеристик системи автентифікації.

Отримані результати підтверджують, що перехід від оцінювання безпеки виключно за точнісними показниками до комплексного аналізу ризиків створює підґрунтя для прийняття обґрунтованих інженерних рішень щодо вибору та реалізації програмних механізмів захисту.

Висновки

У роботі розроблено та обґрунтовано формалізовану методику комплексного аналізу і кількісної оцінки критичності ризиків у біометричних системах голосової автентифікації, яка базується на модифікованій моделі управління ризиками з урахуванням ймовірності, впливу та адаптивності сучасних загроз.

Запропонований підхід дозволяє подолати обмеження традиційних методів оцінювання безпеки, що ґрунтуються виключно на точнісних показниках FAR та FRR, і забезпечує формалізовану пріоритезацію загроз з урахуванням архітектурних особливостей embedding-моделей голосу.

За результатами кількісної оцінки встановлено, що атаки із застосуванням синтезованого та клонованого мовлення (deepfake та voice conversion) мають найвищий рівень критичності для сучасних систем голосової автентифікації, що зумовлює необхідність їх пріоритетного усунення на етапі програмної реалізації системи.

Обґрунтовано програмний підхід до зниження критичності найбільш небезпечних загроз шляхом інтеграції модуля виявлення життєдіяльності на основі аналізу нелінійних спектрально-фазових характеристик аудіосигналу, що забезпечує істотне зменшення інтегрального показника ризику deepfake-атак.

Отримані результати підтверджують практичну доцільність використання розробленої методики як інструменту підтримки інженерних рішень при проєктуванні та програмній реалізації кіберстійких систем голосової біометричної автентифікації та створюють підґрунтя для подальшої автоматизації оцінки адаптивних кіберризиків.

Фінансування

Це дослідження не отримало конкретної фінансової підтримки.

Конкуруючі інтереси

Автори заявляють, що у них немає конкуруючих інтересів.

Список використаних джерел

1. Скорик Ю., Безрук В. Вибір переважного методу біометричної автентифікації / Ю. Скорик, В. Безрук // International Science Journal of Engineering & Agriculture. — 2023. — Т. 2, № 4. — С. 28–34. — https://doi.org/10.46299/j.isjea.20230204.04.
2. Adelusi J. Voice Biometrics for Authentication: A Comprehensive Exploration [Електрон. ресурс] / J. Adelusi. — 2024. — Режим доступу: https://www.researchgate.net/publication/387060240_Voice_Biometrics_for_Authentication_A_Comprehensive_Exploration (дата звернення: 30.11.2025)
3. Самофал А. (2022). Система біометричної ідентифікації та аутентифікації персоналу на промислових об'єктах : автореф. дис. … канд. техн. наук. Київ, 113 с.
4. Руда, Х. (2025). Дослідження масштабованості систем біометричної автентифікації на основі ембеддінгів голосу. *Social Development and Security*, *15*(1), 161-170. https://doi.org/10.33445/sds.2025.15.1.15
5. Філоненко П., Винокурова О. (2011). Аналіз біометричних систем автентифікації та ідентифікації з використанням гібридних інтелектуальних методів для захисту від несанкціонованого доступу // Радіотехніка, № 166.
6. Ruda K., et al. (2024). Comparison of Digital Signal Processing Methods and Deep Learning Models in Voice Authentication. *Cybersecurity: Education, Science, Technique*, 1(25), 140–160.
7. Jain A. K., Ross A., Prabhakar S. (2004). An introduction to biometric recognition. *IEEE Transactions on Circuits and Systems for Video Technology*, 14(1), 4–20.
8. ISO/IEC 2382-37:2017. Information technology — Vocabulary — Part 37: Biometrics.
9. Saaty T. L. (2008). Decision making with the analytic hierarchy process. *International Journal of Services Sciences*, 1(1), 83–98.
10. Daugman J. (2004). How iris recognition works. IEEE Transactions on Circuits and Systems for Video Technology, 14(1), 21–30.
11. Galbally J., Marcel S., Fierrez J. (2014). Biometric antispoofing methods: A survey in face recognition. IEEE Access, 2, 1530–1552. https://doi.org/10.1109/ACCESS.2014.2322355.
12. Snyder D., Garcia-Romero D., Sell G., Povey D., Khudanpur S. (2018). X-vectors: Robust DNN embeddings for speaker recognition. Proceedings of ICASSP, 5329–5333.
13. Biggio B., Roli F. (2018). Wild patterns: Ten years after the rise of adversarial machine learning. Pattern Recognition, 84, 317–331. https://doi.org/10.1016/j.patcog.2018.07.023.
14. Kinnunen T., Li H. (2010). An overview of text-independent speaker recognition: From features to supervectors. Speech Communication, 52(1), 12–40. https://doi.org/10.1016/j.specom.2009.08.010.
15. Wu Z., Evans N., Kinnunen T., Yamagishi J., Alegre F., Li H. (2015). Spoofing and countermeasures for speaker verification: A survey. Speech Communication, 66, 130–153. https://doi.org/10.1016/j.specom.2015.02.007.
16. Behl A., Behl K. (2017). Cyberwar, cyberterrorism and cybercrime: A review. Journal of Global Information Technology Management, 20(3), 190–203. https://doi.org/10.1080/1097198X.2017.1364669.
17. ISO/IEC 27005:2018. Information technology – Security techniques – Information security risk management.
18. Ruan K. (2017). Introducing cybernomics: A unifying economic framework for measuring cyber risk. Computers & Security, 65, 77–89. https://doi.org/10.1016/j.cose.2016.12.004.

References

1. Skoryk, Y., & Bezruk, V. (2023). Selection of the preferred biometric authentication method. *International Science Journal of Engineering & Agriculture, 2*(4), 28–34. https://doi.org/10.46299/j.isjea.20230204.04
2. Adelusi, J. (2024). *Voice biometrics for authentication: A comprehensive exploration*. https://www.researchgate.net/publication/387060240_Voice_Biometrics_for_Authentication_A_Comprehensive_Exploration
3. Samofal, A. (2022). *System of biometric identification and authentication of personnel at industrial facilities* (Extended abstract of PhD dissertation). Kyiv, Ukraine.
4. Ruda, K. (2025). Research on the scalability of voice-embedding-based biometric authentication systems. *Social Development and Security, 15*(1), 161–170. https://doi.org/10.33445/sds.2025.15.1.15
5. Filonenko, P., & Vynokurova, O. (2011). Analysis of biometric authentication and identification systems using hybrid intelligent methods for protection against unauthorized access. *Radiotekhnika*, (166).
6. Ruda, K., et al. (2024). Comparison of digital signal processing methods and deep learning models in voice authentication. *Cybersecurity: Education, Science, Technique, 1*(25), 140–160.
7. Jain, A. K., Ross, A., & Prabhakar, S. (2004). An introduction to biometric recognition. *IEEE Transactions on Circuits and Systems for Video Technology, 14*(1), 4–20.
8. ISO/IEC. (2017). *ISO/IEC 2382-37:2017 Information technology — Vocabulary — Part 37: Biometrics*. https://www.iso.org/standard/66375.html
9. Saaty, T. L. (2008). Decision making with the analytic hierarchy process. *International Journal of Services Sciences, 1*(1), 83–98.
10. Daugman, J. (2004). How iris recognition works. *IEEE Transactions on Circuits and Systems for Video Technology, 14*(1), 21–30.
11. Galbally, J., Marcel, S., & Fierrez, J. (2014). Biometric antispoofing methods: A survey in face recognition. *IEEE Access, 2*, 1530–1552. https://doi.org/10.1109/ACCESS.2014.2322355
12. Snyder, D., Garcia-Romero, D., Sell, G., Povey, D., & Khudanpur, S. (2018). X-vectors: Robust DNN embeddings for speaker recognition. In *Proceedings of the IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)* (pp. 5329–5333).
13. Biggio, B., & Roli, F. (2018). Wild patterns: Ten years after the rise of adversarial machine learning. *Pattern Recognition, 84*, 317–331. https://doi.org/10.1016/j.patcog.2018.07.023
14. Kinnunen, T., & Li, H. (2010). An overview of text-independent speaker recognition: From features to supervectors. *Speech Communication, 52*(1), 12–40. https://doi.org/10.1016/j.specom.2009.08.010
15. Wu, Z., Evans, N., Kinnunen, T., Yamagishi, J., Alegre, F., & Li, H. (2015). Spoofing and countermeasures for speaker verification: A survey. *Speech Communication, 66*, 130–153. https://doi.org/10.1016/j.specom.2015.02.007
16. Behl, A., & Behl, K. (2017). Cyberwar, cyberterrorism and cybercrime: A review. *Journal of Global Information Technology Management, 20*(3), 190–203. https://doi.org/10.1080/1097198X.2017.1364669
17. ISO/IEC. (2018). *ISO/IEC 27005:2018 Information technology — Security techniques — Information security risk management*. https://www.iso.org/standard/75281.html
18. Ruan, K. (2017). Introducing cybernomics: A unifying economic framework for measuring cyber risk. *Computers & Security, 65*, 77–89. https://doi.org/10.1016/j.cose.2016.12.004