Хмельницький національний університет
Факультет інформаційних технологій
Кафедра комп'ютерної інженерії та інформаційних систем

КВАЛІФІКАЦІЙНА РОБОТА

Кіберфізична система віддаленого моніторингу комутаційних вузлів мережі на основі MRTG

Назва теми

Рівень вищої освіти *другий (магістерський)*

Галузь знань *12 «Інформаційні технології»*

Шифр, назва

Спеціальність *123 «Комп'ютерна інженерія»*

Шифр, назва

Освітня програма *«Комп'ютерна інженерія та програмування»*

Назва

Шифр КвРКІ 240117.16.01.45 ПЗ

Виконав здобувач IV курсу, група КІ2м-24-1 Підпис Денис КОВАЛЕНКО Ініціали, прізвище

Керівник канд.-техн. наук, доцент Науковий ступінь, учене звання Підпис Олексій ІВАНОВ Ініціали, прізвище

Нормоконтролер д. техн. наук, професор Науковий ступінь, учене звання Підпис Сергій ЛИСЕНКО Ініціали, прізвище

До захисту допускаю:
завідувач кафедри КІІС Підпис Ольга ПАВЛОВА Ініціали, прізвище
«21» _травня_ 2026 р.

дата

Хмельницький 2026

ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет Інформаційних технологій

Кафедра Комп'ютерної інженерії та інформаційних систем

Рівень вищої освіти другий (магістерський)

Галузь знань 12 Інформаційні технології

Спеціальність 123 Комп'ютерна інженерія

Освітня програма «Комп'ютерна інженерія та програмування»

ЗАТВЕРДЖУЮ
Завідувачка кафедри КІІС
Ольга ПАВЛОВА

" 12 " 01 2026 р.

ЗАВДАННЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ

Коваленку Денису Олександровичу

Прізвище, ім'я, по батькові студента

1. Тема проекту (роботи) Кіберфізична система віддаленого моніторингу комутаційних вузлів мережі на основі MRTG

Керівник проекту (роботи) Іванов Олексій Валентинович., к.т.н.,доцент

Прізвище, ім'я, по батькові, науковий ступінь, вчене звання

Затверджена наказом ректора університету від 12.01.2026 р. № 6

2. Термін подання здобувачем роботи на кафедру 01.05.2026 р.

3. Вихідні дані до роботи Завдання на кваліфікаційну роботу

4. Зміст пояснювальної записки (перелік питань, які потрібно розробити)

Кіберфізична система віддаленого моніторингу комутаційних вузлів мережі та аналіз предметної області, виявлення наявних проблем і постановка задачі

Моделювання кіберфізичної системи віддаленого моніторингу комутаційних вузлів мережі на основі MRTG

Проєктування системи збору, зберігання та візуалізації мережевих параметрів у кіберфізичній системі віддаленого моніторингу

Програмно-апаратна реалізація кіберфізичної системи віддаленого моніторингу комутаційних вузлів мережі на основі MRTG

5. Перелік графічного матеріалу (із зазначенням обов'язкових креслень)

Архітектура ПЗ проєкту

Архітектура ПЗ для кіберфізичної системи

Апаратне забезпечення проєкту

6. Консультанти розділів кваліфікаційної роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв

7. Дата видачі завдання «_12_»_____01_____2026 р.

КАЛЕНДАРНИЙ ПЛАН

№з/п	Назва етапів (розділів) дипломного проєкту (роботи)	Термін виконання етапів проєкту (роботи)	Примітка
1	Вибір напряму дослідження та узгодження тематики кваліфікаційної роботи з керівником	12.01.2026	виконано
2	Ознайомлення з предметною областю; формулювання мети та задач дослідження; визначення об'єкта та предмета дослідження	15.01.2026	виконано
3	Робота над розділом 1 – дослідження предметної області та постановка задачі	01.02.2026	виконано
4	Робота над розділом 2 – моделювання кіберфізичної системи віддаленого моніторингу комутаційних вузлів мережі на основі MRTG	01.03.2026	виконано
5	Робота над розділом 3 – проєктування системи збору, зберігання та візуалізації параметрів комутаційних вузлів мережі	29.03.2026	виконано
6	Оформлення пояснювальної записки згідно вимог	25.04.2026	виконано
7	Попередній захист ВКР	26.04.2025	виконано
8	Захист ВКР на засіданні ЕК	травень 2026 року	

Здобувач _____ Денис КОВАЛЕНКО
Підпис Ім'я, ПРІЗВИЩЕ

Керівник кваліфікаційної роботи _____ Олексій ІВАНОВ
Підпис Ім'я, ПРІЗВИЩЕ

РЕФЕРАТ

Тема кваліфікаційної роботи магістра: Кіберфізична система віддаленого моніторингу комутаційних вузлів мережі на основі MRTG

Автор роботи: Денис Коваленко

Керівник роботи: Олексій Іванов

Пояснювальна записка: 90 с., 7 рис., 3 табл., 1 дод., 81 джерел.

КІБЕРФІЗИЧНА СИСТЕМА, ВІДДАЛЕНИЙ МОНІТОРИНГ, КОМУТАЦІЙНИЙ ВУЗОЛ, КОМП'ЮТЕРНА МЕРЕЖА, MRTG, МЕРЕЖЕВИЙ ТРАФІК, ВІЗУАЛІЗАЦІЯ ДАНИХ.

Об'єктом дослідження є процес віддаленого моніторингу комутаційних вузлів комп'ютерної мережі.

Предметом дослідження є методи та засоби збору, зберігання, візуалізації й аналізу параметрів функціонування комутаційних вузлів мережі на основі MRTG.

Метою кваліфікаційної роботи магістра є розроблення кіберфізичної системи віддаленого моніторингу комутаційних вузлів мережі на основі MRTG, яка забезпечує автоматизований збір мережевих параметрів, їх зберігання, графічне представлення та підтримку аналізу стану мережевої інфраструктури.

Для розв'язання поставлених задач використовувалися методи системного аналізу комп'ютерних мереж, методи мережевого моніторингу, методи збору статистичних даних за допомогою SNMP, методи побудови часових рядів, методи графічної візуалізації інформації, методи аналізу параметрів навантаження мережевих інтерфейсів, а також методи проєктування програмно-апаратних систем.

Наукова новизна отриманих результатів:

− набув подальшого розвитку метод організації віддаленого моніторингу комутаційних вузлів мережі на основі інтеграції SNMP-збору статистичних даних із засобами часового аналізу навантаження;

− набула подальшого розвитку інформаційна технологія побудови кіберфізичних систем моніторингу мережевої інфраструктури із застосуванням MRTG для візуалізації параметрів роботи комутаційного обладнання.

На основі проведених досліджень розроблена архітектура і компоненти програмного забезпечення кіберфізичної системи віддаленого моніторингу комутаційних вузлів мережі, що включає модулі SNMP-опитування, обробки статистичних даних, збереження історичних показників, генерації графіків MRTG та веб-інтерфейс перегляду результатів..

Практична значимість отриманих результатів полягає у створенні системи, яка дозволяє адміністратору мережі дистанційно контролювати стан комутаційних вузлів, аналізувати завантаження портів і каналів зв'язку, своєчасно виявляти перевантаження, відмови та тенденції зміни мережевого трафіку, а також приймати обґрунтовані рішення щодо модернізації мережевої інфраструктури.

У першому розділі проведено аналіз предметної області віддаленого моніторингу комутаційних вузлів мережі, досліджено існуючі програмні засоби моніторингу, розглянуто особливості використання SNMP та MRTG, сформульовано постановку задачі дослідження.

У другому розділі побудовано модель кіберфізичної системи віддаленого моніторингу комутаційних вузлів мережі, визначено структуру системи, взаємодію її компонентів та інформаційні потоки між фізичним і програмним рівнями.

У третьому розділі виконано проєктування системи збору, зберігання та візуалізації мережевих параметрів, розроблено архітектуру програмного забезпечення, визначено склад функціональних модулів та принципи їх взаємодії.

У четвертому розділі здійснено програмно-апаратну реалізацію кіберфізичної системи віддаленого моніторингу на основі MRTG, налаштовано SNMP-взаємодію з комутаційними вузлами, проведено тестування працездатності системи та аналіз отриманих результатів.

ЗМІСТ

СКОРОЧЕННЯ ТА УМОВНІ ПОЗНАКИ

АПЗ - антивірусне програмне забезпечення

БД - база даних

БПР - блок прийняття рішень

ГА - генетичний алгоритм

ОС - операційна система

ПЗ - програмне забезпечення

СВВ - система виявлення вторгнень

ЕС - експертна система

DDoS - Distributed Denial of Service (розподілена відмова в обслуговуванні)

IDS - система виявлення вторгнень

ВСТУП

Сучасні телекомунікаційні та корпоративні мережі є важливою основою функціонування інформаційних сервісів, внутрішніх систем підприємств, засобів зв'язку, серверної інфраструктури та прикладних програмних комплексів. Їх стабільність безпосередньо залежить від працездатності комутаційних вузлів, каналів передавання даних, маршрутизаторів, серверів і допоміжного мережевого обладнання. У разі відмови або перевантаження окремого вузла може порушуватися робота цілих сегментів мережі, знижуватися якість доступу до сервісів, виникати затримки, втрати пакетів або повна недоступність окремих ресурсів.

Зі збільшенням кількості мережевих пристроїв ручний контроль їхнього стану стає недостатньо ефективним. Адміністратор не завжди має можливість оперативно перевіряти кожен комутатор, порт, uplink-канал або системний параметр обладнання. Особливо це стосується розподілених мереж, у яких комутаційні вузли можуть бути розташовані у різних приміщеннях, будівлях або територіально віддалених об'єктах. У таких умовах важливого значення набувають системи віддаленого моніторингу, які дають змогу автоматизовано збирати інформацію про стан обладнання, аналізувати мережеве навантаження та своєчасно виявляти ознаки перевантаження або деградації роботи.

Актуальність роботи полягає у необхідності розроблення кіберфізичної системи віддаленого моніторингу комутаційних вузлів мережі, яка поєднує фізичні мережеві пристрої з програмними засобами збору, зберігання, візуалізації та аналізу параметрів функціонування. Такий підхід дозволяє сформувати єдиний інформаційний контур контролю, у якому реальний стан обладнання відображається через статистичні показники, часові ряди, графіки трафіку та звіти для адміністратора.

Особливе значення у межах роботи має використання MRTG як інструменту графічної візуалізації мережевого трафіку. MRTG дає можливість отримувати дані з мережевих пристроїв за допомогою SNMP, формувати графіки зміни параметрів

у часі та накопичувати історичну інформацію про роботу комутаційних вузлів. Це дозволяє не лише контролювати поточне навантаження, а й аналізувати динаміку роботи мережі за попередні періоди, виявляти регулярні пікові навантаження, оцінювати завантаження uplink-каналів і планувати подальше розширення мережевої інфраструктури.

Кіберфізичний характер системи проявляється у зв’язку між фізичним станом мережевого обладнання та програмним контуром його контролю. Комутатори, маршрутизатори й інші пристрої виступають фізичними об’єктами, з яких надходять статистичні дані. Протокол SNMP забезпечує комунікаційний рівень доступу до параметрів обладнання, а програмний рівень на основі MRTG виконує регулярне опитування, обробку отриманих значень, збереження статистики та побудову графіків. У результаті формується цифрове представлення стану комутаційного вузла, яке може використовуватися для прийняття рішень щодо обслуговування, модернізації або усунення проблем.

Метою кваліфікаційної роботи є розроблення кіберфізичної системи віддаленого моніторингу комутаційних вузлів мережі на основі MRTG, яка забезпечує автоматизований збір мережевих параметрів, їх зберігання, графічне представлення та підтримку аналізу стану мережевої інфраструктури.

Поставлена мета досягається розв’язанням таких основних завдань:

- проаналізувати предметну область віддаленого моніторингу комутаційних вузлів мережі;
- розглянути відомі підходи та програмні засоби моніторингу мережевої інфраструктури;
- визначити переваги та обмеження використання MRTG у системах контролю мережевого трафіку;
- сформувати модель кіберфізичної системи віддаленого моніторингу комутаційних вузлів;
- розробити архітектуру системи збору, зберігання та візуалізації мережевих параметрів;

− налаштувати взаємодію комутаційних вузлів із сервером моніторингу за допомогою SNMP;

− реалізувати конфігурацію MRTG для отримання статистики з мережевих пристроїв;

− перевірити працездатність системи та проаналізувати отримані результати моніторингу.

Об’єктом роботи є процес віддаленого моніторингу комутаційних вузлів комп’ютерної мережі.

Предметом роботи є методи та засоби збору, зберігання, візуалізації й аналізу параметрів функціонування комутаційних вузлів мережі на основі SNMP та MRTG.

Для розв’язання поставлених завдань використано методи аналізу комп’ютерних мереж, методи мережевого моніторингу, методи збору статистичних даних за допомогою SNMP, методи формування часових рядів, методи графічної візуалізації трафіку, а також методи аналізу параметрів завантаження мережевих інтерфейсів.

Наукова новизна отриманих результатів полягає у подальшому розвитку підходу до побудови кіберфізичної системи віддаленого моніторингу комутаційних вузлів, у якій фізичні параметри роботи мережевого обладнання інтегруються з програмним контуром збору, збереження та візуального аналізу статистичних даних на основі MRTG.

Практична значимість отриманих результатів полягає у розробленій системі віддаленого моніторингу, яка дозволяє адміністратору контролювати стан комутаційних вузлів, аналізувати завантаження мережевих інтерфейсів, виявляти перевантаження, переглядати історичні графіки трафіку та приймати обґрунтовані рішення щодо обслуговування або модернізації мережевої інфраструктури.

За темою кваліфікаційної роботи опубліковано одну публікацію [81] у Збірнику наукових праць за матеріалами XVI Всеукраїнської науково-практичної конференції «Актуальні проблеми комп’ютерних наук АПКН-2024». (Хмельницький – 2023. – С. 303-305).

1 АНАЛІЗ ВІДОМИХ МЕТОДІВ КІБЕРФІЗИЧНА СИСТЕМА ВІДДАЛЕНОГО МОНІТОРИНГУ КОМУТАЦІЙНИХ ВУЗЛІВ

1.1 Аналіз предметної області і виявлення наявних проблем і завдань

Сучасні комп’ютерні мережі є основою функціонування підприємств, навчальних закладів, державних установ, сервісних платформ і внутрішніх інформаційних систем. Через мережеву інфраструктуру передаються службові дані, запити користувачів, мультимедійний трафік, повідомлення між серверами, дані відеоспостереження та інші інформаційні потоки. У таких умовах стабільність мережі безпосередньо впливає на доступність сервісів, якість обслуговування користувачів і безперервність основних процесів організації [60, 69].

Важливе місце в такій інфраструктурі займають комутаційні вузли. Вони забезпечують передавання даних між кінцевими пристроями, серверами, маршрутизаторами, точками бездротового доступу та іншими елементами мережі. Порушення роботи одного комутатора може вплинути не лише на окремий пристрій, а й на цілий сегмент мережі, особливо якщо через нього проходить трафік декількох груп користувачів або підключення до серверних ресурсів. Через це контроль стану комутаційних вузлів є важливою частиною адміністрування мережевої інфраструктури [31, 35].

У невеликих мережах перевірка обладнання може виконуватися вручну: через перегляд стану портів, журналів подій, інтерфейсу керування або діагностичних команд. Проте зі збільшенням кількості пристроїв такий підхід стає малоефективним. Ручний контроль потребує значного часу, залежить від уважності адміністратора і не дає повної картини зміни параметрів у часі. Частина проблем може залишатися непоміченою до моменту, коли вони вже вплинули на роботу користувачів або прикладних сервісів [67, 73].

Особливо актуальною ця проблема є для розподілених мереж, де комутаційні вузли можуть бути розташовані в різних приміщеннях, корпусах, технічних шафах або віддалених філіях. У таких умовах фізичний доступ до обладнання не завжди можливий у потрібний момент. Тому виникає потреба у віддаленому моніторингу,

який дозволяє автоматизовано отримувати інформацію про стан пристроїв, контролювати доступність вузлів, оцінювати завантаження інтерфейсів і своєчасно реагувати на погіршення параметрів мережі [69, 80].

Віддалений моніторинг комутаційних вузлів передбачає регулярний збір параметрів, що характеризують роботу обладнання та його інтерфейсів. До таких параметрів належать обсяг вхідного і вихідного трафіку, завантаження uplink-каналів, кількість помилок, відкинуті пакети, стан портів, доступність вузла, швидкість передавання, а також системні показники пристрою, зокрема завантаження процесора, використання пам’яті або температура, якщо такі метрики підтримуються обладнанням [20, 21, 34]. Накопичення цих даних дозволяє оцінювати не тільки поточний стан мережі, а й її поведінку за попередні періоди.

Одним із найпоширеніших механізмів отримання параметрів із мережевих пристроїв є протокол SNMP. Його використання дозволяє збирати інформацію з обладнання різних виробників за умови підтримки відповідних MIB-об’єктів. Через SNMP можуть передаватися дані про стан інтерфейсів, лічильники трафіку, кількість помилок, доступність пристроїв та окремі системні параметри. Підтримка SNMP у мережевому обладнанні різних виробників робить цей підхід зручним для побудови систем моніторингу різнорідної інфраструктури [20, 21, 31, 34].

У межах цієї роботи основна увага приділяється використанню MRTG як засобу графічного контролю параметрів комутаційних вузлів. MRTG виконує періодичне опитування мережевих пристроїв, отримує значення лічильників через SNMP, обробляє ці дані та формує графіки зміни параметрів у часі [1, 2, 3]. Такий підхід є зручним для практичного адміністрування, оскільки графіки дозволяють швидко побачити завантаження інтерфейсів, визначити пікові періоди, помітити нетипові відхилення та оцінити потребу в модернізації окремих каналів.

Перевагою графічного моніторингу є наочність. Окремі числові значення лічильників не завжди дають змогу швидко оцінити реальний стан мережі, тоді як графік показує динаміку зміни трафіку, регулярні піки, поступове зростання навантаження або різкі відхилення. Саме тому формування часових рядів і графічне

представлення даних є важливою складовою системи віддаленого моніторингу [9, 14, 76].

Кіберфізичний характер такої системи проявляється у поєднанні фізичного мережевого обладнання з програмним контуром збору та обробки даних. Комутатор як фізичний пристрій має обмеження за пропускною здатністю, кількістю портів, температурним режимом і ресурсами обробки трафіку. Програмна частина системи отримує від нього числові показники, зберігає їх, будує графіки та створює інформаційну основу для прийняття рішень (рисунок 1.1). Унаслідок цього реальний стан комутаційного вузла відображається у вигляді цифрового профілю, який можна аналізувати дистанційно [67, 69, 70].

Рисунок 1.1 – Узагальнена схема кіберфізичної системи віддаленого моніторингу комутаційних вузлів

Основними проблемами предметної області є різнорідність мережевого обладнання, складність вибору контрольованих параметрів, необхідність правильного налаштування частоти опитування, зберігання історичних даних і забезпечення безпечного віддаленого доступу. Якщо опитування виконується занадто рідко, короткочасні пікові навантаження можуть залишатися непоміченими. Якщо інтервал занадто малий, зростає навантаження на сервер моніторингу, мережу керування та самі пристрої. Через це частота збору даних має відповідати критичності вузлів і потрібній точності контролю [2, 66, 76].

Окреме значення має безпека системи моніторингу. Віддалений доступ до мережевих пристроїв і статистичних даних може створювати додаткові ризики у разі неправильного налаштування облікових даних, відкритих інтерфейсів керування або відсутності обмежень доступу. Тому система моніторингу має поєднувати автоматизований збір інформації з принципом найменших привілеїв, сегментацією мережі керування та контролем доступу до веб-сторінок зі статистикою [23, 26, 28, 29].

У підсумку, предметна область віддаленого моніторингу комутаційних вузлів охоплює фізичні мережеві пристрої, протоколи збору даних, програмні засоби обробки статистики, механізми зберігання часових рядів і графічну візуалізацію. Основними завданнями в межах цієї роботи є забезпечення регулярного збору параметрів, підтримка роботи з різнорідним обладнанням, формування зрозумілих графіків, зберігання історичних даних, своєчасне виявлення перевантажень і безпечна організація віддаленого доступу.

1.2 Порівняльний аналіз переваг та недоліків існуючих рішень

Для віддаленого моніторингу комутаційних вузлів мережі можуть використовуватися різні програмні засоби, які відрізняються способом збору даних, рівнем автоматизації, складністю налаштування, вимогами до ресурсів і можливостями візуалізації. У межах цієї роботи основна увага приділяється рішенням, що підтримують отримання параметрів через SNMP, оскільки саме цей підхід дозволяє працювати з мережевим обладнанням різних виробників і контролювати показники інтерфейсів, трафіку, доступності та системного стану пристроїв [20, 21, 31, 34].

Одним із найпростіших і водночас практичних рішень є MRTG. Його основне призначення полягає у періодичному опитуванні мережевих пристроїв, отриманні значень лічильників через SNMP і побудові графіків зміни параметрів у часі [1, 2, 3]. Перевагою MRTG є зрозуміла логіка роботи, невисокі вимоги до обчислювальних ресурсів і зручність використання для контролю трафіку на

інтерфейсах. Це робить його доцільним для невеликих і середніх мереж, навчальних стендів, лабораторних робіт і локальних систем моніторингу, де головним завданням є не складна автоматизація, а наочне представлення мережевого навантаження.

Разом із цим MRTG має обмеження. Він менш гнучкий у порівнянні з сучасними комплексними системами моніторингу, не має розвиненої системи виявлення подій, не забезпечує повноцінного централізованого керування великою кількістю вузлів і потребує уважного налаштування конфігураційних файлів. Проте для теми цієї роботи така особливість не є критичним недоліком, оскільки система орієнтована саме на віддалений контроль комутаційних вузлів, побудову графіків, накопичення часових рядів і підтримку аналізу стану мережі [4, 5, 9].

Близьким за ідеєю до MRTG є Cacti. Це рішення також активно використовує SNMP, RRDTool і графічне представлення часових рядів [46, 47, 49]. Його перевагою є зручніший веб-інтерфейс, наявність шаблонів, можливість організованого керування пристроями та графіками. Cacti краще підходить для випадків, коли потрібно обслуговувати більшу кількість об’єктів моніторингу та мати більш зручне керування через веб-середовище. Водночас Cacti є складнішим у розгортанні й адмініструванні, ніж MRTG, тому для простої кіберфізичної системи контролю комутаційних вузлів його функціональність може бути надмірною.

Zabbix належить до більш потужних комплексних систем моніторингу. Він підтримує SNMP-опитування, SNMP traps, шаблони для мережевих пристроїв, інтеграції з обладнанням Cisco, MikroTik та іншими платформами [36, 37, 38, 40, 41]. Перевагою Zabbix є широка функціональність, можливість формування сповіщень, побудова панелей, контроль серверів, мережевих пристроїв, сервісів і прикладних систем. Такий інструмент добре підходить для великих інфраструктур, де потрібен централізований моніторинг різних типів ресурсів. Недоліком є більша складність налаштування, потреба в серверній інфраструктурі та необхідність попередньої підготовки шаблонів, тригерів і правил обробки подій.

LibreNMS також є сучасним рішенням для автоматизованого моніторингу мережі. Воно підтримує SNMP, автоматичне виявлення пристроїв, групування обладнання та механізми сповіщення [50, 51, 52, 53]. Перевагою LibreNMS є орієнтація саме на мережеву інфраструктуру, зручність роботи з великою кількістю пристроїв і можливість автоматизованого збору параметрів. Для мереж із багатьма вузлами це рішення є значно зручнішим, ніж ручне налаштування кожного графіка. Проте для невеликої системи, де головним є демонстрація зв'язку між комутаційним вузлом, SNMP-збором і графічним відображенням параметрів, LibreNMS може бути складнішим, ніж потрібно.

Nagios Core використовується для контролю доступності вузлів, служб і сервісів, а також може застосовуватися для SNMP-моніторингу [54, 55, 56]. Його сильною стороною є перевірка станів і формування сповіщень. Це рішення добре підходить для задач, де потрібно швидко визначити, чи працює вузол, сервіс або певний мережевий компонент. Водночас Nagios більше орієнтований на подієвий контроль і перевірки станів, ніж на просту побудову історичних графіків трафіку. Через це для задачі графічного аналізу параметрів комутаційних вузлів він поступається рішенням, які безпосередньо працюють із часовими рядами.

PRTG є комерційною системою моніторингу, яка має зручний інтерфейс, підтримує SNMP-сенсори, користувацькі сенсори та готові сценарії контролю трафіку [57, 58, 59]. Його перевагою є простота використання для адміністратора, швидке додавання пристроїв, наявність готових інструментів візуалізації та сповіщень. Недоліком є комерційна модель використання, що може обмежувати застосування в навчальних, малих або експериментальних середовищах. Для цієї роботи важливо, щоб система могла бути побудована на доступних інструментах, тому MRTG має перевагу з погляду простоти та відкритості.

Окрему групу становлять сучасні рішення на основі Prometheus, Grafana та Telegraf. Вони широко використовуються для збору, збереження та візуалізації метрик у сучасних інфраструктурах [61, 62, 63, 71, 75]. Їхньою перевагою є гнучкість, розвинена візуалізація, підтримка панелей стану та можливість роботи з великою кількістю джерел даних. Проте такі рішення частіше орієнтовані на

складні середовища, серверні платформи, хмарні сервіси та DevOps-практики. Для простої системи моніторингу комутаційних вузлів на базі SNMP їх використання може вимагати додаткових компонентів і складнішої схеми розгортання.

Порівняльну характеристику основних рішень для віддаленого моніторингу мережевої інфраструктури подано в таблиці 1.1..

Таблиця 1.1 – Порівняння систем моніторингу мережі

Тип системи	Переваги	Недоліки
Базові SNMP-системи	Простота впровадження, низька вартість	Обмежена аналітика, ручне налаштування
Комерційні платформи	Висока функціональність, централізація	Висока вартість, вимоги до ресурсів
Хмарні системи	Масштабованість, віддалений доступ	Залежність від інтернету, ризики безпеки
Системи графічного аналізу трафіку	Наочність, простота інтерпретації даних	Обмежена автоматизація управління

З аналізу наведених рішень видно, що кожна система має власну сферу доцільного використання. Zabbix, LibreNMS, PRTG і Prometheus із Grafana краще підходять для великих або складних інфраструктур, де потрібно об’єднати багато типів метрик, створювати сповіщення, панелі стану та інтеграції з іншими сервісами. Cacti є близьким до MRTG за принципом роботи з графіками, але має розвиненіший веб-інтерфейс і більші можливості керування. Nagios є корисним для контролю доступності та подій, але менш орієнтований на просте графічне представлення історії трафіку.

Для цієї роботи доцільним є використання MRTG, оскільки воно відповідає поставленій задачі: забезпечити віддалений збір параметрів комутаційних вузлів через SNMP, сформувати графіки зміни навантаження, накопичувати історичні дані та надати адміністратору зрозумілий інструмент аналізу. MRTG не потребує

складної інфраструктури, дозволяє наочно продемонструвати кіберфізичний зв’язок між мережевим обладнанням і програмним контуром моніторингу та добре підходить для реалізації системи, орієнтованої на контроль комутаційних вузлів [1, 2, 3, 9, 76].

У підсумку, порівняння існуючих рішень показало, що для задачі віддаленого моніторингу комутаційних вузлів важливими є підтримка SNMP, можливість побудови часових графіків, простота налаштування, доступність інструменту та зрозумілість отриманих результатів. Саме за цими ознаками MRTG є доцільною основою для подальшого розроблення кіберфізичної системи моніторингу, а інші рішення можуть розглядатися як функціональні аналоги або альтернативи для складніших інфраструктур

1.3 Особливості використання SNMP та MRTG у системах мережевого моніторингу

У системах віддаленого моніторингу комутаційних вузлів важливим є не тільки сам факт отримання даних з обладнання, а й спосіб, за допомогою якого ці дані збираються, обробляються та подаються адміністратору. Для мережевої інфраструктури таким базовим механізмом часто виступає SNMP, оскільки він дозволяє отримувати параметри з комутаторів, маршрутизаторів, серверів і допоміжного обладнання без постійного ручного доступу до кожного пристрою. Завдяки цьому протоколу система моніторингу може працювати з різнорідним обладнанням і формувати єдину картину стану мережі [20, 21, 31].

SNMP використовується за моделлю взаємодії між керуючою системою та мережевим пристроєм. На стороні пристрою працює SNMP-агент, який надає доступ до певних параметрів обладнання. На стороні системи моніторингу працює компонент опитування, який надсилає запити до пристрою та отримує відповіді зі значеннями потрібних показників. У контексті комутаційних вузлів такими показниками можуть бути лічильники вхідного й вихідного трафіку, кількість помилок на інтерфейсах, відкинуті пакети, стан портів, час роботи пристрою,

завантаження процесора або інші параметри, якщо вони підтримуються конкретною моделлю обладнання [20, 34, 35].

Основою доступу до параметрів у SNMP є MIB-об’єкти. Вони визначають структуру даних, які можуть бути отримані з пристрою. Частина таких об’єктів є стандартною і підтримується багатьма виробниками, наприклад дані про мережеві інтерфейси. Інша частина може бути специфічною для конкретного виробника або серії обладнання. Через це під час побудови системи моніторингу важливо враховувати, які саме MIB-об’єкти доступні для конкретних комутаторів і які з них потрібні для вирішення поставлених завдань [21, 31, 34].

Для контролю комутаційних вузлів найбільш важливими є параметри, пов’язані з інтерфейсами. Саме через інтерфейси проходить основний мережевий трафік, тому їхній стан прямо впливає на якість роботи сегментів мережі. Доцільно контролювати обсяг переданих і прийнятих даних, швидкість зміни цих показників, кількість помилок, відкинутих пакетів і доступність порту. Якщо на певному інтерфейсі постійно зростає кількість помилок або відкидань, це може вказувати на перевантаження, пошкодження кабелю, неправильне узгодження швидкості, фізичні проблеми з портом або некоректну конфігурацію [20, 21, 35].

Використання SNMP є зручним ще й тому, що цей протокол підтримується значною кількістю мережевого обладнання. Це дозволяє створювати систему моніторингу, яка не прив’язана лише до одного виробника пристроїв. У реальній мережі можуть одночасно використовуватися комутатори MikroTik, Cisco, Juniper, Aruba або інше обладнання, і за умови правильної конфігурації SNMP більшість базових параметрів можна отримувати в єдиному форматі [31, 34, 37]. Для кіберфізичної системи це має важливе значення, оскільки фізичні вузли можуть бути різними, але програмний контур моніторингу повинен забезпечувати їх спільне відображення.

Разом із перевагами SNMP має певні обмеження. Насамперед вони пов’язані з безпекою, налаштуванням доступу та правильним вибором версії протоколу. Застарілі або спрощені варіанти налаштування можуть передавати службову інформацію недостатньо захищеним способом або використовувати слабкі

параметри доступу. Через це під час організації віддаленого моніторингу важливо обмежувати доступ до SNMP лише з боку сервера моніторингу, використовувати окрему мережу керування, налаштовувати списки доступу та застосовувати безпечніші механізми автентифікації, якщо це підтримується обладнанням [23, 26, 28, 29].

У межах цієї роботи SNMP розглядається як комунікаційна основа між комутаційними вузлами та сервером моніторингу. Його завдання полягає в тому, щоб забезпечити регулярне отримання параметрів з фізичних пристроїв. Проте сам SNMP не виконує повноцінного аналізу, не будує графіки та не створює зручного історичного представлення даних. Для цього потрібен програмний компонент, який зможе періодично опитувати пристрої, обробляти отримані значення, зберігати їх і подавати у зрозумілій формі. У цій ролі використовується MRTG [1, 2, 3].

MRTG є інструментом, призначеним для графічного представлення мережевих параметрів, насамперед трафіку на інтерфейсах. Його робота базується на періодичному опитуванні мережевих пристроїв, отриманні значень лічильників через SNMP і побудові графіків зміни показників у часі [1, 2]. У типовій схемі MRTG звертається до пристрою через заданий інтервал, отримує поточні значення лічильників, обчислює зміну показників між двома вимірюваннями та формує графік, який показує динаміку навантаження.

Важливою особливістю MRTG є перетворення лічильників у більш зручні для аналізу значення. Наприклад, мережевий пристрій може надавати загальну кількість байтів, що пройшли через інтерфейс. Саме по собі це число не дає повного розуміння поточного навантаження. MRTG порівнює значення за різні моменти часу і визначає інтенсивність передавання, тобто фактичну швидкість зміни параметра. У результаті адміністратор отримує не просто накопичений лічильник, а графік, який показує реальне навантаження на порт або канал [2, 3, 9].

Для комутаційних вузлів такий підхід є практично корисним, оскільки дозволяє бачити не лише поточну активність, а й характер її зміни. На графіках можна визначити періоди максимального навантаження, регулярні піки, поступове

збільшення трафіку, простої або різкі відхилення. Це допомагає відрізняти нормальну поведінку мережі від ситуацій, які можуть свідчити про проблему. Наприклад, стабільне зростання навантаження на uplink-каналі може вказувати на потребу в модернізації, а різке короткочасне перевантаження - на нетипову активність або неправильно організований обмін даними [66, 74, 76].

Ще однією важливою складовою є зберігання історичних даних. Для ефективного моніторингу недостатньо бачити тільки поточний стан мережі. Потрібно мати можливість переглядати статистику за попередні години, дні, тижні або місяці. Історичні графіки дозволяють виявляти повторювані проблеми, порівнювати навантаження в різні періоди та оцінювати вплив змін у конфігурації мережі. У системах такого типу для роботи з часовими рядами може використовуватися RRD-підхід, який дає змогу зберігати дані у впорядкованому вигляді та не допускати неконтрольованого збільшення обсягу сховища [9, 10, 11].

Особливість часових рядів полягає в тому, що кожне значення параметра прив’язується до конкретного моменту часу. Завдяки цьому система може показувати не лише окремий стан пристрою, а й розвиток ситуації. Для комутаційних вузлів це має велике значення, оскільки багато проблем не виникають миттєво. Вони можуть проявлятися поступово: повільним зростанням навантаження, збільшенням кількості помилок, повторенням пікових значень у певні години або зміною характеру трафіку після підключення нових пристроїв. Аналіз часових рядів дозволяє виявляти такі ознаки раніше, ніж вони призведуть до помітного збою [9, 66, 76].

У кіберфізичній системі віддаленого моніторингу SNMP і MRTG виконують взаємодоповнювальні функції. SNMP забезпечує доступ до параметрів фізичних пристроїв, а MRTG перетворює отримані значення на графічне представлення, зручне для аналізу. Фізичний рівень системи формують комутатори та інші мережеві пристрої, комунікаційний рівень забезпечує SNMP-збір, а програмний рівень відповідає за обробку, зберігання та відображення даних. Унаслідок цього формується єдиний контур контролю, у якому стан обладнання можна оцінювати дистанційно [1, 2, 20, 21].

Практичне використання MRTG вимагає правильного налаштування конфігураційних файлів. У них задаються адреси пристроїв, параметри доступу, об’єкти моніторингу, назви графіків, інтервали опитування та шляхи збереження результатів. Такий підхід може бути менш зручним, ніж повністю графічне налаштування в сучасних платформах, проте він забезпечує прозорість логіки роботи системи. Для цієї роботи це є перевагою, оскільки дозволяє чітко показати, які саме параметри збираються, з яких вузлів вони надходять і як перетворюються у графіки [2, 4, 5].

Важливим етапом є вибір інтервалу опитування. Занадто великий інтервал може приховувати короткі пікові навантаження, а занадто малий - створювати зайве навантаження на сервер моніторингу та мережу керування. Для критичних інтерфейсів доцільно використовувати коротший інтервал збору даних, а для другорядних параметрів - більший. Такий підхід дозволяє збалансувати точність моніторингу та ресурсні витрати системи [2, 66, 76].

У підсумку, використання SNMP та MRTG у системах мережевого моніторингу дозволяє побудувати зрозумілий і практичний механізм контролю комутаційних вузлів. SNMP забезпечує отримання параметрів із фізичних пристроїв, MRTG виконує їх обробку та графічне представлення, а часові ряди створюють основу для аналізу змін у роботі мережі. Така комбінація є доцільною для розроблення кіберфізичної системи віддаленого моніторингу, оскільки вона поєднує фізичну інфраструктуру, стандартний механізм збору даних і програмний засіб візуалізації результатів.

1.4 Методологічні підходи до вирішення задачі за темою дослідження

Розроблення кіберфізичної системи віддаленого моніторингу комутаційних вузлів мережі потребує поєднання кількох методологічних підходів. Це пов’язано з тим, що система має охоплювати фізичні пристрої мережі, механізми збору параметрів, програмні засоби обробки даних, зберігання статистики та подання результатів у зручній для адміністратора формі. Через це розв’язання задачі не

може обмежуватися лише встановленням окремого програмного засобу. Необхідно сформувати логіку взаємодії всіх компонентів, визначити контрольовані параметри та забезпечити їх регулярне отримання з комутаційних вузлів [1, 2, 20, 21].

Першим методологічним підходом є системний аналіз мережевої інфраструктури. У його межах комутаційний вузол розглядається не як ізольований пристрій, а як елемент загальної інформаційної системи, через який проходять потоки даних між користувачами, серверами, маршрутизаторами та іншими вузлами. Такий підхід дозволяє визначити роль кожного пристрою в мережі, критичність окремих портів, значення uplink-каналів і наслідки можливого перевантаження або відмови. Для системи віддаленого моніторингу це важливо, оскільки першочергового контролю потребують саме ті вузли та інтерфейси, які найбільше впливають на стабільність роботи мережі [31, 35, 69].

Другим підходом є використання стандартизованого збору параметрів за допомогою SNMP. Цей підхід дає змогу отримувати дані з різнорідного мережевого обладнання без розроблення окремих механізмів для кожного виробника. Через SNMP можуть збиратися значення лічильників інтерфейсів, показники вхідного та вихідного трафіку, кількість помилок, відкинуті пакети, стан портів і доступність пристроїв [20, 21, 34]. У межах роботи SNMP виступає основним комунікаційним механізмом між фізичними комутаційними вузлами та програмною частиною системи моніторингу.

Третім підходом є формування набору контрольованих показників. Для ефективного моніторингу недостатньо збирати всі доступні параметри без попереднього відбору. Надмірна кількість метрик ускладнює аналіз, збільшує навантаження на систему та може відволікати від справді важливих ознак погіршення роботи мережі. Через це для комутаційних вузлів доцільно виділяти основні групи параметрів: трафік на інтерфейсах, завантаження uplink-портів, кількість помилок, кількість відкинутих пакетів, доступність вузла, стан портів, а також системні показники пристрою за наявності відповідних MIB-об’єктів [20, 21, 35].

Четвертий підхід пов’язаний із періодичним опитуванням пристроїв. Система моніторингу повинна отримувати параметри не одноразово, а через визначені часові інтервали. Саме повторюваний збір значень дозволяє простежити динаміку роботи мережі, виявити поступове зростання навантаження, регулярні піки або короткочасні відхилення. Водночас інтервал опитування має бути збалансованим. Занадто часті запити можуть створювати зайве навантаження на мережу керування та обладнання, а занадто рідкі - приховувати короткі проблемні події [2, 66, 76].

П’ятим підходом є використання часових рядів для зберігання статистичних даних. Значення мережевих параметрів мають сенс лише тоді, коли вони пов’язані з конкретним моментом часу. Завдяки цьому можна оцінювати не тільки поточний стан комутаційного вузла, а й його поведінку протягом певного періоду. Часові ряди дозволяють виявляти повторювані навантаження, порівнювати робочі та неробочі періоди, аналізувати наслідки змін у конфігурації та оцінювати потребу в модернізації окремих каналів. Для таких задач доцільним є використання RRD-підходу, який забезпечує зберігання історичних значень без неконтрольованого збільшення обсягу даних [9, 10, 11].

Шостим підходом є графічна візуалізація результатів моніторингу. Для адміністратора важливо не тільки отримати числові значення параметрів, а й швидко побачити загальну картину роботи мережі. Графіки дозволяють наочно оцінити зміну трафіку, визначити періоди максимального навантаження, помітити різкі відхилення та порівняти поведінку різних інтерфейсів. Саме тому MRTG є доречним інструментом для цієї роботи, оскільки він поєднує SNMP-опитування з формуванням графіків і звітів, придатних для подальшого аналізу [1, 2, 3, 9].

Сьомим методологічним підходом є порівняння фактичних параметрів із очікуваною поведінкою мережі. У реальній інфраструктурі не кожне зростання трафіку є проблемою. Наприклад, підвищене навантаження у робочий час може бути нормальним явищем, тоді як різкий пік у нетиповий період може свідчити про неконтрольований обмін даними, резервне копіювання, помилку конфігурації або іншу подію. Через це під час аналізу графіків потрібно враховувати не лише

абсолютні значення, а й час виникнення навантаження, його тривалість, повторюваність і зв’язок з іншими параметрами [66, 74, 76].

Восьмим підходом є врахування кіберфізичної природи системи. У межах роботи фізичний рівень представлений комутаторами та іншими мережевими пристроями, комунікаційний рівень забезпечується SNMP-збором параметрів, а програмний рівень реалізується засобами MRTG, механізмами зберігання часових рядів і веб-представленням результатів. Така структура дозволяє перетворити реальний стан фізичного вузла на цифрове представлення, яке може бути проаналізоване віддалено. Це створює основу для своєчасного реагування на перевантаження, деградацію або втрату доступності вузла [1, 2, 67, 69].

Окреме значення має методологічний підхід до безпеки віддаленого моніторингу. Оскільки система працює з параметрами мережевого обладнання та використовує віддалений доступ, необхідно обмежувати коло пристроїв, які можуть звертатися до SNMP-агентів, застосовувати списки доступу, захищати веб-інтерфейс перегляду графіків і не надавати зайвих прав обліковим даним опитування. Такий підхід зменшує ризик несанкціонованого доступу до службової інформації та підтримує безпечну експлуатацію системи моніторингу [23, 26, 28, 29].

Для практичної реалізації задачі доцільно застосувати поетапний підхід. Спочатку визначаються комутаційні вузли, які потребують контролю, та параметри, що мають збиратися. Далі налаштовується SNMP-доступ до пристроїв і перевіряється можливість отримання потрібних MIB-об’єктів. Після цього формується конфігурація MRTG, задаються інтервали опитування, налаштовується зберігання статистики та створюються графіки для перегляду результатів. Завершальним етапом є перевірка працездатності системи, аналіз отриманих графіків і визначення можливостей подальшого використання системи для підтримки адміністрування мережі [2, 4, 5].

У підсумку, методологічна основа роботи передбачає системний аналіз комутаційних вузлів, використання SNMP для збору параметрів, відбір ключових мережевих показників, періодичне опитування пристроїв, збереження часових

рядів, графічну візуалізацію результатів і врахування вимог безпеки. Поєднання цих підходів дозволяє сформувати кіберфізичну систему віддаленого моніторингу, у якій фізичні мережеві пристрої пов’язані з програмним контуром контролю, аналізу та підтримки рішень адміністратора.

1.5 Висновки до розділу 1

У розділі було проаналізовано предметну область віддаленого моніторингу комутаційних вузлів мережі та визначено її значення для підтримання стабільної роботи мережевої інфраструктури. Показано, що комутаційні вузли є важливими елементами комп’ютерної мережі, оскільки через них проходять інформаційні потоки між користувачами, серверами, маршрутизаторами та іншими мережевими пристроями. Порушення роботи таких вузлів може впливати на доступність сервісів, якість передавання даних і безперервність роботи окремих сегментів мережі.

Було встановлено, що ручний контроль стану обладнання не забезпечує достатньої оперативності в умовах зростання кількості пристроїв, портів і мережевого навантаження. Особливо це стосується розподілених мереж, у яких комутаційні вузли можуть бути розташовані у віддалених приміщеннях, технічних шафах або окремих філіях. Це обґрунтовує потребу у віддаленому моніторингу, який дозволяє автоматизовано отримувати параметри роботи обладнання, накопичувати статистику та своєчасно виявляти ознаки перевантаження або деградації мережі.

Проаналізовано існуючі програмні засоби моніторингу мережевої інфраструктури, зокрема MRTG, Cacti, Zabbix, LibreNMS, Nagios Core, PRTG, Prometheus, Grafana та Telegraf. Порівняння показало, що комплексні системи мають ширші можливості щодо автоматичного виявлення пристроїв, формування сповіщень, побудови панелей стану та інтеграції з іншими сервісами. Водночас для задачі графічного контролю параметрів комутаційних вузлів доцільним є використання MRTG, оскільки він забезпечує просте SNMP-опитування, побудову

часових графіків і достатню наочність результатів без надмірного ускладнення системи.

Розглянуто особливості використання SNMP та MRTG у системах мережевого моніторингу. SNMP визначено як основний механізм отримання параметрів із фізичних мережевих пристроїв, а MRTG - як програмний засіб для періодичного опитування вузлів, обробки отриманих значень і формування графіків зміни параметрів у часі. Показано, що така комбінація дозволяє пов’язати фізичний стан комутаційного обладнання з програмним контуром збору, зберігання та візуалізації даних.

Визначено основні методологічні підходи до вирішення задачі за темою роботи. До них належать системний аналіз мережевої інфраструктури, стандартизований збір параметрів через SNMP, вибір контрольованих показників, періодичне опитування пристроїв, збереження історичних даних у вигляді часових рядів, графічна візуалізація результатів і врахування вимог безпеки віддаленого доступу.

У межах постановки задачі було визначено, що подальша робота спрямована на розроблення кіберфізичної системи віддаленого моніторингу комутаційних вузлів мережі на основі MRTG. У результаті сформовано основу для подальшого моделювання, проєктування та реалізації системи, що дозволяє перейти від ручного фрагментарного контролю до системного віддаленого моніторингу мережевої інфраструктури.

2 МОДЕЛЬ КІБЕРФІЗИЧНОЇ СИСТЕМИ ВІДДАЛЕНОГО МОНІТОРИНГУ КОМУТАЦІЙНИХ ВУЗЛІВ МЕРЕЖІ

2.1 Загальна структура кіберфізичної системи моніторингу мережевої інфраструктури

Кіберфізична система віддаленого моніторингу комутаційних вузлів мережі розглядається як сукупність фізичних мережевих пристроїв, комунікаційного механізму збору параметрів, програмних засобів обробки даних, сховища статистичної інформації та інтерфейсу перегляду результатів. Основна ідея такої системи полягає в тому, що реальний стан мережевого обладнання перетворюється на цифрові показники, які можна збирати, зберігати, аналізувати та використовувати для прийняття адміністративних рішень. У межах цієї роботи фізичну основу системи формують комутаційні вузли мережі, а програмну частину - засоби SNMP-опитування, MRTG, механізми роботи з часовими рядами та веб-представлення графіків.

Загальна структура системи включає кілька взаємопов’язаних рівнів. Першим є фізичний рівень, до якого належать комутатори, маршрутизатори, uplink-канали, мережеві інтерфейси та інші пристрої, що забезпечують передавання даних у мережі. Саме на цьому рівні виникають реальні події, які впливають на роботу інфраструктури: зростання трафіку, перевантаження портів, збільшення кількості помилок, втрата доступності вузла або деградація якості передавання даних. Через це фізичний рівень є джерелом первинної інформації для системи моніторингу.

Другим рівнем є комунікаційний рівень збору параметрів. Його основою виступає SNMP, який дозволяє отримувати значення мережевих і системних показників із пристроїв, що підтримують відповідні MIB-об’єкти. Через SNMP система може звертатися до комутаційного вузла, отримувати дані про стан інтерфейсів, обсяг вхідного та вихідного трафіку, кількість помилок, відкинуті пакети, доступність пристрою, а також окремі службові параметри обладнання. Завдяки цьому фізичний стан мережевого вузла стає доступним для подальшої програмної обробки.

Третім рівнем є програмний рівень моніторингу. У цій роботі він реалізується на основі MRTG, який виконує періодичне опитування мережевих пристроїв, обробляє отримані значення та формує графіки зміни параметрів у часі. MRTG відіграє роль проміжної ланки між SNMP-даними та адміністратором, оскільки перетворює числові значення лічильників на зрозумілу графічну форму. Це важливо, оскільки окремі числові показники не завжди дозволяють швидко оцінити стан мережі, тоді як графік показує динаміку, пікові навантаження, повторювані відхилення та поступові зміни.

Четвертим рівнем є рівень зберігання статистичних даних. Для системи моніторингу важливо не лише отримати поточне значення параметра, а й зберегти його у прив’язці до часу. Саме історія зміни параметрів дозволяє оцінювати поведінку мережі за попередні періоди, знаходити повторювані проблеми, порівнювати навантаження в різні часові проміжки та визначати тенденції зростання трафіку. Для таких задач застосовуються підходи до зберігання часових рядів, зокрема RRD, який дозволяє організувати збереження даних без неконтрольованого збільшення обсягу сховища .

П’ятим рівнем є рівень візуалізації та аналізу. Він включає графіки, HTML-сторінки, звіти та інші форми представлення результатів моніторингу. На цьому рівні адміністратор отримує можливість переглядати стан контрольованих інтерфейсів, оцінювати динаміку трафіку, визначати моменти перевантаження та порівнювати роботу різних вузлів. Графічне представлення особливо важливе для практичного аналізу, оскільки дозволяє швидко відрізнити нормальну поведінку мережі від нетипових змін.

Узагальнена структура кіберфізичної системи віддаленого моніторингу комутаційних вузлів може бути подана як послідовність взаємодії: комутаційні вузли мережі передають параметри через SNMP-збір, сервер моніторингу MRTG обробляє отримані значення, база часових рядів зберігає історію, графіки та звіти відображають результати, а адміністратор на основі цієї інформації виконує аналіз і реагування (рисунок 2.1). Така структура відображає повний цикл роботи системи - від фізичного стану обладнання до управлінського рішення.

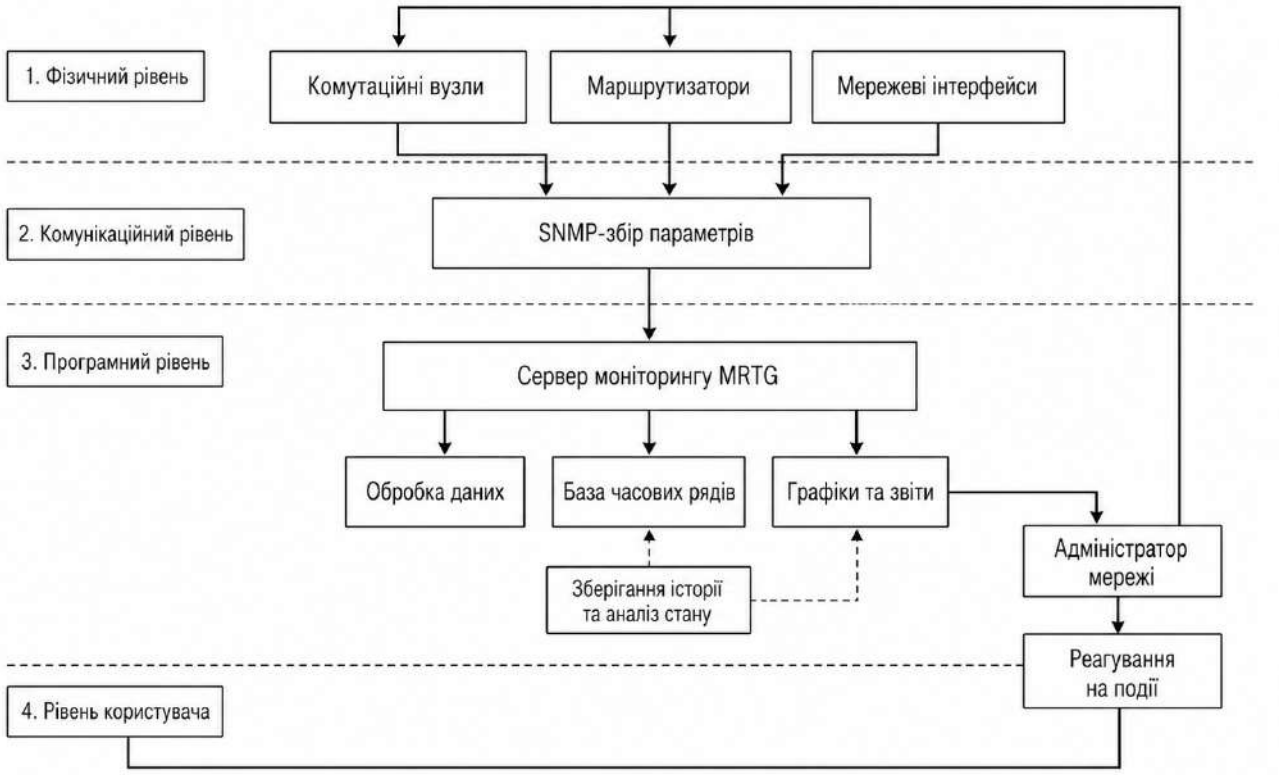


Рисунок 2.1 – Загальна структура кіберфізичної системи віддаленого моніторингу комутаційних вузлів

Кіберфізичний характер системи проявляється в тому, що кожен програмний показник має зв’язок із реальним фізичним станом обладнання. Наприклад, зростання графіка трафіку на uplink-порту може відповідати збільшенню кількості активних користувачів, запуску резервного копіювання, передаванню великих файлів або перевантаженню сегмента мережі. Збільшення кількості помилок на інтерфейсі може бути пов’язане з фізичним пошкодженням кабелю, несправністю порту, некоректним узгодженням швидкості або електромагнітними завадами. Втрата доступності вузла може вказувати на проблеми живлення, збій обладнання або порушення зв’язку. Унаслідок цього система моніторингу не просто показує абстрактні числові значення, а відображає стан реальних фізичних компонентів мережі.

Для побудови моделі системи важливо визначити не лише її рівні, а й інформаційні потоки між ними. Основний потік даних починається на фізичному рівні, де комутаційний вузол накопичує статистику своєї роботи. Далі ця

інформація через SNMP стає доступною для сервера моніторингу. MRTG періодично виконує запити до пристрою, отримує значення відповідних лічильників, обчислює зміну параметрів між циклами опитування та передає результати до механізму збереження. Після цього дані використовуються для побудови графіків і перегляду адміністратором.

Окреме значення має часовий аспект функціонування системи. Моніторинг не є одноразовим вимірюванням, оскільки стан мережі постійно змінюється. Саме повторюваність збору даних дозволяє побачити не тільки поточне значення параметра, а й його зміну в часі. Наприклад, одиничне значення завантаження інтерфейсу не завжди дає підстави для висновку про проблему. Натомість графік за кілька годин або днів може показати, чи є перевантаження випадковим, регулярним або поступово зростаючим. Це дозволяє використовувати систему не лише для фіксації поточного стану, а й для аналізу тенденцій.

Загальна структура системи також повинна враховувати вимоги до безпеки. Оскільки сервер моніторингу отримує доступ до мережевого обладнання, необхідно обмежити взаємодію лише дозволеними вузлами, налаштувати параметри SNMP-доступу, захистити веб-сторінки з графіками та мінімізувати права облікових даних, які використовуються для опитування пристроїв. Такий підхід зменшує ризики несанкціонованого доступу до службової інформації та підтримує безпечну експлуатацію системи.

У межах моделі доцільно розділити систему на функціональні підсистеми. До першої належить підсистема збору параметрів, яка відповідає за взаємодію з комутаційними вузлами через SNMP. Друга підсистема забезпечує обробку отриманих значень і перетворення лічильників у показники, придатні для аналізу. Третя підсистема відповідає за зберігання статистичних даних у часовій формі. Четверта підсистема формує графіки та звіти. П’ята підсистема пов’язана з аналізом результатів і реагуванням адміністратора на виявлені відхилення.

Такий поділ дозволяє чітко визначити роль кожного компонента системи. Комутаційні вузли не виконують аналізу, а лише надають параметри власного стану. SNMP забезпечує доступ до цих параметрів. MRTG організовує періодичне

опитування, обробку та побудову графіків. Сховище часових рядів забезпечує накопичення історії. Адміністратор використовує отримані графіки та звіти для оцінювання ситуації й вибору подальших дій. Це дозволяє уникнути змішування функцій і зробити модель системи зрозумілою для подальшого проєктування.

У підсумку, загальна структура кіберфізичної системи віддаленого моніторингу комутаційних вузлів базується на поєднанні фізичного рівня мережевого обладнання, комунікаційного рівня SNMP, програмного рівня MRTG, сховища часових рядів і рівня візуального аналізу. Така структура забезпечує перехід від фізичних подій у мережі до цифрового представлення стану обладнання, що створює основу для своєчасного виявлення перевантажень, деградацій і порушень доступності.

2.2 Модель взаємодії фізичного, комунікаційного та програмного рівнів системи

Модель кіберфізичної системи віддаленого моніторингу комутаційних вузлів доцільно розглядати як взаємодію трьох основних рівнів: фізичного, комунікаційного та програмного. Кожен із них виконує окрему роль, але повноцінна робота системи можлива лише за умови їх узгодженої взаємодії. Фізичний рівень формує джерело первинних параметрів, комунікаційний рівень забезпечує передавання цих параметрів до сервера моніторингу, а програмний рівень виконує обробку, зберігання та візуальне представлення результатів.

Фізичний рівень системи представлений комутаційними вузлами, маршрутизаторами, мережевими інтерфейсами, uplink-каналами та іншими елементами інфраструктури, які безпосередньо беруть участь у передаванні даних. У межах цієї роботи основна увага зосереджена саме на комутаційних вузлах, оскільки вони забезпечують зв’язок між кінцевими пристроями, серверними ресурсами та іншими сегментами мережі. Кожен комутаційний вузол має набір інтерфейсів, через які проходить вхідний і вихідний трафік, а також набір службових параметрів, що характеризують його стан.

На фізичному рівні виникають події, які можуть впливати на якість роботи мережі. До таких подій належать зростання навантаження на інтерфейси, перевищення пропускної здатності каналу, поява помилок передавання, втрата пакетів, нестабільність лінку, відключення порту або повна недоступність пристрою. Частина таких подій може бути короткочасною, а частина - поступово накопичуватися протягом певного періоду. Саме тому для коректного контролю недостатньо одиничної перевірки стану вузла. Потрібне регулярне отримання параметрів і збереження їх у часовій послідовності.

Комунікаційний рівень забезпечує зв’язок між фізичними пристроями та програмною частиною системи. У розробленій моделі цей рівень реалізується через SNMP-збір параметрів. Комунікаційний рівень виконує роль посередника, який дозволяє серверу моніторингу звертатися до мережевого обладнання та отримувати потрібні значення без ручного входу адміністратора на кожен пристрій. Завдяки цьому комутаційні вузли можуть залишатися фізично віддаленими, але їх стан відображається у програмному середовищі моніторингу.

Основна логіка взаємодії на комунікаційному рівні полягає у періодичному опитуванні пристроїв. Сервер моніторингу надсилає запити до SNMP-агентів, які працюють на комутаторах або маршрутизаторах, після чого отримує відповідь зі значеннями потрібних параметрів. Такі параметри можуть включати лічильники вхідного й вихідного трафіку, стан інтерфейсів, кількість помилок, кількість відкинутих пакетів, час роботи пристрою та інші показники. Отримані значення передаються на програмний рівень для подальшої обробки.

Важливою особливістю комунікаційного рівня є те, що він має бути стабільним і передбачуваним. Якщо запити до пристроїв виконуються нерегулярно або частина відповідей втрачається, графіки та часові ряди можуть містити пропуски, що ускладнює аналіз. Через це в моделі враховується необхідність вибору раціонального інтервалу опитування. Інтервал має бути достатньо малим, щоб система могла помічати важливі зміни, але не настільки частим, щоб створювати зайве навантаження на мережу керування або обладнання.

Програмний рівень системи відповідає за перетворення отриманих параметрів у зручну для аналізу форму. У межах цієї роботи основним програмним компонентом є сервер моніторингу MRTG. Він виконує опитування пристроїв, приймає значення лічильників, обчислює зміну параметрів між циклами збору та формує графічне представлення результатів. У такій моделі MRTG виступає не просто інструментом побудови графіків, а центральним елементом програмного контуру системи.

Окреме місце на програмному рівні займає обробка даних. Більшість параметрів, які надходять із мережевого обладнання, є накопичувальними лічильниками. Наприклад, пристрій може передавати загальну кількість байтів, що пройшли через певний інтерфейс від моменту запуску. Для адміністратора важливішим є не саме накопичене значення, а швидкість його зміни за певний проміжок часу. Саме тому програмний рівень виконує перетворення таких значень у показники, які відображають реальне навантаження на інтерфейс.

Після обробки дані зберігаються у вигляді часових рядів. Це дозволяє пов’язати кожне значення з конкретним моментом часу та сформувати історію зміни параметрів. Завдяки цьому система може показувати не лише поточне навантаження, а й динаміку роботи комутаційного вузла за попередні періоди. Історичні дані мають важливе значення для виявлення повторюваних піків, оцінювання стабільності роботи обладнання, пошуку причин інцидентів і планування модернізації мережі.

Візуалізація є завершальною частиною програмного рівня. На цьому етапі оброблені дані подаються у вигляді графіків, таблиць або HTML-сторінок. Графічне представлення дозволяє швидко оцінити стан інтерфейсів, визначити періоди підвищеного навантаження, помітити різкі стрибки трафіку або виявити тривале зростання використання каналу. Для адміністратора це значно зручніше, ніж аналіз окремих числових значень, оскільки графік відображає поведінку параметра в часі.

Між фізичним, комунікаційним і програмним рівнями існує чіткий інформаційний зв’язок. Фізичний рівень формує реальні параметри роботи

обладнання. Комунікаційний рівень забезпечує їх передавання до сервера моніторингу. Програмний рівень перетворює ці параметри на інформаційний результат, придатний для аналізу. У підсумку створюється замкнений контур контролю, у якому адміністратор отримує цифрове представлення стану фізичної мережевої інфраструктури.

У моделі взаємодії також важливим є зворотний зв’язок. Після перегляду графіків і звітів адміністратор може виконати певні дії: перевірити фізичне підключення, змінити конфігурацію порту, обмежити або перерозподілити трафік, оновити обладнання, змінити схему підключення або посилити контроль за певним сегментом мережі. Після цього система моніторингу знову фіксує стан обладнання, і на графіках можна оцінити, чи дали виконані дії очікуваний результат.

Цей зворотний зв’язок є однією з ознак кіберфізичного характеру системи. Програмний рівень не просто пасивно відображає дані з фізичних пристроїв, а формує інформаційну основу для впливу на стан мережі. Якщо на графіках виявлено перевантаження, адміністратор може змінити конфігурацію або розширити пропускну здатність каналу. Якщо зафіксовано зростання помилок, може бути перевірено кабель, порт або параметри узгодження швидкості. Якщо вузол стає недоступним, може бути виконана перевірка живлення, підключення або стану обладнання.

Модель взаємодії рівнів також дозволяє визначити межі відповідальності кожного компонента. Фізичні пристрої відповідають за формування первинних параметрів і надання їх через SNMP. Комунікаційний рівень відповідає за стабільну передачу цих параметрів. Програмний рівень відповідає за регулярне опитування, обробку, зберігання та візуалізацію. Адміністратор використовує результати для аналізу та реагування. Такий розподіл функцій спрощує подальше проєктування системи, оскільки кожен рівень має чітке призначення.

Для роботи системи важливо, щоб усі рівні були узгоджені між собою. Якщо фізичний пристрій не підтримує потрібні параметри, програмний рівень не зможе побудувати повний графік. Якщо неправильно налаштовано SNMP-доступ, сервер моніторингу не отримає дані. Якщо інтервал опитування вибрано невдало, графіки

можуть не відображати реальну динаміку навантаження. Якщо результати подані незручно, адміністратор може не помітити важливі відхилення. Через це модель системи має враховувати не лише окремі компоненти, а й якість їхньої взаємодії.

У розробленій моделі взаємодія рівнів відбувається за послідовною логікою: фізичний вузол формує параметри, SNMP-збір отримує ці параметри, MRTG обробляє їх, база часових рядів зберігає історію, графіки та звіти відображають результат, а адміністратор виконує аналіз і реагування. Після реагування стан фізичної мережі змінюється, і система знову фіксує ці зміни через наступні цикли моніторингу. Це дозволяє підтримувати безперервний контроль за станом комутаційних вузлів.

У підсумку, модель взаємодії фізичного, комунікаційного та програмного рівнів показує, як реальні параметри мережевого обладнання перетворюються на цифрову інформацію для аналізу. Фізичний рівень забезпечує джерело даних, комунікаційний рівень передає ці дані, програмний рівень обробляє та візуалізує їх, а адміністратор на основі отриманої інформації приймає рішення щодо подальших дій. Така модель є основою для подальшого опису збору параметрів, формування часових рядів і побудови механізмів виявлення перевантажень та відхилень.

2.3 Модель збору параметрів комутаційних вузлів за допомогою SNMP

Модель збору параметрів комутаційних вузлів є одним із ключових елементів кіберфізичної системи віддаленого моніторингу. Саме на цьому етапі фізичний стан мережевого обладнання перетворюється на набір цифрових показників, які можуть бути оброблені, збережені та представлені у вигляді графіків. У межах розробленої системи збір параметрів виконується за допомогою SNMP, що забезпечує стандартизовану взаємодію між сервером моніторингу та комутаційними вузлами мережі.

Основна ідея SNMP-збору полягає в тому, що кожен контрольований пристрій має вбудований або налаштований SNMP-агент. Цей агент надає доступ

до службових параметрів пристрою через визначені ідентифікатори об’єктів. Сервер моніторингу виконує роль керуючої сторони, яка періодично надсилає запити до пристроїв і отримує від них значення потрібних показників. Така модель дозволяє контролювати стан обладнання без ручного входу в інтерфейс кожного комутатора.

У загальному вигляді процес збору параметрів складається з кількох послідовних етапів. Спочатку формується перелік комутаційних вузлів, які потрібно контролювати. Для кожного вузла задається мережева адреса, параметри доступу до SNMP, перелік інтерфейсів і набір показників, які мають збиратися. Після цього сервер моніторингу через визначені часові інтервали звертається до пристроїв, отримує актуальні значення параметрів і передає їх на подальшу обробку. У результаті формується безперервний потік статистичних даних про роботу мережевої інфраструктури.

Вхідними даними для моделі збору є список комутаційних вузлів, їх IP-адреси, параметри SNMP-доступу, перелік контрольованих інтерфейсів, ідентифікатори потрібних параметрів, а також інтервал опитування. До вхідних параметрів також належать відомості про тип обладнання, логічне розташування пристрою в мережі, призначення портів і критичність конкретного вузла. Ця інформація потрібна для того, щоб система не просто збирала випадкові значення, а формувала осмислену картину стану мережі.

Вихідними даними моделі є отримані значення мережевих показників. До них належать лічильники вхідного та вихідного трафіку, кількість помилок на інтерфейсах, кількість відкинутих пакетів, стан портів, доступність пристрою, час безперервної роботи, а також окремі системні параметри, якщо вони підтримуються обладнанням. На основі цих даних надалі формуються часові ряди, графіки та звіти для адміністратора.

Для комутаційних вузлів найважливішою групою параметрів є показники інтерфейсів. Саме інтерфейси відображають реальне навантаження на мережу, оскільки через них проходить основний трафік. Контроль вхідного та вихідного трафіку дозволяє оцінити, які порти використовуються найактивніше, де

виникають пікові навантаження і чи не наближається використання каналу до граничного значення. Особливо важливими є uplink-порти, оскільки вони часто з’єднують комутатор із маршрутизатором, серверним сегментом або іншим рівнем мережевої інфраструктури.

Окрему увагу в моделі збору приділено показникам помилок і відкинутих пакетів. Зростання кількості помилок може свідчити про фізичні проблеми з кабелем, нестабільність порту, некоректне узгодження швидкості або несправність обладнання. Відкинуті пакети можуть виникати через перевантаження інтерфейсу, нестачу буферів або надмірний обсяг трафіку. Якщо такі параметри розглядати разом із графіком завантаження, можна точніше визначити характер проблеми та її можливу причину.

Модель збору також враховує доступність комутаційного вузла. Якщо пристрій не відповідає на SNMP-запит або стає недоступним у мережі, це фіксується як важлива подія. Недоступність вузла може бути пов’язана з проблемами живлення, відмовою обладнання, розривом каналу зв’язку, помилкою маршрутизації або блокуванням доступу до SNMP. Для адміністратора така інформація має першочергове значення, оскільки втрата доступності комутатора може вплинути на роботу цілого сегмента мережі.

У межах моделі важливо розрізняти накопичувальні та поточні параметри. Накопичувальні лічильники, наприклад загальна кількість переданих байтів, самі по собі не показують поточне навантаження. Для їх практичного використання потрібно визначити різницю між двома послідовними значеннями та співвіднести її з проміжком часу між вимірюваннями. Саме так формується показник інтенсивності трафіку. Поточні параметри, наприклад стан порту або доступність пристрою, можуть аналізуватися без такого перетворення, оскільки вони відображають стан у конкретний момент часу.

Цикл SNMP-збору має повторюваний характер. На початку циклу сервер моніторингу перевіряє перелік контрольованих пристроїв і параметрів. Далі для кожного вузла виконується запит до потрібних об’єктів. Якщо відповідь отримано, значення передаються на обробку. Якщо відповідь не отримано, система фіксує

відсутність даних або недоступність вузла. Після завершення циклу система очікує до наступного інтервалу опитування і повторює процедуру. Завдяки цьому формується неперервна послідовність вимірювань.

Важливим елементом моделі є інтервал опитування. Він визначає, як часто система буде звертатися до комутаційних вузлів. Короткий інтервал дозволяє точніше фіксувати швидкі зміни навантаження, але збільшує кількість запитів до обладнання. Довший інтервал зменшує навантаження на мережу керування, але може приховувати короткочасні піки. Через це інтервал опитування має вибиратися з урахуванням критичності вузла, кількості контрольованих пристроїв і вимог до точності моніторингу.

Для критичних uplink-портів доцільно використовувати менший інтервал опитування, оскільки саме на таких інтерфейсах найчастіше проявляються перевантаження, що впливають на роботу значної частини мережі. Для менш важливих портів або другорядних системних параметрів можна застосовувати більший інтервал. Такий підхід дозволяє збалансувати деталізацію моніторингу та навантаження на систему.

У моделі збору параметрів також враховується можливість роботи з різними типами обладнання. Навіть якщо пристрої підтримують SNMP, набір доступних параметрів може відрізнятися. Одні комутатори надають лише базову інформацію про інтерфейси, інші дозволяють отримувати додаткові системні показники, температуру, завантаження процесора, стан живлення або інші службові дані. Через це модель має бути гнучкою: обов’язковими слід вважати базові параметри інтерфейсів і доступність вузла, а додаткові показники можуть підключатися за наявності підтримки з боку конкретного пристрою.

З погляду кіберфізичної логіки, SNMP-збір виконує роль перетворювача між фізичним станом комутаційного вузла та програмним представленням цього стану. Реальне завантаження порту, поява помилок або втрата лінку виникають на фізичному рівні. SNMP дає можливість отримати цифрове відображення цих подій, а програмна частина системи перетворює їх у графіки та часові ряди. Унаслідок

цього адміністратор може аналізувати не сам пристрій безпосередньо, а його цифровий профіль, сформований за результатами опитування.

Для стабільної роботи моделі важливо забезпечити правильне налаштування доступу до SNMP. Сервер моніторингу має бути дозволеним джерелом запитів, а сторонні пристрої не повинні мати можливості звертатися до SNMP-агента. Це дозволяє зменшити ризик несанкціонованого перегляду службових параметрів і обмежити доступ до інформації про структуру мережі. Крім цього, доцільно використовувати окрему мережу керування або обмеження доступу на рівні мережевого обладнання.

Результати SNMP-збору мають бути придатними для подальшої обробки в MRTG. Для цього потрібно, щоб кожен контрольований параметр мав зрозуміле призначення, правильну одиницю вимірювання та відповідність конкретному інтерфейсу або пристрою. Якщо на етапі збору неправильно вибрано параметр, графік може не відображати реального стану мережі. Тому модель передбачає попередню перевірку коректності отриманих значень і відповідності їх очікуваній поведінці пристрою.

У розробленій моделі SNMP-збір не є самостійною завершеною дією. Він є частиною ширшого процесу моніторингу, який включає отримання параметрів, їх перетворення, збереження, візуалізацію та подальший аналіз. Без етапу збору система не має первинних даних, а без наступних етапів ці дані залишаються лише набором числових значень. Саме поєднання SNMP-збору з MRTG-обробкою та графічним представленням створює повноцінну систему віддаленого контролю.

У підсумку, модель збору параметрів комутаційних вузлів за допомогою SNMP забезпечує регулярне отримання цифрових показників із фізичних мережевих пристроїв. Вона визначає склад вхідних і вихідних даних, перелік контрольованих параметрів, порядок опитування, значення інтервалу збору та вимоги до коректності отриманих значень. Така модель є основою для подальшого формування часових рядів, побудови графіків і виявлення перевантажень або відхилень у роботі мережі.

2.4 Формування часових рядів мережевих параметрів у системі моніторингу

Формування часових рядів є важливою складовою кіберфізичної системи віддаленого моніторингу, оскільки саме цей механізм дозволяє перейти від одиничних значень параметрів до аналізу їх зміни в часі. Для контролю комутаційних вузлів недостатньо лише періодично отримувати поточні показники з пристроїв. Реальна користь системи проявляється тоді, коли зібрані значення накопичуються, впорядковуються за часовими мітками та надалі використовуються для побудови графіків, виявлення тенденцій і визначення відхилень у роботі мережі.

Часовий ряд у межах цієї роботи розглядається як послідовність значень певного мережевого параметра, зафіксованих через однакові або заздалегідь визначені проміжки часу. Для кожного контрольованого інтерфейсу або вузла формується власний набір таких послідовностей. Наприклад, окремо можуть накопичуватися ряди для вхідного трафіку, вихідного трафіку, кількості помилок, відкинутих пакетів або доступності пристрою. Це дозволяє аналізувати не один узагальнений показник, а кілька незалежних характеристик стану мережевого обладнання.

Початковим етапом формування часового ряду є отримання значення параметра під час чергового циклу опитування. На цьому кроці система приймає дані від SNMP-агента, визначає, до якого пристрою, інтерфейсу та показника вони належать, і фіксує момент часу, у який ці дані були отримані. Після цього значення стає елементом майбутнього часового ряду. Якщо подібна процедура повторюється багаторазово, формується впорядкована часово послідовність, яка відображає поведінку параметра протягом певного періоду.

Для мережевого моніторингу важливо враховувати, що частина параметрів надходить у вигляді накопичувальних лічильників. Це означає, що пристрій не повідомляє безпосередньо поточну інтенсивність трафіку, а передає загальне число байтів або пакетів, що пройшли через інтерфейс від моменту запуску. Через це під

час формування часового ряду необхідно виконувати проміжне перетворення: обчислювати різницю між двома послідовними значеннями та співвідносити її з інтервалом часу між вимірюваннями. Унаслідок цього отримується не просто накопичений лічильник, а показник фактичного навантаження на інтерфейс.

Для інших параметрів, наприклад доступності вузла або стану порту, таке перетворення може не знадобитися. У таких випадках часовий ряд формується безпосередньо з послідовності станів, зафіксованих у різні моменти часу. Це дозволяє бачити, коли саме виникали розриви зв’язку, нестабільність порту або відключення пристрою. Такий підхід є корисним не лише для побудови графіків, а й для подальшого аналізу причин мережевих інцидентів.

У моделі системи часові ряди виконують одразу кілька функцій. По-перше, вони зберігають історію зміни мережевих параметрів. По-друге, вони створюють основу для побудови графіків. По-третє, саме на їх основі можуть виявлятися пікові навантаження, нетипові відхилення або тривалі зміни в роботі мережі. Якщо система має лише поточне значення параметра, вона показує стан вузла лише в один момент часу. Якщо ж значення накопичуються у вигляді часового ряду, стає можливою повноцінна оцінка динаміки функціонування комутаційного вузла.

Формування часових рядів тісно пов’язане з вибором інтервалу опитування. Саме він визначає, наскільки детально система зможе відображати зміни параметрів. Якщо значення збираються через надто великі проміжки часу, графік буде надто згладженим, а короткочасні піки можуть залишитися непоміченими. Якщо ж опитування виконується занадто часто, зростає навантаження на сервер моніторингу, мережу керування та самі пристрої. Через це часовий крок повинен бути достатнім для фіксації важливих змін, але не надмірним з погляду витрат ресурсів.

Ще однією важливою особливістю є поділ часових рядів за рівнем деталізації. Для поточного контролю корисними є більш детальні ряди з коротким інтервалом між вимірюваннями. Для тривалого зберігання доцільно використовувати узагальнене представлення, де частина значень агрегується за більшими часовими проміжками. Такий підхід дозволяє не втрачати історію роботи

мережі та водночас не допускати надмірного зростання обсягу даних. У практичній реалізації це дає можливість переглядати як нещодавню динаміку, так і довгострокову тенденцію зміни параметрів.

Для комутаційних вузлів найбільше значення мають часові ряди трафіку на інтерфейсах. Саме вони дозволяють визначити години пікового навантаження, знайти порти з найбільшою активністю та оцінити, чи наближається використання каналу до граничних можливостей. Окремо важливо формувати часові ряди для помилок і відкинутих пакетів, оскільки їх зміна часто вказує не на зростання нормального навантаження, а на появу проблем у роботі обладнання або каналу зв’язку.

Часові ряди також відіграють важливу роль у формуванні аналітичної картини для адміністратора. Якщо на графіку видно регулярне зростання навантаження в певні години, це може свідчити про нормальний робочий режим мережі. Якщо ж система фіксує різкий аномальний сплеск у нетиповий період, це вже може бути підставою для додаткової перевірки. Аналогічно, стабільне накопичення помилок або повторювані втрати доступності вузла формують підґрунтя для висновку про нестабільний стан обладнання.

У структурі кіберфізичної системи часовий ряд виступає як проміжна форма подання стану фізичного об’єкта. Фізичний рівень формує реальні події, SNMP-збір перетворює їх на цифрові значення, а часовий ряд поєднує ці значення в послідовність, яка вже придатна для графічного та аналітичного використання. Це означає, що часовий ряд є не просто технічним способом зберігання даних, а важливою частиною всієї логіки моделі моніторингу.

У межах цієї роботи формування часових рядів розглядається як обов’язкова умова побудови повноцінної системи віддаленого моніторингу. Без часової складової система була б зведена до набору разових вимірювань, які не дозволяють оцінювати тенденції, повторюваність навантажень чи поступове погіршення стану обладнання (рисунок 2.2). Натомість часові ряди створюють основу для переходу від простого збору даних до аналізу функціонування мережевої інфраструктури.

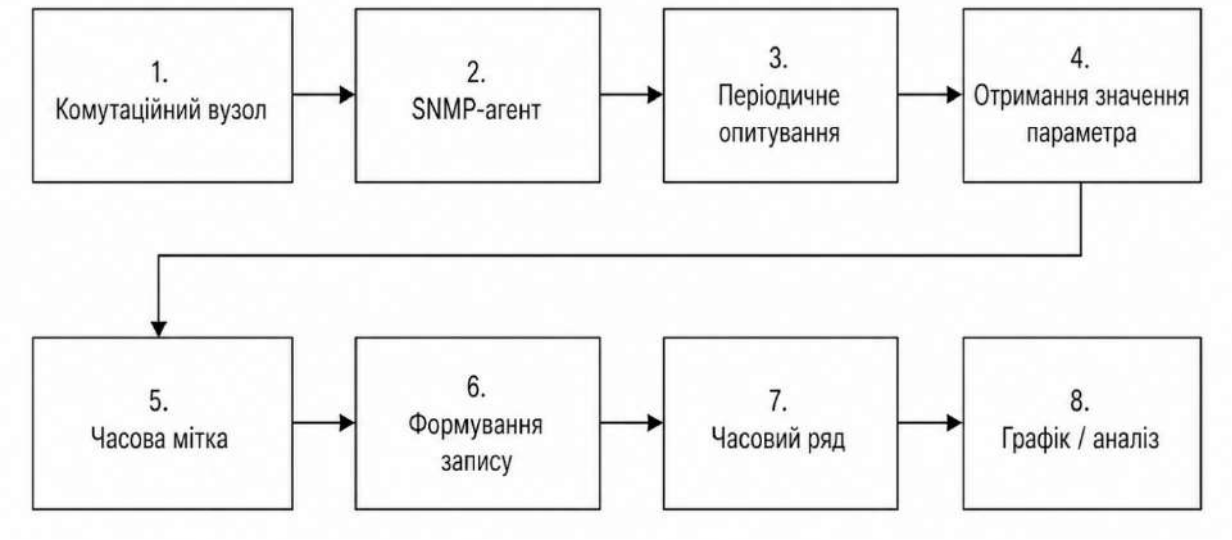


Рисунок 2.2 – Схема формування часового ряду мережевого параметра в системі моніторингу

У підсумку, формування часових рядів мережевих параметрів є центральним елементом моделі моніторингу, оскільки забезпечує накопичення історичних даних, побудову графіків і створює основу для виявлення змін у роботі комутаційних вузлів. Саме завдяки часовим рядам система отримує можливість не лише фіксувати поточний стан мережі, а й відображати її поведінку в динаміці.

2.5 Визначення контрольованих показників стану комутаційних вузлів

Для побудови кіберфізичної системи віддаленого моніторингу важливо визначити, які саме параметри комутаційних вузлів мають контролюватися. Надмірна кількість показників ускладнює аналіз, створює зайве навантаження на систему збору даних і може відволікати адміністратора від справді важливих ознак погіршення роботи мережі.

Водночас занадто обмежений набір параметрів не дає повної картини стану обладнання. Через це контрольовані показники мають відображати як навантаження на мережеві інтерфейси, так і якість передавання даних, доступність вузлів та загальний технічний стан пристроїв.

Основною групою контрольованих параметрів є показники трафіку. До них належать обсяг вхідних і вихідних даних, швидкість передавання, завантаження портів і використання uplink-каналів. Саме ці параметри дозволяють оцінити, наскільки активно використовується комутаційний вузол і чи не наближається навантаження до межі пропускної здатності. Особливо важливим є контроль uplink-портів, оскільки через них часто проходить трафік між окремими сегментами мережі, серверною частиною або маршрутизатором.

Другою важливою групою є показники якості передавання. Вони включають кількість помилок на інтерфейсах, відкинуті пакети, втрати та ознаки нестабільної роботи порту. Якщо обсяг трафіку зростає без збільшення кількості помилок, це може свідчити про нормальне навантаження мережі. Якщо ж разом зі зростанням трафіку збільшується кількість помилок або відкинутих пакетів, це вже може вказувати на перевантаження, фізичну проблему лінії, несправність порту або невдалу конфігурацію.

Окреме значення має контроль доступності комутаційного вузла. Навіть якщо система не отримує детальних параметрів від пристрою, сам факт його доступності або недоступності є важливим для адміністратора.

Втрата доступності може свідчити про збій живлення, відключення каналу, зависання обладнання, помилку маршрутизації або некоректне налаштування керування. У моделі системи доступність розглядається як базовий показник, без якого неможливо забезпечити повноцінний віддалений контроль.

До додаткових показників належать системні параметри пристрою (таблиця 2.1). Якщо обладнання підтримує відповідні об’єкти моніторингу, доцільно контролювати завантаження процесора, використання оперативної пам’яті, температуру, стан живлення та час безперервної роботи.

Такі параметри не завжди безпосередньо показують стан мережевого трафіку, але вони допомагають оцінити технічний стан самого вузла. Наприклад, високе завантаження процесора комутатора може пояснювати затримки в обробці трафіку або нестабільність керування.

Таблиця 2.1 – Контрольовані показники стану комутаційних вузлів

Група показників	Приклади параметрів	Практичне значення
Показники трафіку	Вхідний трафік, вихідний трафік, завантаження порту, використання uplink-каналу	Дають змогу оцінити навантаження на інтерфейси та виявити перевантажені канали
Показники якості передавання	Помилки, відкинуті пакети, втрати, нестабільність лінку	Допомагають виявити проблеми фізичного середовища, порту або перевантаження
Показники доступності	Доступність вузла, відповідь на запит, стан порту	Дозволяють визначити факт роботи або недоступності пристрою
Системні показники	Завантаження процесора, пам’ять, температура, час роботи	Характеризують технічний стан обладнання та його ресурсне навантаження
Аналітичні показники	Пікові значення, середнє навантаження, повторювані відхилення	Використовуються для аналізу тенденцій і планування розвитку мережі

Показники трафіку є базовими для системи на основі MRTG, оскільки саме вони найкраще відображають практичне використання комутаційних вузлів. На основі цих параметрів можна визначити, які порти використовуються найактивніше, у які періоди виникає найбільше навантаження та чи вистачає пропускної здатності наявних каналів. Якщо графік завантаження регулярно наближається до максимальної швидкості інтерфейсу, це є підставою для розгляду питання про модернізацію або зміну топології підключення.

Показники помилок і відкинутих пакетів потрібно аналізувати разом із показниками трафіку. Саме поєднання цих даних дозволяє краще зрозуміти характер проблеми. Якщо помилки з’являються навіть за невеликого

навантаження, причиною може бути фізичне пошкодження кабелю або несправність порту. Якщо кількість відкинутих пакетів зростає лише під час пікового навантаження, це може свідчити про нестачу пропускної здатності або перевантаження буферів.

Системні показники мають допоміжний характер, але вони підвищують повноту картини. Наприклад, тривале високе завантаження процесора комутатора може впливати на стабільність роботи служб керування. Підвищення температури може свідчити про проблеми з вентиляцією або розміщенням обладнання. Тривалий час безперервної роботи, навпаки, може підтверджувати стабільність вузла, якщо при цьому не спостерігається зростання помилок або втрат.

У підсумку, набір контрольованих показників має бути достатнім для оцінювання стану комутаційного вузла, але не надмірним. Для розробленої системи основними є показники трафіку, стану інтерфейсів, помилок, відкинутих пакетів і доступності вузлів. Додаткові системні параметри використовуються за наявності підтримки з боку обладнання. Такий підхід дозволяє сформувати практичну модель моніторингу, у якій увага зосереджується на тих параметрах, що безпосередньо впливають на стабільність і якість роботи мережі.

2.6 Модель виявлення перевантажень, деградацій та аномальних відхилень

Модель виявлення перевантажень, деградацій та аномальних відхилень є логічним продовженням моделі збору параметрів і формування часових рядів. Якщо попередні етапи забезпечують отримання та збереження даних, то на цьому етапі ці дані використовуються для оцінювання стану комутаційного вузла. Основна мета моделі полягає в тому, щоб за значеннями мережевих параметрів визначити, чи працює вузол у нормальному режимі, чи в його роботі з’явилися ознаки перевантаження, поступової деградації або нетипової поведінки.

Під перевантаженням у межах цієї роботи розуміється ситуація, коли навантаження на інтерфейс або комутаційний вузол наближається до межі його пропускної здатності або перевищує допустимий рівень для стабільної роботи.

Найчастіше це проявляється у високих значеннях вхідного або вихідного трафіку, регулярному досягненні пікових значень, збільшенні затримок, появі відкинутих пакетів або зростанні кількості помилок. Для uplink-каналів така ситуація є особливо критичною, оскільки перевантаження одного магістрального інтерфейсу може впливати на роботу значної частини мережевого сегмента.

Деградація роботи комутаційного вузла відрізняється від звичайного короткочасного перевантаження тим, що її ознаки можуть накопичуватися поступово. Наприклад, протягом кількох днів або тижнів може зростати середнє навантаження на порт, збільшуватися кількість помилок або частіше з’являтися короткочасна недоступність вузла. Окремо кожна така подія може не виглядати критичною, але їх повторюваність вказує на погіршення стану мережевого обладнання або каналу зв’язку. Саме тому модель має враховувати не тільки поточне значення параметра, а й його поведінку в часі.

Аномальним відхиленням вважається така зміна параметра, яка не відповідає звичному режиму роботи мережі. Наприклад, різке зростання трафіку в неробочий час, нестандартне навантаження на порт, який зазвичай використовується рідко, або поява великої кількості помилок без очевидного збільшення трафіку можуть бути ознаками аномальної ситуації. У таких випадках система не обов’язково повинна автоматично робити остаточний висновок про причину проблеми, але вона має надати адміністратору підставу для додаткової перевірки.

Основою моделі виявлення є порівняння фактичних значень параметрів із допустимими або очікуваними межами. Для кожного контрольованого показника може бути визначено умовний поріг, після перевищення якого параметр потребує уваги. Наприклад, для завантаження інтерфейсу може бути встановлено рівень, після якого порт вважається наближеним до перевантаження. Для помилок або відкинутих пакетів важливим є не лише абсолютне значення, а й швидкість їх зростання. Якщо кількість таких подій збільшується протягом кількох циклів опитування, це може вказувати на стійку проблему.

У спрощеному вигляді логіку оцінювання стану параметра можна подати через порівняння поточного значення з допустимим порогом:

Для більш коректної оцінки недостатньо аналізувати лише одне вимірювання. Разовий пік може бути випадковим і не завжди свідчить про проблему. Тому модель має враховувати повторюваність перевищень. Якщо високі значення з’являються протягом кількох послідовних інтервалів або повторюються у схожий час, така ситуація потребує більшої уваги. Це дозволяє відрізняти короткочасне навантаження від стійкого перевантаження або поступової деградації.

Важливим є також поєднання кількох параметрів. Наприклад, високе завантаження інтерфейсу без помилок може свідчити про інтенсивне, але нормальне використання каналу. Якщо ж одночасно з високим трафіком зростає кількість відкинутих пакетів або помилок, імовірність проблеми значно вища. Аналогічно, зростання помилок за низького навантаження може вказувати не на перевантаження, а на фізичну несправність кабелю, порту або модуля підключення.

Для системи на основі MRTG основним інструментом виявлення таких ситуацій є графічний аналіз часових рядів. Графіки дозволяють побачити не лише числове перевищення, а й характер зміни параметра. Плавне зростання середнього навантаження може свідчити про поступове збільшення кількості користувачів або сервісів. Різкий короткий сплеск може бути пов’язаний із разовим обміном великим обсягом даних. Регулярні піки в один і той самий час можуть вказувати на планові процеси, наприклад резервне копіювання або синхронізацію даних.

У моделі доцільно виділити три основні стани контрольованого параметра: нормальний стан, попереджувальний стан і критичний стан. Нормальний стан означає, що параметр перебуває в допустимих межах і не має ознак нестабільності. Попереджувальний стан виникає тоді, коли параметр наближається до порогового значення або демонструє небажану тенденцію. Критичний стан фіксується у разі перевищення допустимого рівня, повторюваної втрати доступності, різкого збільшення помилок або стійкого перевантаження інтерфейсу.

Такий поділ дозволяє не зводити аналіз лише до простого визначення «працює» або «не працює». Для адміністратора важливо бачити проміжні ознаки проблеми ще до того, як вона призведе до повної відмови. Наприклад, якщо uplink-

порт протягом тривалого часу працює на рівні, близькому до максимальної пропускної здатності, це ще не є аварією, але вже є підставою для планування модернізації або перерозподілу трафіку.

У межах кіберфізичної системи модель виявлення відхилень пов’язує цифрові дані з реальними діями щодо мережевої інфраструктури. Якщо графіки показують перевантаження, може бути виконано зміну схеми підключення або збільшення пропускної здатності. Якщо зафіксовано зростання помилок, перевіряється фізичне середовище передавання. Якщо вузол періодично стає недоступним, аналізуються живлення, стабільність каналу та стан самого обладнання. Унаслідок цього система моніторингу стає інструментом не лише спостереження, а й підтримки експлуатаційних рішень.

У підсумку, модель виявлення перевантажень, деградацій та аномальних відхилень базується на аналізі часових рядів, порогових значень, повторюваності подій і взаємозв’язку кількох параметрів. Вона дозволяє оцінювати стан комутаційних вузлів не лише за поточними значеннями, а й за характером зміни показників у часі. Це створює основу для своєчасного реагування на проблеми мережевої інфраструктури та підтримує практичну цінність розробленої системи віддаленого моніторингу.

2.7 Висновки до розділу 2

У розділі було сформовано модель кіберфізичної системи віддаленого моніторингу комутаційних вузлів мережі. Розглянуто загальну структуру системи, у якій фізичні мережеві пристрої поєднуються з комунікаційним рівнем збору параметрів і програмним контуром обробки, зберігання та візуалізації даних. Показано, що така система дозволяє перетворити реальний стан комутаційних вузлів на цифрове представлення, придатне для подальшого аналізу адміністратором.

Було визначено основні рівні системи: фізичний, комунікаційний, програмний і рівень користувача. Фізичний рівень представлено комутаційними

вузлами, маршрутизаторами та мережевими інтерфейсами. Комунікаційний рівень забезпечує отримання параметрів за допомогою SNMP. Програмний рівень реалізує опитування пристроїв, обробку отриманих значень, зберігання статистики та формування графіків. Рівень користувача пов’язаний із переглядом результатів моніторингу, аналізом стану мережі та реагуванням на виявлені відхилення.

Описано модель взаємодії фізичного, комунікаційного та програмного рівнів системи. У межах цієї моделі комутаційний вузол виступає джерелом первинних параметрів, SNMP забезпечує їх передавання до сервера моніторингу, а MRTG виконує обробку та графічне подання результатів. Такий підхід дозволяє організувати безперервний цикл контролю, у якому стан фізичного обладнання регулярно відображається у вигляді цифрових показників і графіків.

Було розглянуто модель збору параметрів комутаційних вузлів за допомогою SNMP. Визначено, що вхідними даними для цієї моделі є перелік контрольованих пристроїв, їхні мережеві адреси, параметри доступу, інтерфейси та набір показників, які потрібно контролювати. Вихідними даними є значення трафіку, помилок, відкинутих пакетів, стану портів, доступності вузлів та інших параметрів, які надалі використовуються для формування часових рядів і графіків.

Окрему увагу приділено формуванню часових рядів мережевих параметрів. Показано, що часовий ряд дозволяє перейти від одиничного вимірювання до аналізу зміни параметра в часі. Це важливо для виявлення регулярних пікових навантажень, поступового зростання трафіку, повторюваних помилок, нестабільності портів і тривалих змін у роботі комутаційних вузлів. Завдяки цьому система моніторингу може використовуватися не лише для перегляду поточного стану мережі, а й для аналізу її поведінки за попередні періоди.

Визначено основні контрольовані показники стану комутаційних вузлів. До них належать вхідний і вихідний трафік, завантаження uplink-каналів, кількість помилок, відкинуті пакети, стан портів, доступність вузлів і системні параметри обладнання. Такий набір показників дозволяє оцінювати не лише факт роботи пристрою, а й якість його функціонування, ступінь завантаження та можливі ознаки технічних проблем.

3 АРХІТЕКТУРА КІБЕРФІЗИЧНОЇ СИСТЕМИ ВІДДАЛЕНОГО МОНІТОРИНГУ НА ОСНОВІ MRTG

3.1 Обґрунтування архітектури кіберфізичної системи віддаленого моніторингу

Розроблення архітектури кіберфізичної системи віддаленого моніторингу комутаційних вузлів виконано з урахуванням того, що система має поєднувати фізичне мережеве обладнання, механізм збору параметрів, програмну обробку даних, збереження історії та візуальне подання результатів. Основна вимога до архітектури полягає в тому, щоб стан реальних комутаційних вузлів міг регулярно перетворюватися на цифрові показники, які надалі використовуються для аналізу, побудови графіків і підтримки рішень адміністратора мережі.

У межах роботи архітектуру системи побудовано за багаторівневим принципом. Такий підхід дозволяє чітко розділити функції між окремими частинами системи та уникнути змішування фізичного, комунікаційного й програмного рівнів. Фізичний рівень відповідає за формування первинних параметрів, комунікаційний рівень забезпечує передавання цих параметрів до сервера моніторингу, програмний рівень виконує опитування, обробку та зберігання даних, а рівень користувача забезпечує перегляд графіків і подальше реагування.

У цій архітектурі MRTG є центральним елементом програмного рівня, але повноцінна робота системи забезпечується лише за наявності фізичних вузлів, каналу збору параметрів, сховища даних, механізму візуалізації та дій адміністратора. Це дозволяє розглядати систему як завершений кіберфізичний контур, у якому цифрова частина постійно пов’язана з фізичною інфраструктурою.

Фізичний рівень архітектури представлено комутаційними вузлами, маршрутизаторами та мережевими інтерфейсами. Саме ці елементи формують первинні дані про роботу мережі. До таких даних належать вхідний і вихідний трафік, стан портів, кількість помилок, кількість відкинутих пакетів, доступність вузла та інші параметри, які можуть бути отримані від обладнання. Фізичний рівень

є джерелом реальних подій, а програмна частина системи лише відображає ці події в цифровій формі.

Комунікаційний рівень архітектури реалізовано через SNMP-збір параметрів. Його призначення полягає в тому, щоб забезпечити регулярний доступ сервера моніторингу до параметрів комутаційних вузлів. У цій частині системи важливими є IP-адреси пристроїв, параметри доступу, перелік контрольованих інтерфейсів, ідентифікатори потрібних параметрів і частота опитування. Комунікаційний рівень виконує роль каналу, через який стан фізичних пристроїв передається до програмної частини системи.

Програмний рівень побудовано навколо сервера моніторингу MRTG. Він виконує періодичне опитування пристроїв, отримує значення параметрів, обробляє їх і формує графічне представлення. Оскільки частина мережевих параметрів надходить у вигляді накопичувальних лічильників, програмний рівень також виконує перетворення цих значень у показники, придатні для практичного аналізу. Наприклад, загальна кількість переданих байтів перетворюється на інтенсивність трафіку за певний проміжок часу.

Залежність між двома послідовними значеннями лічильника та інтенсивністю параметра можна подати так:

$$q_i(t) = \big(x_i(t) - x_i(t - \Delta t)\big)/\Delta t, \tag{3.1}$$

де $q_i(t)$ - інтенсивність зміни і-го параметра в момент часу t;

$x_i(t)$ – поточне значення лічильника і-го параметра;

$x_i(t - \Delta t)$ - попереднє значення цього лічильника;

Δt - інтервал між двома послідовними циклами опитування.

Наприклад, якщо комутаційний вузол передає загальну кількість байтів на інтерфейсі, то без порівняння з попереднім значенням складно оцінити поточне навантаження. Після обчислення різниці між двома вимірюваннями можна визначити, наскільки активно використовувався інтерфейс у заданому часовому проміжку.

Сховище статистичних даних у розробленій архітектурі потрібне для збереження історії параметрів. Воно забезпечує накопичення значень у вигляді часових рядів, що дає змогу оцінювати не тільки поточний стан мережі, а й поведінку вузлів за попередні періоди. Завдяки цьому адміністратор може переглядати графіки за різні часові проміжки, знаходити повторювані піки, порівнювати навантаження та визначати поступові зміни у роботі мережі.

Підсистема візуалізації відповідає за подання результатів у вигляді графіків і звітів. Вона є важливою частиною архітектури, оскільки саме через неї цифрові дані стають зрозумілими для адміністратора. Графіки дозволяють швидко побачити перевантаження, різкі стрибки трафіку, періоди простою, нестабільність порту або поступове зростання навантаження. У межах роботи візуалізація розглядається не як допоміжний елемент, а як основний інструмент аналізу стану комутаційних вузлів(рисунок 3.1).

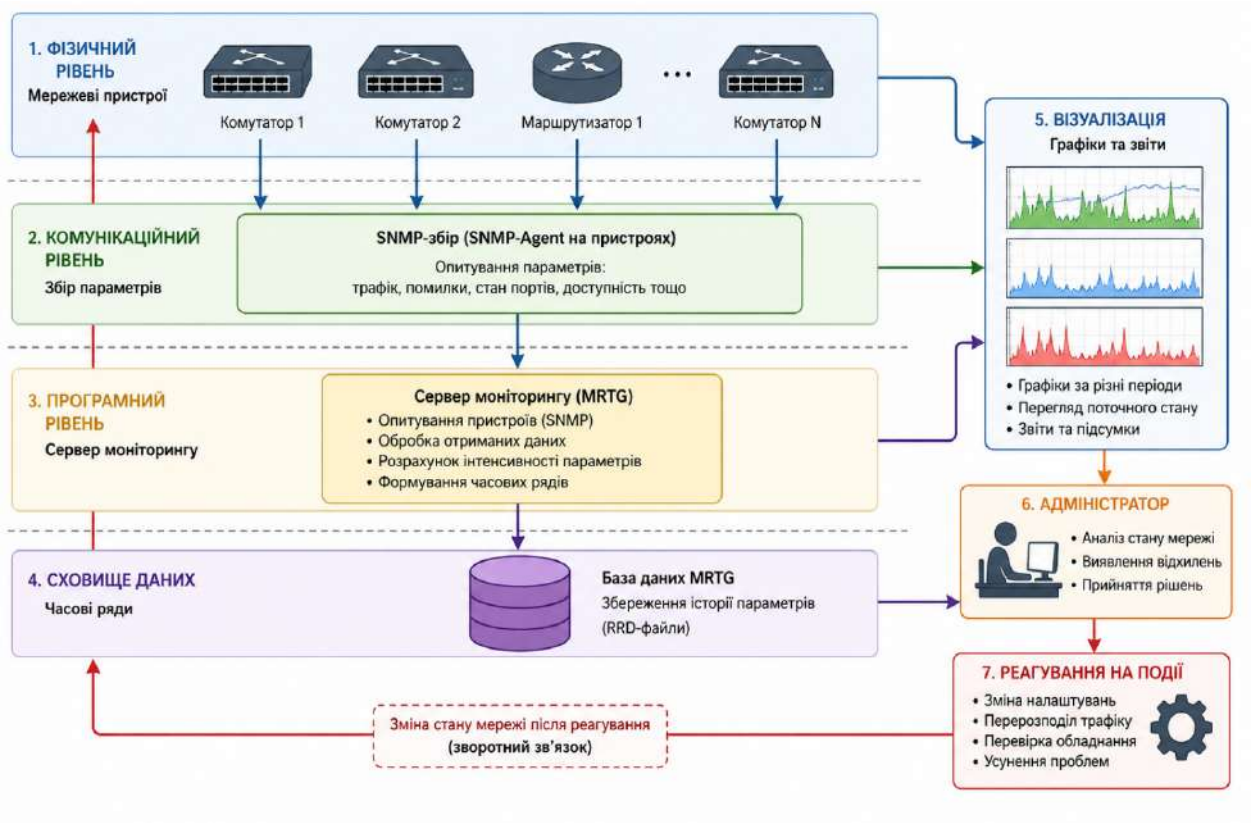


Рисунок 3.1 – Архітектура кіберфізичної системи віддаленого моніторингу на основі MRTG

Важливою особливістю архітектури є наявність зворотного зв’язку. Адміністратор не тільки переглядає графіки, а й виконує певні дії на основі отриманої інформації. До таких дій можуть належати перевірка фізичного підключення, зміна налаштувань порту, перерозподіл трафіку, оновлення обладнання, зміна схеми підключення або посилення контролю за окремим вузлом. Після виконання таких дій система знову фіксує зміну параметрів, що дозволяє оцінити результат реагування.

Спочатку дані виникають на фізичному рівні, потім передаються через SNMP-збір, обробляються сервером моніторингу, зберігаються у сховищі, відображаються у вигляді графіків і використовуються адміністратором для прийняття рішень. Завершальним етапом є реагування, після якого стан фізичної мережі може змінитися, а система знову зафіксує ці зміни.

Обґрунтування вибору саме такої архітектури пов’язане з її простотою, зрозумілістю та практичною придатністю. У системі не передбачено надмірно складних компонентів, які ускладнювали б реалізацію або відволікали від основної задачі. Основна увага зосереджена на стабільному зборі параметрів, формуванні часових рядів, побудові графіків і підтримці аналізу стану мережі. Це відповідає поставленій задачі, оскільки система має бути придатною для віддаленого контролю комутаційних вузлів без зайвого ускладнення.

У підсумку, розроблена архітектура кіберфізичної системи віддаленого моніторингу на основі MRTG забезпечує послідовний зв’язок між фізичними комутаційними вузлами та програмним контуром аналізу. Вона включає рівень мережевого обладнання, SNMP-збір параметрів, сервер моніторингу, сховище часових рядів, візуалізацію та механізм реагування.

Така структура створює основу для подальшого проєктування інформаційних потоків, підсистеми збору параметрів, підсистеми зберігання даних і механізмів контролю критичних станів.

3.2 Розроблення структури взаємодії комутаційних вузлів і сервера моніторингу

Структуру взаємодії комутаційних вузлів і сервера моніторингу розроблено з урахуванням того, що система має забезпечувати регулярне отримання параметрів із фізичних мережевих пристроїв без безпосереднього ручного доступу до кожного вузла. Основна взаємодія в системі відбувається між комутаторами, SNMP-агентами, сервером моніторингу MRTG, сховищем часових рядів і веб-компонентом перегляду результатів. Така побудова дозволяє організувати послідовний рух даних від фізичного обладнання до графічного представлення стану мережі.

У розробленій структурі комутаційний вузол виступає джерелом первинних параметрів. На ньому формується статистика роботи інтерфейсів, накопичуються значення лічильників трафіку, фіксується стан портів, кількість помилок, відкинутих пакетів і службові параметри пристрою. Ці дані не передаються самостійно до сервера моніторингу, а стають доступними через SNMP-агент, який працює на мережевому обладнанні. Саме SNMP-агент забезпечує можливість отримання параметрів у відповідь на запити сервера.

Сервер моніторингу виконує активну роль у процесі збору даних. Він не очікує випадкового надходження інформації, а самостійно запускає цикл опитування відповідно до заданої конфігурації. У конфігурації визначаються адреси контрольованих пристроїв, параметри доступу, перелік інтерфейсів, потрібні показники та інтервал опитування. Завдяки цьому взаємодія між сервером і комутаційними вузлами має керований характер і може бути повторена у кожному наступному циклі збору.

Під час одного циклу опитування сервер моніторингу звертається до SNMP-агента конкретного пристрою, отримує значення потрібних параметрів, перевіряє їхню наявність і передає на обробку. Якщо пристрій відповідає коректно, дані використовуються для оновлення часових рядів і графіків. Якщо відповідь не отримано, це фіксується як відсутність даних або можлива недоступність вузла.

Унаслідок цього система дозволяє контролювати не лише навантаження на інтерфейси, а й сам факт доступності комутаційного вузла.

Структура взаємодії має враховувати, що один сервер моніторингу може обслуговувати декілька комутаційних вузлів. Для кожного пристрою формується окремий набір параметрів, але загальна логіка збору залишається однаковою. Це дозволяє масштабувати систему: до неї можна додавати нові вузли, нові інтерфейси або нові параметри без зміни загального принципу роботи. У такій побудові сервер моніторингу виступає центральною точкою збору й обробки інформації.

Для впорядкування даних у системі кожне отримане значення має бути пов’язане з конкретним пристроєм, інтерфейсом, параметром і моментом часу. Без цього неможливо коректно побудувати графік або порівняти значення за різні періоди. Тому в структурі взаємодії передбачено, що після отримання параметра система формує запис, який містить ідентифікатор вузла, ідентифікатор інтерфейсу, тип показника, значення параметра та часову мітку.

Після отримання й упорядкування даних сервер моніторингу виконує їх обробку. Для параметрів, які надходять у вигляді накопичувальних лічильників, визначається різниця між поточним і попереднім значенням. Це дозволяє отримати інтенсивність зміни показника, наприклад швидкість вхідного або вихідного трафіку. Для станів портів, доступності вузлів або інших дискретних показників виконується фіксація поточного стану без додаткового перетворення.

Окреме значення має взаємодія сервера моніторингу зі сховищем часових рядів. Після обробки значення не повинні втрачатися, оскільки їх подальша користь полягає саме в накопиченні історії. Сховище забезпечує збереження даних у часовій послідовності, що дозволяє переглядати стан мережі за різні періоди. У результаті адміністратор може бачити не тільки поточне значення параметра, а й те, як цей параметр змінювався протягом години, дня, тижня або довшого проміжку.

Веб-компонент системи взаємодіє вже не з фізичними комутаційними вузлами, а з результатами обробки та збереженими даними. Його завдання полягає у відображенні графіків, звітів і підсумкової інформації для адміністратора.

Завдяки цьому користувач системи не працює безпосередньо з SNMP-запитами або службовими лічильниками, а отримує підготовлене представлення стану мережі. Це спрощує аналіз і дозволяє швидше виявляти проблеми.

У структурі взаємодії також передбачено зворотний зв’язок. Після перегляду графіків адміністратор може виконати певні дії щодо мережі: змінити налаштування порту, перевірити кабель, перерозподілити трафік, замінити обладнання або змінити схему підключення. Після цього сервер моніторингу продовжує опитування пристроїв і фіксує новий стан мережі. Це дозволяє оцінити, чи вплинули виконані дії на параметри комутаційного вузла.

Важливою умовою правильної взаємодії є узгодженість часових інтервалів. Якщо сервер опитує різні вузли з однаковою періодичністю, результати легше порівнювати між собою. Наприклад, можна одночасно оцінити завантаження uplink-портів на різних комутаторах або порівняти зміну трафіку на кількох сегментах мережі. Якщо ж інтервали опитування різні, аналіз також можливий, але потребує уважнішого зіставлення часових міток.

Розроблена структура взаємодії також враховує можливість втрати відповіді від пристрою. У реальній мережі комутаційний вузол може тимчасово не відповідати через перевантаження, втрату зв’язку, неправильні параметри доступу або технічну несправність. У такому випадку система не повинна зупиняти весь процес моніторингу. Вона має зафіксувати відсутність даних для конкретного вузла та продовжити опитування інших пристроїв. Це підвищує стійкість системи та дозволяє уникнути залежності всієї архітектури від одного проблемного елемента.

У підсумку, розроблена структура взаємодії комутаційних вузлів і сервера моніторингу забезпечує послідовний рух даних від фізичного обладнання до графічного представлення результатів. Комутаційні вузли формують первинні параметри, SNMP-агенти надають доступ до них, сервер MRTG виконує опитування й обробку, сховище часових рядів накопичує історію, а веб-компонент подає результати адміністратору. Така взаємодія створює основу для подальшого розроблення інформаційних потоків і підсистеми збору параметрів у межах кіберфізичної системи.

3.3 Розроблення інформаційних потоків у системі моніторингу

Інформаційні потоки в кіберфізичній системі віддаленого моніторингу розроблено так, щоб забезпечити послідовне передавання даних від фізичних комутаційних вузлів до програмного рівня обробки, зберігання та візуального представлення. Основне призначення інформаційних потоків полягає в тому, щоб кожна подія або зміна стану мережевого обладнання могла бути зафіксована, перетворена на цифровий параметр і використана для аналізу стану мережі.

У межах розробленої системи інформаційний потік починається на рівні комутаційного вузла. Саме там формуються первинні параметри, які відображають роботу мережевого обладнання. До таких параметрів належать лічильники вхідного та вихідного трафіку, стан інтерфейсів, кількість помилок, кількість відкинутих пакетів, доступність вузла та окремі службові показники пристрою. Ці значення є первинними даними, які ще не мають зручної для адміністратора форми, але є основою для подальшої обробки.

Перший інформаційний потік формується між комутаційним вузлом і SNMP-агентом. У цій частині системи фізичний стан пристрою відображається у вигляді доступних параметрів. SNMP-агент не виконує аналітичної обробки, а лише надає доступ до значень, які можуть бути зчитані сервером моніторингу. Це дозволяє відокремити фізичний рівень від програмного рівня й забезпечити стандартизований спосіб отримання даних.

Другий інформаційний потік виникає між SNMP-агентом і сервером моніторингу MRTG. Сервер надсилає запит до пристрою, а у відповідь отримує значення потрібного параметра. Такий обмін виконується періодично, відповідно до заданого інтервалу опитування. Завдяки повторюваності цього процесу система отримує не випадкові окремі значення, а послідовність вимірювань, придатну для формування часових рядів.

Третій інформаційний потік пов’язаний з обробкою отриманих значень на сервері моніторингу. На цьому етапі виконується перевірка отриманих даних, прив’язка значення до конкретного вузла, інтерфейсу та моменту часу, а також

перетворення накопичувальних лічильників у показники інтенсивності. Наприклад, якщо комутатор надає загальну кількість переданих байтів, система обчислює різницю між двома послідовними значеннями та визначає навантаження за відповідний проміжок часу.

Спочатку параметр існує як частина стану фізичного вузла, далі стає доступним через SNMP-агент, після цього надходить на сервер моніторингу, зберігається у вигляді часового запису та виводиться у графічній формі. Такий підхід дозволяє описати інформаційний рух у системі без надмірного ускладнення моделі.

Четвертий інформаційний потік формується між сервером моніторингу та сховищем часових рядів. Після обробки дані не повинні втрачатися, оскільки їхня основна цінність проявляється під час аналізу динаміки. Сховище зберігає значення у часовій послідовності, що дозволяє переглядати історію зміни параметрів за різні періоди. Завдяки цьому система підтримує не лише поточний контроль, а й ретроспективний аналіз стану комутаційних вузлів.

П’ятий інформаційний потік пов’язаний із візуалізацією результатів. На цьому етапі дані зі сховища перетворюються на графіки, звіти або веб-сторінки. Візуалізація є важливою частиною системи, оскільки адміністратор працює не з окремими числовими значеннями, а з підготовленим представленням стану мережі. Графіки дозволяють побачити динаміку трафіку, регулярні піки, поступове зростання навантаження або різкі відхилення.

Окремо виділено інформаційний потік від підсистеми візуалізації до адміністратора. Цей потік має аналітичний характер, оскільки він передає вже не первинні дані, а зручну для оцінювання інформацію. Адміністратор отримує можливість переглянути стан окремого інтерфейсу, порівняти завантаження кількох портів, визначити проблемний період або помітити повторювані відхилення. Це створює основу для прийняття подальших рішень.

Завершальним є потік зворотного впливу, який виникає після аналізу результатів. Якщо на графіках виявлено перевантаження, зростання помилок або недоступність вузла, адміністратор виконує відповідні дії щодо мережевого

обладнання. Це може бути перевірка фізичного з’єднання, зміна конфігурації порту, перерозподіл трафіку, заміна кабелю, перезапуск обладнання або модернізація каналу. Після виконання таких дій система знову фіксує параметри пристрою, і нові значення потрапляють у наступні цикли моніторингу.

У розробленій архітектурі інформаційні потоки мають циклічний характер. Вони не завершуються після одного вимірювання, оскільки моніторинг виконується постійно. Кожен новий цикл опитування створює нову порцію даних, яка проходить той самий шлях: фізичний пристрій, SNMP-агент, сервер MRTG, обробка, сховище, графік, аналіз. Саме повторюваність цього процесу забезпечує актуальність системи та дозволяє бачити зміну параметрів у часі.

Важливою вимогою до інформаційних потоків є їхня однозначність. Кожне отримане значення повинно бути пов’язане з конкретним вузлом, інтерфейсом, параметром і часом отримання. Якщо хоча б один із цих елементів не визначено, дані можуть втратити практичну цінність. Наприклад, значення трафіку без прив’язки до інтерфейсу не дозволяє встановити, який саме порт був перевантажений. Значення без часової мітки не дозволяє побудувати коректний графік або порівняти його з іншими подіями.

Також важливо, щоб інформаційні потоки залишалися стійкими до часткових збоїв. Якщо один комутаційний вузол тимчасово не відповідає, система не повинна припиняти опитування інших пристроїв. У такому випадку для проблемного вузла фіксується відсутність даних, а загальний цикл моніторингу продовжується. Це дозволяє зберегти працездатність системи навіть за наявності окремих несправностей або втрати доступності частини обладнання.

У підсумку, розроблені інформаційні потоки забезпечують повний шлях даних від фізичного стану комутаційного вузла до графічного представлення та подальшого реагування. Вони поєднують SNMP-збір, серверну обробку, зберігання часових рядів, візуалізацію та аналітичні дії адміністратора. Така побудова дозволяє системі працювати як цілісний кіберфізичний контур, у якому зміни в реальній мережевій інфраструктурі регулярно відображаються у цифровому середовищі моніторингу.

3.4 Розроблення підсистеми збору параметрів через SNMP

Підсистему збору параметрів через SNMP розроблено як одну з основних частин кіберфізичної системи віддаленого моніторингу комутаційних вузлів. Її призначення полягає в регулярному отриманні параметрів із фізичного мережевого обладнання та передаванні цих даних до сервера моніторингу для подальшої обробки, збереження й візуалізації. Саме ця підсистема забезпечує зв’язок між реальним станом комутаційних вузлів і програмним контуром контролю.

У розробленій архітектурі SNMP-збір виконує роль комунікаційного механізму, який дозволяє серверу моніторингу отримувати значення параметрів без ручного входу адміністратора на кожен комутатор. Для цього на мережевих пристроях використовується SNMP-агент, який надає доступ до службових показників обладнання. Сервер моніторингу звертається до агента через визначені інтервали часу, отримує потрібні значення та передає їх до наступних етапів обробки.

Підсистема збору побудована за циклічним принципом. Спочатку сервер моніторингу визначає перелік пристроїв, які мають бути опитані. Далі для кожного комутаційного вузла виконується звернення до потрібних параметрів. Після отримання відповіді значення перевіряються, прив’язуються до конкретного вузла, інтерфейсу та часу отримання, а потім передаються до підсистеми обробки. Після завершення циклу система очікує до наступного інтервалу опитування і повторює процес.

До складу підсистеми збору входять такі основні елементи: перелік контрольованих вузлів, параметри доступу до SNMP, набір контрольованих показників, механізм періодичного опитування, обробник відповідей і блок фіксації помилок доступу. Такий склад дозволяє не лише отримувати значення параметрів, а й контролювати сам факт успішного або неуспішного звернення до пристрою. Якщо комутаційний вузол не відповідає, система фіксує відсутність даних і не припиняє опитування інших пристроїв.

Для кожного контрольованого вузла було визначено набір параметрів, які мають найбільше практичне значення для віддаленого моніторингу. До них належать вхідний і вихідний трафік на інтерфейсах, стан портів, кількість помилок, кількість відкинутих пакетів, доступність вузла та, за наявності підтримки обладнанням, окремі системні показники. Основний акцент зроблено на параметрах інтерфейсів, оскільки саме вони найкраще відображають реальне навантаження на комутаційний вузол.

Під час розроблення підсистеми враховано різницю між накопичувальними та поточними параметрами. Накопичувальні лічильники, наприклад загальна кількість переданих байтів, потребують подальшого перетворення для визначення інтенсивності трафіку. Поточні параметри, наприклад стан порту або доступність вузла, можуть використовуватися без складного перерахунку. Це враховано під час передавання даних до підсистеми обробки, оскільки різні типи параметрів потребують різної логіки інтерпретації.

Важливою частиною підсистеми є налаштування інтервалу опитування. Для критичних інтерфейсів, через які проходить значна частина трафіку, інтервал має бути достатньо коротким, щоб система могла виявляти помітні зміни навантаження. Для менш важливих параметрів допускається більший інтервал, щоб не створювати зайвого навантаження на сервер моніторингу та мережу керування. Унаслідок цього підсистема збору може працювати збалансовано: отримувати достатньо детальні дані й не перевантажувати інфраструктуру зайвими запитами.

Підсистема збору також має враховувати можливі помилки під час опитування. До таких ситуацій належать недоступність пристрою, неправильні параметри доступу, відсутність відповіді від SNMP-агента, відсутність потрібного параметра або тимчасовий збій мережевого зв’язку. У таких випадках система не повинна зупиняти весь процес моніторингу. Для проблемного вузла фіксується відсутність значення, а опитування інших пристроїв продовжується. Це підвищує стійкість системи та дозволяє зберегти контроль над доступною частиною мережі.

З погляду безпеки, підсистема збору параметрів потребує обмеження доступу до SNMP-агентів. Сервер моніторингу має бути єдиним або одним із небагатьох дозволених джерел запитів. Доступ сторонніх пристроїв до службових параметрів комутаторів повинен бути обмежений. Крім цього, параметри SNMP-доступу не мають використовуватися для ширших прав, ніж потрібно для моніторингу. Такий підхід підтримує принцип мінімально необхідного доступу та зменшує ризики несанкціонованого перегляду інформації про мережеву інфраструктуру.

Окремо враховано необхідність відповідності отриманих параметрів реальним інтерфейсам обладнання (рисунок 3.2). Якщо в конфігурації помилково вказано неправильний ідентифікатор параметра, система може будувати графік, який не відповідає потрібному порту або не має практичного значення. Через це під час розроблення підсистеми передбачено перевірку відповідності параметрів, назв інтерфейсів і логічного призначення портів. Це дозволяє уникнути ситуацій, коли графіки формально створюються, але не відображають потрібний фрагмент мережі.

У розробленій підсистемі SNMP-збір не розглядається як разова дія. Він працює безперервно, формуючи регулярний потік даних про стан комутаційних вузлів. Кожен цикл опитування оновлює уявлення системи про стан мережі, а послідовність таких циклів створює основу для часових рядів і подальшого графічного аналізу. Завдяки цьому адміністратор отримує не фрагментарну інформацію, а системно зібрані дані про роботу обладнання.

У підсумку, підсистему збору параметрів через SNMP розроблено як комунікаційну основу всієї системи віддаленого моніторингу. Вона забезпечує регулярне звернення до комутаційних вузлів, отримання значень контрольованих параметрів, фіксацію часу отримання, виявлення недоступності пристроїв і передавання даних до наступних етапів обробки. Саме ця підсистема забезпечує перехід від фізичного стану мережевого обладнання до цифрового представлення, яке використовується в MRTG для формування графіків і підтримки аналізу стану мережі.

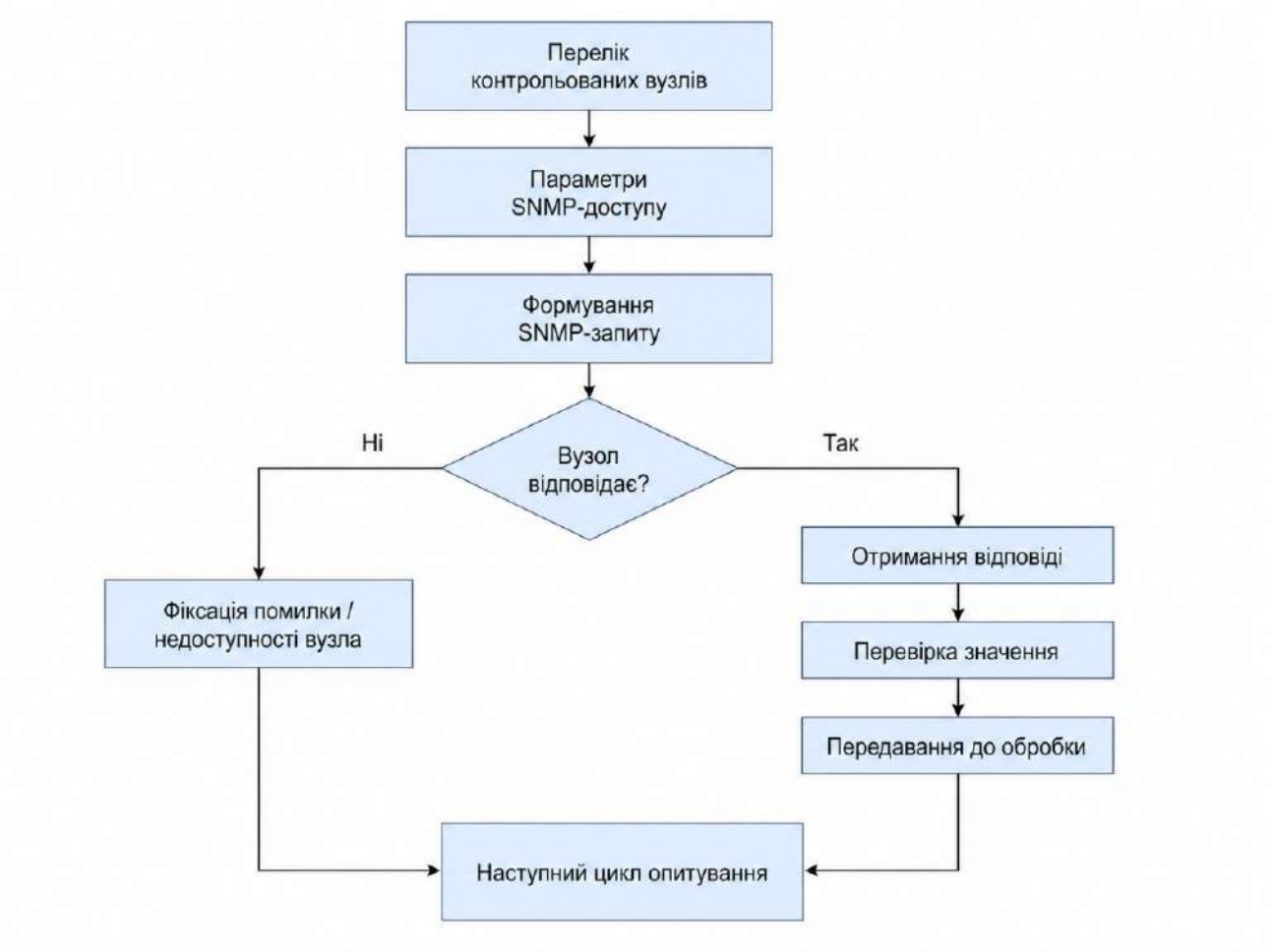


Рисунок 3.2 – Схема роботи підсистеми збору параметрів через SNMP

3.5 Розроблення підсистеми зберігання та обробки статистичних даних

Підсистему зберігання та обробки статистичних даних розроблено для впорядкування параметрів, які надходять від комутаційних вузлів через SNMP-збір. Її основне призначення полягає в тому, щоб перетворити окремі отримані значення на послідовну історію роботи мережевого обладнання. Без такої підсистеми моніторинг обмежувався б лише переглядом поточного стану вузлів, тоді як для аналізу перевантажень, деградацій і повторюваних відхилень потрібна саме історія зміни параметрів у часі.

У розробленій системі статистичні дані надходять до підсистеми зберігання після етапу SNMP-опитування та первинної перевірки значень. Кожен отриманий параметр пов’язується з конкретним комутаційним вузлом, інтерфейсом, типом

показника та часовою міткою. Це дозволяє надалі не просто зберігати числові значення, а формувати впорядковані часові ряди, придатні для побудови графіків і подальшого аналізу.

Основними даними, які зберігаються у підсистемі, є значення вхідного й вихідного трафіку, кількість помилок, кількість відкинутих пакетів, стан портів, доступність вузлів і додаткові системні параметри обладнання. Для кожного показника формується окрема послідовність значень. Наприклад, для одного uplink-порту можуть окремо накопичуватися значення вхідного трафіку, вихідного трафіку, помилок і відкинутих пакетів. Такий поділ дозволяє не змішувати різні типи параметрів і забезпечує коректне формування графіків.

Підсистема обробки виконує кілька важливих функцій. Насамперед вона перевіряє, чи отримане значення є коректним і чи може бути використане для подальшого збереження. Якщо вузол не відповів або значення не було отримано, у системі фіксується пропуск. Якщо значення отримано, воно передається до етапу перетворення. Для накопичувальних лічильників виконується обчислення різниці між поточним і попереднім значенням, після чого визначається інтенсивність зміни параметра.

Особливе значення має обробка лічильників трафіку. Комутатори часто передають не поточну швидкість передавання даних, а загальну кількість байтів, які пройшли через інтерфейс. Таке значення саме по собі не є зручним для аналізу. Тому підсистема обробки порівнює його з попереднім значенням і визначає, який обсяг даних було передано за інтервал між двома опитуваннями. Після цього результат може бути відображений на графіку як навантаження на інтерфейс.

Окремо враховано ситуації, коли значення лічильника може змінитися некоректно. Наприклад, після перезавантаження пристрою накопичувальний лічильник може почати відлік з меншого значення. У такому випадку пряме обчислення різниці між поточним і попереднім значенням може дати помилковий результат. Через це підсистема обробки повинна враховувати можливі розриви послідовності, пропуски даних або перезапуск обладнання. Такі ситуації не завжди

означають проблему з трафіком, але вони мають бути правильно відображені в історії моніторингу.

Збереження статистики в часовій формі дозволяє використовувати дані для різних типів аналізу. Поточні графіки показують оперативний стан мережі, короткострокова історія допомагає оцінити останні зміни, а довгострокові дані дозволяють виявляти тенденції. Наприклад, якщо середнє навантаження на uplink-порт поступово зростає протягом кількох тижнів, це може свідчити про збільшення кількості користувачів або сервісів. Якщо помилки з'являються періодично, можна шукати зв'язок із певним часом, навантаженням або фізичним станом обладнання.

У підсистемі зберігання важливо уникати неконтрольованого збільшення обсягу даних. Моніторинг виконується регулярно, тому навіть невелика кількість параметрів із часом може створити значний обсяг статистики. Для розв'язання цієї задачі використовується підхід, за якого детальні значення зберігаються для найближчих періодів, а для довших проміжків можуть застосовуватися узагальнені значення. Це дозволяє зберігати історію роботи мережі без надмірного навантаження на сховище.

Підсистема зберігання також забезпечує підготовку даних для візуалізації. Графіки не будуються безпосередньо з випадкових відповідей пристроїв, а формуються на основі впорядкованих часових рядів. Це дає змогу коректно відображати зміну параметрів за різні періоди: останні хвилини, години, дні або тижні. Завдяки цьому адміністратор може переглядати як оперативну ситуацію, так і загальну тенденцію розвитку навантаження.

У розробленій підсистемі обробка і зберігання статистичних даних виконують проміжну, але дуже важливу роль. Вони знаходяться між SNMP-збором і графічним представленням результатів. Якщо на цьому етапі дані будуть неправильно прив'язані до часу, інтерфейсу або типу параметра, подальші графіки можуть виявитися неточними. Через це підсистема зберігання повинна забезпечувати цілісність, послідовність і логічну впорядкованість отриманих значень.

У підсумку, підсистему зберігання та обробки статистичних даних розроблено як основу для формування історії роботи комутаційних вузлів. Вона забезпечує перевірку отриманих параметрів, перетворення накопичувальних лічильників, формування часових рядів, збереження статистики та підготовку даних до візуалізації. Завдяки цій підсистемі віддалений моніторинг набуває не лише поточного, а й аналітичного значення, оскільки дозволяє оцінювати зміну стану мережі в часі.

3.6 Розроблення підсистеми візуалізації результатів моніторингу

Підсистему візуалізації результатів моніторингу розроблено для подання зібраних і оброблених параметрів комутаційних вузлів у зрозумілій графічній формі. Її призначення полягає в тому, щоб перетворити часові ряди, сформовані на основі SNMP-даних, у графіки та звіти, придатні для швидкого аналізу стану мережевої інфраструктури. Саме ця підсистема є основною точкою взаємодії адміністратора з результатами роботи системи.

У межах розробленої архітектури візуалізація не розглядається як другорядний елемент. Якщо дані лише зберігаються у вигляді числових значень, їх практична цінність для адміністратора залишається обмеженою. Для аналізу стану мережі важливо бачити не тільки окреме значення параметра, а й характер його зміни в часі. Графік дозволяє швидше визначити, чи є навантаження нормальним, чи спостерігається перевантаження, деградація, повторюваний пік або нетипове відхилення.

Основними вхідними даними для підсистеми візуалізації є часові ряди мережевих параметрів. До них належать значення вхідного та вихідного трафіку, помилок, відкинутих пакетів, доступності вузлів і стану портів. Для кожного контрольованого інтерфейсу може формуватися окремий графік, який показує зміну параметра за визначений період. Це дозволяє не змішувати дані різних портів і забезпечує точніший аналіз конкретного елемента мережі.

У підсистемі передбачено відображення результатів за різними часовими проміжками. Для оперативного контролю використовуються короткі періоди, які дозволяють оцінити поточне навантаження. Для аналізу тенденцій застосовуються довші інтервали, за якими можна побачити повторювані піки, поступове зростання трафіку або зміну характеру роботи мережі після налаштування обладнання. Такий підхід дозволяє використовувати систему як для щоденного контролю, так і для планування подальшого розвитку інфраструктури.

У процесі візуалізації важливо відображати вхідний і вихідний трафік окремо, оскільки ці показники можуть мати різну поведінку. Наприклад, для порту, підключеного до сервера, вихідний трафік може бути значно більшим за вхідний. Для користувацького сегмента, навпаки, вхідне навантаження може переважати над вихідним. Якщо ці показники аналізуються окремо, адміністратор може краще зрозуміти характер використання конкретного інтерфейсу.

Окреме значення має візуалізація пікових значень. Середнє навантаження не завжди показує реальний стан каналу, оскільки короткочасні перевантаження можуть згладжуватися. Графік дозволяє побачити моменти різкого зростання трафіку і порівняти їх із робочим часом, резервним копіюванням, оновленнями або іншими подіями в мережі. Це допомагає відрізнити нормальне планове навантаження від випадкових або небажаних відхилень.

$$L_i(t) = \frac{q_i(t)}{B_i} \cdot 100\backslash\%, \tag{3.2}$$

де $L_i(t)$ - рівень завантаження і-го інтерфейсу в момент часу t;

$q_i(t)$ - поточна інтенсивність трафіку на інтерфейсі;

B_i - максимальна пропускна здатність відповідного інтерфейсу.

Підсистема візуалізації також має відображати проблемні параметри, які не завжди пов’язані з великим обсягом трафіку. До таких параметрів належать помилки, відкинуті пакети та періоди недоступності вузла. Якщо на графіку видно, що кількість помилок зростає навіть за невеликого навантаження, це може вказувати на фізичну проблему з кабелем, портом або мережевим модулем. Якщо

відкинуті пакети з’являються лише під час піків, причиною може бути перевантаження інтерфейсу або нестача ресурсів обладнання.

Для зручності аналізу підсистема візуалізації повинна забезпечувати логічне групування графіків. Доцільно окремо формувати графіки для uplink-портів, користувацьких сегментів, серверних підключень і службових інтерфейсів. Такий поділ дозволяє швидше знайти потрібний фрагмент мережі та не переглядати зайві графіки. Особливо це важливо у випадках, коли система контролює декілька комутаційних вузлів і велику кількість портів.

Результати візуалізації мають бути доступні через веб-сторінки або локальний інтерфейс перегляду. Це спрощує роботу адміністратора, оскільки не потрібно вручну відкривати файли зі статистикою або виконувати команди для кожного пристрою. Підготовлені графіки дозволяють швидко оцінити стан мережі та перейти до аналізу конкретного вузла або інтерфейсу.

У підсумку, підсистему візуалізації розроблено як інструмент перетворення збережених статистичних даних у наочне представлення стану комутаційних вузлів. Вона забезпечує побудову графіків, перегляд параметрів за різні періоди, аналіз завантаження інтерфейсів, виявлення пікових навантажень, помилок і відкинутих пакетів. Завдяки цьому адміністратор отримує не набір розрізнених чисел, а зрозумілу картину роботи мережевої інфраструктури.

3.7 Розроблення механізмів контролю критичних станів і реагування

Механізми контролю критичних станів і реагування розроблено для того, щоб система віддаленого моніторингу не обмежувалася лише пасивним відображенням графіків, а давала можливість своєчасно виявляти проблемні ситуації в роботі комутаційних вузлів. У межах розробленої архітектури контроль критичних станів базується на аналізі параметрів, які надходять через SNMP, зберігаються у вигляді часових рядів і відображаються засобами MRTG. Основну увагу приділено таким ситуаціям, як перевантаження інтерфейсів, зростання

кількості помилок, збільшення відкинутих пакетів, втрата доступності вузла та повторювані відхилення в роботі мережі.

Під критичним станом у роботі комутаційного вузла розуміється ситуація, за якої один або кілька параметрів виходять за межі допустимого режиму та можуть впливати на стабільність функціонування мережевого сегмента. Наприклад, тривале завантаження uplink-інтерфейсу на рівні, близькому до максимальної пропускної здатності, може свідчити про ризик перевантаження. Зростання кількості помилок на порту може вказувати на фізичну проблему з кабелем або інтерфейсом. Втрата відповіді від вузла може бути ознакою відмови обладнання, проблеми живлення або порушення зв’язку.

Для зручності аналізу в розробленій системі доцільно виділяти три стани контрольованого параметра: нормальний, попереджувальний і критичний. Нормальний стан означає, що параметр перебуває в допустимих межах і не має ознак нестабільності. Попереджувальний стан фіксується тоді, коли параметр наближається до небажаного рівня або демонструє стійку негативну тенденцію. Критичний стан визначається у разі перевищення допустимого порогу, повторюваного порушення роботи або повної втрати доступності контрольованого вузла.

$$S_i(t) = \begin{cases} S_{\text{норм}}, & x_i(t) < x_i^{\text{поп}} \\ S_{\text{поп}}, & x_i^{\text{поп}} \le x_i(t) < x_i^{\text{кр}} \\ S_{\text{кр}}, & x_i(t) \ge x_i^{\text{кр}} \end{cases} \tag{3.3}$$

де $S_i(t)$ - стан і-го контрольованого параметра в момент часу t;

$x_i(t)$ - поточне значення і-го параметра;

$x_i^{\text{поп}}$ - попереджувальне порогове значення;

$x_i^{\text{кр}}$ - критичне порогове значення;

$S_{\text{норм}}$ - нормальний стан параметра;

$S_{\text{поп}}$ - попереджувальний стан;

$S_{\text{кр}}$ - критичний стан.

Для контролю завантаження інтерфейсів використовуються графіки вхідного та вихідного трафіку. Якщо навантаження короткочасно зростає, але швидко повертається до звичного рівня, така ситуація може бути пов’язана з нормальними процесами, наприклад передаванням великих файлів або резервним копіюванням. Якщо ж високе навантаження повторюється регулярно або триває протягом значного часу, це розглядається як ознака потенційного перевантаження. Особливо важливим є контроль uplink-портів, оскільки вони забезпечують зв’язок між сегментами мережі.

Окремий механізм контролю пов’язаний із помилками та відкинутими пакетами. Такі показники мають аналізуватися не ізольовано, а разом із рівнем трафіку. Якщо кількість помилок зростає за високого навантаження, імовірною причиною може бути перевантаження каналу або нестача ресурсів обладнання. Якщо помилки з’являються за невеликого трафіку, більше уваги потрібно приділяти фізичному стану лінії, порту або мережевого модуля. Такий підхід дозволяє точніше відрізняти логічні проблеми навантаження від фізичних несправностей.

Важливим критичним станом є втрата доступності комутаційного вузла. Якщо сервер моніторингу не отримує відповідь від пристрою, система фіксує відсутність даних. Така ситуація може мати різні причини: відключення живлення, збій обладнання, розрив зв’язку, помилка маршрутизації, блокування SNMP-запитів або неправильні параметри доступу. У розробленій системі така подія розглядається як одна з найбільш важливих, оскільки недоступність комутаційного вузла може вплинути на цілий сегмент мережі.

Механізм реагування на критичні стани побудовано як послідовність дій адміністратора на основі отриманих графіків і показників. У разі виявлення перевантаження може виконуватися перевірка активних підключень, перерозподіл трафіку, зміна схеми підключення або збільшення пропускної здатності каналу. Якщо система показує зростання помилок, перевіряється фізичне середовище передавання, кабель, порт, SFP-модуль або налаштування швидкості й дуплексу.

Якщо вузол недоступний, першочергово перевіряються живлення, канал зв’язку, маршрутизація та параметри керування.

Для зручності в межах системи контроль критичних станів можна подати як цикл: отримання параметра, порівняння з допустимими межами, визначення стану, перегляд графіка, прийняття рішення, реагування, повторна перевірка результату. Такий цикл дозволяє не тільки виявити проблему, а й оцінити наслідки виконаних дій. Якщо після зміни конфігурації або перевірки обладнання графіки показують зниження навантаження чи зникнення помилок, це підтверджує ефективність реагування.

3.8 Висновки до розділу 3

У розділі було розроблено архітектуру кіберфізичної системи віддаленого моніторингу комутаційних вузлів мережі на основі MRTG. Визначено, що система має будуватися як сукупність взаємопов’язаних рівнів, до яких належать фізичні мережеві пристрої, комунікаційний рівень збору параметрів, сервер моніторингу, сховище часових рядів, підсистема візуалізації та механізм реагування адміністратора на виявлені події. Такий підхід дозволив сформувати цілісну архітектуру, у якій стан фізичного обладнання регулярно перетворюється на цифрові показники для подальшого аналізу.

У межах архітектури було визначено склад кіберфізичної системи віддаленого моніторингу. До її основних компонентів віднесено комутаційні вузли, SNMP-збір параметрів, сервер моніторингу MRTG, сховище статистичних даних, графіки та звіти, адміністратора мережі й дії реагування. Запропонована структура показує, що MRTG є центральним програмним компонентом системи, але повноцінна робота рішення забезпечується лише за умови узгодженої взаємодії всіх рівнів.

Було розроблено структуру взаємодії комутаційних вузлів і сервера моніторингу. У цій структурі комутаційні вузли формують первинні параметри, SNMP-агенти надають доступ до них, сервер MRTG виконує періодичне

опитування, а отримані значення передаються на обробку та зберігання. Такий підхід дозволив описати контрольовану взаємодію між фізичним обладнанням і програмною частиною системи, де кожне значення пов’язується з конкретним вузлом, інтерфейсом, типом параметра та часовою міткою.

Окремо було розроблено інформаційні потоки в системі моніторингу. Визначено шлях даних від фізичного стану комутаційного вузла до графічного представлення результатів. Первинні параметри проходять через SNMP-агент, сервер MRTG, блок обробки, сховище часових рядів і підсистему візуалізації, після чого стають доступними адміністратору у вигляді графіків і звітів. Така побудова забезпечує логічну послідовність руху даних і дозволяє уникнути втрати зв’язку між фізичним джерелом параметра та його цифровим відображенням.

Було розроблено підсистему збору параметрів через SNMP. Її призначення полягає в регулярному отриманні значень із комутаційних вузлів, перевірці наявності відповіді, фіксації часу отримання даних і передаванні результатів до подальшої обробки. У підсистемі враховано набір контрольованих вузлів, параметри доступу, перелік SNMP-запитів, інтервал опитування та можливі помилки під час звернення до обладнання. Це дозволило сформувати стійкий механізм збору даних, який не зупиняє роботу всієї системи у разі недоступності окремого вузла.

У розділі також було розроблено підсистему зберігання та обробки статистичних даних. Показано, що отримані значення мають зберігатися не як випадковий набір чисел, а як часові ряди, прив’язані до конкретного вузла, інтерфейсу, параметра та моменту часу. Такий підхід дозволяє аналізувати не лише поточний стан мережі, а й динаміку зміни параметрів за попередні періоди.

Було розроблено підсистему візуалізації результатів моніторингу. Її призначення полягає у перетворенні часових рядів на графіки та звіти, зручні для адміністратора. Візуальне представлення дозволяє швидко оцінити навантаження інтерфейсів, помітити пікові значення, виявити нетипові зміни трафіку, зростання кількості помилок або відкинутих пакетів.

4 РЕАЛІЗАЦІЯ ТА ПЕРЕВІРКА КІБЕРФІЗИЧНОЇ СИСТЕМИ ВІДДАЛЕНОГО МОНІТОРИНГУ КОМУТАЦІЙНИХ ВУЗЛІВ

4.1 Вибір програмно-апаратних компонентів реалізованої системи

Для реалізації кіберфізичної системи віддаленого моніторингу комутаційних вузлів було обрано програмні та апаратні компоненти, які забезпечують збір параметрів із мережевого обладнання, їх обробку, зберігання, побудову графіків і перегляд результатів адміністратором. Вибір компонентів виконано з урахуванням теми роботи, у якій основним засобом моніторингу визначено MRTG, а базовим механізмом отримання параметрів із мережевих пристроїв - SNMP.

Апаратну основу реалізованої системи становлять комутаційні вузли мережі, сервер моніторингу та робоче місце адміністратора. Комутаційні вузли виступають фізичними об’єктами контролю, з яких отримуються показники стану інтерфейсів, вхідного й вихідного трафіку, помилок, відкинутих пакетів і доступності. Сервер моніторингу виконує роль центрального елемента програмного контуру, на якому налаштовано збір, обробку, зберігання та візуалізацію параметрів. Робоче місце адміністратора використовується для перегляду сформованих графіків і прийняття рішень щодо подальших дій.

До складу реалізованої системи включено комутаційні вузли, які підтримують роботу SNMP-агента. Це є обов’язковою умовою, оскільки без підтримки SNMP сервер моніторингу не може отримувати параметри пристрою у стандартизованому вигляді. Для кожного контрольованого вузла було визначено IP-адресу, перелік інтерфейсів, які підлягають моніторингу, та параметри доступу до SNMP. Основну увагу приділено тим портам, через які проходить найбільший обсяг трафіку, зокрема uplink-з’єднанням і портам, що обслуговують важливі сегменти мережі.

Сервер моніторингу реалізовано як окремий вузол, на якому встановлено необхідні програмні засоби. Його призначення полягає в періодичному опитуванні комутаційних вузлів, отриманні значень параметрів, обробці результатів і формуванні графіків. Для стабільної роботи сервер повинен мати постійний доступ

до мережі керування, достатній обсяг дискового простору для збереження статистики та можливість запуску служб, які забезпечують роботу MRTG і веб-перегляд результатів.

Основним програмним компонентом обрано MRTG. Його використання обґрунтовано тим, що він напряму відповідає задачі роботи: дозволяє отримувати параметри з мережевих пристроїв через SNMP, формувати часові графіки та створювати HTML-сторінки для перегляду результатів. MRTG не потребує складної серверної інфраструктури, має зрозумілу конфігураційну логіку та добре підходить для демонстрації принципу роботи кіберфізичної системи моніторингу комутаційних вузлів.

Для збереження статистичних даних використано підхід часових рядів. Його перевага полягає в тому, що кожне значення параметра зберігається разом із часовою прив’язкою. Завдяки цьому система може відображати не лише поточний стан інтерфейсу, а й історію зміни навантаження. Це важливо для аналізу пікових періодів, повторюваних відхилень, поступового зростання трафіку та оцінки стабільності роботи мережевого обладнання.

Для перегляду результатів моніторингу використано веб-компонент. Він забезпечує доступ до сформованих сторінок і графіків через браузер адміністратора. Такий спосіб подання результатів є зручним, оскільки адміністратору не потрібно працювати безпосередньо з конфігураційними файлами або службовими даними. Достатньо відкрити сторінку моніторингу, вибрати потрібний вузол чи інтерфейс і переглянути графік зміни параметрів за визначений період.

У межах реалізації було також враховано вимоги до безпеки доступу. SNMP-доступ до комутаційних вузлів налаштовано так, щоб параметри могли отримуватися лише з боку сервера моніторингу. Це зменшує ризик несанкціонованого звернення до службових параметрів обладнання. Веб-доступ до результатів моніторингу також має бути обмежений для сторонніх користувачів, оскільки графіки трафіку та дані про стан вузлів можуть розкривати особливості роботи мережевої інфраструктури.

Використання такої сукупності компонентів дозволило реалізувати повний цикл роботи системи: від отримання параметрів із фізичного комутаційного вузла до перегляду графічного результату адміністратором. Комутаційні вузли формують первинні дані, SNMP забезпечує їх передавання, MRTG виконує обробку та побудову графіків, а веб-компонент надає доступ до результатів. Це відповідає розробленій у попередньому розділі архітектурі та підтверджує практичну завершеність системи.

У підсумку, для реалізації кіберфізичної системи віддаленого моніторингу було обрано компоненти, які забезпечують простоту розгортання, достатню функціональність і відповідність поставленій задачі. Основу системи становлять комутаційні вузли з підтримкою SNMP, сервер моніторингу з налаштованим MRTG, сховище часових рядів і веб-інтерфейс перегляду результатів. Така конфігурація дозволяє здійснювати віддалений контроль стану мережевої інфраструктури та використовувати отримані дані для подальшого аналізу.

4.2 Налаштування SNMP-доступу до комутаційних вузлів

Для забезпечення віддаленого збору параметрів із комутаційних вузлів було виконано налаштування SNMP-доступу. Цей етап є одним із ключових у реалізації системи, оскільки саме через SNMP сервер моніторингу отримує значення трафіку, стану інтерфейсів, помилок, відкинутих пакетів і доступності обладнання. Без коректного налаштування SNMP робота MRTG була б неможливою, оскільки сервер не мав би доступу до первинних параметрів фізичних мережевих пристроїв.

Перед налаштуванням SNMP було визначено перелік комутаційних вузлів, які підлягають моніторингу. Для кожного пристрою було зафіксовано IP-адресу, роль у мережевій інфраструктурі, перелік важливих інтерфейсів і тип параметрів, які необхідно отримувати. Основну увагу приділено uplink-портам, через які проходить основний трафік між сегментами мережі, а також портам, що використовуються для підключення важливих пристроїв або серверних ресурсів.

Налаштування SNMP-доступу виконано з урахуванням принципу мінімально необхідного доступу. Сервер моніторингу отримує можливість зчитувати параметри обладнання, але не виконує зміну конфігурації комутаційних вузлів. Такий підхід є доцільним, оскільки система призначена для моніторингу, а не для віддаленого адміністрування конфігурацій. Це зменшує ризики випадкового або несанкціонованого впливу на роботу мережевого обладнання.

У процесі налаштування було активовано SNMP-агент на комутаційних вузлах, задано параметри доступу та обмежено коло пристроїв, які можуть надсилати SNMP-запити. Як дозволене джерело запитів використано сервер моніторингу. Це дозволило запобігти ситуації, коли сторонні пристрої можуть отримувати службову інформацію про мережеву інфраструктуру. Додатково було враховано, що статистичні параметри мережі можуть розкривати структуру трафіку, тому доступ до них має бути контрольованим.

Загальна логіка налаштування SNMP-доступу включала такі дії: увімкнення SNMP-служби на пристрої, задання параметрів доступу, обмеження доступу за IP-адресою сервера моніторингу, перевірку відповіді від пристрою та контроль доступності потрібних параметрів. Після цього виконувалася перевірка, чи сервер моніторингу може отримувати значення лічильників інтерфейсів і чи ці значення відповідають фактичним портам обладнання.

Фрагмент узагальнених параметрів налаштування SNMP-доступу подано нижче.

```
SNMP service: enabled
Allowed manager: IP-адреса сервера моніторингу
Access mode: read-only
Monitored objects: interface traffic, interface status, errors, discards
Polling source: MRTG server
```

Наведений фрагмент відображає загальний принцип конфігурації, який застосовано під час реалізації системи. Важливим є те, що доступ налаштовано лише для читання. Це дозволяє отримувати параметри для моніторингу, але не надає серверу моніторингу прав на зміну конфігурації комутаційного вузла.

Після налаштування SNMP-доступу було виконано перевірку доступності комутаційних вузлів із сервера моніторингу. Перевірка підтвердила можливість отримання відповідей від SNMP-агентів і доступність основних параметрів інтерфейсів. На цьому етапі особливу увагу приділено відповідності назв і номерів портів, оскільки неправильна прив’язка інтерфейсу могла б призвести до побудови графіка не для того порту, який фактично потрібно контролювати.

Для кожного комутаційного вузла було визначено перелік інтерфейсів, які включено до моніторингу. Не всі порти мають однакове значення для аналізу стану мережі, тому до основного набору потрапили інтерфейси з найбільшим практичним значенням.

Для перевірки доступності параметрів використовувався запит до SNMP-агента, після якого аналізувалась відповідь пристрою (таблиця 4.1). Якщо відповідь була отримана, параметр вважався доступним для подальшого використання в MRTG. Якщо відповідь не надходила або значення не відповідало очікуваному параметру, виконувалася перевірка налаштувань доступу, правильності IP-адреси, доступності пристрою в мережі та коректності вибраного об’єкта моніторингу.

Таблиця 4.1 – Параметри налаштування SNMP-доступу до комутаційних вузлів

Параметр	Призначення	Результат налаштування
IP-адреса пристрою	Ідентифікація комутаційного вузла в мережі	Сервер моніторингу звертається до потрібного вузла
SNMP-агент	Надання параметрів стану обладнання	Пристрій відповідає на запити моніторингу
Режим доступу	Обмеження прав сервера моніторингу	Використано доступ лише для читання
Дозволене джерело запитів	Захист від стороннього доступу	Запити дозволено лише з боку сервера моніторингу
Контрольовані інтерфейси	Вибір портів для моніторингу	До моніторингу включено важливі uplink- і службові порти
Перелік параметрів	Визначення даних для збору	Отримуються трафік, помилки, відкинуті пакети та стан портів

Після завершення налаштування SNMP-доступу було сформовано основу для подальшого конфігурування MRTG. Сервер моніторингу отримав можливість регулярно звертатися до комутаційних вузлів і зчитувати потрібні параметри. Це дозволило перейти до створення конфігураційних файлів MRTG, у яких визначаються конкретні вузли, інтерфейси, назви графіків і шляхи збереження результатів.

У підсумку, налаштування SNMP-доступу забезпечило зв’язок між фізичними комутаційними вузлами та програмним контуром моніторингу. Було активовано можливість отримання параметрів із мережевого обладнання, обмежено доступ до SNMP-запитів, визначено контрольовані інтерфейси та перевірено доступність потрібних показників. Це створило практичну основу для подальшого конфігурування MRTG і побудови графіків стану мережевої інфраструктури.

4.3 Конфігурування MRTG для збору мережевих параметрів

Після налаштування SNMP-доступу було виконано конфігурування MRTG для збору мережевих параметрів із комутаційних вузлів. Цей етап є основним у практичній реалізації системи, оскільки саме MRTG виконує регулярне опитування обладнання, отримує значення параметрів, обробляє їх і формує графіки для подальшого перегляду адміністратором. У межах реалізованої системи MRTG використано як центральний програмний компонент моніторингу.

Конфігурування MRTG виконано після перевірки доступності комутаційних вузлів через SNMP. Спочатку було визначено перелік пристроїв, які включено до моніторингу, після чого для кожного з них підготовлено параметри доступу, IP-адреси, назви інтерфейсів і цільові показники. Основну увагу приділено портам, які мають найбільше значення для стабільності мережі: uplink-інтерфейсам, портам підключення серверних ресурсів і портам, через які проходить основний робочий трафік.

Для формування конфігурації MRTG було використано підхід, за якого кожен контрольований інтерфейс описується окремим блоком. У такому блоці задається джерело даних, назва графіка, максимальне значення для інтерфейсу, шлях до сторінки результату та пояснювальні підписи. Це дозволяє зробити структуру конфігурації зрозумілою і придатною для подальшого розширення. У разі додавання нового комутаційного вузла або нового порту достатньо створити ще один конфігураційний блок.

Узагальнений приклад конфігураційного блоку MRTG подано нижче.

```
Target[switch1_port1]: 1:public@192.168.1.10
MaxBytes[switch1_port1]: 125000000
Title[switch1_port1]: Моніторинг порту 1 комутатора Switch-1
PageTop[switch1_port1]: <h1>Порт 1 комутатора Switch-1</h1>
Options[switch1_port1]: growright,bits
YLegend[switch1_port1]: Трафік, біт/с
ShortLegend[switch1_port1]: біт/с
LegendI[switch1_port1]: Вхідний трафік
LegendO[switch1_port1]: Вихідний трафік
```

Наведений фрагмент показує загальну логіку налаштування одного контрольованого інтерфейсу. У параметрі Target визначається порт, SNMP-параметр доступу та IP-адреса комутаційного вузла. Параметр MaxBytes задає максимальну пропускну здатність інтерфейсу в байтах за секунду. Поля Title, PageTop, YLegend, LegendI і LegendO використовуються для оформлення графіка та пояснення того, які саме дані відображаються.

Під час конфігурування було враховано, що MRTG відображає вхідний і вихідний трафік окремо. Це важливо для аналізу роботи комутаційних вузлів, оскільки характер використання інтерфейсу може бути різним у двох напрямах. Наприклад, порт, підключений до сервера, може мати значний вихідний трафік, тоді як користувацький порт частіше має переважання вхідного потоку. Окреме відображення цих напрямів дозволяє точніше оцінити реальне навантаження.

Для зручності перегляду результатів було задано зрозумілі назви графіків і сторінок. Назви сформовано так, щоб адміністратор міг швидко визначити, до

якого комутатора та порту належить конкретний графік. Це особливо важливо у випадках, коли система контролює кілька пристроїв одночасно. Якщо графіки мають нечіткі або технічні назви, аналіз результатів ускладнюється, тому в конфігурації використано зрозуміле позначення вузлів та інтерфейсів.

Окремо було налаштовано інтервал запуску MRTG. Періодичність опитування визначає, як часто система отримує нові значення параметрів із комутаційних вузлів. Для контролю мережевого трафіку використано регулярний цикл збору, який дозволяє формувати послідовність значень і будувати графіки зміни навантаження в часі. Такий підхід дає змогу фіксувати як поточний стан інтерфейсів, так і поступові зміни в роботі мережі.

Після створення конфігураційного файлу було виконано тестовий запуск MRTG. На цьому етапі перевірено правильність параметрів доступу, доступність комутаційних вузлів, коректність вибраних інтерфейсів і можливість створення графіків. У разі помилок перевірялися IP-адреси пристроїв, параметри SNMP-доступу, номери інтерфейсів і права доступу до каталогу, у якому зберігаються результати роботи MRTG.

Для автоматизації роботи було налаштовано регулярний запуск MRTG. Це дозволило системі працювати без ручного запуску кожного циклу опитування. Після налаштування автоматичного виконання сервер моніторингу самостійно звертається до комутаційних вузлів, оновлює статистику та формує нові графіки. Унаслідок цього адміністратор отримує актуальну інформацію про стан мережі без необхідності вручну запускати збір даних.

У процесі конфігурування також було визначено каталог для збереження HTML-сторінок і графічних файлів. Це потрібно для подальшого перегляду результатів через веб-компонент. MRTG формує сторінки, на яких відображаються графіки за різні часові періоди, що дозволяє аналізувати поточне навантаження, короткострокову динаміку та довші тенденції зміни трафіку.

Після завершення конфігурування MRTG було отримано перші графіки трафіку для контрольованих інтерфейсів. Це підтвердило працездатність зв’язку між комутаційними вузлами, SNMP-збором і сервером моніторингу. Отримані

графіки стали основою для подальшого аналізу навантаження, виявлення пікових періодів і перевірки стабільності роботи обраних мережевих портів.

4.4 Реалізація зберігання статистичних даних і формування графіків

Після конфігурування MRTG було реалізовано зберігання статистичних даних і формування графіків для контрольованих комутаційних вузлів. Цей етап є важливим для практичної роботи системи, оскільки саме він забезпечує перехід від окремих SNMP-відповідей до повноцінної історії зміни мережевих параметрів. У результаті адміністратор отримує не лише поточне значення трафіку, а й можливість переглядати динаміку роботи інтерфейсів за різні часові періоди.

Зберігання статистики реалізовано на основі часової прив’язки отриманих параметрів. Кожне значення, отримане під час чергового циклу опитування, пов’язується з конкретним комутаційним вузлом, інтерфейсом і моментом часу. Такий підхід дозволяє формувати часові ряди для кожного контрольованого параметра. Для одного інтерфейсу можуть накопичуватися окремі ряди для вхідного трафіку, вихідного трафіку, помилок або відкинутих пакетів.

Особливістю реалізації є те, що більшість параметрів трафіку надходить від мережевого обладнання у вигляді накопичувальних лічильників. Тому перед побудовою графіків такі значення мають бути оброблені. MRTG порівнює поточне значення лічильника з попереднім і визначає зміну параметра за інтервал опитування. Унаслідок цього на графіку відображається не загальна кількість переданих байтів, а інтенсивність трафіку за певний проміжок часу.

Для збереження результатів було задано робочий каталог, у якому формуються службові файли, HTML-сторінки та графічні зображення. У цьому каталозі зберігаються дані, необхідні для оновлення графіків і перегляду результатів моніторингу. Структура каталогу організована так, щоб для кожного контрольованого вузла або інтерфейсу можна було швидко знайти відповідні графіки та сторінки перегляду.

Фрагмент налаштування робочого каталогу і параметрів відображення подано нижче.

```
WorkDir: /var/www/html/mrtg
Options[_]: growright,bits
RunAsDaemon: Yes
Interval: 5
```

Параметр WorkDir визначає місце збереження сформованих HTML-сторінок і графіків. Параметр Options задає загальні особливості відображення графіків, зокрема напрям побудови та одиниці вимірювання. Параметр RunAsDaemon використовується для організації постійної роботи MRTG, а Interval визначає періодичність оновлення статистики.

Формування графіків реалізовано автоматично після кожного циклу збору даних. Система отримує нові значення параметрів, оновлює часові записи та перебудовує графічне представлення. У результаті на сторінках моніторингу відображаються актуальні графіки, які показують зміну вхідного та вихідного трафіку. Для кожного інтерфейсу формується окремий набір графіків, що дозволяє аналізувати стан конкретного порту без змішування з іншими даними.

У процесі реалізації було враховано потребу в перегляді статистики за різні часові проміжки. Короткострокові графіки дають можливість оцінити поточну ситуацію, а довші періоди дозволяють побачити загальну тенденцію навантаження. Це корисно для виявлення повторюваних піків, поступового зростання трафіку або зміни режиму роботи мережі після внесення налаштувань.

Сформовані графіки використовуються для оцінювання завантаження інтерфейсів. Якщо графік показує стабільне навантаження в межах допустимого рівня, робота інтерфейсу вважається нормальною. Якщо ж навантаження регулярно наближається до максимальної пропускної здатності, це може свідчити про потребу в оптимізації або модернізації каналу. Різкі короткочасні піки можуть бути пов’язані з окремими процесами передавання даних, резервним копіюванням або нетиповою активністю в мережі.

Окремо було реалізовано можливість перегляду вхідного та вихідного трафіку на одному графіку. Це дозволяє порівнювати характер використання інтерфейсу в обох напрямах. Для деяких портів вхідний і вихідний трафік можуть бути приблизно рівними, а для інших один напрям може переважати. Така інформація допомагає краще зрозуміти роль конкретного інтерфейсу в мережевій інфраструктурі.

Для зручності подання результатів було використано зрозумілі заголовки графіків. У назві вказується комутаційний вузол, порт або призначення інтерфейсу. Це спрощує навігацію між сторінками моніторингу та зменшує ризик помилкового аналізу не того порту. Особливо це важливо у випадку, коли система контролює кілька комутаторів або значну кількість інтерфейсів.

Реалізований механізм зберігання та формування графіків підтвердив практичну працездатність обраної архітектури. Дані, отримані з комутаційних вузлів через SNMP, не залишаються окремими службовими значеннями, а перетворюються на візуальну історію роботи мережі. Це дозволяє використовувати систему не тільки для оперативного перегляду стану інтерфейсів, а й для аналізу змін у роботі мережевої інфраструктури.

У підсумку, у межах реалізованої системи було забезпечено збереження статистичних даних, їх часову прив’язку, автоматичне оновлення графіків і підготовку результатів до веб-перегляду. Це дало змогу сформувати практичний інструмент для аналізу трафіку, виявлення пікових навантажень і оцінювання стабільності роботи комутаційних вузлів.

4.5 Реалізація веб-інтерфейсу перегляду результатів моніторингу

Для зручного перегляду результатів моніторингу було реалізовано веб-доступ до сформованих графіків і сторінок MRTG. Такий підхід дозволив адміністратору переглядати стан комутаційних вузлів через браузер без безпосередньої роботи з конфігураційними файлами, службовими каталогами або консольними командами. У результаті система стала більш зручною для

практичного використання, оскільки основні результати збору й обробки параметрів подаються у вигляді готових веб-сторінок.

Веб-доступ реалізовано через каталог, у якому MRTG зберігає HTML-сторінки та графічні файли. Після кожного циклу опитування комутаційних вузлів графіки оновлюються, а адміністратор отримує можливість переглянути актуальні значення трафіку та історію зміни параметрів. Такий спосіб роботи є зручним, оскільки результати моніторингу не потребують додаткового перетворення перед переглядом. Система автоматично формує сторінки, які можна відкрити з робочого місця адміністратора.

У процесі реалізації було визначено робочий каталог для збереження результатів MRTG. Саме в ньому розміщуються сторінки для кожного контрольованого інтерфейсу, графіки вхідного та вихідного трафіку, службові файли оновлення статистики й загальна сторінка перегляду. Така організація дозволяє структурувати результати моніторингу та швидко знаходити потрібний комутаційний вузол або порт.

Узагальнений приклад налаштування каталогу для веб-доступу подано нижче.

```
WorkDir: /var/www/html/mrtg
```

Цей параметр визначає місце, куди MRTG записує сформовані HTML-сторінки та графіки. Після налаштування веб-сервера адміністратор може відкривати результати моніторингу через браузер. У практичній реалізації це спрощує роботу з системою, оскільки всі графіки доступні в одному середовищі перегляду.

Для зручної навігації між графіками було сформовано загальну сторінку індексу. Вона дозволяє перейти до потрібного вузла або інтерфейсу без ручного пошуку окремих HTML-файлів у каталозі. У такій сторінці доцільно розміщувати назви комутаторів, номери портів, короткий опис призначення інтерфейсу та посилання на відповідні графіки. Це особливо важливо тоді, коли система контролює декілька пристроїв і значну кількість портів.

Фрагмент команди для формування індексної сторінки може мати такий вигляд:

```
indexmaker /etc/mrtg.cfg > /var/www/html/mrtg/index.html
```

Після виконання такої дії створюється сторінка, яка об’єднує результати моніторингу в єдиному місці. Це робить перегляд результатів більш зручним і зменшує кількість ручних дій адміністратора. Замість відкриття окремих файлів можна перейти на головну сторінку MRTG і вибрати потрібний графік.

Важливим елементом реалізації веб-доступу є налаштування прав доступу до каталогу з результатами. Веб-сервер повинен мати можливість читати HTML-сторінки та графічні файли, а MRTG - записувати оновлені результати. Якщо права доступу налаштовано неправильно, графіки можуть не оновлюватися або сторінки можуть бути недоступними через браузер. Через це на етапі реалізації було перевірено можливість створення файлів, їх оновлення та відкриття через веб-інтерфейс.

Окрему увагу приділено обмеженню доступу до сторінок моніторингу. Дані про трафік, активність портів і доступність вузлів можуть розкривати особливості роботи мережевої інфраструктури, тому такі сторінки не повинні бути відкритими для сторонніх користувачів. Веб-доступ до результатів доцільно обмежувати локальною мережею керування, окремими IP-адресами або механізмом автентифікації. Це дозволяє забезпечити зручність перегляду без зайвого ризику для безпеки мережі.

У реалізованій системі веб-сторінки виконують роль кінцевого інтерфейсу перегляду результатів. Вони не змінюють конфігурацію комутаційних вузлів і не впливають на роботу SNMP-збору, а лише відображають уже підготовлені дані. Це зручно з погляду безпеки, оскільки користувач веб-сторінки переглядає результати моніторингу, але не отримує прямого доступу до керування обладнанням.

Через веб-інтерфейс адміністратор може переглядати графіки за різні часові періоди. Це дозволяє оцінити поточний стан інтерфейсу, побачити короткострокові піки, проаналізувати добову динаміку або визначити довші тенденції зміни навантаження. Наявність таких графіків у браузері робить систему практично

придатною для щоденного використання, оскільки не потрібно щоразу виконувати окремі команди для отримання статистики.

4.6 Перевірка працездатності системи на контрольованих мережевих вузлах

Після налаштування SNMP-доступу, конфігурування MRTG, збереження статистичних даних і реалізації веб-доступу було виконано перевірку працездатності кіберфізичної системи віддаленого моніторингу. Метою перевірки було підтвердження того, що всі основні компоненти системи працюють узгоджено: комутаційні вузли надають параметри через SNMP, сервер моніторингу отримує ці параметри, MRTG обробляє значення, графіки оновлюються, а адміністратор має доступ до результатів через веб-інтерфейс.

Перевірка виконувалася поетапно. Спочатку було перевірено доступність контрольованих комутаційних вузлів із сервера моніторингу. Для цього використовувалася мережева перевірка з’єднання, яка дозволила переконатися, що сервер має доступ до IP-адрес пристроїв. Після цього було перевірено роботу SNMP-агента на кожному вузлі. Якщо пристрій відповідав на SNMP-запит, він вважався доступним для подальшого моніторингу.

Наступним етапом стала перевірка отримання параметрів інтерфейсів. Було перевірено, чи сервер моніторингу може отримати значення вхідного та вихідного трафіку, стан портів, кількість помилок і відкинутих пакетів. Особливу увагу приділено відповідності отриманих параметрів реальним портам обладнання. Це важливо, оскільки помилкова прив’язка інтерфейсу може призвести до побудови графіка, який не відповідає потрібному фрагменту мережі.

Після перевірки SNMP-відповідей було виконано тестовий запуск MRTG. На цьому етапі система зчитала параметри з контрольованих вузлів, створила службові файли статистики, сформувала HTML-сторінки та побудувала перші графіки. Наявність графіків підтвердила, що дані успішно проходять увесь шлях: від комутаційного вузла до веб-представлення результатів.

Окремо було перевірено оновлення графіків після повторних циклів опитування. Для цього результати переглядалися через певний проміжок часу після запуску системи. Було встановлено, що графіки оновлюються, нові значення додаються до історії, а система коректно відображає зміну трафіку в часі. Це підтвердило працездатність механізму періодичного збору та збереження статистичних даних.

У процесі перевірки було також оцінено поведінку системи у випадку тимчасової недоступності вузла. Якщо пристрій не відповідав на запит, система не припиняла роботу повністю, а продовжувала обробку інших контрольованих інтерфейсів. Така поведінка є важливою для практичної експлуатації, оскільки відмова одного пристрою не повинна порушувати моніторинг решти мережевої інфраструктури.

Результати перевірки показали, що реалізована система забезпечує базові функції віддаленого моніторингу комутаційних вузлів. Було підтверджено отримання параметрів через SNMP, формування часових значень, побудову графіків і доступ до результатів через веб-інтерфейс. Це дозволяє використовувати систему для контролю стану інтерфейсів, аналізу трафіку та виявлення ознак перевантаження або нестабільної роботи мережі.

У підсумку, перевірка працездатності підтвердила, що реалізована система виконує поставлені функції та забезпечує зв’язок між фізичними комутаційними вузлами і програмним контуром моніторингу. Отримані результати свідчать про практичну придатність розробленого рішення для віддаленого контролю мережевої інфраструктури.

4.7 Аналіз результатів роботи системи моніторингу

Після перевірки працездатності системи було виконано аналіз результатів її роботи. Основну увагу приділено тому, наскільки реалізована система забезпечує віддалений контроль стану комутаційних вузлів, чи коректно відображає зміну

мережевих параметрів у часі та чи може використовуватися адміністратором для виявлення перевантажень, помилок або нестабільної роботи інтерфейсів.

У результаті роботи системи було отримано графіки вхідного та вихідного трафіку для контрольованих інтерфейсів. Такі графіки дозволили оцінити характер використання мережевих портів, визначити періоди підвищеного навантаження та порівняти активність різних напрямів передавання даних. Для комутаційних вузлів це має важливе практичне значення, оскільки саме інтерфейси відображають реальну інтенсивність роботи мережі.

Аналіз графіків показав, що система дозволяє візуально відрізняти нормальний режим роботи інтерфейсу від потенційно проблемного. У нормальному режимі навантаження змінюється поступово, не наближається до граничної пропускної здатності та не супроводжується різкими стрибками. Якщо ж на графіку спостерігаються регулярні піки, тривале високе навантаження або різкі нетипові зміни, це може бути підставою для додаткової перевірки відповідного сегмента мережі.

Окремо було проаналізовано значення вхідного та вихідного трафіку. У деяких випадках один напрям передавання може переважати над іншим, що є нормальним для певних типів підключень. Наприклад, серверний порт може мати більший вихідний трафік, а користувацький сегмент - більший вхідний. Завдяки окремому відображенню двох напрямів адміністратор може точніше оцінити характер використання інтерфейсу та визначити, чи відповідає він очікуваній ролі порту в мережі.

Важливим результатом роботи системи є можливість перегляду історії зміни параметрів. На відміну від разової перевірки стану обладнання, графіки MRTG дозволяють аналізувати поведінку інтерфейсів протягом певного періоду. Це допомагає визначити, чи було навантаження випадковим, регулярним або поступово зростаючим. Такий підхід є корисним для планування модернізації мережі, пошуку причин перевантажень і оцінювання наслідків змін у конфігурації.

У межах аналізу також було враховано показники помилок і відкинутих пакетів. Якщо такі значення залишаються на низькому рівні, це свідчить про

стабільну роботу інтерфейсу. Якщо ж кількість помилок або відкидань зростає, необхідно перевіряти фізичне середовище, якість кабельного підключення, стан порту або рівень навантаження на канал. Поєднання графіків трафіку з показниками якості передавання дозволяє точніше визначити характер можливої проблеми.(Рисунок 4.1-4.3)

Для узагальнення результатів роботи системи було визначено основні критерії оцінювання.

До них належать доступність контрольованих вузлів, коректність отримання SNMP-параметрів, регулярність оновлення графіків, зрозумілість візуального представлення, можливість перегляду історії та практична придатність результатів для адміністратора.

Такі критерії дозволяють оцінити систему не лише з технічного боку, а й з погляду її використання в реальній експлуатації.

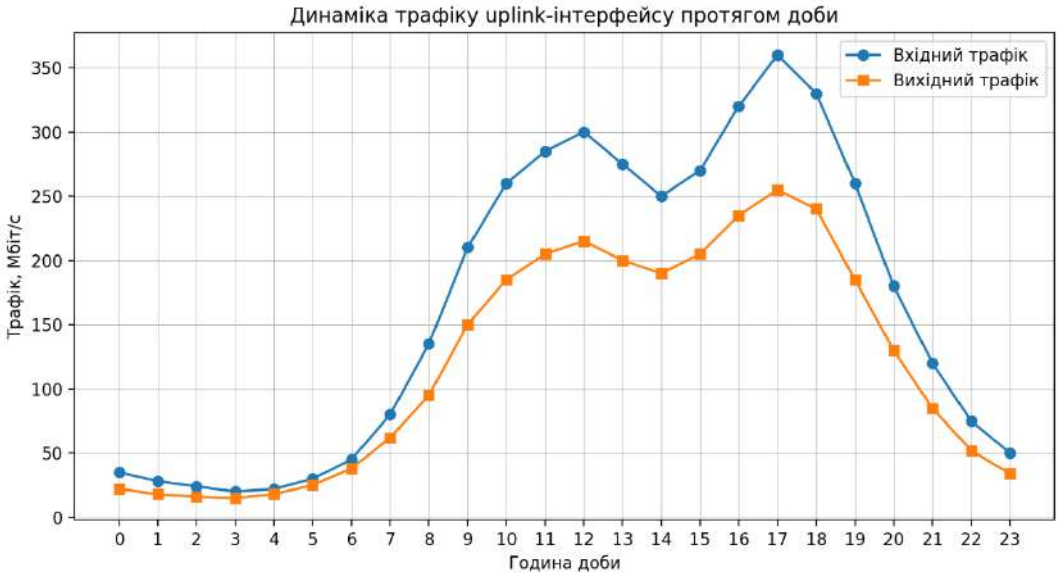


Рисунок 4.1 – Динаміка трафіку uplink-інтерфейсу протягом доби

Отримані результати підтвердили, що система може використовуватися як інструмент оперативного контролю. Адміністратор має можливість переглянути стан потрібного інтерфейсу, оцінити завантаження, побачити нетипові піки та визначити, чи потребує конкретний порт додаткової перевірки. Це особливо

корисно для uplink-інтерфейсів, оскільки їх перевантаження може впливати на роботу значної частини мережі.

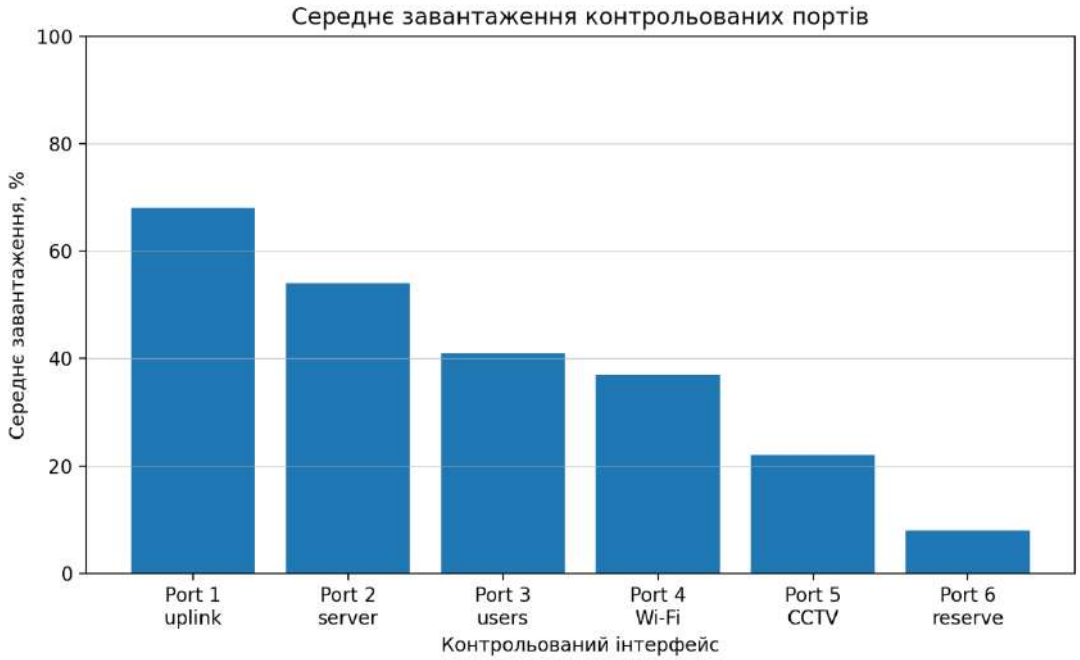


Рисунок 4.2 – Середнє завантаження контрольованих портів

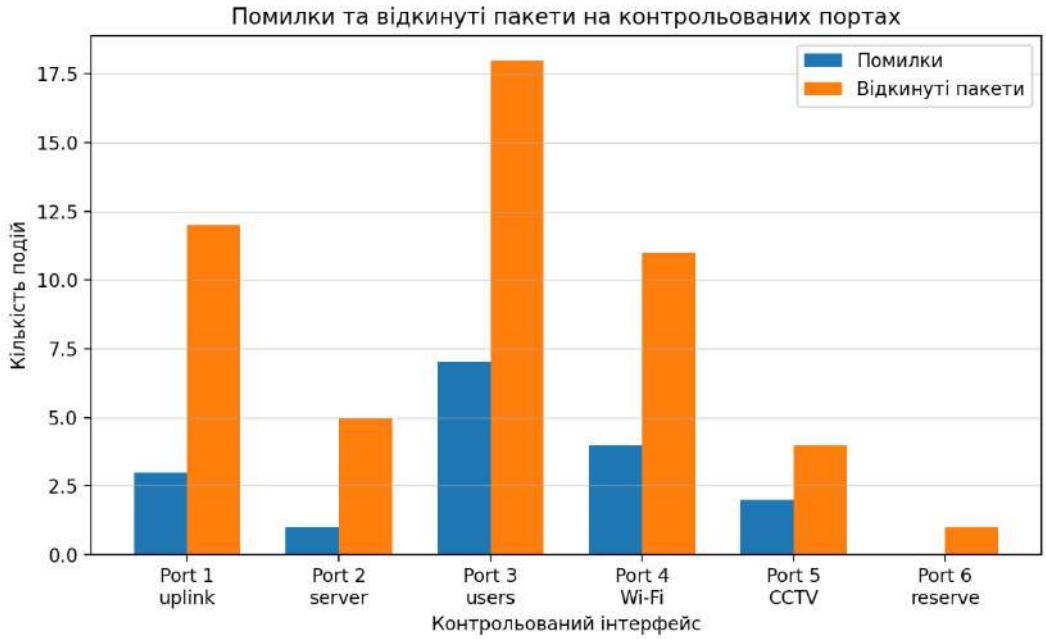


Рисунок 4.3 – Помилки та відкинуті пакети на контрольованих портах

Разом із цим аналіз показав, що система має найбільшу практичну цінність у поєднанні з досвідом адміністратора. MRTG формує графіки й показує зміну

параметрів, але остаточне рішення щодо причин відхилення приймається після аналізу контексту. Наприклад, короткочасний пік може бути нормальним під час резервного копіювання, а може вказувати на небажану активність. Тому результати моніторингу доцільно розглядати як інформаційну основу для подальших дій, а не як автоматичний висновок про причину проблеми.

Практична користь реалізованої системи полягає також у тому, що вона зменшує залежність від ручної перевірки обладнання. Замість періодичного входу на кожен комутатор адміністратор отримує централізований перегляд графіків і може швидше визначити, який вузол або інтерфейс потребує уваги. Це скорочує час первинної діагностики та робить контроль мережевої інфраструктури більш системним.

У підсумку, аналіз результатів роботи системи показав, що реалізоване рішення забезпечує віддалений збір параметрів, побудову графіків, перегляд історії трафіку та підтримку виявлення відхилень у роботі комутаційних вузлів. Система є придатною для контролю стану мережевої інфраструктури, оцінювання завантаження інтерфейсів і прийняття рішень щодо обслуговування або модернізації мережі.

4.8 Висновки до розділу 4

У розділі було описано програмно-апаратну реалізацію кіберфізичної системи віддаленого моніторингу комутаційних вузлів мережі на основі MRTG. Реалізована система поєднує фізичні мережеві пристрої, SNMP-доступ до параметрів обладнання, сервер моніторингу, механізми збереження статистичних даних, формування графіків і веб-доступ до результатів. Це дозволило перейти від теоретичної архітектури до практичного рішення, яке забезпечує віддалений контроль стану мережевої інфраструктури.

Було обґрунтовано вибір програмно-апаратних компонентів реалізованої системи. До її складу включено комутаційні вузли з підтримкою SNMP, сервер моніторингу, MRTG, сховище часових рядів, веб-компонент і робоче місце

адміністратора. Такий склад компонентів забезпечив повний цикл роботи системи: від отримання параметрів із фізичного обладнання до перегляду графіків і прийняття рішень за результатами аналізу.

У межах реалізації було налаштовано SNMP-доступ до комутаційних вузлів. Було визначено контрольовані пристрої, IP-адреси, важливі інтерфейси та параметри, які підлягають збору. Доступ до SNMP було організовано з урахуванням принципу мінімально необхідних прав, тобто сервер моніторингу отримує можливість зчитувати параметри обладнання, але не змінює конфігурацію комутаційних вузлів. Це дозволяє використовувати систему для безпечного віддаленого контролю без зайвого втручання в роботу мережі.

Було виконано конфігурування MRTG для збору мережевих параметрів. У конфігурації визначено контрольовані інтерфейси, параметри SNMP-доступу, максимальну пропускну здатність портів, назви графіків, робочий каталог і періодичність оновлення. Після налаштування MRTG система отримала можливість регулярно звертатися до комутаційних вузлів, обробляти значення лічильників і формувати графіки вхідного та вихідного трафіку.

Окремо було реалізовано зберігання статистичних даних і формування графіків. Отримані параметри зберігаються з часовою прив’язкою, що дозволяє формувати історію зміни показників. Такий підхід забезпечує не лише перегляд поточного стану інтерфейсів, а й аналіз динаміки навантаження за попередні періоди. Завдяки цьому система може використовуватися для виявлення пікових навантажень, повторюваних відхилень і поступового зростання трафіку.

Було реалізовано веб-доступ до результатів моніторингу. Сформовані MRTG HTML-сторінки та графіки доступні через браузер адміністратора, що спрощує перегляд результатів і робить систему зручною для практичного використання. Було враховано необхідність обмеження доступу до сторінок моніторингу, оскільки дані про трафік, активність портів і доступність вузлів можуть розкривати особливості роботи мережевої інфраструктури.

Перевірка працездатності системи показала, що основні компоненти працюють узгоджено. Комутаційні вузли відповідають на SNMP-запити, сервер

моніторингу отримує параметри, MRTG формує статистику й графіки, а веб-компонент забезпечує перегляд результатів. Було підтверджено, що система не зупиняє роботу повністю у разі тимчасової недоступності окремого вузла, а продовжує обробку доступних пристроїв.

Аналіз результатів роботи системи показав, що реалізоване рішення дозволяє контролювати вхідний і вихідний трафік, оцінювати завантаження контрольованих портів, виявляти помилки та відкинуті пакети, а також переглядати доступність комутаційних вузлів. Сформовані графіки дали можливість наочно представити результати моніторингу й підтвердити практичну придатність системи для аналізу стану мережевої інфраструктури.

У підсумку, у четвертому розділі було реалізовано та перевірено кіберфізичну систему віддаленого моніторингу комутаційних вузлів мережі на основі MRTG. Отримані результати підтвердили, що система забезпечує автоматизований збір параметрів, збереження статистики, побудову графіків, веб-доступ до результатів і підтримку аналізу стану мережі. Реалізоване рішення може використовуватися як практичний інструмент для контролю завантаження інтерфейсів, виявлення відхилень і підтримки рішень адміністратора щодо обслуговування або модернізації мережевої інфраструктури.

ВИСНОВКИ

У роботі за результатами виконаних теоретичних та практичних напрацювань розроблено кіберфізичну систему віддаленого моніторингу комутаційних вузлів мережі на основі MRTG. Запропоноване рішення поєднує фізичні мережеві пристрої, SNMP-збір параметрів, сервер моніторингу, сховище часових рядів, графічне представлення результатів і дії адміністратора щодо реагування на виявлені відхилення. Набула подальшого розвитку архітектура кіберфізичної системи моніторингу мережевої інфраструктури, у якій стан комутаційних вузлів відображається у вигляді цифрових параметрів, придатних для аналізу, візуалізації та підтримки експлуатаційних рішень.

Поставлену мету було досягнуто шляхом розв’язання таких основних завдань:

– проаналізовано предметну область віддаленого моніторингу комутаційних вузлів мережі та визначено основні проблеми, пов’язані з ручним контролем обладнання, віддаленим розміщенням вузлів, зростанням мережевого навантаження, потребою в історичному аналізі параметрів і забезпеченням безпечного доступу до результатів моніторингу;

– виконано порівняльний аналіз існуючих рішень для моніторингу мережевої інфраструктури, зокрема MRTG, Cacti, Zabbix, LibreNMS, Nagios Core, PRTG, Prometheus, Grafana та Telegraf, унаслідок чого обґрунтовано доцільність використання MRTG як простого, доступного та практичного інструменту для графічного контролю параметрів комутаційних вузлів;

– розглянуто особливості використання SNMP та MRTG у системах мережевого моніторингу, визначено роль SNMP як механізму отримання параметрів із фізичних мережевих пристроїв, а MRTG - як засобу періодичного опитування, обробки лічильників, формування часових рядів і побудови графіків;

– сформовано модель кіберфізичної системи віддаленого моніторингу, у якій фізичний рівень представлено комутаційними вузлами та мережевими інтерфейсами, комунікаційний рівень - SNMP-збором параметрів, програмний

рівень - сервером моніторингу MRTG, а рівень користувача - переглядом графіків, аналізом результатів і реагуванням адміністратора;

– визначено контрольовані показники стану комутаційних вузлів, до яких належать вхідний і вихідний трафік, завантаження uplink-каналів, кількість помилок, відкинуті пакети, стан портів, доступність вузлів і додаткові системні параметри обладнання;

– розроблено архітектуру кіберфізичної системи віддаленого моніторингу на основі MRTG, яка включає підсистему SNMP-збору, підсистему обробки та зберігання статистичних даних, підсистему візуалізації результатів і механізми контролю критичних станів;

– реалізовано налаштування SNMP-доступу до комутаційних вузлів, конфігурування MRTG для збору мережевих параметрів, збереження статистичних даних, формування графіків і веб-доступ до результатів моніторингу;

– здійснено перевірку працездатності реалізованої системи на контрольованих мережевих вузлах, унаслідок чого підтверджено можливість отримання SNMP-параметрів, автоматичного оновлення графіків, перегляду результатів через веб-інтерфейс і аналізу стану мережевої інфраструктури.

Практична значимість отриманих результатів полягає у створенні системи, яка дозволяє адміністратору віддалено контролювати стан комутаційних вузлів, переглядати графіки трафіку, виявляти перевантажені інтерфейси, аналізувати помилки й відкинуті пакети, оцінювати доступність вузлів і приймати рішення щодо обслуговування або модернізації мережі. Впровадження результатів роботи дозволяє перейти від фрагментарної ручної перевірки обладнання до системного віддаленого моніторингу мережевої інфраструктури.

За темою кваліфікаційної роботи підготовлено тези, у яких розглянуто принцип побудови кіберфізичної системи віддаленого моніторингу комутаційних вузлів мережі на основі MRTG.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1. MRTG : Index of /mrtg/pub. Oetiker+Partner *AG*, 2022. URL: https://oss.oetiker.ch/mrtg/pub/ (дата звернення: 27.04.2026).

2. Oetiker T. MRTG-REFERENCE(1) : MRTG 2.17.10 configuration reference. Ubuntu Manpage Repository, 2022. URL: https://manpages.ubuntu.com/manpages/jammy/man1/mrtg-reference.1.html (дата звернення: 27.04.2026).

3. Oetiker T. MRTG(1) : Multi Router Traffic Grapher. Ubuntu Manpage Repository, 2022. URL: https://manpages.ubuntu.com/manpages/jammy/man1/mrtg.1.html (дата звернення: 27.04.2026).

4. Oetiker T. CFGMAKER(1) : Creates mrtg.cfg files for MRTG. Ubuntu Manpage Repository, 2022. URL: https://manpages.ubuntu.com/manpages/jammy/man1/cfgmaker.1.html (дата звернення: 27.04.2026).

5. Oetiker T. INDEXMAKER(1) : Creates index files for MRTG web sites. Ubuntu Manpage Repository, 2022. URL: https://manpages.ubuntu.com/manpages/jammy/man1/indexmaker.1.html (дата звернення: 27.04.2026).

6. Oetiker T. MRTG-TRAFFIC-SUM(1) : Traffic accounting for MRTG. Ubuntu Manpage Repository, 2022. URL: https://manpages.ubuntu.com/manpages/jammy/man1/mrtg-traffic-sum.1.html (дата звернення: 27.04.2026).

7. MRTG package in Ubuntu 22.04 LTS. Ubuntu Packages, 2022. URL: https://packages.ubuntu.com/jammy/mrtg (дата звернення: 27.04.2026).

8. MRTG package in Ubuntu 24.04 LTS. Ubuntu Packages, 2024. URL: https://packages.ubuntu.com/noble/mrtg (дата звернення: 27.04.2026).

9. Oetiker T. RRDtool Version 1.8.0. GitHub Releases, 2022. URL: https://github.com/oetiker/rrdtool-1.x/releases/tag/v1.8.0 (дата звернення: 27.04.2026).

10. Oetiker T. RRDTOOL(1) : Round Robin Database Tool. Ubuntu Manpage Repository, 2022. URL: https://manpages.ubuntu.com/manpages/jammy/man1/rrdtool.1.html (дата звернення: 27.04.2026).

11. Oetiker T. RRDCREATE(1) : Set up a new Round Robin Database. Ubuntu Manpage Repository, 2022. URL: https://manpages.ubuntu.com/manpages/jammy/man1/rrdcreate.1.html (дата звернення: 27.04.2026).

12. Oetiker T. RRDUPDATE(1) : Store a new set of values into the RRD. Ubuntu Manpage Repository, 2022. URL: https://manpages.ubuntu.com/manpages/jammy/man1/rrdupdate.1.html (дата звернення: 27.04.2026).

13. Oetiker T. RRDFETCH(1) : Fetch data from an RRD. Ubuntu Manpage Repository, 2022. URL: https://manpages.ubuntu.com/manpages/jammy/man1/rrdfetch.1.html (дата звернення: 27.04.2026).

14. Oetiker T. RRDGRAPH(1) : Round Robin Database tool graphing functions. Ubuntu Manpage Repository, 2022. URL: https://manpages.ubuntu.com/manpages/jammy/man1/rrdgraph.1.html (дата звернення: 27.04.2026).

15. Oetiker T. RRDINFO(1) : Extract header information from an RRD. Ubuntu Manpage Repository, 2022. URL: https://manpages.ubuntu.com/manpages/jammy/man1/rrdinfo.1.html (дата звернення: 27.04.2026).

16. Oetiker T. RRDCACHED(1) : Data caching daemon for RRDtool. Ubuntu Manpage Repository, 2022. URL: https://manpages.ubuntu.com/manpages/jammy/man1/rrdcached.1.html (дата звернення: 27.04.2026).

17. RRDtool package in Ubuntu 24.04 LTS. Ubuntu Packages, 2024. URL: https://packages.ubuntu.com/noble/rrdtool (дата звернення: 27.04.2026).

18. Net-SNMP 5.9.4. SourceForge, 2024. URL: https://sourceforge.net/projects/net-snmp/files/net-snmp/5.9.4/ (дата звернення: 27.04.2026).

19. Net-SNMP Documentation. Net-SNMP Project, 2024. URL: http://www.net-snmp.org/docs/ (дата звернення: 27.04.2026).

20. SNMP - RouterOS. *MikroTik Documentation*, 2026. URL: https://help.mikrotik.com/docs/spaces/ROS/pages/8978519/SNMP (дата звернення: 27.04.2026).

21. SNMP Configuration Guide, Cisco IOS XE 17. Cisco Systems, 2022. URL: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/snmp/configuration/xe-17-x/snmp-xe-17-book.html (дата звернення: 27.04.2026).

22. SNMP Support : SNMP Configuration Guide, Cisco IOS XE 17. Cisco Systems, 2022. URL: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/snmp/configuration/xe-17-x/snmp-xe-17-book/nm-snmp-cfg-snmp-support.html (дата звернення: 27.04.2026).

23. Configure SNMPv2c/v3 on Catalyst 9000 Series Switches. Cisco Systems, 2025. URL: https://www.cisco.com/c/en/us/support/docs/switches/catalyst-9500-series-switches/224891-configure-snmpv2c-v3-on-catalyst-9000.html (дата звернення: 27.04.2026).

24. Configuring Simple Network Management Protocol : Catalyst 9200 Series Switches. Cisco Systems, 2025. URL: https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9200/software/release/17-17/configuration_guide/nmgmt/b_1717_nmgmt_9200_cg/configuring_simple_network_management_protocol.html (дата звернення: 27.04.2026).

25. Configuring and Validating SNMP. Cisco Systems, 2025. URL: https://www.cisco.com/c/en/us/td/docs/IIOT/wireless/urwb/1718/config-guide/b-curwb-scg-17-18-x/m-configuring-and-validating-snmp.html (дата звернення: 27.04.2026).

26. Cisco IOS and IOS XE Software SNMP Denial of Service Vulnerability. Cisco Security Advisory, 2025. URL:

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-snmp-x4LPhte (дата звернення: 27.04.2026).

27. Cisco IOS XE Software Simple Network Management Protocol Vulnerability. Cisco Security Advisory, 2025. URL: https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-snmpwred-x3MJyf5M (дата звернення: 27.04.2026).

28. Static Tundra : Russian state-sponsored espionage group targets network devices. Cisco Talos Intelligence Group, 2025. URL: https://blog.talosintelligence.com/static-tundra/ (дата звернення: 27.04.2026).

29. Russian Government Cyber Actors Targeting Networking Devices and Critical Infrastructure. Federal Bureau of Investigation, 2025. URL: https://www.fbi.gov/investigate/cyber/alerts/2025/russian-government-cyber-actors-targeting-networking-devices-critical-infrastructure (дата звернення: 27.04.2026).

30. High Vulnerability in Cisco IOS and IOS XE Software. *CERT-EU*, 2025. URL: https://cert.europa.eu/publications/security-advisories/2025-035/ (дата звернення: 27.04.2026).

31. Network Management and Monitoring Guide. Juniper Networks, 2026. URL: https://www.juniper.net/documentation/us/en/software/junos/network-mgmt/index.html (дата звернення: 27.04.2026).

32. Configure SNMP in Junos OS. Juniper Networks, 2026. URL: https://www.juniper.net/documentation/us/en/software/junos/network-mgmt/topics/topic-map/configure-snmp-in-junos-os.html (дата звернення: 27.04.2026).

33. Remote Network Monitoring (RMON). Juniper Networks, 2026. URL: https://www.juniper.net/documentation/us/en/software/junos/network-mgmt/topics/topic-map/remote-nework-monitoring-rmon.html (дата звернення: 27.04.2026).

34. Monitoring a device using SNMP. Hewlett Packard Enterprise, 2024. URL: https://arubanetworking.hpe.com/techdocs/AOS-CX/10.13/HTML/monitoring_6300-6400/Content/mon-dev-by-usi-snm.htm (дата звернення: 27.04.2026).

35. AOS-CX 10.13 SNMP/MIB Guide. Hewlett Packard Enterprise, 2025. URL: https://arubanetworking.hpe.com/techdocs/AOS-CX/10.13/PDF/snmp_mib.pdf (дата звернення: 27.04.2026).

36. Zabbix Documentation 7.0. Zabbix SIA, 2024. URL: https://www.zabbix.com/documentation/7.0/en/manual (дата звернення: 27.04.2026).

37. SNMP agent : Zabbix Documentation 7.0. Zabbix SIA, 2024. URL: https://www.zabbix.com/documentation/7.0/en/manual/config/items/itemtypes/snmp (дата звернення: 27.04.2026).

38. SNMP traps : Zabbix Documentation 7.0. Zabbix SIA, 2024. URL: https://www.zabbix.com/documentation/7.0/en/manual/config/items/itemtypes/snmptrap (дата звернення: 27.04.2026).

39. Monitor a network switch or router with Zabbix. Zabbix SIA, 2024. URL: https://www.zabbix.com/documentation/7.0/en/manual/guides/monitor_switch (дата звернення: 27.04.2026).

40. Cisco IOS by SNMP monitoring and integration with Zabbix. Zabbix Integrations, 2024. URL: https://www.zabbix.com/integrations/cisco_snmp (дата звернення: 27.04.2026).

41. MikroTik by SNMP monitoring and integration with Zabbix. Zabbix Integrations, 2024. URL: https://www.zabbix.com/integrations/mikrotik_snmp (дата звернення: 27.04.2026).

42. What's new in Zabbix 7.0 LTS. Zabbix SIA, 2024. URL: https://www.zabbix.com/whats_new_7_0 (дата звернення: 27.04.2026).

43. Release Notes for Zabbix 7.4.0. Zabbix SIA, 2025. URL: https://www.zabbix.com/rn/rn7.4.0 (дата звернення: 27.04.2026).

44. Release Notes for Zabbix 7.0.24. Zabbix SIA, 2026. URL: https://www.zabbix.com/rn/rn7.0.24 (дата звернення: 27.04.2026).

45. SNMP and SNMP traps in Zabbix 7.0. InitMAX, 2025. URL: https://www.initmax.cz/wp-content/uploads/2025/01/snmp-a-snmp-traps-in-zabbix-7.0.pdf (дата звернення: 27.04.2026).

46. Cacti Documentation. The Cacti Group, 2025. URL: https://docs.cacti.net/ (дата звернення: 27.04.2026).

47. Cacti Manual. The Cacti Group, 2025. URL: https://www.cacti.net/downloads/docs/pdf/manual.pdf (дата звернення: 27.04.2026).

48. Cacti 1.2.29 Release. The Cacti Group, 2025. URL: https://github.com/Cacti/cacti/releases/tag/release%2F1.2.29 (дата звернення: 27.04.2026).

49. Principles of Operation. The Cacti Group, 2025. URL: https://github.com/Cacti/documentation/blob/develop/Principles-of-Operation.md (дата звернення: 27.04.2026).

50. LibreNMS Documentation. LibreNMS Project, 2026. URL: https://docs.librenms.org/ (дата звернення: 27.04.2026).

51. SNMP Configuration Examples. LibreNMS Project, 2026. URL: https://docs.librenms.org/Support/SNMP-Configuration-Examples/ (дата звернення: 27.04.2026).

52. Alerting. LibreNMS Project, 2026. URL: https://docs.librenms.org/Alerting/ (дата звернення: 27.04.2026).

53. Device Groups. LibreNMS Project, 2026. URL: https://docs.librenms.org/Extensions/Device-Groups/ (дата звернення: 27.04.2026).

54. Nagios Core Documentation. Nagios Enterprises, 2024. URL: https://assets.nagios.com/downloads/nagioscore/docs/nagioscore/4/en/ (дата звернення: 27.04.2026).

55. Nagios Core 4.5.9 Release. GitHub Releases, 2024. URL: https://github.com/NagiosEnterprises/nagioscore/releases/tag/nagios-4.5.9 (дата звернення: 27.04.2026).

56. SNMP Monitoring. Nagios Enterprises, 2025. URL: https://www.nagios.com/solutions/snmp-monitoring/ (дата звернення: 27.04.2026).

57. PRTG Manual : SNMP Traffic Sensor. Paessler, 2025. URL: https://www.paessler.com/manuals/prtg/snmp_traffic_sensor (дата звернення: 27.04.2026).

58. PRTG Manual : SNMP Custom Sensor. Paessler, 2025. URL: https://www.paessler.com/manuals/prtg/snmp_custom_sensor (дата звернення: 27.04.2026).

59. Monitoring MikroTik RouterOS with PRTG. Paessler, 2026. URL: https://blog.paessler.com/monitoring-mikrotik-routeros-with-prtg (дата звернення: 27.04.2026).

60. Network Monitoring : Best Practices Guide. *SolarWinds*, 2025. URL: https://www.solarwinds.com/monitoring-and-observability-guide/network-monitoring (дата звернення: 27.04.2026).

61. Prometheus Documentation. Prometheus Authors, 2025. URL: https://prometheus.io/docs/introduction/overview/ (дата звернення: 27.04.2026).

62. Grafana Documentation. Grafana Labs, 2025. URL: https://grafana.com/docs/grafana/latest/ (дата звернення: 27.04.2026).

63. Telegraf SNMP Input Plugin. *InfluxData*, 2025. URL: https://docs.influxdata.com/telegraf/v1/input-plugins/snmp/ (дата звернення: 27.04.2026).

64. SNMP Network Monitoring with OpenNMS Meridian. OpenNMS, 2024. URL: https://www.opennms.com/en/blog/2024-03-21-snmp-network-monitoring/ (дата звернення: 27.04.2026).

65. OpenNMS Meridian Documentation. OpenNMS, 2024. URL: https://docs.opennms.com/meridian/2024/ (дата звернення: 27.04.2026).

66. Alhilali A. H., Al Farawn A., Mjhool A. Y. Design and implement a real-time network traffic management system using SNMP protocol. *Eastern-European Journal of Enterprise Technologies*. 2023. Vol. 5, No. 9 (125). P. 35–44. DOI: https://doi.org/10.15587/1729-4061.2023.286528. URL: https://journals.uran.ua/eejet/article/view/286528 (дата звернення: 27.04.2026).

67. Espinel-Villalobos R. I., Ardila-Triana E., Zarate-Ceballos H., Ortiz-Triviño J. E. Design and Implementation of Network Monitoring System for Campus Infrastructure Using Software Agents. *Ingeniería e Investigación*. 2022. Vol. 42, No. 1. Article e87564. DOI: https://doi.org/10.15446/ing.investig.v42n1.87564. URL:

https://www.scielo.org.co/scielo.php?pid=S0120-56092022000100109&script=sci_arttext (дата звернення: 27.04.2026).

68. Бешлей Г. В., Іванюк М. М., Бешлей М. І. Розробка прототипу телекомунікаційної мережі для тестування та розвитку систем моніторингу Zabbix. *Вчені записки ТНУ імені В. І. Вернадського. Серія : Технічні науки*. 2024. Т. 35 (74), № 3. Ч. 2. С. 9–21. DOI: https://doi.org/10.32782/2663-5941/2024.3.2/02. URL: https://tech.vernadskyjournals.in.ua/journals/2024/3_2024/part_2/4.pdf (дата звернення: 27.04.2026).

69. Tonge A. S., Baniya B. K., GC D. Efficient, Scalable, and Secure Network Monitoring Platform : Self-Contained Solution for Future SMEs. *Network*. 2025. Vol. 5, No. 3. Article 36. DOI: https://doi.org/10.3390/network5030036. URL: https://www.mdpi.com/2673-8732/5/3/36 (дата звернення: 27.04.2026).

70. Yaseen N., Wijewardena A., Liyanage M. From Counters to Telemetry : A Survey of Programmable Network-Wide Monitoring. *Network*. 2025. Vol. 5, No. 3. Article 38. DOI: https://doi.org/10.3390/network5030038. URL: https://www.mdpi.com/2673-8732/5/3/38 (дата звернення: 27.04.2026).

71. Sanches J., Pereira P. R. Network and Systems Monitoring with Prometheus and Grafana. *Proceedings of 20th Iberian Conference on Information Systems and Technologies (CISTI 2025) - Volume 1* / eds. A. Rocha, C. J. Costa, F. G. Peñalvo, R. Gonçalves. Cham : Springer, 2026. P. 367–378. DOI: https://doi.org/10.1007/978-3-032-10929-3_32. URL: https://web.tecnico.ulisboa.pt/paulo.pereira/publica/Network_and_Systems_Monitoring_with_Prometheus_and_Grafana.pdf (дата звернення: 27.04.2026).

72. Baikole A. M., Purwadi J., Indriyanta G. Evaluating SNMP Protocol for Monitoring and Restoring Device Access using RAD Method. *International Journal of Informatics and Computation*. 2026. Vol. 8, No. 1. P. 146–157. DOI: https://doi.org/10.35842/ijicom.v8i1.226. URL: https://ijicom.respati.ac.id/index.php/ijicom/article/download/226/160 (дата звернення: 27.04.2026).

73. Taynor D. Monitoring a Small Network with SNMP. *Honors Research Projects*. Akron : The University of Akron, 2025. Paper 1960. URL: https://ideaexchange.uakron.edu/context/honors_research_projects/article/3560/viewcontent/auto_convert.pdf (дата звернення: 27.04.2026).

74. Alwanto H., Yel M. B. Analysis of Enterprise Network Performance Using the SNMP (Simple Network Management Protocol) Method. *Journal Innovations Computer Science*. 2025. Vol. 4, No. 2. P. 335–344. DOI: https://doi.org/10.56347/jics.v4i2.346. URL: https://www.journal.kawanad.com/index.php/jics/article/download/346/267 (дата звернення: 27.04.2026).

75. Mohammed Zeeshan A. Network Monitoring Using Grafana : An Integrated Approach for Enterprise Infrastructure Management. *International Journal of Engineering Research and Applications*. 2025. Vol. 15, Issue 8. P. 1–5. DOI: https://doi.org/10.9790/9622-15080105. URL: https://www.ijera.com/papers/vol15no8/15080105.pdf (дата звернення: 27.04.2026).

76. Ajlan I. K., Yusof A. F. bin. Network Monitoring Using SNMP and RRDtool. *IAR Journal of Engineering and Technology*. 2022. Vol. 3, No. 2. P. 1–5. DOI: https://doi.org/10.47310/iarjet.2022.v03i02.001. URL: https://iarconsortium.org/iarjet/35/158/network-monitoring-using-snmp-and-rrdtool-1811/ (дата звернення: 27.04.2026).

77. Yuliandoko H., Utomo A. P., Maulana A. N. WEB Based Monitoring System for SFP Interface Traffic, Case Study in Riyad Network Banyuwangi. *Jurnal Jaringan Telekomunikasi*. 2023. Vol. 13, No. 3. P. 232–240. URL: https://core.ac.uk/download/pdf/587784132.pdf (дата звернення: 27.04.2026).

78. Pandia M. T. M., Wadly F. Design and Build a Network Monitoring System Using Nagios at PT. Telkom Access. *Journal of Information Technology, Computer Science and Electrical Engineering*. 2025. Vol. 2, No. 1. P. 47–57. DOI: https://doi.org/10.61306/jitcse.v2i1.160. URL: https://ysmk.org/ejournal/index.php/jitcse/article/download/160/166/382 (дата звернення: 27.04.2026).

79. Anne S. N. AI-Driven Network Monitoring : A Smart Approach Using SNMP and ML Integration. *International Journal of Multidisciplinary Research in Science, Engineering, Technology & Management*. 2024. Vol. 11, Issue 3. P. 431–435. URL: https://www.ijmrsetm.com/admin/img/30_%20AI-Driven%20Network%20Monitoring.pdf (дата звернення: 27.04.2026).

80. Network Performance Monitoring Trends Report 2024. LiveAction, 2024. URL: https://www.liveaction.com/wp-content/uploads/2024/03/LiveAction_NPM_Report_FINAL.pdf (дата звернення: 27.04.2026).

81. Комп’ютерні інтелектуальні системи та мережі (КІСМ-2026) : XIX Всеукраїнська науково-практична WEB конференція аспірантів, студентів та молодих вчених. URL: https://sites.google.com/view/kicm/ (дата звернення: 26.02.2026).

ДОДАТОК А
(обов'язковий)

Наукова публікація

Коваленко Д.О.
Хмельницький національний університет
Гуральник О.Б.
Асистент, Хмельницький національний університет

КІБЕРФІЗИЧНА СИСТЕМА ВІДДАЛЕНОГО МОНІТОРИНГУ КОМУТАЦІЙНИХ ВУЗЛІВ МЕРЕЖІ НА ОСНОВІ MRTG

Розглянуто підхід до побудови кіберфізичної системи віддаленого моніторингу комутаційних вузлів мережі, яка інтегрує фізичні мережеві пристрої та програмні засоби збору, зберігання і візуалізації параметрів функціонування.

MRTG (Multi Router Traffic Grapher) належить до класу систем графічної візуалізації трафіку, які формують часові ряди та графіки зміни параметрів мережі. Практична цінність такого підходу полягає в тому, що навіть за відсутності складної аналітики адміністратор отримує інструмент для швидкого розпізнавання трендів і відхилень, а накопичені дані дозволяють ретроспективно встановлювати причини інцидентів або планувати модернізацію.

Узагальнено архітектуру системи можна подати як взаємодію трьох рівнів. Фізичний рівень включає комутатори доступу/агрегації та інші мережеві пристрої, що надають статистику інтерфейсів, продуктивності та станів. Комунікаційний рівень забезпечує отримання показників через стандартизований протокол SNMP, який підтримується більшістю мережевих пристроїв і дозволяє працювати з MIB-об'єктами виробника або стандартними таблицями інтерфейсів. Програмний рівень включає сервіс опитування (polling), механізм зберігання часових рядів та веб-компонент відображення. На цьому рівні MRTG періодично виконує запити SNMP, обробляє відповіді, записує значення в базу часових рядів (часто застосовується RRD-підхід) і генерує HTML-сторінки та графіки для огляду.

Для віддаленого моніторингу принциповими є стабільність циклу збору та узгодженість частоти опитування з вимогами точності. Занадто часті запити збільшують навантаження на пристрої та мережу керування, а надто рідкі - можуть "згладжувати" пікові події. Типова стратегія полягає у виборі інтервалу 1–5 хвилин для критичних портів і більшого інтервалу для другорядних метрик. Важливим є також коректне приведення лічильників інтерфейсів до швидкості (rate), оскільки саме похідні значення відображають реальне навантаження.

Для комутаційних вузлів ключовими є показники, що безпосередньо пов'язані з пропускною здатністю та якістю передавання: вхідний і вихідний трафік на інтерфейсах, завантаження uplink-каналів, кількість помилок (errors), відкинутих пакетів (discards), ознаки флапінгу лінку та доступність вузла. Додатково доцільно контролювати системні параметри пристрою, які впливають на його роботу: завантаження CPU, використання пам'яті, температуру та стани живлення (за наявності відповідних MIB). У кіберфізичній логіці це формує

"цифровий профіль" фізичного вузла, що відображає, як реальні апаратні обмеження проявляються у мережевих показниках.

Графічне представлення даних дає можливість швидко відрізняти нормальні добові/тижневі патерни від аномалій. Наприклад, плавне зростання середнього навантаження на uplink протягом кількох тижнів є сигналом до планування розширення каналу, а короткі регулярні піки можуть вказувати на резервне копіювання або пакетні обміни, які потребують QoS-налаштувань. Збільшення помилок і відкидань на інтерфейсі, що корелює зі зростанням трафіку, часто є проявом перевантаження або проблем фізичного середовища. Таким чином, система на базі MRTG виступає не лише "лічильником трафіку", а інструментом виявлення причинно-наслідкових зв'язків між змінами навантаження та деградацією якості.

Рисунок 1 – Схема функціонування системи моніторингу

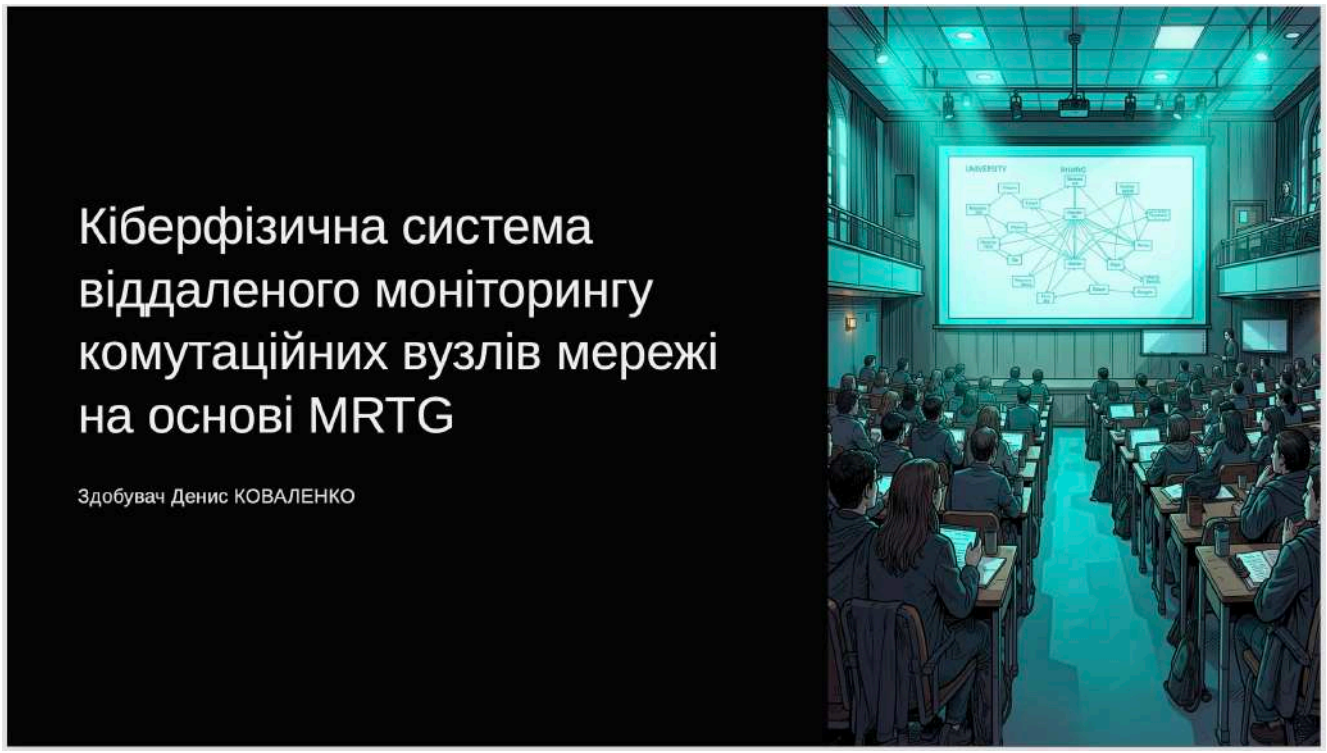
Оскільки моніторинг є віддаленим, система повинна мінімізувати ризики несанкціонованого доступу як до пристроїв, так і до даних статистики. На рівні SNMP важливим є застосування сучасніших механізмів захисту (де можливо), сегментація мережі керування, обмеження доступу списками ACL та принцип найменших привілеїв для облікових даних опитування. На рівні веб-доступу до графіків і звітів мають застосовуватися автентифікація, контроль ролей, а також захист транспортного каналу.

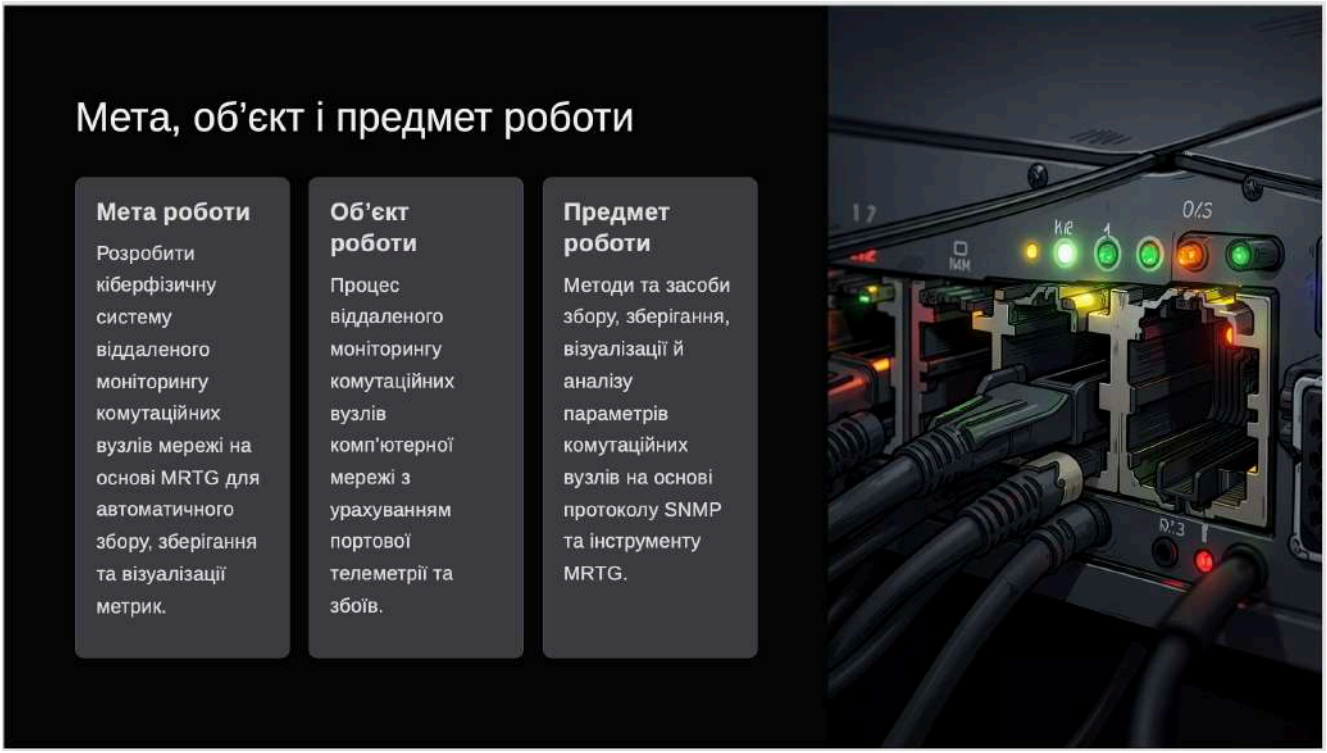
Надійність системи забезпечується стійкістю до відмов у двох контурах: збору та відображення. У разі недоступності окремого вузла система має коректно фіксувати факт недоступності та не "ламати" цикл опитування інших пристроїв. У разі пікового навантаження доцільним є рознесення компонентів або оптимізація переліку метрик для критичних сегментів мережі. Накопичення історичних даних потребує керованого розміру сховища; RRD-підхід, що використовує агрегування з часом, дозволяє зберігати довгі історії без необмеженого росту обсягу.

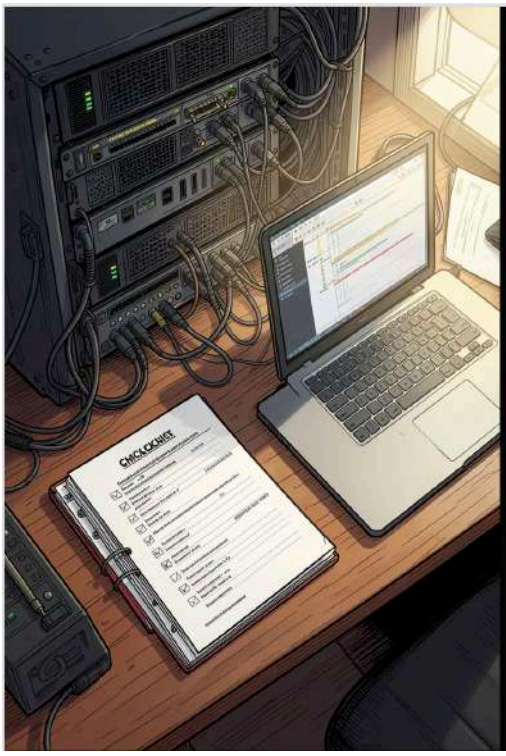
Запропонований підхід до побудови кіберфізичної системи віддаленого моніторингу комутаційних вузлів на основі MRTG забезпечує інтеграцію фізичних мережевих пристроїв із програмним контуром збору, зберігання та візуалізації статистики. Використання SNMP як стандартизованого механізму доступу до показників дозволяє підтримувати різнорідне обладнання й спрощує інтеграцію у єдину систему контролю. Формування часових рядів і наочних графіків створює основу для оперативного виявлення перевантажень, деградацій та аномалій, а також для планування розвитку мережевої інфраструктури на основі історичних даних.

ДОДАТОК Б
(обов’язковий)

Презентація







Задачі роботи

1. Проаналізувати предметну область віддаленого моніторингу комутаційних вузлів.
2. Оцінити існуючі рішення для моніторингу мережевої інфраструктури та визначити критерії вибору.
3. Сформувати модель кіберфізичної системи моніторингу з визначенням рівнів та компонентів.
4. Розробити архітектуру системи на базі MRTG із врахуванням SNMP-агентів і сховища часових рядів.
5. Реалізувати SNMP-збір параметрів (трафік, статус портів, помилки, dropped packets).
6. Налаштувати MRTG, механізми зберігання статистики та веб-доступ для адміністраторів.
7. Перевірити працездатність системи в тестовому середовищі та проаналізувати результати.

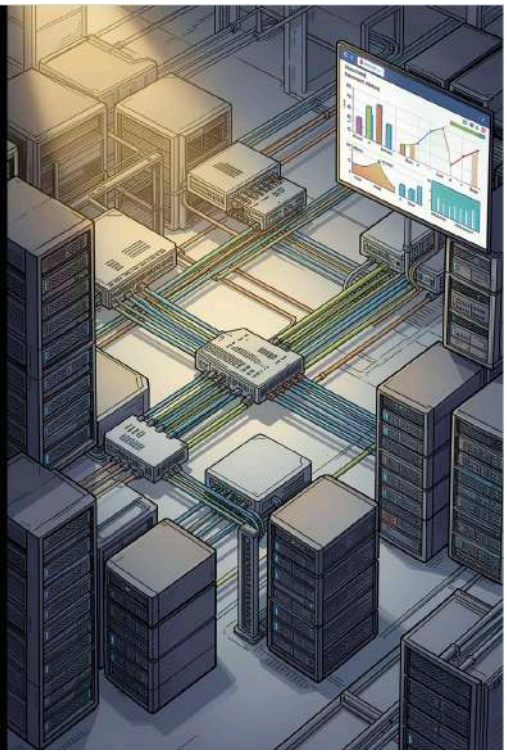
Наукова новизна та практична цінність

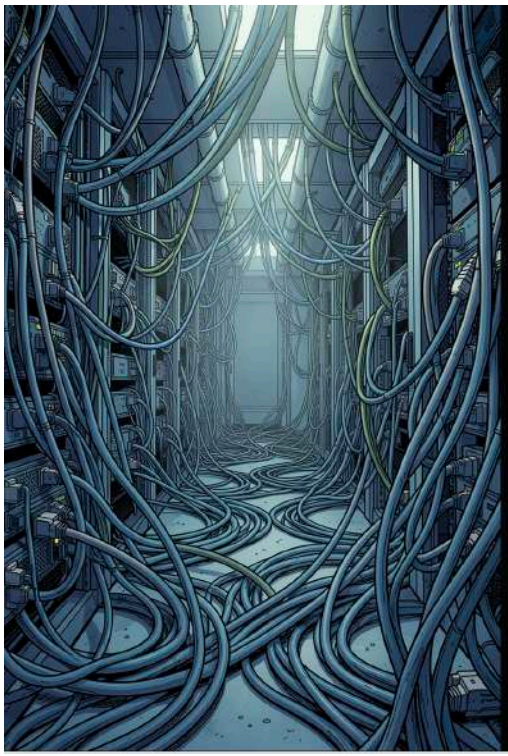
Наукова новизна

Розвиток архітектури кіберфізичної системи, що інтегрує фізичні комутаційні вузли з SNMP-збором, обробкою MRTG та збереженням часових рядів для глибшого аналізу мережевих параметрів.

Практична цінність

Система дозволяє адміністратору дистанційно контролювати стан комутаторів, аналізувати трафік, виявляти перевантаження, помилки та недоступність, що підвищує оперативність реагування та надійність інфраструктури.



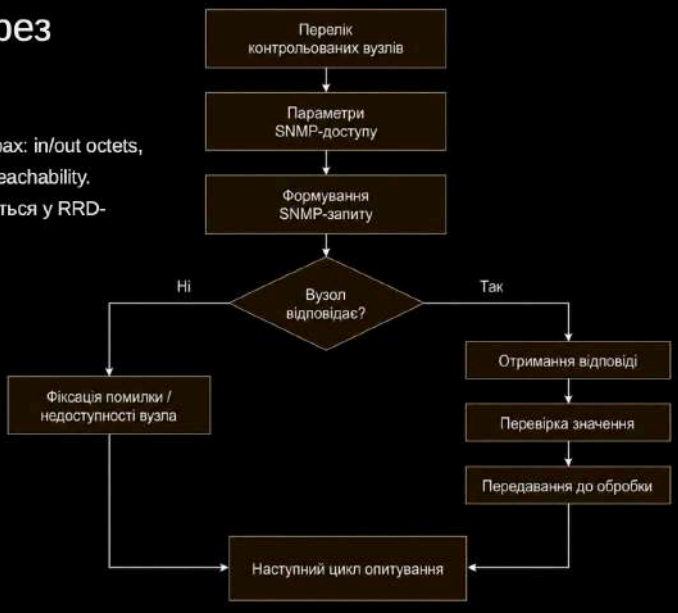


Актуальність роботи

Сучасні мережі містять сотні комутаторів, тисячі портів та численні uplink-з'єднання. Ручна діагностика не забезпечує необхідної швидкості виявлення проблем. Автоматизована система моніторингу з історією параметрів і графіками дозволяє виконувати превентивний аналіз і скоротити час простою сервісів.

Модель збору параметрів через SNMP

SNMP дозволяє опитувати менаґовані об'єкти на комутаторах: in/out octets, status per port, error counters, dropped packets, sysUpTime, reachability. Polling виконується з регулярним інтервалом; дані зберігаються у RRD-файлах для кожного OID та інтерфейсу.



Архітектура системи на основі MRTG

Компоненти архітектури:

- Фізичний рівень: комутатори, порти, uplink
- Комунікаційний рівень: SNMP v2/v3, UDP
- Програмний рівень: MRTG-демони, скрипти збору
- Сховище даних: RRD-файли (часові ряди)
- Візуалізація: веб-інтерфейс MRTG, додаткові дашборди
- Адміністратор + реагування: алерти, процедури

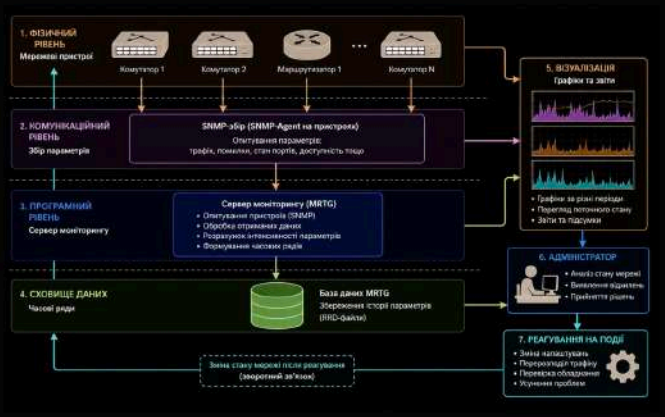


Рисунок 3.1 ілюструє зв'язки між компонентами та потоки даних від обладнання до адміністратора.

Реалізація системи

Коротко про реалізовані компоненти та інтеграції, що забезпечують повну працездатність моніторингу.

1 — SNMP-досту

Реалізовано доступ до комутаційних вузлів, підтримка SNMP v2c/v3

2 — Конфігурація MRTG

генерація конфігів, періодичний запуск збору, інтеграція з TSDB

3 — Збереження статистики

записи часових рядів, політики зберігання, індексація по метаданим

4 — HTML-графіки

формування статичних і динамічних сторінок з графіками та таблицями

5 — Веб-досту

HTTP інтерфейс для перегляду результатів моніторингу та експорту даних

Перевірка працездатності

Послідовність тестів для підтвердження коректності роботи всіх компонентів системи.

01

Перевірка доступності вузлів

ICMP/ARP, перевірка списку IP та здатності відповісти на запит.

02

Перевірка SNMP-відповідей

коректність OID, час відповіді, відсутність помилок у PDU.

03

Перевірка інтерфейсів

перевірка індексів інтерфейсів, пов'язаних OID, робочих режимів і швидкостей.

04

Тестовий запуск MRTG

імітація навантаження, перевірка створення графіків і логів.

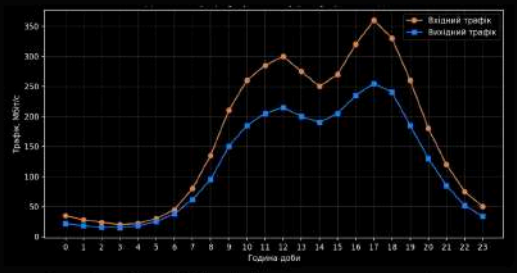
05

Перевірка оновлення графіків і веб-доступу

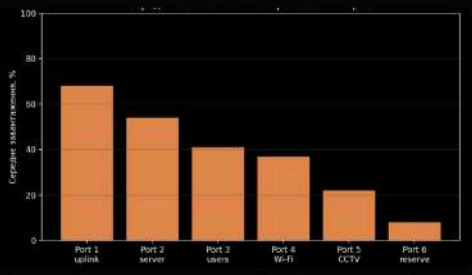
коректне відображення даних, доступність сторінок, права доступу.

Результати роботи системи

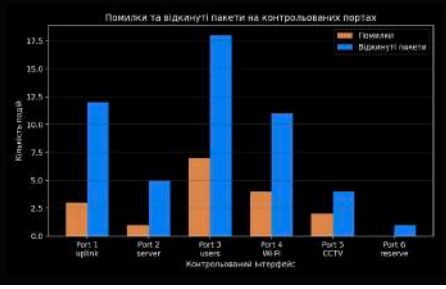
Ключові візуальні докази працездатності — графіки, що ілюструють реальні метрики мережі.



Динаміка трафіку uplink-інтерфейсу — приклад типового добового профілю.

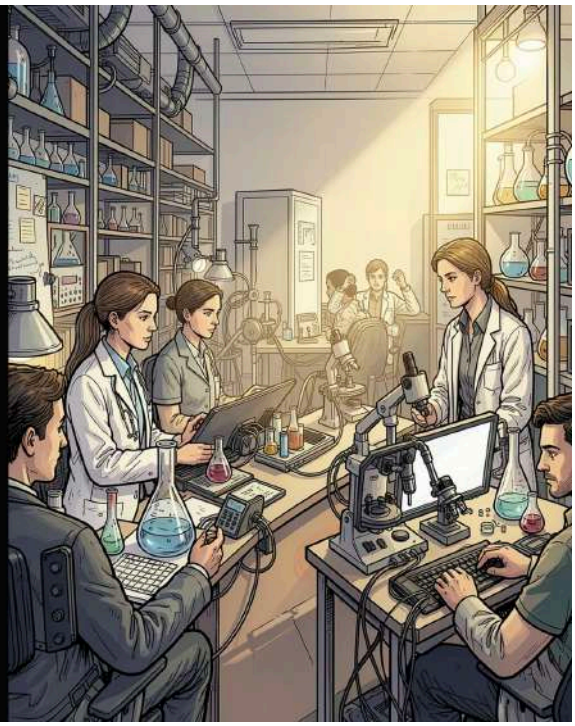


Середнє завантаження контрольованих портів за тестовий період.



Висновки

- Проаналізовано предметну область мережевого моніторингу та вимоги для SNMP-збору.
- Сформовано модель системи та розроблено архітектуру з модулями збору, обробки та візуалізації.
- Реалізовано SNMP-збір даних, інтеграцію з MRTG та збереження у вигляді часових рядів.
- Організовано веб-доступ до результатів моніторингу та автоматичну генерацію графіків.
- Проведено перевірку працездатності — підтверджено коректність збору, обробки та відображення метрик.
- Підтверджено практичну придатність рішення для навчальної та дослідної інфраструктури кафедри.



Thu May 14 23:43:44 EEST 2026, Медзатий Дмитро Миколайович, Хмельницький національний університет, ХНУ

Anti-Plagiarism (http://ap.km.ua) v-15.701

Максимальне співпадіння з одним документом 0.0%

Словники перевірки: en_US, ru_RU, ua_UA. **Помилок в документах: 10%**

	Документ		Сумарний збіг по Базі Даних	
ID: 271509 Назва: МКР Кіберфізична система віддаленого моніторингу комутаційних вузлів мережі на основі MRTG Додано в БД: 2026-05-14 Автора: Денис КОВАЛЕНКО Керівники: Олексій ІВАНОВ Консультанти: Опоненти:	Символи	Лексеми	Символи	Лексеми
	180392	1425	2424 (1%)	32 (2%)

Джерело плагіату

ID	Опис	Наявність плагіату в документі	
		Символи	Лексеми

Протокол аналізу звіту подібності експертом

Заявляю, що я ознайомився (-лась) з Повним звітом подібності, який був згенерований Системою виявлення і запобігання плагіату щодо роботи:

Автор: Денис КОВАЛЕНКО

Співавтор:

Назва: Кіберфізична система віддаленого моніторингу комутаційних вузлів мережі на основі MRTG

Експерт: Олексій ІВАНОВ

Підрозділ: Кафедра комп'ютерної інженерії та інформаційних систем

Коефіцієнт подібності 1:1.74%

Коефіцієнт подібності 2:0.56%

Мікропробіли: 4

Заміна букв: 3

Інтервали: 0

Білі знаки: 6

Дата створення звіту: 2026-05-14 23:19:40.0

Після аналізу Звіту подібності констатую наступне:

☒ **Запозичення, виявлені в роботі є законними і не є плагіатом. Рівень подібності не перевищує допустимої межі. Таким чином робота незалежна і приймається.**

☐ **Запозичення не є плагіатом, але перевищено граничне значення рівня подібностей. Таким чином робота повертається на доопрацювання.**

☐ **Виявлено запозичення і плагіат або навмисні текстові спотворення (маніпуляції), як передбачувані спроби укриття плагіату, які роблять роботу невідповідною вимогам законодавства (Ст. 32. ЗУ Про вищу освіту, пункт 3.1, Ст. 42. ЗУ Про освіту) та вимог НАЗЯВО (Критерій 5), а також кодексу етики і процедурам. Таким чином робота не приймається.**

Обгрунтування:

2026-05-15 Доцент Андрій Ніченорук

Дата експерт

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

РЕЦЕНЗІЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ МАГІСТРА

Здобувач: Денис КОВАЛЕНКО

Тема: Кіберфізична система віддаленого моніторингу комутаційних вузлів мережі на основі MRTG

Спеціальність**:** 123 «Комп'ютерна інженерія»

Обсяг кваліфікаційної роботи магістра:

Кількість листів креслень _–__; кількість сторінок записки _90__

1. Короткий зміст роботи та прийнятих рішень _ У роботі запропоновано засіб захисту даних у розподілених комп'ютерних системах із використанням протоколу доказу "нульового дня".

2. Висновок про відповідність роботи дипломному завданню _____ Кваліфікаційна робота магістра відповідає виданому завданню

3. Характеристика виконання кожного розділу, ступінь використання останніх досягнень науки і техніки і передових методів роботи: _У першому розділі проведено аналіз предметної області віддаленого моніторингу комутаційних вузлів мережі, розглянуто особливості функціонування мережевої інфраструктури, основні проблеми ручного контролю обладнання, а також переваги й недоліки відомих рішень для моніторингу мережі. У другому розділі сформовано модель кіберфізичної системи віддаленого моніторингу комутаційних вузлів мережі, визначено її фізичний, комунікаційний, програмний і користувацький рівні. У третьому розділі розроблено архітектуру кіберфізичної системи віддаленого моніторингу на основі MRTG. У четвертому розділі реалізовано програмно-апаратну частину кіберфізичної системи віддаленого моніторингу комутаційних вузлів мережі. Виконано вибір програмних і апаратних компонентів, налаштовано SNMP-доступ до комутаційних вузлів, сконфігуровано MRTG для збору мережевих параметрів, реалізовано зберігання статистичних даних, формування графіків і веб-доступ до результатів моніторингу. Проведено перевірку працездатності системи та виконано аналіз отриманих результатів.

4. Позитивні сторони роботи: ___ Запропонована кіберфізична система віддаленого моніторингу комутаційних вузлів мережі на основі MRTG дозволяє забезпечити регулярний автоматизований збір параметрів мережевого обладнання через SNMP, формувати часові ряди трафіку та стану інтерфейсів, візуалізувати результати у вигляді графіків і звітів, а також підвищити оперативність виявлення перевантажень, помилок, відкинутих пакетів і недоступності вузлів. Розроблене рішення забезпечує узгоджену взаємодію між комутаційними пристроями, SNMP-агентами, сервером моніторингу MRTG, підсистемою зберігання статистичних даних, веб-інтерфейсом перегляду результатів та механізмами реагування адміністратора на виявлені відхилення в роботі мережевої інфраструктури.

5. Негативні сторони роботи: ___У роботі трапляються окремі неточності в описі алгоритмічної та програмної реалізації засобу захисту даних, які потребують додаткового уточнення для більшої логічної цілісності викладеного матеріалу.

6. Оцінка графічного оформлення та пояснювальної записки роботи: ___–_____

7. Відгук про роботу в цілому: ___В загальному робота виконана на високому рівні.

8. Інші зауваження: ___–_____

9. Оцінка кваліфікаційної роботи магістра:

Розглянувши позитивні та негативні сторони представленої кваліфікаційної роботи магістра вважаю, що робота заслуговує оцінки « »

Рецензент (прізвище, ім'я, по батькові, посада, місце роботи) ___

Бадюкевич Леонід Петрович, зав. каф. ІПЗ, ХНУ

" 1 травня " _____2026р.

РІШЕННЯ ЕКСПЕРТНОЇ КОМІСІЇ

КАФЕДРИ КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ ТА ІНФОРМАЦІЙНИХ СИСТЕМ
ПРО ДОПУСК КВАЛІФІКАЦІЙНОЇ РОБОТИ ДО ЗАХИСТУ

Назва кваліфікаційної роботи Кіберфізична система віддаленого моніторингу комутаційних вузлів мережі на основі MRTG
Автор Денис КОВАЛЕНКО
Освітня програма Інформаційні системи та технології
Рівень вищої освіти другий (магістерський)
Спеціальність 123 Комп'ютерна інженерія
Науковий керівник: к.т.н., доцент Олексій ІВАНОВ

На основі аналізу кваліфікаційної роботи на дотримання вимог академічної доброчесності (у т.ч. відсутності ознак академічного плагіату) з урахуванням результатів перевірки роботи спеціалізованим програмним засобом(ами) комісія зробила такий висновок:

№	Висновок	Позначка про відповідність
1	Ознаки академічного плагіату	
1.1	Запозичення, виявлені в роботі, є законними і не є академічним плагіатом (далі – зазначаються підстави віднесення запозичень до правомірних, якщо потрібно). Робота приймається до захисту.	відповідає
1.2	Виявлені запозичення не є академічним плагіатом, розміщені в розділах, які не описують безпосередньо авторське дослідження, але кількість цитат перевищує обсяг, виправданий поставленою метою роботи (далі – зазначаються детальні та аргументовані підстави віднесення запозичень до правомірних). Робота приймається до захисту, але має бути відкоригована.	
1.3	Виявлені запозичення не є академічним плагіатом, але частково розміщені в розділах, які описують безпосередньо авторське дослідження, а кількість цитат перевищує обсяг, виправданий поставленою метою роботи. Робота може бути допущена до захисту після того як буде відкоригована та доопрацьована і успішно пройде повторну перевірку на академічний плагіат.	
1.4	Робота містить навмисні текстові спотворення, передбачувані спроби укриття текстових запозичень або інші прояви академічного плагіату. Робота містить фабрикацію або фальсифікацію даних. Робота не допускається до захисту.	
2	Інші види порушень академічної доброчесності	

Підтвердження:

Запозичення, виявлені в роботі, є законними і не є плагіатом, оскільки:

1) усі запозичення фрагментарні, або мають належним чином оформленні посилання;

2) окремі виявлені збіги є загальновживаними фразами або виразами, про що свідчить посилання системи на збіг з джерелами на один фрагмент речення;

3) всі зафіксовані системою ознаки модифікації тексту відносяться до комбінування латинських символів зі україномовними скороченнями індексів в формулах, що не є модифікацією тексту.

4) значна частина знайденого плагіату відноситься до списку використаних джерел

Сумарний обсяг всіх запозичень, визначений системою виявлення збігів/ ідентичності/схожості StrikePlagiarism, складає 1.74% і адресується; та системою Anti-Plagiarism складає 0%, що, з урахуванням наведених обгрунтувань, відповідає характеру наукового дослідження і свідчить на користь кваліфікаційної роботи.

15.12.2025

Завідувач кафедри _____ Ольга ПАВЛОВА
Підпис Ім'я, ПРІЗВИЩЕ

Гарант освітньої програми _____ Олег САВЕНКО
Підпис Ім'я, ПРІЗВИЩЕ

Керівник кваліфікаційної роботи _____ Олексій ІВАНОВ
Підпис Ім'я, ПРІЗВИЩЕ

Зав. кафедри КІІС
д-р. філософії Ользі ПАВЛОВІЙ

Денис КОВАЛЕНКО

ПІБ здобувача вищої освіти

ФІТ, 2 курсу, групи КІ2м-24-1

ЗАЯВА

З правилами чинного Положення про систему забезпечення академічної доброчесності у Хмельницькому національному університеті, згідно з яким виявлення академічного плагіату є підставою для відмови в допуску кваліфікаційної роботи до захисту і застосування заходів академічної відповідальності, ознайомлений (а). Про використання спеціалізованих програмних засобів (СПЗ) StrikePlagiarism та Anti-Plagiarism для перевірки кваліфікаційних робіт здобувачів вищої освіти на наявність академічного плагіату оповіщений (а). Надаю університету право на передачу моєї роботи для обробки та збереження в базах даних СПЗ і використання роботи для виявлення академічного плагіату в інших роботах, які перевіряються СПЗ.

Також надаю свою згоду на обробку й збереження університетом моєї роботи в Інституційному репозитарії Хмельницького національного університету.

Робота надається для перевірки в електронному варіанті. Електронна версія моєї роботи збігається (ідентична) з друкованою.

1 травня 2026 року