УДК 004.7:004.451.3:004.056.5
DOI: https://doi.org/10.53920/ITS-2025-1;2-10

Ольга Миколаївна ТКАЧЕНКО,
доктор технічних наук, професор,
Київський національний університет імені Тараса Шевченка
ORCID ID: 0000-0001-7983-9033
Наталія Вікторівна ГАЛАГАН,
кандидат технічних наук, доцент,
Державний університет інформаційно-комунікаційних технологій
ORCID ID: 0000-0001-8582-3126
Наталія Олександрівна ЛАЩЕВСЬКА,
кандидат технічних наук, доцент,
Державний університет інформаційно-комунікаційних технологій
ORCID ID: 0000-0003-2148-115X
Володимир Олексійович ТКАЧЕНКО,
здобувач другого (магістерського) рівня вищої освіти,
Державний університет інформаційно-комунікаційних технологій
ORCID ID: 0009-0004-6260-6662

ПІДВИЩЕННЯ НАДІЙНОСТІ IoT-ВУЗЛІВ НА ОСНОВІ МЕХАНІЗМІВ ВИЯВЛЕННЯ ЗАВИСАНЬ

Стрімке зростання кількості IoT-вузлів у критично важливих сферах підвищує потребу в забезпеченні їх надійної роботи, особливо в умовах обмежених ресурсів, нестабільного середовища та відсутності постійного технічного контролю. У статті розглянуто проблему зависань і некоректних режимів роботи IoT-пристроїв, які можуть призводити до втрати даних, збоїв у керуванні та зниження загальної ефективності системи. Проаналізовано сучасні підходи до виявлення та запобігання зависанням, що включають апаратні watchdog-механізми, програмні засоби діагностики, інтелектуальні методи виявлення аномалій, а також хмарні рішення для віддаленого моніторингу. Визначено їх ключові обмеження, пов'язані з високими вимогами до ресурсів, недостатньою гнучкістю, низькою адаптивністю та слабкою придатністю до роботи на мікроконтролерах із малою пам'яттю. Запропоновано архітектуру легковагої системи контролю стану IoT-вузлів, що поєднує локальний моніторинг, спрощений аналіз аномалій, адаптивні порогові методи та базові механізми самовідновлення. Представлено метод раннього виявлення зависань, який включає використання heartbeat-сигналів, локальних апаратно-програмних перевірок, аналізу ресурсів та мінімальної телеметрії. Метод дозволяє виявляти відхилення до виникнення критичної відмови та знижує потребу у мережевій активності,

що особливо важливо для автономних енергообмежених пристроїв. Результати дослідження підтверджують доцільність поєднання апаратних і програмних механізмів із легкими аналітичними моделями. Зроблено висновок про необхідність подальшої розробки універсальних алгоритмів аномалій та уніфікованих методик тестування для різних IoT-платформ з метою підвищення відмовостійкості та автономності сучасних IoT-систем.

Ключові слова: *IoT-вузли, надійність, виявлення зависань, аномалії, watchdog, моніторинг стану, самовідновлення, вбудовані системи, TinyML, енергоефективність.*

Olha TKACHENKO,
Doctor of Technical Sciences, Professor,
Taras Shevchenko National University of Kyiv
Nataliia HALAHAN,
Candidate of technical sciences, associate professor,
State University of Information and Communication Technologies
Natalia LASHCHEVSKA,
Candidate of technical sciences, associate professor,
State University of Information and Communication Technologies
Volodymyr TKACHENKO,
graduate student,
State University of Information and Communication Technologies

IMPROVING THE RELIABILITY OF IOT NODES BASED ON FAILURE DETECTION MECHANISMS

The rapid expansion of IoT devices in critical domains requires highly reliable operation, especially under constraints of limited computing resources, unstable environments, and the absence of continuous maintenance. This article addresses the problem of software hangs and abnormal operating modes in IoT nodes, which often result in data loss, functional degradation, or complete device failure. Existing approaches such as hardware watchdog timers, software monitoring mechanisms, cloud-based diagnostics, and lightweight anomaly detection techniques are reviewed and their limitations identified. These limitations include insufficient adaptability, high memory and energy demands, limited observability of low-level faults, and reduced effectiveness on resource-constrained microcontrollers. The study proposes a lightweight architecture for IoT node state monitoring that integrates modular observation, simplified anomaly analysis, adaptive thresholds, and basic self-healing mechanisms. A method for early hang detection is developed, combining heartbeat messages, local resource monitoring, low-overhead anomaly indicators, and event-driven telemetry. This approach ensures timely detection of poten-

tial failures before a complete system halt and minimizes communication overhead, making it suitable for energy-limited autonomous devices. The results demonstrate that the combination of hardware safeguards with low-complexity software analytics significantly improves reliability and reduces downtime. The findings emphasize the need for unified testing methodologies, fault taxonomies, and scalable anomaly detection models tailored to heterogeneous IoT platforms. The proposed solutions support the development of more resilient, adaptive, and self-recovering IoT systems capable of maintaining stable operation in real-world environments.

Keywords: *IoT nodes, reliability, hang detection, anomaly detection, watchdog, state monitoring, self-healing, embedded systems, TinyML, energy efficiency*

Постановка проблеми. Стрімке зростання кількості IoT-пристроїв у критично важливих сферах - таких як промислова автоматизація, енергетика, транспорт, агромоніторинг, охорона здоров'я та «розумна інфраструктура» - висуває підвищені вимоги до надійності їх функціонування. На відміну від традиційних обчислювальних систем, IoT-вузли працюють у ресурсно-обмежених умовах, мають обмежену енергоефективність, значну варіативність апаратних платформ та нерідко експлуатуються у віддалених або важкодоступних місцях. За таких умов зависання програмного забезпечення, збої виконання або часткова втрата працездатності пристрою можуть призводити до тривалих простоїв, втрати даних, порушення безпеки або виходу з ладу цілих сегментів IoT-мереж [1].

Наявні механізми контролю стану вбудованих систем - такі як watchdog-таймери, brown-out detection або апаратні схеми відновлення - часто реалізуються некоректно, не адаптовані до складних сценаріїв роботи або не враховують комбінацію апаратних і програмних чинників, що спричиняють зависання. Крім того, високий рівень гетерогенності IoT-екосистеми ускладнює розроблення універсальних методів контролю, діагностики та автоматичного відновлення працездатності.

Таким чином, виникає науково-технічна проблема забезпечення гарантованої надійності IoT-вузлів шляхом створення ефективних механізмів виявлення, прогнозування та запобігання зависанням у реальному часі. Розв'язання цієї проблеми має безпосередній зв'язок із важливими науковими та практичними завданнями, зокрема [2, 3]:

- підвищення стійкості розподілених IoT-систем;
- мінімізація простоїв і втрат даних у критично важливих застосунках;
- створення самовідновлюваних embedded-систем;
- забезпечення кіберфізичної безпеки в умовах потенційних збоїв;
- підвищення довговічності та автономності енергообмежених пристроїв.

Розробка й удосконалення механізмів виявлення та запобігання зависанню IoT-вузлів є актуальним науковим завданням, оскільки спрямована на формування теоретичних основ та практичних методів підвищення надійності вбудованих систем, що є ключовим чинником їх ефективного та безпечного використання у сучасних і перспективних IoT-застосунках.

Аналіз останніх досліджень і публікацій. Проблематика забезпечення надійності IoT-вузлів залишається одним із ключових напрямів сучасних досліджень у сфері вбудованих систем та інтернету речей. Інтенсивний ріст кількості IoT-пристроїв, їх застосування у критично важливих сферах та робота в умовах обмежених обчислювальних і енергетичних ресурсів зумовили зростання уваги до питань відмовостійкості, раннього виявлення збоїв та запобігання зависанням. У наукових працях останніх років окреслюються кілька основних підходів до розв'язання цієї проблеми [5].

Першу групу становлять дослідження, присвячені апаратним засобам контролю працездатності, зокрема watchdog-таймерам, brown-out-детекторам та механізмам апаратного перезапуску. Ці засоби вважаються базовими для виявлення критичних зависань, однак вони здатні реагувати лише на повні втрати керованості і не забезпечують виявлення часткових деградацій продуктивності або логічних помилок, які не призводять до повного блокування виконання. У низці робіт підкреслюється, що неправильна конфігурація watchdog-механізмів або надмірно просте «годування» їх у циклі програми нерідко нівелює їх ефективність.

Іншим напрямом є розроблення вдосконалених апаратно-програмних рішень на базі багаторівневих та адаптивних контролерів. Запропоновано модифіковані схеми watchdog із динамічною зміною таймаутів, моніторингом окремих підсистем (пам'яті, шин, периферії) або з використанням апаратних логічних блоків для детекції аномалій у поведінці системи. Попри перспективність таких рішень, вони часто збільшують апаратну складність і енергоспоживання, що обмежує можливості їх застосування у низькопотужних IoT-вузлах [4].

Значну увагу привертають дослідження, орієнтовані на використання методів машинного навчання для локального виявлення аномалій у роботі вбудованих систем. Зокрема, в контексті технологій TinyML розглядається можливість виконання спрощених моделей класифікації або прогнозування на мікроконтролерах із дуже обмеженими ресурсами. Показано, що аналіз часових характеристик задач, поведінки периферійних інтерфейсів, використання пам'яті чи енергоспо-

живання може слугувати основою для раннього виявлення ймовірних збоїв ще до того, як вони переростуть у повне зависання. Проте більшість запропонованих моделей не враховує жорсткі обмеження типових IoT-вузлів, що часто мають десятки кілобайт оперативної пам'яті та працюють від автономних джерел живлення [6, 7].

Окремий напрям досліджень становлять архітектури самовідновлення (self-healing systems), у яких поєднано аналіз стану, предиктивні механізми та адаптивні стратегії відновлення. Такі підходи передбачають автоматичне перемикання між режимами роботи, ізоляцію проблемних компонентів, перезапуск окремих модулів або введення системи у безпечний режим до відновлення нормального стану. Хоча такі рішення активно розвиваються, більшість з них орієнтована на системи з більшими ресурсами (edge-обчислення, промислові контролери), а отже потребує адаптації для енергообмежених IoT-вузлів.

Важливою складовою сучасних досліджень є також методології тестування та fault-injection. Дослідники відзначають недостатність єдиних стандартів для порівняння механізмів виявлення зависань, а також низьку повторюваність експериментів через різницю в апаратних платформах. Наявні методики не завжди враховують специфіку реального середовища експлуатації IoT-пристроїв, таких як нестабільна напруга живлення, переривання комунікацій або тимчасові перевантаження задач.

У роботі A Roadmap Towards Resilient Internet of Things for Cyber-Physical Systems (Ratasich et al., 2018) представлено огляд сучасного стану досліджень у сфері залежності (dependability), tolerance до відмов, anomaly detection та self-healing для IoT / cyber-physical systems (CPS). Автори виокремлюють ключові виклики - гетерогенність систем, масштабованість, динамічність середовища, потребу в неінтрузивних методах моніторингу і відновлення.

У роботі Adaptive Fault Detection exploiting Redundancy with Uncertainties in Space and Time (Ratasich, Platzer, Grosu, Bartocci, 2019) запропоновано підхід до адаптивного fault-детектування із використанням надлишковості (redundancy) та моделей, які враховують невизначеність у просторі й часі. Цей підхід демонструє, як можна реалізувати раннє виявлення помилок у системах з асинхронними та багаточасовими сигналами.

В дослідженні IoTRepair: Systematically Addressing Device Faults in Commodity IoT (Norris, Celik, McDaniel та ін., 2020) представлена система для автоматичного оброблення помилок (fault handling) на боці IoT-пристроїв. IoTRepair містить модуль ідентифікації дефектів, бібліотеку функцій для обробки різних типів fault'ів та handler, що дозволяє автономно реагу-

вати на помилки. У результаті автори зменшили кількість невірних станів пристроїв майже на 50% [8].

У роботі Industrial Internet of Things embedded devices fault detection and classification. A case study (2023) показано підхід для детектування та класифікації типових для промислових IoT-пристроїв fault'ів, з використанням машинного навчання на базі характеристик енергоспоживання, навантаження процесора та основного додатку. Це демонструє, що навіть на embed-системах можна застосовувати data-driven методи для моніторингу стану пристрою.

В огляді Real-time anomaly detection in distributed IoT systems: a comprehensive review and comparative analysis (Pustelnyk & Levus, 2025) систематизовано сучасні методи виявлення аномалій у розподілених IoT-системах: від статистичних і класичних підходів до моделей машинного й глибокого навчання. Авторами виділено ключові критерії ефективності: точність, latency, обчислювальна ефективність, можливість роботи в реальному часі — й підкреслено, що для ресурсно-обмежених пристроїв існує потреба в легковагих, адаптивних і гібридних моделях.

Публікація Techniques in reliability of internet of things (IoT) (2025) узагальнює сучасні підходи до підвищення reliability IoT-систем: fault tolerance, надійні комунікаційні протоколи, цілісність даних, прогностичне обслуговування (predictive maintenance), енергоефективність та тестування. Ця праця показує, що надійність IoT - багатогранна задача, яка потребує комплексних рішень [9].

Також варто відзначити публікацію Intelligent Fault Detection and Self-Healing Mechanisms in Wireless Sensor Networks Using Machine Learning and Flying Fox Optimization (2025), де на прикладі бездротових сенсорних мереж (WSN) показано, що ML-модель (Light Gradient Boosting Machine) для fault detection та алгоритм оптимізації стратегій відновлення (Flying Fox Optimization) дозволяє досягти ~94.6 % точності і високої стійкості мережі після відновлення. Це демонструє практичну спроможність підходів self-healing навіть в умовах обмежених ресурсів [11].

Узагальнення робіт демонструє, що, попри широкий спектр запропонованих рішень, залишається низка невирішених аспектів, які потребують подальшого дослідження. Серед них - відсутність чіткої класифікації типів зависань і пов'язаних із ними механізмів відновлення, недостатній розвиток легковагих алгоритмів прогнозування збоїв, придатних для ресурсно-обмежених мікроконтролерів, відсутність інтегрованих гібридних підходів, які поєднують переваги апаратних і програмних засобів, а також брак уніфікованих критеріїв і процедур тестування ефективності таких систем у реальних сценаріях [10].

Отже, аналіз наукових та прикладних досліджень свідчить про те, що проблема підвищення надійності IoT-вузлів, зокрема шляхом розроблення ефективних механізмів виявлення та запобігання зависанню, залишається актуальною та містить низку аспектів, які потребують подальшого розвитку. Це визначає доцільність і наукову значущість дослідження, присвяченого створенню комплексного підходу до раннього виявлення відхилень, попередження зависань та забезпечення самовідновлення вбудованих IoT-систем.

Метою статті є розроблення та обґрунтування ефективних підходів до підвищення надійності IoT-вузлів шляхом створення та дослідження механізмів виявлення та діагностики зависань програмно-апаратних компонентів у реальному часі. Для досягнення цієї мети поставлено наступні завдання:

- проаналізувати наявні рішення і визначити їх обмеження в умовах ресурсно-обмежених IoT-платформ;
- розробити модель або архітектуру системи контролю стану IoT-вузлів;
- запропонувати метод раннього виявлення зависань та некоректних режимів роботи.

Виклад основного матеріалу дослідження.

Аналіз наявних рішень та їх обмежень у контексті ресурсно-обмежених IoT-платформ

Сучасні підходи до підвищення надійності IoT-вузлів переважно базуються на трьох групах механізмів:

1) апаратні засоби контролю і відновлення,

2) програмні механізми моніторингу стану,

3) інтелектуальні методи прогнозування та виявлення збоїв.

Попри значний прогрес у цій галузі, кожна група рішень має істотні обмеження, які проявляються особливо гостро в умовах обмеженої пам'яті, енергоспоживання та обчислювальних ресурсів IoT-платформ.

1. Апаратні механізми контролю (Watchdog, Brown-Out Reset, Hardware Recovery)

Наявні рішення:

- класичні watchdog-таймери (independent, windowed);
- brown-out detection (виявлення падіння напруги живлення);
- апаратні схеми автоматичного перезапуску (reset controllers).

Обмеження:

- Неможливість розрізнити типи відмов. Watchdog фіксує лише факт зависання, але не діагностує його походження - помилку ПЗ, взаємне блокування, збій периферії, деградацію сенсорів тощо.

- Надмірність реакції. Однотипне «жорстке перезавантаження» не підходить для критичних IoT-вузлів, де важливо зберегти дані або уникнути довгого відновлення.
- Не враховується складність сучасних IoT-стеків. На MCU із кількома потоками, RTOS, чергами та обробниками апаратних переривань простий watchdog стає недостатнім.
- Обмежена конфігурованість. Недостатньо гнучкі схеми таймінгу для адаптації до різних режимів навантаження.

2. Програмні механізми моніторингу стану (RTOS health monitor, task supervisor, heartbeat-сигнали)

Наявні рішення:

- моніторинг задач у RTOS (FreeRTOS Task Watchdog, Zephyr Health Monitoring);
- періодичні heartbeat-сигнали між компонентами;
- контроль черг, стеків, heap-фрагментації;
- механізми exception-handling і перехоплення критичних помилок.

Обмеження:

- Високе навантаження на CPU та RAM. Навіть прості супервізори можуть займати десятки кілобайт пам'яті, що є критичним для MCU з 64–256 КБ RAM.
- Уразливість до самих зависань. Програмні монітори не працюють коректно, якщо зависає планувальник або RTOS.
- Неповна спостережність. Моніторинг не охоплює низькорівневі апаратні збої: некоректну роботу сенсорів, I^2C-deadlock, UART-переповнення, «залипання» шин SPI.
- Складність конфігурації. Потрібно вручну визначати пороги, інтервали, критичні події — це знижує універсальність.
- Відсутність адаптивності. Фіксовані пороги не працюють при зміні навантаження або енергорежиму (наприклад, перехід у sleep).

3. Інтелектуальні методи (ML-класифікація, anomaly detection, predictive maintenance)

Наявні рішення:

- нейронні мережі для виявлення аномалій у поведінці вузлів;
- машинне навчання на основі метрик (CPU load, memory pattern, енергоспоживання);
- edge-AI-підходи для раннього прогнозування збоїв;
- моделі self-healing на базі статистики або lightweight ML.

Обмеження:

- Високі вимоги до ресурсів.

- Навіть оптимізовані моделі TinyML потребують:
  - 10–100 КБ пам'яті для моделі,
  - прискорених обчислень (FPU, DSP),
  - стабільного енергоживлення.
- Потреба у навчальних даних. Для відмов у IoT-вузлах часто бракує якісних датасетів, особливо залежних від конкретної апаратної конфігурації.
- Ризик хибних спрацьовувань. Моделі погано адаптуються до змін навколишнього середовища (температура, вологість, деградація сенсорів).
- Складність інтеграції. Потрібні додаткові фреймворки, оптимізаційні інструменти (TensorFlow Lite Micro), що збільшує footprint.

4. Хмарні та мережеві підходи (Cloud analytics, remote device management)

Наявні рішення:

- аналітика збоїв у хмарі;
- контроль працездатності через IoT-платформи (AWS IoT, Azure IoT, ThingsBoard);
- віддалене оновлення ПЗ (OTA);
- telemetry monitoring.

Обмеження:

- Залежність від підключення. Під час втрати зв'язку вузол залишається без механізмів детекції/самовідновлення.
- Затримки. Аналіз у хмарі не підходить для реального часу при критичних зависаннях.
- Підвищене енергоспоживання. Постійна телеметрія значно скорочує строк автономної роботи IoT-пристроїв.

5. Системні обмеження IoT-платформ

У контексті IoT особливо проявляються такі фундаментальні обмеження:

- обмежений обсяг пам'яті та слабкі CPU → унеможливлюють використання «важких» моделей чи складної телеметрії;
- енергообмеження (акумулятори, energy harvesting) → не допускають часті діагностичні цикли;
- гетерогенність апаратних платформ → ускладнює універсальні рішення;
- нестабільність середовища експлуатації → виникають збої, не характерні для традиційних комп'ютерних систем;
- відсутність локального оператора → більшість вузлів працюють без фізичного доступу.

Отже, наявні рішення можуть виявляти частину збоїв або забезпечувати базове відновлення, однак вони залишають критичну прогалину між простою реакцією (watchdog reset) та інтелектуальною діагностикою.

Це робить актуальним розроблення легковагових універсальних механізмів виявлення та запобігання зависанню, які: працюють на ресурсно-обмежених MCU, не потребують великих обчислень, здатні діагностувати різні типи збоїв, забезпечують адаптивні режими контролю, мінімізують втрати даних і простої системи.

Модель системи контролю стану IoT-вузлів

1. Архітектурні принципи

Архітектура базується на наступних принципах:

Модульність – кожен вузол складається з кількох незалежних модулів: датчиків, актуаторів, RTOS-завдань і комунікаційного модуля.

Мінімізація ресурсів – використовуються легковагі методи моніторингу та обробки даних для MCU з 32–256 КБ RAM і обмеженою флеш-пам'яттю.

Прогностичний контроль – поєднуються класичні watchdog-таймери та спрощені моделі ML/TinyML для раннього виявлення відхилень.

Self-healing / recovery – система здатна ізолювати проблемний модуль, здійснити локальне перезавантаження або перевести вузол у безпечний режим до відновлення.

Адаптивність – підстроювання порогів та частоти перевірок під енергетичний стан і поточне навантаження.

2. Структурні компоненти системи

A. Модуль спостереження (Monitoring Module)

Функції: збір телеметрії, контроль стану RTOS-завдань, стеків, черг, пам'яті, периферії.

Методи: heartbeat-сигнали, періодичні тайм-слоти перевірки, watchdog-перевірка критичних підсистем.

Особливість: низьке енергоспоживання, мінімальні накладні витрати CPU.

B. Модуль аналізу стану (State Analysis Module)

Функції: виявлення аномалій і потенційних hang-сценаріїв.

Методи: прості статистичні пороги (CPU load, memory usage, stack depth); легковагі ML-моделі (TinyML) для прогнозування зависань; обробка подій з апаратних датчиків (brown-out, temperature, voltage).

Особливість: адаптивне налаштування порогів, комбінування програмних і апаратних сигналів.

C. Модуль прийняття рішень (Decision & Recovery Module)

Функції: визначення типу відмови і вибір стратегії відновлення.

Стратегії: локальний reset окремого модуля; перехід вузла у безпечний режим (safe-mode) до стабілізації стану; збереження критичних даних перед перезавантаженням.

Особливість: мінімізація downtime, підтримка критичних функцій навіть під час відновлення.

D. Модуль комунікації (Communication Module)

Функції: передача статусу вузла, помилок та відновлених станів на центральний сервер або edge-нод.

Особливість: оптимізація трафіку, передача лише критичних подій (event-driven), підтримка low-power протоколів (MQTT-SN, CoAP).

3. Принципи взаємодії модулів

Збір даних: Monitoring Module регулярно збирає ключові параметри системи.

Обробка та прогнозування: State Analysis Module перевіряє параметри на відхилення та можливі hang-сценарії.

Прийняття рішення: Decision & Recovery Module визначає необхідність дії (перезапуск, safe-mode, повідомлення).

Комунікація: Communication Module інформує edge/сервер про статус вузла та виконані відновлювальні дії.

Адаптація: Після виконання recovery система оновлює пороги та частоту перевірок з урахуванням останніх станів.

4. Особливості для ресурсно-обмежених IoT

Легка інтеграція TinyML / статистичних моделей без додаткових обчислювальних блоків.

Event-driven архітектура: активність компонентів лише при аномаліях або критичних подіях.

Мінімізація пам'яті: зберігаються лише критичні телеметричні дані, історія станів стискається або агрегується.

Енергозбереження: динамічне налаштування частоти перевірок залежно від батарейного стану.

Метод раннього виявлення зависань та некоректних режимів IoT-вузлів

Метою запропонованого методу є - вчасно виявляти збої у роботі IoT-вузлів (зависання, некоректні режими, збої сенсорів) для зменшення простоїв та забезпечення безперервного функціонування мережі при мінімальному енергоспоживанні.

Основні принципи

- Локальний моніторинг: вузол самостійно оцінює свій стан без надмірного навантаження.

- Виявлення аномалій у режимі реального часу: аналізуються частота виконання задач, стан сенсорів, використання ресурсів.
- Мінімізація комунікацій: вузол передає лише сигнал тривоги або стислу телеметрію.
- Модульність: метод легко інтегрується з існуючою прошивкою та архітектурою мережі.

Компоненти методу:

1 Watchdog + Heartbeat

Watchdog timer: апаратний або програмний таймер перезавантажує вузол при зависанні.

Heartbeat-сигнал: вузол періодично надсилає короткий пакет статусу (наприклад, кожні 1–5 хвилин).

Аналіз центром: якщо heartbeat не отримано протягом N інтервалів → вузол позначається як «підозрілий».

2 Локальний аналіз ресурсів

CPU та пам'ять: контроль перевантаження (наприклад, використання > 90% протягом 1 хвилини).

Стан сенсорів: перевірка аномальних або відсутніх показників.

Внутрішні таймери/процеси: перевірка регулярності виконання ключових функцій.

3 Використання легких алгоритмів аномалій

Порогові методи: перевищення очікуваних меж.

Ковзаючі середні та зміни тенденцій: виявлення раптових відхилень.

Прості евристики: наприклад, якщо вузол не змінив стан керованого пристрою протягом X циклів – сигнал тривоги.

4 Телеметрія та логування

Стисла телеметрія: CPU, пам'ять, напруга живлення, стан сенсорів.

Події аномалій: лог зберігається локально для відновлення та надсилається при доступності мережі.

5 Автоматичне реагування

Локальна перезагрузка: у разі критичної аномалії.

Режим збереження енергії: при частих збоях для зменшення пошкоджень.

Сповіщення центру контролю: про стан вузла для планування технічного втручання.

Отже, перевагами запропонованого методу є наступні:

- Виявлення зависань ще до повного виходу вузла з ладу.
- Мінімальні витрати енергії та мережевих ресурсів.
- Можливість адаптації для різних типів вузлів та сенсорів.
- Простота інтеграції у прошивки IoT-пристроїв.

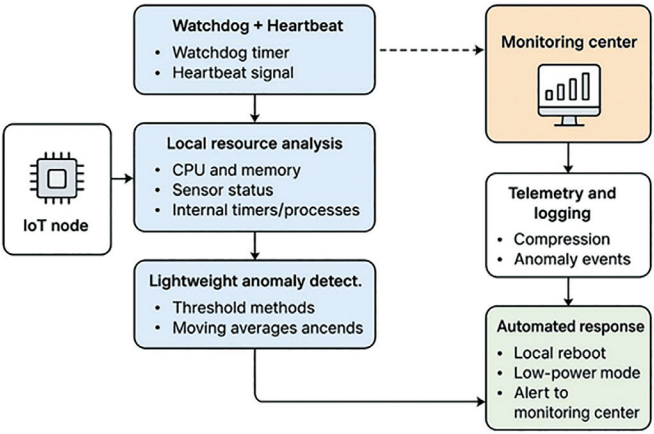

Рис. 1. Структурна схема роботи методу

Висновки та пропозиції. У ході дослідження встановлено, що більшість наявних механізмів контролю працездатності IoT-вузлів не забезпечують повного виявлення різних типів зависань та не адаптовані до умов обмежених ресурсів. Запропонована архітектура контролю стану та метод раннього виявлення відхилень забезпечують підвищення надійності, скорочення простоїв і мінімізацію енергоспоживання. Поєднання апаратних засобів, легковагих алгоритмів аномалій та адаптивного моніторингу дає змогу підвищити відмовостійкість і стабільність роботи IoT-вузлів. Отримані результати підтверджують ефективність запропонованого підходу для різних типів ресурсно-обмежених пристроїв.

Пропозиції:

- використовувати комбіновану схему контролю, що поєднує watchdog, локальну діагностику та адаптивний аналіз аномалій.
- запровадити мінімалістичну телеметрію та event-driven повідомлення для економії енергії.
- інтегрувати локальні self-healing механізми та модульне перезавантаження компонентів замість повного reset.
- створити стандартизоване середовище для тестування та порівняння алгоритмів виявлення зависань.
- використовувати уніфіковані критерії оцінювання ефективності для різних IoT-платформ.
-

ЛІТЕРАТУРА/ REFERENCES

1. Alauthman, A., & Al-Hyari, A. (2025). Intelligent Fault Detection and Self-Healing Mechanisms in Wireless Sensor Networks Using Machine Learning and Flying Fox Optimization. *Computers*, 14(6), 233. DOI: 10.3390/computers14060233.

2.(2025). Implementation of edge AI for early fault detection in IoT networks: evaluation of performance and scalability in complex applications. Discover Internet of Things, Article 108.

3.El Ahmadi, S. E. A., & El Abbadi, L. (2025). A Predictive Self-Healing Model for Optimizing Production Lines: Integrating AI and IoT for Autonomous Fault Detection and Correction. *Engineering Proceedings*, 97(1), 6. DOI: 10.3390/engproc2025097006.

4.(2025). Techniques in reliability of internet of things (IoT). Procedia Computer Science, 256, 55-62. DOI: 10.1016/j.procs.2025.02.095.

5.(2025). Self-Healing Networks with AI-Based Fault Prediction in IoT Ecosystems. *International Journal of Scientific Research & Engineering Trends*, 11(2). DOI: 10.61137/ijsret.vol.11.issue2.410.

6.(2024). Industrial Internet of Things embedded devices fault detection and classification. A case study. *Internet of Things*, 25, 101042. DOI: 10.1016/j.iot.2023.101042.

7. (2024). Reliability on the Internet of Things with designing approach for exploratory analysis. *Frontiers in Computer Science*, 6 (2024). DOI: 10.3389/fcomp.2024.1382347.

8.Zaitsev Ievgen, Bondarenko Oleh, Golubenko Oleksandr, Antonenko Artem, Savchenko Andrii. Securing Applied Information Systems With SAST Integration Into the Gulp Pipeline. In: Applied Information Systems and Technologies in the Digital Society : proceedings of the 9th International Scientific and Practical Conference "Applied Information Systems and Technologies in the Digital Society" AISTDS'2025, Kyiv, Ukraine, October 1, 2025 / ed. Vitaliy Snytyuk [et al.].

9. (2025). Review and Analysis of Fault Detection in Self-Healing Hardware System. *International Journal of Analog Integrated Circuits*, 11(1), 11–15.

10. R. T. Taha, A. O. Abdullah, A. Dronach, S. K. Shnain, A. M. Khaleefah and O. Tkachenko, "The Convergence of Edge Computing and IoT-A Paradigm Shift in Data Processing," *2024 36th Conference of Open Innovations Association (FRUCT)*, Lappeenranta, Finland, 2024, pp. 787–796, doi: 10.23919/FRUCT64283.2024.10749961.

11. Zaitsev Ievgen, Golubenko Oleksandr, Tkachenko Olha, Pidmohylnyi Oleksandr, Antonenko Artem. Exploring Advanced Hypothesis Generation in Astronomy Through theImplementation of a Mathematical Model of Linguistic Neural Networks. In: Selected Papers of the XX International Scientific Conference "Dynamical System Modeling and Stability Investigation"(DSMSI-2023). Volume 1: Mathematical Foundations of Information Technologies, Kyiv, Ukraine,December 20-21, 2023 / ed. Denys Khusainov, Josef Diblik, Oleksii Bychkov [et al.]. CEUR-WS.org, 2023. Vol. 3687. P. 121–128. URL: https://ceur-ws.org/Vol-3687/.

СТАТТЯ НАДІЙШЛА ДО РЕДАКЦІЇ 01.10.2025