План лекції.

Тема 2. Класифікація та моніторинг нетипових об'єктів

- Види нетипових об'єктів моніторингу (IoT, SCADA, периферійні пристрої).
- Підходи до класифікації.
- Проблеми сумісності, протоколи та адаптація засобів моніторингу.
- Способи адаптації засобів моніторингу
- Особливості моніторингу IoT-інфраструктур
- Вимоги до безпеки моніторингу нетипових об’єктів
- Приклади застосування та кейси

У контексті системного моніторингу нетиповими об’єктами вважаються ті елементи IT-інфраструктури, які не є традиційними об’єктами моніторингу — такими як сервери, віртуальні машини, мережеві пристрої чи стандартні додатки. Натомість ці об’єкти мають специфічні апаратні або програмні характеристики, працюють у нестандартних середовищах або виконують вузькоспеціалізовані функції, які не завжди легко інтегруються у загальні моніторингові рішення.

До нетипових об’єктів належать, зокрема, пристрої Інтернету речей (IoT), елементи SCADA-систем, переносні або мобільні пристрої, вбудовані системи керування, промислові контролери, периферійне обладнання, а також системи, побудовані на нестандартних або пропрієтарних протоколах. Часто вони не мають підтримки звичних для адміністраторів засобів моніторингу, не можуть використовувати SNMP або agent-based рішення, або взагалі не мають операційної системи в класичному розумінні.

Головна відмінність таких об’єктів від звичних — обмеження у доступі, нестача стандартних інтерфейсів, слабка або нестабільна телеметрія, а також фізична розподіленість, енергетична автономність або мобільність. На практиці це означає, що моніторинг нетипових об'єктів потребує спеціальних підходів, адаптації протоколів, додаткового програмного шару, або навіть окремих шлюзів між ними та центральною системою моніторингу.

Водночас, роль таких об’єктів у сучасних критичних IT-інфраструктурах стрімко зростає. Наприклад, сенсори температури та вологості в агросекторі можуть безпосередньо впливати на прийняття рішень у режимі реального часу, а збій у роботі контролера у SCADA-системі водопостачання може призвести до зупинки цілого району. Таким чином, ефективний моніторинг нетипових об’єктів є не просто бажаним, а обов’язковим компонентом для підтримки стабільності, надійності та безпеки критичних операцій.

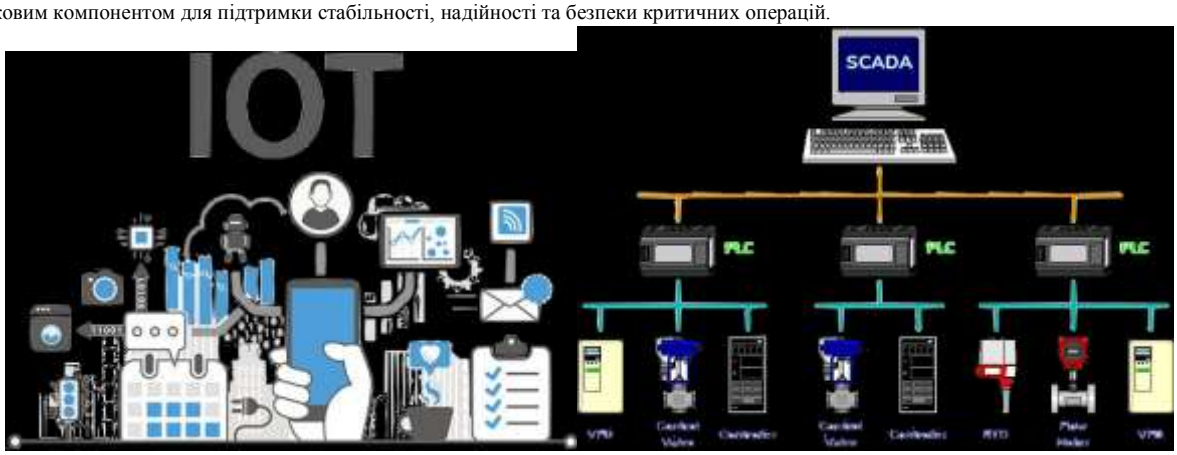

Рис.02.01.

Види нетипових об'єктів моніторингу (IoT, SCADA, периферійні пристрої).

Сучасні IT-системи дедалі частіше виходять за межі традиційних серверних та мережевих об’єктів, охоплюючи широкий спектр пристроїв, які складно вписати у звичну архітектуру моніторингу. Ці об’єкти часто мають нестандартні характеристики, не підтримують типові протоколи або працюють у специфічних умовах, тому їх обслуговування та нагляд потребують окремого підходу. Розглянемо основні категорії таких нетипових об’єктів:

IoT-пристрої (сенсори, камери, лічильники тощо)

Інтернет Речей (Internet of Things, IoT) — це концепція глобальної мережі фізичних об’єктів, які здатні збирати, передавати та обробляти дані завдяки підключенню до Інтернету. У цьому середовищі “речами” можуть бути як побутові прилади, так і промислові системи — від звичайного розумного термостата до складного комплексу контролю виробничих процесів або екологічного моніторингу. Ключовою особливістю IoT є автономність пристроїв, що дозволяє їм взаємодіяти між собою, з іншими системами та із зовнішніми службами без прямої участі людини.

У сучасних умовах, коли IT-інфраструктури виходять за межі центрів обробки даних, IoT-пристрої формують один із наймасштабніших і найдинамічніших класів нетипових об’єктів моніторингу. Їхнє широке впровадження — як у споживчому, так і в промисловому сегменті — створює нові виклики для системного адміністрування, кібербезпеки, моніторингу у реальному часі та управління інцидентами.

Архітектура IoT-систем

Типова IoT-екосистема складається з кількох рівнів:

- ✓ **Пристрої-збирачі даних** — сенсори, контролери, лічильники, камери, які фіксують параметри навколишнього середовища (температуру, тиск, рух, освітлення тощо).
- ✓ **Комунікаційний рівень** — модулі зв’язку, які забезпечують передачу зібраної інформації (через Wi-Fi, LTE, Zigbee, LoRa, NB-IoT, Bluetooth, 5G та інші).
- ✓ **Шлюзи (gateways)** — пристрої, що приймають дані від десятків або сотень сенсорів, агрегують їх і передають на обчислювальні потужності.
- ✓ **Платформи збору й обробки** — хмарні або локальні сервіси, які зберігають, аналізують та візуалізують телеметрію.
- ✓ **Керуючі модулі** — системи, що можуть автоматично надсилати команди назад до пристроїв (наприклад, увімкнення вентиляції чи тривожного сигналу).

Для нормального функціонування така система повинна відповідати кільком технічним і організаційним умовам — надійне з'єднання, енергоефективність, узгодженість форматів даних, безпечний доступ та низька затримка.

Інтернет Речей відрізняється різноманіттям протоколів, кожен із яких має свою нішу.

Протоколи обміну даними: від LoRa до MQTT

- **LoRaWAN як основа енергоефективного моніторингу IoT-інфраструктур**

Зі стрімким розвитком Інтернету речей (IoT) зростає потреба в мережах, які можуть забезпечити далекодіючий зв'язок між пристроями за мінімального енергоспоживання. Багато сценаріїв використання IoT передбачають встановлення датчиків або пристроїв у важкодоступних, віддалених чи розподілених локаціях — наприклад, на сільськогосподарських угіддях, у лісах, на промислових майданчиках або в транспортних системах. Часто такі пристрої працюють автономно протягом років на одному заряді батареї, передаючи невеликі об'єми даних з певною періодичністю. Саме під такі задачі створено клас технологій, відомий як LPWAN (Low Power Wide Area Network) — мережі з низьким енергоспоживанням і великим радіусом дії.

Однією з провідних технологій цього класу є LoRaWAN. Вона базується на двох компонентах: LoRa — фізичному рівні (радіомодуляція, що забезпечує далекодіючий бездротовий зв'язок) та LoRaWAN — протоколі зв'язку і системній архітектурі, яка відповідає за взаємодію пристроїв у мережі, їх безпеку, маршрутизацію та масштабування.

- ✓ **Архітектура мережі LoRaWAN.** На відміну від поширених mesh-мереж, у яких вузли передають повідомлення один через одного (що навантажує пристрої і знижує строк служби батареї), LoRaWAN використовує архітектуру типу "зірка" (star topology). У цій моделі кінцеві пристрої не зв'язуються з якимось конкретним шлюзом, а передають повідомлення у радіоефір, які можуть бути прийняті кількома шлюзами одночасно.

  Далі шлюзи (gateways) передають дані на мережевий сервер, який:
  - ❖ відкидає дублікати;
  - ❖ здійснює перевірку автентичності та безпеки;
  - ❖ визначає оптимальний маршрут підтвердження;
  - ❖ адаптує параметри передачі — зокрема швидкість передачі (Data Rate) залежно від умов зв'язку.

  Завдяки цьому пристрої можуть вільно переміщатися, а хендовер між зонами покриття шлюзів відбувається без розриву зв'язку, що робить LoRaWAN зручним для моніторингу мобільних об'єктів (наприклад, транспорту чи логістичних одиниць).

Рис.02.02

- ✓ **Енергозбереження та "ALOHA-подібний" доступ.** Ще однією визначальною перевагою LoRaWAN є асинхронна модель обміну. Вузли "прокидаються" лише тоді, коли мають дані до передачі, або відповідно до запрограмованого графіка. Цей підхід, відомий як ALOHA-модель доступу, дозволяє мінімізувати час активності радіомодуля, що критично важливо для продовження терміну автономної роботи пристроїв.

  У порівняльному дослідженні, проведеному GSMA, LoRaWAN показала на 3–5 разів вищу ефективність енергоспоживання, ніж інші LPWAN-технології, зокрема NB-IoT, SIGFOX, Weightless-P тощо.
- ✓ **Мережна ємність і масштабованість.** Для підтримки великої кількості вузлів у мережі LoRaWAN застосовується комбінація таких технологій:
  - ❖ **мультиканальний багатомодемний прийом** — шлюзи можуть одночасно обробляти кілька сигналів із різними параметрами;
  - ❖ **адаптивна швидкість передачі (ADR)** — пристрої автоматично налаштовують параметри передачі (наприклад, знижують час перебування в ефірі) залежно від відстані до шлюзу;
  - ❖ **паралельна обробка повідомлень із різними коефіцієнтами розширення (spreading factors)** — завдяки ортогональності сигналів навіть при однаковій частоті декілька пристроїв можуть "говорити" одночасно.

  Ці можливості дозволяють мережі LoRaWAN бути надзвичайно масштабованою. За потреби — шляхом додавання шлюзів — можна в 6–8 разів збільшити пропускну здатність без змін у пристроях-клієнтах.
- ✓ **Класи пристроїв: баланс між енергоефективністю та доступністю.** Для оптимізації під різні сценарії використання LoRaWAN підтримує три класи пристроїв:
  - ❖ **Клас A: мінімальне енергоспоживання**. Пристрої передають дані і лише тоді відкривають короткі "вікна" для прийому. Ідеально для моніторингових сценаріїв, де затримка у відповіді не є критичною.
  - ❖ **Клас B:** пристрої мають заплановані часові вікна для прийому, синхронізуються за маяками від шлюзів. Компроміс між автономністю і часом реакції.
  - ❖ **Клас C: майже постійне прослуховування ефіру.** Максимальна доступність, але найвище енергоспоживання. Використовується, коли критично важливо швидко доставити керуючу команду (наприклад, в системах управління аварійними ситуаціями).
- ✓ **Безпека: багаторівневий підхід.** Для забезпечення захисту даних LoRaWAN впроваджує два рівні безпеки:

- ❖ Мережева безпека: автентифікація пристроїв при підключенні до мережі;
- ❖ Прикладна безпека: шифрування даних від сенсора до сервісу кінцевого користувача.

Обидва рівні базуються на стандартах AES із 128-бітним ключем. При цьому навіть оператор мережі не має доступу до корисних даних, якщо він не є власником додатку.

LoRaWAN є провідною LPWAN-технологією, яка поєднує:

- далекодіючу радіопередачу;
- ультранизьке енергоспоживання;
- гнучку архітектуру "зірка";
- високу масштабованість;
- адаптивну передачу даних;
- розвинену модель безпеки.

Ці характеристики роблять LoRaWAN універсальним вибором для моніторингу розподілених, мобільних, або автономних об'єктів, зокрема в агросекторі, логістиці, екологічному контролі, міському середовищі, енергетиці тощо. У контексті системного моніторингу IoT це одна з ключових технологій, які дозволяють забезпечити якісний зворотний зв'язок від нетипових об'єктів без складної інфраструктури або витрат на живлення.

- **MQTT (Message Queuing Telemetry Transport)** як інфраструктурна основа обміну повідомленнями в IoT-середовищах

У контексті моніторингу нетипових об'єктів, зокрема IoT-пристроїв, важливу роль відіграє не лише фізичний рівень (зокрема LoRa, Wi-Fi, ZigBee чи LTE), але й прикладні протоколи, які забезпечують ефективну, стабільну і масштабовану доставку телеметричних даних. Одним із найпоширеніших таких протоколів є MQTT (Message Queuing Telemetry Transport) — компактний, легкий та орієнтований на публікацію/підписку транспортний механізм обміну повідомленнями через посередника.

Попри те, що MQTT часто асоціюють із Інтернетом речей, сам протокол був створений ще у 1999 році Арленом Ніппе та Енді Стенфорд-Клерком як засіб передавання телеметричних даних через супутникові канали для нафтогазової промисловості. Наразі протокол активно використовується не лише в IoT-інфраструктурах, а й у мобільних додатках (наприклад, Facebook використовує MQTT для реалізації чату у своєму мобільному застосунку), у системах автоматизації, у транспортних платформах, а також у сфері охорони здоров'я.

- ✓ **Архітектура та принцип роботи.** MQTT працює поверх TCP/IP, що забезпечує надійність передачі, однак головною архітектурною особливістю протоколу є модель публікації/підписки (publish/subscribe) з використанням MQTT-брокера — спеціального посередника, що приймає повідомлення від видавців (publishers) і доставляє їх підписникам (subscribers) відповідно до тем (topics).

  Такий підхід дає змогу:

  - ❖ роз'єднати логіку відправника й отримувача повідомлень у просторі та часі;
  - ❖ підтримувати гнучку маршрутизацію повідомлень;
  - ❖ зменшувати навантаження на мережу завдяки одноразовому з'єднанню з брокером, яке дозволяє отримувати повідомлення з кількох каналів;
  - ❖ працювати з мінімальним обсягом даних навіть у вузькосмугових мережах (наприклад, у сільській місцевості, в транспорті або на промислових об'єктах).

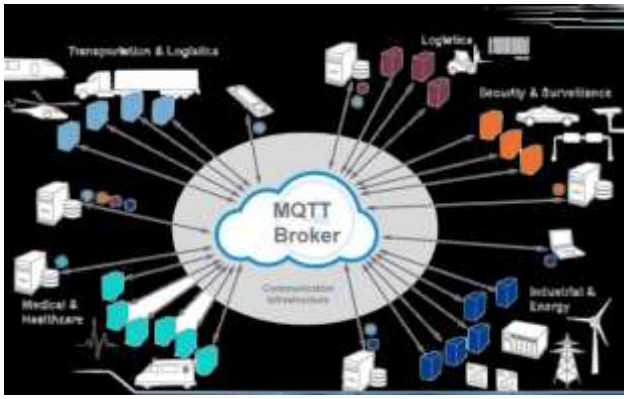

Рис.02.03

Наприклад, у сфері охорони здоров'я MQTT дозволяє лікарям у режимі реального часу отримувати дані з медичних сенсорів, встановлених на пацієнтах, які можуть перебувати на значній відстані. У транспорті — це може бути телеметрія з бортових систем транспортних засобів; у розумних будинках — передача даних від сенсорів температури, руху або вологи.

- ✓ **Технічні переваги та особливості.** MQTT спроектовано як надзвичайно легкий протокол, що забезпечує мінімальне навантаження на мережу. Це досягається завдяки:
  - ❖ невеликому розміру бінарних пакетів (мінімальний заголовок MQTT становить усього 2 байти);
  - ❖ відсутності надлишкових метаданих у повідомленнях;
  - ❖ підтримці push-механізму — передавання даних лише тоді, коли це необхідно, без опитування пристроїв;
  - ❖ можливості мультиплексування — тобто підписки на кілька тем через одне з'єднання.
- ✓ **MQTT реалізує три рівні надійності доставки повідомлень:**
  - ❖ QoS 0 (at most once) — повідомлення доставляється максимум один раз, без підтвердження;
  - ❖ QoS 1 (at least once) — доставляється принаймні один раз (з підтвердженням);
  - ❖ QoS 2 (exactly once) — гарантується унікальна доставка, застосовується у критичних сценаріях, хоч і з підвищеним трафіком.

Також варто зазначити, що MQTT не є закритим або пропрієтарним протоколом. У 2013 році він був відкритий для спільноти та переданий під управління організації OASIS, що сприяло появі великої кількості відкритих реалізацій (наприклад, Mosquitto, EMQX, HiveMQ) та розширило його популярність серед розробників IoT-рішень.

- ✓ **Застосування MQTT в IoT-моніторингу.** У системному моніторингу нетипових об'єктів MQTT може використовуватись як:
  - ❖ універсальний транспортний механізм для збору телеметрії;
  - ❖ інтерфейс підключення до SCADA-систем або хмарних аналітичних платформ;
  - ❖ інфраструктура обміну повідомленнями між вбудованими пристроями;
  - ❖ канал сповіщень і тригерів, який працює у реальному часі;
  - ❖ основа для розгортання адаптивного моніторингу з можливістю віддалено змінювати конфігурацію сенсорів або запускати сценарії реагування.

MQTT — надлегкий протокол передачі повідомлень через TCP/IP, який, хоча й не є спеціалізованим "протоколом Інтернету речей", став де-факто стандартом у сфері IoT-комунікацій. Його популярність зумовлена низькими накладними витратами, енергоефективністю, стабільною роботою навіть при нестабільних або обмежених каналах зв'язку, а також підтримкою гнучкої архітектури pub-sub. Завдяки цим перевагам MQTT є виправданим і рекомендованим вибором для моніторингових систем із сенсорами, мобільними вузлами чи пристроями SCADA-класу, де критичними є швидкість реагування, масштабованість і компактність даних.

Окрім MQTT, в екосистемі Інтернету речей активно застосовуються й інші протоколи, які відіграють важливу роль у зборі, обміні й маршрутизації даних між пристроями та інфраструктурними елементами. Їх використання залежить від вимог до енергоефективності, надійності, пропускної здатності, топології мережі й масштабованості. Нижче подано огляд ключових протоколів, які мають значення для побудови ефективних систем моніторингу нетипових об'єктів.

- **CoAP, AMQP, XMPP, NB-IoT** — використовуються в залежності від вимог до ресурсоємності, безпеки, частоти передачі, затримок та обмежень пристрою.
  - **CoAP (Constrained Application Protocol)** — це протокол прикладного рівня, спеціально розроблений для комунікації між обмеженими вузлами у вузькосмугових мережах, де ресурси (оперативна пам'ять, потужність процесора, пропускна здатність) є обмеженими. CoAP розроблено групою IETF CoRE (Constrained RESTful Environments) як спрощену альтернативу HTTP, що дозволяє зберегти логіку REST-комунікації (ресурсний підхід, URL-адресація, методи GET, POST, PUT, DELETE), але працює поверх UDP, що знижує накладні витрати на з'єднання.
    Його надзвичайно компактна структура — заголовок CoAP має лише 4 байти — дозволяє ефективно використовувати його в сенсорних мережах, зокрема для передачі даних із лічильників, датчиків вологості, температури, руху, тощо. CoAP також підтримує обсервацію ресурсів (сповіщення про зміни без потреби опитування) та можливість перетворення запитів на HTTP у шлюзі, що робить його зручним для інтеграції з веб-сервісами.

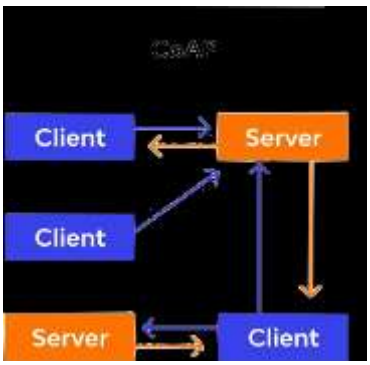

Рис.02.04.

  - **AMQP (Advanced Message Queuing Protocol)** — це надійний, стандартизований, відкритий протокол черг повідомлень, який використовується для асинхронної комунікації між різними компонентами розподілених систем. Як і MQTT, AMQP реалізує модель "publisher-subscriber" через брокера повідомлень, однак він є більш функціонально насиченим, підтримує транзакції, черги з пріоритетами, маршрутизацію повідомлень, що робить його придатним для складних бізнес-додатків і високонавантажених IoT-платформ.
    Протокол підтримується організацією OASIS та має сертифікацію ISO/IEC, що підтверджує його відповідність промисловим вимогам. Завдяки гнучкості, високій безпеці, стандартності та сумісності, AMQP може застосовуватися для відправки великих обсягів телеметрії, взаємодії з аналітичними сервісами або хмарними платформами, де потрібна гарантія доставки та контроль черг.

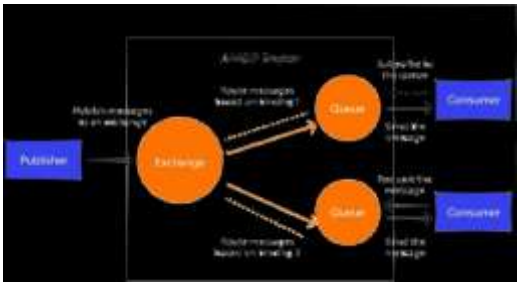
Рис.02.05.

    Хоча AMQP вимагає більшої обчислювальної потужності (що може бути недоцільно для пристроїв з обмеженими ресурсами), він ефективний у промислових, енергетичних або логістичних системах, де потрібна інтеграція з ERP, MES або SCADA.
  - **XMPP (Extensible Messaging and Presence Protocol)** — протокол з відкритим кодом, побудований на базі XML і першопочатково призначений для миттєвого обміну повідомленнями, голосових/відеодзвінків і сповіщень про присутність. Його децентралізована архітектура схожа на email-систему — будь-хто може розгорнути XMPP-сервер, що робить протокол гнучким, автономним і масштабованим. У контексті IoT, XMPP дозволяє реалізувати:
    - ✓ машинно-машинну (M2M) комунікацію без залучення людини;
    - ✓ обмін структурованими даними в реальному часі;
    - ✓ розширення функціоналу через плагіни, що дозволяє адаптувати протокол до специфіки прикладної галузі.

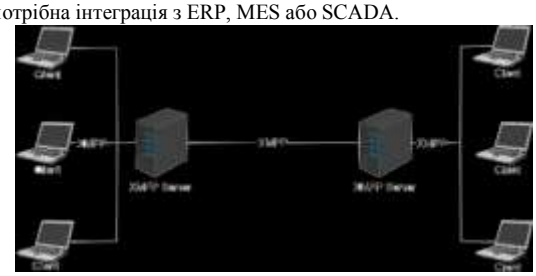
Рис.02.06.

    Приклади застосування XMPP в IoT:
    - ✓ Google Cloud Print (управління друком через хмару);
    - ✓ Logitech Harmony Hub (інтеграція з домашніми мультимедійними системами);
    - ✓ інфраструктура розумного дому, яка вимагає дво- або багатостороннього зв'язку.

    XMPP забезпечує високий рівень безпеки (TLS, SASL), але може бути надмірно важким для ультраобмежених пристроїв. Проте для вузлів середнього рівня (хаби, контролери, шлюзи) XMPP — ефективне рішення для управління та комунікації.
  - **NB-IoT (Narrowband Internet of Things)** — це стільниковий стандарт зв'язку, розроблений 3GPP для пристроїв, які передають невеликі обсяги даних на великі відстані з мінімальним енергоспоживанням. Це одна з трьох основних LPWAN-технологій для стільникових мереж, поряд із eMTC і EC-GSM-IoT. Ключові характеристики NB-IoT:
    - ✓ Масштабованість: тисячі підключень до однієї базової станції;
    - ✓ Енергоефективність: автономна робота пристрою до 10 років від однієї батареї;
    - ✓ Висока проникність сигналу (наприклад, у підвалах, через бетонні перекриття);
    - ✓ Можливість розгортання поверх існуючих GSM / LTE-мереж або окремо;
    - ✓ Низька вартість модулів і підтримка eSIM/Remote SIM Provisioning (RSP), що спрощує масштабні розгортання.

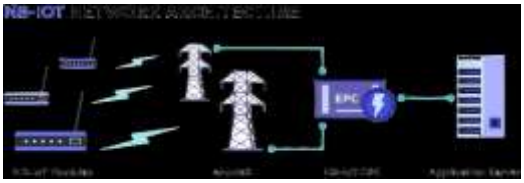

Рис.02.07.

NB-IoT ідеально підходить для медичних сенсорів, лічильників, систем розумного дому, а також інфраструктури розумних міст (смарт-паркінги, освітлення, моніторинг стану доріг тощо). Компанії як Vodafone, Huawei, u-Blox уже впровадили перші промислові рішення на базі NB-IoT, і очікується його подальше масове розгортання в найближчі роки.

Узагальнюючи, вибір протоколу для IoT-моніторингу нетипових об'єктів має бути зумовлений такими чинниками, як: тип і обчислювальні можливості пристрою, частота передачі даних, необхідна гарантія доставки, топологія мережі, вимоги до енергоспоживання, сумісність із хмарними платформами та засобами безпеки. MQTT, CoAP, AMQP, XMPP, а також NB-IoT формують гнучку палітру рішень для побудови надійної, масштабованої та економічно ефективної системи моніторингу.

Специфіка моніторингу IoT-пристроїв

У системному моніторингу IoT-пристрої вважаються нетиповими об'єктами, оскільки часто:

- мають обмежені ресурси (ЦП, пам'ять, енергоживлення);
- працюють на власних ОС або мікроконтролерах без підтримки SNMP чи агентів;
- змінюють місцезнаходження або мережу доступу;
- не гарантують постійний зв'язок, тобто є «іноді онлайн»;
- передають дані за нестандартними інтервалами.

Тому традиційні засоби моніторингу (Nagios, Zabbix, Prometheus) не завжди можуть бути безпосередньо застосовані. Для їх обслуговування використовуються спеціалізовані IoT-платформи (ThingsBoard, AWS IoT, Azure IoT Hub), або будується гібридна модель з проміжними перетворювачами протоколів.

Застосування IoT у різних сферах

- **Розумний будинок**: автоматичне керування опаленням, освітленням, технікою, пожежною сигналізацією. Пристрої взаємодіють через локальну мережу або хмару та потребують моніторингу на предмет збоїв, енергоспоживання, зниження якості сигналу.
- **Промисловість**: дистанційне керування обладнанням, моніторинг виробничих показників, діагностика несправностей. Пристрої інтегруються з SCADA, але мають інший життєвий цикл, інтерфейси і потребують зонального моніторингу (цех/підрозділ/виробнича дільниця).
- **Охорона здоров'я**: «розумні браслети» пацієнтів, моніторинг медичних показників у режимі реального часу, безконтактні дрони для доставки медичних препаратів — тут моніторинг стає питанням життя і смерті, а дані повинні бути захищеними й оперативно доставленими.
- **Агросектор**: IoT-сенсори дозволяють контролювати рівень вологи у ґрунті, визначати склад добрив, відстежувати переміщення худоби або стан її здоров'я. Це приклади розподілених IoT-систем із слабким живленням, які критично залежать від мережі LoRaWAN або Zigbee.
- **Ритейл та логістика**: розумні полиці, контроль залишків, каси самообслуговування, відстеження логістичних маршрутів у реальному часі. Тут моніторинг часто включає не лише технічний стан пристрою, а й інтеграцію з ERP/CRM-системами.
- **Smart City**: моніторинг сміттєвих контейнерів, вуличного освітлення, пішохідного руху, стану доріг, кліматичних умов — все це створює високонавантажені IoT-середовища, що потребують гнучкого, масштабованого моніторингу.

Підсумовуючи, Інтернет Речей — це не просто набір пристроїв, а ціла філософія побудови цифрового середовища, у якому взаємодіють «розумні» об'єкти. Їхня кількість і значення в IT-інфраструктурі продовжують стрімко зростати, і саме тому моніторинг IoT-пристроїв перетворюється з другорядної задачі на обов'язкову складову підтримки бізнесу, безпеки та операційної стабільності. У межах системного моніторингу критичних та нетипових об'єктів, IoT сьогодні відіграє таку саму важливу роль, як колись відігравали сервери і маршрутизатори.

SCADA-системи та промислові контролери (PLC, RTU)

SCADA (Supervisory Control and Data Acquisition) — це клас технологічних систем, призначених для дистанційного керування, збору, візуалізації та аналізу даних з фізичних об'єктів у промислових, енергетичних, комунальних, транспортних та інфраструктурних середовищах. У контексті моніторингу IT-інфраструктури SCADA-системи відносяться до нетипових об'єктів, оскільки поєднують цифрові й фізичні компоненти (датчики, механізми, електроніку) і функціонують у режимі реального часу з підвищеними вимогами до надійності.

Основне призначення SCADA-систем

- Моніторинг фізичних параметрів (температура, тиск, потік, рівень, напруга, струм, швидкість тощо);
- Передача даних з об'єктів польового рівня до центральної диспетчерської системи;
- Управління об'єктами на основі заданих алгоритмів (автоматичне або ручне);
- Візуалізація та сповіщення: генерація тривог, трендів, гістограм, вікон попередження.

Типова ***архітектура SCADA-систем*** має багаторівневу структуру:

- **Польовий рівень**: включає датчики, виконавчі механізми та контролери (PLC, RTU), що безпосередньо взаємодіють з фізичними об'єктами.
- **Контрольний рівень**: SCADA-сервери, які агрегують дані, виконують логіку, зберігають історію, взаємодіють з HMI та іншими IT-системами.
- **Інтерфейс користувача (HMI)**: оператори взаємодіють із системою через візуальні панелі, спостерігаючи за станом об'єктів у реальному часі.

На відміну від класичних IT-систем, у SCADA домінують реактивні сценарії, пов'язані з миттєвим реагуванням на зміну фізичного середовища.

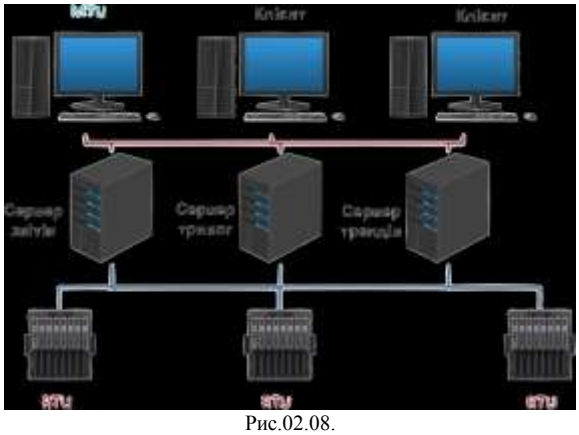

Рис.02.08.

Промислові контролери: PLC та RTU. PLC (Programmable Logic Controller) та RTU (Remote Terminal Unit) — це ключові вузли автоматизації, на які покладається функція локального контролю, збору даних і попередньої обробки сигналів.

PLC:

- Працює на об'єктах з високими вимогами до часу відгуку (десятки мс);
- Призначений для роботи в умовах підвищеного шуму, вібрацій, температур;
- Зазвичай розміщується у безпосередній близькості до об'єкта (лінії, насосні станції, виробничі вузли);
- Програмується у спеціальних середовищах відповідно до стандарту IEC 61131-3.

RTU:

- Оптимізований для віддалених об'єктів (гідротехнічні споруди, нафтогазові вежі, трансформаторні підстанції);
- Може працювати на батарейному живленні або із резервними джерелами;
- Забезпечує телеметричну передачу даних з низькою частотою (1-10 хв);
- Часто підтримує польові промислові протоколи (Modbus, DNP3, IEC 60870-5-104).

Особливості моніторингу SCADA-систем. Моніторинг SCADA має низку характерних ознак:

- Робота в режимі реального часу — критично важлива, особливо у випадках аварійних ситуацій;
- Точність і надійність збору даних — втрати або спотворення даних можуть призвести до катастроф;
- Масштабованість і резервування — системи розгортаються у кількох географічних точках з резервними серверами;
- Інтеграція з IT-системами — SCADA має взаємодіяти з ERP, CMMS, SIEM, хмарними рішеннями тощо;
- Розмежування мереж OT і IT — з міркувань безпеки SCADA працює в окремих сегментах.

Безпека SCADA-систем. Уразливість SCADA-систем до кібератак обумовлена їх критичною важливістю та часто застарілими компонентами. Підхід до безпеки включає:

- Сегментацію мережі, використання DMZ, VPN, ізоляцію інтерфейсів;
- Шифрування телеметрії, автентифікацію пристроїв;
- Регулярний аудит конфігурацій та виявлення змін;
- Використання спеціалізованих систем моніторингу OT-безпеки (наприклад, Nozomi, Claroty).

Значення для моніторингу IT-інфраструктури. Моніторинг SCADA є ключовим для стабільності технологічних процесів, безпеки праці та екологічного контролю. Він має низку викликів:

- Гібридна природа даних: фізичні параметри, логічні події, сигнали тривоги;
- Велика кількість розподілених об'єктів: потреба у віддаленому доступі та нагляді;
- Інтеграція з класичними IT-інструментами моніторингу — наприклад, Zabbix, Prometheus, PRTG часто потребують адаптації для SCADA;
- Критичність затримок та відмов: навіть незначний збій у моніторингу може призвести до зупинки виробництва або небезпечної ситуації.

Приклади реалізації проектів на SCADA-системах.

❖***Система обліку продукції*** обліковує продукцію, що виробляється на технологічних лініях. Ви отримуєте:

- ✓ Підрахунок продукції на кожному робочому місці та загальний випуск;
- ✓ Мотивація робітників, за рахунок візуалізації плану та фактичного виконання (перевиконання) плану;
- ✓ Можливість синхронізації з CRM-системою підприємства або SAP;
- ✓ Безперервний доступ до звітів в режимі online.

Рис.02.09.

Ця система реалізована як SCADA-рішення для відстеження обсягів виробленої продукції на кожному робочому місці виробничої лінії. Крім аналітики виконання виробничого плану, вона може синхронізуватись із CRM або обліковими системами (наприклад, SAP), надаючи керівництву актуальні звіти в режимі реального часу.

Моніторинг такої системи передбачає:

- ✓ Збір телеметрії з ПЛК (PLC), що рахують продукцію — типові сигнали: імпульси з давачів, лічильники продукції, події;
- ✓ Відстеження виконання змінного плану в реальному часі через SCADA-інтерфейс;
- ✓ Моніторинг інтеграцій із зовнішніми системами (CRM, SAP): виявлення помилок синхронізації, контроль затримок оновлень;
- ✓ Аналіз стабільності візуалізації та наявності даних на табло/панелях працівників — доступність Web-клієнтів, реакція HMI;
- ✓ Сповіщення про збої у підрахунках або порушення в логіці ПЛК (наприклад, відсутність сигналу з конкретного сенсора > 5 хв).

Особливістю моніторингу таких SCADA-систем є фокус не лише на технічному стані контролерів, а й на логіці обліку продукції – зміна у рецептах чи подвоєний імпульс може вказувати на помилку, а не на реальний приріст випуску.

❖***Автоматизація бетонного заводу.*** Система управління працює в трьох режимах: автоматичному, ручному та змішаному. Для безперервної роботи БВЗ достатньо двох людей: оператора та водія навантажувача.

Ви отримуєте:

- ✓ Точне дозування всіх інгредієнтів, згідно рецепту;
- ✓ Коригування обсягу подачі води, залежно від вологості інгредієнтів;
- ✓ Архівація даних за зміну, по типу продукту, тощо;
- ✓ Зв'язок з системою бухгалтерського обліку.

Система SCADA на бетонному заводі управляє процесами дозування, змішування та подачі компонентів. Вона може працювати в автоматичному, ручному або змішаному режимі, забезпечуючи точність та узгодженість рецептур. Дані про виробництво зберігаються та передаються до бухгалтерських систем.

Рис.02.10.

Моніторинг системи автоматизації бетонного заводу охоплює:

- ✓ Контроль PLC/RTU, що керують дозаторами, міксерами, конвеєрами — перевірка доступності, збоїв циклів, помилок при дозуванні;
- ✓ Вимірювання параметрів якості (зважування, вологість інгредієнтів), звірка з рецептом;
- ✓ Спостереження за режимами роботи — автоматичний/ручний: хто і коли перемкнув, чи дозволено змішування вручну, наскільки стабільно працює автомат;
- ✓ Моніторинг архівації — чи всі дані за зміну збережено, чи передано їх до облікової системи;
- ✓ Виявлення "тихих відмов" — наприклад, часткова відмова вагового контролера, яка не спричинила аварію, але порушила рецепт.

Моніторинг для бетонного заводу потребує врахування режимів роботи (ручний ≠ автоматичний), тому важливо не лише фіксувати "аварії", а й аналізувати відхилення від нормальних сценаріїв — наприклад, незвичну кількість ручних коригувань або пропуск дозування окремого інгредієнта.

SCADA-системи з PLC та RTU — це приклад високовідповідальних, нетипових об'єктів, для яких системний моніторинг є критично важливим компонентом життєзабезпечення. Їх моніторинг вимагає специфічних підходів, розуміння фізичної сутності керованих процесів, підтримки промислових протоколів та дотримання найвищих стандартів безпеки.

Периферійні пристрої (POS-термінали, банкомати, кіоски)

Ця група охоплює різноманітні точки взаємодії з клієнтами, які, хоч і мають комп'ютерну начинку, часто функціонують без локальних IT-фахівців. Це зумовлює потребу в дистанційному моніторингу – доступності терміналів, справності платіжних модулів, стану операційної системи, оновлень програмного забезпечення, а також виявлення несанкціонованих дій (наприклад, відкриття корпусу термінала чи втручання в платіжний процес).

Такі пристрої зазвичай мають низький рівень ресурсів, але використовують стандартні операційні системи (наприклад, Windows Embedded або Linux), тому можуть моніторитись агентськими або гібридними рішеннями.

Мобільні об'єкти (транспорт, дрони, польові вузли)

Мобільні пристрої мають властивість змінювати географічне положення, виходити з радіусу дії мереж, а також змінювати режими роботи в залежності від контексту або навколишніх умов. Це створює складнощі в гарантованій доставці метрик, ідентифікації пристрою у системі, виявленні втрати зв'язку.

Моніторинг тут здебільшого базується на телеметрії, GPS-даних, датчиках руху, а також системах аналітики, які обробляють події, що надходять асинхронно. У контексті критичних IT-систем особливу увагу приділяють збереженню буферів даних, коли з'єднання розривається, а також відновленню журналів після повернення об'єкта в зону покриття.

Вбудовані системи (embedded control, smart appliances)

Це пристрої з жорстко заданою логікою поведінки — побутові пристрої, smart-термостати, системи управління доступом, охоронні системи тощо. Їх моніторинг зазвичай обмежується передачею телеметрії через стандартизований або власний протокол у хмару або до шлюзового сервера. Більшість з них не підтримують SNMP, не мають відкритих API, а іноді й не мають постійного мережевого з'єднання. Додатковою проблемою є велика кількість виробників і стандартів, що ускладнює централізовану інтеграцію.

Реалізація моніторингу таких пристроїв вимагає створення адаптивних шлюзів, конвертерів протоколів, або застосування IoT-платформ, які абстрагують взаємодію з конкретними моделями пристроїв.

Ці категорії не є вичерпними, але ілюструють спектр викликів, які постають перед IT-командами у спробах побудови комплексної системи моніторингу в умовах різноманіття середовищ, протоколів, вимог до доступності та безпеки. Саме тому класифікація нетипових об'єктів і вибір правильних підходів до їх обслуговування стають ключовими завданнями для архітекторів сучасних IT-систем.

Підходи до класифікації нетипових об'єктів

Класифікація нетипових об'єктів IT-інфраструктури є важливою складовою при побудові ефективної системи моніторингу. Різноманітність форм-факторів, протоколів, режимів роботи та критичності вимагає структурованого підходу до опису та управління такими об'єктами. Нижче розглянуто найбільш поширені класифікаційні ознаки.

1. **За ступенем критичності.** Це одна з ключових ознак, що визначає пріоритетність моніторингу, рівень резервування, швидкість реагування на інциденти. Критичні об'єкти – збої в роботі призводять до зупинки виробничих процесів, фінансових втрат або загроз безпеці (SCADA, PLC у хімічній промисловості, пожежні датчики, енергетичні системи, системи охорони).
   Високопріоритетні об'єкти – забезпечують безперервність обслуговування користувачів або партнерів, але мають допустимі вікна простою (POS-термінали, банкомати, телеметрія транспорту).
   Допоміжні або неключові об'єкти – порушення роботи не спричиняє негайних ризиків, але може вплинути на продуктивність, комфорт, автоматизацію (розумні лічильники, системи моніторингу мікроклімату, камери відеонагляду).

   Ступінь критичності враховується під час побудови SLA, визначення порогів тривог, застосування резервування або самовідновлення.

2. **За фізичною та логічною мобільністю.** Фіксовані об'єкти – постійно розташовані у визначеній географічній точці; приклади: вбудовані контролери HVAC, сервери у шафах, промислові датчики.
   Мобільні об'єкти – переміщуються під час роботи, вимагають телеметрії та геотрекінгу; приклади: дрони, транспорт, мобільні пункти управління.
   Віртуально-динамічні – створюються/знищуються динамічно у віртуальних або хмарних середовищах, мають логічну, а не фізичну мобільність (напр., контейнеризовані вузли IoT, елементи MEC – Mobile Edge Computing).

Застосування: цієї класифікаційної ознаки впливає на обрану технологію зв'язку, потребу в буферизації, вибір частоти опитування, необхідність в автономному збереженні метрик.

3. **За типом взаємодії з IT-інфраструктурою.** Периферійні пристрої – об'єкти, що знаходяться "на краю" мережі, мають прямий або обмежений зв'язок із центром, часто не мають постійного підключення (наприклад, термінали самообслуговування, сенсори в полях).
   Вбудовані системи – інтегровані у більший пристрій або систему, часто функціонують як "чорний ящик" (розумні прилади, мікроконтролери в обладнанні).
   Мережеві пристрої – мають власну мережеву логіку, повноцінний стек протоколів і можуть взаємодіяти із зовнішніми компонентами напряму (IP-камери, контролери із SNMP/Ping/HTTP доступом).

Тип взаємодії з IT-інфраструктурою визначає можливість агентського чи безагентського моніторингу, доступні API, протоколи або необхідність фізичного втручання.

4. **За типом протоколів та доступних інтерфейсів.** Із підтримкою стандартів моніторингу (наприклад, SNMP, MQTT, HTTP/REST, OPC-UA): дають змогу швидко інтегрувати у існуючу систему.
   Закриті або пропрієтарні пристрої: потребують розробки адаптерів, використання SDK, або реверс-інжинірингу протоколу.
   Low-power специфікації: використовують енергоефективні протоколи (LoRaWAN, NB-IoT, Zigbee), обмежені у пропускній здатності та частоті передачі.

Обраний протокол впливає на тип з'єднання, частоту моніторингу, підтримку QoS, можливість двостороннього управління.

5. **За режимом роботи.** Постійно активні об'єкти – працюють у безперервному режимі, передають телеметрію у реальному часі або з високою частотою (SCADA, камерні системи, енергетичні контролери).
   Періодично активні об'єкти – пробуджуються через певні інтервали, надсилають дані пакетами (наприклад, розумні лічильники, польові сенсори LoRa).
   On-demand об'єкти – активуються за запитом або при настанні події (наприклад, трекер для активів, датчик перевищення рівня рідини, викликаний вручну).

Режим роботи визначає потребу в буферизації, кешуванні, наявність шлюзів або брокерів повідомлень.

Класифікація нетипових об'єктів моніторингу є базовою передумовою для побудови ефективної системи спостереження, керування та реагування. Від обраної класифікаційної моделі залежить підбір технологій, засобів збору даних, протоколів, інтерфейсів, а також побудова логіки тривог та звітності. Класифікація також дозволяє оптимізувати ресурси, визначити пріоритети обслуговування та реалізувати моніторинг як частину загальної стратегії цифрової трансформації.

Проблеми сумісності та адаптації

Нетипові об'єкти моніторингу суттєво відрізняються від традиційних серверів або мережевого обладнання тим, що часто не підтримують усталені стандарти спостереження, мають унікальні апаратні або програмні особливості, а іноді — взагалі не передбачають зовнішнього нагляду. Це породжує цілу низку викликів, пов'язаних з інтеграцією таких пристроїв у загальну моніторингову інфраструктуру. Нижче розглянуто ключові проблеми сумісності та адаптації.

1. Відсутність стандартних агентів або SNMP-підтримки

У більшості нетипових пристроїв, особливо вбудованих систем, відсутні стандартні агенти моніторингу, які застосовуються для серверів (наприклад, Zabbix Agent, Prometheus Node Exporter).

Також SNMP (Simple Network Management Protocol), який є де-факто стандартом для збору метрик у класичних IT-середовищах, може бути недоступним або реалізований лише частково.

Наслідки:

- неможливість безпосередньої інтеграції пристрою у традиційну систему моніторингу;
- потреба в проміжному рівні: шлюзах, брокерах, адаптерах;
- збільшення витрат на налаштування та обслуговування.

Приклад: POS-термінали або банкомати часто мають закриті ОС і не надають SNMP-інтерфейс, що змушує використовувати SDK або API, надані виробником.

2. Різноманіття нестандартних протоколів

Нетипові об'єкти можуть використовувати спеціалізовані, галузеві або застарілі протоколи, що не підтримуються "з коробки" більшістю засобів моніторингу. Серед них:

Modbus – індустріальний протокол обміну даними між PLC-контролерами;
MQTT – брокерний протокол публікації/підписки для IoT (включає виклики на адаптацію парсерів);
Zigbee – бездротовий протокол ближнього радіозв'язку, складний для централізованого збору;
OPC UA – використовується в SCADA, потребує OPC-шлюзів або спеціальних клієнтів;
CAN (Controller Area Network) – у транспорті, не має звичних мережевих інтерфейсів;
BACnet – протокол автоматизації будівель;
LwM2M – легкий M2M-протокол для обмежених пристроїв.

Наслідки:

- необхідність реалізації або придбання конвертерів даних;
- складність підтримки гетерогенних середовищ;
- потенційна втрата частини даних при невдалому парсингу.

3. Відсутність ОС або повноцінного стеку TCP/IP

Багато вбудованих або енергоощадних пристроїв функціонують без повноцінної операційної системи або взагалі не підтримують стек TCP/IP. Це характерно для:

- сенсорів, що працюють через LoRaWAN або Zigbee;
- популярних мікроконтролерів (на кшталт STM32, ESP32 без Real Time OS).
- приладів, що працюють лише за низькорівневими шинами зв'язку.

Наслідки:

- неможливість прямого мережевого опитування пристрою;
- необхідність використання шлюзів/хабів з трансляцією протоколів;
- обмеження на швидкість, обсяг та регулярність телеметрії.

4. Використання пропрієтарних рішень

Велика кількість пристроїв (особливо SCADA, медичне обладнання, виробничі контролери) працюють на закритих платформах з власними протоколами, API, форматами логів. Виробники таких рішень обмежують можливості інтеграції:

- API доступний лише за NDA (Non-Disclosure Agreement) або платною ліцензією;
- SDK працює лише під Windows;
- телеметрія експортується в CSV або XML формати, не оптимізовані для потокової обробки.

Наслідки:

- потреба в адаптації за допомогою скриптів, зовнішніх парсерів;
- підвищені витрати на розробку/тестування;
- ризик vendor lock-in.

Приклад: інтеграція медичних моніторів в реанімаціях — вимагає використання OEM-драйверів або створення middleware.

5. Низький рівень телеметрії, обмежений обсяг журналів

Нетипові пристрої часто мають обмежену кількість метрик, не ведуть або дуже обмежено ведуть журнали подій, не зберігають історію, або обнуляють її при перезавантаженні. Наслідки:

- неможливість аналізу трендів і побудови повноцінної аналітики;
- ускладнене розслідування інцидентів (немає логів за момент аварії);
- потреба у зовнішньому лог-збиранні (наприклад, через syslog або telemetry collector на шлюзі).

Приклад: розумний лічильник води може передавати лише одне число раз на добу, без індикації внутрішніх станів чи попередніх значень.

Проблеми сумісності та адаптації в моніторингу нетипових об'єктів — це не лише технічне, а й стратегічне завдання. Вони потребують багаторівневої інтеграції, розробки кастомних конекторів, впровадження шлюзових рішень, здатних перекодовувати, буферизувати й транслювати дані. Саме тому побудова гнучкої, модульної системи моніторингу, здатної взаємодіяти з гетерогенним середовищем — критично важлива для успішного супроводу таких систем.

Способи адаптації засобів моніторингу до нетипових об'єктів

У середовищі, де наявні IoT-пристрої, SCADA-контролери, сенсори або мобільні вузли, стандартні механізми опитування та збору метрик часто є непридатними. У відповідь на це формується цілий набір технічних та організаційних рішень, спрямованих на адаптацію засобів моніторингу до специфічних обмежень, форматів і протоколів. Розглянемо основні способи такої адаптації.

Використання шлюзів-проксі або конвертерів протоколів

Конвертери протоколів, також відомі як шлюзи-проксі, є ключовим інструментом для інтеграції нетипових або закритих IoT- та промислових пристроїв у стандартні системи моніторингу. Ці програмні чи апаратні компоненти виступають своєрідними «перекладачами» між специфічними протоколами окремих пристроїв та уніфікованими каналами збору метрик, що використовуються в сучасних NMS-рішеннях.

У найпростішому випадку це може виглядати так: пристрій працює за протоколом Modbus, але система моніторингу підтримує лише SNMP. У цьому разі конвертер опитує пристрій по Modbus, перетворюючи його відповіді на SNMP-трапи або доступні через SNMP GET/SET. У більш просунутих сценаріях можливе перетворення даних з OPC UA у REST/HTTP-сервіси, де інформація з промислових контролерів доступна у форматі JSON, або публікація телеметрії з Zigbee-пристроїв у MQTT-брокер, що дозволяє централізовано збирати й обробляти події.

Використання таких шлюзів дає змогу стандартизувати вхідні дані, спростити масштабування моніторингової системи (оскільки не потребує змін у самих пристроях), а також забезпечити безпечне розміщення компонентів у проміжних зонах — наприклад, у DMZ або на IoT-шлюзах, що працюють на периферії мережі. Це особливо актуально у великих або гетерогенних інфраструктурах, де різні класи пристроїв мають різні протоколи, можливості й вимоги до безпеки.

Підключення через SCADA-сервери або проміжні хаби

У промислових та великих IoT-системах пристрої зазвичай не підключаються до систем моніторингу напряму, а через проміжні компоненти — такі як SCADA-сервери, IoT-хаби чи брокери. Ці проміжні вузли збирають і агрегують дані з багатьох джерел, перетворюючись на центральні точки збору метрик для моніторингу. Наприклад, системи Zabbix або Prometheus можуть отримувати інформацію не безпосередньо з PLC-контролерів, а через SCADA-сервери, використовуючи протоколи OPC, MQTT або REST API. В мережах LoRaWAN дані з сенсорів надходять на мережевий сервер, а вже звідти їх забирає моніторингова система.

Такий підхід має кілька важливих переваг: по-перше, він значно знижує навантаження на кінцеві пристрої, оскільки саме проміжні сервери виконують основну роботу з обробки запитів; по-друге, централізує логіку доступу, безпеки та обробки даних, що спрощує управління системою; і по-третє, ці проміжні компоненти часто забезпечують зручні API та готові інтеграції, що полегшує підключення до різних моніторингових рішень.

Застосування проміжного ПЗ або агентів на периферійних пристроях

Коли на об'єкті можливо встановити додаткове програмне забезпечення, часто використовують легковагові агенти, скрипти, мікросервіси або спеціальні демони, які відповідають за збір та передачу даних з пристроїв. До типових рішень належать Python-агенти, які опитують внутрішні API пристрою і передають метрики через REST або MQTT, а також Node-RED — популярний інструмент для оркестрації IoT-телеметрії. Для периферійних терміналів можуть застосовуватися WMI або PowerShell-скрипти, що дозволяють організувати збір інформації без значних витрат ресурсів.

Основні переваги такого підходу — це гнучкість у налаштуванні логіки опитування і форматуванні даних, підтримка push-механізмів, що дозволяють пристрою самостійно відправляти інформацію, а також можливість кешувати дані локально і повторно відправляти їх у разі тимчасового відключення зв'язку. Це підвищує надійність і ефективність збору метрик у складних умовах.

Підтримка індустріальних протоколів у сучасних системах моніторингу

Сучасні системи моніторингу, такі як Zabbix, Icinga, PRTG, OpenNMS та інші, все частіше підтримують промислові протоколи через вбудовані плагіни, модулі або спеціальні інтерфейси. Це значно полегшує інтеграцію промислового обладнання у загальну систему

спостереження. Наприклад, Zabbix може працювати з MQTT та Modbus завдяки відповідним модулям, PRTG має готові сенсори для протоколів OPC UA, BACnet і CAN, а Prometheus може отримувати дані через REST або MQTT-брокери з push-метриками.

Головні переваги такого підходу — це зменшення необхідності у використанні зовнішніх конвертерів протоколів, підвищена стабільність роботи завдяки підтримці великої спільноти користувачів і розробників, а також уніфікація системи сповіщень, налаштувань тригерів і збереження історії подій. Це робить моніторинг більш надійним і зручним у підтримці.

Спільне використання CMDB/Asset Management для фіксації конфігурацій

У великих інфраструктурах із численними нестандартними пристроями часто використовують CMDB (Configuration Management Database – базу даних управління конфігураціями) або системи обліку активів (Asset Management). Вони зберігають мета-інформацію про об'єкти, які неможливо або не потрібно активно моніторити в реальному часі. Такі системи фіксують характеристики пристроїв без телеметрії, зберігають інвентаризаційні дані — модель, місце розташування, IP-адресу, протокол доступу — і інтегруються з Service Desk чи системами аудиту подій. Наприклад, якщо сенсор не має власного API, його стан (online/offline) у CMDB може відслідковуватися не через прямі дані пристрою, а за сигналами «heartbeat» від шлюзу або періодичним ping-запитом. Це допомагає покрити «темні зони» моніторингу, доповнює загальну картину системи і підвищує рівень обізнаності та аналітики в управлінні інфраструктурою.

Адаптація засобів моніторингу до нетипових об'єктів — це багаторівневий процес, що вимагає гнучкості, інтеграційного мислення та технічного розмаїття. Успішне рішення рідко грунтується на одному підході — натомість поєднуються шлюзи, API, брокери, CMDB та інструменти обліку. Саме тому адаптивна архітектура моніторингових систем є ключем до повноцінного нагляду за сучасною, децентралізованою IT-інфраструктурою.

Особливості моніторингу IoT-інфраструктур

Баланс між частотою збору даних та енергоспоживанням

Моніторинг IoT-інфраструктур має низку унікальних викликів, з-поміж яких однією з найкритичніших є необхідність збереження балансу між частотою збору даних і енергоспоживанням. Багато IoT-пристроїв, зокрема ті, що працюють на батареях, встановлюються у віддалених або важкодоступних місцях — на дахах будівель, у колодязях, підземних шахтах, на сільськогосподарських полях тощо. В таких умовах доступ до пристроїв для регулярного обслуговування або заміни батарей є обмеженим або дорогим, тому від них очікують автономної роботи протягом кількох років — зазвичай від 3 до 10.

Водночас, системи моніторингу потребують актуальних і регулярних даних для забезпечення контролю за станом об'єктів. Це створює конфлікт: чим частіше пристрій передає дані або відповідає на запити (особливо у pull-моделі моніторингу, де ініціатива йде від системи), тим швидше розряджається батарея. Навіть на перший погляд нешкідливі дії, як-от часті ping-запити або регулярне опитування, можуть за кілька тижнів вичерпати ресурс живлення.

Щоб вирішити цю проблему, в IoT застосовують низку стратегій. По-перше, віддається перевага push-моделі, коли пристрій сам ініціює передачу даних — або при виникненні події (тривога, зміна параметра), або за заданим розкладом. По-друге, застосовуються адаптивні алгоритми: якщо система працює стабільно й не фіксує змін, пристрій може зменшувати частоту виходу на зв'язок. Ще одним підходом є локальне кешування даних — пристрій зберігає показники в пам'яті і передає їх пакетно через певний інтервал часу. Нарешті, використовуються енергоефективні протоколи зв'язку, зокрема LoRaWAN, NB-IoT, BLE, які дозволяють значно зменшити витрати енергії на передачу інформації, зберігаючи при цьому достатню надійність зв'язку.

Таким чином, грамотне проєктування моніторингу в IoT-середовищах потребує не лише технічних знань, але й врахування особливостей роботи кінцевих пристроїв, енергетичних обмежень і реальних умов розгортання інфраструктури.

Мережеві ризики при використанні загальнодоступних каналів

У багатьох випадках IoT-пристрої передають дані через канали зв'язку, які не є повністю контрольованими або захищеними — наприклад, через безліцензійні частоти (LoRaWAN), мобільні мережі (NB-IoT), або публічні Wi-Fi/Ethernet-сегменти. Це створює низку мережевих ризиків, які безпосередньо впливають на надійність і безпеку моніторингу.

Основні загрози включають:

Перехоплення чи модифікація даних під час передачі через незахищений канал;

Відсутність або слабке шифрування, зокрема при неправильному налаштуванні шлюзів;

DoS-атаки (відмова в обслуговуванні) через перевантаження каналу чи проміжних вузлів;

Втрати або нестабільна доставка даних, що особливо критично в умовах віддалених регіонів або складного радіооточення.

Рекомендовані заходи захисту:

- ✓ Застосування end-to-end шифрування: TLS, DTLS, AES, VPN;
- ✓ Чітке розмежування прав доступу до шлюзів, брокерів, API;
- ✓ Буферизація даних на пристрої з можливістю повторної передачі у випадку втрати зв'язку.

Загалом, для захисту IoT-систем у відкритих мережах потрібен продуманий підхід до архітектури, який враховує як технічні, так і інфраструктурні аспекти.

Проблеми автентифікації та безпечного з'єднання

Забезпечення надійної автентифікації в IoT-інфраструктурі часто ускладнене через апаратні обмеження: багато пристроїв не мають повноцінної операційної системи або засобів апаратного шифрування. Це робить їх вразливими до низки загроз, особливо якщо йдеться про віддалене підключення через інтернет або загальнодоступні мережі.

Типові уразливості:

- ✓ жорстко зашиті паролі або ключі у прошивках, які неможливо змінити без перепрошивки;
- ✓ відкриті порти (наприклад, Telnet, HTTP), що доступні ззовні без належного контролю;
- ✓ використання застарілих або небезпечних протоколів, що не забезпечують шифрування.

Рекомендовані захисні заходи:

- ✓ використання одноразових ключів (pre-shared keys) або цифрових сертифікатів для автентифікації пристроїв;
- ✓ інтеграція токенів доступу (JWT, OAuth) при роботі з API або хмарними сервісами;
- ✓ фільтрація та блокування запитів на рівні брокерів або IoT-шлюзів;
- ✓ перехід на сучасні протоколи захищеного з'єднання — TLS, DTLS з актуальними криптоалгоритмами.

Таким чином, безпечна автентифікація є обов'язковою умовою для захисту IoT-систем від зовнішніх вторгнень, підміни пристроїв або несанкціонованого збору даних.

Підтримка OTA-оновлень та віддаленого контролю

Підтримка OTA-оновлень (Over The Air) та віддаленого контролю є одним із ключових елементів ефективного управління IoT-інфраструктурою. Вона дозволяє централізовано оновлювати програмне забезпечення пристроїв, змінювати конфігурацію, проводити діагностику та тестування без необхідності фізичного доступу до обладнання. Це особливо важливо для масштабованих мереж або пристроїв, розташованих у важкодоступних місцях.

Основними потребами є оновлення прошивок для усунення вразливостей або помилок, зміна налаштувань з урахуванням нових вимог, а також можливість перезавантаження пристрою чи запуску самотестування. Однак реалізація OTA супроводжується низкою викликів. Найпоширеніший — ризик пошкодження пристрою (так званий "bricking") у разі збою під час оновлення. Також важливими є вимоги до захищеності оновлень — необхідне шифрування, перевірка цифрових підписів, цілісності файлів, щоб уникнути підміни чи втручання. Крім того, часто оновлення доволі об'ємні, а канали зв'язку, особливо в LoRaWAN або NB-IoT, мають обмежену пропускну здатність, що ускладнює передачу.

Для подолання цих викликів застосовуються спеціалізовані OTA-платформи, як-от Mender, Balena або Amazon IoT Core Device Management, які автоматизують процес оновлення, контролюють його перебіг та забезпечують безпеку. Також використовується перевірка хеш-сум або цифрових підписів перед застосуванням оновлення, а інкрементальні оновлення — коли передаються тільки змінені частини прошивки — допомагають зменшити обсяг переданих даних.

Загалом, наявність надійної OTA-механіки значно підвищує керованість, безпеку та життєвий цикл IoT-пристроїв, особливо в умовах динамічного розвитку систем і змін у середовищі їхнього функціонування.

Моніторинг IoT-інфраструктури вимагає нестандартного підходу, що враховує обмеження в ресурсах, нестабільність підключення, необхідність енергозбереження та високий рівень безпеки. Це високовідповідальне середовище, де помилка моніторингу може не тільки ускладнити адміністрування, але й призвести до значних втрат — як технічних, так і репутаційних.

Вимоги до безпеки моніторингу нетипових об'єктів

Моніторинг нетипових об'єктів IT-інфраструктури (IoT, SCADA, периферійні пристрої, мобільні вузли тощо) повинен враховувати не лише технічну складність середовища, а й загрози безпеці, які прямо впливають на достовірність даних, стійкість систем і захист критичних операцій. Уразливість моніторингового каналу або механізму збору телеметрії може спричинити як некоректні рішення, так і компрометацію об'єктів у реальному світі.

1. Визначення зони ризику

Перший важливий крок — класифікувати об'єкти за рівнем їхньої доступності та потенційного ризику. Для цього застосовують критерії зонування, що враховують, чи має пристрій інтернет-доступ і якою мірою він піддається зовнішнім загрозам, таким як атаки типу DoS, MITM або мережеве сканування. Також важливо враховувати можливість фізичного доступу до пристрою, адже якщо зловмисник може безпосередньо вплинути на обладнання, ризики значно зростають. Крім того, аналізують розташування пристроїв — чи знаходяться вони в публічних або контрольованих мережах, а також чи є у мережі захищені сегменти або використовується сегментація для обмеження доступу.

Зони ризику можна поділити на три рівні:

Зона 0 — це повністю ізольовані пристрої, доступ до яких можливий лише локально, без віддаленого моніторингу;

Зона 1 — пристрої, розміщені в захищених мережах, наприклад у корпоративних VPN або DMZ;

Зона 2 — пристрої, які мають потенційно публічний доступ або підключені через загальнодоступні канали.

Визначення зони ризику є ключовим, адже від цього залежить, які саме заходи безпеки необхідно впроваджувати: вибір типів шифрування, способів автентифікації, а також сценаріїв моніторингу.

2. Захист телеметричних каналів

Передача даних від нетипових пристроїв повинна бути надійно захищена від будь-якого перехоплення або зміни інформації. Навіть прості показники, як-от "температура = 21°C", можуть мати критичне значення для роботи промислових процесів, тому їх потрібно передавати безпечно. Для цього застосовують різні технології захисту: TLS або DTLS — для захищеного шифрування даних у протоколах HTTP(S), MQTT, CoAP; VPN-рішення, такі як IPsec, OpenVPN або WireGuard, дозволяють створювати безпечні тунелі для передачі інформації між пристроями й центром моніторингу. Крім того, використовуються брокери MQTT або AMQP із підтримкою TLS/SSL і аутентифікації клієнтів, а для додаткової ізоляції каналів між різними мережевими сегментами застосовують VLAN або програмно-визначені мережі (SDN).

Важливим є і правильне керування сертифікатами безпеки: рекомендується використовувати короткострокові або автоматично оновлювані сертифікати, наприклад, через протокол ACME. Також слід уникати спільного використання сертифікатів між різними пристроями, щоб не створювати уразливі точки через однакові ключі доступу.

ACME (Automatic Certificate Management Environment) — це стандартний протокол, який автоматизує процес отримання, підтвердження, оновлення та скасування цифрових сертифікатів для шифрування (наприклад, SSL/TLS сертифікатів). Його основна мета — спростити і зробити безпечним керування сертифікатами, які потрібні для захищеного обміну даними в інтернеті.

ACME дозволяє серверам автоматично підтверджувати право власності на домен або пристрій і отримувати сертифікати від центрів сертифікації (наприклад, Let's Encrypt) без ручного втручання, що значно знижує ризик помилок і дозволяє підтримувати актуальні сертифікати без зайвих витрат часу. Це особливо корисно для IoT-пристроїв та інших систем, де велика кількість пристроїв потребує регулярного оновлення сертифікатів.

3. Верифікація достовірності даних від об'єктів

У ситуаціях, коли об'єкти моніторингу розташовані віддалено або працюють у нестабільному середовищі, існує реальна загроза отримання спотворених або навіть підроблених телеметричних даних. Щоб цього уникнути, критично важливо забезпечити достовірність отримуваної інформації.

Один з ключових способів — використання цифрових підписів або HMAC безпосередньо на рівні пристрою. Завдяки цьому можливо переконатися, що дані дійсно надійшли від довіреного джерела, і що їх не було змінено в процесі передавання. Окрім цього, широко застосовуються методи контекстного аналізу та виявлення аномалій — наприклад, коли система фіксує показники, які виходять за межі фізично можливих (скажімо, тиск у трубі зростає до 9999 одиниць без жодної причини), це одразу викликає тривогу.

Ще одним підходом є крос-перевірка: дані від одного пристрою можуть бути підтверджені з іншого джерела — наприклад, відеоспостереженням або сенсором іншого типу. Актуальність інформації також перевіряється за допомогою часових міток: усі повідомлення мають бути відмічені точним часом, і при обробці перевіряється, що затримка передачі не виходить за допустимі межі — це допомагає захиститися від повторного надсилання старих (і потенційно маніпульованих) даних.

Для пристроїв, які не мають апаратної підтримки шифрування або криптографічних операцій, можуть використовуватися довірені шлюзи або проксі. Вони приймають необроблені дані, здійснюють верифікацію або підписування на себе, і вже в такому вигляді пересилають інформацію в систему моніторингу. Такий підхід дозволяє підвищити рівень безпеки навіть у обмежених за ресурсами середовищах.

4. Моніторинг самої системи моніторингу

Система моніторингу сама по собі є критичним елементом інфраструктури, особливо коли йдеться про промислові або IoT-середовища. Її компрометація чи відмова може призвести не лише до втрати спостереження за об'єктами, а й до нездатності вчасно реагувати на інциденти. Тому однією з ключових вимог безпеки є постійний контроль за працездатністю та захищеністю самої системи моніторингу.

По-перше, необхідно забезпечити повне логування — кожен запит до API, брокерів телеметрії чи інших точок входу в систему має бути задокументований. Це дозволяє не лише відслідковувати несанкціоновану активність, а й відновити картину подій у разі інциденту. Додатково важливо впровадити аудит дій користувачів: хто, коли та які операції виконував у моніторинговому середовищі. Це особливо актуально для систем із кількома рівнями доступу.

Ще один обов'язковий елемент — використання систем виявлення вторгнень (IDS/IPS), розгорнутих у мережевому сегменті моніторингу. Вони можуть своєчасно зафіксувати підозрілу активність, наприклад, спроби сканування або несанкціонованих підключень. Для перевірки достовірності самих моніторингових даних доцільно застосовувати синтетичні тести — наприклад, генерувати контрольні сигнали й перевіряти, чи система їх правильно обробляє та реєструє. Це допомагає виявити "мовчазні" збої, коли система нібито працює, але не збирає або не показує реальні дані.

Нарешті, важливо мати захищене резервне копіювання всієї конфігурації системи моніторингу, журналів подій та налаштувань. У разі атаки або аварії це дозволить швидко відновити працездатність без втрати історичних даних і ключових параметрів.

У сучасних архітектурах дедалі частіше впроваджується концепція багаторівневого моніторингу — тобто коли система не лише спостерігає за зовнішніми об'єктами, а й постійно контролює саму себе (self-monitoring). Такий підхід дозволяє оперативно виявляти несправності, порушення логіки збору даних або спроби злому в реальному часі.

Захист моніторингу нетипових об'єктів — це не лише про шифрування чи автентифікацію. Це цілий набір архітектурних, криптографічних і процедурних рішень, які забезпечують надійність, цілісність і довіру до отриманих даних. В умовах зростання кількості розумних пристроїв, відсутність фокусу на безпеку моніторингу може стати критичною вразливістю, здатною поставити під загрозу роботу всього бізнесу чи інфраструктури.

Приклади застосування та кейси

Промисловість: SCADA-моніторинг насосних станцій

У промисловому секторі насосні станції є критичними об'єктами, що забезпечують безперервне транспортування води, нафти, газу або інших рідин через трубопровідні системи. Будь-яка зупинка чи несправність може спричинити не лише економічні збитки, а й техногенні ризики. Саме тому їх моніторинг в режимі реального часу є життєво необхідним.

Основні параметри, які підлягають спостереженню, — це тиск у системі, витрата рідини, рівень у резервуарах, температура та навантаження на двигуни. Крім цього, важливо фіксувати аварійні сигнали, зокрема перевантаження насосів, перегрів, витік або відмову електроживлення. В умовах промислових об'єктів також необхідно контролювати резервні джерела живлення, адже у разі аварії живлення може бути єдиним способом забезпечити завершення критичних технологічних циклів.

Для реалізації такого моніторингу застосовуються SCADA-системи, що підтримують промислові протоколи зв'язку, такі як Modbus RTU або TCP, а також OPC UA. В ролі польових пристроїв зазвичай виступають PLC-контролери або RTU, які безпосередньо зчитують сигнали з сенсорів та виконавчих пристроїв. Дані передаються на SCADA-сервер, де проходять візуалізацію, зберігаються історії подій і налаштовуються сценарії оповіщення. У випадках, коли необхідно інтегрувати SCADA-систему до ширшої системи моніторингу (наприклад, загальної NMS компанії), використовуються шлюзи або проксі-конвертери, які транслюють дані в більш загальноприйняті формати — наприклад, SNMP або REST API.

Особливістю такого середовища є його суворі умови — пристрої часто працюють на відкритому повітрі, у вологому, запиленому або навіть вибухонебезпечному середовищі. Ще однією проблемою є нестабільний або обмежений канал зв'язку, особливо в польових умовах. Через це SCADA-моніторинг має бути максимально стійким до втрат даних, з можливістю буферизації, повторних спроб передачі, а також мінімальної затримки в надсиланні аварійних повідомлень.

Таким чином, моніторинг насосних станцій — це приклад висококритичного застосування, де безпека, стійкість і швидкість реакції системи мають ключове значення.

Ритейл: POS-термінали та касові комплекси

У сфері ритейлу POS-термінали та касові комплекси є ключовими вузлами взаємодії з клієнтом, і навіть короткочасна їх недоступність може призвести до втрати прибутку, черг, негативного клієнтського досвіду та збоїв у роботі магазинів. Тому забезпечення їх стабільної роботи та оперативне виявлення проблем є пріоритетом для служб моніторингу.

Основними цілями моніторингу таких пристроїв є контроль їх доступності, стану підключення до процесингових центрів, вчасне оновлення програмного забезпечення й прошивки, а також облік транзакцій, включаючи помилки авторизації або нестандартну поведінку. Не менш важливою є перевірка цілісності системи — пристрій не повинен бути модифікований сторонніми особами або зазнавати впливу зловмисного ПЗ, особливо в умовах, коли з ним працює непрофесійний персонал або він фізично доступний клієнтам.

Для реалізації моніторингу в ритейлі зазвичай використовуються легковагові агенти, встановлені безпосередньо на касові пристрої, або спеціалізоване внутрішнє ПЗ компанії, яке фіксує технічний стан, збої та мережеву активність. Важливу роль відіграє інтеграція з CMDB (системою обліку конфігурацій), яка дозволяє зіставляти технічні дані з реальним розташуванням, моделлю, версією прошивки тощо. Дані передаються у централізовані системи моніторингу через VPN-тунелі, що забезпечує безпечну комунікацію навіть у випадку використання публічних або мобільних каналів. Як транспорт можуть використовуватись MQTT або HTTPS — це дає змогу гнучко працювати з нестабільними або низькошвидкісними каналами.

Оскільки ритейл-інфраструктура, як правило, географічно сильно розподілена (сотні або тисячі магазинів у різних регіонах), важливими є масштабованість рішення, автоматичне виявлення проблем та мінімізація потреби у фізичному втручанні з боку технічного персоналу на місцях. Такі особливості формують вимоги до системи моніторингу як до високодоступного, автономного й самодостатнього інструменту в операційній структурі роздрібної мережі.

Енергетика: віддалене опитування лічильників

У сфері енергетики дедалі ширше впроваджуються системи віддаленого опитування лічильників, які дозволяють автоматизовано зчитувати дані про споживання електроенергії, води, газу або тепла. Такі «розумні» лічильники допомагають підвищити точність обліку, зменшити витрати на ручне обслуговування та забезпечити оперативне виявлення несправностей або несанкціонованих втручань.

Основними об'єктами моніторингу є самі показники споживання (наприклад, щодобове або погодинне використання), наявність і стабільність зв'язку з лічильником, а також коректність роботи пристрою. Важливим аспектом є фіксація нетипових ситуацій, таких як раптове

зникнення сигналу, від'єднання пристрою, виявлення відкриття корпусу або різке падіння/стрибок показників, що може вказувати на спроби шахрайства.

Передача даних зазвичай здійснюється через енергоефективні протоколи — NB-IoT, LoRaWAN, GPRS або LTE Cat-M1, які дозволяють забезпечити зв'язок навіть у складних умовах (наприклад, у підвальних приміщеннях). У ролі прикладного рівня часто використовуються MQTT, CoAP або LwM2M — протоколи, що адаптовані до пристроїв з обмеженими ресурсами і дозволяють як періодичне опитування, так і передачу подій у режимі push. Крім того, важливим елементом є підтримка OTA-оновлень для конфігурації лічильників, що дозволяє дистанційно змінювати налаштування без фізичного доступу.

Особливість цього сценарію полягає у тому, що більшість лічильників виходить на зв'язок лише кілька разів на добу, зберігаючи таким чином заряд батареї на тривалий період — іноді понад 10 років. Це вимагає адаптації логіки моніторингу до нерегулярного трафіку й асинхронних повідомлень. Зважаючи на критичність даних і потенційний вплив на рахунки споживачів, канали передачі повинні бути належним чином захищені — як на транспортному рівні (TLS, DTLS), так і з боку автентифікації (сертифікати, ключі, унікальні токени).

Ще один важливий аспект — зв'язок між технічними даними та реальними споживачами. Для цього використовується CMDB або подібні системи обліку, які дозволяють зіставити конкретний пристрій із його фізичною адресою, власником або обліковим записом. Це забезпечує повноцінний контекст у разі виникнення інцидентів і спрощує роботу служби підтримки.

Аграрна сфера: IoT для моніторингу стану ґрунту і метеоданих

В аграрній сфері технології IoT відкривають нові можливості для точного землеробства — підходу, що базується на регулярному зборі, аналізі та використанні даних про навколишнє середовище та стан ґрунту для прийняття рішень у реальному часі. Завдяки встановленню сенсорів на полях, фермери отримують доступ до інформації про вологість і температуру ґрунту, рівень pH, освітленість, атмосферний тиск, опади та інші параметри, які прямо впливають на врожайність.

Ключовими цілями моніторингу є отримання метео- та ґрунтових показників у режимі реального часу, контроль працездатності сенсорів, а також стану їх живлення — більшість таких пристроїв працюють на батареях і розміщуються у важкодоступних місцях. Зібрані дані використовуються не лише для спостереження, а й для активації автоматизованих дій, зокрема запуску систем зрошення або подачі добрив. У більш комплексних рішеннях інформація з полів агрегується і аналізується на рівні всієї ферми або навіть регіону, з урахуванням супутникових знімків та історичних трендів.

Для передачі даних зазвичай використовуються енергоефективні бездротові технології — передусім LoRaWAN або NB-IoT. Це дозволяє сенсорам працювати роками без підзарядки, передаючи дані з періодичністю раз на кілька хвилин або тільки у випадку події (наприклад, різкого зниження вологості). Отримана телеметрія потрапляє у хмарні сервіси, де візуалізується через веб-інтерфейси, доповнюється аналітичними звітами або рекомендаціями щодо агрономічних дій.

Особливістю таких систем є велика кількість розподілених, часто автономних пристроїв із обмеженим живленням та нестабільним зв'язком — особливо у віддалених сільських районах. Це вимагає ретельної організації логіки моніторингу, адаптації частоти опитування, використання буферизації даних на стороні сенсора, а також підтримки можливості віддаленого оновлення конфігурацій (OTA). Погодні умови також можуть впливати як на самі вимірювання, так і на якість зв'язку, що слід враховувати при інтерпретації даних.

Узагальнення

Наведені приклади демонструють, що нетипові об'єкти значно різняться між собою — як за технічними можливостями та протоколами зв'язку, так і за умовами експлуатації чи рівнем критичності. Це вимагає від систем моніторингу високої гнучкості, здатності працювати з нестандартними пристроями та форматами, інтегруватися з проміжним програмним забезпеченням і зовнішніми платформами. Водночас, важливими залишаються автоматизація, масштабованість і дотримання вимог до безпеки на всіх рівнях.

Висновки

Моніторинг нетипових об'єктів IT-інфраструктури — це не просто розширення традиційних підходів, а окрема стратегічна задача, що вимагає глибокого розуміння контексту, технічних обмежень і динаміки середовища. Ці об'єкти вирізняються високою варіативністю, обмеженими ресурсами, а також нестандартними протоколами та інтерфейсами, що ускладнює їх інтеграцію в класичні системи моніторингу.

Одним з ключових кроків у роботі з такими об'єктами є класифікація – за критичністю, мобільністю, типом взаємодії, протоколами та режимами роботи. Вона дозволяє обрати оптимальні методи збору даних, частоту опитування, типи сповіщень і необхідні заходи безпеки. Без чіткої класифікації будь-яка спроба моніторингу ризикує стати фрагментарною або неефективною.

З урахуванням відсутності у багатьох нетипових об'єктів повноцінної ОС, TCP/IP-стеку або стандартних SNMP-агентів, необхідність адаптації інструментів моніторингу стає критичною. Це вимагає застосування проміжного ПЗ, шлюзів-проксі, протокол-конвертерів або специфічних інтеграцій. Сучасні системи моніторингу мають розвиватися в бік глибокої підтримки індустріальних стандартів і роботи з подієво-орієнтованими даними з пристроїв із мінімальним енергоспоживанням.

Насамкінець, нетипові об'єкти (IoT, SCADA, вбудовані або периферійні системи) вже є невід'ємною частиною загальної цифрової екосистеми, а отже — і стратегії забезпечення надійності, безпеки та доступності IT-інфраструктури. Їх ефективний моніторинг дозволяє не лише вчасно виявляти збої, але й підвищувати контрольованість бізнес-процесів, розширювати автоматизацію та знижувати ризики на стику IT та OT-середовищ.