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

МАГІСТЕРСЬКА КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Комплексні системи моніторингу інфраструктури телекомунікаційної мережі»

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

Керівник: к.т.н., доцент каф. ІКСТ
_____ Онищук О.В.
«18» 12 2023 р.

Опонент: д.т.н., професор каф. ІРТС
_____ Осадчук В.С.
«18» 12 2023 р.

Допущено до захисту
Завідувач кафедри ІКСТ
_____ проф. Кишак В.М.

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

Лукашину Євгену Віталійовичу .
(прізвище, ім’я, по батькові)

1. Тема роботи Комплексні системи моніторингу інфраструктури телекомунікаційної мережі
керівник роботи Онищук Олег Володимирович, 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 18 грудня 2023 року

3. Вихідні дані до роботи Швидкість передавання даних - 1 Гбіт/с; затримка передавання даних в мережі – 0,1 мс; затримка оброблення даних – 50 мс; доступність і надійність мережі – 99,99999%; щільність з'єднання в IoE мережі – 10^7 пристроїв/км^2;

4. Зміст текстової частини: Аналіз функціональних параметрів сучасних корпоративних мереж; розробка та реалізація наборів симуляцій; аналіз результатів проведених досліджень; економічна частина; охорона праці та безпека в надзвичайних ситуаціях.

5. Перелік ілюстративного матеріалу (з точним зазначенням обов’язкових креслень)
Сегмент топології корпоративної мережі спеціального призначення; схема дротового поширення сигналів з багатопроменевим ефектом; узагальнена модель провідного каналу передавання даних; алгоритм роботи дистанційно моніторингу керованої мережі.

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Спеціальна частина	Онищук О.В., професор кафедри ІКСТ	1.09.23	18.12.23
Економічна частина	Кавецький В.В. доцент каф. ЕПВМ	1.09.23	18.12.23
Охорона праці та безпека в надзвичайних ситуаціях	Дембіцька С.В. професор кафедри БЖДПБ	1.09.23	18.12.23

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 моніторингу	06.10.2023р.	
4.	Оцінювання продуктивності	27.10.2023р.	
5.	Розробка та реалізація наборів симуляцій	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	18.12.2023р.	
11.	Захист МКР ЕК	19.12.2023р.	

Студент _____ (підпис) Лукашин Є.В.

Керівник роботи _____ (підпис) Онищук О.В.

АНОТАЦІЯ

УДК 621.391

Лукашин Є. В. Комплексні системи моніторингу інфраструктури телекомунікаційної мережі – магістерська кваліфікаційна робота зі спеціальності 172 – Телекомунікації та радіотехніка, освітня програма – Телекомунікаційні системи та мережі – Вінниця: ВНТУ 2023 р. 149 – стор., 35 – рис., 13 – табл., 65 – бібл. – українською мовою.

Метою кваліфікаційної роботи є розробка методів та засобів проектування та реалізації комплексних систем моніторингу телекомунікаційних мереж. Із врахуванням промислових сценаріїв застосування моніторингу, стану інженерних систем у режимі реального часу, оперативне управління обладнанням, розмежування доступу до інформації.

Виконано дослідження моніторингу та аналізу керування телекомунікаційної мережі за допомогою інструменту Zabbix. З використанням Проксі-сервера усі зібрані дані зберігаються в буфері та надсилаються на сервер.

Ключові слова: система моніторингу; Zabbix; Проксі-сервер; телекомунікації; буфер; сервер;

ABSTRACT

UDC 621.391

Lukashyn E. V. Complex systems for monitoring the infrastructure of the telecommunication network - master's thesis on specialty 172 - Telecommunications and radio engineering, educational program - Telecommunication systems and networks - Vinnytsia: VNTU 2023. 149 - p., 35 - fig., 13 - table ., 65 - bibl. - in the Ukrainian language.

The purpose of the qualification work is to develop methods and tools for designing and implementing complex systems for monitoring telecommunication networks. Taking into account industrial monitoring application scenarios, real-time status of engineering systems, operational management of equipment, delimitation of access to information.

A study of monitoring and analysis of telecommunication network management using the Zabbix tool was carried out. Using a proxy server, all collected data is buffered and sent to the server.

Keywords: monitoring system; Zabbix; Proxy server; telecommunications; buffer; server;

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ

LLD – виявлення низького рівня

API – інтерфейс прикладного програмування

IPS є одиницею вимірювання швидкості

IDS - системи управління базами даних

WLAN - бездротова локальна мережа

LAN - локальна мережа

VPN – віртуальна приватна мережа

WAN — це телекомунікаційна мережа, яка охоплює велику територію

OSI є базовою моделлю відкритих систем

Мережевий менеджмент - системи управління мережею

Управління системою - засоби управління системою

Вбудовані системи - вбудовані системи діагностики та управління

Protocol analysers - аналізатори протоколів

IANA (Internet Assigned Numbers Authority) – присвоєння номерів в Інтернеті

User-driven security model - Керована користувачем модель безпеки

DM – розподілений моніторинг на основі вузлів

ВСТУП

Актуальність теми дослідження визначається зростаючим значенням телекомунікаційних мереж у сучасному суспільстві. Телекомунікаційні мережі використовуються для забезпечення різноманітних послуг, таких як передача даних, телефонний зв'язок, відеоконференції та багато інших. Для забезпечення стабільної та безперебійної роботи таких мереж необхідно здійснювати їх моніторинг

Сучасні телекомунікаційні мережі є складними системами, що включають в себе різноманітні компоненти, такі як обладнання, мережеві протоколи, програмне забезпечення та персонал. Для забезпечення стабільної та безперебійної роботи таких мереж необхідно здійснювати їх моніторинг.

Моніторинг телекомунікаційних мереж - це процес збору, зберігання та аналізу інформації про стан мережі та її компонентів. Метою моніторингу є виявлення проблем та несправностей в мережі на ранніх етапах їх розвитку, а також оцінка ефективності роботи мережі.

Пропускна здатність мережі може коливатися від 10 до 100 Мбіт/с; Однак адміністраторам тепер потрібно керувати не лише бездротовими мережами (понад 10 Гбіт/с), а й бездротовими мережами.

Їм потрібні більш просунуті інструменти моніторингу та аналізу мережевого трафіку, щоб підтримувати стабільність і доступність мережевої системи, наприклад, щоб своєчасно виправляти помилки в разі проблем з мережею або уникати простоїв мережі, гарантувати надійність мережі та приймати правильні рішення. в мережевому плануванні.

Сьогодні на ринку доступно багато інструментів моніторингу мережі. Більшість із них забезпечують моніторинг пропускної здатності мережі. Крім того, вони дозволяють збирати дані про продуктивність мережевих пристроїв. Відмінності між інструментами автоматизованих систем, що надаються різними постачальниками, можуть включати додаткові функції, такі як прогнозування

тенденцій і логічне групування. Крім того, різні компанії, що займаються моніторингом мережі, мають різні моделі.

На етапі аналізу, який розуміється як більш складний і інтелектуальний процес розуміння інформації, зібраної на етапі моніторингу, порівняння її з даними, отриманими раніше, і формулювання гіпотез щодо можливих причин повільної або ненадійної роботи мережі.

Завдання моніторингу виконують програмно-апаратні лічильники, тестери, мережеві аналізатори, комплексні засоби моніторингу комунікаційних пристроїв, а також агенти системи керування. Аналітична задача вимагає більш активної участі людини і використання таких складних інструментів, як експертні системи, в яких накопичується практичний досвід багатьох мережевих фахівців.

Загалом, у мене є певний досвід роботи з Zabbix, і я можу з упевненістю рекомендувати його.

Zabbix відповідає приблизно 90% вимогам до надійного інструменту моніторингу телекомунікаційної мережі. Проводить супервізію з агентом і без нього. Ви можете знайти такі функції, як низькорівневе виявлення, автоматичне виявлення та логічне групування.

Тому система моніторингу Zabbix абсолютно безкоштовна. Немає обмежень щодо можливостей і кількості керованих пристроїв. Крім того, Zabbix заснований на відкритому коді. Тому він користується потужною підтримкою.

Zabbix — це комплексний інструмент моніторингу, який може:

стежити за динамікою роботи серверів і мережевого обладнання, оперативно реагувати на аварійні ситуації та попереджати про можливі проблеми із завантаженням. Система моніторингу Zabbix може збирати статистику в певному робочому середовищі та в деяких випадках діяти певним чином.

Сервер є ядром, на якому зберігаються всі системні дані, включаючи статистичні, операційні та конфігураційні дані. Віддалено керує мережевими

сервісами та інформує адміністратора про наявні проблеми з підконтрольним обладнанням.

Проксі-сервер — це сервер, який збирає дані про доступність і продуктивність пристрою, діючи від імені сервера. Усі зібрані дані зберігаються в буфері та надсилаються на сервер. Необхідний для балансування навантаження на сервер.

Комплексні системи моніторингу телекомунікаційних мереж є найбільш ефективним способом моніторингу таких мереж. КСМТН дозволяють отримувати всебічну інформацію про стан мережі, а також автоматизувати процес моніторингу.

Об'єктом дослідження є комплексні системи моніторингу телекомунікаційних мереж.

Предметом дослідження є методи та засоби проектування та реалізації КСМТН.

Метою дослідження є розробка методів та засобів проектування та реалізації КСМТН.

Завдання дослідження.

Для досягнення поставленої мети необхідно вирішити такі завдання:

- моніторинг керування телекомунікаційними мережами;

- аналіз методики моніторингу телекомунікаційної мережі;

- загальний метод інструменту Zabbix для центрального телекомунікаційного моніторингу мережі;

- технічне рішення для збору даних та тестування продуктивності snmp для сервера Zabbix.

Структура магістерської роботи.

Магістерська робота складається з вступу, чотирьох розділів, висновків та списку використаних джерел.

РОЗДІЛ 1 МОНІТОРИНГ КЕРУВАННЯ ТЕЛЕКОМУНІКАЦІЙНИМИ МЕРЕЖАМИ

1.1 Сфера застосування

Кілька десятиліть тому інформація про стан мережі та продуктивність інфраструктури збиралася в одному місці. Роль «інтелектуального аналізатора» була покладена тільки на системних адміністраторів. Щоб мати повний огляд системи, адміністратор мав бути метою, тобто він мав контролювати все одразу. Мені знадобилося надто багато часу, щоб розібратися з деякими проблемами та прийомами. Для спрощення роботи адміністраторів і скорочення часу обробки даних в мережу введено системи моніторингу.

Моніторинг мережі – це система, яка показує низьку продуктивність мережі або несправні мережеві пристрої. Моніторинг базується на аналізі пропускної здатності, системних помилок, втрати пакетів, затримки, доступності маршрутизаторів, комутаторів і часу відповіді. При виникненні конкретного збою мережевий адміністратор повідомляється за допомогою попереджувального банера, електронної пошти, телефону тощо.

Моніторинг мережі також є стратегічним інструментом у нинішніх структурах. Це допомагає оптимізувати потік даних і виявити ненадійне обладнання. Крім того, він перевіряє потенціал пристроїв і їх умови, наприклад швидкість температури та використання. У результаті моніторинг допомагає оптимізувати продуктивність мережі та зменшити потенційний час простою. Основними перевагами оптимізованої мережі для структур є: зниження витрат на інфраструктуру, продуктивність співробітників і швидкість і надійність потоків даних.

Існує помилкова думка, що моніторинг мережі також забезпечує контроль безпеки та запобігає несанкціонованому доступу до мережі. Для цього типу моніторингу безпеки використовуються системи запобігання вторгненням (IPS) або системи виявлення вторгнень (IDS). Моніторинг мережі використовується лише для моніторингу використання та надійності мережі.

Моніторинг мережі підтримує широкий спектр пристроїв, таких як сервери, маршрутизатори, комутатори та навіть кінцеві пристрої. Крім того, його можна використовувати в усіх мережах, таких як WLAN, LAN, VPN і навіть WAN.

1.2 Типи моніторингу мережі

1.2.1 Моніторинг мережі

Інструменти моніторингу мережі пропонують широкий спектр аналітики та аналізу активності для різних типів пристроїв і служб. Це було досягнуто шляхом використання різних типів протоколів, що працюють на різних рівнях OSI.

Моніторинг мережі використовується для вимірювання загальної продуктивності мережі. Вимірювання здійснюється шляхом перевірки кількості надісланих і отриманих пакетів. Під час цього процесу вимірюється кількість проміжних пристроїв, які досягають місця призначення. Крім того, вимірюються затримки мережевих шляхів і пристроїв. З цього можна оцінити втрату пакетів, пропускну спроможність і апаратну затримку. В результаті покращується якість послуг у телекомунікаційних мережах.

Моніторинг веб-сайтів допомагає контролювати стан вашого сервера. Він вимірює час роботи сервера, продуктивність з’єднання, поточні записи DNS, пропускну здатність і навіть апаратні ресурси.

В основному використовується два види моніторингу веб-сайту: внутрішній і зовнішній. Внутрішній моніторинг відповідає за виявлення проблем, пов’язаних із внутрішньою структурою або розробкою окремих програм. За підсумкову перевірку відповідає зовнішній огляд. Моніторинг веб-сайтів відповідає за такі інтернет-протоколи, як: HTTP, HTTPS, FTP, SNMP, STPM, SSH, TELNET, POP3, DNS, SSL, TCP, UDP.

Моніторинг кінцевого користувача відбувається, коли бот періодично генерує певні дії користувача. Це означає, що він запускає спеціальний сценарій,

ніби користувач запустив меню або навіть клацнув. Якщо робот щось не може зробити, кінцевий користувач не зможе цього зробити. Останньою функцією є моніторинг на рівні коду. Ці модулі можуть виявляти затримки системних викликів, витоки пам’яті та затримки виконання SQL-запитів.

1.2.2 Аналітичний шлях

Важливою частиною моніторингу є аналіз маршруту. Аналіз маршрутизації – це набір інструментів, програм і алгоритмів, які відстежують мережеву маршрутизацію. Працює на мережевому рівні.

Routing Analytics включає наступні системні монітори та протоколи маршрутизації OSPF, IS-IS, EIGRP і BGP. У результаті цей маршрут отримує кожне повідомлення про оновлення, як і всі інші маршрутизатори. Крім того, він використовує алгоритм Дейкстри, який обчислює повну карту топології мережі, включаючи всі шляхи.

Крім того, Routing Analytics записує повну історію подій маршрутизації, які пізніше можна використовувати для усунення проблем. Загалом аналіз маршрутизації підвищує швидкість і ефективність мережі, одночасно допомагаючи зменшити витрати та підвищити продуктивність співробітників.

1.3 Значення та основні принципи методів моніторингу телекомунікаційних мереж

Управління роботою локальної мережі є основою будь-якої мережі, необхідною для підтримки її в належному стані. Моніторинг - це перший крок до керування мережею. Враховуючи важливість цієї функції, її часто відокремлюють від систем керування та здійснюють за допомогою спеціальних засобів. Такий поділ функцій контролю та керування корисний у малих та середніх мережах, для яких встановлення інтегрованої системи керування є економічно невигідним. Використання окремих інструментів моніторингу

дозволяє адміністратору помітити проблемні ділянки мережі і в цьому випадку може переналаштувати їх вручну.

Моніторинг мережі зазвичай поділяється на етапи моніторингу та аналізу.

Спочатку виконується більш проста процедура: збір основних даних про роботу: статистика кадрів і пакетів, що циркулюють в мережі, стан портів на обладнанні і т.д.

Етап аналізу передбачає більш складний і інтелектуальний процес осмислення зібраної інформації, порівняння її з попередньо отриманими даними та висновків про можливі причини повільної або неефективної роботи мережі.

Важливим завданням моніторингу є: вирішення апаратних і програмних засобів лічильників, тестерів, аналізаторів, інтегрованих засобів контролю пристроїв і агентів системи керування. Аналіз потребує більш активної участі людини та використання складних інструментів – експертних систем, які збирають практичний досвід багатьох мережевих спеціалістів.

Відповідно до рекомендацій ISO будуть виділені наступні функції засобів управління мережею:

Управління мережевою конфігурацією: налаштування мережевих компонентів, таких як встановлення мережевих адрес та ідентифікаторів, керування налаштуваннями операційної системи мережі, підтримка топології мережі та іменування об’єктів.

Управління помилками - виявлення та подальше усунення наслідків мережевих збоїв.

Аналіз продуктивності – на основі зібраної статистичної інформації можна оцінити час відгуку системи для подальшого планування розвитку мережі.

Управління безпекою - поєднує контроль доступу та цілісність даних. Функція має процедуру аутентифікації, підтримується шифрування та управління правами. Це включає в себе важливі механізми для керування паролями, доступу та підключення до інших мереж.

Час безвідмовної роботи мережі – поєднує журналювання та керування використовуються ресурси та пристрої. Ця функція оперує поняттями часу використання та оплати ресурсів.

З наведеного переліку видно, що системи управління виконують не тільки функції моніторингу та аналізу мережі, необхідні для отримання даних початкової конфігурації мережі, але й функції активного впливу на мережу – управління конфігурацією та безпекою, які необхідні для розробки плану конфігурації та оптимізації мережі. Етап створення плану конфігурації мережі виходить далеко за рамки функцій системи керування, але деякі системи керування включають експертні підсистеми, які допомагають адміністратору чи інтегратору визначити необхідні дії щодо конфігурації мережі.

Інструменти керування мережею не слід плутати з інструментами для керування операційною системою комп’ютера (SystemManagement). Серед представників засобів управління – системи HPOpenView, SunNetManager і IBMNetView.

Засоби керування системою зазвичай виконують такі функції:

Розрахунок використаного обладнання та програмного забезпечення. Він автоматично збирає інформацію з комп’ютерів і створює записи в базі даних. Тоді адміністратор може швидко дізнатися, що він має і де це знаходиться. Наприклад, дізнайтеся, для яких пристроїв потрібно оновити драйвери принтера, на яких комп’ютерах достатньо пам’яті та місця на диску тощо.

Установка програмного забезпечення. Після завершення сканування адміністратор може створювати дистрибутиви програмного забезпечення, що є дуже ефективним способом скорочення витрат. Система також може забезпечувати централізоване встановлення та керування програмами, запущеними з файлових серверів, і дозволяти кінцевим користувачам запускати ці програми з будь-якої робочої станції в мережі.

Аналіз роботи та існуючих проблем. Адміністратор може віддалено керувати ресурсами будь-якого комп'ютера в мережі. База даних системи

управління містить детальну інформацію про налаштування всіх комп'ютерів мережі, що дозволяє дистанційно аналізувати поточні проблеми.

Сучасні засоби управління мережею відповідають за:

- контроль додатків, сервісів, програм і користувачів;
- мінімізація витрат на управління мережею;
- реалізація процесів у структурі управління мережею;
- уніфікація управління з використанням конвергентної системи;
- створити план розвитку мережі;
- уникнути простоїв, зниження продуктивності, мережевих аномалій.
- структуровані кабельні системи;

Недоліком систем управління є те, що: одна система відповідає лише за частину мережі, а наявність кількох систем викликає проблеми в отриманні даних, реагуванні на події та управлінні їх елементами.

Завдяки структурованій кабельній системі зв’язок відбувається в межах однієї або кількох будівель за допомогою даних, зображення та голосу. Він є основою інформаційної платформи кожної сучасної компанії, що відповідає за надання всіх послуг.

1.4 Основи моніторингу телекомунікаційних мереж

Враховуючи сучасний стан інформаційно-телекомунікаційних технологій у сфері консолідації даних у телекомунікаційних мережах, постає проблема моніторингу.

Доцільно створювати програми моніторингу, які забезпечують доступ до інформації, мережевого контенту, топології, кінцевих і проміжних пристроїв. У широкому розумінні моніторинг — це систематичне спостереження за станом об'єктів, явищ і процесів з метою їх оцінки, контролю або прогнозування. Моніторинг – це безперервний збір і обробка інформації для покращення процесу прийняття рішень і надання додаткової інформації громадськості або як

інструмент зворотного зв’язку для реалізації проекту, оцінки програми чи розробки політики. Він виконує від однієї до трьох організаційних функцій:

1. Визначає критичні явища або явища, що змінюють навколишнє середовище, для яких буде розроблено майбутній план дій;

2. Допомагає встановити зв’язок із середовищем через зворотний зв’язок про попередні успіхи та невдачі певної політики чи алгоритму;

3. Може бути корисним для визначення відповідності нормам і договірним зобов'язанням.

Ці завдання належать до сфери управління мережею. Кілька програм моніторингу мережі: ping, сервери SNMP, Zabbix (з відкритим кодом), NetXMS (з відкритим кодом), Intellipool Network Monitor, ManageEngine OpManager, аналізатор пакетів: HP OpenView Network, моніторинг мережевого трафіку, аналіз і усунення несправностей, NetVizor, NetDecision, .

У мережах Ethernet концентратори та комутатори є першими точками підключення комп’ютерів або інших мережевих пристроїв до мережі. Разом ці комп’ютери утворюють сегмент мережі, який дозволяє їм «спілкуватися» безпосередньо один з одним. Для менш «розумних» пристроїв вони просто отримують кадри на один порт і пересилають їх на всі порти. Це ідеальне рішення для моніторингу безладу. Натомість комутатори сканують усі отримані кадри та перевіряють MAC-адреси джерела та призначення. Тільки після цього пакет буде відправлено на запитаний порт.

Більшість комутаторів не дозволяють здійснювати вільний моніторинг, але їх можна налаштувати для пересилання пакетів на спеціальний порт моніторингу.

Моніторинг і аналіз мережі є важливим кроком у контролі мережі. Для реалізації якого розроблено низку програм та інструментів, які працюють автономно, якщо необхідно їхнє втручання. Автономне програмне забезпечення для моніторингу та аналізу включає діагностичні засоби, аналізатори, експертні системи, сканери та тестери, а також багатофункціональні системи.

Доступна практично необмежена кількість конфігурацій мережі. Однак розуміння та дотримання основних принципів моніторингу мережі дозволить зберегти вашу мережу чистою майже в будь-якій ситуації. Звичайно, прозорість мережі не є кінцевою метою. Це якраз необхідна основа для коректної та грамотної роботи з програмами аналізу та моніторингу мережі.

1.5 Висновки до розділу 1

У цьому розділі пояснюється, що таке моніторинг мережі, що він робить, що він робить, що він робить і діапазон пристроїв, які він підтримує.

Моніторинг мережі – це система, яка показує низьку продуктивність мережі або несправні мережеві пристрої. Моніторинг базується на аналізі пропускної здатності, системних помилок, втрати пакетів, затримки, доступності маршрутизаторів, комутаторів і часу відповіді.

Моніторинг мережі підтримує широкий спектр пристроїв, таких як сервери, маршрутизатори, комутатори та навіть кінцеві пристрої. Крім того, його можна використовувати в усіх мережах, таких як WLAN, LAN, VPN і навіть WAN.

Моніторинг мережі використовується для вимірювання загальної продуктивності мережі. Вимірювання здійснюється шляхом перевірки кількості надісланих і отриманих пакетів.

Важливою частиною моніторингу є аналіз маршруту. Аналіз маршрутизації – це набір інструментів, програм і алгоритмів, які відстежують мережеву маршрутизацію. Працює на мережевому рівні.

Моніторинг веб-сайтів допомагає контролювати стан вашого сервера. Він вимірює час роботи сервера, продуктивність з’єднання, поточні записи DNS, пропускну здатність і навіть апаратні ресурси.

Доступна практично необмежена кількість конфігурацій мережі. Однак розуміння основ моніторингу мережі забезпечить видимість мережі майже в будь-якій ситуації. Звичайно, прозорість мережі не є кінцевою метою. Це якраз

необхідна основа для коректної та грамотної роботи з програмами аналізу та моніторингу мережі.

РОЗДІЛ 2 АНАЛІЗ МЕТОДИКИ МОНІТОРИНГУ ТЕЛЕКОМУНІКАЦІЙНОЇ МЕРЕЖІ

2.1 Методи моніторингу стану мережі

Мережевий метод удосконалення набору впливів на керований об'єкт, які вибираються з набору можливих впливів n про нові програми та оновлення про новини на об'єкті та стан навколишнього середовища для досягнення поставленої мети.

У процесі прогнозування різноманітні методи пошуку та підходи дослідження. Серед наукових тем:

1) система управління та підтримки інформаційних елементів імовірнісних процесів, що відбуваються в системі;

2) процес із системною структурою, реалізований різними способами, динамічно розвивається, розбиваючи систему на її структурні елементи та враховуючи їх у їх взаємній взаємодії;

3) історичний підхід передбачає розгляд кожного явища у зв'язку з історичними формами та щодо них;

4) структурований фреймворк, над яким працює Yavish;

5) глобальні знання та взаємозв’язки та в контексті різних наук, що вивчають ці явища, тощо.

До теперішнього часу розроблені відомі методи прогнозування, пов'язані із забезпеченням вибору оптимальних рішень для конкретних проектів. При цьому необхідно адаптувати методики до конкретних прогнозних і програмних рекомендацій.

Залежно від формату, отриманого від експертів, виділяють такі групи експертних методів: методи прямої оцінки та методи зворотного зв'язку. Відмінність полягає в тому, що в першому випадку експерт отримується з інформації та інформаційно-обґрунтованої інформації. У випадку другого типу методів результати будуть відповідно скориговані.

У зв'язку з постійним зростанням і ускладненням завдань, які виконує зв'язок, підвищенням ефективності обчислювальних пристроїв і підвищенням вимог до обслуговування інформація про інформацію, що передається в телекомунікаційній мережі. Однак через різний характер потреб у прогнозуванні телекомунікаційних послуг вимірювання навіть найкращі методи ще не в змозі забезпечити повну достовірність прогнозу.

2.2 Інтегровані системи управління та аналізу даних

Такий поділ функцій контролю та фактичного управління корисний у малих і середніх мережах, для яких встановлення інтегрованої системи керування є економічно недоцільним. Використання офлайн-інструментів керування допомагає мережевому адміністратору визначити проблемні області та параметри мережі, у такому випадку він може вимкнути або переналаштувати їх самостійно.

Процес моніторингу мережі зазвичай поділяється на два етапи: моніторинг і аналіз.

На етапі моніторингу здійснюється більш проста процедура - процедура збору первинних даних про роботу мережі: статистика про кількість кадрів і пакетів різних протоколів, що циркулюють в мережі, стан портів концентраторів, комутаторів і маршрутизатори. і т.д.

На етапі аналізу, який розуміється як більш складний і інтелектуальний процес розуміння інформації, зібраної на етапі моніторингу, порівняння її з даними, отриманими раніше, і формулювання гіпотез щодо можливих причин повільної або ненадійної роботи мережі.

Завдання моніторингу виконують апаратні та програмні лічильники, тестери, мережеві аналізатори, комплексні засоби моніторингу комунікаційних пристроїв, а також агенти системи керування. Аналітична задача вимагає більш активної участі людини і використання таких складних інструментів, як

експертні системи, в яких накопичується практичний досвід багатьох мережевих фахівців.

Інструменти моніторингу Zabbix, які використовуються для аналізу та діагностики комп'ютерних мереж, можна розділити на кілька широких класів.

• Агенти системи керування, які підтримують функції однієї зі стандартних MIB і надають інформацію через SNMP або Загальний протокол керування інформацією (CMIP). Для отримання даних від агентів зазвичай потрібна система моніторингу, яка збирає дані агентів в автономному режимі.

• Вбудовані системи діагностики та управління (Embedded Systems). Ці системи реалізуються у вигляді програмно-технічних модулів, встановлених у комунікаційному обладнанні, а також у вигляді програмних модулів, вбудованих в операційні системи. Вони виконують діагностичні та контрольні функції одного приладу, що є їх основною відмінністю від централізованих систем управління.

• Аналізатори протоколів (Protocol Analyzers). Це програмні або програмно-апаратні системи, які, на відміну від систем керування, обмежуються лише функціями моніторингу та аналізу трафіку в мережах. Хороший аналізатор протоколів може перехоплювати та декодувати пакети з великої кількості протоколів, що використовуються в мережах, зазвичай кілька десятків.

• Обладнання для діагностики та сертифікації кабельних систем. Традиційно це обладнання можна розділити на чотири основні групи: мережеві монітори, пристрої сертифікації кабельних систем, сканери та кабельні тестери.

• Мережеві монітори (також звані мережевими аналізаторами) призначені для перевірки різних категорій кабелів. Мережеві монітори також збирають дані про статистику трафіку - середню інтенсивність загального мережевого трафіку, середню швидкість потоку пакетів з певним типом помилки.

• Пристрої сертифікації кабельних систем проводять сертифікацію відповідно до вимог одного з міжнародних стандартів для кабельних систем.

• Кабельні сканери використовуються для діагностики мідних кабельних систем.

• Тестери використовуються для перевірки кабелів на наявність фізичних пошкоджень.

2.3 Протоколи керування мережею

Розділимо засоби моніторингу та аналізу комп'ютерних мереж на кілька великих класів:

Системи керування мережею — централізовані програмні системи, які збирають дані про стан мережевих вузлів і комунікаційних пристроїв, а також дані про мережевий трафік. Ці системи не тільки відстежують і аналізують мережу, але й виконують дії з керування мережею в автоматичному або напівавтоматичному режимі: увімкнення та вимкнення портів пристроїв, зміна параметрів мосту, таблиць адрес мосту, комутаторів і маршрутизаторів, а також

Прикладами систем управління є популярні системи HPOpenView, SunNetManager і IBMNetView.

Системні заходи управління (System Management). Системний контроль часто виконує функції, аналогічні системам управління, але по відношенню до інших об'єктів. У першому випадку предметом перевірки є програмно-апаратні засоби комп'ютерів мережі, а в другому - комунікаційне обладнання. Однак деякі функції цих двох типів систем управління можуть збігатися; наприклад, засоби управління системою можуть виконувати найпростіший аналіз мережевого трафіку.

Вбудовані системи діагностики та управління (Embedded Systems). Ці системи реалізуються у вигляді апаратних і програмних модулів, встановлених в комунікаційному обладнанні, а також у вигляді програмних модулів, вбудованих в операційні системи. Вони виконують діагностичні та контрольні функції одним пристроєм, що є їх основною відмінністю від централізованих систем управління. Прикладом засобів цього класу є модуль управління хабом Distrebuted 5000, який виконує функції автоматичної сегментації портів у разі виявлення збою, виділення портів у внутрішній сегмент хаба та ін. Як правило,

інтегровані модулі керування неповний робочий день діють як агенти SNMP, надаючи дані про стан пристрою системам керування.

Аналізатори протоколів. Це програмні або програмно-апаратні системи, які, на відміну від систем керування, обмежуються лише функціями моніторингу та аналізу трафіку в мережах. Хороший аналізатор протоколів може перехоплювати та декодувати пакети з великої кількості протоколів, що використовуються в мережах, зазвичай кілька десятків. Аналізатори протоколів дозволяють задавати конкретні логічні умови для захоплення окремих пакетів і повного декодування захоплених пакетів, тобто відображають у зручній для фахівця формі вкладеність пакетів протоколів різного рівня один в одного з декодуванням. вмісту. окремі поля кожного пакета.

Обладнання для діагностики та сертифікації кабельних систем. Традиційно таке обладнання можна розділити на чотири основні групи: мережеві монітори, пристрої сертифікації кабельних систем, кабельні сканери та тестери (мультиметри).

- Мережеві монітори (їх ще називають мережевими аналізаторами) призначені для перевірки кабелів різних категорій. Необхідно розрізняти мережеві монітори та аналізатори протоколів. Мережеві монітори збирають лише дані про статистику трафіку – середній обсяг загального мережевого трафіку, середню швидкість потоку пакетів із певним типом помилки тощо.

- Призначення приладів для сертифікації кабельних систем безпосередньо випливає з їх назви. Сертифікація проводиться відповідно до вимог одного з міжнародних стандартів для кабельних систем.

- Кабельні сканери використовуються для діагностики мідних кабельних систем.

- Тестери використовуються для перевірки кабелів на фізичні розриви.

- Експертні системи, ці системи поєднують у собі виявлення причин збоїв у роботі мережі та можливі методи відновлення мережі в працездатний стан. Експертні системи часто реалізуються як окремі підсистеми різноманітних засобів моніторингу та аналізу мережі: системи керування мережею, аналізатори

протоколів, мережеві аналізатори. Найпростішим варіантом експертної системи є контекстно-довідкова система. Більш складними експертними системами є т. зв бази знань, які містять елементи штучного інтелекту. Прикладом такої системи є експертна система, інтегрована з системою керування Spectrum від Cabletron.

- Багатофункціональні аналітичні та діагностичні прилади. В останні роки поширення локальних мереж викликало необхідність розробки недорогих портативних пристроїв, які поєднують у собі функції кількох пристроїв: аналізаторів протоколів, сканерів кабелів і навіть деяких функцій програмного забезпечення для керування мережею.

2.4 Протокол SNMP

2.4.1 Основні елементи SNMP та їх функції

Протокол SNMP отримує всю інформацію з інформаційної бази керування (MIB). MIB — база даних зі стандартизованою структурою. База даних має деревовидну структуру, і всі змінні класифіковані тематично. Кожне піддерево містить певну тематичну підмножину змінних. Найважливіші компоненти, що відповідають за роботу вузлів мережі, згруповані в підгрупі MIB-II.

Існує два типи MIB: стандартні та пропрієтарні. Стандартні MIB визначаються Радою Інтернет-активності (IAB), тоді як пропрієтарні MIB визначаються виробником пристрою. Бази даних, наведені в таблиці 1, містять багато змінних, які можуть бути корисними для діагностики мереж і мережевих пристроїв.

У MIB кожен об’єкт має назву та тип. Ім'я об'єкта характеризує його позицію в дереві MIB. У цьому випадку ім'я дочірнього вузла включає в себе ім'я батьківського вузла і вказується як ціле число.

SNMP — це протокол прикладного рівня. Він призначений для обміну інформацією між мережевими пристроями. Використовуючи цей протокол,

мережевий адміністратор може аналізувати мережеве обладнання та знаходити та вирішувати багато мережевих проблем.

У SNMPv3 терміни «агент» і «менеджер» більше не використовуються, замість них використовуються терміни «сутності». Як і раніше, один об’єкт знаходиться на керованому пристрої, а інший опитує програми.

Стандарт SNMP був створений для вирішення проблем обробки помилок і аналізу продуктивності та надійності.

Обробка помилок. Виявляйте, визначайте та вирішуйте проблеми та збої в мережі. На цьому рівні повідомлення про помилки реєструються, фільтруються, маршрутизуються та аналізуються на основі моделі кореляції.

Аналіз продуктивності та надійності. Оцінка на основі статистичної інформації про такі параметри, як час відгуку системи, пропускна здатність каналів зв'язку, інтенсивність трафіку в окремих сегментах мережі, ймовірність спотворення даних, індекс доступності мережевих послуг. Результати цього аналізу дозволяють контролювати вашу угоду про рівень обслуговування (SLA).

Відповідно до SNMP, управління має бути простим, навіть за рахунок потужності, масштабованості та безпеки. Тому при розробці стандартів SNMP були враховані такі умови:

• Широкий спектр застосування. Системи, якими керує SNMP, можуть бути будь-якими: від принтерів до мейнфреймів;

• Легко додавайте функції керування. Керована система має обмежену функціональність контролю, дуже проста і не може контролювати себе. Натомість усіма керованими системами керує комплексна система керування, функціональність якої може бути розширена;

• Стійкість у критичних ситуаціях. Наприклад, у разі перевантаження мережі та проблем, тобто з великою кількістю помилок.

Розберемо архітектуру SNMP з точки зору досягнення поставлених перед SNMP цілей. Для цього ми використовуємо концепцію стилю архітектури мережевого програмного забезпечення. Архітектурний стиль — це узгоджений набір архітектурних обмежень, накладених на ролі та характеристики

архітектурних елементів (компонентів, з'єднувачів і даних) і на зв'язки між ними, які з'являються в будь-якій архітектурі та відповідають цьому стилю.

Інгредієнти.

Архітектура SNMP передбачає побудову системи управління за схемою «менеджер-агент», тобто використання архітектурного стилю «клієнт-сервер». Система SNMP містить кілька керованих вузлів, кожен з яких містить досить простий сервер агента SNMP, а також принаймні один вузол, що містить складний клієнт менеджера SNMP.

Система обробки повідомлень отримує вихідні блоки даних (PDU) від диспетчера, додає до них відповідний заголовок і повертає їх диспетчеру.

За шифрування та аутентифікацію відповідає система безпеки. Усі вихідні повідомлення спочатку передаються від системи обробки повідомлень до системи безпеки перед надсиланням, де всі поля в заголовку повідомлення, блок даних (PDU), шифруються, а потім генерується код автентифікації та додається до заголовка повідомлення. Потім повідомлення надсилається назад до системи обробки повідомлень. Точно така ж операція, тільки в зворотному порядку, виконується для всіх вхідних повідомлень.

Система контролю доступу керує службами автентифікації для контролю доступу до MIB на основі вмісту блоків даних.

Менеджер взаємодіє з агентами через SNMP для обміну інформацією про керування. Ця взаємодія в основному здійснюється у формі періодичного опитування агентів менеджером з найму, оскільки агенти просто обмінюються інформацією, але не знають, що з нею робити. Видно, що система, побудована на таких принципах, втрачає масштабованість, оскільки є спеціальний клієнт, який запитує всі сервери. Однак ця схема полегшує реалізацію систем, керованих за допомогою протоколу SNMP.

Схема даних описується структурою керуючої інформації (SMI). Схема даних визначає, як виглядає керуюча інформація, тобто описує її синтаксис. SMI базується на абстрактній синтаксичній нотації номер 1. Конкретні набори інформації керування для різних типів пристроїв, протоколів тощо описані в

базах даних інформації керування (MIB). MIB визначає, яка інформація керування існує. Наприклад, у випадку пристрою з підтримкою IP MIB описує таблицю маршрутизації, прапор активації для функції маршрутизації, кількість надісланих і отриманих пакетів, кількість помилок різних типів тощо.

Таким чином, кожен пристрій містить набір значень змінних, визначених у ряді MIB, описаних правилами SMI. Цей набір змінних відповідає даним, які керують інформацією SNMP.

Важливим питанням є іменування змінних. У SNMP кожній змінній присвоюється унікальний ідентифікатор об’єкта (OID). Простір імен OID є ієрархічним і контролюється Органом нумерації Інтернету (IANA). Кожен компонент іменника є числом. У текстовому вигляді імена записуються у вигляді десяткових чисел, розділених крапками, зліва направо. Для легшого розуміння числа можна зіставити з текстовими рядками. Загалом структура імен подібна до системи доменних імен (DNS) Інтернету.

MIB визначає набір змінних, тобто певну гілку дерева OID, яка описує керуючу інформацію в певному полі. Наприклад, гілка 1.3.6.1.2.1.1 описує загальну системну інформацію. Давайте опишемо деякі змінні цієї гілки:

• sysDescr (1.3.6.1.2.1.1.1) - короткий опис системи;

• sysUpTime (1.3.6.1.2.1.1.3) - час з моменту останнього перезавантаження;

• sysName (1.3.6.1.2.1.1.5) - ім'я системи.

Змінні та інформація про їхні типи також визначені в MIB. А самі типи змінних знаходяться в SMI.

Крім прямих даних, над ними необхідно виконувати операції. Усі ці операції змінювалися та розширювалися разом із розвитком протоколу SNMP. Основні операції:

- змінне читання;

- змінна нотація;

- читання змінної після заданої змінної (необхідно для перегляду таблиць змінних).

Операції з даними в SNMP подібні до віддаленого налагодження будь-якої програми: стан системи описується певним набором змінних, які можна переглядати та змінювати.

2.5. Висновки до розділу 2

У цьому розділі аналізуються та визначаються методи моніторингу стану мережі. Тут також пояснюється, що таке інтегровані системи управління та аналізу даних і яка їх роль. Що таке протоколи керування мережею та їх функції.

Мережевий метод управління передбачає реалізацію комплексу впливів на керований об'єкт, які вибираються з набору можливих впливів на основі програми управління та отриманої інформації про поведінку об'єкта та стан навколишнього середовища, для досягнення поставленої мети.

Залежно від того, як використовується інформація, отримана від експертів, виділяють такі групи експертних методів прогнозування: методи прямої оцінки та методи зворотного зв'язку.

Інтегровані системи управління здійснюють постійний моніторинг роботи локальної мережі, яка є основою будь-якої телекомунікаційної мережі, необхідної для її працездатності.

Засоби моніторингу та аналізу комп'ютерних мереж були розділені на кілька великих класів. Також описано найважливіший протокол керування мережею.

SNMP — це протокол прикладного рівня. Він призначений для обміну інформацією між мережевими пристроями. Використовуючи цей протокол, мережевий адміністратор може аналізувати мережеве обладнання та знаходити та вирішувати багато мережевих проблем.

РОЗДІЛ 3 ЗАГАЛЬНИЙ МЕТОД ІНСТРУМЕНТУ ZABBIX ДЛЯ ЦЕНТРАЛЬНОГО ТЕЛЕКОМУНІКАЦІЙНОГО МОНІТОРИНГУ МЕРЕЖІ

3.1 Презентація інструменту ZABBIX

3.1.1 Загальні характеристики Zabbix

Zabbix - це безкоштовне та відкрите програмне забезпечення для моніторингу мережі, яке може використовуватися для збору та аналізу інформації про стан мережевих пристроїв, серверів, програмного забезпечення та інших компонентів IT-інфраструктури.

Загальні характеристики Zabbix моніторингу мережі:

Мультиплатформність. Zabbix працює на всіх популярних операційних системах, включаючи Linux, Windows, macOS та Solaris.

Розширюваність. Zabbix дозволяє додавати власні модулі та плагіни для розширення його функціональності.

Модульність. Zabbix складається з набору модулів, кожен з яких відповідає за певний аспект моніторингу.

Автоматизація. Zabbix дозволяє автоматизувати процес моніторингу за допомогою скриптів та інших інструментів.

Гнучкість. Zabbix дозволяє налаштовувати його відповідно до потреб конкретного підприємства.

Мережевий моніторинг в Zabbix

Zabbix дозволяє моніторити мережеві пристрої на різних рівнях:

Фізичний рівень. Zabbix дозволяє моніторити такі параметри фізичного рівня, як температура, напруга, швидкість обертання вентиляторів та інші.

Мережевий рівень. Zabbix дозволяє моніторити такі параметри мережевого рівня, як пропускна здатність, затримка, втрати пакетів та інші.

Рівень застосунків. Zabbix дозволяє моніторити такі параметри рівня застосунків, як доступність, продуктивність та інші.

Для моніторингу мережевих пристроїв в Zabbix використовуються такі засоби:

Сканер мережі. Сканер мережі дозволяє автоматично виявляти мережеві пристрої та додавати їх до системи моніторингу.

Провайдери. Провайдери - це модулі, які дозволяють отримувати інформацію про стан мережевих пристроїв.

Методи моніторингу. За допомогою Zabbix можна використовувати різні методи моніторингу, включаючи SNMP, IPMI, HTTP, SSH та інші.

Використання Zabbix для моніторингу мережі

Для використання Zabbix для моніторингу мережі необхідно виконати такі кроки:

Встановити Zabbix. Zabbix можна встановити на будь-якому сервері, на якому працює одна з підтримуваних операційних систем.

Налаштувати Zabbix. Для настройки Zabbix необхідно створити базу даних, налаштувати параметри безпеки та створити моніторингові правила.

Додати мережеві пристрої до Zabbix. Для цього можна використовувати сканер мережі або вручну додати пристрої до системи моніторингу.

Створити моніторингові правила. Моніторингові правила дозволяють визначити, які параметри мережевих пристроїв потрібно моніторити.

Переваги використання Zabbix для моніторингу мережі

Застосування Zabbix для моніторингу мережі має такі переваги:

Можливість моніторингу широкого спектру мережевих пристроїв. Zabbix підтримує широкий спектр мережевих пристроїв, включаючи маршрутизатори, комутатори, сервери, веб-сервери та інші.

Гнучкість налаштувань. Zabbix дозволяє налаштовувати його відповідно до потреб конкретного підприємства.

Автоматизація. Zabbix дозволяє автоматизувати процес моніторингу, що звільняє персонал від рутинних завдань.

Доступність. Zabbix - це безкоштовне та відкрите програмне забезпечення, яке можна використовувати безкоштовно.

Недоліки використання Zabbix для моніторингу мережі

Застосування Zabbix для моніторингу мережі має такі недоліки:

Необхідність знань та навичок. Для використання Zabbix необхідно мати певні знання та навички в області моніторингу мереж.

Вимога до ресурсів. Zabbix може вимагати значних ресурсів сервера, особливо для моніторингу великих мереж.

3.1.2 Архітектура Zabbix

Архітектура Zabbix моніторингу мережі є розподіленою, що дозволяє масштабувати систему для моніторингу великих мереж. Зазвичай архітектура Zabbix складається з наступних компонентів:

Zabbix-сервер. Zabbix-сервер є центральним компонентом системи, який відповідає за зберігання даних, обробку інформації та відображення результатів моніторингу.

Zabbix-проксі. Zabbix-проксі є додатковими серверами, які використовуються для збору даних від мережевих пристроїв. Zabbix-проксі можуть розміщуватися в різних місцях мережі, що дозволяє оптимізувати передачу даних.

Zabbix-агент. Zabbix-агент - це програмне забезпечення, яке встановлюється на мережевих пристроях і відповідає за збір даних та передачу їх на Zabbix-сервер.

Zabbix-сервер.

Zabbix-сервер є центральним компонентом системи Zabbix. Він відповідає за такі функції:

Зберігання даних. Zabbix-сервер зберігає дані, зібрані Zabbix-агентами та Zabbix-проксі.

Обробка інформації. Zabbix-сервер обробляє дані, зібрані Zabbix-агентами та Zabbix-проксі, і генерує звіти та графіки.

Відображення результатів моніторингу. Zabbix-сервер відображає результати моніторингу в веб-інтерфейсі.

Zabbix-проксі

Zabbix-проксі - це додаткові сервери, які використовуються для збору даних від мережевих пристроїв. Zabbix-проксі можуть розміщуватися в різних місцях мережі, що дозволяє оптимізувати передачу даних.

Zabbix-проксі відповідають за такі функції:

Збір даних. Zabbix-проксі збирають дані від мережевих пристроїв за допомогою SNMP, IPMI, HTTP, SSH та інших методів.

Передача даних. Zabbix-проксі передають зібрані дані на Zabbix-сервер.

Zabbix-агент

Zabbix-агент - це програмне забезпечення, яке встановлюється на мережевих пристроях і відповідає за збір даних та передачу їх на Zabbix-сервер.

Zabbix-агент відповідають за такі функції:

Збір даних. Zabbix-агент збирають дані з мережевих пристроїв за допомогою SNMP, IPMI, HTTP, SSH та інших методів.

Передача даних. Zabbix-агент передають зібрані дані на Zabbix-сервер.

Переваги розподіленої архітектури Zabbix

Розподілена архітектура Zabbix має такі переваги:

Масштабованість. Розподілена архітектура дозволяє масштабувати систему для моніторингу великих мереж.

Ефективність. Розподілена архітектура дозволяє оптимізувати передачу даних, що може підвищити ефективність системи моніторингу.

Надійність. Розподілена архітектура підвищує надійність системи моніторингу, оскільки відмова одного компонента не призведе до повної зупинки системи.

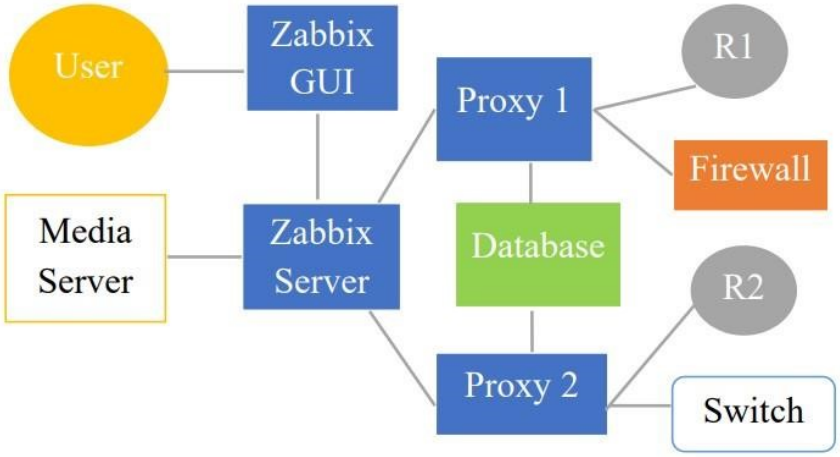


Рисунок 3.1 – Компоненти Zabbix

Архітектура Zabbix моніторингу мережі складається з таких компонентів:

Zabbix-сервер. Zabbix-сервер є центральним компонентом системи моніторингу. Він відповідає за збір, зберігання та обробку інформації про стан мережевих пристроїв.

Zabbix-прокси. Zabbix-прокси - це додаткові компоненти, які можна використовувати для розвантаження Zabbix-сервера. Вони відповідають за збір інформації про стан мережевих пристроїв, розташованих в локальній мережі.

Zabbix-агент. Zabbix-агент - це програмне забезпечення, яке встановлюється на мережевих пристроях. Воно відповідає за збір інформації про стан пристроїв та передачу її на Zabbix-сервер.

Zabbix-інтерфейс. Zabbix-інтерфейс - це веб-інтерфейс, який дозволяє користувачам отримувати доступ до інформації про стан мережевих пристроїв.

Залежно від розміру мережі та вимог до масштабованості, архітектура Zabbix моніторингу мережі може бути реалізована в різних варіантах.

Для невеликих мереж, що не вимагають високої масштабованості, можна використовувати просту архітектуру з одним Zabbix-сервером. У цьому випадку Zabbix-сервер буде відповідати за збір інформації про всі мережеві пристрої.

Для великих мереж, що вимагають високої масштабованості, можна використовувати розподілену архітектуру. У цьому випадку Zabbix-сервер буде

відповідати за збір інформації про мережеві пристрої, розташовані в певній частині мережі. Zabbix-прокси будуть використовуватися для розвантаження Zabbix-сервера та збору інформації про мережеві пристрої, розташовані в інших частинах мережі.

3.1.3 Переваги Zabbix

Zabbix - це безкоштовне та відкрите програмне забезпечення для моніторингу мережі, яке має ряд переваг:

Можливість моніторингу широкого спектру мережевих пристроїв. Zabbix підтримує широкий спектр мережевих пристроїв, включаючи маршрутизатори, комутатори, сервери, веб-сервери та інші.

Гнучкість налаштувань. Zabbix дозволяє налаштовувати його відповідно до потреб конкретного підприємства.

Автоматизація. Zabbix дозволяє автоматизувати процес моніторингу, що звільняє персонал від рутинних завдань.

Доступність. Zabbix - це безкоштовне та відкрите програмне забезпечення, яке можна використовувати безкоштовно.

Конкретні переваги Zabbix моніторингу мережі включають:

Широкий спектр параметрів для моніторингу. За допомогою Zabbix можна моніторити широкий спектр параметрів мережевих пристроїв, включаючи фізичні параметри, мережеві параметри та параметри застосунків.

Глибокий аналіз даних. Zabbix дозволяє проводити глибокий аналіз даних, що допомагає виявляти проблеми в мережі на ранніх етапах їх розвитку.

Сучасний інтерфейс. Zabbix має сучасний інтерфейс, який дозволяє легко отримувати доступ до інформації про стан мережевих пристроїв.

Можливість масштабування. Zabbix можна масштабувати для задоволення потреб великих мереж.

Загалом, Zabbix - це потужний інструмент для моніторингу мережі, який має ряд переваг, що роблять його привабливим вибором для підприємств будь-якого розміру.

3.2 Веб-інтерфейс Zabbix

Веб-інтерфейс Zabbix - це інструмент, який дозволяє користувачам отримувати доступ до інформації про стан мережевих пристроїв. Він складається з таких основних елементів:

Головна сторінка. Головна сторінка відображає загальний стан мережі та її компонентів. На головній сторінці відображаються такі дані:

Загальний стан мережі

Стан основних компонентів мережі, таких як маршрутизатори, комутатори та сервери

Оновлення про останні події в мережі

Менеджер пристроїв. Менеджер пристроїв дозволяє користувачам переглядати список пристроїв, які моніторяться Zabbix. У менеджері пристроїв можна переглядати такі дані:

Ім'я пристрою

Тип пристрою

Стан пристрою

Список моніторингових правил, які застосовуються до пристрою

Менеджер моніторингу. Менеджер моніторингу дозволяє користувачам створювати та налаштовувати моніторингові правила. Моніторингові правила визначають, які параметри пристроїв необхідно моніторити та які дії необхідно виконувати в разі відхилення параметрів від норми.

Менеджер графіків. Менеджер графіків дозволяє користувачам переглядати графіки, що відображають стан мережевих пристроїв. Графіки можуть бути використані для виявлення тенденцій у даних моніторингу та для виявлення проблем у мережі.

Менеджер сповіщень. Менеджер сповіщень дозволяє користувачам налаштовувати сповіщення, які будуть надсилатися в разі виникнення проблем у мережі. Сповіщення можуть бути надіслані по електронній пошті, SMS або іншим способом.

Веб-інтерфейс Zabbix можна налаштувати відповідно до потреб конкретного підприємства. Наприклад, користувачі можуть налаштувати веб-інтерфейс, щоб відображати лише ту інформацію, яка є для них важливою.

3.3 Інтерфейс прикладного програмного забезпечення

3.3.1 Переваги архітектури Zabbix

Архітектура Zabbix моніторингу мережі має ряд переваг, які роблять її привабливим вибором для підприємств будь-якого розміру.

Однією з основних переваг архітектури Zabbix є її масштабованість. Zabbix можна масштабувати для задоволення потреб великих мереж. Для цього можна використовувати розподілену архітектуру, в якій Zabbix-сервери розподіляються по різних вузлах мережі.

Іншою перевагою архітектури Zabbix є її гнучкість. За допомогою Zabbix можна моніторити широкий спектр мережевих пристроїв. Для цього Zabbix підтримує різні методи моніторингу, включаючи SNMP, IPMI, HTTP та SSH.

Ще однією перевагою архітектури Zabbix є її надійність. Zabbix має ряд функцій, які допомагають забезпечити надійність системи моніторингу. Наприклад, Zabbix підтримує резервне копіювання даних та відновлення в разі несправності.

Нарешті, архітектура Zabbix є доступною. Zabbix є безкоштовним та відкритим програмним забезпеченням. Це означає, що будь-яке підприємство може використовувати Zabbix для моніторингу своєї мережі безкоштовно.

Конкретні переваги архітектури Zabbix моніторингу мережі включають:

Розподілена архітектура дозволяє масштабувати Zabbix для задоволення потреб великих мереж.

Підтримка різних методів моніторингу дозволяє моніторити широкий спектр мережевих пристроїв.

Функції забезпечення надійності допомагають забезпечити безперебійну роботу системи моніторингу.

Безкоштовна та відкрита ліцензія дозволяє використовувати Zabbix безкоштовно.

Загалом, архітектура Zabbix моніторингу мережі є потужним і гнучким інструментом, який може використовуватися для задоволення потреб підприємств будь-якого розміру.

3.4 Взаємодія пам'яті

3.4.1 Кеш-пам’ять

Zabbix використовує спеціальні методи для покращення продуктивності пам’яті. У цьому розділі ми опишемо, як Zabbix може відновити дані в обхід бази даних. Додатково буде представлено метод об’єднання кількох вкладок в одну масову операцію.

Zabbix використовує техніку кешування. Кеш — це прошарок між Zabbix-сервером або Zabbix-проксі та базою даних. Хорошим прикладом може бути кеш конфігурації. Як показано на рисунку 3.2, виклики до бази даних не здійснюються для отримання даних з бази даних.

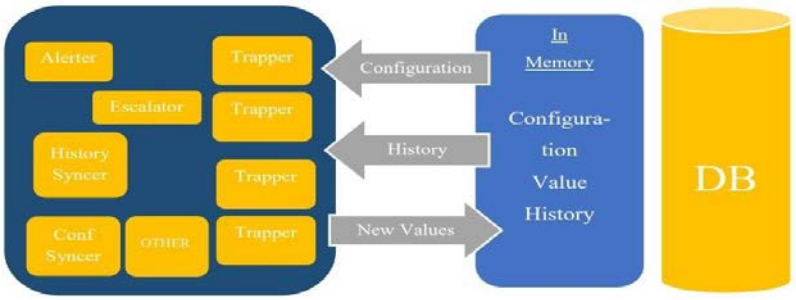


Рисунок 3.2 – Методи кешування

Дані конфігурації витягуються з кешу. Крім того, Zabbix має кеш значень. Це значно підвищує ефективність використання обчислювальних ресурсів. Щоб отримати дані для оцінки тригерів, вони витягуються безпосередньо з пам’яті, а не з бази даних.

3.4.2 Операції групи

Пакетні операції Ще однією функцією, яка покращує продуктивність Zabbix, є кеш історії записів. Як показано на рисунку 3.3, замість виконання кількох вставок і оновлень бази даних, вони об’єднуються в одну пакетну операцію. Однак, як грошова техніка, масові транзакції використовуються лише на сервері. Тому він реалізований лише на Zabbix сервері та Zabbix проксі.

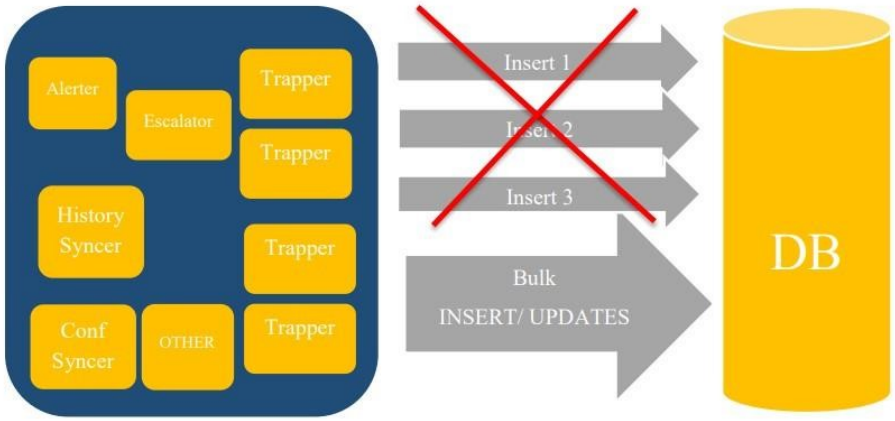


Рисунок 3.3 - Масові операції

3.5 Порівняльна характеристика систем моніторингу мережі

3.5.1 Огляд системи моніторингу Nagios

Nagios - це безкоштовне та відкрите програмне забезпечення для моніторингу мережі та IT-інфраструктури. Воно використовується для

моніторингу широкого спектру мережевих пристроїв, серверів, програмного забезпечення та інших компонентів.

Основні характеристики Nagios:

Мультиплатформність. Nagios працює на всіх популярних операційних системах, включаючи Linux, Windows, macOS та Solaris.

Розширюваність. Nagios дозволяє додавати власні модулі та плагіни для розширення його функціональності.

Модульність. Nagios складається з набору модулів, кожен з яких відповідає за певний аспект моніторингу.

Автоматизація. Nagios дозволяє автоматизувати процес моніторингу за допомогою скриптів та інших інструментів.

Гнучкість. Nagios дозволяє налаштовувати його відповідно до потреб конкретного підприємства.

Мережевий моніторинг в Nagios.

Nagios дозволяє моніторити мережеві пристрої на різних рівнях:

Фізичний рівень. Nagios дозволяє моніторити такі параметри фізичного рівня, як температура, напруга, швидкість обертання вентиляторів та інші.

Мережевий рівень. Nagios дозволяє моніторити такі параметри мережевого рівня, як пропускна здатність, затримка, втрати пакетів та інші.

Рівень застосунків. Nagios дозволяє моніторити такі параметри рівня застосунків, як доступність, продуктивність та інші.

Для моніторингу мережевих пристроїв в Nagios використовуються такі засоби:

Сканер мережі. Сканер мережі дозволяє автоматично виявляти мережеві пристрої та додавати їх до системи моніторингу.

Провайдери. Провайдери - це модулі, які дозволяють отримувати інформацію про стан мережевих пристроїв.

Методи моніторингу. За допомогою Nagios можна використовувати різні методи моніторингу, включаючи SNMP, IPMI, HTTP, SSH та інші.

Використання Nagios для моніторингу мережі

Для використання Nagios для моніторингу мережі необхідно виконати такі кроки:

Встановити Nagios. Nagios можна встановити на будь-якому сервері, на якому працює одна з підтримуваних операційних систем.

Налаштувати Nagios. Для настройки Nagios необхідно створити базу даних, налаштувати параметри безпеки та створити моніторингові правила.

Додати мережеві пристрої до Nagios. Для цього можна використовувати сканер мережі або вручну додати пристрої до системи моніторингу.

Створити моніторингові правила. Моніторингові правила дозволяють визначити, які параметри мережевих пристроїв потрібно моніторити.

Переваги використання Nagios для моніторингу мережі.

Застосування Nagios для моніторингу мережі має такі переваги:

Можливість моніторингу широкого спектру мережевих пристроїв. Nagios підтримує широкий спектр мережевих пристроїв, включаючи маршрутизатори, комутатори, сервери, веб-сервери та інші.

Гнучкість налаштувань. Nagios дозволяє налаштовувати його відповідно до потреб конкретного підприємства.

Автоматизація. Nagios дозволяє автоматизувати процес моніторингу, що звільняє персонал від рутинних завдань.

Доступність. Nagios - це безкоштовне та відкрите програмне забезпечення, яке можна використовувати безкоштовно.

Недоліки використання Nagios для моніторингу мережі

Застосування Nagios для моніторингу мережі має такі недоліки:

Необхідність знань та навичок. Для використання Nagios необхідно мати певні знання та навички в області моніторингу мереж.

Вимога до ресурсів. Nagios може вимагати значних ресурсів сервера, особливо для моніторингу великих мереж.

Загалом, Nagios - це потужне та гнучке програмне забезпечення для моніторингу мережі, яке може використовуватися для задоволення потреб підприємств будь-якого розміру.

3.5.2 Огляд системи моніторингу «Обсервіум»

Огляд системи моніторингу «Обсервіум» моніторингова мережа.

«Обсервіум» - це хмарна система моніторингу мережі та IT-інфраструктури, розроблена компанією «Інфозахист». Система дозволяє моніторити широкий спектр мережевих пристроїв, серверів, програмного забезпечення та інших компонентів.

Основні характеристики «Обсервіум»:

Мультиплатформність. «Обсервіум» працює на всіх популярних операційних системах, включаючи Linux, Windows, macOS та Solaris.

Розширюваність. «Обсервіум» дозволяє додавати власні модулі та плагіни для розширення його функціональності.

Модульність. «Обсервіум» складається з набору модулів, кожен з яких відповідає за певний аспект моніторингу.

Автоматизація. «Обсервіум» дозволяє автоматизувати процес моніторингу за допомогою скриптів та інших інструментів.

Гнучкість. «Обсервіум» дозволяє налаштовувати його відповідно до потреб конкретного підприємства.

Мережевий моніторинг в «Обсервіум».

«Обсервіум» дозволяє моніторити мережеві пристрої на різних рівнях:

Фізичний рівень. «Обсервіум» дозволяє моніторити такі параметри фізичного рівня, як температура, напруга, швидкість обертання вентиляторів та інші.

Мережевий рівень. «Обсервіум» дозволяє моніторити такі параметри мережевого рівня, як пропускна здатність, затримка, втрати пакетів та інші.

Рівень застосунків. «Обсервіум» дозволяє моніторити такі параметри рівня застосунків, як доступність, продуктивність та інші.

Для моніторингу мережевих пристроїв в «Обсервіум» використовуються такі засоби:

Сканер мережі. Сканер мережі дозволяє автоматично виявляти мережеві пристрої та додавати їх до системи моніторингу.

Провайдери. Провайдери - це модулі, які дозволяють отримувати інформацію про стан мережевих пристроїв.

Методи моніторингу. За допомогою «Обсервіум» можна використовувати різні методи моніторингу, включаючи SNMP, IPMI, HTTP, SSH та інші.

Використання «Обсервіум» для моніторингу мережі

Для використання «Обсервіум» для моніторингу мережі необхідно виконати такі кроки:

Створити обліковий запис в системі «Обсервіум».

Додати мережеві пристрої до системи моніторингу. Для цього можна використовувати сканер мережі або вручну додати пристрої до системи моніторингу.

Створити моніторингові правила. Моніторингові правила дозволяють визначити, які параметри мережевих пристроїв потрібно моніторити.

Переваги використання «Обсервіум» для моніторингу мережі

Застосування «Обсервіум» для моніторингу мережі має такі переваги:

Можливість моніторингу широкого спектру мережевих пристроїв. «Обсервіум» підтримує широкий спектр мережевих пристроїв, включаючи маршрутизатори, комутатори, сервери, веб-сервери та інші.

Гнучкість налаштувань. «Обсервіум» дозволяє налаштовувати його відповідно до потреб конкретного підприємства.

Автоматизація. «Обсервіум» дозволяє автоматизувати процес моніторингу, що звільняє персонал від рутинних завдань.

Доступність. «Обсервіум» - це хмарна система, яка доступна з будь-якого місця в Інтернеті.

Недоліки використання «Обсервіум» для моніторингу мережі

Застосування «Обсервіум» для моніторингу мережі має такі недоліки:

Платна ліцензія. «Обсервіум» є платною системою.

Необхідність наявності Інтернет-підключення. Для використання «Обсервіум» необхідно мати Інтернет-підключення.

3.6. Висновки до розділу 3

У цьому розділі описано інструмент моніторингу мережі Zabbix із загальною інформацією про Zabbix, його основні функції та принципи роботи. Крім того, описані основні переваги, які відрізняють Zabbix від інших інструментів моніторингу.

Загалом Zabbix — це інструмент моніторингу мережі, який здійснює централізований моніторинг доступності та продуктивності мереж і мережевих пристроїв. У разі виникнення помилки адміністратор мережі сповістить вас через певний гаджет або поштову скриньку. Zabbix - це абсолютно безкоштовний інструмент моніторингу мережі. Немає обмежень щодо можливостей і кількості керованих пристроїв.

Zabbix пропонує широкий спектр функцій і можливостей. Підтримка інструментів на основі та без агентів, які використовуються для моніторингу мережевих пристроїв, таких як маршрутизатори, комутатори та сервери. Мережеві пристрої повинні підтримувати SNMP.

Zabbix відповідає приблизно 90% вимогам до надійного інструменту моніторингу телекомунікаційної мережі. Проводить супервізію з агентом і без нього. Ви можете знайти такі функції, як низькорівневе виявлення, автоматичне виявлення та логічне групування.

Zabbix не підтримує тренди. Цю функцію не ввімкнула команда Zabbix, оскільки вона знижує загальну продуктивність. Zabbix — надійний і передбачуваний інструмент моніторингу мережі. Якщо Zabbix попереджає користувача про певні помилки, то він може бути на 100% впевнений, що така проблема існує. Ті самі принципи надійності застосовуються до відновлення та візуалізації. Крім того, однією з головних переваг Zabbix є його масштабованість, оскільки його можна використовувати в середовищах будь-якого розміру.

РОЗДІЛ 4 ТЕХНІЧНЕ РІШЕННЯ ДЛЯ ЗБОРУ ДАНИХ ТА ТЕСТУВАННЯ ПРОДУКТИВНОСТІ SNMP ДЛЯ СЕРВЕРА ZABBIX

4.1 Протокол SNMP для Zabbix Server

4.1.1 Топологія мережі

SNMP (Simple Network Management Protocol) - це стандартний мережевий протокол, який використовується для моніторингу та управління мережевими пристроями. SNMP працює шляхом обміну інформацією між агентом SNMP, який працює на мережевому пристрої, та менеджером SNMP, який працює на сервері моніторингу.

Zabbix Server - це система моніторингу мережі та IT-інфраструктури, яка підтримує SNMP. Zabbix Server може використовувати SNMP для моніторингу широкого спектру мережевих пристроїв, включаючи маршрутизатори, комутатори, сервери, веб-сервери та інші.

Для використання SNMP з Zabbix Server необхідно виконати такі кроки:

Налаштуйте SNMP на мережевому пристрої. Для цього необхідно налаштувати на пристрої агент SNMP та надати йому доступ менеджеру SNMP.

Налаштування SNMP на мережевому пристрої зазвичай включає в себе такі кроки:

Включення підтримки SNMP на пристрої.

Налаштування імені та пароля для SNMP.

Налаштування рівня доступу для SNMP.

Додайте мережевий пристрій до Zabbix Server. Для цього можна використовувати сканер мережі або вручну додати пристрій до системи моніторингу.

Для додавання мережевого пристрою до Zabbix Server необхідно вказати його IP-адресу, ім'я та тип.

Створіть моніторингові правила для мережевого пристрою. Моніторингові правила визначають, які параметри мережевого пристрою потрібно моніторити.

Для створення моніторингового правила необхідно вказати тип параметра, який потрібно моніторити, та параметри для визначення нормального стану параметра.

Після виконання цих кроків Zabbix Server зможе отримувати інформацію про стан мережевого пристрою за допомогою SNMP.

Ось деякі з переваг використання SNMP з Zabbix Server:

SNMP є стандартним протоколом, який підтримується широким спектром мережевих пристроїв.

SNMP простий у налаштуванні та використанні.

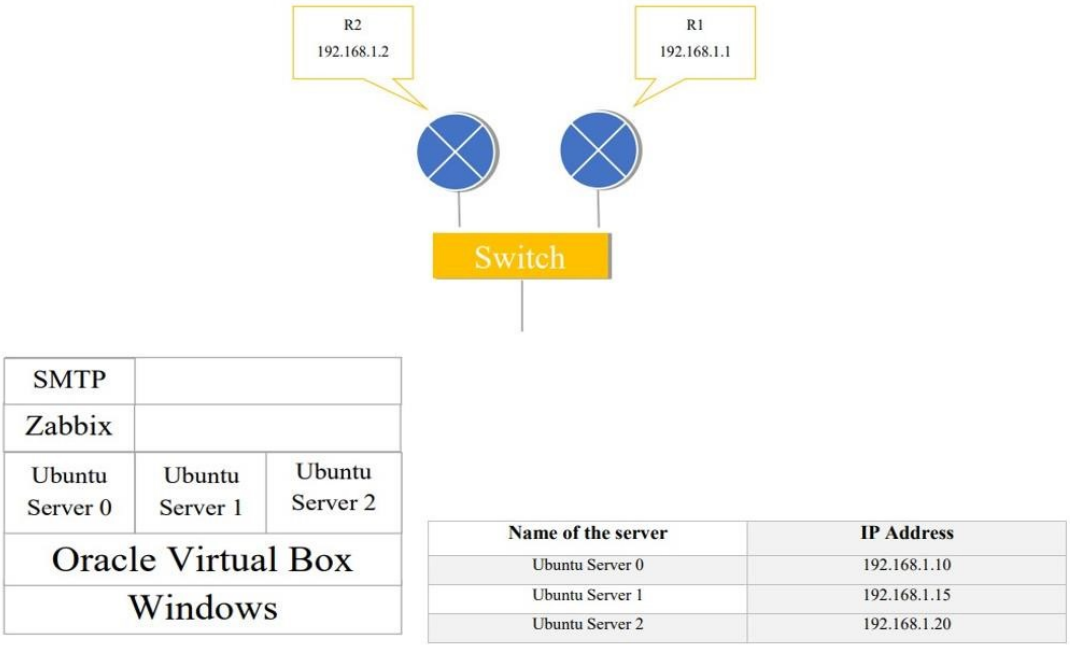
SNMP дозволяє моніторити широкий спектр параметрів мережевих пристроїв.

Ось деякі з недоліків використання SNMP з Zabbix Server:

SNMP може бути менш безпечним, ніж інші протоколи моніторингу.

SNMP може не надавати доступ до всіх параметрів мережевих пристроїв.

По-перше, вам потрібно переглянути розділ Інтернету. На рисунку 4.1 показана схема логічної мережі, що складається з ПК1, сервера Zabbix, комутатора Cisco Catalyst і двох маршрутизаторів Cisco. Дві додаткові віртуальні машини будуть частиною мережі: Ubuntu Server і Windows Server. Сервер Zabbix буде встановлено на PC1 як віртуальну машину. Крім того, сервери Ubuntu і Windows також будуть встановлені як віртуальні машини. З’єднання між PC1 і комутатором здійснюється через прямий кабель. Перемикач також буде підключений до R1 і R2 за допомогою прямого кабелю.



Name of the server	IP Address
Ubuntu Server 0	192.168.1.10
Ubuntu Server 1	192.168.1.15
Ubuntu Server 2	192.168.1.20

Рисунок 4.1 - Топологія мережі

Далі вам потрібно ввімкнути сервер SNMP на маршрутизаторах 1 і 2. Це можна зробити за допомогою команди в Cisco CLI: # snmp-server.

4.2 Встановлення сервера Zabbix

4.2.1 Встановлення сервера Linux

Встановлення сервера Linux для моніторингу мережі.

Для встановлення сервера Linux для моніторингу мережі необхідно виконати такі кроки

Вибір операційної системи. Для моніторингу мережі можна використовувати будь-яку операційну систему Linux, але найбільш поширеними варіантами є Ubuntu, CentOS та Debian.

Встановлення операційної системи. Операційну систему Linux можна встановити за допомогою стандартного процесу інсталяції.

Оновлення операційної системи. Після встановлення операційної системи необхідно оновити її до останньої версії. Це допоможе забезпечити стабільність та безпеку системи.

Встановлення Zabbix. Zabbix - це безкоштовна та відкрита система моніторингу мережі та IT-інфраструктури. Zabbix можна встановити за допомогою диспетчера пакетів або вручну.

Налаштування Zabbix. Після встановлення Zabbix необхідно налаштувати його відповідно до потреб вашої мережі. Це включає в себе такі завдання, як:

Налаштування сервера Zabbix

Додавання агентів Zabbix до мережевих пристроїв

Створення моніторингових правил

Налаштування сервера Zabbix

Налаштування сервера Zabbix включає в себе такі завдання:

Створення нового користувача та пароля для адміністратора Zabbix.

Налаштування безпеки сервера Zabbix.

Налаштування поштової служби для відправлення сповіщень.

Додавання агентів Zabbix до мережевих пристроїв.

Агент Zabbix - це програмне забезпечення, яке встановлюється на мережевих пристроях і дозволяє отримувати інформацію про їх стан.

Для додавання агентів Zabbix до мережевих пристроїв необхідно виконати такі кроки:

Завантажте агент Zabbix для відповідного типу мережевого пристрою.

Встановіть агент Zabbix на мережевому пристрої.

Налаштуйте агент Zabbix. Це включає в себе такі завдання, як:

Вказування імені хоста та IP-адреси сервера Zabbix.

Вказування імені користувача та пароля для сервера Zabbix.

Налаштування рівня доступу для агенту Zabbix.

Створення моніторингових правил.

Мониторингові правила визначають, які параметри мережевих пристроїв потрібно моніторити.

Для створення моніторингового правила необхідно вказати такі параметри:

Тип параметра, який потрібно моніторити.

Параметри для визначення нормального стану параметра.

Дії, які потрібно виконати, якщо параметр виходить за межі нормального стану.

Поради щодо встановлення сервера Linux для моніторингу мережі

Використовуйте стійку та надійну операційну систему Linux.

Оновлення операційної системи до останньої версії.

Використовуйте надійне джерело для завантаження Zabbix.

Налаштуйте сервер Zabbix відповідно до потреб вашої мережі.

Додайте агенти Zabbix до всіх мережевих пристроїв, які потрібно моніторити.

Створіть моніторингові правила для всіх параметрів, які потрібно моніторити.

Кроки встановлення сервера Linux для моніторингу мережі

Крок 1. Вибір операційної системи

Вибір операційної системи Linux залежить від ваших потреб та досвіду. Якщо ви не маєте великого досвіду роботи з Linux, ви можете вибрати Ubuntu або Debian. Ці операційні системи є простими у використанні та мають велику спільноту підтримки. Якщо ви маєте досвід роботи з Linux, ви можете вибрати CentOS. Ця операційна система є більш стійкою та надійною, але вона також більш складна у налаштуванні.

Ви можете встановити операційну систему Linux за допомогою стандартного процесу інсталяції. Для цього вам знадобиться завантажити образ операційної системи з Інтернету та записати його на USB-накопичувач або DVD. Потім ви можете запустити комп'ютер з USB.

4.3 Моніторинг сервера Zabbix

4.3.1 Моніторинг SNMP

Моніторинг SNMP.

SNMP (Simple Network Management Protocol) - це стандартний протокол мережного управління, який використовується для моніторингу та управління мережевими пристроями. SNMP працює шляхом обміну інформацією між агентом SNMP, який працює на мережевому пристрої, та менеджером SNMP, який працює на сервері моніторингу.

Моніторинг SNMP для мережі.

SNMP можна використовувати для моніторингу широкого спектру мережевих пристроїв, включаючи маршрутизатори, комутатори, сервери, веб-сервери та інші. SNMP дозволяє мониторити такі параметри мережевих пристроїв, як:

Доступність

Пропускна здатність

Затримка

Втрати пакетів

Температура

Напруга

Швидкість обертання вентиляторів

Інші параметри

Переваги використання SNMP для моніторингу мережі.

SNMP є стандартним протоколом, який підтримується широким спектром мережевих пристроїв.

SNMP простий у налаштуванні та використанні.

SNMP дозволяє мониторити широкий спектр параметрів мережевих пристроїв.

Недоліки використання SNMP для моніторингу мережі.

SNMP може бути менш безпечним, ніж інші протоколи моніторингу.

SNMP може не надавати доступ до всіх параметрів мережевих пристроїв.

Використання SNMP для моніторингу мережі.

Для використання SNMP для мониторингу мережі необхідно виконати такі кроки:

Налаштуйте SNMP на мережевих пристроях. Для цього необхідно настроїти на пристрої агент SNMP та надати йому доступ менеджера SNMP.

Додайте мережеві пристрої до системи моніторингу. Для цього можна використовувати сканер мережі або вручну додати пристрій до системи моніторингу.

Створіть моніторингові правила для мережевих пристроїв. Моніторингові правила визначають, які параметри мережевих пристроїв потрібно контролювати.

Налаштування SNMP на мережевих пристроях.

Налаштування SNMP на мережевих пристроях зазвичай включає такі кроки:

Увімкнення підтримки SNMP на пристрої.

Налаштування імені та пароля для SNMP.

Налаштування рівня доступу для SNMP.

Додавання мережевих пристроїв до системи моніторингу.

Для додавання мережевих пристроїв до системи моніторингу необхідно вказати їх IP-адресу, ім'я та тип.

Створення моніторингових правил для мережевих пристроїв.

Для створення моніторингового правила необхідно вказати такі параметри:

Тип параметра, який потрібно контролювати.

Параметри визначення нормального стану параметра.

Дії, які потрібно виконати, якщо параметр виходить за межі нормального стану.

Приклади моніторингових правил для мережевих пристроїв.

Монторінг доступності: Це моніторингове правило визначає, чи доступне мережевий пристрій. Якщо пристрій не доступний, система моніторингу має створити сповіщення.

Монторінг пропускної здатності: Це моніторингове правило визначає, чи досягла пропускна здатність мережевого пристрою заданого порога. Якщо пропускна здатність досягла порога, система моніторингу має створити сповіщення.

Монторінг затримки: Це моніторингове правило визначає, чи перевищила затримка мережевого пристрою завдань порог. Якщо затримка перевищила поріг, система моніторингу має створити сповіщення.

4.3.2 Створення хоста та елементів

Першим кроком є створення хоста. Це мережевий пристрій або послуга, яку контролюватиме сервер Zabbix. Перший маршрутизатор матиме назву R1, і це ім’я використовуватиметься для моніторингу та середовища Zabbix загалом. За допомогою імені хоста ми зможемо розрізняти пристрої. Контроль R1 здійснюватиметься через SNMP, оскільки локальна інсталяція Zabbix Agent неможлива. Додатково необхідно вказати IP-адресу пристрою. Відповідно до логічного плану мережі, зображеного на рисунку 1, IP-адреса

Маршрутизатор R1 – 192.168.1.1

Елемент збирає та відображає такі дані хоста, як ЦП, пам’ять і використання пропускної здатності. Щоб контролювати використання ЦП, вам потрібно створити два елементи. Перший - простий процесор. Вимірює кількість доступних ресурсів. По-друге, використання ЦП.

Для створення хоста та елементів моніторингу мережі необхідно виконати такі кроки:

Встановіть систему моніторингу. Для моніторингу мережі можна використовувати будь-яку систему моніторингу, яка підтримує SNMP. Наприклад, можна використовувати Zabbix, Nagios або SolarWinds.

Налаштуйте систему моніторингу. Для цього необхідно налаштувати такі параметри, як:

Ім'я та пароль адміністратора

Доступ до мережі

Налаштування безпеки

Створіть хост. Хост - це об'єкт у системі моніторингу, який представляє мережевий пристрій. Для створення хоста необхідно вказати такі параметри, як:

Ім'я хоста

IP-адреса хоста

Тип хоста

Створіть елементи. Елементи - це об'єкти у системі моніторингу, які представляють параметри мережевого пристрою. Для створення елемента необхідно вказати такі параметри, як:

Назва елемента

Тип елемента

Значення елемента

Налаштування хоста.

Для налаштування хоста необхідно виконати такі кроки:

Увійдіть до системи моніторингу.

Перейдіть до розділу "Хости".

Натисніть кнопку "Створити".

У вікні створення хоста необхідно вказати такі параметри:

Ім'я хоста: Вкажіть ім'я хоста.

IP-адреса хоста: Вкажіть IP-адресу хоста.

Тип хоста: Вкажіть тип хоста. Наприклад, маршрутизатор, комутатор, сервер або інший тип пристрою.

Налаштування елементів.

Для налаштування елементів необхідно виконати такі кроки:

Увійдіть до системи моніторингу.

Перейдіть до розділу "Елементи".

Натисніть кнопку "Створити".

У вікні створення елемента необхідно вказати такі параметри:

Назва елемента: Вкажіть назву елемента.

Тип елемента: Вкажіть тип елемента. Наприклад, доступність, пропускна здатність, затримка, температура, напруга тощо.

Значення елемента: Вкажіть значення елемента. Наприклад, "1" для доступності, "100 Мбіт/с" для пропускної здатності тощо.

Приклади елементів.

Елемент доступності: Цей елемент визначає, чи доступний мережевий пристрій.

Елемент пропускної здатності: Цей елемент визначає пропускну здатність мережевого пристрою.

Елемент затримки: Цей елемент визначає затримку мережевого пристрою.

Елемент температури: Цей елемент визначає температуру мережевого пристрою.

Елемент напруги: Цей елемент визначає напругу мережевого пристрою.

Створення сповіщень.

Для створення сповіщень необхідно виконати такі кроки:

Увійдіть до системи моніторингу.

Перейдіть до розділу "Сповіщення".

Натисніть кнопку "Створити".

У вікні створення сповіщення необхідно вказати такі параметри:

Назва сповіщення: Вкажіть назву сповіщення.

Тип сповіщення: Вкажіть тип сповіщення. Наприклад, електронний лист, SMS, SNMP тощо.

Параметри сповіщення: Вкажіть параметри сповіщення. Наприклад, значення елемента, при якому буде створено сповіщення.

Приклад сповіщення.

Сповіщення про доступність: Це сповіщення буде створено, якщо мережевий пристрій стане недоступним.

Загалом, створення хоста та елементів моніторингу мережі є простим завданням. Для цього необхідно виконати кілька кроків у системі моніторингу.

Універсального OID не існує, кожен номер порту має власний OID SMNP. Обидва елементи мають постійні частини. Останнє число є унікальним OID, який залежить від порту. Команда #show snmp mib ifmib ifindex для пристроїв Cisco використовується для отримання номера індексу інтерфейсу. На риснку 4.5 показано результат виконання цієї команди.

Оскільки мій маршрутизатор підключений до комутатора через порт FastInternet0/1-, індекс №2.

```
Router#show snmp MIB IFMib IFIndex
       13:55:48.387: %SYS-5-CONFIG_I: Configured from console by console
Serial0/0/0: Ifindex = 3
Async0/0/1: Ifindex = 8
FastEthernet0/1: Ifindex = 2
VoIP-Null0: Ifindex = 5
Null0: Ifindex = 6
Serial0/0/1: Ifindex = 4
Async0/0/0: Ifindex = 7
FastEthernet0/0: Ifindex = 1
```

Рисунок 4.5 – Вихід команди для індексу порту

4.3.3 Моніторинг моделей

Моніторинг моделей мережі - це процес спостереження за станом моделей мережі та виявлення потенційних проблем. Моніторинг моделей мережі важливий, оскільки він може допомогти запобігти проблемам, які можуть призвести до збоїв у роботі мережі або погіршення її продуктивності.

Параметри моніторингу моделей мережі.

Існує широкий спектр параметрів, які можна використовувати для моніторингу моделей мережі. Деякі з найпоширеніших параметрів включають:

Доступність: Цей параметр визначає, чи доступна модель мережі.

Пропускна здатність: Цей параметр визначає пропускну здатність моделі мережі.

Затримка: Цей параметр визначає затримку моделі мережі.

Втрати пакетів: Цей параметр визначає кількість пакетів, які втрачені моделлю мережі.

Точність: Цей параметр визначає точність моделі мережі.

Методи моніторингу моделей мережі.

Існує два основних методи моніторингу моделей мережі:

Активний моніторинг: Цей метод передбачає активне тестування моделей мережі за допомогою спеціального програмного забезпечення.

Пасивний моніторинг: Цей метод передбачає моніторинг моделей мережі за допомогою даних, які генеруються моделлю.

Активний моніторинг.

Активний моніторинг є більш точним методом моніторингу моделей мережі, оскільки він дозволяє безпосередньо тестувати моделі. Однак активний моніторинг може бути більш ресурсомістким, оскільки він вимагає, щоб моделі мережі були доступні для тестування.

Пасивний моніторинг.

Пасивний моніторинг є менш точним методом моніторингу моделей мережі, оскільки він заснований на даних, які генеруються моделлю. Однак пасивний моніторинг є більш ефективним методом моніторингу моделей мережі, оскільки він не вимагає, щоб моделі мережі були доступні для тестування.

Сценарій моніторингу моделей мережі.

Загальний сценарій моніторингу моделей мережі включає в себе такі кроки:

Вибір параметрів моніторингу: Вибір параметрів моніторингу залежить від конкретних потреб вашої мережі.

Встановлення методу моніторингу: Вибір методу моніторингу залежить від ваших ресурсних обмежень і вимог до точності.

Налаштування системи моніторингу: Налаштування системи моніторингу включає в себе створення хостів, елементів та сповіщень.

Виконання моніторингу: Система моніторингу буде регулярно збирати дані про моделі мережі та відправляти сповіщення, якщо будуть виявлені потенційні проблеми.

Завдання моніторингу моделей мережі

Завдання моніторингу моделей мережі включають в себе:

Виявлення потенційних проблем: Моніторинг моделей мережі може допомогти виявити потенційні проблеми, які можуть призвести до збоїв у роботі мережі або погіршення її продуктивності.

Попередження про потенційні проблеми: Моніторинг моделей мережі може допомогти попередити про потенційні проблеми, щоб можна було вжити заходів для їх усунення.

Вимірювання продуктивності моделей мережі: Моніторинг моделей мережі може допомогти виміряти продуктивність моделей мережі та виявити можливі способи її покращення.

Загальні рекомендації щодо моніторингу моделей мережі.

Ось кілька загальних рекомендацій щодо моніторингу моделей мережі:

Використовуйте широкий спектр параметрів моніторингу: Це допоможе вам отримати більш точне уявлення про стан моделей мережі.

Налаштуйте систему моніторингу таким чином, щоб вона надсилала вам сповіщення про потенційні проблеми: Це допоможе вам швидко вжити заходів для їх усунення.

Регулярно аналізуйте дані моніторингу: Це допоможе вам виявити тенденції та можливі проблеми.

4.3.4 Моніторинг маршрутизатора

Моніторинг маршрутизатора мережі - це процес спостереження за станом маршрутизатора та виявлення потенційних проблем. Моніторинг

маршрутизатора важливий, оскільки він може допомогти запобігти проблемам, які можуть призвести до збоїв у роботі мережі або погіршення її продуктивності.

Параметри моніторингу маршрутизатора.

Існує широкий спектр параметрів, які можна використовувати для моніторингу маршрутизатора. Деякі з найпоширеніших параметрів включають:

Доступність: Цей параметр визначає, чи доступний маршрутизатор.

Пропускна здатність: Цей параметр визначає пропускну здатність маршрутизатора.

Затримка: Цей параметр визначає затримку маршрутизатора.

Втрати пакетів: Цей параметр визначає кількість пакетів, які втрачені маршрутизатором.

Температура: Цей параметр визначає температуру маршрутизатора.

Напруга: Цей параметр визначає напругу маршрутизатора.

Статус портів: Цей параметр визначає статус портів маршрутизатора.

Статус протоколів: Цей параметр визначає статус протоколів, які використовуються маршрутизатором.

Методи моніторингу маршрутизатора

Існує два основних методи моніторингу маршрутизатора:

Активний моніторинг: Цей метод передбачає активне тестування маршрутизатора за допомогою спеціального програмного забезпечення.

Пасивний моніторинг: Цей метод передбачає моніторинг маршрутизатора за допомогою даних, які генеруються маршрутизатором.

Активний моніторинг.

Активний моніторинг є більш точним методом моніторингу маршрутизатора, оскільки він дозволяє безпосередньо тестувати маршрутизатор. Однак активний моніторинг може бути більш ресурсомістким, оскільки він вимагає, щоб маршрутизатор був доступний для тестування.

Пасивний моніторинг.

Пасивний моніторинг є менш точним методом моніторингу маршрутизатора, оскільки він заснований на даних, які генеруються

маршрутизатором. Однак пасивний моніторинг є більш ефективним методом моніторингу маршрутизатора, оскільки він не вимагає, щоб маршрутизатор був доступний для тестування.

Сценарій моніторингу маршрутизатора.

Загальний сценарій моніторингу маршрутизатора включає в себе такі кроки:

Вибір параметрів моніторингу: Вибір параметрів моніторингу залежить від конкретних потреб вашої мережі.

Встановлення методу моніторингу: Вибір методу моніторингу залежить від ваших ресурсних обмежень і вимог до точності.

Налаштування системи моніторингу: Налаштування системи моніторингу включає в себе створення хостів, елементів та сповіщень.

Виконання моніторингу: Система моніторингу буде регулярно збирати дані про маршрутизатор та відправляти сповіщення, якщо будуть виявлені потенційні проблеми.

Завдання моніторингу маршрутизатора.

Завдання моніторингу маршрутизатора включають в себе:

Виявлення потенційних проблем: Моніторинг маршрутизатора може допомогти виявити потенційні проблеми, які можуть призвести до збоїв у роботі мережі або погіршення її продуктивності.

Попередження про потенційні проблеми: Моніторинг маршрутизатора може допомогти попередити про потенційні проблеми, щоб можна було вжити заходів для їх усунення.

Вимірювання продуктивності маршрутизатора: Моніторинг маршрутизатора може допомогти виміряти продуктивність маршрутизатора та виявити можливі способи її покращення.

Загальні рекомендації щодо моніторингу маршрутизатора.

Ось кілька загальних рекомендацій щодо моніторингу маршрутизатора:

Використовуйте широкий спектр параметрів моніторингу: Це допоможе вам отримати більш точне уявлення про стан маршрутизатора.

Налаштуйте систему моніторингу таким чином, щоб вона надсилала вам сповіщення про потенційні проблеми: Це допоможе вам швидко вжити заходів для їх усунення.

Регулярно аналізуйте дані моніторингу: Це допоможе вам виявити тенденції та можливі проблеми.

4.4 Моніторинг серверів Zabbix

4.4.1 Моніторинг агента Zabbix

Моніторинг агента Zabbix - це процес спостереження за станом агента Zabbix та виявлення потенційних проблем. Моніторинг агента Zabbix важливий, оскільки він може допомогти запобігти проблемам, які можуть призвести до збоїв у роботі системи Zabbix або погіршення її продуктивності.

Параметри моніторингу агента Zabbix.

Існує широкий спектр параметрів, які можна використовувати для моніторингу агента Zabbix. Деякі з найпоширеніших параметрів включають:

Доступність: Цей параметр визначає, чи доступний агент Zabbix.

Пропускна здатність: Цей параметр визначає пропускну здатність агента Zabbix.

Затримка: Цей параметр визначає затримку агента Zabbix.

Втрати пакетів: Цей параметр визначає кількість пакетів, які втрачені агентом Zabbix.

Статус протоколів: Цей параметр визначає статус протоколів, які використовуються агентом Zabbix.

Методи моніторингу агента Zabbix.

Існує два основних методи моніторингу агента Zabbix:

Активний моніторинг: Цей метод передбачає активне тестування агента Zabbix за допомогою спеціального програмного забезпечення.

Пасивний моніторинг: Цей метод передбачає моніторинг агента Zabbix за допомогою даних, які генеруються агентом Zabbix.

Активний моніторинг.

Активний моніторинг є більш точним методом моніторингу агента Zabbix, оскільки він дозволяє безпосередньо тестувати агент Zabbix. Однак активний моніторинг може бути більш ресурсомістким, оскільки він вимагає, щоб агент Zabbix був доступний для тестування.

Пасивний моніторинг.

Пасивний моніторинг є менш точним методом моніторингу агента Zabbix, оскільки він заснований на даних, які генеруються агентом Zabbix. Однак пасивний моніторинг є більш ефективним методом моніторингу агента Zabbix, оскільки він не вимагає, щоб агент Zabbix був доступний для тестування.

Сценарій моніторингу агента Zabbix

Загальний сценарій моніторингу агента Zabbix включає в себе такі кроки:

Вибір параметрів моніторингу: Вибір параметрів моніторингу залежить від конкретних потреб вашої системи Zabbix.

Встановлення методу моніторингу: Вибір методу моніторингу залежить від ваших ресурсних обмежень і вимог до точності.

Налаштування системи моніторингу: Налаштування системи моніторингу включає в себе створення хостів, елементів та сповіщень.

Виконання моніторингу: Система моніторингу буде регулярно збирати дані про агента Zabbix та відправляти сповіщення, якщо будуть виявлені потенційні проблеми.

Завдання моніторингу агента Zabbix

Завдання моніторингу агента Zabbix включають в себе:

Виявлення потенційних проблем: Моніторинг агента Zabbix може допомогти виявити потенційні проблеми, які можуть призвести до збоїв у роботі системи Zabbix або погіршення її продуктивності.

Попередження про потенційні проблеми: Моніторинг агента Zabbix може допомогти попередити про потенційні проблеми, щоб можна було вжити заходів для їх усунення.

Вимірювання продуктивності агента Zabbix: Моніторинг агента Zabbix може допомогти виміряти продуктивність агента Zabbix та виявити можливі способи її покращення.

Загальні рекомендації щодо моніторингу агента Zabbix.

Ось кілька загальних рекомендацій щодо моніторингу агента Zabbix:

Використовуйте широкий спектр параметрів моніторингу: Це допоможе вам отримати більш точне уявлення про стан агента Zabbix.

Налаштуйте систему моніторингу таким чином, щоб вона надсилала вам сповіщення про потенційні проблеми: Це допоможе вам швидко вжити заходів для їх усунення.

4.4.2 Автоматичне визначення

Автовизначення автоматично виявляє пристрої у вашій мережі. Крім того, виявлені пристрої можна автоматично додавати, оскільки хости та шаблони можна призначати автоматично. Дозволяє шукати контрольовані пристрої з агентом або без нього.

Автоматичне виявлення широко використовується в мережах середнього та корпоративного класу. Перш ніж ви зможете почати використовувати цю функцію, необхідно виконати деякі передумови. Рекомендується логічне групування хостів. Пристрої, якими керує SNMP, повинні перевіряти назву спільноти SNMP. Пристрої, якими керує агент, повинні перевіряти, чи працює агент Zabbix.

Давайте створимо нову топологію мережі та класифікуємо пристрої за типом. Після цього відкриття необхідно створити вузли для кожної групи. Вам потрібно створити дію, щоб автоматично створити хост і призначити шаблон. Послідовність цього процесу показано на рисунку 4.8.

4.4.3 Топологія мережі

Для корпоративних мереж важливо організовувати пристрої в групи. Це забезпечує ясність і прозорість моніторингу та управління. Пристрої можна групувати на основі їхнього географічного розташування, типу та функції.

Зверніть увагу, що Zabbix Server і Ubuntu Server1-3 встановлені як віртуальні машини на ПК.

4.5 Zabbix рішення для технічного моніторингу

Пристрій на одній стороні каналу (клієнт) періодично надсилає серію запитів на пристрій (сервер) на іншій стороні каналу, отримує (або не отримує) відповідь і зберігає результати. Запити бувають наступних типів:

- Запит HTTP GET на цільову URL-адресу
- Запит HTTP GET для метаданих цільової URL-адреси
- Exo-запит ICMP до цільової адреси (за замовчуванням)
- Запит на мітку часу ICMP для адреси призначення
- Передавати UDP-пакети на цільовий пристрій
- Запити часових позначок UDP на цільову адресу
- Пакети TCP ping до цільового пристрою

Перші два типи запитів, звичайно, пов’язані не з якістю каналу, а скоріше з доступністю та швидкістю Інтернет-сервісів, останні 4 запити є розширеними та вимагають підтримки RPM від пристрою з роллю Сервер. Окрім підтримки RPM, для цих тестів також потрібна розширена ліцензія. У нашому випадку ми використовуємо комутатори ex2200 із базовою роллю клієнта та ліцензією на роль сервера й не можемо використовувати роль сервера RPM для розширеного тестування. Тому в цьому розділі ми обмежимося exo-запитами ICMP. Тим більше, що це набагато більш універсальний сценарій.

Між офісами обох перевізників є два канали L2. Клієнт розміщується зліва. В принципі, достатньо було б використовувати по одному пристрою з кожного

боку, але виявляється, що на момент організації тесту пристрої ex-isp1 і ex-isp2 вже використовувалися в цій частині мережі.

Тепер ми можемо перейти до конфігурації RPM. Збережіть таку конфігурацію на пристрої ex2200rpm:

iddqd@ex2200-rpm> показати служби конфігурації gee probe rpm { jitter test {

тип зонда icmp-ping-timestamp; адреса призначення 2.2.2.2; опитування № 15; пробний інтервал 1; тестовий інтервал 15; адреса джерела 2.2.2.1; розмір даних 1400; пороги { втрата послідовності 2;

} апаратна позначка часу;

Стрижні зонда {

перевірити вібрацію {

тип зонда icmp-ping-timestamp; адреса призначення 1.1.1.2; опитування № 15; пробний інтервал 1; тестовий інтервал 15; адреса джерела 1.1.1.1; розмір даних 1400; пороги { втрата послідовності 2;

} апаратна позначка часу;

Явна конфігурація не вимагає особливих пояснень. Потім ми виправляємо це і йдемо, і протягом хвилини ми можемо отримати результати тесту.

Тепер ми перейдемо до налаштувань Zabbix, щоб контролювати тести RPM. Вбудованої функції SNMP у Zabbix недостатньо для автоматичного виявлення тестів RPM. Zabbix використовує метод snmp walk для автоматичного виявлення. Де індекси SNMP та їх значення використовуються як параметри.

Наприклад, щоб знайти об’єкт ifDescr, введіть:

$ snmpwalk -v 2c -c public 192.168.1.1 IF-MIB::ifDescr

IF-MIB: ifDescr. 4 = ЛІНІЯ: WAN

IF-MIB::ifDescr.7 = РЯДОК: LAN1

IF-MIB::ifDescr.11 = РЯДОК: LAN2

Метод виявлення в Zabbix виявить індекси 4,7,11 та їхні значення WAN, LAN1 і LAN2. Однак Juniper не надав такої зручної функції виявлення тесту

RPM. Найрелевантнішим знайденим об’єктом є об’єкт jnxRpmResSampleValue. Тоді таблиця повернення об’єктів виглядає так:

iddqd @ex2200-rpm> показати snmp mib walk jnxRpmResSampleValue
jnxRpmResSampleValue.3.71.101.101.6.74.105.116.116.101.114.1 = 1989
jnxRpmResSampleValue.3.71.101. 10 1.6 .74.105 .116.116.101.114.1
101.6.74.105.116.116.101.114.1 116.101 .114.2 = -424
jnxRpmResSampleValue.3.71.101.101 .6.74.105.116.116.101.114.3 = 810
jnxRpmResSampleValue.4.6 6.65 .82.83.6.74.105.116 .1 1 6.101.114.3 1 = 3352
jnxRpmResSampleValue. 4.66.65.8 2.83.6.74.105.116.116. 101,114,2 = 1612.

З таблиці вище ми бачимо, що jnxRpmResSampleValue — це об’єкт MIB, який ми обходимо, а числа .3.66.101.101.6.74.105.116.116.101.114 — це назва нашого тесту. Більше того, ми можемо це довести. Як індекс SNMP

(остання цифра після крапки) – порядковий номер тестових параметрів:

1 - RTT

2 – Тремтіння при ходьбі вперед-назад

3 - коливання між прибуттям і поверненням

Якщо ви подивіться на результати тесту RPM і порівняєте їх із числами, які повертає snmpwalk, щоб знайти OID (тобто числове значення) об’єктів MIB у JunOS, таких як jnxRpmResSampleValue, jnxRpmResultsSampleTable, jnxRpmHistorySummaryTable та будь-які інші, ви можете виконати команду: show snmp mib walk jnxRpmResSampleValue. Іншими словами, сценарій автоматичного виявлення.

Таким чином, без зовнішньої допомоги Zabbix не зможе впоратися з тестовим виявленням RPM. Для зручності необхідно надати допомогу у вигляді зовнішнього скрипта, скрипт написаний на Python 2.7 zbx_junper_rpm і використовує тільки одну зовнішню бібліотеку - pysnmp. Ця бібліотека присутня в більшості дистрибутивів Ubuntu і може бути встановлена за допомогою команди: apt install python-pysnmp4 або в будь-якому дистрибутиві через менеджер PIP за допомогою команди: pip install pysnmp.

Два параметри hostname і community надаються як вхідні дані сценарію, і повернутий JSON виглядає так:

"дані":
"{#RPMTEST}::Струшення",
" {#RPMUUID} ": " 4.66.65.82.83.6.74.105.116.116.101.114 ",
"{#RPMOWNER}": "БАРИ"
"{#RPMTEST}": "Струшування",
"{#RPMUUID}": "3.71.101.101.6.74.105.116.116.101.114", {{1}}
"{#RPMOWNER}": "Бог"

Визначені користувачем макроси {#RPMUUID}, {#RPMOWNER} і {#RPMTEST} також використовуються в назвах елементів, їхніх ключах, тригерах і навіть графічних зображеннях. Скрипт повинен мати форму chmod + x і бути розміщений у каталозі зовнішніх скриптів Zabbix, у нашому випадку це каталог: /etc/zabbix/etc/externalscripts. Ми не будемо описувати налаштування Zabbix нижче, а просто перейдемо до шаблонів. Модель містить 3 елементи: RTT, Jitter і PacketLoss. Для будь-якого тесту RPM, визначеного сценарієм RPM, тест RPM не вимірює тремтіння, тому цей параметр просто автоматично вимикається.

Для більш складних тестів модель можна модифікувати відповідно до вимог інфраструктури, яка її використовує. У цьому випадку скрипт не потребуватиме жодних змін, тобто всі три елемента масштабування будуть відображені на діаграмі, яка також буде створена автоматично.

4.6. Висновки з розділу 4

Технічне рішення, описане вище, дозволяє збирати дані та тестувати продуктивність SNMP для сервера Zabbix. Це рішення є ефективним і простим у використанні.

Для підвищення ефективності збору даних та тестування продуктивності SNMP для сервера Zabbix можна використовувати наступні рекомендації:

Використовуйте широкий спектр параметрів моніторингу. Це допоможе вам отримати більш точне уявлення про стан сервера Zabbix.

Налаштуйте систему моніторингу таким чином, щоб вона надсилала сповіщення про потенційні проблеми. Це допоможе вам швидко вжити заходів для їх усунення.

Регулярно аналізуйте дані моніторингу. Це допоможе вам виявити тенденції та можливі проблеми.

Приклади реалізації.

Ось кілька прикладів реалізації технічного рішення, описаного вище:

Використовування системи Zabbix. Система Zabbix підтримує SNMP і дозволяє збирати дані та тестувати продуктивність SNMP для сервера Zabbix.

Використовування системи Nagios. Система Nagios підтримує SNMP і дозволяє збирати дані та тестувати продуктивність SNMP для сервера Zabbix.

Використовування системи SolarWinds. Система SolarWinds підтримує SNMP і дозволяє збирати дані та тестувати продуктивність SNMP для сервера Zabbix.

Вибір конкретного рішення залежить від ваших потреб та бюджету.

5 ЕКОНОМІЧНА ЧАСТИНА

Виконання науково-дослідної роботи завжди передбачає отримання певних результатів і вимагає відповідних витрат. Результати виконаної роботи завжди дають нам нові знання, які в подальшому можуть бути використані для удосконалення та/або розробки (побудови) нових, більш продуктивних зразків техніки, процесів та програмного забезпечення.

Дослідження на тему «Комплексні системи моніторингу інфраструктури телекомунікаційної системи» може бути віднесено до фундаментальних і пошукових наукових досліджень і спрямоване на вирішення наукових проблем, пов’язаних з практичним застосуванням. Основою таких досліджень є науковий ефект, який виражається в отриманні наукових результатів, які збільшують обсяг знань про природу, техніку та суспільство, які розвивають теоретичну базу в тому чи іншому науковому напрямку, що дозволяє виявити нові закономірності, які можуть використовуватися на практиці.

Для цього випадку виконаємо такі етапи робіт:

1) здійснимо проведення наукового аудиту досліджень, тобто встановлення їх наукового рівня та значимості;

2) проведемо планування витрат на проведення наукових досліджень;

3) здійснимо розрахунок рівня важливості наукового дослідження та перспективності, визначимо ефективність наукових досліджень.

5.1 Оцінювання наукового ефекту

Основними ознаками наукового ефекту науково-дослідної роботи є новизна роботи, рівень її теоретичного опрацювання, перспективність, рівень розповсюдження результатів, можливість реалізації. Науковий ефект НДР на тему «Комплексні системи моніторингу інфраструктури телекомунікаційної

системи» можна охарактеризувати двома показниками: ступенем наукової новизни та рівнем теоретичного опрацювання.

Значення показників ступеня новизни і рівня теоретичного опрацювання науково-дослідної роботи в балах наведені в табл. 5.1 та 5.2.

Таблиця 5.1 – Показники ступеня новизни науково-дослідної роботи виставлені експертами

Ступінь новизни	Характеристика ступеня новизни	Значення ступеня новизни, бали		
		Експерти (ПІБ, посада)		
		1	2	3
Принципово нова	Робота якісно нова за постановкою задачі і ґрунтується на застосуванні оригінальних методів дослідження. Результати дослідження відкривають новий напрям в даній галузі науки і техніки. Отримані принципово нові факти, закономірності; розроблена нова теорія. Створено принципово новий пристрій, спосіб, метод	0	0	0
Нова	Отримана нова інформація, яка суттєво зменшує невизначеність наявних значень (по-новому або вперше пояснені відомі факти, закономірності, впроваджені нові поняття, розкрита структура змісту). Проведено суттєве вдосконалення, доповнення і уточнення раніше досягнутих результатів	57	56	53

Відносно нова	Робота має елементи новизни в постановці задачі і методах дослідження. Результати дослідження систематизують і узагальнюють наявну інформацію, визначають шляхи подальших досліджень; вперше знайдено зв'язок (або знайдено новий зв'язок) між явищами. В принципі відомі положення розповсюджені на велику кількість об'єктів, в результаті чого знайдено ефективне рішення. Розроблені більш прості способи для досягнення відомих результатів. Проведена часткова раціональна модифікація (з ознаками новизни)	0	0	0
Традиційна	Робота виконана за традиційною методикою. Результати дослідження мають інформаційний характер. Підтверджені або поставлені під сумнів відомі факти та твердження, які потребують перевірки. Знайдено новий варіант рішення, який не дає суттєвих переваг в порівнянні з існуючим	0	0	0
Не нова	Отримано результат, який раніше зафіксований в інформаційному полі, та не був відомий авторам	0	0	0
Середнє значення балів експертів		55,3		

Згідно отриманого середнього значення балів експертів ступінь новизни характеризується як нова, тобто отримана нова інформація, яка суттєво зменшує невизначеність наявних знань (по-новому або вперше пояснені відомі факти, закономірності, впроваджені нові поняття, розкрита структура змісту) та проведено суттєве вдосконалення, доповнення і уточнення раніше досягнутих результатів.

Таблиця 5.2 – Показники рівня теоретичного опрацювання науково-дослідної роботи виставлені експертами

Характеристика рівня теоретичного опрацювання	Значення показника рівня теоретичного опрацювання, бали		
	Експерт (ПІБ, посада)		
	1	2	3
Відкриття закону, розробка теорії	0	0	0
Глибоке опрацювання проблеми: багатоаспектний аналіз зв’язків, взаємозалежності між фактами з наявністю пояснень, наукової систематизації з побудовою евристичної моделі або комплексного прогнозу	62	64	60
Розробка способу (алгоритму, програми), пристрою, отримання нової речовини	0	0	0
Елементарний аналіз зв’язків між фактами та наявною гіпотезою, класифікація, практичні рекомендації для окремого випадку тощо	0	0	0
Опис окремих елементарних фактів, викладення досвіду, результатів спостережень, вимірювань тощо	0	0	0
Середнє значення балів експертів	62,0		

Згідно отриманого середнього значення балів експертів рівень теоретичного опрацювання науково-дослідної роботи характеризується як глибоке опрацювання проблеми: багатоаспектний аналіз зв’язків, взаємозалежності між фактами з наявністю пояснень, наукової систематизації з побудовою евристичної моделі або комплексного прогнозу.

Показник, який характеризує рівень наукового ефекту, визначаємо за формулою [23]:

$$E_{нау} = 0,6 \cdot k_{нов} + 0,4 \cdot k_{теор}, \qquad (5.1)$$

де $k_{нов}, k_{теор}$ - показники ступеня новизни та рівня теоретичного опрацювання науково-дослідної роботи, $k_{нов} = 55,3, k_{теор} = 62,0$ балів;

0,6 та 0,4 – питома вага (значимість) показників ступеня новизни та рівня теоретичного опрацювання науково-дослідної роботи.

$$E_{нау} = 0,6 \cdot k_{нов} + 0,4 \cdot k_{теор} = 0,6 \cdot 55,3 + 0,4 \cdot 62,00 = 58,00 \text{ балів.}$$

Визначення характеристики показника $E_{нау}$ проводиться на основі висновків експертів виходячи з граничних значень, які наведені в табл. 5.3.

Таблиця 5.3 – Граничні значення показника наукового ефекту

Досягнутий рівень показника	Кількість балів
Високий	70…100
Середній	50…69
Достатній	15…49
Низький (помилкові дослідження)	1…14

Відповідно до визначеного рівня наукового ефекту проведеної науково-дослідної роботи на тему «Комплексні системи моніторингу інфраструктури телекомунікаційної системи», даний рівень становить 58,00 балів і відповідає статусу - середній рівень. Тобто у даному випадку можна вести мову про потенційну фактичну ефективність науково-дослідної роботи.

5.2 Розрахунок витрат на здійснення науково-дослідної роботи

Витрати, пов’язані з проведенням науково-дослідної роботи на тему «Комплексні системи моніторингу інфраструктури телекомунікаційної системи», під час планування, обліку і калькулювання собівартості науково-дослідної роботи групуємо за відповідними статтями.

5.2.1 Витрати на оплату праці

До статті «Витрати на оплату праці» належать витрати на виплату основної та додаткової заробітної плати керівникам відділів, лабораторій, секторів і груп, науковим, інженерно-технічним працівникам, конструкторам, технологам, креслярам, копіювальникам, лаборантам, робітникам, студентам, аспірантам та іншим працівникам, безпосередньо зайнятим виконанням конкретної теми, обчисленої за посадовими окладами, відрядними розцінками, тарифними ставками згідно з чинними в організаціях системами оплати праці.

Основна заробітна плата дослідників

Витрати на основну заробітну плату дослідників ($З_о$) розраховуємо у відповідності до посадових окладів працівників, за формулою [23]:

$$З_о = \sum_{i=1}^{k} \frac{M_{ni} \cdot t_i}{T_p}, \qquad (5.2)$$

де k – кількість посад дослідників залучених до процесу досліджень;

M_{ni} – місячний посадовий оклад конкретного дослідника, грн;

t_i – число днів роботи конкретного дослідника, дн.;

T_p – середнє число робочих днів в місяці, T_p=21 дні.

$$З_о = 16560{,}00 \cdot 21 / 21 = 16560{,}00 \; грн.$$

Проведені розрахунки зведемо до таблиці.

Таблиця 5.4 – Витрати на заробітну плату дослідників

Найменування посади	Місячний посадовий оклад, грн	Оплата за робочий день, грн	Число днів роботи	Витрати на заробітну плату, грн
Керівник проекту	16560,00	788,57	21	16560,00

Інженер-дослідник телекомунікаційних систем	15900,00	757,14	21	15900,00
Профідний фахівець	8400,00	400,00	15	6000,00
Всього				38460,00

Основна заробітна плата робітників

Витрати на основну заробітну плату робітників ($З_р$) за відповідними найменуваннями робіт НДР на тему «Комплексні системи моніторингу інфраструктури телекомунікаційної системи» розраховуємо за формулою:

$$З_р = \sum_{i=1}^{n} C_i \cdot t_i , \quad (5.3)$$

де C_i – погодинна тарифна ставка робітника відповідного розряду, за виконану відповідну роботу, грн/год;

t_i – час роботи робітника при виконанні визначеної роботи, год.

Погодинну тарифну ставку робітника відповідного розряду C_i можна визначити за формулою:

$$C_i = \frac{M_M \cdot K_i \cdot K_c}{T_p \cdot t_{зм}}, \quad (5.4)$$

де M_M – розмір прожиткового мінімуму працездатної особи, або мінімальної місячної заробітної плати (в залежності від діючого законодавства), приймемо $Мм$=6700,00 грн;

K_i – коефіцієнт міжкваліфікаційного співвідношення для встановлення тарифної ставки робітнику відповідного розряду (табл. Б.2, додаток Б) [23];

K_c – мінімальний коефіцієнт співвідношень місячних тарифних ставок робітників першого розряду з нормальними умовами праці виробничих

об’єднань і підприємств до законодавчо встановленого розміру мінімальної заробітної плати.

$T_р$ – середнє число робочих днів в місяці, приблизно $T_р$ = 21 дн;

$t_{зм}$ – тривалість зміни, год.

$C_1 = 6700{,}00 \cdot 1{,}10 \cdot 1{,}35 / (21 \cdot 8) = 59{,}22$ *грн.*

$З_{р1} = 59{,}22 \cdot 6{,}45 = 381{,}99$ *грн.*

Таблиця 5.5 – Величина витрат на основну заробітну плату робітників

Найменування робіт	Тривалість роботи, год	Розряд роботи	Тарифний коефіцієнт	Погодинна тарифна ставка, грн	Величина оплати на робітника грн
Установка електронно-обчислювального обладнання	6,45	2	1,10	59,22	381,99
Підготовка робочого місця дослідника телекомунікаційних систем	4,50	2	1,10	59,22	266,50
Монтаж дослідних компоненттів телекомунікаційної системи	5,00	5	1,70	91,53	457,63
Демонтаж дослідних компоненттів телекомунікаційної системи	4,00	4	1,50	80,76	323,04
Всього					1429,16

Додаткова заробітна плата дослідників та робітників

Додаткову заробітну плату розраховуємо як 10 … 12% від суми основної заробітної плати дослідників та робітників за формулою:

$$З_{дод} = (З_о + З_р) \cdot \frac{Н_{дод}}{100\%}, \quad (5.5)$$

де $Н_{дод}$ – норма нарахування додаткової заробітної плати. Приймемо 10%.

$З_{дод}$ = (38460,00 + 1429,16) · 10 / 100% = 3988,92 грн.

5.2.2 Відрахування на соціальні заходи

Нарахування на заробітну плату дослідників та робітників розраховуємо як 22% від суми основної та додаткової заробітної плати дослідників і робітників за формулою:

$$З_н = (З_о + З_р + З_{дод}) \cdot \frac{Н_{зп}}{100\%} \quad (5.6)$$

де $Н_{зп}$ – норма нарахування на заробітну плату. Приймаємо 22%.

Зн = (38460,00 + 1429,16 + 3988,92) · 22 / 100% = 9653,18 грн.

5.2.3 Сировина та матеріали

До статті «Сировина та матеріали» належать витрати на сировину, основні та допоміжні матеріали, інструменти, пристрої та інші засоби і предмети праці, які придбані у сторонніх підприємств, установ і організацій та витрачені на проведення досліджень за темою «Комплексні системи моніторингу інфраструктури телекомунікаційної системи».

Витрати на матеріали на даному етапі проведення досліджень в основному пов’язані з використанням моделей елементів та моделювання роботи і досліджень за допомогою комп’ютерної техніки та створення експериментальних математичних моделей або програмного забезпечення, тому

дані витрати формуються на основі витратних матеріалів характерних для офісних робіт.

Витрати на матеріали (M), у вартісному вираженні розраховуються окремо по кожному виду матеріалів за формулою:

$$M = \sum_{j=1}^{n} H_j \cdot Ц_j \cdot K_j - \sum_{j=1}^{n} B_j \cdot Ц_{вj}, \quad (5.7)$$

де H_j – норма витрат матеріалу j-го найменування, кг;

n – кількість видів матеріалів;

$Ц_j$ – вартість матеріалу j-го найменування, грн/кг;

K_j – коефіцієнт транспортних витрат, ($K_j = 1{,}1 \ldots 1{,}15$);

B_j – маса відходів j-го найменування, кг;

$Ц_{вj}$ – вартість відходів j-го найменування, грн/кг.

$M_1 = 3 \cdot 93{,}00 \cdot 1{,}03 - 0 \cdot 0 = 287{,}37$ *грн.*

Проведені розрахунки зведемо до таблиці.

Таблиця 5.6 – Витрати на матеріали

Найменування матеріалу, марка, тип, сорт	Ціна за 1 кг, грн	Норма витрат, кг	Величина відходів, кг	Ціна відходів, грн/кг	Вартість витраченого матеріалу, грн
Тека для паперів CALIPSO BOX	93,00	3	0	0	287,37
Папір для записів Calipso Parers Light A5	113,00	4	0	0	465,56
Офісний папір Calipso Plus A4-500-80	214,00	3	0	0	661,26

Органайзер офісний Calipso Office	157,00	3	0	0	485,13
Картридж для принтера Canon LBP6500	1128,00	1	0	0	1161,84
Канцелярське приладдя (набір офісного працівника)	194,00	3	0	0	599,46
Диск оптичний NewLine CD-RW	27,50	4	0	0	113,30
USB Flesh-пам'ять Kingston 16 GB	159,00	1	0	0	163,77
Всього					3937,69

5.2.4 Розрахунок витрат на комплектуючі

Витрати на комплектуючі *($К_в$)*, які використовують при проведенні НДР на тему «Комплексні системи моніторингу інфраструктури телекомунікаційної системи», розраховуємо, згідно з їхньою номенклатурою, за формулою:

$$К_в = \sum_{j=1}^{n} Н_j \cdot Ц_j \cdot К_j \qquad (5.8)$$

де $Н_j$ – кількість комплектуючих j-го виду, шт.;

$Ц_j$ – покупна ціна комплектуючих j-го виду, грн;

$К_j$ – коефіцієнт транспортних витрат, ($К_j$ *= 1,1 … 1,15*).

$К_в = 1 \cdot 5915,00 \cdot 1,05 = 6210,75$ *грн.*

Проведені розрахунки зведемо до таблиці.

Таблиця 5.7 – Витрати на комплектуючі

Найменування комплектуючих	Кількість, шт.	Ціна за штуку, грн	Сума, грн
Мультикор Roxtone SFBN0804L10, 12 каналів, довжина 10 м	1	5915,00	6210,75
Конектор обжимний	12	8,00	100,80
Кабель мережевий	20	16,00	336,00
Адаптери	4	789,00	3313,80
Всього			9961,35

5.2.5 Спецустаткування для наукових (експериментальних) робіт

До статті «Спецустаткування для наукових (експериментальних) робіт» належать витрати на виготовлення та придбання спецустаткування необхідного для проведення досліджень, також витрати на їх проектування, виготовлення, транспортування, монтаж та встановлення.

Балансову вартість спецустаткування розраховуємо за формулою:

$$B_{спец} = \sum_{i=1}^{k} Ц_i \cdot C_{пр.i} \cdot K_i \ , \qquad (5.9)$$

де $Ц_i$ – ціна придбання одиниці спецустаткування даного виду, марки, грн;

$C_{пр.i}$ –кількість одиниць устаткування відповідного найменування, які придбані для проведення досліджень, шт.;

K_i – коефіцієнт, що враховує доставку, монтаж, налагодження устаткування тощо, (K_i = *1,10…1,12);*

k – кількість найменувань устаткування.

$B_{спец} = 52899{,}00 \cdot 1 \cdot 1{,}04 = 55014{,}96$ *грн.*

Отримані результати зведемо до таблиці:

Таблиця 5.8 – Витрати на придбання спецустаткування по кожному виду

Найменування устаткування	Кількість, шт	Ціна за одиницю, грн	Вартість, грн
Персональний комп'ютер із процесором s1366 Intel Core i7-950 3.06-3.36GHz 4/8 8MB DDR3 800/1066 130W (4 ядра, 8 потоків)	1	52899,00	55014,96
КОНЦЕНТРАТОР VINGA TYPE-C TO 4K HDMI+2*USB3.0+SD+TF+PD+ USB-C 3.1 GEN10	1	929,00	966,16
Комутатор TP-LINK TL-SG105	1	699,00	726,96
Принт-сервер DIGITUS Fast Ethernet, NAS, 1xRJ45, 1xUSB A 2.0 (DN-13020)	1	2662,00	2768,48
Маршрутизатор TP-Link ER605	1	2499,00	2598,96
Всього			62075,52

5.2.6 Програмне забезпечення для наукових (експериментальних) робіт

До статті «Програмне забезпечення для наукових (експериментальних) робіт» належать витрати на розробку та придбання спеціальних програмних засобів і програмного забезпечення, (програм, алгоритмів, баз даних) необхідних для проведення досліджень, також витрати на їх проектування, формування та встановлення.

Балансову вартість програмного забезпечення розраховуємо за формулою:

$$B_{прг} = \sum_{i=1}^{k} Ц_{iпрг} \cdot C_{прг.i} \cdot K_i \ , \qquad (5.10)$$

де $Ц_{iпрг}$ – ціна придбання одиниці програмного засобу даного виду, грн;

$C_{прг.i}$ – кількість одиниць програмного забезпечення відповідного найменування, які придбані для проведення досліджень, шт.;

K_i – коефіцієнт, що враховує інсталяцію, налагодження програмного засобу тощо, (K_i = *1,10…1,12);*

k – кількість найменувань програмних засобів.

$B_{прг} = 5789,00 \cdot 1 \cdot 1,01 = 5846,89$ *грн.*

Отримані результати зведемо до таблиці:

Таблиця 5.9 – Витрати на придбання програмних засобів по кожному виду

Найменування програмного засобу	Кількість, шт	Ціна за одиницю, грн	Вартість, грн
Програмний продукт проектування та дослідження мереж Zabbix	1	5789,00	5846,89
Всього			5846,89

5.2.7 Амортизація обладнання, програмних засобів та приміщень

В спрощеному вигляді амортизаційні відрахування по кожному виду обладнання, приміщень та програмному забезпеченню тощо, розраховуємо з використанням прямолінійного методу амортизації за формулою:

$$A_{обл} = \frac{Ц_б}{T_в} \cdot \frac{t_{вик}}{12} \ , \qquad (5.11)$$

де $Ц_б$ – балансова вартість обладнання, програмних засобів, приміщень тощо, які використовувались для проведення досліджень, грн;

$t_{вик}$ – термін використання обладнання, програмних засобів, приміщень під час досліджень, місяців;

$T_в$ – строк корисного використання обладнання, програмних засобів, приміщень тощо, років.

$A_{обл} = (8555,00 \cdot 1) / (5 \cdot 12) = 142,58$ *грн.*

Проведені розрахунки зведемо до таблиці.

Таблиця 5.10 – Амортизаційні відрахування по кожному виду обладнання

Найменування обладнання	Балансова вартість, грн	Строк корисного використання, років	Термін використання обладнання, місяців	Амортизаційні відрахування, грн
Оргтехніка	8555,00	5	1	142,58
Пакет прикланого програмного забезпечення розробки	8526,00	3	1	236,83
Персональний комп'ютер інженера-дослідника	29699,00	3	1	824,97
Персональний комп'ютер системи обчислення даних	42355,00	3	1	1176,53
Приміщення дослідної лабораторії	416500,00	30	1	1156,94
Пристрій виводу інформації	6850,00	5	1	114,17
Робоче місце дослідника	8210,00	7	1	97,74

телекомунікаційних систем				
Всього				3749,77

5.2.8 Паливо та енергія для науково-виробничих цілей

Витрати на силову електроенергію (B_e) розраховуємо за формулою:

$$B_e = \sum_{i=1}^{n} \frac{W_{yi} \cdot t_i \cdot Ц_e \cdot K_{вni}}{\eta_i}, \quad (5.12)$$

де W_{yi} – встановлена потужність обладнання на визначеному етапі розробки, кВт;

t_i – тривалість роботи обладнання на етапі дослідження, год;

$Ц_e$ – вартість 1 кВт-години електроенергії, грн; (вартість електроенергії визначається за даними енергопостачальної компанії), приймемо $Ц_e$ = 7,50 грн;

$K_{вni}$ – коефіцієнт, що враховує використання потужності, $K_{вni} < 1$;

η_i – коефіцієнт корисної дії обладнання, $\eta_i < 1$.

$B_e = 0,45 \cdot 120,0 \cdot 7,50 \cdot 0,95 / 0,97 = 405,00$ *грн.*

Проведені розрахунки зведемо до таблиці.

Таблиця 5.11 – Витрати на електроенергію

Найменування обладнання	Встановлена потужність, кВт	Тривалість роботи, год	Сума, грн
Персональний комп'ютер із процесором s1366 Intel Core i7-950 3.06-3.36GHz 4/8 8MB DDR3 800/1066 130W (4 ядра, 8 потоків)	0,45	120,0	405,00

Оргтехніка	0,26	15,0	29,25
Персональний комп'ютер інженера-дослідника	0,40	160,0	480,00
Персональний комп'ютер системи обчислення даних	0,25	160,0	300,00
Пристрій виводу інформації	0,23	6,0	10,35
Робоче місце дослідника телекомунікаційних систем	0,10	160,0	120,00
Всього			1344,60

5.2.9 Службові відрядження

До статті «Службові відрядження» дослідної роботи на тему «Комплексні системи моніторингу інфраструктури телекомунікаційної системи» належать витрати на відрядження штатних працівників, працівників організацій, які працюють за договорами цивільно-правового характеру, аспірантів, зайнятих розробленням досліджень, відрядження, пов’язані з проведенням випробувань машин та приладів, а також витрати на відрядження на наукові з’їзди, конференції, наради, пов’язані з виконанням конкретних досліджень.

Витрати за статтею «Службові відрядження» розраховуємо як 20…25% від суми основної заробітної плати дослідників та робітників за формулою:

$$B_{св} = (З_о + З_р) \cdot \frac{Н_{св}}{100\%}, \qquad (5.13)$$

де $Н_{св}$ – норма нарахування за статтею «Службові відрядження», приймемо $Н_{св} = 20\%$.

$B_{св}$ = (38460,00 + 1429,16) · 20 / 100% = 7977,83 грн.

5.2.10 Витрати на роботи, які виконують сторонні підприємства, установи і організації

Витрати за статтею «Витрати на роботи, які виконують сторонні підприємства, установи і організації» розраховуємо як 30…45% від суми основної заробітної плати дослідників та робітників за формулою:

$$B_{сп} = (З_о + З_р) \cdot \frac{Н_{сп}}{100\%}, \quad (5.14)$$

де $Н_{сп}$ – норма нарахування за статтею «Витрати на роботи, які виконують сторонні підприємства, установи і організації», приймемо $Н_{сп}$= 30%.

$B_{сп}$ = (38460,00 + 1429,16) · 30 / 100% = 11966,75 грн.

5.2.11 Інші витрати

До статті «Інші витрати» належать витрати, які не знайшли відображення у зазначених статтях витрат і можуть бути віднесені безпосередньо на собівартість досліджень за прямими ознаками.

Витрати за статтею «Інші витрати» розраховуємо як 50…100% від суми основної заробітної плати дослідників та робітників за формулою:

$$І_в = (З_о + З_р) \cdot \frac{Н_{ів}}{100\%}, \quad (5.15)$$

де $Н_{ів}$ – норма нарахування за статтею «Інші витрати», приймемо $Н_{ів}$ = 50%.

$І_в$ = (38460,00 + 1429,16) · 50 / 100% = 19944,58 грн.

5.2.12 Накладні (загальновиробничі) витрати

До статті «Накладні (загальновиробничі) витрати» належать: витрати, пов'язані з управлінням організацією; витрати на винахідництво та раціоналізацію; витрати на підготовку (перепідготовку) та навчання кадрів; витрати, пов'язані з набором робочої сили; витрати на оплату послуг банків; витрати, пов'язані з освоєнням виробництва продукції; витрати на науково-технічну інформацію та рекламу та ін.

Витрати за статтею «Накладні (загальновиробничі) витрати» розраховуємо як 100…150% від суми основної заробітної плати дослідників та робітників за формулою:

$$B_{нзв} = (З_о + З_р) \cdot \frac{Н_{нзв}}{100\%}, \quad (5.16)$$

де $Н_{нзв}$ – норма нарахування за статтею «Накладні (загальновиробничі) витрати», приймемо $Н_{нзв}$ = 100%.

$В_{нзв}$ = (38460,00 + 1429,16) · 100 / 100% = 39889,16 грн.

Витрати на проведення науково-дослідної роботи на тему «Комплексні системи моніторингу інфраструктури телекомунікаційної системи» розраховуємо як суму всіх попередніх статей витрат за формулою:

$$B_{заг} = З_о + З_р + З_{дод} + З_н + М + К_в + В_{спец} + В_{прг} + А_{обл} + В_е + В_{св} + В_{сп} + І_в + В_{нзв}. \quad (5.17)$$

$В_{заг}$= 38460,00 +1429,16 +3988,92 +9653,18 +3937,69 +9961,35 +62075,52 + 5846,89 + 3749,77 +1344,60 +7977,83 +11966,75 +19944,58 +39889,16 = 220225,40 грн.

Загальні витрати *ЗВ* на завершення науково-дослідної (науково-технічної) роботи та оформлення її результатів розраховується за формулою:

$$ЗВ = \frac{B_{заг}}{\eta}, \quad (5.18)$$

де η - коефіцієнт, який характеризує етап (стадію) виконання науково-дослідної роботи, приймемо η=0,9.

ЗВ = 220225,40 / 0,9 = 244694,89 грн.

5.3 Оцінювання важливості та наукової значимості науково-дослідної роботи

Оцінювання та доведення ефективності виконання науково-дослідної роботи фундаментального чи пошукового характеру є достатньо складним процесом і часто базується на експертних оцінках, тому має вірогідний характер.

Для обґрунтування доцільності виконання науково-дослідної роботи на тему «Комплексні системи моніторингу інфраструктури телекомунікаційної системи» використовується спеціальний комплексний показник, що враховує важливість, результативність роботи, можливість впровадження її результатів у виробництво, величину витрат на роботу.

Комплексний показник K_P рівня науково-дослідної роботи може бути розрахований за формулою:

$$K_P = \frac{I^n \cdot T_C \cdot R}{B \cdot t}, \qquad (5.19)$$

де I – коефіцієнт важливості роботи. Приймемо $I = 4$;

n – коефіцієнт використання результатів роботи; $n = 0$, коли результати роботи не будуть використовуватись; $n = 1$, коли результати роботи будуть використовуватись частково; $n = 2$, коли результати роботи будуть використовуватись в дослідно-конструкторських розробках; $n = 3$, коли

результати можуть використовуватись навіть без проведення дослідно-конструкторських розробок. Приймемо n=2;

T_C – коефіцієнт складності роботи. Приймемо $T_C = 3$;

R – коефіцієнт результативності роботи; якщо результати роботи плануються вище відомих, то $R = 4$; якщо результати роботи відповідають відомому рівню, то $R = 3$; якщо нижче відомих результатів, то $R = 1$. Приймемо $R = 3$;

B – вартість науково-дослідної роботи, тис. грн. Приймемо B =244694,89 грн;

t – час проведення дослідження. Приймемо t = 0,08 років, (1 міс.).

Визначення показників I, n, T_C, R, B, t здійснюється експертним шляхом або на основі нормативів [23].

$$K_P = \frac{I^n \cdot T_C \cdot R}{B \cdot t} = 4^2 \cdot 3 \cdot 3 \,/\, 244{,}7 \cdot 0{,}08 = 7{,}06.$$

Якщо $K_P > 1$, то науково-дослідну роботу на тему «Комплексні системи моніторингу інфраструктури телекомунікаційної системи» можна вважати ефективною з високим науковим, технічним і економічним рівнем.

5.4 Висновок до розділу 4

Витрати на проведення науково-дослідної роботи на тему «Комплексні системи моніторингу інфраструктури телекомунікаційної системи» складають 244694,89 грн. Відповідно до проведеного аналізу та розрахунків рівень наукового ефекту проведеної науково-дослідної роботи на тему «Комплексні системи моніторингу інфраструктури телекомунікаційної системи» є середній, а дослідження актуальними, рівень доцільності виконання науково-дослідної

роботи $K_P > 1$, що свідчить про потенційну ефективність з високим науковим, технічним і економічним рівнем.

6. ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ

У приміщенні, де відбувалася розробка комплексних систем моніторингу інфраструктури телекомунікаційної мережі присутні такі шкідливі та небезпечні фактори [25]:

- підвищена чи понижена температура повітря робочої зони;
- недостатнє освітлення робочої зони;
- недостатність природного освітлення;
- підвищений рівень шуму на робочому місці;
- відсутність чи нестача природного світла;
- фізичні перевантаження (статичні);
- нервово - психічні перевантаження (перенапруга аналізаторів, емоційні навантаження).

Відповідно до визначених факторів формуємо рекомендації щодо безпечних умов праці під час виконання роботи.

6.1 Технічні рішення щодо безпечного виконання роботи

Роботодавець повинен забезпечити гігієнічні й ергономічні вимоги щодо організації робочих приміщень для експлуатації ПК, робочого середовища, робочих місць з ПК, режиму праці і відпочинку при роботі з ПК тощо, які викладені у Правилах.

Основні вимоги до виробничого приміщення для експлуатації ПК:

- приміщення не може бути розміщено у підвалах та цокольних поверхах;
- площа на одне робоче місце в такому приміщенні повинна становити не менше 6,0м^2, а об’єм не менше 20,0 м^3;
- приміщення повинно мати природне та штучне освітлення відповідно до ДБН В.2.5-28-2018 [29];
- необхідно щоденно проводити вологе прибирання;

– поруч з приміщенням для роботи з ПК мають бути обладнані: побутова кімната для відпочинку під час роботи; кімната психологічного розвантаження.

Організація робочого місця користувача комп'ютера повинна забезпечувати відповідність усіх елементів робочого місця та їх взаємного розташування ергономічним вимогам. Виконуючи практичні завдання щодо використання робочої пози, потрібно:

– зменшувати величину статичних напружень;

– розподіляти статичні напруження;

– передбачати можливість змін пози під час роботи.

Для роботи операторів ПК у положенні сидячи рекомендовані такі параметри робочого простору: ширина - не менше 700 мм, глибина - не менше 400 мм, висота робочої поверхні над підлогою – 700 …750 мм. Під робочою поверхнею необхідно передбачити простір для ніг: висота - менше 600 мм, ширина - не менше 500 мм, глибина - не менше 400 мм. За необхідності огляду робочого місця його висота не повинна перевищувати 1200 мм

Під час роботи сидячи нижня частина корпуса розслаблена, а основне статичне навантаження припадає на м'язи шиї, спини, таза, стегон. Неправильна сидяча поза може викликати застій крові в ногах, а якщо виконується великий обсяг роботи для пальців рук – запалення суглобів.

При проектуванні письмового столу варто враховувати наступне:

– висота столу повинна бути обрана з урахуванням можливості сидіти вільно, у зручній позі, при необхідності спираючи на підлокітники;

– нижня частина столу повинна бути сконструйована так, щоб оператор міг зручно сидіти, не був змушений підбирати ноги;

– поверхня столу повинна мати властивості, що виключають появу відблисків у поле зору оператора;

– конструкція столу повинна передбачати наявність висувних шухляд (не менш 3-х для збереження документації, канцелярського приладдя, особистих речей).

На робочому місці розробника комплексних систем моніторингу інфраструктури телекомунікаційної мережі існує небезпека поразки електричним струмом. Електричний струм, впливаючи на тіло людини, може заподіяти йому явні чи приховані пошкодження, в тому числі опіки всього тіла або окремих його ділянок; електричні удари характерні внутрішніми ушкодженнями тощо.

Приміщення, де виконується робота, згідно ПУЕ «Правила влаштування електроустановок» класифікується як приміщення без підвищеної небезпеки [35].

Безпечна експлуатація електроустановок здійснюється у відповідності з вимогами ПУЕ [35] та «Правила безпечної експлуатації електроустановок» [31] і передбачає такі заходи та засоби:

– недоступність струмоведучих частин, прокладання електрокабелів під підлогою, в спеціальних каналах, скрите виконання освітлювальної проводки, ізоляцію струмо-провідних елементів ($R_{із} \geq 0.5$ МОм);

– захисне заземлення всіх металевих струмопровідних частин електроустановок та ПК ($R_{з\ доп} \leq$ 4 Ом);

– використання пониженої напруги 36 В (для аварійного освітлення щита) в операторському пункті та виробничому приміщені;

– застосування попереджувальної сигналізації, написів, плакатів при проведенні планово-попереджувальних ремонтів і профілактичних випробувань електрообладнання;

– проведення організаційних заходів (спеціальне навчання, атестація та переатестація осіб електротехнічного персоналу, інструктажі тощо).

6.2. Технічні рішення з гігієни праці та виробничої санітарії

6.2.1 Мікроклімат

Температура, відносна вологість, швидкість руху повітря біля тіла людини, а також температура стін і навколишніх предметів утворюють мікроклімат на робочому місці. Температуру, відносну вологість і швидкість руху повітря вимірюють на висоті 1,0 м від підлоги або робочої площадки при роботах, що виконуються сидячи, і на висоті 1,5 м – при роботах, що виконуються стоячи, і не ближче 1 м від нагрівальних приладів і зовнішніх стін.

Робота, яка виконується розробником комплексних систем моніторингу інфраструктури телекомунікаційної мережі згідно за енерговитратами відноситься до категорії I а (енерговитрати до 139Дж/с) [24]. Допустимі параметри мікроклімату для цієї категорії наведені в табл.6.1.

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

Таблиця 6.1 – Параметри мікроклімату

Для забезпечення комфортних умов використовуються як організаційні методи (раціональна організація проведення робіт залежно від пори року і доби, чергування праці і відпочинку), так і технічні засоби (вентиляція, кондиціонування повітря, опалювальна система).

6.2.2. Склад повітря робочої зони

Забруднення повітря робочої зони регламентується граничнодопустимими концентраціями (ГДК) в мг/м^3 згідно ДСН 3.3.6.042-99 [33]. Джерелами запиленості повітря в приміщенні є одяг людей і пил, що проникає з вулиці. У

приміщенні немає значного виділення шкідливих газів. ГДК шкідливих речовин, які знаходяться в досліджуваному приміщені, наведені в таблиці 6.2.

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

Таблиця 6.2 – ГДК шкідливих речовин у повітрі

Параметри іонного складу повітря на робочому місці, що обладнане ПК, повинні відповідати допустимим нормам (табл.6.3).

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

Таблиця 6.3 – Рівні іонізації повітря приміщень при роботі на ПК

Забезпечення складу повітря робочої зони здійснюється за допомогою системи припливно-витяжної вентиляції, регулярного провітрювання, та вологого прибирання.

6.2.3 Виробниче освітлення

Правильно спроектоване освітлення, яке відповідає вимогам санітарних норм здійснює позитивний психологічний вплив на працівника, знижує втому, створює оптимальні умови для роботи органів зору, і тим самим підвищує безпеку праці і знижує травматизм.

Освітлення створюється природним сонячним світлом (природне) і світлом від електричних ламп (штучне). Природне освітлення є найсприятливішим для людини, так як сонячне світло має оптимальний спектр, в ньому наявна достатня кількість ультрафіолетових променів. Штучне освітлення передбачається у приміщеннях, де недостатньо природного світла, і для освітлення у вечірні та нічні години.

Норми освітленості при штучному освітленні та КПО (для III пояса світлового клімату) при природному та сумісному освітленні, які необхідно забезпечити під час виконання роботи зазначені у таблиці 6.4 (за ДБН В.2.5-28-2018 Природне і штучне освітлення [29]):

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 або верхнє	Бокове	Верхнє або верхнє	Бокове
Високої точності	0,3 – 0,5	III	г	великий	світлий	700	300	5	2	3	1,2

Таблиця 6.4 - Норми освітленості в приміщенні

Для забезпечення достатнього освітлення передбачені такі заходи:

1) Максимальне використання бічного природного освітлення.

2) Систематичне очищення скла від бруду.

3) Використання жалюзі на вікнах для регулювання кількості природного світла у приміщенні.

4) Загальне штучне освітлення створюється за допомогою люмінесцентних ламп.

6.2.4 Виробничий шум

Шум визначають як сукупність аперіодичних звуків різної інтенсивності та частоти. Шум заважає роботі, знижує працездатність і продуктивність праці, при тривалій і інтенсивній дії викликає захворювання організму.

У закритих приміщеннях шум, багаторазово відбиваючись від стін та стелі, посилюється. Тому рекомендується проводити їх акустичну обробку за допомогою звукопоглинальних облицювань з пористих матеріалів, які мають великий коефіцієнт звукопоглинання.

Нормативним документом, який регламентує рівні шуму для різних категорій робочих місць службових приміщень, є ДСН 3.3.6.037-99 [32].

Характер робіт	Допустимі рівні звукового тиску (дБ) в стандартизованих октавних смугах зі середньогеометричними частинами (Гц)									Допуст-мий рівень звуку, дБА
	32	63	125	250	500	1000	2000	4000	8000	
Виробничі приміщення	86	71	61	54	49	45	42	40	38	50

Таблиця 6.5 - Рівень звукового тиску

Для зменшення шуму здійснюють своєчасний ремонт та профілактику обладнання.

6.2.5. Виробничі випромінювання

На робочому місці розробника комплексних систем моніторингу інфраструктури телекомунікаційної мережі у зв’язку із експлуатацією електричної апаратури, існує ризик виникнення підвищеного рівня електромагнітного випромінювання.

Ступінь біологічного впливу електромагнітних полів на організм людини залежить від частоти коливань, напруженості та інтенсивності поля, тривалості його впливу.

Підвищений рівень електромагнітних випромінювань шкодить здоров’ю людини. Від цього страждає передусім нервова і серцево-судинна системи, виникають головний біль і перевтома, знижується точність робочих рухів,

порушується сон. Електромагнітне випромінювання викликає зміни тиску крові, гіпотонію або гіпертонію.

Рівні електромагнітних випромінювань моніторів, які вважаються безпечними для здоров'я користувачів, регламентуються нормами MPR II 1990:10 Шведського національного комітету з вимірювань та досліджень (табл.6.6) [34, с.348].

Вид поля	TCO	MPR II
Змінне електричне поле 5 Гц – 2 кГц 2 кГц – 400 кГц	10 В/м 1 В/м на відстані 0,3 м від центра екрана і 0,5 м навколо монітора	2,5 В/м 2,5 В/м на відстані 0,5 м навколо монітора
Змінне магнітне поле 5 Гц – 2 кГц 2 кГц – 400 кГц	250 нТл 200 мА/м 25 нТл 20 мА/м на відстані 0,3 м від центра екрана і 0,5 м навколо монітора	250 нТл 200 мА/м 25 нТл 20 мА/м на відстані 0,5 м навколо монітора

Таблиця 6.6 - Допустимі рівні випромінювань моніторів ПК

Для захисту людини від дії електромагнітних випромінювань використовують обмеження часу перебування персоналу в робочій зоні та встановлюють раціональні режими експлуатації ПК і роботи працюючого персоналу.

6.3 Безпека в надзвичайних ситуаціях. Дослідження безпеки роботи в умовах дії загрозливих чинників надзвичайних ситуацій

6.3.1 Дія радіації на живі організми

Так як 70% маси тіла складається з води, то під впливом радіації розпочинається утворення вільних радикалів гідроксокгрупи і гідрогени, які в свою чергу утворюють пероксид гідрогену. Утворені радикали окислюють і відновлюють молекули органічних сполук. Цими речовинами є білки, ліпіди, нуклеопротеїди, ферменти та інші.

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.

Біологічна дія залежить від виду випромінювання. Залежно від передатної енергії зарядженій частці на одиницю довжини пробігу в речовині всі іонізуючі випромінювання ділять на рідко-іонізуючі і щільно-іонізуючі. Довжина пробігу частинок випромінювання в людському організмові називається лінією передачі енергії.

Лінія передачі енергії заряджених частинок збільшується при зниженні їх швидкості тому в кінці пробігу віддана енергія найбільша.

Наявність прихованого періоду дії реакції. Прихованим періодом називається проміжок часу, що охоплює період від моменту опромінення до появи змін, які реєструються клінічно. Тривалість цього періоду зворотно-пропорційна поглинутій дозі. Чим вища поглинута доза тим коротший прихований період.

Властивість кумуляції – накопичення. Це означає, якщо якась ділянку опромінювати кілька раз, то загальний біологічний ефект залежить від загальної поглинутої дози.

У формуванні біологічного ефекту особливу роль відіграє діяльність інтегруючих систем організму – нервової системи, ендокринного апарату гуморальної системи, що утворилася внаслідок опромінення.

Кінцевим результатом біологічної дії ультра-випромінювання є виникнення променевих хвороб різних ступенів важкості.

Для зниження рівня забруднення радіоактивними речовинами використовують дезактивацію.

6.3.2 Визначення товщин захисних шарів сховища в умовах радіоактивного випромінювання

Вихідні дані: $t_п$ = 1,6 год; $t_к$ = 10,7 год; P_{1max} = 270 Р/год; $Д_д$ = 2,6 Р; $h_1 = h_2$; сховище – окремо розташоване.

Коефіцієнт послаблення для сховища визначається за формулою

$$K_{посл.сх} = K_P \prod_{i=1}^{n} 2^{h_i/d_i}, \qquad (6.3.1)$$

де $K_р$ – коефіцієнт розташування сховища (для окремо розташованих $K_р$ = 1);

n – кількість захисних шарів перекриття;

d_i – товщина половинного ослаблення і-го захисного шару, см;

h_i – товщина i-го захисного шару, см.

Так як за умовою задачі $h_1 = h_2 = h$, то попередня формула зводиться до наступної

$$K_{посл.сх} = K_P 2^{h/d_1} 2^{h/d_2} = K_P 2^{2h(1/d_1+1/d_2)}, \qquad (6.3.2)$$

звідки можна виразити товщину захисного шару

$$h = \frac{\lg(K_{посл.сх}/K_P)}{2(1/d_1+1/d_2)\lg 2} \text{ [см]}. \qquad (6.3.3)$$

Коефіцієнт послаблення для сховища можна виразити із формули

$$Д_Д = \frac{1{,}33 P_{1\max}\left(\sqrt[4]{t_к^3} - \sqrt[4]{t_п^3}\right)}{K_{посл.сх}} \text{ [Р]}, \qquad (6.3.4)$$

звідки

$$K_{посл.сх} = \frac{1{,}33 P_{1\max}\left(\sqrt[4]{t_к^3} - \sqrt[4]{t_п^3}\right)}{Д_Д}; \qquad (6.3.5)$$

$$K_{посл.сх} = \frac{1{,}33 \cdot 270\left(\sqrt[4]{10{,}7^3} - \sqrt[4]{1{,}6^3}\right)}{2{,}6} = 621.$$

Товщина шару половинного ослаблення для радіоактивного зараження: бетон – d_1 = 5,7 см, ґрунт – d_2 = 8,1 см.

Отже, товщини захисних шарів бетону та ґрунту дорівнюють

$$h_1 = h_2 = h = \frac{\lg(621/1)}{2(1/5{,}7+1/8{,}1)\lg 2} = 15{,}49 \text{ (см)}.$$

Висновки до розділу 6

Встановлено, що товщини захисних шарів бетону та ґрунту для захисту від радіоактивного випромінювання мають складати 15,49 см.

ВИСНОВКИ

У цій магістерській роботі пояснюється, як використовувати моніторинг Zabbix для тестування вашої мережі за допомогою розширених протоколів безпеки та компіляції аналізу збоїв мережевого обладнання. Розкриваються всі переваги та недоліки цієї системи.

У ході дослідження було проведено аналіз сучасних комплексних систем моніторингу інфраструктури телекомунікаційної мережі. Було визначено, що такі системи є важливим інструментом для забезпечення безперебійної роботи та безпеки телекомунікаційних мереж.

Особливу увагу було приділено системі Zabbix, яка є однією з найпопулярніших систем моніторингу на ринку. Було розглянуто основні можливості системи Zabbix, її переваги та недоліки.

На основі проведеного дослідження було розроблено технічне рішення для збору даних та тестування продуктивності SNMP для сервера Zabbix. Це рішення дозволяє збирати дані про стан сервера Zabbix за допомогою SNMP, тестувати продуктивність SNMP та надсилати сповіщення про потенційні проблеми.

Також було розроблено рекомендації щодо підвищення ефективності збору даних та тестування продуктивності SNMP для сервера Zabbix. Ці рекомендації включають використання широкого спектру параметрів моніторингу, налаштування сповіщень та регулярний аналіз даних моніторингу.

У висновку можна сказати, що система Zabbix є ефективним інструментом для моніторингу інфраструктури телекомунікаційної мережі. Вона має широкий спектр можливостей, які дозволяють забезпечити надійне та ефективне моніторування.

На основі проведеного дослідження можна зробити наступні рекомендації щодо використання системи Zabbix для моніторингу інфраструктури телекомунікаційної мережі:

Використовуйте широкий спектр параметрів моніторингу. Це допоможе вам отримати більш точне уявлення про стан вашої мережі.

Налаштуйте сповіщення таким чином, щоб вони надсилалися про потенційні проблеми. Це допоможе вам швидко усунути проблеми, перш ніж вони призведуть до збоїв у роботі мережі.

Регулярно аналізуйте дані моніторингу. Це допоможе вам виявити тенденції та можливі проблеми.

Крім того, можна порекомендувати наступні заходи для підвищення ефективності моніторингу:

Автоматизуйте процеси моніторингу. Це допоможе вам звільнити час для інших завдань.

Інтегруйте систему моніторингу з іншими системами. Це допоможе вам отримати більш повний огляд стану вашої мережі.

Застосування цих рекомендацій допоможе вам отримати максимальну користь від використання системи Zabbix для моніторингу інфраструктури телекомунікаційної мережі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Network Monitoring Approaches: An Overview [Електронний ресурс] — Режим доступу: (PDF) Network Monitoring Approaches: An Overview (researchgate.net)

2. Matityahu, E.; Shaw, R.; Carpio, D.; aj.: Gigabits zero-delay tap and methods thereof. 2011, [cit. 2015-04-21], uS Patent App. 13/034,730. [Електронний ресурс] — Режим доступу: http://www.google.com/patents/US20110211446

3. Cisco Systems, Inc.: Catalyst Switched Port Analyzer (SPAN) Configuration Example Cisco [online]. [cit. 2015-04-21].

4. KELLY, J.: An Examination of Pattern Matching Algorithms for Intrusion Detection Systems. Master's thesis, Ottawa Carleton Institute for Computer Science, Carleton University, Canada, 2006.

5. Rohde & Schwarz (Ed.) (2006). R&S ETX DTV Monitoring Receiver operating manual, 2068.0909.12 – 02. Munich: Rohde & Schwarz.

6. Програмне забезпечення для моніторингу мережі. [Електронний ресурс] – Режим доступу до ресурсу: http://www.spiceworks.com/free-networkmonitoring-management-software.

7. Моніторинг та керування мережею. [Електронний ресурс] – Режим доступу ресурсу: http://aggregate.tibbo.com/solutions/network_management/network_monitoring

8. Особливості Zabbix. [Електронний ресурс] – Режим доступу до ресурсу: http://www.zabbix.com/features.php. Згадана

9. Проектування пакетів. [Електронний ресурс] – Режим доступу до ресурсу: http://www.networkworld.com/article/2338253/infrastructure-management.

10. Маршрутна аналітика. [Електронний ресурс] – Режим доступу до ресурсу: http://www.glennodonnell.com/documents/d2751-RouteAnalytics.

11. Покращення моніторингу мережі за допомогою Route Analytics. Дизайн пакетів. [Електронний ресурс] – Режим доступу до ресурсу: http://www.packetdesign.com/resources/white-papers.

12. Zabbix True Open Source. [Електронний ресурс] – Режим доступу до ресурсу: http://www.zabbix.com/true_open_source.php.

13. Безагентний моніторинг. [Електронний ресурс] – Режим доступу до ресурсу: http://www.eginnovations.com/web/egagentles.

14. Моніторинг мережі. [Електронний ресурс] – Режим доступу до ресурсу:

http://www.helpsystems.com/intermapper/network-monitoring.

15. 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.

16. Zabbix автоматичне виявлення. [Електронний ресурс] – Режим доступу до ресурсу: http://www.zabbix.com/auto_discovery.php

17. Zabbix. Відкриття низького рівня. [Електронний ресурс] – Режим доступу до ресурсу: http://habrahabr.ru/company/zabbix/blog/203050

18. Zabbix. Послуги. [Електронний ресурс] – Режим доступу до ресурсу: http://www.zabbix.com/services.php

19. Zabbix. Документація. [Електронний ресурс] – Режим доступу до ресурсу: https://www.zabbix.com/documentation.

20. Налаштування моніторингу Zabbix nginx, php-fpm, apache. [Електронний ресурс] – Режим доступу до ресурсу: https://serveradmin.ru/monitoring-webservera-nginx-i-php-fpm-v-zabbix

21. Додавання точок мережі Zabbix 5.0 [Електронний ресурс] – Режим доступу до ресурсу: https://it-school.pw/dobavlenie-uzlov-seti-v-zabbix-5-0-lts

22. Моніторинг безпеки мережі Zabbix. [Електронний ресурс] – Режим доступу до ресурсу: https://habr.com/ru/post/215509

23. Методичні вказівки до виконання економічної частини магістерських кваліфікаційних робіт / Уклад. : В. О. Козловський, О. Й. Лесько, В. В. Кавецький. – Вінниця : ВНТУ, 2021. – 42 с.

24. 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

25. ДСТУ ISO 45001:2019 Системи управління охороною здоров'я та безпекою праці. Вимоги та настанови щодо застосування (ISO 45001:2018, IDT). URL: http://online.budstandart.com/ua/catalog/ doc-page.html?id_doc=88004.

26. НПАОП 0.00-4.12-05. Типове положення про порядок проведення навчання і перевірки знань з питань охорони праці. URL: http://zakon.rada.gov.ua/ laws/show/z0231-05

27. ДСТУ 8829:2019 Пожежовибухонебезпечність речовин і матеріалів. Номенклатура показників і методи їхнього визначення. Класифікація. URL: https://www.alutal.com.ua/wp-content/uploads/2021/02/ dstu-8829-2019-1.pdf

28. ДСТУ 8828:2019 Пожежна безпека. Загальні положення. URL: https://dwg.ru/dnl/15125

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

30. НАПБА.01.001-14. Правила пожежної безпеки в Україні. К. : МВС України, 2014. 47 с

31. ДБНВ.2.5-27-2006. Захисні заходи електробезпеки в електроустановках будинків і споруд. К. : Мінбуд України, 2006. 154 с

32. ДСН 3.3.6.037-99 Санітарні норми виробничого шуму, ультразвуку та інфразвуку. - [Електронний ресурс] - Режим доступу: http://document.ua/sanitarni-normi-virobnichogo-shumu-ultrazvuku-ta-infrazvuku-nor4878.html

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

33. Охорона праці та промислова безпека: навч.посіб. [К.Н.Ткачук, В.В.Зацарний, Р.Н.Сабарно та ін.]; за ред. К.Н.Ткачука, В.В.Зацарного. – К.: Основа. – 2009. – 454 с.

34. Правила улаштування електроустановок. URL: http://www.energiy. 34 com.ua/PUE.html

35. 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

36. Сакевич В. Ф. Основи розробки питань цивільної оборони в дипломних проектах / В. Ф. Сакевич. – Вінниця : ВДТУ, 2001. – 109 с.

ДОДАТКИ

Додаток А

(обов’язковий)

ІЛЮСТРАТИВНА ЧАСТИНА

КОМПЛЕКСНІ СИСТЕМИ МОНІТОРИНГУ ІНФРАСТРУКТУРИ ТЕЛЕКОМУНІКАЦІЙНОЇ МЕРЕЖІ

назва магістерської кваліфікаційної роботи

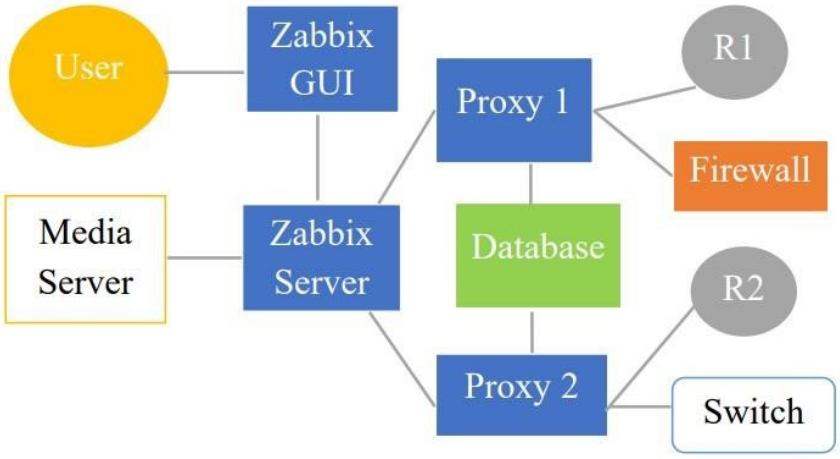


Рисунок 3.1 – Компоненти Zabbix

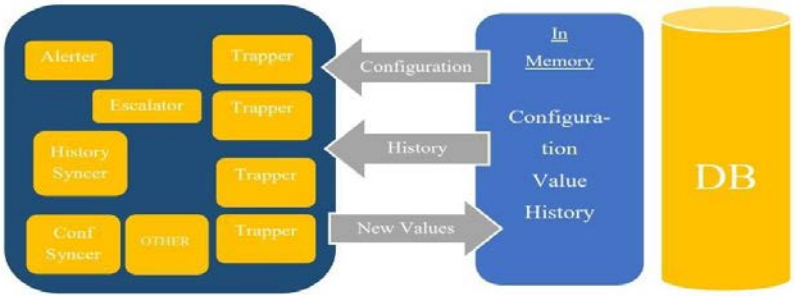


Рисунок 3.2 – Методи кешування

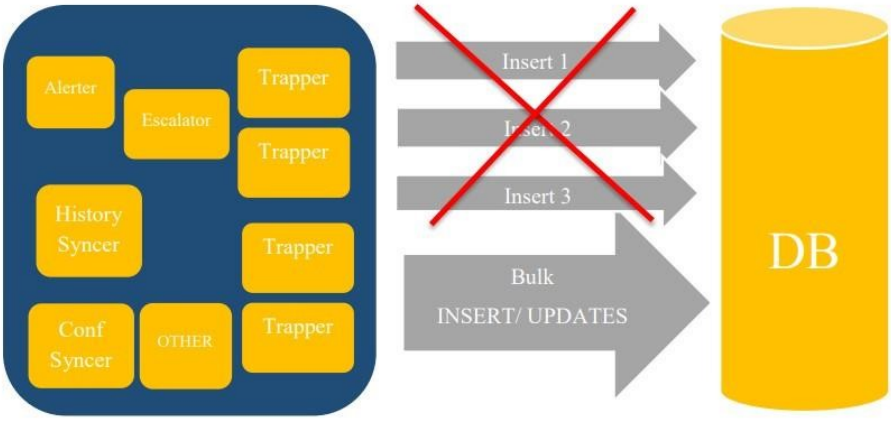
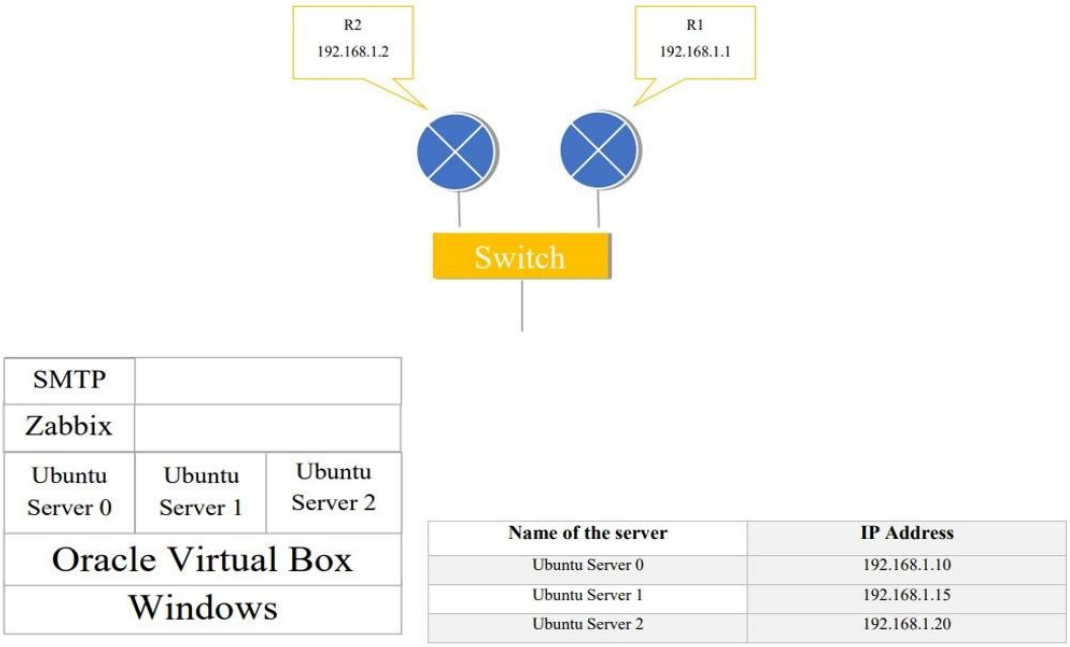


Рисунок 3.3 - Масові операції



Name of the server	IP Address
Ubuntu Server 0	192.168.1.10
Ubuntu Server 1	192.168.1.15
Ubuntu Server 2	192.168.1.20

Рисунок 4.1 - Топологія мережі

```
Router#show snmp MIB IFMib IFIndex
       13:55:48.387: %SYS-5-CONFIG_I: Configured from console by console
Serial0/0/0: Ifindex = 3
Async0/0/1: Ifindex = 8
FastEthernet0/1: Ifindex = 2
VoIP-Null0: Ifindex = 5
Null0: Ifindex = 6
Serial0/0/1: Ifindex = 4
Async0/0/0: Ifindex = 7
FastEthernet0/0: Ifindex = 1
```

Рисунок 4.5 – Вихід команди для індексу порту

Додаток Б

(обов’язковий)

Протокол перевірки кваліфікаційної роботи на наявність текстових запозичень

ПРОТОКОЛ
ПЕРЕВІРКИ КВАЛІФІКАЦІЙНОЇ РОБОТИ
НА НАЯВНІСТЬ ТЕКСТОВИХ ЗАПОЗИЧЕНЬ

Назва роботи: Комплексні системи моніторингу інфраструктури 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 95,13% Схожість 4,87%

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 _____ Васильківський М.В.
(підпис) (прізвище, ініціали)

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

Автор роботи _____ Лукашин Є.В.
(підпис) (прізвище, ініціали)

Керівник роботи _____ Оніщук О.В.
(підпис) (прізвище, ініціали)