

Міністерство освіти і науки України

Харківський національний університет радіоелектроніки

Кафедра комп'ютерно-інтегрованих технологій, автоматизації, робототехніки та
безпекової інженерії

**II Всеукраїнська конференція
«Інтелектуальні технології цивільної безпеки та
робототехнічні системи аварійно-рятувальних робіт»**



**II All-Ukrainian Conference
“Intelligent Civil Safety Technologies and Robotic Systems for
Emergency and Rescue Operations”**

ICSTRO

2026

I All-Ukrainian Conference

September 17 - 18, 2026

Kharkiv

ЗМІСТ

І. І. Хондак, Пронюк Г.В.

Сталий розвиток як основа забезпечення екологічної безпеки та соціальної відповідальності у сфері цивільної безпеки 8

Vladyslav Yevsieiev

Neuro-Fuzzy Method for Predicting and Assessing the Level of Technological Hazard in Cyber-Physical Civil Protection Systems 11

М.Ю. Білоусов, В.В. Невлюдова, М.Г. Стародубцев

Цифровізація та роботизація в промисловому виробництві 15

Б. І. Кислий, С. В. Сотник

Забезпечення стійкості кіберфізичних систем до DDOS-атак під час управління критичними об'єктами у надзвичайних ситуаціях 19

Гурін Д.В.

Аналіз доцільності використання колаборативних роботів у виробництві компонентів відновлюваних джерел енергії 24

Vladyslav Yevsieiev, Kyrylo Luchaninov

Intelligent Method for Dynamic Emergency Risk Assessment at Critical Infrastructure Facilities Based on Digital Twin 29

Д. В. Кухаренко, І. Д. Федосов-Ніконов

Розробка та створення сучасного блока живлення на базі мікроконтролера ESP32-WROOM-32U 33

І.К. Сезонова

Інтелектуальні технології в системі державної політики цивільної безпеки 36

Пронюк Г.В., Хондак І.І.

Модель підтримки прийняття рішень для багатокритеріального вибору варіанта реагування на надзвичайні ситуації 39

Д. В. Лукієнко, С. В. Сотник

Нейромережеве прогнозування техногенних ризиків на основі даних промислових кіберфізичних систем 43

Kyrylo Horovy

Method for Predicting Pre-Failure States of Microelectronic Manufacturing Equipment Based on Digital Twin and Intelligent Analysis of Process Parameters 47

Самойленко Владислав

Важливість динамічної стійкості в розробці гуманоїдних роботів 52

М. О. Іванов, С. В. Сотник

Особливості застосування дронів у надзвичайних ситуаціях 55

Vladyslav Yevsieiev, Svetlana Starikova

Intelligent System for Adaptive Management of the Educational Process in General Secondary Education Institutions Based on Artificial Intelligence Technologies 60

Б. І. Кислий, С. В. Сотник

Автоматизовані системи виявлення аномалій у роботі технологічного обладнання на основі аналізу цифрових протоколів обміну (MODBUS, DNP3) 64

Гурін Д.В., Грижжак В.М.

Розроблення підсистеми автоматизованого доступу та обліку робочого часу 69

Д. В. Лукієнко, С. В. Сотник

Методи криптографічного захисту телеметричних даних у розподілених системах
моніторингу стану небезпечних об'єктів 73

Д. Р. Придятько, С. В. Сотник

Порівняльний аналіз сучасних методів виявлення вибухонебезпечних предметів у
сфері цивільної безпеки 78

МЕТОДИ КРИПТОГРАФІЧНОГО ЗАХИСТУ ТЕЛЕМЕТРИЧНИХ ДАНИХ У РОЗПОДІЛЕНИХ СИСТЕМАХ МОНІТОРИНГУ СТАНУ НЕБЕЗПЕЧНИХ ОБ'ЄКТІВ

Д. В. Лукієнко, С. В. Сотник

Харківський національний університет радіоелектроніки

Україна, 61166, Харків, пр. Науки, 14

E-mail: dmytro.lukiienko@nure.ua, svetlana.sotnik@nure.ua

Анотація: У роботі розглянуто методи криптографічного захисту телеметричних даних у розподілених системах моніторингу стану небезпечних об'єктів. Побудовано модель загроз, що охоплює перехоплення, підміну й повторне відтворення повідомлень, компрометацію вузлів і спотворення архівів. Проаналізовано застосування автентифікованого шифрування, полегшених алгоритмів для вузлів з обмеженими ресурсами, електронного цифрового підпису та захищених транспортних протоколів. Розглянуто питання керування ключами, захисту від повторів за умов нестійкої синхронізації часу, забезпечення доказової цілісності архівів і переходу до постквантових алгоритмів. Окреслено співвідношення між рівнем захисту, енергоспоживанням вузлів і затримкою доставлення даних.

Ключові слова: криптографічний захист, телеметрія, розподілена система моніторингу, небезпечний об'єкт, автентифіковане шифрування, керування ключами.

CRYPTOGRAPHIC PROTECTION METHODS FOR TELEMETRY DATA IN DISTRIBUTED MONITORING SYSTEMS OF HAZARDOUS FACILITIES

D. V. Lukiienko, S. V. Sotnik

Kharkiv National University of Radio Electronics

Ukraine, 61166, Kharkiv, Nauky Ave., 14

E-mail: dmytro.lukiienko@nure.ua, svetlana.sotnik@nure.ua

Annotation: The work considers cryptographic protection methods for telemetry data in distributed monitoring systems of hazardous facilities. A threat model is built covering interception, message spoofing and replay, node compromise and archive tampering. The application of authenticated encryption, lightweight algorithms for resource-constrained nodes, digital signatures and secure transport protocols is analyzed. Key management, replay protection under unstable time synchronization, evidential integrity of archives and migration to post-quantum algorithms are discussed. The trade-off between protection level, node energy consumption and data delivery latency is outlined.

Key words: cryptographic protection, telemetry, distributed monitoring system, hazardous facility, authenticated encryption, key management.

Моніторинг небезпечних об'єктів – хімічних виробництв, магістральних трубопроводів, гідротехнічних споруд, сховищ палива, гірничих виробок – ґрунтується на безперервному зборі телеметрії з територіально рознесених вимірювальних вузлів, і саме на підставі цих даних ухвалюються рішення про зупинку процесу, евакуацію персоналу чи оголошення тривоги [1-6]. Спотворення телеметрії за наслідками прирівнюється до відмови самої системи захисту, а показання, яким не можна довіряти, є небезпечнішими за їх відсутність, оскільки створюють хибне відчуття контрольованості ситуації.

Розподілена архітектура таких систем суттєво посилює вимоги до захисту: вимірювальні вузли розташовані поза периметром охорони, живляться від автономних джерел і передають дані відкритими радіоканалами чи мережами операторів зв'язку, що робить їх уразливими до перехоплення, підміни, повторного відтворення повідомлень, компрометації вузлів і спотворення архівів. При цьому для телеметрії небезпечних об'єктів пріоритетність

73

властивостей захисту відрізняється від типової корпоративної – на перший план виходять цілісність, автентичність джерела й актуальність повідомлення, тоді як конфіденційність відіграє другорядну роль.

Додаткової складності надають обмежені ресурси автономних вузлів (енергоживлення, обчислювальна потужність, обмежений розмір кадру в каналах малої потужності), нестійка синхронізація часу в підземних спорудах і металевих конструкціях, необхідність довготривалого зберігання архівів з доказовою цілісністю для розслідування аварій, а також перспектива компрометації класичних криптоалгоритмів квантовими обчисленнями. Відсутність узгодженої методики поєднання автентифікованого шифрування, полегшених криптографічних примітивів, керування ключами в польових умовах та постквантових рішень обумовлює **актуальність** розроблення комплексних методів криптографічного захисту телеметричних даних у розподілених системах моніторингу стану небезпечних об'єктів.

Модель загроз доцільно формувати за етапами життєвого циклу повідомлення. Під час передавання можливі пасивне перехоплення, активне втручання типу «людина посередині», повторне відтворення раніше перехоплених пакетів і селективне блокування тривожних повідомлень. На рівні вузла – фізичний доступ, зчитування ключів з пам'яті, підміна прошивки, клонування пристрою. На рівні сервера – несанкціонована зміна архіву та підробка звітності. Окремо слід урахувувати відмову в обслуговуванні, за якої дані не спотворюються, але не надходять вчасно. Виходячи з цієї моделі, базовим механізмом захисту телеметрії слід вважати автентифікацію та контроль цілісності повідомлень із забезпеченням їхньої свіжості, тоді як шифрування застосовується відповідно до вимог конфіденційності.

Загальну послідовність криптографічного оброблення телеметрії подано на рис. 1. Сформований вузлом пакет обробляється криптомодулем, який виконує автентифіковане шифрування, формує тег автентичності та додає лічильник повідомлень. Далі дані проходять канал передавання, перевіряються шлюзом на рівні автентичності джерела, надходять до сервера моніторингу для контролю цілісності й розміщуються в захищеному архіві. Контур керування ключами охоплює всі етапи, оскільки без коректної генерації, розподілу та ротації ключів решта механізмів втрачає сенс.



Рисунок 1 – Схема криптографічного оброблення телеметричних даних

Основою захисту потоку є автентифіковане шифрування з приєднаними даними, яке одночасно забезпечує конфіденційність корисного навантаження та цілісність службових полів. Практично застосовують блокові шифри в режимах GCM або CCM, а також поточкові схеми з вбудованою автентифікацією. Український стандарт ДСТУ 7624:2014 визначає симетричний блоковий шифр «Калина», а ДСТУ 7564:2014 – геш-функцію «Купина», що дає змогу будувати рішення відповідно до національних вимог [7, 8]. Заголовок пакета, ідентифікатор вузла та лічильник слід включати саме як приєднані дані, інакше злоумисник може змінити маршрутизацію повідомлення без порушення перевірки.

Вузли з обмеженими ресурсами потребують полегшених алгоритмів. Мікроконтролер з автономним живленням, працюючи в мережі малої потужності, передає короткі пакети розміром у десятки байтів, тому додавання довгого коду автентичності суттєво збільшує час

радіопередавання й енергоспоживання. У таких випадках застосовують компактні схеми автентифікованого шифрування, зокрема родину ASCON, а параметри тегів автентичності слід обирати з урахуванням допустимого ризику підробки та ресурсних обмежень вузла.

Асиметричні механізми доцільні там, де необхідні автентифікація вузлів, масштабоване керування ключами та можливість криптографічного підтвердження походження даних. Електронний цифровий підпис на еліптичних кривих, зокрема за ДСТУ 4145-2002, дозволяє однозначно пов'язати повідомлення з конкретним вузлом і забезпечити криптографічне підтвердження походження даних навіть у разі компрометації сервера. Узгодження ключів за ефемерною схемою Діффі – Геллмана на еліптичних кривих (ECDHE) дає змогу отримувати сеансові ключі з властивістю прямої секретності.

Водночас підпис кожного окремого відліку є надлишковим: раціональним рішенням є симетрична автентифікація поточкових даних і підпис агрегованих блоків або тривожних повідомлень.

Керування ключами залишається найскладнішою частиною системи. Потрібні захищена генерація на самому вузлі, зберігання в апаратному елементі безпеки, персоналізація під час монтажу, планова ротація, негайне відкликання при виявленні компрометації та надійне знищення ключів під час виведення обладнання з експлуатації. Спільний ключ на всі вузли є поширеною й неприпустимою спрощеною практикою: компрометація одного пристрою в польових умовах відкриває всю мережу. Ієрархія «кореневий ключ – ключ групи – сеансовий ключ» дає змогу локалізувати наслідки інциденту.

Захист від повторного відтворення потребує окремої уваги через особливості об'єктів моніторингу. Позначки часу є природним рішенням, але залежать від синхронізації, яка в підземних спорудах, металевих конструкціях або за навмисних завад може бути втрачена. Тому доцільно поєднувати монотонні лічильники повідомлень, збережені в незалежній пам'яті, з вікнами допустимого відхилення часу та захищеним протоколом синхронізації. Сервер має відхиляти пакети з невідповідним лічильником, але фіксувати такі спроби як подію безпеки, а не просто ігнорувати їх. Перспективним напрямом є застосування предиктивної аналітики для завчасного виявлення аномалій у потоці телеметрії та прогнозування розвитку небезпечної ситуації [9].

Вибір рівня, на якому застосовується криптографія, визначає реальну межу довіри. Захист на транспортному рівні за протоколами TLS або DTLS зручний, проте шлюз розшифровує дані, тому його компрометація призводить до можливості підміни показань. Наскрізний захист від вузла до сервера моніторингу зберігає цілісність незалежно від довіри до проміжних елементів, хоча ускладнює агрегацію та фільтрацію трафіку. Для об'єктів підвищеної небезпеки обґрунтованим є поєднання обох підходів: транспортне шифрування ділянки зв'язку та наскрізна автентифікація самого вимірювання.

Цілісність архіву має самостійне значення, оскільки саме архів є основою розслідування аварій. Послідовне зв'язування записів гешами, побудова деревоподібних структур контрольних сум і періодичне засвідчення станів архіву дають змогу виявити ретроспективну зміну даних. Журнали доступу мають захищатися тими самими механізмами, інакше зміну можна приховати редагуванням журналу.

Криптографічний захист не повинен знижувати доступність системи. Якщо перевірка автентичності не пройшла, такі дані не повинні використовуватися для формування керувальних рішень, але можуть зберігатися в ізольованій карантинній зоні з відповідною позначкою та реєстрацією події безпеки. Аналогічно відмова служби ключів не має призводити до зупинення збирання телеметрії. Доцільно передбачати режим зниженої функційності, за якого вузол продовжує вимірювання й локальне накопичення з подальшим захищеним відвантаженням після відновлення зв'язку.

Ресурсні обмеження визначають остаточну конфігурацію. Криптографічні перетворення збільшують обсяг пакета, час роботи радіомодуля та споживання енергії, що безпосередньо впливає на строк служби автономного живлення. Апаратні прискорювачі в сучасних мікроконтролерах суттєво зменшують ці витрати, тому вибір елементної бази слід здійснювати одночасно з вибором алгоритмів, а не після нього.

Окремою перспективою є перехід до постквантових алгоритмів. Системи моніторингу небезпечних об'єктів експлуатуються десятиліттями, а архіви зберігаються тривалий час, тому актуальним є сценарій відкладеного розкриття раніше перехоплених даних. З урахуванням сучасного стану стандартизації доцільно розглядати гібридне застосування класичних і постквантових механізмів, зокрема ML-KEM (FIPS 203) для встановлення ключів та ML-DSA (FIPS 204) або SLH-DSA (FIPS 205) для цифрового підпису. Це зберігає сумісність з наявним обладнанням і зменшує ризик помилок раннього впровадження.

Технічні механізми діють лише разом з організаційними процедурами. Потрібні розподіл ролей адміністрування ключів, регламент реагування на інциденти, контроль цілісності прошивок вузлів і періодичний аудит. Вимоги до кібербезпеки промислових систем керування мають ураховуватися на етапі проєктування, а не додаватися після введення в експлуатацію.

ВИСНОВКИ. Телеметрія розподілених систем моніторингу небезпечних об'єктів потребує захисту, у якому пріоритетними є цілісність, автентичність джерела та актуальність повідомлення, а конфіденційність має підпорядковане значення. Ефективним є багаторівневий підхід: автентифіковане шифрування потоку, полегшені алгоритми для автономних вузлів, підпис агрегованих блоків, наскрізна перевірка цілісності незалежно від довіри до шлюзів та захищене зберігання архіву. Основними обмеженнями залишаються енергоресурс вузлів, розмір кадру каналів малої потужності, складність керування ключами в польових умовах і нестійка синхронізація часу. Аналіз показує, що вирішальним чинником є не вибір окремого шифру, а побудова повного життєвого циклу ключів і збереження доступності системи за часткової відмови криптографічних служб. Подальші дослідження потребують розроблення методики оцінювання співвідношення між рівнем захисту, енергоспоживанням вузла та своєчасністю доставлення тривожних повідомлень.

ЛІТЕРАТУРА

1. Nevludov, I. Sh., & et al. (2025). Application of artificial intelligence in additive manufacturing (3D printing). *Proceedings of the XVIII International Scientific and Practical Conference "Information Technologies and Automation – 2025"*, October 30-31, 2025. Odessa, Ukraine, 2025, pp. 1006-1009
2. Sotnik, S. (2026). Method of combined indexing for effective search in multi-attribute catalogs of technical components. *Radio Electronics, Computer Science, Control*, 2(77), pp. 208-229. DOI:10.15588/1607-3274-2026-2-18
3. Nevliudov, I., & et al. (2026). Implementing Industry 5.0 technologies in civil safety emergency systems for intelligent management. Scientific Forum: Theory and Practice of Research: Collection of Scientific Papers «SCIENTIA» with Proceedings of the XII International Scientific and Theoretical Conference, July 17, 2026. San Francisco, USA: International Center of Scientific Resea, 2026, pp. 337-339
4. Sotnik, S. (2025). Development of a range measurement module on an ultrasonic sensor with a GSM module. *Radio Electronics, Computer Science, Control*, 2, pp. 32-44
5. Shrubkovskiy, Y. V., & et al. (2025). Development of a structural scheme for automatic dosing of liquid components. *Proceedings of the V International Scientific Conference "Period of Transformation Processes in World Science: Tasks and Challenges"*, June 6, 2025, Kropyvnytskyi, Ukraine, 2025, pp. 242-246
6. Sotnik, S. (2024). Integration of IoT into security systems: opportunities and risks.

International Journal of Academic Engineering Research (IJAER), 8(11), pp. 56-61

7. Фесенко, А., & et al. (2024). Порівняння алгоритмів стиснення та геш-функцій готових програмних рішень у розрізі створення власного застосунку. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 3(23), 284-309

8. Сніосек, О., & et al. (2025). Модель постквантової інфраструктури відкритих ключів з використанням квантового генератора випадкових чисел для автономної системи диференціальної корекції глобальних навігаційних супутникових систем. Вісник Херсонського національного технічного університету, 3(4 (95)), 235-244

9. Nevliudov, I., & et al. (2026). Predictive analytics and artificial intelligence in emergency warning systems. *Proceedings of the VIII International Scientific and Theoretical Conference Modern Vision of Implementing Innovations in Scientific Studies*, August 7, 2026. Marseille, French Republic, 2026, pp. 108-111