КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (34), 2026
ISSN 2663 – 4023
DOI 10.28925/2663-4023.2026.34.1306
УДК 004.056.53:57.087.1

Лісовський Богдан Володимирович
аспірант кафедри БІТ
Національний університет «Львівська політехніка», Львів, Україна
ORCID:0009-0002-3475-4989
bohdan.v.lisovskyi@lpnu.ua

Журавель Ігор Михайлович
д.т.н., професор, зав. каф. БІТ
Національний університет «Львівська політехніка», Львів, Україна
ORCID:0000-0003-1114-0124
ihor.m.zhuravel@lpnu.ua

МОДЕЛІ БЕЗПЕРЕРВНОЇ БІОМЕТРИЧНОЇ АВТЕНТИФІКАЦІЇ КОРИСТУВАЧА ДЛЯ ПІДВИЩЕННЯ РІВНЯ ЗАХИСТУ ІНФОРМАЦІЙНИХ СИСТЕМ

Анотація. У статті розглянуто задачу підвищення рівня захисту автентифікації користувача інформаційних систем на основі біометричних даних, що формуються з носимих пристроїв. Обґрунтовано доцільність переходу від одноразової (статичної) перевірки особи до безперервної автентифікації, за якої легітимність користувача підтверджується протягом усього сеансу роботи. Показано обмеженість одноразової перевірки особи, за якої відкритий сеанс залишається вразливим до перехоплення та несанкціонованого використання після успішного входу. Як спільний набір факторів використано відбиток пальця, частоту серцевих скорочень, варіабельність серцевого ритму, насиченість крові киснем та температуру шкіри, що доступні на сучасних смарт-годинниках. Запропоновано та формалізовано чотири моделі автентифікації: адаптивну модель з урахуванням контекстного ризику, інтелектуальну модель на основі машинного навчання, модель багатомодальної автентифікації з ваговими коефіцієнтами та контекстно-залежну модель, що додатково враховує поведінкові фактори. Для кожної моделі наведено математичний опис, схему прийняття рішення та визначено переваги й недоліки з погляду точності, стійкості до підробки, обчислювальної складності й енергоспоживання носимого пристрою. Наведено ілюстративний числовий приклад і виконано аналіз стійкості моделей до основних типів атак. Запропоновано практично відтворюваний спосіб підбору вагових коефіцієнтів на основі індивідуальних показників похибки факторів. Виконано порівняльний аналіз моделей за дев’ятьма критеріями, що дає змогу обґрунтовано обирати модель залежно від вимог до безпеки, ресурсів пристрою та умов експлуатації.

Ключові слова: безперервна автентифікація; біометрична автентифікація; носимі пристрої; мультимодальна біометрія; адаптивна автентифікація; машинне навчання; рівень довіри.

ВСТУП

Сучасні інформаційні системи дедалі частіше зберігають та обробляють конфіденційні дані безпосередньо на персональних і носимих пристроях користувача. Традиційні методи автентифікації, що ґрунтуються на знанні (паролі, PIN-коди) або володінні (токени, смарт-картки), мають принципове обмеження: вони підтверджують особу лише в момент входу до системи. Після успішної автентифікації сеанс залишається відкритим, а отже, у разі залишення пристрою без нагляду, перехоплення сеансу чи примусового доступу зловмисник отримує ті самі права, що й легітимний користувач. Це створює суттєвий ризик для систем з підвищеними вимогами до захисту.

Часткове розв’язання цієї проблеми забезпечує безперервна автентифікація – підхід, за якого легітимність користувача перевіряється не одноразово, а періодично або неперервно протягом усього сеансу роботи. Найзручнішим джерелом даних для такого режиму є біометричні сигнали, що збираються пасивно, без активної участі користувача. Поширення носимих пристроїв (смарт-годинників, фітнес-браслетів) з набором фізіологічних давачів робить можливим неперервний збір таких сигналів у фоновому режимі. У попередніх роботах авторів розглянуто автентифікацію на основі біометричних

сигналів мобільних пристроїв [1] та сформульовано принципи збирання фізіологічних біометричних даних з носимих пристроїв [2].

Водночас у літературі описано низку різних за принципом дії моделей автентифікації, кожна з яких має власні компроміси між точністю, стійкістю до підробки, обчислювальними витратами та енергоспоживанням. Відсутність систематизованого зіставлення цих моделей на спільному наборі біометричних факторів ускладнює обґрунтований вибір моделі під конкретні умови експлуатації, що й визначає актуальність роботи.

Постановка проблеми. Надійна автентифікація користувача є однією з базових умов захисту сучасних інформаційних систем, які дедалі частіше обробляють і зберігають конфіденційні дані безпосередньо на персональних та носимих пристроях [4]. Традиційні методи автентифікації, що ґрунтуються на знанні (паролі, PIN-коди) або володінні (токени, смарт-картки), підтверджують особу лише в момент входу до системи. Після успішної перевірки сеанс залишається відкритим, а отже, у разі залишення пристрою без нагляду, перехоплення сеансу чи примусового доступу зловмисник отримує ті самі права, що й легітимний користувач. Така обмеженість одноразової (статичної) перевірки створює суттєвий ризик, особливо для систем із підвищеними вимогами до безпеки.

Розв’язання цієї проблеми пов’язане з важливим науково-практичним завданням – забезпеченням захисту інформації від несанкціонованого доступу протягом усього сеансу роботи, а не лише на його початку. Перспективним напрямом є безперервна (continuous) автентифікація, за якої легітимність користувача перевіряється неперервно або періодично [12-14]. Зручним джерелом даних для такого режиму слугують біометричні сигнали носимих пристроїв (смарт-годинників, фітнес-браслетів), які збираються пасивно, без активної участі користувача [3, 4]. У попередніх роботах авторів розглянуто автентифікацію на основі біометричних сигналів мобільних пристроїв [1] та сформульовано принципи збирання фізіологічних біометричних даних з носимих пристроїв [2]. Водночас практична побудова таких систем потребує обґрунтованого вибору моделі автентифікації, яка поєднує біометричні фактори носимого пристрою, ураховує ресурсні обмеження та забезпечує належний рівень захисту, – що й визначає актуальність і практичну значущість дослідження.

Аналіз останніх досліджень і публікацій. Огляди застосування біометрії на носимих пристроях [3, 4] поділяють біометричні ознаки на фізіологічні (відбиток пальця, електрокардіограма, фотоплетизмограма, температура) та поведінкові (хода, динаміка натискань, жести). Фундаментальні засади біометричного розпізнавання та показники якості систем – частоту хибних допусків (FAR), хибних відмов (FRR) і рівну похибку (EER) – узагальнено в [5].

Фізіологічні сигнали серцево-судинної системи розглядаються як перспективне джерело для безперервної автентифікації. Так, у [6] запропоновано глибоку нейронну мережу CorNET для ідентифікації особи за сигналом фотоплетизмограми із зап’ястка; у [7] показано, що параметри варіабельності серцевого ритму, отримані з фотоплетизмограми, придатні для машинного оброблення; у [8] досліджено верифікацію за електрокардіограмою з носимих пристроїв з урахуванням рухової активності.

Окремий напрям становить мультимодальне злиття біометричних ознак. Розрізняють злиття на рівні ознак, на рівні оцінок та на рівні рішень; на практиці найпоширенішим є злиття на рівні оцінок як компроміс між інформативністю та простотою реалізації. Класичні підходи до такого злиття та нормалізації оцінок викладено в [9, 10], а принциповий підхід до злиття – у [11]. Можливість поєднання фізіологічних і поведінкових ознак безпосередньо на носимому пристрої продемонстровано в [12].

Адаптивні та ризик-орієнтовані підходи передбачають динамічне підлаштування вимог до автентифікації залежно від обчисленого рівня ризику. Модель керування автентифікацією, орієнтовану на досвід користувача, запропоновано в [13]; емпіричне дослідження застосування таких систем наведено в [14]; новітні ознаки оцінювання ризику розглянуто в [15]. Питання поєднання біометричних сигналів носимих пристроїв висвітлено також в огляді [16].

Аналіз показує, що згадані моделі здебільшого досліджуються ізольовано. Бракує порівняння кількох моделей, побудованих на єдиному наборі факторів носимого пристрою та орієнтованих саме на безперервний режим роботи, що й становить наукову новизну цієї роботи.

Слід розрізняти статичну та безперервну автентифікацію: перша виконує разову перевірку на вході, друга – періодичну або неперервну перевірку протягом усього сеансу. Саме безперервний режим дає змогу протидіяти загрозам, що виникають після входу до системи, проте він висуває жорсткіші вимоги до енергоефективності та пасивності збору даних, що й зумовлює зростання інтересу до фізіологічних сигналів носимих пристроїв [3, 16].

Мета статті. Метою роботи є формалізація та порівняльний аналіз моделей безперервної біометричної автентифікації користувача, побудованих на спільному наборі біометричних факторів носимого пристрою, для обґрунтованого підвищення рівня захисту інформаційних систем. Для

досягнення мети поставлено такі завдання: сформулювати узагальнену концепцію безперервної автентифікації; навести математичний опис чотирьох моделей (адаптивної, інтелектуальної на основі машинного навчання, багатомодальної з ваговими коефіцієнтами та контекстно-залежної); визначити переваги й недоліки кожної моделі; навести ілюстративний приклад; проаналізувати стійкість моделей до атак та виконати їх порівняльний аналіз за сукупністю критеріїв. Як спільний набір факторів обрано відбиток пальця (FP), частоту серцевих скорочень (HR), варіабельність серцевого ритму (HRV), насиченість крові киснем (SpO2) та температуру шкіри (temp), що доступні на сучасних смарт-годинниках.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Узагальнена концепція безперервної автентифікації. На відміну від одноразової перевірки, безперервна автентифікація підтримує динамічний показник довіри до користувача. Концепцію рівня довіри, який знижується за відсутності підтверджень і поновлюється за успішного розпізнавання, для безперервної автентифікації запропонував П. Бурс [17]; згодом С. Мондал і П. Бурс узагальнили її до модально-незалежної моделі довіри, застосовної до будь-якої біометричної ознаки [18]. Спираючись на цю концепцію, у роботі використано формалізацію, за якої рівень довіри оновлюється з надходженням кожного нового вікна біометричних спостережень і поступово згасає з часом за відсутності підтверджень:

$$T(t) = T(t-1) \cdot e^{-\lambda \Delta t} + (1 - e^{-\lambda \Delta t}) \cdot S(t) \quad (1)$$

де T(t) – рівень довіри в момент часу t; S(t) – поточна оцінка збігу біометричних ознак з еталоном користувача; – коефіцієнт згасання довіри; t – інтервал між спостереженнями. Доступ до системи зберігається, доки рівень довіри не нижчий за поріг Tmin; у протилежному випадку ініціюється повторна (підсилена) автентифікація. Узагальнену схему процесу подано на рис. 1.

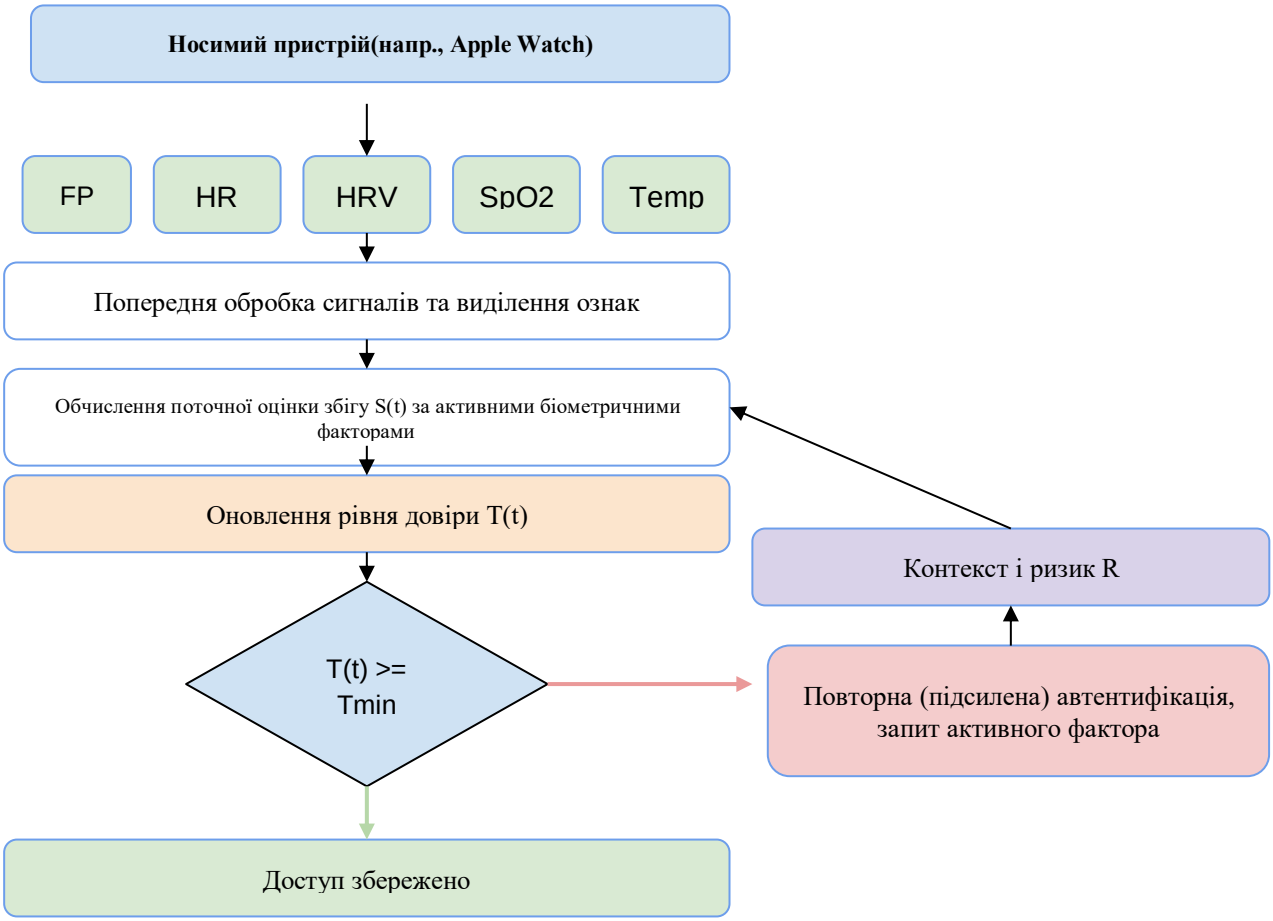

Рис. 1. Узагальнена схема безперервної біометричної автентифікації користувача

Біометричні сигнали обробляються у ковзному вікні фіксованої тривалості: для кожного вікна обчислюється оцінка S(t), після чого оновлюється рівень довіри згідно з (1). Вибір тривалості вікна та коефіцієнта згасання λ є компромісом між швидкістю виявлення зловмисника та кількістю хибних відмов для легітимного користувача. Розглянуті нижче моделі різняться способом обчислення оцінки S(t) та правилом прийняття рішення, проте всі вони вбудовуються в наведену схему безперервного контролю.

Залежно від задачі безперервна автентифікація може працювати в режимі верифікації (порівняння «один до одного» з еталоном заявленого користувача) або ідентифікації (порівняння «один до багатьох»). Якість будь-якої з моделей оцінюють за стандартними показниками: частотою хибних допусків (FAR), частотою хибних відмов (FRR) та рівною похибкою (Equal Error Rate, EER) – значенням, за якого частота хибних допусків дорівнює частоті хибних відмов (FAR = FRR); чим менша EER, тим точніша система. Для інтегральної характеристики використовують ROC-криву та площу під нею (AUC) [5]. Зниження порогу зменшує FRR (підвищує зручність), але збільшує FAR (підвищує ризик), тому вибір робочої точки є компромісом між безпекою та зручністю, що особливо важливо для безперервного режиму з частими перевірками.

Нормалізація біометричних оцінок. Часткові оцінки збігу різних факторів мають різні шкали та розподіли, тому перед поєднанням їх потрібно нормалізувати до єдиного діапазону [0, 1]. Найпоширенішим є метод мінімаксної нормалізації:

$$s' = (s - s_{min})/(s_{max} - s_{min}) \tag{2}$$

де s_{min} і s_{max} – мінімальне та максимальне значення оцінки. Метод простий, але чутливий до викидів. За наявності оцінок з вираженими відхиленнями застосовують нормалізацію за середнім μ і стандартним відхиленням σ (z-оцінку):

$$s' = (s - \mu)/\sigma \tag{3}$$

Для підвищення стійкості до викидів використовують також робастну tanh-нормалізацію:

$$s' = \frac{1}{2}\{tanh(0.01 \cdot (s - \mu)/\sigma) + 1\} \tag{4}$$

Вибір методу нормалізації істотно впливає на якість подальшого злиття оцінок [10]: мінімаксна нормалізація доцільна для стабільних факторів (наприклад, відбитка пальця), тоді як для фізіологічних сигналів, що змінюються з функціональним станом користувача, надійнішими є z-оцінка або tanh-нормалізація. Усі наведені нижче оцінки s_i вважаються попередньо нормалізованими.

Модель 1. Адаптивна модель з урахуванням ризику.

В основу цієї моделі покладено відомий підхід ризик-орієнтованої автентифікації, запропонований, зокрема, у роботах [13, 14], за яким вимоги до перевірки динамічно змінюються залежно від обчисленого рівня ризику; такий підхід широко застосовують у системах виявлення шахрайства та адаптивного контролю доступу. У цій роботі його адаптовано до безперервної біометричної автентифікації над спільним набором фізіологічних факторів. Адаптивна модель ураховує контекст роботи користувача через інтегральний показник ризику R та динамічно змінює суворість перевірки: рішення про підтвердження особи описується функцією A = f(R, FP, HR, HRV, SpO2, temp) і набуває вигляду:

$$A(t) = 1, \text{ якщо } S(t) \geq \tau(R); \quad A(t) = 0, \text{ якщо } S(t) < \tau(R) \tag{5}$$

де S(t) – поточна оцінка збігу за активними факторами; τ(R) – адаптивний поріг прийняття рішення. Поріг зростає зі збільшенням ризику:

$$\tau(R) = \tau_0 + (1 - \tau_0) \cdot R, R \in [0,1] \tag{6}$$

де τ_0 – базовий поріг для низького ризику. Поточна оцінка збігу обчислюється за множиною активних факторів A(R), склад якої залежить від рівня ризику:

$$S(t) = \Sigma_{i \in A(R)} \delta_i s_i / \Sigma_{i \in A(R)} \delta_i \tag{7}$$

де δ_i – коефіцієнт значущості і-го фактора. Інтегральний ризик обчислюється як зважена сума часткових індикаторів (геолокація, час доступу, мережа, стан пристрою, історія невдалих спроб):

$$R = \Sigma \rho_j r_j, j = 1, \ldots, m, \Sigma_{p_j} = 1 \quad (8)$$

За низького ризику для підтвердження особи достатньо пасивних фізіологічних факторів (HR, HRV, SpO2, temp); за високого – множина активних факторів розширюється, і додатково вимагається активний фактор (відбиток пальця), що підвищує точність перевірки [13-15].

Перевагами моделі є гнучкий баланс між безпекою та зручністю, мінімізація зайвих запитів до користувача за типових умов і природна інтеграція з безперервним режимом. Адаптивний поріг також забезпечує реакцію на аномальний контекст (наприклад, нову геолокацію чи незвичний час доступу). До недоліків належать залежність якості рішень від коректності моделі оцінювання ризику, потреба в доступі до контекстних даних (що порушує питання приватності) та можливість маніпуляції контекстними індикаторами.

Модель 2. Інтелектуальна модель на основі машинного навчання. Інтелектуальна модель розглядає автентифікацію як задачу класифікації. Із виміряних сигналів формується вектор ознак x = (FP, HR, HRV, SpO2, temp, …), на якому навчають класифікатор gθ, що повертає ймовірність належності спостереження легітимному користувачеві:

$$p = g_\theta(x) = P(y = 1|x; \Theta) \quad (9)$$

Параметри моделі θ визначають мінімізацією функції втрат на навчальній вибірці з регуляризацією:

$$\theta^* = arg\ min_\theta (1/N) \Sigma L(y_k, g_\theta(x_k)) + \lambda \left|\left|\theta\right|\right|^2 \quad (10)$$

де N – обсяг навчальної вибірки; L – функція втрат; $\lambda\|\theta\|^2$ – регуляризаційний доданок, що запобігає перенавчанню. Для фізіологічних сигналів інформативними ознаками є часові та частотні характеристики варіабельності серцевого ритму (зокрема SDNN, RMSSD, співвідношення LF/HF), статистики частоти серцевих скорочень і температури. Рішення приймається порівнянням ймовірності p з порогом. За орієнтир для вибору порогу часто беруть точку рівної похибки (EER, Equal Error Rate – це ключова метрика для оцінки ефективності систем біометричної ідентифікації та аутентифікації), де FAR = FRR, що збалансовує обидва типи похибок; для систем з підвищеними вимогами до безпеки поріг зміщують у бік меншого FAR ціною зростання частки хибних відмов. У безперервному режимі класифікація виконується для кожного вікна, а отримані оцінки агрегуються в часі. Як класифікатори у відтворюваних умовах доцільно застосовувати метод опорних векторів, випадковий ліс або k-найближчих сусідів, а за наявності достатнього обсягу даних – згорткові та рекурентні нейронні мережі [6, 7].

Перевагою моделі є потенційно найвища точність та здатність ураховувати складні нелінійні залежності між біометричними ознаками й виявляти нетипові патерни самих сигналів. Водночас базова модель оперує лише біометричними ознаками і не використовує контекстних чи ризикових сигналів, тому її чутливість до контекстного ризику є низькою. Недоліками є також потреба в репрезентативній навчальній вибірці, ризик перенавчання, нижча інтерпретованість рішень («чорна скриня») та підвищені обчислювальні й енергетичні витрати, що є критичним для носимих пристроїв.

Модель 3. Модель багатомодальної автентифікації з ваговими коефіцієнтами.

Модель багатомодальної автентифікації, на відміну від адаптивної, не використовує показник ризику, а поєднує часткові оцінки окремих факторів на рівні оцінок (score-level fusion) із заздалегідь підібраними ваговими коефіцієнтами:

$$S = \Sigma w_i s_i, i = 1, \ldots, n, \Sigma\, w_i = 1, w_i \geq 1, w_i \geq 0 \quad (11)$$

де s_i – нормалізована оцінка збігу за і-м фактором; w_i – ваговий коефіцієнт; n – кількість факторів. Рішення приймається порівнянням сумарної оцінки з порогом:

$$A = 1, \text{ якщо } S \geq \tau; \quad A = 0, \text{ якщо } S < \tau \quad (12)$$

Вагові коефіцієнти підбираються експериментально. Для відтворюваності в умовах дослідження доцільно обирати ваги обернено пропорційно до індивідуальної похибки кожного фактора (EER):

$$w_i = (1/EER_i)/\Sigma\,(1/EER_j), j = 1, \ldots, n \quad (13)$$

що надає більшу вагу надійнішим факторам без потреби в складній оптимізації. Теоретичні засади такого злиття узагальнено в [9-11], а практичну реалізацію поєднання фізіологічних факторів у [12].

Перевагами моделі є простота реалізації, низькі обчислювальні витрати та прозорість рішення. Недоліками – статичність вагів (вони не враховують зміни контексту чи стану користувача), потреба в коректній нормалізації оцінок та чутливість до деградації окремого фактора.

Модель 4. Контекстно-залежна модель.

Контекстно-залежна модель розширює набір біометричних факторів поведінковими ознаками (динаміка натискань і жестів, хода, патерни використання застосунків, типова геолокація), які використовуються як додаткові. Підсумкова оцінка формується поєднанням біометричної та поведінкової складових:

$$S_{ctx} = \alpha \cdot S_{bio} + (1 - \alpha) \cdot S_{beh}, \alpha \in (0,1) \quad (14)$$

де S_bio – оцінка за фізіологічними факторами; S_beh – оцінка за поведінковими ознаками; α – коефіцієнт балансу складових. Поведінкова складова, своєю чергою, є зваженою сумою часткових поведінкових оцінок:

$$S_{beh} = \Sigma\, v_k b_k, k = 1, \ldots, q, \Sigma\, v_k = 1 \quad (15)$$

На відміну від адаптивної моделі, де контекст впливає лише на поріг, тут поведінкові фактори безпосередньо беруть участь у формуванні оцінки збігу. Поведінкові ознаки складно відтворити, тому їх додавання підвищує стійкість до підробки. Можливість поєднання фізіологічних і поведінкових сигналів на носимому пристрої підтверджено в [12].

Перевагою є найвища стійкість до підробки, оскільки зловмиснику потрібно відтворити одночасно фізіологічні та поведінкові патерни, а також природна придатність до безперервного режиму. Недоліки – найвищі обчислювальні та енергетичні витрати, потреба в тривалому накопиченні поведінкового профілю та потенційне зниження точності за зміни поведінки користувача (хвороба, стрес, фізичне навантаження).

Концептуальне зіставлення моделей.

Усі чотири моделі побудовано на спільному наборі біометричних факторів носимого пристрою, але вони різняться додатковими вхідними даними та способом формування підсумкового рішення (рис. 2). Адаптивна модель доповнює факторний набір контекстним ризиком, інтелектуальна – заміщує евристичне злиття навченим класифікатором, багатомодальна спирається на фіксовані вагові коефіцієнти, а контекстно-залежна додає поведінкові фактори. Спільним для всіх моделей є кінцевий етап – прийняття рішення A(t) та оновлення рівня довіри T(t) у межах безперервного контролю.

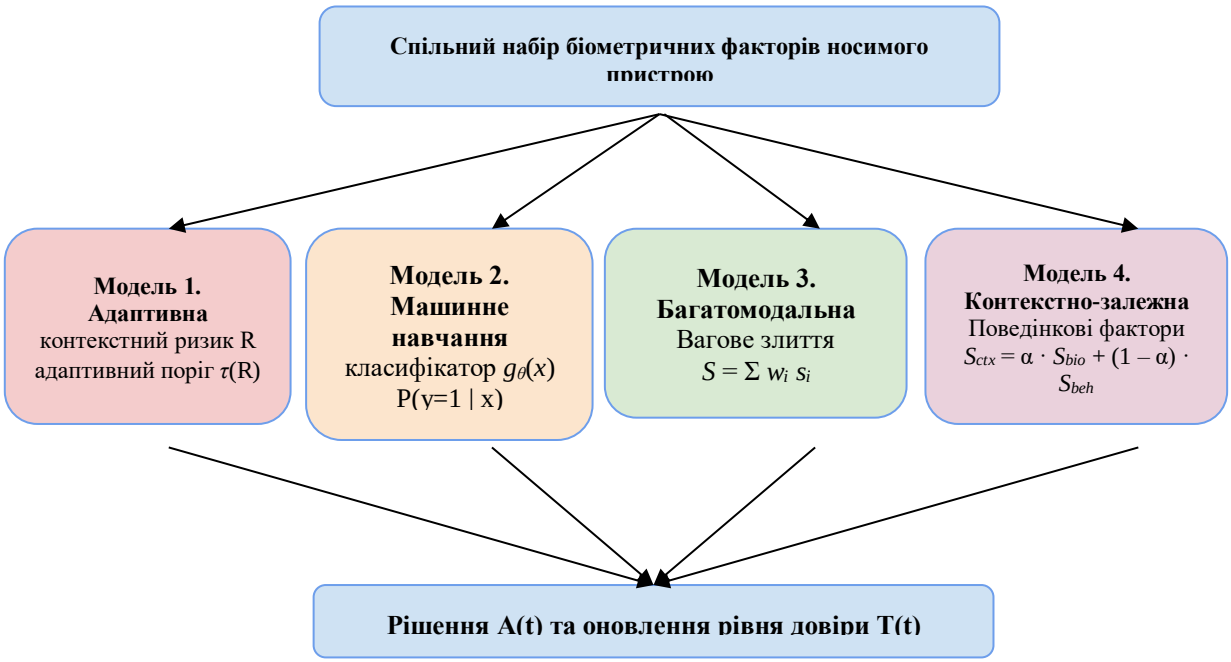

Рис. 2. Концептуальне зіставлення чотирьох моделей безперервної автентифікації

Ілюстративний приклад.

Розглянемо спрощений приклад роботи багатомодальної моделі (модель 3) для умовного набору нормалізованих оцінок збігу за п'ятьма факторами. Вагові коефіцієнти обчислено за формулою (13) на основі типових значень рівної похибки EER кожного фактора. Вхідні дані та результати наведено в табл. 1 для двох сценаріїв – легітимного користувача та зловмисника.

Наприклад, для наведених значень EER обернені величини $1/EER_i$ становлять 50; 6,7; 10; 5 та 4 відповідно, а їх сума дорівнює 75,7. Поділивши кожну обернену величину на цю суму, отримуємо нормовані вагові коефіцієнти w_i, наведені в табл. 1 (їх сума дорівнює одиниці). Такий підхід не потребує ітеративної оптимізації й легко відтворюється у звичайному табличному процесорі.

Таблиця 1

Приклад обчислення сумарної оцінки для багатомодальної моделі

Фактор	EER_i	w_i	s_i (легіт.)	s_i (зловм.)
FP	0,02	0,661	0,95	0,30
HR	0,15	0,088	0,80	0,60
HRV	0,10	0,132	0,85	0,55
SpO_2	0,20	0,066	0,70	0,65
temp	0,25	0,053	0,65	0,60
Сумарна оцінка S	–	1,000	0,89	0,40

За фіксованого порогу τ = 0,6 легітимний користувач (S = 0,89) успішно проходить автентифікацію, тоді як зловмисник (S = 0,40) відхиляється. Приклад також демонструє визначальну роль найнадійнішого фактора (відбитка пальця з найбільшою вагою): попри відносно близькі оцінки за фізіологічними факторами, низька оцінка зловмисника за відбитком (0,30) призводить до відмови.

Для адаптивної моделі (модель 1) приймемо базовий поріг τ_0 = 0,6, що збігається з фіксованим порогом багатомодальної моделі; відмінність полягає лише в тому, що в адаптивній моделі цей поріг не є сталим, а підвищується зі зростанням ризику згідно з (6). Так, за низького ризику (R = 0,1) поріг становить $\tau = \tau_0 + (1 - \tau_0) \cdot R = 0{,}64$, і для підтвердження особи достатньо пасивних фізіологічних факторів; за підвищеного ризику (R = 0,5) поріг зростає до τ = 0,80, через що система додатково запитує активний фактор (відбиток пальця). Оскільки оцінка зловмисника за відбитком низька, у режимі підвищеного ризику доступ блокується навіть за прийнятних фізіологічних оцінок. Наведені обчислення відтворювані стандартними засобами та не потребують спеціалізованого обладнання.

Безпосередньо безперервність контролю демонструє динаміка рівня довіри. Нехай після входу T(0) = 0,90, поріг довіри $T_{min} = 0{,}6$, а коефіцієнт згасання задано так, що $e^{-\lambda \Delta t} = 0{,}7$. Для легітимного користувача, який стабільно отримує оцінку S(t) ≈ 0,89, рівень довіри за формулою (1) залишається близьким до 0,90 і не опускається нижче T_{min}, тож доступ зберігається. Якщо ж після входу пристроєм заволодіває зловмисник з оцінкою S(t) ≈ 0,40, рівень довіри поступово спадає і вже на третьому вікні опускається нижче порогу T_{min}, що ініціює повторну автентифікацію (табл. 2).

Таблиця 2

Динаміка рівня довіри T(t) для легітимного користувача та зловмисника

Вікно t	S(t), легіт.	T(t), легіт.	S(t), зловм.	T(t), зловм.
0	–	0,90	–	0,90
1	0,89	0,90	0,40	0,75
2	0,89	0,89	0,40	0,65
3	0,89	0,89	0,40	0,57

Таким чином, навіть за відсутності негайної відмови система виявляє підміну користувача протягом кількох вікон спостереження: рівень довіри легітимного користувача залишається стабільно високим, тоді як для зловмисника він монотонно спадає й перетинає поріг T_{min}. Саме це й забезпечує безперервність захисту впродовж сеансу.

Аналіз стійкості до атак.

Розглянемо стійкість моделей до основних типів атак на системи автентифікації. До них належать атаки пред'явлення (підроблений відбиток пальця, фотографія, штучний фізіологічний сигнал), повторні атаки з відтворенням перехоплених біометричних даних, перехоплення відкритого сеансу та атаки на сховище біометричних шаблонів.

Безперервний режим роботи сам собою істотно знижує ризик перехоплення сеансу: оскільки легітимність користувача переперевіряється протягом усього сеансу, несанкціоноване використання

відкритого сеансу швидко виявляється через падіння рівня довіри T(t). Використання фізіологічних сигналів забезпечує природну перевірку «живучості», оскільки відтворити живий серцевий ритм чи варіабельність серцевого ритму значно складніше, ніж статичну біометричну ознаку [4]. Мультимодальність підвищує бар'єр для зловмисника, адже потребує одночасної підробки кількох незалежних факторів.

Стійкість окремих моделей різниться. Адаптивна модель (модель 1) протидіє атакам через реакцію на аномальний контекст: підозрілі геолокація, час чи мережа підвищують ризик і автоматично посилюють вимоги до перевірки. Інтелектуальна модель (модель 2) здатна виявляти нетипові патерни сигналів, характерні для підробки чи повторного відтворення. Багатомодальна модель (модель 3) забезпечує стійкість завдяки тому, що компрометації одного фактора недостатньо для подолання порогу. Контекстно-залежна модель (модель 4) має найвищу стійкість, оскільки вимагає одночасного відтворення фізіологічних і поведінкових патернів, що практично недосяжно для зловмисника. Спільною умовою захищеності всіх моделей є належний захист біометричних шаблонів, оскільки їх компрометація є незворотною.

Додатковим рівнем захисту є виявлення атак пред'явлення (presentation attack detection, PAD), що ґрунтується на ознаках «живучості» сигналу – природній мінливості серцевого ритму, узгодженості кількох фізіологічних показників між собою та реакції організму на фізичну активність. Поєднання PAD з динамічним рівнем довіри (1) дає змогу не лише відхиляти підроблені спроби, а й поступово знижувати рівень довіри в разі виявлення підозрілих ознак, забезпечуючи плавну, а не різку реакцію системи на потенційну загрозу.

Порівняльний аналіз моделей за критеріями.

Зведене зіставлення розглянутих моделей за дев'ятьма критеріями подано в табл. 3. Для кількісного порівняння оцінки переведено в бальну шкалу від 1 до 5, орієнтовану так, що більший бал відповідає сприятливішому для впровадження значенню критерію (тобто «більше – краще» для всіх критеріїв). Бали є експертними порядковими оцінками на основі структури моделей та узагальнення джерел [3-16], а не результатами прямих вимірювань. Інтегральний показник обчислено як суму балів за всіма дев'ятьма критеріями з подальшим нормуванням до діапазону 0–10 за рівних вагових коефіцієнтів.

Таблиця 3

Порівняльний аналіз моделей безперервної біометричної автентифікації

Критерій (більше – краще)	M1 Адаптивна	M2 Машинне навчання	M3 Багатомодальна	M4 Контекстно-залежна
Урахування контексту / ризику	4	2	1	4
Незалежність від попереднього навчання	4	2	3	3
Обчислювальна ефективність	3	2	4	2
Стійкість до підробки (спуфінгу)	4	4	3	5
Енергоефективність	3	2	4	2
Потенційна точність	4	5	3	4
Інтерпретованість рішення	4	2	4	3
Простота відтворення робочої системи	3	3	4	2
Придатність для безперервного режиму	4	4	3	5
Сума балів (макс. 45)	33	26	29	30
Нормований показник, 0-10	7,3	5,8	6,4	6,7

За рівноважного підсумовування найвищий інтегральний показник має адаптивна модель (7,3), далі – контекстно-залежна (6,7) та багатомодальна (6,4), а найнижчий – інтелектуальна модель на основі машинного навчання (5,8). Відмінності між моделями невеликі, а підсумковий рейтинг чутливий до вибору вагових коефіцієнтів: за пріоритету стійкості до підробки та придатності до безперервного режиму вперед виходить контекстно-залежна модель, а за пріоритету точності – інтелектуальна. Це кількісно підтверджує відсутність універсально найкращої моделі.

Окремого пояснення потребують два критерії. Низький бал урахування контексту для інтелектуальної моделі (М2) стосується саме базового варіанта, що оперує лише біометричними ознаками й не використовує контекстних чи ризикових сигналів; здатність такої моделі виявляти нелінійні залежності та нетипові патерни стосується самих біометричних сигналів, а не контексту роботи користувача. Щодо простоти відтворення робочої системи: сам алгоритм класифікації (метод опорних векторів, випадковий ліс, k-найближчих сусідів) відтворюється тривіально стандартними бібліотеками, однак для отримання працездатної системи потрібні ще репрезентативна навчальна вибірка та калібрування моделі й порогу. Тому фіксоване вагове злиття (М3) відтворити простіше (вищий бал), ніж інтелектуальну модель (М2).

Як видно з таблиці, не існує універсально найкращої моделі: вибір визначається пріоритетами конкретної системи. Для пристроїв з обмеженими ресурсами та вимогою прозорості рішень доцільна багатомодальна вагова модель; за наявності достатніх даних і потреби в максимальній точності – інтелектуальна модель; для систем з мінливим контекстом і підвищеними вимогами до балансу безпеки та зручності – адаптивна; для застосувань з найвищими вимогами до стійкості, зокрема для моніторингу функціонального стану операторів критичної інфраструктури, – контекстно-залежна. На практиці перспективним є гібридний підхід, що поєднує адаптивне керування порогом (модель 1) з ваговим злиттям факторів (модель 3).

Особливості практичної реалізації.

Усі розглянуті моделі орієнтовані на роботу в умовах обмежених обчислювальних та енергетичних ресурсів носимого пристрою. Тому на практиці частину обчислень (зокрема навчання класифікатора в моделі 2) доцільно виконувати поза пристроєм, а на самому пристрої залишати лише етап виведення (inference) та оновлення рівня довіри. Поріг прийняття рішення τ та поріг довіри T_{min} зручно калібрувати з орієнтиром на точку рівної похибки (EER) на етапі реєстрації користувача, що забезпечує відтворюваність налаштувань без складної оптимізації.

Окремої уваги потребує захист самих біометричних шаблонів, оскільки їх компрометація є незворотною. Для зберігання еталонів доцільно застосовувати незворотні перетворення та захищені апаратні сховища пристрою, а передавання даних здійснювати каналами зі шифруванням, що узгоджується з принципами збирання фізіологічних біометричних даних, сформульованими в [2]. Питання приватності особливо гостро постає для адаптивної та контекстно-залежної моделей, які потребують доступу до контекстних і поведінкових даних користувача [4].

Спільним практичним обмеженням фізіологічних факторів є їх залежність від функціонального стану користувача: фізичне навантаження, стрес чи захворювання змінюють частоту серцевих скорочень та варіабельність серцевого ритму, що може спричиняти тимчасове зростання кількості хибних відмов. Часткова компенсація цього ефекту досягається мультимодальністю (моделі 3 і 4) та адаптивним порогом (модель 1), які знижують вплив деградації окремого фактора на підсумкове рішення.

Важливим практичним параметром є частота збору та оброблення сигналів. Висока частота підвищує оперативність виявлення зловмисника, але збільшує енергоспоживання та навантаження на процесор пристрою; низька частота заощаджує ресурс, проте збільшує час реакції системи. Компромісним рішенням є подійно-орієнтований збір, за якого оброблення активується за певних умов, та адаптивна частота, що зростає за підвищеного ризику. Узгодження частоти збору з показниками автономності пристрою є окремою інженерною задачею [2, 16].

З погляду інтеграції розглянуті моделі доцільно реалізовувати як окремий модуль безперервного контролю, що працює паралельно з основним механізмом входу та передає до системи керування доступом поточний рівень довіри. Це дає змогу застосовувати моделі поверх наявних систем автентифікації без їх докорінної перебудови та поетапно підвищувати рівень захисту інформаційної системи.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

У роботі систематизовано та формалізовано чотири моделі безперервної біометричної автентифікації користувача, побудовані на спільному наборі факторів носимого пристрою (FP, HR, HRV, SpO_2, temp): адаптивну з урахуванням ризику, інтелектуальну на основі машинного навчання, багатомодальну з ваговими коефіцієнтами та контекстно-залежну. Для кожної моделі наведено математичний опис, правило прийняття рішення, ілюстративний приклад та визначено переваги й недоліки, а також проаналізовано стійкість до основних типів атак.

Наукова новизна полягає в тому, що для моделей автентифікації різного принципу дії на єдиному наборі біометричних факторів та в орієнтації запропоновано безперервний режим роботи, а також підбір вагових коефіцієнтів за індивідуальною похибкою факторів (формула 13). Виконаний порівняльний

аналіз за дев'ятьма критеріями дає змогу обґрунтовано обирати модель залежно від вимог до безпеки, ресурсів пристрою та умов експлуатації.

Практична цінність результатів полягає в можливості їх застосування для побудови систем безперервного контролю доступу та моніторингу функціонального стану операторів критичної інфраструктури. Аналіз показав, що жодна модель не є універсально найкращою, а найбільш перспективним є гібридний підхід, що поєднує адаптивне керування порогом із ваговим злиттям факторів. Напрямом подальших досліджень є експериментальна перевірка такої гібридної моделі на реальних даних носимих пристроїв з оцінюванням показників FAR, FRR та EER.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Lisovskyi, B. V., & Zhuravel, I. M. (2025). User authentication in information systems based on biometric signals from mobile devices. *Modern Information Security, 64*(4), 116-122. https://doi.org/10.31673/2409-7292.2025.041211
2. Lisovskyi, B. V., & Zhuravel, I. M. (2025). Principles of collecting physiological biometric data from wearable devices for authentication systems. *Modern Information Security, 62*(2). https://doi.org/10.31673/2409-7292.2025.022701
3. Liu, S., et al. (2021). Recent advances in biometrics-based user authentication for wearable devices: A contemporary survey. *Digital Signal Processing*, 103120. https://doi.org/10.1016/j.dsp.2021.103120
4. Khan, S., et al. (2020). Biometric systems utilising health data from wearable devices. *ACM Computing Surveys, 53*(4), 1-29. https://doi.org/10.1145/3400030
5. 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. https://doi.org/10.1109/TCSVT.2003.818349
6. Biswas, D., et al. (2019). CorNET: Deep learning framework for PPG-based heart rate estimation and biometric identification in ambulant environment. *IEEE Transactions on Biomedical Circuits and Systems, 13*(2), 282-291. https://doi.org/10.1109/TBCAS.2019.2892297
7. Tsai, Y.-Y., et al. (2025). Photoplethysmography-based HRV analysis and machine learning for real-time stress quantification in mental health applications. *APL Bioengineering, 9*(2). https://doi.org/10.1063/5.0256590
8. Bıçakcı, H. S., Santopietro, M., & Guest, R. (2022). Activity-based electrocardiogram biometric verification using wearable devices. *IET Biometrics*. https://doi.org/10.1049/bme2.12105
9. Ross, A., & Jain, A. (2003). Information fusion in biometrics. *Pattern Recognition Letters, 24*(13), 2115-2125. https://doi.org/10.1016/S0167-8655(03)00079-5
10. Jain, A., Nandakumar, K., & Ross, A. (2005). Score normalization in multimodal biometric systems. *Pattern Recognition, 38*(12), 2270-2285. https://doi.org/10.1016/j.patcog.2005.01.012
11. Dass, S. C., Nandakumar, K., & Jain, A. K. (2005). A principled approach to score level fusion in multimodal biometric systems. *Lecture Notes in Computer Science*, 1049-1058. https://doi.org/10.1007/11527923_109
12. Vhaduri, S., & Poellabauer, C. (2019). Multi-modal biometric-based implicit authentication of wearable device users. *IEEE Transactions on Information Forensics and Security, 14*(12), 3116-3125. https://doi.org/10.1109/TIFS.2019.2911170
13. Sepczuk, M., & Kotulski, Z. (2018). A new risk-based authentication management model oriented on user's experience. *Computers & Security, 73*, 17-33. https://doi.org/10.1016/j.cose.2017.10.002
14. Wiefling, S., Lo Iacono, L., & Dürmuth, M. (2019). Is this really you? An empirical study on risk-based authentication applied in the wild. In *ICT systems security and privacy protection* (pp. 134-148). Springer. https://doi.org/10.1007/978-3-030-22312-0_10
15. Han, A. H., & Lee, D. H. (2023). Detecting risky authentication using the OpenID Connect token exchange time. *Sensors, 23*(19), 8256. https://doi.org/10.3390/s23198256
16. Pourbemany, J., Zhu, Y., & Bettati, R. (2023). A survey of wearable devices pairing based on biometric signals. *IEEE Access*, 1. https://doi.org/10.1109/ACCESS.2023.3254499
17. Bours, P. (2012). Continuous keystroke dynamics: A different perspective towards biometric evaluation. *Information Security Technical Report, 17*(1-2), 36-43. https://doi.org/10.1016/j.istr.2012.02.001
18. Mondal, S., & Bours, P. (2017). A study on continuous authentication using a combination of keystroke and mouse biometrics. *Neurocomputing, 230*, 1-22. https://doi.org/10.1016/j.neucom.2016.11.031

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (34), 2026
ISSN 2663 – 4023

Bohdan Lisovskyi
Postgraduate student
Work place: Lviv Polytechnic National University, Department of Information Technology Security, Lviv, Ukraine
ORCID:0009-0002-3475-4989
bohdan.v.lisovskyi@lpnu.ua

Ihor Zhuravel
Doctor of Technical Sciences, Professor, Head of Department
Work place: Lviv Polytechnic National University, Department of Information Technology Security, Lviv, Ukraine
ORCID:0000-0003-1114-0124
ihor.m.zhuravel@lpnu.ua

CONTINUOUS BIOMETRIC USER AUTHENTICATION MODELS FOR ENHANCING THE SECURITY OF INFORMATION SYSTEMS

Abstract. This paper addresses the problem of enhancing the security of user authentication in information systems based on biometric data acquired from wearable devices. The paper substantiates the expediency of transitioning from one-time (static) identity verification to continuous authentication, in which the legitimacy of the user is confirmed throughout the entire working session. It is shown that one-time identity verification is limited, since after a successful login the open session remains vulnerable to interception and unauthorized use. Fingerprint, heart rate, heart rate variability, blood oxygen saturation, and skin temperature – all available on modern smartwatches – are used as a common set of factors. Four authentication models are proposed and formalized: an adaptive model accounting for contextual risk, an intelligent model based on machine learning, a multimodal authentication model with weighting coefficients, and a context-aware model that additionally takes behavioral factors into account. For each model, a mathematical description and a decision-making scheme are provided, and the advantages and disadvantages are determined in terms of accuracy, spoofing resistance, computational complexity, and the energy consumption of the wearable device. An illustrative numerical example is presented, and an analysis of the models' resistance to the main types of attacks is carried out. A practically reproducible method for selecting weighting coefficients based on the individual error rates of the factors is proposed. A comparative analysis of the models against nine criteria is performed, which makes it possible to reasonably select a model depending on the security requirements, device resources, and operating conditions.

Keywords: continuous authentication; biometric authentication; wearable devices; multimodal biometrics; adaptive authentication; machine learning; trust level.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Lisovskyi, B. V., & Zhuravel, I. M. (2025). User authentication in information systems based on biometric signals from mobile devices. *Modern Information Security*, *64*(4), 116-122. https://doi.org/10.31673/2409-7292.2025.041211
2. Lisovskyi, B. V., & Zhuravel, I. M. (2025). Principles of collecting physiological biometric data from wearable devices for authentication systems. *Modern Information Security*, *62*(2). https://doi.org/10.31673/2409-7292.2025.022701
3. Liu, S., et al. (2021). Recent advances in biometrics-based user authentication for wearable devices: A contemporary survey. *Digital Signal Processing*, 103120. https://doi.org/10.1016/j.dsp.2021.103120
4. Khan, S., et al. (2020). Biometric systems utilising health data from wearable devices. *ACM Computing Surveys*, *53*(4), 1-29. https://doi.org/10.1145/3400030
5. 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. https://doi.org/10.1109/TCSVT.2003.818349
6. Biswas, D., et al. (2019). CorNET: Deep learning framework for PPG-based heart rate estimation and biometric identification in ambulant environment. *IEEE Transactions on Biomedical Circuits and Systems*, *13*(2), 282-291. https://doi.org/10.1109/TBCAS.2019.2892297

7. Tsai, Y.-Y., et al. (2025). Photoplethysmography-based HRV analysis and machine learning for real-time stress quantification in mental health applications. *APL Bioengineering, 9*(2). https://doi.org/10.1063/5.0256590
8. Bıçakcı, H. S., Santopietro, M., & Guest, R. (2022). Activity-based electrocardiogram biometric verification using wearable devices. *IET Biometrics*. https://doi.org/10.1049/bme2.12105
9. Ross, A., & Jain, A. (2003). Information fusion in biometrics. *Pattern Recognition Letters, 24*(13), 2115-2125. https://doi.org/10.1016/S0167-8655(03)00079-5
10. Jain, A., Nandakumar, K., & Ross, A. (2005). Score normalization in multimodal biometric systems. *Pattern Recognition, 38*(12), 2270-2285. https://doi.org/10.1016/j.patcog.2005.01.012
11. Dass, S. C., Nandakumar, K., & Jain, A. K. (2005). A principled approach to score level fusion in multimodal biometric systems. *Lecture Notes in Computer Science*, 1049-1058. https://doi.org/10.1007/11527923_109
12. Vhaduri, S., & Poellabauer, C. (2019). Multi-modal biometric-based implicit authentication of wearable device users. *IEEE Transactions on Information Forensics and Security, 14*(12), 3116-3125. https://doi.org/10.1109/TIFS.2019.2911170
13. Sepczuk, M., & Kotulski, Z. (2018). A new risk-based authentication management model oriented on user's experience. *Computers & Security, 73*, 17-33. https://doi.org/10.1016/j.cose.2017.10.002
14. Wiefling, S., Lo Iacono, L., & Dürmuth, M. (2019). Is this really you? An empirical study on risk-based authentication applied in the wild. In *ICT systems security and privacy protection* (pp. 134-148). Springer. https://doi.org/10.1007/978-3-030-22312-0_10
15. Han, A. H., & Lee, D. H. (2023). Detecting risky authentication using the OpenID Connect token exchange time. *Sensors, 23*(19), 8256. https://doi.org/10.3390/s23198256
16. Pourbemany, J., Zhu, Y., & Bettati, R. (2023). A survey of wearable devices pairing based on biometric signals. *IEEE Access*, 1. https://doi.org/10.1109/ACCESS.2023.3254499
17. Bours, P. (2012). Continuous keystroke dynamics: A different perspective towards biometric evaluation. *Information Security Technical Report, 17*(1-2), 36-43. https://doi.org/10.1016/j.istr.2012.02.001
18. Mondal, S., & Bours, P. (2017). A study on continuous authentication using a combination of keystroke and mouse biometrics. *Neurocomputing, 230*, 1-22. https://doi.org/10.1016/j.neucom.2016.11.031

Отримано редакцією журналу / Received: 05.02.26
Прорецензовано / Revised: 19.02.26
Схвалено до друку / Accepted: 24.09.26