

УДК 004.7

*Єфіменко А. А., магістрант
Єфіменко А.А., к.т.н., доцент*

Державний університет «Житомирська політехніка»

АДАПТАЦІЯ МЕТОДОЛОГІЇ DEVOPS ДЛЯ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ТА БЕЗПЕКИ ІОТ-СИСТЕМ

Від «розумних» будинків, що функціонують на основі взаємопов'язаних пристроїв, до промислової автоматизації та концепцій «розумних міст», які базуються на використанні автономних сенсорів, стрімкий розвиток технологій Інтернету речей (ІоТ) суттєво трансформує сучасні галузі та сприяє формуванню нових бізнес-моделей. Водночас управління такими складними екосистемами пов'язане зі значними викликами. ІоТ-системи взаємодіють із великою кількістю пристроїв, опрацьовують значні обсяги даних у реальному масштабі часу та вимагають високого рівня надійності, масштабованості й безпеки.

Традиційні підходи до управління життєвим циклом програмного забезпечення, орієнтовані на розробку стандартизованих рішень, виявляються недостатньо ефективними в умовах ІоТ-середовищ. Це зумовлює необхідність адаптації сучасних інженерних практик, зокрема DevOps, до специфіки таких систем [1].

Методологія DevOps розглядається як сучасна інженерна парадигма, що поєднує процеси розробки та експлуатації програмного забезпечення з метою підвищення рівня автоматизації та скорочення часу доставки змін. Вона застосовується не лише у класичних ІТ-системах, але й у вбудованих рішеннях, зокрема в робототехніці та системах інтелектуальних агентів. [2] У свою чергу, екосистема ІоТ подається як набір фізичних пристроїв, таких як датчики та виконавчі пристрої, зінтегрованих в розлогих мережевих структурах, що містять набори серверів та шлюзів, які забезпечують надійне їх підключення та взаємодію.

Аналіз наукових і технічних джерел свідчить, що DevOps-методологія широко застосовується у хмарних і веб-орієнтованих системах, забезпечуючи безперервну інтеграцію, доставку та автоматизацію процесів розробки і експлуатації. Водночас її застосування у сфері ІоТ залишається обмеженим через низку специфічних факторів, зокрема обмеженість обчислювальних ресурсів пристроїв, гетерогенність апаратного забезпечення, складність реалізації безпечних механізмів оновлення програмного забезпечення (ОТА), а також нестабільність мережевих з'єднань [3]. У науковій літературі недостатньо представлено цілісні підходи до інтеграції

DevOps-практик у життєвий цикл IoT-систем, що враховують зазначені обмеження та забезпечують узгодженість між етапами розробки, тестування, розгортання та моніторингу.

Метою дослідження є формування підходу до адаптації DevOps-методології для IoT-систем, визначення її ключових принципів та розроблення концептуальної моделі, яка забезпечує автоматизацію процесів розробки, тестування, розгортання та супроводу IoT-пристроїв з урахуванням їх специфічних характеристик. Основна ідея дослідження полягає у встановленні відповідності між типовими проблемами IoT-середовищ та можливостями DevOps-практик, а також у формуванні узагальненої моделі, що інтегрує підходи безперервної інтеграції, доставки та моніторингу в єдину систему управління життєвим циклом IoT.

У межах дослідження проведено ідентифікацію основних проблем IoT-систем, зокрема складності архітектури, відсутності автоматизованих процесів розгортання, обмежених можливостей моніторингу та підвищених ризиків інформаційної безпеки. На основі цього здійснено зіставлення зазначених проблем із відповідними DevOps-практиками, включаючи використання CI/CD для автоматизації процесів збірки та розгортання firmware, а також впровадження засобів централізованого моніторингу та управління конфігураціями.

Отримані результати дозволили узагальнити підходи до інтеграції DevOps у IoT-системи та сформулювати концептуальні положення щодо побудови адаптованої DevOps-моделі, яка враховує обмеження IoT-пристроїв та специфіку їх функціонування.

Таким чином, адаптація DevOps-методології до IoT-середовищ може слугувати основою для підвищення ефективності та безпеки функціонування розподілених систем. Перспективи подальших досліджень включають розроблення спеціалізованих DevSecOps-рішень для IoT, інтеграцію механізмів автоматизованого аналізу безпеки.

Список використаних джерел

1. Жовнір , Ю., Грибовський , О., Орлов, М., Дуда, О., & Кунанець, Н. "Методологія розроблення та супроводу інформаційних систем, базованих на технології інтернету речей", Управління розвитком складних систем, (60), 56–70, 2024.
2. LALIT SAINI, Dr. VISHAL SHRIVASTAVA, Dr. KRISHAN KANT LAVANIA, Dr. AKHIL PANDEY, "DevOps in IOT", International Journal of Research Publication and Reviews, vol. 5, no. 4, pp. 297-308, 2024.
3. Georges Bou Gbantous, Asif Qumer Gill, "Evaluating the DevOps Reference Architecture for Multi-cloud IoT-Applications," SN Computer Science, vol. 2, no. 3, pp. 1-12, 2021.