КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (28), 2025
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2025.28.835
УДК 004.6:621.396:621.3:004.056

Довженко Надія Михайлівна
кандидат технічних наук, доцент, доцент кафедри інформаційної
та кібернетичної безпеки імені професора Володимира Бурячка
Київський столичний університет імені Бориса Грінченка
доцент кафедри цифрових технологій в енергетиці
Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського», Київ, Україна
ORCID ID: 0000-0003-4164-0066
n.dovzhenko@kubg.edu.ua

Іваніченко Євген Вікторович
кандидат технічних наук, доцент,
заступник декана з науково-методичної та навчальної роботи
Київський столичний університет імені Бориса Грінченка, Київ, Україна
ORCID ID: 0000-0002-6408-443X
y.ivanichenko@kubg.edu.ua

Аушева Наталія Миколаївна
доктор технічних наук, професор,
завідувачка кафедри кафедри цифрових технологій в енергетиці
Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського», Київ, Україна
ORCID ID: 0000-0003-0816-2971
nataauscheva@gmail.com

Шевчук Юрій
DataArt, 3530 Carol Ln, Northbrook, Illinois 60062, USA
ORCID ID: 0009-0008-3331-3886
shev4ukyuri@gmail.com

Тарас Луковський
кандидат технічних наук, доцент кафедри захисту інформації
Національний університет "Львівська політехніка", Львів, Україна
ORCID ID: 0009-0008-1652-8121
taras.i.lukovskyi@lpnu.ua

ДОСЛІДЖЕННЯ АРХІТЕКТУРИ ДАТА-ЦЕНТРІВ З ІНТЕГРАЦІЄЮ IOT-КОМПОНЕНТІВ ДЛЯ ЗАБЕЗПЕЧЕННЯ ЕНЕРГОЕФЕКТИВНОСТІ ТА КІБЕРСТІЙКОСТІ

Анотація. Впровадження технології Інтернету речей (IoT) в інфраструктуру центрів обробки даних (ЦОД) є надзвичайно актуальною темою в умовах зростання обсягів оброблюваної інформації, енергоспоживання та розвитку хмарних і AI-сервісів. Інтеграція IoT дозволяє будувати багаторівневі архітектури, що включають розподілені сенсорні мережі, edge computing, інтелектуальну аналітику та автоматизоване управління інфраструктурою в цілому. У роботі проаналізовано типову архітектуру, роль ключових компонентів (сенсорів, актуаторів, шлюзів, edge-вузлів), а також узагальнено практичний досвід провідних компаній щодо оптимізації енергоспоживання та підвищення стійкості інфраструктури. Показано, що використання IoT-компонентів сприяє досягненню значущих показників за ключовими метриками KPI: зниження середнього часу виявлення та усунення відхилень, покращення енергоефективності, підвищення точності виявлення аномалій. Окрема увага приділена аналізу загроз безпеки IoT-інфраструктури у ЦОД, включаючи уразливості протоколу MQTT, відсутність TLS, відкриті API тощо. Підкреслено необхідність впровадження безпечної архітектури IoT за принципом security-by-design, із сегментацією мереж, контролем доступу

та використанням сучасних засобів виявлення та реагування на вторгнення (IDS/IPS). Отримані результати підтверджують перспективність застосування IoT для побудови гнучких, енергоефективних та кіберстійких дата-центрів нового покоління.

Ключові слова: Інтернет речей (IoT); центри обробки даних (ЦОД); енергоефективність; edge computing; управління інфраструктурою ЦОД (DCIM); сенсорні мережі; безпека; інфраструктура; кіберстійкість.

ВСТУП

Сучасна цифрова трансформація суспільства супроводжується стрімким зростанням обсягів даних, що потребують зберігання, оброблення та аналітики. Це, своєю чергою, стимулює постійний розвиток та масштабування центрів обробки даних (ЦОД), які виступають фундаментальними компонентами інформаційно-комунікаційної інфраструктури. На цьому тлі зростає актуальність проблем підвищення енергоефективності, автоматизації процесів, моніторингу операційних параметрів та забезпечення високого рівня безпеки у складних, високонавантажених інженерних середовищах ЦОД.

Оцінювання рівня сталого розвитку (sustainability) центрів обробки даних залишається складним завданням, оскільки наявні метрики зазвичай охоплюють лише окремі аспекти їх функціонування, зокрема повторне використання води або частку енергії з відновлюваних джерел. Водночас варто враховувати, що енергоспоживання ЦОД має істотні наслідки на рівні енергетичних систем: існує підвищений ризик дефіциту енергоресурсів та нестабільності електромереж через зростання попиту на електроенергію.

Одним із перспективних напрямів підвищення ефективності функціонування ЦОД є інтеграція технологій Інтернету речей (IoT). Використання IoT-компонентів у середовищі дата-центрів сприяє переходу до нової моделі управління, що базується на розподілених сенсорних мережах, обчисленнях на периферії (edge computing) та аналітиці великих даних у режимі реального часу. Такий підхід відкриває широкі можливості для оптимізації енергоспоживання, динамічного керування системами охолодження та електричними навантаженнями, а також впровадження предиктивного обслуговування й механізмів раннього виявлення аномалій. У цьому контексті формуються підґрунтя для створення «розумних» дата-центрів, здатних автономно адаптувати внутрішні процеси до змін зовнішнього середовища.

Водночас широке застосування IoT у дата-центрах супроводжується низкою технічних та організаційних викликів. Серед них — необхідність забезпечення кібербезпеки, забезпечення сумісності гетерогенних пристроїв, ефективне управління великою кількістю сенсорів та мінімізація затримок у передачі даних. Перспективи подальшого розвитку цієї сфери значною мірою пов’язані з інтеграцією штучного інтелекту та технологій машинного навчання, що створює передумови для підвищення рівня автономності, гнучкості та адаптивності інфраструктури центрів обробки даних.

АКТУАЛЬНІСТЬ ВПРОВАДЖЕННЯ IOT У СУЧАСНИХ ДАТА-ЦЕНТРАХ

Центри обробки даних залишаються ключовою інфраструктурною платформою для підтримки хмарних сервісів, соціальних мереж, фінансових систем, державних інформаційних ресурсів та обчислювальних задач штучного інтелекту. Протягом останнього десятиліття розміри та енергетичні потреби дата-центрів демонструють стійке зростання. При цьому сучасний ЦОД — це не лише IT-обладнання, а й комплексні

системи енергопостачання, HVAC-комплекси, підсистеми моніторингу та управління надійністю й кібербезпекою сервісів. У результаті дата-центр перетворюється на один із найдинамічніших елементів економіки цифрового бізнесу [1].

Дата-центри нового покоління генерують значні обсяги операційної телеметрії. Окрім характеристик IT-інфраструктури — серверів, мережевих комутаторів і систем зберігання даних — вирішальне значення набувають параметри фізичного середовища: температури, вологості, енергоспоживання, завантаженості систем охолодження тощо. Традиційні засоби моніторингу, що фокусуються переважно на логічному рівні (операційна система, мережеві сервіси), не забезпечують повної картини «фізичного здоров'я» ЦОД. Саме тому індустрія все активніше впроваджує IoT-сенсори та edge-аналітику для реалізації комплексного підходу до моніторингу за концепцією DCIM (Data Center Infrastructure Management) [2].

Концепція розумної будівлі демонструє значний потенціал у контексті автоматизованого управління підключеними пристроями через розгалужені сенсорні мережі. Інтернет речей (IoT) відіграє тут ключову роль, забезпечуючи підключення пристроїв до мережі Інтернет, генерацію даних у реальному часі та вплив на фізичне середовище. Прикладом виступають житлові та офісні приміщення, де цифрові контролери та сенсори стають стандартом. Розумні будівлі оптимізують енергоспоживання, здійснюють моніторинг стану середовища, фіксують активність та керують підключеними пристроями на основі зібраної інформації.

Використання IoT у дата-центрах дозволяє перенести подібну «розумність» у сферу ЦОД, відкриваючи нові підходи до управління ресурсами на основі даних.

Світове енергоспоживання дата-центрів демонструє стійку тенденцію до зростання. Якщо у 2014 році, за оцінками Міжнародного енергетичного агентства (IEA), воно становило близько 194 ТВт·год (≈ 1 % глобального попиту), то до 2022 року збільшилося до 240–340 ТВт·год, що відповідає 1–1,3 % кінцевого світового споживання електроенергії [3].

З огляду на стрімкий розвиток генеративного штучного інтелекту та GPU-кластерів високої продуктивності, IEA прогнозує подвоєння цього показника до ≈ 460 ТВт·год вже у 2024 році та подальше зростання до ≈ 945 ТВт·год до 2030 року. За даними Deloitte, частка дата-центрів у глобальному електроспоживанні може досягти ≈ 2 % (близько 536 ТВт·год) у 2025 році [4].

ISSN 2663 - 4023

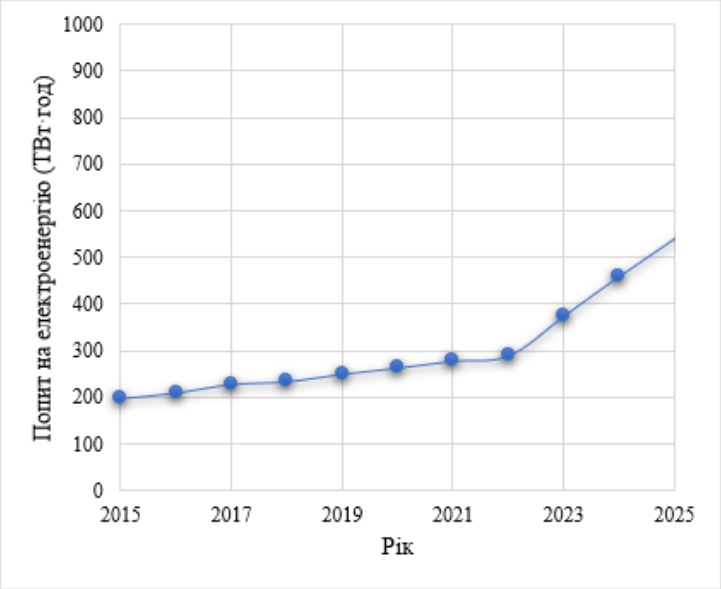

Рис. 1. Глобальна динаміка електроспоживання дата-центів (згідно з даними 2014-2030рр, IEA/Deloitte)

Поряд із цим спостерігається тенденція до зростання фізичних масштабів окремих об'єктів. Зокрема, комплекс Tahoe Reno 1 компанії Switch (кампус «The Citadel», Невада, США) вже охоплює площу близько 120 000 м² із потужністю 130 МВт, з перспективою розширення до 650 МВт. Інший приклад — гіпермасштабний Tulip Data City у Бенгалуру (Індія) із проєктною площею ≈ 90 000 м² та потужністю 100 МВт, розрахований на 12 000 стійок. Зростання таких об'єктів зумовлене вибуховим попитом на хмарні сервіси та аналітику великих даних, що, у свою чергу, є одним із ключових драйверів зростання енергоспоживання ІКТ-сектора.

З економічної точки зору, глобальний ринок дата-центрів демонструє динамічний розвиток. За даними JLL, його обсяг у 2020 році становив 153 млрд дол. США, а до 2026 року очікується зростання до ≈ 317 млрд дол., що відповідає приросту у 107 % за шість років [5]. При цьому щорічні капіталовкладення для підтримання темпів масштабування AI-інфраструктури можуть досягати 6,7 трлн дол. США до 2030 року (Рис. 2).

У структурі операційних витрат ЦОД домінуючим фактором залишається енергоспоживання, що підкреслює необхідність впровадження енергоефективних рішень.

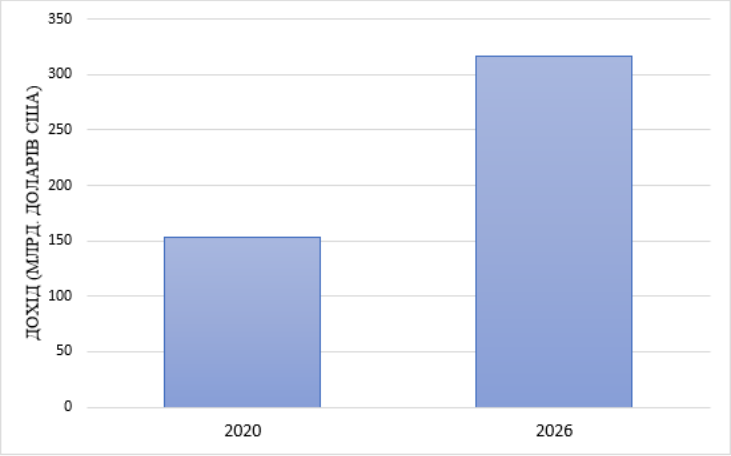

Рис.2. Прогноз зростання доходів світового ринку дата-центрів, 2020–2026 рр

Екологічний аспект також відіграє дедалі важливішу роль. За даними Центру сталого розвитку Мічиганського університету, у 2022 році ІКТ-сектор спожив 1 183 ТВт·год електроенергії (≈4,5% глобального попиту), з яких на дата-центри припало 240–340 ТВт·год. Відповідно до прогнозів IEA, до 2030 року частка ЦОД у структурі попиту ІКТ може зрости до чверті, а викиди CO_2 — подвоїтися за умови недостатніх темпів декарбонізації енергетичних систем [6]. У відповідь на ці виклики галузь інтенсивно інвестує у відновлювані джерела енергії та передові системи охолодження, прагнучи знизити показник PUE до <1,2 навіть для кластерів із тепловим навантаженням >50кВт на стійку.

Щоб гарантувати високу доступність, визначену в угодах про рівень обслуговування (SLA), дата-центри проєктуються з урахуванням відповідного рівня надмірності систем. Класифікація Tier, розроблена Uptime Institute, забезпечує стандартизований підхід до оцінки доступності та надійності інфраструктури. Відповідно до цієї класифікації:

- Tier I передбачає один шлях розподілу електроживлення та охолодження без резервування і забезпечує мінімальний рівень доступності 99.671 %;
- Tier II доповнюється резервними компонентами, підвищуючи доступність до 99.741%;
- Tier III передбачає декілька активних шляхів розподілу з можливістю обслуговування без зупинки й забезпечує 99.982 % доступності;
- Tier IV забезпечує повну відмовостійкість систем і гарантує 99.995 % доступності.

В умовах динамічного розвитку ІКТ-сектора традиційні підходи до управління ресурсами вже не задовольняють потреби сучасних дата-центрів. Саме тому впровадження IoT-компонентів розглядається як перспективний інструмент для забезпечення постійного моніторингу фізичного середовища, адаптивного керування ключовими параметрами роботи систем, інтелектуального розподілу навантажень та оптимізації енергоспоживання [7].

Система IoT у дата-центрах зазвичай включає сенсори температури, вологості, споживання електроенергії, датчики відкриття дверей, диму, вібрацій, води, цифрові лічильники для контролю енергоспоживання у реальному часі, а також контролери систем кондиціонування, вентиляції й резервного живлення.

Переваги такого підходу полягають у можливості реалізації:

- оперативного управління в реальному часі з метою запобігання збоїв та аварій;
- предиктивного обслуговування для мінімізації простоїв;
- оптимального розподілу навантажень на основі актуальних даних;
- енергоефективного керування із потенційним зниженням витрат на охолодження на 30–40 % завдяки використанню динамічних алгоритмів із підтримкою IoT.

Особливо перспективним напрямом є впровадження обчислень на периферії (edge computing), що передбачає локальну обробку великих обсягів даних безпосередньо на вузлах ЦОД. Це дозволяє зменшити затримки, знизити навантаження на магістральні мережі та підвищити масштабованість системи [8].

Водночас широке впровадження IoT у ЦОД супроводжується низкою викликів, серед яких — потреба у стандартизації протоколів, забезпечення кібербезпеки IoT-пристроїв, сумісність обладнання різних виробників та інтеграція з наявною інфраструктурою. Попри

ці труднощі, поступове впровадження IoT-технологій уже сьогодні демонструє позитивні результати в гіпермасштабних дата-центрах провідних компаній, таких як Amazon, Microsoft і Google.

АРХІТЕКТУРА IOT У СЕРЕДОВИЩІ ДАТА-ЦЕНТРУ

Ефективне впровадження IoT-технологій у центрах обробки даних передбачає створення багаторівневої, гнучкої та безпечної архітектури, яка забезпечує взаємодію сенсорних пристроїв, контролерів, обчислювальних вузлів і аналітичних платформ. Такі архітектурні рішення мають підтримувати не лише масштабоване збирання та передачу великих обсягів даних, а й їхню локальну обробку, фільтрацію, зберігання та прийняття рішень у режимі реального часу.

Загалом архітектуру IoT у середовищі ЦОД умовно можна поділити на чотири функціональні рівні.

Перший рівень — рівень збору даних (Data Acquisition Layer) — включає фізичні сенсори та виконавчі пристрої (актуатори), які розміщуються у критичних точках інфраструктури: серверних стійках, системах кондиціонування повітря, джерелах безперебійного живлення (UPS), електричних щитах, вентиляційних каналах. Вони здійснюють вимірювання ключових параметрів, таких як температура, вологість, струм, напруга, вібрації, стан дверей, задимленість тощо. Сучасні сенсори, що підтримують автономне живлення (через PoE або акумулятори), функціонують за допомогою інтерфейсів RS485, I2C, MQTT, Modbus, Zigbee.

Другий рівень — комунікаційний рівень (Network & Connectivity Layer) — відповідає за передачу даних від сенсорів до шлюзів (IoT hubs) або локальних серверів. Тут застосовуються як провідні технології (Ethernet, PoE), так і бездротові протоколи (Wi-Fi 6, Bluetooth Low Energy, Zigbee, LoRaWAN). Особливо важливими аспектами є сегментування мережі для запобігання кіберзагрозам та резервування каналів зв’язку у критичних ділянках.

Третій рівень — рівень обробки даних (Edge Processing & Fog Layer) — передбачає виконання обробки сенсорних даних на периферійних пристроях — edge-серверах або інтелектуальних шлюзах. Тут здійснюється попередня аналітика, агрегація та фільтрація даних, а також виявлення аномалій. Це суттєво зменшує обсяг трафіку, що надходить до центральних серверів, і скорочує час реакції систем. Для таких задач часто використовуються мікросервісні платформи (Docker, Kubernetes) та моделі машинного навчання для предиктивного аналізу.

Четвертий рівень — рівень управління та аналітики (Cloud or On-prem Analytics Layer) — забезпечує довготривале зберігання даних, їхню візуалізацію, прийняття стратегічних рішень та інтеграцію з системами управління ЦОД (DCIM). Аналітичні системи базуються на сховищах типу InfluxDB, TimescaleDB, NoSQL (наприклад, MongoDB), з використанням візуалізаційних інструментів (Grafana, Prometheus, Power BI). Штучний інтелект широко застосовується для оцінки навантажень, аналізу поведінки обладнання, прогнозування відмов та оптимізації енергоспоживання.

Типова IoT-архітектура ЦОД може включати: сенсори температури та вологості у кожному серверному ряду, шлюзи з підтримкою MQTT/REST API, локальний edge-сервер на базі Raspberry Pi або промислового ПК, централізовану платформу (Azure IoT Hub, AWS Greengrass або власну on-premise систему).

Рис. 3 ілюструє типові точки розміщення сенсорів у ЦОД: контроль температури на вході у стійку, диференціальний тиск під підлогою, контроль витрати повітря, виявлення протікань тощо.

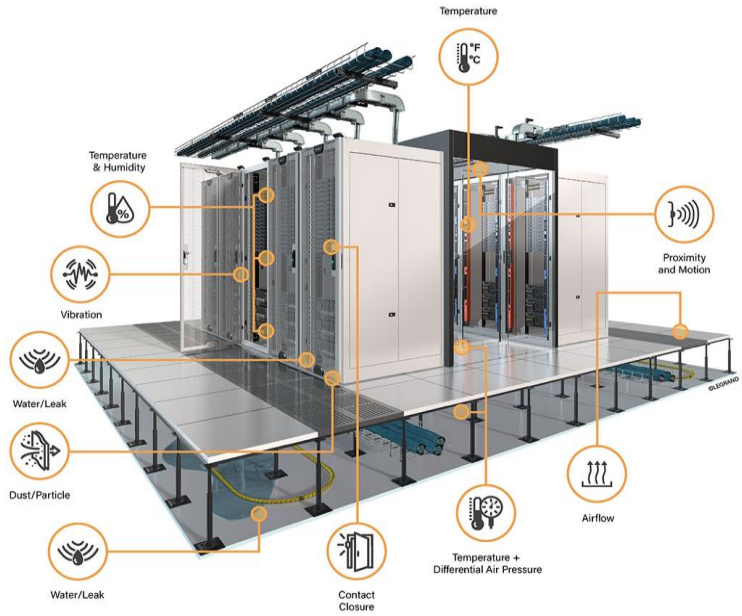

Рис.3. Приклад типової архітектури IoT для ЦОД [9]

Важливо також забезпечити інтеграцію IoT-платформи із наявними системами BMS/SCADA, щоб уникнути фрагментації автоматизації та створити єдине кероване середовище для інженерної та IT-інфраструктури.

Ієрархія взаємодії між рівнями систем зазвичай включає:

- Транспортний рівень — протоколи BACnet/IP, OPC UA або Modbus/TCP забезпечують двосторонню телеметрію між сенсорною підсистемою та контролерами HVAC, PDU й електрощитів;
- Логічний рівень — єдина шина подій (наприклад, Apache Kafka) корелює дані BMS із показниками IoT-сенсорів, забезпечуючи повний контекст для аналітики DCIM;
- Рівень візуалізації — уніфіковані ідентифікатори активів дають змогу будувати консолідовані дашборди для відображення параметрів температури, швидкості повітря, енергоспоживання та індикації збоїв.

Завдяки такій інтеграції оператори ЦОД отримують можливість адаптивно керувати режимами роботи CRAC-блоків, вентиляторів, систем UPS без дублювання функцій та втрати даних.

Безпека архітектури IoT є критичним аспектом. Усі пристрої мають бути захищені шляхом використання унікальних цифрових сертифікатів, шифрування TLS/SSL, контролю доступу на основі ролей, регулярного оновлення прошивок та суворої політики ізоляції IoT-мережі від продукційної мережі ЦОД.

В цілому архітектура IoT у дата-центрах має відповідати таким принципам:

- масштабованість — можливість безперешкодного додавання нових пристроїв;
- надійність — резервування каналів зв’язку та обчислювальних вузлів;
- інтероперабельність — підтримка відкритих стандартів і протоколів;
- енергоефективність — мінімальне енергоспоживання сенсорів та актуаторів;
- відповідність вимогам безпеки і захисту даних (ISO 27001, IEC 62443).

Архітектура IoT у ЦОД є динамічною системою, що функціонує як замкнений цикл: від генерації даних до їх аналізу та прийняття управлінських рішень.

Процес обробки даних у такій архітектурі включає такі етапи (Рис.4):

- Генерація даних IoT-пристроями — безперервний збір телеметрії про стан середовища та обладнання;
- Попередня обробка на периферійних вузлах (edge computing) — фільтрація, агрегація, виявлення аномалій за допомогою ML-моделей;
- Динамічне управління маршрутами передачі (SDN) — оптимізація маршрутизації трафіку на основі актуального стану мережі [10];
- Передача даних до центрального (cloud) ЦОД — зберігання даних, глибока аналітика, прогнозування;
- Прийняття рішень та зворотний зв'язок — автоматизоване управління системами охолодження, живлення, навантаженнями через DCIM-платформи [11].

Після викладення технічної архітектури постає питання кількісного оцінювання її ефективності. Метрики — це ключові інструменти, які дають змогу вимірювати, порівнювати та відстежувати продуктивність систем у динаміці. У контексті ЦОДів метрики дозволяють не лише виявляти зони неефективності, а й оцінювати вплив упроваджених змін, зокрема щодо сталого розвитку.

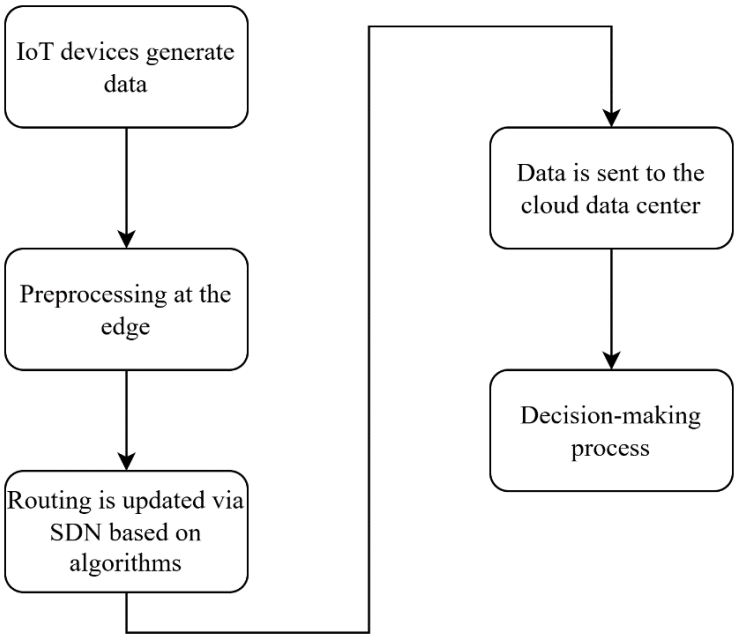

Рис. 4. Потік даних в інфраструктурі Інтернету речей з периферійними обчисленнями та маршрутизацією на основі SDN

Одним із важливих внесків цього розділу є ідентифікація та класифікація метрик за основними вимірами функціонування ЦОД: енергоефективність, охолодження, екологічна сталість, продуктивність, тепловий і повітряний менеджмент, мережеві показники, безпека, сховища та фінансовий вплив.

Класичні SLA-метрики (наприклад, % доступності) не відображають переваг сучасної сенсорної екосистеми та edge-аналітики. Тому для ЦОД із впровадженою IoT-

архітектурою доцільно застосовувати розширений набір KPI, що охоплюють реактивну здатність експлуатаційної команди, енергоефективність та якість алгоритмічного прогнозування.

Їхній повний перелік і цільові орієнтири наведено у таблю 1.

Таблиця 1

Ключові KPI для оцінки ефекту IoT-архітектури

Показник	Опис	Цільове значення
MTTD	Середній час виявлення критичних відхилень	≤ 30 с
MTTR	Середній час відновлення після інциденту	< 15 хв (HVAC-алерти)
ΔPUE	Покращення PUE після впровадження IoT	≥ 0,05 протягом кварталу
Energy Cost Avoidance	Заощаджена енергія завдяки предиктивному охолодженню	≥ 10 % річного споживання
Anomaly Detection Accuracy	Точність ML-моделі (precision / recall)	≥ 95 % / ≥ 90 %

Показники MTTD і MTTR безпосередньо впливають на показник «дні без збоїв» (DBD), тоді як ΔPUE та Energy Cost Avoidance демонструють довгострокові енергетичні ефекти — навіть покращення PUE на 0,05 для об'єкта з потужністю 10 МВт може забезпечити ≈ 4,4 ГВт·год економії на рік. Точність Anomaly Detection Accuracy визначає надійність системи й знижує кількість хибно-позитивних сповіщень.

У сукупності застосування цих метрик створює прозору аналітичну базу для ухвалення рішень щодо масштабування або коригування IoT-стратегії дата-центру.

Сучасна IoT-архітектура в ЦОД — це не просто набір окремих компонентів, а інтегрована, самонавчальна екосистема, що забезпечує безперервний цикл «дані — аналіз — дія». Вона сприяє зниженню ризиків інцидентів, оптимізації операційних витрат та підвищенню енергоефективності, що особливо актуально в умовах зростання вартості енергоресурсів та швидкого масштабування AI-кластерів.

ПРАКТИЧНІ ПРИКЛАДИ ВПРОВАДЖЕННЯ IOT У СУЧАСНИХ ДАТА-ЦЕНТРАХ

Реальні кейси демонструють, що провідні компанії у сфері хмарних обчислень, телекомунікацій і обробки великих даних активно впроваджують технології Інтернету речей (IoT) для оптимізації своєї інфраструктури. Своєю чергою можна згадати застосування сенсорних мереж, edge computing, систем предиктивного обслуговування та інтелектуальної аналітики.

Google впроваджує мережі датчиків для неперервного моніторингу споживання електроенергії, температури й вологості, що дозволило зменшити показник PUE (Power Usage Effectiveness) до рекордних значень. Аналітична платформа Google DeepMind, побудована на методах глибинного підкріплювального навчання, не лише знизила споживання енергії системами охолодження на 40 %, а й довела під час польових експериментів можливість додаткової економії 9 – 13 % завдяки адаптивному керуванню HVAC-обладнанням [12].

Facebook (Meta) оптимізує параметри мікроклімату у серверних залах, застосовуючи сенсори CO_2, швидкості повітря, температури й вологості разом із

системами керування змінною швидкістю вентиляторів. У недавньому дослідженні інженерів Meta продемонстровано, що комплексне управління життєвим циклом IT-обладнання та вдосконалені моделі RL дають змогу скоротити експлуатаційні витрати й водночас зменшити сумарні шкідливі викиди завдяки зниженню частки embodied-carbon у структурі вуглецевого сліду ЦОД [13].

Microsoft Azure використовує комплекс IoT-телеметрії та моделей машинного навчання для предиктивного обслуговування серверного обладнання, що забезпечило 14–21 % економії енергії на охолодження без порушення температурних та експлуатаційних обмежень [14]. Amazon Web Services (AWS) використовує IoT для оптимізації розподілу обчислювальних ресурсів у гібридному середовищі, включаючи edge-локації. Такий підхід мінімізує латентність трафіку IoT-пристроїв користувачів і підвищує ефективність обробки запитів.

IBM інтегрує edge-computing із IoT для скорочення затримок під час обробки телеметричних даних у ЦОД, що уможливлює оперативне балансування навантажень та запобігання збоям у роботі кластерів [15].

Таким чином, на сьогодні застосування IoT у галузі дата-центрів є реальністю для провідних учасників ринку. Дослідження показують, що сенсорна інфраструктура та edge-аналітика не лише дозволяють оптимізувати витрати, а й сприяють підвищенню стійкості, масштабованості та адаптивності ЦОД (рис.5).

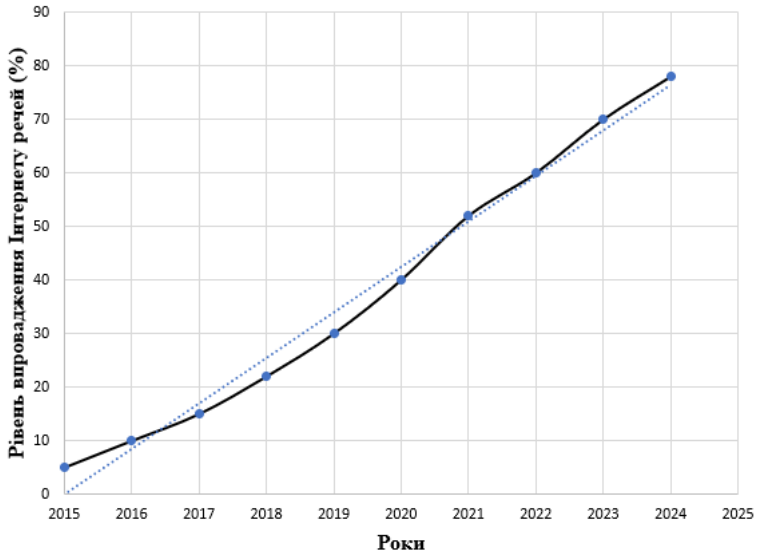

Рис. 5. Тенденції впровадження Інтернету речей (IoT) у центрах обробки даних з 2015 по 2024 рік

На прикладі трьох провайдерів, які інтегрували предиктивну аналітику на основі щільної сенсорної мережі (Digital Realty, Tencent та Nokia Bell Labs), показано, що зниження MTTD та MTTR безпосередньо впливає на скорочення незапланованого простою. Для операторів класу Tier III–IV одна хвилина простою коштує 7–9 тис.дол., отже зменшення часу реагування забезпечує значну економію (рис. 6).

ISSN 2663 - 4023

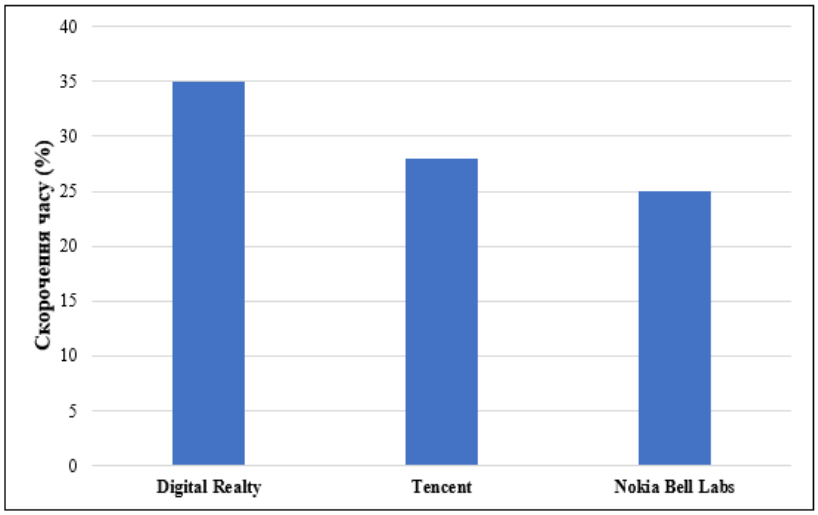

Рис. 6. Скорочення часу реагування на відмови завдяки Інтернету речей

Впровадження IoT у різних регіонах демонструє стабільні результати щодо підвищення енергоефективності. Наприклад, у кластерах у Франкфурті, Сінгапурі та Осло зафіксовано зниження Scope 2-викидів щонайменше на третину завдяки сенсорній оптимізації систем охолодження та точному контролю температури (рис. 7).

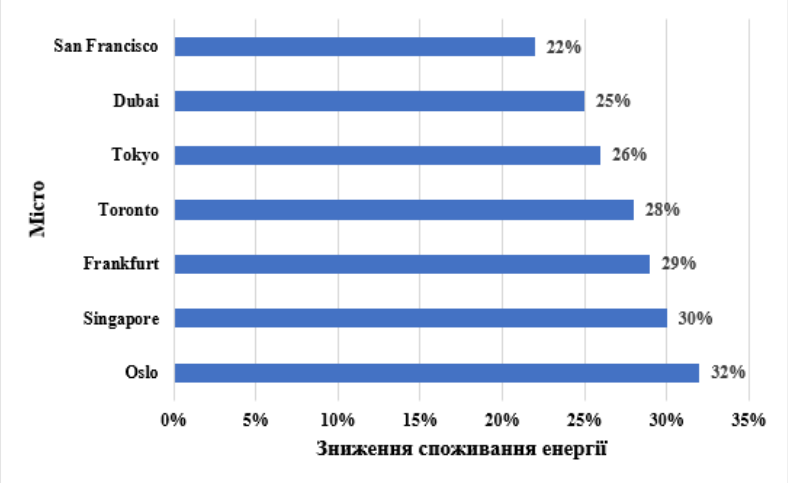

Рис.7. Економія енергії в центрах обробки даних завдяки впровадженню Інтернету речей

Результати підтверджують, що комбінування IoT та edge-аналітики забезпечує універсальний підхід до енергоефективного управління дата-центрами, ефективний як у «холодних» регіонах, так і у мегаполісах із високою тепловою інерцією [17].

ОСНОВНІ IOT-КОМПОНЕНТИ В АРХІТЕКТУРІ ДАТА-ЦЕНТРУ

Сучасні центри обробки даних дедалі активніше впроваджують IoT-технології з метою підвищення енергоефективності, стійкості інфраструктури та гнучкості управління. Енергоефективність у цьому контексті визначається як здатність усіх

підсистем ЦОД забезпечувати цільове обчислювальне навантаження при мінімальних енергетичних витратах. Основними джерелами неефективності залишаються втрати енергії при її перетворенні, нераціональне використання вентиляційних систем, наявність «зомбі»-серверів, неефективні стратегії охолодження та слабка інтеграція автоматизованих засобів керування.

Серед основних практик оптимізації енерговикористання можна відзначити широке впровадження автоматизованих платформ управління (DCIM), віртуалізацію та консолідацію серверних ресурсів, використання технології DVFS для адаптивного регулювання частоти процесорів, боротьбу з неактивними серверами, автоматизоване керування освітленням та — перспективно — розвиток локальних систем генерації енергії.

Успішне впровадження цих практик неможливе без глибокої інтеграції IoT-компонентів на всіх рівнях архітектури ЦОД. Саме сенсорні системи, периферійні вузли обробки даних, актуатори та шлюзи створюють основу для побудови гнучкої, самонавчальної інфраструктури. Їхнє впровадження забезпечує не лише оптимізацію енергоспоживання, а й підвищення експлуатаційної надійності та адаптивність до змін у робочих навантаженнях.

До найважливіших компонентів IoT-інфраструктури ЦОД належать, передусім, сенсори моніторингу мікроклімату. Сенсори температури, вологості, тиску, рівня CO_2 та запиленості повітря дозволяють в реальному часі оцінювати стан навколишнього середовища у серверних залах. На основі цих даних здійснюється динамічне керування системами охолодження, що, згідно з численними практичними кейсами [12] – [14], дозволяє знижувати витрати енергії на 20–30 %. Типовими прикладами таких сенсорів є DHT22, Sensirion SHT3x, Bosch BME680, які встановлюються безпосередньо у серверних стійках та повітроводах.

Важливу роль відіграють також енергетичні сенсори та цифрові лічильники, які здійснюють моніторинг споживання електроенергії як на рівні окремих стояків, так і по фазах живлення. Пристрої на зразок Schneider iEM3155, Siemens Sentron PAC, Shelly EM дозволяють з високою точністю здійснювати облік енергії та створювати оперативні звіти. Це є базою для подальшої оптимізації розподілу навантажень та впровадження моделей прогнозного енергоменеджменту.

Вібраційні сенсори та акселерометри забезпечують моніторинг механічного стану обладнання. Вони встановлюються як на жорстких дисках та системах зберігання, так і на джерелах безперебійного живлення чи компресорах. Сенсори ADXL345, Bosch BMA400 дають змогу виявляти аномальні вібрації, які є раннім індикатором потенційних відмов обладнання.

Інтеграція систем відеонагляду з IoT-інтерфейсом дозволяє поєднувати фізичний контроль доступу з розширеною аналітикою. Камери, такі як Hikvision SmartIP та AXIS IoT-integrated cameras, підтримують ONVIF та відкриті API для інтеграції з DCIM-платформами. Вони є ключовим елементом забезпечення фізичної безпеки та дозволяють автоматизувати виявлення аномальних подій.

Важливим класом пристроїв виступають актуатори та керовані виконавчі механізми, які реалізують фізичні дії у відповідь на результати аналітики або системних тригерів. Це, зокрема, увімкнення/вимкнення вентиляційних систем, перемикання джерел живлення, блокування доступу тощо. Сучасні актуатори — Zigbee-реле, smart contactors, PoE Switch-controlled actuators — тісно інтегруються із сенсорною мережею, створюючи замкнутий цикл «моніторинг — аналітика — дія».

IoT-шлюзи (gateways) відіграють роль проміжної ланки між сенсорами та периферійними обчислювальними вузлами або центральними платформами. Вони

забезпечують буферизацію, первинну обробку та маршрутизацію даних. Широко застосовуються рішення на базі Raspberry Pi з Node-RED, Cisco IR Gateway, Advantech IoT Edge Gateway, які підтримують стандартизовані протоколи обміну — MQTT, CoAP, Modbus.

Таблиця 2

Основні IoT-компоненти в архітектурі дата-центру

Компонент	Функція	Особливості використання в ЦОД
Сенсори температури і вологості	Моніторинг мікроклімату	Розміщуються у стійках, серверних кімнатах, повітроводах, охолоджувачах
Енергетичні сенсори та цифрові лічильники	Облік споживання електроенергії	Зчитування даних з кожної фази або вузла живлення; інтеграція з системами енергоменеджменту
Вібраційні сенсори та акселерометри	Виявлення механічних збоїв	Використовуються для моніторингу дисків, ІБЖ, компресорів, серверних платформ
Камери з IoT-інтерфейсом	Відеонагляд і аналітика	Інтеграція із системами контролю доступу, DCIM; підтримка API (ONVIF)
Актуатори та виконавчі механізми	Реакція на події та автоматизація	Керування вентиляцією, системами живлення, дверима, освітленням
IoT-шлюзи (gateways)	Буферизація та передача даних	Підтримка протоколів MQTT, Modbus, REST API; забезпечення сумісності сенсорної мережі
Периферійні обчислювальні вузли (edge nodes)	Обробка даних, виявлення аномалій	Виконання ML-аналітики та локальних рішень у реальному часі; зниження латентності

Периферійні обчислювальні вузли (edge nodes) виконують функції локальної обробки даних, виявлення аномалій та реалізації алгоритмів машинного навчання. Використання edge-компонентів (NVIDIA Jetson, Intel NUC, Balena edge servers) дозволяє досягати низької латентності та забезпечувати швидку реакцію системи на зміну робочих умов без надмірного навантаження центральних DCIM-серверів.

Комплексна інтеграція зазначених компонентів формує основу для створення замкненого інтелектуального контуру керування інфраструктурою ЦОД: від первинного збору даних — до автоматизованого прийняття рішень та виконання контрольних дій. Завдяки застосуванню таких IoT-архітектур провідні дата-центри демонструють стабільне покращення ключових операційних метрик — зниження середнього часу виявлення відхилень (MTTD), прискорення усунення інцидентів (MTTR), оптимізацію енергоспоживання та підвищення рівня надійності послуг.

Таким чином, IoT-компоненти сьогодні є невід'ємною частиною сучасної архітектури дата-центрів, що дозволяє переходити від реактивних моделей експлуатації до прогнозних та адаптивних стратегій управління інфраструктурою.

ЗАГРОЗИ ТА ВРАЗЛИВОСТІ IOT-КОМПОНЕНТІВ У СЕРЕДОВИЩІ ДАТА-ЦЕНТРУ

Попри значні переваги, що супроводжують впровадження IoT-технологій у центрах обробки даних, їх інтеграція створює новий вектор уразливостей, який потребує належного контролю. Велика кількість малопотужних пристроїв, що часто постачаються з обмеженими ресурсами без вбудованих механізмів захисту, широке використання відкритих протоколів (MQTT, CoAP, Zigbee, BLE), а також відсутність централізованих політик безпеки — усе це формує привабливе середовище для кіберзагроз. Згідно з даними Unit 42 IoT Threat Report (2023), 72 % IoT-пристроїв у дата-центрах мають

критичні або високі уразливості, зокрема незашифрований трафік, слабку автентифікацію та використання застарілих прошивок.

Одним із найбільш поширених векторів атак у середовищі IoT-інфраструктури дата-центрів є віддалене проникнення через незахищені шлюзи. IoT-шлюзи часто працюють на полегшених Linux-дистрибутивах із відкритими службами SSH, Telnet або HTTP/HTTPS за замовчуванням. Уразливості, такі як CVE-2022-0544 (неправильна обробка SSH-ключів), відкривають шлях для отримання root-доступу та подальшого просування вглиб мережі. Показовим є інцидент ShadowPad (2022), у якому злам шлюзів HVAC у колокаційному центрі в Сінгапурі призвів до втрати резервності на рівні N+2.

Не менш актуальною загрозою є зараження IoT-пристроїв ботнетами (Mirai, Mozi, Mukashi). Сканування глобального простору IPv4/IPv6 на наявність типових пар облікових даних дозволяє швидко створювати ботнети, які використовуються для DDoS-атак. У 2022 році NETSCOUT Threat Intelligence зафіксувала атаку 1,12 Tbps, у якій 60 % ботів становили саме IoT-пристрої, розгорнуті у середовищі ЦОД.

Окрім цього, загрозу становлять витоки конфіденційної телеметрії та підміна даних через атаки типу MITM або DNS-spoofing. З метою зниження латентності адміністраторами часто вимикається шифрування TLS на внутрішніх MQTT-каналах, що створює можливості для зловмисників впливати на контроль критичних параметрів. Так, інцидент CoolRISC (2021) демонструє, як зміщення показників диференціального тиску на 15 % призвело до перегріву серверних рядів.

Важливим аспектом є атаки на актуатори, що дають змогу здійснювати фізичний вплив на інфраструктуру ЦОД. Компрометація контролера може призвести до відключення CRAC-блоків, зниження обертів вентиляторів або відключення секцій UPS. Тактика Kill-the-Chiller (MITRE ATT&CK ID T0803), що імітує легітимний сигнал сервісного режиму, у 2019 році призвела до аварійної зупинки колокаційного ЦОД у Далласі на 47 хвилин із втратою ≈200 ТБ даних.

Окремої уваги потребує зловживання специфічними протоколами IoT (Replay, Injection, Spoofing). Використання MQTT 3.1 без шифрування та автентифікації дає змогу зловмисникам підключатися до ключових топіків, а CoAP є чутливим до атак типу UDP reflection. Застосування Replay-атак може спричинити некоректну роботу систем охолодження та перевитрати енергії.

Узагальнену інформацію про поширені вразливості IoT-компонентів у середовищі дата-центру наведено у табл. 3.

Аналіз практичних сценаріїв підтверджує, що більшість уразливостей зосереджені на базовому рівні конфігурації. Вони не потребують складних експлойтів, а можуть бути використані навіть через неавторизований доступ або прослуховування трафіку. Наприклад, бюджетні сенсорні модулі часто постачаються без TLS/DTLS, що робить їх чутливими до підміни критичних показників. Відкриті порти та дефолтні облікові записи на IoT-шлюзах спрощують отримання root-доступу та організацію подальших атак. Камери з відкритими IoT API можуть стати джерелом витоку конфіденційної інформації, а MQTT-брокери без шифрування та контролю доступу перетворюються на потенційні точки повного контролю над системою керування охолодженням.

Таблиця 3

Поширені IoT-вразливості в інфраструктурі дата-центру

Компонент	Типова вразливість	Потенційні наслідки
Сенсори (DHT, BME)	Відсутність TLS, статичні IP-адреси	Зчитування та модифікація даних сенсорів

IoT-шлюзи (Linux-based)	Відкриті порти SSH/HTTP, застарілі ядра	Повний контроль над передачею IoT-трафіку
Камери з IoT API	API без токенів або перевірки доступу	Компрометація відеопотоку, несанкціонований доступ
MQTT-брокери	Незашифрований трафік, відсутність ACL	Захоплення обміну повідомленнями у реальному часі

Як показано на Рис.8, за даними дослідження Ponemon Institute [18], у 2023 році до 40 % зареєстрованих інцидентів у ЦОД були пов'язані саме з IoT-компонентами.

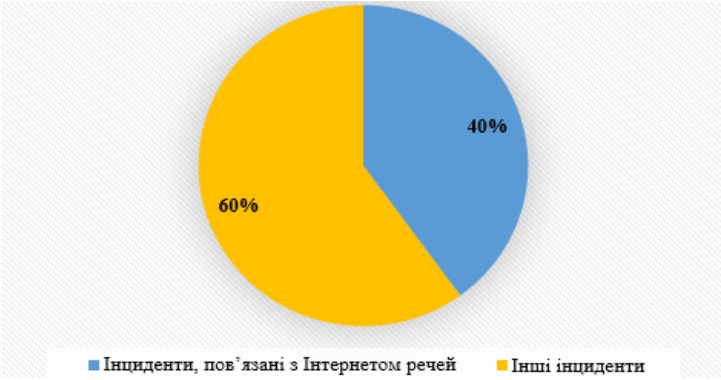

Рис.8. Частка інцидентів, пов'язаних з IoT, у загальній структурі подій ЦОД (2023 р.)

Таким чином, IoT-компоненти, попри свої очевидні переваги для управління дата-центрами, несуть із собою суттєві ризики. Недостатній рівень захисту базових елементів може спровокувати каскадні відмови, вплинути на показники енергоефективності (PUE), призвести до збоїв охолодження чи компрометації фізичної безпеки.

Ефективний захист потребує системного підходу: впровадження TLS 1.3/DTLS для сенсорних каналів, використання унікальних X.509-сертифікатів для шлюзів, повне відключення анонімних MQTT-сесій, впровадження ACL, а також регулярного оновлення прошивок камер і вимкнення тестових облікових записів.

У підсумку, інтеграція IoT у архітектуру ЦОД має супроводжуватися не лише оптимізаційними заходами, а й системною побудовою політик безпеки — що є ключовим чинником забезпечення сталого та безпечного функціонування сучасних дата-центрів.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Інтеграція IoT у середовище дата-центрів сьогодні стає одним із ключових напрямів еволюції їхньої архітектури у відповідь на потреби підвищення енергоефективності, масштабованості та гнучкості управління. Проведене дослідження підтвердило, що застосування IoT-компонентів — сенсорних мереж, edge-аналітики та автоматизованих механізмів керування — забезпечує значний потенціал для оптимізації ключових операційних показників ЦОД. Зокрема, на основі аналізу практичних кейсів провідних компаній продемонстровано, що впровадження IoT-рішень дозволяє досягати зниження енергоспоживання систем охолодження на 20–40 %, скорочення MTTD та MTTR, а також забезпечує більш гнучке управління ресурсами.

У ході роботи систематизовано типову архітектуру IoT для ЦОД, визначено роль основних IoT-компонентів (сенсорів, шлюзів, edge-вузлів, актуаторів), а також наведено приклади їх практичного застосування. Окрему увагу приділено проблематиці

кібербезпеки: проведений аналіз показав, що впровадження IoT-технологій, поряд із перевагами, формує додаткові вектори атак. Найбільш поширеними є загрози, пов'язані з незахищеними сенсорними каналами, відкритими IoT-шлюзами, відсутністю контролю доступу до брокерів MQTT та слабкою аутентифікацією API. Підкреслено важливість впровадження комплексних політик безпеки, що включають застосування TLS/DTLS, X.509-сертифікатів, списків ACL та регулярного оновлення компонентів IoT.

Таким чином, результати дослідження підтверджують, що ефективна інтеграція IoT у архітектуру дата-центрів дозволяє не лише знижувати витрати та підвищувати стійкість інфраструктури, а й формує передумови для переходу до адаптивних і прогнозних моделей управління. Водночас забезпечення кіберстійкості IoT має розглядатися як критично важлива умова для гарантування сталого та безпечного функціонування сучасних ЦОД.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. McKinsey & Company. (2024) The cost of compute: A $7 trillion race to scale data centers. https://www.mckinsey.com/industries/technology-media-and-telecommunications/our-insights/the-cost-of-compute-a-7-trillion-dollar-race-to-scale-data-centers
2. Dovzhenko, N., Mazur, N., Kostiuk, Y., & Rzaieva, S. (2024). Integration of iot and artificial intelligence into intelligent transportation systems. *Electronic Professional Scientific Journal «Cybersecurity: Education, Science, Technique», 2(26),* 430–444. https://doi.org/10.28925/2663-4023.2024.26.708
3. *Digitalisation and energy.* (2021). International Energy Agency. https://www.iea.org/reports/digitalisation-and-energy
4. *As generative AI asks for more power, data centers seek more reliable, cleaner energy solutions.* (2024). Deloitte United States. https://www2.deloitte.com/us/en/insights/industry/technology/technology-media-and-telecom-predictions/2025/genai-power-consumption-creates-need-for-more-sustainable-data-centers.html
5. *Data center market to cross $300 billion by 2026.* (2023). FacilitiesNet. https://www.facilitiesnet.com/datacenters/tip/Data-Center-Market-to-Cross-300-Billion-by-2026--54016
6. *Data centers: Rapid growth will test U.S. tech sector's decarbonization ambitions.* (2024). S&P Global. https://www.spglobal.com/ratings/en/research/articles/241030-data-centers-rapid-growth-will-test-u-s-tech-sector-s-decarbonization-ambitions-13302390
7. Zhebka, V. (2025). Information technologies for real-time monitoring of heterogeneous networks. *Electronic Professional Scientific Journal «Cybersecurity: Education, Science, Technique», 3(27),* 591–603. https://doi.org/10.28925/2663-4023.2025.27.787
8. Barabash, O., Ausheva, N., Dovzhenko, N., Obidin, D., Musienko, A., & Fedchuk, T. (2023). Development of a hybrid network traffic load management mechanism using smart components. in Proc. *IEEE 7th Int. Conf. Methods and Systems of Navigation and Motion Control (MSNMC),* 38–41.
9. *SmartSensors – environmental monitoring for racks.* (2023). https://www.raritan.com/ap/products/power/rack-management/smart-sensors
10. Barabash, O., Kravchenko, Y., Mukhin, V., Kornaga, Y., & Leshchenko, O. (2017). Optimization of Parameters at SDN Technologie Networks. *International Journal of Intelligent Systems and Applications, 9(9),* 1–9. https://doi.org/10.5815/ijisa.2017.09.01
11. Dovzhenko, N., Barabash, O., Musienko, A., Ivanichenko, Y., & Krasheninnik, I. (2024). Enhancing Sensor Network Efficiency Through Optimized Flooding Mechanism. *CEUR Workshop Proceedings, 3654,* 465–470. https://ceur-ws.org/Vol-3654/short15.pdf
12. Luo, J. et al. (2022). Controlling Commercial Cooling Systems Using Reinforcement Learning. https://doi.org/10.48550/arXiv.2211.07357
13. Wu, C.-J. et al. (2024). Beyond Efficiency: Scaling AI Sustainably. *IEEE Micro, 44, 2,* 19–27. https://doi.org/10.48550/arXiv.2406.05303
14. Xianyuan, Z. et al. (2025). Data Center Cooling System Optimization Using Offline Reinforcement Learning. https://doi.org/10.48550/arXiv.2501.15085
15. *Edge computing white paper.* (2022). IBM. https://www.ibm.com/edge-computing
16. Dovzhenko, N., Ivanichenko, Y., Skladannyi, P., & Ausheva, N. (2024). Integration of security and fault tolerance in sensor networks based on the analysis of energy consumption and traffic. *Electronic*

Professional Scientific Journal «Cybersecurity: Education, Science, Technique», 1(25), 390–400. https://doi.org/10.28925/2663-4023.2024.25.390400

17. *Next-generation modular data center white paper.* (2024). Huawei. https://digitalpower.huawei.com/upload-pro/index/index/Prefabricated-Modular-Data-Center-White-Paper.pdf
18. *2023 global study on closing the IT security gap: Addressing cyber-security gaps from edge to cloud.* (2023). Ponemon Institute. https://paths.ext.hpe.com/c/2023-global-study-closing-it-security-gap

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (28), 2025
ISSN 2663 - 4023

Nadiia Dovzhenko
PhD, Associate Professor, Associate Professor of the Department
of Information and Cybernetic Security named after Professor Volodymyr Buryachok
Borys Grinchenko Kyiv Metropolitan University
Associate Professor of the Department of Digital Technologies in Energy
National Technical University of Ukraine «Igor Sikorsky Kyiv Polytechnic Institute» Kyiv, Ukraine
ORCID ID: 0000-0003-4164-0066
n.dovzhenko@kubg.edu.ua

Yevhen Ivanichenko
PhD, Associate Professor,
Deputy Dean for Scientific-Methodological and Educational Work
Borys Grinchenko Kyiv Metropolitan University Kyiv, Ukraine
ORCID ID: 0000-0002-6408-443X
y.ivanichenko@kubg.edu.ua

Nataliya Ausheva
Doctor of Technical Sciences, Professor,
Head of the Department of Digital Technologies in Energy
National Technical University of Ukraine «Igor Sikorsky Kyiv Polytechnic Institute» Kyiv, Ukraine
ORCID ID: 0000-0003-0816-2971
nataauscheva@gmail.com

Yurii Shevchuk
DataArt, 3530 Carol Ln, Northbrook, Illinois 60062, USA
ORCID ID: 0009-0008-3331-3886
shev4ukyuri@gmail.com

Taras Lukovskyy
PhD, Associate Professor of the Department of Information Security
Lviv Polytechnic National University, Lviv, Ukraine
ORCID ID: 0009-0008-1652-8121
taras.i.lukovskyi@lpnu.ua

RESEARCH ON DATA CENTER ARCHITECTURE WITH INTEGRATION OF IOT COMPONENTS FOR ENSURING ENERGY EFFICIENCY AND CYBER RESILIENCE

Abstract: The implementation of the Internet of Things (IoT) technologies into data center (DC) infrastructures is a highly relevant topic amid the increasing volumes of processed information, rising energy consumption, and the development of cloud and AI-based services. The integration of IoT enables the design of multi-layered architectures comprising distributed sensor networks, edge computing, advanced analytics, and automated infrastructure management. This study analyzes a typical architecture, the role of key components (sensors, actuators, gateways, edge nodes), and summarizes the practical experience of leading companies in optimizing energy consumption and enhancing infrastructure resilience. It is demonstrated that the use of IoT components contributes to achieving significant performance improvements across key KPI metrics, including reduced mean time to detect and resolve deviations, improved energy efficiency, and enhanced anomaly detection accuracy. Particular attention is paid to the analysis of security threats within IoT-based DC infrastructures, including MQTT protocol vulnerabilities, lack of TLS encryption, open APIs, and other issues. The necessity of implementing a secure IoT architecture based on the security-by-design principle is emphasized, incorporating network segmentation, access control, and the use of advanced intrusion detection and prevention systems (IDS/IPS). The obtained results confirm the potential of IoT applications in building flexible, energy-efficient, and cyber-resilient next-generation data centers.

Keywords: Internet of Things (IoT); data centers; energy efficiency; edge computing; data center infrastructure management (DCIM); sensor networks; security; infrastructure; cyber resilience.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. McKinsey & Company. (2024) The cost of compute: A $7 trillion race to scale data centers. https://www.mckinsey.com/industries/technology-media-and-telecommunications/our-insights/the-cost-of-compute-a-7-trillion-dollar-race-to-scale-data-centers
2. Dovzhenko, N., Mazur, N., Kostiuk, Y., & Rzaieva, S. (2024). Integration of iot and artificial intelligence into intelligent transportation systems. *Electronic Professional Scientific Journal «Cybersecurity: Education, Science, Technique», 2(26),* 430–444. https://doi.org/10.28925/2663-4023.2024.26.708
3. *Digitalisation and energy.* (2021). International Energy Agency. https://www.iea.org/reports/digitalisation-and-energy
4. *As generative AI asks for more power, data centers seek more reliable, cleaner energy solutions.* (2024). Deloitte United States. https://www2.deloitte.com/us/en/insights/industry/technology/technology-media-and-telecom-predictions/2025/genai-power-consumption-creates-need-for-more-sustainable-data-centers.html
5. *Data center market to cross $300 billion by 2026.* (2023). FacilitiesNet. https://www.facilitiesnet.com/datacenters/tip/Data-Center-Market-to-Cross-300-Billion-by-2026--54016
6. *Data centers: Rapid growth will test U.S. tech sector's decarbonization ambitions.* (2024). S&P Global. https://www.spglobal.com/ratings/en/research/articles/241030-data-centers-rapid-growth-will-test-u-s-tech-sector-s-decarbonization-ambitions-13302390
7. Zhebka, V. (2025). Information technologies for real-time monitoring of heterogeneous networks. *Electronic Professional Scientific Journal «Cybersecurity: Education, Science, Technique», 3(27),* 591–603. https://doi.org/10.28925/2663-4023.2025.27.787
8. Barabash, O., Ausheva, N., Dovzhenko, N., Obidin, D., Musienko, A., & Fedchuk, T. (2023). Development of a hybrid network traffic load management mechanism using smart components. in Proc. *IEEE 7th Int. Conf. Methods and Systems of Navigation and Motion Control (MSNMC),* 38–41.
9. *SmartSensors – environmental monitoring for racks.* (2023). https://www.raritan.com/ap/products/power/rack-management/smart-sensors
10. Barabash, O., Kravchenko, Y., Mukhin, V., Kornaga, Y., & Leshchenko, O. (2017). Optimization of Parameters at SDN Technologie Networks. *International Journal of Intelligent Systems and Applications, 9(9),* 1–9. https://doi.org/10.5815/ijisa.2017.09.01
11. Dovzhenko, N., Barabash, O., Musienko, A., Ivanichenko, Y., & Krasheninnik, I. (2024). Enhancing Sensor Network Efficiency Through Optimized Flooding Mechanism. *CEUR Workshop Proceedings, 3654,* 465–470. https://ceur-ws.org/Vol-3654/short15.pdf
12. Luo, J. et al. (2022). Controlling Commercial Cooling Systems Using Reinforcement Learning. https://doi.org/10.48550/arXiv.2211.07357
13. Wu, C.-J. et al. (2024). Beyond Efficiency: Scaling AI Sustainably. *IEEE Micro, 44, 2,* 19–27. https://doi.org/10.48550/arXiv.2406.05303
14. Xianyuan, Z. et al. (2025). Data Center Cooling System Optimization Using Offline Reinforcement Learning. https://doi.org/10.48550/arXiv.2501.15085
15. *Edge computing white paper.* (2022). IBM. https://www.ibm.com/edge-computing
16. Dovzhenko, N., Ivanichenko, Y., Skladannyi, P., & Ausheva, N. (2024). Integration of security and fault tolerance in sensor networks based on the analysis of energy consumption and traffic. *Electronic Professional Scientific Journal «Cybersecurity: Education, Science, Technique», 1(25),* 390–400. https://doi.org/10.28925/2663-4023.2024.25.390400
17. *Next-generation modular data center white paper.* (2024). Huawei. https://digitalpower.huawei.com/upload-pro/index/index/Prefabricated-Modular-Data-Center-White-Paper.pdf
18. *2023 global study on closing the IT security gap: Addressing cyber-security gaps from edge to cloud.* (2023). Ponemon Institute. https://paths.ext.hpe.com/c/2023-global-study-closing-it-security-gap