УДК 004.7 DOI: 10.31673/2412-4338.2025.048910

Дідовець Владислав Максимович
Державний університет інформаційно-комунікаційних технологій, Київ
ORCID 0009-0008-2713-3416

Адаменко Володимир Олексійович
Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського» ,Київ
ORCID 0000-0003-0601-8394

ТЕНДЕНЦІЇ РОЗВИТКУ СИСТЕМ МОНІТОРИНГУ КОМП'ЮТЕРНИХ МЕРЕЖ В СУЧАСНОМУ СВІТІ

Анотація *Сучасні інформаційно-комунікаційні системи функціонують у середовищі швидкої цифрової трансформації, що супроводжується зростанням обсягів трафіку, ускладненням мережевих топологій і переходом до хмарних та мікросервісних архітектур. Це формує підвищений попит на високоточні та масштабовані системи моніторингу, здатні в режимі реального часу забезпечувати спостереження за станом інфраструктури, раннє виявлення інцидентів і підтримку стабільності сервісів. У статті представлено огляд найпоширеніших платформ моніторингу комп'ютерних мереж — Zabbix, Prometheus у зв'язці з Grafana, SolarWinds Network Performance Monitor та Datadog. Визначено їхні ключові функції, архітектурні підходи, моделі збору та агрегування телеметрії, механізми оповіщення та сфери застосування в корпоративних, DevOps і хмарних середовищах.*

Особливу увагу приділено сучасним інтелектуальним підходам, що базуються на машинному навчанні та нейронних мережах. Показано, що алгоритми прогнозування навантаження, виявлення аномалій і кореляції подій дозволяють суттєво скоротити середній час виявлення та локалізації інцидентів, зменшити кількість хибнопозитивних сповіщень і забезпечити проактивне управління інфраструктурою. Наведено результати прикладних досліджень 2024 року, що демонструють зниження простоїв, прискорення реагування на інциденти та підвищення ефективності підтримки SLA при інтеграції AI-модулів у моніторингові системи.

Окреслено виклики впровадження інтелектуальних систем моніторингу — від потреби у високоякісних даних та проблем конфіденційності до складності масштабування моделей. У підсумку стаття формує уявлення про сучасний стан ринку моніторингу, тенденції переходу від статичних правил до адаптивної аналітики та перспективи розвитку мережевої спостережуваності в умовах зростаючої складності цифрової інфраструктури.

Ключові слова*: системи моніторингу мереж, мережеве адміністрування, штучний інтелект, нейронні мережі, Zabbix, Prometheus, SolarWinds, Datadog.*

Didovets Vladyslav
State University of Information and Communication Technologies, Kyiv
ORCID: 0009-0008-2713-3416

Adamenko Volodymyr
National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Kyiv
ORCID 0000-0003-0601-8394

Trends in the Development of Computer Network Monitoring Systems in the Modern World

Abstract*. Modern information and communication systems operate in the context of rapid digital transformation, driven by increasing traffic volumes, more complex network topologies, and the widespread adoption of cloud and microservice architectures. These trends generate a strong demand for high-precision and scalable monitoring platforms capable of ensuring real-time visibility, early incident detection, and reliable service continuity. This article provides an analytical overview of the most widely used monitoring platforms — Zabbix, Prometheus combined with Grafana, SolarWinds Network Performance Monitor, and Datadog. Their major features, architectural principles, data collection and aggregation models, alerting mechanisms, and practical use cases across corporate, DevOps, and cloud environments are examined.*

Special attention is given to modern AI-driven approaches, including machine learning and neural network-based anomaly detection, load forecasting, and event correlation. The presented findings demonstrate that such techniques significantly reduce mean time to detect and localize incidents, lower false-positive alert rates, and support proactive infrastructure management. The article summarizes applied research results from 2024, which confirm reduced

downtime, faster operational response, and improved SLA metrics once AI modules are integrated into monitoring workflows.

Key challenges of intelligent monitoring are highlighted, including the need for high-quality datasets, privacy and data governance issues, and the complexity of scaling analytical models. Overall, the article outlines current trends in network monitoring evolution, emphasizing the shift from static rule-based mechanisms to adaptive analytics and intelligent observability capable of supporting resilient digital infrastructures.

Keywords*: network monitoring systems, network administration, artificial intelligence, neural networks, Zabbix, Prometheus, SolarWinds, Datadog.*

1. Вступ

В сучасному світі кожна компанія використовує у своїй діяльності комп'ютерні мережі. Залежно від того чи це невелика компанія, кав'ярня, мережа коворкінгів, державна установа, промислове підприємство або велика компанія вони мають свою архітектуру, складність та вимоги. Їх призначення в цьому випадку не змінюється і їх головне завдання забезпечувати нормальну роботу компанії та людей, що працюють або користуються сервісами. Проте кожна мережа потребує догляду та контролю й ця задача покладається на IT-відділи компанії, що використовують для цього різне програмне забезпечення. Один з прикладів такого програмного забезпечення є система моніторингу комп'ютерних мереж.

Система моніторингу комп'ютерних мереж (Network Monitoring System, NMS) – це програмно-апаратне рішення, яке призначене для відстеження працездатності та продуктивності мережевих пристроїв і сервісів. Основними завданнями систем моніторингу комп'ютерних мереж є: вимірювання встановлених метрик (затримки, пропускна здатність, втрати пакетів, навантаження на сервіс тощо), які налаштовуються фахівцями, контроль за дотриманням політик встановлених в мережі, виявлення збоїв, перевантажень та контроль за станом обладнання (завантаженість дисків, пам'яті, процесора та відеокарти). Це надає змогу IT-відділу вчасно реагувати на проблеми, передбачати їх появу та обслуговувати й проводити оновлення мережі.

Зростання обсягів даних зумовлених більшим попитом на сервіси й збільшенням кількості пристроїв, як у власності простих користувачів, так і у власності компанії зумовило необхідність розосереджувати сервіси, використовувати хмарні технології та контейнеризацію. Це ускладнює адміністрування та підтримку комп'ютерних мереж та систем оскільки зростає навантаження та обсяг інформації, яку необхідно обробити. Традиційні інструменти моніторингу можуть не бути не в змозі забезпечити широкий набір інструментів та можливостей аналізувати постійно великі обсяги даних при зростаючих потребах компанії. Це створює потребу у нових системах, які вміють передбачати інциденти або проблеми, аналізувати поточні події, надавати звітність вказуючи можливі причини та рішення, аналізувати в режимі 24/7 й найголовніше навчатися на реальній системі в режимі реального часу. Така система дозволила б краще адмініструвати мережу та допомогла зробити її максимально ефективною. Для початку оглянемо як працюють сучасні системи моніторингу та які можливості вони надають.

2. Аналіз останніх досліджень і публікацій.

Останні роки спостерігається активний розвиток систем моніторингу комп'ютерних мереж, спричинений зростанням обсягів даних, збільшеним використанням хмарних сервісів та мікросервісної архітектури. У роботі [1] зазначається, що класичні системи моніторингу (Zabbix, Nagios, PRTG) не завжди здатні забезпечити належний рівень масштабованості та швидкодії при обробці великих обсягів даних. Згідно з дослідженням [2], однією з головних проблем сучасних платформ моніторингу є обмежена спостережуваність (observability). Вони зосереджені переважно на зборі метрик, але не надають глибокого контекстного аналізу подій.

Також відзначається [3], що традиційні інструменти моніторингу часто не здатні виявляти складні аномалії або прогнозувати збої, оскільки ґрунтуються переважно на статичних правилах. Водночас нові тенденції у сфері моніторингу спрямовані на інтеграцію методів машинного навчання та штучного інтелекту, які дозволяють системам самостійно виявляти відхилення, адаптуватися до змін середовища та автоматизувати прийняття рішень.

Таким чином, наявні дослідження підтверджують необхідність розробки інтелектуальних систем моніторингу, здатних забезпечити комплексну аналітику стану мереж та своєчасне попередження про потенційні проблеми.

3. Мета і задачі дослідження.

Метою дослідження є аналіз сучасних систем моніторингу комп'ютерних мереж та тенденцій їх розвитку. Виявлення їх принципу роботи й з'ясування переваг та недоліків.

Для досягнення цієї мети поставлено такі задачі:

1. Провести огляд популярних систем моніторингу різних архітектур (Open-Source, DevOps, Enterprise, SaaS) та визначити їхні функціональні переваги й недоліки.
2. Проаналізувати технічні принципи роботи систем моніторингу, включаючи механізми збору, агрегації та зберігання даних (SNMP, NetFlow, агентний та pull-підходи).
3. Розглянути перспективу використання нейронних мереж в системах моніторингу та описати задачі, які здатні виконати нейронні мережі.
4. Сформувати висновки щодо перспектив розвитку інтелектуальних систем моніторингу та окреслити ключові виклики впровадження (зокрема, питання конфіденційності та перенесення знань).

4. Огляд сучасних систем моніторингу.

Zabbix – це відкрита система для моніторингу служб і стану комп'ютерної мережі. Ця система дозволяє вимірювати трафік, пропускну здатність, втрату пакетів, стан обладнання, працездатність сервісів та налаштувати власні специфічні шаблони для конкретних сценаріїв[7; 10]. Приклади моніторингу продемонстровано на рис. 1-2. Також Zabbix пропонує понад 300 шаблонів для швидкого старту, які створені під популярних постачальників мережевого обладнання. Процедура моніторингу Zabbix базується на отриманні метрик, які надходять різними способами:

1. Активний та пасивний збір – агент самостійно надсилає дані або запити до сервера та чекає на відповідь.
2. SNMP (Simple Network Management Protocol) — використовується для відстеження роботи мережевих пристроїв.
3. IPMI(Intelligent Platform Management Interface) — використовується для моніторингу апаратної частини серверів або комп'ютерів.
4. HTTP/HTTPS чекери — для перевірки роботи вебсайту та API.
5. UserParameters та External Checks — можливість додавати власні скрипти, які збирають необхідну інформацію.
6. Збір логів — читання та аналіз подій з файлів журналів.
7. Веб сценарії — перевірка працездатності вебзастосунків використовуючи налаштовані сценарії.

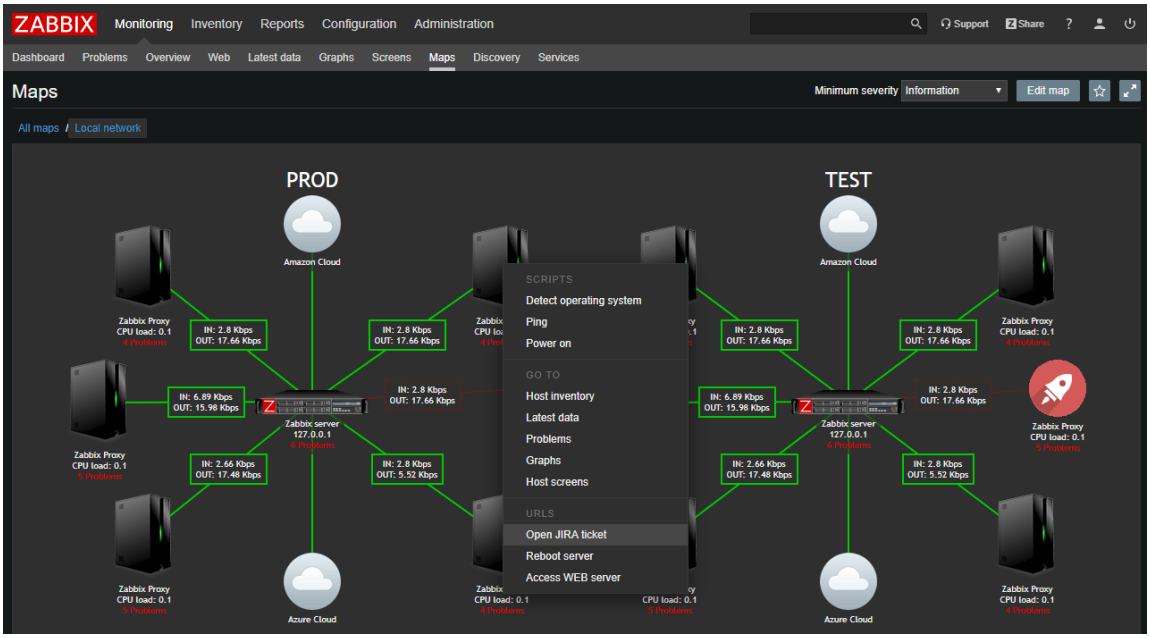

Рис. 1. Приклад карти мережі в Zabbix

Переваги:

1. Масштабованість: Zabbix розроблений для роботи у великих середовищах й здатен працювати з тисячами пристроїв.

2. Економічна вигода: Zabbix є безкоштовним програмним забезпеченням, що вигідно для невеликого бізнесу на початкових етапах. Хоча за подальшу підтримку та налаштування потрібно буде платити.

3. Широкий спектр охоплення: Дозволяє охопити всю IT-інфраструктуру, додатки, сайти або хмарні сервіси.

Недоліки:

1. Налаштування з нуля вимагає достатнього рівня знань.
2. При помилці в налаштуванні здатен заспамити повідомленнями.
3. Є обмеження по інтеграції зі сторонніми розробниками.

Сфера застосування: Застосовується Zabbix в корпоративних середовищах, дата-центрах та хмарних середовищах, які вимагають ретельного контролю великої кількості об'єктів.

Рис. 2. Приклад моніторингу серверу в Zabbix

Prometheus + Grafana – це поєднання open source системи моніторингу Prometheus та графічної оболонки Grafana для візуалізації. В цьому випадку Grafana лише забезпечує вивід даних у зручному для людини вигляді. Продемонстровано на рис. 3. Prometheus – це open source система моніторингу призначена для збору, зберігання та запиту даних, що являють собою тимчасові події або виміри[4; 5]. Методи збору даних Prometheus + Grafana:

1. Pull-модель. Сервер Prometheus періодично опитує звертається до експортерів (невеликі програми-агенти, які збирають метрики), або інструментованих застосунків через HTTP-запити та отримує від них дані метрик.

2. Push gateway. У випадку коли пряме опитування неможливе використовується метод push gateway(проміжний шлюз), який приймає метрики від короткочасних асинхронних процесів і передає їх у Prometheus.

3. Service discovery. Для забезпечення гнучкого підключення нових вузлів, система застосовує Service discovery – механізм автоматичного виявлення сервісів, який дозволяє Prometheus інтегруватися Kubernetes, Consul та іншими джерелами даних.

4. Експортери. Для збору інформації зі сторонніх сервісів використовуються експортери. Вони збирають та перетворюють метрики у зрозумілий формат для Prometheus.

Переваги:

1. Гнучкість та потужність. Використання мови запитів PromQL дозволяє створювати складні аналітичні запити та власні метрики.

2. Ефективний збір даних. Завдяки моделі "pull" спрощується інтеграція з багатьма сервісами через експортери, що дозволяє ефективно збирати метрики з різних джерел.

3. Масштабованість. Prometheus розроблений для моніторингу великих динамічних систем, забезпечуючи високий рівень продуктивності.

4. Інтеграція зі сторонніми інструментами. Prometheus здатен легко інтегруватися з іншими інструментами, такими як Grafana, для візуалізації даних.

5. Автоматичні сповіщення. Дозволяє налаштувати сповіщення про критичні події в мережі для своєчасного реагування.

Недоліки:

1. Обмеженість зберігання. Prometheus не призначений для швидкого зберігання великих обсягів даних. Тож для зберігання цих даних необхідне інше програмне забезпечення.

2. Складність збереження запитів. Збереження сформованих запитів використовуючи вебінтерфейс може бути складним та вимагати створення окремих консолей.

3. Недостатня підтримка спостережуваності. Prometheus більше орієнтований на моніторинг, але не на спостереження. Тобто він не може надати повну картину поведінки мережі чи системи. Й для цих цілей потрібні додаткові інструменти.

Застосовується Prometheus у DevOps командах для моніторингу мікросервісної архітектури й контейнерних кластерів (Kubernetes, Docker Swarm). Також він використовується стартапами та провайдерами Saas-моделей для збору телеметрії з хмарних сховищ.

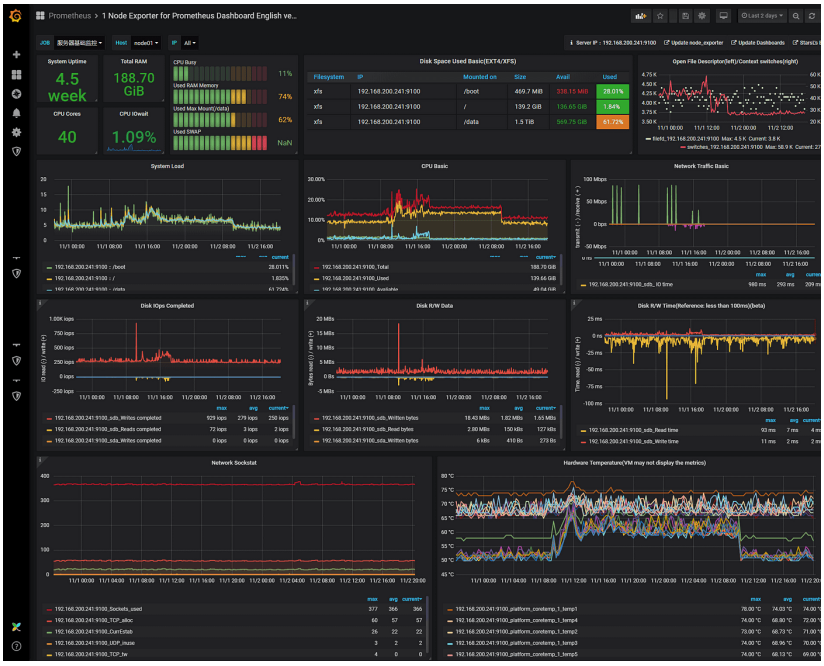

Рис. 3. Моніторинг стану обладнання в Prometheus + Grafana

SolarWinds Network Performance Monitor – це комерційна система моніторингу мережевої інфраструктури. Система SolarWinds використовує протокол SNMP для підтримки широкого спектра мережевого обладнання та має функцію автоматичного виявлення пристроїв[11]. Модуль NetPath використовується для аналізу шляху між джерелом та призначенням, а інструмент PerfStack використовується для кореляції різних метрик на одній панелі[11]. Продемонстровано на рис. 4-6. Методи збору даних SolarWinds Network Performance Monitor:

1. SNMP опитування. NPM опитує агентів використовуючи протокол SNMP на маршрутизаторах, комутаторах та серверах, збираючи метрики пропускної здатності, затримки, втрати пакетів та доступності пристроїв.

2. Аналіз потоків (NetFlow/sFlow тощо). Система збирає дані про використання пропускної здатності. Що дозволяє розуміти коли та ким використовуються мережеві ресурси.

3. Автовиявлення. NPM надсилає SNMP повідомлення для пошуку й автоматичного оновлення актуального списку мережевих пристроїв і їхніх інтерфейсів.

4. Контроль доступності (ICMP). За допомогою протоколу ICMP система перевіряє наявність та доступність пристрою для швидкого виявлення відмов.

5. Агенти SolarWinds. За допомогою програмного забезпечення встановленого для забезпечення зв’язку між серверами та сервером SolarWinds агенти збирають докладну інформацію про продуктивність хостів, програми, бази даних тощо.

Переваги:

1. Комплексний моніторинг мережі. SolarWinds Network Performance Monitor (NPM) здатен контролювати широкий спектр пристроїв від різних виробників, включаючи маршрутизатори, комутатори, сервери та брандмауери. Це дозволяє IT-відділу контролювати весь перелік обладнання.

2. Швидке виявлення та усунення несправностей. Завдяки інструментам NetPath та PerfStack можна швидко виявляти та діагностувати проблеми з продуктивністю, що значно скорочує час простою мережі[6].

3. Інтелектуальна система оповіщень. SolarWinds можна налаштувати свою систему оповіщень для своєчасних повідомлень про проблеми.

4. Настроювана інформаційна панель. Користувачі SolarWinds можуть налаштувати панелі моніторингу для візуалізації даних, що дозволяє легко відстежувати ключові показники.

5. Масштабованість. SolarWinds Підходить для організацій різного розміру, від малих, середніх або великих компаній. Це програмне забезпечення здатне масштабуватися відповідно до зростаючих потреб мережі.

Недоліки:

1. Складність налаштування та використання. Початкове налаштування SolarWinds може викликати труднощі й вимагати достатніх технічних знань.

2. Високі системні вимоги. SolarWinds може впливати на продуктивність інших додатків чи сервісів, якщо спільно використовує апаратне забезпечення з іншими.

3. Обмежена інтеграція з хмарними сервісами. SolarWinds краще підходить для звичайних локальних мереж компанії й може мати обмеження та труднощі в роботі з різними хмарними сервісами.

4. Модульна структура та висока вартість. З розростанням інфраструктури зростатиме й вартість користування, оскільки буде використовуватися більше функцій та сенсорів.

SolarWinds орієнтований на середні та великі підприємства, провайдерів зв'язку, й організації, що потребують моніторингу багатовендерної мережевої інфраструктури.

Рис. 4.Моніторинг мережі в SolarWinds Network Performance Monitor

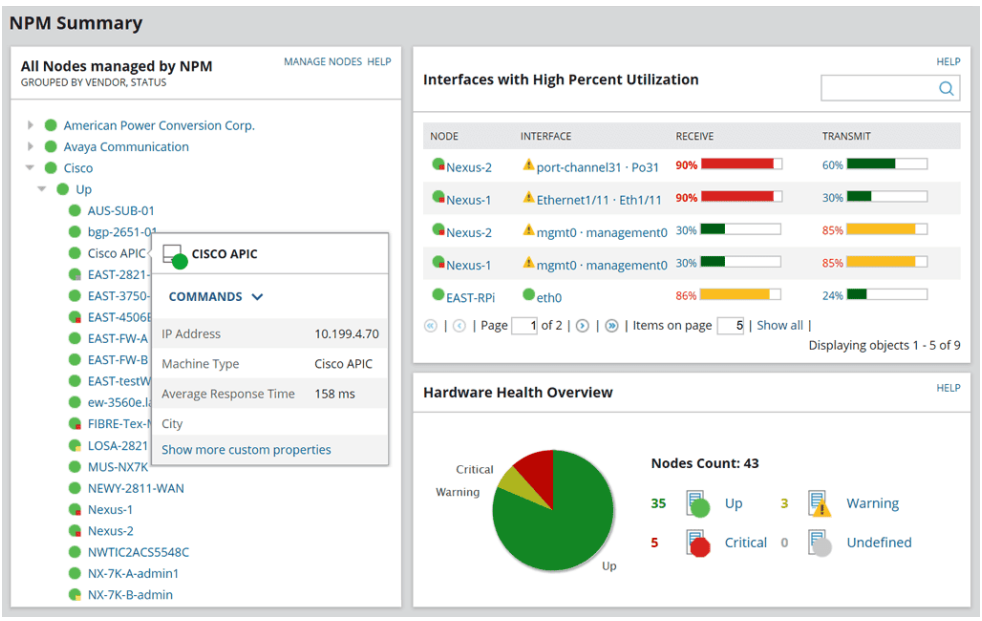

Рис. 5. Моніторинг стану програмного забезпечення та інтерфейсів в SolarWinds Network Performance Monitor

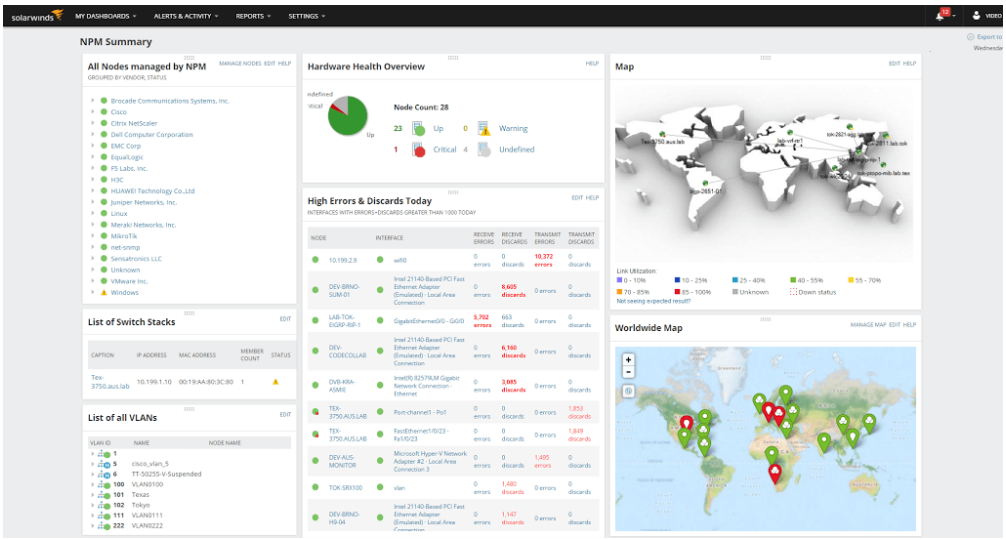

Рис. 6. Загальний монітор мережі в SolarWinds Network Performance Monitor

Datadog – це хмарна платформа(Saas) для моніторингу та забезпечення безпеки хмарних застосунків та інфраструктури. Вона надає систему для спостереження за інфраструктурою, що допомагає отримувати дані в режимі реального часу[6; 8; 9]. Datadog збирає інформацію з серверів, баз даних, контейнерів, сервісів, додатків тощо. Продемонстровано на рис. 7-9. Ця платформа намагається забезпечити для користувача повну видимість його сервісів чи інфраструктури пропонуючи широкий спектр продуктів та інтегруючись з понад 1000 різноманітних технологій. Особливістю Datadog є вбудовані функції машинного навчання: модуль Watchdog автоматично виявляє аномалії, прогнозує навантаження і виконує кореляцію подій для пошуку першопричин[7]. Модуль Watchdog — це вбудований в Datadog рушій на основі штучного інтелекту (ШІ), який автоматично аналізує терабайти даних, зібраних з усієї інфраструктури та застосунків. Його основна мета — виявляти та допомагати розв'язувати проблеми якомога швидше, до того, як вони вплинуть на кінцевих користувачів. Це робить Datadog одним із небагатьох великих рішень, які вже почали інтегрувати штучний інтелект у моніторинг.

Основні функції Datadog:

1. Моніторинг продуктивності застосунків (APM): Datadog забезпечує відстеження розподілених транзакцій на рівні коду за допомогою штучного інтелекту, щоб допомогти діагностувати та усувати проблеми з продуктивністю. Також корелює дані відстеження з метриками,

логами та даними користувачів для складання повної картини стану застосунку й розуміння, що відбувається.

2. Моніторинг інфраструктури: Datadog збирає метрики, візуалізує дані та надсилає сповіщення про проблеми в режимі реального часу, щоб контролювати стан і продуктивність хмарних або гібридних середовищ. Це також стосується серверів, контейнерів та хмарних сервісів.

3. Управління логами: Datadog пропонує агрегацію, пошук та аналіз різних логів для швидкого усунення проблем і отримання глибшого розуміння поведінки застосунків та причин можливих проблем.

4. Моніторинг безпеки: Виявляє потенційні загрози безпеці в режимі реального часу, скануючи вразливості, неправильні конфігурації та інші ризики. Що допомагає аналізувати та розуміти потенційні проблеми безпеки.

5. Моніторинг цифрового досвіду (DEM): Datadog включає моніторинг реальних користувачів (RUM) та синтетичний моніторинг, щоб допомогти командам відстежувати користувацький досвід та проактивно тестувати важливі функції застосунків. Це допомагає зрозуміти продуктивність інтерфейсу та підвищити ефективність роботи команд розробників.

6. Моніторинг продуктивності мережі (NPM): Datadog дозволяє аналізувати моделі мережевого трафіку в хмарних середовищах.

7. Настроювані панелі та сповіщення: Дозволяє створити персоналізовані панелі для візуалізації ключових показників продуктивності та налаштовувати окремі сповіщення про системні аномалії або критичні проблеми.

Переваги:

1. Комплексність та уніфікована платформа: Datadog дозволяє об’єднати в одному місці моніторинг інфраструктури, продуктивність застосунків (APM), управління логами, безпеку та моніторинг користувацького досвіду. Цей підхід значно спрощує роботу для DevOps та IT-команд, оскільки не потрібно шукати по декількох вкладкам необхідні дані.

2. Велика кількість інтеграцій: Платформа підтримує інтеграцію з понад 1000 технологій і сервісів, включаючи великих хмарних провайдерів (AWS, Azure, GCP), а також бази даних, контейнери, сервери та інші інструменти. Це дозволяє легко підключати всі необхідні компоненти вашого стека.

3. Простота використання та візуалізація: Datadog має інтуїтивно зрозумілий інтерфейс та гнучкі dashboard(інтерактивна панель моніторингу). Це дозволяє командам швидко реагувати, моніторити та відстежувати ключові показники.

4. Висока швидкість і аналітика в реальному часі: Платформа здатна надавати дані в режимі реального часу, що є критично важливим для швидкої діагностики та усунення несправностей. Це дозволяє оперативно реагувати на інциденти й вирішувати їх.

5. Інтеграція з машинним навчанням (Watchdog): Watchdog автоматично виявляє аномалії та допомагає з аналізом першопричин, що значно прискорює пошук і усунення проблем.

Недоліки:

1. Висока вартість: Цінова модель може бути складною і стає дорожчою в міру масштабування, особливо з активацією додаткових функцій, як-от APM або моніторинг логів. Занадто високі рахунки можуть змусити компанії шукати дешевші альтернативи.

2. Складність при масштабуванні: Хоча початкове налаштування може бути простим, з розширенням інфраструктури використання Datadog стає все більш складним і дорогим, що вимагає більших зусиль.

3. Обмеження на зберігання даних: За замовчуванням Datadog може мати обмежені терміни зберігання логів. Щоб збільшити цей термін, потрібно додатково купувати місце для зберігання.

4. Залежність від вендора (Vendor Lock-in): Висока інтеграція з Datadog може ускладнити перехід на інше рішення в майбутньому, оскільки вивчення нової системи займе час, а міграція може бути складною.

Сфера застосування: Datadog орієнтований на організації, що використовують хмарні платформи та мікросервісні архітектури. Його широко використовують DevOps та SRE команди для агрегованого моніторингу та аналізу логів, метрик і трасувань, а також для забезпечення безпеки застосунків і інфраструктури.

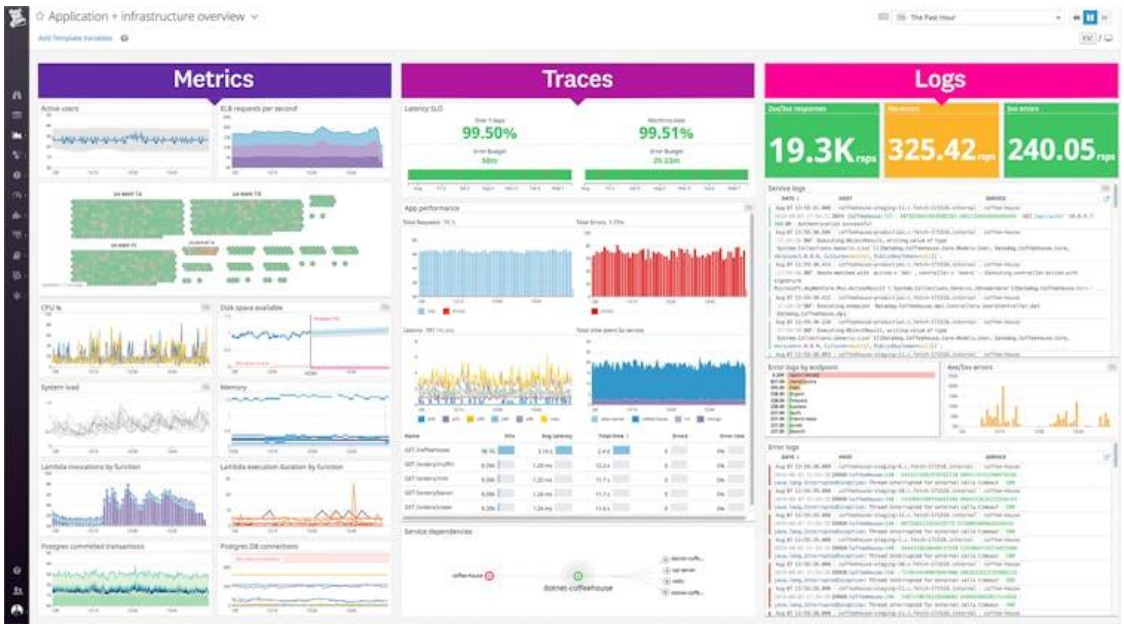

Рис. 7. Вивід метрик, трейсів та логів в Datadog

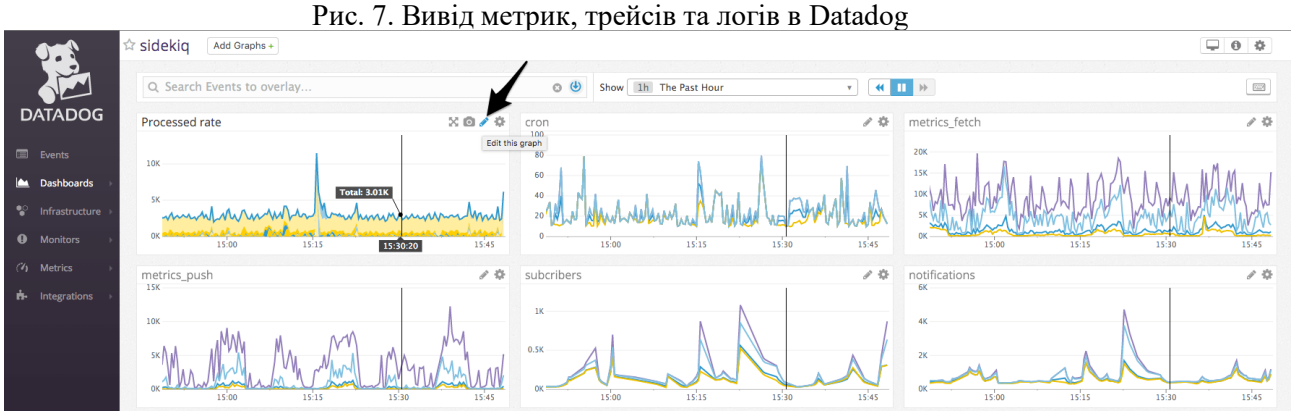

Рис. 8. Вивід метрик в Datadog

Рис. 9. Панель моніторингу інфраструктури в Datadog

Підсумувавши аналіз популярних систем моніторингу можна зазначити, що жодна з них не є універсальним рішенням і вибір такої системи має базуватися на конкретно визначених потребах. Zabbix забезпечує гнучкість, безкоштовну ліцензію та готові шаблони, але потребує достатньої кваліфікації та може бути складним у налаштуванні. Prometheus+Grafana підходить для

DevOps-середовищ та мікросервісів завдяки потужній pull-архітектурі й гнучким запитам, але не пристосований до довгострокового зберігання даних і забезпечення повної спостережуваності. SolarWinds NPM пропонує комплексний моніторинг SNMP і NetFlow та інструменти для кореляції трас, що прискорюють діагностику, однак висока вартість і складність розгортання обмежують його вибір. Datadog забезпечує інтегрований підхід до метрик, логів та безпеки з підтримкою AI-аналізу, але SaaS-модель може бути дорогою та вимагає врахування vendor lock-in. Таким чином, оптимальна система має відповідати масштабу інфраструктури, бюджету та готовності впроваджувати інтелектуальні засоби аналізу.

5. Принципи роботи систем моніторингу

Попри різноманіття програм для моніторингу комп'ютерних мереж та систем, більшість таких систем базується на схожих принципах роботи. Розглянемо основні складові їх роботи:

1. Архітектура (Менеджер – агенти/експортери). Ця архітектура передбачає використання централізованого сервера (менеджера) та керованих пристроїв, що опитуються (агенти) в мережі. Для цього використовується протокол SNMP (Simple Network Management Protocol), який є стандартним способом обміну інформацією між пристроями. Централізована система NMS (Network Management System) опитує пристрої та отримує від них метрики(дані про стан, пропускну здатність, затримку, температуру тощо) й аналізує, після чого формується звіт та повідомлення для системного адміністратора.
2. Періодичне опитування та аналіз. Циклічне опитування усіх хостів та агентів з метою актуалізації показників та перевірки працездатності. Раз на заданий проміжок часу відбувається опитування й відображення результатів через консоль або графічне зображення. У разі виявлення відхилень чи аномалій відбувається ескалація повідомлення, щоб виконати перезапуск служб чи перевірку. У випадку якщо метрика стає недоступна відбувається сповіщення критичну ситуацію.
3. Методики збору даних. Системи моніторингу використовують різноманітні протоколи(SNMP, WMI (для серверів Windows), NetFlow/sFlow/IPFIX для аналізу мережевого трафіку), syslog сервери та агентів для отримання інформації.
4. Система оповіщень. Зібрані метрики зберігаються у базах даних та відображаються на панелях аналізу чи показників. Системи моніторингу можуть надавати інструменти та механізми для створення власних тригерів та логіки оповіщень.
5. Агентський або без агентський підхід. Системи моніторингу відрізняються за способом збору даних. Одні використовують агентів або експортерів для збору інформації та опитування інші використовують для опитування протокол SNMP.

Концепція застосування штучного інтелекту та нейронних мереж у системах моніторингу

Оскільки сучасні комп'ютерні мережі генерують великі обсяги даних й в майбутньому цей обсяг даних буде збільшуватися виникає потреба у вдосконаленні та оптимізації систем моніторингу[10]. Після проведеного аналізу сучасних систем моніторингу було з'ясовано, що не всі вони здатні задовольнити повністю потреби в аналізі та моніторингу мережі й частина процесів потребує постійного та ретельного контролю за налаштуваннями для правильності отриманих даних використання нейронних мереж здатне покращити та зробити системи моніторингу ефективнішими.

6. Результати прикладних досліджень ефективності систем моніторингу

У 2024 році LiveAction опублікувала звіт "Network Performance Monitoring Trends Report", у якому зазначено, що 63% компаній після впровадження рішень з підтримкою AI значно зменшили середній час виявлення інцидентів (MTTD) — у середньому на 25–35%. Компанії, які використовували AI-аналіз у моніторингу, змогли зменшити кількість простоїв на 40% у порівнянні з традиційними методами.

Згідно з даними Statsig (2024), інтеграція модуля Watchdog у Datadog дозволила зменшити кількість хибнопозитивних тривог на 41%, а також скоротити час реагування на інциденти до 12 хвилин у середньому. Це забезпечило покращення SLA для компаній на понад 18%.

SolarWinds у внутрішньому аналізі 2024 року виявила, що використання PerfStack та NetPath дозволило скоротити час на локалізацію причин інцидентів до 8 хвилин (порівняно з 23 хвилинами при використанні лише SNMP-метрик). Це на 34% покращило час вирішення (MTTR).

Zabbix у дослідженні спільноти DevOpsSchool показав, що налаштування кастомізованих шаблонів знижує час на інтеграцію нових хостів на 45%, а обсяг помилкових налаштувань зменшується на 29% при використанні шаблонів із валідацією.

Prometheus у середовищах Kubernetes показав найкращі результати у DevOps-командах з автоматичним масштабуванням: середній час адаптації до змін середовища — 6 хвилин. Компанії, що використовували Prometheus разом із Grafana Alerting, відзначили зниження обсягу повторних інцидентів на 21%.

7.Висновки та перспективи подальших досліджень.

Проведений аналіз сучасних систем моніторингу комп'ютерних мереж свідчить про високий рівень розвитку цього напрямку. Результати досліджень підтверджують ефективність використання штучного інтелекту в таких системах — як у прогнозуванні збоїв, так і в оптимізації реагування на інциденти. Зокрема, AI-модулі типу Watchdog демонструють скорочення часу реагування до 30%, а нейронні мережі — значне зменшення кількості хибнопозитивних сигналів.

Подальші дослідження мають бути зосереджені на побудові відкритих AI-платформ для моніторингу, підвищенні прозорості алгоритмів та покращенні адаптації таких рішень до індивідуальних інфраструктур користувача. Також актуальними залишаються питання конфіденційності, навчання моделей на реальних даних та уніфікації форматів обміну телеметрією.

Список використаної літератури

1. Network Observability Platform | Network Observability by Broadcom. URL: https://networkobservability.broadcom.com/hubfs/Network%20Observability%20FY25/2024%20HBR%20Paper%20-%20Network%20Observability.pdf (дата звернення: 10.10.2025).

2. Network Performance Monitoring Trends Report 2024. LiveAction. URL: https://www.liveaction.com/resources/analyst-report/network-performance-monitoring-trend-report-2024/ (дата звернення: 10.10.2025).

3. Network observability tools promise benefits, but obstacles hinder results. Network World. URL: https://www.networkworld.com/article/957284/network-observability-tools-promise-benefits-but-obstacles-hinder-results.html (дата звернення: 12.10.2025).

4. Overview | Prometheus. Prometheus - Monitoring system & time series database. URL: https://prometheus.io/docs/introduction/overview/ (дата звернення: 12.10.2025).

5. What is Prometheus? | Grafana Cloud documentation. Grafana Labs. URL: https://grafana.com/docs/grafana-cloud/introduction/what-is-observability/prometheus/ (дата звернення: 14.10.2025).

6. Datadog Docs. Datadog Infrastructure and Application Monitoring. URL: https://docs.datadoghq.com/ (date of access: 12.10.2025).

7. What is Zabbix and How it works? An Overview and Its Use Cases - DevOpsSchool.com. DevOpsSchool.com. URL: https://www.devopsschool.com/blog/what-is-zabbix-and-how-it-works-an-overview-and-its-use-cases/ (дата звернення: 14.10.2025).

8. Team T. S. What is Datadog?. Statsig | The modern product development platform. URL: https://www.statsig.com/perspectives/what-is-datadog (дата звернення: 14.10.2025).

9. Agent. Datadog Infrastructure and Application Monitoring. URL: https://docs.datadoghq.com/agent/?tab=Host-based (дата звернення: 14.10.2025).

10. Importance of Network Monitoring: Top 8 Benefits for Businesses. Motadata. URL: https://www.motadata.com/blog/importance-of-network-monitoring/ (дата звернення: 14.10.2025).

11. Network Performance Monitor - Observability Self-Hosted. Observability, Database, and IT Service Management | SolarWinds. URL: https://www.solarwinds.com/network-performance-monitor (дата звернення: 14.10.2025).