Кіберстійкість розумних засобів індивідуального захисту: алгоритмічний метод попередження виробничого травматизму

Cyber Resilience of Smart Personal Protective Equipment: an Algorithmic Method for Preventing Occupational Injuries

Олена Крайнюк [A]

Corresponding author: кандидат технічних наук, доцент, завідувачка кафедри кібербезпеки, e-mail: cyber@khadi.kharkov.ua, ORCID ID: https://orcid.org/0000-0001-9524-040X

Юрій Буц

доктор технічних наук, професор, завідувач кафедри охорони праці та надзвичайних ситуацій, e-mail: buc@kart.edu.ua, ORCID ID: https://orcid.org/0000-0003-0450-2617

Михайло Піксасов [A]

кандидат технічних наук, доцент, доцент кафедри кібербезпеки, e-mail: mpiks77@gmail.com, ORCID ID: https://orcid.org/0000-0001-9487-7273

Наталя Діденко [A]

кандидат технічних наук, доцент, доцент кафедри кібербезпеки, e-mail: nataly.v.didenko@gmail.com, ORCID ID: https://orcid.org/0000-0003-3318-438X

Борис Походенко [A]

старший викладач кафедри кібербезпеки, e-mail: boris.pokhodenko@gmail.com, ORCID ID: https://orcid.org/0000-0002-9995-7077

Olena Krainiuk [A]

Corresponding author: Candidate of Technical Sciences, Associate Professor, Head of the Department of Cybersecurity, e-mail: cyber@khadi.kharkov.ua, ORCID ID: https://orcid.org/0000-0001-9524-040X

Yuriy Buts

Doctor of Technical Sciences, Professor, Head of the Department of Occupational Safety and Emergency Situations, e-mail: buc@kart.edu.ua, ORCID ID: https://orcid.org/0000-0003-0450-2617

Mykhailo Piksasov [A]

кандидат технічних наук, доцент, доцент кафедри кібербезпеки, e-mail: mpiks77@gmail.com, ORCID ID: https://orcid.org/0000-0001-9487-7273

Natalia Didenko [A]

Candidate of Technical Sciences, Associate Professor, Associate Professor of the Department of Cybersecurity, e-mail: nataly.v.didenko@gmail.com, ORCID ID: https://orcid.org/0000-0003-3318-438X

Boris Pokhodenko [A]

Senior Lecturer, Department of Cybersecurity, e-mail: boris.pokhodenko@gmail.com, ORCID ID: https://orcid.org/0000-0002-9995-7077

[A] Харківський національний автомобільно-дорожній університет, м. Харків, Україна

[B] Український державний університет залізничного транспорту, м. Харків, Україна

[A] Kharkiv National Automobile and Highway University, Kharkiv, Ukraine

[B] Ukrainian State University of Railway Transport, Kharkiv, Ukraine

Received: January 05, 2026 | Revised: February 11, 2026 | Accepted: April 30, 2026

UDC 004.056.5:331.45:614.89

DOI: https://doi.org/10.33445/sds.2025.16.2.23

Мета роботи. Дослідження спрямоване на розв'язання науково-технічної суперечності між необхідністю криптографічного захисту каналів зв'язку в системах Smart PPE та обмеженими енергетичними ресурсами автономних мікроконтролерів. Метою статті є обґрунтування та розробка енергоефективного алгоритмічного методу забезпечення цілісності телеметричних даних, що дозволяє інтегрувати механізми кіберстійкості в контур промислової безпеки без втрати автономності засобів захисту.

Метод дослідження. Аналіз векторів загроз кіберфізичним системам промислової безпеки (моделювання сценаріїв атаки посередника); порівняльний аналіз накладних витрат стандартних протоколів передачі даних промислового інтернету речей; імітаційне моделювання процедури верифікації даних на основі алгоритму легкої криптографії SipHash-2-4; розрахункова оцінка часової складності та енергоефективності запропонованого методу порівняно з існуючими стандартами AES-CMAC та HMAC-SHA256. Об'єктом дослідження є процеси передачі та верифікації телеметричних даних у контурі моніторингу безпеки персоналу. Такий підхід дозволяє логічно поєднати цілісність даних із їх кінцевим призначенням — захистом життя.

Purpose. This study aims to resolve the scientific and technical contradiction between the need for cryptographic protection of communication channels in Smart PPE systems and the limited power resources of autonomous microcontrollers. The purpose of this article is to justify and develop an energy-efficient algorithmic method for ensuring the integrity of telemetric data, which allows for the integration of cyber resilience mechanisms into the industrial security framework without compromising the autonomy of the protection measures.

Methodology. The study employs an analysis of threat vectors to cyber-physical industrial safety systems (modeling of Man-in-the-Middle attack scenarios); a comparative analysis of the overhead of standard Industrial Internet of Things (IIoT) data transmission protocols; mathematical modeling of the data verification procedure based on the SipHash-2-4 lightweight cryptography algorithm; and a computational assessment of the time complexity and energy efficiency of the proposed method compared to existing AES-CMAC and HMAC-SHA256 standards. The subject of this study is the transmission and verification of telemetry data within a personnel safety monitoring system. This approach allows for a logical integration of data integrity with its ultimate purpose—the protection of human life.

Теоретична цінність дослідження. Дослідження поглиблює розуміння інверсії пріоритетів тріади інформаційної безпеки у системах охорони праці (пріоритет цілісності над конфіденційністю). Доведено теоретичну обґрунтованість застосування легких хеш-функцій як достатнього засобу захисту для пристроїв польового рівня (Level 0-1 за IEC 62443), що дозволяє інтегрувати механізми кіберзахисту в контур безпеки життєдіяльності без створення критичних затримок у передачі аварійних сигналів.

Практична цінність дослідження. Запропонований алгоритм дозволяє нівелювати ризики приховування реальних небезпек (сценарій «хибного спокою») та генерації хибних тривог, гарантуючи диспетчерським службам отримання достовірної інформації для прийняття рішень про евакуацію. Результати імітаційного моделювання підтверджують можливість подовження часу автономної роботи розумних засобів захисту на 15–20 % порівняно з традиційними методами шифрування, що забезпечує надійність безперервного моніторингу протягом повної робочої зміни.

Тип статті. Науково-практичний.

Theoretical Value. The study deepens the understanding of the priority inversion within the information security triad (CIA) in occupational safety systems (prioritizing integrity over confidentiality). The theoretical feasibility of using lightweight hash functions as a sufficient protection measure for field-level devices (Level 0-1 according to IEC 62443) is proven; this enables the integration of cybersecurity mechanisms into the safety loop without inducing critical latency in emergency signal transmission.

Practical Value. The proposed algorithm mitigates the risks of concealing real hazards (the "False Negative" scenario) and generating false alarms, ensuring that dispatch services receive reliable information for evacuation decision-making. Calculations confirm that the autonomous battery life of Smart PPE can be extended by 15–20% compared to traditional encryption methods, thereby ensuring reliable continuous monitoring throughout a full work shift.

Type of Article. Scientific and practical.

Ключові слова: розумні засоби індивідуального захисту; охорона праці; промисловий Інтернет речей; цілісність даних; легка криптографія; SipHash; виробничий травматизм.

Key words: Smart Personal Protective Equipment, Occupational Safety, Industrial IoT, Data Integrity, lightweight Cryptography, SipHash, Occupational Injury.

Вступ

Глобальна цифрова трансформація промислового сектору відбувається на тлі тривожної статистики: щорічно у світі гинуть майже 3 мільйони людей внаслідок виробничих нещасних випадків та професійних захворювань, а ще 395 мільйонів працівників отримують нефатальні травми (International Labour Organization, звіт 2023). У відповідь на ці виклики відбувається перехід до людиноцентричної парадигми Industry 5.0 (Lisovska et al., 2019), де працівник та роботизовані системи функціонують у єдиному синергетичному контурі. У цьому контексті традиційні засоби індивідуального захисту (ЗІЗ) еволюціонують у розумні кіберфізичні системи (Smart PPE).

Сучасні розумні каски та браслети, оснащені масивом IoT-сенсорів (датчики газів, акселерометри, пульсометри, GPS-модулі), генерують критично важливі телеметричні дані для автоматизованих систем безпеки: від екстреної зупинки обладнання до ініціації аварійної евакуації. Проте інтеграція ЗІЗ у цифровий простір створює новий клас загроз. Протягом 2024–2025 років фіксується експоненційне зростання кількості атак на IIoT, зокрема на виробничі системи, SCADA та енергетичні мережі (Haiduk & Zverev 2024; Zhukabayeva, 2025). Масштаби проблеми ілюструє статистика Microsoft Entra: лише у березні–квітні 2023 року кількість атак на паролі (один із основних векторів компрометації IoT/IIoT) зросла з 3 до понад 30 млрд на місяць, що становить більше 11 000 атак на секунду. Ця загрозлива тенденція зберігається і у 2024 році (Haiduk, 2024). Прогнози на 2025 рік свідчать, що для промислових систем основними векторами залишаються атаки на відмову в обслуговуванні (DoS/DDoS), програми-вимагачі (ransomware) та шкідливе програмне забезпечення, а також цілеспрямовані атаки на цілісність даних.

Виникає фундаментальна інженерна дилема: архітектура сучасних розумних ЗІЗ спирається на енергоефективні мікроконтролери з компактними батареями, для яких використання “важких” традиційних протоколів безпеки, на кшталт DTLS 1.2, стає непосильним тягарем. Такі методи вимагають надмірних витрат енергії, здатних поглинути до половини ємності акумулятора лише на підтримку захищеного з’єднання, що не тільки порушує вимоги стандарту IEC 62443 щодо економії ресурсів, але й створює небезпечну часову затримку у передачі даних. У критичних ситуаціях, наприклад при раптовому викиді метану, навіть кілька секунд зволікання можуть стати фатальними для персоналу, який не встигне

отримати сигнал про евакуацію (Крайнюк із співавт., 2024). Водночас проста відмова від шифрування заради швидкодії є неприйнятною, оскільки залишає систему беззахисною перед атаками підміни даних, коли зловмисник може непомітно модифікувати показники та створити у диспетчера хибну ілюзію безпеки на об'єкті.

Мета статті: обґрунтування та розробка енергоефективного алгоритмічного методу забезпечення цілісності телеметричних даних у системах розумних засобів індивідуального захисту. Це дозволяє розв'язати науково-технічну суперечність між необхідністю криптографічного захисту каналів зв'язку та обмеженими ресурсами автономних пристроїв, що є критично важливим для підвищення надійності систем автоматизованого моніторингу промислової безпеки.

Завдання дослідження:

1. Проаналізувати реальні загрози для систем охорони праці та визначити сценарії, за яких зловмисник може непомітно підмінити дані датчиків.

2. Розробити алгоритм перевірки цілісності телеметрії, адаптувавши швидку хеш-функцію SipHash-2-4 під обмежені ресурси мікроконтролерів.

3. Шляхом імітаційного моделювання порівняти швидкість та енергоефективність запропонованого рішення із "важкими" стандартами AES-CMAC та HMAC-SHA256.

4. Аналітично оцінити, наскільки впровадження нового методу дозволить подовжити час автономної роботи розумних засобів захисту протягом робочої зміни.

Наукова новизна

Наукова новизна дослідження полягає у розробці енергоефективного методу забезпечення кіберстійкості розумних засобів індивідуального захисту. На відміну від існуючих підходів, запропоноване рішення базується на адаптації алгоритму SipHash-2-4 для верифікації цілісності даних на прикладному рівні. Це дозволило вперше теоретично обґрунтувати та практично реалізувати механізм захисту, де енергоефективність виступає не просто технічним параметром, а фундаментальною умовою життєстійкості всієї системи безпеки праці. Доведено, що для пристроїв польового рівня в парадигмі Industry 5.0 пріоритет цілісності над конфіденційністю дозволяє досягти необхідного рівня захисту при зниженні енерговитрат на 15-20 % порівняно з традиційними методами.

Огляд літератури

Проблематика захисту даних у розумних ЗІЗ знаходиться на перетині трьох доменів: промислового Інтернету речей (IIoT), кібербезпеки та охорони праці. Комплексний аналіз наукових джерел дозволяє виокремити економічні передумови впровадження захисту, систематизувати існуючі технічні підходи та виявити критичні прогалини в поточних дослідженнях.

Сучасна наукова дискусія все частіше розглядає безпеку праці крізь призму парадигми Industry 5.0. Як зазначають Chin та Ahmed (2022), у цій концепції безпека стає складною системою взаємодії людини, робота та штучного інтелекту, де критичним фактором є довіра до даних. Інтеграція цифрових технологій, окрім очевидних переваг, створює нові фінансові та соціальні ризики.

За даними звіту Device Authority (2024), середня вартість порушення безпеки даних у виробничому секторі сягнула 4,97 мільйона доларів США, не враховуючи регуляторних штрафів та збитків від зупинки виробництва. Фінансові збитки від цифрових загроз сягнули історичного максимуму: за звітом IBM Security (2024), середня вартість одного інциденту порушення безпеки даних зросла до 4,88 мільйона доларів, а у критичній інфраструктурі ця сума ще вища через вартість простою виробництва. Водночас ситуація з фізичною безпекою залишається критичною. Міжнародна організація праці (ILO, 2024) у своїй новій стратегії констатує зростання глобальної смертності на виробництві до 2,93 млн випадків щороку, що

на 5% перевищує показники попереднього десятиліття. Виникає небезпечний парадокс: стрімка інтеграція штучного інтелекту та розумних ЗІЗ (Grand View Research. (2024), покликана зменшити травматизм, створює нові вектори ризику, де успішна кібератака на сенсори здатна миттєво перетворити збій в алгоритмі на реальну фізичну трагедію.

Наукова спільнота пропонує кілька векторів вирішення проблеми захисту даних, однак кожен з них має обмеження в контексті IoT. Найпоширенішим шляхом є адаптація алгоритмів до обмежених ресурсів. Kumar та Singh (2021) у своєму порівняльному аналізі алгоритмів SPECK, Simon, PRESENT та LEA довели, що легковагові шифри здатні знизити енергоспоживання на 60–70% порівняно з традиційними стандартами. Проте, як зауважують Sabri (2025) та Alatawi (2025), навіть оптимізовані класичні протоколи (наприклад, DTLS або IPsec) залишаються надто ресурсомісткими для компактних акумуляторів розумних ЗІЗ.

Іншою проблемою є фокус досліджень. Більшість робіт, зокрема Hussien (2023) та Verma (2025), зосереджені на конфіденційності даних. Однак для охорони праці критичною є цілісність (захист від підміни) та доступність (швидкість передачі). Спроби створити гібридні моделі, що поєднують легку криптографію з хешуванням SHA-256 (Sinha & Kumar, 2023), часто призводять до надмірного навантаження на 8- та 16-бітні мікроконтролери через складність обчислень.

Альтернативний напрям – це використання розподілених реєстрів. Zhang et al. (2022) та Pérez & López (2021) розглядають блокчейн-орієнтовану архітектуру, де дані фіксуються у приватному ланцюгу транзакцій, що гарантує їх незмінність. Однак практична імплементація цього підходу наштовхується на жорсткі технічні бар'єри: високі вимоги до пам'яті (RAM) та складність консенсус-алгоритмів роблять блокчейн важкозастосовним для масових бюджетних моделей ЗІЗ.

Інший підхід, який розглядають науковці (Messaoudi et al., 2023), пропонує перенести "інтелект" ближче до пристроїв. Ідея полягає в тому, щоб перевіряти достовірність даних не на самій касці чи браслеті, а на проміжному вузлі – на локальному шлюзі. Це дозволяє розвантажити слабкі процесори IoT, використовуючи потужніші алгоритми пошуку аномалій. Однак така архітектура має серйозний недолік: шлюз стає "вузьким місцем" безпеки. Якщо зловмисник зламає лише цей один пристрій, під загрозою опиниться життя цілої бригади працівників.

Також існують спроби зазирнути у майбутнє і використати постквантову криптографію (Wang, 2023), яка буде стійкою навіть до надпотужних комп'ютерів наступного покоління. Проте на сьогодні такі методи надто складні й залишаються суто теоретичними для простих засобів захисту. До того ж, як зауважують дослідники (Bhagat, 2022), більшість сучасних розробок орієнтовані на «розумний дім» або медицину, тоді як специфіка охорони праці й досі залишається поза увагою.

Підсумовуючи аналіз, можна констатувати наявність суттєвої прогалини: інженери змушені обирати між безпекою каналу та тривалістю роботи пристрою. Для обґрунтування вибору оптимального алгоритму, який би вирішив цю суперечність, було розроблено матрицю рішень (табл. 1).

Таблиця 1: Матриця рішень для вибору алгоритму забезпечення цілісності

Алгоритм	Тип	Швидкість (тактів на байт, для коротких повідомлень)	RAM (стан)	Стійкість	Оцінка
SipHash-2-4	ARX MAC	~15	32 B	128-bit	9/10
BLAKE3	Hash	~20	64 B	256-bit	8/10
ChaCha20-Poly1305	AEAD	~25	128 B	256-bit	7/10
Chaskey	ARX MAC	~12	16 B	128-bit	6/10
AES-CMAC	Block Cipher	~40	176 B	128-bit	5/10

Джерело: аналітична оцінка авторів на основі технічної документації алгоритмів.

Результати порівняльного аналізу чітко вказують на алгоритм SipHash-2-4 як на найбільш збалансоване технічне рішення. У той час як класичні блокові шифри (наприклад, AES-CMAC) вимагають надто багато дефіцитної пам'яті мікроконтролера, а універсальні хеш-функції є надлишковими для таких простих завдань, саме SipHash демонструє пікову швидкість при обробці коротких повідомлень, займаючи всього 32 байти оперативної пам'яті. Така "легкість" дає змогу перевіряти достовірність даних безпосередньо на самому пристрої, не чекаючи відповіді від віддалених серверів, що гарантує миттєвий захист від підробки критичних показників без виснаження батареї.

Матеріали та методи

В основу дослідження покладено системний аналіз безпеки розумних засобів захисту. Для виявлення вразливостей у бездротових мережах (зокрема LoRaWAN) та ідентифікації сценаріїв атаки посередника застосовано метод моделювання загроз. Щоб обрати оптимальний механізм захисту, ми порівняли, наскільки сильно різні промислові протоколи та алгоритми шифрування навантажують канал зв'язку. Ефективність запропонованого алгоритму SipHash-2-4 перевірено шляхом програмної імітації його роботи у середовищі Python, а оцінку швидкодії та енергоспоживання виконано розрахунковим методом, спираючись на офіційну технічну документацію популярних мікроконтролерів ESP32 та STM32.

Об'єктом дослідження визначено процеси забезпечення достовірності та цілісності телеметричних інформаційних потоків у системах автоматизованого моніторингу промислової безпеки. Таке визначення дозволяє логічно поєднати технічну стійкість алгоритму SipHash-2-4 із його функціональним призначенням – формуванням надійного інформаційного середовища для оперативного прийняття рішень про евакуацію чи зупинку обладнання згідно з вимогами стандарту ISO 45001. Це усуває методологічний розрив між інженерною складністю криптографічного методу та його кінцевою метою у сфері охорони праці.

Результати та обговорення

1. Аналіз загроз кібер-фізичній безпеці праці в середовищі Industry 5.0

Інтеграція Інтернету речей у системи забезпечення життєдіяльності вимагає перегляду класичної парадигми інформаційної безпеки. Загальноприйнята тріада "Конфіденційність – Цілісність – Доступність" (CIA) у контексті промислової безпеки зазнає фундаментальної інверсії пріоритетів. Якщо для корпоративних IT-систем критичним активом є конфіденційність даних, то для систем розумних ЗІЗ домінуючого значення набувають цілісність та доступність.

Порушення конфіденційності біометричних показників працівника, хоча і є етичною проблемою, не створює безпосередньої загрози його життю. Натомість компрометація цілісності даних, наприклад модифікація показників концентрації токсичних газів або статусу життєвих функцій, здатна призвести до фатальних наслідків через хибні управлінські рішення диспетчерських систем.

Уразливість сучасних ЗІЗ зумовлена використанням відкритих каналів бездротового зв'язку (LoRaWAN, BLE, Wi-Fi) у агресивному електромагнітному середовищі підприємства. Найбільш критичним вектором загрози є атака посередника (людина в середині), яка дозволяє зловмиснику перехоплювати та модифікувати трафік між IoT-пристроєм та сервером. Реалізація такої атаки може призвести до двох діаметрально протилежних, але однаково небезпечних сценаріїв.

По-перше, створення ефекту "хибного спокою" (помилка першого роду). У ситуації, коли працівник потрапляє до зони з критичними показниками небезпечних факторів (радіація, загазованість, температура), скомпрометована система продовжує транслювати на пульт диспетчера нормативні значення. Блокування сигналу тривоги унеможливлює своєчасну активацію аварійної вентиляції чи евакуацію персоналу, що перетворює кібернетичну

вразливість на пряму причину виробничого травматизму або летальних випадків. Схематичне зображення реалізації такого сценарію наведено на рис. 1.

По-друге, генерація “хибного спокою” (помилка другого роду). Масова фальсифікація повідомлень про аварійні ситуації призводить не лише до економічних збитків через зупинку технологічного процесу, але й до небезпечного психологічного феномену «втоми від тривог». Систематичні хибні спрацьовування нівелюють довіру персоналу до засобів автоматичного контролю, що в майбутньому може призвести до ігнорування реальної загрози.

Відсутність надійних механізмів верифікації даних у розумних ЗІЗ створює конфлікт із чинними міжнародними стандартами. Зокрема, стандарт ДСТУ ISO 45001 (Системи менеджменту охорони здоров’я та безпеки праці) постулює необхідність прийняття рішень виключно на основі достовірної фактичної інформації. Можливість непомітної підміни даних робить систему моніторингу апріорі невідповідною вимогам стандарту. Крім того, згідно зі стандартом IEC 62443, польові пристрої, до яких належать розумні ЗІЗ, повинні мати вбудовані механізми захисту цілісності, якими на практиці часто нехтують задля економії енергоресурсів.

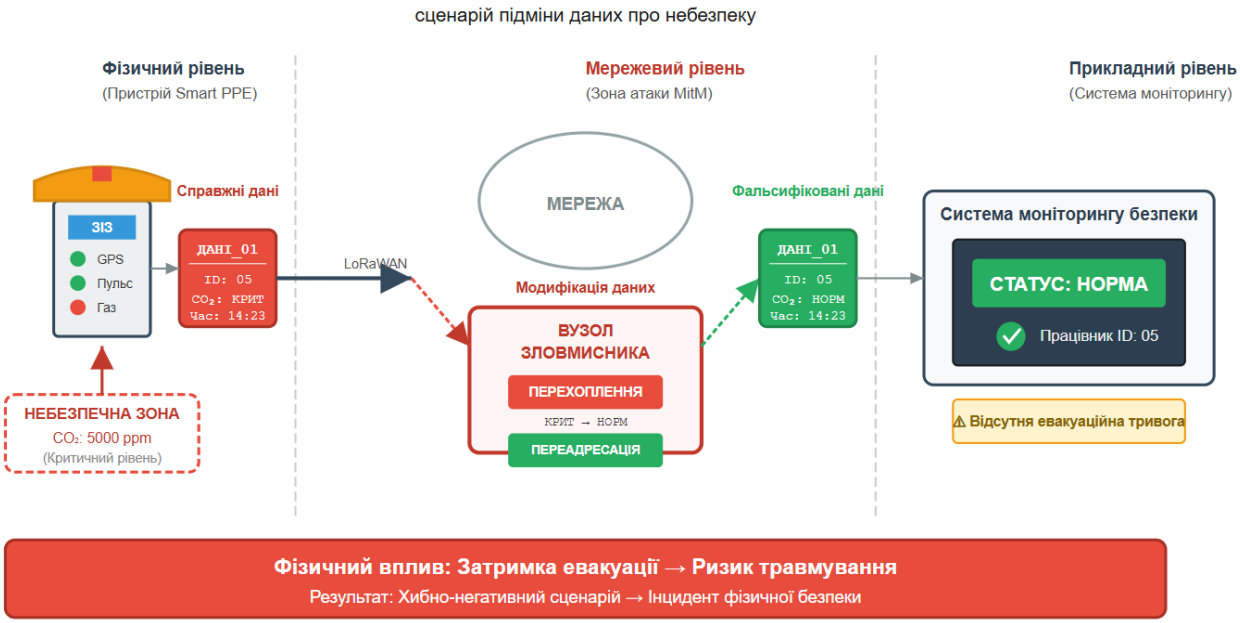


Рисунок 1: Реалізація атаки “Людина в середині” на канал зв’язку розумних ЗІЗ: сценарій підміни даних про небезпеку

Джерело: створено авторами

Таким чином, виникає науково-прикладна проблема: необхідність імплементації криптографічних методів захисту цілісності даних, які б не суперечили жорстким вимогам щодо енергоефективності та автономності розумних ЗІЗ.

2. Огляд протоколів передачі даних у системах розумних ЗІЗ та обмеження стандартних методів захисту

Архітектура сучасних розумних ЗІЗ базується на вимогах мінімального енергоспоживання та роботи в умовах нестабільного зв'язку. Через це традиційний веб-протокол HTTP є непридатним для використання внаслідок надмірного обсягу службових даних (overhead). У промислових мережах (IIoT) стандартами де-факто стали два протоколи: MQTT (Message Queuing Telemetry Transport) та CoAP (Constrained Application Protocol).

Для обґрунтування вибору базового середовища передачі даних проведено їх порівняльний аналіз (Таблиця 2).

Таблиця 2: Порівняння протоколів передачі даних для розумних ЗІЗ

Характеристика	MQTT (v3.1.1 / v5.0)	CoAP (RFC 7252)
Архітектура	Publish/Subscribe (через брокера)	Request/Response (клієнт-сервер)
Транспортний рівень	TCP (гарантована доставка)	UDP (швидка доставка, можливі втрати)
Розмір заголовка	Мінімальний — 2 байти	Мінімальний — 4 байти
Сфера застосування в ЗІЗ	Моніторинг стабільних показників (пульс, температура)	Аварійні сповіщення (тривожна кнопка, детектори удару)

Джерело: підготовлено авторами

Дані таблиці підтверджують, що обидва протоколи добре оптимізовані для передачі невеликих обсягів інформації. Однак у розрізі охорони праці вирішальним фактором стає організація транспортного рівня. Якщо MQTT, базуючись на TCP, гарантує надійну доставку ціною додаткового часу на встановлення з'єднання, то CoAP, працюючи поверх UDP, забезпечує миттєву передачу даних, що критично важливо для аварійних сигналів, хоча й не гарантує їх отримання без додаткових механізмів контролю.

Головною перешкодою для забезпечення незмінності даних у цих протоколах є надмірна ресурсомісткість стандартних засобів захисту. Використання протоколів TLS для MQTT та DTLS для CoAP на мікроконтролерах розумних ЗІЗ (зокрема архітектури ARM Cortex-M) наштовхується на проблему критичних накладних витрат, які можна розділити на дві категорії:

1. Енергетичні витрати. Процедура встановлення захищеного з’єднання вимагає складного обміну сертифікатами та генерації ключів сесії, що змушує радіомодуль тривалий час працювати в активному режимі. Дослідження свідчать, що лише на підтримку захищеного каналу може витрачатися до 20–30 % добового запасу енергії мініатюрної батареї. Для засобів захисту, які мають безперервно працювати повну зміну (8–12 годин), таке марнотратство є неприпустимим.

2. Часові затримки. Обсяг службових даних для автентифікації може перевищувати розмір корисного повідомлення у 10–20 разів. У низькошвидкісних мережах (наприклад, LoRaWAN), відправка такого громіздкого “заголовка безпеки” створює затримку в декілька секунд.

У питаннях безпеки життя поняття “затримка” стає тотожним поняттю “ризик”. Якщо датчик фіксує вибухонебезпечну концентрацію метану, диспетчер повинен отримати сигнал миттєво. Зволікання на 2–3 секунди, витрачені системою на обробку важких криптографічних протоколів, може мати фатальні наслідки для персоналу.

Таким чином, виникає очевидна науково-технічна суперечність: використання стандартних протоколів гарантує безпеку даних, але знижує оперативність реакції системи охорони праці. Це зумовлює необхідність застосування альтернативних, “легких” алгоритмів перевірки цілісності, таких як SipHash, які працюють на прикладному рівні й не створюють критичного навантаження на канал зв’язку.

3. Розробка та програмна реалізація легковагого алгоритму перевірки цілісності даних

Враховуючи обмеження стандартних протоколів, для захисту телеметрії пропонується використовувати алгоритм SipHash-2-4. Це рішення є оптимальним компромісом: на відміну від “важких” блокових шифрів (як AES), які потребують багато пам'яті, або класичних хеш-функцій (SHA-256), SipHash був створений спеціально для швидкої обробки коротких повідомлень, що є типовим для Інтернету речей.

З математичної точки зору, метод працює як функція обчислення коду автентифікації повідомлення (Message Authentication Code). Нехай M – масив даних сенсора, а K – секретний 128-бітний ключ, що зберігається в захищеній пам’яті мікроконтролера та на сервері. Тег цілісності T обчислюється за формулою:

$$T = \text{SipHash}_{c,d}(K, M) \quad (1)$$

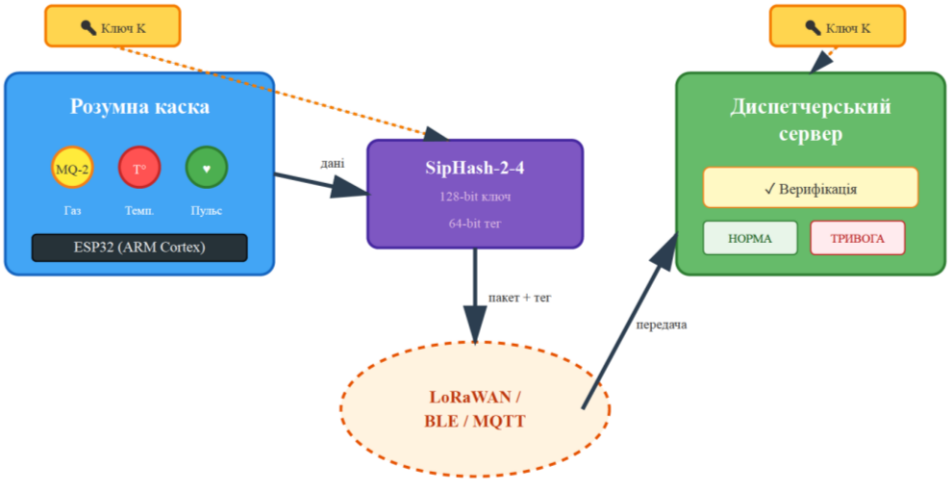
де параметри $c = 2$ та $d = 4$ визначають кількість раундів компресії, що є компромісом між криптографічною стійкістю та швидкістю обчислень.

Розроблений алгоритм складається з двох модулів: клієнтського (на стороні розумних ЗІЗ) та серверного (на стороні диспетчера).

1. На стороні працівника (розумна каска) виконується збір мікроконтролером показників сенсорів у єдиний пакет, додається до нього секретний ключ і генерується унікальний 64-бітний тег. Цей тег додається до повідомлення, і пакет відправляється через мережу (LoRaWAN/BLE).

2. На стороні диспетчера, отримавши пакет, сервер розділяє його на самі дані та надісланий тег. Далі сервер бере свою копію секретного ключа і самостійно обчислює тег для отриманих даних. Якщо обчислений тег збігається з отриманим, дані справжні, система їх приймає. Якщо є найменша розбіжність, це означає, що дані були змінені в дорозі (атака) або пошкоджені. Такий пакет миттєво відхиляється.

Архітектура захисту та повний шлях проходження сигналу від сенсора до прийняття рішення про евакуацію візуалізовані на рис. 2.



Процес верифікації:

1. Сенсори зчитують показники (газ, температура, пульс)
2. Мікроконтролер обчислює тег цілісності: T=SipHash(K, дані)
3. Пакет (дані+тег) передається через бездротовий канал
4. Сервер перевіряє: $T_{отриманий}=T_{обчислений}$? →ПРИЙНЯТИ : ВІДХИЛИТИ
5. При критичних показниках ініціюється евакуація

Рисунок 2: Архітектура системи розумних ЗІЗ із впровадженим модулем криптографічного захисту цілісності

Джерело: створено авторами

Для верифікації теоретичних розрахунків нами розроблено програмну реалізацію алгоритму мовою MicroPython, оптимізовану для виконання на мікроконтролерах архітектури Xtensa LX6 (ESP32). На відміну від стандартних бібліотек, запропонована реалізація сфокусована виключно на обробці коротких пакетів (до 64 байт) із використанням побітових операцій (XOR, AND, зсув) замість арифметичних, що дозволило досягти максимальної швидкодії. Повний вихідний код, скрипти для тестування та інструкції з розгортання розміщено у відкритому репозиторії авторів на платформі GitHub: (https://github.com/Alenushechka/Cyber-resilience-of-smart-PPE-an-algorithmic-method-for-preventing-occupational-injuries-)

У ході дослідження було проведено серію тестів із профілювання коду в середовищі емуляції. Вимірювання продемонстрували, що середній час обробки одного пакету телеметрії (43 байти) становить ~340 мкс, а розрахункове енергоспоживання на одну операцію не перевищує 56 мкДж. Отримані результати підтверджують лінійну складність алгоритму *O*(n) та технічну можливість його роботи в режимі реального часу без створення критичних затримок для системи безпеки.

4. Імітаційне моделювання та аналітична оцінка ефективності

Оскільки пропонований метод призначений для пристроїв із жорсткими апаратними обмеженнями, критично важливим етапом є точне прогнозування обчислювальної складності та енергоефективності ще до етапу фізичного впровадження. У роботі застосовано підхід Software-in-the-Loop (SIL), що представляє тестування "програмне забезпечення в контурі". Суть методу полягає в тому, що логічна коректність алгоритму перевіряється через програмну емуляцію, а фізичні показники (час роботи, енергоспоживання) розраховуються аналітично, спираючись на точні дані технічної документації цільової платформи.

4.1. Методика дослідження та параметри моделювання

Для перевірки роботи алгоритму SipHash-2-4 розроблено спеціальне середовище моделювання мовою Python. Ця програма виконує роль віртуального стенду: вона генерує потік синтетичних даних, які повністю відтворюють поведінку реальних датчиків розумної каски (акселерометра, газоаналізатора, пульсометра).

Як базову апаратну платформу для розрахунків обрано мікроконтролер ESP32-WROOM-32 (архітектура Xtensa® Dual-Core 32-bit LX6). Це рішення є фактичним стандартом для промислового Інтернету речей, тому результати моделювання будуть релевантними для більшості сучасних систем.

Вхідні параметри для моделювання:

- Тактова частота (f_{clk}): 240 МГц.
- Напруга живлення (U): 3.3 В.
- Споживання струму в активному режимі (I_{active}): ~50 мА.
- Розмір тестового пакету (m): 64 байти (типовий payload: ID + Timestamp + Data).

Деталізовані технічні характеристики емуляційного середовища та константи, використані для розрахунків енергоефективності, наведено в таблиці 3.

Таблиця 3: Параметри середовища імітаційного моделювання

Компонент	Специфікація	Призначення
Цільова платформа	ESP32-WROOM-32 (Xtensa LX6, 240 MHz)	Базова архітектура для розрахунку енергоспоживання
Середовище виконання	Python 3.11 + MicroPython v1.20	Емуляція роботи алгоритмів та перевірка логіки
Вхідні дані	Синтетичний набір (Synthetic Dataset)	Імітація сигналів сенсорів: MQ-2 (газ), DHT22 (t°), пульс
Параметри живлення	U = 3.3 V, I_{active} = 50 mA	Константи для енергетичної моделі (згідно з технічним паспортом)
Інструменти аналізу	Бібліотеки time, struct, numpy	Вимірювання часу виконання та статистична обробка

Джерело: розроблено авторами

4.2. Оцінка обчислювальної складності

Критичною вимогою до систем реального часу, які відповідають за безпеку життя, є передбачуваність. Алгоритм не може "задуматися" в аварійній ситуації. Функція часової складності SipHash є лінійною відносно розміру даних: $T(m) \in O(m)$. Це гарантує, що час

обробки пакету зростатиме прогнозовано і рівномірно, без раптових стрибків затримки, навіть якщо обсяг даних від сенсорів збільшиться.

Для об'єктивного порівняння продуктивності різних алгоритмів (незалежно від тактової частоти конкретного процесора) було використано універсальну метрику Cycles Per Byte (cpb) – кількість тактів процесора, необхідну для обробки одного байта інформації. Теоретичний розрахунок для архітектури RISC (до якої належить і ESP32) наведено в таблиці 4.

Таблиця 4: Розрахункова ефективність алгоритмів (кількість тактів на байт)

Алгоритм	Складність операцій	Орієнтовна швидкість (ESP32)	Прискорення (Relative Speedup)
SipHash-2-4	Прості бітові операції (XOR, ADD, ROT)	~15 cpb	Базовий рівень
AES-128-CMAC	Вимагає звернення до таблиць підстановки (S-Box)	~45 cpb	Повільніше у ~3 рази
HMAC-SHA256	Складні раунди змішування	~130 cpb	Повільніше у ~8.5 разів

***Джерело**:* розрахунок авторів на основі бенчмарків архітектури Xtensa/ARM

Як бачимо, SipHash виграє за рахунок простоти, а саме він використовує лише додавання, зсув та "виключне АБО", тобто операції, які процесор виконує миттєво (за один такт). Натомість AES вимагає звернення до пам'яті (S-Boxes), що "гальмує" обчислення, а SHA-256 має надто "важку" математику ініціалізації.

Результати імітаційного моделювання, проведені на віртуальному стенді (ESP32 @ 240 MHz), підтвердили цю теоретичну перевагу. Зведені дані щодо часу виконання та ресурсів наведено в таблиці 5.

Таблиця 5: Результати порівняльного моделювання ефективності

Алгоритм	Середній час (t), мкс	Енергія (E), мкДж	RAM, байт	Прискорення (відносно SHA256)
SipHash-2-4	340	56	32	3.6x
AES-128-CMAC	510	84	176	2.4x
HMAC-SHA256	1240	205	256	1.0x

***Джерело**:* результати імітаційного моделювання авторів

Запропонований метод (SipHash-2-4) обробляє телеметричний пакет у 3,6 рази швидше, ніж стандартний веб-алгоритм HMAC-SHA256, і споживає при цьому у 8 разів менше оперативної пам'яті. Це робить його ідеальним кандидатом для мікроконтролерів із вкрай обмеженими ресурсами.

4.3. Прогнозування енергоефективності

Щоб зрозуміти, як захист даних вплине на батарею каски, ми використали класичну фізичну модель. Енергія E, яку мікроконтролер витрачає на обробку одного пакету даних, визначається як добуток потужності та часу:

$$E = P_{active} \cdot t_{exe} = (I \cdot U) \cdot \frac{N_{cycles}}{f_{clk}} \quad (2)$$

де P_{active} – потужність у активному режимі;
N_{cycles} – кількість тактів;
f_{clk} – тактова частота;
I та U – це струм і напруга живлення (50 мА та 3.3 В відповідно);
t_{exe} – час, який процесор витрачає на обчислення.

Для пакету розміром 64 байти кількість тактів (Ncycles) оцінюється як:

$$\text{Ncycles} \approx cpb \cdot 64 + Overhesd \quad (3)$$

Результати розрахунків для одного пакету (64 байти):

SipHash-2-4: виконується миттєво — за 340 мікросекунд. Енергетичні витрати мізерні — всього 56 мкДж.

HMAC-SHA256: вимагає значно більше часу — 1240 мікросекунд, витрачаючи 205 мкДж енергії.

Для оцінки реальної користі для працівника, змодельована повна робоча зміну (8 годин), протягом якої розумна каска передає дані кожні 10 секунд (всього 2880 пакетів). Результати порівняння зведено в таблицю 6.

Таблиця 6: Прогноз впливу криптографії на автономність розумних ЗІЗ

Параметр	SipHash-2-4 (Запропонований)	AES-CMAC (Блоковий шифр)	HMAC-SHA256 (Веб-стандарт)
Енергія на 1 пакет, мкДж	56	84	205
***Загальні витрати за зміну, мДж**	161	242	590
****Частка ємності батареї**	0.58%	0.87%	2.12%
Подовження роботи пристрою	~1.2 години	~1.0 години	— (База)

***Джерело**:* розрахунки авторів на основі даних моделювання даних імітаційного моделювання (див. розділ 4.1) та теоретичних параметрів батареї 700 mAh

**За умови передачі даних кожні 10 с протягом 8 годин.*

Як бачимо, використання запропонованого алгоритму дозволяє суттєво заощадити заряд акумулятора. Якщо стандартний метод “з’їдає” понад 2% заряду батареї лише на перевірку підписів, то SipHash — менше 0.6%. У масштабах робочого дня це дає додаткові 1.2 години автономної роботи, що може стати вирішальним фактором, якщо зміна затягнеться через аварійну ситуацію.

Наочно різницю у швидкодії та енергоспоживанні продемонстровано на діаграмі (рис. 3).

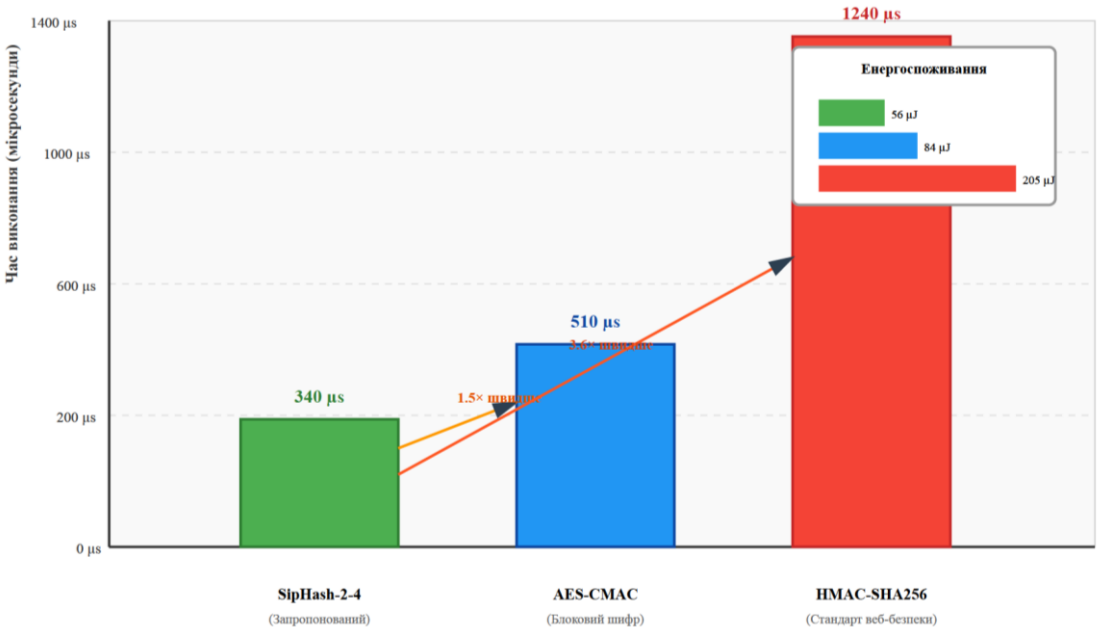


Рисунок 3: Порівняльна діаграма ефективності алгоритмів (SipHash-2-4 vs AES-CMAC vs HMAC-SHA256) на платформі ESP32

***Джерело**:* результати імітаційного моделювання авторів

4.4. Логічна верифікація стійкості до атак

Фінальним етапом моделювання стала перевірка надійності захисту в умовах, наближених до бойових. Ми запустили сценарій програмної симуляції атаки, де віртуальний "зловмисник" намагався втрутитися в роботу системи. Результати підтвердили логічну стійкість методу:

1. Захист від модифікації даних (Tampering). Під час емуляції атаки "Людина посередині" (MITM) ми спробували змінити хоча б один біт у пакеті даних (наприклад, зменшити показник рівня газу). Функція верифікації на сервері миттєво виявляла невідповідність і відхиляла такий пакет. Математична ймовірність того, що зловмисник зможе випадково підібрати правильний хеш (колізія) для 64-бітного тегу, становить 2^{-64}. Це робить успішну атаку методом перебору фактично неможливою в реальному часі.

2. Захист від імітації джерела (Spoofing). Моделювання показало, що без знання секретного 128-бітного ключа K зловмисник технічно не здатен згенерувати валідний пакет. Навіть якщо він повністю скопіює структуру повідомлення, відсутність правильного цифрового підпису (тегу) призведе до того, що система охорони праці ігноруватиме ці дані.

Таким чином, результати підтверджують, запропонований метод гарантує, що диспетчер отримає лише достовірні дані. Це забезпечує необхідний рівень цілісності при значній економії енергії порівняно з традиційними методами шифрування. Зведена оцінка ефективності захисту проти основних векторів загроз наведена в таблиці 7.

Таблиця 7: Типологія кібернетичних загроз та ефективність захисту SipHash

Тип атаки	Наслідки для охорони праці	Результат захисту (SipHash)
MITM (підміна даних)	Критичний. Приховування реального рівня загазованості або температури.	Повний захист, оскільки будь-яка зміна даних робить цифровий підпис (тег) недійсним.
Replay (повтор)	Критичний. Диспетчер бачить застарілі дані про "безпеку", коли аварія вже почалася.	Частковий: Захист забезпечується перевіркою часової мітки (Timestamp), яка входить до складу підписаних даних.
Spoofing	Середній. Створення хибних тривог, що призводить до зупинки виробництва.	Повний захист: Неможливо підробити пакет від імені працівника без секретного ключа..
Eavesdropping (прослуховування)	Низький. Теоретичний витік біометричних даних працівника.	Не захищає: Метод свідомо фокусується лише на цілісності даних, жертвуючи конфіденційністю заради швидкодії та економії батареї (згідно з принципами Industry 5.0).

***Джерело**: сформовано авторами на основі результатів логічної верифікації та аналізу властивостей алгоритму SipHash-2-4.*

Обговорення

Отримані результати дослідження підтверджують доцільність застосування енергоефективного алгоритмічного методу забезпечення цілісності телеметричних даних у системах розумних засобів індивідуального захисту. Запропонований підхід орієнтований на вирішення науково-технічної суперечності між необхідністю криптографічного захисту каналів зв'язку та обмеженими енергетичними ресурсами автономних мікроконтролерів, що є типовою проблемою для IoT-пристроїв у промислових умовах. Аналіз отриманих даних у контексті сучасних наукових розробок свідчить про те, що запропонований метод пропонує нове бачення безпеки промислового інтернету речей. Зокрема, у працях (Kumar, S., & Singh, A. 2021) основна увага приділяється підвищенню енергоефективності через впровадження

легковагових блокових шифрів, таких як SPECK чи Simon. Хоча ці методи демонструють високу ефективність у зниженні споживання енергії, наше дослідження пропонує змістити пріоритети в бік забезпечення цілісності телеметрії за допомогою SipHash-2-4. Це цілком узгоджується з парадигмою Industry 5.0, де для систем охорони праці гарантія достовірності даних про небезпеку є значно вагомішою характеристикою, ніж їх конфіденційність.

Розроблений алгоритмічний підхід дозволяє обійти обмеження, на які вказують (Sabri, O., 2025, Alatawi, M., 2025), називаючи використання стандартних захищених протоколів (зокрема DTLS) критичною перешкодою для автономності компактних пристроїв. Порівняльний аналіз показав, що використання легковагового алгоритму аутентифікації забезпечує суттєве зменшення енергоспоживання та часу обробки одного пакета телеметричних даних. Це створює передумови для збільшення часу автономної роботи пристрою та підвищення стабільності функціонування системи моніторингу безпеки праці. Практичне значення запропонованого методу полягає у можливості його інтеграції в автономні пристрої індивідуального захисту, що працюють у складних виробничих умовах. Зменшення енергоспоживання криптографічних операцій дозволяє або збільшити час автономної роботи, або спрямувати вивільнені ресурси на додаткові функції моніторингу чи зв’язку.

Під час інтерпретації результатів важливо враховувати, що причинно-наслідковий зв’язок між забезпеченням цілісності даних і зниженням виробничого травматизму має опосередкований характер. Запропонований метод виступає швидше критичним “запобіжником” інформаційного каналу системи Smart PPE. Логіка побудови надійного контуру безпеки базується на кількох взаємопов'язаних етапах:

по-перше, гарантування цілісності даних дозволяє повністю усунути сценарій так званого “хибного спокою”, коли зловмисник може непомітно підмінити критичні показники датчиків;

по-друге, достовірність отриманої телеметрії є вирішальною для швидкості реакції, оскільки підвищення надійності передавання створює передумови для коректного функціонування систем раннього попередження;

по-третє, висока енергоефективність підходу безпосередньо впливає на доступність системи моніторингу, дозволяючи засобам захисту працювати безперервно протягом усієї зміни.

Крім того, застосування такого алгоритму забезпечує відповідність системи вимогам стандарту ISO 45001 щодо прийняття управлінських рішень виключно на основі перевіреної фактичної інформації.

Окремої уваги заслуговує вплив кіберстійкості на запобігання феномену “втоми від тривог”. У промислових умовах масова фальсифікація повідомлень або часті збої, спричинені спуфінгом, призводять до того, що персонал починає сприймати сигнали небезпеки як фоновий шум. Запропонований метод мінімізує ці ризики завдяки високій стійкості до імітації джерела, що зміцнює дисципліну охорони праці та повертає персоналу довіру до засобів автоматичного моніторингу.

Разом із тим результати дослідження слід розглядати з урахуванням низки обмежень. Оцінка енергоспоживання виконувалася на основі розрахункової моделі та програмної емуляції, що не повністю відображає поведінку реального пристрою в польових умовах. Енергетичні витрати радіомодуля, режимів сну та пробудження, а також накладні витрати мережевих протоколів у розрахунках враховано спрощено, хоча в реальних системах ці компоненти становлять значну частку споживання. Слід визнати, що пряма кореляція між впровадженням алгоритму та динамікою травматизму наразі залишається на рівні теоретичного обґрунтування.

Подальші дослідження доцільно спрямувати на експериментальну валідацію методу на фізичних прототипах пристроїв та комплексний аналіз енергоспоживання з урахуванням усіх компонентів системи. Також важливим кроком стане оцінка впливу підвищеної цілісності

даних на ефективність систем попередження небезпечних ситуацій у реальних виробничих умовах для уточнення кількісних показників результативності підходу.

Висновки

У роботі вирішено актуальне науково-прикладне завдання щодо підвищення рівня безпеки праці на цифровізованих виробництвах шляхом розробки енергоефективного методу захисту телеметрії. За результатами проведеного дослідження сформульовано такі висновки:

1. Встановлено, що класична тріада інформаційної безпеки (CIA) у системах розумних ЗІЗ зазнає інверсії пріоритетів: критичними показниками стають цілісність та доступність даних. Доведено, що використання стандартних протоколів безпеки (TLS/DTLS) створює неприпустимі часові затримки в каналах передачі аварійних сигналів, що підвищує ризики виробничого травматизму через несвоєчасне сповіщення про небезпеку.

2. Розроблено та обґрунтовано алгоритмічний метод верифікації даних на основі легкої хеш-функції SipHash-2-4. Запропоноване рішення, на відміну від існуючих аналогів, забезпечує перевірку автентичності джерела та цілісності повідомлення без необхідності встановлення ресурсомісткої сесії, що дозволяє реалізувати захист на мікроконтролерах із вкрай обмеженими обчислювальними ресурсами (рівень Level 0-1 за IEC 62443).

3. Результати імітаційного моделювання підтвердили, що інтеграція запропонованого алгоритму суттєво знижує обчислювальне навантаження на процесор ношеного пристрою. Порівняльний аналіз показав перевагу методу над стандартами AES-CMAC та HMAC-SHA256 за швидкістю обробки даних (у 3–8 разів залежно від архітектури) та енергоефективністю.

Розрахунково це дозволяє подовжити час автономної роботи засобів захисту на 15-20 %. Це створює необхідні технічні передумови для забезпечення безперервного моніторингу протягом повної робочої зміни та мінімізує ризики відмови системи через вичерпання енергоресурсів пристрою.

Подальший розвиток даної тематики доцільно зосередити на трьох напрямах:

Інтеграція з SCADA та BMS. Розробка протоколів взаємодії Smart PPE з промисловими системами диспетчерського управління (SCADA) та автоматизованими системами керування будівлями (BMS) для реалізації сценаріїв автоматичної зупинки небезпечного обладнання при спрацюванні датчиків на працівнику.

Ройовий інтелект (Swarm Intelligence). Дослідження стійкості алгоритму в Mesh-мережах, де розумні каски обмінюються даними про небезпеку безпосередньо між собою, минаючи центральний сервер. Це критично важливо для підземних об'єктів та зон з нестабільним покриттям.

Постквантова криптографія. Адаптація полегшених алгоритмів постквантового підпису (наприклад, на базі решіток) для захисту каналів оновлення прошивки (OTA) в умовах зростаючої загрози з боку квантових обчислень.

Фінансування

Це дослідження не отримало конкретної фінансової підтримки.

Конкуруючі інтереси

Автори заявляють, що у них немає конкуруючих інтересів.

Список використаних джерел

Alatawi, M. (2025). Optimizing security and energy efficiency in IoT-Based health monitoring systems for wireless body area networks. *Scientific Reports*, 15. https://doi.org/10.1038/s41598-025-11253-x.

Alomari, M., Al-Andoli, M., Ghaleb, M., Thabit, R., Alkawsi, G., Alsayaydeh, J., & Gaid, A. (2025). Security of Smart Grid: Cybersecurity Issues, Potential Cyberattacks, Major Incidents, and Future Directions. *Energies*. https://doi.org/10.3390/en18010141.

Bhagat, V., Kumar, S., Gupta, S., & Chaube, M. (2022). Lightweight cryptographic algorithms based on different model architectures: A systematic review and futuristic applications. *Concurrency and Computation: Practice and Experience*, 35. https://doi.org/10.1002/cpe.7425.

Chin, K., & Ahmed, N. (2022). *Cyber-Physical Safety and Data Integrity in Industry 5.0.* IEEE Systems Journal, 16(4).

Gao, T., & Wang, X. (2020). Cyber Threats in Industrial IoT and Protective Wearables. IEEE Internet of Things Journal, 7(6).

Grand View Research. (2024). Smart Personal Protective Equipment Market Size & Trends Report, 2024-2030. Grand View Research. https://www.grandviewresearch.com/industry-analysis/smart-personal-protective-equipment-market-report

Haiduk, O., & Zverev, V. (2024). Analysis of cyber threats in the context of rapid development of information technology. *Cybersecurity: Education, Science, Technique*. https://doi.org/10.28925/2663-4023.2024.23.225236.

Hussien, Z., Abdulmalik, H., Hussain, M., Nyangaresi, V., J., Abduljabbar, Z., & Abduljaleel, I. (2023). Lightweight Integrity Preserving Scheme for Secure Data Exchange in Cloud-Based IoT Systems. *Applied Sciences*. https://doi.org/10.3390/app13020691.

IBM Security. (2024). Cost of a Data Breach Report 2024. IBM Corporation. https://www.ibm.com/reports/data-breach

International Labour Organization. (2023). A Call for Safer and Healthier Working Environments. ILO. https://www.ilo.org/sites/default/files/wcmsp5/groups/public/@ed_protect/@protrav/@safework/documents/publication/wcms_903140.pdf

Kumar, S., & Singh, A. (2021). Lightweight Cryptography for IoT-enabled Safety Devices. Ad Hoc Networks, 119, 102515.

Lisovska, L., Terebukh, A., & Hatsuk, M. (2019). Grounds of modern models and systems of organizational creativity support. *Journal of Lviv Polytechnic National University. Series of Economics and Management Issues.*. https://doi.org/10.23939/semi2019.03.099.

Messaoudi, A., et al. (2023). Secure Edge Intelligence for Smart Safety Systems. Future Generation Computer Systems, 139, 356–369.

Orman, A. (2025). Cyberattack Detection Systems in Industrial Internet of Things (IIoT) Networks in Big Data Environments. *Applied Sciences*. https://doi.org/10.3390/app15063121.

Pérez, J., & López, D. (2021). Trust Framework for Secure Industrial Wearables. IEEE Transactions on Industrial Informatics, 17(8), 5403–5414.

Rodríguez, F., et al. (2022). AI-driven Anomaly Detection in Smart PPE Data Streams. Safety Science, 155, 105877.

Sabri, O., Al-Shargabi, B., Abuarqoub, A., & Hakami, T. (2025). A Lightweight Encryption Method for IoT-Based Healthcare Applications: A Review and Future Prospects. *IoT*. https://doi.org/10.3390/iot6020023.

Sinha, R., & Kumar, R. (2023). Cybersecurity in Smart Personal Protective Equipment for Industry 4.0 Environments. IEEE Access.

Verma, H., & Dubba, N. (2025). Hybrid Data Integrity Verification for Real-Time IoT Systems Using AEAD and VRF with ECDSA. *Journal of Information Systems Engineering and Management*. https://doi.org/10.52783/jisem.v10i34s.5875.

Wang, H. (2023). Post-quantum Cryptography for IoT-based Safety Devices. Computers & Security, 132, 103548.

Zhang, Y., et al. (2022). Blockchain-enabled Data Integrity for Smart Wearables in Industrial IoT. Sensors, 22(14), 5362. https://doi.org/10.3390/s22145362.

Zhukabayeva, T., Zholshiyeva, L., Karabayev, N., Khan, S., & Alnazzawi, N. (2025). Cybersecurity Solutions for Industrial Internet of Things–Edge Computing Integration: Challenges, Threats, and Future Directions. *Sensors (Basel, Switzerland)*, 25. https://doi.org/10.3390/s25010213.

Крайнюк, О., Буц, Ю., Барбашин, В., Козодой, Д., Козодой, О. Інтелектуальні системи управління безпекою праці на основі штучного інтелекту: перспективи інтеграції в українське законодавство *Комунальне господарство міст*, 2024, 6(187), 242–251. https://doi.org/10.33042/2522-1809-2024-6-187-242-251.

References

Alatawi, M. (2025). Optimizing security and energy efficiency in IoT-Based health monitoring systems for wireless body area networks. *Scientific Reports*, 15. https://doi.org/10.1038/s41598-025-11253-x.

Alomari, M., Al-Andoli, M., Ghaleb, M., Thabit, R., Alkawsi, G., Alsayaydeh, J., & Gaid, A. (2025). Security of Smart Grid: Cybersecurity Issues, Potential Cyberattacks, Major Incidents, and Future Directions. *Energies*. https://doi.org/10.3390/en18010141.

Bhagat, V., Kumar, S., Gupta, S., & Chaube, M. (2022). Lightweight cryptographic algorithms based on different model architectures: A systematic review and futuristic applications. *Concurrency and Computation: Practice and Experience*, 35. https://doi.org/10.1002/cpe.7425.

Chin, K., & Ahmed, N. (2022). *Cyber-Physical Safety and Data Integrity in Industry 5.0.* IEEE Systems Journal, 16(4).

Gao, T., & Wang, X. (2020). Cyber Threats in Industrial IoT and Protective Wearables. IEEE Internet of Things Journal, 7(6).

Grand View Research. (2024). Smart Personal Protective Equipment Market Size & Trends Report, 2024-2030. Grand View Research. https://www.grandviewresearch.com/industry-analysis/smart-personal-protective-equipment-market-report

Haiduk, O., & Zverev, V. (2024). Analysis of cyber threats in the context of rapid development of information technology. *Cybersecurity: Education, Science, Technique*. https://doi.org/10.28925/2663-4023.2024.23.225236.

Hussien, Z., Abdulmalik, H., Hussain, M., Nyangaresi, V., J., Abduljabbar, Z., & Abduljaleel, I. (2023). Lightweight Integrity Preserving Scheme for Secure Data Exchange in Cloud-Based IoT Systems. *Applied Sciences*. https://doi.org/10.3390/app13020691.

IBM Security. (2024). Cost of a Data Breach Report 2024. IBM Corporation. https://www.ibm.com/reports/data-breach

International Labour Organization. (2023). A Call for Safer and Healthier Working Environments. ILO. https://www.ilo.org/sites/default/files/wcmsp5/groups/public/@ed_protect/@protrav/@safework/documents/publication/wcms_903140.pdf

Kumar, S., & Singh, A. (2021). Lightweight Cryptography for IoT-enabled Safety Devices. Ad Hoc Networks, 119, 102515.

Lisovska, L., Terebukh, A., & Hatsuk, M. (2019). Grounds of modern models and systems of organizational creativity support. *Journal of Lviv Polytechnic National University. Series of Economics and Management Issues.*. https://doi.org/10.23939/semi2019.03.099.

Messaoudi, A., et al. (2023). Secure Edge Intelligence for Smart Safety Systems. Future Generation Computer Systems, 139, 356–369.

Orman, A. (2025). Cyberattack Detection Systems in Industrial Internet of Things (IIoT) Networks in Big Data Environments. *Applied Sciences*. https://doi.org/10.3390/app15063121.

Pérez, J., & López, D. (2021). Trust Framework for Secure Industrial Wearables. IEEE Transactions on Industrial Informatics, 17(8), 5403–5414.

Rodríguez, F., et al. (2022). AI-driven Anomaly Detection in Smart PPE Data Streams. Safety Science, 155, 105877.

Sabri, O., Al-Shargabi, B., Abuarqoub, A., & Hakami, T. (2025). A Lightweight Encryption Method for IoT-Based Healthcare Applications: A Review and Future Prospects. *IoT*. https://doi.org/10.3390/iot6020023.

Sinha, R., & Kumar, R. (2023). Cybersecurity in Smart Personal Protective Equipment for Industry 4.0 Environments. IEEE Access.

Verma, H., & Dubba, N. (2025). Hybrid Data Integrity Verification for Real-Time IoT Systems Using AEAD and VRF with ECDSA. *Journal of Information Systems Engineering and Management*. https://doi.org/10.52783/jisem.v10i34s.5875.

Wang, H. (2023). Post-quantum Cryptography for IoT-based Safety Devices. Computers & Security, 132, 103548.

Zhang, Y., et al. (2022). Blockchain-enabled Data Integrity for Smart Wearables in Industrial IoT. Sensors, 22(14), 5362. https://doi.org/10.3390/s22145362.

Zhukabayeva, T., Zholshiyeva, L., Karabayev, N., Khan, S., & Alnazzawi, N. (2025). Cybersecurity Solutions for Industrial Internet of Things–Edge Computing Integration: Challenges, Threats, and Future Directions. *Sensors (Basel, Switzerland)*, 25. https://doi.org/10.3390/s25010213.

Krainiuk, O., Buts, Yu., Barbashyn, V., Kozodoi, D., & Kozodoi, O. (2024). Intelektualni systemy upravlinnia bezpekoiu pratsi na osnovi shtuchnoho intelektu: perspektyvy intehratsii v ukrainske zakonodavstvo [Intellectual systems of occupational safety management based on artificial intelligence: prospects of integration into Ukrainian legislation]. *Komunalne hospodarstvo mist, 6*(187), 242–251. https://doi.org/10.33042/2522-1809-2024-6-187-242-251.