Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Факультет комп'ютерно-інформаційних систем і програмної інженерії
(повна назва факультету)
Кафедра комп'ютерних систем та мереж
(повна назва кафедри)

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня

магістр
(назва освітнього ступеня)

на тему: *Методи підвищення ефективності та моніторингу роботи локальної комп'ютерної мережі*

Виконав(ла): студент(ка) *VI* курсу, групи *СІм-61*
спеціальності *123 «Комп'ютерна інженерія»*
(шифр і назва спеціальності)

		Кардаш І.А.
	(підпис)	(прізвище та ініціали)
Керівник		Варавін А.В.
	(підпис)	(прізвище та ініціали)
Нормоконтроль		Луцик Н.С.
	(підпис)	(прізвище та ініціали)
Завідувач кафедри		Осухівська Г.М.
	(підпис)	(прізвище та ініціали)
Рецензент		
	(підпис)	(прізвище та ініціали)

Тернопіль
2023

Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Факультет *комп'ютерно-інформаційних систем і програмної інженерії*
(повна назва факультету)

Кафедра *комп'ютерних систем та мереж*
(повна назва кафедри)

ЗАТВЕРДЖУЮ
Завідувач кафедри
Осухівська Г.М.
(підпис) (прізвище та ініціали)
« ____ » _____ 2023 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

на здобуття освітнього ступеня *магістр*
(назва освітнього ступеня)

за спеціальністю *123 «Комп'ютерна інженерія»*
(шифр і назва спеціальності)

студенту _____
(прізвище, ім'я, по батькові)

1. Тема роботи *Методи підвищення ефективності та моніторингу роботи локальної комп'ютерної мережі*

Керівник роботи *кандидат фізико-математичних наук, Варавін Антон Валерійович*
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Затверджені наказом ректора від «*1*» *січня* *2023* року № *4/7 – 1132*

2. Термін подання студентом завершеної роботи *26.12.2023*

3. Вихідні дані до роботи

4. Зміст роботи (перелік питань, які потрібно розробити)
Аналіз завдання, Аналіз можливих рішень, Вибір програмних компонентів, Створення алгоритму роботи, Реалізація проектних рішень, Тестування, Аналіз результатів.

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, слайдів)
1. Вступ.
2.Про моніторинг локальної мережі
3. Сучасні системи моніторингу
4. Критерії ефективності та параметри роботи систем моніторингу локальної мережі
5. Методи моніторингу
6. Алгоритм роботи системи моніторингу
7. Аналіз результатів моніторингу
8. Висновки.

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Охорона праці та	*Осухівська Г.М., зав. каф. КС*		
безпека в надзвичайних	*Стадник І.Я., проф. каф. ОХ*		
ситуаціях			

7. Дата видачі завдання _____

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1	*Аналіз досліджень у сфері проектування систем*	*28.09.2023 –*	*Виконано*
	моніторингу локальної комп'ютерної мережі	*10.10. 2023*	
2	*Аналіз можливих рішень*	*12.10. 2023*	*Виконано*
3	*Створення алгоритму роботи*	*16.10. 2023*	*Виконано*
4	*Реалізація системи моніторингу локальної мережі*	*25.10. 2023*	*Виконано*
5	*Виконання розділу «Охорона праці та безпека в*	*09.11. 2023 –*	*Виконано*
	надзвичайних ситуаціях»	*11.11. 2023*	
6	*Оформлення пояснювальної записки та графічного*	*15.11. 2023–*	*Виконано*
	матеріалу	*14.12. 2023*	
7	*Попередній захист кваліфікаційної роботи магістра*	*19.12. 2023*	*Виконано*
8	*Захист кваліфікаційної роботи магістра*	*26.12.2023*	

Студент _____ Кардаш І.А.
(підпис) (прізвище та ініціали)

Керівник роботи _____ Варавін А.В.
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Методи підвищення ефективності та моніторингу роботи локальної комп’ютерної мережі // Кваліфікаційна робота магістра // Кардаш Іван Анатолійович // ТНТУ, Комп’ютерна інженерія, група СІм-61 // Тернопіль, 2023 // с. –64, рис. – 25 , табл. – 2 , додат. – 2 , бібліогр. – 11.

Ключові слова: моніторинг, система, протокол, мережа, zabbix, метод моніторингу.

Кваліфікаційну роботу магістра присвячено дослідженню технологій та методів моніторингу локальної комп’ютерної мережі з метою підвищення ефективності моніторингу. Розглянуто актуальні методи моніторингу, та обрано найбільш оптимальні серед них. На основі обраних методів розроблено алгоритм роботи системи моніторингу локальної мережі, яка має вищі показники ефективності, в порівнянні з аналогами. Описано розгортання системи моніторингу, та процес моніторингу безпосередньо. Проаналізовано результати моніторингу локальної комп’ютерної мережі.

ABSTRACT

Methods to enhance efficiency and monitor the operation of a local computer network // Master's qualification work// Kardash Ivan Anatoliyovych // TNTU, Computer Engineering, group SIM-61// Ternopil , 2023 // p. - 64 , fig. - 25 , table. - 2 , append. - 2, bibliogr. - 11 .

Keywords: monitoring, system, protocol, network, zabbix, monitoring method.

The master's qualification work is devoted to the research of technologies and methods of local computer network monitoring in order to improve the monitoring efficiency. Current monitoring methods were considered, and the most optimal among them were selected. On the basis of the selected methods, an algorithm of the local network monitoring system has been developed, which has higher efficiency indicators compared to analogues. The deployment of the monitoring system and the monitoring process itself are described. The results of local computer network monitoring were analyzed.

ЗМІСТ

ВСТУП

Сучасні локальні мережі це стабільні та надійні системи обміну даними між комп'ютерами в межах підприємства, але тільки на перший погляд. Будь яка система може мати проблеми з ефективністю роботи, але щоб визначити причину втрат ефективності, необхідний спеціальний інструмент.

Актуальність теми моніторингу мережі полягає в тому що ефективний моніторинг дозволить уникнути перебоїв або збоїв в мережі. У цьому дослідженні моніторинг мережі відіграє ключову роль, оскільки для оцінки продуктивності локальної мережі необхідно отримати повну статистику її роботи. Важливо вивчити параметри, такі як пропускна здатність, затримки та завантаження мережі, щоб отримати повноцінне уявлення про ефективність мережі.

Тема наукового дослідження: Методи підвищення ефективності та моніторингу роботи локальної комп'ютерної мережі.

Мета наукового дослідження: Дослідити способи підвищення ефективності та моніторингу локальної мережі, провести моніторинг мережі та дослідити його результати.

Предмет наукового дослідження: методи підвищення ефективності та моніторингу локальної комп'ютерної мережі.

Об'єкт наукового дослідження: методи та критерії ефективності завдання моніторингу локальної мережі.

Завдання наукового дослідження:

1. Розглянути та дослідити критерії ефективності для завдання моніторингу локальної мережі;
2. Дослідити методи моніторингу локальної мережі та обрати найоптимальніші для ефективного моніторингу локальної комп'ютерної мережі;
3. Розробити алгоритм моніторингу локальної комп'ютерної мережі, на основі обраних методів;
4. Встановити обрану систему моніторингу та провести моніторинг мережі;
5. Дослідити результати моніторингу та зробити висновки.

Поставлені задачі будуть розв’язані шляхом дослідження теоретичних відомостей та проведення експериментів та тестів. Буде встановлено систему моніторингу та проведено декілька досліджень її роботи, на основі яких, буде оформлено висновки по підвищенню ефективності та продуктивності роботи.

Методи дослідження: для вирішення поставлених у дипломній роботі задач використано такі методи дослідження: системного аналізу, узагальнення, порівняння, теоретичної електротехніки, синтезу.

Наукова новизна отриманих результатів: удосконалено та підвищено ефективність системи моніторингу локальної комп’ютерної мережі. Для цього використано різні методи моніторингу локальної мережі та розроблено алгоритм. В результаті отримано метод моніторингу, який працює з вищою ефективністю, в порівнянні з методами.

Практичне значення одержаних результатів дипломної роботи полягає у тому, що запропоновані та реалізовані програмні засоби системи моніторингу локальної комп’ютерної мережі дозволяють ефективніше відстежувати стан мережі та пристроїв у ній, своєчасно запобігати проблемам з якістю чи надійністю мережі, що значно покращує якість комунікації між робочими станціями в межах підприємства.

Публікації. За результатами виконаних в кваліфікаційній роботі магістра досліджень опубліковано 2 тези наукової конференції «Інформаційні моделі, системи та технології», проведеної в ТНТУ 13-14 грудня 2023.

РОЗДІЛ 1
ОГЛЯД ТА АНАЛІЗ МЕТОДІВ МОНІТОРИНГУ ЛОКАЛЬНОЇ МЕРЕЖІ ТА МЕТОДІВ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ЇХ РОБОТИ

1.1. Огляд актуальних методів моніторингу локальних мереж

Моніторинг мережі – це систематична перевірка комп’ютерної мережі, з метою виявлення повільних чи несправних компонентів мережі, які негативно впливають як на швидкість роботи мережі так і на її пропускну здатність. До таких проблем можуть належати перевантажені або збої/заморожені сервери, несправні маршрутизатори, комутатори та інші пристрої які мають порушення в роботі. Якщо мережа вийшла з ладу або має критичні помилки, система моніторингу попереджає адміністратора мережі. Моніторинг мережі - це підмножина управління мережею. [1]

Ping, як один із основних інструментів, використовується для моніторингу мережі, а системи моніторингу мережі застосовуються для відстеження трафіку, такого як моніторинг відеопотоків, VoIP та POP3 серверів. Використання програмних та апаратних засобів, агентів управління та інструментів аналізу сприяє розв'язанню завдань моніторингу та управління мережею. Переваги систем моніторингу мережі включають покращену видимість мережі, що дозволяє контролювати всі аспекти мережі, включаючи підключені пристрої та трафік, який проходить через неї. Протоколи моніторингу мережі найкращим чином відслідковують стан мережі та виявляють затримки продуктивності. Дотримання нормативних вимог.

Інструменти моніторингу мережі стають невід'ємною частиною для організацій, які повинні забезпечити відповідність нормативним вимогам, таким як PCI DSS, HIPAA, FISMA, SOX та інші. Ці вимоги передбачають моніторинг мережі як складової внутрішнього контролю, доповнюючи зовнішні заходи безпеки для забезпечення відповідності.

Запобігання простоям є ще однією важливою функцією. Простої можуть великою мірою впливати на продуктивність і призводити до значних фінансових витрат. Виявлення передсмертних ознак збою пристрою чи проблеми мережі є

ключовим аспектом рішень для моніторингу мережі, дозволяючи уникнути несподіваних простоїв.

Швидке виявлення та усунення проблем стає можливим завдяки моніторингу мережі. Виявлення джерела проблеми, чи то коливання трафіку, помилка конфігурації чи інше, стає легше завдяки мережним картам та інструментам автоматизації.

Також програми для моніторингу мережі можуть служити для виявлення загроз безпеки. Вони не лише контролюють продуктивність, але й надійно виявляють незвичайні чи підозрілі дії, допомагаючи виявити потенційні загрози до безпеки системи.

1.2. Важливість та основи моніторингу локальної мережі

Виявлення проблем з продуктивністю на ранніх етапах є ключовим елементом моніторингу мережі. Ефективний попереджувальний моніторинг може запобігти можливим простоям або збоям в роботі мережі. У цьому дослідженні моніторинг мережі відіграє центральну роль, оскільки для оцінки продуктивності локальної мережі важливо мати повну статистику роботи. Аналіз пропускної здатності, затримок та навантаження мережі є необхідним для отримання повної картини ефективності мережі. Збір даних виконується за допомогою протоколів керування мережею.

Технічно моніторинг локальної мережі, це простий процес, що являє собою збір та накопичення даних, за допомогою керуючих протоколів мережі. Отримуються дані про пропускну здатність, швидкодію, затримки та інші параметри, від вузлів системи. Ці дані обробляються і на їх основі формуються звіти, що подаються в будь якій, зручній формі [1].

1.3. Протоколи керування мережею

Протоколи керування мережею представляють собою набір правил і процедур, які регулюють взаємодію пристроїв у комп'ютерній мережі і визначають, як контролювати цю взаємодію. Ці протоколи виконують різні функції, такі як маршрутизація, комутація, адресація, керування багатокористувацьким доступом та інші [3].

Низка основних протоколів керування мережею включає:

– протокол інформації про маршрутизацію (RIP) – протокол маршрутизації для передачі інформації про маршрути в мережі;

– простий протокол керування мережею (SNMP) – використовується для збору інформації про стан пристроїв в мережі, дозволяє адміністраторам моніторити та налаштовувати пристрої;

– протокол динамічної конфігурації хоста (DHCP) – використовується для автоматичного надання мережевих налаштувань пристроям, таких як IP-адреси;

– протокол резервування віртуального маршрутизатора (VRRP) – забезпечує високий рівень доступності за допомогою віртуальних IP-адрес для групи маршрутизаторів;

– вибір найкоротшого шляху (OSPF) – протокол маршрутизації, що визначає оптимальні маршрути внутрішньої мережі;

– протокол керуючих повідомлень Інтернету (ICMP) використовується для надсилання повідомлень про помилки та діагностики мережі, таких як пакети "ping".

Ці протоколи сприяють ефективному та надійному функціонуванню комп'ютерних мереж, дозволяючи пристроям ефективно спілкуватися та обмінюватися інформацією.

1.4. Огляд і порівняння систем моніторингу локальної мережі

Для забезпечення ефективної роботи комп'ютерної мережі необхідно постійно виконувати моніторингу її стану. Використання засобів контролю дозволяє адміністраторам вчасно виявляти та усувати будь-які загрози нормальному функціонуванню [2].

Мережеві аналізатори, також відомі як мережеві монітори, призначені для тестування кабелів різних категорій. Важливо відрізняти мережеві монітори від аналізаторів протоколів. Мережеві монітори фіксують лише статистичні дані про трафік, такі як середня інтенсивність загального трафіку мережі, середня інтенсивність потоку пакетів з певним типом помилок і інше. Мережеві аналізатори - це великогабаритні та вартісні пристрої (зазвичай понад $20000), які призначені для використання в лабораторних умовах спеціалізованим технічним персоналом і дозволяють вимірювати різні електромагнітні характеристики кабелю. Далі буде виконано огляд і порівняння сучасних систем моніторингу.

Рис. 1.1 Network Olympus

Network Olympus (Рис. 1.1) – це інноваційна програма, яка функціонує у форматі служби та володіє зручним веб-інтерфейсом, надаючи користувачам велику гнучкість у роботі. Однією з основних переваг є наявність конструктора сценаріїв, що дозволяє вийти за межі простих перевірок і враховувати різноманітні умови роботи пристроїв.

Основна особливість програми полягає в можливості створення складних сценаріїв моніторингу для точного виявлення проблем і автоматизації їх усунення. Ключовим елементом сценарію є сенсор, який дозволяє будувати логічні ланцюжки. Залежно від результатів перевірки, ці ланцюжки можуть ініціювати різні оповіщення та дії, спрямовані на вирішення завдань користувача.

Один із найсильніших аспектів - можливість редагування кожного елементу ланцюжка у будь-який момент, зі змінами, які негайно застосовуються до всіх пристроїв, пов'язаних із сценарієм. Вся активність мережі фіксується в журналі та спеціальних звітах, що дозволяє ефективно відслідковувати та аналізувати події.

Переваги	Недоліки
Групові сенсори	Тільки веб-інтерфейс
Простота налаштування	Установка тільки під Windows
Нескладно освоїти	Немає багатокористувацького доступу
Конструктор сценаріїв моніторингу	

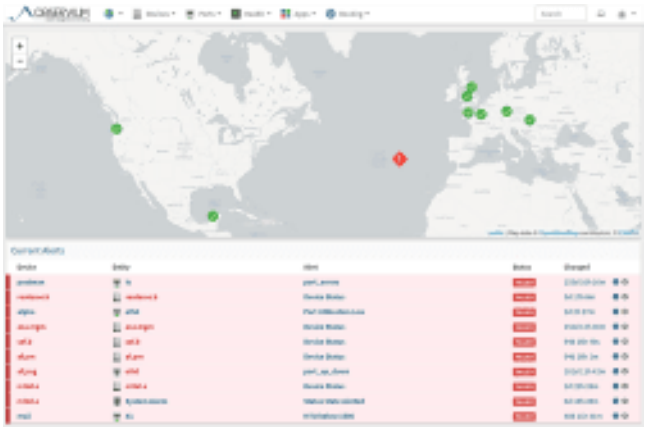


Рис. 1.2 Observium

Додаток Observium (Рис. 1.2), робота якого заснована на використанні протоколу SNMP, дозволяє не тільки дослідити стан мережі будь-якого масштабу в режимі реального часу, а й аналізувати рівень її продуктивності. Це рішення інтегрується з обладнанням від Cisco, Windows, Linux, HP, Juniper, Dell, FreeBSD, Brocade, Netscaler, NetApp і інших вендорів. Завдяки ідеально відпрацьованому

графічному інтерфейсу, ця програма надає системним адміністраторам масу варіантів для налаштувань - починаючи від діапазонів для автовизначення і закінчуючи даними протоколу SNMP, необхідними для збору інформації про мережу.

Також вони отримують доступ до даних про технічні характеристики всього обладнання, яке зараз підключено до мережі. Всі звіти, які формуються за допомогою аналізу журналу подій, Observium може представляти у вигляді діаграм і графіків, наочно демонструючи "слабкі" сторони мережі. Ви можете використовувати як демо-версію (яка, виходячи з нашого досвіду, володіє недостатнім набором можливостей), так і платну ліцензію, річна вартість використання якої становить 200 фунтів стерлінгів.

Переваги	Недоліки
Доступна безкоштовна версія	Немає підтримки мобільних пристроїв
"Граничні" сигнали	Не проста в установці
Функції автоматичного виявлення	Не для невеликих мереж
Доступна для багатьох систем	Недоліки безкоштовної версії

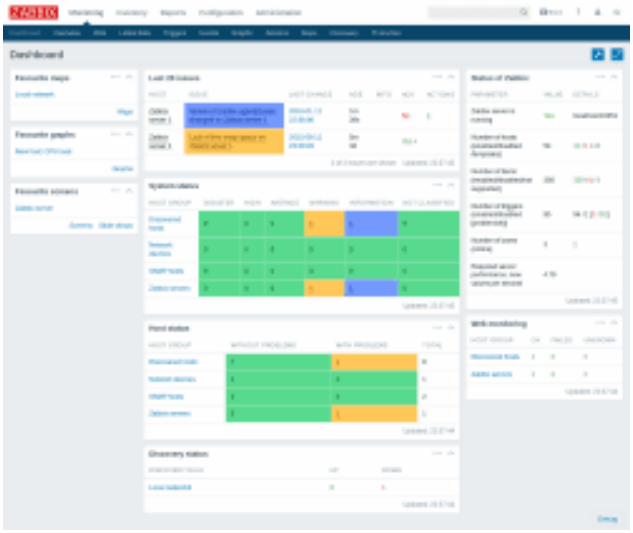


Рис. 1.3 Zabbix

Система моніторингу Zabbix (Рис. 1.3) представляє собою універсальне рішення для відкритого мережевого моніторингу, здатне адаптуватися під різні

мережеві моделі. Основною метою є надання підтримки систем з багатосерверною архітектурою, інтегруючись з серверами Linux, FreeBSD та Windows [6].

Цей додаток відмінно справляється з управлінням сотнями мережевих вузлів, роблячи його важливим інструментом для системних адміністраторів, що працюють на великих підприємствах. Розгортання Zabbix у вашій локальній мережі передбачає запуск програмних агентів або використання SNMP-протоколу (чи іншого захищеного віддаленого доступу). Управління здійснюється через веб-інтерфейс на PHP.

Це програмне забезпечення також надає повноцінний набір інструментів для відстеження стану апаратної частини мережі. Звертає на себе увагу, що для повного використання всіх переваг цього рішення системному адміністратору слід мати базові знання мов Perl або Python (або інших мов, які можна використовувати з Zabbix).

Переваги	Недоліки
Безкоштовна	Нема версії для Windows
Проста інсталяція	Складний громіздкий інтерфейс
Безліч плагінів	Високе навантаження на комп'ютер
Потужні налаштування сповіщень	Немає дашбордів

Найбільш оптимальною, гнучкою у використанні та продуктивною буде система моніторингу Zabbix. Основними перевагами, які є актуальними для роботи з локальними мережами невеликих підприємств, є те що вона безкоштовна та має можливості з підключення плагінів. Потужні налаштування сповіщень, дають можливість, автоматизувати виявлення помилок і пришвидшити їх виправлення, через надсилання сповіщень про помилки до месенджера в чат чи через чат-бот.

1.5. Огляд інструменту Zabbix

1.5.1. Функції, архітектура та переваги Zabbix. Zabbix надає розширений функціонал для моніторингу мережевих пристроїв, таких як маршрутизатори, комутатори та сервери, і підтримує як агентський підхід, так і підхід без агента. Для моніторингу використовується протокол SNMP. Здатний контролювати доступність та ефективність пристроїв, а також підтримує моніторинг віртуальних машин за допомогою VMware.

Zabbix володіє можливістю моніторингу баз даних та веб-сервісів, а також спроможність виявлення та групування мережевих пристроїв. У випадку неполадок або відмови мережі, системний адміністратор отримує попередження [6].

Архітектура Zabbix включає компоненти (Рис. 1.4), такі як Zabbix Server, Zabbix Proxy, Zabbix Agent і веб-інтерфейс. Кожен з них відіграє визначену роль у системі моніторингу. Zabbix Server виконує функції віддаленого моніторингу мережі, зберігає конфігурації та дані. Zabbix Proxy збирає дані продуктивності від імені сервера і переадресовує їх. Проксі розподіляє робоче навантаження, зменшуючи обчислювальні можливості сервера введення-виведення.

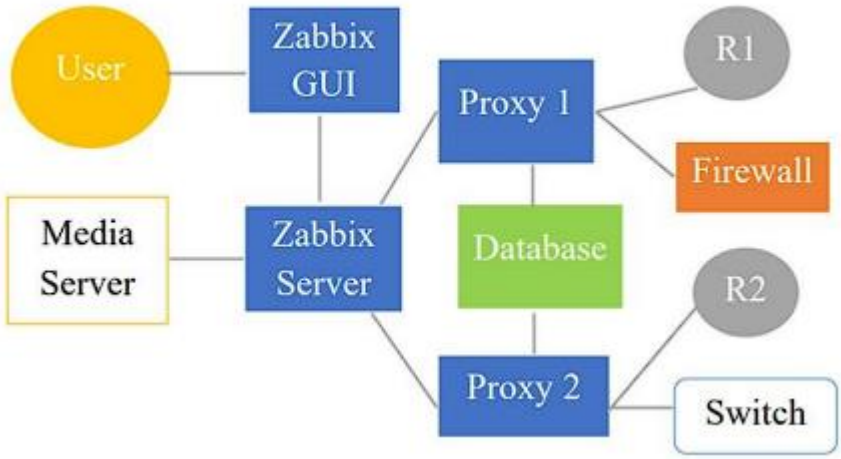


Рис. 1.4 Компоненти Zabbix

Хоча Zabbix володіє великим спектром функцій, відмічено, що він не має можливості прогнозування тенденцій, тобто попереднього повідомлення про можливі помилки.

Агент Zabbix відповідає за моніторинг ресурсів мережевих пристроїв, таких як жорсткий диск, пам'ять та статистика процесора. Його присутність на кожному пристрої є обов'язковою умовою для забезпечення ефективного моніторингу ресурсів, завдяки власним системним дзвінкам, які забезпечують збір статистичних даних.

Веб-інтерфейс, який входить до складу Zabbix Server, зазвичай розміщується на тому ж сервері, що й сам сервер Zabbix. Цей інтерфейс оперує напряму з базою даних, поминаючи Zabbix Server, що призводить до підвищення продуктивності. Важливо відзначити, що відсутність веб-інтерфейсу у системі Zabbix Server неможлива.

До складу системи Zabbix входять також два ключові компоненти – медіа-сервер і база даних. Медіа-сервер відповідає за відсилання сповіщень через електронну пошту і SMS, в той час як в базі даних зберігаються конфігураційні та історичні дані.

Ця комбінація компонентів дозволяє Zabbix забезпечувати три основні типи моніторингу: проста перевірка, агент Zabbix та зовнішня перевірка. Проста перевірка дозволяє перевіряти доступність різних служб без додаткових налаштувань на хості. Агент Zabbix відповідає за локальний контроль робочого навантаження обладнання. За допомогою зовнішньої перевірки, виконується моніторинг віддалено, за допомогою SNMP, SSH, TCP, ICMP, IPMI.

Важливо відзначити, що моніторинг хосту може відбуватися і без проксі, але у такому випадку абсолютно всі дані моніторингу збираються ьа накопичуються безпосередньо сервером Zabbix. Крім того, що графічний інтерфейс системи моніторингу Zabbix, база даних ,сервер та медіа-сервер можуть виявитись об'єднані на одній машині, що робить цей метод особливо важливим для малих та середніх мереж.

1.5.2. Веб-інтерфейс та прикладний програмний інтерфейс Zabbix.

Навігація в інтерфейсі Zabbix дуже складна для новачків, і це може призвести до труднощів для користувачів, які тільки вперше зустрілися з цією системою моніторингу. Навіть досвідчені користувачі можуть витрачати занадто багато часу на виконання основних операцій через велику кількість кліків.

Наприклад, якщо адміністратор мережі хоче створити елемент та пов'язаний з ним тригер, цей процес вимагає кількох кроків, і в разі втрати зв'язку це може призвести до додаткових ускладнень. Відсутність зручного способу збереження ключа елемента може ускладнити подальшу роботу.

Крім того, інформація в інтерфейсі знаходиться в різних місцях, що ускладнює процес відстеження та аналізу даних [6]. Наприклад, конфігурація елемента та дані моніторингу розташовані в різних розділах, що може вимагати переходу між різними частинами системи для отримання повної інформації.

У результаті цей простий процес може перетворитися на справжній кошмар для системного адміністратора, і вирішення цих проблем може значно полегшити використання Zabbix для користувачів будь-якого рівня досвіду.

Прикладний програмний інтерфейс (API) може демонструвати низьку ефективність, особливо при операціях, пов'язаних із зв'язуванням шаблонів. Наприклад, якщо потрібно пов'язати 10 000 хостів із простим шаблоном, це може зайняти від 10 до 20 хвилин, залежно від обладнання, і призвести до мільйонів SQL-запитів. Проблема також полягає в відсутності належної перевірки та звітування про помилки, що може призводити до загальних помилкових повідомлень, скриваючи конкретні проблеми API.

Планується перенесення API з інтерфейсної частини на бік сервера Zabbix для поліпшення продуктивності. Це включатиме функції захисту з використанням відкритих ключів шифрування, таких як SSL або TLS для агентів, проте це може потребувати уваги до негативного впливу на швидкість та роботу сервера Zabbix [8].

У сфері безпеки Zabbix використовує шифрування, але відсутність вбудованої підтримки може створювати складнощі для користувачів. Використання сторонніх інструментів, таких як Stunnel та Open VPN, вирішує цю проблему, але не інтегрується належним чином, особливо в великих середовищах.

Щодо мов програмування та архітектури, вибір C для критичних частин, таких як сервер, агент і проксі, дозволяє створювати ефективний код. З іншого боку, використання PHP для веб-інтерфейсу має свої переваги та недоліки, а SQL обрано як механізм зберігання транзакцій для забезпечення узгодженості обмежень на рівні бази даних.

Зауважимо, що масштабування традиційних баз даних SQL може бути складною задачею, особливо для великих операцій зчитування.

1.6. Висновки до розділу 1

В першому розділі, було розглянуто актуальні системи та методи моніторингу локальної мережі. Результатом став вибір системи моніторингу локальної мережі Zabbix, як найбільш продуктивної, доступної та зручної. Було проведено огляд її структури, архітектури, особливостей прикладного та веб-інтерфейсів. Також були поставлені завдання, кваліфікаційної роботи та була сформована методологія дослідження, в якій було обрано методи теоретичних досліджень, це полегшить дослідження.

Загалом, в першому розділі були виконані такі завдання:

- досліджено методи моніторингу локальної мережі;
- досліджено системи моніторингу та обрано найбільш актуальну і продуктивну з них.

Виходячи з результатів порівняння систем моніторингу мережі, можна дійти висновку що найбільш оптимальним, гнучким у використанні та продуктивним буде система моніторингу Zabbix. Основними перевагами які є актуальними для роботи з локальними мережами невеликих підприємств, є те що вона безкоштовна та має можливості з підключення плагінів. Потужні налаштування сповіщень, дають можливість, автоматизувати виявлення помилок і пришвидшити їх виправлення, через надсилання сповіщень про помилки до месенджера в чат чи через чат-бот.

РОЗДІЛ 2
ФОРМУВАННЯ КРИТЕРІЇВ ЕФЕКТИВНОСТІ МОНІТОРИНГУ ТА ВИБІР МЕТОДІВ МОНІТОРИНГУ ЛОКАЛЬНОЇ КОМП'ЮТЕРНОЇ МЕРЕЖІ ЗГІДНО НИХ

2.1. Формування критеріїв ефективності для завдання моніторингу мережі

Першим кроком, при формуванні списку методів та інструментів для виконання моніторингу локальної мережі, є формування критеріїв ефективності та параметрів роботи системи моніторингу.

Визначення критеріїв ефективності для моніторингу мережі є важливим завданням для забезпечення стабільності та продуктивності мережевого середовища. Далі наведено основні критерії ефективності для завдання моніторингу мережі.

Охоплення, важливий параметр що поєднує в собі широку функціональність (Забезпечення моніторингу різноманітних параметрів, таких як пропускна здатність, використання ресурсів, виявлення помилок та безпека) та відстеження всіх пристроїв (можливість моніторингу всіх пристроїв у мережі, включаючи сервери, комутатори, маршрутизатори та інші мережеві пристрої).

Швидкодія. суть полягає в миттєвому виявленні проблем (має здатність виявляти аномалії та проблеми в реальному часі для оперативної реакції на них) та в мінімальному часі відгуку (забезпечує швидкий відгук на запитання та запити моніторингу).

Безпека. Захист від несанкціонованого доступу: Забезпечення безпеки зібраних даних та системи моніторингу в цілому. Виявлення загроз безпеки: Здатність виявляти потенційні загрози та атаки в мережі.

Точність та надійність, тобто забезпечує точні вимірювання різних параметрів мережі для надійної аналітики та може працювати стабільно і ефективно без системних відмов та збоїв.

Складність та простота використання. Немало важливо щоб система мала легкий у використанні інтерфейс для швидкого доступу до необхідних функцій та даних. Також система моніторингу повинна мати просту конфігурацію, щоб можна

було легко налаштувати систему моніторингу відповідно до конкретних потреб мережі.

Масштабованість. Здатність масштабування: Можливість розширення моніторингу при збільшенні розміру мережі. Підтримка великих обсягів даних: Забезпечення ефективності при обробці великих обсягів мережевих даних.

Згідно з наведеними критеріями ефективності можна підібрати необхідні методи та інструменти для моніторингу локальної мережі.

2.2. Ключові параметри, моніторинг яких необхідно виконувати

Моніторинг локальної мережі є важливою частиною управління і підтримки мережевої інфраструктури. В таблиці 2.1 наведено параметри які необхідно моніторити [10].

Таблиця 2.1

Параметри, моніторинг яких необхідно виконувати

Стан з'єднань	Перевірка доступності обладнання та пристроїв у мережі. Моніторинг пакетних втрат.
Пропускна здатність	Вимірювання швидкості передачі даних в мережі. Виявлення потенційних ускладнень у пропускній здатності.
Використання ресурсів	Моніторинг використання пропускної здатності, CPU і пам'яті на обладнанні.
Пакетний аналіз	Аналіз типів та обсягів трафіку для виявлення аномалій. Виявлення незвичайних або потенційно небезпечних пакетів.

Продовження таблиці 2.1

Споживання ресурсів мережі	Моніторинг використання ресурсів мережі для кожного пристрою. Виявлення надмірного використання або низької активності.
Безпека	Виявлення спроб несанкціонованого доступу чи атак. Моніторинг виявлення інтегрованих систем безпеки.
Доступність служб та додатків	Моніторинг доступності ключових служб та додатків.

Тепер на основі параметрів моніторингу та критеріїв ефективності, можна обрати методи та інструменти моніторингу мережі.

2.3. Вибір методів моніторингу стану мережі

Метод управління мережею представляє собою комплекс впливів на керований об'єкт, обраний з численних можливих варіантів, що враховують програму управління та інформацію про поведінку об'єкта та стан навколишнього середовища. Мета полягає в досягненні конкретного результату.

У процесі прогнозування використовуються різні загальнонаукові підходи, включаючи системний, системно-структурний, історичний, структурний та комплексний. Кожен з них дозволяє розглядати явище з різних точок зору, сприяючи глибшому розумінню та аналізу.

Сучасні методи прогнозування, розвиваючись відповідно до вимог проектів, вимагають адаптації до конкретних завдань. Це включає адаптацію методів до конкретних вимог прогнозної та програмної роботи.

В залежності від способу використання експертної інформації розрізняють методи прямих оцінок і методи зворотного зв'язку. Обидва підходи використовують експертні думки, проте різняться у видачі результатів: перший забезпечує безпосередній результат, а другий включає послідовні ітерації з впливом на експертів у процесі обробки попередніх результатів.

З урахуванням постійного росту складності завдань автоматизованих систем управління та зростання вимог до якості обслуговування телекомунікаційних мереж, прогнозування поведінки таких мереж стає ключовою задачею. Навіть найкращі розглянуті методи можуть не повністю задовольнити вимоги щодо прогнозів для всіх необхідних параметрів через різноманітність прогнозів для вимог обслуговування телекомунікаційних мереж.

Таблиця 2.1

Протоколи та інструменти для моніторингу локальної мережі

Протокол моніторингу	Призначення та критерії ефектисвності
ICMP (Internet Control Message Protocol): Використовується для відправки пакетів Echo Request і отримання відповідей Echo Reply (ping). Може бути використаний для визначення доступності та стану мережевих пристроїв	Даний метод ідеально підходить для виконання періодичного опитування про стан та доступність пристроїв у мережі. Також він відповідає критеріям ефективності, вказаним вище, адже забезпечує безпечну та швидку роботу, з різними типами пристроїв та достатньо простий у використанні.
LLDP (Link Layer Discovery Protocol): Дозволяє мережевим пристроям взаємодіяти та обмінювати інформацією про свою конфігурацію та підключення.	Надає можливість отримання інформації про фізичну топологію мережі та деталі щодо зв'язків між підключеними пристроями. Протокол достатньо універсальний та не створює зайвого навантаження на системи, тому відповідає критеріям.

Продовження таблиці 2.2

NetFlow: Протокол, який використовується для моніторингу трафіку в мережі.	Дозволяє збирати статистику про комунікацію між пристроями. Протокол створений спеціально для аналізу трафіку, що проходить через пристрій, де він розгорнутий.
SNMP (Simple Network Management Protocol): Дозволяє моніторити та управляти мережевими пристроями, такими як роутери, комутатори, сервери, за допомогою стандартних запитів та відповідей.	З допомогою протоколу можна збирати дані з усіх пристроїв у мережі та дозволяє виконувати керування пристроями, що відкриває можливості автоматичного реагування на проблеми з мережею. Забезпечує безпеку системи, працює точно за рахунок отримання даних напряму від мережевих пристроїв, простий у використанні і необмежений в розширенні кількості підключених пристроїв.

Ці протоколи та інструменти можуть використовуватися для відстеження та аналізу аспектів локальної мережі вказаних у пункті 2.2, забезпечуючи адміністраторам інформацію про доступність, продуктивність та безпеку мережевих ресурсів. Далі буде розглянуто ці протоколи та їх будову більш докладно.

2.4. Метод моніторингу на базі ICMP протоколу

Моніторинг, ґрунтуючись на протоколі ICMP (Internet Control Message Protocol), визначається як один із наибільш поширених методів визначення доступності та слідкування за станом мережевих пристроїв. ICMP використовується для висилання спеціальних пакетів (зазвичай Echo Request або "ping" пакетів) та отримання відповідей від інших пристроїв у мережі.

ICMP (Рис. 2.1) – повідомлення розділене на дві широкі категорії: звіт про помилку та запит.

Рис. 2.1 Структура ICMP повідомлення

Основні аспекти моніторингу на основі ICMP включають:

– Ping (Echo Request/Echo Reply): Пристрій надсилає Echo Request пакет іншому пристрою, і після отримання його, пристрій відправляє Echo Reply. Цей процес використовується для визначення часу відправлення та отримання пакетів, а також для визначення доступності пристрою в мережі.

– Traceroute: Traceroute використовує ICMP-пакети для визначення шляху, яким йде сигнал від одного пристрою до іншого. Це дозволяє адміністраторам відстежувати маршрут і виявляти проблеми на шляху до певного пристрою.

– ICMP Redirect: Повідомлення ICMP Redirect використовується для сповіщення пристроїв про зміну маршруту до певного призначення. Це може бути корисним для оптимізації маршрутів в мережі.

– ICMP Error Messages: ICMP також використовується для передачі повідомлень про помилки, таких як Destination Unreachable або Time Exceeded. Це може бути корисним для виявлення проблем в мережі.

– ICMP Flood атаки: У випадках атак типу ICMP Flood атакувач надсилає велику кількість ICMP-пакетів до цільового пристрою, перевантажуючи його ресурси, і може спричинити відмову в обслуговуванні (DoS).

Моніторинг на базі ICMP є ефективним інструментом для базового визначення доступності пристроїв в мережі та виявлення проблем на рівні маршрутизації та

затримок у передачі даних. Однак важливо також враховувати інші методи моніторингу, оскільки ICMP не завжди надає повний обзор стану мережі.

Даний метод ідеально підходить для виконання другого етапу роботи системи моніторингу, що вказаний в першому пункті «Моніторинг стану пристроїв», оскільки з допомогою цього протоколу можна виконувати автоматизоване періодичне опитування стану всіх пристроїв у мережі. Також він відповідає критеріям ефективності, вказаним вище, адже забезпечує безпечну та швидку роботу, з різними типами пристроїв та достатньо простий у використанні.

2.5. Метод моніторингу на базі LLDP (Link Layer Discovery Protocol) протоколу

Моніторинг локальної мережі, опираючись на протокол LLDP (Link Layer Discovery Protocol), відкриває перед адміністраторами безпрецедентні можливості отримання інформації про фізичну топологію мережі та деталі щодо зв'язків між підключеними пристроями. Перевагою використання LLDP є автоматичне визначення та обмін інформацією про пристрої у мережі, що надає детальний огляд її структури.

Основні аспекти моніторингу, які базуються на протоколі LLDP (Рис. 2.2), включають:

– Деталізація Топології Мережі: LLDP виходить за межі простого визначення зв’язків між пристроями, дозволяючи адміністраторам отримати повноцінну картину топології, включаючи інформацію про порти, комутації та можливості мережевих вузлів.

– Широкий Спектр Інформації про Пристрої: LLDP передає різноманітні дані про підключені пристрої, такі як ім'я, тип, модель, серійний номер, а також технічні характеристики. Це дозволяє не лише ідентифікувати пристрої, але і зрозуміти їх можливості та характеристики.

– Динамічний Моніторинг Змін в Топології: Завдяки LLDP, адміністратори можуть динамічно відстежувати зміни у фізичних підключеннях, виявляти нові пристрої або реагувати на відключення існуючих, що важливо для оперативного управління та попередження можливих проблем.

– Виявлення та Аналіз Потенційних Проблем: Моніторинг на основі LLDP допомагає ідентифікувати проблеми у фізичних підключеннях, такі як відсутність з'єднання чи зміни в топології, що може вплинути на продуктивність і безпеку мережі.

– Слідкування за Шляхами Даних: За допомогою LLDP можна моніторити шляхи переміщення даних в мережі, що важливо для виявлення потенційних проблем в трафіку та оптимізації шляхів.

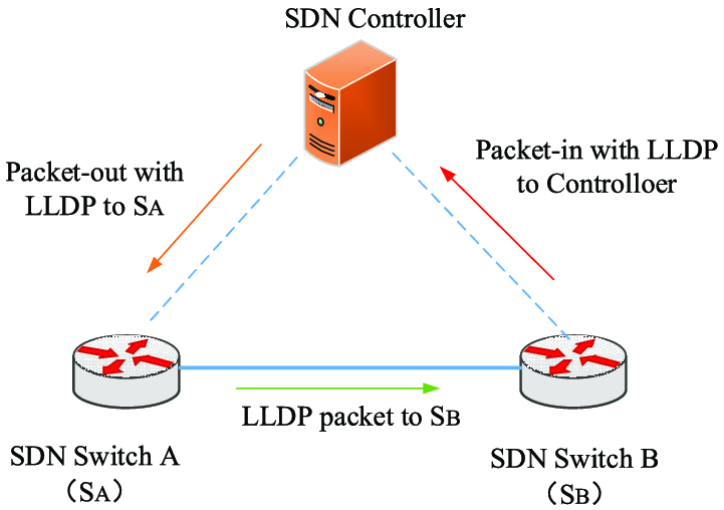


Рис. 2.2 Схема роботи протоколу LLDP;

Використання спеціалізованих інструментів та програмного забезпечення для аналізу і відображення інформації, яку надають пристрої за допомогою протоколу LLDP, дозволяє адміністраторам отримати повний інсайт у структуру та стан мережі. Тобто цей метод відмінно підходить для збору інформації про мережу, її структуру та апаратну складову, тому цей метод буде використано для для першого етапу роботи системи моніторингу мережі. Це простий але продуктивний інструмент, який може працювати в мережах будь якого типу, тому відповідає критеріям ефективності.

2.6. Метод моніторингу на базі NetFlow протоколу

Моніторинг локальної мережі на основі протоколу NetFlow є потужним інструментом для отримання детальної інформації про трафік та використання ресурсів. NetFlow дозволяє збирати дані на рівні мережевих пристроїв, таких як маршрутизатори та комутатори, і аналізувати їх для здобуття важливих відомостей щодо ефективності мережі.

Коли пакети проходять через мережеві пристрої, NetFlow збирає інформацію про кожен пакет, включаючи інформацію про джерело, призначення, протокол, об'єм передачі даних та інші атрибути (Рис. 2.3). Ці дані агрегуються в потоки, які надають зручну форму для подальшого аналізу.

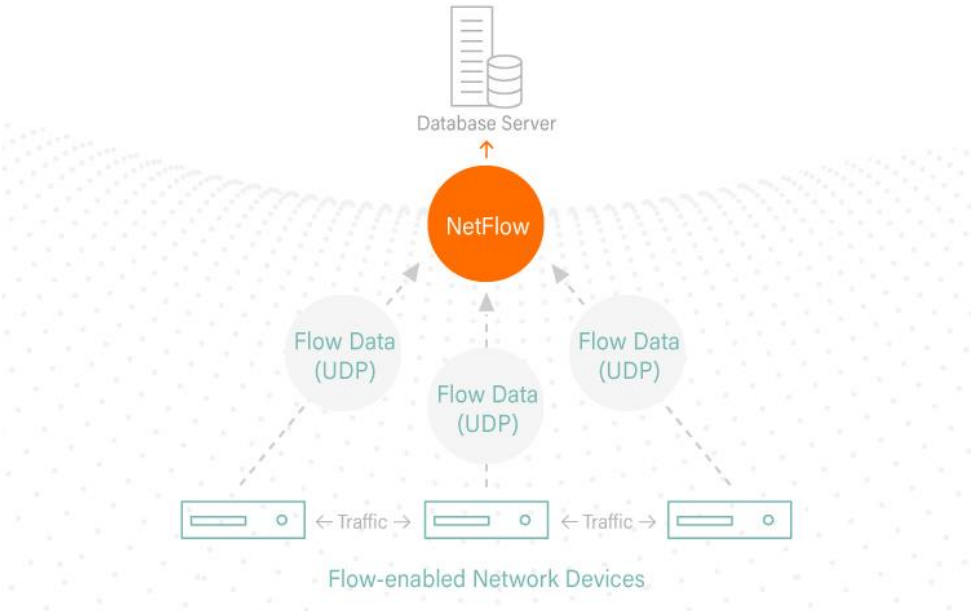


Рис. 2.3 Схема роботи протоколу NetFlow;

Один із ключових аспектів моніторингу NetFlow - це аналіз трафіку. Адміністратори можуть переглядати статистику про те, яким чином використовуються мережеві ресурси, які протоколи є найбільш активними, та виявляти ефективність передачі даних.

Крім того, NetFlow допомагає виявляти точки затору в мережі. Аналізуючи дані, адміністратори можуть ідентифікувати сегменти мережі, де трафік інтенсивний, і вживати заходів для оптимізації пропускної спроможності.

Особливо важливим є виявлення аномального трафіку. NetFlow може автоматично виявляти аномалії в патернах трафіку, що може свідчити про можливі атаки або інші проблеми в мережі.

Основна перевага моніторингу на основі NetFlow полягає в тому, що він дозволяє адміністраторам отримувати не лише загальний огляд трафіку, але і докладні інсайди, які полегшують виявлення проблем, оптимізацію мережі та планування ресурсів.

На третьому етапі роботи системи моніторингу, необхідний потужний інструмент для аналізу мережевого трафіку, яким NetFlow і є. За допомогою цього інструменту можна проаналізувати трафік в мережі, не впливаючи на її продуктивність, та виявити аномальний трафік або несанкціонований вхід. Цим методом можна виявити інциденти безпеки, реагуванням на які займеться протокол SNMP та алгоритм дій вказаний користувачем.

2.7. Метод моніторингу на базі SNMP протоколу

Основним методом моніторингу та керування мережею в системі моніторингу Zabbix, є протокол SNMP, який активно працює на всіх етапах роботи системи моніторингу і за рахунок цього моментально реагує на інциденти безпеки [7].

Моніторингова система, побудована на основі SNMP протоколу, функціонує за принципами взаємодії між менеджером та агентами (Рис. 2.4), утворюючи основний механізм, який забезпечує обмін інформацією про стан та параметри системи.

Рис. 2.4 Кроки моніторингу SNMP;

Ключові етапи роботи моніторингової системи, заснованої на SNMP (Рис. 2.5), можна розглядати наступним чином:

1. Налаштування:

– Адміністратор проводить конфігурацію моніторингової системи, визначаючи агентів та параметри, які вони мають моніторити.

– Встановлюються спільноти доступу для обміну інформацією між агентами та менеджерами.

2. Взаємодія Менеджера та Агента:

– Менеджер використовує SNMP-запити (GET, GETNEXT, SET) для отримання даних від агентів.

– Агенти відповідають на ці запити, передаючи значення відповідних об'єктів інформаційної бази управління (MIB).

3. SNMP-Трапи (Traps):

– Агенти можуть автоматично надсилати SNMP-трапи, повідомляючи менеджера про виникнення певних подій або зміну стану.

– Це забезпечує реальний час інформування менеджера про важливі події.

4. MIB (Management Information Base):

– MIB визначає структуру, ідентифікацію та типи даних для моніторингу об'єктів на агентах.

– Адміністратор вибирає, які об'єкти MIB слід відстежувати.

5. SNMP-версії:

– Система може користуватися різними версіями SNMP, такими як SNMPv1, SNMPv2c чи SNMPv3, залежно від вимог безпеки та функціональності.

6. Відображення та Аналіз Даних:

– Менеджер обробляє та відображає інформацію для аналізу та виявлення аномалій чи проблем у мережі.

– Графіки, таблиці та алерти використовуються для представлення даних.

7. Керування Пристроями:

– Менеджер може використовувати SNMP SET-запити для відправлення команд агентам для зміни конфігурації чи виконання конкретних дій.

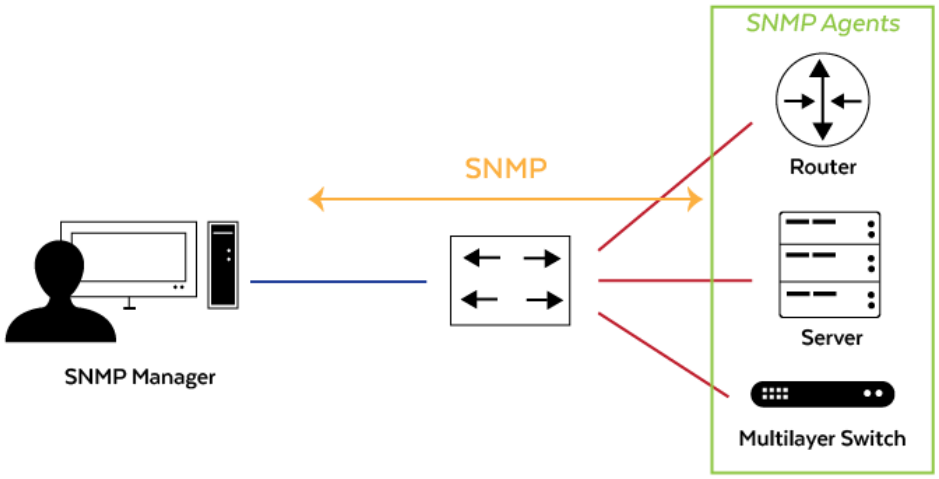


Рис. 2.5 Схема роботи протоколу SNMP;

Моніторингова система, що базується на SNMP протоколі, забезпечує доступ до реальних даних про стан мережі та сприяє вчасному виявленню та вирішенню проблем. Цей метод є ефективним для здійснення моніторингу та управління різними аспектами мережевої інфраструктури. Цей метод моніторингу не тільки збирає дані про мережу але й може виконувати різні дії з системою, щоб запобігти проблемам. Він бере найактивнішу участь на усіх етапах роботи системи, може реагувати на відмови в обслуговуванні, проводити журналювання, автоматичні відновлювальні заходи та на основі його даних включно з даними інших методів, може надавати повні звіти про роботу системи моніторингу [7].

2.8. Основні компоненти SNMP і їх функції

Стандарт SNMP був розроблений з метою вирішення завдань обробки помилок та аналізу продуктивності та надійності в мережевому середовищі.

Обробка помилок:

На першому рівні роботи системи виконується реєстрація повідомлень про помилки, їх фільтрація, маршрутизація та аналіз на основі кореляційної моделі. Мета - виявлення, визначення та усунення наслідків збоїв та відмов у роботі мережі.

Аналіз продуктивності і надійності:

На другому рівні системи оцінюється продуктивність і надійність на основі статистичної інформації про різні параметри, такі як час реакції системи, пропускна спроможність каналів зв'язку, інтенсивність трафіку та інші. Результати аналізу дозволяють контролювати угоду про рівень обслуговування (SLA).

Характеристики SNMP згідно критеріїв ефективності для завдання системи моніторингу локальної мережі:

Управління за допомогою SNMP має бути простим, навіть за ціною втрати потужності, масштабованості і захищеності. При розробці стандартів враховувалися такі умови:

Широке застосування: Системи, що використовують SNMP, можуть бути різноманітними - від принтерів до мейнфреймів.

Простота додавання керуючих функцій: Керована система є простою, функціонально обмеженою, і всі керовані системи контролюються складною керуючою системою, функціональність якої можна розширювати.

Стійкість у критичних ситуаціях: SNMP повинен залишатися стійким при перевантаженні та проблемах в мережі, таких як множинні помилки.

Архітектура розподіленої системи:

Архітектура системи описується через обробні елементи, які об'єднують елементи даних та з'єднувачі. Це визначає розподілену структуру системи, де компоненти взаємодіють між собою для забезпечення функціональності та обробки інформації.

Такий підхід до управління мережею за допомогою SNMP дозволяє ефективно вирішувати завдання моніторингу, аналізу та усунення помилок у роботі мережевих систем.

Архітектура SNMP (Рис. 2.6) визначається архітектурним стилем "клієнт-сервер" з використанням проксі-агентів та менеджерів проміжного рівня для підвищення масштабованості та адміністративної керованості. Розглянемо цю архітектуру з погляду досягнення поставлених перед SNMP цілей за допомогою понять архітектурного стилю мережевого програмного забезпечення [6].

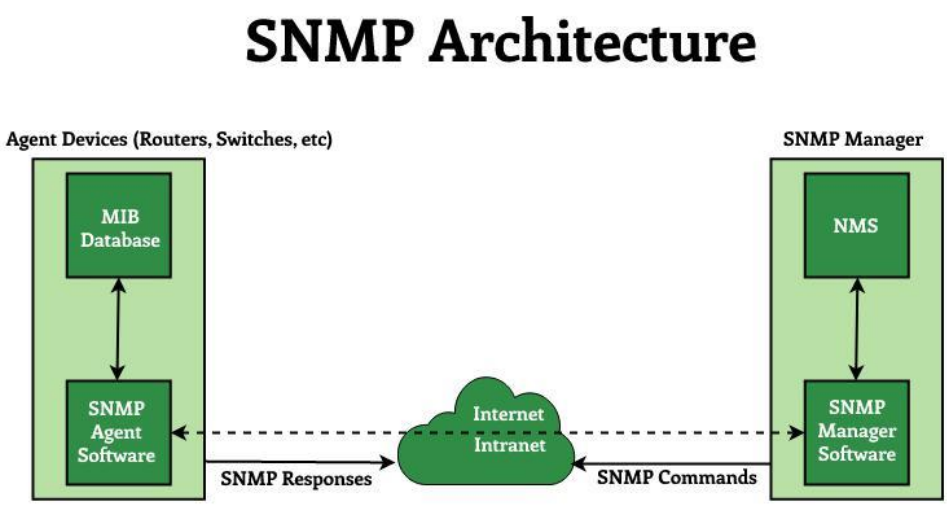


Рис. 2.6 Архітектура SNMP

Компоненти: Архітектура SNMP використовує підхід "менеджер-агент", що відповідає архітектурному стилі "клієнт-сервер". У системі є керовані вузли, кожен з

яких містить агента SNMP, тобто простий сервер. Одночасно, існує вузол, що містить складного клієнта - менеджера SNMP. Взаємодія відбувається за допомогою протоколу SNMP, де менеджер періодично опитує агентів для обміну керуючою інформацією.

Проксі-агент та Менеджер проміжного рівня: Для підвищення масштабованості та адміністративної керованості вводяться проксі-агенти та менеджери проміжного рівня. Проксі-агент може пересилати операції протоколу SNMP, а менеджер проміжного рівня приховує деталі керуючої інформації від систем управління верхнього рівня, інтегруючи одержувані від агентів дані.

Архітектурний стиль "багаторівневий клієнт-сервер": Введення проксі-агентів та менеджерів проміжного рівня дозволяє створювати багаторівневі системи управління, що відповідають архітектурному стилі "багаторівневий клієнт-сервер". Це поліпшує масштабованість та адміністративну ефективність системи [3].

Всі ці елементи архітектури спільно спрямовані на досягнення цілей SNMP, забезпечуючи ефективний обмін інформацією, масштабованість та простоту в реалізації систем управління мережами.

Системи SNMP маніпулюють керуючою інформацією, яка представлена у вигляді змінних на керованих пристроях. Ці змінні можуть включати ім'я системи, час з моменту її перезапуску, записи в таблиці маршрутизації та інші параметри. Загалом, змінні поділяються на скалярні і таблиці.

Структура цієї керуючої інформації описується в Схемі Даних Управління (Structure of Management Information, SMI), яка базується на мові Abstract Syntax Notation One (ASN.1). Кожна змінна має унікальний ідентифікатор об'єкта (Object Identifier, OID), що дозволяє однозначно ідентифікувати кожну змінну.

Місце для ідентифікації змінних надається ієрархічним простором імен OID, який контролюється Internet Assigned Numbers Authority (IANA). У текстовому вигляді імена представлені як десяткові числа, розділені крапками, але для зручності можуть бути також відображені у вигляді текстових рядків. Структура імені схожа на систему доменних імен DNS.

Кожен пристрій містить набір значень змінних, визначених в межах конкретних баз керуючої інформації (Management Information Bases, MIBs).

Наприклад, для пристроїв, що підтримують IP, MIB може описувати таблицю маршрутизації, статистику передачі та прийому пакетів тощо.

Операції, які можна виконувати над цими даними, включають зчитування та запис змінних, а також зчитування наступної змінної в таблиці. Операції в SNMP схожі на віддалене налагодження програми, де стан системи представлений набором змінних, які можна переглядати та змінювати.

2.9. Формування алгоритму роботи системи моніторингу локальної мережі

Будь яка система, в тому числі і система моніторингу локальної мережі, повинна мати чіткий алгоритм роботи, який забезпечить точний збір даних та швидку і чітку реакцію на позаштатні ситуації. Алгоритм роботи системи моніторингу локальної мережі може включати в себе декілька ключових етапів для ефективного виявлення, відстеження та вирішення проблем в мережевому середовищі. Для спрощення формування алгоритму роботи, краще створити структурну схему етапів роботи системи моніторингу (Рис. 2.7). Логічно, що в першу чергу необхідно зібрати всі доступні дані про структуру системи та пристрої в ній. Для точного моніторингу необхідно періодично перевіряти доступність та стан пристроїв. Коли інформація про пристрої наявна та актуальна є сенс аналізувати і перевіряти трафік який йде до них, щоб завчасно виявити інциденти безпеки. При виявленні проблем з безпекою потрібно запустити процес реагування на них та запустити захисні дії. Після цього всі дані про інцидент треба зібрати та повідомити адміністраторів. Тоді коли небезпека минула, необхідно почати відновлювальні заходи, бажано, щоб вони були автоматичні, оскільки не завжди адміністратор зможе зробити це вручну. Фінальним етапом, в якому і полягає вся суть системи моніторингу, буде аналіз накопиченої інформації та формування звітів про роботу системи на протязі якогось періоду часу [9].

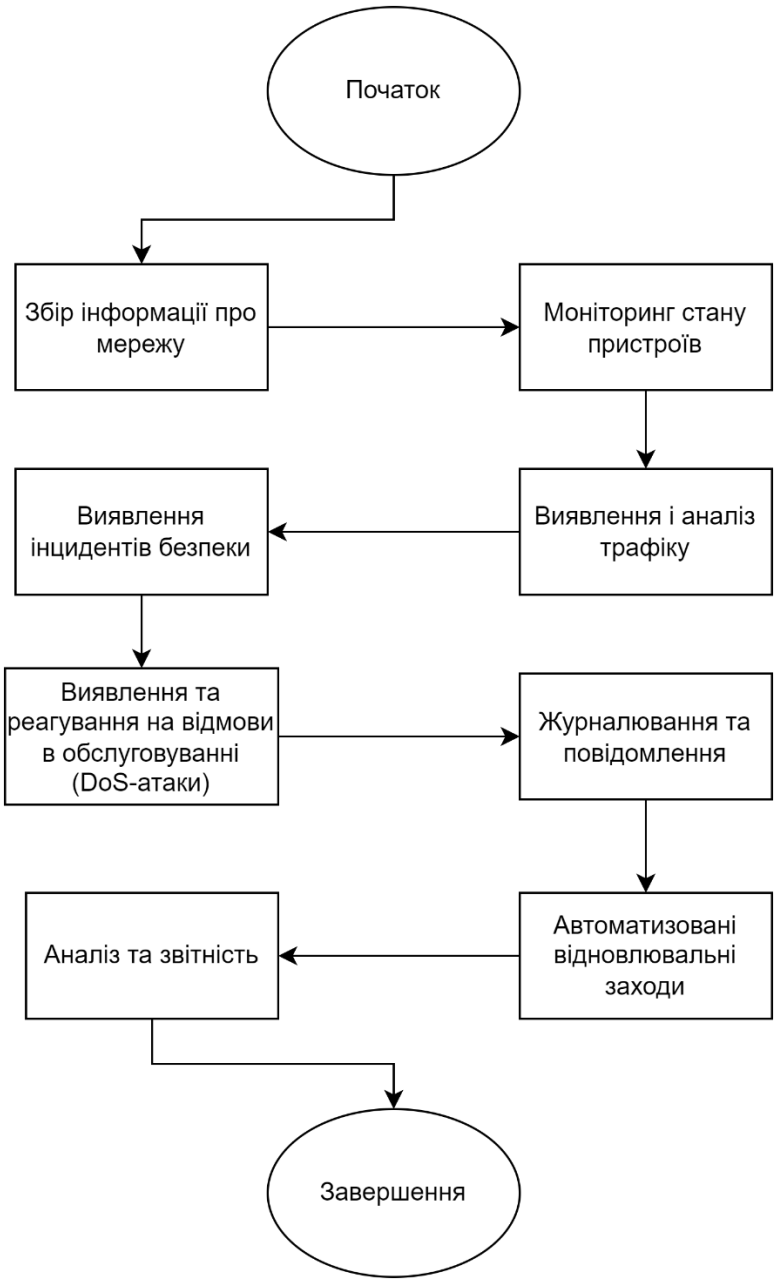


Рис. 2.7 Структурна схема етапів роботи системи моніторингу локальної мережі

Згідно сформованої структурної схеми етапів роботи системи моніторингу, можна описати загальний алгоритм роботи системи (Рис. 2.8):

1) Збір інформації про мережу:

a) Збір базової інформації про всі пристрої в мережі, такі як IP-адреси, MAC-адреси, типи пристроїв і т.д. Це дає можливість отримати інформацію про кількість користувачів у мережі, кількість підмереж та типи підключених пристроїв.

b) Виявлення топології мережі для визначення зв’язків між пристроями. Маючи інформацію про підключені пристрої та методи їх підключення, можна

побудувати віртуальну топологію, що дає можливість розрахувати значення ефективності роботи в ідеальних умовах.

2) Моніторинг стану пристроїв:

a) Система відстежує доступність пристроїв у мережі. Сервер системи моніторингу періодично надсилає запити на пристрої і за наявністю відповіді відмічає, чи пристрій доступний.

b) Періодична перевірка стану пристроїв, визначення їхньої продуктивності та реакції на запити. У відповідях від пристроїв до сервера, наведено дані про роботу пристрою, час витрачений на відповідь та час коли було отримано запит та надіслано відповідь, що дає можливість розрахувати затримку.

3) Виявлення і аналіз трафіку:

a) Аналіз мережевого трафіку для виявлення нештатних ситуацій, атак або аномальної активності. Сервер системи моніторингу перевіряє пакети які проходять в мережі і при виявленні нетипового трафіку, зберігає відомості.

b) Моніторинг широкого спектру протоколів і портів для визначення та класифікації різних видів трафіку.

4) Виявлення інцидентів безпеки:

a) Виявлення підозрілого чи неавторизованого доступу до мережі. При спробах підключення посторонніх осіб або надходженні нетипового трафіку, система позначає це як інцидент безпеки, зберігає відомості про це.

b) Моніторинг подій для реагування на інциденти безпеки та ідентифікації потенційних загроз. Всі дії, виконані на вирішення проблеми також фіксуються системою.

5) Виявлення та реагування на відмови в обслуговуванні (DoS-атаки):

a) Аналіз великої кількості запитів для виявлення можливих атак DoS або DDoS. Трафік при атаках, має особливі характеристики, за якими можливо визначити спробу порушення роботи зловмисниками.

b) Застосування заходів для обмеження чи фільтрації трафіку в разі атак. Правильно налаштована системи моніторингу, може чітко зреагувати на початок атаки та провести запуск заходів протидії, таких як фільтрація трафіку, виявлення аномалій, розгортання CDN, та інших технічних і організаційних заходів.

6) Журналювання та повідомлення:

a) Запис подій та виявлених аномалій в системний журнал.

b) Висилання повідомлень адміністраторам чи відповідальним особам про виявлені проблеми.

7) Автоматизовані відновлювальні заходи:

a) Застосування автоматичних засобів відновлення для усунення проблем і відновлення стабільності мережі.

8) Аналіз та звітність:

a) Проведення аналізу ефективності мережі та виявлення тенденцій у її роботі.

b) Генерація звітів для адміністраторів та відповідальних осіб. Звіти можуть бути подані в будь якій зручній формі.

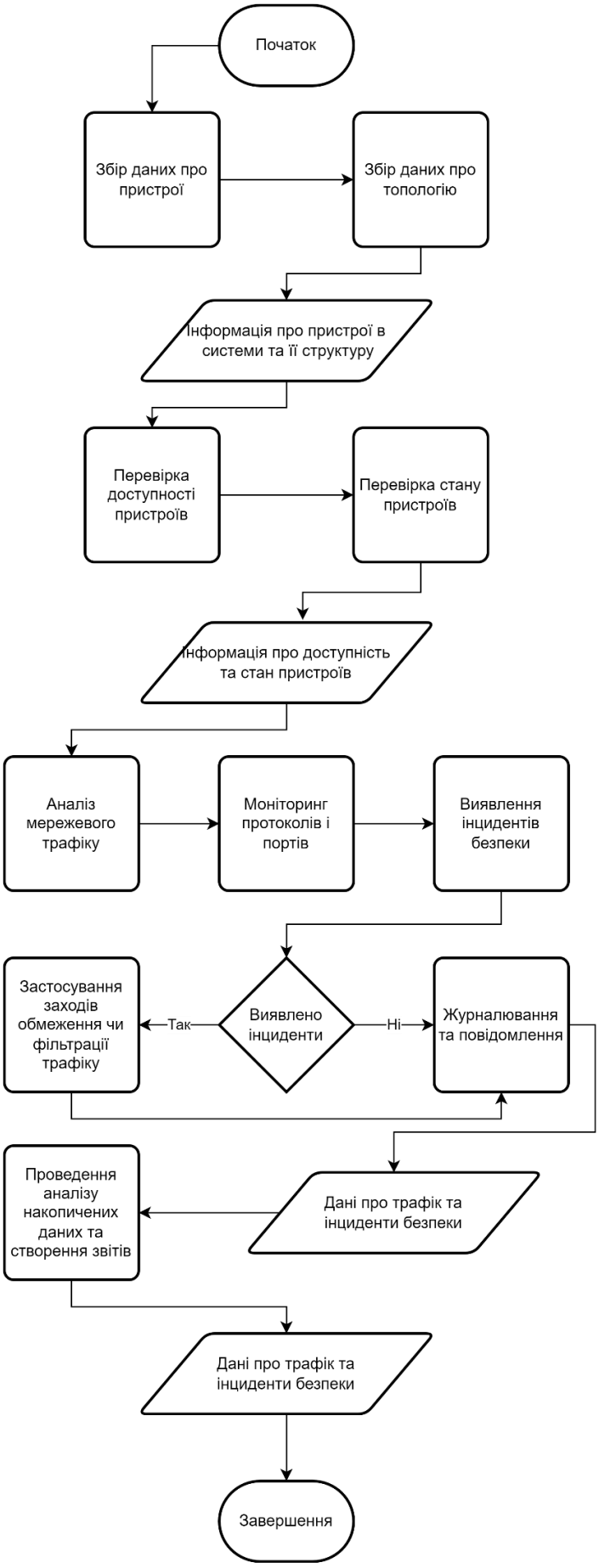


Рис. 2.8 – Блок-схема алгоритму роботи системи моніторингу

Цей алгоритм допомагає забезпечити надійність, безпеку та ефективність локальної мережі шляхом постійного моніторингу та реагування на потенційні проблеми. На кожному кроці роботи системи моніторингу застосовуються різні методи та інструменти моніторингу та керування мережею, обрані в другому пункті.

2.10. Висновки до розділу 2

В розділі було сформовано основні критерії ефективності та параметри для завдання моніторингу локальної мережі. Охоплення, швидкодія, безпека, точність та надійність, складність та простота використання, масштабованість – це параметри, яким повинна відповідати система моніторингу локальної мережі, щоб забезпечити справну, безвідмовну роботу локальної мережі. Також наведено параметри роботи системи моніторингу, які мають бути забезпечені обраними методами моніторингу.

Опираючись на критерії ефективності було підібрано основні методи моніторингу локальної мережі та обрано ті які будуть використані для подальшого моніторингу локальних мережі системою Zabbix, до яких належать: ICMP – один із найбільш поширених методів визначення доступності та слідкування за станом мережевих пристроїв; LLDP що надає безпрецедентні можливості отримання інформації про фізичну топологію мережі та деталі щодо зав'язків між підключеними пристроями; SNMP протокол, що функціонує за принципами взаємодії між менеджером та агентами, утворюючи основний механізм, який забезпечує обмін інформацією про стан та параметри системи; NetFlow – надає детальну інформацію про трафік. Всі ці протоколи можуть використовуватися для моніторингу локальної мережі, основним методом, що покриває найбільшу кількість параметрів роботи мережі, є протокол SNMP. Всі протоколи відповідають критеріям ефективності для завдання моніторингу локальної мережі.

На основі критеріїв ефективності та обраних методів моніторингу було сформовано загальний алгоритм роботи системи моніторингу. По принципу роботи система моніторингу достатньо проста, спочатку збирається докладна інформація про мережу і її розмір, щоб була повна інформація про кількість вузлів у системі. Далі визначається яким чином ці вузли між собою з'єднані, це дає можливість побудувати

віртуальну схему мережі, щоб результати моніторингу були більш достовірні. Тоді виконується періодична перевірка стану пристроїв та аналіз трафіку в мережі, а результати зберігаються. Якщо при перевірці, виявлено підозрілий трафік, або спробу несанкціонованого доступу, виконуються наперед зазначені дії, при цьому ці дії, реакція на них системи та їх результат також записуються. При виявленні відмови в обслуговуванні (DoS-атаки), система може виконати алгоритм налаштований користувачем, таким чином захистивши систему. Дані про всі події чи аномалії зберігаються в журнали, а адміністраторам надсилаються повідомлення про проблему. Наступним кроком виконуються автоматизовані відновлювальні заходи, тобто автоматично виконується алгоритм відновлення працездатності системи без участі адміністратора. В результаті всі дані об’єднуються та генеруються звіти які аналізуються системою. Результати аналізу разом з звітами надаються адміністратору або вповноваженим особам.

Загалом в 2 розділі було обрано методи моніторингу локальної мережі які відповідають критеріям ефективності та забезпечують моніторинг ключових параметрів роботи мережі. На основі цих методів було побудовано алгоритм роботи системи моніторингу.

РОЗДІЛ 3
ВПРОВАДЖЕННЯ МЕТОДІВ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ТА МОНІТОРИНГУ РОБОТИ ЛОКАЛЬНОЇ КОМП'ЮТЕРНОЇ МЕРЕЖІ

3.1. Планування конфігурації потужності та пам'яті

Перш ніж розпочати установку Zabbix Server та Ubuntu Server, важливо ретельно оцінити потреби системи, враховуючи розмір вашої мережі та кількість пристроїв, які плануєте контролювати. З часом обсяг збережених даних буде зростати, тому важливо правильно розрахувати обчислювальні ресурси та обсяг пам'яті заздалегідь.

Хоча, згідно з документацією Zabbix, мінімальні вимоги складають лише 128 МБ оперативної пам'яті та 256 МБ вільного місця на жорсткому диску для Zabbix Server, варто мати на увазі, що ці значення є лише орієнтовними. Фактичні вимоги можуть змінюватися в залежності від численних факторів.

Під час планування ресурсів враховуйте такі параметри, як розмір мережі, інтенсивність використання системи, тип і кількість моніторингових об'єктів. Це дозволить вам забезпечити ефективну та стабільну роботу Zabbix Server в реальних умовах експлуатації. На рисунку 3.1 наведено рекомендовані вимоги до мереж різного розміру.

Network Size	Platform	CPU/Memory	Database	Monitored Hosts
Small	Ubuntu Linux	Virtual Appliance	SQLite	100
Medium	Ubuntu Linux 64	2 CPU cores/2GB	MySQL InnoDB	500
Large	Ubuntu Linux 64	4 CPU cores/8GB	RAID10 MySQL InnoDB or PostgreSQL	>1000
Very Lange	RedHat Enterprise	8 CPU cores/16GB	Fast RAID10 MySQL InnoDB or PostgreSQL	>10000

Рис. 3.1 Оптимальні системні вимоги Zabbix server

Обсяг пам'яті необхідно визначити заздалегідь. У таблиці 3.1 вказані формули розрахунку необхідного дискового простору для історії і подій, з урахуванням майбутнього розширення.

Таблиця 3.1

Планування необхідної пам’яті

Параметри	Рекомендоване вільне місце на жорсткому диску
Конфігурація Zabbix	10Мб
Історія	Дні *(елемент/частота оновлення) *24*3600 байт
Тенденції	дні *(елемент/3600)*24*3600* байт
Події	дні *події*24*3600* байт

Історія в контексті моніторингу представляє собою фіксацію даних протягом визначеного періоду, такого як тижні чи навіть місяці. Наприклад, якщо є необхідність зберігати дані протягом 10 днів, при частоті отримання 30 нових значень розміром у 100 байт кожне, отримуємо:

10×30×24×3600×100=2592000000 байт (≈2.472 ГБ)10×30×24×3600×100=2592000000байт(≈2.472ГБ)

Тенденції відображають статистику зміни даних для кожного елемента, зберігаючи максимальні, мінімальні та середні дані щогодини. Для обчислення обсягу пам'яті, необхідного для тенденцій при параметрах 100 байт на елемент, 1800 елементів і 10 днів, використовуючи формулу, отримуємо:

10×(18003600)×24×3600×100=4320000 байт (≈4.119 МБ)10×(36001800)×24×3600×100=4320000байт(≈4.119МБ)

Кожна подія потребує близько 130 байт. Наприклад, Zabbix генерує подію щосекунди. За допомогою розрахунків, можна оцінити об'єм дискового простору, який буде відведено під події:

130 байт×365×24×3600=4 ГБ130байт×365×24×3600=4ГБ

Сумуючи обсяги пам'яті для всіх чотирьох параметрів, ми отримуємо орієнтоване значення, яке дозволяє вибрати потрібний накопичувач.

Враховуючи проведені розрахунки, обрано 20 ГБ дискового простору для Zabbix Server. Цей обсяг має бути достатнім для зберігання конфігураційних, історичних, тенденційних та подійних даних протягом декількох років активного моніторингу.

3.2. Порядок встановлення Zabbix Server

Для початку роботи з системою моніторингу Zabbix server, необхідно для початку встановити Ubuntu server. Після установки та налаштування сервера та всіх необхідних компонентів, можна почати установку Zabbix server. Завершальним етапом стане вхід в графічний інтерфейс Zabbix. На рисунку 3.2 вказано етапи установки системи моніторингу Zabbix.

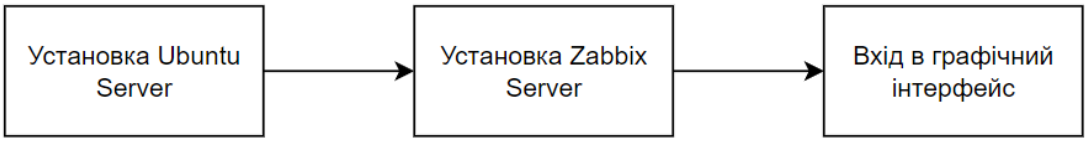


Рис. 3.2 Етапи установки

3.3. Встановлення Ubuntu server

Для роботи, мною було обрано Ubuntu Server 22.04 LTC (Рис. 3.3), який буде встановлено як віртуальну машину в Oracle.

Під час процесу встановлення Ubuntu Server, необхідно виконати кілька кроків, які сприятимуть подальшій установці Zabbix Server:

Встановлення Open SSH Server, що дозволить здійснювати з'єднання з Ubuntu Server через програму Putty. Це полегшить адміністрування сервера за допомогою віддаленого доступу.

Призначення IP-адреси Ubuntu Server на інтерфейсі eth1. Обрано адресу 192.168.1.10, яка також буде IP-адресою Zabbix Server.

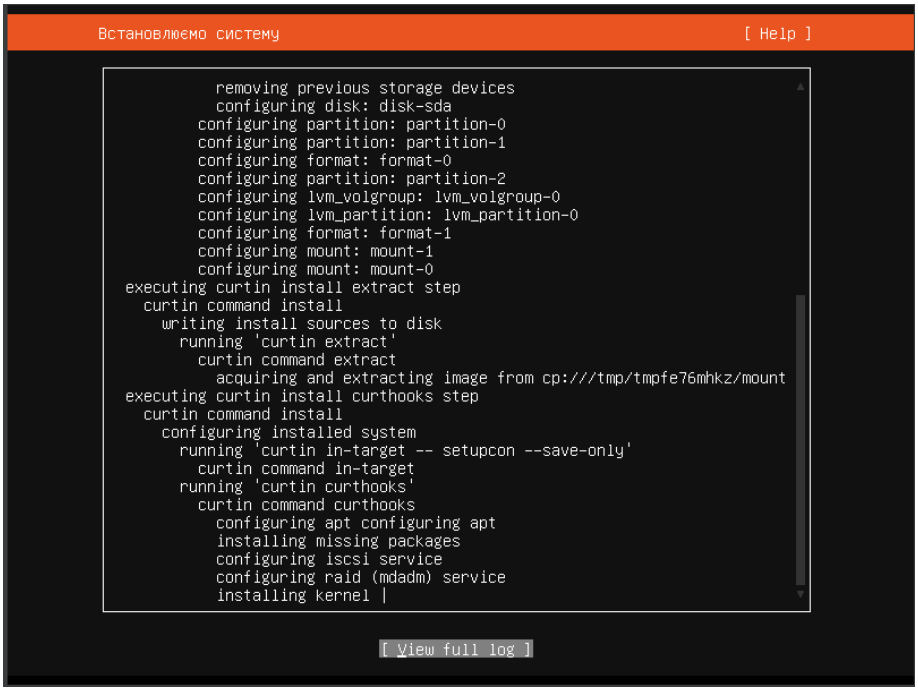


Рис. 3.3 Установка Ubuntu server

В кінці налаштування, треба встановити та налаштувати менеджер SNMP на сервері. Це дозволить серверу Zabbix контролювати пристрої за допомогою SNMP [7]. Для того, щоб це можна було зробити, у командному рядку Linux, треба набрати наступні команди:

```
sudo apt-get install libsnmp-mib-compiler-perl
sudo apt-get install snmp-mibs-downloader
sudo apt-get install libsnmp-base
sudo apt-get install libsnmp-dev
sudo apt-get install snmp
sudo apt-get install snmpd
```

Рис. 3.4 Лістинг команд установки SNMP

По завершенню налаштування, ми отримали налаштований сервер Ubuntu за SNMP. Далі треба встановити PostgreSQL (Рис. 3.6), який необхідний для організації

бази даних з якою працюватиме Zabbix. Це виконується офіційної документації, на сайті розробника за допомогою наступних команд:

```
sudo sh -c 'echo "deb https://apt.postgresql.org/pub/repos/apt $(lsb_release -cs)-pgdg main" >
/etc/apt/sources.list.d/pgdg.list'
wget --quiet -O - https://www.postgresql.org/media/keys/ACCC4CF8.asc | sudo apt-key add
sudo apt-get update
sudo apt-get -y install postgresql
```

Рис. 3.5 – Лістинг коду для установки Установка PostgreSQL;

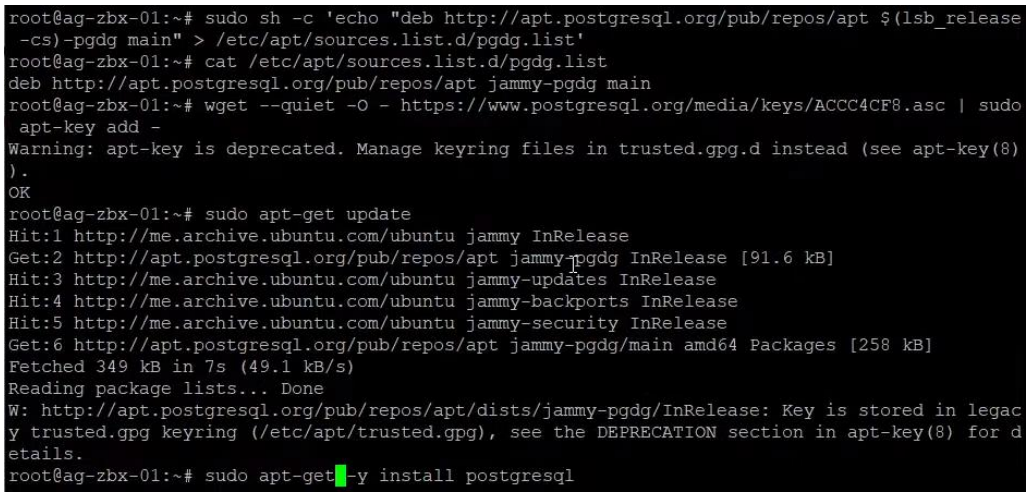


Рис. 3.6 Установка PostgreSQL

По завершенню установки, ми отримали готову базу для установки Zabbix server.

3.4. Встановлення Zabbix server та його налаштування

Перед початком установки, необхідно перейти на офіційну сторінку Zabbix, та перейти на вкладку продукту. На ній треба обрати наші налаштування (Рис. 3.7), після чого відкриється відповідна інструкція по установці та налаштуванню системи.

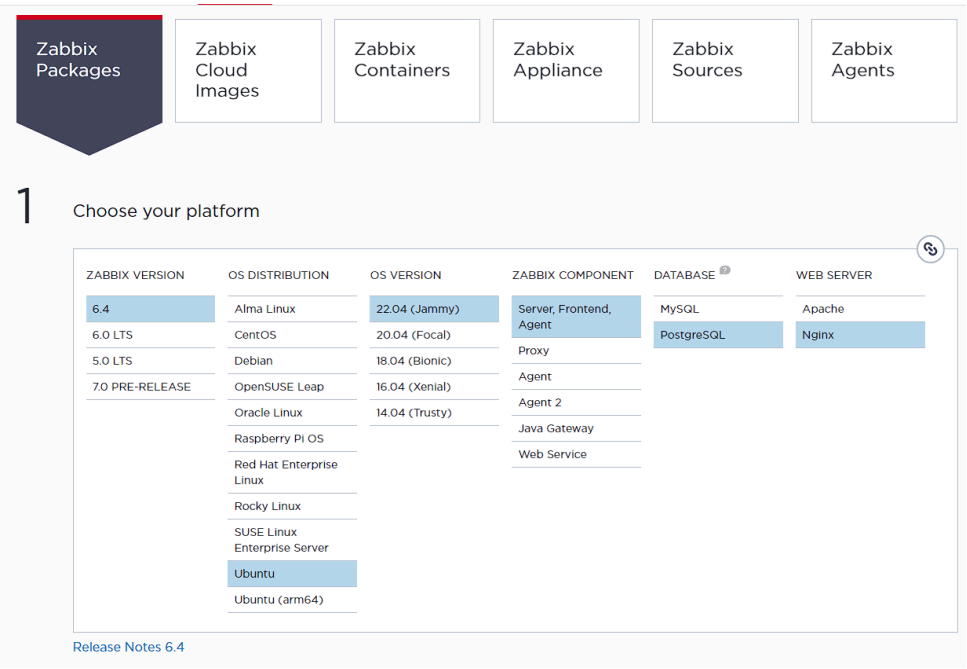


Рис. 3.7 Вибір версії Zabbix

Далі згідно документації, встановлюємо Zabbix server (Рис. 3.8) та завантажуємо скрипти роботи для бази даних, яку буде створено далі за допомогою наступних команд:

```
sudo wget http://repo.zabbix.com/zabbix/2.4/ubuntu/pool/main/z/zabbixrelease/zabbix-
release_2.4- 1 + trusty_all.deb
sudo dpkg -i zabbix-release_2.4-1 + trusty_all.deb
sudo apt-get
```

Рис. 3.7 Лістинг коду для установки Zabbix server

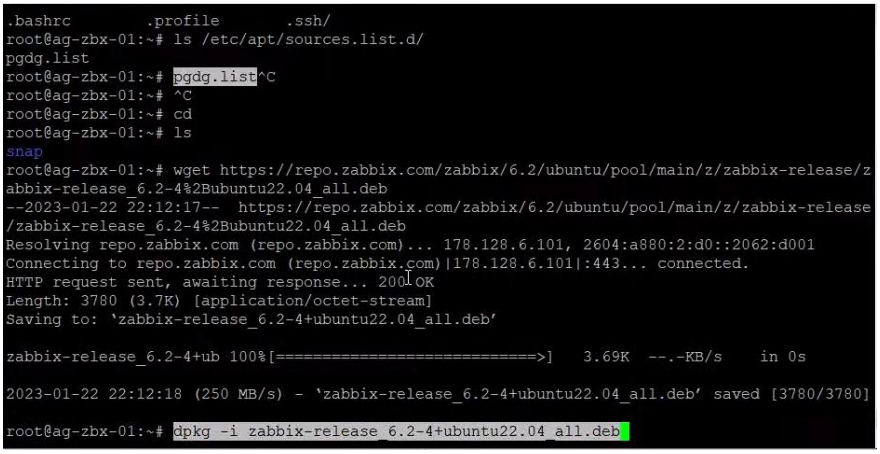


Рис. 3.8 Установка Zabbix server

У даному випадку встановлено пакет Zabbix v6.2, який включає компоненти, такі як Zabbix Server, інтерфейс Zabbix (GUI), Zabbix Proxy, Medial Server та Zabbix Database. Додатково, я розгорнув Zabbix Agent локально на Zabbix Server за допомогою команди:

```
sudo apt-get install zabbix-agent zabbix-server-mysql
zabbix-frontend-php snmpd php5-mysql php5-curl
```

Zabbix Agent відповідає за моніторинг локальних процесів на сервері Zabbix, забезпечуючи додаткові можливості для детального аналізу та контролю. Це рішення дозволяє ефективно керувати різноманітними аспектами системи та взаємодіяти з мережею компонентів Zabbix.

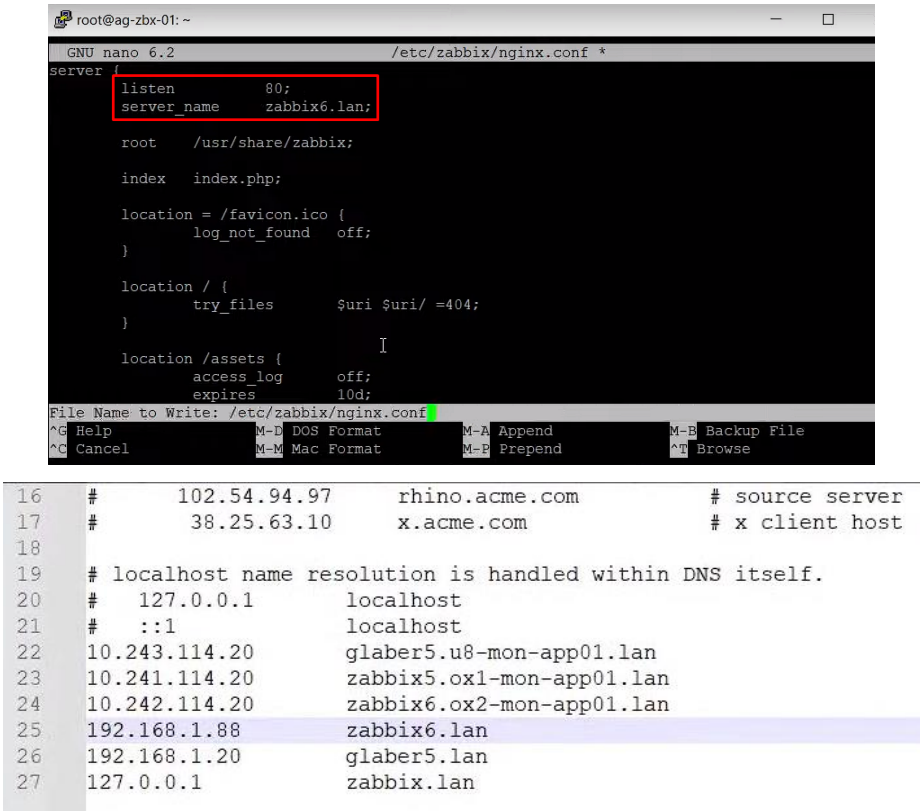
Далі необхідно створити базу даних, з допомогою наступних команд:

```
# sudo -u postgres createuser --pwprompt zabbix
# sudo -u postgres createdb -O zabbix zabbix
```

І тоді задіяти скрипти, завантажені раніше наступною командою:

```
# zcat /usr/share/zabbix-sql-scripts/postgresql/server.sql.gz | sudo -u zabbix psql zabbix
```

Фінальним кроком установки є налаштування хоста (Рис. 3.9), а саме порту та IP адреси, яку матиме сервер Zabbix.




```
16  #       102.54.94.97     rhino.acme.com          # source server
17  #        38.25.63.10     x.acme.com              # x client host
18
19  # localhost name resolution is handled within DNS itself.
20  #   127.0.0.1       localhost
21  #   ::1             localhost
22  10.243.114.20       glaber5.u8-mon-app01.lan
23  10.241.114.20       zabbix5.ox1-mon-app01.lan
24  10.242.114.20       zabbix6.ox2-mon-app01.lan
25  192.168.1.88        zabbix6.lan
26  192.168.1.20        glaber5.lan
27  127.0.0.1           zabbix.lan
```

Рис. 3.9 Налаштування хоста

Перед початком користування необхідно також налаштувати часовий пояс відповідно до регіону, де знаходиться сервер, та перезапуск сервера Nginx. Таким чином Zabbix Server було встановлено та проведено стартове налаштування. Крім того, Zabbix Agent було встановлено локально на Zabbix Server.

Наступним кроком є вхід у графічний інтерфейс Zabbix, та стартове налаштування з’єднання.

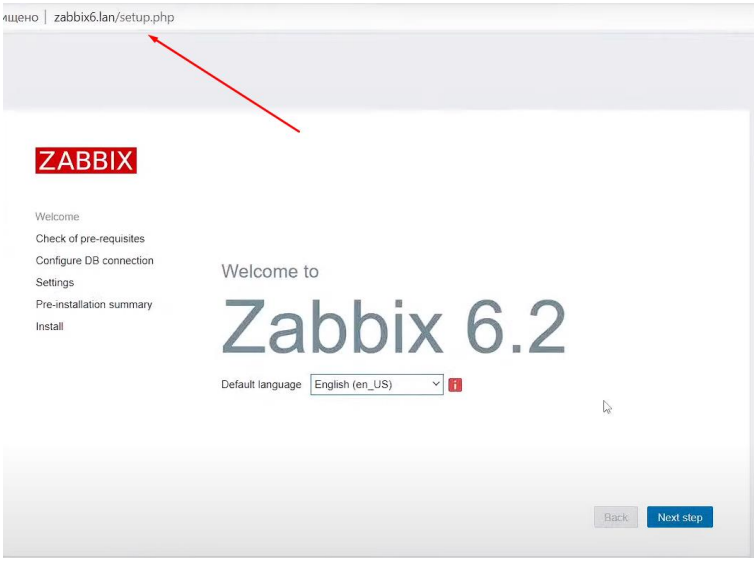


Рис. 3.10 Стартове вікно Zabbix

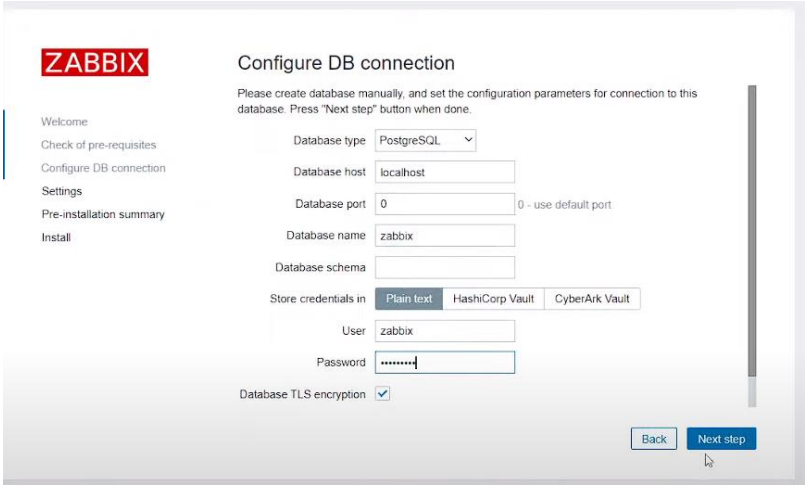


Рис. 3.11 Стартове налаштування з’єднання

3.5. Моніторинг за допомогою шаблонів

У ході процесу моніторингу на базі агента використовується програмне забезпечення, яке локально встановлюється на конкретному хості для збору даних моніторингу. Цей агент, який, у даному випадку, буде представлений програмним продуктом Zabbix Agent, спроможний надавати більш точну інформацію в порівнянні з рішеннями без агента. Важливою перевагою такого підходу є можливість забезпечити докладний збір даних про процеси на сервері.

Агент, що використовується в даному випадку, є легким програмним забезпеченням, яке не великою обсягом займає на диску. Тим не менше, слід

зазначити, що його використання може супроводжуватися певним впливом на продуктивність мережі [6].

У цьому конкретному сценарії моніторингу використовується Zabbix Agent на сервері Ubuntu, який виступає в якості віртуальної машини. Інсталяція агента здійснюється за допомогою команди sudo apt-get install zabbix-agent. Після завершення встановлення необхідно провести його налаштування. Це включає вказівку адреси, на яку будуть відправлятися зібрані агентом дані. У даному випадку це 192.168.1.10.

Далі, для розпочатку моніторингу, необхідно додати Ubuntu-сервер як хост у систему Zabbix, назвавши його "Linux Server 2". Також вказується шаблон OS Linux та відповідний IP-адреса (192.168.1.20). Використання даного шаблону надає можливість контролювати показники, такі як завантаження процесора, використання диска та мережевий трафік.

Такий підхід до моніторингу дозволяє забезпечити точність та ефективність збору даних, враховуючи особливості конкретного сервера та його процесів.

3.6. Автоматичне виявлення

У великих мережах ручне призначення шаблонів на кожному хості може бути часовим і ресурсозатратним завданням. Для автоматизації цього процесу використовується функція Auto Discovery.

Auto Discovery дозволяє автоматично виявляти пристрої в мережі. Знайдені пристрої можуть бути автоматично додані, імпортовані та призначені хостами та шаблонами. Це спрощує процес моніторингу, особливо у великих мережах. Auto Discovery може працювати як з агентами, так і без них, що забезпечує гнучкість у виборі методу моніторингу.

Перед використанням Auto Discovery важливо виконати певні попередні кроки. Рекомендується логічно групувати хости та перевіряти налаштування, такі як назва спільноти SNMP для пристроїв, що контролюються за допомогою SNMP, та наявність та налаштування агента Zabbix для пристроїв, які контролюються за його допомогою.

Створення нової топології мережі та класифікація пристроїв за їхнім типом є необхідним етапом. Після цього потрібно створити відповідні виявлення для кожної групи хостів. Для автоматичного створення хосту та призначення шаблону, необхідно налаштувати дію.

3.7. Додавання хоста локальної мережі, моніторинг якої буде виконано

Після всіх налаштувань, ми потрапили в робочий протір Zabbix. Для продовження роботи необхідно додати в систему хост мережі, моніторинг якої буде проведено. Такі налаштування спричинені тим, що сервер Zabbix, знаходиться в тій же локальній мережі.

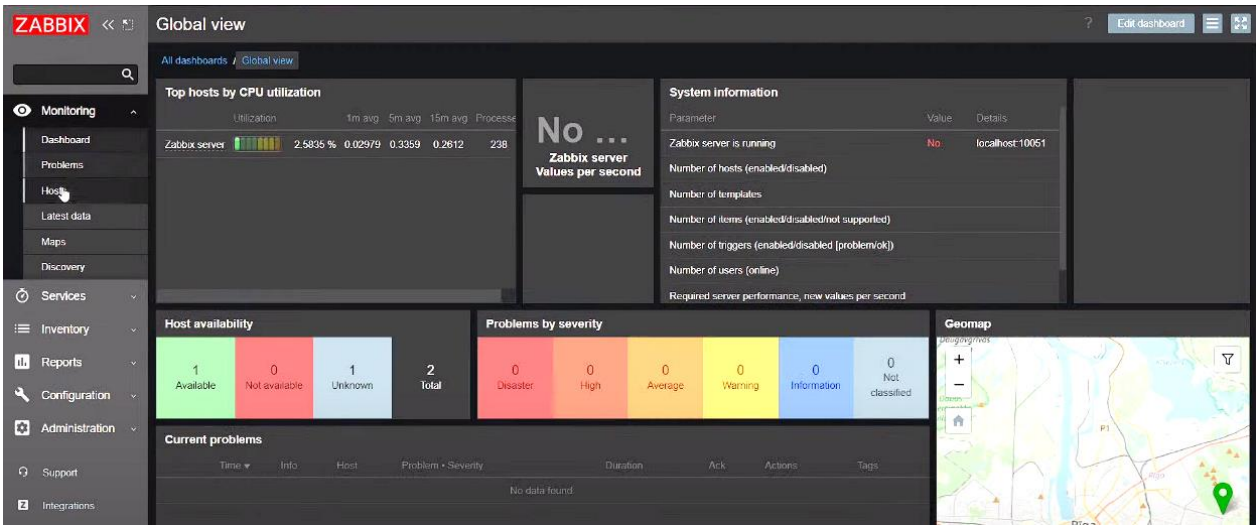


Рис. 3.12 Робочий простір Zabbix

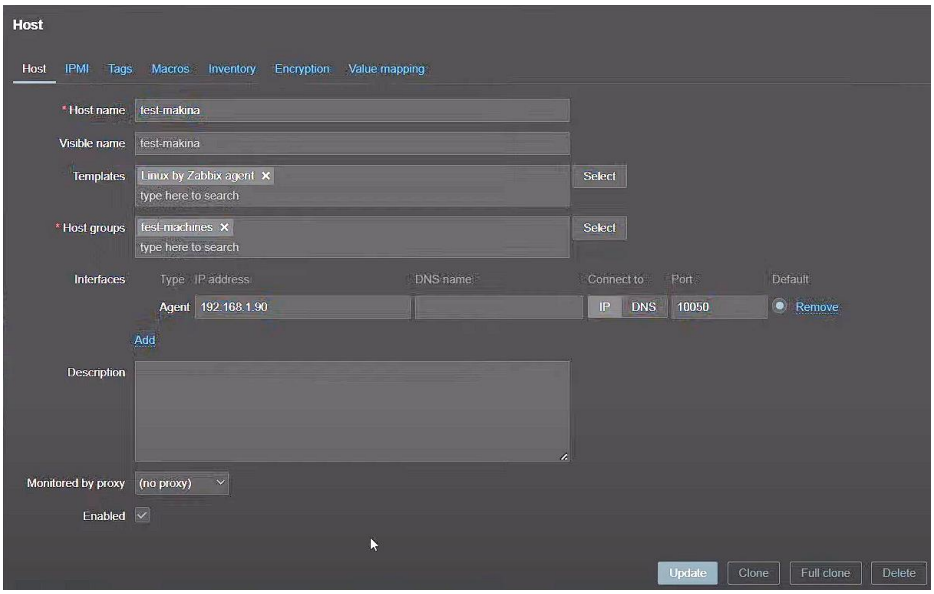


Рис. 3.13 Додавання локальної мережі в систему моніторингу

Після додавання мережі та налаштування параметрів моніторингу, дані про мережу почали отримуватися на сервер і тепер можна їх проаналізувати, але спочатку, для наведення контексту, треба описати мережу, моніторинг якої буде проведено.

3.8. Загальний опис мережі, моніторинг якої буде проведено

Локальна комп’ютерна мережа, моніторинг якої буде проведено, складається з:

– Чотирьох світчів, 3 з яких під’єднані до четвертого за допомогою оптоволоконних з’єднань;

– Безпосередньо сервера, де налаштований Zabbix;

– Роутера;

– 12 точок доступу Unifi;

– Трьох WiFi камер.

Більш точних даних про мережу, вказати не можна, оскільки це реальна діюча мережа підприємства і ці дані конфіденційні, втім цієї інформації достатньо, щоб зрозуміти як проходить моніторинг.

3.9. Аналіз результатів моніторингу

Налаштована система моніторингу, починає опитування та отримання даних, відразу після запуску в мережі. Система працює згідно алгоритму вказаному в 2 розділі. Збір базової інформації про всі пристрої в мережі, такі як IP-адреси, MAC-адреси, типи пристроїв і т.д. Виконується цей процес з допомогою протоколу ICMP. Це дає можливість отримати інформацію про кількість пристроїв у мережі, кількість підмереж (Рис. 3.15 та типи підключених пристроїв (Рис. 3.14). Це підтверджує, що використання протоколу ICMP в процесі моніторингу, дає свій результат. Система бачить всі пристрої та отримує повну інформацію про пристрої, їх стан, активні тригери і дані які можна отримати від них.

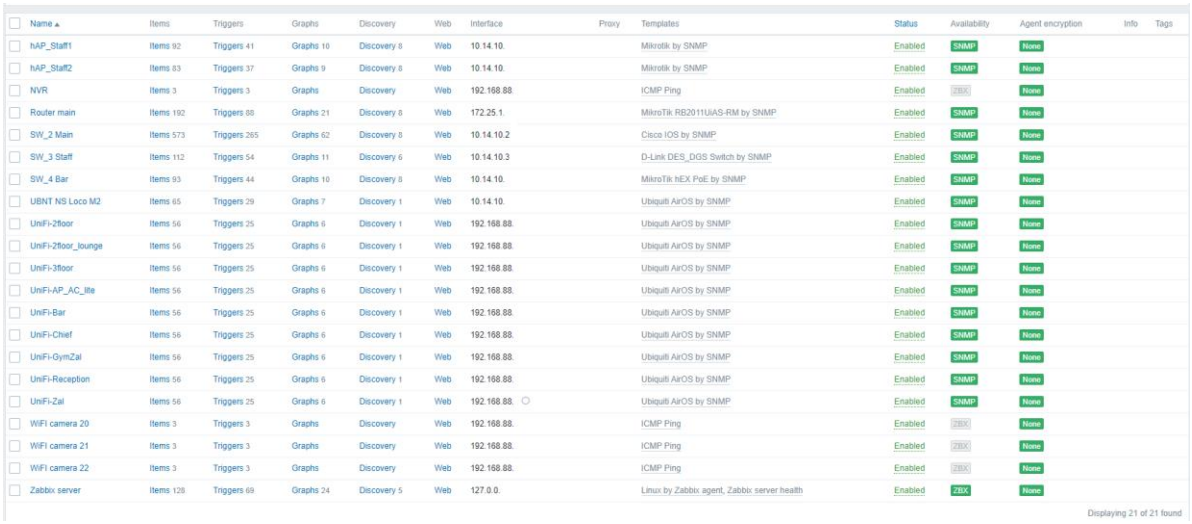


Рис. 3.14 Пристрої в локальній мережі та їх стан, дані про них

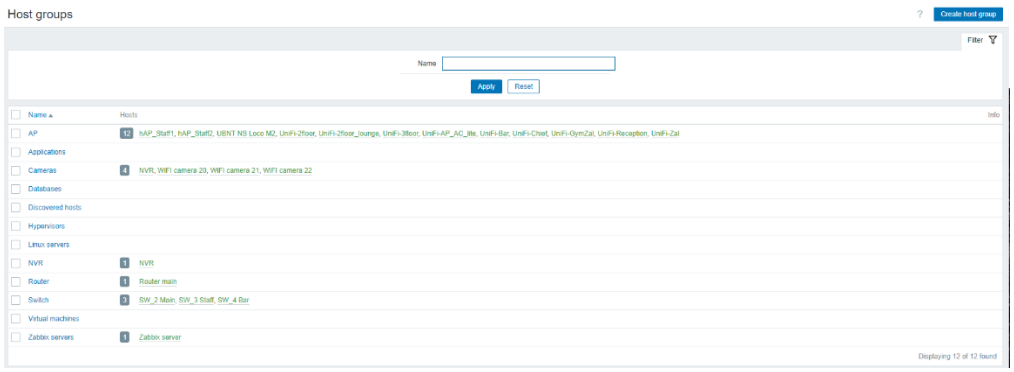


Рис. 3.15 Підмережі в локальній комп’ютерній мережі

Виявлення топології мережі для визначення зв’язків між пристроями. Маючи інформацію про підключені пристрої та методи їх підключення, автоматично побудовано віртуальну топологію (Рис. 3.16), що дає можливість розрахувати

значення ефективності роботи в ідеальних умовах. В цьому етапі використано протокол LLDP. Завдяки цьому, можна згенерувати актуальну топологію локальної комп'ютерної мережі. Цей метод працює швидко і не дає зайвого навантаження на систему.

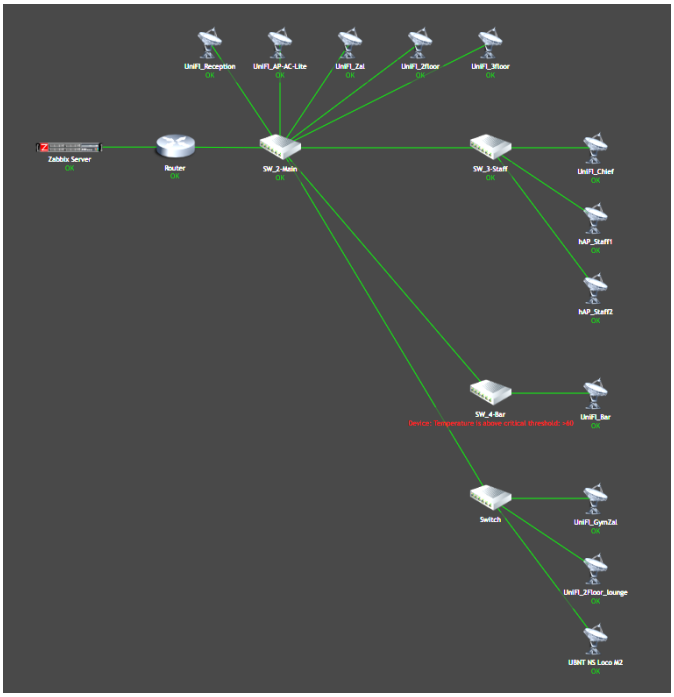


Рис. 3.16 Згенерована топологія локальної комп'ютерної мережі

Система відстежує доступність пристроїв у мережі. Сервер системи моніторингу періодично надсилає запити на пристрої і за наявністю відповіді відмічає, чи пристрій доступний. Періодична перевірка стану пристроїв, визначення їхньої продуктивності та реакції на запити. У відповідях від пристроїв до сервера, наведено дані про роботу пристрою, час витрачений на відповідь та час коли було отримано запит та надіслано відповідь, що дає можливість розрахувати затримку (Рис. 3.17) та визначити втрати пакетів на шляху (Рис. 3.18). Завдяки використанню цього метода, можна отримувати точну інформацію про доступність пристрою і якість з'єднання з ним.

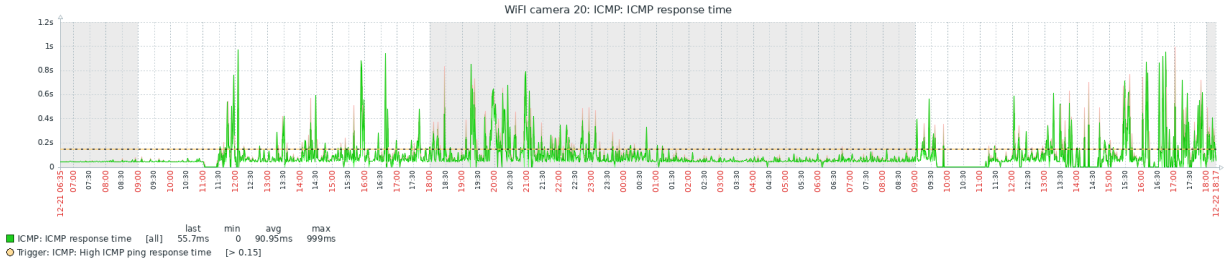


Рис. 3.17 Затримки до WiFi камери

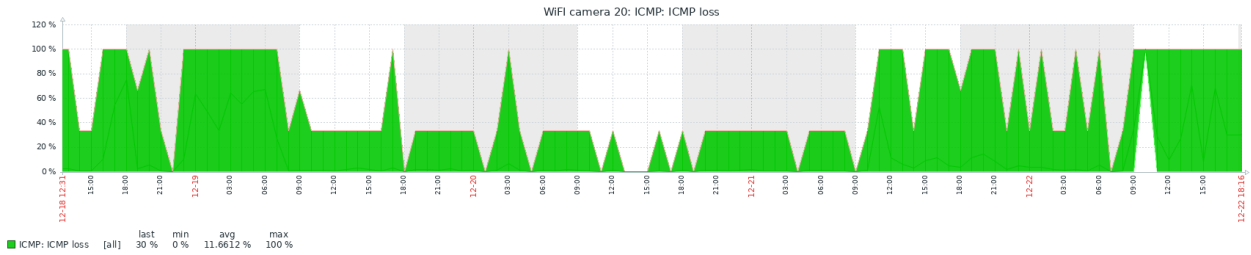


Рис. 3.18 Втрати пакетів до WiFi камери

За допомогою протоколу SNMP, можна отримати дані від роутера, про використання каналу провайдера, та від світчів, про рівень сигналу на оптоволоконному з’єднанні. Також цей протокол дає можливість надсилати команди цим керуючим пристроям, що дає можливість не тільки отримувати повну інформацію про роботу каналів зв’язку і безпосередньо пристроїв, а й переналаштовувати їх в режимі реального часу.

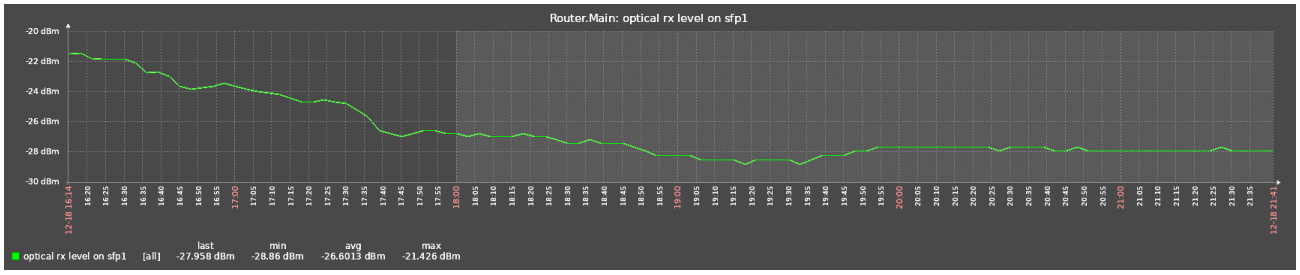


Рис. 3.19 Рівень сигналу на оптоволоконному з’єднанні

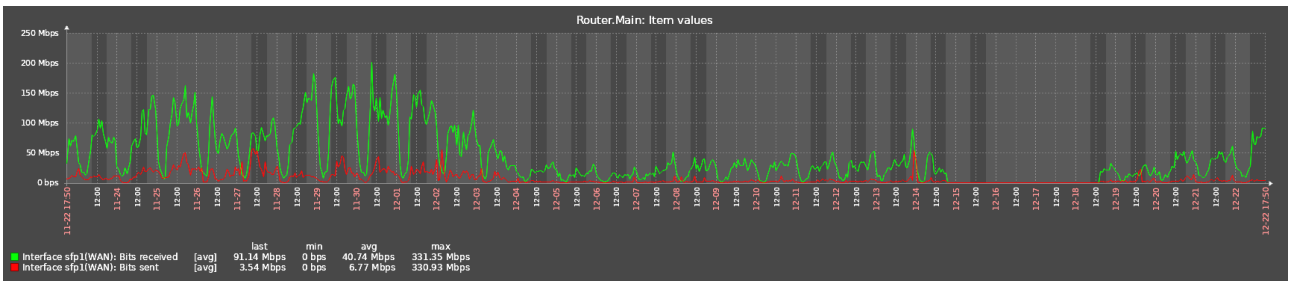


Рис. 3.20 Використання каналу провайдера

Також система Zabbix з допомогою системи Zabbix agent, дозволяє працювати з тригерами. Тригери в системі моніторингу Zabbix використовуються для визначення умов, при яких буде спрацьовувати сповіщення або виконуватися інші дії. Тригери можуть бути налаштовані для моніторингу різних параметрів і станів системи, і якщо стан визначеної умови виконується, тоді тригер вважається активним. Використання тригерів сильно спрощує виявлення проблем та їх вирішення, оскільки при спрацюванні тригера можна запустити скрипт який, наприклад активує резервну лінію зв'язку, або підключення до глобальної мережі через резервний провайдер.

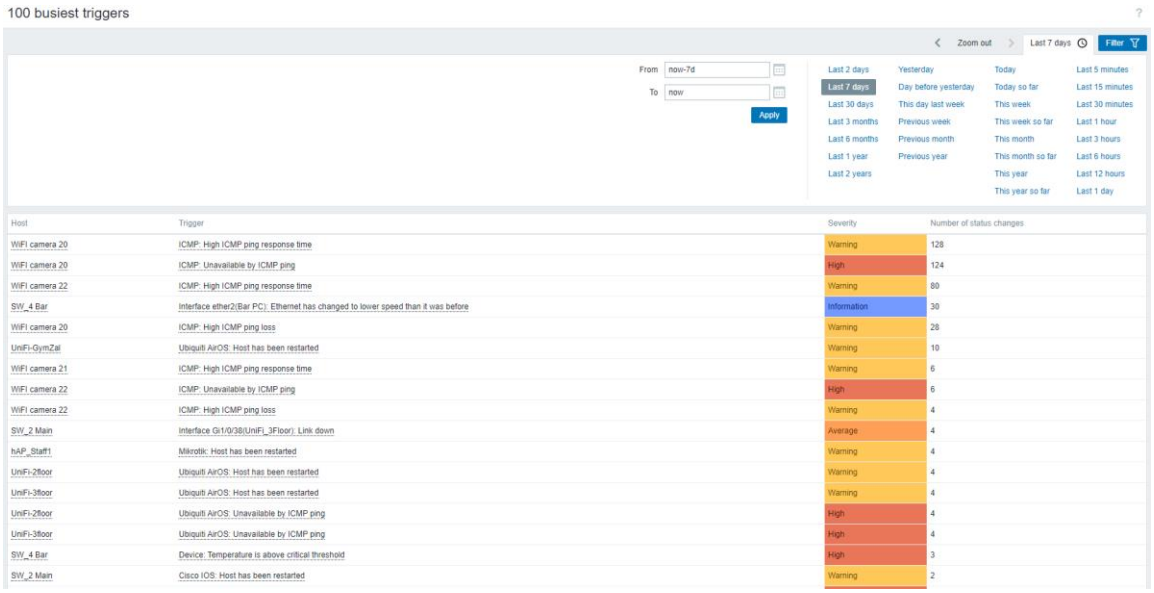


Рис. 3.21 Найчастіші спрацювання трігерів

В загальному система працює справно, згідно створеного алгоритму. Навантаження на систему при роботі мінімальне, оскільки кількість трафіку яким обмінюється сервер Zabbix з пристроями, мінімальна. Сервер робить запити тільки до керуючих пристроїв, таких як світчі та роутери, а вони вже надають всі необхідні дані. Для наглядності додано графік використання процесора в роутері, який показує зміну навантаження на його після запуску системи моніторингу.

Позначка на рисунку 3.22, це момент запуску моніторингу, після чого можна побачити пік навантаження, оскільки було виконано автоматичне виявлення мережі та збір загальних даних про мережу, далі навантаження повернулись до норми, і різниці між роботою з моніторингом і без немає, навіть наявні деякі покращення.

Скоріш за все система виявила якісь проблеми в налаштуваннях та виправила їх за допомогою SNMP протоколу. Це показує ефективність роботи системи та позитивний влив на роботу локальної комп’ютерної мережі.

Рис. 3.22 Вплив системи моніторингу на навантаження на процесор роутера

3.10. Висновки до розділу 3

В розділі було описано процес установки та налаштування системи моніторингу Zabbix, яка полягає в виконанні трьох основних етапів. Спочатку треба встановити та налаштувати Ubuntu server, на якому буде розгорнуто систему моніторингу. Наступним кроком, є розгортання Zabbix server, до цього етапу належить установка всіх необхідних компонентів системи та створення хоста. Останній крок, це вхід в графічний інтерфейс та впровадження системи моніторингу в локальну комп’ютерну мережу.

Після впровадження системи моніторингу в мережу, було проведено моніторинг локальної мережі, на протязі тижня. В результаті було отримано результати вказані в підпункті 3.9, які показують що система моніторингу Zabbix, працююча за розробленим алгоритмом, працює справно та виконує свої функції в повній мірі без серйозного впливу на продуктивність мережі. Всі дані від інформації про топологію до спрацювання тригерів, збираються точно і своєчасно, що дає можливість відзначити такий метод моніторингу ефективним. Після запуску системи, можна побачити пік навантаження, оскільки було виконано автоматичне виявлення мережі та збір загальних даних про мережу, далі навантаження повернулись до норми, і різниці між роботою з моніторингом і без немає, навіть наявні деякі покращення.

Скоріш за все система виявила якісь проблеми в налаштуваннях та виправила їх за допомогою SNMP протоколу. Це показує ефективність роботи системи та позитивний влив на роботу локальної комп'ютерної мережі. Враховуючи те, що залишається достатньо великий запас по продуктивності, є можливість для розширення функціоналу системи моніторингу Zabbix server.

В загальному моніторингу, показали що продуктивність локальної мережі підвищилась, після впровадження системи моніторингу, тому основне завдання роботи, знайти метод підвищення ефективності роботи системи моніторингу, виконано.

РОЗДІЛ 4
ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ

4.1 Охорона праці

Тема кваліфікаційної роботи звучить як, «Методи підвищення ефективності та моніторингу роботи локальної комп'ютерної мережі». В роботі розглянуто шляхи підвищення ефективності роботи системи моніторингу комп'ютерної мережі, ця система розміщена на сервері та є абсолютно автономною, саме тому ніяким чином не впливає на рівень безпеки працівників. Втім, вона працює на серверному обладнанні та для підтримки працездатності іноді вимагає втручання адміністратора, який в свою чергу, має свій кабінет оснащений комп'ютером.

Приміщення, в якому установлено робоче місце з комп'ютером, відповідає проектній документації будинку, погодженій з уповноваженими державними органами. В Державних санітарих правилах і нормах роботи з візуальними дисплейними терміналами електронно-обчислювальних машин ДСанПІН 3.3.2.007-98, затверджених Постановою Головного державного санітарного лікаря України №7 від 10 грудня 1998 року. Правила поширюються на умови й організацію праці при роботі з візуальними дисплейними терміналами (ВДТ) усіх типів вітчизняного та зарубіжного виробництва на основі електронно-променевих трубок (ЕПТ), що використовуються в електронно-обчислювальних машинах (ЕОМ) колективного використання та персональних ЕОМ (ПЕОМ).

На підприємстві згідно з ДСанПІН 3.3.2.007-98 кожній кімнаті, де обладнані робочі місця співробітників, що працюють на комп'ютері, наявні елементи природного та штучного освітлення. При цьому, на вікнах встановлено легко регульовані жалюзі чи штори, які дозволять працівникам коригувати рівень освітлення в приміщенні. Комп'ютери в кімнаті розміщено таким чином, щоб світло потрапляло на екрани моніторів з півдня чи північного сходу. З метою досягнення максимального рівня безпечності і охорони праці при роботі з комп'ютером, виробничі приміщення обладнано аптечками першої медичної допомоги, системами автоматичної пожежної сигналізації і вогнегасниками. В приміщенні, в якому разом працюють 5 або більше комп'ютерів, на видимому місці Встановлено службовий

вимикач, який у разі потреби дозволить повністю відключити електричне живлення кімнати.

Згідно з ДБН "П.1.2-2:2016 [15] Пожежна безпека об'єктів будівництва" в приміщенні де працює адміністратор забезпечені евакуаційні шляхи, тобто забезпечені належної ширини евакуаційних шляхів та дверей, які відповідають вимогам до протипожежної безпеки. Інженерні комунікації встановлені так, щоб запобігати поширенню вогню через них. Система пожежогасіння встановлена та повністю справна. Також наявна система димовідведення, що забезпечує безпечну евакуацію. Будівля поділена на зони, розділені пожежостійкими перегородками, що зашкоджує поширенню пожежі.

Електробезпеку робочого місця регламентують Правила безпечної експлуатації електроустановок споживачів, які затверджені наказом Держнаглядохоронпраці від 09.01.98 N 4, зареєстрованих у Міністерстві юстиції України 10.02.98 за N 93/2533 (НПАОП 40.1-1.21-98). Використовувана електромережа відповідає правилам :

– живлення електромережі проектовано, як окрему групову трьох провідну мережу з використанням фази, робочого «нуля» та захисного «нуля»;

– захисний «нуль» застосовано для реалізації заземлення електропристроїв;

– усі електричні та електронні пристрої мають захист від короткого замикання та непередбачуваних аварійних ситуацій;

– монтаж та експлуатація електромережі задовольняють вимогам щодо унеможливлення виникнення джерела загоряння через коротке замикання та перевантаження;

– усі лінії електроживлення виконанні не з легкозаймистого матеріалу або з негорючою ізоляцію;

– електричне устаткування підключено до мережі лише за допомогою справних штепсельних з’єднань і розеток заводського виготовлення;

– у розетках і штепселях передбачено контакти заземлення.

Оскільки робота виконується на серверному обладнанні є сенс перевірити дотримання норм охорони праці в серверному приміщенні. Приміщення відповідає стандарту TIA/EIA-569, що визначений Американським інститутом телекомунікацій

(TIA) та Американським інститутом електротехнічних інженерів (EIA) та містить вимоги та рекомендації для планування та будівництва серверних приміщень або центрів обробки даних. Згідно стандарту, висота серверного приміщення складає 3 метра (при нормі не менше 2,44 м), площа приміщення 15 м². Розміщене приміщення так, що є можливість розширення за рахунок сусіднього приміщення. Важливим аспектом є встановлена вентиляція, згідно вимог ASHRAE (American Society of Heating, Refrigerating and Air-Conditioning Engineers – американське товариство інженерів опалення, вентиляції та кондиціювання повітря), з захистом від пилу. Такі заходи забезпечують концентрації шкідливих речовин що не перевищують гранично допустиму норму та значно підвищують надійність роботи і безпечність обслуговування серверного обладнання.

Серверна кімната оснащена системами:

- Охоронної сигналізації;
- Пожежної сигналізації;
- Пожежогасіння;
- Контролю доступу;
- Кондиціонування;
- Освітлення;
- Аварійного освітлення (для роботи при відключенні робочого освітлення).

Як висновок, серверне приміщення як і робоче місце адміністратора, відповідає міжнародним вимогам та стандартам, оскільки вони обладнані необхідним оснащенням та мають відповідні розміри. Всі системи, від вентиляції до сигналізацій, присутні.

4.2 Безпека в надзвичайних ситуаціях

4.2.1 Організація цивільного захисту [16] на об’єктах промисловості та виконання заходів щодо запобігання виникненню надзвичайних ситуацій техногенного походження. Зростаючий вплив людини на навколишнє середовище, швидкий розвиток технологій і посилення експлуатації окремих територій земної кулі призводить до істотних змін у навколишньому середовищі, порушує екологічну рівновагу і процеси природної саморегуляції. Ризик виникнення стихійних лих і техногенних аварій стрімко росте. Як наслідок, засоби масової інформації майже щодня повідомляють про надзвичайні ситуації, що відбуваються у світі: стихійні лиха, аварії, катастрофи на підприємствах і транспорті, що супроводжуються загибеллю людей, руйнуванням житлових будинків, об'єктів господарювання, інфраструктури, забрудненням і зараженням довкілля.

У зв’язку з його прийняттям низка законодавчих актів України, що регулювали відносини у відповідній сфері, визнано такими, що втратили чинність, серед них закони України: «Про Цивільну оборону України», «Про пожежну безпеку», «Про війська Цивільної оборони України», «Про аварійно-рятувальні служби», «Про захист населення і територій від надзвичайних ситуацій техногенного та природного характеру», «Про правові засади цивільного захисту».

Цивільний захист [17] – це функція держави, спрямована на захист населення, територій, навколишнього природного середовища та майна від надзвичайних ситуацій шляхом запобігання таким ситуаціям, ліквідації їх наслідків і надання допомоги постраждалим у мирний час та в особливий період. Цивільний захист забезпечується з урахуванням особливостей, визначених Законом України «Про основи національної безпеки України», суб’єктами, уповноваженими захищати населення, території, навколишнє природне середовище і майно, Кодексом цивільного захисту – у мирний час, а також в особливий період – у межах реалізації заходів держави щодо оборони України.

Основні принципи здійснення цивільного захисту:

1) гарантування та забезпечення державою конституційних прав громадян на захист життя, здоров’я та власності;

2) комплексного підходу до вирішення завдань цивільного захисту;

3) пріоритетності завдань, спрямованих на рятування життя та збереження здоров’я громадян;

4) максимально можливого, економічно обґрунтованого зменшення ризику виникнення надзвичайних ситуацій;

5) централізації управління, єдиноначальності, підпорядкованості, статутної дисципліни Оперативно-рятувальної служби цивільного захисту, аварійно-рятувальних служб;

6) гласності, прозорості, вільного отримання та поширення публічної інформації про стан цивільного захисту, крім обмежень, встановлених законом;

7) добровільності – у разі залучення громадян до здійснення заходів цивільного захисту, пов'язаних з ризиком для їхнього життя і здоров'я;

8) відповідальності посадових осіб органів державної влади та органів місцевого самоврядування за дотримання вимог законодавства з питань цивільного захисту;

9) виправданого ризику та відповідальності керівників сил цивільного захисту за забезпечення безпеки під час проведення аварійно-рятувальних та інших невідкладних робіт.

Запобігання виникненню надзвичайних ситуацій техногенного та природного характеру - підготовка і реалізація комплексу правових, соціально-економічних, політичних, організаційно-технічних, санітарно-гігієнічних та інших заходів, спрямованих на регулювання техногенної та природної безпеки, проведення оцінки рівнів ризику, завчасне реагування на загрозу виникнення надзвичайної ситуації техногенного та природного характеру на основі даних моніторингу, експертизи, досліджень та прогнозів щодо можливого перебігу подій з метою недопущення їх переростання у надзвичайну ситуацію техногенного та природного характеру або пом'якшення її можливих наслідків.

Функції запобігання надзвичайним ситуаціям техногенного та природного характеру в Україні виконує Єдина державна система запобігання і реагування на надзвичайні ситуації техногенного і природного характеру, положення про яку затверджено Постановою Кабінету Міністрів України № 1198.

Ця система включає в себе:

- центральні та місцеві органи виконавчої влади
- державні підприємства

- установи та організації, які здійснюють нагляд за забезпеченням техногенної і природної безпеки, організація проведення роботи по запобіганню НС з метою захисту населення, території та довкілля.

Запобігання виникненню надзвичайних ситуацій техногенного походження на виробництві передбачає впровадження комплексу заходів та принципів забезпечення безпеки:

- Систематичний аналіз потенційних небезпек та надзвичайних ситуацій на всіх етапах виробничого процесу.
- Відповідність стандартам та нормативам з технічної безпеки та охорони праці відповідно до галузевих вимог.
- Забезпечення професійної підготовки та підвищення кваліфікації персоналу для свідомого та безпечного виконання робочих завдань.
- Регулярне технічне обслуговування та перевірка обладнання для запобігання технічним збоям та аварій.
- Системи моніторингу та контролю за виробничими процесами для своєчасного виявлення аномалій.
- Забезпечення ефективної системи електробезпеки та відповідність електроустановок вимогам безпеки.
- Розробка та практична впровадження планів евакуації та рятувальних заходів в разі надзвичайних ситуацій.
- Встановлення та регулярна перевірка систем пожежогасіння та димовідведення для запобігання пожежам та мінімізації їх наслідків.
- Безпечне управління відходами та дотримання вимог щодо хімічної безпеки при використанні речовин.

З метою запобігання виникненню надзвичайних ситуацій природного і техногенного характеру місцеві органи виконавчої влади у відповідності до чинного законодавства повинні здійснювати комплекс організаційних та інженерно-технічних заходів, зокрема.

Організаційні-економічні заходи – щорічне уточнення прогнозних даних щодо ризику виникнення надзвичайних ситуацій, визначення найбільш гострих проблемних питань щодо запобігання надзвичайним ситуаціям;

Інженерно-технічні заходи – до них належать удосконалення технологічних процесів, підвищення надійності технологічного обладнання та експлуатаційної надійності систем, своєчасне оновлення виробничих фондів, застосування якісної конструкторської документації, високоякісної сировини, матеріалів, комплектуючих виробів, використання кваліфікованого персоналу, створення і використання ефективних систем контролю та технічної діагностики, безаварійної зупинки виробництва, локалізація і ліквідація аварійних ситуацій;

Заходи, що здійснюються на потенційно небезпечних об'єктах – створення об'єктових і локальних систем оповіщення працюючого персоналу, систем раннього виявлення витоку небезпечних хімічних речовин, запровадження систем автоматичного контролю і сигналізації про ймовірність витоку небезпечних і шкідливих речовин та інші системи безпеки.

4.2.2 Оцінка стійкості роботи промислового підприємства до дії світлового випромінювання ядерного вибуху. Оцінка стійкості промислового підприємства до впливу світлового випромінювання, виниклого в результаті ядерного вибуху, є завданням, що передбачає ретельний аналіз та комплексні заходи для забезпечення безпеки працівників, інфраструктури та навколишнього середовища [15].

1. Технічний Аналіз:

– Глибокий розгляд технічних аспектів впливу світлового випромінювання на основі характеристик ядерного вибуху. Врахування параметрів, таких як дози опромінення, інтенсивність випромінювання, інтервал часу та інші важливі показники.

2. Оцінка Вразливості Технологічних Процесів:

– Визначення впливу випромінювання на ключові технологічні процеси підприємства та класифікація обладнання за ступенем чутливості. Впровадження заходів для захисту важливого устаткування.

3. Організаційні Процедури та Навчання:

– Розробка та впровадження ефективних організаційних процедур для реагування на надзвичайні ситуації. Навчання персоналу з евакуації, роботи з

протипожежним та протививідомим обладнанням, а також надання першої допомоги в умовах випромінювання.

4. Оцінка Відповідності Інфраструктури та Засобів Захисту:

– Перевірка будівель, споруд та інфраструктури на відповідність стандартам безпеки в умовах ядерного випромінювання. Визначення та покращення засобів захисту.

5. Зони Ризику та Евакуаційні Маршрути:

– Визначення та позначення зон ризику, розробка евакуаційних планів та встановлення чітких маршрутів для персоналу. Систематичні тренування для перевірки ефективності евакуації.

6. Системи Оповіщення та Комунікації:

– Розгортання ефективних систем оповіщення для персоналу та населення. Забезпечення надійних засобів зв'язку для координації дій в екстрених ситуаціях.

7. Запаси та Резерви:

– Визначення необхідних запасів, включаючи противорадіаційні матеріали та інші резервні засоби для забезпечення функціонування підприємства в умовах надзвичайної ситуації.

8. Співпраця з Органами Державного Управління:

– Активна співпраця з органами цивільного захисту, правоохоронними та рятувальними службами для забезпечення координації дій та обміну інформацією в разі надзвичайних ситуацій.

Ця комплексна оцінка забезпечує високий рівень підготовленості промислового підприємства до можливих наслідків світлового випромінювання внаслідок ядерного вибуху, допомагаючи зменшити ризики та максимізувати стійкість у випадку кризової ситуації.

Для підвищення стійкості до світлового випромінювання в будівлях і спорудах які будуються повинні застосовуватися вогнестійкі конструкції, а також вогнезахисна обробка горючих елементів будівель. У кам’яних будівлях перекриття повинні бути виготовлені з армованого бетону або виконані з бетонних плит. Великі за розміром будівлі повинні розділятися на секції вогнетривкими стінами (брандмауерами).

Складські приміщення для зберігання легкозаймистих речовин (бензин, гас, нафта, мазут і т.п.) повинні розміщуватися в окремих блоках заглиблене біля кордонів території об’єкта або за її межами.

Деякі унікальні види технологічного обладнання доцільно розміщувати в найбільш міцних спорудах (підвалах, підземних спорудах) або в будівлях з легких негорючих конструкцій павільйонного типу, під навісами або відкрито.

ВИСНОВКИ

У даній кваліфікаційній роботі обґрунтовано вибір методів моніторингу локальної комп’ютерної мережі та підвищення ефективності її роботи.

1. В першому розділі, було розглянуто актуальні системи та методи моніторингу локальної мережі. Результатом став вибір системи моніторингу локальної мережі Zabbix, як найбільш продуктивної, доступної та зручної. Застосування цієї системи дозволить виконувати моніторинг мережі більш точно та з меншим навантаженням на обладнання.

2. Досліджено методи моніторингу локальної мережі та обрано найоптимальніші для ефективного моніторингу локальної комп’ютерної мережі. Ці методи в комплексі, забезпечать повний моніторинг всіх важливих параметрів локальної мережі.

3. Було сформовано основні критерії ефективності та параметри для завдання моніторингу локальної мережі. Дотримання цих критеріїв, при розробці системи моніторингу, забезпечить чітку та швидку роботу системи моніторингу.

4. На основі критеріїв ефективності та обраних методів моніторингу було сформовано загальний алгоритм роботи системи моніторингу. Цей алгоритм дозволить повністю використати потенціал обраних методів моніторингу, та виконувати точний моніторинг локальної комп’ютерної мережі.

5. Впроваджено обрану систему моніторингу та виконано моніторинг комп’ютерної мережі згідно алгоритму. Це дало розуміння про можливості системи моніторингу на основі розробленого алгоритму.

6. Проаналізовано результати моніторингу, які показали підвищення ефективності роботи системи моніторингу. Згідно результатів аналізу, система моніторингу локальної мережі, має вищу ефективність роботи в порівнянні з аналогічними системами, що підтверджує ефективність роботи алгоритму на основі вибраних методів.

Впровадження одержаних результатів дипломної роботи дозволить підвищити ефективність моніторингу в режимі реального часу та дозволить відстежувати стан мережі та пристроїв у ній, своєчасно запобігати проблемам з якістю чи надійністю

мережі, що значно покращує якість комунікації між робочими станціями в межах підприємства.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Моніторинг і аналіз локальних мереж. URL: http://ni.biz.ua/10/10_19/10_190257_v-o-p-r-o-s---momenti-inertsii-secheniy-prostih-form.html (Дата звернення 16.12.2023).

2. Моніторинг мережі. Протоколи, найкращі практики, інструменти 2021. URL: https://eska.global/blog/setevoj-monitoring-protokoly-luchshie-praktiki-instrumenty-2020 (Дата звернення 16.12.2023).

3. Проценко Я. В. Дослідження методів моніторингу ресурсів і сервісів локальної комп'ютерної мережі : кваліфікаційна робота на здобуття ступеня вищої освіти «магістр» / Проценко Я. В.; науковий керівник доц., к.т.н. Лєпа Є. В. – Херсон : ХНТУ, 2020. – 80 с.

4. Марків В.А., Осухівська Г.М., Лещишин Ю.З., Луцків А.М. Комп’ютерна система аутентифікації осіб // Матеріали XX наукової конференції ТНТУ ім. І. Пулюя. 2017. С. 90–91.

5. Краус Н.М. Методологія та організація наукових досліджень: навчальнометодичний посібник. – Полтава: Оріяна, 2012. – 183 с.

6. Карпенко Р. С. Аналіз можливостей системи моніторингу ZABBIX для оператора зв'язку : дипломна робота … бакалавра : 172 Телекомунікації та радіотехніка / Карпенко Руслан Сергійович. – Київ, 2021. – 76 с.

7. Простий протокол мережевого управління (SNMP). URL: https://cqr.company/ua/wiki/protocols/simple-network-management-protocol-snmp/ (Дата звернення 16.12.2023).

8. Документація Zabbix. URL: https://www.zabbix.com/documentation/current/ua (Дата звернення 16.12.2023).

9. Enterprise IT monitoring with Zabbix. URL: https://www.zabbix.com/enterprise_monitoring (Дата звернення 16.12.2023).

10. Лещишин Ю. З., Романишин Н.Р., Наконечний В. В., Паламарчук А.О. Розробка системи зв’язку як інтегрованого елементу роботизованих систем // Зб. тез доповідей XXI Всеукр. наук.-пр. конф. Житомир, 2016. С. 102.

11. Leschyshyn Y., Scherbak L., Nazarevych O., Gotovych V., Tymkiv P., Shymchuk G. Multicomponent Model of the Heart Rate Variability Change-point // IEEE

XVth International Conference on the Perspective Technologies and Methods in MEMS Design (MEMSTECH). 2019. P. 110–113.

12. Tymkiv P., Leshchyshyn Y. Algorithm Reliability of Kalman Filter Coefficients Determination for Low-Intensity Electroretinosignal // IEEE 15th International Conference on the Experience of Designing and Application of CAD Systems (CADSM). 2019. P.1-5.

13. Leschyshyn Y., Semchyshyn O. Periodically correlated heart rate variability detection by Neyman - Pearson criterion // 9th International Conference - The Experience of Designing and Applications of CAD Systems in Microelectronics. 2007. P. 139–140.

14. Лупенко С.А., д.т.н., проф.; Луцик Н.С., докт. філософ., доц.; Луцків А.М. к.т.н., доц.; Осухівська Г.М., к.т.н., доц.; Тиш Є.В., к.т.н. Методичні рекомендації до виконання кваліфікаційної роботи магістра // Затверджено на засіданні кафедри комп’ютерних систем та мереж, протокол №1 від 30 серпня 2021 р. – с. 34.

15. ДБН П.1.2-2:2016 Система забезпечення надійності та безпеки будівельних об'єктів. Навантаження і впливи. Нормипроектування –К.: МінбудУкраїни, 2006- 75с.

16. Наказ Держнаглядохоронпраці від 09.01.98 N 4, зареєстрованих у Міністерстві юстиції України 10.02.98 за N 93/2533 (НПАОП 40.1-1.21-98).

17. Указ Президента України «Про Концепцію захисту населення і територій у разі загрози та виникнення надзвичайних ситуацій» м. Київ 26 березня 1999 року N 284/99

ДОДАТОК А

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ТЕРНОПІЛЬСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ ІМЕНІ ІВАНА ПУЛЮЯ

М А Т Е Р І А Л И

XI НАУКОВО-ТЕХНІЧНОЇ КОНФЕРЕНЦІЇ

«ІНФОРМАЦІЙНІ МОДЕЛІ, СИСТЕМИ ТА ТЕХНОЛОГІЇ»

13-14 грудня 2023 року

ТЕРНОПІЛЬ
2023

УДК 004.7
І. Кардаш; Ю. Лещишин, к.т.н.; А. Варавін, к.ф.-м.н.

(Тернопільський національний технічний університет імені Івана Пулюя)

МОНІТОРИНГ ЕФЕКТИВНОСТІ РОБОТИ ЛОКАЛЬНИХ МЕРЕЖ

I. Kardash; Yu. Leshchyshyn, Ph.D.; A. Varavin, Ph.D.

MONITORING OF THE EFFICIENCY OF LOCAL NETWORKS

Сучасні локальні мережі це стабільні та надійні системи обміну даними між комп'ютерами в межах підприємства, але тільки на перший погляд. Будь яка система може мати проблеми з ефективністю роботи, але щоб визначити причину втрат ефективності, необхідний спеціальний інструмент.

Моніторинг мережі – це процес, при якому всі мережеві компоненти, такі як маршрутизатори, комутатори, сервери та віртуальні машини, відстежуються на предмет збоїв та продуктивності та постійно оцінюються для підтримки та оптимізації їх доступності. Випереджальне виявлення проблем із продуктивністю допомагає виявити проблеми на початковому етапі. Ефективний попереджувальний моніторинг може запобігти простоям, або збоям мережі. В даному дослідженні моніторинг мережі займає центральну позицію, оскільки для оцінки ефективності роботи локальної мережі необхідно отримати, повну статистику роботи. Необхідно дослідити пропускну здатність, затримки, навантаження мережі, щоб отримати повну картину ефективності мережі. Збір даних виконується через протокол керування мережі SNMP.

Зазвичай при використанні SNMP присутні керовані та керівні системи. До складу керованої системи входить компонент, який називається агентом, який відправляє звіти керівній системі. По суті SNMP агенти передають управлінську інформацію на керівні системи як змінні (такі як «вільна пам'ять», «ім'я системи», «кількість процесів, що працюють» тощо). В контексті дослідження SNMP протокол призначений для отримання даних з бази керівної інформації, не визначаючи її а посилаючись на адреси в цій базі. Мережева станція управління надсилає запит з адресою необхідних даних на агента, який перенаправляє її на субагента, та оформляє відповідь до менеджера. Ці дані накопичуються, систематизуються системою моніторингу мережі та утворюють статистику роботи локальної мережі. За цією статистикою можна визначити вразливі точки системи.

Найпопулярнішим та найпродуктивнішим інструментом моніторингу мережі, є система моніторингу служб і станів Zabbix. Основними перевагами її є універсальність за рахунок колосальної кількості користувацьких розширень, що дає можливість не тільки глибокого моніторингу мережі, а й можливість автоматично реагувати на тригери (зміни в роботі мережі), підключаючи резервні пристрої чи зміну налаштувань мережі.

Програма збирає повні дані про мережеву активність та на їх основі формує зручні звіти, які можна подати в різних формах. На базі цих звітів можна дати оцінку роботи локальної мережі, дослідити вразливі ділянки мережі та спроектувати вирішення цих вразливостей. Тому подальші дослідження будуть спрямовані на вибір найбільш універсальної та продуктивної системи моніторингу, її інтеграція локальну мережу з метою проведення постійного моніторингу, щоб в подальшому виявити проблеми з ефективністю роботи системи та виправити їх.

Література

1. Юрій Рамський, Василь Олексюк, Анатолій Балик, 2016. Адміністрування комп'ютерних мереж та систем. Навчальний посібник – Київ: «Богдан», 2016. – 236 с.

УДК 004.7
І. Кардаш; Ю. Лещишин, к.т.н.; А. Варавін, к.ф.-м.н.
(Тернопільський національний технічний університет імені Івана Пулюя)

КРИТЕРІЇ ЕФЕКТИВНОСТІ РОБОТИ ДЛЯ ЗАДАЧІ МОНІТОРИНГУ ЛОКАЛЬНОЇ МЕРЕЖІ

I. Kardash; Yu. Leshchyshyn, Ph.D.; A. Varavin, Ph.D.

WORK EFFICIENCY CRITERIA FOR THE LOCAL NETWORK MONITORING TASK

Важливою частиною роботи локальної мережі, є її моніторинг, для своєчосного виявлення проблем з роботою. Втім системи моніторингу також мають свої критерії ефективності, від яких залежить точність результатів моніторингу. Моніторинг мережі буде проводитись з використанням системи моніторингу локальної мережі Zabbix.

Ефективний моніторинг локальної мережі є ключовим аспектом забезпечення стабільності та продуктивності інфраструктури. Ось кілька критеріїв ефективності моніторингу локальної мережі: Доступність – моніторинг повинен бути постійно доступним для відстеження змін у стані мережі та реагування на проблеми у реальному часі. Продуктивність – моніторинг повинен мати низьку вплив на продуктивність мережі. Забезпечення швидкодії та ефективності алгоритмів збору та аналізу даних є важливим. Масштабованість – моніторинг повинен бути здатний масштабуватися для відстеження росту кількості пристроїв та об'єму трафіку в мережі. Надійність – система моніторингу повинна бути надійною і стійкою до відмов, щоб забезпечити постійний доступ до даних про стан мережі. Сповіщення і тривоги – забезпечення можливості налаштування тривіальних та ефективних механізмів сповіщення про проблеми в мережі. Аналіз трафіку – здатність аналізувати трафік для виявлення аномалій, виявлення причин проблем та планування потрібних ресурсів. Логування та звітність – можливість реєстрації і зберігання історії подій, а також генерації звітів для подальшого аналізу та планування. Безпека – забезпечення безпеки даних моніторингу, у тому числі шифрування та контроль доступу.

Також важливим критерієм ефективності моніторингу локальної мережі є протоколи які підтримуються системою моніторингу. Існує кілька протоколів, які мають великий вплив на продуктивність локальної мережі (LAN). Для моніторингу локальної мережі (LAN) використовуються різні протоколи і інструменти. Ось декілька загальновживаних протоколів та інструментів для моніторингу локальної мережі: SNMP (Simple Network Management Protocol) – використовується для моніторингу та управління мережевими пристроями. Дозволяє отримувати інформацію про стан пристроїв, їх роботу та навантаження; NetFlow – використовується для моніторингу трафіку в мережі. Надає детальну інформацію про потоки даних, що проходять через мережеві пристрої; Wireshark (Ethernet Protocol Analyzer) – дозволяє аналізувати та перехоплювати пакети даних в мережі. Надає можливість вивчення структури та вмісту мережевих пакетів.

Кожен з наведених вище критеріїв ефективності впливає на моніторингові дослідження локальної мережі, тому подальші дослідження будуть спрямовані на дослідження цих критеріїв ефективності, на основі даних отриманих з системи моніторингу мережі Zabbix.

Література

1. Юрій Рамський, Василь Олексюк, Анатолій Балик, 2016. Адміністрування комп’ютерних мереж та систем. Навчальний посібник – Київ: «Богдан», 2016. – 236 с.