УДК 004.75:004.77

# ІНСТРУМЕНТИ МОНІТОРИНГУ В DEVOPS-АРХІТЕКТУРАХ

Астахов Д.Ю.[1]; Трофименко О.Г. к.т.н., доц.[2]
[1,2] Національний університет «Одеська юридична академія»
[1,2] Україна, Одеса
[1] astakhovnil@gmail.com; [2]ORCID: 0000-0001-7626-0886

***Анотація.*** *Здійснено порівняльний аналіз сучасних інструментів моніторингу, які застосовуються в DevOps-архітектурах. Розглянуто функціональні особливості Prometheus, Grafana, Zabbix, ELK Stack та Datadog, визначено їхню релевантність до різних типів інфраструктур і задач спостережуваності. Запропоновано критерії вибору інструментів залежно від вимог до глибини аналізу, типу даних і архітектури системи.*
***Ключові слова****: DevOps; моніторинг; інструменти моніторингу; хмарна архітектура.*

***Вступна частина***. У сучасних умовах цифрової трансформації та зростання складності інформаційних систем, забезпечення їх стабільності, адаптивності та керованості стає критично важливим завданням. Особливої актуальності набуває моніторинг як інструмент не лише технічного контролю, а й стратегічного управління ризиками, продуктивністю та безпекою. У DevOps-культурі, яка базується на принципах неперервної інтеграції, доставки та експлуатації, моніторинг трансформується з реактивного механізму у проактивну систему підтримки життєвого циклу програмного забезпечення.

***Мета роботи*** – систематизація функціональних характеристик сучасних інструментів моніторингу і визначення критеріїв вибору відповідного інструмента залежно від типу даних, архітектури системи та вимог до глибини аналітики.

***Основна частина***. Сучасні інструменти моніторингу не лише збирають метрики, журнали та трасування, а й інтегруються з аналітичними платформами, забезпечуючи основу для математичного моделювання, прогнозування та прийняття рішень у складних динамічних середовищах. Зараз у DevOps-архітектурах широко застосовуються інструменти Prometheus, Grafana, Zabbix, ELK Stack та Datadog.

*Prometheus* (https://prometheus.io/) – це відкритий інструмент моніторингу та оповіщення, розроблений для хмарно-орієнтованих середовищ. Його архітектура базується на моделі збору часових рядів метрик через HTTP-запити, що дозволяє ефективно інтегрувати його з мікросервісами та контейнерами. Prometheus підтримує гнучку мову запитів PromQL, яка дозволяє формулювати складні аналітичні запити для виявлення аномалій, трендів та кореляцій. Його агентська модель (через node_exporter) забезпечує глибоку інтроспекцію, а можливість інтеграції з Alertmanager дозволяє реалізувати реактивні та проактивні сценарії реагування [1]. У поєднанні з Grafana, яка забезпечує візуалізацію даних, Prometheus формує основу для реалізації наскрізної спостережуваності мікросервісної архітектури.

*Grafana* (https://grafana.com/) – це платформа візуалізації, яка часто використовується в парі з Prometheus, але також підтримує понад 30 джерел даних, включно з Elasticsearch, InfluxDB, Loki та іншими. Вона дозволяє створювати динамічні дашборди, що є критично важливими для оперативного аналізу стану системи. Grafana підтримує анотації, порогові значення, алерти та інтеграцію з зовнішніми системами, що робить її універсальним інструментом для команд DevOps, SRE та SecOps.

*Zabbix* (https://www.zabbix.com/) є універсальним рішенням, що підтримує як агентський, так і безагентський режим збору даних. Його функціональність охоплює моніторинг серверів, мережевого обладнання, баз даних та вебзастосунків. Завдяки гнучкій системі тригерів і

шаблонів, комплексна платформа моніторингу Zabbix придатна для масштабованих інфраструктур з гетерогенними компонентами. Її можливості інтеграції з SNMP, IPMI та JMX роблять її придатною для гібридних середовищ, де поєднуються фізичні та віртуальні ресурси.

*ELK Stack* (Elasticsearch, Logstash, Kibana) (https://www.elastic.co/elastic-stack/) – це потужна екосистема для логування та аналізу подій. Elasticsearch забезпечує індексацію та пошук, Logstash – збір і трансформацію даних, а Kibana – візуалізацію. ELK особливо ефективний для аналізу журналів безпеки, трасування подій та побудови кореляційних моделей. У поєднанні з Beats або Filebeat, ELK може працювати як агентська система, що дозволяє реалізувати глибоку спостережуваність у складних багаторівневих архітектурах.

*Datadog* (https://www.datadoghq.com/) – комерційна хмарна платформа моніторингу та аналітики, яка підтримує понад 500 інтеграцій з хмарними сервісами, базами даних, контейнерами та фреймворками. Вона поєднує метрики, логи, трасування та безпеку в єдиному інтерфейсі, що дозволяє реалізувати наскрізну спостережуваність [2]. Datadog підтримує машинне навчання для виявлення аномалій, автоматичне масштабування та інтеграцію з CI/CD-пайплайнами, що робить її особливо релевантною для DevSecOps-практик.

На рис. 1.1 наведено UML-діаграму компонентів, яка моделює структурну інтеграцію інструментів моніторингу в архітектуру DevOps-пайплайну, а узагальнені характеристики розглянутих інструментів – в табл. 2.1.

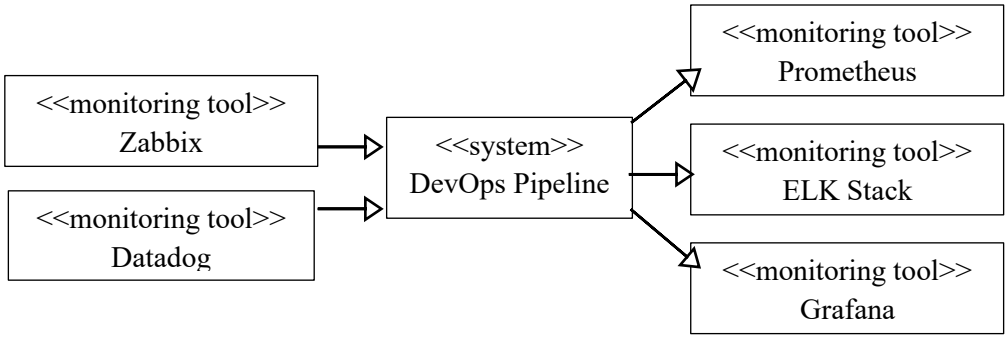


Рисунок 1.1 – Діаграма компонентів структурної інтеграції інструментів у DevOps-пайплайн

Таблиця 2.1 – Порівняння сучасних інструментів моніторингу в DevOps

| Інструмент | Тип даних | Архітектура | Підтримка агентів | Основні функції | Підходить для |
|---|---|---|---|---|---|
| Prometheus | Метрики (база часових рядів, TSDB, Time Series Database) | Модель збору даних pull (pull-based) | + | Збір часових рядів, мова запитів PromQL, система оповіщень (alerting) | Мікросервісна архітектура, Kubernetes |
| Grafana | Візуалізація даних | На основі інформаційних панелей (dashboard-based) | - | Створення дашбордів, оповіщення, інтеграція з Prometheus, ELK Stack | Візуальний аналітичний моніторинг |
| Zabbix | Метрики, журнали подій (логи) | Agent/ Agentless | ± | Моніторинг серверів, SNMP, шаблони, тригери, авто-виявлення ресурсів | Гібридні інфраструктури |
| ELK Stack (Elasticsearch, Logstash, Kibana) | Логи, події | Конвеєрна архітектура (pipeline-based) | + | Індексація, пошук, візуалізація, кореляція подій | Аналітика безпеки, аудит |
| Datadog | Метрики, логи, трасування | Хмарна модель (SaaS, agent-based) | + | Індексація, пошук, візуалізація, кореляція, ML-аналітика, інтеграції, моніторинг CI/CD, безпека | Хмарні середовища, DevSecOps |

Жоден із розглянутих інструментів не є універсальним у повному сенсі. Наприклад, Prometheus не обробляє журнали подій, що обмежує його застосування для аудиту безпеки або аналізу логів. Він також не підтримує трасування запитів без додаткових інтеграцій. Grafana не виконує збір даних, тому її застосування обмежується візуалізацією та аналітикою. Zabbix має обмежену підтримку сучасних хмарних сервісів і контейнерних платформ, що ускладнює його використання в Kubernetes-середовищах. ELK Stack не збирає метрики у форматі часових рядів, тому не придатний для аналізу продуктивності або автоматичного масштабування [3]. Datadog, хоча й охоплює всі типи даних, є комерційним рішенням, що може бути недоступним для невеликих команд або академічних проєктів.

Зважаючи на специфіку, Prometheus доцільно використовувати для моніторингу мікросервісів, контейнерів та хмарних середовищ, де критично важливий збір метрик у реальному часі. Його інтеграція з Kubernetes є однією з найкращих у галузі. Grafana рекомендована як універсальний інтерфейс саме для візуалізації даних з різних джерел, особливо коли потрібно швидко створити дашборди для ухвалення рішень. Zabbix оптимальний для традиційних IT-інфраструктур, включно з фізичними серверами, мережевим обладнанням та базами даних, позаяк його гнучка система тригерів дозволяє реалізувати складні сценарії реагування. ELK Stack є незамінним для аналізу логів, безпекових подій та аудиту. Його застосування доцільне в системах, де важлива кореляція подій та трасування інцидентів. Datadog рекомендований для великих хмарних платформ, DevSecOps-проєктів та середовищ з високими вимогами до інтеграції, автоматизації та безпеки.

***Висновки***. Кожен із інструментів має свої переваги, залежно від архітектури системи, вимог до глибини аналізу та типу даних. Вибір інструмента моніторингу має базуватися на вимогах до типу даних, архітектури системи, глибини інтроспекції та можливостей інтеграції з аналітичними модулями. У контексті проєктування складних інформаційних систем ці інструменти забезпечують основу для реалізації математичних моделей прогнозування, класифікації та оптимізації, що відповідає цілям дослідження та професійної підготовки в галузі DevOps та інформаційної безпеки.

## СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ


[1] Golems GABB. (2025, Jule 25). *Monitoring tools for Kubernetes: Prometheus vs Grafana vs Datadog*. https://gole.ms/blog/monitoring-tools-kubernetes-prometheus-vs-grafana-vs-datadog

[2] Better Stack. (2025, January 12). *Datadog vs. Prometheus: a side-by-side comparison for 2025*. https://betterstack.com/community/comparisons/datadog-vs-prometheus/

[3] Refonte Learning. (2025, April 24). *Monitoring & Logging with Prometheus, Grafana, ELK, and Loki (2025 Guide for DevOps).* https://www.refontelearning.com/blog/monitoring-logging-prometheus-grafana-elk-stack-loki



Astakhov D.Yu., Trofymenko O.G.


**Monitoring tools in DevOps architectures**


***Abstract.*** *A comparative analysis of modern monitoring tools used in DevOps architectures is performed. The functional features of Prometheus, Grafana, Zabbix, ELK Stack and Datadog are considered, their relevance to different types of infrastructures and observability tasks is determined. Criteria for selecting tools are proposed depending on the requirements for the depth analysis, data type and system architecture.*



***Keywords:*** *DevOps; monitoring; monitoring tools; cloud architecture.*