УДК 004.722:621.391

СИСТЕМИ МОНІТОРИНГУ ТА ПРОГНОЗУВАННЯ НАВАНТАЖЕННЯ В ІНФОКОМУНІКАЦІЯХ

Костромицький А.І., Кривонос П.Р.
e-mail: andrii.kostromytskyi@nure.ua, pavlo.kryvonos@nure.ua
Харківський національний університет радіоелектроніки, каф. ІМІ
м. Харків, Україна

This work explores the importance of load forecasting systems in infocommunications and implementation of monitoring systems according to modern system requirements to ensure constant availability and prevent incidents. Tools for ensuring constant availability and monitoring were proposed and explained their functionality, this includes ELK stack for log monitoring, Prometheus for system physical and program specific metrics, auto-scaling tools such as AWS Auto Scaling which can be used with Prometheus to create specific rules of auto scaling. Load Balancing tools were proposed to ensure availability even on incident appearance by redirecting traffic from broken instances to working ones without downtime.

Метою роботи є аналіз необхідності імплементації систем моніторингу в інфокомунікаційних системах для покращення досвіду користувачів та попередження інцидентів.

Інфокомунікаційні системи вже давно стали невід'ємною частиною сучасного світу; від них залежать майже всі процеси: від спілкування між людьми до складання складних пристроїв. Такі системи, незалежно від масштабів та складності, потребують постійного контролю і можливості відновити роботу якомога швидше при виникненні інцидентів.

Для контролю параметрів систем використовуються програми для моніторингу тієї чи іншої частини інфраструктури, наприклад, стек ELK (Elasticsearch, Logstash, Kibana) пропонує можливість детального аналізу журналів (логів) системи. Для контролю телеметрії та фізичних показників системи використовується інструмент Prometheus з експортерами метрик. Використання даних інструментів дає змогу аналізувати інциденти, попереджати їх та реагувати на них вчасно. Однак варто враховувати, що хмарні провайдери мають вбудовані інструменти моніторингу, що можуть підійти для контролю навантаження на ділянки системи, тому кращим способом застосування сторонніх інструментів збору метрик буде перевірка специфічних показників, наприклад, показників безпосередньо центрів обробки інформації [1].

Особливу увагу у разі використання сторонніх інструментів моніторингу варто приділити безпеці передачі даних, оскільки передача логів та метрик відбувається шляхом їх відправлення з цільового сервісу, що контролюється, до екземпляру, що отримує, обробляє та зберігає ці дані. Здебільшого такі інструменти мають окремі порти, за якими вони і працюють, однак це не гарантує захисту від можливого втручання в процес

передачі, що може призвести до маніпуляцій з трафіком. Зазвичай для забезпечення безпеки в такому випадку відповідні порти відкриваються виключно для сервісів, що передають та отримують дані, однак більш безпечним методом буде розгортання систем в ізольованій мережі.

Для забезпечення доступності такі провайдери, як Microsoft Azure, AWS, пропонують інструменти масштабування з можливістю вказання умов, за яких відбувається запуск додаткових вузлів. Найбільш оптимальним методом для автоматичного масштабування буде саме адаптивне масштабування, оскільки при цьому методі хмарний провайдер зчитує метрики системи і на основі певних метрик приймається рішення про масштабування. Таким чином, використання Prometheus дає можливість створювати правила для автоматичного масштабування за певних потреб. Окремим пунктом забезпечення доступності є налаштування системи балансування навантаження (Load Balancing), завдяки якій трафік рівномірно розподіляється між всіма екземплярами інфокомунікаційної системи; така система значно зменшить навантаження, а у разі виникнення інцидентів перенаправить запити користувачів з ділянок системи, що перестали працювати, на робочі [2].

З використанням всіх цих інструментів інфокомунікаційна система показує значно кращі результати роботи, що здебільшого покращує саме доступність сервісів для користувачів. Так, встановлення порогу в 75 % навантаження на процесор для масштабування значно стабілізувало використання ресурсів та знизило затримки при різкому зростанні кількості запитів на 32 %, що є доволі високим показником [3].

Висновок. Системи моніторингу є критичним елементом будь-якої інфокомунікаційної системи, без якого неможливо попередити виникнення інцидентів, що в свою чергу може призвести до труднощів з доступом користувачів до системи і подальшу втрату клієнтів.

Список використаних джерел:

1. Малємаєв М. В. Програмно-апаратний комплекс аналізу інтегральних показників роботи мережевого пристрою для розробки систем виявлення мережевих аномалій : магістерська робота / Одеський нац. ун-т ім. І. І. Мечникова. Одеса, 2022. URL:https://dspace.onu.edu.ua/handle/123456789/42713 (дата звернення: 07.03.2026).

2. Designing a Real-Time Monitoring System for the AWS Cloud: An Adaptive Dashboard-Based Approach with Prometheus and Grafana / A. W. Bello, A. K. Assouma, T. Djara et al. *International Journal of Advanced Computer Science and Applications*. 2024. Vol. 15, No. 5. P. 120–130.

3. Kyrychek H. H., Tseluiko R. O., Tiahunova M. Y., Zhyvohliad V. A. CLOUD SERVICES IN DISTRIBUTED NETWORK INFRASTRUCTURE. *Science and Technology (ST)*. 2025. Vol. 70, No. 2. P. 232–239.