КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (32), 2026
ISSN 2663 – 4023
DOI 10.28925/2663-4023.2026.32.1067
УДК 004.056.5:004.77:796.015

Кузьменко Дмитро Сергійович
магістр
Харківський національний університет радіоелектроніки, Харків, Україна
ORCID: 0009-0006-1366-9530
dmytro.kuzmenko@nure.ua

Коноваленко Оксана Костянтинівна
старший викладач кафедри фізичного виховання та спорту
Харківський національний університет радіоелектроніки, Харків, Україна
ORCID: 0000-0002-7707-0969
oksana.konovalenko@nure.ua

ІНТЕРНЕТ РЕЧЕЙ У СПОРТІ: БЕЗПЕКА СЕНСОРНИХ МЕРЕЖ ДЛЯ МОНІТОРИНГУ ЗДОРОВ'Я

Анотація. Стаття присвячена проблемі забезпечення безпеки сенсорних мереж для моніторингу здоров'я спортсменів у системах Інтернету речей. Показано, що цифровізація спорту та масове впровадження носимих сенсорних пристроїв, пов'язаних із мобільними шлюзами й хмарними платформами, формують новий клас ризиків, пов'язаних із конфіденційністю, цілісністю та доступністю біометричних даних. На основі аналізу міжнародних стандартів і рекомендацій NIST SP 800-213/213A, ENISA та ISO/IEC 27001, а також сучасних наукових досліджень у галузі спортивних IoT-технологій, eHealth, безпеки BLE та автентифікації в IoT-орієнтованій медицині розроблено концептуальну багаторівневу модель захисту спортивної IoT-системи. У межах запропонованого підходу виділено сенсорний, шлюзовий, серверний та прикладний рівні, для кожного з яких охарактеризовано функціональне призначення, типові загрози та конкретні механізми їхнього пом'якшення з урахуванням обмежених ресурсів пристроїв і вимог реального часу. На сенсорному рівні обґрунтовано доцільність застосування енергоефективних криптографічних алгоритмів, режиму BLE LE Secure Connections, secure boot, підписаних оновлень OTA та апаратних модулів безпеки на кшталт Secure Element для захищеного зберігання ключів. На шлюзовому рівні розглянуто використання протоколів MQTT і HTTPS поверх TLS 1.3, взаємної автентифікації (mTLS), а також впровадження елементів edge-аналітики та on-device AI для зменшення обсягу переданих сирих даних і підвищення конфіденційності. Серверний рівень описано як простір масштабованої аналітики й управління ідентичностями, де застосовуються шифрування даних «на носії», централізоване управління ключами, токени JWT з обмеженим часом дії, ротацією ключів і підтримкою механізмів відкликання. На прикладному рівні запропоновано модель розмежування доступу для лікарів, тренерів, аналітиків та адміністративного персоналу, реалізацію багатофакторної автентифікації, ведення захищених журналів аудиту й контроль оновлень прошивок через Signed OTA. Окрему увагу приділено питанням конфіденційності геолокаційних даних, використанню псевдонімізації та «коарсингу» координат, а також етичним і правовим аспектам обробки біометричної інформації спортсменів. Показано, що запропонована модель може слугувати методологічною основою для проєктування, аудиту й стандартизації цифрових рішень у професійному та масовому спорті, зокрема під час розроблення внутрішніх політик безпеки в клубах і федераціях. Інтеграція технічних, організаційних та нормативних заходів, доповнена механізмами контролю якості рішень систем штучного інтелекту та обмеженням їхньої автономності, є необхідною умовою формування цілісної, стійкої й довірчої екосистеми моніторингу здоров'я спортсменів на базі Інтернету речей.

Ключові слова: Інтернет речей (IoT); спортивні сенсорні мережі; інформаційна безпека; біометричні дані; протоколи шифрування; захист даних; моніторинг здоров'я; носимі пристрої.

ВСТУП

Постановка проблеми. У сучасному спорті дані стають основним ресурсом для управління тренувальним процесом, контролю стану здоров'я та профілактики травм спортсменів. Носимі сенсорні пристрої, об'єднані в мережі Інтернету речей (IoT), дають змогу в режимі реального часу відстежувати широкий спектр фізіологічних та біомеханічних показників, що суттєво підвищує об'єктивність тренерських та медичних рішень [1, 2]. Водночас така цифровізація породжує критичну залежність від цілісності й конфіденційності даних [13]. Біометрична інформація відображає не лише поточний стан організму, але й структуру навантажень, тактичні схеми, характер підготовки й фактичне місцезнаходження спортсмена. Витік або спотворення цих даних може спричинити медичні ризики, маніпуляцію спортивною формою, створення нечесних конкурентних переваг для опонентів та репутаційні втрати для клубів й федерацій.

Додаткову складність створює те, що спортивні сенсори є малопотужними пристроями з обмеженими обчислювальними ресурсами й працюють через відкриті бездротові канали, де повноцінні криптографічні засоби часто спрощуються задля економії енергії й зменшення затримок. Будь-які компроміси у безпеці на цьому рівні призводять до підвищення ризиків перехоплення, модифікації та несанкціонованого використання біометричних даних. У результаті захист сенсорних мереж у спорті перетворюється на актуальну науково-практичну проблему, яка знаходиться на перетині інформаційної безпеки, спортивної науки та електронної медицини [2, 5, 9].

Аналіз останніх досліджень і публікацій. Теоретичну та нормативну основу дослідження становлять сучасні стандарти й рекомендації щодо безпеки IoT-пристроїв та бездротових протоколів. У публікаціях NIST SP 800-213 і NIST SP 800-213A наведено комплексний підхід до формування вимог з кібербезпеки для пристроїв Інтернету речей, включно з управлінням ідентичністю, захищеним зберіганням даних, оновленням програмного забезпечення та обробкою вразливостей, що задає рамки для проєктування безпечних сенсорних систем [3, 4]. Європейський погляд на безпеку IoT представлено у рекомендаціях ENISA, де наголошується на підході security-by-design, необхідності безпечного життєвого циклу пристрою, захищеного ланцюга постачання та реалізації політик шифрування, управління доступом, моніторингу й реагування на інциденти [5].

Протокол Datagram Transport Layer Security (DTLS) версії 1.3, формалізований у RFC 9147, забезпечує захищену передачу даних у режимі датаграм із мінімальними затримками, що є особливо важливим для безперервних потоків біометричної телеметрії у реальному часі [6]. У сучасних оглядових дослідженнях, присвячених носимим спортивним IoT-технологіям [1, 10, 16], детально описано класи сенсорів, методи обробки біомедичних сигналів, архітектури інтеграції з хмарними платформами та особливості забезпечення кібербезпеки в таких системах.

Окремі дослідження систематизують підходи до автентифікації в IoT-орієнтованій медицині, пропонуючи класифікації схем автентифікації за технологічними рівнями (хмара, туман, периферія), аналізують атаки й порівнюють ефективність різних протоколів, включно з паролями, біометрією, криптографією на еліптичних кривих та легковаговими протоколами обміну ключами [7, 15]. Значний масив публікацій присвячено вразливостям Bluetooth Low Energy, типовим атакам на процес парування, проблемам повторного використання ключів і нешифрованого трафіку, а також заходам щодо їхнього пом'якшення [8, 11].

У сфері захисту даних про здоров'я та носимих пристроїв активно досліджуються питання конфіденційності, етичні й правові аспекти обробки біометричної інформації, ризики деанонімізація, профілювання та потенційної дискримінації спортсменів [9, 12, 13]. Водночас у працях, присвячених мікросервісним веб-системам та хмарним платформам [15], розроблено моделі управління доступом з використанням токенів JWT, асиметричного підпису, ротації ключів і механізмів відкликання скомпрометованих токенів, що можуть бути адаптовані до серверних частин спортивних IoT-платформ.

Попри наявність значної кількості досліджень, недостатньо опрацьованими залишаються прикладні питання інтеграції вимог стандартів з безпеки IoT, хмарних та edge-рішень із реальними обмеженнями спортивних сенсорних мереж. Бракує моделей, які поєднують енергоефективне шифрування, безпечну автентифікацію пристроїв, управління ключами, політики доступу до даних і вимоги конфіденційності в єдину архітектуру, адаптовану саме до спортивного середовища. Це визначає наукову новизну та практичну значущість проведеного дослідження.

Мета статті. Метою статті є узагальнення сучасних підходів до безпеки IoT-пристроїв і розроблення концептуальної моделі захисту сенсорних мереж для моніторингу здоров'я спортсменів, яка враховує багаторівневу архітектуру спортивних IoT-систем, особливості бездротових протоколів, обмежені ресурси сенсорів і вимоги до конфіденційності, цілісності та доступності біометричних даних. Для досягнення цієї мети необхідно: проаналізувати існуючі стандарти та наукові дослідження, описати узагальнену архітектуру спортивної IoT-системи, ідентифікувати ключові загрози на кожному рівні й запропонувати практичні рекомендації щодо їхнього пом'якшення.

ТЕОРЕТИЧНІ ОСНОВИ ДОСЛІДЖЕННЯ

Технології Інтернету речей у спорті ґрунтуються на ідеї створення екосистеми взаємопов'язаних сенсорів, мобільних шлюзів, серверних і хмарних компонентів, що забезпечують безперервний цикл «вимірювання – передача – аналіз – управління» [1, 2]. Біометричні сенсори, вбудовані в одяг, ремені, браслети або закріплені безпосередньо на тілі спортсмена, формують потоки даних про серцево-судинну, дихальну та опорно-рухову системи. Акселерометри, гіроскопи та GPS-модулі характеризують кінематику рухів і просторове положення, а додаткові сенсори контролюють показники сну, стресу та відновлення [1].

У контексті безпеки ключовими вимогами до таких систем є конфіденційність, цілісність, доступність і відстежуваність даних. Конфіденційність передбачає захист біометричної інформації від несанкціонованого доступу під час передавання, зберігання й обробки. Цілісність означає неможливість непомітного спотворення показників, що є критичним для коректності медичних висновків і тренерських рішень. Доступність гарантує своєчасний доступ уповноважених користувачів до даних, особливо під час медичних інцидентів. Відстежуваність забезпечується за рахунок ведення журналів подій, що дає змогу ідентифікувати джерело змін і відтворити хронологію доступу до інформації [3, 14].

У спортивних IoT-системах ці вимоги накладаються на жорсткі обмеження енергоспоживання, обчислювальних ресурсів і допустимих затримок передавання даних. Це потребує адаптації класичних криптографічних механізмів, використання легковагових протоколів, апаратної підтримки безпеки в сенсорах і ретельного проєктування архітектури всієї системи. Значний потенціал має використання edge-

обчислень, коли частина аналітики переноситься ближче до джерела даних (на сенсор або шлюз), що дає змогу зменшити обсяг переданих сирих даних, знизити затримки та покращити конфіденційність [10, 11].

Суттєвий вплив на організацію захисту мають також нормативні рамки. Стандарт ISO/IEC 27001:2022 пропонує системний підхід до управління інформаційною безпекою на рівні організації, включно з політиками доступу, управління ризиками, інцидент-менеджментом та постійним удосконаленням системи захисту [14]. Поєднання вимог інформаційної безпеки на рівні організації зі спеціалізованими рекомендаціями для IoT-пристроїв створює основу для побудови цілісних політик безпеки спортивних сенсорних мереж.

МЕТОДИКА ДОСЛІДЖЕННЯ

Дослідження має аналітико-оглядовий характер і ґрунтується на комплексному вивченні міжнародних стандартів безпеки IoT-пристроїв, нормативних рекомендацій щодо захисту бездротових протоколів, наукових публікацій у галузі спортивних носимих технологій, електронної охорони здоров'я та кібербезпеки сенсорних мереж. Було здійснено порівняльний аналіз вимог NIST SP 800-213/213A, рекомендацій ENISA та специфікацій протоколу DTLS 1.3 з позицій їхнього застосування в спортивних системах моніторингу здоров'я [3-6].

На основі аналізу праць, присвячених автентифікації в IoT-орієнтованій медицині, безпеці BLE, конфіденційності носимих пристроїв і архітектурі IoT у спорті, сформовано узагальнену багаторівневу модель спортивної IoT-платформи з виділенням сенсорного, шлюзового, серверного та прикладного рівнів. Для кожного рівня визначено типові загрози (перехоплення, підміна, несанкціонований доступ, підробка пристрою, компрометація ключів, помилки конфігурації) та можливі механізми захисту з урахуванням ресурсних обмежень і режиму реального часу.

Практичні аспекти моделі проілюстровано на прикладі реальних рішень, у яких уже використовуються енергоефективні алгоритми шифрування, апаратні модулі безпеки, edge-аналітика, методи псевдонімізації даних і багаторівневе шифрування [8, 10-13]. Таке поєднання теоретичного аналізу й прикладних кейсів дає змогу оцінити реалізовність запропонованих підходів у реальних спортивних клубах та командах, а також сформувати пропозиції щодо удосконалення існуючих практик.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Отримані результати свідчать, що сучасні спортивні IoT-системи формуються як багаторівневі, взаємозалежні архітектури, у яких кожен рівень – від сенсора до хмарної платформи – одночасно є джерелом корисних даних і потенційною точкою уразливості. Аналіз нормативних вимог, наукових досліджень і практичних рішень дав змогу уточнити структуру такої системи, визначити ключові загрози на кожному її рівні та сформувати відповідні механізми захисту.

Узагальнена архітектура спортивної IoT-системи (див. рис. 1) охоплює сенсорний, шлюзовий, серверний та прикладний рівні, які утворюють замкнутий цикл «збір – передавання – аналіз – управління». Кожен рівень виконує унікальні функції та потребує окремого набору технічних і організаційних заходів безпеки.

Сенсорний рівень: захищене вимірювання й передавання. На нижньому рівні функціонують носимі сенсори, які збирають біометричні показники (пульс, ЕКГ, ЕМГ,

температуру тіла, частоту дихання), дані про рухову активність і геолокацію спортсмена [1, 2]. Передавання даних до шлюзу здійснюється через енергоефективні протоколи BLE, ANT+ або Zigbee. Для зниження ризиків прослуховування й підміни трафіку доцільним є використання BLE у режимі LE Secure Connections з AES-CCM та ECC, а також застосування безпечних сценаріїв парування (Numeric Comparison, Passkey) [8]. Частина попередньої обробки (фільтрація, ресемплінг, обчислення базових метрик) може виконуватися безпосередньо на сенсорі, що зменшує обсяг сирих даних, які передаються каналами зв'язку.

Ключову роль відіграють механізми забезпечення довіри до програмного забезпечення сенсорів. Реалізація безпечного завантаження (secure boot) із перевіркою цифрового підпису прошивки перед запуском, а також використання підписаних оновлень OTA з контрольними сумами унеможливлюють непомітну зміну коду на пристрої. Для захищеного зберігання криптографічних ключів доцільно використовувати апаратні модулі безпеки (Secure Element, TPM), які ізолюють секрети від основного обчислювального середовища й суттєво ускладнюють фізичні атаки [3, 4, 8]. Практичну реалізовність таких рішень підтверджують промислові платформи для IoT, у яких A71CH використовується як окремий Secure Element із підтримкою захищеного зберігання ключів, chip-to-cloud автентифікації та захисту від фізичних і логічних атак [17].

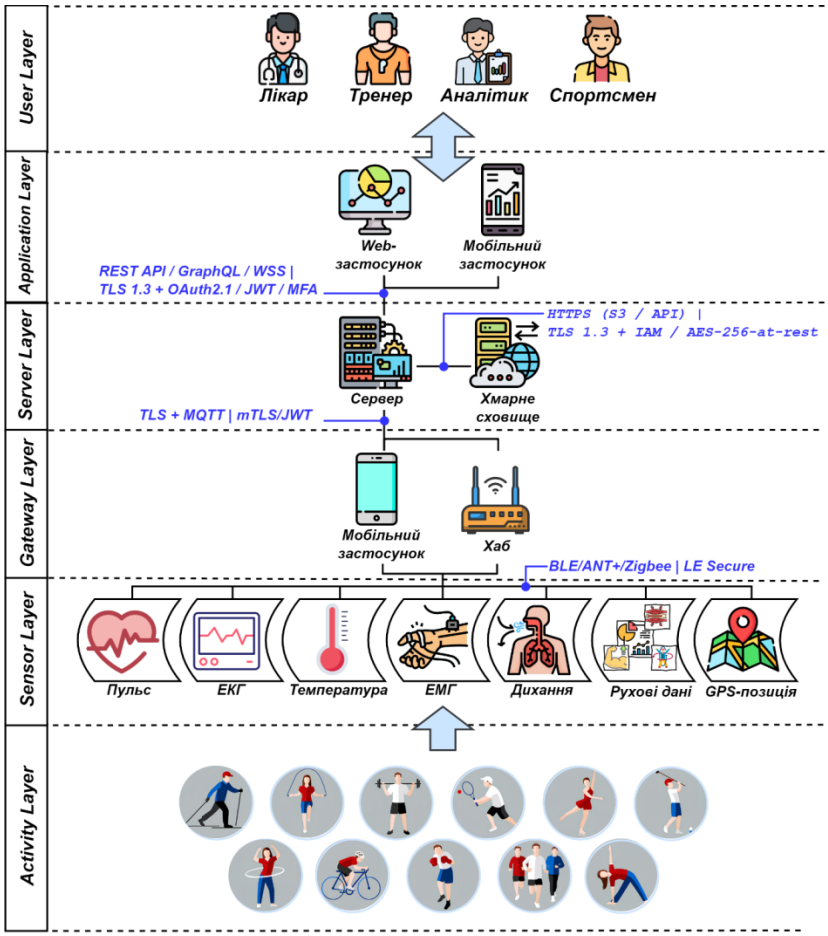

Рис. 1. Багаторівнева архітектура спортивної IoT-системи

Шлюзовий рівень: агрегація, edge-аналітика та взаємна автентифікація. Шлюз, роль якого виконують смартфон, спортивний годинник, спеціалізований хаб чи базова станція, приймає дані від кількох сенсорів, агрегує їх і здійснює попередню аналітику. З'єднання між шлюзом і серверною частиною зазвичай організовується через MQTT або HTTPS, поверх яких налаштовуються захищені сесії на базі TLS 1.3. Впровадження взаємної автентифікації (mTLS) дає змогу перевіряти справжність як сервера, так і шлюзу за допомогою сертифікатів, виданих у процесі безпечного виробничого налаштування (secure provisioning) [6-8].

На цьому рівні доцільно реалізовувати елементи edge-аналітики. Частина задач (виявлення аномалій, розрахунок узагальнених показників навантаження, виявлення критичних станів) може виконуватися локально, без пересилання у хмару повних часових рядів [10; 11]. Це зменшує вимоги до пропускної здатності каналів, скорочує затримки та знижує ризики витоку чутливої інформації. Зокрема, алгоритми машинного навчання у спрощених реалізаціях (on-device AI) можуть працювати на шлюзі й формувати оперативні рекомендації тренеру чи спортсмену, тоді як у хмару передаються лише агреговані статистичні характеристики.

Серверний рівень: масштабована аналітика й управління ключами. Серверний рівень відповідає за прийом, перевірку й аналітичну обробку телеметрії, довготривале зберігання даних та управління ідентичностями. Дані часових рядів зберігаються в спеціалізованих TSDB-сховищах, файли сесій – в об'єктних сховищах (S3/MinIO), а профілі користувачів та конфігураційна інформація – у реляційних базах.

Захист даних «на носії» забезпечується шифруванням з використанням сучасних симетричних алгоритмів (наприклад, AES-256) і централізованим управлінням ключами. Для захисту API, що обслуговують прикладні клієнти, застосовуються токени JWT з обмеженим часом дії, асиметричним підписом і механізмами ротації ключів. Важливим результатом аналізу є виділення вимог до інфраструктури управління ключами: кожен сенсор і шлюз мають отримувати унікальні ключі та сертифікати під час secure provisioning, а система повинна підтримувати швидке відкликання (revocation) у разі втрати чи компрометації пристрою [7, 9, 14, 15].

Інтеграція вимог ISO/IEC 27001:2022 дозволяє узгодити технічні механізми з організаційними процесами управління ризиками, інцидентами та доступом до інформаційних ресурсів, що є критично важливим для великих спортивних клубів і федерацій [14].

Прикладний рівень: контроль доступу та керування пристроями. Прикладний рівень представлений веб- і мобільними застосунками для спортсменів, тренерів, лікарів, аналітиків й адміністративного персоналу. Доступ до функціоналу здійснюється через протоколи REST, GraphQL або WebSocket поверх TLS 1.3 із використанням OAuth 2.1, токенів доступу, багатофакторної автентифікації й детальних ролей доступу.

Запропонована модель розмежування доступу передбачає, що лікар має право переглядати повний медичний профіль спортсмена, тренер – лише узагальнені показники навантаження та відновлення, аналітик – деперсоніфіковані агреговані дані, адміністративний персонал – обмежений набір службової інформації. Усі дії користувачів фіксуються у журналах аудиту, які захищені від редагування та підлягають регулярному аналізу.

Зворотний канал використовується для керування конфігурацією сенсорів і виконання оновлень прошивок. Для цього застосовується керування через MQTT-теми (control) у поєднанні з підписаними пакетами OTA (Signed OTA), цілісність яких

перевіряється за допомогою HMAC або цифрового підпису. Така схема мінімізує ризики несанкціонованої зміни режиму роботи пристрою або інсталяції шкідливої прошивки [3, 4, 7].

Конфіденційність, псевдонімізація та етичні аспекти. Окремий блок результатів стосується конфіденційності та етичних аспектів обробки біометричних даних спортсменів. Показано, що навіть анонімізовані набори геолокаційних даних за відсутності додаткового захисту можуть бути використані для деанонімізація і відновлення маршруту окремих спортсменів, що створює ризики стеження й небажаного профілювання [9, 12, 13].

Перспективним рішенням є застосування псевдонімізації та «коарсингу» геоданих, коли точність координат навмисно знижується до рівня, достатнього для аналізу навантаження, але недостатнього для точного визначення місця перебування. Подібні підходи вже реалізуються в ряді комерційних систем моніторингу у командних видах спорту, що підтверджує їхню практичну доцільність [1, 13].

Запровадження прозорих політик інформованої згоди, обмеження строків зберігання даних, чітке визначення цілей їхнього використання та заборона дискримінаційних рішень на основі алгоритмічного аналізу є ключовими елементами етичного використання спортивних IoT-систем [4, 9, 12, 13].

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Проведене дослідження показало, що ефективний моніторинг здоров’я спортсменів на базі Інтернету речей неможливий без цілеспрямованого впровадження багаторівневих механізмів безпеки. Сенсорний, шлюзовий, серверний та прикладний рівні мають власні специфічні загрози й обмеження, однак лише їх узгоджене врахування дозволяє сформувати цілісну захищену екосистему. Надійні механізми шифрування й автентифікації, безпечне оновлення прошивок, управління ключами, контроль доступу та аудит дій користувачів становлять фундамент довіри до цифрових рішень у спорті.

Запропонована в роботі концептуальна модель багаторівневої архітектури спортивної IoT-системи дає можливість:

- по-перше, описати логічне розділення функцій між сенсорним, шлюзовим, серверним та прикладним рівнями;
- по-друге, прив’язати до кожного з них характерні загрози та відповідні механізми захисту;
- по-третє, інтегрувати технічні заходи з організаційними політиками та міжнародними стандартами. Такий підхід підвищує прозорість і керованість системи з погляду кібербезпеки.

Практична значущість одержаних результатів полягає у тому, що вони можуть бути використані як методологічна основа під час проєктування та аудиту систем моніторингу здоров’я спортсменів, впровадження носимих технологій у спортивних клубах і федераціях, розроблення регламентів доступу до біометричних даних та внутрішніх політик інформаційної безпеки. Врахування описаних вимог на ранніх етапах життєвого циклу системи (від вибору сенсорів та архітектури платформи до експлуатації та виведення з користування) дозволяє зменшити ризики інцидентів і витрат на їх усунення.

Перспективи подальших досліджень пов’язані з кількома напрямами. По-перше, актуальним є розроблення й тестування легковагових криптографічних протоколів,

спеціально оптимізованих під спортивні сенсорні мережі, з урахуванням обмежень енергоспоживання та вимог реального часу. По-друге, потребує розвитку моделювання ризиків для різних видів спорту, з урахуванням специфіки навантажень, інтенсивності тренувальних циклів та рівня підготовленості спортсменів (професійний, юнацький, паралімпійський спорт). По-третє, важливим завданням є створення стандартизованих профілів безпеки для спортивних федерацій і клубів, які враховуватимуть кращі практики NIST, ENISA та ISO/IEC 27001 і водночас адаптуватимуть їх до конкретних умов національних чемпіонатів і міжнародних змагань.

Окремого розвитку потребує інтеграція технологій штучного інтелекту з механізмами захисту даних у спортивних IoT-системах. Моделі, що аналізують великі масиви біометричної інформації та прогнозують ризики перевантажень, повинні функціонувати в режимі контрольованої та пояснюваної аналітики, із чіткими правилами доступу до алгоритмів і результатів їхньої роботи. Важливим аспектом є забезпечення коректності дій таких систем: алгоритми мають бути захищені від некоректних інтерпретацій та помилкових висновків, що можуть виникати внаслідок алгоритмічних спотворень чи «галюцинацій». Тому необхідні механізми перевірки достовірності виводів, обмеження автономності рішень і наявність гарантованого людського контролю, особливо коли йдеться про рекомендації щодо інтенсивності навантаження чи медичної допомоги. Поряд із цим зберігають значущість етичні та правові вимоги: інформована згода спортсменів, прозорість політик зберігання й обробки даних, недопустимість дискримінаційних наслідків алгоритмічного аналізу та відповідність сучасним регуляторним актам у сфері цифрового здоров’я.

У підсумку підвищення рівня безпеки сенсорних мереж у спорті є ключовою передумовою формування культури довіри до цифрової медицини та персоналізованого спорту. Лише за умови поєднання технічних, організаційних та етичних підходів технології Інтернету речей зможуть служити інструментом збереження здоров’я й підвищення результатів без загрози для приватності та безпеки спортсмена.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Seçkin, A. Ç., Ateş, B., & Seçkin, M. (2023). Review on wearable technology in sports: Concepts, challenges and opportunities. *Applied Sciences, 13*(18), 10399. https://doi.org/10.3390/app131810399
2. Tunc, M. A., Gures, E., & Shayea, I. (2021). A survey on IoT smart healthcare: Emerging technologies, applications, challenges, and future trends. *arXiv*. https://doi.org/10.48550/arXiv.2109.02042
3. National Institute of Standards and Technology. (2021a). *IoT device cybersecurity guidance for the federal government: Establishing IoT device cybersecurity requirements (NIST SP 800-213)*. https://doi.org/10.6028/nist.sp.800-213
4. National Institute of Standards and Technology. (2021b). *IoT device cybersecurity guidance for the federal government: IoT device cybersecurity requirement catalog (NIST SP 800-213A)*. https://doi.org/10.6028/nist.sp.800-213a
5. European Union Agency for Cybersecurity. (2020). *Guidelines for securing the Internet of Things: Secure supply chain for IoT*. ENISA. https://doi.org/10.2824/314452
6. Rescorla, E., Tschofenig, H., & Modadugu, N. (2022). *The datagram transport layer security (DTLS) protocol version 1.3 (RFC 9147)*. RFC Editor. https://doi.org/10.17487/rfc9147
7. Khan, M., Din, I., Tha’er, M., & Kim, B.-S. (2022). A survey of authentication in Internet of Things-enabled healthcare systems. *Sensors, 22*(23), 9089. https://doi.org/10.3390/s22239089
8. Barua, A., Alamin, M. A. A., Hossain, M. S., & Hossain, E. (2022). Security and privacy threats for Bluetooth Low Energy in IoT and wearable devices: A comprehensive survey. *IEEE Open Journal of the Communications Society, 2*, 251–281. https://doi.org/10.1109/OJCOMS.2022.3149732

9. Makina, H., Letaifa, A. B., & Rachedi, A. (2023). Survey on security and privacy in Internet of Things-based eHealth applications: Challenges, architectures, and future directions. *Security and Privacy*, *7*(2). https://doi.org/10.1002/spy2.346
10. Singh, A., & Chatterjee, K. (2022). Edge computing-based secure health monitoring framework for electronic healthcare systems. *Cluster Computing*. https://doi.org/10.1007/s10586-022-03717-w
11. Rancea, A., Anghel, I., & Cioara, T. (2024). Edge computing in healthcare: Innovations, opportunities, and challenges. *Future Internet*, *16*(9), 329. https://doi.org/10.3390/fi16090329
12. Cao, W., Shen, W., Zhang, Z., & Qin, J. (2023). Privacy-preserving healthcare monitoring for IoT devices under edge computing. *Computers & Security*, 103464. https://doi.org/10.1016/j.cose.2023.103464
13. Zhang, B., Chen, C., Lee, I., Lee, K., & Ong, K.-L. (2025). A survey on security and privacy issues in wearable health monitoring devices. *Computers & Security*, 104453. https://doi.org/10.1016/j.cose.2025.104453
14. IT Governance Publishing. (2022). *ISO/IEC 27001:2022 and the management system requirements* (pp. 17–21). https://doi.org/10.2307/j.ctv30qq13d.6
15. Kuzmenko, D. S., & Ivanov, V. H. (2024). Security of a genealogical information retrieval system: Modern access control mechanisms. In *Proceedings of the All-Ukrainian scientific and practical conference "Telecommunications, automation, computer-integrated technologies"* (pp. 45–47). Donetsk National Technical University.
16. Van Hooren, B., Goudsmit, J., Restrepo, J., & Vos, S. (2019). Real-time feedback by wearables in running: Current approaches, challenges and suggestions for improvements. *Journal of Sports Sciences, 38*(2), 214–230. https://doi.org/10.1080/02640414.2019.1690960
17. NXP Semiconductors. (2018). *A71CH Plug & Trust secure element: Data sheet (Rev. 1.2)*. https://www.nxp.com/docs/en/data-sheet/A71CH.pdf

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (32), 2026
ISSN 2663 – 4023

Kuzmenko Dmytro
Master's degree
Kharkiv National University of Radio Elecrtonics, Kharkiv, Ukraine
ORCID: 0009-0006-1366-9530
dmytro.kuzmenko@nure.ua

Konovalenko Oksana
Senior Lecturer of the Department of Physical Education and Sports
Kharkiv National University of Radio Elecrtonics, Kharkiv, Ukraine
ORCID: 0000-0002-7707-0969
oksana.konovalenko@nure.ua

INTERNET OF THINGS IN SPORTS: SECURITY OF SENSOR NETWORKS FOR HEALTH MONITORING

Abstract. The article addresses the problem of ensuring the security of sensor networks used for athlete health monitoring within Internet of Things (IoT) ecosystems. It is demonstrated that the digitalisation of sports and the widespread adoption of wearable sensing devices connected to mobile gateways and cloud platforms create a new class of risks related to the confidentiality, integrity, and availability of biometric data. Based on an analysis of international standards and recommendations, including NIST SP 800-213/213A, ENISA guidelines, and ISO/IEC 27001, as well as contemporary research on sports IoT technologies, eHealth, BLE security, and authentication in IoT-enabled healthcare, a conceptual multi-layer security model for sports IoT systems is developed. The proposed approach distinguishes sensor, gateway, server, and application layers, each characterised by its functional role, typical threats, and specific mitigation mechanisms that take into account device resource constraints and real-time operational requirements. At the sensor layer, the study substantiates the use of energy-efficient cryptographic algorithms, BLE LE Secure Connections mode, secure boot, signed OTA firmware updates, and hardware security modules such as Secure Elements for protected key storage. At the gateway layer, the use of MQTT and HTTPS over TLS 1.3, mutual authentication (mTLS), as well as the implementation of edge analytics and on-device AI, is examined to reduce the volume of raw data transmitted and to enhance privacy. The server layer is described as a domain of scalable analytics and identity management, where data-at-rest encryption, centralised key management, short-lived and rotation-enabled JWT tokens, and key revocation mechanisms are applied. At the application layer, a role-based access model for physicians, coaches, analysts, and administrative personnel is proposed, along with multi-factor authentication, protected audit logging, and controlled firmware updates via Signed OTA. Particular attention is given to the confidentiality of geolocation data, the use of pseudonymisation and coordinate coarsening, as well as ethical and legal aspects of processing athletes' biometric information. The results show that the proposed model can serve as a methodological foundation for designing, auditing, and standardising digital solutions in both professional and recreational sports, including the development of internal security policies in clubs and sports federations. The integration of technical, organisational, and regulatory measures, complemented by mechanisms for validating the reliability of AI-generated decisions and limiting the autonomy of algorithmic outputs, is identified as a prerequisite for building a robust, trustworthy, and resilient health monitoring ecosystem in sports based on the Internet of Things.

Keywords: Internet of Things (IoT); sports sensor networks; information security; biometric data; encryption protocols; data protection; health monitoring; wearable devices.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Seçkin, A. Ç., Ateş, B., & Seçkin, M. (2023). Review on wearable technology in sports: Concepts, challenges and opportunities. *Applied Sciences, 13*(18), 10399. https://doi.org/10.3390/app131810399
2. Tunc, M. A., Gures, E., & Shayea, I. (2021). A survey on IoT smart healthcare: Emerging technologies, applications, challenges, and future trends. *arXiv*. https://doi.org/10.48550/arXiv.2109.02042

3. National Institute of Standards and Technology. (2021a). *IoT device cybersecurity guidance for the federal government: Establishing IoT device cybersecurity requirements (NIST SP 800-213)*. https://doi.org/10.6028/nist.sp.800-213
4. National Institute of Standards and Technology. (2021b). *IoT device cybersecurity guidance for the federal government: IoT device cybersecurity requirement catalog (NIST SP 800-213A)*. https://doi.org/10.6028/nist.sp.800-213a
5. European Union Agency for Cybersecurity. (2020). *Guidelines for securing the Internet of Things: Secure supply chain for IoT*. ENISA. https://doi.org/10.2824/314452
6. Rescorla, E., Tschofenig, H., & Modadugu, N. (2022). *The datagram transport layer security (DTLS) protocol version 1.3 (RFC 9147)*. RFC Editor. https://doi.org/10.17487/rfc9147
7. Khan, M., Din, I., Tha'er, M., & Kim, B.-S. (2022). A survey of authentication in Internet of Things-enabled healthcare systems. *Sensors*, *22*(23), 9089. https://doi.org/10.3390/s22239089
8. Barua, A., Alamin, M. A. A., Hossain, M. S., & Hossain, E. (2022). Security and privacy threats for Bluetooth Low Energy in IoT and wearable devices: A comprehensive survey. *IEEE Open Journal of the Communications Society*, *2*, 251–281. https://doi.org/10.1109/OJCOMS.2022.3149732
9. Makina, H., Letaifa, A. B., & Rachedi, A. (2023). Survey on security and privacy in Internet of Things-based eHealth applications: Challenges, architectures, and future directions. *Security and Privacy*, *7*(2). https://doi.org/10.1002/spy2.346
10. Singh, A., & Chatterjee, K. (2022). Edge computing-based secure health monitoring framework for electronic healthcare systems. *Cluster Computing*. https://doi.org/10.1007/s10586-022-03717-w
11. Rancea, A., Anghel, I., & Cioara, T. (2024). Edge computing in healthcare: Innovations, opportunities, and challenges. *Future Internet*, *16*(9), 329. https://doi.org/10.3390/fi16090329
12. Cao, W., Shen, W., Zhang, Z., & Qin, J. (2023). Privacy-preserving healthcare monitoring for IoT devices under edge computing. *Computers & Security*, 103464. https://doi.org/10.1016/j.cose.2023.103464
13. Zhang, B., Chen, C., Lee, I., Lee, K., & Ong, K.-L. (2025). A survey on security and privacy issues in wearable health monitoring devices. *Computers & Security*, 104453. https://doi.org/10.1016/j.cose.2025.104453
14. IT Governance Publishing. (2022). *ISO/IEC 27001:2022 and the management system requirements* (pp. 17–21). https://doi.org/10.2307/j.ctv30qq13d.6
15. Kuzmenko, D. S., & Ivanov, V. H. (2024). Security of a genealogical information retrieval system: Modern access control mechanisms. In *Proceedings of the All-Ukrainian scientific and practical conference "Telecommunications, automation, computer-integrated technologies"* (pp. 45–47). Donetsk National Technical University.
16. Van Hooren, B., Goudsmit, J., Restrepo, J., & Vos, S. (2019). Real-time feedback by wearables in running: Current approaches, challenges and suggestions for improvements. *Journal of Sports Sciences, 38*(2), 214–230. https://doi.org/10.1080/02640414.2019.1690960
17. NXP Semiconductors. (2018). *A71CH Plug & Trust secure element: Data sheet (Rev. 1.2)*. https://www.nxp.com/docs/en/data-sheet/A71CH.pdf

Отримано редакцією журналу / Received: 27.01.26
Прорецензовано / Revised: 18.02.26
Схвалено до друку / Accepted: 26.03.26