Міністерство освіти і науки України
Харківський національний університет радіоелектроніки

Факультет *ННЦЗФН*
(повна назва)

Кафедра *Інформаційно-мережної інженерії*
(повна назва)

КВАЛІФІКАЦІЙНА РОБОТА
Пояснювальна записка

рівень вищої освіти перший (бакалаврський)

Розробка системи моніторингу параметрів серверної кімнати та її автономного електроживлення на базі IoT -технологій
(тема)

Виконав:
студент 4 курсу, групи ТРІМІз-22-1
Ірина Горбатенко
(власне ім'я, прізвище)
Спеціальність *172 Телекомунікація та радіотехніка*
(код і повна назва спеціальності)
Тип програми *освітньо-професійна*
(освітньо-професійна або освітньо-наукова)
Освітня програма *Інформаційно-мережна інженерія*
(повна назва освітньої програми)
Керівник *доц. каф. ІМІ, Станіслав Іваненко*
(посада, власне ім'я, прізвище)

Допускається до захисту
В.о. зав. кафедри _____ Дарія *ЧЕБОТАРЬОВА*
(підпис) (власне ім'я, прізвище)

2026 р.

Не містить відомостей, заборонених до відкритого публікування

Здобувач _____ / *Ірина Горбатенко* /
(підпис) (власне ім'я, прізвище)

Керівник _____ / *Станіслав ІВАНЕНКО* /
(підпис) (власне ім'я, прізвище)

Харківський національний університет радіоелектроніки

Факультет *ННЦЗФН*
Кафедра *Інформаційно-мережної інженерії*
Рівень вищої освіти *перший (бакалаврський)*
Спеціальність *172 Телекомунікація та радіотехніка*
(код і повна назва)
Тип програми *освітньо-професійна*
Освітня програма *Інформаційно-мережна інженерія*
(повна назва)

ЗАТВЕРДЖУЮ
Зав. кафедри
_____
(підпис)
«___» _____ 2026 р.

ЗАВДАННЯ

НА КВАЛІФІКАЦФЙНУ РОБОТУ

здобувачеві *Горбатенко Ірині Михайловні*
(прізвище, ім'я, по батькові)

1. Тема роботи *Розробка системи моніторингу параметрів серверної кімнати та її автономного електроживлення на базі IoT -технологій*
затверджена наказом університету від 18 *травня* 20 *26* р. № 73 *Стз*
2. Термін подання студентом роботи до екзаменаційної комісії*17.07.*2026р.
3. Вихідні дані до роботи *Провести аналіз існуючих систем монітронигу серверних кімнат, розробити систему моніторингу для серверних кімнат на базі IoT -технологій та провести порівняльний аналіз з аналогами для виявлення переваг та недоліків.*

4. Перелік запитань, що необхідно опрацювати в роботі
Вступ
1 Аналіз сучасних тенденцій розвитку IoT для дата-центрів
2 Реалізація та розробка концепції власної IoT-системи моніторінгу
3 Оцінка ефективності та порівняльний аналіз розробленої системи
Висновки
5. Перелік графічного матеріалу із зазначенням креслень, схем, плакатів,

комп'ютерних ілюстрацій *слайди презентації в форматі Power Point (назва роботи, вступ та мета роботи, аналітичний огляд аналогів, апаратна конфігурація сервера моніторингу, алгоритм роботи та логіка оповіщення, шаблони вузлів, візуалізація метрик, висновки)*

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Строк / терміни виконання етапів Роботи	Примітка
1	Аналіз завдання та літературних джерел у галузі ЦОД	19.05.2026-28.05.2026	Виконано
2	Огляд архітектури ДБЖ та підсистем автономного енергозабезпечення серверних	29.05.2026-04.06.2026	Виконано
3	Розробка структурної схеми системи	05.06.2026-11.06.2026	Виконано
4	Обґрунтування та вибір датчиків мікроклімату	12.06.2026-13.06.2026	Виконано
5	Проєктування апаратної частини на базі STM32 Nucleo	14.06.2026-20.06.2026	Виконано
6	Розробка програмного забезпечення мікроконтролера	21.06.2026-24.06.2026	Виконано
7	Проведення випробувань системи	25.06.2026 27.06.2026	Виконано
8	Висновки	28.06.20 26	Виконано
9	Оформлення пояснювальної записки	29.06.2026	Виконано

Дата видачі завдання *18 травня* 20 26 р.

Здобувач _____
(підпис)

Керівник роботи _____ доц. каф. ІМІ, Станіслав ІВАНЕНКО
(підпис) (посада, власне ім'я, прізвище)

РЕФЕРАТ

Пояснювальна записка 94 с., 27 рис., 9 табл., 5 додатків, 31 джерело.

Об'єкт роботи – мікроклімат серверної кімнати, підсистема автономного електроживлення.

Мета роботи – проєктування та реалізація комплексної IoT-системи моніторингу параметрів навколишнього середовища серверної кімнати та її автономного енергозабезпечення на базі мікроконтролера STM32.

Актуальність теми зумовлена потребою підприємств у забезпеченні безперервності й стабільності функціонування критичної IT-інфраструктури в умовах енергетичної нестабільності, що вимагає впровадження гнучких, масштабованих та економічно доцільних інструментів автоматизованого контролю з відкритим кодом.

У кваліфікаційній роботі здійснено системний аналіз функціональних можливостей та архітектурних обмежень комерційних промислових систем моніторингу (APC NetBotz, UniPing, Didactum). На основі міжнародного стандарту ANSI/TIA-942 обґрунтовано вимоги до відмовоустійкості інфраструктури рівня між TIER II та TIER III. Розроблено та реалізовано апаратний прототип системи на базі мікроконтролера STM32 (Nucleo-144), підключеного до масиву первинних цифрових та аналогових перетворювачів за інтерфейсами GPIO, One-Wire та I2C. Спроектовано трирівневий ешелонований контур гарантованого електроживлення, який поєднує промислові ДБЖ подвійного перетворення, дизель-генераторну установку та автономний сонячний вузол потужністю 300 Вт на базі акумулятора LiFePO4.

Виявлено та формалізовано ключові проблеми, зокрема: висока вартість і пропрієтарна закритість комерційного заліза. Запропоновано комплексні технічні рішення, що включають алгоритми граничних обчислень на боці мікроконтролера, оптимізацію передачі JSON-пакетів через Zabbix Sender виключно за фактом тривожних подій. Доведено економічну ефективність розробки, яка знижує витрати порівняно з ринковими аналогами.

ІНТЕРНЕТ РЕЧЕЙ (IoT), МІКРОКОНТРОЛЕР STM32, ZABBIX SENDER, СЕРВЕРНА КІМНАТА, АВТОНОМНЕ ЖИВЛЕННЯ, СОНЯЧНА ПАНЕЛЬ, МОНІТОРИНГ МІКРОКЛІМАТУ

THE ABSTRACT

Explanatory note: 94 p., 27 fig., 9 tab., 5 apps, 31 sources.

Object of study – server room microclimate, autonomous power supply subsystem.

Objective of the study – design and implementation of a comprehensive IoT-based system for monitoring server room environmental parameters and its autonomous power supply based on the STM32 microcontroller.

Relevance of the topic is driven by the enterprises' need to ensure the continuity and stability of critical IT infrastructure operations under conditions of power instability, which requires the implementation of flexible, scalable, and cost-effective open-source automated control tools.

In the qualification framework, a system analysis of the functional capabilities and architectural limitations of commercial industrial monitoring systems (APC NetBotz, UniPing, Didactum) has been carried out. Based on the international ANSI/TIA-942 standard, the infrastructure resilience requirements for levels between TIER II and TIER III have been substantiated. A hardware prototype of the system has been developed and implemented based on the STM32 microcontroller (Nucleo-144) connected to an array of primary digital and analog transducers via GPIO, One-Wire, and I2C interfaces. A three-level tiered guaranteed power supply circuit has been designed, which combines industrial double-conversion UPS, a diesel generator set, and an autonomous 300 W solar node based on a LiFePO4 battery.

Key issues have been identified and formalized, in particular: high cost and proprietary enclosure of commercial hardware. Comprehensive technical solutions have been proposed, including edge computing algorithms on the microcontroller side and optimization of JSON packet transmission via Zabbix Sender exclusively upon the occurrence of alarm events. The economic efficiency of the development has been proven, as it reduces costs compared to market counterparts.

INTERNET OF THINGS (IoT), STM32 MICROCONTROLLER, ZABBIX SENDER, SERVER ROOM, AUTONOMOUS POWER SUPPLY, SOLAR PANEL, MICROCLIMATE MONITO

ЗМІСТ

ПЕРЕЛІК ПОЗНАЧЕНЬ ТА СКОРОЧЕНЬ……..9
ВСТУП……12
1 АНАЛІЗ СУЧАСНИХ ТЕНДЕНЦІЙ РОЗВИТКУ IoT ДЛЯ ДАТА-ЦЕНТРІВ.14
1.1 Класифікація надійності дата-центрів за рівнями TIER та їх вимоги до систем моніторингу мікроклімату…….16
1.2 Контроль показників стану середовища……19
1.3 Аналітичний огляд існуючих рішень: функціонал, переваги та недоліки……..22
1.4 Формулювання наукової проблематики та постановка завдання розробки альтернативної системи…….27
2 РОЗРОБКА ТА РЕАЛІЗАЦІЯ КОНЦЕПЦІЇ АЛЬТЕРНАТИВНОЇ IoT-СИСТЕМИ МОНІТОРИНГУ……...29
2.1 Склад і взаємодія апаратних компонентів системи……...30
2.1.1 Датчики та сенсорні модулі……31
2.1.2 Огляд систем безперебійного живлення (ДБЖ) та підсистеми автономного енергозабезпечення……..35
2.2 Структурна схема системи в Packet Tracer та її принцип роботи…….42
2.3 Вибір апаратної частини……...45
2.4 Алгоритмічне забезпечення та логіка роботи системи……..50
2.5 Налаштування комунікаційних протоколів……53
2.6 Аналіз працездатності датчиків у складі системи ...…….55
2.7 Обґрунтування доцільності розробки альтернативного рішення…….56
3 ОЦІНКА ЕФЕКТИВНОСТІ ТА ПОРІВНЯЛЬНИЙ АНАЛІЗ РОЗРОБЛЕНОЇ СИСТЕМИ……..60
3.1 Технічні та експлуатаційні переваги розробленого рішення……60
3.2 Недоліки та шляхи вдосконалення……..63
3.3 Порівняльний аналіз із промисловими комерційними аналогами…...63
ВИСНОВКИ……...……69

ПЕРЕЛІК ПОСИЛАНЬ……71
ДОДАТОК А – ПРИКЛАД РОБОТИ ГЕРКОНІВ……..75
ДОДАТОК Б – ПРОГРАМНА РЕАЛІЗАЦІЯ НАДСИЛАННЯ ІНФОРМАЦІЇ СТАНУ НА СЕРВЕР ……..……...76
ДОДАТОК В – ПОВНИЙ ЛІСТІНГ ПРОГРАМИ МОНІТОРИНГУ СЕРВЕРНОЇ КІМНАТИ ……..79
ДОДАТОК Г – СЛАЙДИ ПРЕЗЕНТАЦІЇ……..88
ДОДАТОК Д – ТЕЗИ НА ММФ……...…...94

ПЕРЕЛІК ПОЗНАЧЕНЬ ТА СКОРОЧЕНЬ

АКБ - Акумуляторна батарея

АВР - автоматичне введення резерву

АЦП - Аналого-цифровий перетворювач

ДБЖ - Джерело безперебійного живлення

ДГУ- Дизельно-генераторна установка

ДСТУ - Державний стандарт України

ДБН - Державні будівельні норми

ДЦ - Дата-центр (Центр обробки даних)

IoT (Internet of Things) - Інтернет речей

IT (Information Technology) - Інформаційні технології

ККД - Коефіцієнт корисної дії

ПЗ - Програмне забезпечення

ЦАП - Цифро-аналоговий перетворювач

ЦОД - Центр обробки даних

ANSI (American National Standards Institute) - Американський національний інститут стандартів

API (Application Programming Interface) - Інтерфейс прикладного програмування

ARP (Address Resolution Protocol) - Мережевий протокол визначення адреси

ASHRAE - Американське товариство інженерів з опалення, охолодження та кондиціювання повітря

BIG DATA - (Великі данні) - Великі обсяги інформації

BMS (Battery Management System) - Система керування та захисту акумуляторної батареї

CO2 - Вуглекислий газ

CPU (Central Processing Unit) - Центральний процесор

DC/AC - Перетворювач постійного струму в змінний (Інвертор)

DC/DC - Перетворювач постійного струму в постійний зі зміною рівня напруги

DMA (Direct Memory Access) - Прямий доступ до пам'яті

EN (European Norm) - Європейський стандарт

ESD (Electrostatic Discharge) - Електростатичний розряд

FPU (Floating Point Unit) - Апаратний модуль математичних обчислень із плаваючою комою

GPIO (General Purpose Input/Output) - Порти введення-виведення загального призначення

HTTP (HyperText Transfer Protocol) - Протокол передачі гіпертексту

I2C (Inter-Integrated Circuit) - Послідовний асиметричний шинний протокол зв'язку між інтегральними схемами

ICMP (Internet Control Message Protocol) - Протокол міжмережевих керуючих повідомлень

ISO (International Organization for Standardization) - Міжнародна організація зі стандартизації

JSON (JavaScript Object Notation) - Текстовий формат обміну даними

LiFePO4 - Літій-залізо-фосфатний акумулятор

LwIP (Lightweight IP) - Оптимізований легковажний стек протоколів TCP/IP для вбудованих систем

MAC (Media Access Control) - Апаратний контролер рівня управління доступом до середовища

MQTT (Message Queuing Telemetry Transport) - Спрощений мережевий протокол, поверх TCP/IP для обміну повідомленнями між IoT-пристроями

MPPT (Maximum Power Point Tracking) - Слідкування за точкою максимальної потужності сонячної панелі

PDU (Power Distribution Unit) - Інтелектуальний розподільник живлення

PWM (Pulse-Width Modulation) - ШИМ (Широтно-імпульсна модуляція) / тип контролера заряду

RMII (Reduced Media Independent Interface) - Скорочений інтерфейс незалежного від середовища управління передачею даних (між MAC та PHY)

RTC (Real-Time Clock) - Апаратний годинник реального часу

SNMP (Simple Network Management Protocol) - Протокол мережевого управління

SPI (Serial Peripheral Interface) - Послідовний синхронний протокол передачі даних

TCP/IP (Transmission Control Protocol / Internet Protocol) - Набір мережевих протоколів передачі даних

TIA (Telecommunications Industry Association) - Асоціація телекомунікаційної індустрії

TVOC (Total Volatile Organic Compounds) - Сумарна концентрація летких органічних сполук

UART/USART (Universal Synchronous/Asynchronous Receiver-Transmitter) - Універсальний синхронно-асинхронний приймачі-передавач

USB OTG (Universal Serial Bus On-The-Go) - Розширення специфікації USB для легкого з'єднання периферійних пристроїв між собою без ПК

ВСТУП

В останні роки інформаційні технології стали одним із ключових чинників розвитку сучасного суспільства. Такі критичні цифрові сервіси як: хмарні платформи, банківські системи, електронне урядування, засоби зв'язку - залежать від стабільної роботи дата-центрів. Серверні кімнати, у яких розміщується це обладнання, повинні функціонувати цілодобово, безперервно та з високим рівнем надійності. Однак надійність дата-центрів напряму залежить від стану мікроклімату, стабільності електроживлення і фізичної безпеки приміщення.

В теперішніх умовах енергетичної нестабільності, забезпечення безперервної роботи серверних кімнат набуває критичного значення. Часті відключення електроенергії призводять до зупинки серверів, втрати даних, виходу з ладу обладнання через перепади напруги.

Окрім того, на даний час є актуальні кіберфізичні загрози, коли цифровий вплив набуває фізичних наслідків. Наприклад, зловмисник може дистанційно підвищити температуру серверної або вимкнути системи охолодження, спричинивши перегрів і пошкодження серверів. Це ще один пункт, котрий вимагає нових підходів до моніторингу.

Розвиток технологій інтернету речей (IoT) відкриває можливості для створення розподілених систем моніторингу, які можуть збирати, передавати та аналізувати дані з десятків сенсорів у реальному часі. Такі системи дозволяють не лише контролювати параметри, але й передбачати аварійні ситуації за допомогою аналітики або машинного навчання.
Саме тому створення IoT-системи моніторингу параметрів середовища для серверної кімнати з інтеграцією ДБЖ (джерела безперебійного живлення) та альтернативного джерела енергії (сонячної панелі) є актуальним і значущим завданням сучасної інженерії.

Метою кваліфікаційної роботи є розробка комплексної IoT-системи моніторингу серверної кімнати, що забезпечує постійний контроль температури, вологості, концентрації CO_2, руху, стану дверей і енергоспоживання, а також має резервне живлення з можливістю підключення сонячного модуля для автономної роботи під час відключення електроенергії.

Для досягнення поставленої мети необхідно вирішити такі завдання:

1. Провести аналітичний огляд сучасних технологій моніторингу параметрів середовища та рішень IoT у контексті дата-центрів.
2. Розглянути існуючі типи джерел безперебійного живлення (ДБЖ) та систем автономного енергозабезпечення.
3. Обґрунтувати вибір сенсорів для контролю температури, вологості, CO_2, руху, відкриття дверей, диму тощо.
4. Обрати апаратну платформу.
5. Розробити апаратну схему з’єднання сенсорів, мікроконтролера та ДБЖ.
6. Реалізувати базову логіку програмного забезпечення для збору, обробки та передачі даних у локальну мережу або хмару.
7. Провести тестування.

У результаті виконання роботи очікується:

1. Розробка прототипу автономної IoT-системи моніторингу для серверної кімнати з можливістю передачі даних через Ethernet.
2. Підвищення рівня безпеки та надійності дата-центрів за рахунок безперервного збору даних про стан мікроклімату та живлення.

Таким чином, результати роботи матимуть практичну цінність для IT-підприємств.

1 АНАЛІЗ СУЧАСНИХ ТЕНДЕНЦІЙ РОЗВИТКУ IoT ДЛЯ ДАТА-ЦЕНТРІВ

В умовах цифрової залежності, серверні кімнати та дата-центри (ДЦ) перетворилися з допоміжних технічних приміщень на стратегічні вузли інфраструктури, що забезпечують безперервність бізнес-процесів, зберігання та обробку критичних даних. Зростання обсягів трафіку, впровадження хмарних обчислень, штучного інтелекту та аналізу "великих даних" (Big Data) висувають безпрецедентно високі вимоги до надійності, ефективності та керованості цієї інфраструктури.

Традиційні системи управління будівлями та регламентні огляди персоналом, виявляються не завжди неспроможними адекватно реагувати на динамічний характер сучасних ІТ-навантажень. Тому це створює слабкі ланки та несе колосальні ризики, адже вартість однієї хвилини простою дата-центру, за оцінками Uptime Institute, може сягати десятків тисяч доларів [1].

Відповіддю на цей виклик стала парадигма Інтернету речей (IoT), яка докорінно змінює підхід до управління інфраструктурою, перетворюючи пасивне середовище на активний, "свідомий" організм. У цій сфері варто виділити інтеграцію великої кількості сенсорних вузлів, що контролюють критичні параметри – температуру, вологість, рівень шуму, струм навантаження, енергоспоживання та стан систем охолодження. Такі сенсори об’єднуються у єдину мережу, а зібрані дані передаються на сервер або у хмарну інфраструктуру для подальшого аналізу.

Аналіз сучасного стану галузі дозволяє виділити наступні ключові тенденції, що формують ландшафт сучасних систем моніторингу:

- Гіпергранулярність моніторингу мікроклімату. Це найбільш фундаментальний тренд. Замість одного-двох термостатів на приміщення, впроваджуються десятки, а іноді й сотні бездротових IoT-сенсорів температури, вологості, повітряного потоку, тиску та іншого. Вони розміщуються не лише в "холодних" та "гарячих" коридорах, а безпосередньо на рівні окремих стійок, на вході та виході серверного

обладнання. Це дозволяє створювати деталізовані теплові карти в реальному часі, миттєво ідентифікувати локальні гарячі точки та динамічно керувати системами кондиціонування, суттєво оптимізуючі ключовий показник енергоефективності.

- Інтелектуалізація моніторингу електроживлення. Ця тенденція є не менш важливою, адже переважна більшість збоїв у ДЦ прямо чи опосередковано пов'язана з проблемами живлення. Сучасні IoT-рішення виходять далеко за рамки простого пінгування ДБЖ. Вони передбачають глибокий моніторинг всієї лінії живлення: від вводу, стану дизель-генераторних установок (ДГУ) до навантаження на кожній окремій розумній розетці. Збираючи дані про напругу, струм, гармоніки, стан батарей ДБЖ, рівень палива в ДГУ тощо.
- Предиктивне обслуговування. Це логічний розвиток перших двох трендів. Збираючи величезні масиви даних з сенсорів, системи на базі машинного навчання здатні виявляти ледь помітні аномалії, що передують відмові обладнання. Це означає, що система здатна не лише фіксувати факт відхилення параметрів, а й прогнозувати можливі збої у роботі обладнання, що суттєво підвищує надійність функціонування дата-центрів. Наприклад, аналіз мікровібрацій та акустичного профілю вентилятора блоку кондиціонування може спрогнозувати вихід з ладу підшипника заздалегідь до фактичної зупинки. Це дозволяє інженерним службам діяти на випередження, таким чином максимізуючи аптайм.
- Попит на інтегровані платформи. Найбільшою проблемою для малих серверних кімнат є "зоопарк вендорів". Система моніторингу ДБЖ має свій інтерфейс, датчики клімату - свій, а контроль доступу - третій. Ключовий тренд сьогодення - це потреба в єдиній, гнучкій IoT-платформі, яка здатна агрегувати дані з усіх підсистем. Саме така інтеграція дозволяє бачити зв’язок подій: наприклад, як просідання напруги впливає на зростання температури процесорів і як це пов'язано з відкриттям дверей до стійки тощо.

Сучасні IoT-технології надають потужний інструментарій для забезпечення безпрецедентного рівня контролю, надійності та ефективності серверних приміщень. Технологічною основою таких систем є мікроконтролери та одноплатні комп'ютери, зокрема STM32, Arduino або Raspberry Pi, які забезпечують високу гнучкість, енергоефективність і можливість створення кастомізованих рішень. Вони легко інтегруються із веб-інтерфейсами та мобільними застосунками, що спрощує віддалений моніторинг і керування [2]. Всі ці інновації розробляються з однією ключовою метою: гарантувати, що фізичне середовище всередині серверної кімнати буде стабільно та неухильно відповідати стандартам, що висуваються до мікроклімату та фізичної безпеки сучасних серверних приміщень.

1.1 Класифікація надійності дата-центрів за рівнями TIER та їх вимоги до систем моніторингу мікроклімату

Серверні приміщення та дата-центри є критичними об'єктами інформаційної інфраструктури, від безперебійної роботи яких залежить стабільність бізнес-процесів, збереження даних і функціонування цифрових сервісів. Надійність роботи обладнання у таких приміщеннях визначається не лише якістю технічного оснащення, а й ефективністю систем моніторингу, які забезпечують контроль параметрів мікроклімату, електроживлення та фізичної безпеки.

В Україні на даний момент не існує окремого державного стандарту, який би повністю регламентував проектування, побудову та експлуатацію дата-центрів. Тому переважна більшість орієнтується на міжнародні стандарти, зокрема на ANSI/TIA-942 [3]: Telecommunications Infrastructure Standard for Data Centers, розроблений Telecommunications Industry Association (США).

Стандарт TIA-942 описує:

- архітектуру інженерних систем дата-центру;

- вимоги до електроживлення, охолодження, безпеки та структурованих кабельних систем;
- принципи резервування і безперервності роботи;
- класифікацію надійності за рівнями TIER I–IV, які визначають ступінь відмовостійкості об’єкта.

Система класифікації TIER, запропонована Uptime Institute та визначає технічну складність, ступінь відмовостійкості, загальний рівень надійності дата-центру та дозволяє визначити вимоги до систем моніторингу і резервування. Ця класифікація дає змогу оцінити, наскільки надійно захищені розміщені в центрі обробки даних інформаційні ресурси, та безперервно працює його інфраструктура [4].

Рівень TIER I. Є мінімальним стандартом для дата-центрів. Відмовостійкість системи становить близько 99,671%, що відповідає приблизно 28–29 годинам простою на рік.

У таких центрах відсутнє резервування основних підсистем. Будь-який збій у роботі обладнання (джерела живлення, системи охолодження тощо) призводить до повної зупинки серверів. Базові вимоги до моніторингу: контроль температури, вологості та електроживлення. TIER I використовується здебільшого у невеликих компаніях або тестових середовищах, де короткочасна зупинка не спричиняє значних збитків.

TIER II - базове резервування. Цей рівень передбачає часткове дублювання активного обладнання: блоків безперебійного живлення, систем кондиціонування, енергопостачання. Рівень відмовостійкості зростає до 99,749%, тобто допускається близько 22 годин простою на рік. Попри наявність базового резерву, будь-який критичний збій все ще може призвести до тимчасової зупинки серверів. Необхідно контролювати стан усіх основних вузлів: кондиціонерів, ДБЖ, розподільчих щитів. Цей рівень характерний для організацій середнього рівня, які прагнуть підвищити надійність інфраструктури без значних інвестицій.

TIER III - високий рівень надійності. Дата-центри TIER III мають повну схему резервування систем охолодження, електроживлення та комунікацій. Відмовостійкість таких центрів становить 99,982%, що означає лише приблизно 1,6 години (96 хвили н) простою на рік. Головна перевага - це можливість проведення профілактичних або ремонтних робіт без зупинки сервісів, але вимоги до моніторингу теж високі: цілодобовий контроль усіх параметрів, автоматичне сповіщення про збої, автономна робота при відключенні енергії. TIER III є найпоширенішим рівнем у світі: він забезпечує баланс між вартістю будівництва, енергоефективністю та стабільністю. Цей стандарт обирають більшість комерційних дата-центрів, що обслуговують середній і великий бізнес [5].

TIER IV - найвищий рівень надійності. Рівень TIER IV забезпечує максимальний ступінь відмовостійкості - 99,995%, тобто не більше 26 хвилин простою на рік, тому що всі критичні компоненти(контури живлення, охолодження й зв'язку) не лише зарезервовані, а й дублюються за схемою "2N+1", тобто кожен вузол має свого "близнюка" та автоматично перемикается на резерв.

$$2N+1; \tag{1.1}$$

де N – базова потреба в обладнанні ЦОД;

2N -повне дублювання;

+1 – додатковий резерв.

Система має два повністю дубльованих канали живлення та охолодження, де в кожному каналі додатково закладено по одному резервному пристрою на випадок ремонту. Такий підхід дозволяє проводити будь-які технічні або планові роботи без переривання роботи серверів [6]. Система моніторингу має бути інтегрована з усіма інженерними підсистемами й здатна до самодіагностики. TIER IV застосовується для стратегічно важливих об'єктів – урядових структур, військових систем, великих корпорацій.

Також існує комплекс документів, що частково регулюють окремі аспекти проектування. До національних стандартів, що частково імплементують вимоги TIA-942 належать такі чинні нормативні документи:

- ДСТУ EN 50600 [7]. У ньому встановлено вимоги до архітектури дата-центрів, рівнів відмовостійкості, систем моніторингу, безпеки та управління інфраструктурою;
- ДСТУ ISO/IEC 30134 [8]. Стандарт визначає основні показники енергоефективності і встановлює методи оцінювання надійності та сталості функціонування ЦОДів;
- ДСТУ ISO/IEC 11801-1:2019 [9]. Загальні вимоги до структурованих кабельних систем. Документ регламентує проєктування телекомунікаційних і мережевих систем у будівлях, офісах і дата-центрах, забезпечуючи сумісність та надійність кабельної інфраструктури;
- ДБН В.2.5-27:2006 [10]. Цей норматив встановлює вимоги до систем електроживлення, включаючи резервування, заземлення, захист від перевантажень та безпеку експлуатації електричних мереж.

Будь-які відхилення від оптимальних умов можуть спричинити підвищене енергоспоживання, збої в роботі, передчасний вихід із ладу електронних компонентів або навіть втрату даних. Тому підтримання стабільних температурно-вологісних режимів є ключовим завданням систем моніторингу.

1.2 Контроль показників стану середовища

Температура повітря це основний параметр, що визначає тепловий баланс серверного обладнання. Процесори, блоки живлення та дискові системи виділяють велику кількість тепла. Будь-який працюючий сервер виділяє обсяг тепла, що майже повністю еквівалентний його електричній потужності. Якщо

кліматична система не справляється з відведенням цього теплового потоку, температура всередині монтажної шафи миттєво зростає, створюючи ризик перегріву. Згідно з рекомендаціями ДСТУ EN 50600-2-3:2018, оптимальна температура на вході в сервер становить 18–27 °C. Перевищення цих значень призводить до перегріву процесорів, збільшення шумів у блоках живлення і деградації компонентів [11].

Підвищення температури всього на 10 °C скорочує термін служби електролітичних конденсаторів у два рази. Тривале перебування при 35–40 °C призводить до деградації ізоляції, перегріву процесорів і появи помилок у пам’яті. Як приклад: у дата-центрі Google одна з систем охолодження центру обробки даних, включаючи резервні, вийшла з ладу. Це змусило компанію вимкнути свої сервери [12]. Так само надмірно низька температура також небезпечна, оскільки спричиняє конденсацію вологи на металевих поверхнях і платах під час циклів охолодження-нагрівання.

Відносна вологість безпосередньо впливає на електричну стабільність середовища в серверній кімнаті. Вологість у межах 40–55 % , а точка роси 5–15 °C, забезпечує стабільну роботу електронних систем і запобігає як утворенню статичних розрядів, так і появі конденсату. При низькій вологості (<30%) повітря стає сухим, і зростає ризик накопичення статичної електрики (ESD). Один електростатичний розряд у 100 В може бути непомітним для людини, але цього достатньо, щоб пошкодити мікросхему на платі.

При підвищеній вологості (>60%) виникає інша загроза – конденсація. Волога осідає на контактах, що призводить до корозії, коротких замикань або збоїв у сигнальних лініях. Наприклад, при вологості понад 70 % на холодних ділянках(у зонах подачі повітря) може утворюватися тонка плівка води, яка знижує опір ізоляції й провокує короткі замикання [13]. Завдяки безперервному моніторингу можна вчасно виявити тенденцію до пересушування або надмірної вологості повітря, що є критичним для обладнання.

Якість повітря. Пил це одна з найчастіших причин перегріву і зниження ефективності охолодження. Навіть тонкий шар пилу на лопастях вентилятора або радіаторі – знижує тепловідвід на 15–25 %. Крім того, пил може накопичувати електричний заряд і провокувати локальні розряди.

Згідно з вимогами EN 50600-2-3, повітря в серверній має відповідати не більше 3,5 млн частинок розміром >0,5 мкм на м³ [14]. У 2021 році один із українських ЦОДів у місті Київ фіксував часті помилки читання дисків через перегрів жорстких дисків. Причиною виявилася засміченість повітряних фільтрів і відсутність очищення внутрішніх вентиляторів серверів. Після заміни фільтрів та встановлення системи моніторингу чистоти повітря показник стабільності системи зріс на 17 %. Тому вентиляційні системи повинні бути оснащені фільтрами та регулярно обслуговуватися.

Рівномірність розподілу повітря теж відіграє важливу роль в стабільності мікроклімату. При високій швидкості (>0.7 м/с) виникає турбулентність, що створює “мертві зони” охолодження, а при низькій швидкості (<0.2 м/с) гаряче повітря накопичується між стійками, утворюючи “гарячі точки” з температурою на 10–15 °C вище середньої. Виходячи з цього, можна створити таблицю-висновок для наочності.

Таблиця 1.1 – Оптимальні значення та наслідки при відхиленні

Параметр	Оптимальне значення	Критичні наслідки
Температура	18-27 C°	Перегрів, вихід з ладу конденсаторів
Вологість	40-55 %	Електростатичний розряд, конденсація, корозія контактів
Якість повітря		Осідання пилу, перегрів
Швидкість повітря	0.25-0.5 м/с	турбулентність або перегрів

Як видно з приклада, відхилення від норм може призвести до серйозних наслідків і нестабільної роботи систем в цілому. Саме тому впроваджують автоматизовані IoT-системи моніторингу, які постійно відстежують температуру, вологість, чистоту повітря та роботу охолоджувального обладнання.

1.3 Аналітичний огляд існуючих рішень їх функціонал, переваги та недоліки

Моніторинг параметрів серверних кімнат є критично важливим завданням для збереження обладнання. Порушення температурного режиму, підвищена вологість, проблеми з електроживленням або фізичний доступ до обладнання можуть призвести до аварійних ситуацій і втрати даних. З цієї причини на ринку представлено широкий спектр апаратно-програмних рішень для контролю мікроклімату та інженерної інфраструктури серверних приміщень.

Серед найбільш поширених комерційних систем моніторингу виділяються APC NetBotz, UniPing та Didactum які відрізняються рівнем функціональності, масштабованістю та вартістю. UniPing орієнтований на базові задачі моніторингу та використовується переважно у малих серверних кімнатах. Didactum є професійним рішенням промислового рівня, призначеним для великих дата-центрів і складних інженерних систем. APC NetBotz належить до корпоративних рішень і тісно інтегрується з інфраструктурою електроживлення та системами керування від компанії Schneider Electric.

Комерційний статус цих продуктів не позбавляє їх певних недоліків. Головними серед них є висока вартість, закрита архітектура та обмежений потенціал для кастомізації під індивідуальні потреби. У зв’язку з цим актуальним є напрям розробки IoT-систем моніторингу, що базуються на принципах відкритої архітектури та використанні недорогих мікроконтролерів.

Такі системи дозволяють поєднати функціональність класичних рішень із сучасними методами аналітики та прогнозування.

Аналіз існуючих рішень дозволяє визначити сильні сторони сучасних рішень, а також виявити функціональні обмеження, які доцільно усунути під час розроблення власної IoT-системи, яка здатна адаптуватись до змін умов експлуатації та інтегруватися з сучасними інформаційними платформами.

Система UniPing. Є універсальним мережевим контролером, орієнтованим на моніторинг температури, вологості, наявності води, диму, відкриття дверей, а також контроль електроживлення. Пристрій підтримує роботу з широким спектром цифрових і аналогових датчиків, має вбудований веб-інтерфейс та підтримку протоколів SNMP, HTTP, SMTP та інші. Серед переваг UniPing слід відзначити простоту налаштування, можливість надсилання сповіщень через електронну пошту або SNMP traps, а також автономність у разі втрати зв’язку з сервером. Водночас недоліком є обмежена кількість підключених сенсорів і слабка масштабованість при розширенні системи (рис.1.1). Крім того, відсутність сучасних хмарних функцій аналітики та мобільних застосунків знижує гнучкість експлуатації в умовах віддаленого керування [14].

Переваги UniPing:

- простота встановлення та експлуатації;
- підтримка стандартних мережевих протоколів;
- сумісність із поширеними системами моніторингу;
- Підтримка стандартних протоколів, сумісність із системами моніторингу Zabbix, PRTG, Nagios тощо.



Рисунок 1.1 – Пристрій UniPing Server Solution v3

Недоліки UniPing:

- обмежена масштабованість в кількості сенсорів;
- відсутність хмарної аналітики;
- закрита апаратна архітектура [15];

Система Didactum Monitoring System. Належить до більш розвиненого класу професійних рішень, що забезпечують комплексний моніторинг середовища серверних кімнат і критичних об’єктів (рис.1.2). Пристрій підтримує багатоканальну роботу з різними типами сенсорів: температури, вологості, диму, відкриття дверей, протікання, струму та напруги. Його програмне забезпечення дозволяє створювати логічні сценарії реагування: автоматичне ввімкнення охолодження, сповіщення через SMS або SNMP, запис даних у журнал подій, але обробка даних здійснюється переважно на рівні класичного порогового та статистичного аналізу.



Рисунок 1.2 – Пристрій Didactum PDU 4T

Система фіксує поточні значення параметрів, зберігає їх історію та відображає у вигляді графіків, однак не виконує глибокого аналізу даних із застосуванням методів машинного навчання або штучного інтелекту. Didactum реагує на події за заздалегідь заданими правилами, наприклад при перевищенні встановленого температурного порога формується тривожне сповіщення або запускається відповідний сценарій автоматизації. Водночас система не здатна самостійно прогнозувати можливі відмови обладнання, оцінювати ймовірність аварійних ситуацій на основі історичних даних або адаптувати порогові значення залежно від зміни умов експлуатації. Крім того, аналіз параметрів здійснюється ізольовано, без урахування складних взаємозв'язків між ними. Наприклад, одночасні зміни температури, вологості та навантаження на електроживлення не розглядаються як комплексний процес із пошуком першопричини проблеми. Таким чином, аналітика Didactum виконує функцію контролю та сигналізації, але не забезпечує інтелектуальної підтримки прийняття рішень і випереджувального виявлення потенційних загроз, що обмежує її можливості у порівнянні з сучасними IoT-платформами з розвиненими аналітичними модулями [16].

Перевагою Didactum є наявність резервного живлення, підтримка протоколів безпеки та можливість інтеграції з системами керування будівлею (BMS). Однак, як і у випадку з UniPing, система характеризується високою вартістю та закритістю архітектури де користувач не має можливості гнучкого доопрацювання функціоналу або розширення кількості підключених вузлів без використання фірмових модулів. Це створює залежність від виробника і обмежує впровадження в умовах індивідуальних проєктів.

Переваги Didactum:

- висока надійність і промислове виконання;
- модульність і масштабованість;
- підтримка автоматизованих сценаріїв;
- резервне живлення та захист від збоїв.

Недоліки Didactum:

- висока вартість пристроїв і сенсорів, що ускладнює впровадження у підприємствах;
- використання пропрієтарних компонентів – неможливість підключення сторонніх сенсорів;
- закрита програмна архітектура, що обмежує адаптацію під нестандартні завдання;
- обмежені можливості інтелектуальної аналітики.

APC NetBotz. Система побудована за принципом централізованого апаратно-програмного комплексу для безперервного моніторингу фізичного середовища серверних кімнат і дата-центрів. Система використовує закриту архітектуру та пропрієтарні протоколи взаємодії, що забезпечує високий рівень захисту даних і стабільність роботи, але водночас обмежує можливість інтеграції сторонніх сенсорів і програмних модулів (рис.1.3). Виробник робить акцент на єдиній екосистемі Schneider Electric, у межах якої NetBotz є складовою частиною платформи керування інженерною інфраструктурою. Система підтримує всі необхідні сенсори, забезпечує централізований моніторинг та керування через спеціалізоване програмне забезпечення, а також підтримує хмарну інфраструктуру виробника. Основна увага приділяється надійності та безпеці корпоративного рівня [17].



Рисунок 1.3 – Пристрій APC NetBotz 250

Принцип роботи APC NetBotz базується на постійному опитуванні підключених датчиків і порівнянні отриманих значень із заздалегідь

визначеними порогами. Значну увагу приділено інтеграції з джерелами безперебійного живлення, розподільниками живлення та іншими елементами інфраструктури APC, що дозволяє отримувати комплексне уявлення про стан серверної кімнати з точки зору як мікроклімату, так і електроживлення. Таким чином, APC NetBotz функціонує як надійне централізоване рішення для контролю середовища серверних приміщень. Водночас закритість архітектури та обмежена гнучкість роблять систему менш придатною для адаптації під нестандартні завдання або інтеграції з відкритими IoT-платформами, що є важливим чинником при виборі рішення для малих і середніх серверних кімнат.
Переваги APC NetBotz:

- висока стабільність і безпека;
- інтеграція з UPS та системами живлення;
- централізоване керування.

Недоліки APC NetBotz:

- дуже висока вартість;
- залежність від одного виробника;
- обмежена гнучкість конфігурації;
- закрита екосистема.

1.4 Формулювання наукової проблематики та постановка завдання розробки альтернативної системи

Існуючі промислові системи моніторингу хоча й характеризуються високою надійністю та стабільністю але мають обмежену гнучкість, закриту архітектуру та значну вартість впровадження (рис.1.4). Їхні функціональні можливості зводяться до збирання базових параметрів середовища та передавання даних до зовнішніх платформ, без розширених засобів аналітики, автономного прийняття рішень або інтеграції з альтернативними джерелами живлення.

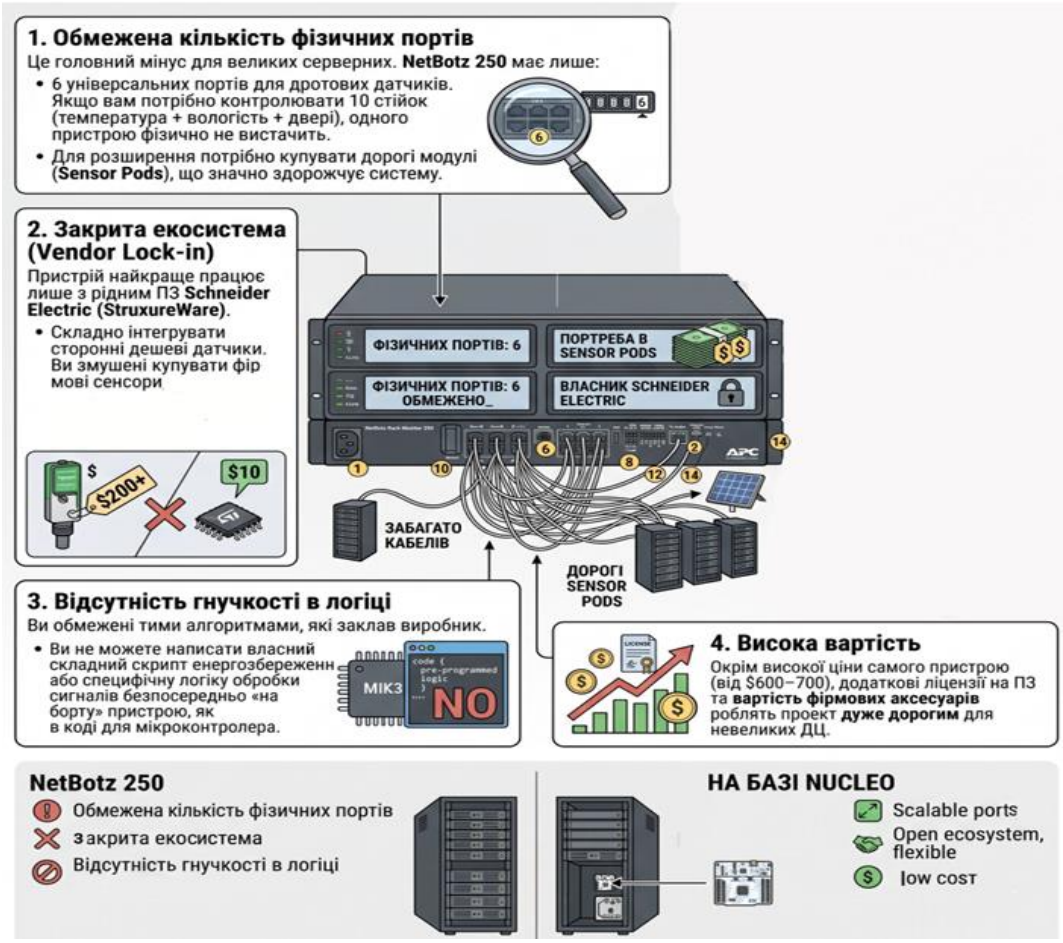


Рисунок 1.4 – Обмеження комерційного продукту

2 РОЗРОБКА ТА РЕАЛІЗАЦІЯ КОНЦЕПЦІЇ АЛЬТЕРНАТИВНОЇ IoT-СИСТЕМИ МОНІТОРИНГУ

У даному розділі розглядається процес розробки та реалізації концепції альтернативної IoT-системи моніторингу серверної інфраструктури. Основна увага приділяється формуванню архітектури системи, вибору апаратних і програмних компонентів, а також принципам їх взаємодії для забезпечення безперервного контролю критичних параметрів.

Розроблювана IoT-система ґрунтується на модульному підході, що дозволяє забезпечити масштабованість, гнучкість та адаптацію до вимог серверних середовищ рівня між TIER II та TIER III. Концепція системи передбачає розподілену структуру, у якій сенсорні вузли здійснюють збір первинних даних, мікроконтролерні платформи виконують їх попередню обробку, а серверна частина відповідає за зберігання, аналіз та візуалізацію інформації.

Головним елементом є використання доступних мікроконтролерних платформ і сенсорних модулів, що забезпечують контроль параметрів мікроклімату та електроживлення серверної інфраструктури. Для підвищення надійності роботи системи передбачено інтеграцію з системами безперебійного живлення, що дозволяє підтримувати працездатність моніторингу навіть у разі перебоїв електропостачання [18].

Передача даних між компонентами IoT-системи здійснюється з використанням стандартних протоколів обміну даними, що спрощує інтеграцію системи з існуючою IT-інфраструктурою. Особлива увага приділяється своєчасному виявленню аварійних ситуацій та формуванню сповіщень для оперативного реагування. Запропонована концепція створює основу для подальшого розвитку функціональності, зокрема впровадження алгоритмів інтелектуального аналізу даних, прогнозування відмов та автоматизації процесів управління серверною інфраструктурою [19].

2.1 Склад і взаємодія апаратних компонентів системи

Архітектура розробленої системи дозволяє забезпечити відповідність вимогам стандарту TIA-942 щодо моніторингу критичної інфраструктури (Environmental Monitoring). Апаратна частина складається з функціональних підсистем: сенсорної мережі, підсистеми електроживлення, обчислювального ядра та виконавчих механізмів (рис.2.6) [20].

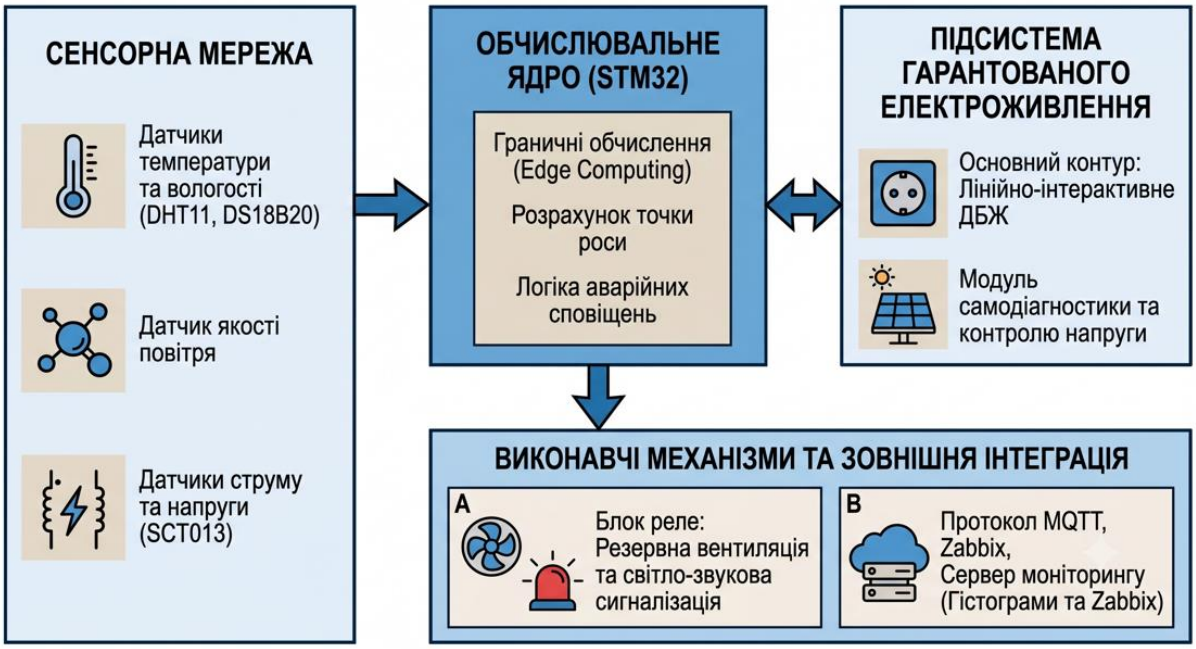


Рисунок 2.6 – Функціональна схема архітектури та взаємодії модулів IoT-системи

Організація роботи системи базується на чотирьох взаємопов'язаних підсистемах:

- Сенсорна мережа. Виступає первинною ланкою системи, що здійснює безперервний зйом фізичних параметрів середовища. Вона містить цифрові первинні перетворювачі температури та вологості (DHT та DS18B20), комбіновані сенсори якості повітря (CO2), а також аналогові трансформатори струму (SCT013) і вимірювачі напруги. Програма в STM32 за таймером або в головному циклі while(1) сама формує запит до

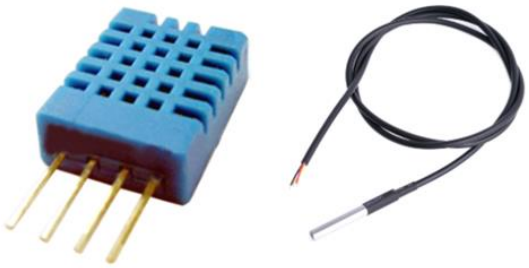
датчика. Датчик лише відповідає на цей запит, модулюючи рівень сигналу на лінії зв'язку.

- Обчислювальне ядро. Побудоване на базі мікроконтролера архітектури STM32. Ядро виконує первинну фільтрацію сигналів, математичний розрахунок точки роси для запобігання утворенню конденсату та реалізує алгоритми логічного аналізу аварійних подій (Edge Computing).
- Підсистема гарантованого електроживлення. Забезпечує високу відмовостійкість системи відповідно до вимог стандартів надійності TIER. Має гібридну структуру, що поєднує ДБЖ для штатного режиму та низьковольтний контур із резервним акумулятором (АКБ). Двосторонній зв'язок з обчислювальним ядром дозволяє не лише стабільно живити контролер, а й здійснювати безперервний програмний моніторинг залишкової ємності та напруги батарей через модуль самодіагностики.
- Виконавчі механізми та зовнішня інтеграція. Реалізує реакцію системи на виявлені девіації кліматичних параметрів. Підсистема розділена на два функціональні контури:
    - Контур А (Локальне автоматичне керування): за допомогою блоку силових реле здійснює комутацію резервної вентиляції при зафіксованому погіршенні якості повітря та активує локальну світло-звукову сигналізацію в разі виникнення критичних загроз;
    - Контур Б (Мережева інтеграція): використовуючи легковаговий протокол MQTT, здійснює передачу масивів телеметрії на сервер моніторингу Zabbix для довгострокового аналізу, побудови гістограм та генерації миттєвих сповіщень персоналу.

2.1.1 Датчики та сенсорні модулі

Датчики та сенсорні модулі відіграють ключову роль у системах моніторингу, оскільки забезпечують збір первинної інформації про стан навколишнього середовища та інженерних систем. До основних типів датчиків,

що використовуються у серверних середовищах, належать датчики температури та вологості (рис.2.7), які дозволяють контролювати мікроклімат серверної кімнати.



а б

Рисунок 2.7 – Різновидність датчиків температури:
а) датчик температури та вологості DHT11; б) водонепроникний датчик температури DS18B20.

Важливу роль також відіграють датчики електроживлення, зокрема вимірювачі напруги, струму та споживаної потужності. Вони дозволяють здійснювати моніторинг стану електричноїФ мережі, виявляти перевантаження та аномалії у роботі джерел живлення, у тому числі систем безперебійного живлення.



а б

Рисунок 2.8 – Вимірювачі напруги:
а) датчик змінного струму; б) вимірювальний трансформатор напруги.

На зображенні зображені два різні підходи до вимірювання струму. Кліщовий датчик струму (а), працює за трансформаторним принципом і дозволяє вимірювати змінний струм без фізичного розриву провідника. Це робить його безпечним у використанні та зручним для встановлення в діючих електрощитах і серверних шафах. Такі датчики використовуються для контролю навантаження, аналізу енергоспоживання та виявлення перевантажень у серверному обладнанні. Вони підходять виключно для змінного струму і не можуть застосовуватися для вимірювання постійного струму.

Другий елемент (б) є індуктивною котушкою або трансформатором струму без захисного корпусу. Він також реагує на магнітне поле, яке створюється струмом у провіднику, проте потребує більш уважного монтажу та додаткової ізоляції. Подібні елементи використовуються де важливі компактність і можливість інтеграції в апаратну схему. У порівнянні з кліщовими датчиками вони менш зручні для швидкого монтажу, але можуть забезпечувати вищу точність за правильної реалізації.

Для підвищення рівня безпеки серверних приміщень використовуються датчики відкриття дверей, руху та вібрації, які забезпечують контроль фізичного доступу до обладнання (рис.2.9). Такі сенсори дозволяють своєчасно виявляти несанкціонований доступ або інші потенційно небезпечні події.



Рисунок 2.9 – Приклад датчиків: а)датчик вібрації; б)герконовий датчик; в)доплерівський радар для контролю присутності

Модуль радара, що працює на ефекті Доплера, випромінює електромагнітні хвилі та приймає сигнал, відбитий від об’єктів. Якщо об’єкт

рухається, частота відбитої хвилі змінюється відносно випроміненої, і за цією різницею модуль визначає наявність та факт руху. Такі датчики здатні виявляти рух без прямого контакту й часто використовуються для контролю присутності людини або сторонньої активності в приміщенні.

Герконовий датчик складається з двох металевих контактів, запаяних у скляну колбу, які замикаються або розмикаються під дією магнітного поля. Коли поруч знаходиться магніт, контакти замикаються і фіксується подія. Найчастіше герконові датчики застосовуються для контролю відкриття дверей, люків або серверних шаф.

Датчик вібрації реагує на механічні коливання або удари, перетворюючи їх у електричний сигнал. Під час вібрації всередині датчика змінюється положення чутливого елемента, що призводить до спрацювання. Такі датчики використовуються для виявлення струсів, ударів або несанкціонованих дій із обладнанням серверних приміщень.

Датчики виявлення аварійних ситуацій (рис.2.10), зокрема сенсори задимлення, протікання води та наявності диму. Їх використання є критично важливим для запобігання пожежам та пошкодженню обладнання внаслідок аварій інженерних систем.



Рисунок 2.10 – Датчики аварійних ситуацій: а)датчик чадного газу CO; б)датчик рідини

Сучасні сенсорні модулі для IoT-систем моніторингу зазвичай підтримують стандартні інтерфейси підключення до мікроконтролерних платформ, що спрощує їх інтеграцію.

2.1.2 Огляд систем безперебійного живлення та підсистеми автономного енергозабезпечення

З метою підвищення рівня відмовостійкості інформаційної інфраструктури та забезпечення безперервності бізнес-процесів у проекті реалізовано концепцію рівневого енергозабезпечення з гібридною схемою із використанням масиву сонячних панелей та місткого літій-залізо-фосфатного (LiFePO4)буфера. Дана концепція передбачає фізичне та логічне розділення ліній живлення для важкого обчислювального навантаження серверів, загального комунікаційного обладнання та критичних вузлів моніторингу.

У штатному режимі електроенергія надходить від центральної електромережі через автоматичне введення резерву (ATS/ABP) на вхід центрального промислового ДБЖ з технологією подвійного перетворення (рис2.11,а). Це ДБЖ безперервно забезпечує якісним синусоїдальним сигналом критичні серверні стійки, включаючи критичний вузол де рзміщенно маршрутизатор Juniper та інші комутатори ядра.

Паралельно функціонує автономний сонячний контур. Масив сонячних панелей через гібридний інвертор здійснює постійне онлайн-живлення акумуляторної батареї. Головною особливістю штатного режиму є те, що інвертор активує режим Grid-Tie і безпосередньо підмішує генеровані сонячні вати в лінію змінного струму (AC) на вхід центрального ДБЖ, суттєво знижуючи споживання енергії з міської електромережі.

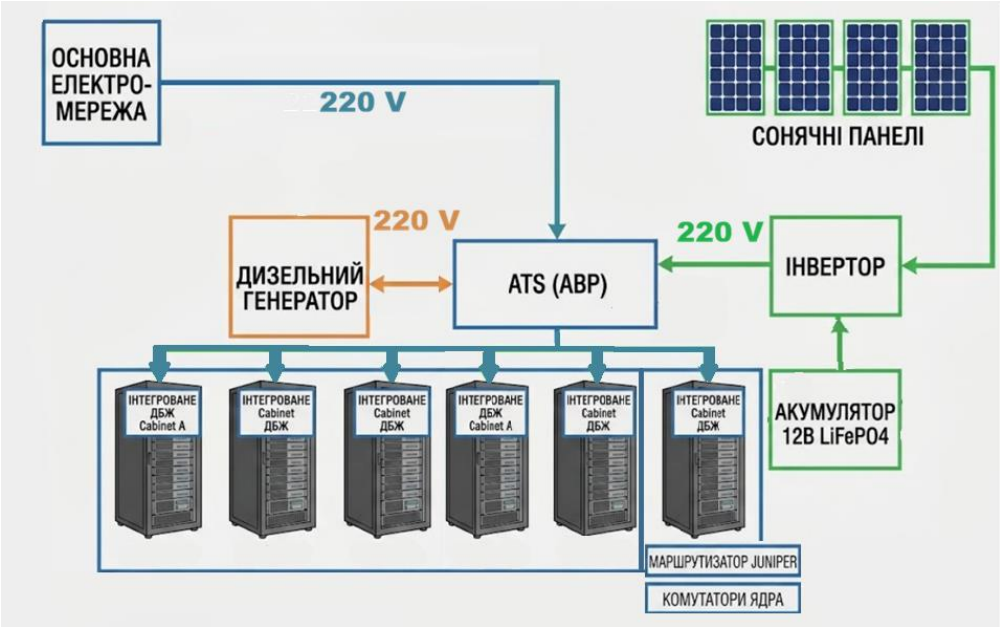


Рисунок 2.11(а) – Функціональна схема гібридної системи електроживлення у штатному режимі

У разі зникнення напруги в основній електромережі, система автоматично відпрацьовує каскадний алгоритм захисту:

- Перший етап. ДБЖ миттєво підхоплює все навантаження (сервери, маршрутизатор Juniper, комутатори).
- Другий етап. Модуль АВР фіксує аварію і через лінію керування ініціює запуск дизель-генераторної установки.
- Третій етап (критична ізоляція). На рисунку 2.11(б) відображено найгірший сценарій, коли паливо в ДГУ вичерпано або генератор зазнав аварії, а внутрішні ємності ДБЖ підійшли до критичного мінімуму. У цей момент автоматика знеструмлює другорядне навантаження (великі серверні групи перекреслені червоним хрестом). Вся потужність сонячного вузла та накопичена енергія з акумуляторів спрямовуються виключно на підтримання життєдіяльності ядра мережі (відмічено зеленою галочкою): маршрутизатора Juniper, комутаторів ядра та мікроконтролерного модуля моніторингу на базі STM32.

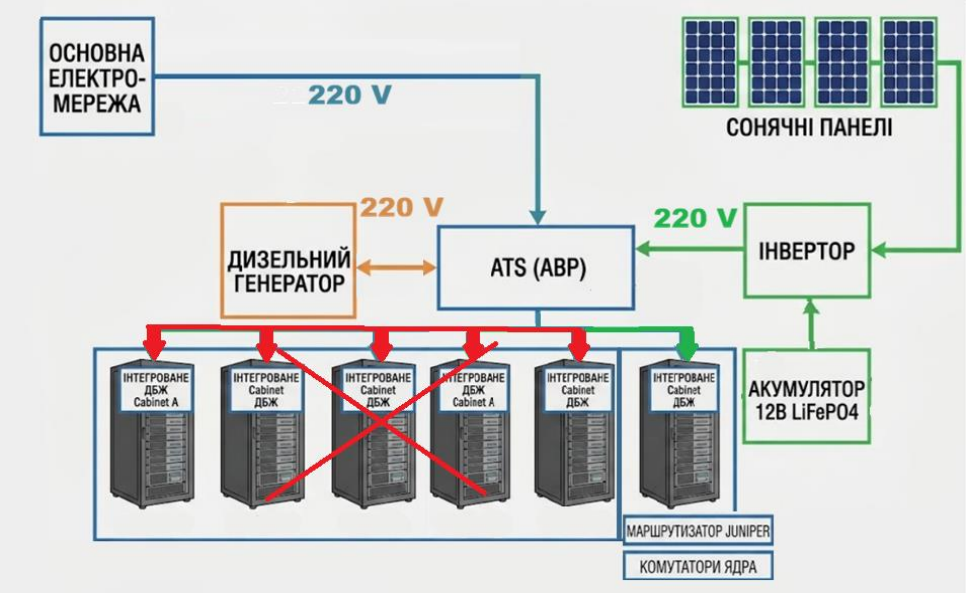


Рисунок 2.11 (б) – Функціональна схема гібридної системи електроживлення у нештатному режимі

Існуюча інфраструктура серверної кімнати базується на промислових джерелах безперебійного живлення з технологією подвійного перетворення (On-line Double Conversion). До цього обладнання належать стійкові ДБЖ GE Digital Energy VH Series та Legrand Daker DK Plus (рис. 2.12–2.13). Вони гарантують нульовий час перемикання, ідеальну синусоїду та повну фільтрацію високочастотних завад із мережі.



Рисунок 2.12 – ДБЖ GE Digital Energy



Рисунок 2.13 – ДБЖ Legrand

Ємність штатних свинцево-кислотних батарей цих ДБЖ розрахована на автономну роботу системи протягом 15–20 хвилин при номінальному навантаженні. Цього часу вистачить для запуску дизель-генераторної установки.

Для забезпечення гарантованої безперервної роботи низьковольтної системи моніторингу (на базі мікроконтролера STM32), локальних датчиків та критичних каналів зв'язку (медіаконвертер, шлюзи керування) розроблено та впроваджено автономний сонячний вузол низької потужності. Цей контур функціонує незалежно від наявності палива в ДГУ.

Специфікація обраного обладнання для автономного контуру зв'язку та моніторингу:

- Фотоелектричний модуль: AXIOMA energy AX-300M (рис. 2.14). В якості генератора енергії обрано монокристалічну сонячну панель номінальною потужністю 300 Вт. Монокристалічна технологія забезпечує вищий ККД порівняно з полікристалічними аналогами, що критично важливо в умовах обмеженої площі монтажу на об'єкті [21].



Рисунок 2.14 – Монокристалічна сонячна панель AXIOMA energy

- Гібридний мережевий інвертор: Victron Energy MultiPlus 12/1200/50 (рис. 2.15). Це система, яка поєднує в одному корпусі багатофункціональний DC/AC інвертор із чистою синусоїдою, адаптивний зарядний пристрій для літієвих АКБ (12 В) та надшвидкісне реле перемикання змінного струму. Головною особливістю пристрою є підтримка мережевого режиму (Grid-Tie) з функцією PowerAssist, що дозволяє синхронізувати сонячну генерацію з промисловою мережею та паралельно підмішувати додатковупотужність від акумулятора.



Рисунок 2.15 – Гібридний інвертор Victron Energy MultiPlus

- Накопичувач енергії: Літій-залізо-фосфатна акумуляторна батарея LogicPower LiFePO4 12V 50Ah (рис. 2.16). Детальні характеристики представлені у таблиці 2.1.



Рисунок 2.16 – Акумулятор LogicPower

Переваги обраної моделі LiFePO4 полягають у високій щільності енергії, здатності приймати великі струми заряду, що дозволяє повністю відновити ємність за 2–3 години активної інсоляції та утриманні стабільної номінальної напруги на рівні 12 В практично до повного розряду [22].

Таблиця 2.1 – Характеристики для батареї LogicPower LiFePO4 [20]

Тип батареї	LiFePO4 (літій-залізо-фосфатна)
Номінальна напруга	12 В
Ємність	50 Ah
Енергетична ємність	600 Wh
Максимальний робочий струм	~50 А
Цикли заряд/розряд	2000–6000+
Температура експлуатації	-20…+60 °C
Температура зарядки	0…45 °C
BMS (система захисту)	Так. Захист від перевантаження, короткого замикання, балансування

Для підтвердження автономності третього рівня проведемо розрахунок необхідної генерації. Для цього знаходимо сумарне споживання обладнання та множимо на кількість годин. Для приклада маршрутизатор Juniper MX80 (350-400 Вт.) та два комутатори EX4200 (100 Вт. кожний), медіаконвертер та STM32 з датчиками (до 10 Вт.) Таким чином, виходить:

$$P_{load} = 400+200+10=610 \text{ Вт.}$$

Добова потреба цього вузла в енергії для забезпечення режиму роботи 24/7 становить:

$$E_{day}=P_{load}*24 \text{ год } =610*24=14\ 640 \text{ Вт}=14.6 \text{ кВт*год}. \quad (2.1)$$

Визначимо реальну генерацію однієї сонячної панелі AXIOMA AX-300M (300 Вт) за один світловий день у найнесприятливіший зимовий період (грудень-лютий):

$$E=P*K*\eta, \quad (2.2)$$

де P– потужнісь панелі,

K– коефіцент інсоляції(залежить від сезону, для зими 3 години сонця[23]),

η – кефіцент втрат системи =0.7(втрати в кабелях та запилення панелей)

Отримаємо:

$$E=300 \text{ Вт} * 3 * 0.7 = 630 \text{ Вт*год}.$$

Для забезпечення повної, стовідсоткової автономії всього вузла зв'язку виключно за рахунок сонячної енергії взимку знадобилася б така кількість панелей:

$$\frac{14\ 640 \text{ Вт}*\text{год}}{630 \text{ Вт}*\text{год}} = 23.23 = 24 \text{ панелі}.$$

Замість побудови громіздкої та економічно недоцільної повністю автономної сонячної станції, яка б потребувала понад 24 панелі для роботи взимку, система функціонує в режимі постійного підживлення та гарантованого резерву. Замість побудови масштабної сонячної станції, система використовує чотири фотоелектричних модуля AX-300M панель потужністю 300 Вт. та літій-залізо-фосфатний акумулятор LogicPower LiFePO4 загальною потужністю 1200 Вт (1.2 кВт) та акумуляторного масиву LogicPower загальною енергетичною ємністю 2400 Вт·год (2.4 кВт·год).

2.2 Структурна схема системи в Packet Tracer та її принцип роботи

Для ефективного моніторингу мікроклімату у серверній з 4 кондиціонерами по всім кутам і 3 рядами стійок, датчики мають перекривати “гарячі зони” та зони забору повітря. Розташування холодних та гарячих коридорів представлено на рис. 2.17. Це такі повітряні потоки в серверній. Сервери завжди засмоктують холодне повітря спереду і видувають гаряче ззаду. Якщо розставити стійки хаотично, гаряче і холодне повітря змішуються, і охолодження стає неефективним. Тому стійки розставлені рядами так, щоб передні панелі серверів дивилися одна до одної і це буде холодний коридор. Задні частини серверів дивилися одна до одної – це гарячий коридор.

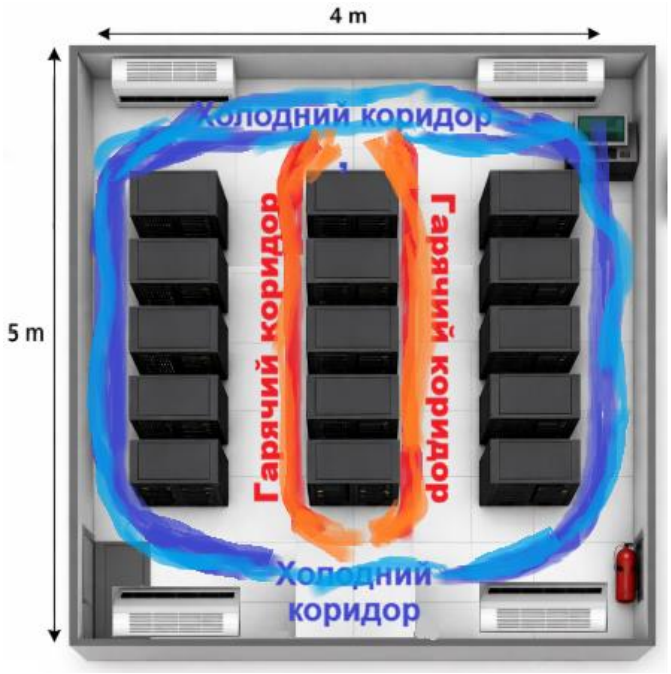


Рисунок 2.17 – Візуальне зображення повітря у “холодних та гарячих” коридорів у серверній кімнаті

У холодному коридорі подається охолоджене повітря зображене синім кольором з кондиціонерів після чого сервери його забирають для охолодження, в той час як у гарячому коридорі накопичується тепле повітря зазначене червони кольором, яке видувають сервери, і звідти воно вже забирається

кондиціонерами. Саме тому слід уважно обирати місця для зняття метрік (рис2.18).

Датчики температури. Тепле повітря завжди підіймається вгору, тому фізично датчики краще розміщувати у верхній третині стійок.

1. Датчик T1: Центр кімнати, на центральній стійці в середньому ряду. Сюди найважче дістатися холодному повітрю від кутових кондиціонерів. Тому ця зона має більше вірогідності на перегрів.
2. Датчик T2: Лівий ряд, верхня стійка (ближче до кондиціонера). Цей датчик показує температуру повітря, що надходить до обладнання.
3. Датчик T3: Правий ряд, нижня стійка (по діагоналі від T2). За рахунок діагонального охоплення приміщення можна бачити різницю температур між різними кутами кімнати.

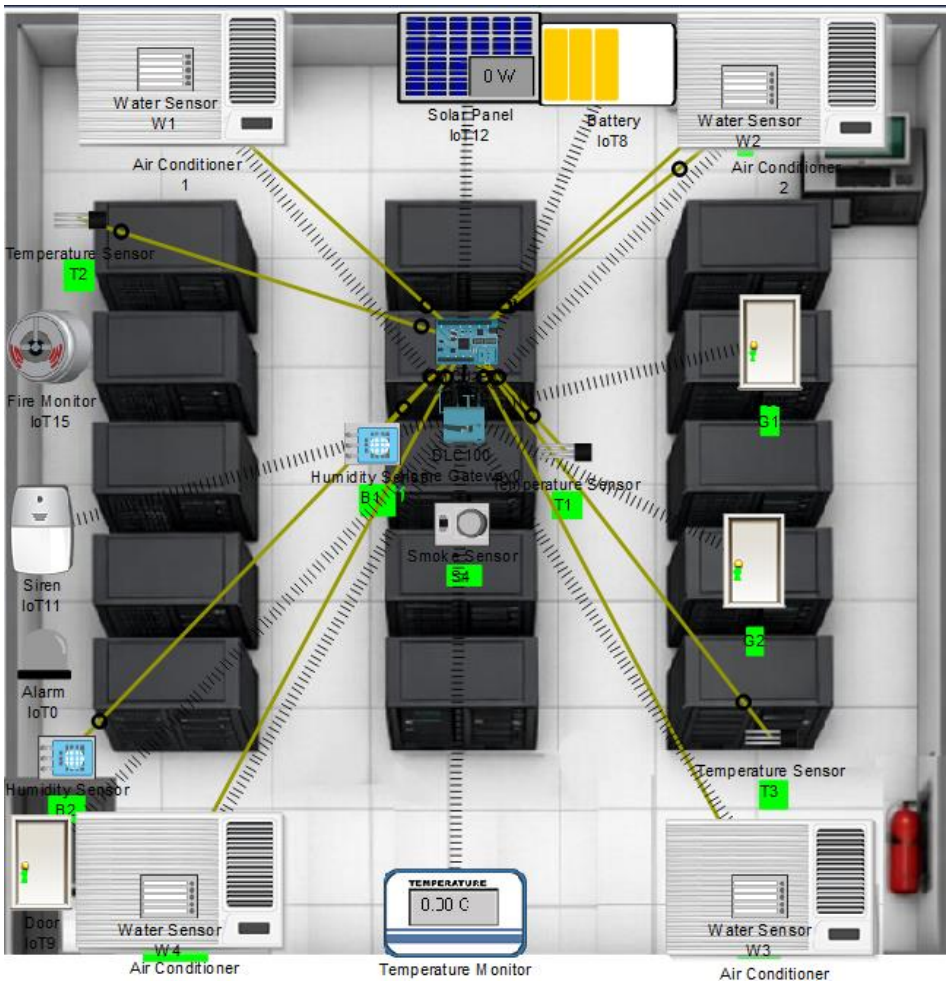


Рисунок 2.18 – Схема розташування датчиків на плані

Датчики вологості: вологість розподіляється по кімнаті більш рівномірно, але її важливо контролювати, щоб уникнути статичної електрики або конденсату.

1. Датчик B1: Центр кімнати. Для отримання значення у найбільш навантаженій точці.
2. Датчик B2: Біля входу. Вологість часто змінюється там, де відбувається обмін повітрям із зовнішнім середовищем, в даному випадку це двері.

Датчик диму: дим легший за повітря і завжди піднімається вгору, збираючись під стелею, тому розміщуємо датчик диму S4 по центру кімнати на стелі. Це забезпечить рівномірне покриття, та не буде впритул до кондиціонерів, оскільки сильний потік повітря буде здувати дим від сенсора.

Датчик затоплення: вода завжди тече і збирається під джерелами вологи, тому розмістити датчики W треба на підлозі під кожним кондиціонером, та біля вхідних дверей. Конденсат з кондиціонерів є найчастішою причина протікань у серверних.

Геркони: це магнітні контакти для контролю відкриття дверей/вікон. Розміщуємо G1 та G2 на вхідних дверях, та на двух шкафах з обладнанням, котрі необхідно контролювати.

Датчик світла: використовується для економії енергії, щоб слідкувати за світлом яке могли забути вимкнути, або для виявлення стороннього світла. Розміщуємо у центрі кімнати на стелі, спрямованим униз. Таким чином він має охоплювати загальний простір, щоб розуміти, чи увімкнене основне освітлення.

2.3 Вибір апаратної частини

Вибір сенсорного забезпечення для розроблюваної системи базувався на критеріях високої точності вимірювань, енергоефективності, цифрового інтерфейсу підключення та доступності на ринку електронних компонентів. Основним елементом моніторингу середовища обрано цифрові датчики

температури та вологості, які дозволяють отримувати калібровані значення без необхідності використання зовнішніх аналого-цифрових перетворювачів.

Контроль якості повітряного середовища та газового складу реалізовано на базі цифрового металооксидного сенсора CCS811 (рис.2.19).



Рисунок 2.19 – Модуль датчик якості повітря CCS811

На відміну від простих електрохімічних аналогів, даний модуль виконує вимірювання сумарної концентрації летких органічних сполук (TVOC) та розраховує еквівалентний рівень вуглекислого газу (eCO_2) [24].

Підсистема температури та вологості побудована на датчиках DHT11 та DS18B20. Моніторинг температурно-вологісних режимів розділено на зони. Цифрові датчики DHT11 забезпечують моніторинг базових показників температури та відносної вологості повітря в приміщенні, що дозволяє оцінювати загальний кліматичний фон. Для контролю найбільш теплонавантажених вузлів застосовано герметичні датчики DS18B20. Використання інтерфейсу 1-Wire дозволяє розміщувати сенсори на значній відстані (2–3 метри) від контролера, забезпечуючи точковий вимір температури безпосередньо всередині обладнання.

Підсистема фізичної безпеки побудована на датчиках МС-38 та додатково на LM393. Контроль доступу та безпеки реалізовано комбінованим методом, а саме:

- Контроль периметра: Магнітоконтактні сповіщувачі МС-38 встановлюються безпосередньо на двері серверної кімнати та дверцята телекомунікаційних шаф за якими необхідний додатковий контроль. Це

дозволяє фіксувати точний час доступу до обладнання та корелювати температурні флуктуації з діями персоналу.

- Оптичний контроль: Модулі на базі компаратора LM393 виконують функцію датчиків освітленості. Вони фіксують різку зміну рівня світла, що дозволяє виявити несанкціоноване проникнення, забуте вимкнене світло або перебування людей у приміщенні [25].

В якості керуючого ядра системи моніторингу серверного приміщення обрано відлагоджувальну плату сімейства STM32 Nucleo-144 (рис.2.20). Вибір даної платформи зумовлений наступними факторами:

- Плата оснащена потужним 32-бітним мікроконтролером STM32 у корпусі LQFP144. Велика кількість портів вводу-виводу, дозволяє підключити весь необхідний набір сенсорів без використання додаткових розширювачів портів або мультиплексорів.
- Ключовою вимогою до системи моніторингу серверної є надійність передачі даних. Плата підтримує підключення по стандарту Ethernet, що дозволяє інтегрувати пристрій у локальну мережу підприємства через дротове з'єднання. Це забезпечує більш стабільний зв'язок у порівнянні з Wi-Fi рішеннями, які можуть бути вразливими до електромагнітних завад від серверного обладнання.
- Апаратна підтримка годинника реального часу (RTC). Наявність кварцового резонатора 32.768 кГц дозволяє реалізувати точний відлік часу на апаратному рівні. Це критично важливо для логування подій навіть у випадку тимчасової втрати зв'язку з сервером.
- Підтримка роз'єму ST Zio сумісного з Arduino Uno дає можливість використовувати готові модулі розширення на етапі прототипування[26].

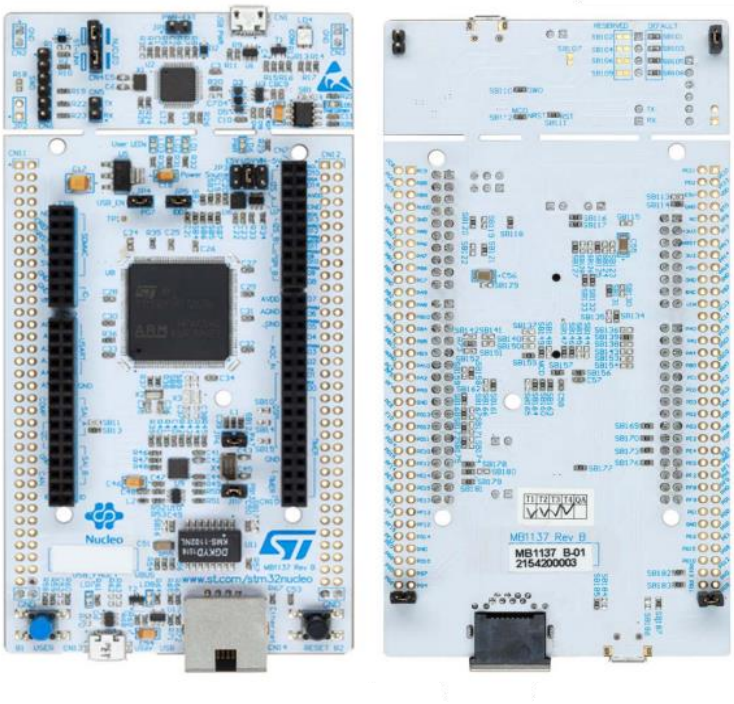


Рисунок 2.20 – Налагоджувальна плата STM32 NUCLEO-F767ZI

Таблиця 2.2 – Технічні характеристики плати STM32 Nucleo-144 [27]

Характеристика	Опис та значення
Мікроконтролер	STM32 (32-бітний ARM Cortex-M)
Кількість портів (GPIO)	До 114 ліній вводу-виводу загального призначення, доступних через роз'єми розширення.
Комунікаційні інтерфейси	I2C, SPI, UART/USART, CAN, USB OTG
Мережеві можливості	Роз'єм Ethernet
Аналогові інтерфейси	Багатоканальні 12-бітні АЦП (ADC) та ЦАП (DAC) для роботи з аналоговими сигналами
Живлення зовнішніх пристроїв	Вихід 3.3 В та 5.0 В
Тактування	Кварцовий резонатор LSE 32.768 кГц

Для зручності на рисунку 2.21 представлена технічна карта роз'ємів плати, яка вказує на фізичне розташування та назви кожного з контактів. На основі цієї інформації можна створити таблицю 5, яка буде містити дані про датчики, які піни вони використовують та який тип сигналу необхідний для працездатності [28]. Завдяки наявності апаратного модуля FPU (Floating Point Unit), система виконує складні математичні операції з плаваючою комою (розрахунок точки роси, фільтрація шуму датчиків) апаратно, що забезпечує високу швидкодію та точність.

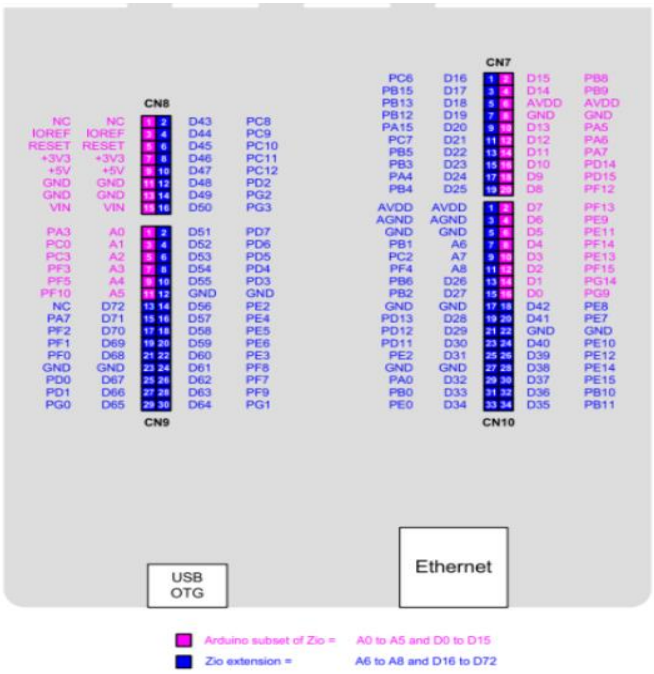


Рисунок 2.21 – Схема розпіновки плати NUCLEO-F767ZI

Таблиця 2.3 – Інформація використаних датчиків

Датчик	Кількість	Пін	Тип сигналу
LM393 (Світло)	2	PC6, PC7	GPIO input
DHT11 (Temp/Hum)	2	PF12, PF13	Single-wire
MC-38 (Геркон)	3	PD11, PD12, PD13	GPIO output
DS18B20 (Temp)	3	PA3	OneWire
CCS811 (Air)	1	PB8 , PB9 (SDA)	I2C1

2.4 Алгоритмічне забезпечення та логіка роботи системи

Розробка програмного забезпечення для керуючого модуля виконана в інтегрованому середовищі STM32CubeIDE на мові C та представлена в додатку А. Архітектура базується на циклічному опитуванні сенсорів та обробці переривань для критичних подій. Апаратною платформою виступає відлагоджувальна плата NUCLEO-F767ZI на базі високопродуктивного мікроконтролера STM32F767ZIT6 з ядром ARM Cortex-M7, 216 МГц. Використання даного мікроконтролера дозволило відмовитися від зовнішніх мережевих модулів на користь інтегрованого Ethernet-MAC контролера.

Архітектура побудована на трьох рівнях, які взаємодіють через стандартизовані інтерфейси:

-Апаратний рівень. Відповідає за взаємодію з кристалом мікроконтролера. Механізм DMA використовується для передачі даних. Особливістю реалізації є драйвер ETH MAC, який працює через інтерфейс RMII з фізичним трансивером на платі. Це дозволяє здійснювати прийом та передачу мережевих пакетів у фоновому режимі, не блокуючи обчислювальне ядро.

-Рівень системних служб та мережевого стека. Інтегровано повноцінний TCP/IP стек LwIP. Це стек з відкритим кодом, оптимізований для вбудованих систем. Він бере на себе всі складні процеси: ARP-запити, ICMP, фрагментацію пакетів та підтримку стабільності TCP-з'єднань. Поверх LwIP працює MQTT-клієнт, який інкапсулює дані телеметрії у легковажні пакети для відправки на сервер [26, 27, 28].

-Рівень логіки керує життєвим циклом пристрою. В ньому реалізовано головний алгоритм опитування, який збирає дані з датчиків. Саме на цьому рівні приймаються рішення про аварійні ситуації, такі як, наприклад, геркон зафіксував відкриття дверей, система миттєво формує повідомлення у вигляді алерта.

Обґрунтування порогових значень відбувається на основі галузевих стандартів. Логіка роботи програмного забезпечення базується на нормативних вимогах до мікроклімату дата-центрів, проаналізованих у Розділі 1, стандарт TIA-942 та рекомендації ASHRAE.

У пам'ять мікроконтролера зашито три рівні станів системи: «Норма», «Попередження» та «Аварія» (рис.2.22).



Рисунок 2.22 – Частина алгоритму багаторівневої моделі оповіщення

Визначення зон реагування:

Температурний режим. Згідно з вимогами стандарту, оптимальний діапазон становить 18–27 °C. Вихід за ці межі свідчить про неефективність системи охолодження.

- Діапазон “Норма”:*18*˚C - *26.9*˚C. Система працює в штатному режимі, дані передаються на сервер для статистики кожні 10 хвилин.
- Поріг “Попередження” спрацьовує при температурі $\geq$ *27*˚C. Це значить, що температура вийшла за межі рекомендованої, але загрози обладнанню ще немає. В такому випадку здійснюється відправка метрик на сервер з налаштованою системою моніторингу різних станів (Zabbix).
- Поріг “Аварія” вмикається при *35*˚*C* та більше. Це означає критичний перегрів. При такій температурі починається деградація ізоляції та різко зростає ризик виходу з ладу жорстких дисків. Інформування буде відбуватися як і з попереднім алертом.

Режим вологості. Нормативне значення відносної вологості складає 30–60%.

- Нижній поріг “Аварія, якщо значення H < 30%. Це означає що висока ймовірність накопичення статичного заряду, котра може миттєво пошкодити електронні компоненти серверів при торканні.
- Верхній поріг “Аварія” якщо значення H > 60%. При таких показниках виникає конденсація вологи на платах, корозія контактів, та коротке замикання.

Якість повітря. Контроль ефективності вентиляції здійснюється за рівнем CO_2 в одиницях ppm (parts per million — частин на мільйон, де 1000 ppm це 0.1% вмісту газу в повітрі

- Норма: 400–800 ppm .
- Поріг “Попередження” спрацьовує коли значення > 1000 ppm. Це свідчить про те, що вентиляція не справляється.

Енергоживлення та програмний моніторинг. Незважаючи на те, що перемикання на резервне живлення відбувається автоматично на апаратному рівні самого інвертора, програмний моніторинг напруги акумуляторного масиву за допомогою мікроконтролера є критично важливим для забезпечення живучості системи. Для гібридного вузла моніторингу в алгоритмі керування встановлено такі фізично обґрунтовані пороги напруги для LiFePO4 акумуляторів:

- “Робота від АКБ” ($U \leq 13.1$ В $- 12.8$ В). Фіксує момент зникнення зовнішнього живлення, коли напруга батареї під робочим навантаженням просідає.
- “Критичний розряд” ($U < 11.5$ В): свідчить про повне виснаження енергетичного буфера. Система негайно відправляє аварійне повідомлення.

Система аналізує швидкість падіння напруги під навантаженням, що дозволяє адміністратору оцінити реальний час автономної роботи об'єкта до моменту виснаження батареї. Що стосується дизель-генераторної установки, її

моніторинг здійснюється не через STM32, а за допомогою збору стандартних SNMP-метрик через власні MIB-файли обладнання. Необхідна інформація надходить на сервер моніторингу та відображається у вигляді графіків (рис. 2.23).

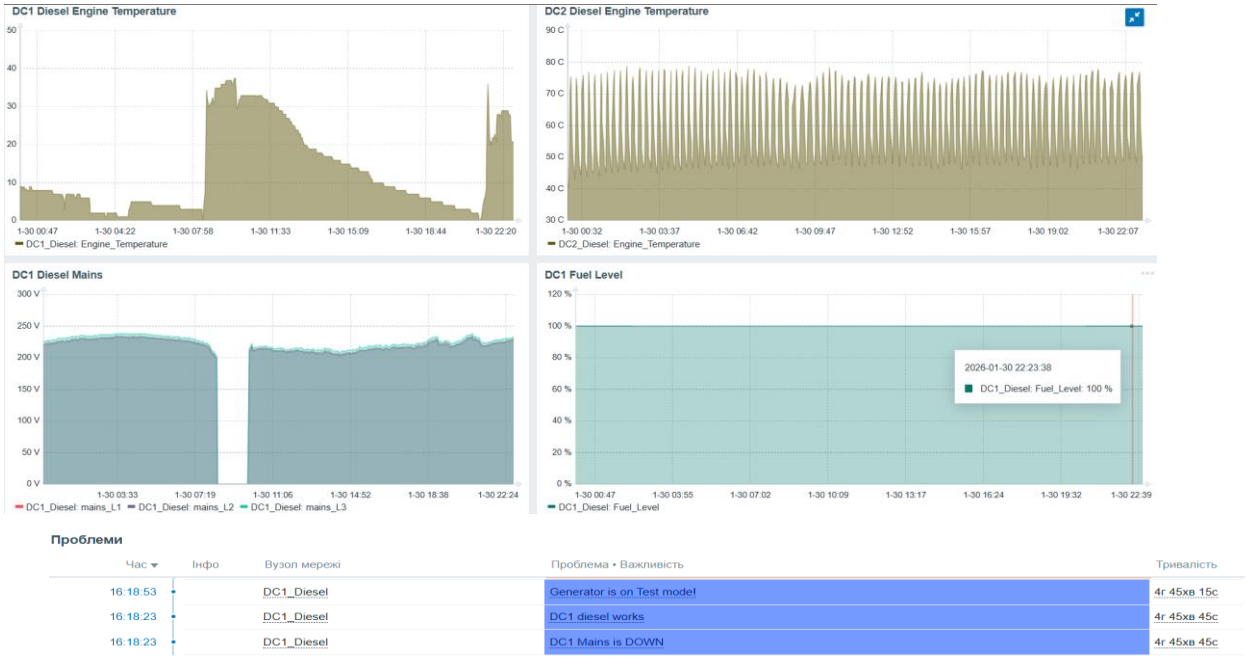


Рисунок 2.23 – Результат оповіщення в системі моніторингу

2.5 Налаштування комунікаційних протоколів та датчиків

Комунікаційна складова розробленої системи базується на комплексному використанні стеку протоколів TCP/IP та протоколу Zabbix Sender. Фундаментом програмної архітектури є стек з відкритим кодом LwIP, який виступає в ролі інтелектуального комунікаційного мосту між фізичним рівнем Ethernet та прикладним програмним забезпеченням.

LwIP функціонує як автономний фоновий процес, що бере на себе всі складні механізми мережевого обміну: ARP-запити, фрагментацію пакетів та контроль доставки, приклад коду представлен у додатку Б. Зокрема, якщо пакет із даними буде втрачено через перешкоди, стек самостійно здійснить повторну відправку, гарантуючи, що система моніторингу не пропустить критичну

подію. Розроблений алгоритм дозволяє мікроконтролеру самостійно ініціювати з'єднання при виникненні тривожних подій.

Процес передачі даних реалізовано через функцію Zabbix_Send_Trap, яка виконує наступні кроки:

1. Встановлення зв'язку. Створення TCP-з'єднання та підключення до IP-адреси сервера Zabbix на порт 10051.
2. Формування пакету. Генерація JSON, що містить назву хоста, унікальний ключ датчика та його поточне логічне значення.
3. Інкапсуляція. Формування специфічного заголовка протоколу, що починається з сигнатури ZBXD\x01, та розрахунок довжини пакету для коректної інтерпретації сервером [29].

Така реалізація забезпечує миттєву доставку сповіщень про стан навколишнього середовища та інших чинників. Детальний приклад формування та надсилання пакетів надано у додатку Б.

У роботі реалізовано комплексну взаємодію мікроконтролера з периферійними пристроями через різнорідні цифрові інтерфейси. Основним інструментом збору метеоданих обрано протоколи One-Wire (DS18B20) та Single-wire (DHT11). Для забезпечення їх функціонування розроблено програмні драйвери, що базуються на прецизійному формуванні часових інтервалів за допомогою апаратного таймера TIM1 з дискретністю 1 мкс. Це дозволяє системі коректно виконувати дешифрацію 40-бітових пакетів та перевірку контрольної суми для забезпечення достовірності даних.

Моніторинг критичних подій у реальному часі (освітленість, стан дверей) реалізовано за допомогою GPIO Input у режимі Input Pull-up. Такий підхід забезпечує високу завадостійкість сигнальних ліній в умовах серверної. Повний лістінг файлу main.c представлено у додатку В.

2.6 Аналіз працездатності датчиків у складі системи

Тестування розробленої системи моніторингу проводилось в умовах діючої кімнати. Метою випробувань була перевірка точності зчитування даних з датчиків різних типів, стабільності роботи мережевого стеку та коректності відображення параметрів у середовищі налагодження в реальному часі.

Під час випробувань було задіяно механізм Live Expressions, що дозволило спостерігати за динамікою зміни параметрів без зупинки процесора (рис.2.24).

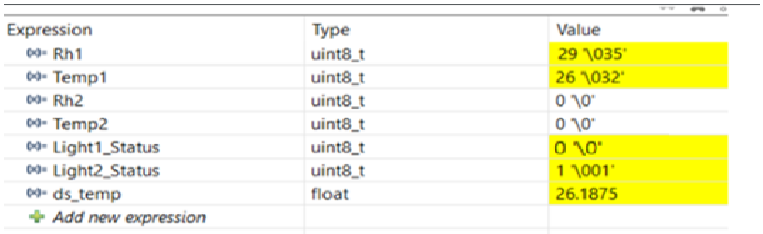


Рисунок 2.24 – Контроль значень температури, вологості та освітленості

У таблиці 2.4 наведено призначення та типи даних основних змінних, що використовуються для збереження та обробки інформації з датчиків.

Таблиця 2.4 – Інформація змінних

Змінна	Тип даних	Опис та призначення
Rh1	uint8_t	Відносна вологість (Relative Humidity) з першого датчика DHT11
Temp1	uint8_t	Температура з першого датчика DHT11. Ціле число у градусах Цельсія
Light1_Status	uint8_t	Статус освітленості від датчика LM393. Логічна «1» означає стан «темно», «0» - наявність світла.
ds_temp	Float	Температура з датчика DS18B20. Тип float дозволяє зберігати дані з плаваючою комою.

Датчик DS18B20 продемонстрував точність, що є критичним для виявлення зон локального перегріву. Дані з датчика DHT11 корелюють із показниками контрольних приладів, що підтверджує правильність реалізації Single-wire протоколу. LM393 стабільно фіксували стан «Логічна 1» (темно) та «Логічний 0» (світло), що дозволяє використовувати їх як надійний інструмент контролю несанкціонованого доступу до приміщення або забутого світла. Таким чином результати випробувань підтверджують, що розроблений програмно-апаратний комплекс на базі мікроконтролера STM32F767ZI повністю відповідає вимогам надійності та точності.

2.7 Обґрунтування доцільності розробки альтернативного рішення

Розроблювана альтернативна IoT-система моніторингу базується на принципах відкритої архітектури та високої модульності, що дозволяє гнучко адаптувати її під індивідуальні потреби будь-якого об'єкта. На відміну від закритих пропрієтарних рішень, ця система передбачає можливість масштабування для одночасного підключення та обробки даних від великої кількості різнорідних сенсорів. До базового контуру моніторингу інтегруються датчики температури, вологості, струму, напруги, диму, вібрації та витоку газів. Ключовою перевагою є наявність спеціалізованих модулів контролю стану джерел безперебійного живлення, що забезпечує глибоку діагностику їх роботи, а не лише фіксацію факту перемикання на резерв, що є критичним для підтримання живучості IT-інфраструктури.

На відміну від UniPing, Netbotz та Didactum, запропонована система має аналітичну платформу. Дані надходять на локальний шлюз де здійснюється аналітична обробка, що дозволяє візуалізувати дані в реальному часі, будувати графіки, аналізувати тренди та реалізовувати алгоритми прогнозування відмов на основі машинного навчання. Основними перевагами розробленої системи є відкритість програмного коду, низька собівартість, гнучкість масштабування та можливість адаптації під специфічні потреби користувача (рис.2.25).

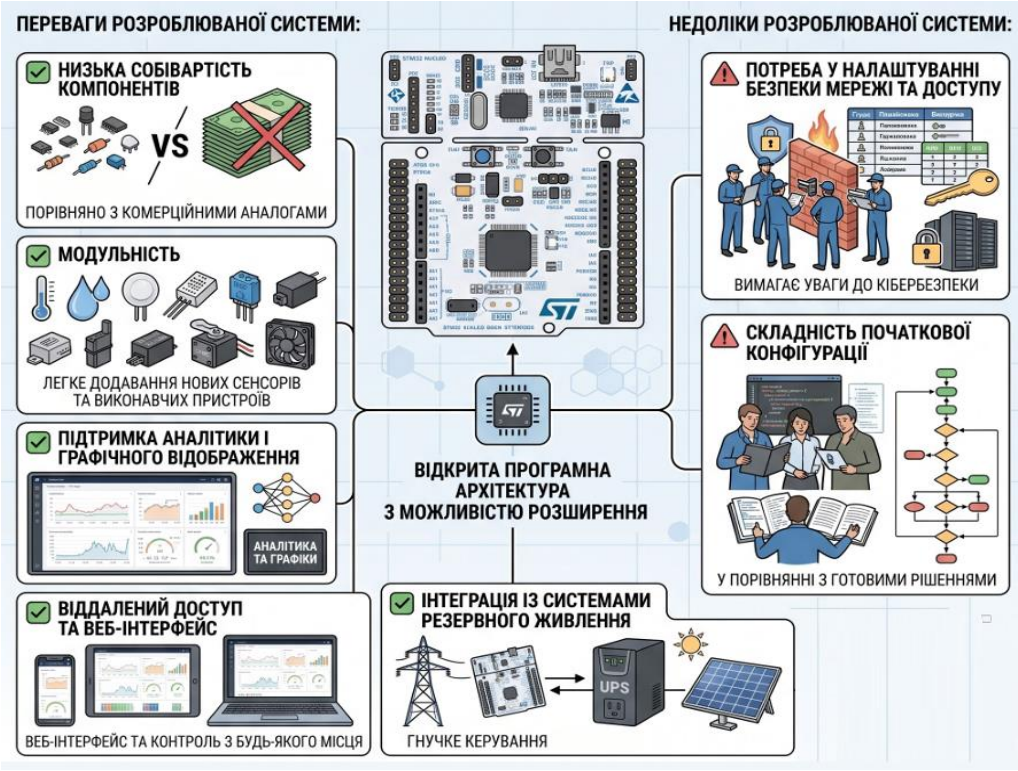


Рисунок 2.25 – Переваги розроблюваної системи

Використання віддаленого веб-інтерфейсу спрощує адміністрування і дає змогу отримувати повідомлення у разі аварійних ситуацій у реальному часі. Недоліками на етапі прототипування можуть бути обмеженість обчислювальних ресурсів мікроконтролера та необхідність ретельного налаштування системи безпеки для запобігання несанкціонованому доступу.

Переваги розроблюваної системи:

- відкрита програмна архітектура з можливістю розширення;
- низька собівартість компонентів порівняно з комерційними аналогами;
- модульність - легке додавання нових сенсорів та виконавчих пристроїв;
- підтримка аналітики і графічного відображення;
- віддалений доступ та веб-інтерфейс;
- інтеграція із системами резервного живлення.

Недоліки розроблюваної системи:

- потреба у налаштуванні безпеки мережі та доступу;
- складність початкової конфігурації у порівнянні з готовими рішеннями.

Ключовою особливістю є інтеграція енергомоніторингу з автономним живленням – система буде здійснювати контроль параметрів лінійно-інтерактивного або лінійного джерела безперебійного живлення (ДБЖ), підключеного через DC/DC-конвертор до сонячної панелі. Це дозволить не лише реєструвати стан енергосистеми, а й аналізувати ефективність її роботи та рівень заряду акумуляторів.

Велика кількість існуючіх систем моніторингу серверних приміщень орієнтовані на забезпечення базового контролю параметрів мікроклімату та електроживлення з використанням порогових механізмів реагування [13, 14, 15]. Науково-практична проблема, що постає у даній предметній області, полягає у відсутності доступних та масштабованих систем моніторингу серверних приміщень, які поєднували б відкриту архітектуру, можливість гнучкого розширення функціоналу та підтримку аналітичної обробки даних для підвищення надійності функціонування інженерної інфраструктури. Зокрема, актуальним є питання переходу від реактивного контролю до випереджувального виявлення потенційно небезпечних станів на основі аналізу історичних даних.

У зв’язку з цим виникає необхідність розробки індивідуальної IoT-системи моніторингу серверної кімнати та автономного електроживлення, яка забезпечує збір і обробку даних з різнорідних сенсорів у режимі реального часу, підтримує аналітичні методи оцінювання стану системи та може бути адаптована до конкретних умов експлуатації без залежності від пропрієтарних апаратних і програмних рішень.

Завданням даної роботи є проектування та реалізація прототипу IoT-системи моніторингу, орієнтованої на рівень між TIER II та TIER III, що дозволяє підвищити ефективність контролю стану серверної інфраструктури та зменшити ризик виникнення аварійних ситуацій. Запропонована система базується на використанні доступних мікроконтролерних платформах, забезпечує візуалізацію параметрів, формування сповіщень про аварійні ситуації та створює передумови для подальшого впровадження алгоритмів

інтелектуального аналізу даних. Науково-технічна суть задачі полягає у розробленні універсальної IoT-платформи, здатної:

- здійснювати збір, передачу та обробку даних від множини сенсорів у режимі реального часу;
- виконувати аналітичну оцінку стану середовища з використанням алгоритмів порогового контролю;
- реагувати на відхилення шляхом активації виконавчих пристроїв (наприклад, вмикання охолодження чи сигналізації).
- забезпечувати візуалізацію даних;
- контролювати стан джерел автономного живлення та енергетичних перетворювачів;

Розробка передбачає створення архітектури, яка включає:

- сенсорний рівень (датчики фізичних параметрів);
- рівень збору та передачі даних;
- аналітичний рівень (обробка даних, формування звітів, аналітика)

Розроблена система має забезпечити:

- підвищення надійності функціонування серверного обладнання завдяки цілодобовому контролю параметрів середовища;
- зниження енергоспоживання шляхом оптимізації роботи систем охолодження та живлення;
- своєчасне виявлення аварійних ситуацій і можливість автономного реагування;
- незалежність від пропрієтарних апаратних платформ і програмного забезпечення;
- можливість подальшого розширення системи без значних фінансових витрат.

Практична реалізація проекту дозволить створити адаптивну, економічно доступну IoT-систему, орієнтовану на застосування у дата-центрах, телекомунікаційних вузлах, навчальних або корпоративних серверних кімнатах.

3 ОЦІНКА ЕФЕКТИВНОСТІ ТА ПОРІВНЯЛЬНИЙ АНАЛІЗ РОЗРОБЛЕНОЇ СИСТЕМИ

На основі проведених експериментальних випробувань у реальних умовах діючого об'єкта здійснюється детальний аналіз архітектурних та програмних переваг розробленого прототипу, що базується на обчислювальному ядрі STM32 NUCLEO-F767ZI [25]. Для забезпечення об'єктивності дослідження в розділі чітко окреслено виявлені функціональні обмеження поточного рішення та сформульовано науково-технічні шляхи його подальшої модернізації й адаптації під вимоги кібербезпеки.

Глибокий порівняльний аналіз створеної IoT-платформи з комерційними апаратно-програмними комплексами проходить за критеріями гнучкості архітектури, масштабованості та аналітичного потенціалу, що дозволяє підтвердити практичну цінність і конкурентоспроможність.

3.1 Технічні та експлуатаційні переваги розробленого рішення

Розроблена IoT-система моніторингу має комплекс технологічних та конструктивних переваг порівняно з існуючими інфраструктурними рішеннями, що було експериментально підтверджено під час її випробувань. Головною особливістю архітектури є велика кількість ліній вводу-виводу загального призначення (GPIO) на корпусі, що дозволяє гнучко масштабувати сенсорну мережу без закупівлі сторонніх розширювачів портів або мультиплексорів.

Модель взаємодії через функцію Zabbix Sender дозволяє мікроконтролеру самостійно ініціювати TCP-з'єднання лише при виникненні тривожних подій – виході параметрів за межі встановлених значень або миттєвій зміні стану окремих датчиків. Це мінімізує фоновий трафік та усуває необхідність постійного навантаження мережі періодичним опитуванням пристрою.

Іншою важливою перевагою є реалізація обчислень безпосередньо на базі обчислювального ядра платформи STM32. Високопродуктивний 32-бітний мікроконтролер із частотою 216 МГц та апаратним модулем математичних обчислень FPU дозволяє в реальному часі здійснювати прецизійну обробку даних, включаючи програмний розрахунок на основі показників температури та вологості. Це дає можливість прогнозувати ризик утворення конденсату на електронних платах і попереджати загрозу короткого замикання ще до її фізичної появи.

Комерційні системи моніторингу використовують пасивний пороговий контроль, за якого тривожний сигнал формується лише після факту перевищення відносної вологості або температури повітря. Проте головну небезпеку для друкованих плат обчислювального обладнання становить випадіння конденсату, яке призводить до миттєвого короткого замикання, корозії контактних груп та деградації провідників. Для реалізації випереджувального захисту розрахунку температури точки роси в реальному часі використовується алгоритм Магнуса-Тетенса. За допомогою проміжних коефіцієнтів, логарифмічної залежності та поточних показників температури навколишнього середовища що зчитується сенсором DS18B20 або DHT11 та відносною вологістю, котра читається датчиком DHT11 (рис.3.1). Формула розрахунку точки роси:

$$\text{Tp} = \frac{(b * f(T,Rh))}{(a - f(T,Rh))}, \tag{3.1}$$

$$f(\text{T, Rh}) = \frac{a*T}{b+T} + \ln(\frac{Rh}{100}),$$

де:

a (постійна) = 17,27 ° C;

b (постійна) = 237,7 ° C;

T – температура повітря ° C;

Rh – відносна вологість повітря, %.

Ці числові значення є емпіричними коефіцієнтами у формулі, яка математично описує залежність тиску насиченої водяної пари від температури навколишнього середовища. Вони були отримані експериментальним шляхом та є чинними для стандартного атмосферного тиску в реальних земних умовах. Саме комбінація коефіцієнтів a=17,27 та b=237,7 ° C забезпечує максимальну точність розрахунків у найбільш критичному для життєдіяльності техніки температурному діапазоні від 0 до +50 ° C [30].

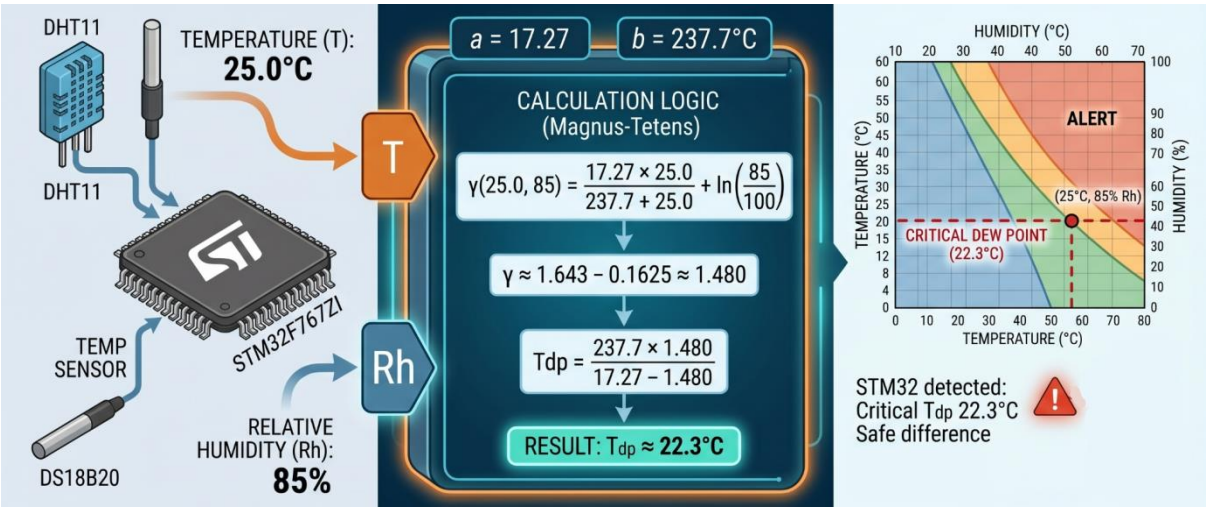


Рисунок 3.1 – Часова діаграма випереджувального спрацювання предиктивного захисту за розрахунком точки роси

На рисунку 3.1 зображено алгоритм збору даних з датчиків температури та вологості, обчислення точки роси й аналізу ризика утворення конденсату. У разі наближення параметрів до критичних значень формується тривожне повідомлення для системи моніторингу.

Крім того, вибір дротового з'єднання за стандартом Ethernet-MAC через фізичний інтерфейс та оптимізований мережевий стек LwIP забезпечує безпрецедентну стабільність передачі даних у локальну мережу. На відміну від бездротових Wi-Fi рішень, такий підхід повністю виключає ризики вразливості до потужних електромагнітних завад від серверного обладнання.

3.2 Недоліки та шляхи вдосконалення

Поряд із суттєвими перевагами є і певні обмеження, які формують вектори для подальшої модернізації системи. Основним недоліком на етапі розгортання є складність початкової конфігурації порівняно з готовими комерційними системами класу Plug-and-Play. Оскільки архітектура базується на низькорівневому програмуванні, зміна мережевих параметрів, статичної адресації або порогових значень вимагає безпосереднього коригування коду у файлі main.c та повторного прошивання контролера через середовище розробки STM32CubeIDE.

Додатковим фактором, що потребує уваги на етапі промислового впровадження, є вразливість кіберфізичного контуру та безпека доступу в мережі. Поточна програмна реалізація здійснює передачу структурованих JSON-пакетів телеметрії у відкритому вигляді без застосування алгоритмів шифрування трафіку. У масштабах корпоративної мережі це створює потенційні ризики несанкційного перехоплення даних або підміни інформації зловмисниками. Перспективним шляхом вирішення цієї проблеми є інтеграція криптографічного розширення, що дозволить використовувати захищені сокети для безпечної передачі інформації.

Апаратний годинник реального часу RTC з кварцовим резонатором дозволяє точно фіксувати часові мітки подій, тривале логування великих масивів даних неможливе. Наступні версії пристрою передбачають додавання модуля розширення для зовнішніх SD-карт через інтерфейс SDIO, що забезпечить повну автономність збереження архівів телеметрії [31].

3.3 Порівняльний аналіз із промисловими комерційними аналогами

Для об'єктивного оцінювання конкурентоспроможності створеної IoT-платформи з аналогами було проведено порівняльний аналіз. Ключова

відмінність між ними полягає в архітектурному підході до побудови систем (рис.3.2).

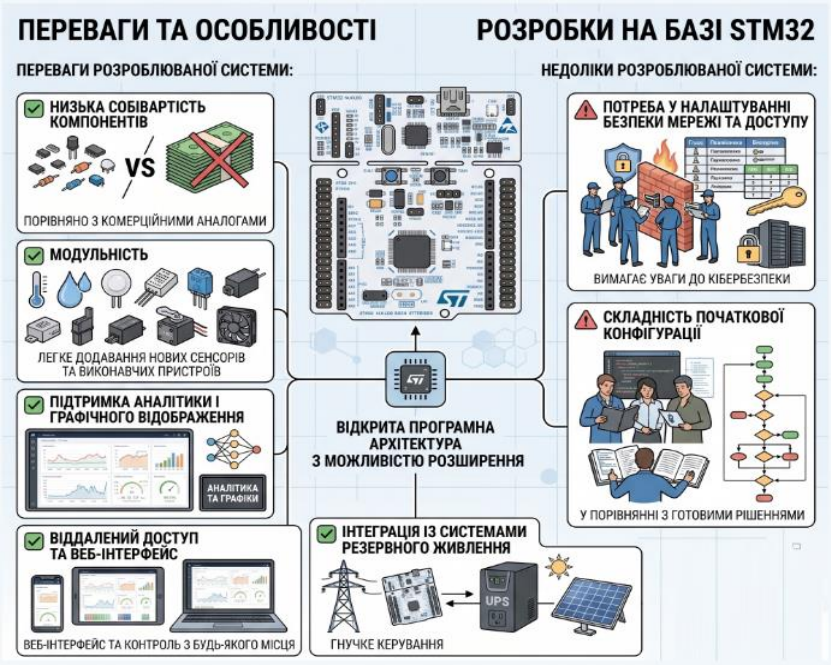


Рисунок 3.2 – Переваги та особливості

Наприклад, комерційний аналог UniPing базується на закритій програмній та пропрієтарній апаратній архітектурі, що повністю унеможливлює гнучке доопрацювання функціоналу, зміну логіки обробки сигналів або підключення доступних сенсорів сторонніх виробників без використання спеціалізованих фірмових модулів розширення. Розроблена система є повністю відкритою і забезпечує універсальний тип збору даних, дозволяючи одночасно комбінувати та обробляти різні цифрові й аналогові інтерфейси, такі як дискретні лінії (GPIO), One-Wire, I2C, а також спеціалізовані однопровідні протоколи (Single-wire).

З економічної точки зору, використання розробленої платформи демонструє високу доцільність для підприємств. Середня ринкова ціна базового блоку UniPing без урахування додаткових сенсорів та ліцензій перевищує сумарну вартість апаратної бази розробленого рішення, що включає відлагоджувальну плату та розширений набір первинних датчиків. Більш детальний аналіз розглнуто у таблиці 3.1.

Таблиця 3.1 – Порівняльна характеристика розробленої IoT-системи та аналогів

Критерій порівняння	UniPing Server	APC NetBotz	Didactum PDU	Розроблена система	Обгрунтування
Вартість	313 $	690 $	654 $	До 130 $	Корпоративні APC та Didactum мають занадто високу ціну; розроблена система має низьку собівартість компонентів
Підтримка MQTT, REST API, SNMP	SNMP v1/v2	Пропріє тарне ПЗ	API лише при купівлі розшир ень.	MQTT та REST API	Промислові аналоги орієнтовані на старий протокол SNMP; розроблена система підтримує інтеграцію в сучасні хмари
Гнучкість розширення архітектури	Підключе ння обмежено го списку фірмових датчиків	Підключ ення лише фірмови х датчиків	Закрит а для сторон ніх плат	Відкритий інтерфейс для будь-яких сенсорів.	Аналоги використовують закриту архітектуру та фірмові шини; розроблена система дозволяє підключати будь-які копійчані сенсори.
Безпека передачі даних (SNMP v3)	Передача у відкрито му вигляді	Шифрув ання за стандарт ом SNMP v3	промис ловий проток ол	шифруван ня не реалізован о	UniPing не забезпечує безпеку мережі як і розроблена система.
Власне енергоспоживанн я	до 10–12 Вт	до 15 Вт	до 6 Вт	менше 1.5 Вт	Архітектура на STM32 споживає мінімум енергії.
Автономність та бездротові комунікації	Ethernet	Ethernet	Має слот під Wi-Fi	Wi-Fi Ethernet	UniPing та APC прив'язані до Ethernet-кабелю; розроблена система має бездротові інтерфейси.
Швидкість розгортання (введення продукту в експлуатацію)	Налаштов ана та протестов ана система	Налашто вана та протесто вана система	Налашт тована та протес тована систем а	Вимагає прошиван ня та збирання	Комерційні пристрої готові до роботи відразу; розроблена IoT-система є прототипом і потребує початкового прошивання та монтажу.

Для проведення комплексного порівняльного аналізу застосовано комбінований метод оцінювання (таблиця 3.2). Критерії, що мають кількісне вираження (вартість обладнання та власне енергоспоживання у ватах), залишено у їхніх абсолютних фізичних величинах. Це дозволяє зберегти наочність розрахунків економічної та енергетичної ефективності пристроїв.

Оцінювання якісних та експлуатаційних параметрів здійснено методом дискретного бального квантування за відносною шкалою від 0 до 1. Крок квантування відображає ступінь апаратної та програмної реалізації конкретних функцій пристроїв.

Таблиця 3.2 – Якісні показники систем

Критерій порівняння	UniPing Server	APC NetBotz	Didactum PDU	Розроблена система
Вартість	313	690	654	130
Підтримка MQTT, REST API	0.33	0	0.33	1
Гнучкість розширення архітектури	0.5	0.0	0.0	1
Безпека передачі даних (SNMP v3)	0	1	1	0.5
Власне енергоспоживання	12	15	6	1.5
Автономність та бездротові комунікації	0.5	0.5	0.5	1
Швидкість розгортання	1	1	1	0.33

Для приведення техніко-економічних та функціональних параметрів до співставного вигляду, дані поточної матриці розраховані на основі вихідних значень попередньої таблиці за допомогою методу лінійного нормування. Для числових критеріїв (Ціна та Енергоспоживання) абсолютні фізичні значення з попередньої таблиці поділено на максимальне зафіксоване значення у відповідній категорії серед усіх досліджуваних пристроїв:

$$X_{\text{норм}} = \frac{X_i}{X_{\max}}. \tag{3.2}$$

Таблиця 3.3 – Нормована матриця порівняльних коефіцієнтів

Критерій порівняння	UniPing Server	APC NetBotz	Didactum PDU	Розроблена система
Вартість	0.453	1	0.947	0.118
Підтримка MQTT, REST API	0.33	0	0.33	1
Гнучкість розширення архітектури	0.5	0.0	0.0	1
Безпека передачі даних (SNMP v3)	0	1	1	0.5
Власне енергоспоживання	0.8	1	0.4	0.1
Автономність та бездротові комунікації	0.5	0.5	0.5	1
Швидкість розгортання	1	1	1	0.33

Оскільки такі параметри, як «Ціна» та «Енергоспоживання», є негативними факторами (де чим менше значення - тим краще), їхні нормовані коефіцієнти було математично інвертовано. Розрахунок виконано шляхом віднімання отриманого раніше значення від одиниці за принципом:

$$\text{Бал} = 1 - X_{\text{норм}}. \tag{3.3}$$

Це дозволило змінити логіку оцінювання на позитивну: тепер у кожному рядку таблиці 3.4 більша цифра означає вищу ефективність пристрою.

Таблиця 3.4 – Приведення оцінок до співставного вигляду

Критерій порівняння	UniPing Server	APC NetBotz	Didactum PDU	Розроблена система
Вартість	0.546	0	0.052	0.811
Підтримка MQTT, REST API	0.33	0	0.33	1

Продовження таблиці 3.4				
Гнучкість розширення архітектури	0.5	0.0	0.0	1
Безпека передачі даних (SNMP v3)	0	1	1	0.5
Власне енергоспоживання	0.2	0	0.6	0.9
Автономність та бездротові комунікації	0.5	0.5	0.5	1
Швидкість розгортання	1	1	1	0.33
Загальний бал	3.076	2.5	3.482	5.541

Аналіз отриманих результатів дозволяє чітко окреслити ключові переваги та недоліки розробленої IoT-системи порівняно з комерційними аналогами. Головними перевагами є відкрита програмна архітектура та висока модульність, що підтверджується максимальним балом 1.0 за гнучкість розширення, тоді як у APC NetBotz та Didactum PDU цей показник дорівнює 0.0 через їхню абсолютну закритість. Завдяки підтримці протоколів MQTT та REST API наша система отримала максимальну оцінку 1.0, суттєво випередивши UniPing та Didactum, які мають лише часткову відповідність (0.33). Також за рахунок оптимізації елементної бази на основі STM32 рішення продемонструвало критично низьку вартість з балом 0.811 (проти 0.0 у APC та 0.052 у Didactum) та найвищу енергоефективність у 0.9 бала, тоді як APC NetBotz за споживання отримав 0.0 балів.

Основними недоліками розробки є нижча швидкість розгортання, де прототип отримав лише 0.33 бала, суттєво поступаючись заводським аналогам, які мають оцінку 1.0 і готові до роботи «із коробки». Також система має компромісний показник безпеки передачі даних (0.5), поступаючись APC та Didactum (1.0), оскільки відкрита архітектура вимагає додаткового ручного налаштування мережевого захисту.

Попри ці експлуатаційні особливості, розроблена система демонструє абсолютну перевагу за підсумковими балами, суттєво випереджаючи всі комерційні альтернативи. У фінальному підрахунку проектована IoT-платформа набрала 5.541 бала, тоді як найближчий ринковий аналог Didactum PDU отримав лише 3.482 бала, а системи UniPing Server та APC NetBotz продемонстрували найнижчу ефективність із результатами 3.076 та 2.5 бала відповідно. Такий вагомий відрив у підсумковій оцінці переконливо доводить, що за сукупністю техніко-економічних та функціональних метрик розроблене рішення є значно ефективнішим для автоматизації моніторингу серверних кімнат.

ВИСНОВКИ

У кваліфікаційній роботі успішно вирішено комплексне інженерне завдання з розробки та дослідження інтелектуальної IoT-системи моніторингу параметрів серверної кімнати та її автономного електроживлення. На основі проведеного аналізу міжнародних стандартів, включаючи ANSI/TIA-942, та чинних національних нормативних документів, було спроектовано архітектуру, орієнтовану на вимоги відмовоустійкості інфраструктури рівня між TIER II та TIER III.

У межах апаратно-програмної реалізації створено робочий прототип системи на базі високопродуктивної 32-бітної мікроконтролерної платформи STM32 Nucleo-144 (NUCLEO-F767ZI). Завдяки великій кількості портів введення-виведення (GPIO), до обчислювального ядра підключено розширений масив первинних цифрових та аналогових перетворювачів, які забезпечують точкове зняття метеоданих (DHT11, DS18B20), контроль якості повітря за рівнем CO_2 та вимірювання параметрів мережі змінного струму, а також моніторинг фізичної безпеки й освітленості приміщення (MC-38, LM393). Програмне забезпечення, розроблене в середовищі STM32CubeIDE на мові C, успішно інтегрує оптимізований легковаговий стек протоколів TCP/IP LwIP, що спільно з використанням вбудованого Ethernet-MAC контролера гарантує високу стабільність і завадостійкість зв'язку в умовах інтенсивних електромагнітних завад від серверних стійок, а додаткові бездротові інтерфейси розширюють мобільність системи.

У роботі математично обґрунтовано та програмно впроваджено трирівневу модель станів («Попередження», «Аварія») з використанням алгоритму Магнуса-Тетенса для прецизійного розрахунку температури точки роси в реальному часі. Це дозволило реалізувати механізм випереджувального захисту обчислювального обладнання від ризику випадіння конденсату на друкованих платах. Окрім автоматичного локального керування припливно-

витяжною вентиляцією через блок силових реле, налаштовано мережеву інтеграцію з сервером моніторингу Zabbix та сучасними хмарними сервісами за протоколами MQTT/REST API. Даний підхід дозволив мікроконтролеру самостійно ініціювати трансляцію структурованих пакетів даних у момент фіксації аномалій, що мінімізує паразитний мережевий трафік.

Особливу увагу в проекті приділено концепції багаторівневого гарантованого електроживлення з гібридною структурою. Стабільність важкого обчислювального навантаження сумарною потужністю 610 Вт забезпечується промисловими ДБЖ подвійного перетворення та резервною дизель-генераторною установою (ДГУ) з автоматичним введенням резерву (АВР). Запропоновано та розраховано автономний сонячний контур на базі 4 фотоелектричних модулів загальною потужністю 1200 Вт, акумуляторного LiFePO4 масиву та гібридного інвертора Victron Energy MultiPlus з підтримкою режиму Grid-Tie.

За результатами проектування було виконано комплексне порівняння розробленого прототипу з провідними комерційними за допомогою побудови матриці приведення оцінок до співставного вигляду. Доведено, що створена IoT-платформа впевнено лідирує за критеріями інтегральної ефективності, поєднуючи відкриту архітектуру, мінімальне власне споживання та гнучкість масштабування копійчаними сенсорами. З економічної точки зору, використання платформи на базі STM32 дозволяє знизити первинні капітальні витрати на розгортання апаратної частини порівняно з закордонними корпоративними системами, що підтверджує високу практичну цінність та доцільність впровадження розробленого проекту на IT-підприємствах.

ПЕРЕЛІК ПОСИЛАНЬ

1. Uptime Announces Annual Outage Analysis Report 2026. Businesswire. 2026. Т. 8 : Annual Report analyzes data on IT and data center outages including causes, frequency, costs, and consequences.

2. АвтономнаIoT-система моніторінгу мікроклімату аудиторій на основі відкритої DIY-архітектурі. 2025. Т. 8 : Прикладні питання математичного моделювання. С. 254. URL: https://doi.org/10.32782/mathematical-modelling/2025-8-1-24.

3. TIA-942-C DATA CENTER INFRASTRUCTURE STANDARD. URL: https://tiaonline.org/wp-content/uploads/2024/05/TIA-942-C-DC-infrastructure-stadard_TIA-white-paper.pdf.

4. Tier Standard: Topology. URL: https://dalgakiran.ua/sites/default/files/dalga_infra.pdf.

5. Инфраструктура ЦОД Tier Standard: Topology. uptimeinstitute. URL: https://dalgakiran.ua/sites/default/files/dalga_infra.pdf.

6. What is Data Center Redundancy? N, N+1, 2N, 2N+1. Coresite.com. URL: https://www.coresite.com/blog/data-center-redundancy-n-1-vs-2n-1.

7. ДСТУ EN 50600-1:2022. Засоби та інфраструктури центрів оброблення даних. Частина 1. Загальні поняття. На заміну ДСТУ EN 50600-1:2018 (EN 50600-1:2012, IDT) ; чинний від 31.12.2023. ДП «Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості» (ДП «УкрНДНЦ»), 2022.

8. ISO/IEC 30134-7:2023(en). Iso.org. URL: https://www.iso.org/obp/ui/en/#iso:std:iso-iec:30134:-7:ed-1:v1:en.

9. ДСТУ ISO/IEC 11801-1:2018 Информационные технологии. Кабельные системы общего назначения для помещений пользователей. Часть 1. Общие требования (ISO/IEC 11801-1:2017/Cor 1:2018, IDT). Поправка № 1:2018

10. ДСТУ Б В.2.5-82:2016. Захисні заходи електробезпеки в електроустановках будинків і споруд. На заміну ДБН В.2.5-27-2006. Інститут «Київпромелектропроект», 2006.

11. ДСТУ EN 50600-2-2:2018. ДСТУ EN 50600-2-2:2018 Інформаційні технології. Інфраструктура та устаткування центрів оброблення даних. Частина 2-2. Електропостачання (EN 50600-2-2:2014, IDT). Чинний від 01.10.2010. Технічний комітет стандартизації «Інформаційні технології» (ТК 20), 2018.

12. Google Report Sheds Light on UK Data Centre Heatwave Outage. Digit.fyi. URL: https://www.digit.fyi/google-report-sheds-light-on-uk-data-centre-heatwave-outage/.

13. Data center temperature and humidity guidelines. Techtarget. Data center design and facilities. URL: https://www.techtarget.com/searchdatacenter/tip/Data-center-temperature-and-humidity-guidelines.

14. Готовое решение для мониторинга серверной комнаты на основе контроллера UniPing server solution v3/SMS. Netping. URL: https://netping.ru/products/uniping-server-solution-v3-sms/.

15. Готовое решение для мониторинга серверной комнаты на основе Uniping server solution v3/SMS. monitoring. URL: https://monitoring.bakinity.az/uniping.html.

16. Monitoring System 100T Bundle Rack Monitoring. didactum-security. URL: https://didactum-security.com/en/DI19001.1_monitoring-system-100t-bundle-rack-monitoring.

17. NetBotz Rack Monitor 250 User Guide. Schneider Electric. URL: https://www.se.com/us/en/download/document/990-9890_EN/.

18. What is an automatic transfer switch?. techtarget.com. URL: https://www.techtarget.com/searchdatacenter/definition/Automatic-transfer-switch-ATS?utm_source=chatgpt.com.

19. Role of ATS (Automatic Transfer Switch) in Data Center Power Infrastructure. acdcis.com. UPS & Batteries. URL: https://acdcis.com/blog/2025/role-of-ats-automatic-transfer-switch-in-data-center-power-infrastructure/?utm_source=chatgpt.com.

20. How Does an Automatic Transfer Switch Work?. shanahanpower.com. Blog Posts, Generators, UPS Systems. URL: https://www.shanahanpower.com/how-does-an-automatic-transfer-switch-work/?utm_source=chatgpt.com (дата звернення: 10.04.2026).

21. Скільки кВт генерує сонячна електростанція взимку?. Montazhservice. URL: https://montazhservice.com.ua/skil-ki-kvt-za-den-generue-sonacna-elektrostancia-20-kvt-vzimku/.

22. Battery LiFePO4 LogicPower 19174 12V 50Ah. URL: https://www.elvis.com.ua/en/product/akumulyator-lifepo4-logicpower-12v-128v-50ag-640wh-bms-80a40a-200h165h170mm-56kg-en.html.

23. Сонячні панелі у похмуру погоду, взимку та в дощ – як працюють і скільки енергії дають. URL: https://w2studio.com.ua/uk/sonyachni-paneli-u-pohmuru-pogodu-vzymku-ta-v-doshh-yak-praczyuyut-i-skilky-energiyi-dayut.

24. Ultra-Low Power Digital Gas Sensor for Monitoring Indoor Air Quality. Rcscomponents. URL: https://www.rcscomponents.kiev.ua/datasheets/ccs811datasheet.pdf.

25. Модуль датчик світла на LM393. Rcscomponents. URL: https://www.rcscomponents.kiev.ua/product/modul-datchyk-svitla-na-lm393-3-kontakta_200078.html.

26. NUCLEO-F767ZI. Rcscomponents. URL: https://www.rcscomponents.kiev.ua/product/nucleo-f767zi-s-stm32f767zit6_118384.html.

27. STM32 Nucleo-144 boards. st.com. URL: https://www.st.com/resource/en/user_manual/um1974-stm32-nucleo144-boards-mb1137-stmicroelectronics.pdf.

28. STM32 Nucleo-144 board. Tme. URL: https://www.tme.eu/Document/0dc998245674f2d750f4cd878a04681d/STM32_Nucleo_144.pdf.

29. SNMP trap. Zabbix. User manual. URL: https://www.zabbix.com/documentation/current/en/manual/config/items/itemtypes/snmptrap.

30. Що таке "точка роси" та як її виміряти?. URL: https://ventalab.ua/shcho-take-tochka-rosy-ta-yak-yii-vymiriaty/.

31. Arm® Cortex®-M7 32-bit MCU+FPU, 462 DMIPS, up to 2 MB flash, 512+16+4 KB RAM, USB OTG HS/FS, 28 comm. Int., LCD, DSI. URL: https://www.st.com/resource/en/datasheet/stm32f767zi.pdf.