КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (33), 2026
ISSN 2663 – 4023
DOI 10.28925/2663-4023.2026.33.1132
УДК 004.056:004.8

Онищук Оксана Олександрівна
кандидат технічних наук, доцент
місце роботи: Волинський національний університет, Луцьк, Україна
ORCID: 0000-0002-8342-3011
oksanaoo2024@gmail.com

ПОРІВНЯННЯ ІНСТРУМЕНТІВ СИСТЕМНОГО МОНІТОРИНГУ NAGIOS, ZABBIX, PROMETHEUS, MS SCOM ДЛЯ ВИЯВЛЕННЯ АНОМАЛІЙ ТА ПРОБЛЕМ В МЕРЕЖІ

Анотація. Сучасні інформаційні системи та корпоративні мережі потребують постійного і всебічного моніторингу для своєчасного виявлення аномалій, зниження продуктивності та відмов, що можуть впливати на стабільність роботи, безпеку та доступність сервісів. У статті проведено детальний порівняльний аналіз чотирьох широко використовуваних систем моніторингу: Nagios, Zabbix, Prometheus та Microsoft System Center Operations Manager (MS SCOM). Досліджено архітектурні особливості кожної платформи, механізми збору та обробки метрик, підходи до виявлення аномалій, масштабованість, ефективність використання ресурсів та можливості інтеграції з сучасними IT-рішеннями, включно з хмарними інфраструктурами, контейнеризованими середовищами та алгоритмами машинного навчання. Для оцінювання систем застосовувалася багатокритеріальна методика, що враховує час реагування, точність виявлення (Precision), повноту (Recall), споживання ресурсів та зручність адміністрування. Використовувалися нормалізовані показники та інтегральний коефіцієнт ефективності для об'єктивного порівняння платформ. Результати показали, що Prometheus забезпечує найшвидше виявлення аномалій та найвищі показники точності і повноти реагування, що робить його надзвичайно ефективним для динамічних і високонавантажених середовищ. Zabbix продемонстрував стабільну та надійну роботу з широким функціоналом, придатним для середніх і великих мереж. MS SCOM ефективний у корпоративних інфраструктурах на базі Windows, забезпечуючи широку інтеграцію та управління, проте створює більше навантаження на ресурси. Nagios відзначився надійністю та простотою, проте проявив нижчу гнучкість і масштабованість у складних та динамічних середовищах. Отримані висновки свідчать, що вибір системи моніторингу має враховувати специфіку мережевої інфраструктури, масштаби мережі, експлуатаційні вимоги та потреби організації.

Ключові слова: Nagios; Zabbix; Prometheus; MS SCOM; системний моніторинг; виявлення аномалій; мережеві інциденти; оцінка продуктивності; масштабованість; ефективність ресурсів.

ВСТУП

У сучасних умовах цифрової трансформації підприємств стабільність та безперервність роботи IT-інфраструктури є критично важливими для забезпечення бізнес-процесів. Зростання складності корпоративних мереж, поширення хмарних сервісів, віртуалізації та контейнеризації підвищують вимоги до систем моніторингу, які повинні своєчасно виявляти аномалії, збої та потенційні проблеми в роботі серверів, мережевого обладнання та прикладних сервісів.

Системи моніторингу дозволяють здійснювати постійний контроль стану IT-інфраструктури, аналізувати продуктивність, відслідковувати відхилення від нормальних показників та оперативно реагувати на інциденти. Серед найбільш поширених інструментів системного моніторингу можна виділити Nagios, Zabbix, Prometheus та Microsoft System Center Operations Manager (MS SCOM). Кожен із цих інструментів має власну архітектуру, підхід до збору метрик, механізми сповіщення та аналітики, а також різні можливості інтеграції й масштабування.

Постановка проблеми. Актуальність теми зумовлена необхідністю вибору оптимального рішення для моніторингу мережевої інфраструктури залежно від вимог організації, масштабу системи, бюджету та рівня автоматизації процесів. Порівняльний аналіз зазначених платформ дозволяє визначити їхні переваги та недоліки в контексті виявлення аномалій, раннього попередження збоїв і забезпечення високої доступності сервісів.

Аналіз останніх досліджень і публікацій. Актуальність розвитку систем моніторингу мережевої інфраструктури та засобів виявлення аномалій підтверджується активним впровадженням міжнародних стандартів управління IT-послугами та інформаційною безпекою. Зокрема, важливість безперервного контролю інфраструктури відображена у стандарті ISO/IEC 27001:2013 [1], а також у практиках управління IT-послугами відповідно до бібліотеки ITIL 4 [2].

У наукових публікаціях останніх років значна увага приділяється дослідженню класичних та сучасних систем моніторингу, зокрема Nagios, Zabbix, Prometheus та MS SCOM. Аналіз літературних джерел свідчить, що традиційні рішення, такі як Nagios, побудовані переважно на моделі періодичного опитування (polling), що може обмежувати їх ефективність у великих розподілених середовищах [3]. Водночас ці системи залишаються актуальними завдяки широким можливостям розширення та великій кількості плагінів.

У працях, присвячених системі Zabbix, підкреслюється її гнучка архітектура, підтримка агентського та безагентського моніторингу, а також розвинений механізм тригерів і шаблонів, що дозволяє ефективно масштабувати систему у корпоративних мережах [4]. Дослідники відзначають зручність централізованого адміністрування та можливості побудови складних сценаріїв сповіщення.

Окремий напрям досліджень стосується використання систем моніторингу, орієнтованих на часові ряди та мікросервісну архітектуру. У цьому контексті Prometheus розглядається як ефективний інструмент для роботи з високочастотними метриками та контейнеризованими середовищами, зокрема Kubernetes [5]. Публікації наголошують на його зручному механізмі запитів PromQL і можливості інтеграції з інструментами візуалізації та аналітики.

Щодо корпоративних рішень, у дослідженнях відзначається, що MS SCOM є ефективним у середовищах, побудованих на технологіях Microsoft, завдяки глибокій інтеграції з Active Directory та іншими компонентами екосистеми [6]. Проте в окремих роботах зазначається складність впровадження та значні вимоги до ресурсів.

Останні публікації також акцентують увагу на інтеграції систем моніторингу з алгоритмами машинного навчання для зменшення кількості хибних спрацювань та підвищення точності виявлення аномалій [7]. Використання методів прогнозування та аналізу часових рядів дозволяє переходити від реактивного до проактивного моніторингу.

Таким чином, аналіз наукових джерел свідчить про активний розвиток підходів до системного моніторингу, їх адаптацію до умов хмарних і гібридних середовищ, а також зростання ролі інтелектуальних методів обробки даних у процесах виявлення мережевих проблем.

Метою роботи є аналіз і порівняння інструментів системного моніторингу Nagios, Zabbix, Prometheus та MS SCOM з точки зору їх функціональних можливостей, архітектурних особливостей, масштабованості, гнучкості налаштування та ефективності виявлення аномалій і проблем у мережі.

Для досягнення поставленої мети передбачається виконання таких завдань:проаналізувати архітектуру та принципи роботи кожної системи; дослідити механізми збору, зберігання та обробки метрик; оцінити інструменти виявлення аномалій та систему сповіщень; порівняти вимоги до впровадження та адміністрування; визначити доцільність використання кожного рішення для різних типів організацій.

Таким чином, результати дослідження можуть бути використані для обґрунтованого вибору системи моніторингу, що забезпечує своєчасне виявлення проблем у мережі та підвищить загальний рівень надійності IT-інфраструктури підприємства.

ТЕОРЕТИЧНІ ОСНОВИ ДОСЛІДЖЕННЯ

У дослідженні систем моніторингу мережевої інфраструктури важливе значення мають теоретичні основи побудови розподілених інформаційних систем, принципи збору та аналізу телеметричних даних, а також моделі виявлення аномалій. Сучасні IT-інфраструктури характеризуються високою динамічністю, використанням віртуалізації, контейнеризації та хмарних сервісів, що вимагає застосування ефективних інструментів моніторингу [8].

Системний моніторинг базується на концепції безперервного збору метрик, журналів подій та трасування мережевого трафіку. Основними підходами є модель періодичного опитування (polling) та модель збору за принципом push. Класичні системи, такі як Nagios, реалізують переважно polling-підхід, коли сервер моніторингу регулярно опитує вузли мережі щодо їхнього стану [9-11]. Такий підхід є надійним, проте може створювати додаткове навантаження в масштабних середовищах.

Більш сучасні платформи, зокрема Zabbix, підтримують як агентський, так і безагентський моніторинг, що забезпечує гнучкість розгортання та масштабування [3]. Теоретичною основою їх

функціонування є клієнт-серверна архітектура з централізованою базою даних для зберігання історичних показників.

Окрему групу становлять системи, орієнтовані на часові ряди та мікросервісну архітектуру. Prometheus реалізує модель збору метрик із використанням pull-механізму та спеціалізованої мови запитів PromQL для аналізу часових рядів [12, 14]. Теоретично така модель дозволяє ефективно виявляти тренди, відхилення та кореляції між подіями в режимі реального часу.

У корпоративному середовищі значну роль відіграють інтегровані рішення, такі як Microsoft System Center Operations Manager, що базуються на концепції централізованого управління IT-службами та інтеграції з іншими компонентами екосистеми Microsoft [5, 15]. Теоретичною основою таких систем є модель управління інцидентами та подіями відповідно до практик ITIL.

Виявлення аномалій у мережі ґрунтується на використанні порогових значень, статистичних методів та алгоритмів машинного навчання. Класичний підхід передбачає встановлення фіксованих тригерів (threshold-based detection), однак сучасні дослідження доводять ефективність адаптивних моделей, що враховують поведінкові характеристики системи та часові залежності [6]. Використання методів кластеризації, регресійного аналізу та нейронних мереж дозволяє зменшити кількість хибних спрацювань і підвищити точність прогнозування збоїв.

Таким чином, теоретичні основи дослідження систем моніторингу включають: принципи побудови клієнт-серверних і розподілених архітектур; методи збору, зберігання та аналізу часових рядів; моделі управління інцидентами та подіями; алгоритми статистичного аналізу та машинного навчання для виявлення аномалій.

Зазначені підходи формують наукове підґрунтя для порівняльного аналізу сучасних систем моніторингу та оцінки їх ефективності у виявленні мережевих проблем.

МЕТОДИКА ДОСЛІДЖЕННЯ

Методика дослідження передбачає комплексний порівняльний аналіз систем моніторингу Nagios, Zabbix, Prometheus та Microsoft System Center Operations Manager з метою визначення їх ефективності у виявленні аномалій та мережевих збоїв. Дослідження базується на поєднанні теоретичного аналізу, експериментального моделювання та статистичної обробки отриманих результатів.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

У результаті проведеного експериментального дослідження було отримано кількісні показники ефективності систем моніторингу Nagios, Zabbix, Prometheus та Microsoft System Center Operations Manager у тестовому середовищі. Оцінювання здійснювалося відповідно до розробленої методики з використанням нормалізації показників та розрахунку інтегрального коефіцієнта ефективності.

На першому етапі формували критеріїв оцінювання та їх вагових коефіцієнтів. Для забезпечення об’єктивності порівняння використовували метод багатокритеріальної оцінки. Інтегральний показник ефективності системи визначається:

$$E = \sum_{i=1}^{n} wi \cdot si$$

де E – інтегральна оцінка ефективності системи моніторингу; wii – ваговий коефіцієнт і-го критерію; si – нормалізована оцінка за і-м критерієм; n – кількість критеріїв.

Нормалізацію. показників обчислювали за формулою:

$$si = \frac{xi - xmin}{xmax - xmin}$$

де xi – фактичне значення показника; xmin, xmax – мінімальне та максимальне значення показника серед досліджуваних систем.

Для оцінювання якості виявлення аномалій використовували метрики точності та повноти:

$$Precision = \frac{TP}{TP + FP}$$

$$Recall = \frac{TP}{TP + FN}$$

$$F1 = 2\text{X}\frac{Precision + Recall}{Precision \cdot Recall}$$

де TP – кількість правильно виявлених аномалій;
FP – кількість хибних спрацювань;
FN – кількість пропущених аномалій.

Експериментальна частина передбачала створення та моделювання тестового середовища з віртуальними серверами та мережевими сервісами, в якому моделюються типові відмови: перевищення навантаження CPU, відмова мережевого вузла, затримка відповіді сервісу, аномальний трафік. Для кожної системи фіксуються показники часу виявлення, кількості хибних спрацювань та споживання ресурсів.

Таблиця 1

Порівняльні результати експерименту

Система	Середній час виявлення, с	Precision	Recall	Навантаження CPU, %	Інтегральна оцінка EEE
Nagios	18	0,82	0,79	22	0,71
Zabbix	14	0,88	0,85	25	0,83
Prometheus	10	0,91	0,89	27	0,89
MS SCOM	16	0,86	0,83	30	0,78

За таблицею 1 результати показали, що найменший середній час виявлення інцидентів продемонструвала система Prometheus (10 с), що пояснюється ефективною роботою з часовими рядами та оптимізованим механізмом збору метрик. Найвищі значення Precision та Recall також були зафіксовані у Prometheus, що свідчить про високу точність і повноту виявлення аномалій.

Zabbix продемонстрував стабільні показники точності та помірний час реагування, що підтверджує його ефективність у середовищах середнього масштабу. MS SCOM показав достатньо високі показники точності, проте характеризувався більшим навантаженням на ресурси. Nagios продемонстрував найнижчий інтегральний коефіцієнт ефективності через більший час реагування та менші показники повноти виявлення.

Розрахунок інтегрального показника ефективності показав, що найбільш збалансованим рішенням за сукупністю критеріїв є Prometheus (E=0,89), що робить його доцільним для використання у високонавантажених та динамічних мережевих середовищах.

Таким чином, результати дослідження підтверджують, що вибір системи моніторингу повинен здійснюватися з урахуванням масштабу інфраструктури, вимог до швидкості реагування та допустимого рівня навантаження на ресурси. Найвищу ефективність у межах проведеного експерименту продемонструвала система Prometheus, тоді як інші рішення можуть бути більш доцільними у специфічних умовах експлуатації.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

У ході проведеного дослідження було здійснено комплексний порівняльний аналіз систем моніторингу Nagios, Zabbix, Prometheus та Microsoft System Center Operations Manager з метою оцінювання їх ефективності у виявленні аномалій та проблем у мережевій інфраструктурі.

У результаті теоретичного аналізу встановлено, що сучасні системи моніторингу відрізняються архітектурними підходами, механізмами збору даних та способами реалізації аналітики. Класичні рішення, орієнтовані на модель періодичного опитування, характеризуються стабільністю та простотою впровадження, проте можуть поступатися в масштабованості та швидкості реагування в умовах високонавантажених розподілених середовищ. Системи, що працюють із часовими рядами та підтримують сучасні хмарні технології, демонструють кращі показники адаптивності та продуктивності.

Експериментальна частина дослідження підтвердила, що найвищий інтегральний показник ефективності отримано для Prometheus, що обумовлено низьким середнім часом виявлення інцидентів та високими значеннями точності й повноти виявлення аномалій. Zabbix показав стабільні результати та високу універсальність у різних сценаріях експлуатації. MS SCOM виявився ефективним у корпоративних середовищах із домінуванням технологій Microsoft, проте характеризувався більшим споживанням ресурсів. Nagios продемонстрував надійність і простоту, але поступився за показниками швидкості реагування та гнучкості аналітики.

Таким чином, проведено багатокритеріальну оцінку сучасних систем моніторингу, визначено їх сильні та слабкі сторони, а також обґрунтовано доцільність використання кожного рішення залежно від умов експлуатації. Отримані результати можуть бути використані при виборі системи моніторингу для корпоративних, хмарних або гібридних мережевих середовищ.

Перспективи подальших досліджень полягають у розширенні експериментальної бази шляхом тестування систем у масштабніших інфраструктурах із використанням реального виробничого навантаження. Доцільним є також поглиблене дослідження інтеграції систем моніторингу з алгоритмами машинного навчання для побудови адаптивних моделей прогнозування збоїв. Окремим напрямом може стати аналіз кіберінцидентів та можливостей виявлення складних атак на основі поведінкових характеристик мережі. Крім того, перспективним є дослідження ефективності моніторингу в середовищах контейнеризації та оркестрації, а також оцінювання енергоефективності систем моніторингу в умовах обмежених ресурсів.

Таким чином, подальший розвиток інтелектуальних підходів до системного моніторингу сприятиме підвищенню надійності, безпеки та стабільності функціонування сучасних інформаційних мереж.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. International Organization for Standardization. (2013). *ISO/IEC 27001:2013 information technology – Security techniques – Information security management systems – Requirements*.
2. Axelos. (2019). *ITIL® foundation: ITIL 4 edition*. The Stationery Office.
3. Barth, W. (2008). *Nagios: System and network monitoring*. No Starch Press.
4. Olups, R. (2016). *Zabbix network monitoring*. Packt Publishing.
5. Brazil, B. (2018). *Prometheus: Up & running*. O'Reilly Media.
6. Microsoft. (n.d.). *System Center Operations Manager documentation*.
7. Chandola, V., Banerjee, A., & Kumar, V. (2009). Anomaly detection: A survey. *ACM Computing Surveys*, 41(3), Article 15.
8. Юрченко, О. М. (2001). *Захист інформації в комп'ютерних системах від несанкціонованого доступу: Навчальний посібник*. Видавництво Європейського університету.
9. Національний орган стандартизації України. (2015). *ДСТУ ISO/IEC 27001:2015. Методи захисту. Системи управління інформаційною безпекою. Вимоги (ISO/IEC 27001:2013, IDT)*.
10. Національний орган стандартизації України. (2015). *ДСТУ ISO/IEC 27002:2015. Інформаційні технології. Методи захисту. Кодекс практик щодо заходів інформаційної безпеки*.
11. Національний орган стандартизації України. (2019). *ДСТУ ISO/IEC 27005:2019. Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки (ISO/IEC 27005:2018, IDT)*.
12. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» № 80/94-ВР. (1994). https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80
13. Закон України «Про інформацію» № 2657-XII. (1992). https://zakon.rada.gov.ua/laws/main/2657-12
14. Закон України «Про основні засади забезпечення кібербезпеки України» № 2163-VIII. (2017). https://zakon.rada.gov.ua/laws/main/2163-19
15. Лєнков, С. В., Перегудов, Д. А., & Хорошко, В. А. (2008). *Методи та засоби захисту інформації* (у 2 т.). Арий.

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (33), 2026
ISSN 2663 – 4023

Oksana Onyshchuk
candidate of technical sciences, associate professor
Workplace: Volyn National University, Lutsk, Ukraine
ORCID: 0000-0002-8342-3011
oksanaoo2024@gmail.com

COMPARISON OF SYSTEM MONITORING TOOLS NAGIOS, ZABBIX, PROMETHEUS, MS SCOM FOR DETECTING NETWORK ANOMALIES AND ISSUES

Abstract. Modern information systems and corporate networks require continuous and comprehensive monitoring to promptly detect anomalies, performance degradations, and failures that may affect operational stability, security, and service availability. This article presents a detailed comparative analysis of four widely used monitoring systems: Nagios, Zabbix, Prometheus, and Microsoft System Center Operations Manager (MS SCOM). The architectural features of each platform, mechanisms for metric collection and processing, approaches to anomaly detection, scalability, resource efficiency, and integration capabilities with modern IT solutions, including cloud infrastructures, containerized environments, and machine learning algorithms, are examined.A multi-criteria evaluation methodology was applied, taking into account response time, detection accuracy (Precision), completeness (Recall), resource consumption, and administrative usability. Normalized metrics and an integrated performance coefficient were used for objective comparison of the platforms. The results showed that Prometheus provides the fastest anomaly detection and the highest levels of precision and recall, making it highly effective for dynamic and high-load environments. Zabbix demonstrated stable and reliable performance with broad functionality suitable for medium and large networks. MS SCOM proved effective in Windows-based corporate infrastructures, offering extensive integration and management capabilities, but with higher resource consumption. Nagios was noted for its reliability and simplicity, though it showed lower flexibility and scalability in complex and dynamic environments.The findings indicate that the choice of a monitoring system should consider the specifics of the network infrastructure, network scale, operational requirements, and organizational needs. This study provides practical recommendations for administrators and system architects to optimize monitoring tool selection, improve incident response efficiency, and ensure the reliability and security of critical network services.

Keywords: Nagios; Zabbix; Prometheus; MS SCOM; system monitoring; anomaly detection; network incidents; performance; scalability.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. International Organization for Standardization. (2013). *ISO/IEC 27001:2013 information technology – Security techniques – Information security management systems – Requirements*.
2. Axelos. (2019). *ITIL® foundation: ITIL 4 edition*. The Stationery Office.
3. Barth, W. (2008). *Nagios: System and network monitoring*. No Starch Press.
4. Olups, R. (2016). *Zabbix network monitoring*. Packt Publishing.
5. Brazil, B. (2018). *Prometheus: Up & running*. O'Reilly Media.
6. Microsoft. (n.d.). *System Center Operations Manager documentation*.
7. Chandola, V., Banerjee, A., & Kumar, V. (2009). Anomaly detection: A survey. *ACM Computing Surveys, 41*(3), Article 15. https://doi.org/10.1145/1541880.1541882
8. Yurchenko, O. M. (2001). *Zakhyst informatsii v kompiuternykh systemakh vid nesanktsionovanoho dostupu* [Protection of information in computer systems from unauthorized access]. Vydavnytstvo Yevropeiskoho universytetu. (in Ukrainian)
9. Natsionalnyi orhan standartyzatsii Ukrainy. (2015). *DSTU ISO/IEC 27001:2015. Metody zakhystu. Systemy upravlinnia informatsiinoiu bezpekoiu. Vymohy (ISO/IEC 27001:2013, IDT)*. (in Ukrainian)
10. Natsionalnyi orhan standartyzatsii Ukrainy. (2015). *DSTU ISO/IEC 27002:2015. Informatsiini tekhnolohii. Metody zakhystu. Kodeks praktyk shchodo zakhodiv informatsiinoi bezpeky*. (in Ukrainian)
11. Natsionalnyi orhan standartyzatsii Ukrainy. (2019). *DSTU ISO/IEC 27005:2019. Informatsiini tekhnolohii. Metody zakhystu. Upravlinnia ryzykamy informatsiinoi bezpeky (ISO/IEC 27005:2018, IDT)*. (in Ukrainian)

12. Zakon Ukrainy “Pro zakhyst informatsii v informatsiino-telekomunikatsiinykh systemakh” No. 80/94-VR. (1994). https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80
13. Zakon Ukrainy “Pro informatsiiu” No. 2657-XII. (1992). https://zakon.rada.gov.ua/laws/main/2657-12
14. Zakon Ukrainy “Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy” No. 2163-VIII. (2017). https://zakon.rada.gov.ua/laws/main/2163-19
15. Lienkov, S. V., Perehudov, D. A., & Khoroshko, V. A. (2008). *Metody ta zasoby zakhystu informatsii* (Vols. 1–2). Arii. (in Ukrainian)

Отримано редакцією журналу / Received: 10.02.26
Прорецензовано / Revised: 25.02.26
Схвалено до друку / Accepted: 25.06.26