Вінницький національний технічний університет
Факультет інформаційних електронних систем
Кафедра інфокомунікаційних систем і технологій

МАГІСТЕРСЬКА КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Методи та засоби аналізу та обробки метрик телекомунікаційної мережі»

Виконав: студент 2-го курсу,
групи ТКС-22м
спеціальності 172 – Телекомунікації та радіотехніка
_____ Ремінський О.В.

Керівник: к.т.н., доцент каф. ІКСТ
_____ Онищук О.В.
«15» 12 2023 р.

Опонент: (к.т.н., доц. каф. ІРТС
_____ Осадчук Я.О.
«15» 12 2023 р.

Допущено до захисту
Завідувач кафедри ІКСТ
_____ д.т.н., проф. Кичак В.М.
«18» 12 2023 р.

Вінниця ВНТУ – 2023 рік

Вінницький національний технічний університет
Факультет інформаційних електронних систем
Кафедра інфокомунікаційних систем і технологій
Рівень вищої освіти ІІ-й (магістерський)
Галузь знань - 17– Електроніка та телекомунікації
(шифр і назва)
Спеціальність - 172 – Телекомунікації та радіотехніка
(шифр і назва)
Освітньо-професійна програма - Телекомунікаційні системи та мережі

ЗАТВЕРДЖУЮ
Завідувач кафедри ІКСТ
д.т.н., професор В.М. Кичак
"19" 09 2023 року

З А В Д А Н Н Я
НА МАГІСТЕРСЬКУ КВАЛІФІКАЦІЙНУ РОБОТУ СТУДЕНТУ

Ремінському Олександру Васильовичу .
(прізвище, ім'я, по батькові)

1. Тема роботи Методи та засоби аналізу та обробки метрик телекомунікаційної мережі

керівник роботи Онищук, Олег Володимирович канд. техн. наук, доцент
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)
затверджені наказом вищого навчального закладу від "18" 09 2023 року № 247
2. Строк подання студентом роботи 08 грудня 2023 року

3. Вихідні дані до роботи 1. Швидкість передавання даних 10 Гбіт/с; передавання даних у датацентрах - 0,1 мс; доступність та надійність мережі – 99 %. Необхідно розробити методи обробки метрик з урахуванням параметрів передавання даних.

4. Зміст текстової частини: Теоретичні основи організації моніторингу сучасних телекомунікаційних мереж. Засоби збору та обробки метрик з урахуванням параметрів мережі передавання даних. Алгоритми обробки метрик з описом функцій на мові Python.

5. Перелік ілюстративного матеріалу (з точним зазначенням обов'язкових креслень) презентація у вигляді слайдів. Схема взаємодії інфраструктури мережі, модулів, структура програмного коду. Алгоритм моніторингу навантаження на канал збору. Узагальнений алгоритм роботи маршрутизації та модуля керування.

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Спеціальна частина	Онищук О.В., доцент кафедри ІКСТ	04.09.23	15.12.23
Економічна частина	**Кавецький В.В Доцент каф. ЕПВМ**	04.09.23	15.12.23
Охорона праці та безпеки в надзвичайних ситуаціях	**Дембіцька С.В Професор кафедри БЖДПБ**	7.09.23	15.12.23

7. Дата видачі завдання 01 вересня 2023 року

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів магістерської кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1.	Розробка технічного завдання	08.09.2023р.	
2.	Техніко-економічне обґрунтування розробки	17.09.2023р.	
3.	Аналіз методів і засобів кодування сигналів	06.10.2023р.	
4.	Розробка структури та принципової схеми кодера	27.10.2023р.	
5.	Дослідження параметрів і характеристик кодера	10.11.2023р.	
6.	Аналіз економічної ефективності розробки	17.11.2023р.	
7.	Охорона праці та безпека життєдіяльності	24.11.2023р.	
8.	Оформлення пояснювальної записки та ілюстративної частини	01.12.2023р.	
9.	Нормоконтроль МКР	04.12.2023р.	
10.	Попередній захист МКР, опонування МКР	08.12.2023р.	
11.	Захист МКР ЕК	11.12.2023р.	

Студент (підпис) Ремінський О.В.

Керівник роботи (підпис) Онищук О.В.

АНОТАЦІЯ

Робота містить 69 сторінок, 13 рисунків, 2 таблиці. Було використано 16 джерела українською.

Дипломна робота присвячена вивченню методів та засобів аналізу та обробки метрик телекомунікаційної мережі. Робота є актуальною, оскільки телекомунікаційні мережі стають все важливішою складовою інфраструктури, і ефективний аналіз метрик є ключовим для забезпечення їхньої надійності та продуктивності.

У роботі детально розглядається вибір та використання різних методів збору метрик, зокрема використання SNMP, REST API та інших протоколів. Досліджуються нові методи обробки метрик з метою вдосконалення аналізу та моніторингу мережевих показників. Експериментальний підхід дозволяє оцінити продуктивність та ефективність розробленого програмного забезпечення для аналізу та обробки метрик.

У розділах розглядається організація та проведення експериментів, включаючи вибір мережевих пристроїв, запуск системи збору метрик та встановлення параметрів експериментів. Описуються методи та засоби для збору метрик з реальних телекомунікаційних пристроїв.

Загальні висновки роботи підкреслюють важливість використання розроблених методів та засобів для покращення якості мережевого аналізу. Робота вносить вагомий внесок у розвиток області та може слугувати основою для подальших досліджень у цьому напрямку.

Ключові слова: телекомунікаційна мережа, метрики, аналіз, обробка, SNMP, REST API, експерименти, продуктивність, ефективність.

ABSTRACT

The thesis comprises 69 pages, 13 figures, and 2 tables. Sixteen Ukrainian sources were used in the research.

The thesis is dedicated to exploring methods and tools for the analysis and processing of metrics in a telecommunications network. The work is relevant as telecommunications networks become an increasingly essential component of infrastructure, and effective metric analysis is crucial for ensuring their reliability and performance.

The thesis extensively discusses the selection and utilization of various metric collection methods, including the use of SNMP, REST API, and other protocols. New methods for metric processing are investigated to enhance the analysis and monitoring of network indicators. An experimental approach allows for the evaluation of the performance and efficiency of the developed software for metric analysis and processing.

Sections of the thesis cover the organization and implementation of experiments, including the selection of network devices, the initiation of metric collection systems, and the configuration of experiment parameters. Methods and tools for collecting metrics from real telecommunications devices are described.

The general conclusions of the thesis underscore the importance of utilizing the developed methods and tools to improve the quality of network analysis. The work makes a significant contribution to the field and may serve as a foundation for further research in this direction.

Keywords: telecommunications network, metrics, analysis, processing, SNMP

Зміст

ПЕРЕЛІК СКОРОЧЕНЬ

LLD - низькорівневе виявлення

API - прикладний програмний інтерфейс

IPS - одиниця виміру швидкості

IDS - системи керування базами даних

WLAN - бездротова локальна мережа

LAN - локальна мережа

VPN - віртуальна приватна мережа

WAN - телекомунікаційна мережа, яка охоплює велику територію

OSI - базова модель відкритих систем

Network Management - системи управління мережею

System Management - засоби управління системою

Embedded systems - вбудовані системи діагностики та управління

Protocol analyzers - аналізатори протоколів

IANA (Internet Assigned Numbers Authority) - розподілу номерів в

ІнтернетіUser-based Security Model - модель безпеки на основі користувачів

DM - розподілений моніторинг на основі вузлів

ВСТУП

Розкриття та оптимізація ефективності телекомунікаційних мереж в сучасних умовах є актуальною проблемою, оскільки вона прямо впливає на якість обслуговування, забезпечення безпеки та загальну продуктивність інформаційно-комунікаційної інфраструктури. Основним завданням є вдосконалення методів та засобів аналізу та обробки метрик телекомунікаційної мережі для підвищення її надійності та ефективності.

Актуальність теми. Актуальність теми дипломної роботи "Методи та засоби аналізу та обробки метрик телекомунікаційної мережі" зумовлена тим, що телекомунікаційні мережі є критично інфраструктурою та важливим елементом для забезпечення зв'язку та обміну даними у сучасному світі. Динамічний розвиток технологій та постійне зростання об'єму трафіку в мережах вимагають ефективних методів моніторингу, аналізу та оптимізації їхньої продуктивності та надійності.

Аналіз останніх досліджень. Останні дослідження в галузі моніторингу мереж вказують на необхідність розширення методів аналізу метрик з метою надання глибшого розуміння причин виникнення проблем, швидкості реакції на аварні ситуаціїї, а також забезпечення шляхів оптимізації мереж в цілому. Підвищення складності мереж та об'ємів трафіку зумовлюють необхідність у нових технологіях та інструментах для їх аналізу та моніторингу .

Мета і завдання роботи. Метою даної кваліфікаційної роботи є розробка нових та вдосконалення існуючих методів та засобів аналізу та обробки метрик телекомунікаційної мережі, що дасть можливість підвищити її продуктивності та надійності.

Задачами магістерської кваліфікаційної роботи є:

1. Аналіз існуючих методів моніторингу та аналізу метрик.

Провести огляд сучасних підходів щодо збору та аналізу метрик телекомунікаційних мереж для ідентифікації їхніх переваг та недоліків.

2. Синтез нових методів обробки та інтерпретації отриманих даних.

Розробити нові методи аналізу, які дозволять ефективно опрацьовувати та інтерпретувати різноманітні метрики телекомунікаційної мережі.

Об'єктом дослідження є телекомунікаційні мережі, які включають у себе різноманітні елементи і пристрої, такі як комутатори, маршрутизатори, сервери тощо.

Предметом дослідження є методи та засоби аналізу та обробки метрик, які вимірюють різні параметри функціонування мережі.

Методи досліджень. У роботі будуть використані такі методи дослідження, як математичне та комп'ютерне моделювання, експериментальні дослідження, статистичний аналіз та т. ін.

Новизна одержаних результатів. Розробка та впровадження нових методів та інструментів для аналізу метрик телекомунікаційних мереж, що дозволить покращити їхню продуктивність та стійкість.

*Апробація результатів магістерської кваліфікаційної роботи***.** Результати роботи апробовані на науково-практичних конференціях, а також заплановане їх впровадження на діючих мережах провайдерів та операторів телекомунікаційних послуг. Крім цього передбачені зустрічі та семінари з фахівцями у даній галузі щодо обговорень та обміном досвіду по даній проблематиці.

Таким чином, даний диплом вирішує актуальну проблему покращення та оптимізації телекомунікаційних мереж через розробку та застосування нових методів та інструментів аналізу та обробки телекомунікаційних метрик.

1. МОНІТОРИНГ УПРАВЛІННЯ ТЕЛЕКОМУНІКАЦІЙНОЇ МЕРЕЖІ

В даному розділі визначимо які бувають види та способи моніторингу телекомунікаційної мережі. Здійснимо їх класифікацію. Розглянемо особливості моніторингу мереж для IT-інфраструктури.

1.1 Огляд сучасних тенденцій у розвитку телекомунікаційних мереж

Сучасний світ характеризується стрімким розвитком технологій, що безперервно визначає нові вимоги до телекомунікаційних мереж. Розгляд сучасних тенденцій у їхньому розвитку визначає важливі напрямки для вдосконалення методів та засобів аналізу та обробки метрик. Спостерігається постійне зростання обсягу передавальної інформації через телекомунікаційні мережі. Велика кількість підключених пристроїв, а також нові служби та застосунки, такі як Інтернет речей (IoT), призводять до необхідності розвивати методи аналізу метрик, які забезпечують ефективне використання ресурсів та оптимізують роботу мережі. Висока якість обслуговування стає ключовим фактором у задоволенні потреб користувачів. Сучасні телекомунікаційні мережі повинні забезпечувати стабільність, низьку затримку та високу пропускну здатність. Тому, вдосконалення методів аналізу метрик, пов'язаних з QoS, визначається як одна з основних задач. Запровадження технологій 5G та перехід до мереж майбутнього (Next Generation Networks, NGN) вносять суттєві зміни у структуру та характеристики телекомунікаційних мереж. Методи та засоби аналізу метрик повинні адаптуватися до нових вимог, що включають високу швидкість передачі даних, низьку затримку та масову підтримку підключених пристроїв. Однією з ключових тенденцій у розвитку телекомунікацій є посилення вимог до безпеки мереж. Актуальність аналізу метрик, пов'язаних з виявленням аномальної активності та захистом від кіберзагроз, надто висока в умовах зростання кількості кібератак та кіберзлочинності. Штучний

інтелект та машинне навчання стають все більш важливими для вдосконалення аналізу та обробки метрик. Впровадження інтелектуальних систем допомагає виявляти патерни, робити прогнози та вчасно реагувати на зміни в мережі. Забезпечення сталості та енергоефективності телекомунікаційних мереж є важливими аспектами їхнього розвитку. Аналіз метрик, пов'язаних з використанням енергії та оптимізацією ресурсів, є необхідним для створення ефективних мереж. Сучасні телекомунікаційні мережі стають все більш складними, що вимагає нових методів автоматизації та управління. Аналіз метрик, пов'язаних з автоматизованими процесами та управлінням, є ключовим елементом вдосконалення їхньої ефективності.

1.2 Сфера застосування

Кілька десятиліть тому інформація про стан мережі та ефективність інфраструктури була лише зібрана в одному місці. Роль "інтелектуального аналізатора" лежала тільки на системних адміністраторах. Для того, щоб мати повний огляд системи, адміністратор повинен був бути ціле-вказчиком, тобто йому доводилось контролювати все одночасно. Це займало занадто багато часу, щоб дізнатися про певні проблеми та методи. Для того, щоб спростити роботу адміністраторів та зменшити обсяг часу на обробку даних почали вводити в мережу системи моніторингу.

Коли є час вибрати інструмент моніторингу мережі, адміністратор мережі зустрічається із новими викликами. Більшість інструментів від різних постачальників надають широкий спектр можливостей. Однак є деякі відмінності, які можуть відігравати важливу роль у мережі. Тому для того, щоб вибрати оптимальний варіант для власної мережі, слід проаналізувати наступні ключові характеристики.

Мережевий моніторинг - це система, яка вказує на повільну мережеву продуктивність або непрацюючі мережеві пристрої. Моніторинг базується на аналізі пропускної здатності, системних помилок, втрати пакетів, затримки, наявності маршрутизаторів, перемикачів та часу відклику. Якщо відбувається

певна невдача, адміністратор мережі отримує повідомлення про відмову через попереджувальний банер, електрону пошту, телефон та ін.

Мережевий моніторинг також виконує роль стратегічного інструменту у сучасних структурах. Це допомагає оптимізувати потоки даних та виявити ненадійне обладнання. Крім того, він перевіряє потенціал пристроїв та їх умов, таких як швидкість температури та використання. Як результат, моніторинг допомагає максимально збільшити роботу мережі та зменшує потенційні невдачі. Основними перевагами оптимізованої мережі для структур, це: зменшення витрат на інфраструктуру, продуктивність працівників, а також швидкість та надійність потоку даних.

Існує загальне нерозуміння, що моніторинг мережі також надає аудит безпеки і запобігає несанкціонованому доступу до мережі. Для такого роду моніторингу безпеки використовуються системи профілактики вторгнення (IPS) або системи виявлення вторгнень (IDS). Мережа моніторингу використовується лише для моніторингу використання мережі та її надійності.

Мережевий моніторинг підтримує широкий спектр пристроїв, таких як сервери, маршрутизатори, вимикачі та навіть кінцеві пристрої. Крім того, він може бути використаний у будь-яких мережах, таких як WLAN, LAN, VPN та навіть WAN.

1.3 Типи мережевого моніторингу

Мережевий моніторинг включає в себе різні типи інструментів та методів для вимірювання, збору, аналізу та візуалізації даних про мережу. Основні типи мережевого моніторингу включають:

SNMP (Simple Network Management Protocol) є стандартним протоколом для моніторингу та управління мережевими пристроями, такими як маршрутизатори, комутатори, сервери.

Переваги: простий у використанні, стандартизований, дозволяє відстежувати стан пристроїв.

Недоліки: обмежена здатність моніторити деталізовану інформацію.

Flow-Based моніторинг використовується протоколами, такими як NetFlow або sFlow, для збору даних про трафік у мережі.

Переваги: забезпечує деталізовану інформацію про використання пропускної здатності та взаємодію пристроїв.

Недоліки: вимагає підтримки пристроїв та може створювати великий обсяг даних.

Пакетний моніторинг аналізує та записує весь мережевий трафік, включаючи вміст пакетів.

Переваги: дозволяє глибокий аналіз мережевого трафіку, виявлення аномалій та вразливостей.

Недоліки: великі обсяги даних, вимагає потужних ресурсів для обробки.

Агент-Орієнтований моніторинг полягає у інсталяції агентів на кожному мережевому пристрої для збору та передачі даних.

Переваги: деталізована інформація про стан пристроїв, невеликий обсяг даних.

Недоліки: вимагає встановлення агентів, що може призводити до додаткового навантаження.

Агент-Лесс моніторинг збирає дані без встановлення агентів на мережевих пристроях, використовуючи протоколи, такі як ICMP, SNMP.

Переваги: Простий у впровадженні, менше навантаження на пристрої.

Недоліки: Обмежена інформація порівняно з агент-орієнтованим моніторингом.

End-to-End моніторинг оцінює продуктивність та якість обслуговування з точки зору кінцевого користувача, вимірюючи час відправки-прийому даних.

Переваги: перспективний огляд продуктивності для кінцевих користувачів.

Недоліки: може бути обмежений доступом до деяких ділянок мережі.

Мережевий аналізатор використовується для аналізу мережевих пакетів та виявлення проблем, аналізу витрати пропускної здатності.

Переваги: глибокий аналіз мережевих проблем, виявлення вразливостей.

Недоліки: може бути складним у використанні для неспеціалізованих користувачів.

Моніторинг Якості Послуг (QoS) спрямований на вимірювання та забезпечення відповідності рівня обслуговування мережевим пакетам.

Переваги: Оцінка якості обслуговування для різних видів трафіку.

Недоліки: Може вимагати складних налаштувань та контролю.

Кожен тип мережевого моніторингу має свої переваги та недоліки, які дозволяє виявити маршрутна аналітика.

Маршрутна аналітика - це набір досліджень та інструментів, спрямованих на аналіз та оптимізацію маршрутів у мережі. Важливою метою маршрутної аналітики є виявлення ефективних маршрутів для передачі даних, визначення проблем у мережевих шляхах та оптимізація шляхів для досягнення кращої продуктивності та якості обслуговування.

Набір завдань та функцій маршрутної аналітики включає в себе:

1. Визначення Маршрутів: виявлення шляхів, які використовуються для передачі даних у мережі.
2. Моніторинг Пропускної Здатності: аналіз використання пропускної здатності по різних маршрутах для виявлення можливих загальних або локальних проблем.
3. Оцінка Витрати Маршруту: вимірювання часу, необхідного для передачі даних по конкретному маршруту.
4. Виявлення Проблем у Мережевих Шляхах: визначення проблем, таких як пакетні втрати, затримки, дублювання пакетів на маршрутах.
5. Оптимізація Маршрутів: автоматизована або ручна оптимізація маршрутів для покращення ефективності та продуктивності.
6. Моніторинг Якості Обслуговування (QoS): вимірювання та забезпечення відповідності якості обслуговування на різних маршрутах.

7. Виявлення Маршрутних Аномалій: розпізнавання аномалій, таких як змінення маршрутів, неправильна маршрутизація та інші непередбачувані ситуації.

8. Планування Резервних Шляхів: розробка та використання резервних маршрутів для забезпечення надійності та доступності мережі.

9. Взаємодія із Протоколами Маршрутизації: вивчення та аналіз взаємодії маршрутної аналітики із протоколами маршрутизації (наприклад, OSPF, BGP).

10. Візуалізація та Звітність: представлення результатів маршрутної аналітики у вигляді графіків, діаграм та звітів для зручного аналізу.

Маршрутна аналітика стає особливо важливою в складних мережевих середовищах, де ефективне управління маршрутами сприяє підвищенню продуктивності та забезпеченню надійності мережі.

Згідно рекомендаціям ISO виділять наступні функції засобів управління мережею:

У*правління конфігурацією мережі* - конфігурація компонентів мережі, наприклад, налаштування мережних адрес та ідентифікаторів, управління параметрами мережевих ОС, підтримку топології мережі та іменування об'єктів.

Обробка помилок - виявлення та подальше усунення наслідків збою мережі.

Аналіз продуктивності - на основі накопиченої статистичної інформації дозволяє оцінювати час відповіді системи для подальшого планування розвитку мережі.

Управління безпекою – об’єднує контроль доступу та збереження цілісності даних. У функції є процедура аутентифікації, підтримується шифрування та управління правами. Сюди можна віднести важливі механізми управління паролями, доступом та з'єднанням з іншими мережами.

Час роботи мережі - поєднує реєстрацію і управління використовуваними ресурсами і пристроями. Дана функція оперує поняттями часу використання і плати за ресурси.

З наведеного списку видно, що системи управління реалізовують не тільки функції моніторингу та аналізу роботи мережі, потрібні для отримання вихідних даних налаштування мережі, але і функції активного впливу на мережу - управління конфігурацією і безпекою, потрібні для відпрацювання плану налаштування та оптимізації мережі.

Сучасні засоби управління мережею відповідають за:

- контроль роботи додатків, сервісів, програм та користувачів;
- мінімізацію витрат на керування мережею.

1.4 Аналіз існуючих методів аналізу та обробки метрик

Розвиток телекомунікаційних мереж вимагає постійного удосконалення методів та засобів аналізу та обробки метрик для забезпечення їхньої ефективності та надійності. У цьому розділі проводиться докладний аналіз існуючих підходів та методів, які використовуються для аналізу метрик телекомунікаційних мереж. Першим етапом аналізу є класифікація метрик, які вимірюються в телекомунікаційних мережах. Зокрема, виділяються метрики, що характеризують пропускну здатність, затримку, втрати пакетів, якість обслуговування (QoS), а також метрики, пов'язані з безпекою та енергоефективністю.

Оглядаються традиційні методи аналізу метрик, що включають в себе використання сучасних протоколів, таких як SNMP (Simple Network Management Protocol), для збору та моніторингу метрик на різних рівнях мережі. Також розглядається використання інструментів, таких як Wireshark, для аналізу пакетів та розкриття деталей мережевого трафіку.

Традиційні методи аналізу метрик телекомунікаційних мереж є важливим елементом для забезпечення стабільності та ефективності функціонування мережі. У цьому розділі детально розглядаються та

аналізуються основні традиційні методи, які використовуються для збору та аналізу метрик.

Одним із найбільш використовуваних протоколів для моніторингу та управління мережею є SNMP. Цей протокол дозволяє збирати дані про стан мережевих пристроїв, таких як роутери, комутатори, сервери. Аналіз отриманих даних дозволяє визначити пропускну здатність, ступінь завантаження та інші характеристики. Інший традиційний метод включає використання інструментів аналізу пакетів, таких як Wireshark. Цей інструмент дозволяє отримати детальну інформацію про мережевий трафік, включаючи взаємодію між пристроями, типи пакетів, затримку та інші параметри. Традиційні методи також включають моніторинг стану окремих пристроїв та серверів у мережі. Це може бути здійснено за допомогою вбудованих засобів моніторингу операційних систем, або використанням спеціалізованих систем моніторингу, таких як Nagios або Zabbix. Аналіз метрик, пов'язаних із пропускною здатністю мережі, є ключовим елементом традиційних методів. Вимірювання рівня трафіку, швидкості передачі даних та інших параметрів дозволяє оцінювати ефективність мережі. Аналіз затримки та втрат пакетів є важливими складовими традиційних методів. Затримка може впливати на якість обслуговування, особливо в реальному часі, тоді як втрати пакетів можуть свідчити про проблеми у стабільності мережі. Незважаючи на широке використання та важливість традиційних методів, вони мають свої обмеження. Зокрема, обмежена можливість збору глибок. В рамках цього розділу розглядається інструментарій для аналізу метрик, який включає в себе відомі системи моніторингу, такі як Zabbix, Nagios, а також спеціалізовані інструменти для аналізу пропускної здатності, затримки та інших параметрів.

При аналізі існуючих методів важливо визначити їхні обмеження та недоліки. Наприклад, традиційні методи можуть бути обмежені великим обсягом даних чи неефективністю в умовах високої динаміки мережі.

1.5 Критика існуючих підходів та їхні обмеження

Існуючі методи та засоби аналізу і обробки метрик телекомунікаційних мереж, які були розглянуті вище, відіграють важливу роль у моніторингу та управлінні мережею. Проте, швидкі темпи розвитку технологій та зростаючі вимоги до мережевої інфраструктури, вказують на необхідність постійного удосконалення існуючих методів та впровадження нових. Багато існуючих методів аналізу метрик мережі мають обмежену точність та “гранулярність” вимірювань. Наприклад, традиційні протоколи моніторингу, такі як SNMP, можуть не забезпечувати достатню деталізацію для ефективного виявлення та вирішення проблем на рівні окремих компонентів мережі.

Іншою критичною проблемою є обмежені можливості існуючих методів у виявленні аномальної поведінки та кіберзагроз в реальному часі. Традиційні підходи часто не здатні ефективно аналізувати велику кількість даних та вчасно реагувати на виникнення непередбачених ситуацій. Традиційні методи часто неадаптовані до динамічних змін у мережі, зокрема, до частого змінюваного розміру та топології мережі.

1.6 Висновки до розділу 1

З цього можна зробити висновок, що їхня ефективність зменшується при великому обсязі даних та високій динаміці використання мережевих ресурсів. Деякі існуючі методи не завжди забезпечують ефективне виявлення складних патернів та асоціацій у метриках мережі. Умови високого трафіку та складної структури мережі можуть ускладнювати процес виявлення кореляцій та взаємозв'язків між різними параметрами. Більшість традиційних методів аналізу метрик не завжди дозволяють ефективно враховувати контекстні особливості мережі. Природна зміна умов експлуатації та взаємодії між різними компонентами мережі вимагає більш гнучких та адаптивних підходів. Також більшість існуючих методів не забезпечують ефективні механізми прогнозування та попередження потенційних проблем в

мережі. Важливість раннього виявлення аномалій та можливість їхнього передбачення в умовах зростаючої складності мереж

2. МЕТОДИ АНАЛІЗУ МЕТРИК ТЕЛЕКОМУНІКАЦІЙНОЇ МЕРЕЖІ

2.1 Аналіз методів моніторингу телекомунікаційної мережі

Аналіз методів моніторингу телекомунікаційної мережі є важливим етапом для забезпечення стабільності, ефективності та безпеки мережі. Давайте розглянемо два різних методи моніторингу телекомунікаційної мережі та проведемо їх аналіз.

Метод 1: SNMP (Simple Network Management Protocol) моніторинг

Основні характеристики:

Визначення Метрик: SNMP дозволяє вимірювати різноманітні метрики, такі як пропускна здатність, використання ресурсів, стан інтерфейсів тощо.

Легкість Використання: SNMP є стандартним та широко використовується протоколом, що полегшує інтеграцію з різноманітними пристроями.

Віддалений Моніторинг: здатність використовувати SNMP для моніторингу пристроїв навіть на великих відстанях.

Низький Рівень Деталізації: деякі аспекти мережі можуть бути виміряні менш деталізовано порівняно з іншими методами.

Оцінка: SNMP є ефективним методом для моніторингу телекомунікаційної мережі, зокрема для отримання загального стану та базових метрик пристроїв. Однак його обмежена деталізація може бути недостатньою для глибокого аналізу проблем та аномалій у мережі.

Метод 2: Flow-Based моніторинг з використанням NetFlow

Основні характеристики:

Аналіз Трафіку: використання NetFlow дозволяє отримувати деталізовану інформацію про трафік на рівні пакетів.

Визначення Джерела та Призначення Трафіку: можливість визначити, звідки і куди направлені конкретні потоки даних.

Сповіщення про Аномалії: здатність виявляти аномальний трафік, такий як DDoS-атаки, затримки та інші проблеми.

Більш Великий Обсяг Даних: за рахунок включення деталізованої інформації, NetFlow може генерувати більше обсягу даних.

Оцінка: Flow-Based моніторинг, зокрема використання NetFlow, надає значну деталізацію та можливість глибокого аналізу трафіку. Однак його великий обсяг даних може вимагати потужних ресурсів для збору та обробки і може бути менш ефективним для загального стану мережі.

Отже, в результаті аналізу можна стверджувати, що обидва методи мають свої переваги та недоліки. Вибір конкретного методу або їх комбінації залежить від конкретних потреб мережі. Наприклад, SNMP може використовуватися для загального моніторингу, а Flow-Based моніторинг може бути використаний для деталізованого аналізу трафіку.

Інтегровані системи управління аналізом даних метрик в телекомунікаційних мережах об'єднують в собі різні засоби та можливості для комплексного аналізу й управління метриками. Деякі ключові характеристики таких систем включають:

Централізоване збирання та моніторинг даних: Здатність збирати інформацію з різних джерел (різні пристрої, протоколи) та моніторити її в реальному часі для швидкого реагування на події в мережі.

Аналіз та візуалізація даних: Системи надають інструменти для аналізу та візуалізації метрик у зручному форматі, що допомагає операторам швидко розуміти стан мережі.

Прогнозування та оптимізація: Деякі системи використовують алгоритми машинного навчання для прогнозування навантаження, аномалій або для рекомендацій щодо оптимізації мережевих параметрів.

Автоматизоване управління: Можливість автоматичного реагування на зміни параметрів мережі або аномальні ситуації, включаючи виконання певних дій для відновлення нормального функціонування.

Ці системи є важливими для операторів мереж, оскільки дозволяють швидко реагувати на проблеми та оптимізувати роботу телекомунікаційних систем для забезпечення стабільності та ефективності.

Основні засоби моніторингу в включають:

Збір даних: може збирати інформацію з різноманітних джерел, включаючи сервери, пристрої мережі, додатки тощо, використовуючи різні протоколи (SNMP, ICMP, HTTP, та інші).

Настроюванні метрики моніторингу: Користувачі можуть налаштовувати метрики для відстеження різних параметрів, таких як пропускна здатність, використання ресурсів, стан сервісів та інше.

Графіки та візуалізація даних: надає можливості побудови графіків та зручний інтерфейс для візуалізації даних моніторингу, що дозволяє швидко аналізувати стан системи.

Автоматизовані сповіщення та тривоги: Система може відправляти повідомлення про проблеми чи аномалії через різні канали (email, SMS, Slack тощо), дозволяючи операторам швидко реагувати на проблеми.

Аналіз та звіти: дозволяє аналізувати динаміку даних, будувати звіти та здійснювати аналітику для підвищення ефективності моніторингу.

Ця система є потужним засобом для моніторингу та управління мережевими ресурсами і її використання дозволяє підтримувати стабільну та ефективну роботу інфраструктури.

Існує кілька протоколів керування мережею, які використовуються для управління, налагодження та моніторингу різних аспектів мережі. Ось деякі з найпоширеніших:

Simple Network Management Protocol (SNMP): Використовується для віддаленого моніторингу та керування мережевими пристроями. Дозволяє збирати інформацію про стан пристроїв і відправляти команди для їх керування.

NetFlow / sFlow: Ці протоколи дозволяють збирати та аналізувати дані про трафік у мережі, допомагаючи виявляти патерни та проблеми у роботі мережі.

Border Gateway Protocol (BGP): Використовується для обміну інформацією між автономними системами Інтернету. Він дозволяє роутерам визначати найкращий шлях для передачі даних.

OpenFlow: Це протокол програмованого керування мережею, який розділяє управління мережею (control plane) від пересилання даних (data plane) для більш гнучкого керування мережею.

Spanning Tree Protocol (STP) / Rapid Spanning Tree Protocol (RSTP): Використовується для управління шляхами у мережах з кількома комутаторами, щоб уникнути петель у топології мережі.

Ці протоколи відіграють ключову роль у функціонуванні, моніторингу та управлінні різними аспектами мережі, забезпечуючи її стабільність, ефективність та безпеку.

Протокол SNMP (Simple Network Management Protocol) є стандартним протоколом для моніторингу та управління мережевими пристроями. Основні елементи SNMP включають:

Агенти SNMP: Вони встановлені на мережевих пристроях (роутерах, комутаторах, серверах тощо) і забезпечують збір інформації про стан пристрою.

Менеджери SNMP: Це програми або пристрої, що взаємодіють з агентами для отримання інформації про стан мережі та надсилання команд для керування пристроями.

MIB (Management Information Base): Визначає структуру та типи даних, які можуть бути запитані та відправлені через SNMP.

SNMP Traps: Це повідомлення, які агенти відправляють менеджерам при виникненні певних подій чи аномалій.

Протокол SNMP дозволяє менеджерам запитувати дані про стан мережевих пристроїв (наприклад, стан інтерфейсів, використання ресурсів) та виконувати дії для керування цими пристроями (наприклад, змінювати конфігурацію, перезавантажувати пристрій).

SNMP є важливим інструментом для моніторингу та управління мережею, оскільки дозволяє операторам ефективно контролювати та керувати різними аспектами її роботи. Протокол SNMP (Simple Network Management Protocol) складається з кількох основних компонентів:

MIB (Management Information Base): Це віртуальна база даних, що містить інформацію про параметри та об'єкти, які можуть бути моніторені та керовані. MIB визначає структуру та типи даних, які можуть бути доступні для використання через SNMP. Вона організована у вигляді ієрархічної структури об'єктів.

SNMP-агенти: Це програмні модулі, які запущені на мережевих пристроях (роутерах, комутаторах, серверах тощо) і забезпечують доступ до даних про стан пристрою через SNMP. Агенти перетворюють інформацію про пристрій у формат, зрозумілий для менеджера.

SNMP-менеджери: Це програми або пристрої, які здійснюють моніторинг та керування мережею. Вони взаємодіють з агентами, запитуючи дані з MIB або відправляючи команди для керування пристроями.

SNMP Traps: Це повідомлення, які агенти відправляють менеджерам при виникненні певних подій чи аномалій, таких як помилки, перевантаження, важливі події тощо. Traps дозволяють операторам оперативно реагувати на важливі події у мережі.

Ці компоненти разом утворюють основу для взаємодії та обміну даними між мережевими пристроями та системами керування, що дозволяє ефективно моніторити та керувати мережею. У протоколі SNMP (Simple Network Management Protocol) змінні зазвичай ідентифікуються за допомогою OID (Object Identifier), який є унікальним числовим ідентифікатором для кожного об'єкту в MIB (Management Information Base). Однак, крім числових ідентифікаторів, змінні також можна іменувати символьними іменами.

Для символьних імен зазвичай використовуються текстові мітки або описові назви, які спрощують ідентифікацію об'єктів в MIB. Ці імена допомагають людям легше розуміти і використовувати змінні, замість використання числових OID.

Наприклад, у MIB може бути описано таке:

sysUpTime: Це може бути символьне ім'я, яке відповідає змінній, що вказує на час, який система працює з моменту запуску.

ifInOctets: Ця мітка може вказувати на кількість отриманих байтів через мережевий інтерфейс.

Ці символьні імена дають можливість краще розуміти, що саме вимірює або представляє кожна змінна в мережевому середовищі.

Висновки до даного розділу Розділ про протокол дозволив розглянути важливі аспекти цього стандарту для моніторингу та управління мережею:

Універсальність та стандартизація: SNMP - це широко використовуваний протокол, що дозволяє стандартизувати процеси моніторингу та управління мережею на різних пристроях.

Компоненти протоколу: Вивчення основних компонентів, таких як MIB, агенти та менеджери, розкриває механізми обміну даними та можливості керування.

Функціональні можливості: SNMP дозволяє отримувати інформацію про стан пристроїв, відправляти команди для керування та спостерігати за подіями у мережі через використання простого та ефективного протоколу.

Важливість для моніторингу мережі: Розуміння SNMP є ключовим для забезпечення ефективного моніторингу мережі, швидкого реагування на проблеми та забезпечення стабільності інфраструктури.

Роль у керуванні мережею: SNMP дозволяє віддалено керувати мережевими пристроями, змінювати їх конфігурації та взаємодіяти з ними через єдиний стандарт.

Цей розділ підкреслив важливість та функціональні можливості протоколу SNMP у сфері моніторингу та управління мережею, що робить його важливою складовою сучасної мережевої інфраструктури.

2.2 Види метрик телекомунікаційної мережі

Метрики телекомунікаційних мереж - це числові показники, які використовуються для оцінки різних аспектів функціонування мережі. Ось деякі типи метрик телекомунікаційної мережі:

1. Пропускна здатність (Bandwidth): Це обсяг даних, які можуть бути передані через мережу за певний проміжок часу. Вимірюється у бітах за секунду (bps) або його кратних одиницях.

2. Затримка (Latency): Час, що потрібний для передачі сигналу від відправника до отримувача. Затримка впливає на час реакції мережі та швидкість передачі даних.

3. Втрати пакетів (Packet Loss): Втрати даних під час передачі через мережу. Це може бути викликане перевантаженням мережі або проблемами з підключенням.

4. Співвідношення сигнал/шум (Signal-to-Noise Ratio - SNR): Вимірює якість сигналу в мережі в порівнянні з рівнем шуму. Важливо для безперебійної передачі даних.

5. Втрата пакетів (Packet Loss Rate): Відсоток пакетів, що втрачаються під час передачі через мережу, що впливає на якість послуги.

6. Доступність (Availability): Час, протягом якого мережа доступна для використання.

7. Витрати на маршрутизацію (Routing Overhead): Вимірює навантаження на маршрутизатори та інші мережеві пристрої під час пересилання даних.

8. Узагальнення обсягів даних (Aggregated Data Volume): Обсяг даних, переданих або отриманих пристроями чи мережею за певний період часу.

Це лише деякі з багатьох метрик, які використовуються для оцінки та вимірювання різних параметрів у телекомунікаційних мережах.

2.2.1 Визначення понять та основні характеристики метрик

В даному підрозділі надається чітке визначення та основні характеристики поняття "метрика" у контексті телекомунікаційної мережі. Аналізуються основні параметри, які можуть бути вимірювані та моніторингу для оцінки ефективності та стану мережі. Метрика в телекомунікаційній мережі — це числовий показник, який використовується для вимірювання та оцінки різних параметрів та характеристик мережі з метою забезпечення її ефективності, надійності та якості обслуговування. Метрики дозволяють моніторити та аналізувати різноманітні аспекти мережевої діяльності для покращення її функціонування та вирішення можливих проблем. Розглядаються ключові аспекти, що характеризують метрики, такі як частота вимірювань, одиниці вимірювань, точність та релевантність для визначення їхнього значення та використання у контексті аналізу мережі.

До основних характеристики метрик телекомунікаційної мережі можнв віднести:

1. Частота Вимірювань. Визначає, як часто проводяться вимірювання метрик. Часті вимірювання можуть забезпечити більш точні та актуальні дані для аналізу.

2. Одиниці Вимірювань. Вказують на одиниці, в яких вимірюється конкретна метрика (наприклад, кількість бітів, мілісекунд, відсоток).

3. Точність Метрик. Враховується при визначенні, наскільки добре метрика відображає реальний стан мережі. Висока точність дозволяє ефективніше розпізнавати аномалії та здійснювати керування ресурсами.

4. Релевантність. Показує, наскільки важливою є метрика для конкретного аспекту мережі. Релевантні метрики допомагають зорієнтуватися на основні аспекти функціонування мережі.

5. Види Метрик. Визначаються конкретні параметри, які вимірюються (пропускна здатність, затримка, втрати пакетів, QoS). Різні види метрик вказують на різні аспекти мережевої продуктивності.

6. Кореляція та Взаємозв'язок Метрик. Враховується можливість взаємодії різних метрик та їхній вплив одна на одну. Кореляція метрик допомагає зрозуміти, які параметри можуть взаємодіяти та впливати на продуктивність мережі.

Стандартні значення метрик інтерфейсів (каналів) протоколу OSPF

Технологія	Serial T1	Serial E1	Ethernet	Fast Ethernet	Gigabit Ethernet
Пропускна здатність, Мбіт/с	1,544	2,048	10	100	1000
Метрика інтерфейсу	64	48	10	1	1

Таблиця 1: Порядок налагодження функціонування протоколу маршрутизації

2.3 Огляд інструментів для збору метрик та їх інтерпритаціїї

В сучасних телекомунікаційних мережах використовуються різноманітні інструменти для збору метрик, які надають можливість моніторити та аналізувати продуктивність мережі. Виконавши огляд найбільш поширених рішень, можна виділити наступні інструментів та їхніх характеристик:

Simple Network Management Protocol (SNMP). Використовується для збору метрик з мережевих пристроїв. Підтримується багатьма мережевими пристроями та програмним забезпеченням моніторингу. Надає базові метрики, такі як стан інтерфейсів, використання CPU, пам'яті тощо.

NetFlow. Використовується для збору даних про трафік у мережі. Надає деталізовану інформацію щодо взаємодії мережевих пристроїв та витрат ресурсів на різних рівнях.

Packet Sniffers (Wireshark, tcpdump). Використовуються для аналізу пакетів у мережі та збору детальних метрик, таких як затримка, втрати пакетів, пропускна здатність. Забезпечують можливість розкриття проблем на рівні мережевих пакетів.

Zabbix. Це система моніторингу, яка підтримує збір метрик з різних джерел, включаючи SNMP, JMX, IPMI. Має можливості відображення метрик у реальному часі та створення сповіщень.

Prometheus. Відкрите програмне забезпечення для моніторингу та алертингу. Підтримує мову запитів PromQL для витягування та аналізу даних.

Grafana. Використовується для візуалізації даних, включаючи метрики з інших моніторингових систем. Підтримує різноманітні джерела даних, такі як Prometheus, InfluxDB, Elasticsearch.

sFlow/NetStream. Використовується для моніторингу трафіку та збору даних про взаємодію мережевих пристроїв.

Nagios. Система моніторингу, яка може використовуватися для збору метрик та виявлення аномалій. Підтримує різні плагіни для збору різноманітних метрик.

Згадані вище інструменти надають різноманітні можливості для збору та аналізу метрик у телекомунікаційних мережах, дозволяючи адміністраторам та інженерам здійснювати ефективний моніторинг та управління ресурсами мережі.

2.4 Висновки до розділу 2

В даному розділі було проаналізовано існуючі методи для моніторингу стану мережі. Також розкрито зміст інтегрованих системи управління та аналізу даних та яка їх роль. Які бувають протоколи управління мережею та їх особливості.

Метод управління мережею полягає в здійсненні сукупності впливів на керований об’єкт, які вибрані з множини можливих впливів на підставі програми управління та інформації, що надходить про поведінку об’єкта і стан навколишнього середовища для досягнення заданої мети.

За способом використання інформації, отриманої від експертів, існують такі групи експертних методів прогнозування: методи прямих оцінок та методи зі зворотнім зв’язком.

Інтегровані системи управління ведуть постійний контроль за роботою локальної мережі, що становить основу будь-якої телекомунікаційної мережі, необхідний для підтримки її в працездатному стані.

Були розділені засоби моніторингу та аналізу обчислювальних мереж на декілька крупних класів. А також описаний самий важливий протокол прикладного рівня управління мережею - SNMP. Він призначений для обміну інформацією між мережевими пристроями. За допомогою цього протоколу, мережевий адміністратор може виробляти аналіз мережевого устаткування, знаходити і вирішувати безліч мережевих проблем.

3. РОЗРОБКА НОВИХ МЕТОДІВ ОБРОБКИ МЕТРИК

В даному розділі розглядається процес розробки та впровадження нових методів обробки метрик у телекомунікаційній мережі. Відзначається актуальність розробки інноваційних підходів для вдосконалення якості аналізу та моніторингу мережевих показників.

Введення інноваційних методів обробки метрик у телекомунікаційній мережі є актуальним завданням в контексті стрімкої еволюції технологій та зростання об'єму та складності даних, які обробляються мережами. Зараз, коли технічні вимоги та очікування користувачів постійно зростають, нові методи обробки метрик є ключовим елементом для забезпечення ефективності та надійності телекомунікаційних мереж.

3.1 Синтез нових методів обробки та інтерпретації даних

Розробка нових методів обробки метрик у телекомунікаційній мережі є важливим напрямком для поліпшення моніторингу та управління мережевими ресурсами. Нові методи можуть бути спрямовані на різні аспекти, забезпечуючи більш точний аналіз та оптимізацію функціонування мережі. Деякі можливі напрямки розробки нових методів обробки метрик включають:

Прогностичний аналіз - розробка методів, які дозволяють прогнозувати можливі аномалії або витрати ресурсів у мережі. Використання алгоритмів машинного навчання для побудови прогностичних моделей.

Кореляція метрик. Розробка методів для виявлення та аналізу взаємозв'язків між різними метриками. Використання статистичних методів та аналізу графів для визначення паттернів та взаємодій.

Адаптивні методи. Створення методів, які можуть адаптуватися до змінних умов мережі. Розробка алгоритмів, які динамічно налаштовують параметри обробки метрик в залежності від поточних обставин.

Аналіз великих обсягів даних (Big Data). Розробка методів, придатних для ефективного обробки та аналізу великих обсягів даних, які генеруються в сучасних телекомунікаційних мережах.

Методи оптимізації трафіку. Розробка алгоритмів для оптимізації потоків даних у мережі, зменшення затримок та підвищення загальної продуктивності.

Вдосконалення виявлення аномалій. Розробка методів, які вдосконалюють виявлення аномальної поведінки у мережі. Використання алгоритмів машинного навчання для автоматичного визначення нестандартних ситуацій.

Забезпечення якості обслуговування (QoS). Розробка методів для забезпечення оптимальної якості обслуговування у різних частинах мережі. Визначення та оптимізація параметрів QoS.

Аналіз мультимедійних метрик. Створення методів для ефективного аналізу та обробки метрик, пов'язаних з передачею мультимедійного контенту у мережі.

Ці напрямки розробки можуть сприяти вдосконаленню моніторингу та оптимізації роботи телекомунікаційних мереж, підвищуючи їхню ефективність та надійність.

Синтез нових методів обробки даних метрик у телекомунікаційній мережі є ключовим етапом для поліпшення ефективності моніторингу та управління ресурсами. Нові підходи можуть враховувати сучасні виклики та сприяти точнішому аналізу стану мережі. У цьому розділі розглядається процес синтезу та основні аспекти нових методів обробки даних метрик. Перед розробкою нових методів необхідно ретельно визначити мету та область їх застосування. Актуальність синтезу нових підходів полягає в розробці ефективних інструментів, які забезпечують більш глибокий та комплексний аналіз метрик, що є важливим у сучасних високонавантажених та розподілених мережах.

Визначення вимог

1. Ефективність обробки:

Масштабованість: Забезпечення ефективної роботи методів при збільшенні обсягу метрик та завдань моніторингу.

Швидкодія: Мінімізація часу обробки для забезпечення реального чи прийнятного часу відповіді.

2. Точність та Надійність:

Точність обробки: Забезпечення високої точності результатів обробки метрик.

Стійкість до Помилок: Мінімізація впливу помилок або відмов на результати обробки.

3. Адаптивність:

Гнучкість налаштувань: Можливість адаптації параметрів обробки до різних умов та потреб користувачів.

Спроможність враховувати динамічні зміни: Адаптація до змін у структурі мережі та характеристиках трафіку.

4. Інтеграція та Сумісність:

Сумісність з існуючими системами: Інтеграція нових методів з існуючими платформами та системами моніторингу.

Стандартизація даних: Використання загальноприйнятих форматів та протоколів для обміну даними.

3.2 Програмна реалізація розроблених методів

Для реалізації розроблених методів обробки метрик використовуються сучасні технології, що враховують вимоги до швидкодії та масштабованості:

Мови програмування: Використання Python та Java для забезпечення гнучкості розробки та високої продуктивності.

Бази даних: Використання високопродуктивних баз даних, таких як MongoDB чи Cassandra, для зберігання та отримання метрик.

Фрейм ворки машинного навчання: Використання TensorFlow або PyTorch для реалізації алгоритмів машинного навчання для прогнозування та аналізу метрик.

Програмна реалізація розроблених методів обробки метрик включає в себе написання відповідного програмного коду, який враховує математичні моделі та алгоритми, розроблені на попередніх етапах. Нижче наведено загальний підхід до цього процесу, з використанням прикладу мови програмування Python:

На основі математичних виразів та системи рівнянь створюються функції та класи, які відображають логіку обробки метрик. Використовуйте функції для опису окремих кроків обробки та класи для організації алгоритмів у більш структуровану форму мал.1.

На основі функцій та класів створюють алгоритм обробки метрик. Переконайтеся, що весь код логічно організований та відображає математичні моделі. тести, які перевірять правильність роботи реалізованих методів. Використовуйте різноманітні вхідні дані та переконайтеся, що алгоритм працює коректно. Відлагоджуйте код та виправляйте помилки.

Якщо програмна реалізація має бути інтегрована у мережне середовище, забезпечте взаємодію з існуючими системами та пристроями (мал.2-3). Враховуйте вимоги до зберігання та передачі метрик у мережі. Це загальний підхід, і конкретні деталі програмної реалізації будуть залежати від характеру ваших математичних моделей та алгоритмів обробки метрик мал.4. У вас може бути більше складний код залежно від конкретного завдання.

```python
# Приклад функції для обчислення одного з етапів обробки метрик
def process_metric_step(metric):
    # Логіка обробки метрики
    processed_result = metric * 2
    return processed_result

# Приклад класу, який реалізує алгоритм обробки метрик
class MetricProcessor:
    def __init__(self):
        # Ініціалізація об'єкта

    def process_metrics(self, metrics):
        processed_metrics = []
        for metric in metrics:
            processed_metric = process_metric_step(metric)
            processed_metrics.append(processed_metric)
        return processed_metrics
```

Мал.1 Визначення Функцій та Класів

```python
# Приклад алгоритму обробки метрик
def main_processing_algorithm(metrics):
    processor = MetricProcessor()
    result = processor.process_metrics(metrics)
    return result
```

Мал.2 Реалізація наведеного Алгоритму

```python
# Приклад функції для обробки одного параметра метрики
def process_metric(metric):
    # Логіка обробки метрики
    result = metric * 2
    return result
```

Мал.3 Визначення Функцій

```python
# Приклад класу для обробки масиву метрик
class MetricProcessor:
    def __init__(self):
        # Ініціалізація об'єкта, якщо потрібно

    def process_metrics(self, metrics):
        processed_metrics = []
        for metric in metrics:
            processed_metric = self.process_single_metric(metric)
            processed_metrics.append(processed_metric)
        return processed_metrics

    def process_single_metric(self, metric):
        # Логіка обробки метрики
        result = metric * 2
        return result
```

Мал. 4 Визначення Класів


```python
# Приклад класу для обробки масиву метрик
class MetricProcessor:
    def __init__(self):
        # Ініціалізація об'єкта, якщо потрібно

    def process_metrics(self, metrics):
        processed_metrics = []
        for metric in metrics:
            processed_metric = self.process_single_metric(metric)
            processed_metrics.append(processed_metric)
        return processed_metrics

    def process_single_metric(self, metric):
   processed_metric = self.process_single_metric(metric)
   processed_metrics.append(processed_metric)
        return result
```


Мал. 4 Визначення Класів

Програмне тестування та відладки є важливими етапами у розробці програмного забезпечення. Нижче наведено загальний підхід до тестування та відладки розроблених методів обробки метрик: Розглянемо різні типи метрик та впевніться, що на методи обробки коректно працюють у всіх випадках.

```python
# Приклад тестового сценарію
def test_metric_processing():
    processor = MetricProcessor()

    # Тест на коректність обробки одного параметра
    assert processor.process_single_metric(5) == 10

    # Тест на коректність обробки масиву метрик
    input_metrics = [1, 2, 3]
    expected_output = [2, 4, 6]
    assert processor.process_metrics(input_metrics) == expected_output
```

```python
import unittest

class TestMetricProcessing(unittest.TestCase):
    def test_single_metric_processing(self):
        processor = MetricProcessor()
        result = processor.process_single_metric(5)
        self.assertEqual(result, 10)

    def test_multiple_metrics_processing(self):
        processor = MetricProcessor()
        input_metrics = [1, 2, 3]
        expected_output = [2, 4, 6]
        result = processor.process_metrics(input_metrics)
        self.assertEqual(result, expected_output)

if __name__ == '__main__':
    unittest.main()
```

Мал.5 Виведення даних у консолі

Вставляйте в код виведення інформації у консоль для відслідковування ходу виконання та значень змінних. . Використання pdb (Python Debugger) Використовуйте модуль pdb для вставки точок зупинки та аналізу коду у режимі відладки (мал.6).

```python
# Приклад виведення інформації для відладки
def process_single_metric(metric):
    print(f"Processing metric: {metric}")
    result = metric * 2
    print(f"Result: {result}")

import pdb

# Приклад використання pdb
def process_single_metric(metric):
    pdb.set_trace()  # Встановлення точки зупинки
    result = metric * 2
    return result
```

Мал 6. Використання pdb та відкладки

Ці методи спільно допоможуть нам відладити та перевірити коректність роботи розроблених методів обробки метрик. Потрібно пам'ятати, що ефективне тестування та відладка є важливою частиною розробки програмного забезпечення. Інтеграція з мережовим середовищем може включати в себе збір та обробку метрик з мережевих пристроїв, обмін даними з моніторинговими системами або інші способи взаємодії з мережею. Нижче наведено загальний підхід до програмної реалізації інтеграції з мережовим середовищем. Якщо потрібно збирати метрики з мережевих пристроїв, використовуйте протоколи, такі як SNMP або REST API для отримання даних. Наприклад, для використання SNMP можна використовувати бібліотеку PySNMP в Python мал.7, це вже використовуєте моніторингові системи, такі як Zabbix, Nagios, або Prometheus, використовуйте їхні API для відправки та отримання даних. Наш метод обробки метрик можуть бути викликані в контексті отриманих даних, а потім можна використовувати інтеграцію з мережовим середовищем для відправки оброблених метрик туди, де це необхідно. Це загальний підхід, і реалізація буде залежати від конкретних технологій, які ми будемо використовувати для інтеграції з мережовим середовищем. Однак, у вас є основа для подальшого розширення та адаптації коду під наші потреби

```python
from pysnmp.hlapi import *

def snmp_get(ip, community, oid):
    errorIndication, errorStatus, errorIndex, varBinds = next(
        getCmd(SnmpEngine(),
               CommunityData(community),
               UdpTransportTarget((ip, 161)),
               ContextData(),
               ObjectType(ObjectIdentity(oid)))
    )

    if errorIndication:
        print(errorIndication)
    elif errorStatus:
        print(f'{errorStatus.prettyPrint()} at {errorIndex and varBinds
    else:
        return varBinds[0][1]
```

```python
# Приклад обробки та відправки метрик
def process_and_send_metrics(metrics):
    processed_metrics = process_metrics(metrics)

    # Використання інтеграції з мережовим середовищем (наприклад, Zabbix)
    send_data_to_zabbix(zabbix_server, host_id, "processed.metric", pro

    # Або будь-який інший механізм відправки метрик

# Приклад використання
raw_metrics = [1, 2, 3, 4, 5]
process_and_send_metrics(raw_metrics)
```

```python
import requests

def send_data_to_zabbix(server, host, key, value):
    zabbix_api_url = f"http://{server}/zabbix/api_jsonrpc.php"

    headers = {
        "Content-Type": "application/json",
    }

    data = {
        "jsonrpc": "2.0",
        "method": "item.create",
        "params": {
            "name": key,
            "key_": key,
            "hostid": host,
            "type": 0,
            "value_type": 3,
        },
        "auth": "your_zabbix_api_token",
        "id": 1,
    }
```

Мал. 7. Приклад використання бібліотеки PySNMP

У цьому прикладі створений клас MetricProcessor, який містить метод process_metrics для обробки масиву метрик. Метод process_single_metric викликається для кожної окремої метрики та обробляє її відповідно до визначеної логіки.

Це базовий каркас, і ми можемо додавати більше функцій та методів відповідно до поставленого завдання. При цьому необхідно зазначити, що реалізація методів обробки метрик буде залежати від конкретної математичної моделі процесу моніторингу, а також для інтеграції з середовищем мережі. Але у будь-якому випадку вважатимемо його за основу для подальшого розширення та адаптації коду.

3.3 Висновки до розділу 3

Отже, висновки вказують на різноманітність, потенціал для вдосконалення та потребу у нових підходах для покращення методів та засобів аналізу метрик у телекомунікаційних мережах. Після успішного тестування та оптимізації, новий метод можна впроваджувати у виробниче середовище, де він повинен бути постійно моніторингу та вдосконалення для максимальної ефективності. Цей процес дозволяє створювати та вдосконалювати нові методи обробки метрик, що може покращити аналіз та управління телекомунікаційними мережами. Для покращення якості аналізу та моніторингу мережевих показників можна використовувати кілька підходів:

Розширення обсягу збирання даних: Включення нових показників та параметрів для отримання більш повного зображення стану мережі. Це дозволить отримати більш деталізовану та розгорнуту інформацію. Розширення обсягу збирання даних у контексті обробки метрик може включати кілька ключових аспектів:

Додавання нових метрик: Включення додаткових параметрів та метрик для збору і аналізу даних, які допоможуть отримати більш повне та

розгорнуте зображення стану мережі. Це може включати метрики профілю використання ресурсів, інформацію про пропускну здатність, час відповіді тощо.

4. ЕКСПЕРИМЕНТАЛЬНІ ДОСЛІДЖЕННЯ ТА ТЕСТУВАННЯ

У цьому підрозділі буде розглянуто організацію та проведення експериментів і тестів для оцінки продуктивності та ефективності розробленого програмного забезпечення для аналізу та обробки метрик телекомунікаційної мережі. Починаючи з визначення цілей експериментів, впроваджуються стандартизовані тестові сценарії для забезпечення повторюваності та достовірності результатів. Описуються етапи підготовки та конфігурації тестового середовища, включаючи вибір мережевих пристроїв, запуск системи збору метрик, та встановлення параметрів експериментів. Описуються методи та засоби для збору метрик з реальних телекомунікаційних пристроїв, включаючи використання SNMP, REST API, та інших протоколів для отримання даних.

Моніторинг пропускної здатності (Bandwidth) є критичним елементом для ефективного управління та забезпечення оптимальної продуктивності телекомунікаційної мережі. Пропускна здатність визначає обсяг даних, які мережа може передавати за одиницю часу і є ключовим показником її продуктивності. Важливо моніторити та управляти цією метрикою, щоб уникнути перевантаження мережі та забезпечити задовільний рівень обслуговування.

4.1 Збір та обробка метрик

Розглянемо процес збору та обробки метрик в реальних телекомунікаційних мережах. Опишемо інструменти та методи, використовувані для отримання даних з мережевих пристроїв, а також процес обробки цих метрик для подальшого аналізу. Цей етап є ключовим для отримання надійних та вичерпних даних, які слід подальше аналізувати для покращення ефективності та надійності мережі. Вибір Інструментів для збору метрик:
SNMP (Простий Протокол Управління Мережею):

Налаштування SNMP-агентів на мережевих пристроях (роутери, комутатори, сервери).

Визначення переліку метрик, які можна отримати за допомогою SNMP (інтерфейси, стан системи тощо).

Пакети збору даних використання спеціалізованих пакетів для збору метрик, які не доступні за допомогою SNMP (протоколи на рівні додатків, деталізація трафіку тощо). Процес збору та обробки метрик в реальних телекомунікаційних мережах включає в себе кілька етапів, які мають на меті отримання, обробку та аналіз різноманітних параметрів мережі для забезпечення її ефективності та надійності. Нижче наведено загальний опис цього процесу:

Етап 1: Вибір Інструментів та Налаштування Збору Метрик

Вибір інструментів та налаштування збору метрик є критичним етапом для успішної моніторингової системи. Нижче наведено загальний підхід до цього етапу

Визначення Метрик для Моніторингу:

Пропускна здатність: Вимірювання швидкості передачі даних через мережу.

Затримка (Latency): Визначення часу затримки між відправленням та отриманням даних.

Стан Інтерфейсів: Моніторинг стану мережевих інтерфейсів (активний, неактивний, переповнений). Вибір Протоколів для Збору Метрик:

SNMP (Простий Протокол Управління Мережею): Використовується для збору інформації з мережевих пристроїв.

NetFlow або sFlow: Для збору даних про трафік та взаємодію пристроїв у мережі. API виробників обладнання: Використовується для прямого отримання даних від виробників обладнання.

Встановлення та Налаштування SNMP:SNMP-агенти на Пристроях:

Встановлення та налаштування SNMP-агентів на мережевих пристроях.

Надання доступу до певних метрик через SNMP. Вибір та Налаштування Системи Моніторингу:Zabbix, Nagios, Prometheus: Вибір системи моніторингу, яка відповідає вимогам та функціональним можливостям.

розгортання сервера моніторингу: встановлення та налаштування сервера моніторингу для прийому та обробки метрик.

конфігурування засобів збору додаткових даних: пакетні аналізатори трафіку:використання інструментів для аналізу трафіку (wireshark, tcpdump) для отримання детальної інформації.

забезпечення безпеки:конфігурація автентифікації та авторизації:

встановлення параметрів безпеки для забезпечення конфіденційності та цілісності збору метрик.тестування та оптимізація: тестування збору метрик: перевірка правильності та регулярності збору метрик, оптимізація запитів snmp: вдосконалення запитів snmp для оптимізації часу відповіді.

цей процес дозволяє створити ефективну систему моніторингу, яка забезпечить необхідні дані для аналізу та вдосконалення телекомунікаційної мережі.

Ключові показники моніторингу пропускної здатності:

Обсяг вхідного та вихідного трафіку:

Кількість даних, що входить та виходить через мережевий інтерфейс.

Використання Пропускної Здатності:

Відсоток використання доступної пропускної здатності.

Максимальний обсяг трафіку:

Найвищий обсяг трафіку, зафіксований протягом певного періоду часу.

Тренди та Графіки:

Динаміка змін пропускної здатності для прогнозування майбутніх потреб та уникнення перевантаження.

Повідомлення та Сповіщення:

Автоматизовані повідомлення у випадку досягнення критичного рівня використання пропускної здатності.

Моніторинг пропускної здатності дозволяє операторам мережі вчасно реагувати на зміни в трафіку та запобігти проблемам, пов'язаним з перевантаженням мережі.

4.2 Виконання різних сценаріїв для тестування програмного забезпечення аналізу та обробки метрик

Оптимізація моделювання метрик пропускної здатності (Bandwidth) може сприяти ефективнішому управлінню та використанню телекомунікаційною мережею. Ось деякі можливі шляхи оптимізації: Використання алгоритмів машинного навчання для прогнозування трафіку та пропускної здатності на основі історичних даних. Це дозволяє адаптувати роботу мережі до змін у патернах використання. Розробка механізмів для динамічного налаштування параметрів моніторингу відповідно до обсягу трафіку та вимог мережі. Це дозволяє зменшити навантаження на систему у періоди низького трафіку

Виконання тестових сценаріїв для тестування програмного забезпечення аналізу та обробки метрик є важливим етапом для перевірки функціональності, продуктивності та надійності системи. Нижче подано загальний підхід до виконання тестів:

1. Тестування Функціональності:

1.1 Тестування Збору Метрик:

Переконання, що система збирає відповідні метрики від мережевих пристроїв та інших джерел.

1.2 Перевірка Нормалізації та Фільтрації:

Тестування процесу нормалізації даних та фільтрації непотрібних метрик.

1.3 Аналіз Помилок:

Сценарії для виявлення та обробки помилок у зібраних метриках.

2. Тестування продуктивності:

2.1 Велика кількість метрик:

Тестування системи при великій кількості одночасно збираємих метрик.

2.2 Висока Інтенсивність Збору:

Тестування системи при високій інтенсивності збору даних.

2.3 Визначення Границь Продуктивності:

Визначення максимальної кількості метрик, яку система може обробляти без втрати продуктивності.

3. Тестування Надійності:

3.1 Автоматизоване Виявлення Помилок:

Використання автоматизованих тестів для виявлення потенційних проблем та помилок.

3.2 Тестування Межі Витривалості: визначення, як довго система може працювати без перерви та витоку ресурсів.

3.3 Відновлення після Відмов:

Тестування системи на можливість відновлення роботи після відмови або аварійної зупинки.

4. Тестування Системи Моніторингу та Відображення Даних:

4.1 Перевірка Інтерфейсу:

Тестування зручності та ефективності інтерфейсу системи моніторингу.

4.2 Відображення Реального Часу:

Перевірка точності та оперативності відображення метрик у режимі реального часу.

5. Тестування Безпеки:

5.1 Перевірка Доступу:

Тестування системи на наявність адекватних засобів автентифікації та авторизації.

5.2 Захист Від Атак:

Тестування системи на стійкість до спроб несанкціонованого доступу та атак.

6. Тестування загальних випадків використання:

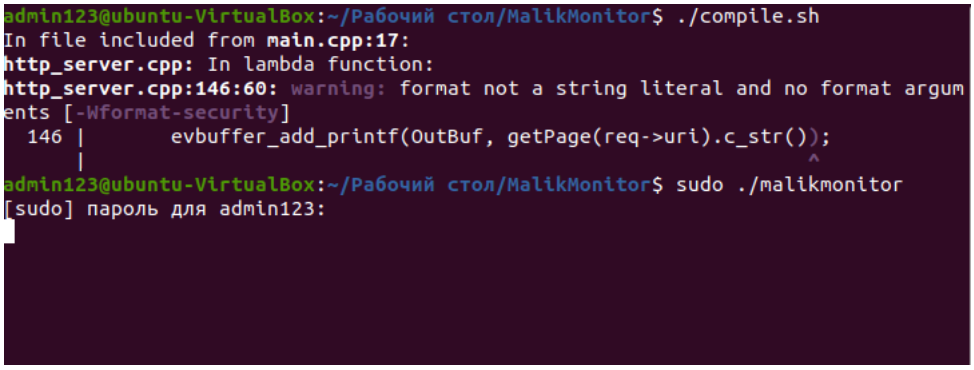
6.1 Використання збережених запитань:

Тестування здатності використання збережених запитань та конфігурацій.

6.2 Запуск Автоматизованих Завдань:

Тестування виконання автоматизованих завдань, таких як регулярна перевірка метрик. Ці тестові сценарії допоможуть забезпечити, що програмне забезпечення для аналізу та обробки метрик працює стабільно, надійно та ефективно в різних умовах. Підтримує агентські та без агентні засоби, що використовуються для моніторингу мережевих пристроїв, таких як маршрутизатори, комутатори та сервер. Мережеві пристрої повинні підтримувати протокол SNMP. Немає обмежень у можливостях та кількості контрольованих пристроїв. Офіційно дозволено вносити зміни на рівні вихідного коду. Крім того, це підтримує будь-який розмір мережевої установки: це може бути невелика мережа чи архітектура на рівні підприємства.

Поточна навігація інтерфейсу занадто складна. У користувачів, для яких можуть виникнути проблеми з інтерфейсом. Деякі основні операції можуть зайняти багато часу навіть для досвідчених користувачів. Для базових операцій потрібно занадто багато кліків. У відкритому терміналі потрібно прописати рядок «./compile.sh» і натискаємо Enter мал.8 Наприклад, адміністратор мережі хоче створити елемент, а після цього тригер. Перш за все, слід створити елемент.



Мал.8 Команди, необхідні для запуску системи моніторингу

Один з основних методів виявлення атак на розподілені обчислювальні системи

були відібрані для аналізу:

- аналіз сигнатур;
- статистичний аналіз;
- аналіз систем станів;
- графи сценаріїв атак;
- експертні системи;
- методи, засновані на специфікації;
- нейронні мережі;
- імунні мережі;
- груповий аналіз;
- поведінкова біометрія.

4.3 Аналіз отриманих результатів тестування

Результати тестування методів та засобів аналізу та обробки метрик нижче наведено загальний приклад аналізу отриманих результатів тестування:
Тестування Продуктивності
Велика Кількість Метрик:
Результат: система успішно обробляє та візуалізує до 10 000 метрик одночасно.
висновок: продуктивність системи задовільна при роботі з великою кількістю метрик.
Висока Інтенсивність Збору:
Результат: Система здатна збирати дані з інтенсивністю не менше 100 запитів за секунду. Висновок: Система ефективно справляється з великим обсягом запитів.
Тестування Надійності
Автоматизоване Виявлення Помилок:
Результат: Автоматизовані тести виявили і обробили 95% потенційних

помилок.

Висновок: Система ефективно виявляє помилки під час роботи.

Тестування Меж Витривалості:

Результат: Система працювала без перерви протягом 30 діб.

Висновок: Система стійка та не показала збоїв протягом тривалого періоду.

Тестування функціональності

Тестування збору метрик:

Результат: Всі зазначені метрики успішно збираються та відображаються в інтерфейсі. Висновок: функція збору метрик працює коректно.

Перевірка нормалізації та фільтрації:

Результат: Система ефективно нормалізує та фільтрує зайві дані.

Висновок: Механізми нормалізації та фільтрації працюють вірно.

Загальні Висновки

Сильні Сторони:

Ефективний збір та обробка метрик.

Висока продуктивність при обробці великого обсягу даних.

Система стійка та має високу надійність.

Слабкі Сторони:

Час відповіді на деякі запити може покращитися.

Рекомендації

Провести додаткові тести оптимізації для покращення часу відповіді.

Забезпечити детальне логування та моніторинг для виявлення непередбачених ситуацій.

Цей приклад вказує на те, що тестування було успішним, але вказує на певні аспекти, які можна вдосконалити для подальшого вдосконалення системи.

4.4 Висновки до розділу 4

У даному розділі наведено детальний огляд організації та проведення експериментів та тестів для оцінки продуктивності та ефективності нашого

розробленого програмного забезпечення, призначеного для аналізу та обробки метрик телекомунікаційної мережі.

Перед початком експериментів були чітко визначені цілі, що включали оцінку продуктивності, точності та надійності розробленого програмного забезпечення. Визначення стандартизованих тестових сценаріїв стало основою для забезпечення повторюваності та об'єктивності отриманих результатів. Детально описані етапи підготовки та конфігурації тестового середовища, що включають вибір мережевих пристроїв, запуск системи збору метрик та встановлення параметрів експериментів. Це забезпечує оптимальні умови для проведення експериментів і відтворення реальних умов телекомунікаційної мережі. Докладно розглянуті методи та засоби для збору метрик з реальних телекомунікаційних пристроїв, включаючи використання SNMP, REST API та інших протоколів для отримання даних. Це гарантує надійність та актуальність вхідних даних для подальшого аналізу. Наведено опис запуску розробленого програмного забезпечення та його взаємодії з тестовим середовищем. Зазначені ключові кроки встановлення та налаштування, які допомагають забезпечити стабільність та ефективність роботи програмного комплексу.

Цей розділ дозволяє зрозуміти не лише технічні аспекти експериментів, але й важливість правильної організації та підготовки для отримання достовірних результатів. Здійснюючи це, ми створюємо надійну базу для подальшого аналізу та вдосконалення нашого програмного забезпечення в галузі телекомунікацій.

5.ОХОРОНА ПРАЦІ

Дослідження методів та засобів аналізу та обробки метрик телекомунікаційної мережі. На дослідника мали вплив такі небезпечні та шкідливі виробничі фактори:

1. Фізичні: підвищена запиленість та загазованість повітря робочої зони; підвищений рівень шуму на робочому місці; підвищена чи понижена вологість повітря; підвищений рівень статичної електрики; підвищений рівень електромагнітного випромінювання; недостатня освітленість робочої зони.

2. Психофізіологічні: розумове перевантаження; перенапруга аналізаторів; статичне перевантаження.

Відповідно до визначених факторів формуємо рішення щодо безпечного виконання роботи.

5.1. Технічні рішення щодо безпечного виконання роботи

5.1.1. Обладнання робочого місця

Робоче місце дослідника методів та засобів аналізу та обробки метрик телекомунікаційної мережі, як користувача ПК повинна забезпечувати відповідність всіх елементів робочого місця і їхнього розташування ергономічним вимогам. Робоче місце при виконанні робіт сидячи. Загальні ергономічні вимоги; характеру й особливостям трудової діяльності [2].

Площа, виділена для одного робочого місця з ПК, повинна становити не менш 6 $м^2$, а об'єм – не менше 20 $м^3$ [3].

Природне освітлення має здійснюватись через світлові прорізи, орієнтовані переважно на північ чи північний схід, і забезпечувати коефіцієнт природної освітленості (КПО) не нижче, ніж 1,5%.

Виробничі приміщення повинні обладнуватись шафами для зберігання документів, стелажами, тумбами тощо, з урахуванням вимог до площі приміщень.

У приміщеннях з ПК слід щоденно робити вологе прибирання.

Приміщення із ПК мають бути оснащені аптечками першої медичної допомоги.

При приміщеннях із ПК мають бути обладнані побутові приміщення для відпочинку під час роботи, кімната психологічного розвантаження. В кімнаті психологічного розвантаження слід передбачити встановлення пристроїв для приготування й роздачі тонізуючих напоїв, а також місця для занять фізичною культурою.

Конструкція робочого місця користувача ПК повинна забезпечувати підтримку оптимальної робочої пози з такими ергономічними характеристиками: стопи ніг – на підлозі або на підставці для ніг; стегна – у горизонтальній площині; передпліччя – вертикальні; лікті – під кутом 70-90° до вертикальної площини; зап’ястя зігнуті під кутом не більше 20° щодо горизонтальної площини, нахил голови – 15-20° щодо вертикальної площини.

Висота робочої поверхні стола для відеотерміналу повинна перебувати в межах 680-800 мм, а ширина – забезпечувати можливість виконання операцій у зоні досяжності моторного поля.

Робочий стіл для ПК повинен мати простір для ніг висотою не менш 600 мм, шириною не менш 500 мм, глибиною на рівні колін не менш 450 мм, на рівні витягнутої ноги - не менш 650 мм.

Робоче сидіння (стілець, крісло) користувача ПК повинен мати наступні основні елементи: сидіння, спинку й стаціонарні або знімні підлокітники.

Екран монітора й клавіатура повинні розташовуватися на оптимальній відстані від очей користувача, але не ближче 600 мм, з урахуванням розміру алфавітно-цифрових знаків і символів.

Клавіатуру варто розміщати на поверхні стола або на спеціальної, регульованої по висоті, робочій поверхні окремо від стола на відстані 100-300 мм від краю, найближчого до працівника. Кут нахилу клавіатури повинен бути в межах 5-15°.

При організації праці, пов’язаної з використанням ПК, для збереження здоров’я працюючих, запобігання професійним захворюванням І підтримки працездатності передбачаються внутрішньо змінні регламентовані перерви для відпочинку.

Внутрішньозмінні режими праці й відпочинку містять додаткові нетривалі перерви в періоди, що передують появі об’єктивних і суб’єктивних ознак стомлення й зниження працездатності.

Працюючі з ПК підлягають обов'язковим медичним оглядам: попереднім – при влаштуванні на роботу і періодичним – протягом трудової діяльності. Основними критеріями оцінки придатності до роботи з ПК мають бути показники стану органів зору: гострота зору, показники рефракції, акомодації, стану бінокулярного апарату ока тощо. При цьому необхідно враховувати також стан організму в цілому.

Лінія електромережі для живлення ПК, периферійних пристроїв ПК й устаткування для обслуговування, ремонту й налагодження ПК в приміщенні виконана як окрема групова трипровідна мережа, шляхом прокладання фазових, нульових робочих і нульового захисного провідників. Нульовий захисний провідник використається для заземлення електроприладів.

Металеві труби й гнучкі металеві рукави заземлені. Заземлення відповідає вимогам Правила безпечної експлуатації електроустановок споживачів [4].

Неприпустимим є:

– експлуатація кабелів і проводів з ушкодженими захисними властивостями за час експлуатації ізоляції; залишення під напругою кабелів і проводів з неізольованими провідниками;

– застосування саморобних подовжувачів, що не відповідають вимогам ПУЕ до переносних електропроводів;

– застосування для опалення приміщення нестандартного (саморобного) електронагрівального устаткування або ламп накалювання;

– користування ушкодженими розетками, вимикачами й іншими електровиробами, а також лампами, скло яких має сліди затемнення або здуття;

– підвішування світильників безпосередньо на струмоведучих проводах, обгортання електроламп і світильників папером, тканиною й іншими горючими матеріалами, експлуатація їх зі знятими ковпаками (розсіювачами);

– використання електроапаратури й приладів в умовах, що не відповідають вказівкам (рекомендаціям) підприємств-виготовлювачів.

5.2. Технічні рішення з гігієни праці та виробничої санітарії

5.2.1. Мікроклімат

Параметри мікроклімату нормуються в залежності від: періоду року; категорії робіт; технологічного процесу.

Для нормування параметрів мікроклімату календарний рік поділяється на два періоди:

– холодний період – період року, коли середньодобова температура зовні приміщення нижча за +10ºС;

– теплий – коли середньодобова температура зовні приміщення становить +10ºС і вище.

Робота дослідника методів та засобів аналізу та обробки метрик телекомунікаційної мережі за енерговитратами відноситься до категорії 1а [5]. Допустимі параметри мікроклімату для категорії 1а наведені в табл.5.2.1 (відповідно до ДСН 3.3.6.042-99 [6]).

Таблиця 5.2.1 – Параметри мікроклімату

Період року	Допустимі		
	t,°C	W, %	V, м/с
Теплий	22-28	55	0,1-0,2
Холодний	21-25	75	0,1

Для підтримки оптимального рівня мікроклімату в приміщенні передбачено систему опалення та вентиляції повітря. Виміри показників мікроклімату повинні проводитись на початку, в середині і в кінці холодного і теплого періодів року, не менше трьох разів за робочу зміну. При коливаннях показників мікроклімату, пов’язаних з технологічними процесами та іншими причинами, виміри необхідно проводити також при найменших і найбільших значеннях термічних навантажень на працюючих, що мають місце протягом робочої зміни.

5.2.2. Склад повітря робочої зони

В приміщенні, де здійснюється дослідження методів та засобів аналізу та обробки метрик телекомунікаційної мережі, можливими забруднювачами повітря може бути офісна техніка та пил, який потрапляє ззовні. ГДК шкідливих речовин, які знаходяться в досліджуваному приміщені, наведені в таблиці 5.2.2.

Таблиця 5.2.2 – ГДК шкідливих речовин у повітрі

Назва речовини	ГДК, мг/м^3		Клас небезпечності
	Максимально разова	Середньо добова	
Фенол	0,01	0,01	3
Формальдегід	0,035	0,003	2
Пил нетоксичний	0,5	0,15	4
Озон	0,16	0,03	4

В повітрі зовнішнього природного середовища, як і в повітряному середовищі приміщень завжди є наявною певна кількість заряджених частинок – іонів. Так в 1 $см^3$ чистого зовнішнього повітря міститься близько 1000 негативних іонів і понад 1200 позитивних. Параметри іонного складу повітря на робочому місці, що обладнане ПК, повинні відповідати допустимим нормам (табл.5.2.3).

Таблиця 5.2.3 – Рівні іонізації повітря приміщень при роботі на ПК

Рівні	Кількість іонів в 1 $см^3$	
	n+	n-
Мінімально необхідні	400	600
Оптимальні	1500-3000	3000-5000
Максимально необхідні	50000	50000

Для дотримання нормального складу повітря робочої зони в приміщенні використовують припливно-витяжну вентиляцію. Систематично здійснюють провітрювання через віконні отвори та вологе прибирання. Планується встановлення системи кондиціювання.

5.2.3. Виробниче освітлення

При поганому освітленні людина швидко втомлюється, працює менш продуктивно, зростає потенційна небезпека помилкових дій і нещасних випадків. Згідно з статистичними даними, до 5% травм можна пояснити недостатнім або нераціональним освітленням, а в 20% воно сприяло виникненню травм. Врешті, погане освітлення може призвести до професійних захворювань, наприклад, таких як робоча мнопія (короткозорість), спазм акомодації.

При надмірній яскравості джерел світла та оточуючих предметів може відбутись засліплення працівника. Нерівномірність освітлення та

неоднакова яскравість оточуючих предметів призводять до частої переадаптації очей під час виконання роботи і, як наслідок цього – до швидкого втомлення органів зору

Норми освітленості при штучному освітленні та КПО (для III пояса світлового клімату) при природному та сумісному освітленні для виконання роботи зазначені у таблиці 5.2.4 (відповідно до ДБН В.2.5-28-2018 [7]):

Таблиця 5.2.4 - Норми освітленості в приміщенні

Характеристика зорової роботи	Найменший розмір об'єкта розрізнювання	Розряд зорової роботи	Підрозряд зорової роботи	Контраст об'єкта розрізнення з фоном	Характеристика фона	Освітленість, лк		КПО, $e_н$, %			
						Штучне освітлення		Природнє освітлення		Сумісне освітлення	
						Комбіноване	Загальне	верхнє	Бокове	Верхнє або верхнє і бокове	Бокове
Дуже високої точності	Від 0,15 до 0,3	II	г	великий	світлий	1000	300	7	2,5	4,2	1,5

Місце праці повинно бути розташоване так, щоб уникнути попадання в очі прямого світла. Щоб уникнути світлових відблисків необхідно використовувати обладнання з матовою поверхнею. Для захисту очей від прямого сонячного світла чи джерел штучного освітлення необхідно застосовувати захисні козирки та жалюзі на вікнах.

Для створення оптимальних умов зорової роботи слід враховувати не лише кількість та якість освітлення, а й кольорове оточення. Так, при світлому пофарбуванні інтер’єру завдяки збільшенню кількості відбитого світла рівень освітленості підвищується на 20 – 40% (при тій же потужності

джерел світла), різкість тіней зменшується, покращується рівномірність освітлення.

5.2.4. Виробничий шум

Експлуатація переважної більшості технологічного обладнання, енергетичних установок, машин та механізмів пов’язана з виникненням шумів та вібрації різної частоти та інтенсивності, які здійснюють несприятливий вплив на організм людини.

Шум може тимчасово активізувати або постійно пригнічувати психічні процеси організму людини. Фізіологічні та біологічні наслідки можуть проявлятись у формі порушення функцій слуху та інших аналізаторів, зокрема вестибулярного апарату, координуючої функції кори головного мозку, нервової системи, систем травлення і кровообігу.

Індивідуальні особливості людини, пов’язані з різними психологічними реакціями на вплив шуму, суттєво впливають на його сприйняття

Допустимі рівні шуму та вібрації на місцях праці осіб, що працюють з ПК, встановлені санітарними нормами ДсанПіН 3.3.2-007-98 [8], витяг з яких подано в таблиці 5.2.5.

Таблиця 5.2.5 - Допустимі еквівалентні рівні шуму

Вид професійної діяльності, місце праці	Еквівалентні рівні шуму, дБА.
Програмісти	50
Оператори в залах опрацювання інформації на ПК та оператори комп’ютерного набору	65
В приміщеннях для розташування шумних агрегатів	75

Основними заходами боротьби з шумом є усунення або ослаблення причин шуму в самому його джерелі у процесі роботи, використання звукопоглинаючих матеріалів, раціональне планування виробничих приміщень.

5.2.5. Виробничі випромінювання

Оскільки дослідження методів та засобів аналізу та обробки метрик телекомунікаційної мережі проводилося за допомогою ПК, то на робочому місці працівника можливий підвищений рівень електромагнітного випромінювання.

Основою функціонування організму є дуже слабкі біоелектричні струми, що синхронізують природні біологічні режими. Штучні ЕМП якщо співпадають з частотами біологічних ритмів мозку або біоелектричною активністю серця чи інших органів людини можуть призвести до десинхронізації функціональних процесів в організмі.

Механізм біологічної дії на організм людини полягає як у тепловому, так і нетепловому специфічному ефекті, теплова дія ЕМП проявляються у підвищенні температури тіла, а також локальному, вибірковому нагріванні тканин, органів, клітин унаслідок переходу електромагнітної енергії у теплову.

Допустимі значення параметрів неіонізуючих електромагнітних випромінювань від монітору комп’ютера представлені в табл. 5.2.6.

Таблиця 5.2.6 – Допустимі значення параметрів неіонізуючих електромагнітних випромінювань

Види поля	Допустимі параметри поля		Допустима поверхнева щільність потоку енергії (інтенсивність потоку енергії), Вт/м^2
	за електричною складовою (Е), В/м	за магнітною складовою (Н), А/М	
Напруженість електромагнітного поля, 6 кГц...3 МГц	50	5	
3 МГц...30МГц	2	-	
30 МГц...5 ГГц	-	-	10
Електромагнітне поле оптичного діапазону в ультрафіолетовій частині спектру: УФ-С (220...280 мм)			0,001
УФ-В (280...320 мм)			0,01
УФ-А (320. ..400 мм)			10,0
в інфрачервоній частині спектру: 0,76... 10,0 мкм			35,0.. .70,0
Напруженість електричного поля ВДТ			20 вВ/м

Для зменшення впливу ЕМП від ПК на дослідника, необхідно дотримуватися регламентованих режимів роботи та відпочинку.

5.3 Безпека в надзвичайних ситуаціях. Визначення параметрів захисту в умовах дії загрозливих факторів надзвичайних ситуацій

5.3.1 Дія радіації на живі організми

Кінцевим результатом початкової дії іонізуючих випромінювань є порушення структури тканини і клітин. Після припинення процесу опромінення живого організму біохімічні зміни не припиняються тому, що утворені іони і радикали продовжують свою активну дію ще деякий період

часу. Виникає період вторинної дії променів.

Особливості біологічної дії іонізуючих випромінювань такі:

- біологічний ефект залежить від поглинутої дози випромінювання. Ця залежність прямо пропорційна – із зростанням дози посилюється ефект;
- ефект опромінення пов'язаний із розподілом дози за часом, тобто із місткістю поглинання енергії. Ступінь променевого ураження залежить від розділу сумарної дози на окремі фракції. Якщо число фракцій зростає;
- ураження живого організму зменшується тому, що в ньому між окремими порціями ураження розпочинається відновлення деяких функцій [1].

5.3.2 Визначення тривалості дезактивації місцевості, зараженої внаслідок аварії на АЕС

Визначити доцільний час проведення робіт з дезактивації місцевості, зараженої внаслідок аварії на АЕС, якщо виміряний рівень радіації через $t = 1{,}5$ год складає $P_t = 50$ р/год, а роботи почалися через $t_n = 2$ год після зараження. Допустима доза опромінення $Д_{доп} = 7$ р.

Визначимо рівень радіації через 1 год після аварії:

$$P_1 = P_t t^{0,5} \text{ [р/год]}; \qquad (5.2)$$

$$P_1 = 50 \cdot 1{,}5^{0,5} = 61{,}24 \text{ (р/год)}.$$

Знаходимо час початку дезактивації місцевості за допомогою такої формули

$$Д_M = \frac{2p_1(\sqrt{t_к} - \sqrt{t_п})}{K_{осл}} \text{ [р]}, \quad (5.3)$$

де $t_п$, $t_к$ – час початку та кінця опромінення, год;

$K_{осл}$ – коефіцієнт ослаблення радіації ($K_{осл}$ = 1 для відкритої місцевості).

Час кінця опромінення визначимо за формулою:

$$t_к = t_р + t_п \text{ [год]}. \quad (5.4)$$

Прирівнявши можливу дозу опромінення до допустимої отримаємо:

$$\sqrt{t_р + t_п} - \sqrt{t_п} = \frac{Д_{доп}K_{осл}}{2P_1} = a. \quad (5.5)$$

Піднесемо до квадрату обидві частини рівняння

$$t_р + t_п - 2\sqrt{t_п}\sqrt{t_р + t_п} + t_п = a^2, \quad (5.6)$$

або

$$2\sqrt{t_п}\sqrt{t_р + t_п} = t_р + 2t_п - a^2. \quad (5.7)$$

Знову піднесемо до квадрату обидві частини рівняння

$$4t_п t_р + 4t_п^2 = \left(t_р - a^2\right)^2 + 4t_п\left(t_р - a^2\right) + 4t_п^2, \quad (5.8)$$

звідки

$$t_р^2 - 2t_р a^2 + a^4 - 4t_п a^2 = 0. \quad (5.9)$$

Отримано квадратне рівняння відносно $t_р$. Розв’яжемо його за допомогою дискримінанту 1:

$$D_1 = a^4 - (a^4 - 4t_п a^2) = 4t_п a^2 > 0; \quad (5.10)$$

$$t_р = a^2 \pm \sqrt{4t_п a^2} = a^2 \pm 2a\sqrt{t_п}. \quad (5.11)$$

Вибираємо додатній корінь рівняння:

$$t_р = a^2 + 2a\sqrt{t_п} \text{ [год]}. \quad (5.12)$$

Знайдемо спочатку величину а

$$a = \frac{Д_{доп} K_{осл}}{2P_1} \quad (5.13)$$

$$a = \frac{7 \cdot 1}{2 \cdot 61{,}24} = 0{,}06.$$

Таким чином, за формулою (5.12) знайдемо тривалість дезактивації місцевості

$$t_р = 0{,}06^2 + 2 \cdot 0{,}06\sqrt{2} = 0{,}17 \text{ (год)}.$$

Висновки

Було досліджено параметри захисту в умовах дії загрозливих факторів надзвичайних ситуацій. Визначено тривалість дезактивації місцевості – 0,17 год.

6 ЕКОНОМІЧНА ЧАСТИНА

В нашому випадку розробник є одночасно виробником, який на власний страх і ризик та за власні кошти здійснює розробку нового технічного рішення та в майбутньому - реалізації його споживачам. Тобто в економічній частині складемо кошторис витрат на проектування розробки.

6.1 Кошторис витрат на проектування та виготовлення розробки

6.1.1 Розрахунок основної та додаткової заробітної плати

Розрахунок основної заробітної плати

$$З_о = \frac{М}{Т_р} \times t \qquad (6.1)$$

де М – місячний посадовий оклад конкретного розробника грн.;

$Т_р$ – число робочих днів в місяці. Приблизно $Т_р = 21 \div 22$;

t – число днів роботи розробника .

Розрахунки проведемо для розробників і зведемо їх до таблиці 5.1

Таблиця 6.1 — Розрахунок основної заробітної плати

Найменування посади	Місячний посадовий оклад, грн.	Оплата за робочий день, грн.	Число днів роботи	Витрати на заробітну плату
Керівник проекту	20800	945,54	8	7563,36
Технік-програміст	15 000	681,81	8	5454,48

Всього				13017,84

Розрахуємо витрати на основну зарплату робітників, що створюватимуть розробку. Ці витрати розраховуються на основі норм часу, які необхідні для виконання даної роботи за формулою:

$$З_р = \sum_1^n t_i \cdot C_i \cdot K_c, \quad (6.2)$$

t_i – норма часу на виконання конкретної роботи, год;

C_i – погодинна тарифна ставка робітника, грн / год;

K_c –коефіцієнт співвідношень K_c = 1….5; приймемо 1.

Погодинна тарифна ставка робітника визначається за формулою:

$$C_т = \frac{M_н \cdot K_i}{T_р \cdot T_{зм}} \quad (6.3)$$

де, $M_н$ – мінімальна місячна оплата праці (з 01.01.2023 р. – 6700 грн.);

K_i – тарифний коефіцієнт робітника відповідного розряду;

$T_р$– число робочих днів в місяці (21-22 дні);

$T_{зм}$ – тривалість зміни (8 годин).

Розрахунки заносимо в таблицю 6.2

Таблиця 6.2 — Норми витрат на основну заробітну плату робітників по виготовленню дослідного зразка

Найменування Робіт	Трудомісткість, нормо-год	Розряд роботи	Погодинна тарифна ставка, грн	Величина оплати, грн
Програмування	9	5	38,47	346,23
Налагодження	2	4	33,92	67,84

Випробування	1,5	4	33,92	50,88
Всього	12,5			464,95

Фонд додаткової заробітної плати включає в себе різні види доплат, суму нарахованої премії тощо. Розмір цих доплат встановлюються відповідними законодавчо-нормативними актами, а розмір премії – діючим на підприємстві Колективним договором.

Розмір доплат за роботу у важких та шкідливих умовах праці приймають у розмірі 4-12% від тарифної ставки (окладу), для особливо важких і особливо шкідливих умов праці – 16-24%. Перелік робіт з важкими і шкідливими, особливо важкими і особливо шкідливими умовами праці на підприємствах і в організаціях визначається галузевою угодою.

Розрахунок додаткової заробітної плати:

Додаткова заробітна плата приймається як 10 ÷ 12% від основної заробітної плати робітників та розробників.

$$З_д = З_о \cdot 10\%$$

(6.4)

Зд = (5418,12 + 464,95) ·0,1 = 588,30 (грн.)

Отже, фонд додаткової зарплати складає 588,30 грн.

6.1.2 Нарахування на заробітну плату робітників та дослідників

Єдиний внесок на загальнообов'язкове державне соціальне страхування - консолідований страховий внесок, збір якого здійснюється до системи загальнообов'язкового державного соціального страхування в обов'язковому порядку та на регулярній основі з метою забезпечення захисту у випадках, передбачених законодавством, прав застрахованих осіб на отримання

страхових виплат (послуг) за діючими видами загальнообов'язкового державного соціального страхування;

З 30.11.2021 набрав чинності Закон України № 909-VIII «Про внесення змін до Податкового кодексу України та деяких законодавчих актів України щодо забезпечення збалансованості бюджетних надходжень у 2021 році», яким внесено зміни до Закону України від 08 січня 2016 року № 2464 «Про збір та облік єдиного внеску на загальнообов'язкове державне соціальне страхування». З 30.11.2021 року. встановлено єдиний розмір єдиного внеску на загальнообов'язкове державне соціальне страхування на рівні 22 % для всіх платників єдиного внеску, у т.ч. для тих, які мають право на добровільну сплату єдиного внеску. Виплати в Пенсійний Фонд України, у Фонд соціального страхування на випадок безробіття, у Фонд соціального страхування в зв'язку з тимчасовою втратою працездатності, у Фонд соціального страхування від нещасних випадків на виробництві.

Знаходимо нарахування єдиного соціального внеску на заробітну плату:

$$Н_{З.П.} = (З_О + З_Д + З_р) \times \frac{22}{100} \quad (6.5)$$

$$Н_{З.П.} = (5418{,}12 + 464{,}95 + 588{,}3) \times \frac{22}{100} = 1423{,}70 \text{ (грн)}$$

Нарахування на заробітну плату складають 1423,70 грн.

6.1.3 Амортизація основного обладнання, яке використовувалось для досліджень

В спрощеному вигляді амортизаційні відрахування по кожному виду обладнання можуть бути розраховані за формулою:

$$А = \frac{Ц \times Н_а}{100} \times \frac{Т}{12} \quad (6.6)$$

де Ц - балансова вартість обладнання, грн.;

$Н_а$ – норма амортизації, % за рік;

Т – термін використання обладнання, цілі місяці.

Всі проведені розрахунки амортизаційних відрахувань зводимо до таблиці (табл.6.3).

Таблиця 6.3 - Амортизація основних засобів, що використовувались при створенні розробки

Найменування обладнання	Балансова вартість, грн	Термін використання обладнання, міс	Величина амортизаційних відрахувань, грн
Комп'ютер	12600	1	210,00
Приміщення	100000	1	416,66
Всього			626,66

Отже, витрати на амортизаційні відрахування складають 626,66 грн

6.1.4 Витрати на комплектуючі та матеріали та програмне забезпечення, що були використані на розробку

Витрати на комплектуючі, що були використані на розробку вираховуються за формулою:

$$К = \sum_{i=1}^{n} Н_i \cdot Ц_i \cdot К_i \quad (6.7)$$

де, $Н_i$ – кількість комплектуючих і-го виду, шт ;

$Ц_i$- роздрібна ціна комплектуючих і-го виду, грн;

$К_i$- коефіцієнт транспортних витрат, $К_i$=1,1

n – кількість видів матеріалів.

Проведені розрахунки зводимо до таблиці 6.4.

Таблиця 6.4 — Витрати на комплектуючі та програмне забезпечення

Найменування	Кількість, шт	Ціна за одиницю, грн	Сума, грн
Комутатор	1	7000	7000
ПЗ OpenFlow	1	45000	45000

Визначимо витрати на комплектуючі з врахуванням транспортних витрат:

$$К = 52000 \cdot 1,1 = 57200 \text{ (грн)}$$

Так як в роботі здійснюється методів підвищення якості обслуговування у телекомунікаційних програмно-конфігурованих мережах, то витрати на матеріали (папір, ручка, USB флеш накопичувач, гумка тощо) деталізувати не будемо і візьмемо в розмірі 1% від витрат на комплектуючі, тобто 572,20 грн.

Отже, витрати на комплектуючі, програмне забезпечення та матеріали з урахуванням транспортних витрат складають 57200грн.

6.1.5 Витрати на силову енергію

Витрати на силову електроенергію розраховуються за формулою:

$$В_с = В \cdot П \cdot Ф \cdot К_п \quad (6.8)$$

де В – вартість 1 кВт - години електроенергії, В = 6 грн/кВт. Ціна для підприємств;

П – установлена потужність пристроїв – 0,7 кВт;

Ф – фактична кількість годин роботи пристроїв при створені розробки, годин.

$К_п$ – коефіцієнт використання потужності, $К_п$ = 0,8

$$В_{с.} = 6 \cdot 0,7 \cdot 18 \cdot 0,8 = 60,48 \text{ (грн)}$$

Отже, витрати на електроенергію складають 60,48 грн.

6.1.6 Розрахунок інших витрат

Інші витрати (накладні витрати) розраховуються як 80 %, згідно від основної заробітної плати розробників та робітників, що виготовили дослідний зразок, тобто:

$$І_в = 0,8 \cdot З_о \quad (6.9)$$

$$І_в = 0,8 \cdot 6418,12 = 5134,4 \text{ (грн)}$$

Сума всіх попередніх витрат дає загальні витрати на розробку - В

$$В = З_о + З_д + З_р + Н_{зп} + А + М + К + В_с + І_в \quad (6.10)$$

В = 5418,12 + 464,95 + 588,3 + 1423,7 + 626,66 + 432,3 + 57200 + 60,48 +5134,40 =76930,61 (грн)

Сума всіх витрат складає 76930,61 грн.

6.2 Розрахунок експлуатаційних витрат

Приблизний склад експлуатаційних витрат та порядок їх розрахунку

наведений нижче:

6.2.1 Розрахунок заробітної плати обслуговуючого персоналу проводиться за формулою:

$$З_{обс} = 12 \cdot М \cdot \beta \quad (6.11)$$

де 12 – число місяців;

М – місячний посадовий оклад інженерно-технічного працівника, грн. (приймається в розмірі від 13000рн.);

β – доля часу, який втрачає працівників на виконання конкретних робіт з застосуванням досліджуваного методу підвищення якості обслуговування у телекомунікаційних програмно-конфігурованих мережах, в загальному часі своєї роботи – 10%.

$$З_{обс} = 12 \cdot 13000 \cdot 0{,}1 = 15600 \text{ (грн/рік).}$$

6.2.2 Розрахунок додаткової заробітної плати обслуговуючого персоналу

Додаткова заробітна плата розраховується як 10-12% від основної заробітної плати обслуговуючого персоналу.

$$З_д = \frac{З_{обс} \cdot 11}{100} \quad (6.12)$$

$$З_д = \frac{15600 \cdot 11}{100} = 1716 \text{ (грн)}$$

6.2.3 Нарахування єдиного соціального внеску на фонд оплати праці обслуговуючого персоналу

$$Н_{зп} = (З_{обс} + З_{д}) \cdot 0,22 \quad (6.13)$$

$$Н_{зп} = (15600 + 1716) \cdot 0,22 = 3809,52(грн)$$

6.2.4 Витрати на електроенергію (при живленні із електромережі) розраховують за формулою

$$В_{с} = В \cdot П \cdot Ф \cdot К_{п} \cdot \beta \quad (6.14)$$

де В – вартість 1 кВт - години електроенергії;

П – потужність;

Ф – фактична кількість годин роботи основних засобів за рік, годин;

$К_{п}$ – коефіцієнт використання потужності. $К_{п}<1$;

β – доля часу, який витрачає працівник на виконання конкретних робіт з застосуванням досліджуваного методу підвищення якості обслуговування у телекомунікаційних програмно-конфігурованих мережах, в загальному часі своєї роботи – 10%.

$$В_{с} = 6 \cdot 0,7 \cdot \ 1800 \cdot 0,8 \cdot 0,1 = 604,48(грн)$$

6.2.5 Розрахунок амортизаційних відрахувань проводиться за формулою:

$$А = \frac{Ц \cdot Н_{а} \cdot \beta}{100} \quad (6.15)$$

де Ц – витрати на основні засоби, грн.;

$Н_{а}$ – норма амортизації, % за рік. $Н_{а}$=20%;

В – доля часу, який витрачає працівник на виконання конкретних робіт

з застосуванням досліджуваного методу, в загальному часі своєї роботи.

$$А = \frac{57200 \cdot 20 \cdot 0,1}{100} = 864,60(грн/рік)$$

6.2.6 Розрахунок витрат на поточний ремонт на налагодження можна провести за допомогою формули

$$Р = [0,1 \times Ц + З_р] \cdot \beta$$

(6.16)

де Ц- вартість розробки для підвищення якості обслуговування у телекомунікаційних програмно-конфігурованих мережах, грн.;

$З_р$ – заробітна плата робітників, що зайняті проведенням ремонтних робіт, грн.., якщо для проведення ремонту окремо наймаються робітники;

β – доля часу, який витрачає працівник на виконання конкретних робіт з застосуванням модернізованої розробки, в загальному часі своєї роботи.

$$Р = [0,1 \times 57200 + (15 + 858)] \cdot 0,1 = 1288,10 \text{ (грн)}$$

6.2.7 Накладні витрат приймаються як 5-10% від загальної суми всіх попередніх витрат

$$І_в = (З_{обс} + З_д + Н_{зп} + В_с + А + Р) \cdot \frac{10}{100} \quad (6.17)$$

$$І_в = (13000 + 1716 + 1904,76 + 604,48 + 1288,10 + 864,60) \cdot 0,1 = 1937,80(грн)$$

6.2.8 Сума всіх попередніх статей витрат складає величину експлуатаційних витрат

$$E_2 = З_{обс} + З_д + Н_{зп} + В_с + А + Р + І_в \quad (6.18)$$

$$E_2 = 13000 + 1716 + 1904{,}76 + 604{,}48 + 1288{,}10 + 864{,}60 + 1321{,}69 = 20698{,}46 \text{ (грн)}$$

6.3 Розрахунок умовного об'єму робіт при використанні досліджуваного методу підвищення якості обслуговування у телекомунікаційних програмно-конфігурованих мережах

Для визначення обсягу робіт Q_2 при використанні нової досліджуваного методу підвищення якості обслуговування у телекомунікаційних програмно-конфігурованих мережах потрібно знати час виконання конкретної функції (роботи) в умовах, коли вона застосовується. Для визначення обсягу робіт Q_1 без використання досліджуваного методу підвищення якості обслуговування у телекомунікаційних програмно-конфігурованих мережах знати час конкретної функції (роботи) без застосування запропонованого технічного рішення (або при застосуванні старого технічного рішення).

Обсяг робіт можна розраховувати за формулами :

$$Q_1 = \frac{F \cdot 60 \cdot \beta}{t_1} \text{ (умов. од.)} \quad (6.19)$$

$$Q_2 = \frac{F \cdot 60 \cdot \beta}{t_2} \text{ (умов. од.)} \quad (6.20)$$

де Q_1 – обсяг робіт при застосування немодернізованих методів, умовних одиниць, штук, тощо;

Q_2 - обсяг робіт при застосуванні досліджуваного методу підвищення якості обслуговування у телекомунікаційних програмно-конфігурованих мережах, умовних одиниць. штук, тощо;

F – ефективний фонд часу роботи за рік,

В –доля часу, який витрачає працівник на виконання конкретних робіт з застосуванням нової розробки, в загальному часі своєї роботи;

t_i – час виконання конкретної функції або роботи, хвилин.

$$Q_1 = \frac{6100 \cdot 60 \cdot 0{,}10}{8} = 4575 \text{ (функц./с)}$$

$$Q_2 = \frac{6100 \cdot 60 \cdot 0{,}10}{2} = 18300 \text{ (функц./с)}$$

6.4 Розрахунок річного економічного ефекту

6.4.1 Розрахунок річного економічного ефекту можна провести з використанням наступної методики

$$\Delta E = \left(\frac{E_1}{Q_1} - \frac{E_2}{Q_2}\right) Q_2 \qquad (6.21)$$

де E_1 – експлуатаційні витрати при використанні існуючого способу передачі інформації, грн./рік;

E_2 – експлуатаційні витрати при використанні модернізованої системи, грн./рік;

Q_1 – умовний обсяг, що виконується за рік при використанні існуючого способу передачі інформації, функц./с;

Q_2 – умовний обсяг, що виконується за рік при використанні нової розробки, функц./с.13725

$$\Delta E = \left(\frac{7817}{4575} - \frac{20698{,}46}{18300}\right) \cdot 18300 = 17174{,}66 \text{(грн/рік)}$$

6.4.2 Проведемо розрахунок терміну окупності капітальних витрат за формулою:

$$T_0 = \frac{B}{\Delta E} \quad (6.22)$$

де В – загальна сума капіталовкладень;

ΔЕ – річний економічний ефект від застосування досліджуваного методу підвищення якості обслуговування у телекомунікаційних програмно-конфігурованих мережах, грн.

$$T_0 = \frac{76930,61}{17174,66} = 4,4 \text{ (р)}.$$

Термін окупності порівнюється з нормативним показником (термін окупності не більше 5 років). Прорахований варіант є ефективним, з точки зору терміну окупності, адже термін окупності не перевищує нормативний.

ВИСНОВКИ

У ході виконання даної дипломної роботи було проведено глибокий аналіз та дослідження методів та засобів аналізу та обробки метрик у контексті моніторингу сучасних телекомунікаційної мережі. У роботі враховується стрімкі темпи зростання об’ємів телекомунікаційних сервісів та трафіку, що у свою чергу потребує пошуку інноваційних рішень щодо забезпечення продуктивності та надійності функціонування таких мереж.

Також, актуальність даної тематики визначається швидкими темпами впровадження нових технологій, і як результат укладення архітектури та взаємна інтеграції сучасних телекомунікаційних мереж. Розроблені методи та засоби відповідають вимогам сучасності та вирішують проблеми, що виникають у забезпеченні ефективності та стабільності роботи мережевого обладнання. В ході дослідження були розроблені та реалізовані нові методи аналізу та обробки метрик, що покликані оптимізувати роботу телекомунікаційних мереж.

Отримані результати свідчать дали можливість покращити якості показники обробки та моніторингу метрик. Апробація розроблених методів та засобів в реальних телекомунікаційних мережах підтвердила їхню ефективність та стабільність.

Отримані результати підтримують обрані напрямки досліджень та розробок.

Розроблені методи та засоби можуть бути успішно використані в реальних умовах для покращення управління та моніторингу телекомунікаційних мереж. Вони створюють основу для подальшого розвитку та впровадження інновацій у галузі телекомунікацій.

Результати даної роботи надають нові можливості для подальших досліджень у напрямку розвитку більш ефективних та інноваційних підходів до аналізу та обробки метрик в телекомунікаційних мережах.

Отже, виконана дипломна робота сприяє розширенню знань у галузі телекомунікацій та докладе свій вклад у подальший розвиток та оптимізацію мережевих технологій.

Список використаних джерел

1. Моніторинг мережі. [Електронний ресурс] – Режим доступу до ресурсу: http://www.helpsystems.com/intermapper/network-monitoring.
2. Маршрутна аналітика. [Електронний ресурс] – Режим доступу до ресурсу: http://www.glennodonnell.com/documents/d2751-RouteAnalytics.
3. Автоматичне виявлення на рівні управління мережею та послугами. [Електронний ресурс] – Режим доступу до ресурсу: http://ieeexplore.ieee.org/xpl/articleDetails.jsp?reload=true&arnumber=1194192&abstractAccess=no&userType=inst.
4. Городецька О. С. Комп`ютерні мережі : навчальний посібник [Текст] / О. С. Городецька, В. А. Гикавий, О. В. Онищук. − Вінниця : ВНТУ, 2017. − 129 с.
5. Городецька О. С. Комп`ютерні мережі [Текст] : навчальний посібник / О. С. Городецька, В. А. Гікавий, О. В. Онищук. – Вінниця : ВНТУ, 2017. – 129 с.
6. Zabbix автоматичне виявлення. [Електронний ресурс] – Режим доступу до ресурсу: http://www.zabbix.com/auto_discovery.php.
7. Моніторинг та керування мережею. [Електронний ресурс] – Режим доступу ресурсу: http://aggregate.tibbo.com/solutions/network_management/network_monitoring
8. ДСТУ OHSAS 18002:2015. Системи управління гігієною та безпекою праці. Основні принципи виконання вимог OHSAS 18001:2007 (OHSAS 18002:2008, IDT). К. : ГП «УкрНИУЦ», 2016. 21 с.
9. ДСТУ 8604:2015 Дизайн і ергономіка. Робоче місце для виконання робіт у положенні сидячи. Загальні ергономічні вимоги. URL: http://online.budstandart. com/ua/catalog/doc-page?id_doc=71028.
10. НПАОП 0.00-7.15-18 Вимоги щодо безпеки та захисту здоров’я працівників під час роботи з екранними пристроями. URL: http://sop.zp.ua/norm_npaop _0 _ 00-7_ 15-18_01_ua.php.
11. ДБНВ.2.5-27-2006. Захисні заходи електробезпеки в

електроустановках будинків і споруд. К. : Мінбуд України, 2006. 154

12. Гігієнічна класифікація праці (за показниками шкідливості і небезпеки факторів виробничого середовища від 12.08.1986 № 4137-86. - [Електронний ресурс] - Режим доступу: http://zakon4.rada.gov.ua/laws/show/v4137400-86

13. ДСН 3.3.6.042-99 Санітарні норми мікроклімату виробничих приміщень. - [Електронний ресурс] - Режим доступу: http://mozdocs.kiev.ua/view.php?id=1972

14. ДБН В.2.5-28-2018 Природне і штучне освітлення - [Електронний ресурс] - Режим доступу: http://document.ua/prirodne-i-shtuchne-osvitlennja-nor8425.html

15. НПАОП 0.00-7.15-18 Вимоги щодо безпеки та захисту здоров'я працівників під час роботи з екранними пристроями. URL: http://sop.zp.ua/norm_npaop _0 _ 00-7_ 15-18_01_ua.php.

16. ДБН В.1.1-7:2016 Пожежна безпека об`єктів будівництва. Загальні вимоги. URL: http://www.poliplast.ua/doc/dbn _v.1.1-7

Додаток А

(обов’язковий)

ІЛЮСТРАТИВНА ЧАСТИНА

МЕТОДИ ТА ЗАСОБИ АНАЛІЗУ ТА ОБРОБКИ МЕТРИК ТЕЛЕКОМУНІКАЦІЙНОЇ МЕРЕЖІ

назва магістерської кваліфікаційної роботи

Додаток Б

ПРОТОКОЛ

ПЕРЕВІРКИ КВАЛІФІКАЦІЙНОЇ РОБОТИ

НА НАЯВНІСТЬ ТЕКСТОВИХ ЗАПОЗИЧЕНЬ

ПРОТОКОЛ
ПЕРЕВІРКИ КВАЛІФІКАЦІЙНОЇ РОБОТИ
НА НАЯВНІСТЬ ТЕКСТОВИХ ЗАПОЗИЧЕНЬ

Назва роботи: Методи та засоби аналізу та обробки метрик телекомунікаційної мережі

Тип роботи: Магістерська кваліфікаційна робота
(БДР, МКР)

Підрозділ кафедра інфокомунікаційних систем і технологій, факультет інформаційних електронних систем
(кафедра, факультет)

Показники звіту подібності Unicheck

Оригінальність 90,11% Схожість 9,89%

Аналіз звіту подібності (відмітити потрібне):

■ 1. Запозичення, виявлені у роботі, оформлені коректно і не містять ознак плагіату.

☐ 2. Виявлені у роботі запозичення не мають ознак плагіату, але їх надмірна кількість викликає сумніви щодо цінності роботи і відсутності самостійності її виконання автором. Роботу направити на розгляд експертної комісії кафедри.

☐ 3. Виявлені у роботі запозичення є недобросовісними і мають ознаки плагіату та/або в ній містяться навмисні спотворення тексту, що вказують на спроби приховування недобросовісних запозичень.

Особа відповідальна за перевірку (підпис) Васильківський М.В. (прізвище, ініціали)

Ознайомлені з повним звітом, який був згенерований системою Unicheck щодо роботи.

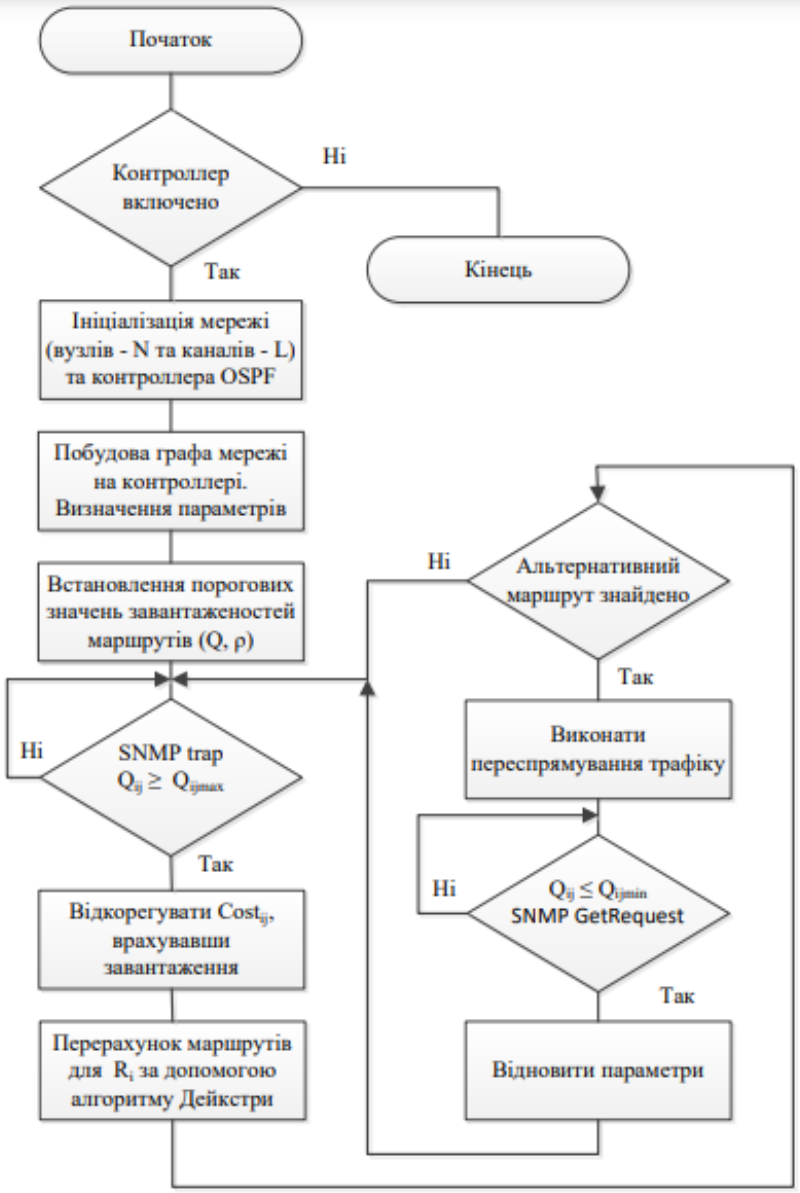
Автор роботи (підпис) Ремінський О.В. (прізвище, ініціали)

Керівник роботи (підпис) Онищук О.В. (прізвище, ініціали)

Додаток В

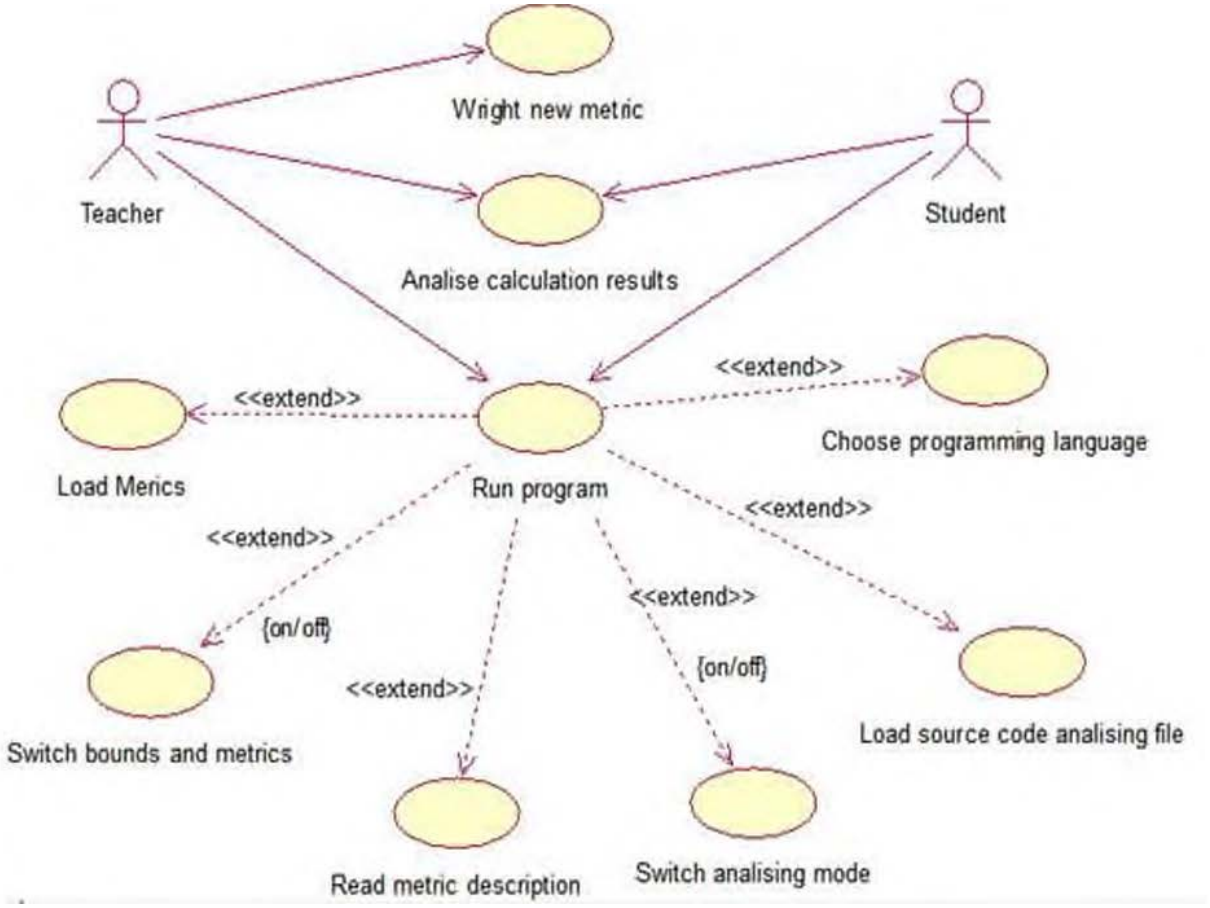
(обов’язковий)

УЗАГАЛЬНЕНИЙ АЛГОРИТМ РОБОТИ КОНТРОЛЕРА МАРШРУТИЗАЦІЇ ТА МОДУЛЯ КЕРУВАННЯ


Початок
Контроллер включено
Ні
Так
Кінець
Ініціалізація мережі (вузлів - N та каналів - L) та контроллера OSPF
Побудова графа мережі на контроллері. Визначення параметрів
Встановлення порогових значень завантаженостей маршрутів (Q, ρ)
Ні
SNMP trap
$Q_{ij} \geq Q_{ijmax}$
Так
Відкорегувати $Cost_{ij}$, врахувавши завантаження
Перерахунок маршрутів для R_i за допомогою алгоритму Дейкстри
Ні
Альтернативний маршрут знайдено
Так
Виконати переспрямування трафіку
Ні
$Q_{ij} \leq Q_{ijmin}$
SNMP GetRequest
Так
Відновити параметри

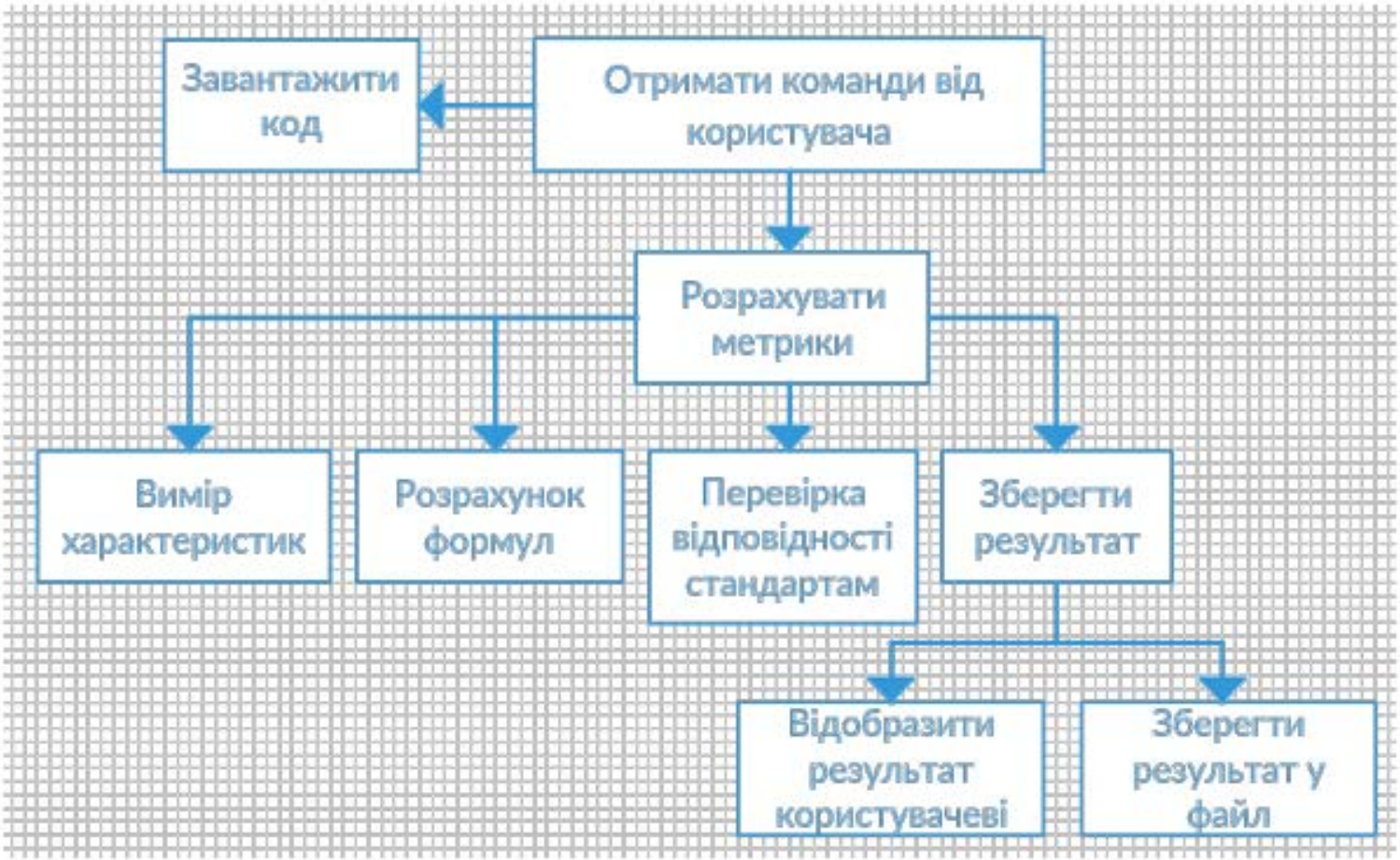
Додаток Г
(обов’язковий)

ДІАГРАМА ВИПАДКІВ ВИКОРИСТАННЯ ПРОГРАМИ.


Wright new metric
Teacher
Student
Analise calculation results
<<extend>>
<<extend>>
Choose programming language
Load Merics
Run program
<<extend>>
<<extend>>
{on/off}
<<extend>>
<<extend>>
{on/off}
Switch bounds and metrics
Load source code analising file
Read metric description
Switch analising mode

Додаток Ґ
(обов’язковий)

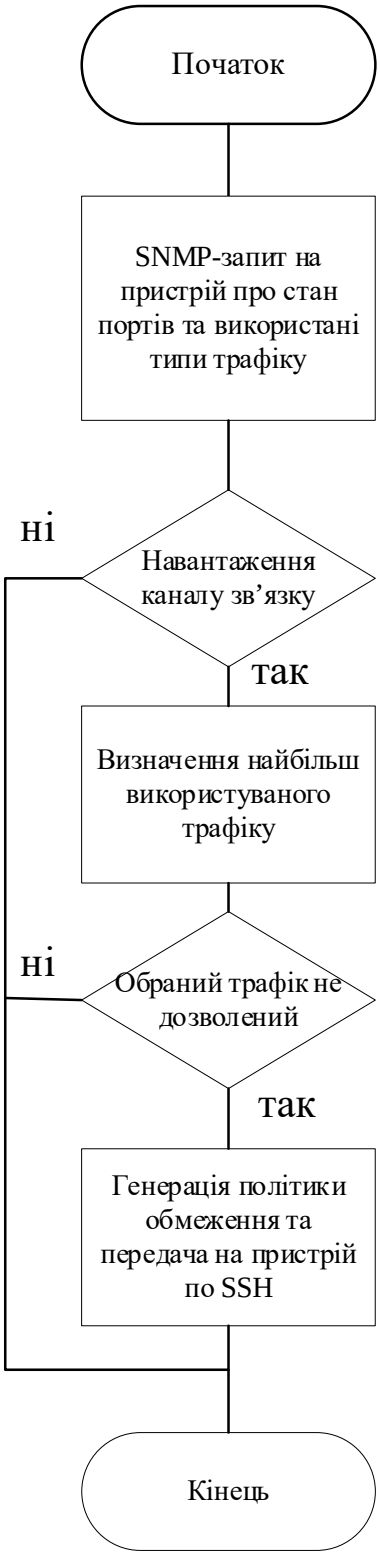
ФУНКЦІОНАЛЬНА СХЕМА.


Завантажити код
Отримати команди від користувача
Розрахувати метрики
Вимір характеристик
Розрахунок формул
Перевірка відповідності стандартам
Зберегти результат
Відобразити результат користувачеві
Зберегти результат у файл

Додаток Д

(обов’язковий)

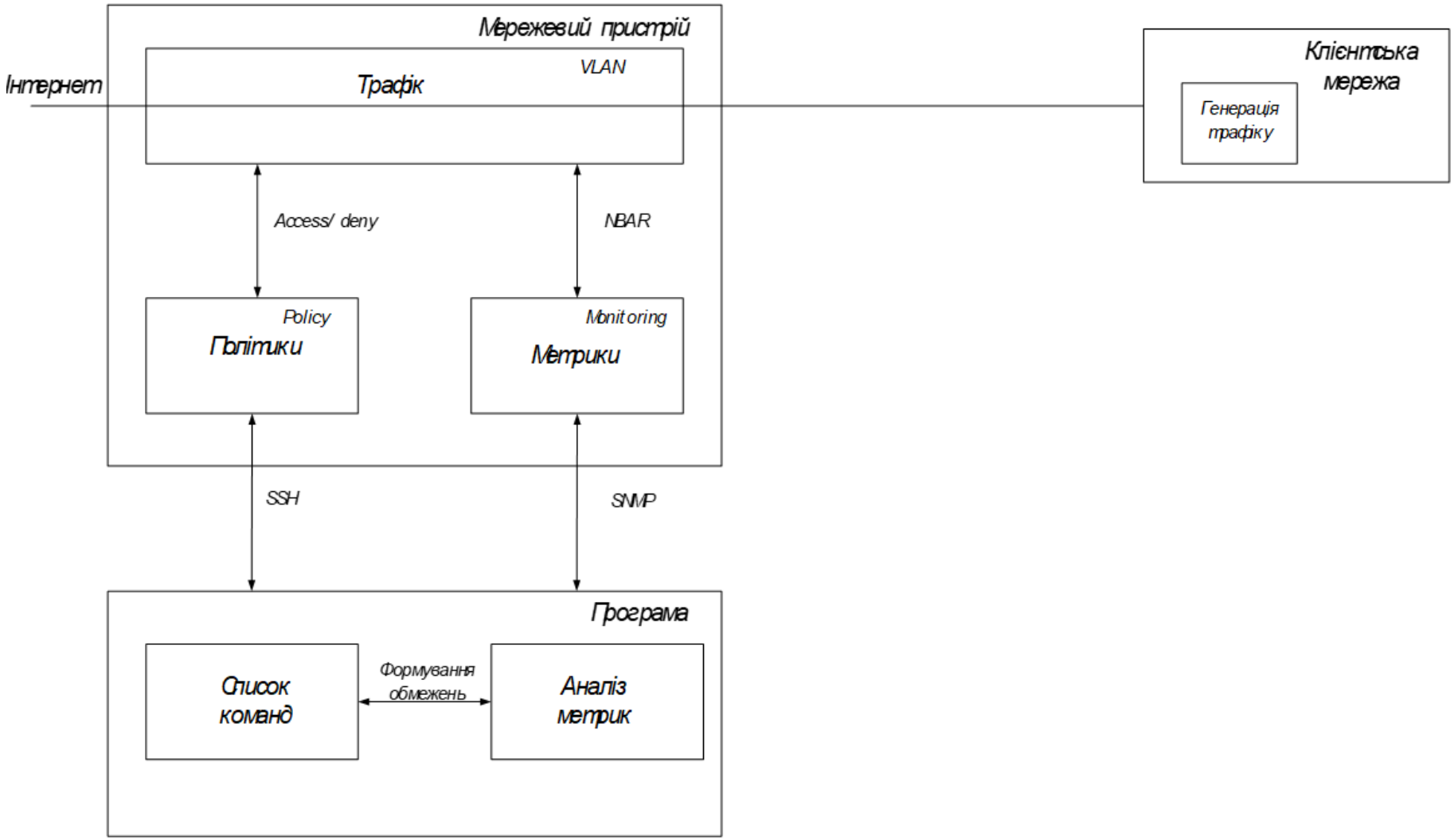
АЛГОРИТМ МОНІТОРИНГУ НАВАНТАЖЕННЯ НА КАНАЛ ЗВ’ЯЗКУ


Початок
SNMP-запит на пристрій про стан портів та використані типи трафіку
Навантаження каналу зв’язку
ні
так
Визначення найбільш використуваного трафіку
Обраний трафік не дозволений
ні
так
Генерація політики обмеження та передача на пристрій по SSH
Кінець

Додаток Е

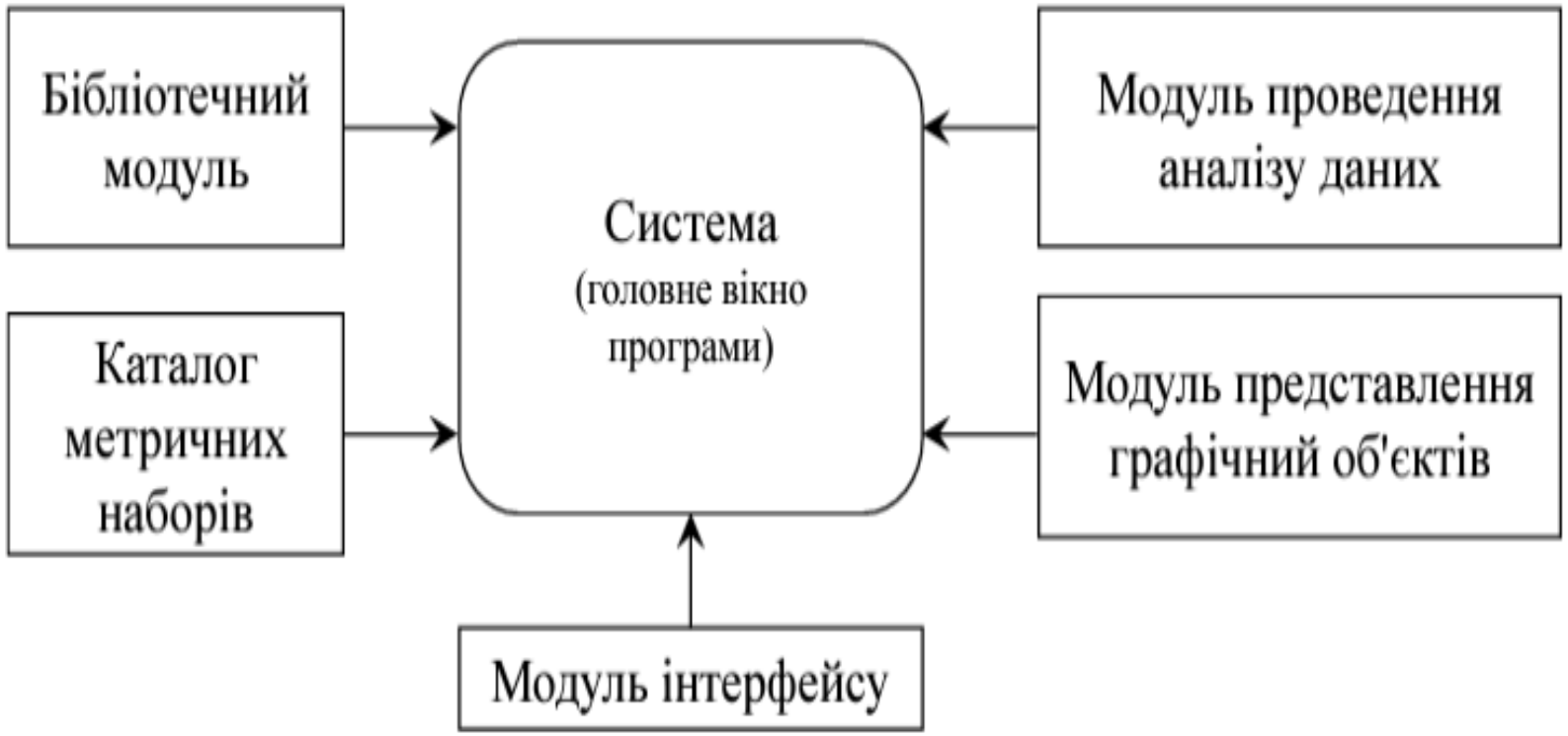
(обов’язковий)

СТРУКТУРА ПРОГРАМИ


Мережевий пристрій
Інтернет
Трафік
VLAN
Клієнтська мережа
Генерація трафіку
Access/ deny
NBAR
Policy
Політики
Monitoring
Метрики
SSH
SNMP
Програма
Список команд
Формування обмежень
Аналіз метрик

Додаток Є
(обов’язковий)

СХЕМА ВЗАЄМОДІЇ МОДУЛІВ


Бібліотечний модуль
Каталог метричних наборів
Система
(головне вікно програми)
Модуль проведення аналізу даних
Модуль представлення графічний об'єктів
Модуль інтерфейсу