Міністерство освіти і науки України
Харківський національний університет радіоелектроніки

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

КВАЛІФІКАЦІЙНА РОБОТА
Пояснювальна записка

рівень вищої освіти перший (бакалаврський)

Розробка системи моніторингу корпоративної мережі підприємства

(тема)

Виконав:
здобувач *4* року навчання,
групи *ТРІМІ-21-1*
Євгеній БРОВКО
(власне ім'я, прізвище)

Спеціальність *172 Телекомунікації та радіотехніка*
(код і повна назва спеціальності)
Тип програми *освітньо-професійна*
(освітньо-професійна або освітньо-наукова)
Освітня програма *Інформаційно-мережна інженерія*
(повна назва освітньої програми)
Керівник *асист. Інна ШТИХ*
(посада, власне ім'я, прізвище)

Допускається до захисту
Завідувач кафедри _____ *Валерій БЕЗРУК*
(підпис) (власне ім'я, прізвище)

2025 р.

Не містить відомостей заборонених до відкритого публікування.

Студент / Євгеній Бровко /

Керівник / Інна Штих /

Харківський національний університет радіоелектроніки

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

ЗАТВЕРДЖУЮ:

Зав. кафедри _____
(підпис)
«____»_____ 2025 р.

ЗАВДАННЯ

НА КВАЛІФІКАЦІЙНУ РОБОТУ

здобувачеві *Бровко Євгенію Олександровичу*
(прізвище, ім'я, по батькові)

1. Тема роботи *Розробка системи моніторингу корпоративної мережі підприємства*

затверджена наказом університету від 23 травня 2025 р. № 410 Ст

2. Термін подання здобувачем роботи до екзаменаційної комісії 17 червня 2025 р.

3. Вихідні дані до роботи *Дослідити існуючі методи моніторингу телекомунікаційних мереж. Провести порівняльний аналіз методів моніторингу для корпоративної мережі АТ «Сумиобленерго». Розробити рішення для створення системи моніторингу мережі що буде забезпечувати збір необхідних даних, надійний запис інформації у бази даних та інформування адміністратора у разі зміни статусу інтерфейсів комутаторів та УАТС. Розробити програму для реалізації системи моніторингу мовою Perl.*

4. Перелік питань, що потрібно опрацювати в роботі
Вступ
1. Огляд існуючих технологій моніторингу у телекомунікаційних мережах
2. Аналіз фрагменту відомчої мережі АТ «Сумиобленерго»
3. Розробка структури системи моніторингу корпоративної мережі
4. Розробка програмного забезпечення для системи моніторингу
5. Вимоги до якості системи моніторингу
Висновки

5. Перелік графічного матеріалу із зазначенням креслеників, схем, плакатів, комп'ютерних ілюстрацій (п.5 включається до завдання за рішенням випускової кафедри) *назва, мета і актуальність кваліфікаційної роботи; архітектура протоколу керування мережею SNMP; загальна характеристика фрагмента мережі АТ «Сумиобленерго»; вибір загальної схеми моніторингу, рішення використанням модему, серверів консолей та спеціалізованих комп'ютерів в кожному вузлі; структурні схеми мережі з використанням модему, серверів консолей та спеціалізованих комп'ютерів в кожному вузлі; розробка програми для моніторингу комутаторів мережі; елементи коду програми; формати даних для станцій; висновки*

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Терміни виконання етапів роботи	Примітка
1	*Ознайомлення із завданням. Уточнення ТЗ.*	*23.05.25*	*виконано*
2	*Підбір літератури за темою роботи.*	*24.05-05.06.25*	*виконано*
3	*Огляд існуючих технологій моніторингу у телекомунікаційних мережах*	*06.06-07.06.25*	*виконано*
4	*Аналіз фрагменту відомчої мережі АТ «Сумиобленерго»*	*08.06-10.06.25*	*виконано*
5	*Розробка структури системи моніторингу корпоративної мережі*	*11.06-12.06.25*	*виконано*
6	*Розробка програмного забезпечення для системи моніторингу*	*13.06-15.06.25*	*виконано*
7	*Вимоги до якості системи моніторингу*	*16.06.25*	*виконано*
8	*Оформлення презентаційного матеріалу, підготовка до захисту в ЕК*	*17.06.25*	*виконано*

Дата видачі завдання 23 травня 2025 р.

Здобувач _____
(підпис)

Керівник роботи _____ асист. Інна ШТИХ
(підпис) (посада, власне ім'я, прізвище)

РЕФЕРАТ

Пояснювальна записка 79 с., 13 рис., 5 табл., 8 джерел, 5 додатків.

Об'єкт дослідження – телекомунікаційна мережа підприємства.

Мета роботи – розробити систему моніторингу корпоративної мережі підприємства.

Контроль за телефонними службовими та корпоративними мережами також є необхідним як з точки зору функціонування мережі, так і з урахуванням необхідності аналізу тенденцій використання мережевого обладнання та каналів передачі даних для розуміння можливостей мережі для її розширення чи розвитку. Тому в роботі було проаналізовано структуру телекомунікаційної мережі підприємства, запропоновано рішення для впровадження оптимальної системи моніторингу.

На основі розробленої системи моніторингу розроблено необхідне програмне забезпечення для обладнання що застосовується у мережі.

ТЕЛЕКОМУНІКАЦІЙНА МЕРЕЖА, СИСТЕМА МОНІТОРИНГУ, ТАРИФІКАЦІЯ ДЗВІНКІВ, ОБРОБКА СТАТИСТИЧНИХ ДАНИХ УАТС.

THE ABSTRACT

Explanatory slip 79 p., 13 fig., 5 tab., 8 sources, 5 attach.

Object of research - enterprise telecommunications network.

The purpose of the work - develop a system for monitoring the company's corporate network.

Control over telephone service and corporate networks is also necessary both from the point of view of network functioning and in view of the need to analyse trends in the use of network equipment and data transmission channels to understand the network's capabilities for expansion or development. Therefore, the paper analyses the structure of the enterprise's telecommunications network and proposes solutions for implementing an optimal monitoring system.

Based on the developed monitoring system, the necessary software for the equipment used in the network was developed.

TELECOMMUNICATION NETWORK, MONITORING SYSTEM, CALL BILLING, PROCESSING OF UATS STATISTICS.

ЗМІСТ

С.

ПЕРЕЛІК СКОРОЧЕНЬ

ЛОМ	–	локально обчислювальна мережа;
МАТС	–	міська автоматична телефонна станція;
СУБД	–	система управління базами даних;
УАТС	–	установча автоматична телефонна станція;
ASN.1	–	Abstract Syntax Notation One (мова для опису абстрактного синтаксису даних);
MIB	–	Management Information Base (віртуальна база даних, яка використовується для управління мережевими об'єктами);
PDU	–	Protocol Data Unit (структурована одиниця даних, яка передається між мережевими елементами за певним протоколом);
Perl	–	Practical Extraction and Reporting Language (високорівнева, інтерпретована, динамічна мова програмування загального призначення);
RMON	–	Remote Monitoring (віддалене спостереження);
SMDR	–	Station Message Detail Recording (спеціалізований апаратний інтерфейс УАТС);
SNMP	–	Simple Network Manager Protocol (простий протокол керування мережею);
USM	–	User-Based Security Model (модель безпеки, орієнтована на користувача);
VACM	–	View-based Access-Control Model (модель контролю доступу на основі подань).

ВСТУП

Наразі спостерігається інтенсивне зростання секторальних та корпоративних комунікаційних мереж. Ці мережі стимулюють прогрес у сфері виготовлення техніки та введення інноваційних рішень, адже будь-який виробничий процес неможливий без належного зв'язку. Керівництво компаній, прагнучи збільшити продуктивність бізнесу, ставить перед собою завдання покращення якості телекомунікаційних послуг та їх функціонального розширення.

Для того, щоб зрозуміти можливості для розширення чи модифікації комунікаційної мережі, важливо аналізувати тенденції використання мережевого обладнання та каналів передачі даних.

Існують спеціалізовані стандарти управління мережами, які спрощують управління об'ємними та різноманітними мережами. Для управління мережами на основі протоколу IP використовується протокол SNMP (Simple Network Manager Protocol), що дозволяє координувати взаємодію між керуючою станцією та об'єктами управління, при цьому дані управління зберігаються безпосередньо в об'єкті. Такий підхід дозволяє централізовано керувати різними елементами мережі.

Контроль за телефонними службовими та корпоративними мережами також є необхідним. Виробники різних систем УАТС (установча автоматична телефонна станція) пропонують методи збору даних про телефонні дзвінки, що дозволяє, з одного боку, виставляти рахунки за користування послугами провайдера окремим абонентам, а з іншого - збирати статистичну інформацію.

1 ОГЛЯД ІСНУЮЧИХ ТЕХНОЛОГІЙ МОНІТОРИНГУ У ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖАХ

1.1 Протокол керування мережею SNMP

Існує дві ключові стратегії для впровадження процесу керування. Перша, яка володіє найбільшими можливостями, ґрунтується на розробці та застосуванні спеціалізованих програмних рішень для контролю над певним мережевим обладнанням. Друга стратегія покладається на використання даних, які представляють мережевий пристрій. У цьому контексті використовується потік даних замість потоку керування. Відмінність потоку даних полягає в можливості створення більш гнучкої, хоча і менш потужної, моделі керування. Головною перевагою є її незалежність не лише від програмного середовища, але й від специфіки апаратної реалізації керованого обладнання.

Для розробки уніфікованого методу керування обладнанням, що підключене до мереж IP, був створений простий протокол мережного керування (Simple Network Management Protocol — SNMP) [1].

З точки зору керування, мережу можна розділити на систему керування та об'єкти керування. Систему керування складають обчислювальні засоби, призначені для генерації керуючих впливів та аналізу інформації, на підставі якої ухвалюються рішення про керування. Об'єкти керування - це ресурси, якими потрібно управляти (активне мережеве обладнання, робочі станції, сервери тощо).

Система керування включає в себе станцію керування та набір допоміжних інструментів (зонди, аналізатори, програми тощо). Зазвичай станція керування представляє собою потужний комп'ютер зі спеціалізованим програмним забезпеченням. Одним з ключових елементів станції керування є опис об'єктів керування (станція також може бути об'єктом керування).

В об'єктах, що підтримують SNMP, існує спеціалізований програмний компонент, відомий як агент. Ці агенти збирають дані про пристрої, на яких вони встановлені, і надають ці дані системам управління мережами (NMS) через протокол SNMP. Ключова ідея протоколу полягає в тому, що всі дані, необхідні для керування пристроєм, зберігаються безпосередньо на ньому -

будь то сервер, модем чи маршрутизатор - у так званій базі даних управління (MIB). SNMP, будучи мережевим протоколом, пропонує лише команди для взаємодії з MIB змінними. Для моніторингу стану мережевого пристрою достатньо отримати доступ до його MIB, яка регулярно оновлюється пристроєм, і проаналізувати значення змінних. Задачі аналізу та обробки інформації, а також прийняття рішень щодо стану об'єкта лежать на системі управління. Вищеописана модель управління за допомогою SNMP представлена на рис. 1.1.

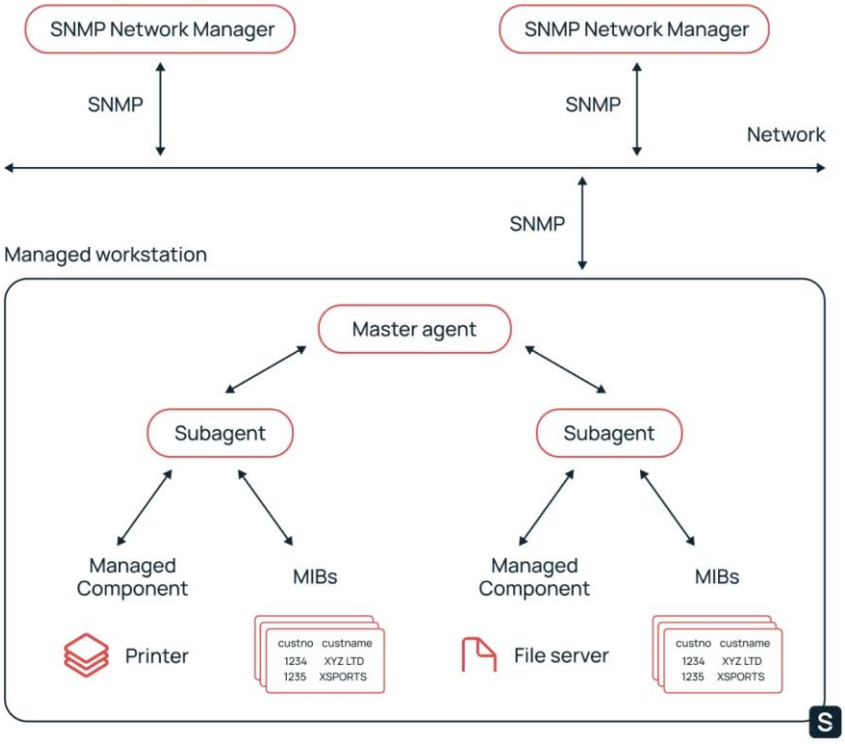

Рисунок 1.1 – Архітектура SNMP

Технологія SNMP включає три основні компоненти:

- структуру управлінської інформації (SMI);
- базу управлінської інформації (MIB);
- протокол SNMP, який встановлює правила взаємодії між менеджером та агентом.

Структура керівної інформації встановлює правила для опису управлінської інформації. Формальний опис об'єктів виконується за допомогою мови Abstract Syntax Notation One (ASN.1). Для визначення імені об'єкта достатньо надати його ідентифікатор (OBJECT IDENTIFIER), який представляє собою послідовність цілих чисел. Всі ідентифікатори розташовані у формі

дерева. На найвищому рівні дерева знаходяться три гілки: iso, ccitt і joint-iso-ccitt, що належать до різних стандартних організацій. У піддереві iso розташований ідентифікатор org (корінь для піддерев різних організацій), одним з підгілок якого є Міністерство оборони США (DOD). Прийнято вважати, хоча це і не зафіксовано офіційно, що перша гілка в піддереві DOD - це Internet [1].

Тобто, об'єкт "Internet" має ідентифікатор "1.3.6.1": internet OBJECT IDENTIFIER ::= { iso(1) org(3) dod(6) 1}.

Щоб коректно розшифрувати значення певного ідентифікатора, одного його недостатньо. Потрібно вказати тип елемента та надати йому визначення. Для цього існує інформаційна база управління (Management Information Base — MIB), де описано всі елементи згідно з граматикою ASN.1. Наявність текстової версії бази MIB у системі управління дозволяє не лише коректно розшифровувати отримані дані, але й надавати користувачу роз'яснення щодо елементів, виходячи з їх опису в базі. Для керованого об'єкта текстова версія бази MIB не є обов'язковою.

Для кращого розуміння структури MIB її зручно представляти у вигляді дерева. Розглянемо приклад (рис. 1.2) де показано частину дерева MIB. Кожен елемент у MIB ідентифікується за допомогою унікального ID-OID, який виражений у вигляді числової послідовності та має ієрархічну будову. OID слугує числовим представленням шляху до об'єкта, вказуючи на значення кожної таблиці в MIB, кожного рядка у таблиці та кожного елемента в рядку.

Для прикладу, OID 1.3.6.1.4.868.2.4.1.1.1.3.3562.3. відповідає iso.org.dod.internet.private.transition.products.chassis.card.slotCps.cpsSlotSummary.cpsModuleTable.cpsModuleEntry.cpsModuleModel.3562.3. Використовуючи перші шість цифр даного OID, можливо навігувати по дереву на схемі.

У вітці internet (1) знаходиться чотири піддерева. Вони включають:

- directory (1) – каталог OSI;
- mgmt (2) – стандартні об'єкти RFC;
- experimental (3) - експерименти з Internet;
- private (4) – залежить від виробника.

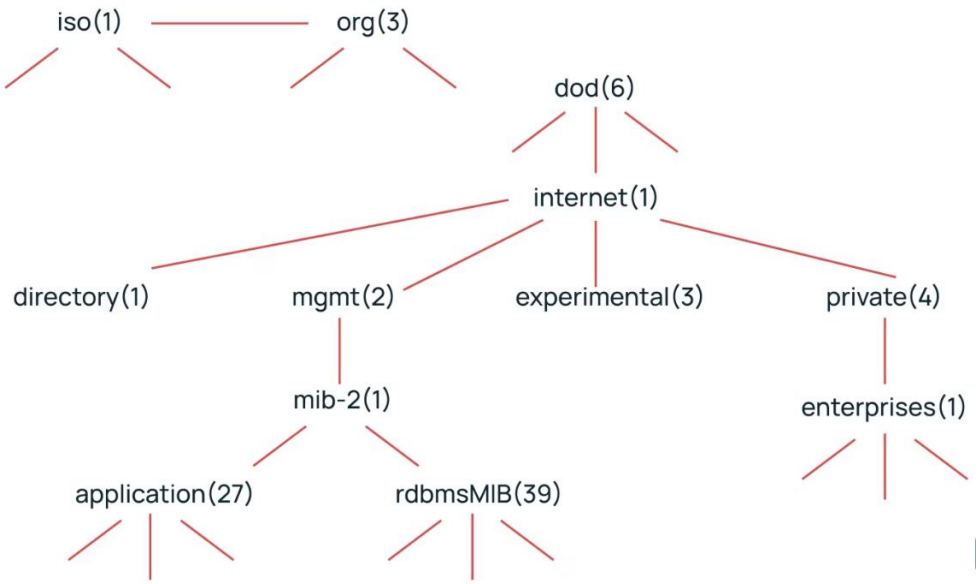

Рисунок 1.2 – Схематичне представлення дерева OID у MIB

Деякі значення OID включають інформацію про виробника апарату, що дозволяє легко знайти специфічні дані про пристрій.

Структура MIB та OID у SNMP у вигляді дерева може здатися складною, проте вона надає певні переваги. Ця система є простою та адаптивною для управління мережевими апаратами, ефективно функціонуючи для мереж будь-якого розміру.

Надалі, коли ми говоримо про "значення змінної", маємо на увазі значення об'єкта з конкретним названим ідентифікатором. Щодо згаданих протоколів, для уникнення конфліктів у структурі об'єктів передбачено спеціальний вузол private (internet 4), в якому одним із гілкових вузлів є "підприємства" (enterprises, private 1).

Протокол SNMP, в свою чергу, є досить простим і функціонує на основі механізму "запит-відповідь". Повідомлення SNMP передаються через UDP дейтаграми. Основні дії, які передбачені протоколом:

– Get_request - отримати значення зазначеної змінної чи інформацію про стан мережного елемента;

– Get_next_request – отримати значення змінної, не знаючи точного її імені (наступний логічний ідентифікатор на дереві MIB);

– Set_request - присвоїти змінній відповідне значення. Використовується для опису дії, яка має бути виконана;

– Get_response - відгук на Get_request, Get_next_request та Set_request.

Містить також інформацію про стан (коди помилок та інші дані);

– Trap - відгук мережного об'єкта на подію чи зміну стану [1].

Схема взаємодії менеджера та агента у протоколі SNMP показано на рис. 1.3.

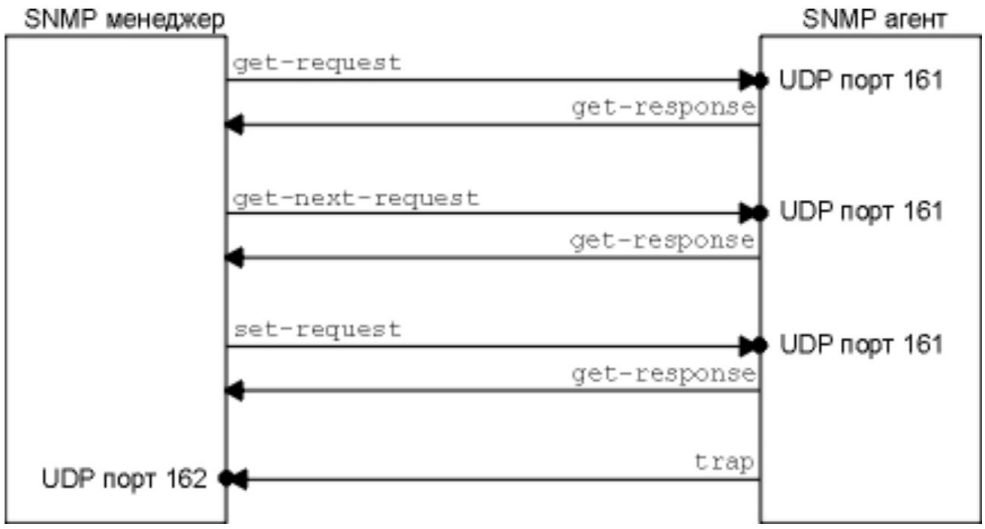

Рисунок 1.3 – Оператори SNMP

Відносини між менеджером та агентом не завжди слідують строгій схемі "запит-відповідь". Іноді активну участь має брати керований пристрій. Щоб дати можливість пристрою ініціативно передавати інформацію, використовується спеціальний блок даних Trap (переривання). Серед подій, які вимагають особливої уваги, можна виділити перезапуск пристрою, втрату зв'язку та інші. Вони залежать від функціоналу пристрою.

Наразі існують три версії протоколу SNMP.

SNMPv1. Ця версія підтримує зазначені вище операції. Безпека в ній заснована на використанні імені спільноти (Community Name), яке передається в заголовку SNMP і є єдиним засобом захисту даних. Для взаємодії програми-агента і менеджера необхідно, щоб обидва визнали однакове ім'я спільноти. Однак, такий метод захисту часто виявляється недостатнім, адже ім'я спільноти передається відкритим текстом у кожному SNMP пакеті [2].

SNMPv2. Одне з інноваційних рішень в SNMPv2 полягає в тому, що елемент управління мережею може виступати як менеджер, так і агент, або виконувати обидві ролі одночасно. Ця концепція дозволяє використовувати SNMP у ієрархічній структурі, де локальні менеджери підзвітні менеджерам

середнього рівня, які, у свою чергу, контролюються менеджером вищого рівня [2].

Також у SNMPv2 з'явилася нова операція get_bulk_request, що дозволяє здійснювати запит на велику кількість однорідних даних (наприклад, таблицю), зменшуючи при цьому кількість запитів і, відповідно, мережевий трафік.

Крім того, було введено новий тип переривань, званий inform, який на відміну від trap переривань потребує підтвердження від менеджера. У випадку використання inform, інформація про переривання зберігається в пам'яті пристрою і у разі невдачі повторно відсилається керуючій станції. Цей тип переривань рекомендується використовувати лише тоді, коли пам'ять керованого об'єкта дозволяє зберегти цю додаткову інформацію.

SNMPv3. У третій версії SNMP протокол став значно складнішим, проте він зберіг сумісність з попередніми версіями. У цій версії обладнання та елементи керування отримали назву "сутність" (entities). Сутність, яка розміщена на роутері (зазвичай відома як агент), та інша сутність, що відповідає за опитування програм, раніше називалася менеджером. Кожна з сутностей містить ядро SNMP та додаткові компоненти. Ядро SNMP включає чотири основні функції: контроль доступу, безпеку, обробку повідомлень та диспетчеризацію. Модуль обробки повідомлень та диспетчер також підтримують функціонал версій SNMPv1 та SNMPv2, включаючи обробку команд set та get, а також форматування даних SNMP або PDU (protocol data unit). Диспетчер виконує функцію контрольного пункту, тобто всі повідомлення проходять через нього. Він визначає версію протоколу повідомлення та направляє його до відповідного модуля для аналізу. У випадку невизначеності версії, наприклад, через помилку у форматі пакета, диспетчер фіксує помилку. Після цього процесор повідомлень передає повідомлення до підсистеми безпеки або контролю доступу, а потім знову диспетчеру, який вже розсилає його до SNMP-додатків [2].

Головним нововведенням версії 3 стала вдосконалена система безпеки. Для забезпечення аутентифікації та конфіденційності використовується User-Based Security Model (USM), модель безпеки, орієнтована на користувача. USM включає модулі для аутентифікації, контролю часу та забезпечення конфіденційності. Модулі аутентифікації та конфіденційності забезпечують цілісність та достовірність даних, а також їх захист. Модуль контролю часу

допомагає запобігти атакам повторного відтворення, блокуючи пакети з застарілими часовими мітками.

В USM застосовуються алгоритми MD5, SHA та інші методи хешування. З метою безпеки пароль не передається через мережу. Замість цього PDU-блок піддається хешуванню двічі з використанням ключів, отриманих з приватного ключа, а перші 12 октетів слугують як код автентифікації повідомлення (MAC), який додається до повідомлення. Процес на приймаючій стороні відбувається в зворотньому порядку.

SNMPv3 пропонує три рівні аутентифікації та конфіденційності: "noAuthNoPriv" без аутентифікації та конфіденційності, "authNoPriv" з аутентифікацією, але без конфіденційності, та "authPriv", що включає як аутентифікацію, так і шифрування даних SNMP.

SNMPv3 також включає модель контролю доступу на основі подань (VACM, View-based Access-Control Model), яка дозволяє обмежувати доступ до змінних MIB. У цій моделі "подання" визначає доступну частину бази MIB, а також встановлює зв'язок між користувачами та цим поданням. Для реалізації механізмів VACM необхідно створити подання та групу на кожному мережевому пристрої, де подання вказує на доступну частину MIB, а група асоціює користувачів, що до неї належать [2].

1.2 Технологія RMON

У SNMP існують дві основні частини: транспортна система для передачі управлінських даних через мережу та структура або модель даних, відома як база даних управління, або MIB. Віддалене спостереження (RMON – Remote Monitoring) представляє собою розширену базу даних управління для підтримки застосунків, яким потрібно більше інформації, ніж може надати SNMP MIB-2.

Бази даних RMON включають в себе набір статистичних, аналітичних та діагностичних даних, забезпечуючи незалежність від виробника обладнання. Різниця між RMON і SNMP полягає в типі збираємих даних: якщо в MIB-2 ці дані описують лише події, що відбуваються на вузлі з встановленим агентом, то дані RMON описують трафік будь-яких (в тому числі неінтелектуальних) мережевих пристроїв. Основною перевагою моніторингу RMON є можливість

зберігання статистичних даних у різні моменти часу безпосередньо в зонді, а також те, що агенти (зонди) RMON виконують первинну обробку даних (фільтрацію та сортування).

Стандарт RMON працює на фізичному та канальному рівнях мережевої моделі OSI та містить 10 груп баз [2]:

- Statistics – загальний мережевий трафік та статистика помилок. Лічильники для підрахунку кількості переданих байтів, пакетів, пакетів з помилками, широкомовних пакетів тощо встановлені як 32-бітні лічильники, які при переповненні скидаються;
- History – на основі групи Statistics, ця група призначена для аналізу динаміки мережі протягом часу, створення базових показників, порівняння змін, що відбуваються в мережі, у різний час. Зонд може зберігати певну кількість статистичних вибірок (залежно від об'єму оперативної пам'яті зонда), яку встановлює користувач, через заданий користувачем інтервал часу (від 1 сек до 3600 сек) для збору як короткотермінової, так і довготермінової статистики;
- Alarms – дозволяє користувачам встановлювати абсолютні або відносні порогові значення для змінних у базах MIB, при досягненні яких зонд відправлятиме попередження (Traps) на керуючу станцію згідно з налаштуваннями у групі Events;
- Hosts – у табличній формі надає статистику трафіку для кожного мережного
  вузла на основі його MAC-адреси;
- HostTopN – розширює попередню групу, ранжуючи вузли, які найбільше навантажують трафік сегмента або створюють найбільшу кількість помилок. Кількість вузлів, що відстежуються, встановлюється користувачем;
- Matrix – відслідковує обсяг трафіку або кількість помилок між двома пристроями згідно з їх MAC-адресами;
- Filter - у поєднанні з групою Packet Capture дозволяє захоплювати пакети для подальшого аналізу. Зонд може фільтрувати пакети для пошуку конкретної інформації всередині пакета. Є можливість вибіркового пошуку пакетів за певною адресою, групою адрес, конкретним

протоколом або будь-якою бажаною комбінацією. Створені фільтри використовуються групами Capture і Events;

- Packet Capture - встановлює обсяг і розмір буферів для захоплення пакетів, які декодуються на керуючій станції. Вказується, продовжувати чи зупиняти захоплення при переповненні буфера, і встановлюється вікно захоплення (проводиться захоплення всього пакета або його частини);
- Events - визначає, які повідомлення (Traps) можуть бути відправлені зондом на керуючу консоль (або кілька станцій) у випадку подій: перевищення порогових значень, захоплення пакетів згідно з вказаним шаблоном, наявність зв'язку, відсутність зв'язку, холодний старт, теплий старт, несанкціонований доступ та інші. Керуюча станція може ігнорувати надходження повідомлення або здійснює запис, отримує повідомлення у журнал та ініціює автоматичні процеси (відображає повідомлення на екрані, запускає конкретний додаток і т.д.);
- Token Ring надає комплект статистичної інформації для мереж Token Ring [2].

Розвиток технології RMON призвів до стандарту RMON2, який покращує аналіз мережевого трафіку та додатків, що використовуються користувачами. Зонди RMON2 проводять збір даних та дозволяють переглядати трафік на рівні мережі та додатків моделі OSI між кінцевими точками.

Агенти RMON можуть бути інтегровані в пристрої, проте це обмежує їх функціонал, або вони можуть представляти собою окремі програмні чи апаратні одиниці.

1.3 Рішення компанії Cisco у сфері управління мережами

Завдяки SNMP протоколу та RMON технології, існують численні програмні та апаратні засоби для контролю та управління мережами. Розроблені великі комерційні системи дозволяють вирішувати різноманітні завдання. Виробники мережевого обладнання пропонують власні програмні рішення. Серед них можна виділити HP OpenView від Hewlett-Packard, NetView for AIX від IBM, SunNet Manager від підрозділу Sun в компанії SunConnect, Spectrum від Cabletron System та NetWare Management System від Novell (переважно використовується для управління локальними мережами, що

базуються на сімействі операційних систем NetWare).

Також наявна велика кількість безкоштовних програм, які зазвичай призначені для вирішення специфічних завдань (наприклад, утиліти для перегляду MIB обладнання, або програми для збирання даних з MIB змінних та їх збереження у базі даних тощо). Проте існують і безкоштовні альтернативи комерційним платформам управління. Наприклад, програма BlueBird (OpenNMS).

Для кращого розуміння функціоналу комерційних систем моніторингу та управління, розглянемо програмні засоби, які пропонує компанія Cisco.

Cisco надає серію програмних продуктів під узагальненою назвою CiscoWorks, яка поділяється на два основні типи:

1. Рішення CiscoWorks2000 представляють собою комплексні рішення для мереж середнього та великого масштабу (enterprise). Вони зосереджені на трьох ключових напрямках: управління глобальними мережами (WAN), управління локальними мережами (LAN) та управління на рівні надання послуг [3].

Для реалізації комплексних рішень у цих сферах Cisco пропонує такі програмні пакети:

- CiscoWorks2000 LAN Management Solution (LMS) – пакет для управління комутованими локальними мережами;
- CiscoWorks2000 Routed WAN Management Solution (RWAN) – пакет для управління маршрутизованими широкомасштабними мережами;
- Network Management Solution (SNMS) – пакет для управління маломасштабними локальними мережами;
- CiscoWorks2000 VPN/Security Management Solution (VMS) – пакет для управління системами мережевої безпеки;
- CiscoWorks IP Telephony Environment Monitor (ITEM) – пакет для управління мультисервісними мережами з підтримкою Cisco IP Telephony та програм IP телефонії [3].

2. Самостійні продукти серії CiscoWorks доповнюють можливості основних рішень для мереж початкового рівня, бездротових мереж та інших галузей управління [3]:

– CiscoWorks for Windows (CWW) – полегшена версія мережного управління, у якій передбачені всі можливості, необхідні управління мережею

малого підприємства, підприємства середніх розмірів чи робочої групи;

– CiscoWorks QoS Policy Manager – програмний комплекс, що полегшує впровадження диференційованих послуг та підтримки якості послуг (Quality of Service, QoS) на основі централізованої політики;

– CiscoWorks Wireless LAN Solution Engine – програмно-апаратний комплекс, що вирішує завдання повсякденного моніторингу та управління інфраструктурою бездротових локальних мереж Cisco Aironet;

– CiscoWorks Hosting Solution Engine – програмно-апаратний комплекс, що автоматизує завдання підтримки центрів обробки даних для бізнес-додатків [3].

Програмний продукт CiscoWorks базується на широко відомому протоколі для управління мережами Simple Network Management Protocol (SNMP), що забезпечує ефективне управління обладнанням Cisco в різноманітних мережевих середовищах. Додавання нових компонентів до існуючої системи управління мережею CiscoWorks може значно покращити її функціональність.

Детальніше розглянемо комплексне рішення для локальних мереж – CiscoWorks2000 LAN Management Solution, адже цей проект зосереджений на аналізі локальної мережі:

– Campus Manager (CM) – для виявлення та управління L2/L3 (Layer2/Layer3 – другого та третього рівня моделі OSI – Open System Interconnection) комутаторами, конфігурування та управління VLAN (Virtual Local Area Network – віртуальні локальні мережі) та ATM LANE (Asynchronous Transfer Mode LAN Emulation – ATM телефонів;

– Device Fault Manager (DFM) – забезпечує в режимі реального часу виявлення та визначення причин збоїв мережного обладнання;

– Cisco nGenius Real-Time Monitor – інструмент для збору та відображення RMON статистики, що генерується комутаторами Catalyst, модулями мережевого аналізу Network Analysis Module та зовнішніми пробниками RMON;

– Resource Manager Essentials – для керування критичними мережевими ресурсами через Інтернет з використанням Web-інтерфейсу .

– CiscoView (CD-One) – графічний засіб управління пристроями;

– CiscoWorks2000 Management Server – загальне управління інтеграцією зі

сторонніми системами мережевого управління, контролем адміністративного доступу та сервісами для всього сімейства рішень CiscoWorks2000 [3].

1.4 Системи тарифікації для УАТС

Сучасні УАТС здатні надавати дані про телефонні дзвінки через спеціалізований апаратний інтерфейс, який зазвичай має назву SMDR (Station Message Detail Recording) або CDR (Call Detail Recording). Під'єднавши до цього інтерфейсу персональний комп'ютер, можна отримувати, зберігати та аналізувати ці дані. Однак, для цього потрібно встановити на комп'ютері спеціальне програмне забезпечення – систему тарифікації.

Система тарифікації – це програма для автоматичного обліку та розрахунку вартості телефонних розмов. Такі системи поділяють на два типи – операторські, які використовуються телекомунікаційними компаніями, та корпоративні, що застосовуються в межах певної організації. У цьому контексті ми зосередимося на функціях корпоративних систем тарифікації, які відповідають потребам кваліфікаційної роботи.

Функціонал сучасних корпоративних систем тарифікації є дуже розширеним. Вони не лише розраховують вартість дзвінка, але й фіксують багато інших параметрів, необхідних для детального обліку. Наприклад, можна відстежити номери абонентів, відділ та кімнату, з якої здійснено дзвінок, географічний регіон спілкування, використану зовнішню лінію та інше.

Зібрані дані зберігаються для подальшого аналізу. Ефективна система тарифікації пропонує розширені можливості для перегляду та автоматизованого пошуку потрібної інформації у базі даних, використовуючи задані критерії пошуку, наприклад, виявлення всіх міжнародних дзвінків відділу маркетингу за останній місяць.

Ці дані можна також представити у формі звітів або експортувати в різноманітні офісні програми, такі як Word, Excel чи бухгалтерські додатки. Найпотужніші системи тарифікації проводять статистичний аналіз даних і візуалізують результати для зручності аналізу.

Основне призначення системи тарифікації – це формування рахунків за телефонні розмови. Крім того, система тарифікації може бути корисною для технічних спеціалістів для аналізу трафіку телефонної мережі, що допомагає в

оптимізації налаштувань та конфігурації системи, а також для реагування на збільшення навантаження. Це сприяє покращенню якості зв'язку та зниженню витрат за рахунок оптимального використання доступних телефонних ліній та вибору економічно вигідних маршрутів для дзвінків.

На сьогоднішній день ринок систем тарифікації є дуже різноманітним. Всі корпоративні системи тарифікації можна умовно розділити на три головні категорії:

- найпростіші тарифікатори;
- системи, що постачаються в комплекті з УАТС;
- універсальні тарифікаційні системи.

Зазвичай до першої категорії відносять програмне забезпечення, створене на замовлення або розроблене незалежно. Раніше, у випадках коли виробники АТС не включали тарифікатор до комплекту, таке ПЗ розробляли дистриб'ютори УАТС самостійно. Ці системи є доступними за ціною та обмежені лише функцією тарифікації, що робить їх малоефективними для фінансового обліку та моніторингу телефонних дзвінків.

Системи, що надаються разом з АТС від виробників, також мають певні недоліки. Вони, як правило, призначені для використання лише з певним типом УАТС, не завжди задовольняють актуальні вимоги до програмного забезпечення, мають високу вартість і не адаптовані для роботи у україномовному середовищі. Більше того, не всі виробники УАТС пропонують власні системи тарифікації.

Універсальні тарифікаційні системи від незалежних розробників програмного забезпечення зазвичай відповідають сучасним стандартам і підтримують АТС від різних виробників. Вони часто пропонують додаткові функції для ведення обліку та аналізу зібраної інформації, а також для фінансового управління, тому їх іноді називають білінговими системами (Billing System). До прикладів білінгових систем зарубіжного виробництва можна віднести такі продукти, як Ringmaster (Ірландія), BackTrack (США), PhonEx Pro (Ізраїль) і CallMaster (Канада).

2 АНАЛІЗ ФРАГМЕНТУ ВІДОМЧОЇ МЕРЕЖІ АТ "СУМИОБЛЕНЕРГО"

2.1 Загальна характеристика фрагмента мережі. Кабельна система

Фрагмент мережі АТ "Сумиобленерго" представляє дві незалежні мережі – телефонну мережу і мережу передачі даних, що об'єднані лише загальної кабельної системою.

Ділянка мережі охоплює п'ять вузлів, що розкидані по місту і з'єднані в конфігурації "зірка", де центральним є вузол А (рис. 2.1).

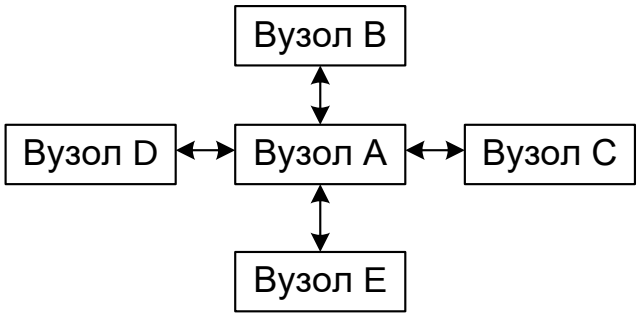

Рисунок 2.1 – Схематичне представлення мережі АТ «Сумиобленерго»

Ця конфігурація вирізняється високою ефективністю використання комунікаційних ліній між вузлами, проте її слабкість полягає у вразливості мережі до збоїв центрального вузла, що призводить до втрати зв'язку між усіма вузлами. Однак, для підвищення надійності мережі застосовуються додаткові заходи, такі як використання гарячого резервування в мультиплексорах та здатність мультиплексорів формувати кільцеву топологію у випадку виходу з ладу комутаційного обладнання центрального вузла, що дозволяє лініям зв'язку з'єднуватися безпосередньо, обходячи пошкоджене обладнання.

У всіх сегментах мережі використовується волоконно-оптичний кабель різних типів для кабельної системи. Різні волоконні пари одного кабелю застосовуються для створення телефонної мережі та мережі зв'язку між вузлами. Окрім участку між вузлом А та вузлом С, де мультиплексор поєднує трафік телефонної мережі та мережі передачі в одну пару волокон.

Занесемо базові характеристики кабельної системи в таблицю 2.1.

Таблиця 2.1 - Базові характеристики кабельної системи

Ділянка мережі	Тип волокна	Кількість волокон	Протяжність, км
Вузол А – вузол В	Одномодове	16	1,2
Вузол А – вузол С	Багатомодове	4	6,5
Вузол А – вузол D	Одномодове	8	11
Вузол А – вузол Е	Одномодове	16	1,5

2.2 Характеристика фрагмента телефонної мережі

Ділянка телефонної мережі побудована на базі цифрових автоматичних станцій Hicom фірми Siemens та NEAX фірми NEC.

У вузлі А встановлено станцію Hicom 382, на вузлі В використовується станція Hicom 350E, на вузлах С і D - станції Hicom 3x3, а на вузлі Е - станція NEAX 2000 IPS. Станції з’єднані потоками Е1. Для чого в них встановлені плати PRI ISDN.

Вузол А та В зв’язані двома потоками Е1, що об'єднані модулем STM-1, через мультиплексори STM-1/STM-4 Metropolis AMU фірми Lucent Technologies. Кожне з'єднання Е1 між станціями та мультиплексором здійснюється по крученій парі, а зв’язок між мультиплексорами організовано по волоконно-оптичній лінії.

Також було створено зв'язок між вузлами А та Е, при цьому використовується єдиний канал Е1, який підключений у вузлі А до того ж мультиплексора Metropolis AMU. Даний мультиплексор обладнаний 16 інтерфейсами для з'єднання каналів Е1 через кабель зі скрученою парою та двома оптичними інтерфейсами STM-1. В результаті, можливо створити дві оптоволоконні лінії в обох напрямках.

Між вузлами А та С діє один потік Е1 через мультиплексори DLC-1100E фірми НАТЕКС. Конфігурація такого мультиплексора має модуль для роботи з АТС за інтерфейсом Е1 та оптичний приймач.

Між вузлами А і D також діє один потік Е1 безпосередньо, через оптичні інтерфейси станцій Hicom 382 і Hicom 3x3, без використання мультиплексорів.

2.3 Характеристика фрагмента мережі передачі

Фрагмент мережі передачі даних організовано на комутаторах фірми Cisco.

На вузлах B, C, D, E застосовують комутатори Catalyst 2950T-24 із 24 портами для з'єднання мережевих пристроїв через Ethernet 10/100BaseT. Це свідчить про те, що хоча на цьому комутаторі можна створювати віртуальні локальні мережі, комутація між ними безпосередньо неможлива. Для такої операції потрібен пристрій третього рівня моделі.

Для з'єднання комутаторів між собою через волоконно-оптичну лінію використовують медіаконвертори, які переводять середовище з 100BaseT (кабель зі скрученою парою) на 100BaseFX (волоконно-оптичний кабель). Для зв'язку між вузлами A та B, D, E застосовують медіаконвертори AT-MC103XL від Allied Telesyn для одномодового кабелю. Тоді як між вузлами A і C пролягає багатомодовий кабель, але комутатори підключені до мультиплексорів DLC-1100E, до конфігурації яких входить модуль для передачі даних з інтерфейсом 10/100BaseT. Отже, між вузлами A та C використовується одна волоконна пара для телефонії та передачі даних.

2.4 Характеристика обладнання з позиції моніторингу

Комутатори Catalyst 2950-24T у всіх вузлах крім A мають програмне забезпечення Cisco IOS версії 12.1(20) EA1a. А комутатор Catalyst 3550 у вузлі A оперує програмним забезпеченням Cisco IOS версії 12.1(11) EA1.

Обидві версії програмного забезпечення пропонують різноманітні інструменти для спостереження за обладнанням. Підтримуються наступні версії протоколу SNMP: v1, v2C (Classic), v3. Вибір конкретної версії відбувається під час налаштувань. Це дозволяє забезпечити гнучкість у рівні безпеки – від доступу до агента SNMP лише на рівні спільноти до реалізації авторизації та шифрування переданих даних. Більше того, застосування протоколу SNMP з версією 2C дозволяє комутатору виступати як менеджер і таким чином, інтегруватися в ієрархічну структуру управління мережею.

Окрім можливості застосування різних моделей безпеки (SNMPv1, SNMPv2C, SNMPv3), у моделі SNMPv3 існують різні рівні безпеки. Для комутаторів Catalyst ці рівні представлені в таблиці 2.2.

Таблиця 2.2 - Рівні безпеки для комутаторів Catalyst

Модель безпеки	Рівень безпеки	Аутентифікація	Шифрування	Опис
1	2	3	4	5
SNMPv1	noAuthNoPriv	Рядок спільноти	Ні	Аутентифікація лише на ім'я спільноти
SNMPv2C	noAuthNoPriv	Рядок спільноти	Ні	Аутентифікація лише на ім'я спільноти
SNMPv3	noAuthNoPriv	Ім'я користувача	Ні	Аутентифікація на ім'я користувача
SNMPv3	AuthNoPriv	MD5 або SHA	Ні	Підтримується автентифікація, що базується на алгоритмах HMAC-MD5 або HMAC-SHA
SNMPv3	AuthPriv	MD5 або SHA	DES	Підтримується автентифікація, що базується на алгоритмах HMAC-MD5 або HMAC-SHA. Підтримується стандарт шифрування DES (56 біт) разом із стандартом автентифікації CBC-DES. Для підтримки шифрування потрібно встановити на комутатор додаткове програмне забезпечення.

Існує також опція конфігурації комутаторів, що дозволяє їм відправляти SNMP-сповіщення, відомі як "пастки", у випадку певних подій (наприклад, коли відбуваються зміни в налаштуваннях SNMP на комутаторі).

Комутатори Cisco підтримують функціонал RMON. В операційній системі Cisco IOS впроваджено чотири групи RMON:

– Statistics - збір статистичних даних про трафік, що проходить через інтерфейс;

– History – збирання статистичних вибірок через певний інтервал;

– Alarm – установка деяким змінним MIB порогових значень та

генерація повідомлень (якщо це визначено групою Event) на станцію, що управляє;

– Event – визначення ситуацій, коли потрібно надіслати повідомлення керуючої станції [4].

Мультиплексори Metropolis AMU фірми Lucent Technologies та DLC-1100E фірми НАТЕКС також підтримують протокол SNMP. Але мультиплексор DLC-1100E необхідно додатково встановити для цього модуль мережевого управління NMI [5].

Усі станції Hicom та NEAX передбачають видачу тарифікаційної інформації на термінальний порт (у даному випадку це com-порт). Крім того, станції Hicom можуть накопичувати цю інформацію на своїх внутрішніх жорстких дисках, а тимчасовий буфер (на кілька сотень записів) мають станції NEAX. Підтримуються різні формати інформації, що видається, які можна налаштувати з терміналу управління станцією. Станції Hicom 382, 3x3, 350H мають по три com-порти, станція NEAX 2000IPS має один com-порт [5].

3 РОЗРОБКА СТРУКТУРИ СИСТЕМИ МОНІТОРИНГУ КОРПОРАТИВНОЇ МЕРЕЖІ

3.1 Вибір рішення для моніторингу мережі передачі даних

Відповідно до поставленого завдання, необхідно налаштувати систему моніторингу, яка буде відстежувати стан комутаторів Cisco Catalyst 2950T-24 і Catalyst 3550-24T, а також їх інтерфейсів. Моніторинг стану комутаторів передбачає збір даних про навантаження на центральний процесор, кількість доступної пам'яті та час безперервної роботи (up-time). Моніторинг стану інтерфейсів включає збір інформації про загальну кількість переданих пакетів через інтерфейс, а також кількість пакетів, що містять помилки. Також потрібно забезпечити негайне повідомлення адміністратора про будь-які зміни статусу інтерфейсу (up або down).

Збір статистики є важливим для внутрішнього моніторингу мережі передачі даних, щоб зрозуміти рівень навантаження на мережеве обладнання та комунікаційні канали. Маючи таку інформацію, можна більш точно визначити, як використовується обладнання та чи потрібне розширення мережі. У цьому дипломному проекті не передбачено завдань, пов'язаних з обробкою або візуалізацією цієї інформації.

Усі комутатори у мережі виконують роль магістральних, тобто до них підключено інше мережеве обладнання, яке забезпечує зв'язок між різними підрозділами, включаючи віддалені. Обслуговування обладнання в підрозділах відбувається іншими співробітниками, ніж обслуговування магістрального обладнання. Тому моніторинг стану інтерфейсів з можливістю повідомлення про зміни є критично важливим для оперативного виявлення та усунення несправностей, що дозволяє уникнути тривалого простою підрозділів без зв'язку.

Обмеженість спектру задач, для яких призначені спеціалізовані програмні рішення, наприклад від компанії Cisco, є очевидною. Крім того, такі рішення часто виявляються надмірно дорогими, з цінами, що коливаються від 5 до 30 тисяч доларів США, залежно від обсягу функцій.

Існуючі безкоштовні програми можуть вирішувати лише обмежене коло завдань і часто важко знайти серед них ту, яка б ідеально відповідала специфічним потребам. Крім того, оновлення та адаптація таких програм можуть становити певні труднощі.

Оптимальним варіантом стає розробка власної програми. До такого рішення призвели кілька ключових аспектів:

- єдина підтримка протоколу управління SNMP обладнанням та доступність на сайті www.cisco.com переліку всіх змінних MIB, які підтримує обладнання;
- навички програмування на мові Perl та наявність готових модулів для роботи з SNMP для цієї мови;
- можливість майбутнього розширення функціоналу та адаптації програми під нові завдання.

3.2 Вибір рішення для тарифікаційної системи

Згідно з поставленим завданням, потрібно здійснити збір тарифікаційних даних зі станцій Hicom та NEAX, а також їх збереження для подальшого аналізу та обробки.

Рахунки за використання телефонного зв'язку АТ "Сумиобленерго" видаються безпосередньо провайдером (у цьому випадку Сумською МАТС), проте вони включають інформацію лише про міжміські дзвінки, не враховуючи дзвінки в межах власної телефонної мережі. Більше того, при підключенні до провайдера через E1 потоки, тарифікація може проводитись за основним номером, тобто одним номером для всіх E1 каналів. Це ускладнює визначення, кому саме з абонентів УАТС виставляти рахунок. Крім того, інформація про внутрішні дзвінки допоможе оцінити завантаженість телефонної мережі, що сприятиме оцінці ефективності використання обладнання та комунікаційних каналів, а також плануванню розвитку мережі.

Отже, збір та обробка тарифікаційної інформації є важливими для компанії. Однак, застосування платних програмних рішень (універсальних або спеціалізованих, що надаються виробником для певної станції) не є економічно виправданим. Більше того, при виставленні рахунків провайдер керується часом дзвінка, зафіксованим на його боці, який може відрізнятися від часу на

УАТС через затримки у встановленні з'єднання. При використанні тарифікаційних систем для конкретної УАТС при підготовці рахунків враховується місцевий час, тому можливі розбіжності з провайдером. Тарифікаційна система в цьому випадку не є обов'язковим елементом для функціонування телефонної мережі, як це може бути для телекомунікаційних компаній, що отримують дохід від надання послуг. І завдання такої системи не є складними, тому можливе розроблення власного програмного забезпечення.

У межах даної кваліфікаційної роботи мають бути вирішені наступні завдання:

- збір даних про дзвінки зі станції та їх завантаження до бази даних;
- візуалізація у вигляді діаграми навантаження на конкретний напрямок.

3.3 Вибір загальної схеми моніторингу

У роботі аналізується частина мережі, яка складається з п'яти вузлів. Технічне обслуговування зазначеного обладнання здійснюється виключно у головному вузлі (вузол А), тоді як у будівлях з іншими вузлами персонал присутній не завжди.

Отже, необхідно організувати систему моніторингу, яка б забезпечила надійну передачу даних про стан устаткування до центрального вузла.

Передача даних про стан комутаторів Cisco Catalyst 2950 та Catalyst 3550 використовуючи протокол SNMP, здійснюється через мережу передачі даних. Для дистанційного управління системами УАТС Hicom та NEAX можливе з'єднання через модем. Таким чином, одним із способів налаштування системи збору даних є розміщення спеціалізованого комп'ютера в центральному офісі та розробка програмного забезпечення, яке б послідовно опитувало комутатори через мережу та з'єднувалося б з системами через телефонну мережу за допомогою модему для завантаження тарифікаційної інформації. Схема такого підключення представлена на рис. 3.1. Виділений комп'ютер під'єднаний через інтерфейс RS-232 (com-порт) до системи у головному вузлі (вузол А) і до модему, через який відбувається з'єднання з модемами віддалених систем.

Комп'ютер також підключений до порту комутатора локальної мережі, що забезпечує зв'язок з іншими комутаторами. Структурна схема показана на рис. 3.2. Вся інформація збирається в бази даних (БД), розташовані на виділеному комп'ютері, де також можуть бути встановлені програми для обробки та відображення зібраної статистики.

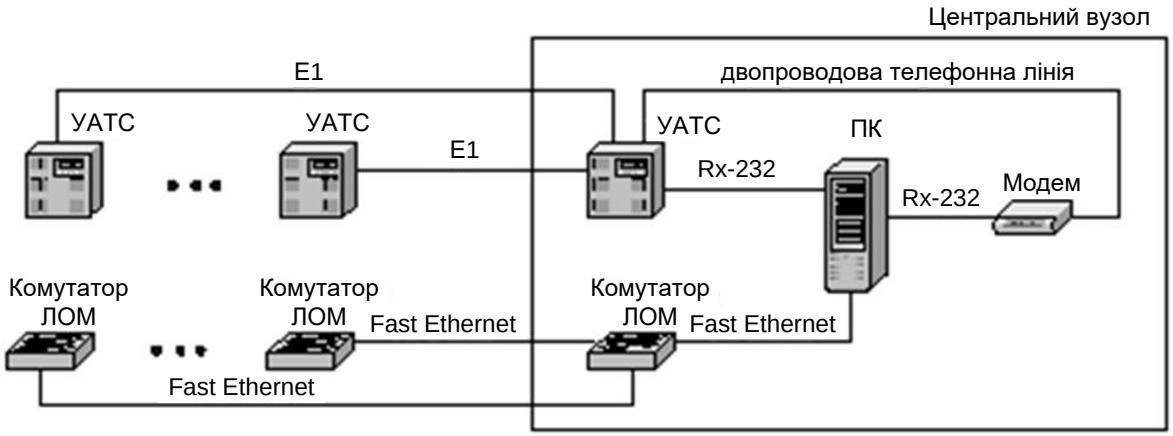

Рисунок 3.1 - Схема підключення розміщення спеціалізованого комп'ютера в центральному офісі, що використовує модем для завантаження тарифікаційної інформації

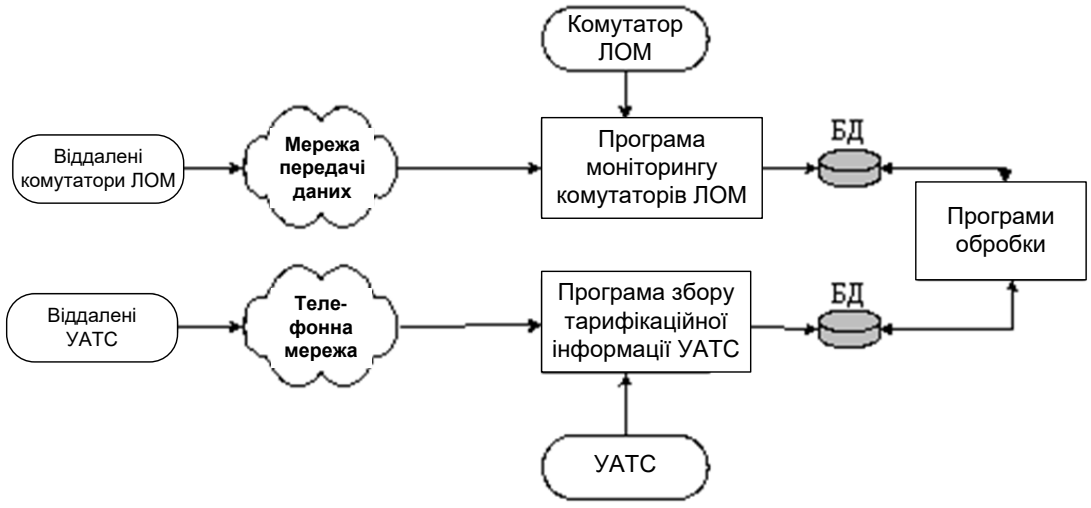

Рисунок 3.2 - Структурна схема корпоративної мережі з використанням модему

Такий підхід містить кілька значних мінусів. Основна проблема полягає в тому, що УАТС NEAX, розміщена на вузлі Е, обладнана лише одним портом

RS-232, через що періодичне з'єднання через модем, підключений до цього порту, ускладнює дистанційне управління станцією. Крім того, з'єднання через модем забезпечує низьку швидкість передачі даних і надійність, а також збільшує навантаження на E1 лінії, які з'єднують станції, при цьому навантаження на міжстанційні лінії в цій мережі є досить високим.

Одним із способів вирішення цих проблем може бути використання так званих серверів консолей - пристроїв, які дозволяють підключатися до консольних портів різноманітного обладнання через мережу передачі даних. Наприклад, компанія Digi Internation пропонує широкий асортимент обладнання для дистанційного доступу до консольних інтерфейсів різних пристроїв. Для наших потреб міг би підійти девайс-сервер Digi One TS (ціна близько 400 доларів США), який оснащений одним інтерфейсом RS-232 та одним інтерфейсом 100BaseT. Завдяки цьому пристрою, управління та збір даних для тарифікації відбувається через мережу передачі даних, що значно прискорює обидва процеси. Додатково, це забезпечує високий рівень безпеки при підключенні до станцій завдяки захисту доступу до сервера консолей за допомогою пароля.

Схема підключення, що використовує сервери консолей, представлена на рис. 3.3, а структурна схема – на рис. 3.4.

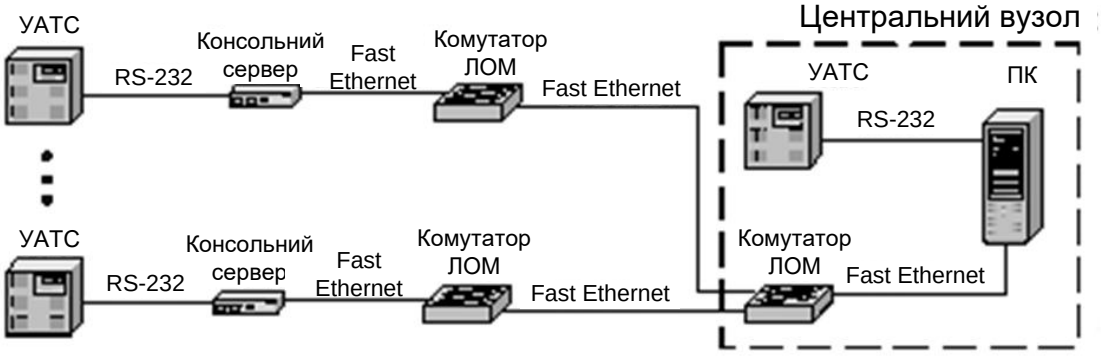

Рисунок 3.3 - Схема підключення розміщення спеціалізованого комп'ютера в центральному офісі, що використовує сервери консолей для завантаження тарифікаційної інформації

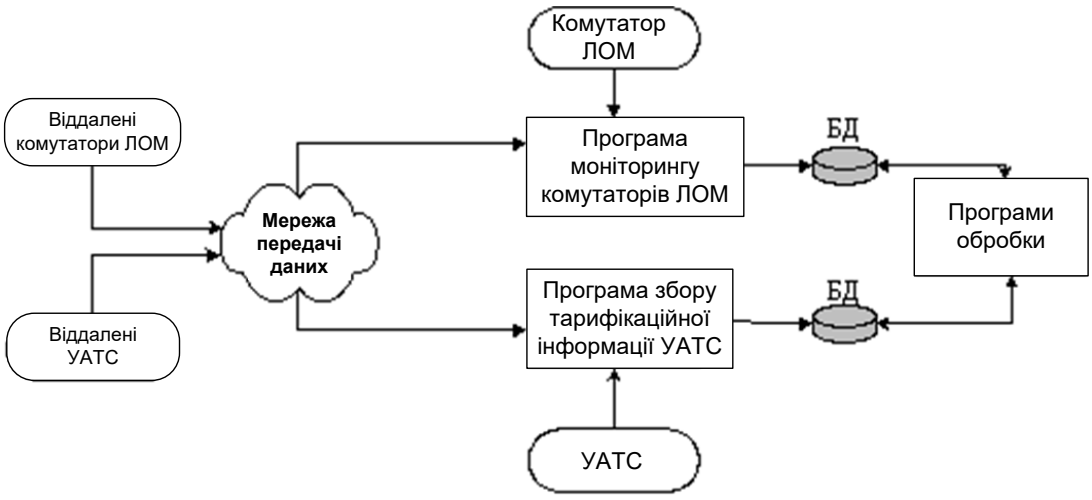

Рисунок 3.4 - Структурна схема корпоративної мережі з використанням серверів консолей

Централізоване рішення з використанням одного комп'ютера є високоефективним з точки зору надійності. Однак, при передачі моніторингових даних через мережу, існує ризик втрати інформації через помилки або перерви у лініях зв'язку. У разі поломки центрального комп'ютера, дані, зібрані під час його несправності, будуть незворотно втрачені.

Застосування окремого персонального комп'ютера для кожного вузла значно підвищує загальну надійність системи.

На рис. 3.5 представлено схему підключення обладнання, де в кожному вузлі використовується окремий комп'ютер. Важливо зазначити, що в усіх вузлах комутатори ЛОМ мають незайняті інтерфейси, що дозволяє додавати нові пристрої до мережі передачі даних.

Структурна схема цього рішення представлена на рис. 3.6. На кожному окремому ПК функціонують програми для моніторингу, які зберігають зібрані дані як у локальній, так і в центральній базі даних, розташованій на комп'ютері в центральному вузлі. Це забезпечує високий рівень надійності збереження інформації завдяки її копіюванню на різні носії. Доступ до локальних баз даних можливий віддалено, і після відновлення зв'язку можна завантажити дані, що були накопичені під час перебоїв у роботі.

У кваліфікаційній роботі було вирішено створити систему моніторингу з використанням окремих ПК у кожному вузлі.

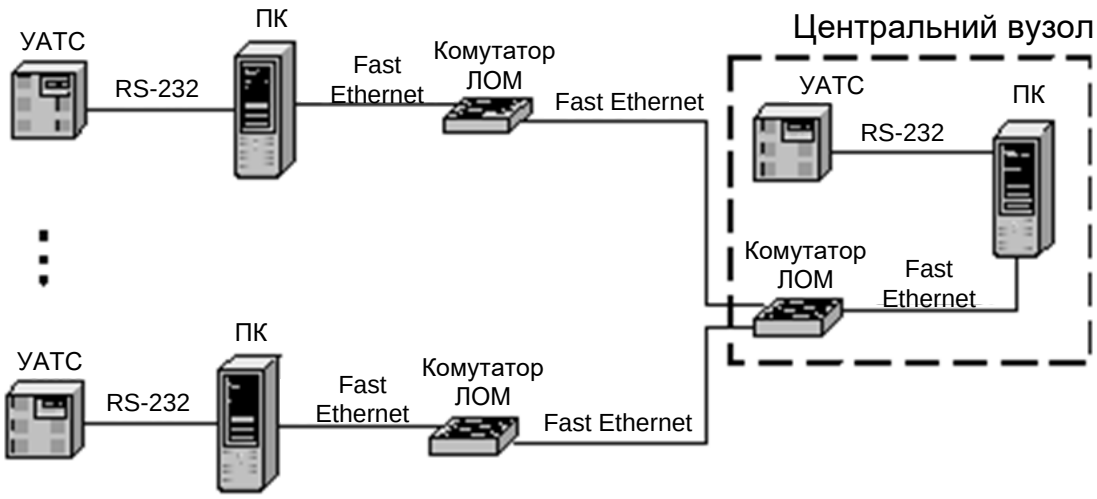

Рисунок 3.5 - Схема підключення розміщення спеціалізованих комп'ютерів у кожному вузлі

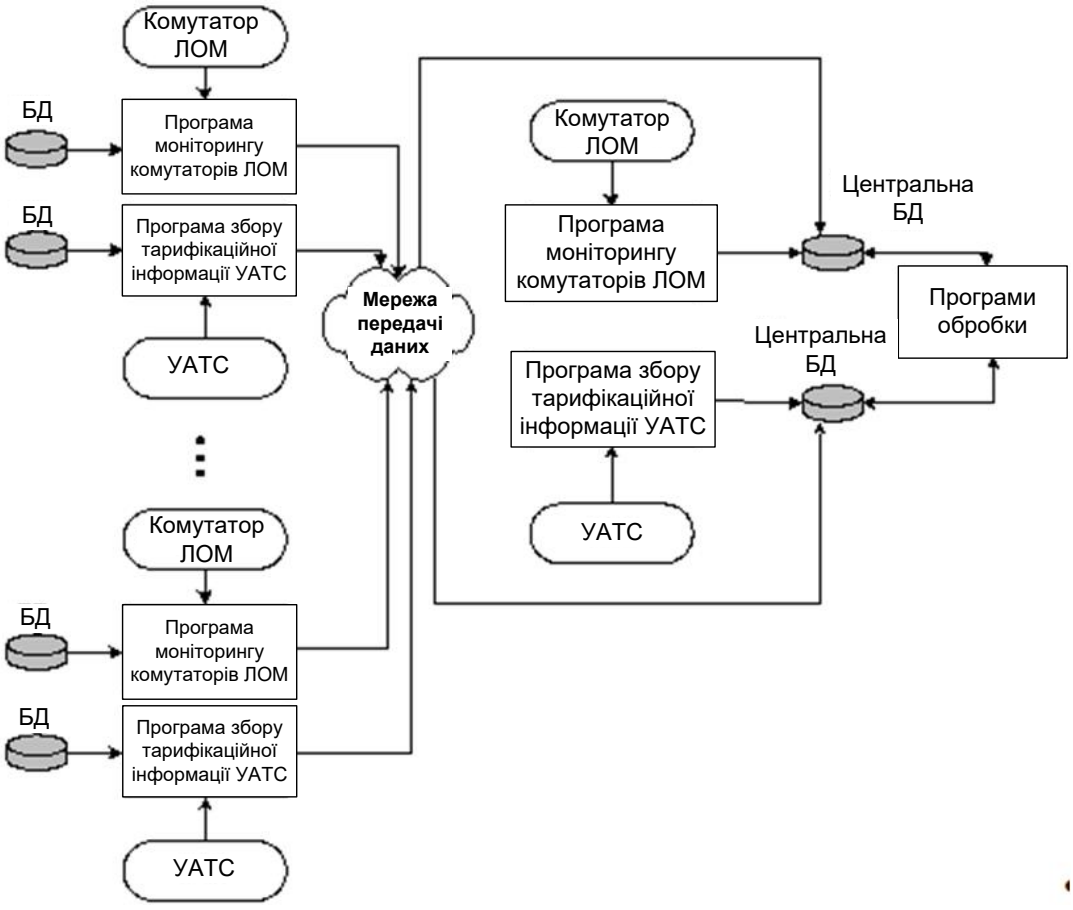

Рисунок 3.6 - Структурна схема корпоративної мережі з використанням окремих комп’ютерів для кожного вузла

3.4 Вибір обладнання та програмного забезпечення

Для обраної моделі системи спостереження, окрім основного обладнання, потрібні тільки настільні комп'ютери. У випадку завдань, які ставляться перед апаратною частиною, вимоги до комп'ютерних ресурсів є невеликими. Наприклад, можна взяти до уваги системні вимоги для існуючих програм тарифікації:

- процесор Intel Pentium з частотою не більше 300 МГц;
- не більше 64 Мбайт оперативної пам'яті;
- потреба у вільному місці на диску – не більше 1 Гбайта.

Враховуючи, що крім програми для збору тарифікаційної інформації будуть працювати програми для моніторингу комутаторів (вимоги до ресурсів яких майже ідентичні до вимог систем тарифікації), системні вимоги повинні бути вищими. Проте всі настільні комп'ютери, що пропонуються на сучасному ринку, значно перевищують вказані вимоги. Таким чином, для цього проекту можна використовувати будь-який домашній настільний комп'ютер. Обрана конфігурація наведена у таблиці 3.1.

Таблиця 3.1 – Необхідна конфігурація обладнання

Найменування	Кількість
Материнська плата INTEL 478 <i845GE> AGP+SVGA+Audio+Lan USB2.0	5
Процесор Intel Pentium-4 1800A/400MHz/512K	5
Оперативна пам’ять DDR DIMM 256 Mb SDRAM	10
Жорсткий диск Seagate Barracuda 80 Gb IDE	5
Мережева карта 10/100Base	5
Корпус ATX Miditower PL 818-1 для P4 без блоку живлення (340)	5
Блок живлення 340 W у корпус ATX Form factor, для P4	5

Відповідно до плану налаштування системи спостереження (рис. 3.5), обрані комп'ютери мають бути оснащені інтерфейсом RS-232 та мережевим адаптером 10/100BaseT для з'єднання з мережею передачі інформації. Не потрібно встановлювати консоль (екран та клавіатуру), оскільки ці комп'ютери

не будуть інтегровані з робочими станціями персоналу, а доступ до них буде забезпечено дистанційно. Вибір процесора Intel Pentium 4 зумовлений вимогами до надійності. Два модулі оперативної пам'яті по 256 Мбайт кожен необхідні для забезпечення достатнього обсягу оперативної пам'яті, щоб вона не стала обмеженням для продуктивності комп'ютера в разі додавання нових функцій у майбутньому.

У кожному вузлі мережі комутатори локальних мереж розміщені у спеціалізованих телекомунікаційних шафах. У вузлах B, C, D, E УАТС і шафи з комутаторами знаходяться в одному приміщенні. У вузлі A УАТС та шафа з комутатором розташовані в різних приміщеннях. Розміщення спеціалізованих комп'ютерів для моніторингу планується у шафах з комутаторами, за винятком вузла A, де комп'ютер буде встановлено в приміщенні з УАТС. Це пов'язано з обмеженням на максимальну довжину кабелю RS-232, який з'єднує станцію та комп'ютер, у 9 метрів.

Програмне забезпечення повинне включати:

– операційну систему;
– інтерпретатор мови Perl;
– систему управління базами даних (СУБД).

Мова Perl, яка підтримує інтерпретацію, вимагає наявності спеціального програмного забезпечення - інтерпретатора для запуску програм. Вибір на користь цієї мови зумовлений кількома аспектами:

- гнучкість мови, що робить її придатною для вирішення різноманітних задач;
- наявність доступних та компактних інтерпретаторів, а також висока швидкість обробки програм;
- великий вибір додаткових модулів (включаючи модулі для роботи з базами даних, SNMP протоколом та com-портами, що є критично важливим для цього проекту);
- ефективність обробки тексту, що необхідна для розробки програм збору тарифікаційної інформації та аналізу даних, отриманих від станції;
- присутність вбудованого інтерпретатора в усіх Linux та Unix системах.

Для збереження даних моніторингу потрібна база даних, оптимізована для зберігання текстових даних та їх швидкого додавання. Тому рекомендується використовувати MySQL. Ця СУБД володіє рядом переваг, важливих для специфічних завдань:

- розповсюджується безкоштовно, має хорошу підтримку;
- призначена для швидкого пошуку та додавання даних, що є критично важливим для оперативного запису інформації, отриманої від програм моніторингу;
- підтримує взаємодію з мовою програмування Perl;
- використовує клієнт-серверну архітектуру, дозволяючи підключення клієнтів через мережу TCP/IP, що необхідно для обробки статистичних даних;
- сумісна з різними операційними системами.

Отже, особливих вимог до операційної системи не висувається. Інтерпретатори Perl доступні для Windows систем, а СУБД MySQL може функціонувати в різних середовищах.

4 РОЗРОБКА ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ДЛЯ СИСТЕМИ МОНІТОРИНГУ

4.1 Розробка програми для моніторингу комутаторів мережі

Програма для моніторингу комутаторів мережі згідно з вимогами та вибраним у розділі 3 підходом має забезпечити:

- збір необхідних даних зі змінних MIB комутатора через протокол SNMP;
- запис зібраної інформації у дві бази даних - локальну, яка розміщена на ПК, що безпосередньо підключений до комутатора, та центральну, розташовану на ПК у центральному вузлі зв'язку;
- інформування адміністратора про зміни статусу інтерфейсів комутатора.

Перед початком розробки програми, що використовує протокол SNMP, потрібно налаштувати SNMP-агента на комутаторі. Для комутаторів Cisco Catalyst 2950 та Catalyst 3550 у простому випадку для активації SNMP-агента достатньо вказати ім'я спільноти. Імена для менеджера та агента при з'єднанні мають співпадати. Це забезпечує базовий механізм авторизації. Зазначені комутатори, як було відмічено в розділі 2, підтримують більш складні механізми безпеки. У конфігураційному файлі комутатора команда налаштування імені спільноти викладена наступним чином:

```
snmp - server community public RO
```

RO (Read-only) позначає, що доступ до цієї назви спільноти для конкретного агента обмежений лише читанням даних з MIB змінних. Вибір рівня RO зумовлений цим, у даній ситуації роль менеджера буде здійснювати програма, що розробляється.

```
($session, $error) = Net::SNMP->session(
-hostname => shift | '192.168.0.10',
-community => shift || 'public',
```

-port => shift | 161);

Отже, потрібно вказати IP адресу агента, назву спільноти та номер порту.

Для збору необхідної інформації важливо знати назви змінних MIB, де зберігаються потрібні дані. Назви змінних залежно від потрібних параметрів, встановлених завданнями та обраним рішенням, можна відшукати на вебсайті виробника обладнання www.cisco.com. Змінні, що будуть застосовуватися у програмі, представлені як:

– $AmountPort = '.1.3.6.1.2.1.2.1.0' - кількість інтерфейсів;

– $AverageCPULoad = '.1.3.6.1.4.1.9.2.1.58.0' - завантаження центрального процесора;

– $ FreeMemory = '.1.3.6.1.4.1.9.2.1.8.0' - обсяг вільної пам'яті;

– $Uptime = '.1.3.6.1.2.1.1.3.0' – час напрацювання на відмову;

– $DescrPort = ".1.3.6.1.2.1.2.2.1.2.$i" - опис інтерфейсу і;

– $SpeedPort = ".1.3.6.1.2.1.2.2.1.5.$i" - швидкість інтерфейсу;

– $OperPort = ".1.3.6.1.2.1.2.2.1.8.$i" - оперативний стан інтерфейсу;

– $AdminPort = ".1.3.6.1.2.1.2.2.1.7.$i" - адміністративний стан інтерфейсу;

– $InOctets = ".1.3.6.1.2.1.2.2.1.10.$i" - кількість вхідних байт (через інтерфейс);

– $OutOctets = ".1.3.6.1.2.1.2.2.1.16.$i" - кількість вихідних байт;

– $ifInErrors = ".1.3.6.1.2.1.2.2.1.14.$i"- кількість вхідних байт з помилками;

– $ifOutErrors = ".1.3.6.1.2.1.2.2.1.20.$i" - кількість вихідних байт з помилками.

Отримання значень змінних у програмі за допомогою засобів спеціального модуля буде виглядати наступним чином:

```
$ResultDescr = $session->get_request($DescrPort);
$ResultSpeed = $session->get_request($SpeedPort);
$ResultOper = $session->get_request($OperPort);
$ResultAdmin = $session->get_request($AdminPort);
$ResultInOctets = $session->get_request($InOctets);
$ResultOutOctets = $session->get_request($OutOctets);
```

```
$ResultInErrors = $session->get_request($ifInErrors);
$ResultOutErrors = $session->get_request($ifOutErrors);
```

Опитування всіх інтерфейсів одного комутатора буде відбуватися черех цикл.

Занесення даних повинно здійснюватися у бази даних. Для взаємодії з СУБД (системами управління базами даних) як MySQL, так і з іншими мовами програмування, наприклад Perl, розроблені спеціальні модулі. У розроблюваній програмі застосовується модуль DBI. Оскільки всі обговорені модулі сумісні з різними операційними системами, їх можна використовувати разом з вбудованим інтерпретатором Linux.

Для підключення до бази даних за допомогою інструментів модуля DBI можна скористатися наступною інструкцією:

```
$dbi_user = 'root';
$dbi_password = '';
$dbi_database = 'Sw_01';
$dbi_host = 'localhost';
$dbi_host2 = '192.168.0.1';
$dbi_dsn = "DBI:mysql:database=$dbi_database;host=$dbi_host";
$dbi_dsn2 = "DBI:mysql:database=$dbi_database;host=$dbi_host2";
$dbh = DBI->connect($dbi_dsn, $dbi_user, $dbi_password, {AutoCommit => 1, RaiseError => 1, PrintError => 1});
$dbh2 = DBI->connect($dbi_dsn2, $dbi_user, $dbi_password, { AutoCommit => 1, RaiseError => 1, PrintError => 1});
```

Отже, потрібно знати ім'я користувача, пароль, назву бази даних і адресу.

Для полегшення подальшого аналізу збирається статистика, і таблиці в базах даних структуровані таким чином, що вони містять інформацію лише за кожен окремий місяць. Водночас існують окремі таблиці для збереження основної інформації про комутатор і даних про інтерфейси. Щоб щомісяця автоматично формувалася нова таблиця, застосовуються інструменти Perl для встановлення поточної дати:

```
($month, $year) = (localtime) [4,5];
$table_name = sprintf (%02d%02d, $month + 1, $year + 1900);
```

Після чого перевіряється наявність у базі даних таблиці зі вказаним ім'ям. Якщо така таблиця відсутня – необхідно її створити:

```
# Виконання запиту SQL з поверненням до програми результатів
$sth = $dbh->prepare("show tables from $dbi_database like 'g$table_name';");
$sth->execute() or die $dbh->errstr;
$ex = $sth->fetchrow_array();
if($ex ne "g$table_name")
# Виконання запиту SQL без повернення до програми результатів
{$ dbh -> do ($ sql _ create _ gtable );
$sth->execute() or die $dbh->errstr;};
```

Запит SQL (Structured Query Language – мова структурованих запитів) створення таблиці для зберігання інформації про комутаторах виглядає так [4]:

```
($sql_create_gtable) = "CREATE TABLE g$table_name (
sID INT(10) UNSIGNED DEFAULT '0' NOT NULL AUTO_INCREMENT,
sDateTime INT(11) UNSIGNED,
sAmount SMALLINT(3) UNSIGNED,
sACPU SMALLINT(3) UNSIGNED,
sFM INT(11) UNSIGNED,
sUptime TEXT,
PRIMARY KEY (sID));";
```

Запит на створення таблиці даних про комутатор описується як:

```
($sql_create_iftable) = "CREATE TABLE if$table_name (
sID INT(10) UNSIGNED DEFAULT '0' NOT NULL AUTO_INCREMENT,
sDateTime INT(11) UNSIGNED,
sDescr TEXT,
sSpeedPort INT(10) UNSIGNED,
```

```
sInOct INT(10) UNSIGNED,
sOutOct INT(10) UNSIGNED,
sOperPort TINYINT(1) UNSIGNED,
sAdminPort TINYINT(1) UNSIGNED,
sInErrors INT(6) UNSIGNED,
sOutErrors INT(6) UNSIGNED,
PRIMARY KEY (sID));";
```

Для встановлення будь-яких змін у статусі інтерфейсу, програма зберігає попередні стани інтерфейсів у файлі state.old. В ході і-го циклу програми з цього файлу витягується відповідне значення та порівнюється із поточним станом. У випадку виявлення неспівпадінь між цими значеннями ініціюється запуск стандартної програми для відправлення електронних листів через Linux Sendmail, і відправляється лист адміністратору.

```
$state_c = $ResultOper->{$OperPort};
$state_o = substr($previous, $i, 1);
$current. = $state_c;
if($state_c ne $state_o)
{open (SENDMAIL, "|/usr/sbin/sendmail-oi-t-odq");
print (SENDMAIL "To: 79022270899@sms.dti.ua Subject: SNMP Alert! Interface $ResultDescr of Sw_01 змінений статус. EOF");
close (SENDMAIL);}
```

Повністю текст цієї програми можна знайти у додатку А. Запуск цієї програми планується кожні десять хвилин . Для цього застосовується планувальник задач для Linux – Cron. Cron – це додаток, що дозволяє виконувати задачі за певним розкладом, забезпечуючи їхній періодичний запуск. Тобто, задачу можна налаштувати на виконання у визначений час або через задані інтервали. Цей додаток завантажується в момент запуску операційної системи і працює на постійній основі, як процес, що кожну хвилину перевіряє налаштування у файлі crontab. Кожен запис у файлі crontab користувача представляє собою один рядок, що містить шість полів. Основний формат запису: хвилина година день_місяця місяць день_тижня команда

Допустимі значення записів:

– хвилина – від 0 до 59;

– година – від 0 до 23;

– день місяця - від 1 до 31;

– місяць - від 1 до 12 (можна використовувати три перші літери з назви місяця, регістр немає значення від jan до dec);

– день тижня - від 0 до 6 (починається з неділі, яка записується як 0 і т.д., можна писати від sun до sat).

Кожен з елементів, що відображають дату та час, може містити символ *, який буде означати будь-яке можливе значення. У цих елементах допускається використання діапазонів значень, які відділяються між собою дефісом. Для ситуації (запуск програми кожні десять хвилин) використання команди в файлі налаштувань crontab може бути представлене наступним чином:

0-59/10 * * * * "шлях до програми"

4.2 Розробка програми для збору тарифної інформації з УАТС

УАТС надають інформацію для тарифікації через порт RS-232 (com-порт), і залежно від обраного методу організації системи моніторингу, програмне забезпечення для збору тарифікаційної інформації має бути запущене на ПК, який безпосередньо підключений до com-порту станції. Для цієї мети для інтерпретатора мови Perl доступні спеціальні модулі, що надають можливості для взаємодії з com-портом. У рамках дипломного проекту було використано модуль Device:SerialPort, розроблений для використання в операційній системі Linux.

Окрім того, інформація про тарифи, зібрана через порт, повинна бути занесена до двох баз даних – локальної (ЛБД) та центральної (ЦБД). Спосіб взаємодії з СУБД MySQL у цьому застосунку аналогічний до того, що використовується у програмі для моніторингу комутаторів. Це означає, що використовується модуль DBI, і дані одночасно записуються у дві бази даних, для яких щомісяця створюються нові таблиці.

Встановлення з'єднання з com-портом у програмі організовано як:

```
$port = '/dev/ttys0';
$ob = Device::SerialPort->new ($port);}
die "Can't open serial port $port: $^E\n" unless ($ob);
```

Параметри com-порту засобами модуля Device::SerialPort налаштовуються наступним чином:

```
$ob->baudrate(38400); # Швидкість передачі через порт
$ob->parity("none"); # Наявність біта парності
$ob->databits(8); # Біти даних
$ob->stopbits(1); # Кількість стопових біт
$ob->handshake('none'); # Управління потоком
$ob->write_settings; # Застосування налаштувань
```

Щоб прочитати один байт інформації з порту використаємо команду:

```
($count, $active) = $ob->read(1);
```

Для розуміння інформації, що надходить від станції, необхідно знати її формат. Для тарифікації достатньо буде наступної інформації:

– номер абонента;
– час початку розмови;
– тривалість розмови.

Формат даних для станції Hicom представлено на рис. 4.1, а для станції NEAX – на рис. 4.2.

Рисунок 4.1 – Формат тарифікаційних даних для Hicom

Рисунок 4.2 – Формат тарифікаційних даних для NEAX

Різноманітні станції потребують унікальних програм для збору даних, які були б адаптовані під специфіку тарифікаційної інформації. Хоча загальна схема алгоритму для будь-яких двох програм залишається незмінною, різниця полягає у блоку "Розбір рядка за шаблоном". Процес читання з порту відбувається символ за символом до моменту формування повного рядка в спеціальній змінній, далі відбувається аналіз рядка за допомогою регулярних виразів та текстових операторів. Регулярний вираз представляє собою шаблон, створений з використанням спеціальних символів, який встановлює правила для виокремлення сегментів тексту. Підтримка таких регулярних виразів ефективно реалізована в Perl.

Процес читання даних з порту у програмі реалізовано через цикл, де відбувається перевірка на наявність інформації. Існує функція тайм-ауту. У випадку, коли дані на com-порту не з'являються протягом встановленого часу, програма припиняє свою роботу. Повторний запуск програми здійснюється згідно з налаштуваннями у файлі конфігурації планувальника Cron через 10 хвилин. Якщо протягом цього часу з'являються дані про дзвінки, вони будуть збережені у тимчасовому буфері станції до моменту їх обробки програмою. Цей буфер використовується для обох видів станцій.

Повний текст програми для збору тарифікаційної інформації зі станції Hicom наведено у додатку Б, а зі станції NEAX – у додатку В.

4.3 Розробка програми обробки статистичних даних

Зібрані зі станції тарифікаційні відомості важливі не лише для формування рахунків для користувачів, а й слугують статистичною базою, що дозволяє аналізувати рівень завантаження обладнання та комунікаційних каналів. Такий аналіз статистики завантаження мережевих вузлів є ключовим.

Щоб краще уявити інформацію про завантаженість мережі, потрібно використовувати графічне зображення. Для створення різноманітних графіків у Perl можна застосувати модуль GD::Graph::lines.

Створення графіка описуємо наступним чином:

my $mygraph=GD::Graph::lines->new(1000,500); графік розміром 1000 на 500 точок

```
$mygraph->set(
x_label =>'Time', # Опис осі x
y_label =>'Count', # Опис осі y
title =>'800') or warn $mygraph->error;
```

Саме малювання графіка відбувається на основі даних, що розташовані у двовимірному масиві. У нашому випадку це масив @data.

```
my $ myimage = $ mygraph -> plot (\ @data ) or die $ mygraph -> error ;
```

Заповнення масиву даних відбувається за допомогою вказівок на період часу та кількість телефонних дзвінків у визначеному напрямку протягом обраного періоду. Результати візуалізуються у вигляді графіка, який зберігається у форматі png.

Програма дозволяє налаштувати дні для аналізу навантаження, вибрати номер напряму, встановити точність графіка (часовий інтервал) та максимально допустиме навантаження. Час поділяється на інтервали. З бази даних, що містить всю інформацію, вибираються записи, які стосуються обраного дня та напрямку. Далі, в циклі розраховується кількість дзвінків за кожен часовий інтервал, які стають точками для побудови графіка. Приклади графіків представлені на рис. 4.3.

Програма не призначена для безперервної роботи і запускається на комп'ютері адміністратора. Під час роботи програми також можливе отримання попереджувального повідомлення, якщо кількість дзвінків перевищить встановлене максимальне навантаження.

Повний текст програми наведено у додатку Г.

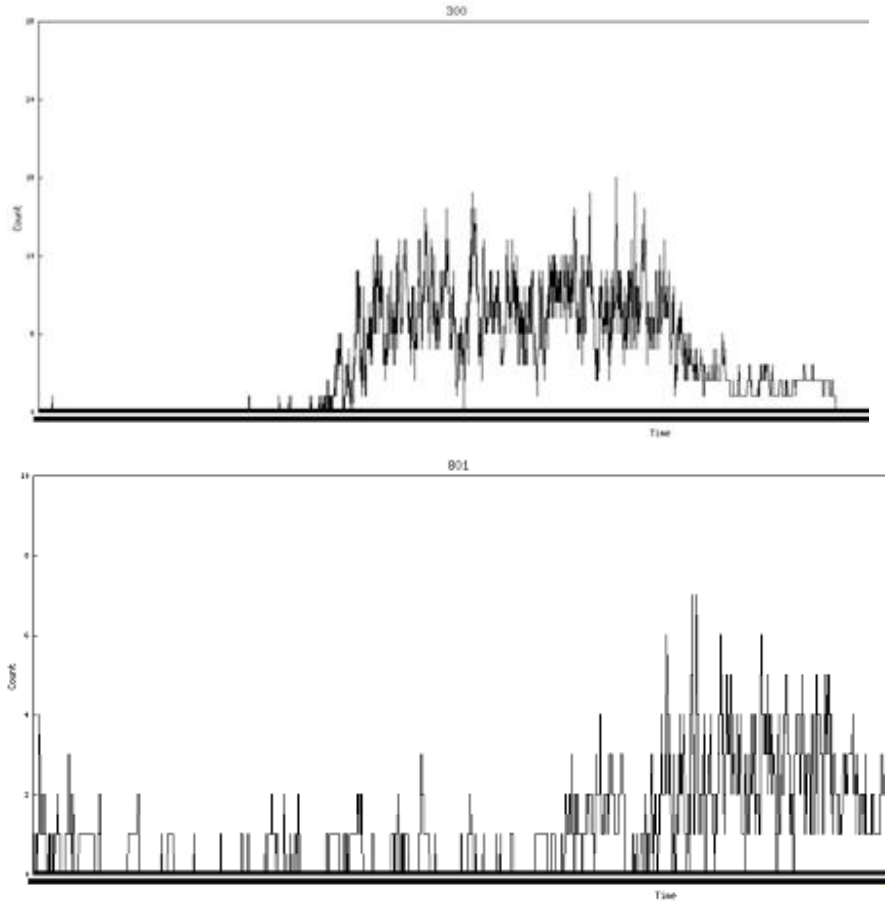

Рисунок 4.3 – Графічне подання результатів моніторингу створеної програми по параметру завантаженості мережі

5 ВИМОГИ ДО ЯКОСТІ СИСТЕМИ МОНІТОРИНГУ

Дані, зібрані в процесі функціонування системи моніторингу, транслюються через мережу передачі даних до центрального вузла. В результаті, структуровану систему моніторингу можна класифікувати як службу передачі даних (ПД) з пакетною комутацією на основі протоколів сімейства Internet Protocol (IP).

Відповідно до Нормативного документа 45.0128-2000 "Мережі та служби передачі даних", для служб ПД на базі протоколів IP встановлені наступні вимоги:

- служба ПД, що використовує пакетну комутацію на основі протоколів, які входять до сімейства Internet Protocol (IP), функціонує як служба без створення віртуальних з'єднань (датаграмна служба);
- основною функцією має бути здатність кінцевого обладнання даних (КОД) відправляти та отримувати IP протокольні пакети (датаграми). При цьому можливі випадки втрати пакетів та зміни в порядку їх передачі, встановленого під час відправлення;
- у точці доступу до служби ПД оператора режим роботи має відповідати документу IETF RFC 791 при використанні версії 4 протоколу IP (IPv4) або документу RFC 2460 або їх наступникам при використанні версії 6 протоколу IP (IPv6);
- доступ до КОД може бути як прямим, так і непрямим. Непрямий доступ можливий через мережу ТМЗК та інші комутовані мережі;
- можливе надання додаткових необов'язкових послуг, таких як пріоритет пакетів, аутентифікація відправника.

Критерії якості обслуговування в службах ПД з пакетною комутацією на основі протоколів, що входять до сімейства Internet Protocol (IP).

В мережах на базі протоколу IP якість обслуговування не гарантується (послуги надаються з негарантованою якістю обслуговування). В даний час розробляються та впроваджуються методи забезпечення якості обслуговування. Показники якості обслуговування в мережах за протоколом IP згідно з Рекомендацією МСЕ-Т I.380 представлено в таблиці 5.1.

Норми цих показників якості обслуговування нині вивчаються.

Попередньо (Рекомендації МСЕ-Т Y.1541) встановлюються класи обслуговування, наведені у таблиці 5.2. Крім того, рекомендуються наступні норми для всіх класів обслуговування, крім "прийнятного":

– час доступу: трохи більше 5 з;
– коефіцієнт втрати IP-пакетів: трохи більше 1x10-3;
– коефіцієнт помилок у IP-пакетах: не більше 1x10-4;
– коефіцієнт помилок у IP-пакетах: не більше 1x10-4;
– критерій відмови: відмовою вважається ситуація, коли коефіцієнт втрати IP-пакетів перевищує 0,75 [6].

Таблиця 5.1 – Показники якості обслуговування

Функція служби передачі даних	Показники для критеріїв оцінки		
	Швидкість	Правильність	Визначеність
Доступ	**Час доступу**		
Надсилання повідомлень користувача	Час перенесення IP-пакету Варіація часу перенесення IP-пакету Пропускна здатність для IP-пакетів	Коефіцієнт помилок в IP-пакетах Інтенсивність появи помилкових IP-пакетів	Коефіцієнт втрати IP-пакетів
Визволення	Час визволення		
Критерій відмови Коефіцієнт готовності служби Середній час між відмовами служби			

Зазначені стандарти представлені для забезпечення зв'язку між крайніми точками в IP-мережі, яка побудована згідно з архітектурною моделлю, описаною в Рекомендації МСЕ-Т Y.1231. Якість сервісу в мережах окремих провайдерів повинна відповідати або перевищувати рівень, вказаний у таблиці 5.2.

Стандарти інших критеріїв якості сервісу мають бути розроблені додатково.

Вибір категорій сервісу, які будуть імплементовані в певній IP-мережі, відбувається за рішенням оператора, що управляє даною мережею.

При створенні нашої системи моніторингу виходимо з стандартів, які відповідають класу сервісу "прийнятний".

Таблиця 5.2 – Попередньо рекомендовані норми для класів обслуговування

Клас обслуговування в службі ПД з IP	Норми для міжнародного зв'язку	
	Час перенесення IP-пакету	Варіація часу перенесення IP-пакету
Прийнятний (з негарантованою якістю обслуговування)	Норми не встановлюються	
Середній	Не більше 1 с	Не більше 1 с
Високий	Не більше 400 мс	Не більше 50 мс
Вищий	Не більше 150 мс	Не більше 50 мс

ВИСНОВКИ

У кваліфікаційній роботі було розроблено систему моніторингу мережі для внутрішніх потреб підприємства АТ "Сумиобленерго". Ця система побудована на основі різноманітних автономних програм, які безперервно збирають дані про стан техніки та інформацію про телефонні дзвінки між основними станціями. Зібрані дані слугують фундаментом для передбачення майбутнього розвитку корпоративної мережі. Реалізація цієї системи також сприяє підвищенню якості зв'язку та зменшенню часу простою у разі збоїв у зв'язку.

Програма була орієнтована та випробувана для використання з певним обладнанням.

Було також запропоновано оптимізований варіант технічного вирішення системи моніторингу, що покращить її роботу та полегшить можливу модернізацію мережі.

Далі розвиток системи моніторингу передбачає введення програм для аналізу статистичних даних, на основі яких можна буде зробити висновки щодо потреби у розвитку мережі. Впровадження системи моніторингу також має бути реалізовано на інших об'єктах корпоративної мережі.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Kenneth C., Donahoo M. TCP/IP Sockets in C: Practical Guide for Programmers - Elsevier, 2009.
2. RFC 1157. Simple Network Managenent Protocol (SNMP).
3. Аткінсон Л. Бібліотека фахівця: MySQL. - К.: Вільямс, 2002.
4. Alkin Tezuysal MySQL Cookbook: Solutions for Database Developers and Administrators – O`Rielly Media, 2022, 850p.
5. Клинтон П. Освой самостоятельно Perl за 24 часа. – К.:Вильямс, 2000.
6. Кристиансен Т., Торкингтон Н. Perl: библиотека программиста. – СПб.: Питер, 2004.
7. Основи Perl. Синтаксис [Електронний ресурс] – URL: https://docstore.mik.ua/perl/syntax.htm (час звернення: 10.05.2025)
8. Дуглас Мауро, Кевін Шмід Основи SNMP 2-е видання. – Символ-Плюс, 2017, 516 с.