ІНФОКОМУНІКАЦІЙНІ ТЕХНОЛОГІЇ

УДК 004.6:621.39
DOI https://doi.org/10.36994/2788-5518-2025-01-09-01

МЕТОДИКА ФОРМУВАННЯ СТРУКТУРИ ЦЕНТРУ ЗБИРАННЯ ТА ОБРОБЛЕННЯ ДАНИХ ПІД ЧАС МОНІТОРИНГУ СТАНУ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Гнатюк В. О., *к.т.н., доцент, Державний університет «Київський авіаційний інститут», Київ, Україна; ДержНДІ технологій кібербезпеки, Київ, Україна. https://orcid.org/0000-0002-4916-7149, viktor.hnatiuk@npp.kai.edu.ua*

Зандер К. Ю., *PhD аспірант, Державний університет «Київський авіаційний інститут», Київ, Україна. https://orcid.org/0009-0006-4944-9249, 8390983@stud.kai.edu.ua*

Анотація. *У статті подано комплексну методику проєктування архітектури центру збирання та обробки даних, призначену для моніторингу стану об'єктів критичної інфраструктури. Дослідження включає розроблення структурної та функціональної схеми, а також логічної моделі, що ілюструє взаємодію між компонентами системи, що беруть участь у збиранні та обробці даних у контексті моніторингу критичної інфраструктури. Запропонований підхід ураховує сучасні вимоги до надійності, відмовостійкості, масштабованості, кібербезпеки та продуктивності в режимі реального часу. Особлива увага приділяється типам датчиків, що використовуються в різних сферах критичної інфраструктури, включаючи енергетику, транспорт, водопостачання, телекомунікації й охорону здоров'я. Методика також досліджує інтеграцію сенсорних мереж з технологіями зв'язку п'ятого покоління (5G) та інтернетом речей (IoT), що дає змогу створювати більш чутливі й гнучкі системи моніторингу. Крім того, дослідження підкреслює багаторівневий підхід до обробки даних за допомогою парадигм периферійних, туманних і хмарних обчислень. Це дає можливість зменшити затримку, збалансувати навантаження між обчислювальними ресурсами й покращити реагування на критичні інциденти. Уведено математичну модель, основану на теорії множин, для визначення складу датчиків, необхідного для ефективного моніторингу інфраструктури. Методика розроблена як основа для побудови інтелектуальних систем моніторингу, здатних забезпечити стабільну та безпечну роботу основних послуг. Вона також підтримує інтеграцію інструментів штучного інтелекту для прогнозування стану системи й раннього виявлення аномалій. Це може значно покращити можливості прогнозного обслуговування та безпеку експлуатації. Результати цього дослідження є особливо цінними для фахівців, які працюють у сфері телекомунікацій, кібербезпеки, автоматизації та реагування на надзвичайні ситуації. Крім того, вони надають практичну інформацію урядовим і регуляторним органам, відповідальним за захист національних інфраструктурних активів.*

Ключові слова: *критична інфраструктура, сенсори, IoT, 5G, обробка даних у реальному часі.*

METHODOLOGY FOR DESIGNING THE ARCHITECTURE OF A DATA COLLECTION AND PROCESSING CENTER FOR CRITICAL INFRASTRUCTURE MONITORING

Viktor Gnatyuk, *Ph.D., Ass. Prof., State University "Kyiv Aviation Institute"; ICTIP, Kyiv, Ukraine. https://orcid.org/0000-0002-4916-7149, viktor.hnatiuk@npp.kai.edu.ua*

Kostiantyn Zander, *State University "Kyiv Aviation Institute", Kyiv, Ukraine. https://orcid.org/0009-0006-4944-9249, 8390983@stud.kai.edu.ua*

Abstract. *The paper presents a comprehensive methodology for designing the architecture of a data collection and processing center intended for monitoring the condition of critical infrastructure facilities. The study includes the development of a structural and functional scheme, along with a logical model illustrating the interaction between system components involved in data acquisition and processing within the context of critical infrastructure monitoring.*

The proposed approach considers modern requirements for reliability, fault tolerance, scalability, cybersecurity, and real-time performance. Special attention is given to the types of sensors used across various critical infrastructure domains, including energy, transportation, water supply, telecommunications,

and healthcare. The methodology also explores the integration of sensor networks with fifth-generation (5G) communication technologies and the Internet of Things (IoT), enabling more responsive and flexible monitoring systems.

Furthermore, the research emphasizes the layered approach to data processing through edge, fog, and cloud computing paradigms. This allows for reduced latency, balanced load distribution across computing resources, and improved responsiveness to critical incidents. A mathematical model based on set theory is introduced to define the sensor composition needed for effective infrastructure monitoring.

The methodology is designed to serve as a foundation for building intelligent monitoring systems capable of ensuring the stable and secure operation of essential services. It also supports the integration of artificial intelligence tools for system condition forecasting and early anomaly detection. This can significantly enhance predictive maintenance capabilities and operational safety.

The results of this study are particularly valuable to professionals working in telecommunications, cybersecurity, automation, and emergency response. Moreover, they provide practical insights for governmental and regulatory bodies responsible for protecting national infrastructure assets.

Key words: *critical infrastructure; sensors; IoT; 5G; real-time data processing.*

Вступ

Критична інфраструктура (далі – КІ) є основою функціонування держави й суспільства, охоплюючи енергетику, транспорт, водопостачання, телекомунікації та інші життєво важливі галузі. В умовах сучасних викликів, таких як кіберзагрози, техногенні аварії, природні катастрофи й військові ризики, необхідність забезпечення надійного моніторингу стану об'єктів КІ набуває стратегічного значення.

Одним із ключових аспектів ефективного моніторингу є створення центру збирання й оброблення даних, який дає змогу в режимі реального часу отримувати, аналізувати та інтерпретувати інформацію з розподілених сенсорних систем. Розробка методики формування структури такого центру є актуальною через низку причин: усе більша складність і масштаб КІ (сучасні об'єкти КІ генерують великі обсяги даних, що потребують ефективної обробки й аналізу; використання технологій Big Data, машинного навчання та інтернету речей (далі – IoT) дає можливість підвищити точність прогнозування аварійних ситуацій); необхідність забезпечення безперервності роботи критичних систем (відмова будь-якого елемента КІ може призвести до каскадних збоїв, значних економічних збитків і загрози для життя людей; централізовані й розподілені системи збору даних допомагають швидко реагувати на аномалії та запобігати критичним відмовам); високі вимоги до безпеки та стійкості (дані, що передаються й обробляються в центрі моніторингу, мають бути захищеними відповідно до міжнародних стандартів (ISO/IEC 27001, IEC 62443); використання 5G, Edge Computing і квантово-стійких алгоритмів шифрування підвищує стійкість системи до атак; інтеграція сучасних технологій зв'язку (5G, SDN (Software-Defined Networking), MEC (Multi-Access Edge Computing) дає змогу зменшити затримки в передачі даних і масштабувати інфраструктуру відповідно до вимог часу; використання блокчейн-технологій у центрі моніторингу забезпечує прозорість і захист даних); міжнародні й національні вимоги до моніторингу КІ (європейська Директива NIS2 (Network and Information Security) і національні законодавчі акти вимагають підвищеної стійкості КІ до кіберзагроз; запровадження єдиних стандартів для центрів збирання даних підвищить ефективність міжгалузевої взаємодії).

Таким чином, розробка методики формування структури центру збирання та оброблення даних є важливим кроком до підвищення безпеки й надійності критичної інфраструктури, що сприятиме своєчасному реагуванню на загрози та мінімізації ризиків для суспільства.

Розробка ефективної методики формування структури центру збирання та оброблення даних (далі – ЦЗОД) для моніторингу об'єктів КІ потребує комплексного підходу, що базується на сучасних дослідженнях у сфері IoT, обробки великих даних, 5G-комунікацій, edge computing і кібербезпеки.

У роботі [1] запропоновано модель побудови графа центрів оброблення даних на основі часових рядів сенсорних вимірювань, що дає змогу виявляти аномалії в поведінці КІ. Такий підхід є перспективним для динамічного моніторингу в режимі реального часу. Подібну архітектуру збору даних від рівня обладнання до рівня застосунків розглянуто в праці [2], де розроблено систему DCDB для модульного та масштабованого моніторингу.

З огляду на потребу в надійній обробці потокових IoT-даних, у роботі [3] представлено систему з використанням механізмів fault-tolerance, що забезпечує надійність передачі й оброблення інформації в умовах міських інфраструктур.

Поглиблений огляд типів даних і їх використання в системах оцінювання ризиків для КІ наведено в публікації [4]. Автори акцентують на необхідності стандартизації форматів даних і їх доступності для державних і комерційних структур.

На особливу увагу заслуговує дослідження [5], де обґрунтовано переваги застосування fog- і cloud-комп'ютингу в розподіленій обробці IoT-даних, що є ключовим при проєктуванні ЦЗОД у системах критичного моніторингу.

У публікації [6] представлено методику оцінювання загроз і ризиків для об'єктів критичної інфраструктури, яка ґрунтується на сценарному підході до аналізу розвитку надзвичайних ситуацій. Автори

обґрунтовують доцільність використання сценаріїв для ідентифікації потенційних загроз, оцінки їхніх наслідків і формування превентивних заходів із захисту інфраструктурних об'єктів. Запропонована методика дає змогу здійснювати комплексний аналіз уразливостей і ризиків з урахуванням специфіки об'єкта, типів загроз і можливих сценаріїв їх реалізації, що є актуальним для розробки ефективних систем моніторингу й реагування.

Проаналізовані джерела дають змогу виокремити основні напрями розвитку: використання розподілених обчислень (Edge/Fog Computing), упровадження 5G та IoT в архітектуру збору даних, застосування AI/ML для прогнозування відмов, а також розробку стандартизованих моделей взаємодії між елементами інфраструктури. На цьому тлі необхідною є розробка цілісної методики побудови структури ЦЗОД з урахуванням особливостей саме критичних об'єктів.

Мета роботи полягає в розробці методики формування структури ЦЗОД, орієнтованої на ефективний моніторинг стану об'єктів критичної інфраструктури з урахуванням сучасних інформаційно-комунікаційних технологій, типів сенсорних даних, вимог до надійності, масштабованості, безпеки та реального часу.

Виконання досліджень

Здійснимо опис структурно-функціональної схеми роботи ЦЗОД під час моніторингу стану об'єктів КІ. Запропонована модель відображає логічну структуру взаємодії компонентів системи збирання та оброблення даних у контексті моніторингу стану об'єктів критичної інфраструктури (далі – ОКІ). Вона базується на таких функціональних рівнях (рис. 1):

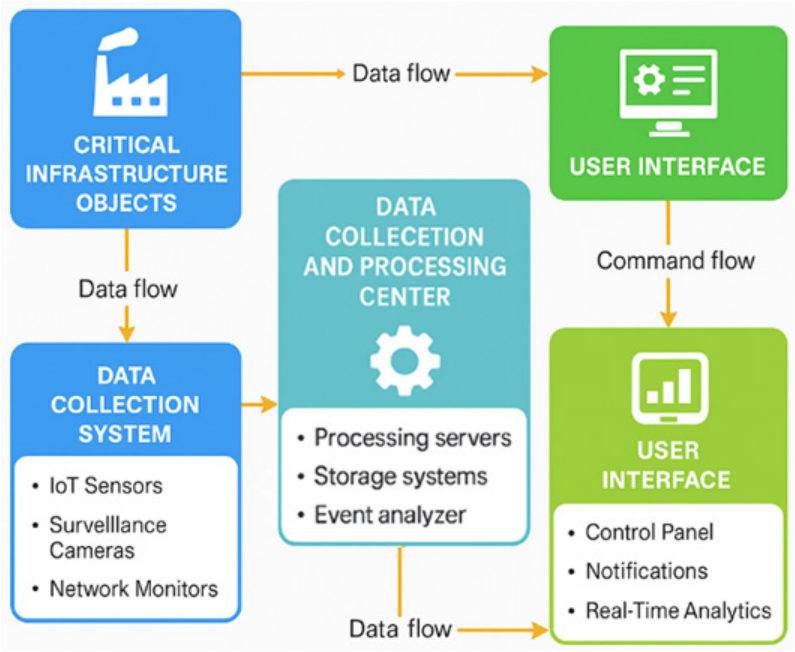

Рис. 1. Схема роботи ЦЗОД під час моніторингу стану об'єктів критичної інфраструктури

1. Об'єкти критичної інфраструктури. До цієї категорії належать інфраструктурні вузли, що мають високу стратегічну важливість: енергетичні системи, транспортні мережі, об'єкти водопостачання, аеропорти тощо. Моніторинг таких об'єктів здійснюється з метою виявлення аномалій, запобігання аваріям і забезпечення безперервності функціонування.
2. Система збору даних складається з набору сенсорів і пристроїв (датчики температури, тиску, вібрації, камери відеоспостереження, GPS-трекери тощо), які розміщуються на ОКІ та виконують безперервне зчитування параметрів стану. Дані формуються в реальному часі й передаються до шлюзу.
3. Комунікаційний шлюз (Communication Gateway) слугує проміжним етапом між сенсорами та центром обробки. Реалізує захищені канали зв'язку (VPN, TLS, IPsec) для передачі даних у режимі реального часу через мережі 5G, LTE, LPWAN, Wi-Fi або дротові інтерфейси.
4. ЦЗОД – основний обчислювальний осередок, де здійснюється агрегація та фільтрація даних; зберігання в централізованій базі (Data Lake або Data Warehouse); попередній і глибокий аналіз із використанням AI/ML-модулів (класифікація, кластеризація, виявлення аномалій); формування інцидентів і передача їх до системи прийняття рішень.
5. Користувацький інтерфейс/центр управління. Інтерфейс для операторів або автоматизованих систем, де здійснюється візуалізація показників; оперативне реагування; автоматичне або ручне управління інфраструктурними об'єктами на основі аналізу даних.

Представлена схема (рис. 1) дає змогу забезпечити масштабовану, адаптивну й безпечну структуру системи моніторингу, яка здатна ефективно функціонувати в реальному часі. Її реалізація забезпечує підвищення якості обслуговування ОКІ та зниження ризиків техногенних або кіберінцидентів.

Підходи, методи, технології та стандарти до побудови ЦЗОД:

1. Підходи до побудови ЦЗОД.

Централізований підхід передбачає використання єдиного центру обробки даних (Data Processing Center, DPC), куди стікається вся інформація. Переваги: спрощене адміністрування, єдина точка контролю безпеки. Недоліки: висока затримка при передачі даних, вразливість до відмови.

Розподілений підхід базується на кількох вузлах обробки даних, які розташовані ближче до джерел даних. Переваги: підвищена відмовостійкість, зменшення затримки. Недоліки: складніше управління, вища вартість інфраструктури.

1.2. Хмарні, гібридні й локальні рішення. Хмарні рішення (AWS, Microsoft Azure, Google Cloud) забезпечують масштабованість і доступність. Гібридні рішення комбінують локальну інфраструктуру з хмарними сервісами, що забезпечує баланс між швидкістю й безпекою. Локальні рішення (on-premise) використовуються в ОКІ, де є жорсткі вимоги до безпеки.

1.3. Використання Edge Computing дає змогу обробляти дані безпосередньо на пристроях або проміжних вузлах перед передачею до основного центру. Це зменшує затримки й навантаження на мережу.

2. Методи оброблення й аналізу даних.

2.1. Машинне навчання для виявлення аномалій використовується для аналізу показників ОКІ та виявлення потенційних відмов. Основні методи: кластеризація (k-Means, DBSCAN), нейронні мережі (Autoencoder, LSTM), байєсівські моделі (Bayesian Networks).

2.2. Фільтрація й агрегування даних: алгоритм Калмана – для прогнозування стану систем, фільтрація за пороговими значеннями – спрощує аналіз даних, методи зменшення шуму – наприклад, Wavelet-трансформація.

2.3. Використання Big Data: Hadoop, Apache Spark для обробки великих обсягів даних, Cassandra, InfluxDB – для зберігання часових рядів.

3. Технології.

3.1. IoT-сенсори, датчики температури, вологості, тиску, вібрації, електромагнітного випромінювання, які збирають дані з ОКІ.

3.2. Бази даних: SQL (PostgreSQL, MySQL) – для структурованих даних, NoSQL (MongoDB, Cassandra) – для масштабованих сховищ, Time-Series DB (InfluxDB, TimescaleDB) – для потокових даних.

3.3. Протоколи передачі даних: MQTT – легкий протокол для IoT, CoAP – протокол для пристроїв з низьким енергоспоживанням, OPC UA – для промислових систем.

3.4. Контейнеризація й оркестрація: Docker – контейнеризація сервісів, Kubernetes – управління контейнерами для масштабованих систем.

4. Стандарти й нормативні вимоги.

4.1. Безпека інформації: ISO/IEC 27001 – забезпечення безпеки інформації, IEC 62443 – кібербезпека для промислових систем.

4.2. Моніторинг і надійність: ISO 22301 – управління безперервністю бізнесу, ITU-T Y.3053 – архітектури для моніторингу КІ.

Перелік сенсорів для моніторингу ОКІ.

Об’єкти критичної інфраструктури охоплюють різні галузі: енергетику, водопостачання, транспорт, зв’язок, оборону тощо. Для кожної сфери використовуються спеціалізовані сенсори для моніторингу стану об’єктів (рис. 2).

1. Сенсори фізичних параметрів.

1.1. Температурні сенсори: термопари (K, J, T, E типи) – для вимірювання високих і низьких температур, RTD (Platinum Resistance Temperature Detectors, PT100/PT1000) – точні вимірювання, ІЧ-пірометри – безконтактний моніторинг температури.

1.2. Вологоміри та гігрометри: ємнісні сенсори вологості – для середовища (вода, повітря), резистивні датчики – контроль рівня вологості.

1.3. Барометри (датчики тиску): абсолютні датчики тиску – атмосферний тиск, диференціальні датчики – моніторинг різниці тисків у системах, п’єзоелектричні датчики – високоточний контроль.

1.4. Сенсори вібрації та механічних коливань: акселерометри MEMS – контроль структурних коливань, геофони – сейсмічний моніторинг, п’єзоелектричні вібраційні сенсори – контроль механічного зносу.

2. Сенсори для моніторингу навколишнього середовища.

2.1. Сенсори газового складу: детектори чадного газу (CO), датчики метану (CH_4), пропану (C_3H_8), бутану (C_4H_{10}), аналізатори кисню (O_2), озону (O_3), азоту, VOC-сенсори (леткі органічні сполуки).

2.2. Радіаційні сенсори: Гейгер-Мюллерові лічильники – гамма, бета-випромінювання, напівпровідникові детектори – альфа, нейтронне випромінювання, сцинтиляційні датчики – спектральний аналіз радіації.

2.3 Хімічні аналізатори: іон-селективні електроди (ISE) – аналіз складу води, оптичні спектрометри – контроль забруднень.

3. Сенсори для моніторингу енергетичних об'єктів.

3.1. Електричні сенсори: напругоміри (Voltage Sensors) – контроль високої та низької напруги, амперметри (Current Sensors) – вимірювання струму, трансформатори струму (CT Sensors) – контроль змінного струму.

3.2. Сенсори потужності й енергії: датчики активної та реактивної потужності, лічильники електроенергії (Smart Meters).

3.3. Теплові сенсори: тепловізори – контроль нагріву електрообладнання, оптичні пірометри – безконтактний контроль перегріву.

4. Сенсори для моніторингу транспортної інфраструктури.

4.1. Датчики навантаження й напруги: тензодатчики (Strain Gauges) – контроль мостів, доріг, п'єзоелектричні сенсори – вимірювання тиску на поверхню.

4.2. GPS і GNSS-сенсори: приймачі GPS/GLONASS/Galileo – відстеження руху, IMU (Inertial Measurement Unit) – тривимірний моніторинг руху,

4.3. Контроль залізничної інфраструктури: лазерні сенсори деформацій, сенсори температури рейок.

5. Сенсори для кібербезпеки й телекомунікацій.

5.1. Сенсори мережевого трафіку: DPI (Deep Packet Inspection) – аналіз трафіку, Intrusion Detection Systems (IDS) – виявлення атак.

5.2. Фізичні сенсори захисту: детектори руху (PIR, ультразвукові), камери відеоспостереження (LiDAR, тепловізійні).

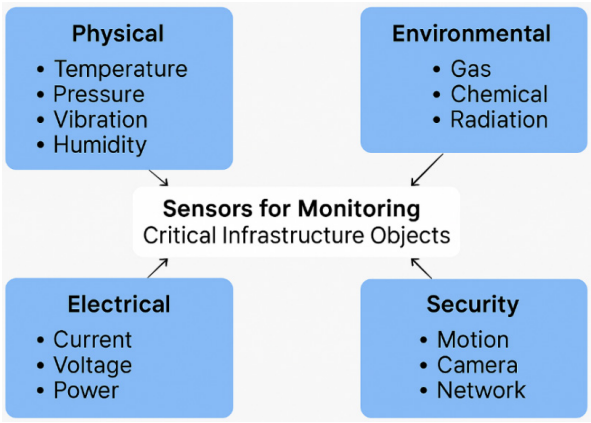

Рис. 2. Сенсори для моніторингу ОКІ

Передача показників з датчиків за допомогою 5G.

Передача показників з датчиків за допомогою 5G є одним із ключових сценаріїв використання технології. 5G забезпечує низьку затримку (1–10 мс) – важливо для моніторингу в реальному часі; високу пропускну здатність – дає змогу передавати великі масиви даних, наприклад, відео з камер або тепловізорів; масштабованість – підтримка до 1 мільйона пристроїв на 1 км² (mMTC); якість обслуговування (QoS) – можливість пріоритезації критичних даних.

Основні 5G-режими передачі даних: eMBB (Enhanced Mobile Broadband) – для камер відеоспостереження, тепловізорів, радарів; mMTC (Massive Machine-Type Communications) – для IoT-сенсорів (температури, вологості, вібрації, газів); URLLC (Ultra-Reliable Low-Latency Communications) – для критично важливих даних (енергетична інфраструктура, залізниця, кібербезпека).

Протоколи для передачі даних по 5G: MQTT (Message Queuing Telemetry Transport) – легкий протокол для IoT; CoAP (Constrained Application Protocol) – ефективний для низькоенергетичних пристроїв; OPC UA (Open Platform Communications Unified Architecture) – стандарт для промислових сенсорних мереж; HTTP/HTTPS + REST API – для інтеграції з вебсервісами.

Приклади використання 5G для сенсорів: енергетика (передача показників трансформаторів, генераторів, розподільчих щитів у режимі реального часу); транспорт (моніторинг залізничних колій, мостів через 5G-з'єднані тензодатчики); промисловість (контроль стану обладнання на заводах через підключені по 5G сенсори вібрації та температури); безпека (передача відео з камер і тепловізорів у центри обробки даних без затримок). 5G забезпечує ефективну та швидку передачу даних від сенсорів, що дає можливість будувати розумні системи моніторингу для КІ.

Математичний опис переліку сенсорів для моніторингу ОКІ на основі теорії множин.

Розглянемо множину S усіх сенсорів, що використовуються для моніторингу ОКІ. Цю множину можна представити як об'єднання підмножин, що відповідають різним сферам моніторингу:

$$S = S_{фіз} \cup S_{екол} \cup S_{енерг} \cup S_{трансп} \cup S_{безп} \ , \quad (1)$$

де $S_{фіз}$ – сенсори фізичних параметрів (температура, тиск, вібрація тощо); $S_{екол}$ – сенсори екологічного моніторингу (газові, хімічні, радіаційні); $S_{енерг}$ – сенсори енергетичної інфраструктури (струм, напруга, потужність); $S_{трансп}$ – сенсори для транспорту (навантаження, GPS, дорожній стан); $S_{безп}$ – сенсори для безпеки та кібербезпеки (камери, мережеві IDS).

Сенсори фізичних параметрів:

$$S_{фіз} = \{S_T, S_P, S_V, S_A, S_H\} , \quad (2)$$

де S_T – температурні сенсори, S_P – сенсори тиску, S_V – вібраційні сенсори, S_A – акселерометри, S_H – сенсори вологості.

Сенсори екологічного моніторингу:

$$S_{екол} = \{S_{CO}, S_{CH4}, S_{O2}, S_{VOC}, S_{рад}\} , \quad (3)$$

де S_{CO} – датчики чадного газу, S_{CH4} – детектори метану, S_{O2} – аналізатори кисню, S_{VOC} – сенсори летких органічних сполук, $S_{рад}$ – радіаційні сенсори.

Сенсори енергетичної інфраструктури:

$$S_{енерг} = \{S_V, S_I, S_P, S_Q\} , \quad (4)$$

де S_V – сенсори напруги, S_I – сенсори струму, S_P – датчики активної потужності, S_Q – датчики реактивної потужності.

Сенсори транспортної інфраструктури:

$$S_{трансп} = \{S_{GPS}, S_{IMU}, S_{strain}\} , \quad (5)$$

де S_{GPS} – GPS-приймачі, S_{IMU} – інерційні сенсори, S_{strain} – датчики напружень.

Сенсори безпеки та кібербезпеки:

$$S_{безп} = \{S_{PIR}, S_{CAM}, S_{IDS}\} , \quad (6)$$

де S_{PIR} – датчики руху, S_{CAM} – відеокамери, S_{IDS} – мережеві сенсори.

Множина сенсорів, які можуть передавати дані через 5G, визначається так:

$$S_{5G} = \{S_{високошвидк}, S_{масові\ IoT}, S_{критичні}\} , \quad (7)$$

де $S_{високошвидк}$ – сенсори, що потребують високої пропускної здатності (наприклад, камери, тепловізори), $S_{масові\ IoT}$ – численні сенсори для моніторингу (температури, вологості, газу), $S_{критичні}$ – сенсори для управління аварійними ситуаціями з мінімальною затримкою.

$$S_{5G} = \{S_{CAM}, S_{GPS}, S_{IMU}, S_{VOC}, S_{CO}, S_{PIR}, S_{IDS}, S_{strain}, S_{рад}\} , \quad (8)$$

Отже, множина сенсорів, що використовують 5G, є підмножиною загальної множини S, тобто $S_{5G} \subseteq S$.

Математичний опис процесу збору, передачі й обробки сенсорних даних із використанням технології 5G на прикладі ОКІ енергетичної підстанції:

1. Модель об'єкта як графа. Розглянемо підстанцію як граф:

$G = (V, E)$, де $V=\{v_1, v_2, \ldots, v_n\}$ – вузли (елементи: трансформатори, вимикачі, захисти, акумулятори), E – зв'язки (електричні або інформаційні).

Кожен вузол обладнаний сенсорами: $S=\{s_1, s_2, \ldots, s_m\}$ — множина сенсорів: s_1 – температура трансформатора; s_2 – рівень напруги; s_3 – струм витоку; s_4 – вібрація корпуса; s_5 – наявність диму/газу.

2. Процес збирання та передачі даних через 5G.

2.1. Формалізація даних.

Кожен сенсор s_i створює вимір: $d_i(t) \in R,\ t \in T,$ де T – дискретний часовий простір.

Узагальнено: $D(t)=[d_1(t), d_2(t), \ldots, d_m(t)]^T$.

2.2. Передача даних.

Передача сенсорних даних здійснюється через 5G з такими параметрами:

затримка: $\tau \approx 1{-}5$ мс;

пропускна здатність: $B \geq 10$ Гбіт/с;

надійність: $R \geq 99.999\%$;

кількість пристроїв: $N \leq 10^6$/км^2.

Модель каналу можна подати так: $y(t)=h(t)\cdot x(t)+n(t)$, де $x(t)$ – сигнал від сенсора; $h(t)$ – коефіцієнт каналу 5G (може бути стохастичним); $n(t)$ – шум (наприклад, гаусівський).

3. Edge-Fog-Cloud обробка.

3.1. Рівні обробки.

Edge (периферійні шлюзи): $f_{edge}(D(t)) = D'(t) \Rightarrow$ попередня обробка: фільтрація, нормалізація, тригер.

Fog: $f_{fog}(D')$ = агрегація даних, локальна аналітика, кластеризація.
Cloud: $f_{cloud}(D')$ = глобальна аналітика, історичний аналіз, машинне навчання.
4. Модель затримки передачі та обробки.
Загальний час обробки сенсорного запиту: $T_{total}=T_{sense}+T_{tx}+T_{edge}+T_{fog}+T_{cloud}$, де T_{sense} – час збору; $T_{tx}\approx\tau$ – час передачі через 5G; T_{edge} – обробка на шлюзі; T_{fog} – обробка на ближчому обчислювальному вузлі; T_{cloud} – аналітика в хмарі.
Можна оптимізувати T_{total} з урахуванням критичності подій: $min\ T_{total}$ за умовами $D'(t) >$ порогу.
5. Виявлення аномалій (напр., машинне навчання).
Формалізуємо вхідний вектор сенсорних даних: $\vec{X} = [d_1(t), d_2(t), ..., d_m(t)]$.
Класифікація стану: $y = f_{ML}(\vec{X})$, $y \in$ {«норма», «відхилення», «аварія»}.
Можна використати, наприклад, алгоритм: SVM; Random Forest; Autoencoder для аномалій.
6. Формалізація подій.
Множина подій: $\Omega=\{\omega_1,\omega_2,...,\omega_k\}$.
Наприклад: ω_1 – перевищення температури; ω_2 – утрата живлення; ω_3 – вторгнення в приміщення.
Тоді можна ввести матрицю реакцій: $A \in \{0,1\}^{k\times r}$, де $a_{ij}=1$, якщо подія ω_i вимагає реакції r_j.

Програмна реалізація на Java (фрагмент)

```
class Sensor {
    String id;
    double readValue() {
        return Math.random() * 100; // симуляція
    }
}

class Node {
    String name;
    List<Sensor> sensors;

    public double[] readAllSensors() {
        return sensors.stream().mapToDouble(Sensor::readValue).toArray();
    }
}

class Transmission5G {
    public double[] transmit(double[] data) {
        // моделювання затримки та шуму
        return Arrays.stream(data)
                     .map(d -> d + new Random().nextGaussian() * 0.1)
                     .toArray();
    }
}

class EdgeProcessor {
    public double[] preprocess(double[] data) {
        return Arrays.stream(data)
                     .filter(d -> d > 5.0) // умовна фільтрація
                     .toArray();
    }
}

class FogNode {
    public double aggregate(double[] data) {
        return Arrays.stream(data).average().orElse(0);
    }
}

class CloudAnalytics {
    public String classify(double value) {
        if (value > 90) return "Аварія";
        if (value > 60) return "Відхилення";
        return "Норма";
    }
}
```

Таблиця 1

Характеристики передачі та обробки даних на етапах системи моніторингу

Показник	Sensor → Edge	Edge → Fog	Fog → Cloud	**Коментарі**
Затримка передачі (мс)	1,0	1,2	0,8	Модельні значення з урахуванням 5G URLLC
Надійність зв'язку (%)	99,9	99,99	99,95	Локальний зв'язок забезпечує високу надійність; іноді не враховується окремо
Об'єм переданих даних (МБ/год)	120	100	250	Зниження обсягу на проміжному рівні за рахунок фільтрації
Частота подій (разів/год)	6	N/A	N/A	Визначається лише на рівні сенсорів
Попереднє оброблення	✓	✓	–	Edge і Fog здійснюють фільтрацію, нормалізацію, оцінку подій
Шифрування	—	✓	✓	Рекомендовано впровадити легке шифрування на сенсорах
Тип обробки	Локальна (Signal)	Агрегація	Аналітика/ML	Зростає складність та обчислювальне навантаження з кожним рівнем

Примітки:

– **N/A** – *Not Applicable, не застосовується для даного рівня;*

– *символ ✓ – функціональність присутня;*

– *символ «–» означає відсутність або неактуальність на відповідному етапі;*

– *усі показники є умовно типовими для енергетичних об'єктів із підтримкою 5G-зв'язку.*

У таблиці 1 наведено узагальнені характеристики роботи математичної моделі збору та обробки даних на прикладі енергетичної підстанції. Розглянуто основні показники для трьох ключових етапів інформаційного ланцюга: від сенсорного рівня (Sensor → Edge), проміжного рівня обробки (Edge → Fog) і передачі до хмарної інфраструктури (Fog → Cloud).

Затримка передачі є критичним параметром для своєчасного реагування на події. Завдяки використанню технологій 5G (режим URLLC), забезпечується низький рівень затримки, особливо на початкових етапах.

Надійність зв'язку зростає в напрямку до хмари, оскільки на рівні Fog і Cloud використовуються більш стабільні канали (оптоволоконні або приватні 5G-мережі). Значення можуть змінюватися залежно від конкретної реалізації.

Обсяг переданих даних зменшується на етапі Edge → Fog за рахунок попередньої обробки (агрегації, фільтрації шумів, усунення надлишкових даних), але збільшується на Fog → Cloud через накопичення історичних даних і їх реплікацію для аналітичної обробки.

Частота подій ураховується лише на рівні сенсорів, оскільки саме там генеруються сповіщення про аномалії або зміни у фізичних параметрах. На вищих рівнях здійснюється лише агрегація або повторне оцінювання їхньої важливості.

Попереднє оброблення реалізується на рівнях Edge та Fog і передбачає виявлення нетипових змін, нормалізацію даних і їх маркування. У хмарній інфраструктурі переважно виконується аналітична обробка, зокрема із застосуванням моделей машинного навчання (ML).

Шифрування впроваджено на етапах Fog → Cloud та Edge → Fog, що забезпечує конфіденційність даних на критичних ділянках. На рівні Sensor → Edge воно відсутнє через обмеження обчислювальних ресурсів сенсорних пристроїв, однак доцільно впровадити легкі криптографічні алгоритми.

Тип обробки на кожному етапі відрізняється: на Sensor та Edge — сигналізація й локальна обробка, на Fog – попередній аналіз та агрегування, на Cloud – глибокий аналіз, виявлення закономірностей, трендів, а також прийняття рішень у рамках систем підтримки.

Висновок

У статті розглянуто комплексний підхід до формування структури ЦЗОД, призначеного для забезпечення ефективного та надійного моніторингу стану ОКІ. Аналіз наявних підходів, технологій і стандартів дав змогу систематизувати перелік сенсорів, які забезпечують багаторівневий моніторинг об'єктів КІ – від фізичних параметрів (температура, тиск, вібрація) до кіберподій (спроби вторгнень, аномальні дії в мережах); оцінити можливості використання технологій 5G для забезпечення високошвидкісного, надійного та масштабованого з'єднання сенсорів і вузлів обробки даних у системах моніторингу; запропонувати математичну модель, що базується на теорії множин, для класифікації

сенсорних потоків відповідно до типу об'єктів КІ та їхніх функціональних характеристик; обґрунтувати доцільність використання гібридної архітектури, яка поєднує edge-, fog- і cloud-технології для обробки даних у реальному часі, а також довгострокового зберігання й аналітики; окреслити структуру ЦЗОД, що враховує вимоги до надійності, відмовостійкості, кібербезпеки та масштабованості, відповідно до особливостей ОКІ; сформулювати наукову новизну, яка полягає у створенні методики, що дає змогу оптимізувати структуру ЦЗОД з урахуванням сучасних технологічних можливостей, характеристик сенсорних потоків і специфіки об'єктів КІ.

Отримані результати можуть бути використані як основа для практичної реалізації центрів моніторингу ОКІ в критично важливих галузях, таких як енергетика, транспорт, водопостачання, зв'язок та оборонна промисловість. Подальші дослідження будуть присвячені моделюванню навантаження на ЦЗОД, а також упровадженню штучного інтелекту для автоматизованого аналізу зібраних даних.

Література

1. Zhang H., Li Z., Ren Z. Data-driven construction of data center graph of things for anomaly detection. *arXiv preprint arXiv:2004.12540*. 2020. https://arxiv.org/abs/2004.12540.

2. Netti A., Mueller M., Auweter A., Guillen C., Ott M., Tafani D., Schulz M. From facility to application sensor data: Modular, continuous and holistic monitoring with DCDB. *arXiv preprint arXiv:1906.07509*. 2019. https://arxiv.org/abs/1906.07509.

3. Morgan K. Geldenhuys, Jonathan Will, Benjamin J. J. Pfister, Martin Haug, Alexander Scharmann, Lauritz Thamsen. Dependable IoT data stream processing for monitoring and control of urban infrastructures. *arXiv preprint arXiv:2108.10721*. 2021. https://arxiv.org/abs/2108.10721.

4. Aron Larsson. Data use and data needs in critical infrastructure risk analysis. *Journal of Risk Research.* 2023. № 26(2). P. 190–210. https://doi.org/10.1080/13669877.2023.2181858.

5. Yassine A., Singh S., Hossain M. S., Muhammad G. (2019). IoT big data analytics for smart homes with fog and cloud computing. *Future Generation Computer Systems.* 2019. № 91. P. 563–573. https://doi.org/10.1016/j.future.2018.08.040.

6. Мурасов Р., Нікітін А., Мещеряков І., Підгородецький М., Поплавець С. Методика оцінювання загроз і ризиків для об'єктів критичної інфраструктури за сценаріями розвитку надзвичайних ситуацій. *Сучасні інформаційні технології у сфері безпеки та оборони*. Київ, Україна, 2024. № 48(3). С. 35–43. https://doi.org/10.33099/2311-7249/2023-48-3-35-43.

References

1. Zhang, H., Li, Z., & Ren, Z. (2020). Data-driven construction of data center graph of things for anomaly detection. *arXiv preprint arXiv:2004.12540*. https://arxiv.org/abs/2004.12540.

2. Netti, A., Mueller, M., Auweter, A., Guillen C., Ott M., Tafani D., Schulz M. (2019). From facility to application sensor data: Modular, continuous and holistic monitoring with DCDB. *arXiv preprint arXiv:1906.07509*. https://arxiv.org/abs/1906.07509.

3. Morgan K. Geldenhuys, Jonathan Will, Benjamin J. J. Pfister, Martin Haug, Alexander Scharmann, Lauritz Thamsen (2021). Dependable IoT data stream processing for monitoring and control of urban infrastructures. *arXiv preprint arXiv:2108.10721*. https://arxiv.org/abs/2108.10721.

4. Aron Larsson (2023). Data use and data needs in critical infrastructure risk analysis. *Journal of Risk Research, 26*(2), 190–210. https://doi.org/10.1080/13669877.2023.2181858.

5. Yassine, A., Singh, S., Hossain, M. S., & Muhammad, G. (2019). IoT big data analytics for smart homes with fog and cloud computing. *Future Generation Computer Systems, 91*, 563–573. https://doi.org/10.1016/j.future.2018.08.040.

6. Murasov R., Nikitin A., Meshcheriakov I., Pidhorodetskyi M., Poplavets S. (2024) "Methodology for assessing threats and risks for critical infrastructure objects under emergency development scenarios", Modern Information Technologies in the Sphere of Security and Defence. Kyiv, Ukraine, 48(3), pp. 35–43. https://doi.org/10.33099/2311-7249/2023-48-3-35-43.

Дата першого надходження рукопису до видання: 12.05.2025
Дата прийнятого до друку рукопису після рецензування: 16.06.2025
Дата публікації: 25.07.2025