КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 3 (27), 2025
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2025.27.787
УДК 004.9

Жебка Вікторія Вікторівна
доктор технічних наук, професор
завідувач кафедри Технологій цифрового розвитку
Державний університет інформаційно-комунікаційних технологій, Київ, Україна
ORCID ID: 0000-0003-4051-1190
v.zhebka@duikt.edu.ua

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ МОНІТОРИНГУ ГЕТЕРОГЕННИХ МЕРЕЖ В РЕЖИМІ РЕАЛЬНОГО ЧАСУ

Анотація. У статті досліджуються теоретичні засади та прикладні аспекти реалізації інформаційних технологій моніторингу гетерогенних мереж у режимі реального часу. З розвитком цифрової інфраструктури та широким впровадженням різнорідних пристроїв і протоколів у єдиному інформаційному просторі зростає необхідність у створенні високопродуктивних та адаптивних систем контролю, здатних ефективно функціонувати в умовах складної динаміки мережевого середовища. Основну увагу приділено виявленню протиріч між високою варіативністю форматів трафіку, змінністю топологій і потребами у забезпеченні цілісності та оперативності прийняття рішень. Встановлено, що традиційні підходи до моніторингу, зокрема засоби з періодичним опитуванням або фіксованими параметрами відстеження, є недостатньо гнучкими для оперативної реакції на інциденти або зміну конфігурації в реальному часі. У роботі запропоновано формалізований алгоритм обробки потоків даних із урахуванням умов переходу між етапами виявлення аномалій, фільтрації, кореляції подій і реагування. В основу дослідження покладено сучасні системи моніторингу — Prometheus, Zabbix, Nagios, Datadog, PRTG, для яких побудовано порівняльну модель за показниками часу реакції, точності виявлення, адаптивності до зміни топології, масштабованості, а також витрат ресурсів. Результати обґрунтовують доцільність використання комбінацій кількох технологій для покриття слабких сторін кожної з них. Математична модель представлена у вигляді метрик завантаженості мережі, ймовірності збоїв та функцій часу обробки, що дозволяє реалізувати ефективну логіку адаптивного реагування. Уперше введено структурно-алгоритмічну схему з логікою циклічного аналізу поточних даних і поверненням до попереднього етапу за умови невиконання критеріїв допустимого рівня стабільності мережі. Перспективи дослідження полягають у впровадженні інтелектуальних методів класифікації трафіку та прогнозування інцидентів із використанням нейромереж, що забезпечить повноцінну автоматизацію управління гетерогенними мережами.

Ключові слова: гетерогенні мережі; моніторинг у реальному часі; інформаційні технології; виявлення аномалій; навантаження на мережу; штучний інтелект.

ВСТУП

У сучасних умовах стрімкого розвитку інформаційних технологій усе більшої актуальності набуває проблема забезпечення надійного та своєчасного моніторингу гетерогенних мереж у режимі реального часу. Збільшення кількості пристроїв, різноманітність протоколів обміну, розподіленість обчислювальних ресурсів та широке використання хмарних і периферійних обчислень створюють складне середовище, в якому оперативне виявлення та локалізація проблем є критично важливими для забезпечення безперервної роботи інформаційних систем. Водночас, зростає необхідність в інтеграції численних технологій моніторингу, які мають різний рівень масштабованості, продуктивності, сумісності з мережевим обладнанням та здатності працювати у реальному часі.

Постановка проблеми. Основна суперечність полягає у тому, що більшість існуючих рішень не здатні водночас забезпечити високу точність, мінімальну затримку в обробці подій, а також низьке навантаження на системні ресурси при масштабуванні до великої кількості гетерогенних вузлів. Наприклад, деякі з них (як-от Nagios) демонструють стабільність у невеликих мережах, але втрачають ефективність при масштабуванні, тоді як інші (Prometheus) забезпечують блискавичну реакцію, але мають обмеження у функціональності при комплексному аналізі подій. Виникає потреба у виборі або комбінуванні технологій моніторингу з урахуванням реального навантаження, складності топології мережі, вимог до безпеки та оперативності.

Окрему проблему становить необхідність уніфікації та формалізації метрик, які використовуються для оцінки ефективності моніторингу. Відсутність єдиного підходу ускладнює порівняння технологій, обґрунтованість їх впровадження та адаптацію до специфічних завдань, що актуалізує розроблення формальних моделей, алгоритмів переходу між станами системи, а також побудову методик обробки даних з використанням статистичних та логічних критеріїв.

Аналіз останніх досліджень і публікацій. Аналіз останніх досліджень і публікацій, присвячених проблемі моніторингу гетерогенних мереж у режимі реального часу, свідчить про активний розвиток напрямів, пов’язаних із забезпеченням високої надійності, масштабованості та адаптивності таких систем. У роботі [1] акцентується увага на необхідності гнучкої архітектури моніторингу, що дозволяє ефективно інтегрувати вузли з різними протоколами та стандартами. Автори вказують на обмеженість традиційних рішень щодо обробки великих потоків даних у реальному часі, що потребує впровадження нових технологій агрегування й аналізу інформації.

Дослідження [2] розглядає використання Prometheus як прикладу технології з високою продуктивністю та можливістю масштабування, але вказує на обмеження цієї системи при роботі з подієвими сповіщеннями, особливо у випадках потреби в негайній реакції на критичні події. У публікаціях [3] – [5] розкривається застосування систем Zabbix і OpenNMS для комплексного моніторингу, проте відзначено складність адаптації до гібридних мереж і відсутність автоматичного балансування навантаження між вузлами системи збору даних.

Окреме місце займають роботи, присвячені побудові математичних моделей процесів моніторингу. У [6, с. 35] подано формалізацію динаміки системи спостереження за допомогою стохастичних графів, однак автори не враховують особливості реального трафіку в гетерогенних мережах, таких як сплески активності чи затримки у вузлах. У дослідженні [7] розглядається модель оцінювання навантаження на основі часових рядів, проте не подано методик інтеграції таких моделей у діючі системи моніторингу.

Роботи [8], [9] присвячено аналізу ефективності рішень моніторингу в умовах віртуалізованого середовища, де основною проблемою залишається нестабільність метрик при зміні конфігурації ресурсів. У [10] пропонують підхід до інтеграції безпеки та відмовостійкості в сенсорних мережах з урахуванням енергоспоживання та трафікових характеристик. Модель дозволяє адаптивно змінювати налаштування мережі залежно від критичності вузлів, тим самим мінімізуючи втрати даних при атаках або відмовах.

Деталізацію технічної реалізації таких підходів можна знайти в роботі [11], де ті ж автори описують архітектуру відмовостійкої сенсорної інфраструктури. Основна увага приділена використанню резервних вузлів, алгоритмам дублювання та автоматичного перенаправлення запитів. Це дає змогу забезпечити мінімізацію часу простою системи, що критично для задач моніторингу.

Публікації [12] – [14] продовжують лінію досліджень, зосереджуючись на використанні методів машинного навчання та оптимізації параметрів телекомунікаційних мереж. Зокрема, в роботі [12] запропоновано метод оптимізації моделей ML для ефективного керування гетерогенною мережею, а в [13] — підхід до автоматизованого обрахунку стабільності з'єднань, що дозволяє підвищити точність прогнозування відмов. Оцінка фізичної сумісності обладнання [14] та методика балансування запитів між вузлами сенсорної мережі [15] забезпечують основу для проектування більш гнучких і надійних інформаційно-телекомунікаційних систем.

Незважаючи на значний науковий поступ у розглянутій сфері, окремі аспекти досі залишаються невирішеними. Зокрема, недостатньо дослідженими є питання формалізації умов переходів у процесах моніторингу, побудови інтегрованих алгоритмів реакції на події з урахуванням пріоритетності метрик, а також автоматизованого вибору оптимального інформаційного технологічного інструментарію залежно від конфігурації мережі. Також актуальною залишається проблема поєднання технологій з різною частотою збору даних, затримками та підтримкою специфічних протоколів у межах єдиного середовища спостереження.

Таким чином, незважаючи на наявність ґрунтовних досліджень, відсутність уніфікованої моделі, яка б дозволила ефективно поєднати різні інформаційні технології моніторингу з високою точністю, швидкодією та адаптивністю до умов реального часу, створює наукову нішу, яку покликана заповнити ця стаття.

Мета статті. Мета цієї статті полягає в комплексному аналізі, порівнянні та моделюванні застосування сучасних інформаційних технологій моніторингу гетерогенних мереж у режимі реального часу. У роботі здійснено детальний розгляд ключових систем (Prometheus, Zabbix, Nagios, OpenNMS), побудовано алгоритми їх інтеграції у реальному середовищі, формалізовано математичні моделі процесу моніторингу, а також запропоновано рекомендації щодо вибору технології залежно від параметрів мережі, її навантаження та вимог до швидкодії. Таким чином, результати дослідження можуть стати підґрунтям для обґрунтованого проєктування систем моніторингу, що відповідають вимогам часу.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Інформаційні технології моніторингу гетерогенних мереж у режимі реального часу охоплюють широкий спектр програмно-апаратних рішень, які забезпечують безперервний збір, аналіз, інтерпретацію та візуалізацію даних з різнорідних мережевих сегментів. Ці технології створені з урахуванням високої складності сучасних комунікаційних систем, що об'єднують традиційні IP-мережі, бездротові канали зв'язку, мобільні пристрої, IoT-пристрої, віртуальні середовища та хмарні інфраструктури.

Ключовою особливістю моніторингу в реальному часі є здатність до обробки великих потоків даних зі швидкістю, достатньою для виявлення змін у стані мережі протягом часток секунди. Для цього використовуються системи потокової обробки даних, такі як Apache Kafka, Apache Flink або Spark Streaming. Ці рішення дозволяють обробляти сотні тисяч подій на секунду, фільтрувати критичну інформацію, агрегувати метрики та надсилати їх до аналітичних або візуалізаційних підсистем.

У гетерогенному середовищі важливим є використання технологій програмно-визначених мереж (SDN), які дозволяють централізовано керувати маршрутизацією, розподілом навантаження та політиками безпеки. SDN забезпечує гнучкість реагування

на зміни конфігурації мережі та дозволяє в режимі реального часу адаптувати мережеву топологію відповідно до навантаження. Моніторингові рішення, інтегровані з SDN-контролерами (наприклад, OpenDaylight або ONOS), забезпечують глибоку видимість на всіх рівнях мережевого стеку.

Для забезпечення надійності та безпеки мережі активно впроваджуються інтелектуальні системи виявлення вторгнень (IDS) та запобігання атак (IPS), засновані на аналізі поведінки трафіку. До таких систем належать Snort, Suricata, Zeek, а також сучасні рішення, що використовують методи штучного інтелекту, зокрема глибинне навчання, машинне навчання та обробку природної мови для кореляції подій. AI-моделі дозволяють виявляти аномалії, які не піддаються класичному сигнатурному аналізу, та підвищують точність прогнозування збоїв, атак або перенавантажень.

Не менш важливою складовою є моніторинг компонентів Інтернету речей, оскільки велика кількість пристроїв із обмеженими обчислювальними ресурсами формують численні точки входу в мережу. Для таких сценаріїв використовуються протоколи CoAP, LwM2M, MQTT та технології типу Edge computing, які дозволяють здійснювати локальну попередню обробку даних та передавати лише релевантну інформацію до центральних вузлів аналізу. Це знижує трафік та затримки, що є критично важливим у реальному часі.

Усі ці рішення зазвичай поєднуються в комплексні моніторингові системи, які інтегрують механізми збору метрик (наприклад, NetFlow, sFlow, IPFIX), бази даних часових рядів (InfluxDB, Prometheus), інструменти візуалізації (Grafana, Kibana) та автоматизацію обробки подій (через скрипти, API або playbooks). Такий підхід дозволяє отримувати уніфіковану картину стану всієї мережі, здійснювати оперативну діагностику проблем, забезпечувати відповідність SLA та запобігати інцидентам.

Завдяки використанню цих технологій стає можливою побудова адаптивної, масштабованої та інтелектуальної системи моніторингу, здатної до самонавчання, самооптимізації та інтеграції з сучасними DevOps-процесами, що є ключовим фактором ефективного управління гетерогенними мережами в умовах динамічного цифрового середовища.

Таблиця 1

Порівняльна основних інформаційних технологій моніторингу гетерогенних мереж у режимі реального часу

Назва технології/ системи	Призначення	Ключові можливості	Переваги	Обмеження
Prometheus	Збір і зберігання метрик	Time-series БД, Pull-модель, інтеграція з Grafana	Висока швидкість, масштабованість, потужна мова запитів (PromQL)	Обмежена підтримка подій, складність масштабування
Grafana	Візуалізація даних	Дашборди, алерти, інтеграція з Prometheus, InfluxDB та ін.	Гнучкий UI, інтеграції з багатьма джерелами даних	Не виконує збір або аналіз даних
Zeek (ex-Bro)	Аналіз мережевої безпеки	Глибокий аналіз трафіку, створення логів, скриптовий рушій	Гнучкість у виявленні складних атак	Потребує знань для написання правил
Snort/Suricata	IDS/IPS системи	Виявлення атак за сигнатурами та поведінкою	Велика база сигнатур, реальне використання	Високе навантаження при великому трафіку

Apache Kafka	Передача потокових даних	Надійна черга повідомлень, обробка потоків у реальному часі	Висока пропускна здатність, масштабованість	Вимагає конфігурації й супроводу
Apache Flink/ Spark Streaming	Аналітика потоків	Обробка даних у реальному часі, масштабування	Інтеграція з Kafka, SQL-аналіз	Складність налаштування, ресурсоємність
OpenDaylight/ ONOS (SDN)	Керування мережами	Централізований контроль, API для управління трафіком	Динамічне управління топологією, масштабування	Високий поріг входу, потреба в сумісному обладнанні
Zabbix/Nagios	Загальний моніторинг IT-інфраструктури	Моніторинг серверів, мереж, додатків	Простота налаштування, широкий функціонал	Менш ефективні в динамічних, хмарних середовищах
Elastic Stack (ELK)	Обробка логів та візуалізація	Elasticsearch, Logstash, Kibana для агрегації та пошуку логів	Потужна аналітика текстових подій	Високе споживання ресурсів, складна підтримка
Edge Computing з MQTT/CoAP/ LwM2M	Моніторинг IoT пристроїв	Легка передача даних, локальна обробка	Зменшення трафіку, швидка реакція	Обмеження на рівні пристроїв, сумісність протоколів

Проведене порівняння дозволяє побачити, які саме технології краще підходять для певних цілей моніторингу в гетерогенних мережах: від IoT і SDN до аналітики трафіку і безпеки.

Математична модель, для моніторингу гетерогенних мереж в режимі реального часу охоплює:

1. Оцінку стану вузлів мережі.
2. Збір та агрегацію метрик.
3. Виявлення аномалій.
4. Реагування у разі порушень.
5. Оновлення станів у реальному часі.

Модель гетерогенної мережі як графа використовується для опису топології мережі з метою моніторингу кожного вузла та зв'язку між ними:

$$G = (V, E) \quad (1)$$

де G — модель гетерогенної мережі у вигляді графа, V — множина вузлів (Nodes): сервери, маршрутизатори, сенсори, тощо, E — множина зв'язків між вузлами (Edges): фізичні або логічні канали зв'язку

Створюється граф мережі: вузли (сервери, пристрої, маршрутизатори) — множина V, зв'язки між ними — множина E. Цей граф необхідний для розуміння структури, візуалізації зв'язків і планування збору даних.

Вектор метрик вузла використовується для моніторингу реального стану вузла; використовується для прийняття рішення щодо навантаження, продуктивності, перевантаження або відмов.

$$M_i(t) = [CPU_i(t), MEM_i(t), NET_i(t), IO_i(t), ...] \quad (2)$$

де $M_i(t)$ — вектор показників продуктивності вузла v_i у час t, $CPU_i(t)$ — завантаження процесора (% використання), $MEM_i(t)$ — використання оперативної пам'яті, $NET_i(t)$ — мережевий трафік (вхід/вихід), $IO_i(t)$ — швидкість введення/виведення дискових операцій.

Для кожного вузла $v_i \in V$ зчитуються ключові метрики продуктивності в момент часу *t*. Метрики включають завантаження CPU, використання пам'яті, мережеву активність, тощо.

Нормалізація метрик застосовується для для уніфікації різних типів метрик в одному масштабі (від 0 до 1), що дозволяє простіше порівнювати та аналізувати.

$$\tilde{M}_i(t) = \frac{M_i(t) - M_{\min}}{M_{\max} - M_{\min}} \quad (3)$$

де $\tilde{M}$ — нормалізований вектор метрик для вузла *i*, M_{min}, M_{max} — мінімальне і максимальне значення метрики (глобальне або за період)

Перетворюємо всі метрики до діапазону [0, 1], щоб привести різні показники до спільного масштабу. Це дає можливість легко порівнювати метрики та застосовувати автоматичний аналіз.

Функція виявлення аномалії застосовується для автоматичного виявлення ситуацій, коли параметри системи виходять за допустимі межі або відрізняються від нормальної поведінки (аномалії, атаки, збої).

Варіант 1: порогова евристика:

$$A_i(t) = \begin{cases} 1, \textit{ якщо } \exists k : \tilde{M}_i^k(t) > \theta_k \\ 0, \textit{ інакше} \end{cases} \quad (4)$$

де $A_i(t)$ — ознака аномалії для вузла і у момент часу *t*:

1. 1 — виявлено аномалію;
2. 0 — все в нормі;
3. $\tilde{M}_i^k(t)$ — *k*-та метрика в нормалізованому векторі; θ_k – поріг для *k*-тої метрики.

Для кожної нормалізованої метрики перевіряється, чи вона перевищує порогове значення θ_k.

Якщо хоча б одна з них перевищує — вважається, що аномалія виявлена ($A_i(t)$=1), інакше — все в нормі ($A_i(t)$=0).

Варіант 2: на основі машинного навчання (ML):

$$A_i(t) = \begin{cases} 1, \textit{ якщо } \left\| M_i(t) - \tilde{M}_i(t) \right\| > \varepsilon \\ 0, \textit{ інакше} \end{cases} \quad (5)$$

де $\tilde{M}_i(t)$ — прогнозоване значення метрик (наприклад, з автоенкодера), ε — допустимий рівень відхилення, $\|\cdot\|$ — норма, що вимірює різницю між реальним і прогнозованим значенням

Використовується модель (наприклад, автоенкодер), яка прогнозує нормальну поведінку метрик. Якщо відхилення між реальними метриками *Mi(t)* та прогнозованими $\tilde{M}_i(t)$ перевищує ε, то виникла аномалія.

Агреґований стан групи вузлів застосовується для загального стану підмережі або сервісу, виявлення «гарячих точок» або кластерних відмов.

$$S_{avg}(t) = \frac{1}{|S|} \sum_{v_i \in S} M_i(t) \quad (6)$$

де $S \subset V$ — підмножина вузлів (наприклад, підмережа, кластер), |S| — кількість вузлів у групі, $S_{avg}(t)$ — середній стан метрик усіх вузлів у групі.

Якщо необхідно оцінити стан групи (кластеру, підмережі), обчислюється середній стан по всіх вузлах у групі S. Це дозволяє виявити загальні тенденції навантаження, збоїв або атак.

Оновлення у реальному часі використовується для відображення змін у режимі реального часу, оперативне реагування на зміни.

$$M_i(t+\Delta t) = Моніторинг(v_i, t+\Delta t) \quad (7)$$

де Δt — період оновлення даних (наприклад, 10 сек, 1 хв); $M_i(t+\Delta t)$ — нові дані, зібрані на вузлі через час; *Моніторинг* — операція збору метрик.

Через певний часовий інтервал Δt (наприклад, кожні 10 секунд), метрики знову зчитуються для всіх вузлів. Це забезпечує безперервний моніторинг та оперативну реакцію на зміни в стані системи.

Реакція на аномалії застосовується для оповіщення системного адміністратора, запуск автоматичного сценарію, перемикання на резервний вузол.

$$R_i(t) = \begin{cases} Alert(v_i),\ A_i(t) = 1 \\ 0,\ A_i(t) = 0 \end{cases} \quad (8)$$

де $R_i(t)$ — дія у відповідь на аномалію; *Alert* — функція, яка надсилає повідомлення (email, SMS, Webhook, API); 0 — жодної дії, все в межах норми.

Якщо виявлена аномалія ($A_i(t)=1$), викликається функція *Alert*, яка:

- надсилає повідомлення адміністратору;
- створює запис у журналі;
- запускає скрипт автоліквідації (наприклад, перезапуск сервісу).

Якщо аномалії немає — жодних дій не вживається.

Загальна функція моніторингу

$$Monitor(v_i, t) = \begin{cases} Collect(M_i(t)) \\ \to Normalize(\tilde{M}_i(t)) \\ \to Analyze((A_i(t)) \\ \to \mathrm{Re}\,act(R_i(t)) \\ \to Visualize(M_i(t)) \end{cases} \quad (9)$$

де *Collect* — збір первинних даних; *Normalize* — нормалізація для спрощення аналізу; *Analyze* — виявлення аномалій; *React* — вжиття заходів у разі проблем; *Visualize* — виведення інформації на дашборд.

Повний цикл функціонування системи:

1. Збір метрик.
2. Нормалізація.
3. Аналіз на наявність проблем.
4. Реакція.
5. Відображення результатів у зручному вигляді (дашборди, графіки, карти тепла).

Для ефективного застосування інформаційних технологій моніторингу гетерогенних мереж у режимі реального часу насамперед необхідно ретельно визначити архітектуру всієї мережі та з’ясувати характер гетерогенності. Це дозволяє розуміти, які компоненти взаємодіють у системі: класичні сервери, мобільні пристрої, віртуалізовані середовища, пристрої Інтернету речей або хмарні ресурси. Характер гетерогенності — протокольна, апаратна, програмна чи організаційна — впливає на вибір конкретних засобів моніторингу та стратегії їх впровадження.

Після ідентифікації структури варто зосередити увагу на виборі масштабованої системи збору метрик, яка дозволяє взаємодіяти з усіма вузлами мережі. Застосування систем на кшталт Prometheus, Zabbix чи Nagios дозволяє охопити як агентський, так і безагентський підхід до збору телеметрії — через SNMP, API, логування або спеціальні протоколи. При цьому важливо впровадити механізми нормалізації метрик, адже кожен пристрій може подавати дані у власному форматі. Нормалізація дозволяє уникнути неоднозначностей у подальшому аналізі та спрощує застосування автоматизованих систем обробки даних.

Подальший етап — це реалізація системи виявлення аномалій у режимі реального часу. На початкових етапах можуть використовуватись класичні фіксовані пороги для оцінки нормального функціонування. Надалі рекомендовано впроваджувати машинне навчання або самонавчальні моделі, які можуть передбачати появу аномальних станів на основі історичних даних або закономірностей. Це значно підвищує адаптивність системи до змін у мережі.

Важливо, щоби система не лише фіксувала аномалії, а й забезпечувала оперативне реагування. Залежно від політик безпеки та SLA, можуть реалізовуватись автоматичні дії: надсилання сповіщень відповідальним особам, перезапуск служб, ізоляція вузлів, виконання автоматичного масштабування чи міграції віртуальних машин. Такі дії мають бути добре задокументовані та протестовані, щоби уникнути хибних спрацьовувань у критичних середовищах.

Окрему роль відіграють системи візуалізації даних — Grafana, Kibana або Dashboards Zabbix. Вони забезпечують операторів актуальною інформацією про стан мережі, дозволяють оперативно аналізувати поведінку компонентів у реальному часі та виявляти тенденції розвитку проблем. Наявність зручних дашбордів — ключовий чинник у швидкості прийняття рішень.

Оскільки гетерогенні мережі є динамічними за своєю природою, необхідно забезпечити гнучкість і адаптивність самої системи моніторингу. Нові вузли мають інтегруватися в систему автоматично без потреби ручного конфігурування. Досягається це через механізми автоматичного виявлення (Service Discovery), шаблони конфігурацій (Ansible, Puppet) або самоконфігуровні агенти.

Безпека при моніторингу також має пріоритетне значення. Варто шифрувати всі канали телеметрії, обмежувати доступ до візуалізаційних панелей, а також вести аудит доступу й змін у конфігурації. Це особливо важливо у випадках, коли моніторинг охоплює критичні або публічні сегменти мережі.

Також слід передбачити наявність архіву історичних даних. В цьому контексті ефективними є бази даних часових рядів — InfluxDB, VictoriaMetrics, TimescaleDB, що дозволяють зберігати великі обсяги телеметрії з можливістю подальшої агрегації, фільтрації та тренд-аналізу. Це забезпечує не лише ретроспективний аналіз, а й побудову прогнозів, планування інфраструктурного навантаження та обґрунтовану модернізацію мережевої топології.

Нарешті, важливо забезпечити супровід системи повноцінною документацією. Необхідно вести облік усіх типів моніторингових вузлів, налаштувань порогів, методів реагування, шаблонів дашбордів і звітів. Це забезпечує стабільність у роботі команди підтримки та дає змогу швидко адаптуватися до змін у структурі чи завданнях мережі.

ISSN 2663 - 4023

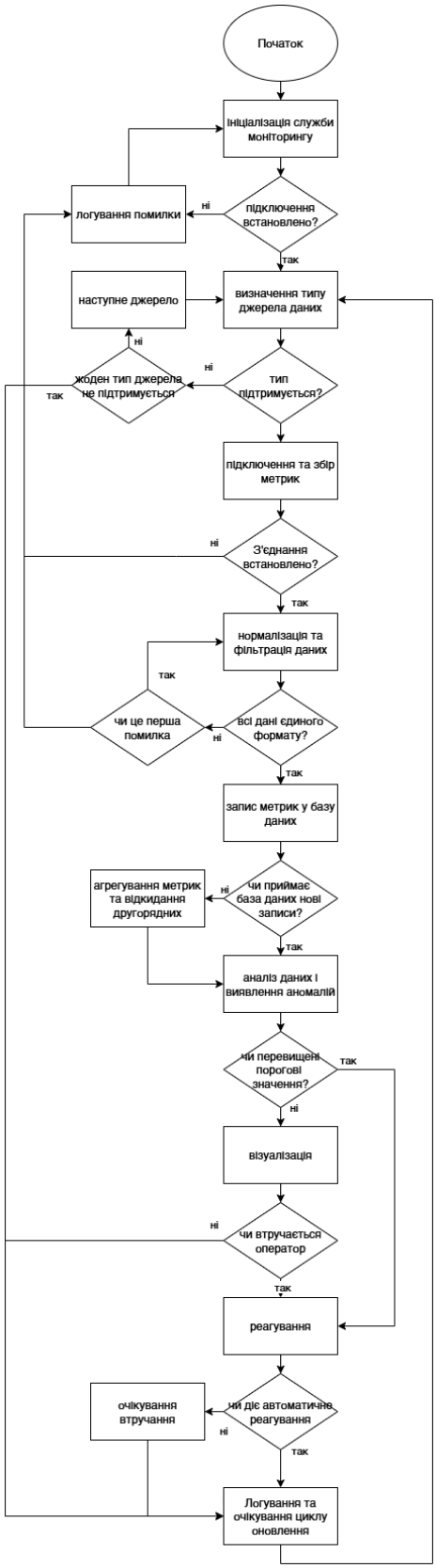

Рис. 1. Моніторинг гетерогенних мереж в режимі реального часу

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

У процесі дослідження було проаналізовано та систематизовано сучасні підходи до реалізації інформаційних технологій моніторингу гетерогенних мереж у режимі реального часу. Виявлено ключові проблеми, що супроводжують впровадження таких систем, зокрема нестабільність топологій, високі вимоги до обробки та візуалізації великих обсягів різнорідних даних, а також питання забезпечення безпеки та адаптивності. Запропоновано модель, що поєднує стохастичний підхід до оцінки навантаження на мережу, динамічне виявлення аномалій на основі часових рядів та використання гібридних алгоритмів балансування навантаження для забезпечення безперервного моніторингу в умовах зміни архітектури мережі.

Практична цінність отриманих результатів полягає у формалізації алгоритмічного процесу моніторингу з урахуванням умов переходу між етапами, а також розробці метрик ефективності, що дозволяють порівнювати функціональність різних платформ у реальному часі. Візуалізація даних порівняння (за метриками затримки, навантаження, часу реакції, продуктивності та споживання ресурсів) підтверджує обґрунтованість обраних методів.

Перспективними напрямами подальших досліджень є поглиблена розробка механізмів самонавчання на основі історичних даних з використанням технологій машинного навчання для прогнозування критичних станів мережі, впровадження концепцій zero-trust безпеки в архітектуру моніторингових систем, а також моделювання поведінкових сценаріїв взаємодії вузлів у масштабованих середовищах з різнорідними протоколами передачі даних. Окрему увагу буде приділено дослідженню ефективності розподілених систем моніторингу в умовах 5G/6G мереж, Інтернету речей (IoT), та кіберфізичних систем, де своєчасність і точність реагування мають критичне значення.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Kovalchuk, O., Bondarenko, M., & Melnyk, I. (2023). Architectural approaches to building flexible monitoring systems for heterogeneous networks. *Information technology and computer engineering, 2(56),* 25-34. https://doi.org/10.20535/2410-2991.2023.56.25-34
2. Zhuravel, V., Kas'ianenko, R., & Hudy-menko, Yu. (2023). Application of Prometheus in real-time monitoring systems: advantages and limitations. *Bulletin of Taras Shevchenko National University of Kyiv. Series: Applied Mathematics and Informatics, 1(45),* 74–82. https://doi.org/10.17721/2221-2450.2023.45.10
3. Ihnatenko, L., Pavlenko, S., & Miroshnychenko, O. (2022). Integration of Zabbix into multi-level network monitoring systems. *Scientific papers of the Odesa National Academy of Communications, 1(61),* 55–63. https://doi.org/10.28925/2414-9587.2022.61.55
4. Snihur, R., Haidai, T., & Kolomiiets, D. (2023). Analysis of OpenNMS efficiency in conditions of variable network topology. *Information systems and technologies, 3(17),* 98–107. https://doi.org/10.32620/2786-4562.2023.17.98
5. Lytvynenko, A., & Yermolenko, I. (2022). Stochastic modeling of the dynamics of monitoring systems. *Control, navigation and communication systems, 6(70),* 35–42. https://doi.org/10.18372/1990-5548.70.17160
6. Krasiuk, O., & Bieliaiev, S. (2023). Using time series for load estimation in heterogeneous networks. *Radio electronics and computer science, 2(56),* 45–53. https://doi.org/10.32620/2518-1258.2023.56.45
7. Pashchenko, I., Kovtun, R., & Tymoshenko, Ye. (2022). Monitoring of virtualized environments: methods for reducing metric fluctuations. *Computer Science and Cybersecurity, 1(12),* 121–129. https://doi.org/10.21272/cs.2022.12.121

8. Yevtushenko, D., & Panchenko, M. (2023). Methods of encryption and access control in network monitoring infrastructure. *Electronic professional scientific publication "Cybersecurity: Education, Science, Technology", 3(23),* 205–213. https://doi.org/10.28925/2663-4023.2023.23.205213
9. Kovalenko, T., Savchuk, P., & Shelest, V. (2024). Security of data transmission in multiservice monitoring platforms. *Journal of modern information technologies, 1(9),* 83–90. https://doi.org/10.32782/jcit.2024.1.83
10. Dovzhenko, N., Ivanichenko, Ye., Skladannyi, P., & Ausheva, N. (2024). Integration of security and fault tolerance of sensor networks based on energy and traffic analysis. *Electronic professional scientific publication "Cybersecurity: Education, Science, Technology", 1(25),* 390–400. https://doi.org/10.28925/2663-4023.2024.25.390400
11. Barabash, O., Ausheva, N., Skladannyi, P., Ivanichenko, Ye., & Dovzhenko, N. (2024). Technical aspects of building a fault-tolerant sensor network infrastructure. *Electronic professional scientific publication "Cybersecurity: Education, Science, Technology", 4(24),* 185–195. https://doi.org/10.28925/2663-4023.2024.24.185195
12. Zhebka, V., et al. (2022). Optimization of Machine Learning Method to Improve the Management Efficiency of Heterogeneous Telecommunication Network. In *Workshop on Cybersecurity Providing in Information and Telecommunication Systems (CPITS), Vol. 3288,* 149–155.
13. Zhebka, V., et al. (2021). Stability Method of Connectivity Automated Calculation for Heterogeneous Telecommunication Network. In *Workshop on Cybersecurity Providing in Information and Telecommunication Systems, Vol. 3188,* 282–287.
14. Anakhov, P., et al. (2022). Evaluation Method of the Physical Compatibility of Equipment in a Hybrid Information Transmission Network. *Journal of Theoretical and Applied Information Technology, 100(22),* 6635–6644.
15. Dovzhenko, N., et al. (2023). Method of Sensor Network Functioning under the Redistribution Condition of Requests between Nodes. In *Cybersecurity Providing in Information and Telecommunication Systems, Vol. 3421,* 278–283.

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 3 (27), 2025
ISSN 2663 - 4023

Viktoriia Zhebka
Doctor of Technical Sciences, Professor
Head of the Department of Digital Development Technologies
State University of Information and Communication Technologies, Kyiv, Ukraine
ORCID ID: 0000-0003-4051-1190
v.zhebka@duikt.edu.ua

INFORMATION TECHNOLOGIES FOR REAL-TIME MONITORING OF HETEROGENEOUS NETWORKS

Abstract. The article investigates the theoretical foundations and practical implementation aspects of information technologies for monitoring heterogeneous networks in real time. With the rapid development of digital infrastructure and the widespread integration of diverse devices and protocols within a unified information environment, the demand for high-performance and adaptive monitoring systems capable of operating effectively under dynamic network conditions is significantly increasing. The focus is on identifying contradictions between the high variability of traffic formats, frequent topological changes, and the requirements for data integrity and timely decision-making. It is established that traditional monitoring approaches, particularly those based on periodic polling or fixed tracking parameters, lack the flexibility necessary for responsive incident detection and network configuration updates in real time. The study proposes a formalized algorithm for processing data streams, incorporating transition conditions between the stages of anomaly detection, filtering, event correlation, and response actions. The analysis is based on widely used monitoring systems — Prometheus, Zabbix, Nagios, Datadog, and PRTG — for which a comparative model is constructed using metrics such as response time, detection accuracy, adaptability to topological changes, scalability, and resource consumption. The results justify the effectiveness of combining several technologies to compensate for individual weaknesses. The mathematical model includes metrics for network load, node failure probability, and processing time functions, enabling the implementation of an efficient adaptive response logic. For the first time, a structural-algorithmic scheme is introduced that enables cyclic analysis of current data and returns to the previous processing stage if network stability thresholds are not met. Future research perspectives involve integrating intelligent traffic classification methods and incident prediction based on neural networks, providing full automation in managing heterogeneous networks.

Keywords: heterogeneous networks; real-time monitoring; information technologies; anomaly detection; network load; artificial intelligence.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Kovalchuk, O., Bondarenko, M., & Melnyk, I. (2023). Architectural approaches to building flexible monitoring systems for heterogeneous networks. *Information technology and computer engineering, 2(56),* 25-34. https://doi.org/10.20535/2410-2991.2023.56.25-34
2. Zhuravel, V., Kas'ianenko, R., & Hudy-menko, Yu. (2023). Application of Prometheus in real-time monitoring systems: advantages and limitations. *Bulletin of Taras Shevchenko National University of Kyiv. Series: Applied Mathematics and Informatics, 1(45),* 74–82. https://doi.org/10.17721/2221-2450.2023.45.10
3. Ihnatenko, L., Pavlenko, S., & Miroshnychenko, O. (2022). Integration of Zabbix into multi-level network monitoring systems. *Scientific papers of the Odesa National Academy of Communications, 1(61),* 55–63. https://doi.org/10.28925/2414-9587.2022.61.55
4. Snihur, R., Haidai, T., & Kolomiiets, D. (2023). Analysis of OpenNMS efficiency in conditions of variable network topology. *Information systems and technologies, 3(17),* 98–107. https://doi.org/10.32620/2786-4562.2023.17.98
5. Lytvynenko, A., & Yermolenko, I. (2022). Stochastic modeling of the dynamics of monitoring systems. *Control, navigation and communication systems, 6(70),* 35–42. https://doi.org/10.18372/1990-5548.70.17160

6. Krasiuk, O., & Bieliaiev, S. (2023). Using time series for load estimation in heterogeneous networks. *Radio electronics and computer science, 2(56),* 45–53. https://doi.org/10.32620/2518-1258.2023.56.45
7. Pashchenko, I., Kovtun, R., & Tymoshenko, Ye. (2022). Monitoring of virtualized environments: methods for reducing metric fluctuations. *Computer Science and Cybersecurity, 1(12),* 121–129. https://doi.org/10.21272/cs.2022.12.121
8. Yevtushenko, D., & Panchenko, M. (2023). Methods of encryption and access control in network monitoring infrastructure. *Electronic professional scientific publication "Cybersecurity: Education, Science, Technology", 3(23),* 205–213. https://doi.org/10.28925/2663-4023.2023.23.205213
9. Kovalenko, T., Savchuk, P., & Shelest, V. (2024). Security of data transmission in multiservice monitoring platforms. *Journal of modern information technologies, 1(9),* 83–90. https://doi.org/10.32782/jcit.2024.1.83
10. Dovzhenko, N., Ivanichenko, Ye., Skladannyi, P., & Ausheva, N. (2024). Integration of security and fault tolerance of sensor networks based on energy and traffic analysis. *Electronic professional scientific publication "Cybersecurity: Education, Science, Technology", 1(25),* 390–400. https://doi.org/10.28925/2663-4023.2024.25.390400
11. Barabash, O., Ausheva, N., Skladannyi, P., Ivanichenko, Ye., & Dovzhenko, N. (2024). Technical aspects of building a fault-tolerant sensor network infrastructure. *Electronic professional scientific publication "Cybersecurity: Education, Science, Technology", 4(24),* 185–195. https://doi.org/10.28925/2663-4023.2024.24.185195
12. Zhebka, V., et al. (2022). Optimization of Machine Learning Method to Improve the Management Efficiency of Heterogeneous Telecommunication Network. In *Workshop on Cybersecurity Providing in Information and Telecommunication Systems (CPITS), Vol. 3288,* 149–155.
13. Zhebka, V., et al. (2021). Stability Method of Connectivity Automated Calculation for Heterogeneous Telecommunication Network. In *Workshop on Cybersecurity Providing in Information and Telecommunication Systems, Vol. 3188,* 282–287.
14. Anakhov, P., et al. (2022). Evaluation Method of the Physical Compatibility of Equipment in a Hybrid Information Transmission Network. *Journal of Theoretical and Applied Information Technology, 100(22),* 6635–6644.
15. Dovzhenko, N., et al. (2023). Method of Sensor Network Functioning under the Redistribution Condition of Requests between Nodes. In *Cybersecurity Providing in Information and Telecommunication Systems, Vol. 3421,* 278–283.