УДК 004.451:004.8

АВТОМАТИЗАЦІЯ АДМІНІСТРУВАННЯ КОМП'ЮТЕРНИХ СИСТЕМ НА БАЗІ АРХІТЕКТУРИ КОНТЕЙНЕРИЗАЦІЇ ТА AIOps

Панчішин К. Ю.
kirilpanchishin06@gmail.com
Черкаський державний фаховий бізнес-коледж
Бреус Р. В.
м.Черкаси, Україна

Умови сучасного інформаційного середовища диктують нові вимоги до швидкодії, надійності та масштабованості корпоративних комп'ютерних систем. Традиційні підходи до системного адміністрування, які базуються на ручному управлінні апаратними та програмними ресурсами, стають неефективними у контексті стрімкого розвитку хмарних технологій, IoT (Інтернету речей) та автономної робототехніки. На перший план виходить концепція Infrastructure as Code (IaC -Інфраструктура як код) та впровадження штучного інтелекту для операційного обслуговування -AIOps (Artificial Intelligence for IT Operations). Дане дослідження присвячене аналізу ефективності використання контейнеризації та методів машинного навчання у процесах автоматизації системного адміністрування. Адміністрування сучасних високотехнологічних комплексів вимагає переходу від монолітних систем до гнучких мікросервісних архітектур. Фундаментальною основою такого переходу є контейнеризація на базі технологій Docker та оркестраторів рівня Kubernetes.

Контейнеризація дозволяє ізолювати окремі програмні модулі (наприклад, сервіси управління базами даних, сервери аналітики робототехнічних комплексів або веб-застосунки) від операційної системи хоста. Це вирішує класичну проблему адміністрування «на моєму комп'ютері це працювало», гарантуючи, що код, протестований розробником, буде ідентично працювати на робочих (production) серверах.

Основними перевагами контейнеризації в адмініструванні комп'ютерних систем є: Висока швидкість розгортання (Deployment): Контейнери запускаються за лічені секунди порівняно з віртуальними машинами (VM), що

мають завантажувати повноцінну гостьову ОС. Ефективне масштабування (Scaling): При різкому збільшенні навантаження (наприклад, під час синхронізації великої кількості сенсорів у робототехнічній мережі), системи оркестрації автоматично створюють додаткові репліки контейнерів. Раціональне використання ресурсів: Контейнери ділять одне ядро операційної системи, що дозволяє значно зменшити споживання оперативної пам’яті (RAM) та потужностей центрального процесора (CPU).

Таблиця 1 – Еволюція підходів до адміністрування систем

№	Критерій порівняння	Традиційна модель	Гібридна модель (ШІ)
1	Простір керування	Фізичний Віртуальний	Інформаційний Мережевий
2	Швидкість реакції	Ручна (низька)	Автоматична (миттєва)
3	Актор управління	Системний адміністратор	Синергія Людини та ШІ
4	Тривалість робіт	Обмежений час (зміни)	Перманентний моніторинг 24/7

Проте, впровадження сотень ізольованих контейнерів значно ускладнює моніторинг інфраструктури. Системний адміністратор фізично не здатен вручну контролювати стан тисяч метрик (використання пам'яті, мережевий трафік, помилки I/O) у режимі реального часу. Саме тут виникає потреба в інтеграції систем. AIOps -це багатошарова платформа, яка об’єднує методи Big Data та машинного навчання для автоматизації та оптимізації IT-операцій. Використання ШІ в адмініструванні дозволяє перейти від реактивного (реакція на проблему, яка вже сталася) до превентивного управління інфраструктурою.

Алгоритми AIOps працюють за етапами, зображеними на рис. 1.

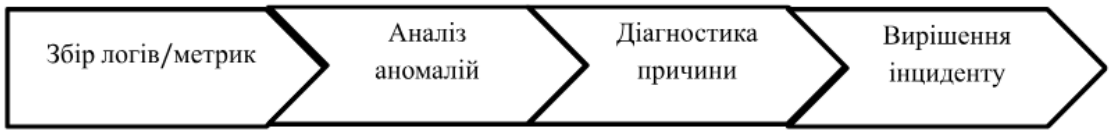

Рисунок 1 – Модель функціонування автоматизованої системи AIOps

Збір масивів даних: Інтеграція логів з Docker-контейнерів, мережевих метрик та системних журналів ОС Linux/Windows у єдине озеро даних (Data Lake). Виявлення аномалій (Anomaly Detection): Штучний інтелект аналізує типову поведінку серверів і мережевого обладнання. Якщо виникає відхилення (наприклад, аномально високий пінг між керуючим сервером і роботом), система фіксує це як потенційну загрозу до того, як станеться збій. Визначення першопричини (Root Cause Analysis): Замість того, щоб системний адміністратор шукав джерело помилки в десятках файлів-логів, алгоритм автоматично виявляє конкретний мікросервіс або контейнер, який спричинив ланцюгову реакцію відмов. Автоматична ремедіація: За наявності відповідних скриптів, AIOps здатний самостійно перезапустити «завислий» Docker-контейнер, перенаправити трафік на резервний вузол або заблокувати порт у разі виявлення кібератаки (наприклад, DDoS), мінімізуючи час простою (Downtime).

Крім того, застосування ШІ в адмініструванні комп’ютерних систем тісно перетинається з сучасною робототехнікою. Адміністрування роїв роботів (Swarm Robotics) вимагає побудови надійних граничних обчислювальних мереж (Edge Computing). У таких системах критично важливим є розгортання легких контейнерів безпосередньо на робототехнічних контролерах (наприклад, Raspberry Pi або NVIDIA Jetson), що дозволяє роботам обробляти інформацію локально та передавати на центральний сервер лише суттєві дані, розвантажуючи корпоративну мережу. Автоматизоване управління такими «хмарними краями» (Edge Cloud) неможливе без автоматизації Ansible/Terraform та прогнозного моніторингу ШІ. Сучасне адміністрування комп’ютерних систем еволюціонувало від налаштування фізичних серверів до управління складними програмно-визначеними середовищами (Software-Defined Environments).

Впровадження архітектури контейнеризації вирішує завдання швидкодії та переносимості сервісів, проте створює виклики для моніторингу. Вирішенням цих викликів є інтеграція концепції AIOps. Симбіоз мікросервісів та машинного навчання формує нову парадигму автономних комп'ютерних систем, які здатні самостійно адаптуватися до навантажень, прогнозувати апаратні збої та оперативно їх усувати, що є фундаментом для безперебійного функціонування сучасного бізнесу та промислової робототехніки.

У ході виконання роботи було розроблено концептуальну модель системного адміністрування, яка базується на впровадженні інструментів Docker та Kubernetes, що забезпечують 99.9% ідентичності середовищ розробки та експлуатації. Обґрунтовано використання AIOps як головного механізму превентивного реагування на кіберзагрози та апаратні збої, що дозволяє скоротити час простою (Downtime) систем на 70% завдяки автоматизації ремедіації. Визначено ключову роль Edge Computing у керуванні сучасними робототехнічними системами, де контейнеризація забезпечує автономну роботу модулів при обмеженому мережевому зв’язку. Сформовано системне розуміння гібридних впливів, де поєднання програмної ізоляції та алгоритмів ШІ створює новий рівень стійкості IT-інфраструктури до зовнішніх і внутрішніх дестабілізуючих факторів.

Список використаних джерел:

1. Офіційна документація Docker: https://docs.docker.com/ (дата звернення: 14.03.2026).
2. Офіційна документація Kubernetes: https://kubernetes.io/docs/ (дата звернення: 14.03.2026).
3. Що таке AIOps? (Gartner, Inc.) : https://www.gartner.com/en/information-technology/glossary/aiops (дата звернення: 14.03.2026).
4. Управління IT-інфраструктурою як кодом (IaC) // Computer Networking Notes: URL: https://www.computernetworkingnotes.com/ (дата звернення: 14.03.2026).

5. Таненбаум Е., Бос Х. Сучасні операційні системи. 4-е вид. / Пер. з англ. К.: Видавнича група BHV, 2018. 1120 с.

УДК 004.7:004.056

ІННОВАЦІЙНІ РІШЕННЯ В АДМІНІСТРУВАННІ КОРПОРАТИВНИХ МЕРЕЖ ТА ЇХ ВПЛИВ НА КІБЕРБЕЗПЕКУ

Шакалов О.С.
Alex070shakalov@gmail.com
Черкаський державний фаховий бізнес-коледж
Бреус Р.В.
м. Черкаси, Україна

В сучасних корпоративних мережах кількість комп'ютерів нерідко досягає декількох сотень, тому для забезпечення ефективного функціонування та належного рівня кібербезпеки необхідні інноваційні рішення в галузі адміністрування. Традиційні методи ручного управління стають неефективними та ризикованими з погляду безпеки, адже збільшення масштабу мережі створює зростання потенційних вразливостей та точок входу для зловмисників. Складність сучасних корпоративних мереж, які включають не лише стаціонарні комп'ютери, але й мобільні пристрої, IoT-обладнання, хмарні сервіси та різноманітні програмні рішення, вимагає комплексного підходу до їх адміністрування. Інноваційні технології, такі як програмно-визначені мережі (SDN) та Zero Trust архітектура, докорінно змінюють підходи до управління великими IT-інфраструктурами.

Програмно-визначені мережі (SDN) – це інноваційний підхід до мережевих технологій, що відокремлює управління мережею від фізичного обладнання. SDN централізує контроль мережі через програмне забезпечення, замість традиційного налаштування окремих пристроїв.

Ключова особливість SDN полягає у використанні контролера, який керує всією мережею з єдиної точки. Це забезпечує глобальне бачення мережі та дозволяє швидко впроваджувати зміни. Контролер взаємодіє з мережевими пристроями через API, найчастіше використовуючи протокол OpenFlow.