УДК 004.056:681.518:531.787

ЗАБЕЗПЕЧЕННЯ КІБЕРЗАХИСТУ ТА ДОСТОВІРНОСТІ ВИМІРЮВАЛЬНОЇ ІНФОРМАЦІЇ В АВТОМАТИЗОВАНИХ СИСТЕМАХ МОНІТОРИНГУ ВИРОБНИЧИХ ПРОЦЕСІВ

Уляна ПАНОВИК[1,2], Роман ГІДЕЙ[2], Валерія БАЛАЦЬКА[1]
[1] Львівський державний університет безпеки життєдіяльності
[2] Національний університет «Львівська політехніка»

Анотація. *Запропоновано інформаційно-алгоритмічну модель кіберзахисту та достовірності вимірювальної інформації в автоматизованих системах моніторингу виробничих процесів. Розроблено модуль довіри для перевірки автентичності, цілісності й метрологічної узгодженості даних. Моделювання підтвердило підвищення індексу цілісності до 0,98 і скорочення часу виявлення спотворень. Результати можуть бути впроваджені в автоматизованих системах моніторингу для підвищення надійності контролю.*

Ключові слова: *кіберзахист, достовірність даних, модуль довіри, метрологічна узгодженість.*

Abstract. *An information and algorithmic model for cybersecurity and measurement data reliability in automated production monitoring systems has been proposed. A trust module was developed to verify data authenticity, integrity, and metrological consistency. Simulation confirmed an increase in the integrity index to 0.98 and a reduction in distortion detection time. The results can be implemented in automated monitoring systems to improve control reliability.*

Keywords: *cybersecurity, data reliability, trust module, metrological consistency.*

Зі збільшенням кількості сенсорів у промислових мережах зростає обсяг вимірювальної інформації, від якої залежить якість управлінських рішень. Відкритість мережевих протоколів і відсутність комплексного метрологічно-кіберзахисного підходу створюють ризики спотворення даних — як навмисного (кібератаки, фальсифікація), так і випадкового (похибки, шуми). Традиційні засоби кіберзахисту не враховують метрологічні параметри, а класичний метрологічний контроль — автентичність джерел і цілісність потоку. Тому необхідна інтеграція метрологічного та кібернетичного підходів для забезпечення точності, автентичності й довіри до даних. У сучасних дослідженнях ця проблема розглядається в межах концепції *trusted sensing*, що поєднує метрологічну достовірність із криптографічною перевіркою даних (хешування, цифрові підписи, блокчейн). Попри наявність стандартів ISO/IEC 27019, IEC 62443 і NIST SP 800-82, поки не існує інтегрованої моделі, яка одночасно враховувала б точність вимірювань, стійкість каналів і автентичність сенсорів [1, 2].

Метою дослідження є розроблення інформаційно-алгоритмічної моделі, що поєднує метрологічні показники точності (похибка, стабільність,

повторюваність) із параметрами кіберзахисту (цілісність, автентичність, стійкість каналу), формуючи єдиний критерій довіри до даних. У моделі використано узагальнений показник достовірності вимірювальної інформації, який відображає взаємозв'язок метрологічної точності, автентичності джерела, цілісності потоку та стійкості каналу до атак. Для його практичного обчислення застосовується індекс довіри Td, що визначає рівень надійності кожного пакета даних. Отже, поставлене завдання полягає у розробленні алгоритму функціонування модуля довіри, який забезпечує автоматичну оцінку *Td* у реальному часі та прийняття рішення щодо достовірності кожного вимірювального пакета (рис. 1).

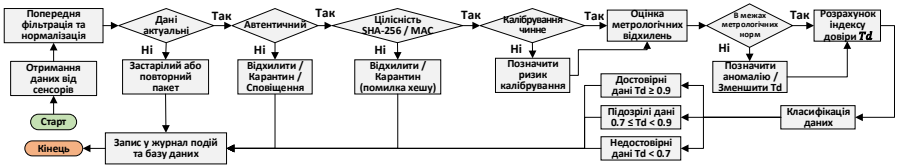

Рисунок 1 – Алгоритм функціонування модуля довіри до сенсорних даних

Розроблена інформаційно-алгоритмічна модель підвищує достовірність вимірювальної інформації шляхом інтеграції метрологічних і кіберзахисних механізмів у структурі автоматизованої системи моніторингу. Система реалізована як багаторівнева архітектура, де дані сенсорів проходять етапи фільтрації, перевірки автентичності, контролю цілісності та оцінювання довіри. Основний контур даних має вигляд: сенсори → контролер → агент шифрування → агрегатор → модуль довіри → база даних → інтерфейс користувача. Сенсори зчитують фізичні параметри, контролер оцифровує сигнали та передає їх до каналу зв'язку. Агент шифрування захищає інформацію за допомогою AES-256 або RSA, агрегатор об'єднує потоки з різних сенсорів і надсилає їх у модуль довіри. Центральний елемент — модуль довіри (Trust Module) — виконує перевірку автентичності, цілісності та метрологічної узгодженості даних. База даних зберігає первинні та перевірені значення разом із журналом подій, забезпечуючи контроль змін і рівня достовірності. Модуль довіри виконує п'ять основних функцій: перевірку автентичності сенсорів, контроль метрологічної узгодженості, перевірку цілісності, оцінку рівня довіри та прийняття рішення. Для кожного сенсора використовується криптографічний ідентифікатор, що запобігає підміні. Цілісність даних контролюється через хешування (SHA-256), а метрологічна узгодженість перевіряється за статистичними критеріями. На основі цих параметрів формується індекс довіри Td: високі значення свідчать про достовірність даних, нижчі — про необхідність повторної перевірки. Модуль забезпечує оперативну оцінку достовірності вимірювань у реальному часі.

Для перевірки ефективності запропонованої моделі проведено імітаційне моделювання у середовищі Python. Дослідження охоплювало два сценарії: нормальний режим роботи — передавання достовірних сенсорних даних без спотворення; атака на сенсорну мережу — випадки підміни даних та змін хеш-кодів пакетів. На вхід подавався масив із 10 000 вимірювальних точок, кожна з яких мала власні параметри похибки, контрольної суми та позначку автентичності. Для кожного пакета обчислювався індекс довіри Td за формулою: $Td = w_1(1 - /E_m/) + w_2 I_c + w_3 A_s + w_4 S_t$, де вагові коефіцієнти w_i приймали значення 0,25 для рівномірного впливу чинників. Порівняльні результати подано у таблиці.

Таблиця – Результати моделювання ефективності модуля довіри

Показник	**Без модуля довіри**	**З модулем довіри**	**Поліпшення**
Частка спотворених даних, E_m %	12 %	2 %	−10 %
Середній час виявлення спотворень, S_t с	7,4	2,3	в 3 рази швидше
Індекс цілісності *Ic*	0,87	0,98	+12,6 %
Коефіцієнт довіри *Td*	0,82	0,96	+17,1 %
Кількість відхилених пакетів A_s (із 10 000)	1180	210	−82 %

Результати свідчать, що використання модуля довіри суттєво підвищує достовірність сенсорних даних та знижує ризик прийняття некоректних рішень у виробничій системі. У нормальному режимі коефіцієнт довіри перевищує 0,95, а при моделюванні атаки система коректно відхиляє більшість спотворених пакетів. Застосування алгоритму на рівні агрегатора дозволяє проводити валідацію у реальному часі без впливу на швидкодію моніторингу.

У ході дослідження розроблено інформаційно-алгоритмічну модель кіберзахисту та достовірності вимірювальної інформації, що поєднує метрологічні критерії з механізмами безпеки. Центральним елементом є модуль довіри, який перевіряє автентичність, цілісність і метрологічну узгодженість даних у реальному часі. Моделювання показало підвищення індексу цілісності до 0,98 і скорочення часу виявлення спотворень, що підтверджує ефективність підходу та його придатність для IoT- і CPS-систем моніторингу виробництва.

Література

1. Janakiraman S. CYBER SECURITY FOR INDUSTRIAL AUTOMATION & CONTROL SYSTEMS. *Oil and Gas Business*. 2024. No. 1. P. 176–194. URL: https://doi.org/10.17122/ogbus-2024-1-176-194

2. Пановик У., Гідей Р. Математичне моделювання процесу агрегації та обробки вимірювальної інформації в автоматизованих метрологічних системах моніторингу. Вимірювальна та обчислювальна техніка в технологічних процесах, 2025. 82(2), с. 37–44. URL: https://doi.org/10.31891/2219-9365-2025-82-6