Міністерство освіти і науки України
Харківський національний університет радіоелектроніки

Факультет *Кібербезпеки*
(повна назва)
Кафедра *Інформаційно-мережної інженерії*
(повна назва)

КВАЛІФІКАЦІЙНА РОБОТА
Пояснювальна записка

рівень вищої освіти перший (бакалаврський)

Забезпечення моніторингу і контролю комп'ютерної мережі

(тема)

Виконав:
здобувач *4* року навчання,
групи *ТРІМІ-22-1*
Владислав ГРИНЬКО
(власне ім'я, прізвище)
Спеціальність *172 Телекомунікації та радіотехніка*
(код і повна назва спеціальності)
Тип програми *освітньо-професійна*

Освітня програма
«Інформаційно-мережна інженерія»
(повна назва освітньої програми)

Керівник *ст. викл. Олександр МАЛІНІН*
(посада, власне ім'я, прізвище)

Допускається до захисту

В.о. зав. кафедри _____ *Дарія ЧЕБОТАРЬОВА*
(підпис) (власне ім'я, прізвище)

2026 р.

Не містить відомостей заборонених до відкритого публікування.

Здобувач / *Владислав ГРИНЬКО* /

Керівник / *Олександр МАЛІНІН* /

Харківський національний університет радіоелектроніки

Факультет *Кібербезпеки*
Кафедра *Інформаційно-мережної інженерії*
(повна назва)
Рівень вищої освіти *перший (бакалаврський)*
Спеціальність *172 Телекомунікації та радіотехніка*
(код і повна назва)
Тип програми *освітньо-професійна*
(освітньо-професійна або освітньо-наукова)
Освітня програма *«Інформаційно-мережна інженерія»*
(повна назва)

ЗАТВЕРДЖУЮ:
Зав. кафедри _____
(підпис)
«*02*» *червня* 2026 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

здобувачеві *Гриньку Владиславу Дмитровичу*
(прізвище, ім'я, по батькові)
1. Тема роботи *Забезпечення моніторингу і контролю комп'ютерної мережі*

затверджена наказом університету від «*02*» *червня* 2026 р. № 466 *Ст*
2. Термін подання студентом роботи до екзаменаційної комісії *14 липня 2026 р.*
3. Вихідні дані до роботи *Тип комп'ютерної мережі: абстрактна, корпоративного рівня. Базова платформа організації СУ: концепція TMN. Інструмент моделювання: методологія IDEF0. Система моніторингу та контролю, що має бути застосована: програмна платформа Zabbix.*
Проаналізувати особливості організації СУ на базі TMN, та підходи щодо її застосування до управління і моніторингу КМ. Проаналізувати фундаментальну архітектуру системи МтК та розробити на її основі типову функціональну модель для КМ. На основі платформи Zabbix проаналізувати практичні аспекти застосування системи моніторингу і контролю у комп'ютерній мережі.

4. Перелік питань, що потрібно опрацювати в роботі
Вступ
1. Загальна концепція реалізації мережного управління.
2. Аналіз концепції TMN в аспекті реалізації системи управління і моніторингу комп'ютерними мережами
3. Аналіз особливостей і архітектурних підходів організації системи моніторингу та контролю комп'ютерної мережі.
4. Система моніторингу та контролю комп'ютерної мережі з використанням програмної платформи Zabbix.
Висновки

5. Перелік графічного матеріалу із зазначенням креслеників, схем, плакатів, комп'ютерних ілюстрацій (слайдів) *Слайди у форматі Power Point (назва, мета і актуальність роботи, основні поняття теорії управління та їх взаємозв'язок, базові функціональні категорії управління телекомунікаційними мережами, система управління у відповідності із стандартом TMN, фундаментальна архітектурна модель системи моніторингу та контролю комп'ютерної мережі, функціональна архітектура системи моніторингу та контролю комп'ютерної мережі, функціональна модель системи моніторингу комп'ютерної мережі на основі методології IDEF0, основні програмні компоненти системи Zabbix, використання платформи Zabbix для організації системи моніторингу та контролю, висновки)*

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Терміни виконання етапів роботи	Примітка
1	*Ознайомлення із завданням. Уточнення ТЗ.*	02.06.26	*виконано*
2	*Підбір літератури за темою роботи.*	03.06 – 07.06.26	*виконано*
3	*Виконання розділу 1*	08.06 – 12.06.26	*виконано*
4	*Виконання розділу 2*	13.06 – 19.06.26	*виконано*
5	*Виконання розділу 3*	20.06 – 29.06.26	*виконано*
6	*Виконання розділу 4*	30.06 – 07.07.26	*виконано*
7	*Оформлення пояснювальної записки*	08.07 – 12.07.26	*виконано*
8	*Оформлення презентаційного матеріалу,*		
	підготовка до захисту у ЕК, захист.	13.07 – 18.07.26	*виконано*

Дата видачі завдання *02 червня 2026 р.*

Здобувач _____
(підпис)

Керівник роботи _____ *(ст. викл. Олександр МАЛІНІН)*
(підпис) (посада, прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 71 с., 17 рис., – табл., 20 джерел, 1 додаток.

СИСТЕМА УПРАВЛІННЯ, ОБ'ЄКТ, СУБ'ЄКТ І СЕРЕДОВИЩЕ, TMN, SNMP, МОДЕЛЬ FCAPS, СИСТЕМА МОНІТОРИНГУ ТА КОНТРОЛЮ, ФУНКЦІОНАЛЬНА АРХІТЕКТУРА, ФУНКЦІОНАЛЬНА МОДЕЛЬ, МЕТОДОЛОГІЯ IDEF0, СИСТЕМА МОНІТОРИНГУ ZABBIX

Об'єкти дослідження – архітектура СУ на базі TMN, система управління і контролю комп’ютерної мережі, програмне забезпечення Zabbix.

Мета роботи – аналіз моделей і принципів організації управління, моніторингу і контролю комп’ютерної мережі на основі TMN та із застосуванням програмної платформи Zabbix.

Проведено аналіз теоретичних і практичних аспектів забезпечення моніторингу та контролю комп'ютерних мереж. Висвітлені загальні принципів побудови сучасних систем управління та їх базові функціональні задачі. В якості фундаментальної основи організації СУ проаналізована архітектура TMN та її інформаційна модель. Проаналізовано механізми взаємодії «менеджер - агент». Проаналізовані функціональні можливості та основні модулі програмної платформи для здійснення моніторингу комп’ютерних мереж Zabbix, а також показані принципи її практичного застосування в якості системи моніторингу та контролю у абстрагованій корпоративній комп’ютерній мережі.

THE ABSTRACT

Explanatory note 71 pages, 17 fig., – tab., 20 sources, 1 app.

MANAGEMENT SYSTEM, OBJECT, SUBJECT AND MEDIA, TMN, SNMP, FCAPS MODEL, MONITORING AND CONTROL SYSTEM, FUNCTIONAL ARCHITECTURE, FUNCTIONAL MODEL, IDEF0 METHODOLOGY, ZABBIX MONITORING SYSTEM

Objects of research – TMN-based management system architecture, computer network management and monitoring system, Zabbix software.

The purpose of work – analyze models and principles for organizing the management, monitoring, and control of a computer network based on the TMN and using the Zabbix software platform.

An analysis of the theoretical and practical aspects of monitoring and controlling computer networks has been conducted. The general principles of designing modern management systems and their basic functional tasks are discussed. The TMN architecture and its information model are analyzed as the fundamental basis for organizing management systems. The mechanisms of “manager–agent” interaction are analyzed. The functional capabilities and main modules of the Zabbix software platform for monitoring computer networks are analyzed, and the principles of its practical application as a monitoring and control system in an abstracted corporate computer network are demonstrated.

ЗМІСТ

С.

Перелік скорочень 8

Вступ 9

1 Загальна концепція реалізації мережного управління 12

1.1 Загальні визначення і базова концепція організації мережного управління як процесу 12

1.2 Формування мети та системи управління 16

1.3 Базові функціональні категорії управління телекомунікаційними мережами 19

2 Аналіз концепції TMN в аспекті реалізації системи управління і моніторингу комп'ютерними мережами 25

2.1 Система управління у відповідності із стандартом TMN 25

2.2 Інформаційна архітектурна модель TMN, як базовий механізм забезпечення аналізу даних в системі управління 29

3 Аналіз особливостей і архітектурних підходів організації системи моніторингу та контролю комп'ютерної мережі 35

3.1 Загальні особливості і функції систем моніторингу та контролю для комп'ютерних мереж 35

3.2 Фундаментальна архітектура системи моніторингу та контролю 38

3.3 Функціональна архітектура системи моніторингу та контролю комп'ютерної мережі 40

4 Система моніторингу та контролю комп'ютерної мережі з використанням програмної платформи Zabbix 46

4.1 Загальні особливості і компоненти системи Zabbix 46

4.2 Практичне використання платформи Zabbix для організації системи моніторингу та контролю 48

Висновки 59

Перелік джерел посилання 62

Додаток А Слайди презентації 64

ПЕРЕЛІК СКОРОЧЕНЬ

API (Application Programming Interface) – прикладний програмний інтерфейс;

BM (Business Management) – рівень управління бізнес-процесами;

CMIP (Common Management Information Protocol) – протокол загальної керуючої інформації;

CMIS (Common Management Information Service) – служба загальної керуючої інформації;

ISO (International Organization for Standardization) – Міжнародна організація по стандартизації;

ITU-T (International Telecommunication Union – Telecommunication Standardization Sector) – Міжнародний союз електрозв'язку - сектор стандартизації телекомунікацій ITU;

LAN (Local Area Network) – локальна обчислювальна мережа;

MIB (Management Information Base) – база даних управляючої інформації;

NE (Network Elements) – елементи мережі;

NEM (Network Element Management) – рівень управління елементами мережі;

NM (Network Management) – рівень управління мережею;

OSI (Open Systems Interconnection) –модель взаємодії відкритих систем;

SLA (Service Level Agreement) – угода про рівень обслуговування;

SM (Service Management) – рівень управління послугами;

SNMP (Simple Network Management Protocol) – простий протокол управління мережею;

TMN (Telecommunications Management Network) – мережа управління телекомунікаціями;

VPN (Virtual Private Network) – віртуальна приватна мережа.

БД – база даних;

КМ – комп’ютерна мережа;

МтК – моніторинг та контроль;

ОС – операційна система;

ПД – передача даних;

ПЗ – програмне забезпечення;

СУ – система управління;

ТКС – телекомунікаційна система.

ВСТУП

На сучасному етапі розвитку інформаційного суспільства комп’ютерні мережі (КМ) стали невід’ємною складовою обміну інформацією між користувачами практично у всіх сферах діяльності людини. Саме КМ різного рівня ієрархії, тобто від звичайних невеликих домашніх або офісних локальних мереж (Local Area Network, LAN) до корпоративних мереж великих підприємств і організацій, – є основою організації глобальної мережі Internet, яка забезпечує взаємодію мільярдів пристроїв у світовому масштабі [1, 2]. Але постійне зростання кількості підключених пристроїв, обсягів переданого трафіку та складності мережної інфраструктури обумовлює необхідність забезпечення ефективного моніторингу і контролю за функціонуванням КМ. Застосування механізмів моніторингу і контролю дозволить своєчасне виявлення аварійних ситуацій, перевантажень, несанкціонованого доступу та інших факторів, що негативно впливають на стабільність і безпеку мережі [3].

У загальному розумінні моніторинг комп’ютерної мережі являє собою процес безперервного спостереження за станом її компонентів, аналізу параметрів функціонування та збору статистичної інформації про роботу мережної інфраструктури. Контроль за мережею передбачає використання механізмів управління, конфігурування та реагування на події, що виникають під час функціонування мережі. У корпоративних КМ моніторинг і контроль дозволяють забезпечити необхідний рівень продуктивності, надійності, доступності та інформаційної безпеки. Сучасні системи моніторингу можуть здійснювати аналіз мережного трафіку, контролювати працездатність мережного обладнання, серверів і програмного забезпечення (ПЗ), визначати топологію мережі, оцінювати параметри якості обслуговування (Quality of Service, QoS), тощо [3, 4].

Моніторинг КМ реалізується на основі різних підходів та механізмів. Одним із найбільш поширених є аналіз мережного трафіку, який дозволяє оцінювати інтенсивність передачі даних (ПД), визначати перевантажені ділянки мережі та виявляти нехарактерну активність. Для реалізації аналізу мережного трафіку широко застосовуються аналізатори протоколів, які дозволяють здійснювати перехоплення та дослідження мережних пакетів. Використання таких засобів забезпечує можливість виявлення помилок в процесі ПД, аналізу структури трафіку, контролю функціонування мережевих сервісів, та ін. Іншим

важливим напрямом є контроль стану мережного обладнання та серверної інфраструктури, що включає спостереження за використанням процесорних ресурсів, пам’яті, пропускної здатності каналів зв’язку, температурними режимами та іншими параметрами. Також у процесі моніторингу та контролю мереж та їх характеристик значну роль відіграють механізми ведення журналів подій, системи оповіщення про відмови, а також програмні комплекси централізованого управління мережею [4, 5].

Механізми моніторингу і контролю є складовими більш загального поняття – системи управління (СУ) комп’ютерними мережами. Однією з базових концепцій у сфері управління мережами стала еталонна модель взаємодії відкритих систем (Open Systems Interconnection, OSI), яка була розроблена Міжнародною організацією зі стандартизації ISO (International Organization for Standardization). Ця модель визначає багаторівневу структуру взаємодії мережних компонентів, забезпечує стандартизований підхід до організації процесів передачі даних та дозволила уніфікувати принципи побудови мережних систем та створити основу для розвитку протоколів управління, моніторингу та контролю мережної інфраструктури. Саме на основі її концепцій були сформовані підходи до централізованого управління мережею, до стандартизації взаємодії між мережним обладнанням різних виробників, зроблено розподіл функцій між рівнями та сформовані загальні функціональні групи задач управління мережею [6, 7].

Більш розвиненим і функціонально завершеним підходом до побудови систем управління сучасними інфокомунікаційними мережами, у тому числі і комп’ютерними мережами різних рівнів ієрархій, – є концепція TMN (Telecommunication Management Network). Цей стандарт, який також визначає багаторівневу структуру взаємодії мережних модулів і компонентів, був розроблений ITU-T з метою уніфікації принципів управління мережами електрозв'язку. У концепції TMN управління розглядається як сукупність функціональних засобів і механізмів, що призначені для збору, передачі, зберігання та обробки інформації про стан мережі, а також для інформаційної підтримки адміністраторів під час прийняття рішень щодо забезпечення ефективного функціонування мережної структури [6, 7].

Таким чином, враховуючи вище викладене, метою цієї кваліфікаційної роботи є загальний аналіз сучасних підходів та механізмів управління телекомунікаційними мережами, принципів організації управління, моніторингу і контролю, що реалізуються безпосередньо в комп’ютерних мережах на

фундаментальній основі концепції TMN та із застосуванням прикладних програмних засобів для забезпечення ефективного функціонування всієї мережної інфраструктури. Актуальність такого аналізу обумовлена постійним ускладненням структури і архітектури сучасних КМ будь якого призначення, зростанням обсягів трафіку, що передається по каналах цих мереж та необхідністю забезпечення безперервного функціонування інформаційних систем, що розгортаються на їх основі. Забезпечення ефективного моніторингу і контролю інфраструктури КМ є необхідною умовою їх надійності, продуктивності та безпеки, а використання сучасних протоколів та засобів управління мережею дозволяє своєчасно виявляти проблеми у функціонуванні, проводити оптимізацію використання ресурсів та підвищувати якість мережних сервісів.

1 ЗАГАЛЬНА КОНЦЕПЦІЯ РЕАЛІЗАЦІЇ МЕРЕЖНОГО УПРАВЛІННЯ

1.1 Загальні визначення і базова концепція організації мережного управління як процесу

У загальному розумінні управління являє собою процес, що спрямований на досягнення визначених цілей шляхом здійснення планування, організації і, за необхідності, координації, контролю та прийняття управлінських рішень. Важливими складовими процесу управління є моніторинг і контроль, які забезпечують інформаційну основу для реалізації ефективного управління об'єктом. Зокрема моніторинг передбачає безперервне або періодичне (як правило, за розкладом) спостереження за станом об'єкта, що знаходиться під управлінням, а також збір, накопичення та первинну обробку інформації про його функціонування. На основі отриманих даних здійснюється контроль, який полягає у порівнянні фактичних параметрів із заданими або нормативними значеннями, виявленні відхилень, аналізі причин їх виникнення та, за необхідності, прийнятті заходів щодо коригування цих фактичних параметрів, яке спрямоване на забезпечення стабільного й ефективного функціонування системи [6 - 9].

Звідси приступаючи до розгляду цих понять і, перш за все, до розгляду загальних принципів організації управління мережною інфраструктурою та послугами, що нею пропонуються користувачам, необхідно визначити, що розуміється під термінами і процесами «управління мережею» та «управління послугами» і як вони реалізуються. Зокрема [6, 7]:

- під управлінням мережею будемо розуміти сукупність організаційних і технічних заходів, які спрямовані на забезпечення ефективного використання всіх ресурсів мережної інфраструктури, на підтримку її працездатності, необхідного рівня продуктивності та надійності, а також виконання встановлених вимог щодо якості обслуговування (Quality of Service, QoS) користувачів незалежно від режиму функціонування мережі;

- під управлінням мережними послугами будемо розуміти процес забезпечення їх своєчасного та гарантованого надання користувачам відповідно до їх потреб. При цьому необхідні послуги мають бути доступними у визначеному місці та в потрібний час, надаватися у необхідному обсязі й з гарантованими показниками QoS, а також відповідати вимогам різних категорій

користувачів щодо функціональних можливостей і економічної доцільності їх використання.

Необхідно також звернути увагу на те, що сучасні КМ разом із сукупністю мережних послуг являють собою складні технічні системи. У більш широкому розумінні вони належать до класу телекомунікаційних систем (ТКС), які складаються з великої кількості взаємопов'язаних елементів, що функціонують як єдине ціле. Характерною особливістю таких складних систем є наявність системних властивостей, які виникають лише внаслідок взаємодії їх складових і не властиві окремим елементам. Таким чином, КМ та реалізовані на їх основі послуги можна розглядати як складні системні телекомунікаційні компоненти, що виступають підсистемами більш масштабної та функціонально складнішої системи телекомунікацій [6, 7, 10].

У теорії складних систем під великою та складною системою розуміють сукупність взаємопов'язаних елементів, для якої практично неможливо сформувати повний опис усіх внутрішніх процесів, взаємозв'язків і режимів функціонування. Такі системи характеризуються багаторівневою структурою та складаються з окремих функціональних підсистем, кожна з яких може розглядатися як самостійна складна система. Зокрема, телекомунікаційна мережа міста, регіону, країни або навіть континенту включає транспортну мережу та мережі доступу, між якими існує функціональна взаємодія. У загалі транспортна мережа забезпечує середовище та канали передачі інформації, тоді як мережі доступу реалізують відповідні послуги. Водночас кожна із мереж доступу, наприклад, телефонна мережа, комп’ютерна мережа або мережа ПД, також має складну структуру, власні функціональні елементи та механізми управління. Крім того, існує взаємозамінність понять архітектурної концепції «транспортна мережа – мережі доступу», при якій транспортна мережа нижчого рівня ієрархії телекомунікаційної системи (наприклад, міста), буде виступати в якості мережі доступу до транспортної мережі регіону, і т.д. При цьому, як зазначено вище, за кожною з цих функціональних підсистем на кожному їх рівні ієрархічної взаємодії «транспорт-доступ» зберігається поняття «великої і складної системи» [6, 7].

У загальному випадку ТКС є динамічною системою, що постійно знаходиться у розвиту, модернізується та адаптується до змін умов свого функціонування. Для неї характерним є те, що випадковим чином у довільні моменти часу можуть виникати відмови окремих елементів. Проте завдяки використанню допоміжних механізмів резервування, відновлення та технічного

обслуговування забезпечується безперервність функціонування ТКС в цілому. Тобто життєвий цикл телекомунікаційної системи значно буде перевищувати термін експлуатації окремих її компонентів, а самі компоненти можуть замінюватися або модернізуватися без припинення роботи всієї ТКС. Також така система належить до класу техніко-соціальних систем, оскільки її функціонування забезпечується взаємодією технічних і людських ресурсів. До технічної складової належать зокрема лінії та канали передачі інформації, системи передачі, комутаційне обладнання, мережні вузли та кінцеві пристрої (термінали) користувачів. Соціальну складову утворюють мережні оператори, адміністратори, обслуговуючий персонал, а також користувачі, які взаємодіють із мережею та використовують послуги, що нею надаються [7, 10].

Таким чином, основними особливостями будь-якої телекомунікаційної мережі, як великої та складної системи є [7, 10]:

- багатофункціональність, що забезпечує одночасне надання різних видів телекомунікаційних та інформаційних послуг;

- наявність значної кількості функціонально неоднорідних компонентів, до яких належать лінії зв'язку, системи передачі, комутаційне обладнання, мережні вузли та кінцеві пристрої;

- просторова розподіленість елементів мережі та поєднання у ній активних і пасивних, а також цифрових і аналогових компонентів;

- багаторівневе ієрархічне структурне подання, яке забезпечує ефективну організацію функцій управління та взаємодію між окремими підсистемами;

- наявність ресурсів, що за якихось причин не були використаними, але які надалі можна застосувати для підвищення надійності, відмовостійкості та забезпечення безперервності функціонування мережі.

Таким чином, з позиції сукупності процесів, що забезпечують функціонування ТКС, поняття «управління телекомунікаціями» (Telecommunication Management) є узагальненим терміном, який охоплює комплекс взаємопов'язаних видів діяльності, що спрямовані на забезпечення ефективної роботи мережі та послуг, що нею надаються. До основних складових такого управління належать [7, 10]:

- експлуатація мережі (Operations);

- технічне обслуговування (Maintenance) телекомунікаційного (мережного) обладнання;

- управління процесами надання телекомунікаційних послуг (Administration);

- планування та проєктування нових мереж і сервісів (Planning);

- введення в експлуатацію та забезпечення доступності мережних ресурсів і послуг (Provisioning).

В якості прикладу практичного застосування зазначених понять і особливостей управління ТКС, можна навести систему загальноканальної сигналізації №7 (ЗКС №7), у якій вони реалізуються засобами прикладної підсистеми експлуатаційного управління (Operation, Maintenance and Administration Part, OMAP).

В рамках узагальнення вищевикладених понять щодо управління телекомунікаціями і особливостей ТКС, як великої та складної системи, можна сказати, що яким би досконалим не було управління ТКС, або будь-якої з її підсистем, його мета повністю практично ніколи не зможе бути досягнутою. Зазначене повною мірою стосується і сучасних комп'ютерних мереж, які також належать до класу великих та складних ТКС.

У теорії управління для опису процесу управління використовують низку базових понять, серед яких є об'єкт управління, суб'єкт управління, зовнішнє середовище, зворотний зв'язок, алгоритм управління та інші. У загальному випадку розглядається насамперед процес взаємодії суб'єкта управління із зовнішнім середовищем та об'єктом управління, який є складовою частиною цього середовища. Об'єктом управління може бути будь-яка система, стан або поведінка якої змінюється під впливом дій управління. Залежно від предметної області до об'єктів управління можуть належати як технічні системи та пристрої, зокрема і комп'ютерні мережі або інші засоби телекомунікацій чи окремі елементи мережної структури, так і біологічні, соціальні чи організаційні системи (наприклад колектив працівників або виробничі процеси). Узагальнену схему взаємодії суб'єкта і об'єкта управління та зовнішнього середовища наведено на рис. 1.1 [7, 10].

На суб'єкт управління одночасно впливають зовнішнє середовище, що має стан *X*, та об'єкт управління, що має стан *Y*, та який є складовою цього середовища. У загальному випадку кожен із станів *X* і *Y* визначається сукупністю параметрів або інших показників, тому в процесі управління їх описують відповідними векторами $\vec{X}$ і $\vec{Y}$, координати яких є окремими величинами чи значеннями цих параметрів або показників [7, 10].

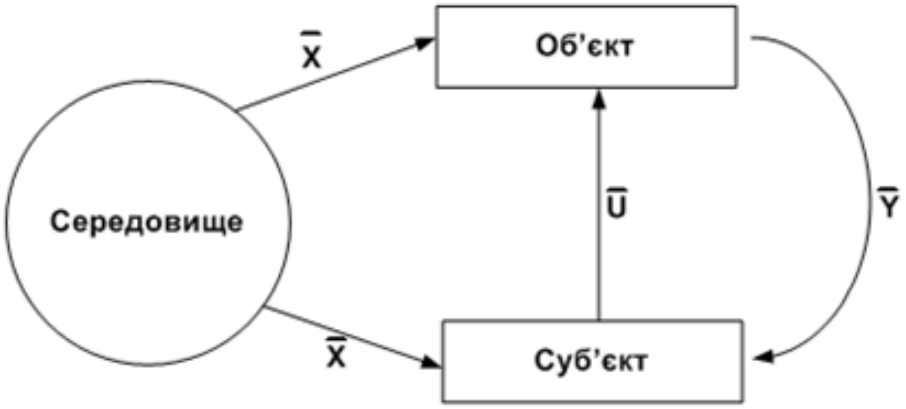


Рисунок 1.1 – Схема взаємодії суб'єкта і об'єкта управління та зовнішнього середовища у процесі організації процесу управління

Для ТКС, що розглядається як об'єкт управління, зовнішнім середовищем може виступати, наприклад, ринок телекомунікаційних послуг. Саме він формує вимоги до функціонування мережі, визначаючи необхідний перелік послуг, показники їх якості, рівень надійності та інші експлуатаційні характеристики. Водночас зовнішнє середовище забезпечує ТКС необхідними матеріальними, фінансовими, інформаційними та кадровими ресурсами, які є необхідними для її розвитку та функціонування. На відміну від об'єкта управління, стан зовнішнього середовища практично не піддається безпосередньому впливу і змінам з боку суб'єкта управління. Натомість стан об'єкта може цілеспрямовано змінюватися шляхом формування спеціального керуючого впливу *U* (див. рис. 1.1), який також описується векторною величиною $\vec{U}$, координати якої відповідають окремим діям управління [7, 10].

1.2 Формування мети та системи управління

Суб'єкт управління характеризується наявністю певних потреб *A*, для задоволення яких він направляє певну свою діяльність. Крім того, він має деякі ресурси управління *R*, що визначають його можливості щодо формування керуючих впливів на об'єкт управління. З огляду на це, процес управління можна визначити як цілеспрямований вплив суб'єкта на об'єкт управління, який є складовою зовнішнього середовища, з метою досягнення поставлених цілей і задоволення власних потреб. Ефективність такого впливу у значній мірі залежить

від повноти інформації про стан об'єкта, доступних ресурсів управління та здатності своєчасно реагувати на зміни умов функціонування системи [7, 10].

Необхідно враховувати, що потреби суб'єкта управління не є постійними. Вони можуть змінюватися під впливом зовнішнього середовища, змін у стані об'єкта управління, а також унаслідок розвитку самої системи та зміни цілей її функціонування. Тому під час аналізу процесів управління потреби суб'єкта доцільно розглядати як змінні величини за відповідним їх поточним станом [7, 10]:

$$A_i = (\alpha_1, \ldots, \alpha_i, \ldots, \alpha_k), \tag{1.1}$$

де α_i – стан i-ої потреби суб'єкта управління, що дає уявлення про важливість цієї потреби.

Як зазначалося, суб'єкт управління буде здійснювати свою діяльність таким чином, щоб задовольнити свої потреби, тобто буде вирішувати задачу багатокритеріальної оптимізації [7, 10]:

$$\alpha_i(X, U) \to \min_{u \in R}, \qquad i = 1, \ldots k.. \tag{1.2}$$

Спосіб вирішення цієї задачі є алгоритмом управління, який реалізує суб’єкт управління з урахуванням своїх потреб, тобто [7, 10]:

$$U^*_X = \varphi(A_t, X), \tag{1.3}$$

де φ – алгоритм, що дає змогу синтезувати керуючий вплив (U) з урахуванням поточного стану зовнішнього середовища потреб суб’єкта управління A_t.

Оскільки суб'єкт управління одночасно може мати значну кількість потреб і виконувати різноманітні функції, він не завжди здатний безпосередньо брати участь у всіх процесах формування та реалізації керуючих впливів. У зв'язку з цим окремі функції управління, зокрема синтез керуючих дій та їх реалізацію, доцільно передати спеціалізованим технічним засобам або автоматизованим системам, що будуть виконувати відповідні функції управління від його імені. У такому випадку між суб'єктом управління, об'єктом управління та зовнішнім

середовищем формується узагальнена схема взаємодії, у якій функції прийняття та реалізації управлінських рішень виконує орган або пристрій управління рис. 1.2 [7, 10].

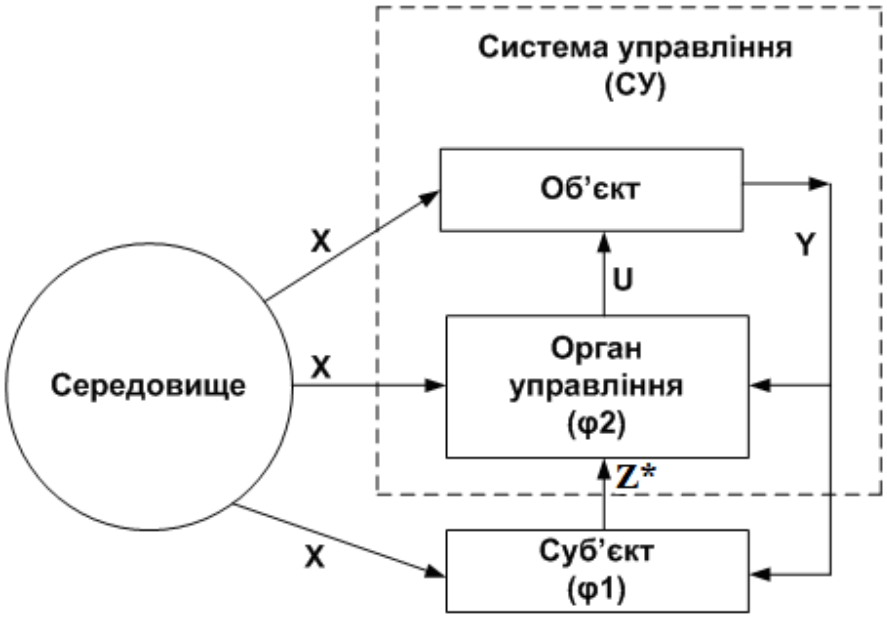


Рисунок 1.2 – Узагальнена функціональна схема взаємодії суб'єкта і об'єкта управління, зовнішнього середовища та органу управління

Суб'єкт ставить задачі і регламентує критерії управління, тоді як орган управління формує необхідні керуючі впливи та передає їх об'єкту для забезпечення заданого режиму його функціонування. Для реалізації цього суб'єкт управління має насамперед поставити (сформулювати) мету управління та передати її органу управління. У загалі мета управління визначає бажаний стан об'єкта, якого є необхідність досягти за наявних умов функціонування зовнішнього середовища X і поточних потреб суб'єкта A_t. Іншими словами, вона характеризує такий стан об'єкта управління, за якого потреби суб'єкта можуть бути задоволені у найбільш повній мірі з урахуванням існуючих обмежень і впливу зовнішніх факторів. У загальному вигляді мету управління можна подати таким чином [7, 10]:

$$Z^* = \varphi_1(A_t, X), \tag{1.4}$$

де Z^* – мета управління;

φ_1 – алгоритм, що дозволяє досягти мети за потребами суб'єкта A_t та відповідним станом середовища *X*.

У реальних телекомунікаційних системах або мережах реалізація поставленої мети управління покладається на СУ, яка на рис. 1.2 позначена штриховою лінією. Основним її призначенням є перетворення задач і потреб суб'єкта управління у відповідні керуючі впливи, що забезпечують досягнення необхідного стану об'єкта управління. Іншими словами, система управління здійснює формалізацію вимог суб'єкта та реалізує їх мовою параметрів і режимів функціонування об'єкта. За такого підходу безпосередня участь суб'єкта в процесі управління стає необов'язковою, оскільки всі функції аналізу поточного стану об'єкта, формування керуючих впливів і реалізації алгоритму управління виконує система управління відповідно до заданих правил і критеріїв. Мета управління, як правило, задається за допомогою сукупності цільових змінних, значення яких визначає суб'єкт управління. Для КМ, наприклад, такими змінними можуть бути пропускна здатність мережі, коефіцієнт бітових помилок, середня затримка передачі пакетів, рівень втрат пакетів, доступність мережних сервісів та інші показники, що характеризують ефективність функціонування мережі.

1.3 Базові функціональні категорії управління телекомунікаційними мережами

Ефективне функціонування сучасних телекомунікаційних мереж, у тому числі і КМ, можливе лише за умови реалізації постійного і ефективного управління, моніторингу та контролю. Це обумовлено безперервним розвитком мережних структур, зміною вимог користувачів до якості надання послуг, появою нових технологій ПД, мережних протоколів і сервісів, а також необхідністю забезпечення стійкої роботи мереж в умовах відмов окремих елементів, зміни топології та постійного зростання обсягів інформаційного трафіку. За таких умов виникає потреба у організації і використання спеціалізованих СУ.

У загальному випадку будь-яку телекомунікаційну мережу можна представити як сукупність двох взаємопов'язаних підсистем: об'єкта управління, який включає мережну інфраструктуру та її компоненти, і системи управління, що здійснює моніторинг, аналіз стану мережі, формування керуючих впливів та

контроль їх реалізації. Взаємодія між цими підсистемами здійснюється шляхом обміну керуючою та службовою інформацією, що забезпечує своєчасне реагування на зміни стану мережі та підтримку необхідних режимів її функціонування. Незалежно від архітектури мережі, типу її обладнання чи технологій ПД, що нею підтримуються, необхідно, щоб СУ виконувала визначений набір базових функціональних задач (функціональних категорій), що є стандартизованими міжнародними організаціями. Зокрема, рекомендація ITU-T X.700 і подібний до неї стандарт ISO/IEC 7498-4 визначають п'ять основних функціональних категорій щодо реалізації управління мережею (так звана модель **FCAPS**), до яких належать [7]:

- управління відмовами (**F**ault Management, FM) – виявлення, локалізація, діагностика та усунення несправностей у мережі;

- управління конфігурацією (**C**onfiguration Management, CM) – конфігурування, облік і підтримка працездатного стану мережного обладнання;

- облік використання мережних ресурсів (**A**ccounting Management, AM) – збір статистичної інформації щодо використання мережних ресурсів і послуг;

- управління продуктивністю (**P**erformance Management, PM) – контроль продуктивності, використання ресурсів мережі та оцінка показників QoS її функціонування;

- управління безпекою (**S**ecurity Management, SM) – забезпечення захисту мережних ресурсів і контролю доступу до них.

Розглянемо ці функціональні категорії управління більш детально.

1) Управління відмовами.

Основним призначенням цієї функціональної категорії є своєчасне виявлення, локалізація, діагностика та усунення несправностей, що виникають під час функціонування мережі. Реалізація функціональних задач, що входять у цю категорію, забезпечує підтримку необхідного рівня доступності мережних ресурсів, мінімізацію часу простою обладнання та зменшення впливу відмов на роботу користувачів і мережних сервісів. У процесі управління відмовами СУ не лише реєструє повідомлення про несправності, але й також виконує їх попередню обробку, фільтрацію, маршрутизацію та аналіз. Зокрема [7]:

- фільтрація дозволяє відокремити критично важливі повідомлення від великої кількості інформаційних подій, що є характерним, наприклад, для сучасних корпоративних КМ;

- маршрутизація забезпечує передачу повідомлень відповідним компонентам СУ або адміністратору мережі;

- кореляційний аналіз дає змогу знайти першопричину виникнення взаємопов'язаних подій, що призвели до збою або аварійної ситуації. Наприклад, пошкодження каналу зв'язку або відмова комутатора може одночасно спричинити появу великої кількості повідомлень про недоступність серверів, мережних сегментів чи прикладних сервісів.

FM може здійснюватися як в автоматичному, так і в напівавтоматичному режимах. У першому випадку наявна СУ самостійно виконує передбачені алгоритмом дії, наприклад, перемикання трафіку на резервні канали, активацію резервного обладнання або перезапуск окремих програмних служб. В напівавтоматичному режимі СУ здійснює моніторинг процесу усунення несправності, надає адміністратору необхідну діагностичну інформацію, формує повідомлення про аварійну ситуацію, реєструє виконані операції та контролює послідовність виконання робіт, тоді як остаточні рішення щодо відновлення працездатності мережі приймає обслуговуючий персонал [7].

У межах FM часто окремо виділяють до розгляду задачі управління проблемами (Problem Management, PbM). На відміну від оперативного реагування на окремі відмови, аварії чи збої, функціональна група PbM спрямована на аналіз причин виникнення складних несправностей або тих, повторюються, визначення їх першоджерела та розробку заходів, які дозволять завчасно запобігти їх повторному виникненню [7]. Такий підхід сприяє підвищенню надійності, відмовостійкості та ефективності функціонування мережі в цілому.

2) Управління конфігурацією.

Ця функціональна категорія виконує задачі, що пов’язані з обліком, налаштуванням та підтримкою робочого стану мережної платформи. До її основних задач належать конфігурування параметрів окремих мережних пристроїв, управління їх конфігураціями, а також моніторинг і контроль структури та топології мережі в цілому. На рівні окремих мережних елементів (Network Elements, NE), до яких належать маршрутизатори, комутатори, точки бездротового доступу, сервери та інше мережне обладнання, СУ забезпечує призначення і зміну мережних адрес, ідентифікаторів, параметрів інтерфейсів, службових характеристик, а також ведення інформації про місцезнаходження обладнання та інші його експлуатаційні параметри [7].

На рівні мережі в цілому процес здійснення управління конфігурацією охоплює формування та підтримку актуальної топологічної моделі мережі, яка відображає взаємозв'язки між мережними елементами. Крім цього, здійснюється контроль змін топології, які пов'язані із введенням в експлуатацію нового обладнання, виведенням окремих вузлів із роботи, створенням або вилученням фізичних і логічних каналів зв'язку, а також оновленням таблиць комутації та маршрутизації [7].

СМ може бути реалізоване в автоматичному, ручному або напівавтоматичному режимах. У першому випадку СУ самостійно виконує виявлення мережних пристроїв, збирає інформацію про їх конфігурацію та автоматично формує топологічну карту мережі на основі аналізу службових протоколів і мережного обміну. У ручному режимі всі зміни вносяться безпосередньо адміністратором мережі. Найбільш поширеним є напівавтоматичний режим, у якому СУ автоматично формує конфігурацію та топологічну модель мережі, а адміністратор перевіряє отримані результати, і за потреби коригує їх та підтверджує внесення змін. Слід зазначити, що алгоритми автоматичного виявлення мережної топології та побудови її моделі у значній мірі залежать від архітектури конкретної СУ, що є однією з важливих функціональних особливостей пропрієтарного програмного забезпечення (ПЗ) від конкретних виробників мережного обладнання [7].

3) Облік використання мережних ресурсів.

Ця функціональна категорія призначена для збору, накопичення та аналізу інформації щодо використання ресурсів мережі та окремих сервісів її користувачами. Зокрема, до основних задач АМ належать реєстрація часу використання мережних пристроїв і сервісів, каналів зв'язку, серверних ресурсів та інших її компонентів. Отримані дані використовуються для ведення мережної статистики, аналізу навантаження, подальшого планування використання ресурсів, а також для реалізації механізмів обліку спожитих послуг і розрахунку вартості їх використання (billing). Крім цього, результати обліку можуть застосовуватися для здійснення контролю щодо дотримання умов угоди про рівень надання послуг (Service Level Agreement, SLA) і прогнозування потреб у подальшому розвитку мережі [7].

Залежно від призначення мережі функції АМ можуть реалізовуватися по-різному. Наприклад, у корпоративних КМ вони здебільшого використовуються для внутрішнього обліку ресурсів, аналізу завантаження мережі та формування

статистичної звітності. Натомість у мережах великих телекомунікаційних провайдерів, ці функції додатково забезпечують тарифікацію послуг, що надаються користувачам, автоматизований розрахунок їх вартості та взаємодію з системами біллінгу. Саме тому механізми АМ часто інтегруються зі спеціалізованими біллінговими платформами або реалізуються як окремі програмні модулі, що враховують вимоги конкретної організації чи сервіс провайдера.

4) Управління продуктивністю.

Ця функціональна категорія призначена для здійснення безперервного контролю, аналізу та оцінки ефективності функціонування мережі на основі статистичної інформації, що збирається та накопичується системою моніторингу. До основних показників, які аналізуються в межах PM, належать час відгуку мережевих сервісів, пропускна здатність каналів зв'язку, інтенсивність мережного трафіку, рівень використання мережних ресурсів, затримка передачі пакетів, їх варіація (джитер), втрати пакетів, коефіцієнт бітових помилок, а також показники доступності і готовності окремих мережних пристроїв, сервісів або мережі в цілому. Отримані результати використовуються як для здійснення оперативного управління мережею, так і для довгострокового планування її розвитку. Аналіз продуктивності дозволяє своєчасно виявляти перевантажені ділянки мережі, прогнозувати потребу в розширенні пропускної здатності каналів зв'язку, оптимізувати розподіл мережних ресурсів, що в цілому підвищує ефективність функціонування мережі. Крім цього, постійний контроль за показниками надійності дає змогу оцінити стабільність роботи обладнання, визначати тенденції до виникнення відмов та своєчасно робити профілактичне технічне обслуговування [7].

Однією із важливих практичних задач PM є контроль виконання вимог угоди SLA, яка визначає показники якості функціонування мережі, гарантовані постачальником послуг або адміністратором мережі. До таких показників можуть належати коефіцієнт доступності мережі, максимально допустимий час усунення відмов, середня та гарантована пропускна здатність каналів зв'язку, максимальна затримка передачі пакетів, допустимий рівень їх втрат та інші параметри, що характеризують користувачів. Звідси можна бачити, що PM забезпечує об'єктивну оцінку поточного стану мережі, дозволяє контролювати потрібну QoS та є основою для прийняття рішень щодо оптимізації роботи, модернізації і подальшого розвитку мережі [7].

5) Управління безпекою.

Ця функціональна категорія призначена для забезпечення захисту мережі та її інформаційних ресурсів і сервісів від несанкціонованого доступу, випадкових або навмисних порушень їх функціонування, а також інших загроз інформаційній безпеці. До базових функцій SM належать аутентифікація користувачів і мережних пристроїв, авторизація та розмежування прав доступу, ведення журналів подій безпеки, контроль виконання політик безпеки, управління криптографічними ключами, використання механізмів шифрування інформації, а також виявлення та реєстрація спроб несанкціонованого доступу до ресурсів [7].

Зазначимо, що у комп'ютерних мережах реалізація функцій SM, як правило, здійснюється не лише засобами СУ мережею, а й спеціалізованими програмно-апаратними комплексами. До них належать зокрема міжмережні екрани (Firewall), системи виявлення та запобігання зловмисним вторгненням, системи автентифікації та централізованого управління доступом, засоби криптографічного захисту інформації, рішення для організації віртуальних приватних мереж (Virtual Private Network, VPN) та інші компоненти комплексної системи інформаційної безпеки. Треба зазначити, що значна частина механізмів SM інтегрується безпосередньо в операційні системи (ОС), мережне обладнання та серверне ПЗ.

Також треба зауважити, що поділ функціональних задач управління на відповідні функціональні категорії, практично в сучасних СУ представляється у вигляді багаторівневих ієрархічних моделей. Найбільш опрацьованою і ефективною такою багаторівневою моделлю є система управління на основі стандарту TMN, який забезпечує управління мережами електрозв'язку та послугами, що ними надаються, шляхом організації взаємодії між компонентами різних телекомунікаційних мереж на основі їх стандартизованих інтерфейсів і діючих протоколів.

2 АНАЛІЗ КОНЦЕПЦІЇ TMN В АСПЕКТІ РЕАЛІЗАЦІЇ СИСТЕМИ УПРАВЛІННЯ І МОНІТОРИНГУ КОМП'ЮТЕРНИМИ МЕРЕЖАМИ

2.1 Система управління у відповідності із стандартом TMN

Мережа управління телекомунікаціями (TMN) запропонована ITU-T у 1996 році та являє собою багаторівневу ієрархічну модель СУ, що призначена для опису процесів управління телекомунікаційними мережами та надання послуг. На кожному рівні ієрархічної архітектури TMN реалізуються однакові базові функціональні категорії задач управління, шо були проаналізовані у попередньому розділі, проте зміст і особливості виконання задач цих функціональних категорій визначаються призначенням відповідного рівня управління TMN. Зокрема, на нижніх рівнях основна увага приділяється контролю технічного стану мережних елементів (NE), їх конфігуруванню та оперативному реагуванню на відмови. На вищих рівнях управління інформація узагальнюється та використовується для аналізу ефективності функціонування мережі, планування її розвитку, управління послугами, ресурсами та бізнес-процесами. По міру переходу від нижчих рівнів моделі до вищих зростає ступінь узагальнення інформації, що надходить із мережі. При цьому технічні параметри функціонування окремих NE поступово трансформуються в узагальнені показники, які характеризують якість надання послуг, ефективність використання ресурсів, економічні показники діяльності мережі та інші аспекти, необхідні для прийняття правильних управлінських і стратегічних рішень. Відповідно з цим концептуальну архітектуру моделі СУ на базі стандарту TMN стосовно описаних раніше функціональних категорій задач управління можна представити у вигляді двомірного подання (рис. 2.1) [7, 11].

В цій моделі реалізовано комплексний підхід щодо організації управління мережами зв'язку – від управління бізнес-процесами та послугами (верхні рівні) до управління конкретним мережним пристроєм або іншим елементом мережного обладнання [11].

Рівень мережних елементів (NE) включає окремі компоненти мережі, зокрема такі як канали зв'язку, мультиплексори, маршрутизатори, комутатори, сервери, кінцеве обладнання користувачів, тощо. Більшість сучасних NE оснащуються вбудованими засобами моніторингу і управління, до яких належать

датчики, лічильники, інтерфейси управління та інші апаратно-програмні компоненти, що забезпечують контроль їх технічного стану і параметрів функціонування [7, 11].

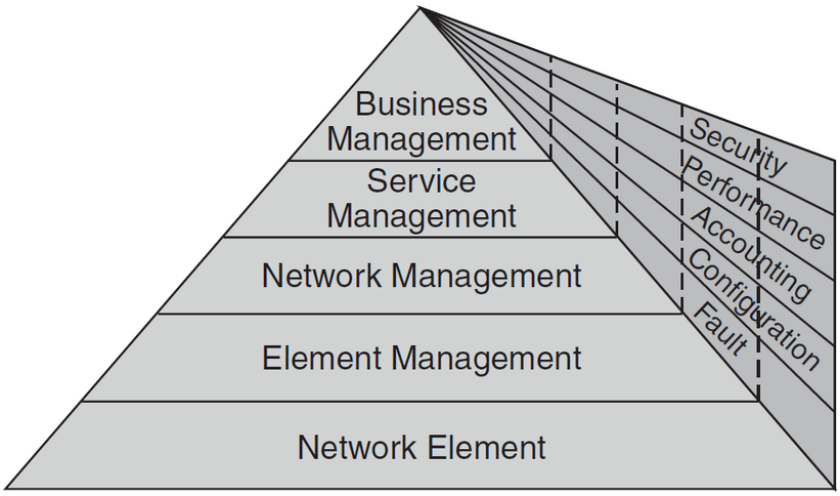


Рисунок 2.1 – Концептуальна архітектура моделі СУ на базі стандарту TMN

Сучасні мережні технології, зокрема Ethernet, FDDI, IP, SDH, підтримують вбудовані механізми моніторингу та управління. Це дозволяє здійснювати контроль за функціонуванням обладнання, збір статистики щодо передачі трафіку, виявлення аварійних ситуацій і зміну окремих параметрів конфігурації без використання додаткових апаратних засобів. У таких випадках функції управління реалізуються безпосередньо спеціалізованим ПЗ відповідно до вимог тих мережний технологій, якими здійснюється управління [7].

У випадку, коли обладнання мережі не підтримує необхідних засобів моніторингу та управління, для взаємодії із СУ використовують спеціалізовані програмно-апаратні модулі або агенти управління. Зокрема може застосовуватися протокол SNMP (механізм моніторингу «агент - менеджер» або протокол загальної керуючої інформації (Common Management Information Protocol, CMIP), який належать до прикладного рівня еталонної моделі OSI.

Рівень управління мережними елементами (Network Element Management, NEM) об'єднує локальні СУ, що здійснюють контроль, конфігурування та моніторингу окремих NE. Такі системи забезпечують автономне управління конкретними пристроями або їх функціональними модулями, наприклад каналом передачі SDH, маршрутизаторами, комутаторами, мультиплексорами, серверами та іншим мережним обладнанням [7, 11].

На цьому рівні особливості функціонування конкретних моделей обладнання різних виробників приховуються від вищих рівнів СУ. Для цього формуються уніфіковані моделі NE, які описують їх стан, конфігурацію, параметри функціонування та доступні ресурси. Атрибути таких моделей використовуються для отримання інформації про стан обладнання і зміни його конфігурації, а також здійснюється контроль продуктивності роботи обладнання та реалізуються інші функції управління. Частіше за все локальні СУ розробляються виробниками мережного обладнання, тобто є пропрієтарними системами. Вони постачаються разом із відповідними програмними засобами адміністрування. Прикладами таких систем є Cisco Prime Infrastructure, Juniper Junos Space, Huawei eSight, а також інші спеціалізовані системи управління, що призначені для моніторингу, конфігурування та технічного обслуговування обладнання конкретного виробника [7].

Рівень управління мережею (Network Management, NM) призначений для централізованого управління мережею як єдиною інфокомунікаційною системою. На цьому рівні координується робота локальних СУ мережними елементами, забезпечується узгоджене функціонування окремих сегментів мережі, а також організується контроль їх взаємодії незалежно від технологій, що використовуються, та типів обладнання. Основними задачами цього рівня є управління конфігурацією мережі, контроль її топології, координація роботи транспортних підмереж, оптимізація маршрутів передачі даних, аналіз продуктивності та забезпечення необхідного рівня QoS функціонування мережі. Завдяки цьому окремі мережні елементи і локальні СУ об'єднуються в єдину систему, що забезпечує узгоджений обмін даних між користувачами, мережними сервісами та прикладними додатками. Саме тут формується цілісне уявлення про стан мережі, що дозволяє ефективно реалізовувати функції моніторингу, контролю, аналізу та централізованого управління нею [7, 11].

Рівень управління послугами (Service Management, SM) призначений для управління послугами, що надаються користувачам. До його основних функцій належать підготовка мережі до надання послуг, їх активація, модифікація, супровід, а також обробка запитів від користувачів. Також на цьому рівні визначаються параметри послуг, зокрема необхідна пропускна здатність, допустимі затримки передачі пакетів, коефіцієнт готовності та інші показники QoS. Відповідно з цим формуються завдання для рівня управління мережею щодо конфігурування необхідних мережних ресурсів, зокрема фізичних або

віртуальних каналів зв'язку. Рівень SM забезпечує контроль якості надання послуг, оцінює відповідність їх параметрів встановленим вимогам та забезпечує контроль за виконанням угод про рівень надання послуг (SLA) між користувачами та оператором. Отримані результати можуть використовуватися для аналізу QoS, формування статистичної звітності та обліку використання мережних послуг [7, 11].

Рівень управління бізнес-процесами (Business Management, BM) є найвищим рівнем архітектури TMN і призначений для стратегічного управління розвитком телекомунікаційної мережі з урахуванням економічних та організаційних аспектів діяльності мережного оператора або підприємства, де розгорнута мережа. На цьому рівні здійснюється планування розвитку мережі, аналізуються доходи і витрати, робиться оцінка ефективності використання ресурсів, а також приймаються рішення щодо модернізації мережі та впровадження нових послуг. Також тут забезпечується підтримку процесів щодо планування, організації та розвитку мережних послуг у урахуванням потреб користувачів, вимог ринку та фінансових можливостей підприємства.

З урахуванням широкого спектру задач, що вирішуються платформою управління TMN, існує декілька підходів, які дозволяють описати її можливі напрямки застосування в рамках організації мережного управління. Кожен такий підхід ґрунтується на відповідній архітектурній моделі управління, що відображає ті властивості TMN, які найбільш повно відповідають потрібному напрямку застосування. Згідно до рекомендації ITU-T M.3010, де наводяться загальні поняття організації управління TMN, також виділяється декілька архітектурних моделей управління в аспекті різних підходів застосування управління на базі концепції TMN, серед яких найпоширенішими є три [7, 12]:

- функціональна архітектура визначає склад функцій управління, їх призначення, взаємозв'язок і порядок взаємодії між окремими компонентами СУ. Вона встановлює, які функції має виконувати система для забезпечення ефективного моніторингу, контролю, конфігурування, аналізу продуктивності, підтримки безпеки та обліку використання мережних ресурсів;

- фізична архітектура описує способи реалізації функцій управління засобами програмного і апаратного забезпечення. Вона визначає склад фізичних компонентів СУ, їх взаємодію, розподіл функцій між серверами управління,

робочими станціями адміністраторів, мережними елементами, агентами управління та каналами передачі службової інформації;

- інформаційна архітектура визначає принципи подання, структурування, зберігання та обміну інформацією між усіма компонентами СУ на основі об'єктно-орієнтованого підходу відповідно до стандартів моделі OSI. Вона регламентує способи опису мережних ресурсів, параметрів їх функціонування, подій і керуючих впливів, що забезпечує уніфіковану взаємодію між різними системами та засобами управління. Ця архітектурна модель TMN найбільш цікава у контексті реалізації систем моніторингу і контролю комп'ютерних мереж, що є ключовою задачею цієї кваліфікаційної роботи, тому що вона за своїми властивостями є основою для організації процесів збору, передачі, зберігання та аналізу інформації про стан мережного обладнання, мережного трафіку, продуктивності та подій безпеки. Саме в ній закладені принципи обміну інформацією управління на основі підходу «агенти - менеджер», що також застосовуються і в інших моделях реалізації мережного управління (наприклад, на основі протоколу SNMP). Крім того, ця архітектурна модель забезпечує механізми інтеграції систем моніторингу з іншими компонентами СУ мережею.

Тому далі розглянемо цю архітектурну модель більш докладно.

2.2 Інформаційна архітектурна модель TMN, як базовий механізм забезпечення аналізу даних в системі управління

На технологічному рівні реалізація управління мережами являє собою процес обробки інформації, яка надходить від **NE**, за допомогою спеціалізованих програмних засобів СУ. При цьому виникає необхідність у організації інформаційної взаємодії між великою кількістю мережних пристроїв і обладнанням телекомунікаційної мережі, а також мережними операторами та постачальниками мережних сервісів і послуг.

Для реалізації такої взаємодії в концепції TMN була створена інформаційна архітектурна модель, яка базується на об'єктно-орієнтованому підході до організації обміну інформацією управління між компонентами мережі. Одним із її базових механізмів є модель «менеджер - агент», що забезпечує збір, передачу, обробку та подальше зберігання керуючої інформації в системах управління і

моніторингу телекомунікаційних мереж. Обмін інформацією між менеджером та агентом здійснюється за допомогою функцій ПД (Data Communication Function, DCF) і функцій передачі повідомлень (Message Communication Function, MCF). Вони забезпечують виконання таких функціональних завдань, як маршрутизація, переприйняття, ретрансляція повідомлень та взаємодія між компонентами СУ, що дозволяє організувати ефективний інформаційний обмін інформацією управління між агентами та менеджерами. Крім того, інформаційна архітектурна модель TMN передбачає використання принципів доменів (областей) управління та доменів знань, які забезпечують розподіл функцій управління між окремими компонентами системи, підвищують її масштабованість і спрощують адміністрування великих телекомунікаційних мереж [7, 12].

Взаємодію між менеджером, агентом та фізичними і/або інформаційними ресурсами, які знаходяться під управлінням, наведено на рис. 2.2.

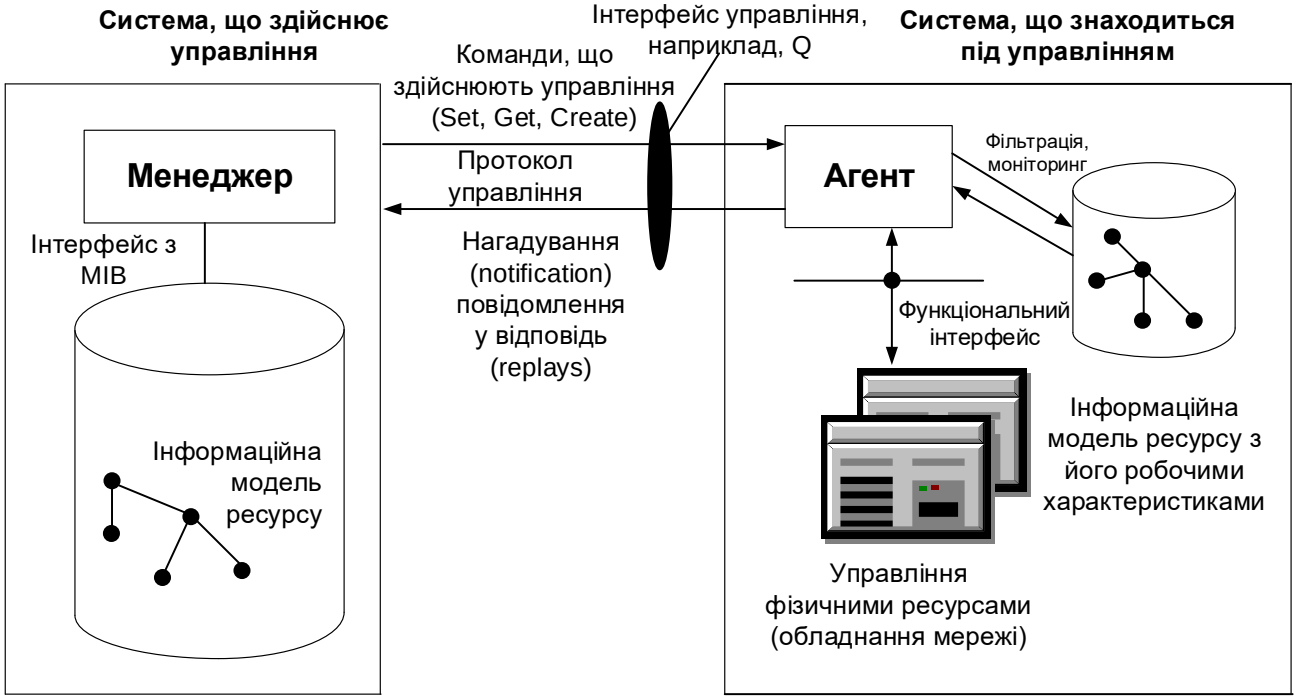


Рисунок 2.2 – Схема взаємодії між менеджером, агентом та ресурсами, що знаходяться під управлінням

В інформаційній архітектурній моделі TMN програмний модуль, який формує команди управління, приймає повідомлення від мережних елементів та безпосередньо координує процес управління, називається «менеджером». Натомість програмний модуль, що функціонує безпосередньо на тому чи іншому

NE, називається «агентом». Основним призначенням агентів є виконання команд, що надходять до нього від менеджера, а також він здійснює збір інформації про стан ресурсу, що знаходиться під управлінням, та передачу результатів виконання операцій або повідомлень про його поточний стан. Вони можуть здійснювати моніторинг і контроль широкого спектру параметрів мережних ресурсів та обладнання, як [7]:

- кількість і поточний стан віртуальних каналів;
- кількість повідомлень про проблемні ситуації та відмови різних типів;
- обсяг вхідного та вихідного мережного трафіку (у байтах або пакетах) для окремих мережних пристроїв або їх груп;
- здійснювати контроль за максимальною довжино черг на вході та виході мережних пристроїв, зокрема маршрутизаторів і комутаторів;
- кількість переданих і прийнятих широкомовних повідомлень;
- стан мережних інтерфейсів та інтерфейсів користувача, включаючи виявлення інтерфейсів, що вийшли з ладу або були повторно введені в експлуатацію.

Для реалізації процесу управління між менеджером і агентом створюється логічний канал взаємодії, через який здійснюється обмін інформацією управління. Після створення такого каналу зв'язку менеджер надсилає агенту відповідні команди, а агент виконує необхідні дії щодо ресурсу, що знаходиться під управлінням, та повертає інформацію про результати їх виконання або підтверджує успішне завершення операції. При цьому як менеджер, так і агент здійснюють контроль стану створеного з'єднання, що дозволяє своєчасно виявляти його порушення, що тим самим забезпечує надійність процесу управління [7, 12].

У такій моделі агент виконує роль проміжної ланки між менеджером та фізичним або програмним ресурсом, що знаходяться під управлінням. За допомогою відповідних функціональних інтерфейсів він взаємодіє з мережним обладнанням і пристроями, отримує інформацію про їх поточний стан, а також забезпечує виконання команд управління. Для опису контрольованого ресурсу агент використовує деяку інформаційну модель, яка має містити сукупність його характеристик і параметрів, що можуть контролюватися або змінюватися в процесі функціонування СУ. Аналогічна інформаційна модель підтримується також і менеджером, тому обидва ці програмні модулі використовують узгоджене подання ресурсу, яким здійснюється управління. Водночас інформаційна модель, що

організується менеджером, є буде більш повною, регламентованою і системно-організованою, тому що вона формується на основі даних, що надходять від багатьох агентів, і кожен з них перед здійсненням передачі зібраної інформації виконує її попередню обробку. Зокрема агенти відфільтровують другорядні дані, що не відповідають запиту від менеджера, та відкидають ті дані, що надійшли з помилками або були явно спотворені. Це зменшує обсяг службового трафіку і підвищує ефективність функціонування СУ. Крім того, менеджер може одночасно підтримувати інформаційні моделі великої кількості ресурсів, якими здійснюється управління, завдяки чому забезпечується централізований моніторинг і управління всією мережею [7].

Один менеджер може одночасно взаємодіяти з декількома агентами, а один агент, у свою чергу, може обслуговувати запити від кількох менеджерів. Така організація інформаційної взаємодії забезпечує централізоване управління великою кількістю NE і підвищує масштабованість СУ.

У телекомунікаційних мережах, управління якими організовано відповідно до концепції TMN, взаємодія між менеджером та агентом здійснюється з використанням протоколу CMIP та сервісу загальної інформації управління (Common Management Information Service, CMIS), які визначені рекомендаціями ITU-T X.711 та ITU-T X.710. Якщо ж реалізується концепція управління комп’ютерними мережами різного рівня ієрархії або в мережі Інтернет, то тут так взаємодія між менеджерами і агентами переважно реалізується за допомогою протоколу SNMP. Первісно цей протокол було розроблено для контролю стану маршрутизаторів і мостів мережі Internet, однак у процесі його розвитку сфера застосування значно розширилася. На сьогодні SNMP підтримується більшістю мережного обладнання, серверних ОС і програмних платформ, тому він став фактичним стандартом управління та моніторингу всіх комп'ютерних мереж, що орієнтовані на підтримку стеку TCP/IP. Основні принципи функціонування протоколу SNMP визначено документом RFC 1157 «Simple Network Management Protocol (SNMP)», який створено робочою групою IETF (Internet Engineering Task Force). Незважаючи на те, що SNMP реалізує модель взаємодії «менеджер - агент», яка є аналогічною концепції TMN, цей протокол не входить до переліку офіційних протоколів управління, що є стандартизованими ITU-T для архітектури TMN.

Також треба зазначити, що між протоколами CMIP і SNMP існують певні відмінності у трактуванні поняття «ресурс під управлінням». У протоколі CMIP «ресурс під управлінням» – це повний опис фізичного або логічного ресурсу

мережі разом із його властивостями, взаємозв'язками та операціями, що ним підтримуються. Натомість у протоколі SNMP «ресурс під управлінням» зазвичай відповідає окремому параметру або характеристиці мережного ресурсу, наприклад значенню лічильника переданих пакетів, кількості помилок, завантаженню процесора чи стану мережного інтерфейсу. Такий підхід значно спрощує процес реалізації систем моніторингу, зменшує обсяг службового трафіку, що і забезпечує високу ефективність використання протоколу SNMP у сучасних комп'ютерних мережах [7].

Інформаційну модель агента часто називають базою даних управляючої інформації (Management Information Base, MIB). База MIB є віртуальним інформаційним масивом, який містить у формалізованому та упорядкованому вигляді інформацію, що пов’язана з мережею зв’язку і з мережним обладнанням. У MIB зберігаються атрибути об’єктів, що знаходяться під управлінням, описи класів, які відповідають елементам мережі. MIB є по суті абстрактним описом характеристик ресурсів, якими здійснюється управління, тобто обладнання та систем зв’язку, і дозволяє зберігати опис дій (операцій управління), які можна здійснювати над об’єктами, що знаходяться під управлінням. Іншими словами, MIB дозволяє програмним додаткам управління (в першу чергу агенту, потім менеджеру) отримувати інформацію про об’єкти, що знаходяться під управлінням. Менеджер також підтримує MIB, але база даних менеджера вторинна по відношенню до бази даних агента з причин, які були перераховані вище. Для оновлення своєї бази даних менеджер завжди запитує агента [7].

Ресурси, які контролюються, мають можливість самостійно формувати повідомлення про свій поточний стан у разі виникнення певних подій. Такі повідомлення (сповіщення) генеруються, коли відбуваються зміни, що можуть вплинути на функціонування мережі або потребують уваги адміністратора мережі. Наприклад, це може бути створення або видалення ресурсу, який контролюється, зміна значень його параметрів, виникнення несправності чи інша подія, яка характеризує зміну стану ресурсу. Передача повідомлень (сповіщень) від агентів до менеджера може здійснюватися як безпосередньо, так і через спеціальні об'єкти, що називаються дискримінаторами передачі подій. Їх основним призначенням є фільтрація повідомлень, які надходять від агентів, відповідно до встановлених критеріїв або рівня їх важливості. Завдяки цьому менеджер отримує лише ті повідомлення, які є суттєвими для здійснення процесу управління та моніторингу. Наприклад, повідомлення про критичну аварійну ситуацію або збій

можуть передаватися негайно, тоді як повідомлення про менш важливі події щодо виникнення менш критичних нештатних ситуацій обробляються після завершення реагування на першочергові критичні ситуації. Такий підхід зменшує інформаційне навантаження на СУ та забезпечує своєчасне реагування на найбільш важливі події [7].

Ще однією характерною особливістю інформаційної моделі TMN є використання асинхронного принципу обміну повідомленнями під час передачі команд управління. У цьому випадку менеджер і агент взаємодіють шляхом обміну службовими повідомленнями без необхідності постійної підтримки синхронного режиму зв'язку, що підвищує ефективність функціонування СУ у великих телекомунікаційних мережах.

Усі операції, які виконуються над ресурсами, якими здійснюється управління, реалізуються за допомогою чотирьох основних типів повідомлень (що мають назву примітивів): запитів, вказівок, відповідей і підтверджень. Послідовність їх використання є такою [7]:

- менеджер надсилає агенту повідомлення-запит, яке містить команду на виконання певної операції;

- після отримання цього повідомлення агент інтерпретує його як вказівку до виконання відповідної дії;

- виконавши необхідну операцію над ресурсом, що знаходиться під управлінням, агент формує повідомлення-відповідь із результатами її виконання;

- повідомлення-відповідь надходить до менеджера в якості підтвердження успішного виконання запиту.

Треба зазначити, що повідомлення-відповідь передається агентом лише у випадку, якщо це було передбачено початковим запитом від менеджера.

У загалі розглянута інформаційна модель TMN є абстрактним підходом щодо здійснення управління мережними ресурсами та відповідних супутніх цьому процесу операцій управління. Вона пропонує єдині принципи подання, зберігання, передачі та обробки інформації, що формується в процесі функціонування СУ мережею. Оскільки інформаційна модель належить до прикладного рівня OSI, вона забезпечує взаємодію із прикладними додатками та сервісами, що реалізують функції моніторингу, контролю та управління, а також зберігання, пошуку та аналізу інформації про стан комп'ютерної мережі або будь якої телекомунікаційної мережі [7].

3 АНАЛІЗ ОСОБЛИВОСТЕЙ І АРХІТЕКТУРНИХ ПІДХОДІВ ОРГАНІЗАЦІЇ СИСТЕМИ МОНІТОРИНГУ ТА КОНТРОЛЮ КОМП'ЮТЕРНОЇ МЕРЕЖІ

3.1 Загальні особливості і функції систем моніторингу та контролю для комп'ютерних мереж

Моніторинг та контроль (МтК) функціонування КМ, що формує інформаційну структуру будь-якого підприємства – від невеликої компанії до великого ЦОД хмарного провайдера, – необхідні для того, щоб адміністратори та мережні інженери вчасно отримували повідомлення про можливі аварійні ситуації та поточні проблеми в мережній інфраструктурі. По суті, з практичної точки зору, МтК — це комплекс заходів із швидкого виявлення проблеми, оповіщення про неї адміністраторів, а також діагностики, яка надає повну і точну інформацію про проблему. Система МтК в КМ дозволяє здійснювати автоматизоване управління роботою додатків і сервісів, що забезпечуються ресурсами мережі. Додатково можливе здійснення моніторингу стану інженерних систем в режимі реального часу, оперативне управління обладнанням, розмежування доступу до інформації. При цьому всі функції управління можуть бути доступні з єдиного інтерфейсу користувача [13].

Організація системи МтК також необхідна для автоматичної підтримки оптимальних режимів роботи обладнання та оперативного запобігання його збоям. Наявність таких централізованих систем дозволяє скоротити час простою мережі у разі надання послуг користувачам та доступу до ресурсів (наприклад, внаслідок збоїв у роботі або у зв'язку з регламентним технічним обслуговуванням обладнання). Таким чином, система моніторингу та контролю інфраструктури КМ має забезпечити [13]:

- безперервний моніторинг усіх мережних параметрів роботи КМ;
- швидке оповіщення персоналу та користувачів у разі виникнення аварійних ситуацій та збоїв у роботі мережі;
- скорочення та оптимізацію експлуатаційних витрат;
- забезпечення постійного централізованого контролю всіх основних мережних параметрів КМ.

Основною задачею системи МтК є надання актуальної інформації для аналізу стану КМ, а також оперативне виявлення аварійних ситуацій або зниження продуктивності в роботі мережних сегментів та окремих компонентів і

швидке усунення причин. Наразі використовуються автоматизовані та напівавтоматизовані системи моніторингу, які аналізують стан мережі та збирають інформацію у спеціалізовані сховища з можливістю її подальшого аналізу адміністратором для здійснення прийняття рішення. Для зберігання отриманої інформації зазвичай використовується конфігураційна база даних (БД), у якій інформація про об'єкти моніторингу представлена у вигляді набору конфігураційних одиниць. Іншими словами, усі мережні пристрої тут виступають у вигляді певних конфігураційних одиниць, інформація про які зберігається в централізованій БД. Таке подання дозволяє згодом інтегрувати систему МтК з графічними візуальними поданнями, такими як: діаграми, графіки, тощо [13].

Технологічні підходи до проведення моніторингу та сама його структура з часом зазнають значних змін. Наприклад, із появою хмарних обчислень та поширенням різних видів віртуалізації виникла необхідність здійснювати контроль за станом не лише фізичного сервера, а й віртуальних серверів, безліч яких може бути розгорнута на тому самому фізичному сервері у вигляді віртуальних машин [14].

Існують досить специфічні види моніторингу, наприклад, від імені кінцевого користувача, коли через задані інтервали часу циклічно імітуються його дії. Зазвичай це програмний бот або планувальник задач операційної системи (ОС) сервера, який запускає спеціальний, заздалегідь створений скрипт-сценарій, а потім автоматично формує звіт про дії, що були виконані в процесі своєї роботи, та про помилки, які виникли при цьому. Також систему моніторингу можна налаштувати за допомогою того самого планувальника задач на виконання будь-яких стандартних сервісних дій. Наприклад, очищати «кошик» комп'ютера, коли він заповнюється, або активувати архівування деяких файлів, коли окреслений відсоток фізичного дискового простору стає зайнятим [13, 14].

При виборі, розробці та впровадженні систем моніторингу спочатку необхідно визначитися з об'єктами, які будуть підлягати контролю, а також визначити важливі події та показники, про які система повинна збирати інформацію та, за необхідності, оперативно повідомляти адміністратору. Для цього весь процес функціонування КМ необхідно проаналізувати з точки зору послуг та інших ресурсів, що надаються нею користувачам. Далі для кожного такого сервісу встановлюється певний рівень якості його надання, після чого він описується в системі моніторингу та контролю як набір взаємопов'язаних компонентів інфраструктури КМ. Іншими словами, формується угода SLA, згідно з якою система здійснює збір та зберігання інформації про якість мережних

сервісів. У результаті, як зазначалося вище, на основі накопиченої та збереженої інформації формуються звіти за певний період часу [13, 14].

Системи моніторингу та управління можуть бути орієнтовані на мережі різного рівня. Для великих систем зазвичай використовується величезна кількість різноманітних функцій, для малих зазвичай достатньо загального аналізу вузлів та надсилання сповіщень. Серед основних функцій моніторингу та управління можна виділити такі [13]:

- спостереження – періодичний збір показників з мережного обладнання, сервісів, що надаються, додатків, тощо;

- зберігання інформації – виступає як додатковий механізм до функції спостереження. Проводиться збір інформації за основними показниками кожного об’єкта моніторингу, для зберігання зазвичай використовуються БД;

- створення звітів – здійснюється як на основі поточних даних спостереження, так і в результаті подальшого аналізу інформації, що була збережена. Наприклад, довгостроковий моніторинг навантаження на сервер може показати, що ресурси, які споживаються, мають тенденцію до постійного збільшення, з чого випливає, що необхідно зробити обчислювальні ресурси більш продуктивними, або перерозподілити задачі з іншим сервером, вибір якого також можна зробити на основі подібного звіту про продуктивність;

- візуалізація – надання звітів у вигляді графіків, спливаючих підказок, діаграм тощо, що дозволяє більш вільно та наочно сприймати інформацію. Для такої візуалізації, як правило, обирають кілька найважливіших параметрів, тоді як у звичайних звітах наводяться всі показники, за якими здійснюється моніторинг;

- пошук вузьких місць – на основі зібраних і проаналізованих даних моніторингу можна зробити висновок про «вузьке» місце в мережі, через яке знижуються загальні показники продуктивності;

- автоматизація сценаріїв – ця функція дозволяє автоматично виконувати процеси, що постійно повторюються, без залучення адміністраторів, що звільняє їх від рутинних завдань.

Завдяки наявності засобів для реалізації всіх цих функцій мережному адміністратору більше не потрібно перевіряти в ручному режимі стан кожного процесу системи моніторингу та контролю. У результаті мінімізується час на вирішення проблем у мережі та усунення аварійних ситуацій. Крім того, значно точніше й швидше здійснюється діагностика КМ, а також можна планувати модернізацію та розширення мережної інфраструктури.

3.2 Фундаментальна архітектура системи моніторингу та контролю

Фундаментальна архітектурна модель системи МтК організована відповідно до базових функціональних категорій управління, що були розглянуті у підрозділі 1.3, та концептуальної архітектури СУ на базі TMN, розглянутої в розділі 2 цієї пояснювальної записки. Вона також має багаторівневу ієрархічну структуру та забезпечує швидку та надійну взаємодію різних рівнів, зворотний зв’язок і досить високий рівень автономності кожного компонента системи (рис. 3.1). У відповідності із стандартами TMN, які лежать в її основі, вона підтримує відкриті прикладні програмні інтерфейси (Application Programming Interface, API) для забезпечення подальшої взаємодії з ПЗ сторонніх виробників. Це дозволяє реалізувати взаємопов’язане виконання всіх функціональних задач з оперативного управління, наприклад, забезпечення взаємодії з системами білінгу та складського обліку, обліку мережних ресурсів, управління персоналом, взаємодії з користувачами, тощо [15].

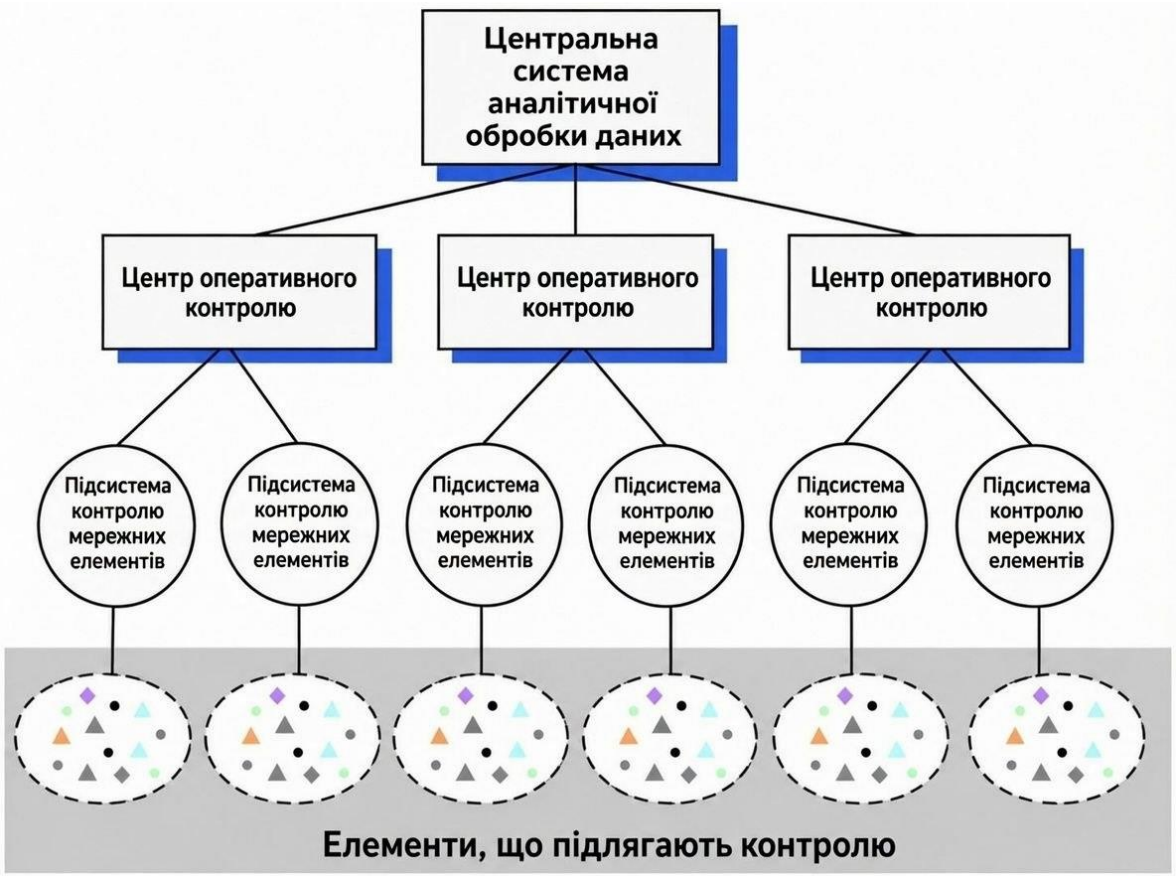


Рисунок 3.1 – Фундаментальна архітектурна модель системи моніторингу та контролю

Перш за все слід зазначити, що в наведеній на рис. 3.1 архітектурній моделі системи МтК задачі, що пов’язані з контролем стану мережі та з контролем/управлінням обслуговуванням (які відповідають рівням SM та NM концептуальної архітектури TMN, рис. 2.1) об’єднані в рамках центрів оперативного контролю. Такий підхід дозволяє скоротити час реагування на зміни стану мережі, забезпечити централізований аналіз отриманої інформації та підвищити ефективність прийняття рішень щодо підтримки працездатності мережної інфраструктури.

Нижній рівень моделі утворюють елементи, що підлягають контролю. До них належать мережні пристрої, сервери, канали зв'язку, кінцеве обладнання користувачів, програмні сервіси та інші компоненти КМ, стан яких необхідно постійно контролювати. Саме на цьому рівні формується первинна інформація про функціонування мережі, яка містить відомості про працездатність обладнання, використання мережних ресурсів, параметри трафіку, продуктивність окремих вузлів, виникнення аварійних подій та інші експлуатаційні показники.

На рівні підсистем контролю мережних елементів здійснюється безпосередній моніторинг окремих груп мережних пристроїв. Тут проводиться збір телеметричних даних, контроль технічного стану обладнання, первинна обробка отриманої інформації, виявлення несправностей і передача результатів моніторингу до вищого рівня системи. Функціонально цей рівень відповідає рівню NEM архітектури TMN (рис. 2.1), оскільки забезпечує взаємодію безпосередньо з мереженим обладнанням та засобами його контролю.

Вище знаходиться рівень, що утворюється центрами оперативного контролю. Вони координують роботу підпорядкованих підсистем контролю мережних елементів. Як вище було зазначено, тут, на відміну від архітектурної моделі TMN, об'єднано функції управління мережею (NM) та управління мережними послугами (SM). Центри оперативного контролю здійснюють аналіз аварійних подій, проводять оцінку продуктивності мережі, контроль параметрів QoS, а також формують рекомендації або керуючі впливи, що необхідні для локалізації аварій та збоїв, і відновлення нормального режиму функціонування КМ.

Самий верхній рівень моделі представлений центральною системою аналітичної обробки даних, яка виконує функції централізованого накопичення, інтеграції та комплексного аналізу інформації, що надходить від центрів оперативного контролю. На цьому рівні здійснюється довгострокове зберігання статистичних даних, аналіз тенденцій щодо зміни параметрів функціонування

мережі, прогнозування можливих відмов та робиться оцінка ефективності використання мережних ресурсів. Крім того, цей рівень відповідає за підтримку прийняття управлінських рішень щодо модернізації та подальшого розвитку мережі. За своїм функціональним призначенням цей рівень у найбільші мірою відповідає рівню BM концепції TMN, однак, на відміну від неї, тут основна увага приділяється не фінансовим аспектам діяльності оператора, а централізованому аналітичному супроводу процесів моніторингу, контролю та управління КМ.

3.3 Функціональна архітектура системи моніторингу та контролю комп’ютерної мережі

Слід зазначити, що система МтК корпоративної комп'ютерної мережі є складним програмно-апаратним комплексом, призначеним для безперервного контролю стану мережі, аналізу її функціонування та своєчасного виявлення аварій та збоїв. Така система має забезпечувати надійну роботу мережі в умовах великої кількості взаємопов'язаних пристроїв, мережних сервісів і користувачів, кожен з яких може висувати різні вимоги до QoS. Практика побудови сучасних систем мережного моніторингу свідчить, що їх розробку та впровадження доцільно здійснювати поетапно, поступово розширюючи функціональні можливості вже діючої системи відповідно до розвитку КМ та зміни вимог до її експлуатації [15].

Така система моніторингу має своєчасно виявляти будь-яких змін у конфігурації мережного обладнання, серверів, мережних сервісів і ПЗ, що можуть вплинути на працездатність або безпекові функції мережі. У разі виявлення таких змін система МтК повинна автоматично повідомити про це адміністратора мережі та, за необхідності, ініціювати виконання додаткових процедур контролю. Наприклад, тимчасове використання альтернативних маршрутів ПД може бути обумовлене поточним режимом роботи мережі. Проте їх часта або непередбачувана зміна може свідчити про виникнення аварійної ситуації, помилки конфігурування або появу інших аномалій, що потребують додаткового аналізу [13, 15].

Виходячи з цього, сучасна система моніторингу та контролю комп'ютерної мережі повинна забезпечувати реалізацію таких основних функцій [16, 17]:

1) формування та управління задачами моніторингу, що включає створення, редагування, активацію, деактивацію та видалення правил проведення контролю,

визначення переліку об'єктів моніторингу, параметрів їх функціонування, періодичності збору інформації та способів її отримання;

2) безперервний контроль стану мережі, який передбачає виявлення змін конфігурації мережних пристроїв і серверів, контроль параметрів їх функціонування, аналіз мережного трафіку, а також автоматичне виявлення аномалій, пов'язаних із порушенням роботи обладнання, мережних сервісів або політик безпеки. Крім цього, система повинна забезпечувати перевірку поточної конфігурації обладнання шляхом її порівняння з еталонними конфігураціями, що дозволяє своєчасно виявляти несанкціоновані або помилкові зміни налаштувань;

3) реєстрацію та документування результатів моніторингу, що передбачає автоматичне ведення журналів подій і формування звітів про стан мережі. Звіти мають містити дату і час виникнення події, найменування об'єкта моніторингу, тип виявленої аварії, збою або іншої аномалії, джерело її виникнення, а також додаткову інформацію, що необхідна для подальшого аналізу та усунення причин її появи.

4) автоматичне формування повідомлень про події та аварійні ситуації у разі відхилення контрольованих параметрів від встановлених нормативних значень або виникнення критичних змін у конфігурації мережі. Це забезпечує оперативне інформування адміністратора мережі та дозволяє своєчасно реагувати на потенційні відмови або порушення функціонування КМ.

Застосування системного аналізу, зокрема методу функціональної декомпозиції, дозволяє окреслити основні функціональні підсистеми, які можуть входити до складу системи МтК корпоративної КМ [16, 17]:

- підсистема збору даних – забезпечує періодичне опитування об'єктів моніторингу відповідно до заданих параметрів та отримання інформації про їх поточний стан. Крім збору даних, вона може виконувати їх первинну обробку, що дозволяє класифікувати отримані значення як нормальні, що не потребують уваги мережного адміністратора, або критичні, які вимагають негайного реагування;

- підсистема зберігання та керування даними – призначена для накопичення, зберігання, архівування та обробки інформації, що отримана в процесі моніторингу. До її складу входять засоби взаємодії з БД або іншими сховищами інформації, а також механізми агрегування і усереднення даних за певні проміжки часу, що дозволяє зменшити обсяг інформації, яка зберігається, без втрати її інформативності;

- підсистема аналізу даних – виконує обробку накопиченої інформації, статистичний аналіз, виявлення закономірностей, тенденцій і аномалій у функціонуванні КМ. Вона забезпечує реалізацію так званого фонового моніторингу, який передбачає довготривале накопичення та аналіз інформації про роботу мережі з метою здійснення оцінки її стану, а також прогнозування можливих відмов і планування подальшого розвитку мережі;

- підсистема оповіщення – забезпечує автоматичне інформування адміністратора мережі про виникнення аварійних ситуацій, критичних подій або інших відхилень від нормального режиму функціонування КМ за допомогою визначених механізмів оповіщення;

- підсистема візуалізації результатів моніторингу – призначена для подання інформації про стан КМ та результати моніторингу у формі, що є зручною для сприйняття користувачем. Для цього використовуються графічні інтерфейси, веб-інтерфейси, інформаційні панелі (dashboard), тощо, що забезпечують швидкий доступ до інформації про стан контрольованих об'єктів.

Перелічені функціональні підсистеми забезпечують реалізацію оперативного моніторингу КМ, який спрямований на здійснення постійного контролю, що направлений на оцінку поточної працездатності мережного обладнання та сервісів, аналіз ефективності їх функціонування, а також своєчасне виявлення і локалізацію аварійних ситуацій та інших подій, які можуть негативно вплинути на роботу мережі [16].

На рисунку 3.2 наведений типовий варіант функціональної архітектури системи моніторингу та контролю корпоративної КМ, що задовольняє вимогам і задачам, які окреслені в зазначених вище функціональних підсистемах.

Використовуючи методологію функціонального моделювання IDEF0 (Integration Definition for Function Modeling), яка використовується для графічного опису, аналізу та формалізації бізнес-процесів, розробимо функціональну модель, що визначає структуру та зв’язки функціональних підсистем вищеописаної системи моніторингу. Методологія IDEF0 дозволяє розбити (декомпозувати) складну систему, до якої відноситься і наведена на рисунку 3.2 система МтК комп’ютерної мережі, на сукупність взаємопов'язаних функцій, які подаються у вигляді ієрархії взаємопов'язаних функціональних блоків. Функціональна модель системи моніторингу, що розробляється, та яка побудована відповідно із методологією IDEF0, наведена на рис. 3.3 та 3.4 [18].



Рисунок 3.2 – Функціональна архітектура системи моніторингу та контролю комп’ютерної мережі

Побудована функціональна модель системи моніторингу комп'ютерної мережі на основі методології IDEF0, складається з двох взаємопов'язаних діаграм: контекстної діаграми (A–0) та діаграми декомпозиції першого рівня (A0).

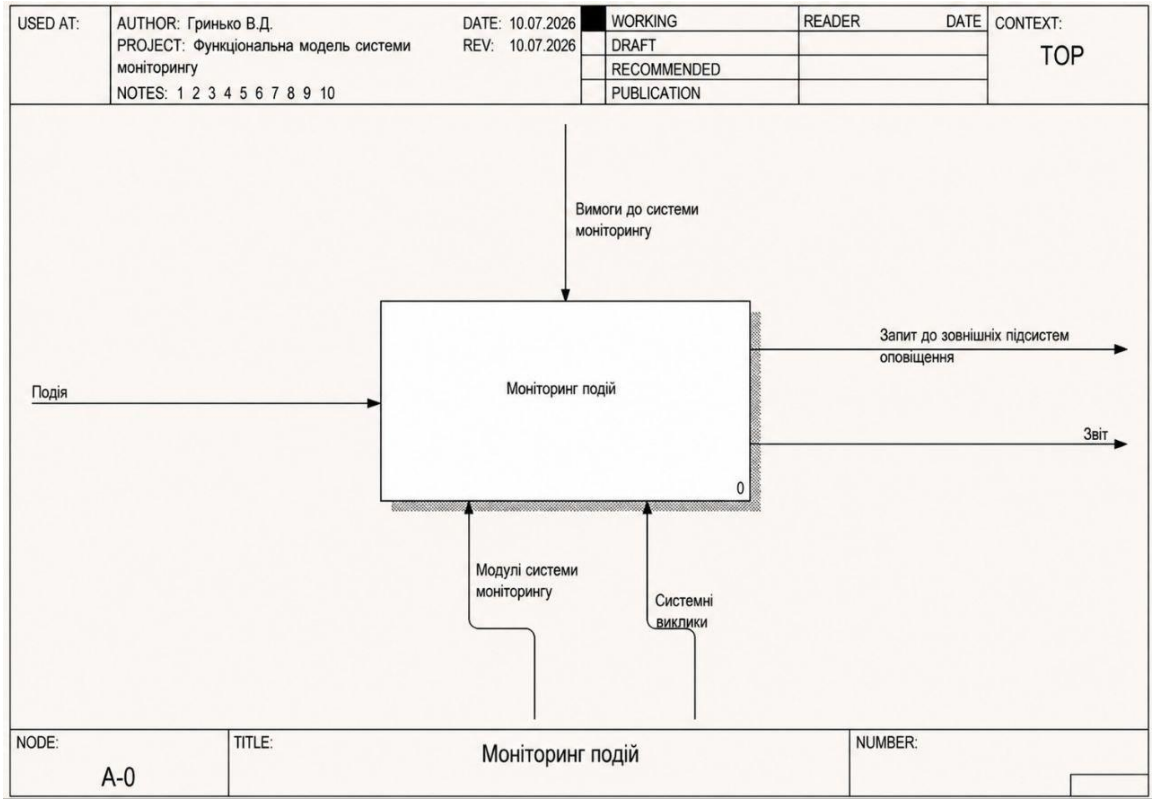


Рисунок 3.3 – Контекстна діаграма (A–0) функціональної моделі системи моніторингу

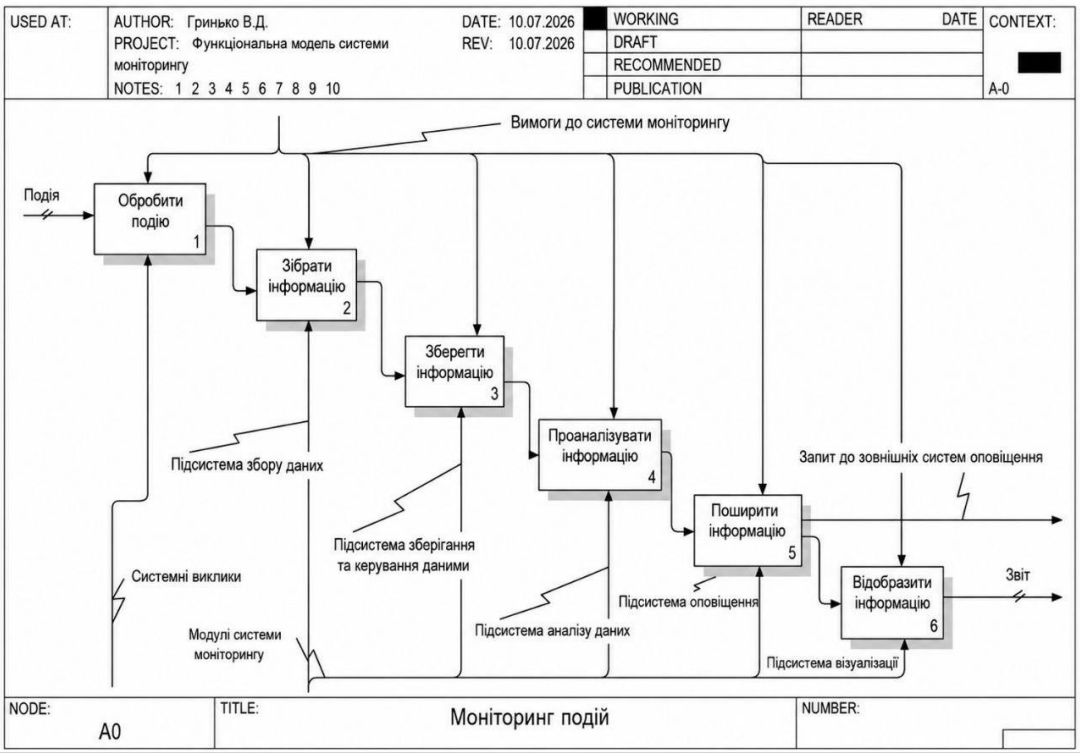


Рисунок 3.4 – Діаграма декомпозиції першого рівня (A0)

На контекстній діаграмі система МтК подана у вигляді єдиного функціонального блока «Моніторинг подій», який своєю назвою відображає її основне функціональне призначення. Для цього блока визначені вхідні потоки інформації, керуючі впливи, механізми реалізації та вихідні результати функціонування відповідно до правил побудови моделей IDEF0.

Для більш детального опису процесу моніторингу виконано функціональну декомпозицію контекстного блока на діаграмі A0. Вона відображає основні підфункції системи МтК та взаємозв'язки між ними за допомогою функціональних блоків та інтерфейсних дуг. Такий підхід дозволяє деталізувати процес моніторингу, визначити послідовність виконання окремих операцій та інформаційні потоки між ними. Декомпозицію виконано з урахуванням основних функціональних підсистем системи МтК комп'ютерної мережі, що були розглянуті вище при побудові функціональної архітектури системи МтК на рис. 3.2. Відповідно до цього функціональний блок «Моніторинг подій» було поділено на шість взаємопов'язаних блоків:

- A1 – обробка події;
- A2 – збір інформації про подію;
- A3 – збереження отриманої інформації;

- A4 – аналіз накопичених даних;
- A5 – поширення результатів аналізу;
- A6 – відображення інформації про результати могіторингу.

Кожен із зазначених блоків відповідає окремому етапу реалізації процесу моніторингу та логічно пов'язаний з відповідною функціональною підсистемою системи моніторингу. Зокрема, блок A2 відповідає підсистемі збору даних, блок A3 – підсистемі зберігання та керування даними, блок A4 – підсистемі аналізу даних, блок A5 – підсистемі оповіщення, а блок A6 – підсистемі візуалізації результатів моніторингу.

Керуючі впливи, що визначені вимогами до системи моніторингу, поширюються на всі функціональні блоки діаграми декомпозиції та визначають правила їх функціонування. Водночас механізми реалізації, які представлені модулями системи моніторингу та системними викликами, забезпечують виконання відповідних функцій, а результати роботи системи формуються у вигляді повідомлень для зовнішніх підсистем оповіщення та звіту для адміністратора мережі.

4 СИСТЕМА МОНІТОРИНГУ ТА КОНТРОЛЮ КОМП'ЮТЕРНОЇ МЕРЕЖІ З ВИКОРИСТАННЯМ ПРОГРАМНОЇ ПЛАТФОРМИ ZABBIX

4.1 Загальні особливості і компоненти системи Zabbix

Програмне забезпечення Zabbix – це програмна система з відкритим вихідним кодом, що вільно розповсюджується, та яка призначена для здійснення комплексного моніторингу та контролю комп'ютерних мереж, мережного обладнання, серверів, операційних систем (ОС), прикладних сервісів і ПЗ. Якщо знову проводити аналогію з фундаментальною архітектурою СУ на основі TMN (рис. 2.1) і, відповідно, створеною на її основі фундаментальною архітектурною моделлю системи МтК комп'ютерних мереж (рис. 3.1), то тут система Zabbix є базовим інструментом збору, обробки та аналізу інформації про стан комп'ютерної мережі. В рамках TMN, Zabbix переважно реалізує функціональні категорії рівнів NEN та NM, забезпечуючи моніторинг працездатності обладнання, контроль параметрів функціонування мережі та оперативне реагування на виявлені події. Платформа Zabbix складається з наступних основних компонентів [19, 20]:

- Сервер Zabbix (Zabbix Server, ядро системи моніторингу) – є центральним компонентом системи МтК. Він виконує періодичний збір даних від агентів, проксі-серверів та інших джерел інформації, здійснює їх обробку, аналіз, зберігання у БД, а також формує повідомлення про події та аварійні ситуації. Крім цього, сервер забезпечує контроль доступності мережних сервісів, виконання правил автоматизації, запуск сценаріїв сповіщення та централізоване управління процесами моніторингу. Саме на сервері зберігаються конфігураційні параметри системи, статистична інформація та історія результатів моніторингу [19, 20];

- Проксі-сервер Zabbix (Zabbix Proxy) призначений для збору інформації про стан віддалених сегментів мережі від імені центрального сервера. Дані, що отримуються, накопичуються у локальному буфері, після чого передаються серверу Zabbix для здійснення подальшої обробки та зберігання. Використання проксі-серверів є доцільним під час моніторингу та контролю географічно розподілених мереж, філій підприємства або сегментів мережі з обмеженою пропускною здатністю каналів зв'язку. Крім цього, застосування проксі дозволяє

більш рівномірно зробити розподіл навантаження між компонентами системи моніторингу та зменшити навантаження на центральний сервер [19, 20];

- Агент Zabbix (Zabbix Agent) являє собою спеціалізований програмний модуль, який встановлюється на об'єктах моніторингу та забезпечує збір інформації про стан локальних ресурсів, ОС і прикладного ПЗ. Агент передає серверу або проксі-серверу дані щодо використання процесора, оперативної пам'яті, фізичного дискового простору, мережних інтерфейсів, файлових систем, тощо. Разом із тим Zabbix підтримує моніторинг не лише за допомогою агентів, але також із використанням протоколів SNMP (версій 1 - 3), IPMI, JMX, HTTP, HTTPS, SSH, Telnet, FTP, ICMP (Ping), зовнішніх сценаріїв і вбудованих механізмів перевірки доступності мережних сервісів. Завдяки використанню системних викликів ОС агенти забезпечують ефективний збір інформації з мінімальним впливом на продуктивність вузла, за яким здійснюється контроль. . Zabbix-агенты підтримуються більшістю сучасних ОС, зокрема Unix/Linux/AIX, Windows, AIX, macOS та іншими. Зазначу, що операційна система ОС AIX (Advanced Interactive eXecutive) – це корпоративна ОС, що відноситься до сімейства Unix, та яка розроблена компанією IBM. Ця ОС, як правило, використовується на потужних серверах IBM Power Systems, є дуже стабільною і надійною, має добру захищеність та здатність обробляти значні об’єми критично важливих корпоративних даних [19, 20].

4) веб-інтерфейс є засобом візуального подання інформації Zabbix, яка зібрана і оброблена системою в результаті комплексного МтК комп'ютерних мереж. Приклад веб-інтерфейсу Zabbix показаний на рис. 4.1, де показано один із варіантів графічного подання топологічної карти комп'ютерної мережі та поточного стану її основних елементів.

Система Zabbix підтримує побудову розподілених систем моніторингу, що дозволяє централізовано контролювати велику кількість мережних вузлів, у тому числі тих, що розташовані у віддалених сегментах мережі. При цьому управління конфігурацією та процесами моніторингу може здійснюватися за ієрархічним принципом. Крім цього, Zabbix забезпечує централізований моніторинг системних журналів (лог-файлів), підтримує створення топологічних карт мережі на основі шаблонів (див. рис. 4.1), формування звітів, аналіз тенденцій змін для показників, що контролюються, виконання автоматизованих сценаріїв за результатами моніторингу, взаємодію з різними БД, а також підтримує управління

обладнанням через інтелектуальний інтерфейс управління платформами (Intelligent Platform Management Interface, IPMI) [19, 20].



Рисунок 4.1 – Приклад веб-интерфейсу Zabbix

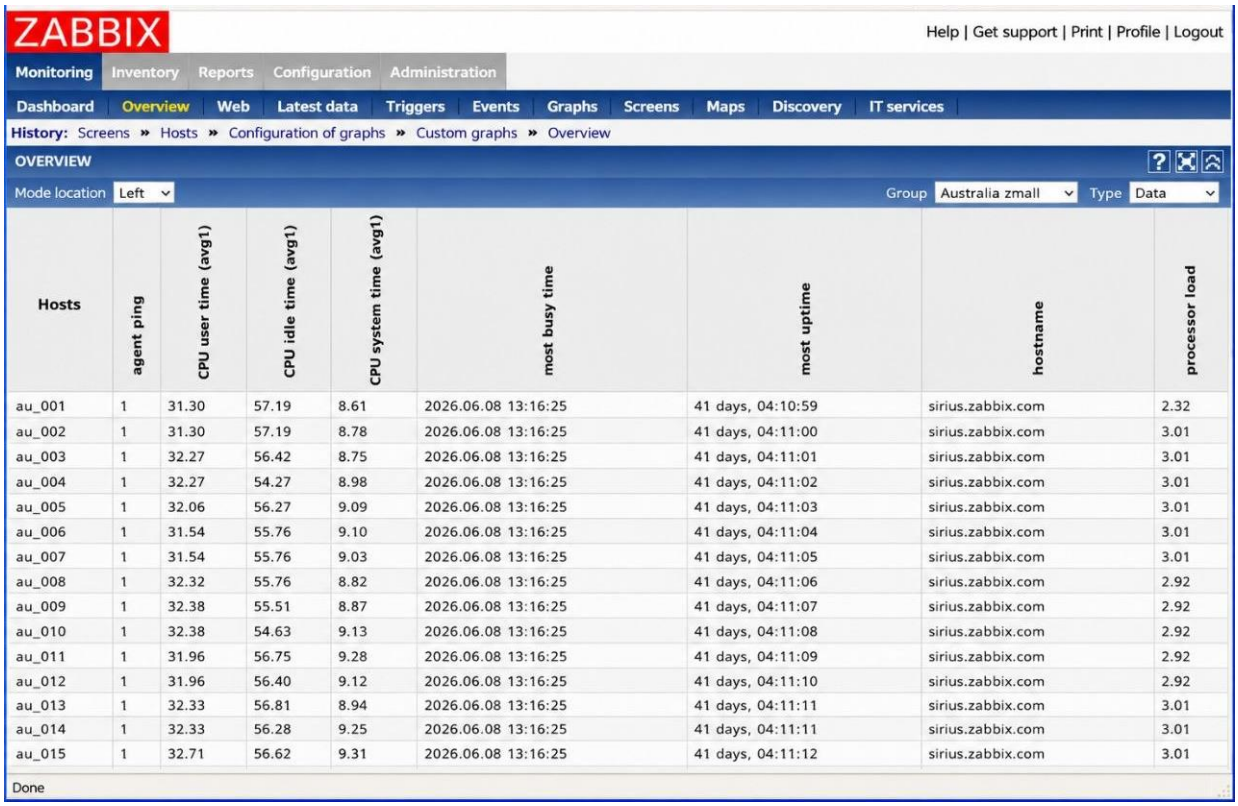
Таким чином, перевагами Zabbix є: відкритий вихідний код, широкі можливості масштабування, підтримка великої кількості протоколів моніторингу, централізоване адміністрування та високий рівень автоматизації процесів моніторингу. Водночас система характеризується досить складною процедурою здійснення початкового налаштування, потребує ретельного проєктування під час розгортання великих мереж, а для реалізації повного набору функцій моніторингу локальних ресурсів також потребує встановлення агентів на вузлах, що контролюються. Крім цього, адміністрування великих інсталяцій та налаштування розмежування прав доступу можуть вимагати додаткових знань і практичного досвіду роботи із системою [19, 20].

4.2 Практичне використання платформи Zabbix для організації системи моніторингу та контролю

Основною логічною одиницею системи Zabbix є вузол мережі (Host), який являє собою будь-який об'єкт моніторингу. Це може бути сервер, маршрутизатор, комутатор, робоча станція чи, навіть, мережна служба. Для кожного вузла задаються

його унікальне ім'я, опис, а також спосіб підключення до системи моніторингу із зазначенням IP-адреси або DNS-імені. З метою спрощення адміністрування та організації процесу моніторингу вузли об'єднуються у логічні групи (Host Groups), наприклад, сервери баз даних, веб-сервери, мережне обладнання або робочі станції. Використання таких груп дозволяє виконувати централізоване налаштування параметрів моніторингу, спрощує відображення інформації про вузли, стан яких необхідно контролювати, та забезпечує зручну фільтрацію результатів моніторингу. Кожний вузол має декілька елементів даних (items), тобто параметрів, за якими проводиться МтК вузла, та які характеризують його поточний стан [19].

На рисунку 4.2 наведено загальне вікно Overview системи Zabbix, яке дозволяє узагальнено в табличному відображенні подивитися результати моніторингу параметрів вузлів мережі. Тут показані значення основних параметрів функціонування кожного вузла та оцінюється їх поточний стан.



Hosts	agent ping	CPU user time (avg1)	CPU idle time (avg1)	CPU system time (avg1)	most busy time	most uptime	hostname	processor load
au_001	1	31.30	57.19	8.61	2026.06.08 13:16:25	41 days, 04:10:59	sirius.zabbix.com	2.32
au_002	1	31.30	57.19	8.78	2026.06.08 13:16:25	41 days, 04:11:00	sirius.zabbix.com	3.01
au_003	1	32.27	56.42	8.75	2026.06.08 13:16:25	41 days, 04:11:01	sirius.zabbix.com	3.01
au_004	1	32.27	54.27	8.98	2026.06.08 13:16:25	41 days, 04:11:02	sirius.zabbix.com	3.01
au_005	1	32.06	56.27	9.09	2026.06.08 13:16:25	41 days, 04:11:03	sirius.zabbix.com	3.01
au_006	1	31.54	55.76	9.10	2026.06.08 13:16:25	41 days, 04:11:04	sirius.zabbix.com	3.01
au_007	1	31.54	55.76	9.03	2026.06.08 13:16:25	41 days, 04:11:05	sirius.zabbix.com	3.01
au_008	1	32.32	55.76	8.82	2026.06.08 13:16:25	41 days, 04:11:06	sirius.zabbix.com	2.92
au_009	1	32.38	55.51	8.87	2026.06.08 13:16:25	41 days, 04:11:07	sirius.zabbix.com	2.92
au_010	1	32.38	54.63	9.13	2026.06.08 13:16:25	41 days, 04:11:08	sirius.zabbix.com	2.92
au_011	1	31.96	56.75	9.28	2026.06.08 13:16:25	41 days, 04:11:09	sirius.zabbix.com	2.92
au_012	1	31.96	56.40	9.12	2026.06.08 13:16:25	41 days, 04:11:10	sirius.zabbix.com	2.92
au_013	1	32.33	56.81	8.94	2026.06.08 13:16:25	41 days, 04:11:11	sirius.zabbix.com	3.01
au_014	1	32.33	56.28	9.25	2026.06.08 13:16:25	41 days, 04:11:11	sirius.zabbix.com	3.01
au_015	1	32.71	56.62	9.31	2026.06.08 13:16:25	41 days, 04:11:12	sirius.zabbix.com	3.01

Рисунок 4.2 – Загальне вікно Overview системи Zabbix для перегляду параметрів вузлів мережі

Зокрема, у вікні Overview відображаються результати перевірки доступності агента (Agent ping), середній час використання процесора (CPU user time), рівень простою процесора (CPU idle time), системний час процесора (CPU system time),

час безперервної роботи (Uptime), ім'я вузла (Hostname) та поточне завантаження процесора (Processor load). Наприклад, найпоширеніший параметр Agent ping, що визначає доступність вузла, на рис. 4.2 дорівнює 1, тобто на останній ping-запит було отримано відповідь (вузол доступний), в іншому випадку його значення б було 0. Крім того, значення цих параметрів періодично оновлюються відповідно до встановленого періоду опитування. Також для деяких items можна вказати спосіб зберігання, часовий інтервал, в межах якого треба проводити моніторинг (наприклад, тільки в 00:00 – 07:00, тобто тільки вночі), тощо [19].

Наведений приклад вікна Overview демонструє один із варіантів подання інформації, що була отримана від множини вузлів мережі. Це забезпечує детальний перегляд параметрів кожного вузла, що спрощує порівняльний аналіз їх функціонування та дозволяє оперативно виявляти відхилення від нормального режиму роботи.

На рисунку 4.3 наведено вікно інформаційної панелі (Dashboard) системи Zabbix, що дозволяє централізовано здійснювати відображення поточного стану комп'ютерної мережі, отриманого в процесі моніторингу. На відміну від вікна Overview, де відображаються параметри окремих вузлів мережі, вікно Dashboard надає адміністратору узагальнену інформацію про функціонування всієї мережі.

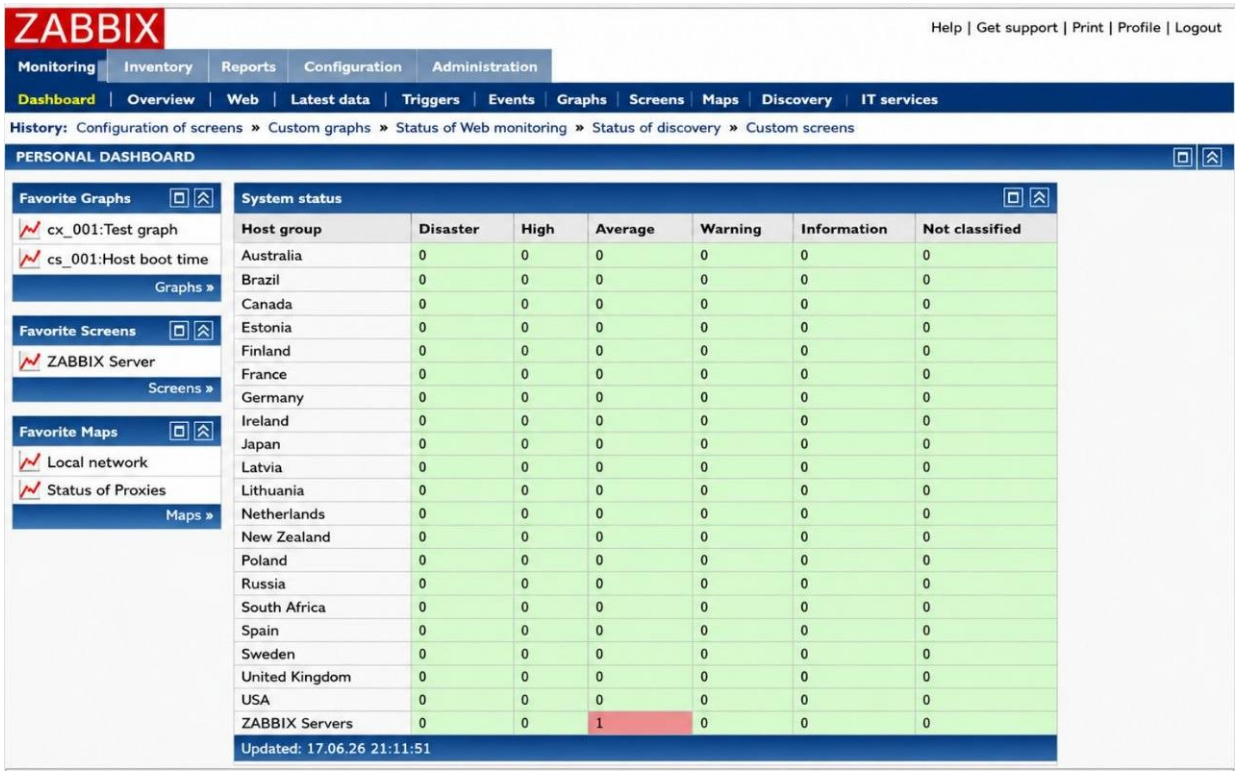


Рисунок 4.3 – Вікно інформаційної панелі (Dashboard) системи Zabbix

Основною частиною інформаційної панелі є таблиця System status, у якій для кожної групи вузлів (Host Groups) відображається кількість виявлених подій за рівнями їх критичності (Disaster, High, Average, Warning, Information та Not classified). Таке подання дозволяє оперативно оцінити загальний стан окремих сегментів мережі та швидко визначити групи вузлів, у яких виникли збої або інші позаштатні ситуації.

Крім цього, Dashboard надає можливості щодо формування і виводу найбільш важливих графічних залежностей (Favorite Graphs), екранів моніторингу (Favorite Screens) та карт мережі (Favorite Maps), що значно спрощує навігацію під час адміністрування системи. Таким чином, вікно Dashboard в якості основного засобу оперативного контролю стану комп'ютерної мережі, забезпечує централізоване відображення ключових показників функціонування та швидкий доступ до детальної інформації про вузли, що контролюються [19].

Таким чином, якщо у вікні Dashboard показується загальний стан груп вузлів, а у вікні Overview – узагальнені параметри вузлів мережі, то далі доцільно детально переглянути параметри конкретного вузла мережі. На рисунку 4.4 наведено вікно «Поточних даних» (Latest data) системи Zabbix, в якому виводяться поточні значення параметрів окремого вузла мережі.

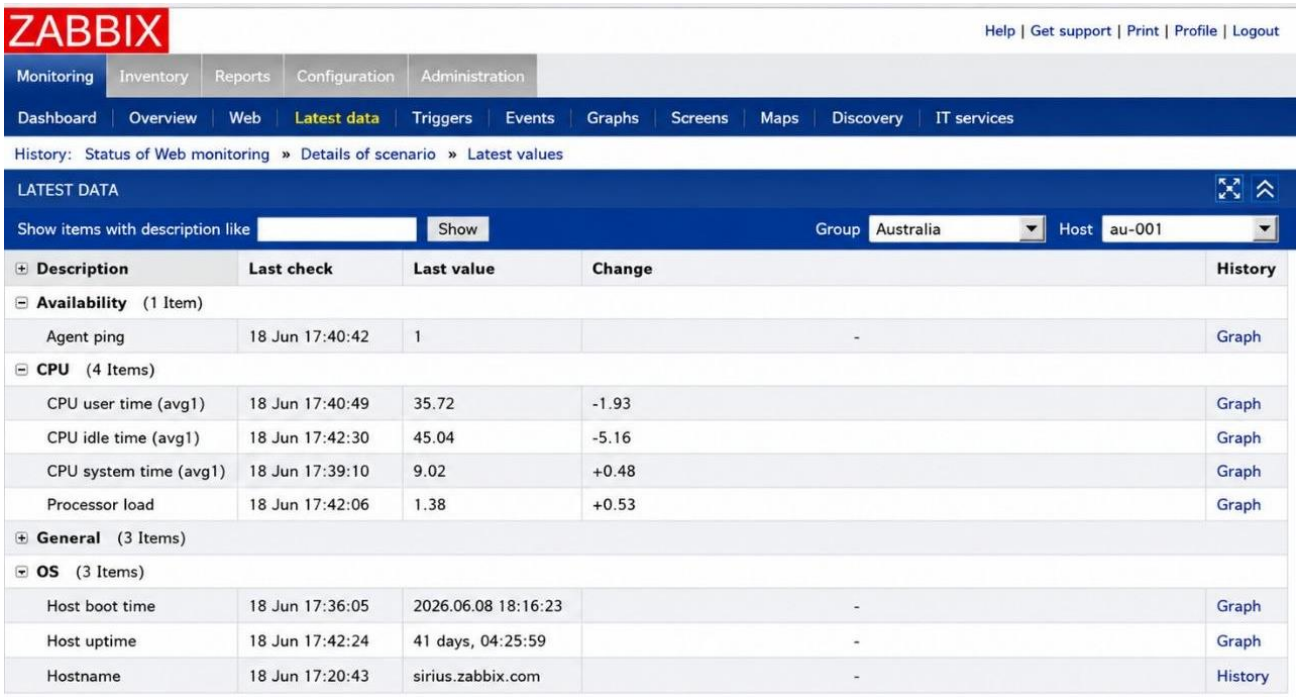


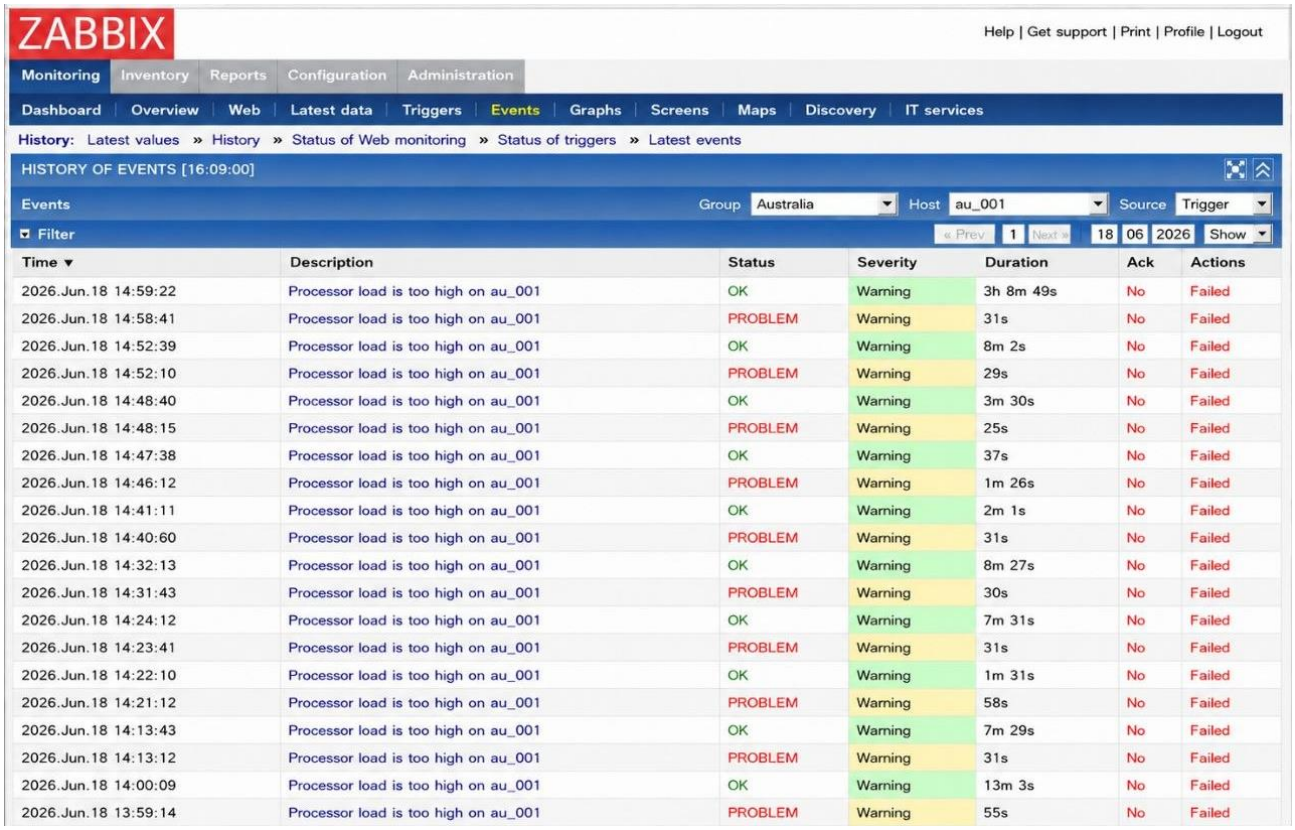
Рисунок 4.4 – Вікно Latest data системи Zabbix із поточними значеннями елементів даних (Items) вузла мережі

На відміну від вікон Dashboard та Overview, що забезпечують узагальнене подання стану груп вузлів або мережі в цілому, вікно Latest data дозволяє детально проаналізувати результати моніторингу конкретного об'єкта. Зокрема, у вікні відображається перелік Items, що налаштовані для вибраного вузла. Для кожного параметра вказуються час останньої перевірки (Last check), останнє отримане значення (Last value) та його зміна відносно попереднього вимірювання (Change). Крім цього, є можливість перейти до перегляду історії вимірювань або вивести графічне подання змін відповідного параметра за деякий час.

На показаному у вікні прикладі можна бачити, що відображаються результати моніторингу вузла au-001, зокрема зроблена перевірка доступності агента (Agent ping), наведені параметри використання процесора, поточне навантаження на процесор (Processor load), час безперервної роботи вузла (Host uptime), ім'я вузла та інші характеристики функціонування. Усі параметри згруповані за функціональним призначенням, що спрощує аналіз технічного вузла.

Далі на основі параметрів (Items), що контролюються, система Zabbix формує події (Events). Адміністратору мережі досить складно стежити за тисячами параметрів та аналізувати їх на предмет наявності нештатної ситуації. Zabbix надає гнучкі можливості щодо здійснення налаштування так званих умов-тригерів (Triggers), які спрацьовують у разі аварій та збоїв, і система здійснює візуальні попередження адміністратора про можливу проблему [19].

На рисунку 4.5 наведено вікно «Події» (Events) системи Zabbix, яка призначена для перегляду журналу подій, які були туди занесені в процесі моніторингу комп'ютерної мережі. На відміну від вікна Latest data (рис. 4.4), де відображаються поточні значення параметрів вузла мережі, вікно «Подій» містить інформацію лише про ті події, що виникли внаслідок спрацювання тригерів, тобто подій, в яких параметри, що контролюються, мають відхилення від встановлених порогових значень. Для кожної такої події показується час її виникнення, опис, поточний стан (Status), рівень критичності (Severity), тривалість (Duration), інформація про підтвердження події (Ack) та результати виконання автоматизованих дій (Actions). Така інформація дозволяє адміністратору оперативно оцінити характер проблеми, визначити її пріоритет і проаналізувати ефективність реагування системи.



Time ▾	Description	Status	Severity	Duration	Ack	Actions
2026.Jun.18 14:59:22	Processor load is too high on au_001	OK	Warning	3h 8m 49s	No	Failed
2026.Jun.18 14:58:41	Processor load is too high on au_001	PROBLEM	Warning	31s	No	Failed
2026.Jun.18 14:52:39	Processor load is too high on au_001	OK	Warning	8m 2s	No	Failed
2026.Jun.18 14:52:10	Processor load is too high on au_001	PROBLEM	Warning	29s	No	Failed
2026.Jun.18 14:48:40	Processor load is too high on au_001	OK	Warning	3m 30s	No	Failed
2026.Jun.18 14:48:15	Processor load is too high on au_001	PROBLEM	Warning	25s	No	Failed
2026.Jun.18 14:47:38	Processor load is too high on au_001	OK	Warning	37s	No	Failed
2026.Jun.18 14:46:12	Processor load is too high on au_001	PROBLEM	Warning	1m 26s	No	Failed
2026.Jun.18 14:41:11	Processor load is too high on au_001	OK	Warning	2m 1s	No	Failed
2026.Jun.18 14:40:60	Processor load is too high on au_001	PROBLEM	Warning	31s	No	Failed
2026.Jun.18 14:32:13	Processor load is too high on au_001	OK	Warning	8m 27s	No	Failed
2026.Jun.18 14:31:43	Processor load is too high on au_001	PROBLEM	Warning	30s	No	Failed
2026.Jun.18 14:24:12	Processor load is too high on au_001	OK	Warning	7m 31s	No	Failed
2026.Jun.18 14:23:41	Processor load is too high on au_001	PROBLEM	Warning	31s	No	Failed
2026.Jun.18 14:22:10	Processor load is too high on au_001	OK	Warning	1m 31s	No	Failed
2026.Jun.18 14:21:12	Processor load is too high on au_001	PROBLEM	Warning	58s	No	Failed
2026.Jun.18 14:13:43	Processor load is too high on au_001	OK	Warning	7m 29s	No	Failed
2026.Jun.18 14:13:12	Processor load is too high on au_001	PROBLEM	Warning	31s	No	Failed
2026.Jun.18 14:00:09	Processor load is too high on au_001	OK	Warning	13m 3s	No	Failed
2026.Jun.18 13:59:14	Processor load is too high on au_001	PROBLEM	Warning	55s	No	Failed

Рисунок 4.5 – Вікно Events системи Zabbix для перегляду журналу подій моніторингу

В наведеному на рис. 4.5 прикладі всі зареєстровані події є пов'язаними з перевищенням допустимого навантаження на процесор вузла `au_001` (Processor load is too high). Після нормалізації цього параметра статус події автоматично змінюється на OK, що свідчить про усунення причини її виникнення. Таким чином наявність такого централізованого журналу подій дозволяє здійснювати оперативний контроль стану комп'ютерної мережі, аналізувати історію виникнення тих або інших проблем та здійснювати оцінку ефективність функціонування системи моніторингу.

Якщо система Zabbix функціонує в автоматичному режимі або немає можливості у адміністратора здійснювати безпосередній контроль, то в цьому випадку Zabbix має можливість надіслати повідомлення на електронну пошту, у SMS-повідомленні або через месенджер, що заздалегідь був вказаний в налаштуваннях. Для цього використовуються підключення до Wi-Fi, Інтернету або мережі мобільних операторів. Крім того, у системі Zabbix навіть передбачені можливості щодо самостійного відновлення роботи проблемного сервісу

комп’ютерної мережі. Для цього виконуються заздалегідь «прописані» адміністратором дії, які запускаються у разі спрацювання певних тригерів [19].

Опція системи Zabbix «Деталізація подій» (Event details) якраз і дозволяє детально проаналізувати конкретну подію, її причини та результати реагування системи моніторингу. Вікно, що відображає таку деталізацію наведене на рис. 4.6.

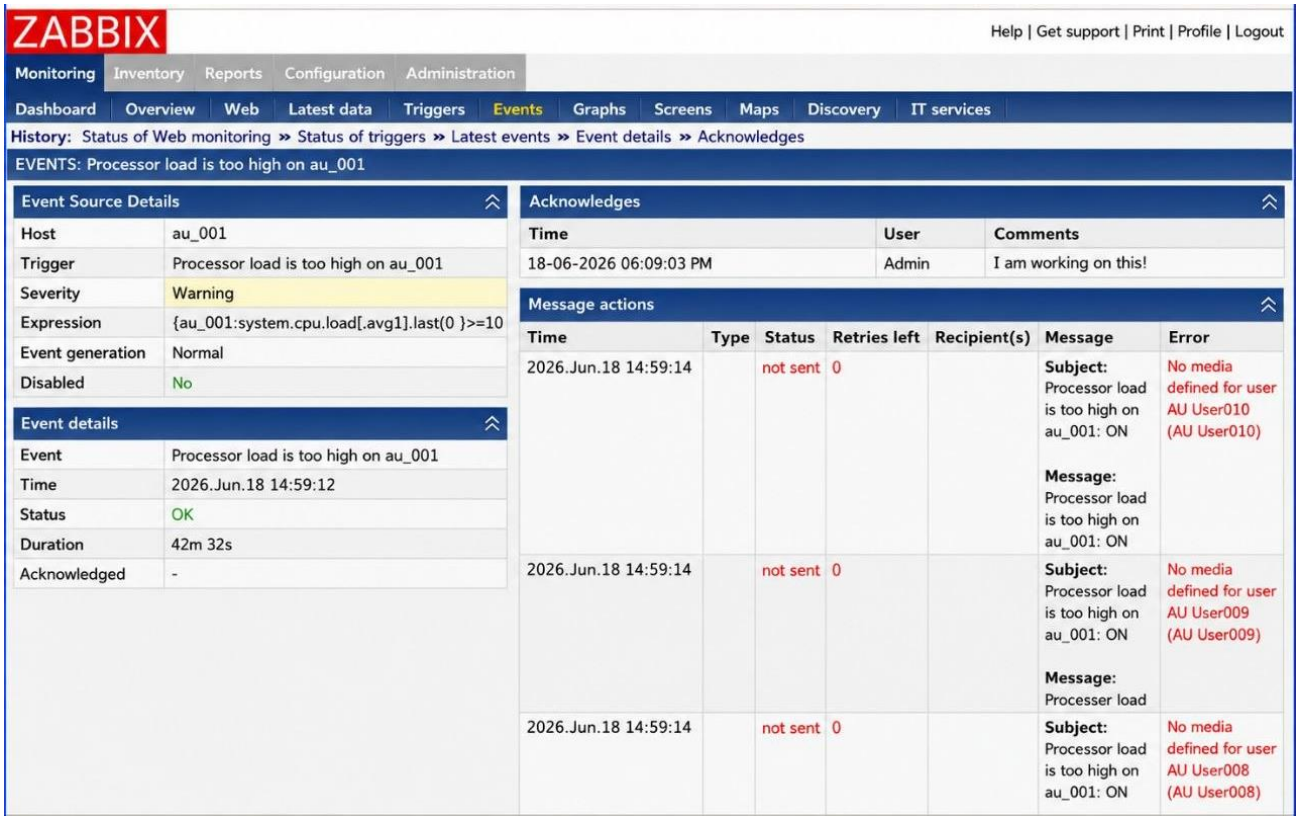


Рисунок 4.6 – Вікно Event details системи Zabbix із детальною інформацією про подію та результати її обробки

У верхній частині вікна наведені основні характеристики події, зокрема вузол мережі (Host), тригер (Trigger), який ініціював її створення, рівень критичності (Severity), вираз тригера (Expression) та тип формування події. Нижче відображаються детальні відомості про саму подію, включаючи час її виникнення, поточний стан, тривалість та інформацію щодо її підтвердження адміністратором (Acknowledged).

Вираз тригера – це логічний вираз, який визначає умову виникнення події в системі Zabbix. Він містить правило порівняння поточного значення параметра, що контролюється, із заданим пороговим його значенням. Якщо ця умова

виконується, тригер переходить у стан PROBLEM (див. рис. 4.5) і система реєструє відповідну подію. Так на рисунку 4.6 наведено наступний вираз тригера:

```
{au_001:system.cpu.load[avg1].last(0)}>=10,
```

що означає: якщо останнє виміряне значення середнього навантаження процесора вузла au_001 за одну хвилину перевищує або дорівнює 10, система формує подію про перевищення допустимого навантаження на процесор.

У окремій частині вікна міститься інформація про підтвердження події (Acknowledgements) та результати виконання автоматизованих дій (Message actions), зокрема відомості про спроби надіслати повідомлення адміністратору, їх статус та одержувачів, а також інформацію про можливі помилки, у процесі доставки. Це дозволяє контролювати не лише факт виникнення проблемної події, а й процес її обробки та ефективність роботи механізмів оповіщення. Таким чином, наявність опції Event details забезпечує повний аналіз окремої проблемної події, дозволяючи адміністратору визначити причину її виникнення, оцінити процес реагування на неї та перевірити виконання механізмів оповіщення, що налаштовані в системі.

Як вже зазначалося вище, на основі зібраних даних щодо будь-якого контрольованого параметра системи моніторингу можна безпосередньо в системі сформувати графік змін – причому не за заздалегідь визначені та жорстко задані часові інтервали, а за будь-який проміжок часу з максимальною роздільною здатністю. Ці можливості в системі Zabbix реалізуються за допомогою опції веб-моніторингу [19].

На рисунку 4.7 наведено вікно «Деталізація сценарію» (Details of scenario) в якому здійснюється детальний аналіз результатів веб-моніторингу з графічним їх поданням. У верхній частині вікна наведені результати виконання окремих етапів сценарію (Steps), для яких відображаються швидкість передавання даних (Speed), час відгуку (Response time), код відповіді HTTP (Response code) та поточний стан перевірки (Status). Нижче показані графіки зміни швидкості передачі даних і часу відгуку сервісу за певний період спостереження, що дозволяє оцінити стабільність його функціонування та виявити можливі відхилення від нормального режиму роботи. Треба зазначити, що система моніторингу формує графік із кроком у 30 секунд (інтервал опитування за замовчуванням).



Рисунок 4.7 – Вікно Details of scenario системи Zabbix для проведення аналізу результатів веб-моніторингу

Для візуалізації логічної структури комп’ютерної мережі, моніторинг якої здійснюється в системі Zabbix, можна створювати топологічні карти цієї мережі, які будуть відображати розташування її вузлів та відповідні зв’язки між ними (рис. 4.8). Слід зазначити, що стан вузлів (доступний чи ні) також буде показаний на топологічній карті.

На наведеному на рис. 4.8 прикладі показана топологічна карта мережі, у центрі якої розташований сервер Zabbix, а навколо нього – віддалені проксі-сервери Zabbix, які забезпечують моніторинг територіально розподілених сегментів мережі. Для кожного вузла на карті відображається його поточний стан, а також можуть виводитися повідомлення про виявлені проблемні ситуації. Зокрема, на рисунку показано повідомлення про недоступність поштового сервера (Gmail (SMTP) server is down on ZABBIX Server), що дозволяє адміністратору швидко локалізувати проблемний вузол.

Крім того, система Zabbix підтримує створення комплексних екранів моніторингу (Screens), що забезпечують одночасне відображення в одному робочому вікні різних засобів візуалізації, зокрема графіків, карт мережі, таблиць,

списків подій, тригерів та інших компонентів системи моніторингу, як це показано на рисунку 4.9 [19].

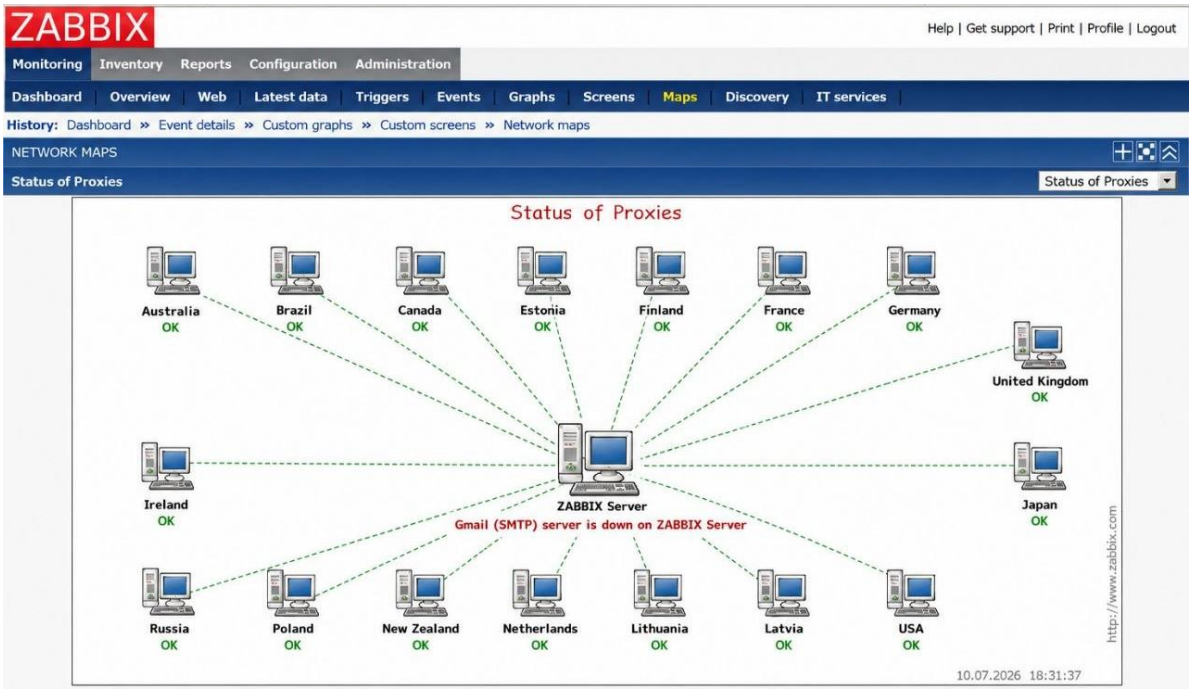


Рисунок 4.8 – Вікно Network Maps системи Zabbix для графічного відображення топології комп'ютерної мережі та стану її вузлів

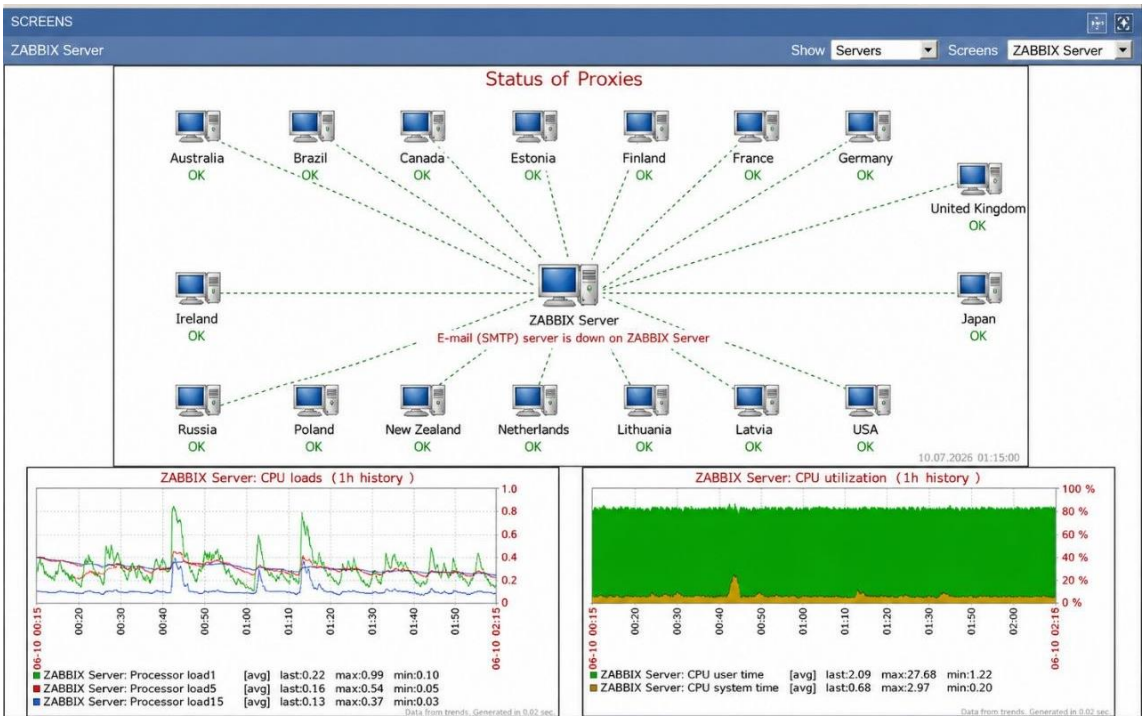


Рисунок 4.9 – Вікно Screens системи Zabbix, в якому надається можливість одночасного відображення результатів моніторингу

У наведеному прикладі у верхній частині вікна відображається топологічна карта мережі із зазначенням стану серверів і проксі-серверів Zabbix, а нижче наведено графіки зміни навантаження на процесор та використання процесорного часу центрального сервера Zabbix. Таке поєднання різних засобів візуалізації дозволяє адміністратору одночасно контролювати як топологію мережі, так і динаміку зміни основних експлуатаційних параметрів її компонентів.

Таким чином, система моніторингу Zabbix, що була проаналізована вище реалізує більшість функцій, необхідних для побудови сучасної системи моніторингу та контролю комп'ютерної мережі, включаючи автоматизований збір інформації, аналіз параметрів функціонування, виявлення аварійних ситуації, формування повідомлень, централізоване відображення результатів моніторингу та підтримку засобів автоматизації адміністрування. Це дозволяє розглядати її як ефективний інструмент щодо практичної реалізації функцій моніторингу і контролю в корпоративних комп'ютерних мережах, а також як одну з найбільш доцільних платформ для побудови сучасних систем мережного адміністрування.

ВИСНОВКИ

У цій кваліфікаційній роботі проведено аналіз теоретичних і практичних аспектів забезпечення моніторингу та контролю комп'ютерних мереж. Аналіз ґрунтувався на висвітлені загальних принципів побудови сучасних СУ та на базових задачах функціональних категорій управління телекомунікаційними мережами. В якості фундаментальної основи організації СУ проаналізована багаторівнева архітектурна модель TMN та її інформаційна модель. Проаналізовано механізми взаємодії «менеджер - агент», роль застосування в цих механізмах протоколів CMIP і SNMP для організації мережного моніторингу та управління абстрактною комп’ютерною мережею. Також проаналізовані функціональні можливості та основні модулі програмної платформи для здійснення моніторингу комп’ютерних мереж Zabbix, а також принципи її практичного застосування в якості системи МтК у корпоративній КМ.

У першому розділі надається загальна характеристика і аналіз концептуальних принципів реалізації мережного управління. Показано, що процес організації мережного управління (як і будь якої іншої системи) базується на взаємодії суб'єкта управління, об'єкта управління та зовнішнього середовища, а ефективність функціонування будь-якої системи управління визначається чітким формулюванням мети управління, визначенням меж об'єкта управління та наявністю достовірної інформації про його поточний стан і вплив зовнішніх факторів. Зокрема обґрунтовано, що КМ, як складова системи телекомунікацій, є складною ієрархічною системою, яка потребує централізованого управління, здатного забезпечити необхідний рівень надійності, продуктивності та якості надання мережних послуг [7, 10].

Також у розділі наводиться опис п'яти основних функціональних напрямів управління мережею відповідно до моделі FCAPS. Зазначається, що ефективне функціонування сучасної КМ забезпечується комплексною реалізацією задач управління помилками, конфігурацією, продуктивністю, безпекою та обліком використання мережних ресурсів. Сукупність цих функціональних напрямів створює основу для побудови сучасних систем управління і моніторингу, які забезпечують своєчасне виявлення проблемних ситуацій, контроль параметрів функціонування мережних ресурсів, можливості неперервного аналізу щодо ефективності використання ресурсів КМ; надають допомогу у централізованому

адмініструванні мережною інфраструктурою; реалізують підтримку необхідного рівня безпеки.

У другому розділі зроблено аналіз концепції TMN в аспекті реалізації СУ і моніторингу КМ. Зазначено, що TMN є однією з фундаментальних моделей побудови СУ як взагалі телекомунікаційними, так і безпосередньо комп'ютерними мережами різних рівнів ієрархії. Її основною перевагою є використання ієрархічного підходу до організації процесів управління, що забезпечує розподіл функцій між окремими рівнями відповідно до їх призначення. Така архітектура дозволяє реалізувати комплексне управління мережею, починаючи від контролю окремих її мережних елементів і завершуючи управлінням мережними послугами та підтримкою процесів модернізації і планування подальшого розвитку [7].

Показано, що в рамках технічного завдання до виконання кваліфікаційної роботи, важливою складовою концепції TMN є її інформаційна модель управління, основу якої становить механізм «менеджер - агент», що забезпечує централізований збір, обробку, передачу та зберігання інформації про стан мережних ресурсів. В цій моделі агенти виконують функції безпосереднього збору інформації про мережні елементи її передачу до менеджерів, тоді як безпосередньо менеджери здійснюють аналіз отриманої інформації, формування команд управління та координацію роботи всієї системи моніторингу [7].

На підставі проведеного аналізу зазначено, що концепцію TMN, її багаторівневу архітектуру та інформаційну модель можна використовувати як фундаментально основу організації сучасних систем моніторингу і контролю КМ.

У відповідності з цим у третьому розділі кваліфікаційної роботи проведений аналіз особливостей і архітектурних підходів організації системи моніторингу та контролю комп’ютерної мережі. Зокрема наведені загальні особливості і функції систем моніторингу та контролю для КМ та запропонована фундаментальна архітектурна модель системи МтК, що організована відповідно до базових функціональних категорій управління та концептуальної архітектури СУ на базі TMN (рис. 3.1). Зазначено, що така архітектурна модель забезпечує ієрархічну організацію процесів моніторингу та контролю, при якій функції збору даних, оперативного аналізу та централізованої аналітичної обробки розподілені між різними рівнями системи. Такий підхід дозволяє зменшити навантаження на окремі компоненти СУ, підвищити масштабованість рішення та забезпечити ефективний контроль стану КМ в реальному масштабі часу [15].

Також у цьому розділі на основі запропонованої фундаментальної архітектурної моделі системи МтК зроблена розробка типової функціональної архітектури системи моніторингу та контролю КМ та визначені її функції. Також на основі методології IDEF0 побудована функціональна модель системи моніторингу КМ, яка складається з двох взаємопов'язаних діаграм: контекстної діаграми (А–0, рис. 3.3) та діаграми декомпозиції першого рівня (А0, рис. 3.4). На контекстній діаграмі систему подано у вигляді єдиного функціонального блока «Моніторинг подій», для якого визначено інформаційні потоки, керуючі впливи, механізми реалізації та результати функціонування. Виконана далі функціональна декомпозиція дозволила виділити основні підфункції системи, встановити взаємозв'язки між ними та деталізувати процес моніторингу відповідно до послідовності виконання основних операцій [18].

У четвертому розділі проаналізована система МтК комп’ютерної мережі з використанням програмної платформи Zabbix та наведені практичні рекомендації щодо використання її функціональних можливостей. Показано, що система Zabbix є сучасною платформою комплексного моніторингу КМ з відкритим вихідним кодом, що вільно розповсюджується. Вона забезпечує централізований контроль технічного стану мережі, її серверного обладнання, мережних сервісів та прикладного ПЗ. Архітектура Zabbix має модульну структуру і включає сервер моніторингу, проксі-сервери, агенти та Web-інтерфейс, що забезпечує її масштабованість, підтримку розподіленого моніторингу та можливість ефективного адміністрування територіально розподілених КМ [19].

Показано, що основною логічною одиницею системи є вузол мережі (Host), навколо якого формуються всі інші об'єкти моніторингу. Такий підхід забезпечує структуровану організацію процесу моніторингу та дозволяє здійснювати контроль стану окремих мережних пристроїв, їх функціональних параметрів і мережних сервісів. Аналіз можливостей Web-інтерфейсу Zabbix показав, що система надає широкий набір засобів збору і аналізу даних та візуалізації результатів моніторингу.

Зазначено, що система Zabbix реалізує більшість функцій, які є необхідними для організації сучасної системи МтК комп'ютерної мережі, що дозволяє розглядати її як ефективний інструмент для застосування у системах мережного адміністрування.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Stallings W. Data and Computer Communications [Електронний ресурс] / William Stallings // Pearson Education, Inc. – 2007. – 901 p. – Режим доступу: https://ftp.utcluj.ro/pub/users/dadarlat/retele_an3/stuff/Data.And.Computer.Communications.8e.WilliamStallings.pdf

2. Олифер В. Компьютерные сети. Принципы, технологии, протоколы: юбилейное издание / Виктор Олифер, Наталья Олифер. – СПб.: Питер, 2020. – 1008 с.

3. Cisco Systems. What is Network Monitoring? [Електронний ресурс] // Cisco. – Доступ здійснено 29.05.2026 – Режим доступу до ресурсу: Cisco – https://www.cisco.com/site/us/en/learn/topics/networking/what-is-network-monitoring.html.

4. IBM. What is network monitoring? [Електронний ресурс] // IBM. – Доступ здійснено 29.05.2026. – Режим доступу: https://www.ibm.com/think/topics/network-monitoring?utm_source=chatgpt.com.

5. Network Performance Monitoring [Електронний ресурс] // SolarWinds. – Доступ здійснено 29.05.2026. – Режим доступу до ресурсу: https://www.solarwinds.com/network-performance-monitor?utm_source=chatgpt.com.

6. Стеклов В.К., Проектування телекомунікаційних мереж / В.К. Стеклов, Л.Н. Беркман – К.: Техніка 2002 – 392с.

7. Колтун Ю.М. Інфокомунікаційні мережі та технології: навч. посібник для студентів усіх форм навчання спеціальності 172 – Телекомунікації та радіотехніка / Упоряд.: Ю.М. Колтун, Ю.В. Скорик. – Харків: ХНУРЕ, 2020. – 200 с.

8. Что такое система мониторинга и контроля проектов: полное руководство [Електронний ресурс] // ADVANTA – система управления проэктами. – Доступ здійснено 07.07.2026. – Режим доступу до ресурсу: https://www.advanta-group.ru/blog/cto-takoe-sistema-monitoringa-i-kontrola/.

9. Мониторинг и контроль [Електронний ресурс] // Хабр Трек – Доступ здійснено 07.07.2026. – Режим доступу до ресурсу: https://track.habr.com/frontend/skill/monitoring-control.

10. Стеклов В.К. Основи управління мережами та послугами телекомунікацій / В.К. Стеклов, Є.В. Кільчицький – К.: Техніка, 2002. – 438 с.

11. Saeed M. Agbariah Automated Policy Compliance and Change Detection Managed Service in Data Networks [Електронний ресурс] // Second International Conference on Advanced Information Technologies and Applications. – 2013. – pp. 1 - 12.

– Режим доступу до ресурсу: https://www.researchgate.net/publication/271376027_Automated_Policy_Compliance_and_Change_Detection_Managed_Service_in_Data_Networks.

12. Егунов М.М. Системы управления сетями связи: Уч. пособ. / М.М. Егунов, О.Г. Шерстнева, Е.А. Абзапарова. – Екатеринбург: УрТИСИ ГОУ ВПО «СибГУТИ», 2009. – 67 с.

13. Джонс Д. Создание унифицированной системы IT-мониторинга в вашем окружении / Дон Джонс. – Нью-Йорк: 2011 – 252 с.

14. Довгань А. Что такое мониторинг в IT или почему админы стали больше спать? [Електронний ресурс] / Алексей Довгань // Хабр – блог компании КРОК. – 2012. – Режим доступу до ресурсу: https://habr.com/ru/companies/croc/articles/144941/.

15. Clemm A. Network Management Fundamentals [Електронний ресурс] / Alexander Clemm // Cisco Press, Pearson Education. – 2006. – 528 p. – Режим доступу до ресурсу: https://api.pageplace.de/preview/DT0400.9781587052804_A26071270/preview-9781587052804_A26071270.pdf

16. Кореньков В. Архитектура и пути реализации системы локального мониторинга ресурсного центра [Електронний ресурс] / Владимир Кореньков, Павел Дмитриенко // Электронный журнал «Системный анализ в науке и образовании». – №3. – 2011. – Режим доступу до ресурсу: https://sanse.ru/index.php/sanse/article/view/43

17. Дмитриенко П.В. Методика оценки эффективности систем мониторинга вычислительных ресурсов [Електронний ресурс] / П. В. Дмитриенко // Компьютерные исследования и моделирование. – Т.4, №3. – 2012. – С. 661 - 668. – Режим доступу до ресурсу: https://crm.ics.org.ru/uploads/crmissues/crm_2012_3/661-668.pdf.

18. МЕТОДОЛОГІЯ IDEF0 [Електронний ресурс] // Електронна бібліотека Stud.com.ua. – Доступ здійснено 09.07.2026. – Режим доступу до ресурсу: https://stud.com.ua/180970/about.

19. Vacche A. D., Lee S. K. Zabbix Mastering / Dalle Vacche Andrea, Kewan Lee Stefan. – Packt Publishing Ltd. – 2013. – 358 p.

20. Будко Н.П. Общие принципы функционирования и требования к построению структур перспективных систем мониторинга распределенных информационно-телекоммуникационных сетей [Електронний ресурс] / Н.П. Будко // Техника средств связи. – №2(154). – 2021. – С. 38 - 59. – Режим доступу до ресурсу: https://cyberleninka.ru/article/n/obschie-printsipy-funktsionirovaniya-i-trebovaniya-k-postroeniyu-struktur-perspektivnyh-sistem-monitoringa-raspredelennyh/viewer.