УДК 621.391.8-047.36 DOI: 10.31673/2412-4338.2024.037785

Треньов Микита Георгійович
Державний університет інформаційно-комунікаційних технологій, Київ
ORCID0009-0002-8459-0599

Прокопенко Андрій Георгійович
Державний університет інформаційно-комунікаційних технологій, Київ
ORCID0009-0009-7227-3458

ОСНОВНІ ПРИНЦИПИ РОБОТИ ТА ВИМОГИ ДО СТВОРЕННЯ СТРУКТУР ПЕРСПЕКТИВНИХ СИСТЕМ МОНІТОРИНГУ РОЗПОДІЛЕНИХ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖ

Анотація. *У статті на основі глибокого аналізу існуючих технологій та систем моніторингу інформаційно-телекомунікаційних мереж загального користування визначено основні вимоги та підходи до побудови перспективних систем мережевого моніторингу нового покоління. З огляду на швидкий розвиток технологій та збільшення навантаження на інформаційні мережі, з'являється необхідність у розробці нових підходів до побудови систем, що забезпечують ефективний моніторинг та контроль мереж. Метою даної роботи є розробка загальних принципів функціонування таких систем, а також визначення основних вимог до побудови надійних і стійких мережевих підсистем моніторингу. В ході дослідження особливу увагу приділено необхідності підвищення надійності та безперервності функціонування підконтрольних мереж, що досягається шляхом впровадження децентралізованих та розподілених архітектур моніторингових підсистем.*

Новизна роботи полягає у визначенні ключових архітектурних принципів, які забезпечують ефективну роботу систем моніторингу в умовах гетерогенності сучасних інформаційно-телекомунікаційних мереж. Зокрема, запропоновано використовувати принципи розподіленості та децентралізації, які дозволяють уникнути єдиної точки відмови та забезпечують стійкість мережі до зовнішніх загроз. У статті також наводиться опис функціональних можливостей підсистеми мережевого моніторингу, зокрема ролі сервера моніторингу, який виступає центральним елементом цієї архітектури. Описано структуру сервера моніторингу, а також його ключові функції, що включають збір, обробку та аналіз даних з різних сегментів мережі в режимі реального часу.

Також сформульовано загальні вимоги до систем моніторингу нового покоління, серед яких забезпечення високої надійності, масштабованості та можливості інтеграції з іншими системами управління та безпеки мережі. Ці вимоги враховують зростаючі обсяги даних, які передаються через мережі, а також необхідність оперативного реагування на загрози та аномалії в мережевому трафіку. Крім того, в роботі розглянуто загальні принципи організації та функціонування підсистем моніторингу, які мають бути адаптовані до умов гетерогенних мереж з різними технологічними стандартами та рівнями доступу.

У результаті дослідження запропоновано підхід до створення перспективних систем мережевого моніторингу, що забезпечують високий рівень стійкості, гнучкості та надійності. Окремо підкреслено значення використання нових методів збору та аналізу даних для підвищення ефективності управління мережею та забезпечення її безпеки.

Ключові слова: *інформаційно-телекомунікаційна мережа, сервер моніторингу, підсистема мережевого моніторингу, база даних, система управління*

Trenov Mykyta
State University of Information and Communication Technologies, Kyiv
ORCID0009-0002-8459-0599

Prokopenko Andriy
State University of Information and Communication Technologies, Kyiv
ORCID0009-0009-7227-3458

BASIC PRINCIPLES OF OPERATION AND REQUIREMENTS FOR THE CREATION OF STRUCTURES OF ADVANCED MONITORING SYSTEMS FOR DISTRIBUTED INFORMATION AND TELECOMMUNICATION NETWORKS

Abstract*. Based on an in-depth analysis of existing technologies and systems for monitoring public information and telecommunication networks, the article identifies the main requirements and approaches to building promising new generation network monitoring systems. Given the rapid development of technologies and the increasing load on information networks, there is a need to develop new approaches to building systems that ensure effective monitoring and control of networks. The purpose of this paper is to develop general principles of functioning of such systems, as well as to determine the basic requirements for building reliable and sustainable network monitoring subsystems. In the course of the study, special attention is paid to the need to increase the reliability and continuity of the controlled networks, which is achieved through the introduction of decentralized and distributed architectures of monitoring subsystems.*

The novelty of the work is to identify the key architectural principles that ensure the effective operation of monitoring systems in the context of heterogeneity of modern information and telecommunication networks. In particular, it is proposed to use the principles of distributedness and decentralization, which allow avoiding a single point of failure and ensure network resilience to external threats. The article also describes the functionality of the network monitoring subsystem, in particular the role of the monitoring server, which is the central element of this architecture. The structure of the monitoring server is described, as well as its key functions, which include collecting, processing, and analyzing data from different network segments in real time.

The general requirements for the new generation of monitoring systems are also formulated, including high reliability, scalability, and the ability to integrate with other network management and security systems. These requirements take into account the growing amount of data transmitted over networks, as well as the need to respond quickly to threats and anomalies in network traffic. In addition, the paper considers the general principles of organization and operation of monitoring subsystems that should be adapted to the conditions of heterogeneous networks with different technological standards and access levels.

As a result of the study, an approach to the creation of advanced network monitoring systems that provide a high level of stability, flexibility and reliability is proposed. The importance of using new methods of data collection and analysis to improve the efficiency of network management and ensure its security is emphasized.

Keywords*: information and telecommunication network, monitoring server, network monitoring subsystem, database, management system.*

1. Вступ

У сучасному світі, де розвиток інформаційно-телекомунікаційних технологій відіграє ключову роль у забезпеченні ефективної роботи різних сфер діяльності, виникає необхідність створення систем моніторингу мереж, здатних забезпечити їх стабільність, безперервність та безпеку. Постійне зростання кількості користувачів, збільшення обсягів даних, а також ускладнення структур мереж вимагають розробки нових підходів до управління та контролю за станом інформаційних мереж.

Ця робота присвячена дослідженню основних принципів роботи перспективних систем мережевого моніторингу, а також визначенню вимог до їх побудови. Вивчення сучасних підходів та аналіз існуючих систем дозволили сформулювати основні вимоги, які повинні бути враховані під час розробки таких систем, зокрема, важливість розподіленості, децентралізації та високої надійності компонентів.

Основною метою дослідження є розробка концептуальної моделі системи моніторингу, яка б враховувала новітні тенденції в розвитку телекомунікаційних технологій, забезпечуючи високу ступінь адаптивності до змін у мережевій інфраструктурі та мінімізацію ризиків, пов'язаних з її функціонуванням. Особлива увага приділяється вибору архітектурних рішень, що дозволять створити стійку та ефективну систему моніторингу, здатну оперативно реагувати на різноманітні виклики та загрози.

2. Функції підсистеми моніторингу інформаційно-телекомунікаційної мережі

Спочатку на інформаційно-телекомунікаційній мережі (ІТКМ) функції моніторингу здійснювали адміністратори, а інформація про технічний стан (ТС) систем збиралася ними у неспеціалізованих програмах (через їхню відсутність). Відомості про експлуатовані об'єкти контролю (ОК) були прив'язані до практичного досвіду роботи конкретного фахівця з мережевою інфраструктурою і повністю губилися під час його звільнення. В даний час з'явилося безліч напів і повністю автоматизованих систем моніторингу, що аналізують ТС мережевих елементів та окремих мереж ІТКМ, що здійснюють збір вимірювальної інформації за контрольованими параметрами та ймовірно-часових характеристик у часові ряди, зручні для візуалізації діаграми, таблиці та графіки, які при необхідності (у разі аномалії) можна аналізувати.

Для зберігання одержуваної під час моніторингу вимірювальної інформації про ОК зазвичай використовується конфігураційна база даних (БД) під різними системами управління (СУБД), де інформація про об'єкти контролю представлена, як набір одиниць конфігурації. Кожен сервер і кожен мережевий пристрій, що піддається моніторингу, є певною одиницею вимірювання, інформацію про яку зберігається в централізованій БД. Таке уявлення дозволяє згодом інтегрувати підсистему моніторингу з підсистемою візуалізації в інтересах системи підтримки прийняття рішень (СППР) на управління ІТКМ (АСУС) та ін. Для моніторингу функціонального стану ІТКМ запропоновано наступний варіант його побудови, рис. 1.

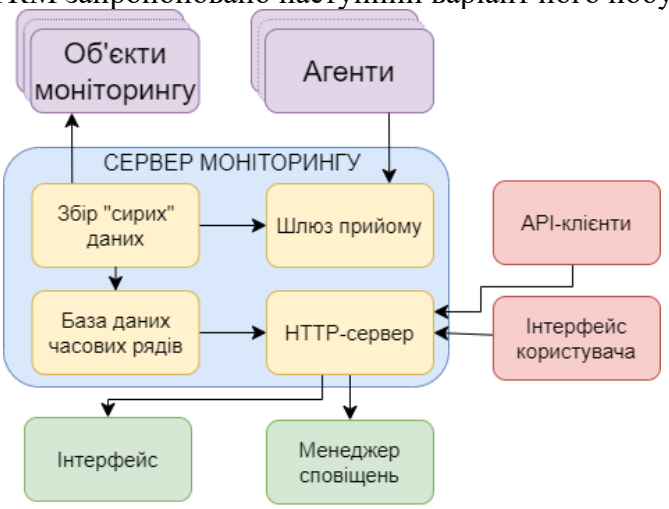

Рис. 1. Структурна схема сервера моніторингу ІТКС загального користування і залежних елементів

Структурно сервер моніторингу складається зі збирача «сирих» даних, бази даних часових рядів та HTTP або SNMP сервера [1], що функціонують у взаємодії з об'єктами моніторингу, підсистемою оповіщення та підсистемою відображення. Складальник «сирих» даних опитує об'єкти моніторингу за протоколом HTTP або SNMP і розміщує зібрані метрики до бази даних часових рядів. У базі даних зберігаються метрики моніторингу за тим самим об'єктом протягом заданого часу спостережень. Таким чином, можна визначити зміни значень параметрів об'єкта в часі.

Сервер моніторингу функціонально призначений для вирішення таких завдань:

- збір вимірювальної інформації про ТС елементів ІТКМ (мережевих пристроях, на яких функціонує ПЗ та ін.);
- обробки, узагальнення, зберігання та відображення інформації про стан елементів;
- зміни кількості об'єктів моніторингу через графічний інтерфейс користувача; графічного та табличного відображення даних (у т. ч. відображення динаміки);
- зміни контрольованих параметрів протягом встановленого часового інтервалу);

- оповіщення посадових осіб про виникнення критичних подій у системі;
- автоматичного чи автоматизованого реагування на виникнення критичних подій (відповідно до заздалегідь налаштованої логіки);
- ведення системних журналів: зміни стану мережевих елементів та їх окремих параметрів, дій системи та дій користувача, зміни параметрів системи.

При виборі, розробці (побудові) та впровадженні систем моніторингу спочатку необхідно визначитися з об'єктами, які будуть контролюватись, а також вибрати показники якості та критерії ефективності (настання критичних подій), які й визначать кількість оповіщень при відмові (збої), частоту сканування та інші параметри, а також наслідки для ІТКМ. Зазвичай на великих мережевих інфраструктурах перед фінальним використанням підсистем моніторингу розгортають тестовий сегмент мережі як стенда, на якому можна оцінити доцільність прийнятих рішень щодо порогових значень на контрольовані параметри, проаналізувати «вузькі місця» в ІТКМ.

До об'єктів моніторингу локальної обчислювальної мережі (ЛОМ) можна віднести такі програмні та технічні засоби: автоматизовані робочі місця (АРМ) посадових осіб; серверне обладнання; спеціалізоване обладнання; сервер друку; комплекс засобів захисту. Для регіональних та глобальних ІТКМ перелік обладнання відповідно буде значно ширшим.

З точки зору функціональної продуктивності ІТКМ підсистема моніторингу повинна здійснювати збір наступних даних про обчислювальні ресурси об'єкта моніторингу:

- тактова частота процесора;
- обсяг вільної оперативної пам'яті;
- вільний та використаний об'єм жорсткого диска;
- кількість переданих, втрачених пакетів та колізій мережевих інтерфейсів;
- збирання відомостей із системних журналів стороннього програмного забезпечення;
- збирання відомостей про запущені процеси;
- відправлення даних в ініціативному порядку та за запитом в активному та пасивному режимах;
- інтерфейс керування вбудованими командами та обладнанням за протоколом SSH.

За допомогою протоколу SNMP сервер моніторингу через збирач «сирих» даних здійснює збір наступних метричних даних мережевого пристрою, забезпеченого підтримкою протоколу обміну інформацією SNMP:

- статус порту: є фізичне підключення або ні, включено/вимкнено – програмно;
- час останньої зміни налаштувань порту;
- розмір найбільшого пакета, який може бути надісланий з пристрою;
- швидкість порту;
- список VLAN (для комутаторів ЛОМ); час роботи пристрою;
- опис пристрою;
- середнє завантаження процесора за 5 с, за 1 хв, за 5 хв; причина перезавантаження;
- опис та стан датчиків температури;
- обсяг вільної оперативної пам'яті;
- список IP-адрес інтерфейсів;
- таблиця маршрутів маршрутизаторів;
- вхідний та вихідний трафік;
- лічильник прийнятих та лічильник відправлених Unicast пакетів;
- лічильник прийнятих та лічильник відправлених Broadcast пакетів;
- лічильник прийнятих та лічильник відправлених Multicast пакетів;
- лічильник прийнятих пакетів з помилками та лічильник відправлених пакетів з помилками;
- лічильник відкинутих пакетів, які не містили помилок, але були відкинуті, наприклад, звільнення буферного простору.

Перелік метричних даних, що збираються, по різних ОК може відрізнятися.

Зібрані збирачем «сирих» метричних даних направляються на сервер моніторингу для обробки інформації та надання звітів у вигляді таблиць та графіків з можливістю експорту у формати CSV, PDF, XML, PNG. Характер метричних даних, необхідні збору, уточнюється і встановлюється функціональним адміністратором.

Серед основних функцій підсистеми моніторингу ІТКС виділимо такі:

- *стеження* – основна функція, що включає періодичний збір показників з вузлів обладнання, сервісів тощо;
- *зберігання інформації* (додаток до стеження). Здійснюється збір інформації за основними показниками кожного об'єкта моніторингу, для зберігання зазвичай використовуються БД;
- *побудова звітів* – здійснюється як на основі поточних даних стеження, так і за довгостроковою інформацією. Наприклад, довгостроковий моніторинг навантаження на сервер може попередити, що споживані ресурси постійно збільшуються, отже необхідно збільшити доступні ресурси або перенести частину завдань на інший сервер, вибір якого також можна здійснити на основі довгострокового звіту;
- *візуалізація* – звіти у візуальному поданні у вигляді графіків, діаграм та підказок сприяють сприйняттю вимірювальної інформації адміністраторами, при цьому можливий вибір для візуалізації кількох важливих метрик, тоді як у звітах будуть представлені всі показники;
- *пошук «вузьких місць»* – на основі аналізу даних моніторингу можна дізнатися, де в інфраструктурі мережі найбільше знижуються загальні показники продуктивності;
- *автоматизація сценаріїв* – функція звільняє адміністратора від рутинних завдань.

З проведеного аналізу функцій існуючих систем мережевого моніторингу визначимо основні функції сервера моніторингу перспективної підсистеми моніторингу ІТКМ, до основних з яких можна віднести функції вибірки, призначення, ping та SNMP:

1) *Функція вибірки*. Мета функції вибірки на сервері моніторингу полягає в отриманні останнього (актуального) опису мережі та подання його до розподіленої бази даних. Програмне застосування компонента вибірки необхідно запускати під час початкового завантаження підсистеми моніторингу. Його функція – записувати необхідні дані мережевої інфраструктури у розподілену базу даних. Згодом його можна запускати періодично (наприклад, щогодини) або на запит, коли мережева інфраструктура зазнає змін (додаються нові пристрої або обладнання виводиться з експлуатації тощо).

2) *Функція призначення*. Метою цієї функції є автоматичне призначення серверу моніторингу мережевих пристроїв для спостереження. Програмне застосування компонента призначення запускається на кожному сервері моніторингу та у його функціонал входить підтримання актуальності зіставлення мережевих пристроїв серверам моніторингу принаймні локального оновлення мережевої інфраструктури. Наприклад, якщо мережевий пристрій не контролюється необхідною мінімальною кількістю серверів, один або кілька з них у результаті починають спостерігати за доступними (забезпечують зв'язність) мережевими пристроями (динамічно беруть їх на моніторинг), поки вимогу забезпечення мінімальним числом серверів моніторингу кожного з них не буде виконано. Це нове призначення негайно оновлюється для спільно використовуваного об'єкта розподілених даних, що поширюється по всій мережі, досягаючи інших серверів моніторингу. Призначення між серверами моніторингу та мережевими пристроями є динамічним, і з часом змінюється, оскільки нові мережеві пристрої додаються до мережі або видаляються з неї в міру того, як балансування робочого навантаження на серверах моніторингу потребує перепризначення мережевих пристроїв з одного сервера на інший. При цьому важливо відзначити, що компоненти призначення можуть виявляти збій сервера моніторингу, видаляючи його із системи та приймаючи від нього обов'язки з моніторингу. Завдання полягає в тому, щоб призначити кожен окремий мережевий пристрій, принаймні як мінімум 2 серверам моніторингу. Для цього сервери знають список вузлів, за якими потрібно стежити, і побічно координують один з одним об'єкт даних, що

змінюється, заданий співвідношенням мережевий пристрій ⇔ сервер моніторингу, щоб виконати фактичний моніторинг всіх вузлів. Наприклад, кожен сервер моніторингу може розпочати випадковий вибір вузлів, за якими ще ведеться спостереження, і призначити їх собі.

3) Функція перевірки зв'язку (ping). Метою функції перевірки зв'язку є виконання перевірки зв'язку з мережевими пристроями, призначеними серверу моніторингу, та записати результати вимірювань у БД. Програмний додаток, що його реалізує, знаходиться на кожному сервері моніторингу і піклується про фактичне зондування мережевих пристроїв. ПЗ періодично перевіряє призначений список мережних пристроїв для оцінки їхньої швидкодії, часу безвідмовної роботи та відстані до мережі (за допомогою часу прийому-передачі пакетів ping). Зібрані дані зберігають у одному примірнику розподіленої БД. Їхня реплікація між усіма екземплярами гарантує, що нові дані автоматично реплікуються та розподіляються по всіх екземплярах БД, забезпечуючи надмірність зберігання.

4) Функція SNMP. Призначення цієї функції полягає у виконанні SNMP запитів до мережевих пристроїв, яким призначено сервер моніторингу, і запис зібраних SNMP значень БД. Програмний додаток, що його реалізує, запускається на кожному сервері моніторингу і піклується про фактичні SNMP запити до мережних пристроїв. Агреговані дані зберігаються в екземплярі розподіленої БД. Реплікація даних між усіма екземплярами гарантує, що нові дані автоматично реплікуються та розподіляються по всіх екземплярах БД, забезпечуючи виконання технології CRDT*.

Завдяки наявності ресурсів для реалізації всіх цих функцій адміністратору ІТКМ немає потреби перевіряти вручну стан кожної складової системи. При цьому проблеми вирішуються і відмови усуваються оперативніше, діагностика здійснюється багатомірно і точно, можливе планування розширення інфраструктури.

3. Вимоги до перспективних систем мережевого моніторингу

Сучасні системи моніторингу, щоб залишатися затребуваними на ринку телекомунікаційних послуг, проходять поряд з мережевими пристроями та технологіями постійний процес удосконалення та модернізації. Це своє чергу впливає зміна вимог до систем моніторингу у бік їх посилення. В даний час виділяють такі вимоги до нових систем моніторингу, що впроваджуються на ІТКМ [2]:

резервування: кожен мережевий пристрій повинен контролюватись довільною мінімальною кількістю серверів, наприклад, що перевищує один. Це означає, що сервери моніторингу повинні перевіряти, які мережеві пристрої мають призначені сервери моніторингу, і, якщо їх кількість нижча за мінімальну (менше двох), самостійно приймати рішення стати сервером моніторингу для будь-якого з цих пристроїв;

*CRDT (Conflict-Free Replicated Data Type) – типи даних, які можна реплікувати на багато вузлів та оновлювати паралельно без координації між вузлами [3].

автоматичний розподіл: система автоматично виконує розподіл між мережевими пристроями та серверами моніторингу. У разі постійної роботи служба повинна працювати автономно без ручного втручання;

автоматична реконфігурація: система повинна мати можливість автоматично виявляти несправні сервери моніторингу (наприклад, через збої мережі або обладнання) та перепризначати мережеві пристрої функціональним серверам моніторингу. Цей процес має виконуватися без ручного втручання;

реплікація даних: зібрані дані мають бути репліковані та розподілені по різних частинах системи. У разі поділу мережі або деградації БД дані, як і раніше, мають бути доступні для вилучення службою моніторингу з інших сегментів мережі;

балансування навантаження: робоче навантаження моніторингу має бути розподілене по мережі та активним серверам моніторингу, а не концентруватися на кількох пристроях.

4. Загальні принципи організації та функціонування підсистем моніторингу ІТКМ

На основі системного аналізу процесів моніторингу ІТКС, проведеного вище, сформулюємо загальні принципи побудови та функціонування систем мережевого моніторингу. Для вирішення завдань підтримки у постійній готовності до застосування та забезпечення ефективної технічної експлуатації мережевих елементів та ІТКМ загалом необхідно застосування сучасної організаційно-технічної ідеології та підходів до побудови систем мережевого моніторингу, заснованої на використанні перспективних інтелектуальних, інформаційних, мережевих та вимірювальних технологій. При цьому функціонал підсистеми моніторингу територіально розподіленої ІТКМ має включати комплекс заходів, що проводяться з метою інформаційного забезпечення СППР (з управління зв'язком – АСУС) та підтримки мережевих елементів у справному (працездатному) стані. Виходячи з цього, основними принципами побудови підсистеми моніторингу ІТКС є:

принцип еволюційного розвитку, що надає можливість підсистемі моніторингу відповідати ІТКМ, що постійно вдосконалюється (еволюціонує), з урахуванням їх топологічної та просторово-часової неоднорідності;

єдності організаційно-технічних, алгоритмічних та програмно-технічних рішень, спрямованих на розробку високоефективних програмних додатків підтримці та відновленню якості функціонування ІТКС та її мережевих елементів на основі даних моніторингу;

інтелектуалізації процесів моніторингу ІТКМ, що базується на застосуванні перспективних ІТ, що розвиваються на стику штучного інтелекту та розподіленої обробки великих даних (вимірювальної інформації мережевих елементів);

гнучкість архітектури підсистеми моніторингу на основі методології відкритих систем, що забезпечує можливість реконфігурації системи контролю в умовах деградації та відновлення мережевої інфраструктури, а також нарощування функцій моніторингу ІТКМ та її мережевих елементів – багаторівневість, ієрархічна побудова.

Але основними архітектурними принципами проектування сучасних підсистем моніторингу розподілених гетерогенних ІТКМ є розподіл та децентралізація для підвищення стійкості та надійності підконтрольної мережі [4]. Зупинимося на них докладно. Механізм децентралізованого розподілу успішно забезпечує встановлення мінімальної кількості серверів моніторингу на один контрольований мережний пристрій, що відповідає заданим системним вимогам. Враховуючи, що на розподіленій ІТКМ обстановка у зв'язку постійно змінюється через динамічну зміну стану каналів зв'язку та надійності мережевих елементів для підвищення стійкості до відмови підсистеми моніторингу пропонується кожному мережевому елементу зіставляти кілька серверів моніторингу, що знаходяться на межах підмереж (сегментів мережі). При цьому принцип розподіленості та децентралізації передбачає розміщення на мережі кількох реплік серверів моніторингу.

Проведений вище аналіз особливостей розвитку сучасних ІТКМ та етапів їх удосконалення показав експоненційне зростання структур [5], що породжується збільшенням географічної розподіленості, а також зростанням рівня різнорідності сегментів мережі, що у свою чергу накладає особливості на підходи та методи побудови структур їх підсистем моніторингу. Причому, великий ступінь розмірності контрольованого простору, з урахуванням багаторівневої структури і гетерогенності ІТКМ, сукупності метрик, що спостерігаються на мережевих елементах, що представляють собою великі дані (Big Data), передбачає розробку моделі системи, здатної врахувати вищевикладені вимоги, що відносяться до перспективних систем моніторингу. Основним із них є децентралізація інфраструктури моніторингу функціонального стану розподілених мережевих ресурсів.

5. Структура перспективної підсистеми моніторингу ІТКМ загального користування

Структуру підсистеми моніторингу такої розподіленої гетерогенної ІТКС можна змоделювати як неповним двонаправленим графом $G = (N, E)$ де N – це набір вузлів, що

становлять мережу, а E – набір зв'язків (бездротових або оптоволоконних), що з'єднують кореспондуючі пари вузлів. Ізольовані вузли мережі (тобто без зв'язків з іншими вузлами) відкидаються. При цьому для побудови підсистеми моніторингу розглянемо два типи вузлів: сервери моніторингу $M(M \in N)$ та мережні пристрої, що підлягають моніторингу $D(D \subset N)$. Зв'язки характеризуються заданою пропускною здатністю $V_{ij} \forall (i,j) \in E$ та затримкою $T_{ij} \forall (i,j) \in E$, у той час як кожен і-й вузол має конкретну якість моніторингу (при розгляді моніторингу як послуги) QoS_i, ∀ і ∈ N, отриманий з реальних вимірювань на мережі. Для розгортання підсистеми моніторингу на мережі можна розмістити не більше $M_{max} = k$ реплік сервера моніторингу. Сервер моніторингу може бути розгорнутий у мережному вузлі, тільки якщо цей вузол має QoSi вище за мінімальний поріг, $QoS_i > QoS_{min}$ [6]. Посилання вузла буде використовуватися, якщо його смуга пропускання вище або дорівнює заданому порогу. При зіставленні мережевих пристроїв і серверів моніторингу врахуємо таке обмеження (воно м. б. встановлено й іншим, залежно від важливості функцій, що виконуються, включення в критично важливу інфраструктуру):

$$\sum_{i=1}^{M_{max}} m_i \geq 2 \quad (1)$$

Оскільки основними принципами проєктування підсистеми моніторингу є *розподіл і децентралізація* для підвищення стійкості та надійності [7], то необхідно використовувати розподілені структури БД для підтримки децентралізованої координації серверів моніторингу. З цією метою сервери мають зберігати розподілене зіставлення серверів моніторингу та мережевих пристроїв, що використовується для динамічного взяття (і зняття) пристроїв на моніторинг. Такий динамічний розподіл має модифікуватися одночасно будь-яким із серверів, що беруть участь, для підтримки виконання умови (1). Щоб забезпечити це, використовуємо технологію *CRDT* і делегуємо синхронізацію даних, а також їхню узгодженість, на базовий рівень зберігання (БД), що забезпечує певні властивості (наприклад, гарантовану кінцеву узгодженість під час реплікації даних) [8].

Розподілене зіставлення на ІТКС серверів моніторингу та мережевих пристроїв наведено на рис. 2 і в табл. 1. У цій мережевій інфраструктурі група маршрутизаторів D1 - D12 представляють фактичні мережеві пристрої, з'єднані між собою оптоволоконними або радіоканалами, що утворюють комірчасту мережу. Навколо них показано сервери моніторингу M1 - M6, що взаємодіють один з одним для обміну інформацією (реплікації моніторингової інформації) і координації своїх дій.

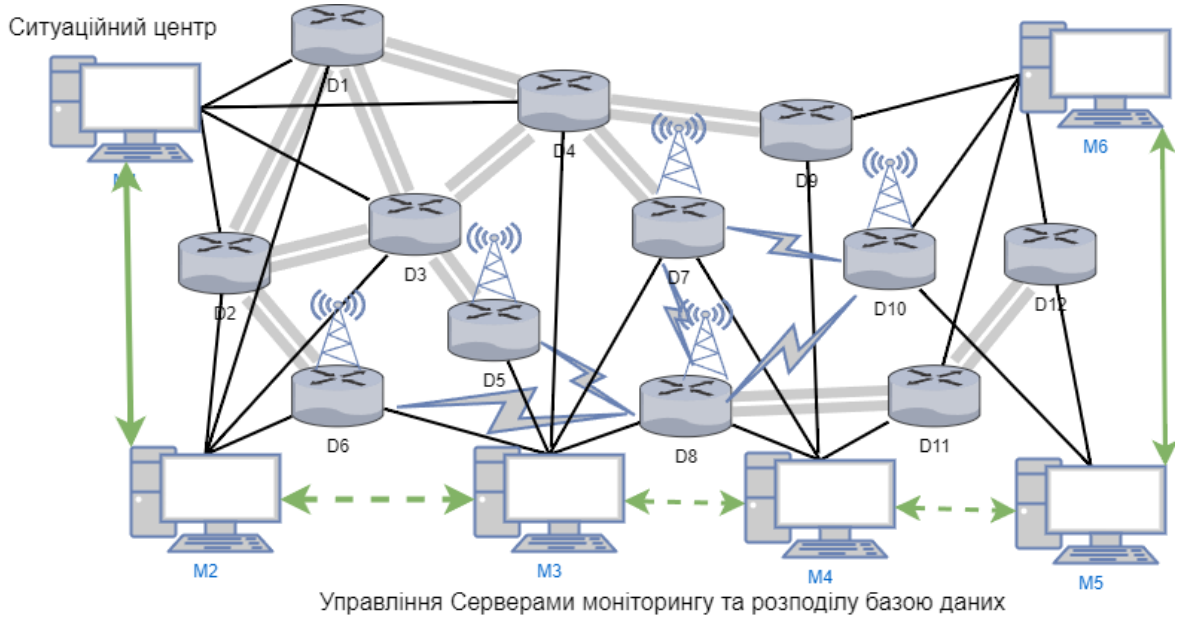

Рис.2 Система мережевого моніторингу

Таблиця 1

Розподіл співставлення серверів моніторингу та мережевих пристроїв

Мережевий пристрій	Сервер моніторингу	Мережевий пристрій	Сервер моніторингу	Мережевий пристрій	Сервер моніторингу
D1	M1, M2	D5	M1, M3	D9	M4, M6
D2	M1, M2	D6	M2, M3	D10	M5, M6
D3	M1, M2	D7	M3, M4	D11	M4, M6
D4	M1, M3	D8	M3, M4	D12	M5, M6

6. Висновоки.

У роботі визначено функції підсистеми мережевого моніторингу ІТКМ та сервера моніторингу як ключового її елемента. Запропоновано варіант структури сервера моніторингу ІТКМ та залежних підсистем. Розглянуто призначені об'єкти моніторингу, а також перелік метричних даних, що збираються з них, з точки зору функціональної продуктивності ІТКМ. Сформульовано загальні вимоги до перспективних систем мережного моніторингу, а також загальні засади організації та функціонування підсистем моніторингу ІТКМ. При цьому для підвищення стійкості та надійності підконтрольної мережі ключовим архітектурним принципом проектування сучасних підсистем моніторингу розподілених гетерогенних ІТКМ визначено принцип розподілу та децентралізації.

Алгоритм децентралізованого розподілу успішно забезпечує встановлення мінімальної кількості серверів моніторингу (M > 2) на один мережний пристрій, що відповідає встановленим системним вимогам. Така стійка та децентралізована архітектура може закласти основу для інших додатків у галузі хмарних обчислень, яким важливо координувати розподілені та узгоджені загальні дані. У цьому БД використовується *CRDT*-технологія, яка реалізує структури розподілених даних.

Список використаної літератури

1. Subramanian M. Network Management: Principles and Practices. 2-ге вид. Prentice Hall, 2012. 695 с.

2. Centelles R., Selimi M., Freitag F., Navarro L. REDEMON: Resilient Decentralized Monitoring System for Edge Infrastructures. Conference proceedings. 2020 20th IEEE/ACM International Symposium on Cluster, Cloud and Internet Computing (CCGRID), Melbourne, Australia 2020, p. 91-100.

3. Kleppmann M. Designing Data-Intensive Applications: The Big Ideas Behind Reliable, Scalable, and Maintainable Systems. O'Reilly Media, 2017. 624 p.

4. Goransson P. Software Defined Networks: A Comprehensive Approach. Morgan Kaufmann, 2014. 352 p.

5. Kurose J. F. Computer Networking: A Top-Down Approach (7th Edition). Pearson, 2016. 864 p.

6. Burns B. Cloud computing: Principles and paradigms. Hoboken, N.J : Wiley, 2011. 637 p.

7. Tanenbaum A. S. Distributed Systems: Principles and Paradigms. CreateSpace Independent Publishing Platform, 2016. 702 p.

8. Coulouris G. Distributed systems: Concepts and design. 5th ed. Boston : Addison-Wesley, 2012. 1047 p.