УДК 004.056.523:57.087.1
DOI: 10.31673/2409-7292.2025.041211

Лісовський Б.В., Журавель І.М.

АВТЕНТИФІКАЦІЯ КОРИСТУВАЧА В ІНФОРМАЦІЙНИХ СИСТЕМАХ НА ОСНОВІ БІОМЕТРИЧНИХ СИГНАЛІВ МОБІЛЬНИХ ПРИСТРОЇВ

Досліджено використання фізіологічних біометричних сигналів, отриманих за допомогою мобільних пристроїв, для підвищення ефективності та надійності автентифікації в інформаційних системах. Встановлено, що динамічні параметри – частота серцевих скорочень (HR), варіабельність серцевого ритму (HRV), насиченість крові киснем (SpO_2), температура шкіри та частота дихання – здатні формувати індивідуальний біометричний профіль користувача, який можна застосовувати для безперервної автентифікації. Проведено порівняння результатів біометричної автентифікації за допомогою мобільних пристроїв з класичними методами, що базуються на відбитках пальців та розпізнаванні обличчя, визначено їх переваги: динамічність, адаптивність і підвищена стійкість до атак типу спуфінг. Запропоновано методику побудови біометричної матриці користувача з періодичним оновленням кожні 5 хвилин, яка демонструє стабільні результати автентифікації та підтверджує доцільність застосування такого підходу навіть без використання складних моделей машинного навчання. Проаналізовано вплив змін фізіологічного стану користувача (стрес, фізичне навантаження, період відновлення) на стабільність процесу автентифікації, а також досліджено ефективність підходів, що поєднують кілька типів біометричних даних для підвищення надійності розпізнавання. Визначено перспективні напрями інтеграції мобільних пристроїв з технологіями машинного навчання, блокчейну та квантово-стійкого шифрування з метою створення безпечних, адаптивних і енергоефективних систем ідентифікації. Показано, що фізіологічні сигнали мобільних пристроїв є ключовим елементом майбутніх систем безперервної автентифікації в інформаційній безпеці.

Ключові слова: фізіологічні біометричні сигнали, мобільні пристрої, автентифікація, блокчейн, безперервна автентифікація, інформаційна безпека, захист інформації, ідентифікація користувача.

Вступ і формулювання проблеми

У цифрову епоху автентифікація – ключовий компонент інформаційної безпеки. Традиційні методи (паролі, PIN-коди) піддаються атакам типу соціальної інженерії, їх легко втратити або скомпрометувати. Це зумовлює активний пошук нових, більш безпечних підходів, які забезпечували б баланс між комфортом і стійкістю.

Перехід до біометричних технологій у цьому контексті є логічним: вони ґрунтуються на фізіологічних або поведінкових характеристиках користувача. Незважаючи на це, що методи, які ґрунтуються на відбитках пальців чи розпізнаванні обличчя, вже широко використовуються, фізіологічні сигнали, що збираються мобільними пристроями (наприклад, WHOOP, Apple Watch, Oura Ring, Smart Ring, Garmin, Colo), відкривають нові вектори для досліджень і практичного застосування.

Мобільні пристрої (smart-годинники, браслети, кільця) дозволяють безперервно вимірювати низку параметрів – частоту серцевих скорочень (HR), варіабельність серцевого ритму (HRV), насиченість крові киснем (SpO_2), температуру, дихальні показники. Саме ці сигнали формують унікальний «біометричний профіль» користувача, придатний для динамічної автентифікації, яка працює у фоновому режимі, а не лише при вході.

Можливості та переваги такого моніторингу підтверджені у низці наукових досліджень. Мобільні пристрої збирають інформацію про (тут розшифруйте що це таке)HR, SpO_2, температуру та респіраторні дані для моніторингу фізіологічних показників людини [1].

Проте поява таких інноваційних та високотехнологічних функцій – тобто можливостей безперервного моніторингу фізіологічних параметрів у реальному часі, інтеграції мультисенсорних даних (серцевий ритм, насичення киснем, температура, варіабельність серцевого ритму тощо) та застосування алгоритмів штучного інтелекту для розпізнавання біометричних патернів – породжує нові виклики:

- фізіологічні сигнали змінюються залежно від стресу, фізичного навантаження чи стану здоров'я, тому необхідно розробляти адаптивні моделі автентифікації;
- питання захисту та приватності біометричних даних мобільних систем залишаються відкритими: як безпечно зберігати, обробляти та забезпечити стійкість до спуфінгу;

Мета дослідження полягає у підвищення ефективності та надійності автентифікації користувачів в інформаційних системах на основі біометричних сигналів, отриманих із мобільних пристроїв.

Для досягнення поставленої мети необхідно виконати такі завдання:

- провести аналіз відомих наукових досліджень щодо використання фізіологічних сигналів для автентифікації особи;
- дослідити особливості основних фізіологічних сигналів (HR, HRV, SpO_2, температура, дихання) та їх придатність для формування біометричного профілю;
- дослідити методи та алгоритми обробки фізіологічних сигналів;
- виявити обмеження та проблеми використання мобільних пристроїв для збору біометрії (зміни фізіологічного стану, наявність шумів, приватність даних);
- окреслити перспективи розвитку систем автентифікації на основі фізіологічних сигналів, зокрема мультимодальних підходів, блокчейн-зберігання та безперервної автентифікації.

Огляд літератури та концептуальні основи автентифікації

Фізіологічні параметри людини – такі як частота серцевих скорочень (HR), варіабельність серцевого ритму (HRV), насиченість крові киснем (SpO_2), температура тіла та показники дихання – розглядаються як перспективні біометричні фактори. Вони формують динамічний біометричний профіль, здатний доповнити чи навіть замінити класичні статичні методи.

Мобільні пристрої можуть надійно відстежувати HR, SpO_2 та температуру, забезпечуючи неперервний доступ до унікальних фізіологічних шаблонів користувача. Подібні висновки наведені також в інших публікаціях [3], де підкреслено, що сенсори для визначення частоти серцевих скорочень і кровотоку, руху та температури відкривають новий рівень інтеграції біометричних даних у інформаційні системи.

На відміну від одноразових біометричних перевірок (відбиток пальця, розпізнавання обличчя), мобільні пристрої можуть забезпечувати безперервне підтвердження особи. Це зменшує ризик використання скомпрометованих облікових даних після первинного входу. Дослідження Laxmi Divya Chhibbar [3] та ін. показало, що сигнали для визначення частоти серцевих скорочень з розумних годинників можна застосовувати для безперервної автентифікації водіїв, навіть у динамічних умовах транспорту [3]. Інша робота (Know Me by My Pulse, 2025) описує практичні реалізації неперервного підтвердження на базі PPG з низьким енергоспоживанням [4]. Таким чином, ці пристрої формують новий клас систем, де користувач не взаємодіє напряму із сенсором – автентифікація відбувається у фоні, під час повсякденної активності.

Порівняння з класичними біометричними методами

Класичні методи (відбиток пальця, обличчя, райдужка) характеризуються високою точністю, проте мають суттєві обмеження: статичність перевірки (лише під час входу); вразливість до атак типу спуфінг (3D-маски, силіконові відбитки); неможливість «змінити» біометричні дані у разі їх витоку.

Біометрія з мобільних пристроїв здатна зменшити ці ризики: динамічність сигналів (частота серцевих скорочень, варіабельність серцевого ритму, температура змінюються в часі, ускладнюючи підробку); неперервність перевірки (захист не обмежується моментом входу); можливість інтеграції у мультимодальні системи, де фізіологічні та поведінкові параметри поєднуються для підвищення точності та стійкості до атак [2, 3].

Характеристика фізіологічних біометричних сигналів

Частота серцевих скорочень (HR)

HR є одним із базових показників, які зчитуються мобільними пристроями. Хоча середні значення HR можуть змінюватися залежно від віку, фізичного стану чи навантаження, дослідження показують наявність індивідуальних патернів серцевої активності, які можуть

© Лісовський Б.В., Журавель І.М. (2025) Автентифікація користувача в інформаційних системах на основі біометричних сигналів мобільних пристроїв. Сучасний захист інформації, 4(64), 116–123. https://doi.org/10.31673/2409-7292.2025.041211

використовуватися для ідентифікації особи. За результатами порівняльного аналізу HR з Apple Watch та Polar H10, дані показали високу узгодженість у стані спокою, що підтверджує придатність HR як біометричного сигналу. Використання HR у системах безперервної автентифікації базується на тому, що навіть при зміні абсолютних значень зберігається індивідуальна форма та динаміка варіацій [6].

Варіабельність серцевого ритму (HRV)

HRV відображає коливання інтервалів між серцевими скороченнями. Вона є маркером стану автономної нервової системи та чутливою до стресу, фізичних навантажень і відновлення. Дослідження Ben O'Grady та ін. (2024) показало, що Apple Watch Series 9 та Ultra 2 забезпечують валідні дані HRV у порівнянні з клінічними приладами (Polar H10 + Kubios), особливо у стані спокою [6,7]. HRV відзначається високою індивідуальністю: профілі користувачів можуть суттєво відрізнятися, що робить цей показник надійним кандидатом для персоналізованої автентифікації.

Одна з базових метрик HRV – RMSSD (Root Mean Square of Successive Differences, середньоквадратичне значення послідовних різниць). Вона використовується для характеристики автономної нервової системи та може слугувати ключовим біометричним параметром:

$$RMSSD = \sqrt{\frac{1}{N-1}\sum_{i=1}^{N-1}(RR_{i+1} - RR_i)^2},$$

де RR_i – послідовні інтервали між ударами серця (R-R інтервали на ЕКГ чи PPG), N – кількість інтервалів.

Насиченість крові киснем (SpO_2)

Показник SpO_2 відображає рівень насичення крові киснем. Хоча середні значення у здорової людини подібні, дослідження вказують на індивідуальні патерни сатурації під час сну та при навантаженні. За результатами клінічних випробувань, Apple Watch та інші мобільні пристрої мають похибку вимірювання SpO_2 близько 2–6% у порівнянні з медичними пульсоксиметрами [8, 9]. Незважаючи на похибки, SpO_2 може використовуватися як допоміжний біометричний параметр, що підвищує надійність мультимодальних систем автентифікації.

Температура тіла та шкіри

Температура тіла та шкіри є показниками, які залежать від індивідуальних особливостей, циркадних ритмів та стану організму. У дослідженнях на основі Oura Ring доведено, що індивідуальні коливання температури можна використовувати як фоновий параметр для підтвердження особи [10]. Для автентифікації температура виступає переважно як контекстуальний фактор, що посилює надійність інших сигналів.

Частота та ритм дихання

Частота та ритм дихання можуть відновлюватися з фотоплетизмограми (PPG) та акселерометричних даних мобільних пристроїв. Роботи з безперервною автентифікацією користувача показали, що поєднання HR, HRV та дихальних патернів значно підвищує точність автентифікації користувача [4]. Індивідуальні особливості дихання формують біометричний маркер, придатний для систем фонової перевірки доступу.

Методи та алгоритми обробки сигналів

Фізіологічні сигнали, зібрані з мобільних пристроїв (HR, HRV, SpO_2, температура, дихання), часто спотворюються через рухові артефакти, електричні шуми або неточності сенсорів. Для забезпечення придатності даних до автентифікації застосовуються методи попередньої обробки:

Фільтрація шумів – використання цифрових фільтрів для очищення PPG та ECG-сигналів від артефактів руху [2].

Нормалізація даних – приведення сигналів до єдиного масштабу (z-score, min-max), що особливо важливо у мультимодальних системах, де поєднуються різні фізіологічні показники.

© Лісовський Б.В., Журавель І.М. (2025) Автентифікація користувача в інформаційних системах на основі біометричних сигналів мобільних пристроїв. Сучасний захист інформації, 4(64), 116–123. https://doi.org/10.31673/2409-7292.2025.041211

Віконування – поділ сигналів на часові вікна (5–60 секунд), що дозволяє аналізувати короткочасні патерни та зменшує вплив випадкових відхилень.

Сучасні біометричні системи широко використовують алгоритми машинного та глибинного навчання для автоматичного розпізнавання унікальних патернів у фізіологічних сигналах.

Класичні методи Machine Learning (машинного навчання, ML):

Support Vector Machine (SVM) – машина опорних векторів, застосовується для класифікації користувачів за HRV та PPG-сигналами [14].

Deep Learning (глибинне навчання, DL):

CNN (Convolutional Neural Networks) – згорткові нейронні мережі, це тип глибинних нейронних мереж, призначений для автоматичного виділення просторових закономірностей у даних, ефективні для аналізу часово-частотних карт HRV та PPG. [15, 16]

RNN/LSTM (Recurrent Neural Networks, Long Short-Term Memory) – рекурентні нейронні мережі враховують послідовність і часову залежність даних, що робить їх особливо ефективними для аналізу фізіологічних сигналів, які змінюються з часом, застосовуються для розпізнавання довгострокових часових залежностей у серцево-дихальних сигналах. [17]

Незважаючи на успіхи машинного та глибинного навчання, доцільне застосування й класичних методів сигнал-обробки без залучення складних моделей:

- визначення відхилень від індивідуальних діапазонів (наприклад, середнє HR або SpO_2 у стані спокою);
- аналіз середнього, стандартного відхилення, спектральних ознак HRV як унікальних параметрів користувача;
- порівняння сигналів користувача з еталонними шаблонами.

Такі методи мають меншу точність у порівнянні з машинним навчанням, але є більш енергоефективними та можуть застосовуватися у мобільних системах із обмеженими обчислювальними ресурсами.

Схема побудови цифрового біометричного профілю користувача

Ключовим етапом є побудова цифрового біометричного профілю користувача. Це відбувається у кілька кроків (рис. 1):

1. Екстракція ознак – виділення характеристик сигналів (HR, HRV, SpO_2, Temp).
2. Формування матриці ознак – створення багатовимірного вектора, що представляє користувача у просторі фізіологічних параметрів.
3. Навчання або ініціалізація профілю – збір даних протягом певного часу (наприклад, 24–48 годин), після чого формується «еталонний шаблон».
4. Верифікація – нові дані порівнюються з біометричною матрицею:

a. у класичних підходах – через метрики подібності (Евклідова відстань та відстань Махаланобіса);

b. у підходах машинного та глибинного навчання – через класифікацію або вбудовування у векторний простір.

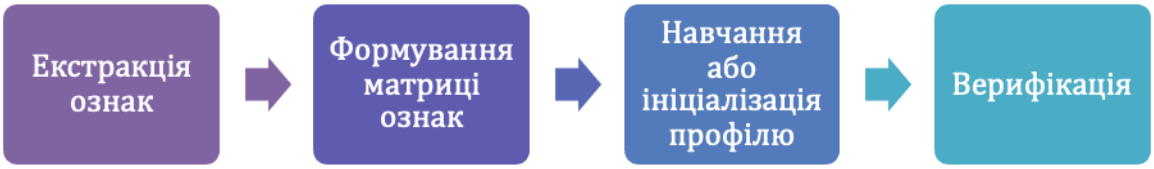

Рис. 1. Структурна схема побудови цифрового біометричного профілю користувача

Для побудови моделі автентифікації на основі фізіологічних даних мобільних пристроїв формується цифровий біометричний профіль користувача, що відображає унікальні характеристики його фізіологічних сигналів. Кожен параметр має різну стабільність, чутливість до зовнішніх факторів і важливість у процесі розпізнавання (табл. 1).

© Лісовський Б.В., Журавель І.М. (2025) Автентифікація користувача в інформаційних системах на основі біометричних сигналів мобільних пристроїв. Сучасний захист інформації, 4(64), 116–123. https://doi.org/10.31673/2409-7292.2025.041211

Після екстракції зазначених параметрів формується вектор ознак користувача:

$$F_u = [HR, HRV, SpO_2, Temp] = [62,65,97,36.4],$$

а з урахуванням ваг – зважений вектор ознак:

$$F_u^{(w)} = [0.30 * HR, 0.35 * HRV, 0.15 * SpO_2, 0.10 * Temp].$$

Ваги параметрів обрано експериментально, виходячи з їх стабільності, індивідуальності та впливу на точність автентифікації:

- HRV (0.35) – має найвищу індивідуальність і складно підробляється, тому отримує найбільшу вагу;
- HR (0.30) – стабільний і доступний параметр, який добре вимірюється усіма wearable-пристроями;
- SpO_2 (0.15) – менш стабільний у спокої, але дає додаткову інформацію при фізичному навантаженні або стресі;
- Температура (0.10) – допомагає розпізнавати фізіологічні стани (сон, хвороба, перегрів), однак більш залежна від середовища, тому її вага нижча.

Таким чином, більші ваги надано найбільш стабільним і унікальним показникам (HRV, HR), а менші – контекстним параметрам (SpO_2, температура), які підсилюють систему, але менш надійні окремо.

Цей вектор є базовим представленням біометричної ідентичності користувача у просторі фізіологічних параметрів і може бути використаний для обчислення метрик схожості (наприклад, косинусної або евклідової відстані) при порівнянні поточних даних із зареєстрованим шаблоном під час автентифікації.

Таким чином, біометрична матриця стає ядром системи автентифікації, дозволяючи гнучко інтегрувати як класичні методи, так і сучасні алгоритми машинного навчання.

Таблиця 1

Основні фізіологічні параметри, що формують біометричний профіль користувача

	Параметр	*Позначення*	*Опис характеристики*	*Приклад значення*	*Вага важливості (0–1)*	*Коментар*
1	Частота серцевих скорочень (Heart Rate)	HR	Середній пульс у стані спокою або під час активності	62 bpm	0.30	Висока стабільність у користувача; базовий фізіологічний маркер
2	Варіабельність серцевого ритму (Heart Rate Variability)	HRV	Стандартне відхилення інтервалів RR; відображає автономну нервову систему	65 ms	0.35	Складно підробити; має індивідуальний патерн
3	Рівень насичення крові киснем (SpO_2)	SpO_2	Співвідношення оксигемоглобіну до загального гемоглобіну	97%	0.15	Менш стабільний, але важливий при фізичному навантаженні або хворобі
4	Температура тіла (Skin/Body Temperature)	Temp	Зміни базальної температури шкіри	36.4 °C	0.10	Піддається впливу середовища, але дає контекстні дані

© Лісовський Б.В., Журавель І.М. (2025) Автентифікація користувача в інформаційних системах на основі біометричних сигналів мобільних пристроїв. Сучасний захист інформації, 4(64), 116–123. https://doi.org/10.31673/2409-7292.2025.041211

Порівняльний аналіз підходів до автентифікації

Класичні біометричні методи – відбиток пальця, розпізнавання обличчя, райдужки або сітківки ока демонструють найвищу разову точність і давно інтегровані в інфраструктуру контролю доступу. У контрольованих умовах вони забезпечують низькі показники помилок і швидку взаємодію з користувачем, однак працюють переважно в точці входу: після первинного допуску ідентичність більше не підтверджується, що створює «вікно ризику» для захоплення активної сесії. До того ж статична біометрія вимагає активної дії (прикласти палець, подивитися в камеру), чутлива до умов середовища (вологі або пошкоджені пальці, складне освітлення, аксесуари), а у разі крадіжки шаблона майже не підлягає відновленню: біометричний «ключ» не можна змінити так само просто, як пароль. Такі методи чудово відповідають сценаріям миттєвого доступу, проте їхня модель загроз у фонових режимах має обмеження.

Запропонований у роботі підхід на основі біометричних сигналів, зібраних із носимих пристроїв (HR, HRV, SpO_2, температура шкіри), вирішує іншу задачу – не лише коректно «впускати», а й постійно підтверджувати, що за клавіатурою, кермом або робочою станцією перебуває саме авторизований користувач. Безперервна або періодична (наприклад, кожні 1–5 хвилин) верифікація істотно звужує вікно для атак на активні сесії і відбувається практично без втручання користувача, адже працює у фоні без явних дій з його боку. Попри те, що разова точність фізіологічної біометрії зазвичай нижча за відбиток чи райдужку, її динамічна природа ускладнюють спуфінг: зловмиснику потрібно синхронно імітувати одразу кілька показників відповідного фізіологічного стану в режимі реального часу. Водночас такий підхід вимагає ретельної обробки сигналів та адаптивного зважування каналів за якістю, а також підвищених вимог до приватності: ці дані належать до медично чутливих, отже мають оброблятися за принципами мінімізації, з локальним обчисленням ознак на пристрої, шифруванням і регулярним оновленням шаблона, що, на відміну від статичної біометрії, зменшує цінність потенційного витоку.

Класичні методи автентифікації, такі як відбитки пальця, потребують спеціалізованих сенсорів і побудови ланцюжків довіри на точках доступу. Вони вимагають фізичного контакту користувача із сенсором або безпосередньої взаємодії з камерою, що після пандемії COVID-19 стало додатковим фактором ризику – користувачі дедалі частіше уникають дотиків до спільних поверхонь, таких як сканери відбитків пальців чи сенсорні панелі, через побоювання передачі вірусів і бактерій. Це підкреслює обмеження традиційних контактних методів і стимулює перехід до безконтактних або фонових способів автентифікації.

Мобільні пристрої, навпаки, ґрунтуються на давачах, що вже інтегровані у пристрої на руці користувача. Це дозволяє перенести акцент на легку та енергоефективну аналітику без додаткових сенсорів, з обчисленням даних безпосередньо на периферії пристрою. Для базового рівня захисту немає потреби у складних моделях машинного навчання – достатньо простих алгоритмів: порогових правил, зваженого вектора ознак і метрик відстані (Евклідова, Махаланобіса) із застосуванням експоненційного згладжування.

Запропонований підхід автентифікації на основі фізіологічних сигналів, отриманих із мобільних пристроїв, поступається класичним біометричним методам (відбиток пальця, сітківка ока, розпізнавання обличчя) за разовою точністю, проте має суттєві переваги у практичному застосуванні. Його головною перевагою є забезпечення безперервної автентифікації користувача у фоновому режимі, що мінімізує ризики несанкціонованого доступу під час активної сесії. Крім того, підхід базується на безконтактному принципі роботи, адже всі необхідні сигнали зчитуються без фізичної взаємодії з сенсорами чи спільними поверхнями. Це особливо важливо у пост пандемічних умовах, коли користувачі уникають дотиків до сканерів або пристроїв через ризик передачі інфекцій.

Таким чином, навіть поступаючись у точності порівняно з класичними методами, система автентифікації на основі фізіологічних біометричних сигналів є безпечнішою,

комфортнішою та більш адаптивною до сучасних умов. Вона вирішує одразу дві ключові проблеми – неперервність підтвердження особи та зменшення потреби у фізичному контакті, що робить цей підхід перспективним напрямом розвитку інформаційної безпеки у сфері мобільних технологій.

Висновки та перспективні напрямки досліджень

Фізіологічні біометричні сигнали мобільних пристроїв характеризуються різною стабільністю, варіативністю та чутливістю до зовнішніх і внутрішніх факторів (температура тіла, стрес, фізичне навантаження, рівень насиченості крові киснем тощо). Попри це, їхнє комбіноване застосування відкриває можливість побудови мультимодальних систем автентифікації, здатних працювати у реальному часі та забезпечувати вищий рівень точності й стійкості до атак порівняно з традиційними методами на основі відбитків пальців чи розпізнавання обличчя.

Найбільш інформативними для персоніфікації користувача залишаються показники серцевої діяльності – частота серцевих скорочень (HR) та варіабельність серцевого ритму (HRV), які відображають унікальні фізіологічні патерни та реакції автономної нервової системи. Разом із ними, показники SpO_2, температура шкіри та частота дихання виконують роль контекстуальних факторів, що дозволяють адаптивно коригувати модель користувача відповідно до його поточного стану.

Поєднання таких сигналів дає змогу реалізувати безперервну та адаптивну автентифікацію, де біометрична матриця користувача оновлюється з урахуванням короткочасних фізіологічних змін. Надалі подібні системи можуть інтегруватися з технологіями машинного навчання, блокчейну та квантово-стійкого шифрування, формуючи нове покоління безпечних рішень для автентифікації в інформаційних системах [5].

Перспективи подальших досліджень включають:

1. Розробку адаптивних моделей, що враховують зміни фізіологічного стану, як це пропонується у дослідженнях [11, 12, 13].
2. Подальше дослідження мультимодальних підходів, що поєднують фізіологічні сигнали з поведінковою біометрією (хода, набір тексту), для досягнення максимальної надійності.

Перелік посилань

1. Manta, C., Jain, S. S., Coravos, A., Mendelsohn, D., & Izmailova, E. S. (2020). An Evaluation of Biometric Monitoring Technologies for Vital Signs in the Era of COVID-19 // Clinical and Translational Science, 13(6), 1034–1044. https://doi.org/10.1111/cts.12874.
2. Sun, W., Guo, Z., Yang, Z., Wu, Y., Lan, W., Liao, Y., Wu, X., & Liu, Y. (2022). A Review of Recent Advances in Vital Signals Monitoring of Sports and Health via Flexible Wearable Sensors // Sensors, 22(20), 7784. https://doi.org/10.3390/s22207784.
3. Chhibbar, L. D., Patni, S., Todi, S., Bhatia, A., & Tiwari, K. (2024). Enhancing security through continuous biometric authentication using wearable sensors // Internet of Things, 28, 101374. https://doi.org/10.1016/j.iot.2024.101374.
4. Shao, W., Liang, Z., Zhang, R., Fang, R., Miao, N., Kourkchi, E., Rafatirad, S., Homayoun, H., & Fang, C. (2025). Know Me by My Pulse: Toward Practical Continuous Authentication on Wearable Devices via Wrist-Worn PPG // arXiv preprint arXiv:2508.13690. https://doi.org/10.48550/arXiv.2508.13690.
5. Журавель Ю.І., Лісовський Б.В. (2025). Аналіз моделей та алгоритмів автентифікації на основі біометричних даних. Сучасний захист інформації, №2(62), 51–58. https://doi.org/10.31673/2409-7292.2025.022701
6. O'Grady, B., Lambe, R., Baldwin, M., Acheson, T., & Doherty, C. (2024). The Validity of Apple Watch Series 9 and Ultra 2 for Serial Measurements of Heart Rate Variability and Resting Heart Rate // Sensors, 24(19), 6220. https://doi.org/10.3390/s24196220.
7. Bonneval, L., Wing, D., Sharp, S., Parra, M. T., Moran, R., LaCroix, A., & Godino, J. (2025). Validity of Heart Rate Variability Measured with Apple Watch Series 6 Compared to Laboratory Measures // Sensors, 25(8), 2380. https://doi.org/10.3390/s25082380.
8. Windisch, P., Schröder, C., Förster, R., Cihoric, N., & Zwahlen, D. R. (2023). Accuracy of the Apple Watch Oxygen Saturation Measurement in Adults: A Systematic Review // Cureus, 15(2), e35355. https://doi.org/10.7759/cureus.35355.

9. Browne, S. H., Bernstein, M., & Bickler, P. E. (2025). Evaluation of Pulse Oximetry Accuracy in a Commercial Smartphone and Smartwatch Device During Human Hypoxia Laboratory Testing // Sensors, 25(5), 1286. https://doi.org/10.3390/s25051286.

10. Alzueta, E., Gombert-Labedens, M., Javitz, H., Yuksel, D., Perez-Amparan, E., Camacho, L., Kiss, O., Zambotti, M., Sattari, N., Alejandro-Pena, A., Zhang, J., Shuster, A., Morehouse, A., Simon, K., Mednick, S., & Baker, F. C. (2024). Menstrual Cycle Variations in Wearable-detected Finger Temperature and Heart Rate, but not in Sleep Metrics, in Young and Midlife Individuals // Journal of Biological Rhythms, 39(5), 395–412. https://doi.org/10.1177/07487304241265018.

11. Muratyan, A., Cheung, W., Dibbo, S. V., & Vhaduri, S. (2021). Opportunistic Multi-Modal User Authentication for Health-Tracking IoT Wearables // arXiv preprint arXiv:2109.13705. https://doi.org/10.48550/arXiv.2109.13705.

12. Sancho, J., Alesanco, Á., & García, J. (2018). Biometric Authentication Using the PPG: A Long-Term Feasibility Study // Sensors, 18(5), 1525. https://doi.org/10.3390/s18051525.

13. Davoodi, M., Soker, A., Behar, J., & Yaniv, Y. (2023). Using Beat-to-Beat Heart Signals for Age-Independent Biometric Verification // Scientific Reports, 13(1). https://doi.org/10.1038/s41598-023-42841-4.

14. Ashtiyani, M., Iavasani, S. N., Alvar, A. A., & Deevband, M. R. (2018). Heart Rate Variability Classification Using Support Vector Machine and Genetic Algorithm // Journal of Biomedical Physics and Engineering, 8(4). https://doi.org/10.31661/jbpe.v0i0.614.

15. Wittenberg, T., Koch, R., Pfeiffer, N., & Eskofier, B. (2020). Evaluation of HRV Estimation Algorithms from PPG Data Using Neural Networks // Current Directions in Biomedical Engineering, 6(3), 505–509. https://doi.org/10.1515/cdbme-2020-3130.

16. Ding, J., Liu, Q., Ling, B. W.-K., & Li, W. (2026). Heart Rate Estimation Based on Joint Convolutional Neural Network and Conditional Generative Adversarial Network via Heart Rate Variabilities and Other Features Extracted from Photoplethysmograms // Biomedical Signal Processing and Control, 112(C), 108831. https://doi.org/10.1016/j.bspc.2025.108831.

17. Ólafsdóttir G. B., Larsson J. Deep Learning Approach for Extracting Heart Rate Variability from a Photoplethysmographic Signal // Bachelor Thesis, Kristianstad University, Sweden. 2020. Режим доступу: https://researchportal.hkr.se/ws/portalfiles/portal/35216086/FULLTEXT01.pdf.

Надійшла 30.10.2025

УДК 004.056.53:004.45:004.8
DOI: 10.31673/2409-7292.2025.041212

Максимович М.В.

ВИКОРИСТАННЯ МЕТОДІВ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ ВИЯВЛЕННЯ ВРАЗЛИВОСТЕЙ НУЛЬОВОГО ДНЯ

Стрімка цифровізація та широко поширене використання відкритого програмного забезпечення істотно підвищують ризики появи нових загроз у ланцюгах постачання ПЗ. Особливо небезпечними є вразливості нульового дня, які можуть непомітно потрапляти у проєкти через сторонні бібліотеки та залишатися невиявленими до моменту їх фактичної експлуатації. У таких умовах актуальним є пошук підходів, здатних забезпечити проактивний аналіз залежностей та своєчасне виявлення потенційно небезпечних компонентів. Метою статті є оцінка можливостей застосування методів штучного інтелекту для ідентифікації вразливих сторонніх бібліотек та аналіз ефективності такого підходу на основі моделювання реального інциденту компрометації сторонньої бібліотеки. У роботі описано характерні властивості вразливостей нульового дня, а також підкреслено обмеження традиційних інструментів забезпечення безпеки, які не завжди здатні оперативно реагувати на нові загрози або враховувати транзитивні залежності. Проведений експеримент передбачав аналіз десяти тестових проєктів із використанням агентного підходу на основі різних моделей штучного інтелекту, що дозволило оцінити їхню здатність виявляти скомпрометовані компоненти, формувати структуровані звіти та надавати рекомендації щодо мінімізації ризиків. Отримані результати підтвердили точність підходу та його потенціал для інтеграції в сучасні процеси розробки та супроводу програмного забезпечення. Водночас підкреслено недетермінованість роботи мовних моделей, що зумовлює необхідність додаткової перевірки отриманих результатів. Проведене дослідження окреслює подальші перспективи розвитку, зокрема вдосконалення механізмів проактивного моніторингу, а також розробку методів верифікації результатів, отриманих із використанням методів штучного інтелекту, що сприятиме підвищенню достовірності та надійності аналітичних висновків.

Ключові слова: штучний інтелект, вразливості нульового дня, безпека ПЗ, автоматизація, відкриті бібліотеки, програмне забезпечення.