

Міністерство освіти і науки України
Державний університет «Житомирська політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки

ПОЯСНЮВАЛЬНА ЗАПИСКА

до випускної кваліфікаційної роботи бакалавра
на тему: «Проект підсистеми моніторингу мережі на
базі технології Zabbix»

Виконав: студент 4-го курсу групи КБ-21-2
спеціальності 125 «Кібербезпека»

 Дмитро НЕРОДЕНКО

Керівник: Старший Викладач кафедри КІ та КБ,

 Олександра ПОКОТИЛО

Рецензент: Доцент кафедри КІ та КБ, к.пед.н., доцент

 Олена ГОЛОВНЯ

Житомир – 2025

Державний університет «Житомирська політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки
Спеціальність 125 «Кібербезпека»
Освітня програма «Кібербезпека»

ЗАТВЕРДЖУЮ

Завідувач

кафедри комп'ютерної
інженерії та кібербезпеки

 Андрій Єфіменко

3 березня 2025 р.

ЗАВДАННЯ

на випускню кваліфікаційну роботу бакалавра

Студент: Нероденко Дмитр Олександрович

Тема роботи: «Проект підсистеми моніторингу мережі на базі технології Zabbix»

затверджена Наказом університету від 3 березня 2025 р. №80/с

Термін здачі студентом закінченої роботи 26 червня 2025 р.

Вихідні дані роботи (зазначається предмет і об'єкт дослідження):
вихідні дані для роботи:

Предметом дослідження є методи, засоби та технології моніторингу мережі, зокрема використання технології Zabbix для моніторингу стану мережевих пристроїв, аналізу трафіку та виявлення проблем з безпекою.

Об'єктом дослідження є процес моніторингу мережевої інфраструктури в локальних мережах, що включає збір і аналіз даних про стан мережевих пристроїв і трафіку.

Обладнання та програмне забезпечення:

1. Програмний емулятор GNS3 2.2.53
2. Гіпервізор Oracle Virtual Box 7.1.2
3. ОС Windows 10 Education та ОС Linux Ubuntu
4. Zabbix та Zabbix Agent
5. Мережевий маршрутизатор C7200
6. Комутатор i86bi_linux_l2-advipservicesk9-ms.high_iron_20170202.

Консультанти з випускної кваліфікаційної роботи із зазначенням розділів, що їх стосуються

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
1	/ Фальковський І.Г	31.03.2025	31.03.2025
2	/ Фальковський І.Г	18.04.2025	18.04.2025
3	/ Фальковський І.Г	21.05.2025	21.05.2025

Студент  Дмитро НЕРОДЕНКО

Керівник  Олександра ПОКОТИЛО

Календарний план

№ з/п	Назви етапів випускної кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Постановка завдання	31.03.2025	
2	Аналіз платформ моніторингу	08.04.2025	
3	Дослідження та аналіз платформи Zabbix	20.04.2025	
5	Побудова локальної мережі	07.05.2025	
6	Встановлення Zabbix Server	09.05.2025	
7	Встановлення Zabbix Agent на робочі станції	15.05.2025	
8	Підключення Zabbix Server до локальної	16.05.2025	
9	Підключення робочих станцій з Zabbix аген-	21.05.2025	
10	Доопрацювання роботи	01.06.2025	
11	Написання пояснювальної записки	20.06.2025	
12	Отримання відгуку та рецензії	21.06.2025	
13	Захист	26.06.2025	

Студент  Дмитро НЕРОДЕНКО

Керівник  Олександра ПОКОТИЛО

АНОТАЦІЯ

Кваліфікаційна робота на тему «Проект підсистеми моніторингу мережі на базі технології Zabbix» включає вступ, три розділи, висновки, список використаних джерел та додатки.

Текстова частина займає 75 сторінки друкованого тексту.

До пояснювальної записки входить список з 20 використаних джерел, що займають 2 сторінки. У роботі представлено 78 рисунка, загальний обсяг 86 сторінок.

У роботі визначено основні завдання для розробки підсистеми моніторингу мережевої активності. Проаналізовано існуючі аналоги та рішення для моніторингу мережевої активності, таких як ManageEngine OpManager, Nagios Core, Zabbix, Paessler PRTG Network Monitor, SolarWinds Network Performance Monitor. Окремо розглянуто функціональні відмінності цих систем, їх можливості щодо налаштування та інтеграції в корпоративну інфраструктуру.

Далі в роботі детально розглянуто використання технологій VLAN, RSTP, SNMPv2, TRUNK для забезпечення стабільності та ефективності моніторингу. Зазначено важливість налаштування цих технологій для зменшення навантаження на окремі сегменти мережі.

У практичній частині описано налаштування Zabbix для моніторингу мережі в реальному часі, включаючи встановлення та налаштування Zabbix Server і Agent, налаштування SNMPv2, а також налаштування сповіщень для оперативного інформування адміністраторів про інциденти у мережі.

Ключові слова: МОНІТОРИНГ, ZABBIX SERVER, ZABBIX, ZABBIX AGENT, GNS3, TELEGRAM, ЛОКАЛЬНА МЕРЕЖА.

					ККІК.КР.Б – 125 – 12 – ПЗ			
Змн.	Арк.	№ докум.	Підпис	Дата	Проект підсистеми моніторингу мережі на базі технології Zabbix	Літ.	Арк.	Аркуші
Розроб.		Нероденко Д.О.		25.06.20				
Керівник		Покотило О.А.		25.06.20			4	88
Реценз.		Головня О.С.		25.06.20				
Н. контр.		Покотило О.А.		25.06.20				
Затверд.		Сфіменко А.А.		25.06.20		ФІКТ, Гр. КБ-21-2		

ANNOTATION

The qualification work on the topic "Design of a Network Monitoring Subsystem Based on Zabbix Technology" includes an introduction, three chapters, conclusions, a list of references, and appendices.

The text part consists of 75 pages of printed text.

The explanatory note includes a list of 16 references, occupying 2 pages. The work includes 78 illustrations, with a total of 94 pages.

The work defines the main tasks for developing a network activity monitoring subsystem. Existing analogues and solutions for network activity monitoring, such as ManageEngine OpManager, Nagios Core, Zabbix, Paessler PRTG Network Monitor, and SolarWinds Network Performance Monitor, have been analyzed. The functional differences of these systems, their capabilities for configuration and integration into corporate infrastructure, are discussed separately.

Further, the work provides a detailed review of the use of VLAN, RSTP, SNMPv2, and TRUNK technologies to ensure the stability and efficiency of monitoring. The importance of configuring these technologies to reduce the load on specific network segments is highlighted.

In the practical part, the setup of Zabbix for real-time network monitoring is described, including the installation and configuration of Zabbix Server and Agent, SNMPv2 configuration, and notification setup for promptly informing administrators about network incidents.

Keywords: MONITORING, ZABBIX SERVER, ZABBIX, ZABBIX AGENT, GNS3, TELEGRAM, LOCAL AREA NETWORK.

		Нероденко Д.О			ККІКБ.КР.Б – 125 – 10 – ПЗ	Арк.
		Покотило О.А				5
Змн.	Арк.	№ докум.	Підпис	Дата		

ЗМІСТ

ВСТУП.....	8
РОЗДІЛ 1. ТЕОРЕТИЧНІ ОСНОВИ МОНІТОРИНГУ ТРАФІКУ В	
КОМП'ЮТЕРНИХ МЕРЕЖАХ.....	10
1.1 Основи функціонування моніторингу мережі.....	10
1.2 Огляд інструментів мережевого моніторингу.....	16
1.3 Детальний огляд інструменту мережевого моніторингу Zabbix.....	24
Висновок до першого розділу.....	28
РОЗДІЛ 2. ПРОЄКТУВАННЯ ТА ПОБУДОВА ЛОКАЛЬНОЇ МЕРЕЖІ.....	29
2.1 Проєктування локальної мережі.....	29
2.2 Розробка схеми адресації мережі.....	35
2.3 Конфігурування IP-адресації в топології проєкту.....	37
Висновок до другого розділу.....	43
РОЗДІЛ 3. ПРАКТИЧНЕ ЗАСТОСУВАННЯ ТЕХНОЛОГІЙ МОНІТОРИНГУ	
МЕРЕЖІ В КОМП'ЮТЕРНИХ МЕРЕЖАХ.....	44
3.1 Встановлення та налаштування системи Zabbix для моніторингу.....	44
3.2 Встановлення та налаштування системи Zabbix Agent на робочі станції.....	50
3.3 Приклади та аналіз результатів моніторингу.....	56
Висновок до третього розділу.....	72
ВИСНОВКИ.....	73
СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ.....	74
ДОДАТКИ.....	76

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

LAN — Local Area Network — локальна мережа

WAN — Wide Area Network — глобальна мережа

SPAN — Switched Port Analyzer — аналізатор портів комутатора

RSPAN — Remote Switched Port Analyzer — віддалений аналізатор портів комутатора

VLAN — Virtual Local Area Network — віртуальна локальна мережа

CLI — Command-Line Interface — інтерфейс командного рядка

VM — Virtual Machine — віртуальна машина

GNS3 — Graphical Network Simulator 3 — графічний мережевий симулятор

VMware — Віртуалізаційне програмне забезпечення для створення віртуальних машин

IOS — Internetwork Operating System — операційна система мережевих пристроїв Cisco

MAC-адреса — Media Access Control address — фізична адреса мережевого інтерфейсу

IP-адреса — Internet Protocol address — мережева адреса пристрою

Wireshark — Інструмент для аналізу мережевого трафіку

NIC — Network Interface Card — мережева карта

PC — Personal Computer — персональний комп'ютер

NAT (Network Address Translation) – Переклад мережевих адрес.

IP (Internet Protocol) – Протокол Інтернету.

MAC (Media Access Control) – Контроль доступу до середовища передачі.

SNMP (Simple Network Management Protocol) – Простий протокол управління мережею.

VB - VirtualBox - Віртуалізаційне програмне забезпечення для створення віртуальних

		Нероденко Д.О			ККІКБ.КР.Б – 125 – 10 – ПЗ	Арк.
		Покотило О.А				7
Змн.	Арк.	№ докум.	Підпис	Дата		

ВСТУП

Актуальність теми. У сучасних мережах моніторинг є ключовим для своєчасного виявлення збоїв, загроз і перевантажень. Zabbix — потужний інструмент, що дозволяє ефективно збирати і аналізувати дані без впливу на роботу мережі. Його застосування забезпечує підвищення безпеки і стабільності мережевої інфраструктури, а також дозволяє швидко реагувати на потенційні проблеми, що може запобігти серйозним збоєм в роботі організації. Тема є особливо актуальною в умовах розвитку нових технологій, де вимоги до безпеки та ефективності роботи мереж зростають. Впровадження автоматизованих систем моніторингу, таких як Zabbix, стає необхідністю для забезпечення стабільного функціонування складних інформаційних систем. Тема актуальна, бо поєднує теоретичні знання з практичним впровадженням систем моніторингу, що дозволяє створити надійну основу для розвитку IT-інфраструктури підприємств.

Метою кваліфікаційної роботи є розробка підсистеми моніторингу мережі на базі технології Zabbix, що дозволить забезпечити ефективний збір, аналіз і візуалізацію даних про стан мережевої інфраструктури для своєчасного виявлення збоїв та загроз. Крім того, система має на меті забезпечити ефективне сповіщення адміністраторів про виникнення інцидентів через доступні можливості Zabbix, такі як налаштування тригерів, сповіщення через Telegram, email або інші канали зв'язку. Це дозволяє оперативно реагувати на проблеми, зменшуючи час простою і підвищуючи загальну надійність та безпеку мережі.

Завданням кваліфікаційної роботи є:

- Постановка завдання
- Аналіз платформ моніторингу
- Аналіз технологій моніторингу мережі Zabbix
- Розробка віртуальної мережевої топології
- Встановлення Zabbix Server, Agent
- Налаштування моніторингу в GNS3
- Тестування та аналіз результатів

		Нероденко Д.О			ККІКБ.КР.Б – 125 – 10 – ПЗ	Арк.
		Покотило О.А				8
Змн.	Арк.	№ докум.	Підпис	Дата		

Об'єктом дослідження є процес моніторингу мережевої інфраструктури в локальних мережах, що включає збір і аналіз даних про стан мережевих пристроїв і трафіку. Цей процес важливий для забезпечення стабільності, безпеки та ефективності роботи мережі, а також для своєчасного виявлення збоїв і загроз. Моніторинг допомагає покращити управління мережевими ресурсами та знизити ризики у сучасних інформаційних системах.

Методи дослідження:

- аналіз технічної документації;
- моделювання мережевої інфраструктури;
- конфігурування мережевих пристроїв Cisco в GNS3;
- практичне тестування моніторингу мережі за допомогою Zabbix;

Предметом дослідження є методи, засоби та технології моніторингу мережі, зокрема використання технології Zabbix для моніторингу стану мережевих пристроїв, аналізу трафіку та виявлення проблем з безпекою.

Під час виконання кваліфікаційної роботи було розроблено локальну мережу з можливістю моніторингу мережі за допомогою Zabbix, який дозволяє централізовано здійснювати моніторинг стану мережі та ефективно управляти її ресурсами для забезпечення надійності та безперебійності інфраструктури організації.

		Нероденко Д.О			ККІКБ.КР.Б – 125 – 10 – ПЗ	Арк.
		Покотило О.А				
Змн.	Арк.	№ докум.	Підпис	Дата		9

РОЗДІЛ 1. ТЕОРЕТИЧНІ ОСНОВИ МОНІТОРИНГУ ТРАФІКУ В КОМП'ЮТЕРНИХ МЕРЕЖАХ

1.1 Основи функціонування моніторингу мережі

У сучасних інформаційно-комунікаційних системах стабільність та ефективність роботи мережі є критично важливими для забезпечення безперервного доступу до сервісів, додатків і ресурсів. Зі зростанням обсягів переданих даних, кількості підключених пристроїв та складності мережевої інфраструктури, потреба у постійному нагляді за її станом стає дедалі актуальнішою.

Моніторинг мережі — це практика постійного спостереження за комп'ютерною мережею з метою виявлення збоїв або недоліків для забезпечення стабільної роботи мережі. Технічно моніторинг мережі можна розглядати як підрозділ управління мережею, проте на практиці ці поняття часто вважаються рівнозначними[8].

Процес моніторингу мережі передбачає використання спеціалізованих систем для виявлення поширених проблем у мережі, збоїв у роботі мережевого обладнання та перевантаження ресурсів — незалежно від того, чи розміщені ці ресурси локально, у дата-центрі чи в хмарному середовищі. До типових мережевих пристроїв належать маршрутизатори, комутатори, веб-сервери та міжмережеві екрани.

Моніторинг мережі збирає та надає звіти про різноманітні дані з комп'ютерної мережі, включаючи маршрутизатори, комутатори, міжмережеві екрани, балансувальники навантаження та навіть кінцеві пристрої, такі як сервери та робочі станції. Зібрані дані фільтруються та аналізуються для виявлення різноманітних мережевих проблем і визначення їхніх першопричин. До таких проблем можуть належати відмови пристроїв, обриви з'єднань, помилки інтерфейсів, втрата пакетів, час відгуку додатків і зміни в конфігурації.

Якісне рішення для моніторингу мережі дозволяє:

Оцінювати стандартну продуктивність. Моніторинг надає можливість відстежувати типову продуктивність мережі. Це також дозволяє легко виявляти будь-які відхилення в роботі, що своєю чергою допомагає швидко знаходити небажані зміни.

		Нероденко Д.О			ККІКБ.КР.Б – 125 – 10 – ПЗ	Арк.
		Покотило О.А				
Змн.	Арк.	№ докум.	Підпис	Дата		10

Ефективно розподіляти ресурси. Командам ІТ потрібне чітке розуміння джерел проблем. Вони також повинні мати змогу зменшити рутинне усунення несправностей і впроваджувати проактивні заходи для запобігання збоям. Якщо провести аналогію з водопроводом, моніторинг дозволяє «усунути тріщини до того, як стається витік».

Виявляти загрози безпеці. Запобігання порушенням безпеки є серйозним викликом для будь-якої організації. Оскільки атаки стають дедалі складнішими й важчими для відстеження, надзвичайно важливо вчасно виявляти й нейтралізовувати загрози. Моніторинг мережі спрощує захист даних і систем, забезпечуючи раннє виявлення підозрілої активності.

Керувати змінним ІТ-середовищем. Нові технології — такі як сенсори з доступом до інтернету, бездротові пристрої та хмарні сервіси — ускладнюють завдання відстеження продуктивності чи виявлення аномалій.

Рішення з моніторингу мережі може:

- Надати повний перелік дротових і бездротових пристроїв;
- Полегшити аналіз довготривалих трендів;
- Допомогти максимально ефективно використовувати наявні ресурси;
- Проактивно виявляти та вирішувати проблеми ще до того, як вони вплинуть на користувачів;

Тісний моніторинг мережі дозволяє організації швидко вирішувати проблеми та запобігати серйозним перебоям, що означає менше збоїв в роботі та краще використання ІТ-ресурсів. Успішно впроваджувати нові технології та оновлення систем. Завдяки моніторингу ІТ-фахівці можуть аналізувати, як обладнання працювало з часом, та використовувати трендовий аналіз для оцінки, чи здатна поточна технологія масштабуватись під потреби бізнесу. Це дозволяє:

- Отримати чітке уявлення про здатність мережі підтримувати запуск нових технологій;
- Зменшити ризики, пов'язані з масштабними змінами;
- Легко демонструвати ефективність інвестицій, використовуючи докладні метрики;

		Нероденко Д.О			ККІКБ.КР.Б – 125 – 10 – ПЗ	Арк.
		Покотило О.А				
Змн.	Арк.	№ докум.	Підпис	Дата		11

Типи показників продуктивності мережевого моніторингу. Показники продуктивності мережі надають цінну інформацію, яка допомагає адміністраторам виявляти проблеми в мережі та оптимізувати її роботу.

Основні показники продуктивності мережевого моніторингу включають:

Затримка (Latency). Затримка — це час, за який пакет даних проходить шлях від джерела до пункту призначення. Висока затримка може негативно впливати на якість користувацького досвіду, особливо в застосунках, які потребують мінімальних затримок, як-от VoIP чи онлайн-ігри.

Втрата пакетів (Packet loss). Цей показник відображає відсоток пакетів, що були втрачені під час передавання. Високий рівень втрат пакетів призводить до зниження продуктивності мережі та часто є ознакою проблем із обладнанням або перевантаженням мережі.

Джитер (Jitter). Джитер означає змінність у часі доставки пакетів даних у мережі. Високий джитер може заважати роботі застосунків із реального часу, таких як потокове відео чи голосовий зв'язок через Інтернет, що призводить до поганої якості або переривань.

Пропускна здатність (Throughput). У контексті моніторингу мережі пропускна здатність — це обсяг даних, який може бути успішно переданий через мережеве з'єднання за певний період часу.

Дублювання пакетів (Packet duplication). Дублювання пакетів виникає, коли однакові пакети передаються по мережі кілька разів, у результаті чого одержувач отримує ті самі дані більше одного разу.

Час затримки (Round Trip Time, RTT). RTT вимірює час, необхідний для передачі сигналу від відправника до одержувача та назад. Це важливий показник для оцінки чутливості та швидкості реакції мережі.

Переупорядкування пакетів (Packet reordering). Переупорядкування пакетів відбувається, коли пакети прибувають у місце призначення не в тому порядку, в якому були відправлені. Це може бути спричинено багатошляховою маршрутизацією або коливаннями маршруту, коли маршрутизатор швидко перемикається між різними маршрутами до однієї цілі, що призводить до нестабільності мережі.

		Нероденко Д.О			ККІКБ.КР.Б – 125 – 10 – ПЗ	Арк.
		Покотило О.А				
Змн.	Арк.	№ докум.	Підпис	Дата		12

Частота помилок (Error rate). Цей показник відстежує частоту виникнення помилок під час передачі даних. Високий рівень помилок може вказувати на проблеми з апаратним забезпеченням мережі або перешкоди, що впливають на цілісність переданої інформації.

Існують різні типи моніторингу залежно від того, що саме потрібно контролювати. Найпоширенішими серед них є моніторинг відмов, журналів, продуктивності мережі, конфігурації та доступності.

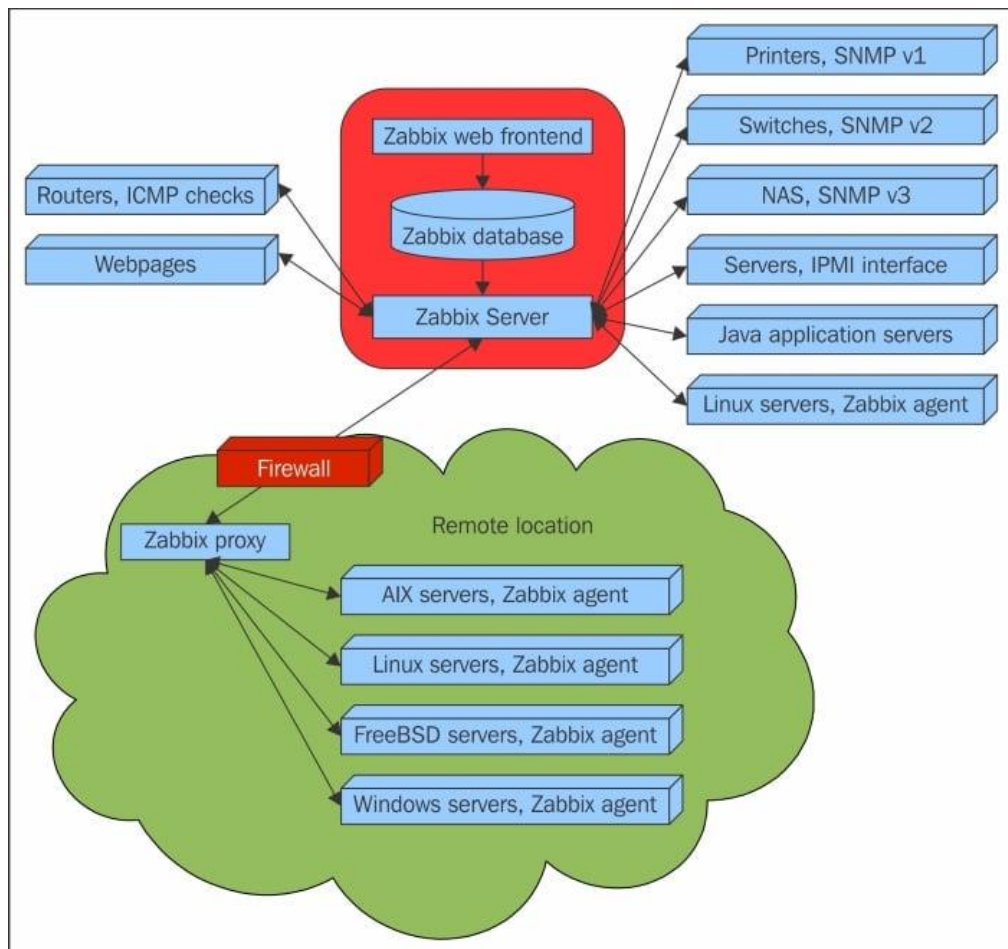


Рисунок 1.1 – Схематичний показ роботи моніторингу з використанням інструменту Zabbix

Моніторинг відмов (Fault monitoring). Як видно з назви, моніторинг відмов передбачає виявлення та повідомлення про збої в комп'ютерній мережі. Він є критично важливим для підтримання безперервної роботи мережі та забезпечення стабільного функціонування всіх програм і сервісів.

Моніторинг журналів (Log monitoring). Ресурси, такі як сервери, застосунки та вебсайти, постійно генерують журнали, які можуть:

		Нероденко Д.О			ККІКБ.КР.Б – 125 – 10 – ПЗ	Арк.
		Покотило О.А				13
Змн.	Арк.	№ докум.	Підпис	Дата		

- Надавати цінну інформацію про активність користувачів;
- Допомогати бізнесу відповідати нормативним вимогам;
- Сприяти оперативному реагуванню на інциденти;
- Підвищувати рівень безпеки мережі;

Моніторинг продуктивності мережі (Network Performance Monitoring, NPM). NPM відстежує такі параметри, як затримка, мережевий трафік, використання пропускну здатності та пропускна спроможність, з метою оптимізації користувацького досвіду. Інструменти NPM надають корисну інформацію для мінімізації простоїв і ефективного усунення мережевих проблем.

Моніторинг конфігурації (Configuration monitoring). Моніторинг конфігурації мережі включає відстеження програмного забезпечення та мікропрограм, які використовуються в мережі, а також виявлення та усунення будь-яких невідповідностей. Це дозволяє уникнути прогалин у видимості та безпеці.

Моніторинг доступності (Network Availability Monitoring). Моніторинг доступності передбачає контроль усієї IT-інфраструктури для визначення часу безперебійної роботи пристроїв. Завдяки постійному спостереженню за станом пристроїв і серверів організації можуть отримувати сповіщення про збої в мережі або недоступність пристроїв. Найбільш поширені методи такого моніторингу — це ICMP, SNMP та Syslog.

SNMP (Simple Network Management Protocol) — це широко вживаний протокол для керування мережею. Він дозволяє пристроям у мережі спілкуватися з центральною системою керування, надаючи важливі дані про стан та здоров'я мережі. Два основні механізми в SNMP — це опитування (polling) та трапи (traps), кожен із яких виконує свою унікальну функцію в моніторингу та керуванні мережею.

SNMP опитування передбачає періодичне запитування мережевою системою керування (NMS) пристроїв у мережі для збору інформації про їхній стан. Система керування надсилає запит агентам SNMP на керованих пристроях, які у відповідь повертають запитані дані. Цей метод дозволяє постійно моніторити та збирати детальну інформацію з часом, що дає змогу NMS підтримувати актуальний стан мережі. Опитування є проактивним, забезпечуючи наявність найновіших даних у

		Нероденко Д.О.			ККІКБ.КР.Б – 125 – 10 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		14

системі керування, але воно також може створювати значне навантаження на мережу, особливо у великих або складних мережах.

SNMP трапи, навпаки, є подієво-орієнтованими повідомленнями, які агент SNMP надсилає системі керування (NMS) без попереднього запиту. Коли відбувається певна подія — наприклад, збій пристрою або перевищення встановленого порогу — агент надсилає трап-повідомлення до NMS, миттєво сповіщаючи про проблему. Трапи є асинхронними, тобто виникають лише при настанні конкретних умов, що знижує навантаження на мережу та забезпечує оповіщення в режимі реального часу. Проте трапи можуть бути менш надійними, ніж опитування, оскільки вони залежать від ініціації зв'язку самим пристроєм, і якщо трап-повідомлення загубиться, система керування може пропустити важливі сповіщення.

Це наводить нас на думку щодо розгляду потенційних загроз безпеки, пов'язаних із використанням систем мережевого моніторингу. Незважаючи на їхню ефективність у забезпеченні контролю за інфраструктурою, вони можуть створювати нові вектори уразливостей, які необхідно враховувати під час проєктування та експлуатації.

До основних загроз належать:

- втрата повідомлень SNMP Traps — оскільки SNMP Traps є асинхронним механізмом передачі даних, існує ризик втрати критично важливих повідомлень у разі короткочасних збоїв у мережі. Це може призвести до того, що система не отримає сигнал про збої обладнання або порушення безпеки

- надмірне навантаження при SNMP Polling — постійне опитування пристроїв для збору телеметрії здатне створити значне навантаження на мережу, особливо у великих інфраструктурах. Це збільшує ризик деградації продуктивності та створює вразливість до DoS-атак

- недостатній контроль змін конфігурації — за відсутності ефективного моніторингу змін у конфігураціях мережевих пристроїв, сторонні зміни можуть залишитися непоміченими, що створює можливість виникнення порушень у роботі або навіть проникнення в систему

		Нероденко Д.О			ККІКБ.КР.Б – 125 – 10 – ПЗ	Арк.
		Покотило О.А				
Змн.	Арк.	№ докум.	Підпис	Дата		15

- недосконалий лог-моніторинг — невчасне або неповне опрацювання системних журналів знижує ймовірність своєчасного виявлення інцидентів інформаційної безпеки.

– низька ефективність візуалізації — обмежені можливості візуального представлення даних (наприклад, графіків, карт аномалій, індикаторів стану) ускладнюють швидку оцінку ситуації та виявлення загроз.

Отже, системи мережевого моніторингу, хоча й підвищують контроль над інфраструктурою, самі потребують ретельного захисту, оскільки можуть стати джерелом нових уразливостей. Врахування вищезгаданих загроз є критично важливим для забезпечення надійності та безпеки всієї мережі.

1.2 Огляд інструментів мережевого моніторингу

Платформи моніторингу мережі є важливими технологічними інструментами, які систематично спостерігають, оцінюють і документують стан роботи, показники продуктивності та рівень безпеки цифрової інфраструктури організації. Ці складні рішення для моніторингу надають ІТ-відділам миттєвий доступ до важливої інформації про поведінку мережі — від шаблонів потоку трафіку та вузьких місць у передачі даних до стану роботи пристроїв і спроб експлуатації потенційних вразливостей.

SolarWinds Network Performance Monitor (NPM) є одним із лідерів у галузі завдяки комплексному підходу до забезпечення видимості мережі та потужним засобам діагностики. Це рішення корпоративного рівня забезпечує моніторинг мережевого обладнання від різних виробників і пропонує інтуїтивно зрозумілі інструменти візуалізації для швидкого виявлення та усунення несправностей.

		Нероденко Д.О			ККІКБ.КР.Б – 125 – 10 – ПЗ	Арк.
		Покотило О.А				
Змн.	Арк.	№ докум.	Підпис	Дата		16

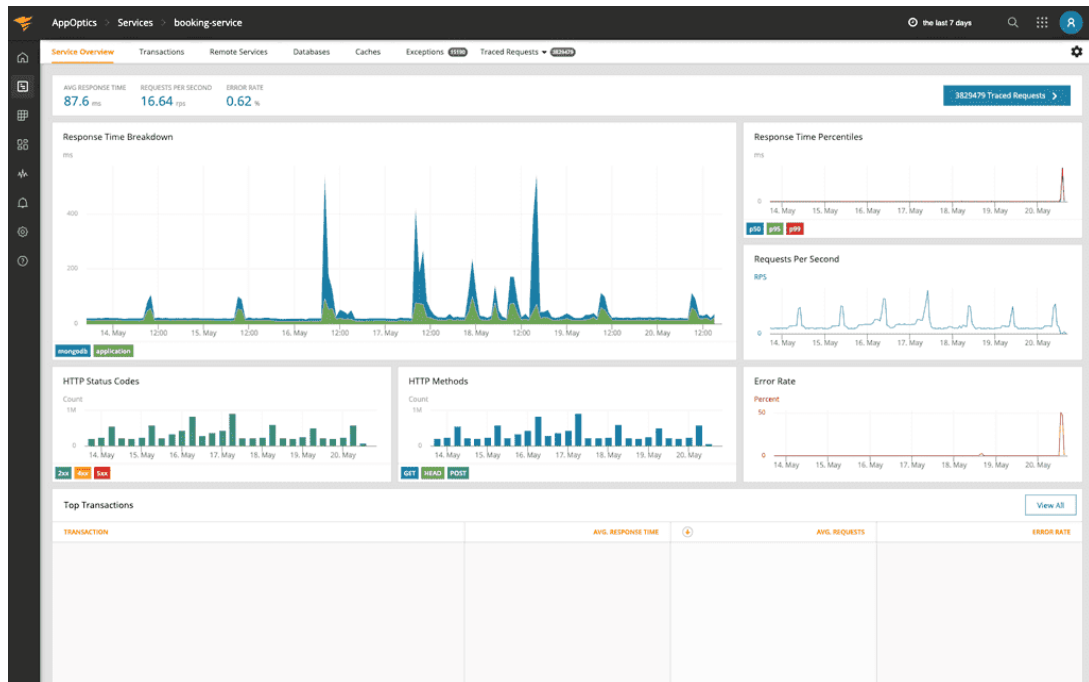


Рисунок 1.2 – Інтерфейс інструменту SolarWinds Network Performance Monitor

Ключові функції:

- Технології NetPath і PerfStack для покращеного усунення несправностей;
- Розширена візуалізація мережі з побудовою топологічних карт;
- Інтелектуальні сповіщення з можливістю налаштування порогових значень;
- Широка підтримка пристроїв від різних виробників;
- Автоматичне виявлення та картографування мережі;
- Моніторинг та аналіз бездротових мереж;

Унікальна особливість:

Технологія NetPath забезпечує покроковий аналіз у гібридних середовищах, візуалізуючи весь маршрут мережевого трафіку для критично важливих додатків і сервісів.

Переваги:

- Виняткова глибина моніторингу;
- Інтуїтивно зрозумілий та гнучкий інтерфейс;
- Відмінна масштабованість для корпоративних мереж;
- Потужна підтримка обладнання незалежно від виробника;

Недоліки:

		Нероденко Д.О			ККІКБ.КР.Б – 125 – 10 – ПЗ	Арк.
		Покотило О.А				
Змн.	Арк.	№ докум.	Підпис	Дата		17

- Вища вартість у порівнянні з багатьма конкурентами;
- Може вимагати значних ресурсів при розгортанні у великих мережах;
- Відносно складний для нових адміністраторів (потребує часу на навчання);

Paessler PRTG Network Monitor. PRTG пропонує уніфікований підхід до моніторингу, який охоплює не лише мережі, але й сервери, додатки та інші компоненти ІТ-інфраструктури. Його модель ліцензування на основі сенсорів забезпечує гнучкість для організацій будь-якого масштабу. Він здійснює моніторинг доступності мережі та використання пропускну здатності, а також різноманітних інших параметрів мережі, таких як якість обслуговування, завантаження пам'яті та процесора — навіть на віддалених машинах.

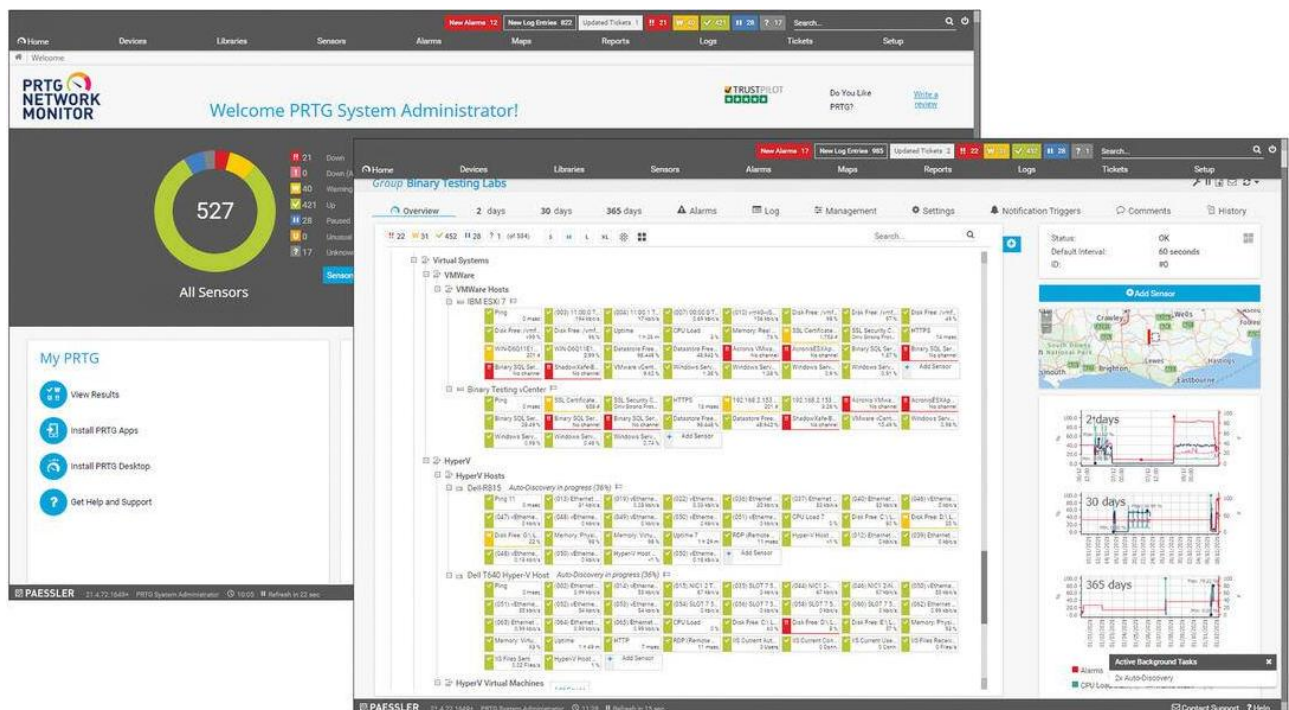


Рисунок 1.3 – Інтерфейс інструменту Paessler PRTG Network Monitor

Ключові функції:

- Понад 250 попередньо налаштованих типів сенсорів;
- Автоматичне виявлення мережевих пристроїв;
- Гнучкі варіанти сповіщень і повідомлень;
- Налаштовувані дашборди та звітність;
- Можливість розгортання локально або в хмарі;
- Мобільні додатки для iOS та Android;

		Нероденко Д.О			Арк.
		Покотило О.А			18
Змн.	Арк.	№ докум.	Підпис	Дата	

Унікальна особливість:

Ліцензування PRTG за принципом «сенсорів» забезпечує виняткову гнучкість, дозволяючи організаціям точно розподіляти ресурси моніторингу саме там, де це найбільше потрібно.

Переваги:

- Прозора модель ліцензування на основі сенсорів;
- Всеохоплюючий моніторинг не лише мереж, а й серверів, додатків тощо;
- Зручний інтерфейс із мінімальними вимогами до налаштування;
- Відмінні мобільні застосунки;

Недоліки:

- Вартість може зрости при збільшенні кількості сенсорів;
- Обмежена можливість кастомізації у порівнянні з деякими корпоративними рішеннями;
- Звітність менш потужна, ніж у спеціалізованих інструментів;

Nagios Core. Як один із піонерів у сфері моніторингу з відкритим кодом, Nagios Core і надалі пропонує потужну платформу для моніторингу мережі з неперевершеною гнучкістю та можливостями налаштування[4].

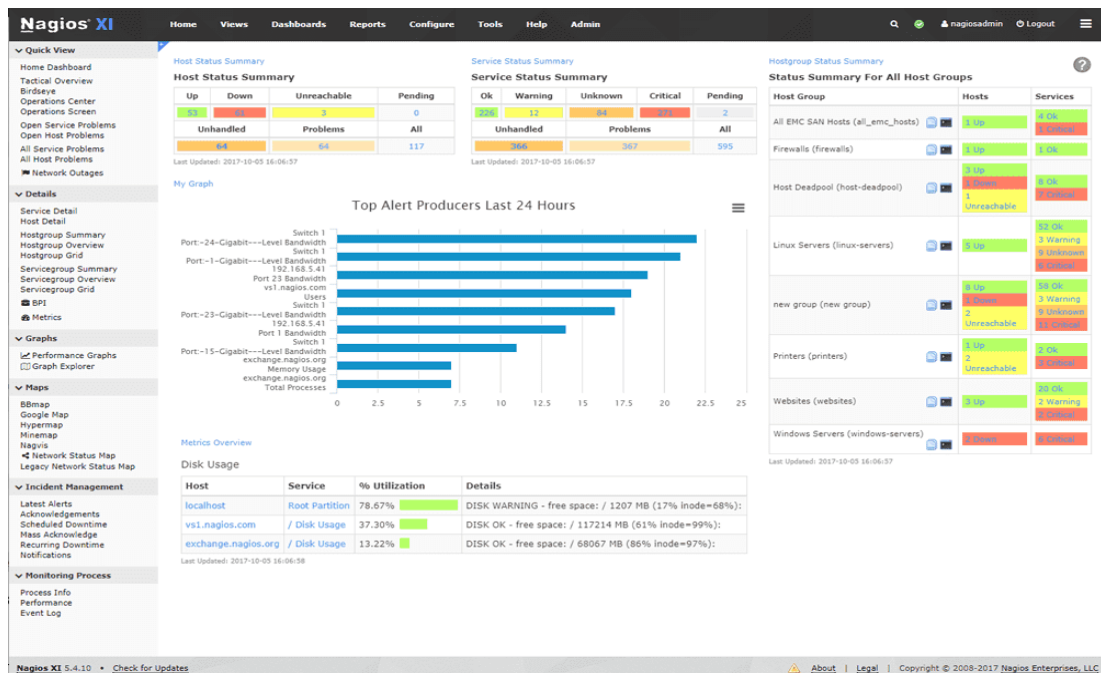


Рисунок 1.4 – Інтерфейс інструменту Nagios Core

Ключові функції:

		Нероденко Д.О			ККІКБ.КР.Б – 125 – 10 – ПЗ	Арк.
		Покотило О.А				19
Змн.	Арк.	№ докум.	Підпис	Дата		

- Розгалужена екосистема плагінів;
- Потужна система сповіщень і повідомлень;
- Обробники подій для автоматизованого усунення несправностей;
- Можливість налаштування під будь-які потреби моніторингу;
- Сильна підтримка спільноти та детальна документація;
- Підтримка мультиорендності (multi-tenant);

Унікальна особливість:

Завдяки екосистемі з понад 5000 плагінів, розроблених спільнотою, Nagios Core дозволяє здійснювати моніторинг практично будь-якого пристрою, сервісу чи показника.

Переваги:

- Повністю безкоштовне open-source рішення;
- Необмежені можливості налаштування;
- Відсутність ліцензійних витрат незалежно від розміру мережі;
- Зріла та стабільна платформа з великою кількістю документації;
- Недоліки:
- Високий поріг входу порівняно з комерційними продуктами;
- Основна конфігурація через текстові файли;
- Менш привабливий і зручний інтерфейс у порівнянні з комерційними аналогами;
- Потребує більшої кількості ручного налаштування й обслуговування

ManageEngine OpManager. OpManager є відомим своєю інтуїтивністю та простотою у використанні, при цьому надаючи розширені можливості моніторингу мережі. Він забезпечує комплексний моніторинг як фізичних, так і віртуальних мереж, а його функції автоматичного виявлення та налаштування значно економлять час ІТ-команд. OpManager ідеально підходить для бізнесу, який шукає зручний у використанні інструмент із потужною автоматизацією та аналітикою. Він чудово підходить для великих, динамічних мереж, особливо якщо потрібно керувати комбінацією фізичних, віртуальних та хмарних середовищ.

		Нероденко Д.О			ККІКБ.КР.Б – 125 – 10 – ПЗ	Арк.
		Покотило О.А				
Змн.	Арк.	№ докум.	Підпис	Дата		20

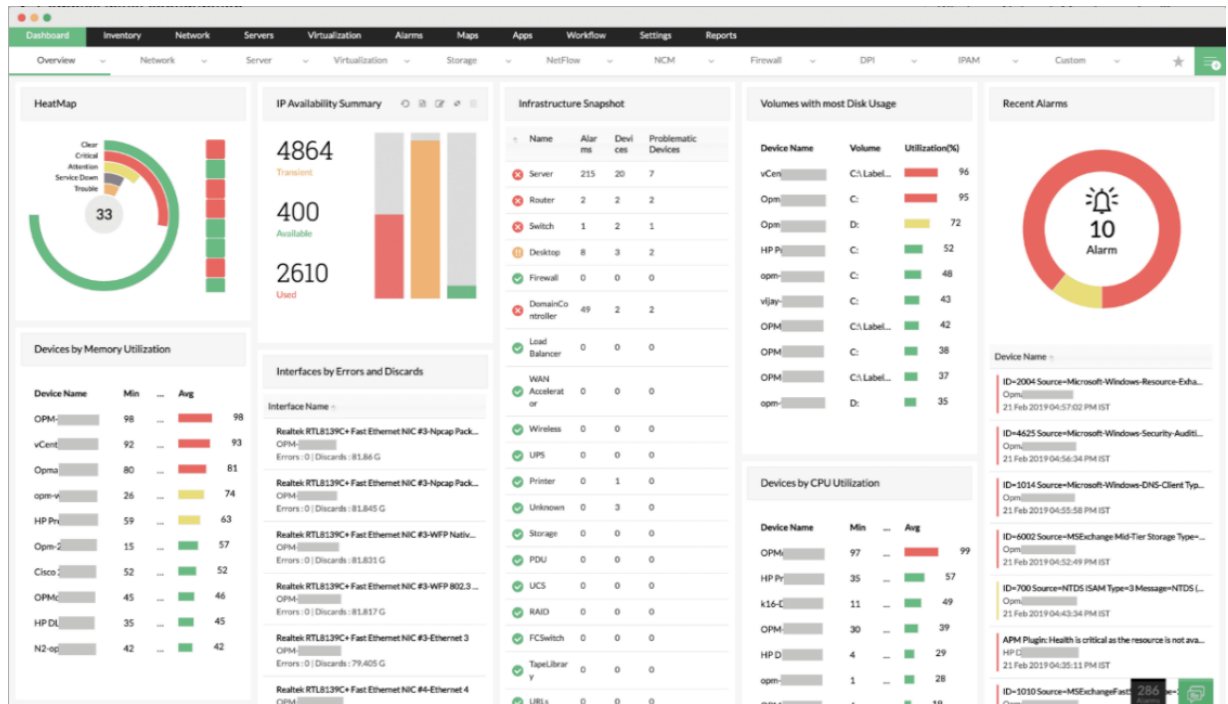


Рисунок 1.5 – Інтерфейс інструменту ManageEngine OpManager

Ключові особливості:

- Моніторинг мережі в режимі реального часу та сповіщення;
- Вбудоване управління конфігураціями;
- Аналіз мережевого трафіку та моніторинг пропускної здатності;
- Автоматичне виявлення пристроїв та побудова карти мережі;
- Інтегроване управління IP-адресами;
- Автоматизація робочих процесів для типових завдань;

Унікальна особливість: інтегровані можливості управління конфігураціями мережі в OpManager дозволяють ІТ-командам керувати, робити резервні копії та відслідковувати зміни в конфігураціях мережевих пристроїв через той самий інтерфейс, який використовується для моніторингу продуктивності.

Переваги:

- Швидке розгортання з мінімальними налаштуваннями;
- Інтуїтивний інтерфейс, що не потребує глибоких технічних знань;
- Відмінне співвідношення ціни та набору функцій;
- Сильна інтеграція з іншими продуктами ManageEngine;

Недоліки:

		Нероденко Д.О			ККІКБ.КР.Б – 125 – 10 – ПЗ	Арк.
		Покотило О.А				
Змн.	Арк.	№ докум.	Підпис	Дата		21

- Менша глибина в розширених функціях моніторингу;
- Обмеженіша кастомізація у порівнянні з корпоративними рішеннями;
- Менш гнучка система звітності у порівнянні зі спеціалізованими інструментами;
- Деякі розширені функції залежать від плагінів;

Zabbix пропонує можливості моніторингу корпоративного рівня у вигляді відкритого програмного забезпечення, забезпечуючи складні функції моніторингу, візуалізації та автоматизації без витрат на ліцензії. *Zabbix* дозволяє здійснювати моніторинг серверів (Linux, Windows, BSD), мережевого обладнання (Cisco, Juniper, MikroTik тощо), віртуальних машин (VMware, Hyper-V), баз даних (MySQL, PostgreSQL), веб-додатків та інше.

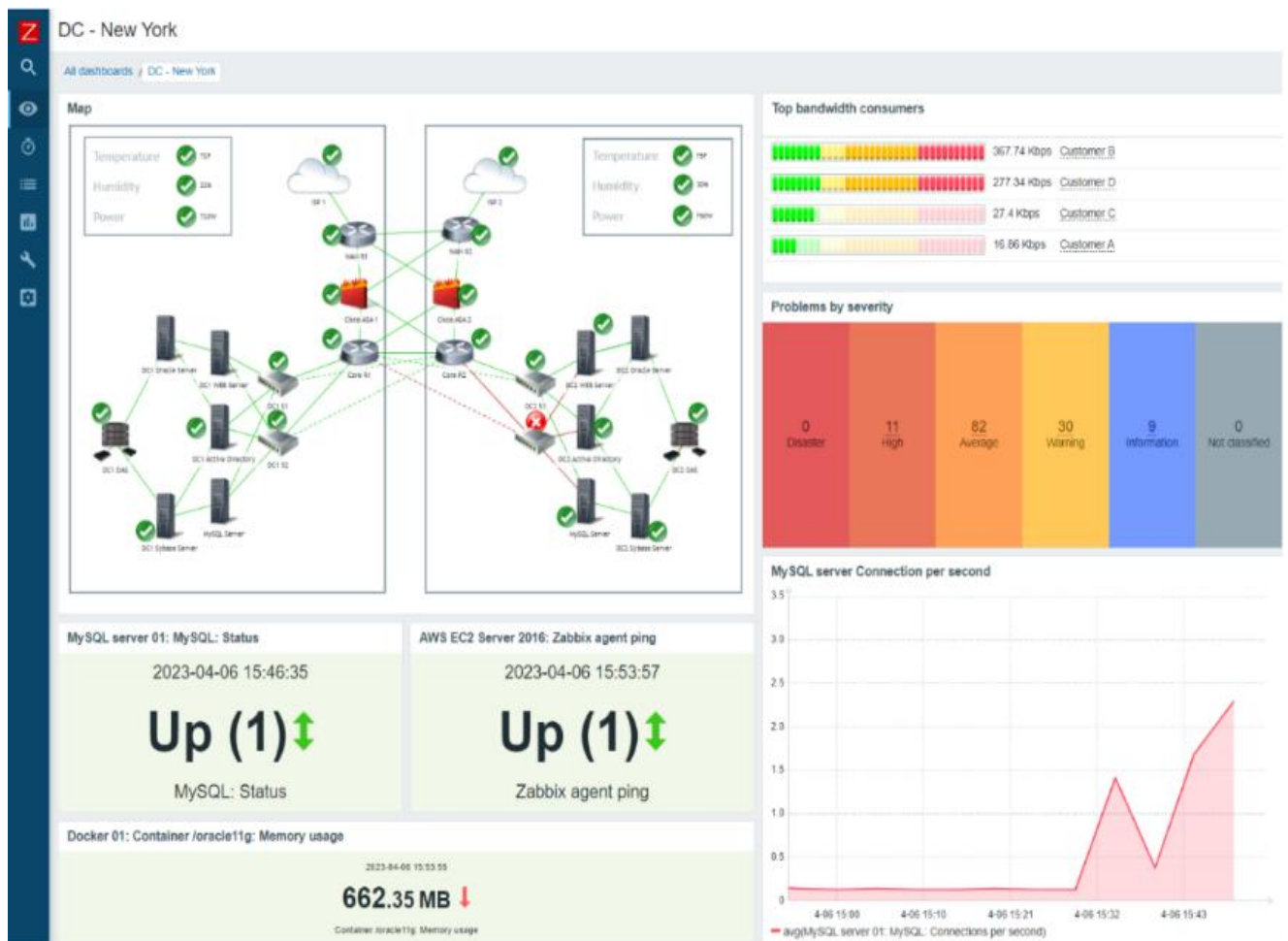


Рисунок 1.6 – Інтерфейс інструменту Zabbix

Ключові особливості:

- Моніторинг з використанням агентів і без агентів;

		Нероденко Д.О			ККІКБ.КР.Б – 125 – 10 – ПЗ	Арк.
		Покотило О.А				22
Змн.	Арк.	№ докум.	Підпис	Дата		

- Автоматичне виявлення мережевих пристроїв;
- Розподілена архітектура моніторингу;
- Налаштовувані дашборди та звіти;
- Потужні можливості кореляції подій;
- Конфігурація на основі шаблонів;

Унікальна особливість: потужний механізм кореляції подій Zabbix може аналізувати кілька сповіщень для визначення першопричин, що суттєво знижує кількість хибних тривог і прискорює вирішення проблем.

Переваги:

- Безкоштовне рішення корпоративного рівня;
- Відмінна масштабованість для великих мереж;
- Сильна інтеграція з базами даних та висока продуктивність;
- Широка бібліотека шаблонів;

Недоліки:

- Складна початкова конфігурація;
- Вища кривизна навчання порівняно з комерційними рішеннями;
- Веб-інтерфейс менш інтуїтивний у порівнянні з новішими інструментами;
- Високі вимоги до ресурсів при дуже великих розгортаннях;

Зважаючи на особливості, переваги та недоліки розглянутих інструментів моніторингу мережі, було обрано інструмент Zabbix. Zabbix є безкоштовним рішенням з відкритим кодом, що надає широкі можливості для моніторингу різних елементів мережі, таких як сервери, пристрої, додатки та сервіси. З його допомогою можна здійснювати моніторинг у реальному часі, аналізувати продуктивність і доступність мережевих компонентів, а також автоматично виявляти проблеми і загрози.

Завдяки гнучкості налаштувань, підтримці різних типів моніторингу (агенти, SNMP, IPMI, JMX, VMware та інші), а також можливості налаштування сповіщень та автоматичних дій, Zabbix дозволяє створити ефективну систему моніторингу, яка підходить як для малих, так і для великих інфраструктур.

		Нероденко Д.О			ККІКБ.КР.Б – 125 – 10 – ПЗ	Арк.
		Покотило О.А				
Змн.	Арк.	№ докум.	Підпис	Дата		23

Порівняння інструментів мережевого моніторингу

Інструмент	Тип ліцензування	Унікальні особливості	Переваги	Недоліки	Гнучкість налаштування
SolarWinds NPM	Платне	NetPath: пок-роковий аналіз маршруту трафіку	Глибокий моніторинг, гнучкий інтерфейс, масштабованість	Висока вартість, складність для новачків	Висока: Гнучкі пороги сповіщень, налаштування NetPath, підтримка кастомних карт та сценаріїв
Paessler PRTG	Платне	Ліцензування за кількістю сенсорів	Зручний інтерфейс, мобільні додатки, гнучка ліцензія	Ціна зростає з кількістю сенсорів, обмежена кастомізація	Середня: Просте додавання сенсорів, обмежене редагування інтерфейсу
Nagios Core	Безкоштовне з відкритим кодом	5,000+ плагінів від спільноти	Безкоштовність, гнучкість, велика підтримка	Складність конфігурації, слабкий інтерфейс	Дуже висока: Повна підтримка власних плагінів, гнучкі скрипти, але через текстові конфігурації
ManageEngine OpManager	Платне	Інтегроване управління конфігураціями	Інтуїтивний інтерфейс, автоматизація, хороша ціна-функціонал	Менша гнучкість звітів, залежність від плагінів	Середня: Просте налаштування типових сценаріїв, обмежена кастомізація дашбордів та звітів
Zabbix	Безкоштовне з відкритим кодом	Кореляція подій та потужні шаблони	Безкоштовність, масштабованість, гнучке налаштування	Висока складність налаштування, ресурсомісткість	Висока: Конфігурація тригерів, шаблони моніторингу, макроси, автоматичні дії, API-інтеграції

1.3 Детальний огляд інструменту мережевого моніторингу Zabbix

Zabbix — це програмне забезпечення, яке моніторить численні параметри мережі, а також стан і цілісність серверів, віртуальних машин, додатків, сервісів, баз даних, вебсайтів, хмарних сервісів та іншого. Zabbix використовує гнучкий механізм сповіщень, що дозволяє користувачам налаштовувати email-повідомлення практично про будь-які події. Це забезпечує швидку реакцію на проблеми з серверами. Zabbix пропонує відмінні можливості звітності та візуалізації даних на основі збереженої інформації, що робить його ідеальним для планування потужностей.

Zabbix підтримує як опитування (polling), так і трапи (traps). Всі звіти, статистика та параметри конфігурації Zabbix доступні через веб-інтерфейс. Веб-інтерфейс гарантує, що стан вашої мережі та здоров'я серверів можна оцінювати з будь-якого місця. Правильно налаштований Zabbix може відігравати важливу роль у моніторингу IT-інфраструктури. Це актуально як для невеликих організацій з кількома серверами, так і для великих компаній із багатьма серверами.

Zabbix є безкоштовним. Програма написана і розповсюджується під ліцензією AGPL-3.0, що означає вільний доступ до вихідного коду для широкого загалу.

Збір даних. Перевірка доступності та продуктивності. Підтримка SNMP (як traps, так і polling), IPMI, JMX, моніторинг VMware. Користувацькі перевірки. Збір необхідних даних з налаштуванням інтервалів. Виконується сервером/проксі та агентами.

Гнучке визначення порогів. Можна визначати дуже гнучкі пороги проблем, які називаються тригерами, що посиляються на значення з бази даних.

Детальне налаштування оповіщення. Надсилання сповіщень можна налаштовувати за графіком ескалації, отримувачами, типом каналу. Сповіщення можна робити змістовними та корисними за допомогою макро-змінних. Автоматичні дії включають виконання віддалених команд.

Графіки в режимі реального часу. Моніторингові елементи миттєво відображаються на графіках за допомогою вбудованого функціоналу.

Можливості веб-моніторингу. Zabbix може імітувати кліки мишкою на веб-сайті та перевіряти його функціональність і час відгуку.

		Нероденко Д.О			ККІКБ.КР.Б – 125 – 10 – ПЗ	Арк.
		Покотило О.А				
Змн.	Арк.	№ докум.	Підпис	Дата		25

Широкі можливості візуалізації. Можливість створювати власні графіки, що поєднують кілька елементів у одному вигляді. Мапи мережі. Слайд-шоу в стилі панелі керування. Звіти. Високорівневий (бізнесовий) огляд моніторингових ресурсів.

Зберігання історичних даних. Дані зберігаються в базі даних. Налаштовувана історія. Вбудована процедура очищення (housekeeping).

Легка конфігурація. Додавання пристроїв як хостів. Хости автоматично потрапляють під моніторинг після внесення в базу даних. Застосування шаблонів до моніторингових пристроїв.

Використання шаблонів. Групування перевірок у шаблони. Шаблони можуть успадковувати інші шаблони.

Виявлення мережі. Автоматичне виявлення мережевих пристроїв. Автоматична реєстрація агентів. Виявлення файлових систем, мережевих інтерфейсів та SNMP OID.

Швидкий веб-інтерфейс. Веб-інтерфейс на PHP. Доступний звідусіль. Зручна навігація по інтерфейсу. Журнал аудиту.

API Zabbix. API забезпечує програмний інтерфейс для масових операцій, інтеграції зі стороннім ПО та інших задач.

Система дозволів. Безпечна аутентифікація користувачів. Можливість обмежувати певним користувачам доступ до певних переглядів.

Повнофункціональний та легко розширюваний агент. Встановлюється на об'єктах моніторингу. Підтримка Linux і Windows.

Бінарні демони. Написані на C для високої продуктивності та невеликого споживання пам'яті. Легко переносити.

Готовність до складних середовищ. Віддалений моніторинг полегшується за допомогою Zabbix Proxy

Огляд Zabbix: архітектура. Zabbix складається з кількох основних програмних компонентів. Їхні функції описані нижче.

Сервер. Сервер Zabbix є центральним компонентом, до якого агенти надсилають інформацію про доступність, цілісність та статистику. Сервер виступає як

		Нероденко Д.О			ККІКБ.КР.Б – 125 – 10 – ПЗ	Арк.
		Покотило О.А				
Змн.	Арк.	№ докум.	Підпис	Дата		26

центральне сховище, в якому зберігаються всі конфігурації, статистичні та операційні дані.

Сховище бази даних. Вся інформація про конфігурації, а також дані, зібрані Zabbix, зберігаються в базі даних.

Веб-інтерфейс. Для зручного доступу до Zabbix з будь-якого місця і з будь-якої платформи надається веб-інтерфейс. Він є частиною сервера Zabbix і зазвичай (але не обов'язково) працює на тій самій фізичній машині, що й сервер.

Агент. Агенти Zabbix встановлюються на об'єкти моніторингу для активного контролю локальних ресурсів і додатків та передачі зібраних даних на сервер Zabbix. Починаючи з версії 4.4, доступні два типи агентів:

Zabbix agent — легкий, підтримується на багатьох платформах, написаний на C;

Zabbix agent 2 — більш гнучкий, легко розширюваний за допомогою плагінів, написаний на Go.

Потік даних. Важливо розуміти загальний потік даних у Zabbix. Щоб створити елемент, який збирає дані, спочатку потрібно створити хост. Відповідно, щоб створити тригер, потрібно мати елемент. Тригер необхідний для створення дії. Наприклад, щоб отримати сповіщення про надмірне завантаження CPU на сервері X, потрібно спочатку додати хост для сервера X, потім створити елемент для моніторингу CPU, далі — тригер, який спрацює при високому навантаженні CPU, і, нарешті, дію, яка надсилатиме вам електронного листа. Така архітектура дозволяє створювати дуже гнучкі налаштування.

Zabbix має широкий спектр можливостей для інтеграції з різноманітними системами та сервісами, що дозволяє адаптувати його до специфічних потреб підприємства та забезпечити безперервний моніторинг різних компонентів інфраструктури.

Одним з основних напрямків інтеграції є інтеграція з системами управління інцидентами, такими як Jira та ServiceNow, що дає змогу автоматизувати процеси реєстрації, відслідковування і вирішення інцидентів у компанії. Це дозволяє

		Нероденко Д.О			ККІКБ.КР.Б – 125 – 10 – ПЗ	Арк.
		Покотило О.А				
Змн.	Арк.	№ докум.	Підпис	Дата		27

оперативно реагувати на проблеми та автоматично створювати завдання для відповідальних осіб без необхідності ручного введення[15].

Крім того, Zabbix підтримує інтеграцію з популярними інструментами для сповіщень, такими як Telegram, Slack, Microsoft Teams, що дозволяє оперативно інформувати відповідальних осіб про події в реальному часі через зручні канали зв'язку.

Завдяки підтримці Active Directory, Zabbix дозволяє інтегрувати управління користувачами та доступами до системи з централізованою системою аутентифікації. Це дає можливість зберігати всі облікові дані в одному місці та застосовувати корпоративні політики доступу.

Окрім цього, Zabbix підтримує інтеграцію з віртуалізаційними платформами (наприклад, VMware, Hyper-V) для моніторингу віртуальних машин, SNMP для моніторингу мережевих пристроїв

Це різноманіття інтеграцій робить Zabbix універсальним інструментом для моніторингу всієї інфраструктури підприємства, дозволяючи централізовано отримувати дані з різних джерел і автоматизувати багато процесів управління[17].

Висновок до першого розділу

У першому розділі було досліджено принципи функціонування систем моніторингу мережі та проаналізував найпоширеніші програмні рішення у цій сфері. Особливу увагу я приділив системі Zabbix, оскільки вона найкраще відповідає поставленим у межах цієї роботи завданням: централізованому збору даних про стан обладнання, гнучкому налаштуванню тригерів та автоматизованому інформуванню про критичні події. На основі проведеної аналітики я дійшов висновку, що саме Zabbix забезпечує необхідний рівень масштабованості, інтеграції та точності моніторингу для реалізації обраної інфраструктури. Крім того, я вже мав базовий практичний досвід роботи з цією системою, що також вплинуло на вибір — це дозволило ефективно адаптувати її можливості до вимог проєкту.

		Нероденко Д.О			ККІКБ.КР.Б – 125 – 10 – ПЗ	Арк.
		Покотило О.А				28
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 2. ПРОЄКТУВАННЯ ТА ПОБУДОВА ЛОКАЛЬНОЇ МЕРЕЖІ

2.1 Проектування локальної мережі

Проектування локальної мережі є важливим етапом створення стабільної, надійної та безпечної інфраструктури для організації. Вірно налаштована локальна мережа забезпечує ефективне використання ресурсів, сприяє високому рівню безпеки і дозволяє оперативно реагувати на будь-які неполадки. Створення мережі, здатної справлятися з високим навантаженням, одночасно оптимізуючи трафік і знижуючи ймовірність виникнення збоїв, є критично важливим для сучасних організацій. Основними елементами налаштування є правильний вибір топології мережі, налаштування VLAN, RSTP, TRUNK та NAT, які разом дозволяють досягти оптимальної продуктивності, ефективності та безпеки мережі.

Налаштування VLAN

VLAN — це технологія, що дозволяє логічно розділити одну фізичну мережу на кілька ізольованих підмереж, таким чином забезпечуючи підвищену безпеку і зручність у керуванні трафіком. За допомогою VLAN можна ефективно організувати доступ до мережі, контролюючи, які пристрої можуть взаємодіяти між собою, а які повинні бути ізольовані[9]. Мережа налаштована так, що кожен сегмент має своє призначення, що дозволяє зменшити обсяг трафіку в кожній підмережі та підвищити безпеку:

VLAN 10 — для робочих станцій основних користувачів.

VLAN 20 — для гостьових робочих станцій.

VLAN 30 — для мережі управління робочими станціями.

VLAN 40 — для робочих станцій привілейованих користувачів.

VLAN 99 — для критичних робочих станцій та серверів.

Розділення мережі на VLAN дозволяє обмежити поширення широкомовного трафіку, а також забезпечити логічну ізоляцію різних груп користувачів і пристроїв. Це не лише зменшує навантаження на кожен сегмент, але й робить систему більш захищеною від потенційних атак і витоків інформації.

Налаштування RSTP

		Нероденко Д.О			ККІКБ.КР.Б – 125 – 10 – ПЗ	Арк.
		Покотило О.А				
Змн.	Арк.	№ докум.	Підпис	Дата		29

RSTP є важливим протоколом для забезпечення надійності мережі, особливо в складних топологіях з кількома шляхами. Основною метою RSTP є уникнення петель у мережі та забезпечення швидкого відновлення зв'язку при виникненні збоїв. Якщо один із маршрутів вийде з ладу, RSTP миттєво активує резервний шлях для передачі даних, що забезпечує безперервність роботи мережі та зменшує час відновлення з'єднання. Це надзвичайно важливо для великих і складних мереж, де можливість виникнення збоїв значно вища[20].

Мережа налаштована так, щоб використовувати RSTP для оптимального управління шляхами та забезпечення стійкості до збоїв. Цей протокол також значно знижує час реакції в разі зміни мережевої топології, дозволяючи швидко відновлювати доступність мережі навіть за умов непередбачених ситуацій[18].

Налаштування TRUNK

TRUNK порти дозволяють передавати трафік з кількох VLAN через один фізичний канал. Це важливий елемент у мережах, де потрібно мінімізувати кількість фізичних з'єднань і зберегти ефективне використання інтерфейсів. Технологія TRUNK дозволяє з'єднувати комутатори і маршрутизатори таким чином, що кожен з них може передавати кілька типів трафіку через один порт. У вашій мережі TRUNK порти налаштовані для з'єднання між комутаторами та маршрутизаторами, що дозволяє передавати трафік від усіх VLAN через один інтерфейс, зменшуючи кількість необхідних фізичних підключень[19].

Це значно спрощує управління мережею, знижує витрати на обладнання і дозволяє організувати зручну і гнучку маршрутизацію трафіку між різними сегментами мережі.

Налаштування NAT

NAT — це технологія, яка дозволяє транслювати внутрішні приватні IP-адреси в публічні, що необхідно для виходу в Інтернет. Мережа використовує NAT для того, щоб всі пристрої всередині мережі могли отримати доступ до Інтернету через одну публічну IP-адресу, при цьому зберігаючи внутрішні адреси приватними і прихованими від зовнішнього світу. Це не лише дозволяє економити

		Нероденко Д.О			ККІКБ.КР.Б – 125 – 10 – ПЗ	Арк.
		Покотило О.А				
Змн.	Арк.	№ докум.	Підпис	Дата		30

публічні IP-адреси, а й захищає мережу від зовнішніх загроз, оскільки внутрішні пристрої не розкривають свої реальні IP-адреси[20].

Крім того, NAT дозволяє керувати доступом до Інтернету, застосовуючи різні стратегії доступу для окремих VLAN або сегментів мережі. Це також забезпечує більшу гнучкість у керуванні ресурсами мережі та спрощує адміністрування.

Мережі проектуються за різними топологіями, кожна з яких має свої особливості і підходить для певних сценаріїв. Основні топології мереж включають:

Шина (Bus) – у цій топології всі вузли підключені до єдиного кабелю, через який передаються дані. Лише вузол з відповідною MAC-адресою приймає інформацію. Це проста топологія, проте має обмеження щодо відстані, масштабованості та функціональності, що робить її менш підходящою для великих або високонавантажених мереж. Вона найкраще підходить для малих мереж або тимчасових з'єднань.

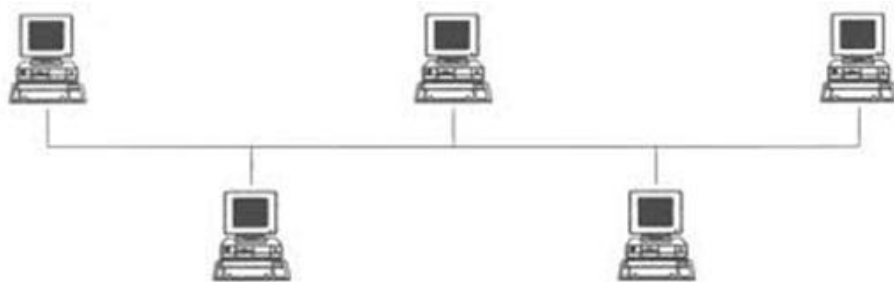


Рисунок 2.1 – Топологія мережі Шина

Кільце (Ring) – в цій топології всі вузли з'єднані в замкнуте кільце, і сигнал передається в одному напрямку через кожен вузол. Вихід з ладу одного вузла може призвести до повного збої мережі, якщо не використовуються резервні шляхи.

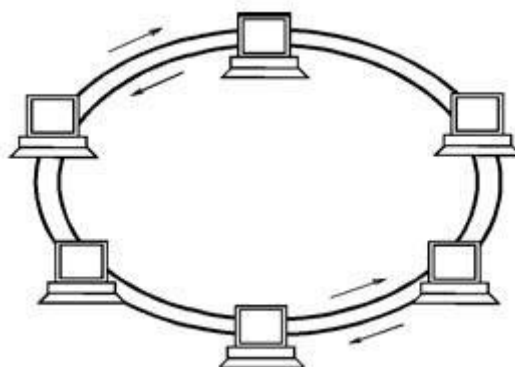


Рисунок 2.2 – Топологія мережі Кільце

Зірка (Star) – всі вузли підключені до центрального вузла через окремі канали зв'язку. У разі виходу з ладу центрального вузла, вся мережа перестає працювати. Це одна з найпоширеніших топологій для корпоративних мереж завдяки її простоті в налаштуванні та масштабуванні.

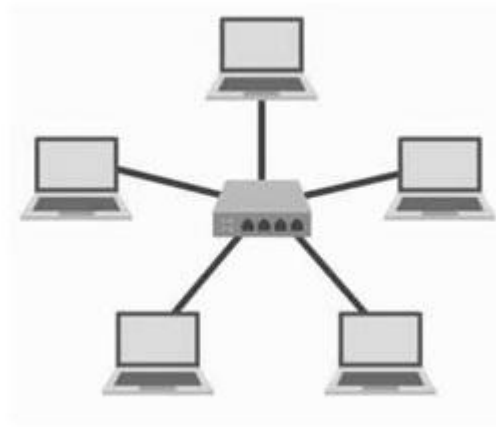


Рисунок 2.3 – Топологія мережі Зірка

На базі цих топологій формуються більш складні похідні топології такі як:

Сітка (Mesh) – кожен вузол підключений до кількох інших вузлів. Це забезпечує високу надійність і безпеку, оскільки є резервні шляхи для передачі трафіку. Однак така топологія має свої недоліки: складність налаштування та обслуговування, а також високі витрати на реалізацію.

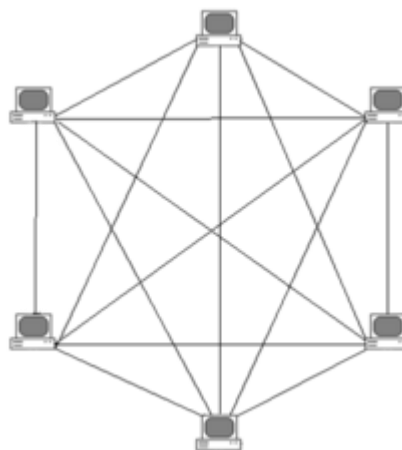


Рисунок 2.4 – Топологія мережі Сітка

Дерево (Tree) – це варіант зіркової топології з ієрархічною структурою, де основний центральний вузол з'єднаний з підлеглими вузлами. Така структура дозволяє масштабувати мережу, однак збій центрального вузла може призвести до

		Нероденко Д.О			ККІКБ.КР.Б – 125 – 10 – ПЗ	Арк.
		Покотило О.А				
Змн.	Арк.	№ докум.	Підпис	Дата		32

виведення мережі з ладу. Вартість кабелів і обслуговування також може бути високою.

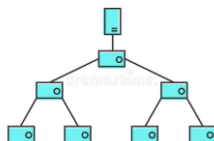


Рисунок 2.5 – Топологія мережі Дерево

Гібридна (Hybrid) – ця топологія поєднує різні типи топологій, що дозволяє створювати гнучку мережу, яку можна масштабувати в залежності від потреб. Основні недоліки – складність проектування та висока вартість установки та налаштування.

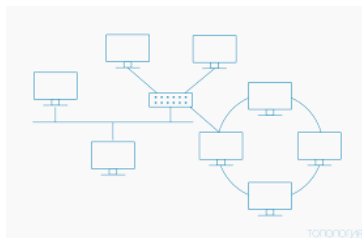
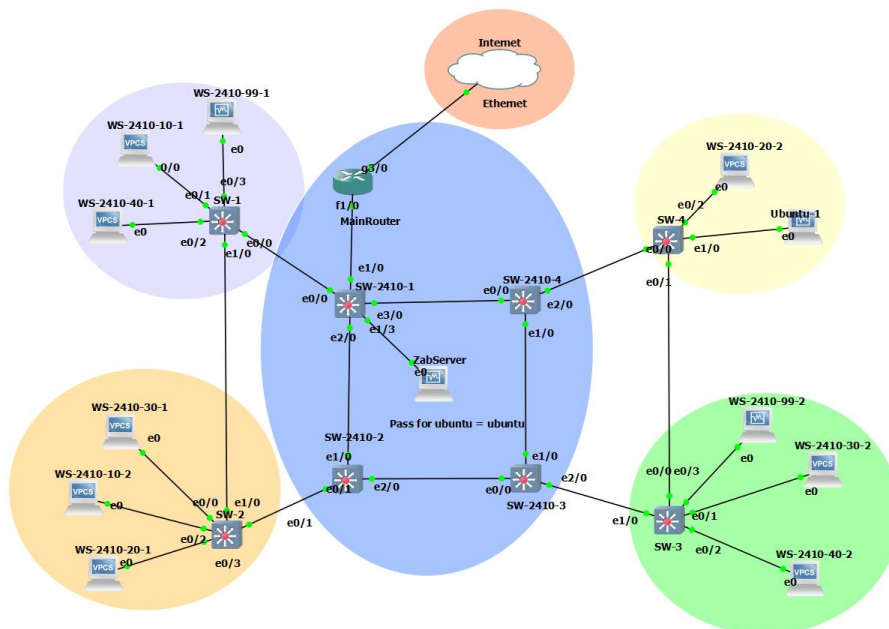


Рисунок 2.6 – Гібридна топологія мережі

Для організації корпоративної мережі було обрано гібридну топологію:



Основним суттєвим покращенням мережевої структури могло б стати впровадження ще одного маршрутизатора AddRouter2, який буде підключений до двох незалежних провайдерів (Internet1 та Internet2) теж саме з MainRouter. Така схема забезпечить повну резервованість як на рівні пристроїв, так і на рівні зовнішніх з'єднань. Тобто MainRouter матиме з'єднання з обома провайдерами (Internet1 та Internet2), і аналогічне підключення матиме MainRouter2. Це дозволить налаштувати механізми балансування навантаження або автоматичного перемикавання трафіку у разі збою одного з каналів зв'язку, що значно підвищить відмовостійкість мережі та її доступність для користувачів.

Перенесення Zabbix-сервера в ізольований сегмент локальної мережі тобто окремий VLAN із застосуванням правил міжмережевого екранування є доцільним покращенням з погляду безпеки. Такий підхід дозволяє забезпечити односторонній зв'язок — сервер має доступ до моніторингових агентів і SNMP-пристроїв, але сам залишається недоступним з інших сегментів мережі, що зменшує ризики зовнішніх атак.

Водночас, варто врахувати, що повна ізоляція Zabbix-сервера без належної маршрутизації та винятків у фаєрволі може унеможливити отримання даних з агентів або SNMP-пристроїв, якщо вони не мають зворотного зв'язку. Тому при впровадженні такої архітектури потрібно налаштувати правила, що дозволяють Zabbix-серверу ініціювати вихідні з'єднання до вузлів моніторингу, але блокують вхідні з'єднання до самого сервера. Це не порушить його основної функціональності, якщо використовується активний режим опитування, а не пасивний.

Для організації корпоративної мережі було обрано гібридну топологію, яка поєднує кращі характеристики різних топологій, та трирівневу модель мережі, яка включає:

Рівень доступу: Це кіцева частина мереж яка забезпечує підключення кінцевих пристроїв до мережі, таких як комп'ютери та сервери.

Рівень розподілення: цей рівень забезпечує з'єднання між різними сегментами мережі, гарантуючи маршрутизацію між VLAN і сегментами.

		Нероденко Д.О			ККІКБ.КР.Б – 125 – 10 – ПЗ	Арк.
		Покотило О.А				
Змн.	Арк.	№ докум.	Підпис	Дата		34

Рівень ядра: є центральною частиною мережі яка виконує функцію магістралі тобто, через яку здійснюється маршрутизація між основними підмережами та з'єднання з зовнішнім світом (наприклад, Інтернетом).

Гібридну топологію було обрано заради кращої роботи мережі а саме за основу було взято сіткоподібну схему мережі та схему мережі у вигляді лісу, з них було взято як хороші сторони так і погані а саме:

З лісоподібної схеми було взято ієрхаїчну систему побудови кінцевих пристроїв а також те що мережа підв'язується до одного маршрутизатора що є великою проблемою.

Сіткоподібна схема забезпечує високу надійність і безпеку, оскільки є резервні шляхи для передачі трафіку але її головною проблемою є складність в налаштуванні та вартість побудови мережі.

Мережа загалом складається з 1 головного маршрутизатора L3, та 4 комутаторів які розподіляють трафік по гілкам мережі а також дають бесперебійну роботу в разі виведення зі строю якогось із центральних комуматорів, також в мережі є ще 4 комутатора що дають змогу обмінюватися інформацією кінцевим пристроям.

2.2 Розробка схеми адресації мережі

Підмережа — це частина більшої мережі, розділена на менші логічні сегменти, що дозволяє оптимізувати структуру мережі і підвищити ефективність її роботи.

Однією з основних цілей створення підмереж є зменшення широкомовного трафіку, що дозволяє уникнути надмірного поширення пакетів через непотрібні маршрути. Також розподіл на підмережі допомагає керувати використанням IP-адрес, що важливо для великих мереж, де може виникнути проблема з адресним простором. Більш детально, це дає можливість значно зменшити кількість непотрібних запитів між різними частинами мережі, оскільки дані обробляються тільки в межах відповідної підмережі, що підвищує швидкість передачі і знижує навантаження на загальну мережу.

		Нероденко Д.О			ККІКБ.КР.Б – 125 – 10 – ПЗ	Арк.
		Покотило О.А				
Змн.	Арк.	№ докум.	Підпис	Дата		35

Розподіл IP-адрес між підмережами виконується таким чином, щоб забезпечити кожен пристрій необхідною адресою, при цьому залишаючи резерв для майбутнього підключення нових пристроїв. Це дозволяє гнучко масштабувати мережу і не переживати щодо нестачі IP-адрес у разі збільшення числа пристроїв або розширення інфраструктури. Додатково, застосування VLAN у межах підмереж дає можливість створювати логічні групи користувачів чи пристроїв, що забезпечує більшу безпеку, оскільки дозволяє обмежити доступ між групами пристроїв, зменшуючи ймовірність несанкціонованого доступу або розповсюдження шкідливого трафіку.

Іншим аспектом є управління трафіком: кожен сегмент мережі має свою власну IP-адресу, що значно спрощує маршрутизацію даних. Це дозволяє знизити навантаження на маршрутизатори та інші мережеві пристрої, оскільки кожен пакет передається лише в межах відповідної підмережі, поки не досягне свого призначення. Використання підмереж також дозволяє легко реалізувати політики безпеки та управляти доступом до різних ресурсів, що є критичним для захисту даних в межах організації.

До того ж, завдяки правильному налаштуванню підмереж можна забезпечити зручність адміністрування мережі. Наприклад, за допомогою VLAN можна створювати різні рівні доступу для користувачів, організувати сегментацію для серверів та робочих станцій, а також для віддалених користувачів, які підключаються через VPN або інші засоби доступу. Це дозволяє мінімізувати кількість мережевих проблем, оптимізувати використання ресурсів і зберігати високий рівень безпеки в кожному з сегментів мережі.

Таким чином, поділ мережі на підмережі дозволяє значно покращити ефективність її роботи, підвищити безпеку та знизити навантаження на мережеві компоненти, забезпечуючи кращу організацію передачі даних, простоту адміністрування та масштабованість в майбутньому.

		Нероденко Д.О			ККІКБ.КР.Б – 125 – 10 – ПЗ	Арк.
		Покотило О.А				
Змн.	Арк.	№ докум.	Підпис	Дата		36

Адресація підмереж на рівні ядра, розподілу та доступу

З'єднання	Інтерфейс	IP-адреса
MainRouter to SW-2410-1	F1/0.10	192.24.10.1
	F1/0.10	192.24.20.1
	F1/0.10	192.24.30.1
	F1/0.10	192.24.40.1
	F1/0.10	192.24.99.1
MainRouter to SW-2410-4	F1/1	Переймає
MainRouter to Internet	G3/0	DHCP
VLAN 10	TRUNK	192.24.10.0
VLAN 20	TRUNK	192.24.20.0
VLAN 30	TRUNK	192.24.30.0
VLAN 40	TRUNK	192.24.40.0
VLAN(RSPAN)	TRUNK	192.24.99.0
WS-2410-10-(1-2)	E0/0	192.24.10.101-102
WS-2410-20-(1-2)	E0/0	192.24.20.101-102
WS-2410-30-(1-2)	E0/0	192.24.30.101-102
WS-2410-40-(1-2)	E0/0	192.24.40.101-102
Zabbix	E0/0	192.24.10.100
WS-2410-99-(1-3)	E0/0	192.24.20.100-102

2.3 Конфігурування IP-адресації в топології проекту

Особливо важливою складовою проектування локальної мережі є правильне налаштування IP-адресації, що забезпечує коректний обмін даними між усіма мережевими пристроями. У межах даної мережі визначну роль виконує маршрутизатор MainRouter, який виступає центральним вузлом маршрутизації між сегментами мережі, об'єднаними в окремі VLAN.

		Нероденко Д.О.			ККІКБ.КР.Б – 125 – 10 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		37

MainRouter відповідає за маршрутизацію між підмережами, трансляцію адрес (NAT) для забезпечення виходу в Інтернет, а також за з'єднання логічно розділених сегментів мережі через TRUNK-з'єднання з комутаторами[11]. На кожному інтерфейсі маршрутизатора була призначена окрема IP-адреса відповідно до конкретного VLAN, що дозволяє здійснювати маршрутизацію на третьому рівні моделі OSI. Це дозволяє ефективно керувати трафіком, забезпечуючи ізоляцію підмереж і одночасно підтримуючи їхню взаємодію через маршрутизатор.

Крім того, на маршрутизаторі було налаштовано протокол SNMPv2 у режимі "public", що дало змогу інтегрувати пристрій до системи моніторингу Zabbix. Це налаштування дозволяє зчитувати з маршрутизатора технічні параметри в реальному часі, такі як завантаженість інтерфейсів, обсяг переданих даних і поточний стан зв'язку, що суттєво підвищує ефективність адміністрування та швидкість реагування на можливі збої.

Таким чином, IP-адресація в проєктованій мережі була реалізована за принципом поділу на логічні підмережі з чітким маршрутом доступу, що проходить через MainRouter, що значно підвищує керованість, масштабованість та безпеку мережевої інфраструктури.

Комутатори другого рівня такі як SW-2410-(1–4) та SW-(1–4) забезпечують ефективну комутацію трафіку в межах VLAN і передачу даних між кінцевими пристроями. Для взаємодії між VLAN і маршрутизатором MainRouter були налаштовані trunk-порти, що дозволяє передавати трафік кількох VLAN через одне з'єднання. Для забезпечення відмовостійкості активовано протокол RSTP, який швидко реагує на зміни в топології, а функція portfast edge пришвидшує активацію портів для кінцевих пристроїв[12]. Така конфігурація підвищує стабільність і надійність усієї мережі.

		Нероденко Д.О			ККІКБ.КР.Б – 125 – 10 – ПЗ	Арк.
		Покотило О.А				
Змн.	Арк.	№ докум.	Підпис	Дата		38

```

MainRouter1(config)#int g3/0
MainRouter1(config-if)#ip add dhcp
MainRouter1(config-if)#ip nat outside
MainRouter1(config-if)#ip nat inside source list 1 int g3/0 ove
MainRouter1(config-if)#ip nat inside source list 1 int g3/0 overload

MainRouter1(config)#access-list 1 permit any
MainRouter1(config)#int f1/0.10
MainRouter1(config-subif)#en
MainRouter1(config-subif)#encapsulation do
MainRouter1(config-subif)#encapsulation dot1Q 10
MainRouter1(config-subif)#ip add 192.24.10.1 255.255.255.0
MainRouter1(config-subif)#no sh
MainRouter1(config-subif)#int f1/0.20
MainRouter1(config-subif)#encapsulation dot1Q 20
MainRouter1(config-subif)#ip add 192.24.20.1 255.255.255.0
MainRouter1(config-subif)#no sh
MainRouter1(config-subif)#int f1/0.30
MainRouter1(config-subif)#encapsulation dot1Q 30
MainRouter1(config-subif)#ip add 192.24.30.1 255.255.255.0
MainRouter1(config-subif)#no sh
MainRouter1(config-subif)#int f1/0.40
MainRouter1(config-subif)#ip add 192.24.40.1 255.255.255.0
MainRouter1(config-subif)#encapsulation dot1Q 40
MainRouter1(config-subif)#no sh
MainRouter1(config-subif)#int f1/0.99
MainRouter1(config-subif)#encapsulation dot1Q 99
MainRouter1(config-subif)#ip add 192.24.99.1 255.255.255.0
MainRouter1(config-subif)#ex
MainRouter1(config)#ip domain-lookup
MainRouter1(config)#ip name-server 8.8.8.8
MainRouter1(config)#int f1/1
MainRouter1(config-if)#no sh
MainRouter1(config-if)#ex
MainRouter1(config)#snmp-server community pub
MainRouter1(config)#snmp-server community public RO
MainRouter1(config)#ex
MainRouter1#
*Jun 20 14:13:04.351: %SYS-5-CONFIG_I: Configured from console by console
MainRouter1#

```

Рисунок 2.8 – Приклад IP-адресації, Nat, DHCP, SNMPv2 на маршрутизаторі MainRouter

```

SW-2410-1(config-vlan)#en
SW-2410-1(config-vlan)#vlan 10
SW-2410-1(config-vlan)#name Users
SW-2410-1(config-vlan)#vlan 20
SW-2410-1(config-vlan)#name Guests
SW-2410-1(config-vlan)#vlan 30
SW-2410-1(config-vlan)#name Managment
SW-2410-1(config-vlan)#vlan 40
SW-2410-1(config-vlan)#name Admins
SW-2410-1(config-vlan)#Vlan 99
SW-2410-1(config-vlan)#name Zabbix
SW-2410-1(config-vlan)#int e0/0
SW-2410-1(config-if)#switchport trunk encapsulation dot1q
SW-2410-1(config-if)#switchport mode trunk
SW-2410-1(config-if)#switchport trunk allowed vlan 10,20,30,40,99
SW-2410-1(config-if)#int e1/0
SW-2410-1(config-if)#switchport trunk encapsulation dot1q
SW-2410-1(config-if)#switchport mode trunk
SW-2410-1(config-if)#switchport trunk allowed vlan 10,20,30,40,99
SW-2410-1(config-if)#int e2/0
SW-2410-1(config-if)#switchport trunk encapsulation dot1q
SW-2410-1(config-if)#switchport mode trunk
SW-2410-1(config-if)#switchport trunk allowed vlan 10,20,30,40,99
SW-2410-1(config-if)#int e3/0
SW-2410-1(config-if)#switchport trunk encapsulation dot1q
SW-2410-1(config-if)#switchport mode trunk
SW-2410-1(config-if)#switchport trunk allowed vlan 10,20,30,40,99
SW-2410-1(config-if)#spanning-tree mode rapid-pvst
SW-2410-1(config)#

```

Рисунок 2.9 – Приклад налаштування комутатора L2(Trunk,RSPAN,VLAN)

		Нероденко Д.О			ККІКБ.КР.Б – 125 – 10 – ПЗ	Арк.
		Покотило О.А				
Змн.	Арк.	№ докум.	Підпис	Дата		39

```

changed state to up
SW-2410-1(config)#interface Ethernet1/3
SW-2410-1(config-if)# switchport access vlan 10
SW-2410-1(config-if)# switchport mode access
SW-2410-1(config-if)# spanning-tree portfast edge
%Warning: portfast should only be enabled on ports connected to a single
host. Connecting hubs, concentrators, switches, bridges, etc... to this
interface when portfast is enabled, can cause temporary bridging loops.
Use with CAUTION

```

Рисунок 2.10 – Приклад налаштування доступу для Zabbix Server

```

PC1 - PuTTY
Welcome to Virtual PC Simulator, version 0.6.2
Dedicated to Daling.
Build time: Apr 10 2019 02:42:20
Copyright (c) 2007-2014, Paul Meng (mirnshi@gmail.com)
All rights reserved.

VPCS is free software, distributed under the terms of the "BSD" licence.
Source code and license can be found at vpcs.sf.net.
For more information, please visit wiki.freecode.com.cn.

Press '?' to get help.

Executing the startup file

PC1> ip 192.24.10.101 255.255.255.0 192.24.10.1
Checking for duplicate address...
PC1 : 192.24.10.101 255.255.255.0 gateway 192.24.10.1

PC1> save
Saving startup configuration to startup.vpc
. done

PC1>

```

Рисунок 2.11 – Приклад налаштування робочої станції WS-2410-10-1

```

Enter configuration commands, one per line. End with CNTL/Z.
SW-1(config)#vlan 10
SW-1(config-vlan)#name Users
SW-1(config-vlan)#vlan 20
SW-1(config-vlan)#name Guests
SW-1(config-vlan)#vlan 30
SW-1(config-vlan)#name Managment
SW-1(config-vlan)#vlan 40
SW-1(config-vlan)#name Admins
SW-1(config-vlan)#Vlan 99
SW-1(config-vlan)#name Zabbix
SW-1(config-vlan)#exi
SW-1(config)#int 0/1
^
% Invalid input detected at '^' marker.

SW-1(config)#int e0/1
SW-1(config-if)#
SW-1(config-if)#switchport mode access
SW-1(config-if)#switchport access vlan 10
SW-1(config-if)#spanning-tree portfast edge
%Warning: portfast should only be enabled on ports connected to a single
host. Connecting hubs, concentrators, switches, bridges, etc... to this
interface when portfast is enabled, can cause temporary bridging loops.
Use with CAUTION

%Portfast has been configured on Ethernet0/1 but will only
have effect when the interface is in a non-trunking mode.
SW-1(config-if)#int e0/2
SW-1(config-if)#switchport mode access
SW-1(config-if)#switchport access vlan 40
SW-1(config-if)#spanning-tree portfast edge
%Warning: portfast should only be enabled on ports connected to a single
host. Connecting hubs, concentrators, switches, bridges, etc... to this
interface when portfast is enabled, can cause temporary bridging loops.
Use with CAUTION

%Portfast has been configured on Ethernet0/2 but will only
have effect when the interface is in a non-trunking mode.
SW-1(config-if)#int e0/3
SW-1(config-if)#switchport mode access
SW-1(config-if)#switchport access vlan 99
SW-1(config-if)#spanning-tree portfast edge
%Warning: portfast should only be enabled on ports connected to a single
host. Connecting hubs, concentrators, switches, bridges, etc... to this
interface when portfast is enabled, can cause temporary bridging loops.
Use with CAUTION

%Portfast has been configured on Ethernet0/3 but will only
have effect when the interface is in a non-trunking mode.
SW-1(config-if)#int e0/0
SW-1(config-if)#switchport trunk encapsulation dot1q
SW-1(config-if)#switchport mode trunk
SW-1(config-if)#switchport trunk allowed vlan 10,20,30,40,99
SW-1(config-if)#
*Jun 20 11:23:16.444: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/0, changed state to down
SW-1(config-if)#

```

Рисунок 2.12 – Приклад налаштування маршрутизації на комутаторі SW-1

		Нероденко Д.О			ККІКБ.КР.Б – 125 – 10 – ПЗ	Арк.
		Покотило О.А				40
Змн.	Арк.	№ докум.	Підпис	Дата		

Далі йдуть налаштування Віртуальних Робочих станці Windows 10 та Linux Ubuntu, а також налаштування Zabbix server.

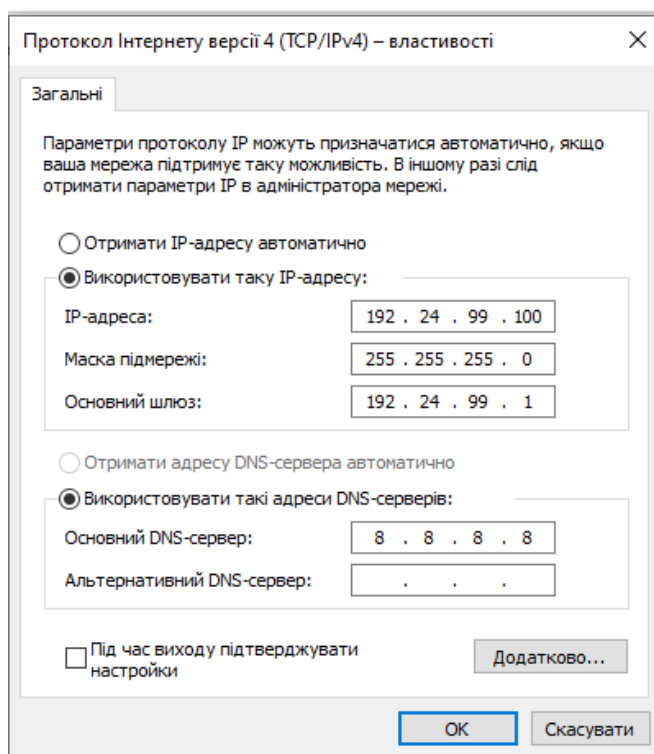


Рисунок 2.13 – Приклад налаштування робочої станції WS-2410-99-1

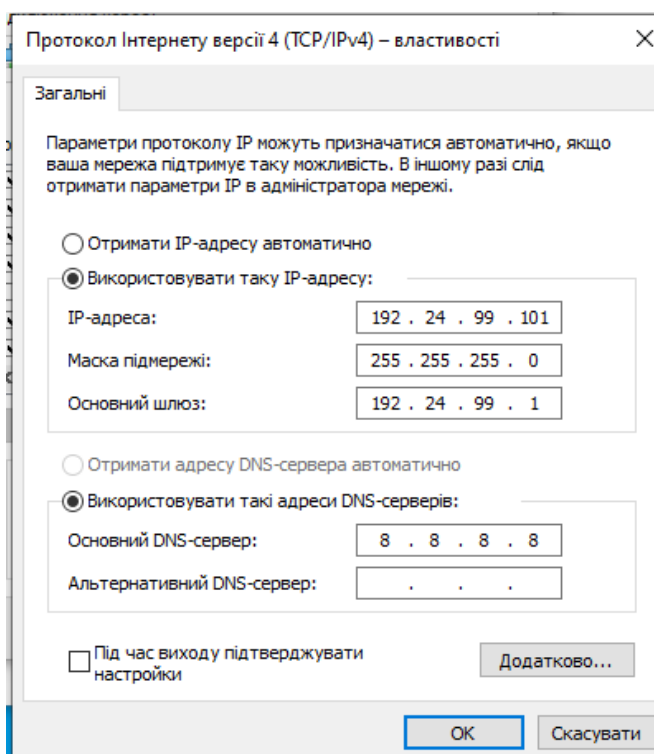


Рисунок 2.14– Приклад налаштування робочої станції WS-2410-99-2

		Нероденко Д.О			ККІКБ.КР.Б – 125 – 10 – ПЗ	Арк.
		Покотило О.А				
Змн.	Арк.	№ докум.	Підпис	Дата		41

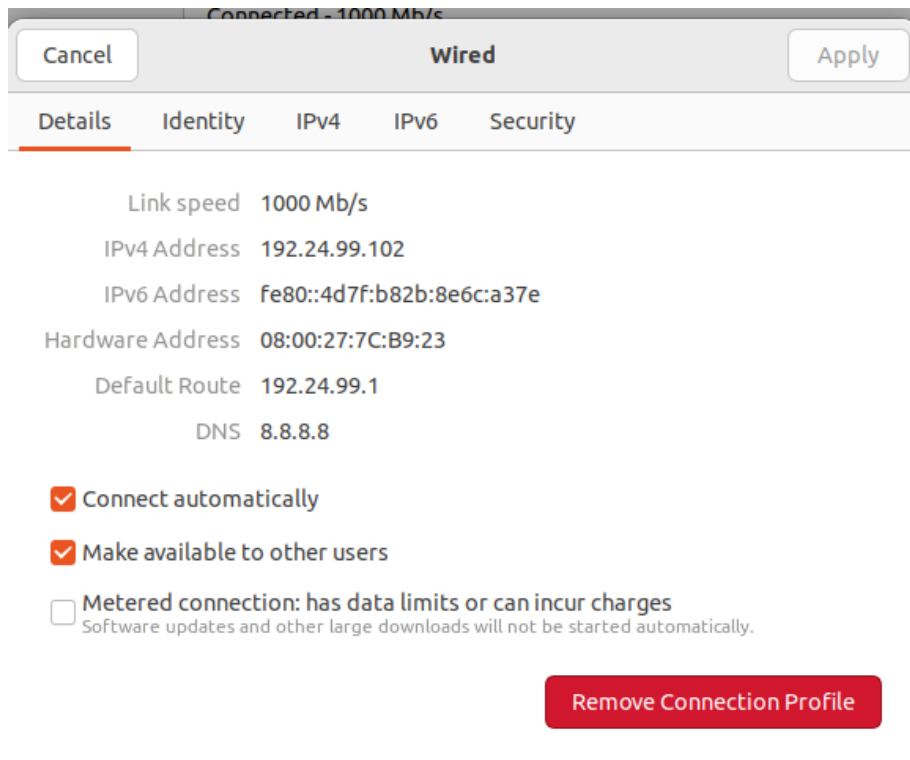


Рисунок 2.15 – Приклад налаштування робочої станції Ubuntu-1

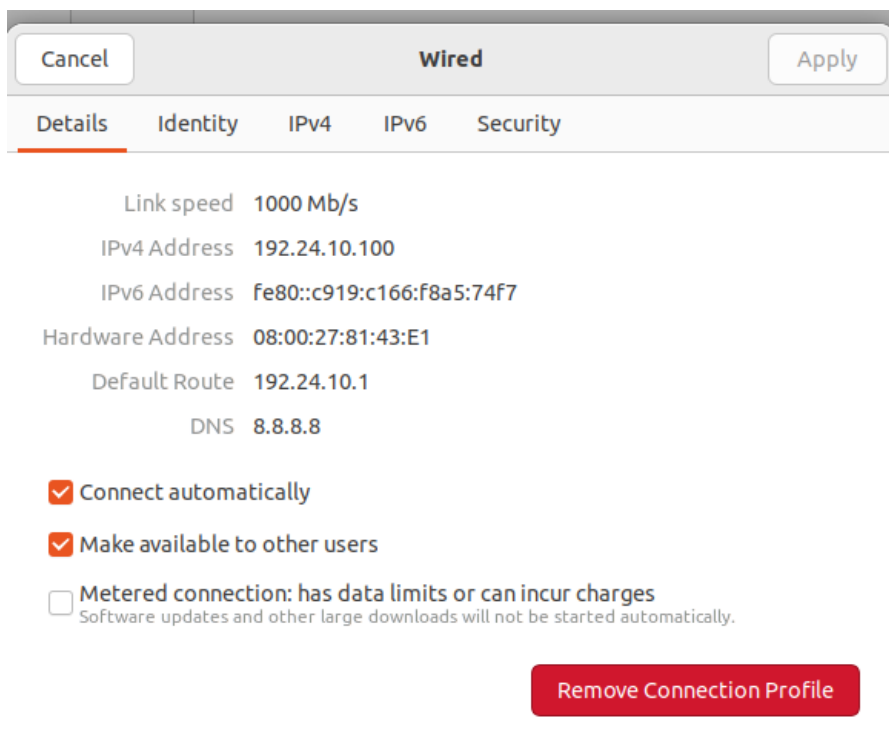


Рисунок 2.16 – Приклад налаштування робочої станції Zabbix Server

Висновок до другого розділу

У другому розділі було детально розглянуто застосування технологій мережевого моніторингу та основи проектування комп'ютерних мереж. Зокрема, акцентовано увагу на важливості планування мережевої інфраструктури для забезпечення її стабільної роботи, безпеки та ефективного моніторингу.

Основні принципи мережевого моніторингу, такі як збір та обробка даних про стан пристроїв, канали зв'язку та продуктивність, є ключовими для виявлення потенційних загроз і збоїв, що дозволяє своєчасно реагувати на проблеми. Важливим аспектом є використання різноманітних протоколів і технологій, зокрема SNMP і ICMP, для моніторингу стану мережі та її безпеки.

Розглянуто також проектування мережі з використанням VLAN, протоколу RSTP та інших важливих компонентів, що забезпечують високу надійність і ефективний моніторинг. Зокрема, обрано гібридну топологію для корпоративної мережі, яка поєднує різні типи топологій, дозволяючи досягти гнучкості та масштабованості мережі.

Також важливим кроком було налаштування схеми адресації мережі, що дозволяє ефективно керувати трафіком і забезпечити безпеку різних сегментів мережі. Для зручності адміністрування було налаштовано SNMPv2 на маршрутизаторі MainRouter, що забезпечує можливість віддаленого моніторингу та управління мережею.

		Нероденко Д.О			ККІКБ.КР.Б – 125 – 10 – ПЗ	Арк.
		Покотило О.А				
Змн.	Арк.	№ докум.	Підпис	Дата		43

РОЗДІЛ 3. ПРАКТИЧНЕ ЗАСТОСУВАННЯ ТЕХНОЛОГІЙ МОНІТО- РИНГУ МЕРЕЖІ В КОМП'ЮТЕРНИХ МЕРЕЖАХ

3.1 Встановлення та налаштування системи Zabbix для моніторингу

Встановлення та налаштування системи Zabbix є важливим етапом у створенні підсистеми моніторингу мережі. Перш за все, необхідно забезпечити коректну інсталяцію сервера Zabbix, бази даних і веб-інтерфейсу, що є основними компонентами системи. Zabbix підтримує різні СУБД, зокрема MySQL, PostgreSQL, що забезпечує гнучкість у виборі платформи для зберігання даних.

Наступним кроком є конфігурування сервера Zabbix, де задаються параметри підключення до бази даних, налаштування мережевого інтерфейсу, таймінг перевірок та інші базові опції. Для збору даних з мережевих пристроїв і серверів використовуються агенти Zabbix, які потрібно встановити на відповідні вузли мережі та налаштувати для взаємодії із сервером.

Особливу увагу варто приділити налаштуванню елементів моніторингу — хостів, елементів даних, тригерів і оповіщень. Хости в Zabbix — це пристрої чи сервери, які підлягають моніторингу, а елементи даних визначають конкретні параметри, що збираються. Тригери встановлюють умови, при яких система генерує оповіщення, що дозволяє швидко реагувати на проблеми.

Для зручності користувачів налаштовують дашборди та звіти, що забезпечують візуалізацію. Також можлива інтеграція Zabbix з різними зовнішніми системами для автоматизації реакцій на інциденти.

Таким чином, правильне встановлення і налаштування Zabbix забезпечує ефективний збір, обробку та аналіз мережевої інформації, що є основою для підтримки стабільної роботи мережі та своєчасного виявлення загроз.

		Нероденко Д.О			ККІКБ.КР.Б – 125 – 10 – ПЗ	Арк.
		Покотило О.А				
Змн.	Арк.	№ докум.	Підпис	Дата		44

```

azabbix@azabbix-virtual-machine:~$ sudo su
[sudo] password for azabbix:
root@azabbix-virtual-machine:~# wget https://repo.zabbix.com/zabbix/7.2/release/ubuntu/pool/main/z/zabbix-release/zabbix-release_latest_7.2+ubuntu22.04_all.deb
--2025-05-15 21:40:01-- https://repo.zabbix.com/zabbix/7.2/release/ubuntu/pool/main/z/zabbix-release/zabbix-release_latest_7.2+ubuntu22.04_all.deb
Resolving repo.zabbix.com (repo.zabbix.com)... 178.128.6.101, 2604:a880:2:d0::2062:d001
Connecting to repo.zabbix.com (repo.zabbix.com)|178.128.6.101|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 7288 (7,1K) [application/octet-stream]
Saving to: 'zabbix-release_latest_7.2+ubuntu22.04_all.deb'

zabbix-release_late 100%[=====] 7,12K --.-KB/s in 0s

2025-05-15 21:40:01 (2,14 GB/s) - 'zabbix-release_latest_7.2+ubuntu22.04_all.deb' saved [7288/7288]

root@azabbix-virtual-machine:~# dpkg -i zabbix-release_latest_7.2+ubuntu22.04_all.deb
Selecting previously unselected package zabbix-release.
(Reading database ... 202619 files and directories currently installed.)
Preparing to unpack zabbix-release_latest_7.2+ubuntu22.04_all.deb ...
Unpacking zabbix-release (1:7.2-1+ubuntu22.04) ...
Setting up zabbix-release (1:7.2-1+ubuntu22.04) ...

```

Рисунок 3.1 – Покрокове встановлення Zabbix частина 1

```

mysql> create database zabbix character set utf8mb4 collate utf8mb4_bin;
Query OK, 1 row affected (0,01 sec)

mysql> create user zabbix@localhost identified by 'password';
Query OK, 0 rows affected (0,01 sec)

mysql> reate user ZabbNerodenkoKB212@localhost identified by 'StrongPass123@';
ERROR 1064 (42000): You have an error in your SQL syntax; check the manual that correspond
s to your MySQL server version for the right syntax to use near 'reate user ZabbNerodenkoK
B212@localhost identified by 'StrongPass123@' at line 1
mysql> create user zabbix@localhost identified by 'password';
ERROR 1396 (HY000): Operation CREATE USER failed for 'zabbix'@'localhost'
mysql> create user ZBXNerodenkoKB212@localhost identified by 'SrongPass123@';
Query OK, 0 rows affected (0,01 sec)

mysql> grant all privileges on zabbix.* to ZBXNerodenkoKB212@localhost;
Query OK, 0 rows affected (0,00 sec)

mysql> set global log_bin_trust_function_creators = 1;
Query OK, 0 rows affected, 1 warning (0,00 sec)

```

Рисунок 3.2 – Покрокове встановлення Zabbix серверу на робочу станцію Linux частина 2

Disable log_bin_trust_function_creators option after importing database schema.

```
# mysql -uroot -p
password
mysql> set global log_bin_trust_function_creators = 0;
mysql> quit;
```

e. Configure the database for Zabbix server
Edit file /etc/zabbix/zabbix_server.conf

```
DBPassword=password
```

f. Start Zabbix server and agent processes
Start Zabbix server and agent processes and make it start at system boot.

```
# systemctl restart zabbix-server zabbix-agent apache2
# systemctl enable zabbix-server zabbix-agent apache2
```

Рисунок 3.3 – Покрокове встановлення Zabbix серверу на робочу станцію Linux частина з офіційного сайту[1]

		Нероденко Д.О			ККІКБ.КР.Б – 125 – 10 – ПЗ	Арк.
		Покотило О.А				45
Змн.	Арк.	№ докум.	Підпис	Дата		

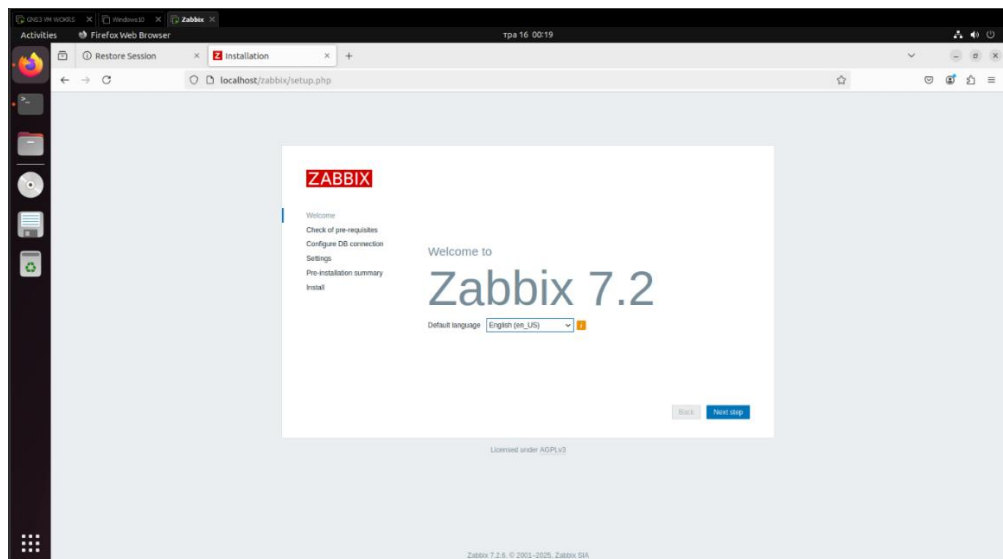


Рисунок 3.4 – Веб частина налаштування Zabbix серверу

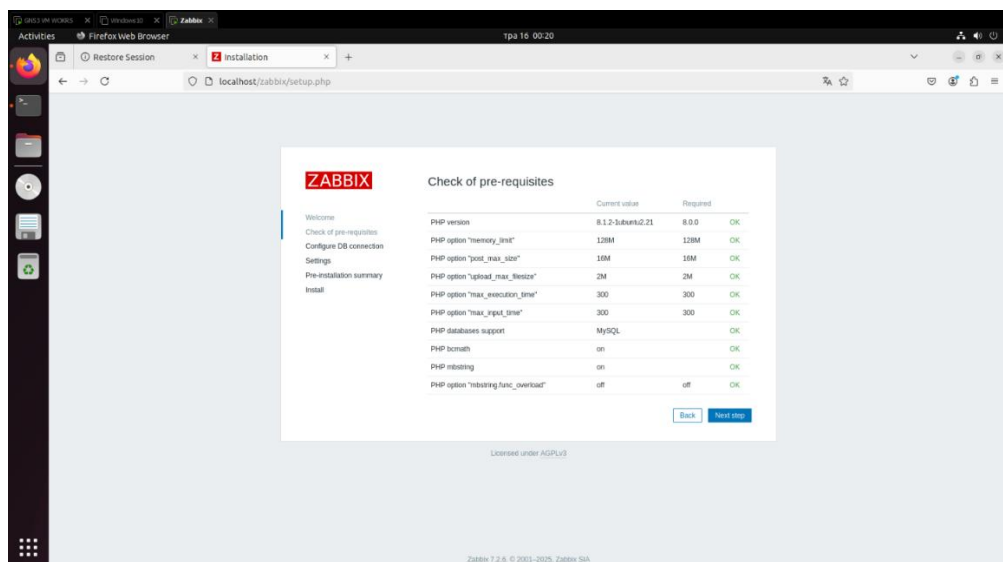


Рисунок 3.5 – Первинна перевірка налаштувань Zabbix серверу

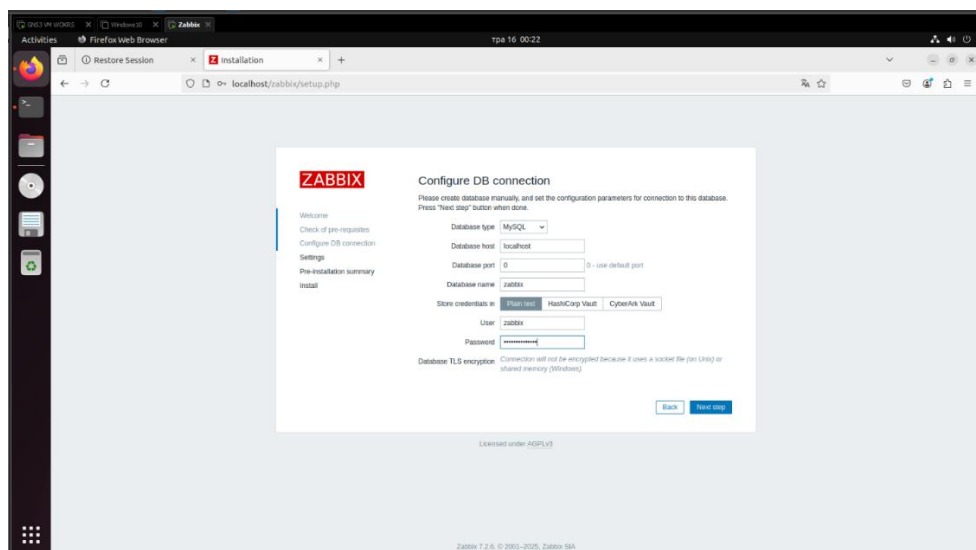


Рисунок 3.6 – Конфігураці з’єднання Zabbix серверу з базою даних

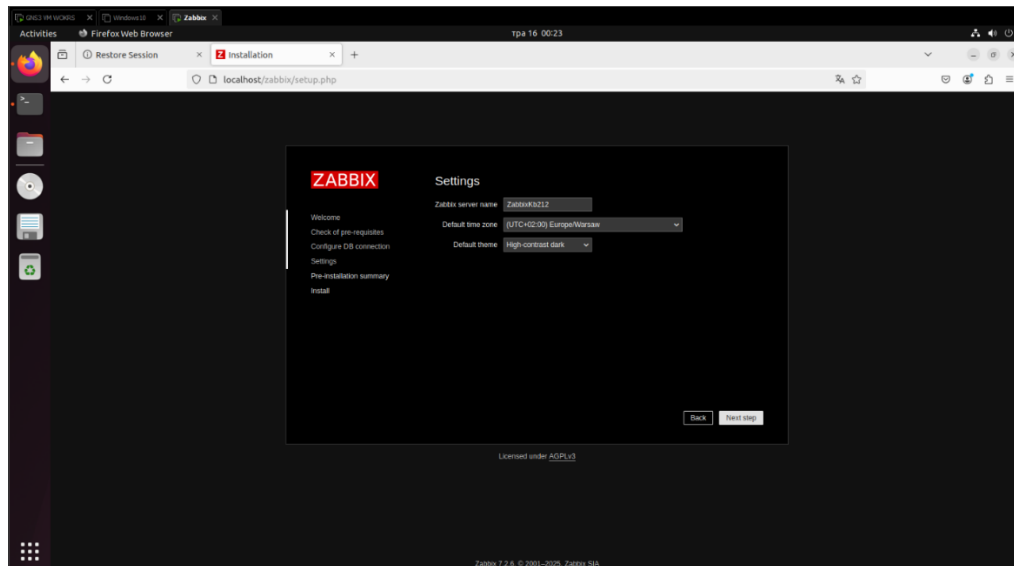


Рисунок 3.7 – Налаштування назви, часової зони Zabbix серверу

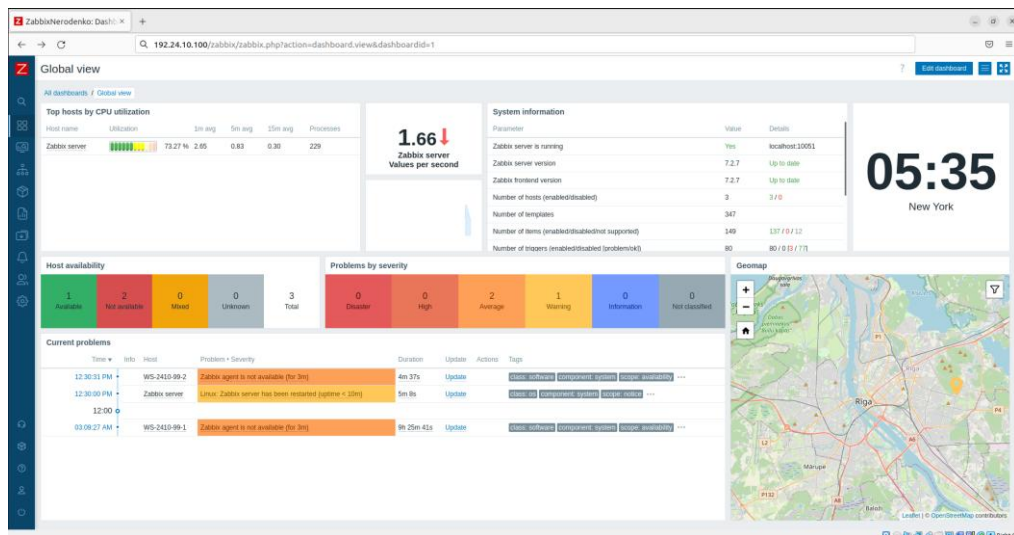


Рисунок 3.8 – Веб інтерфейс Zabbix серверу

Одним з недоліків Zabbix Server є підключення до системи через протокол HTTP. Враховуючи, що HTTP є незашифрованим протоколом, переданий через нього трафік може бути вразливим до перехоплення, що створює ризик витоку чутливої інформації, такої як логіни, паролі та інші важливі дані. Одним з основних покращень системи повинно бути впровадження протоколу HTTPS, який забезпечує шифрування всього трафіку між веб-інтерфейсом Zabbix і користувачами, тим самим запобігаючи можливим атакам. Крім того, доцільно впровадити налаштування доступу користувачів з різними рівнями прав, що дозволить забезпечити гнучкий контроль доступу до системи через інтерфейс Zabbix.

		Нероденко Д.О.			ККІКБ.КР.Б – 125 – 10 – ПЗ	Арк.
		Покотило О.А.				47
Змн.	Арк.	№ докум.	Підпис	Дата		

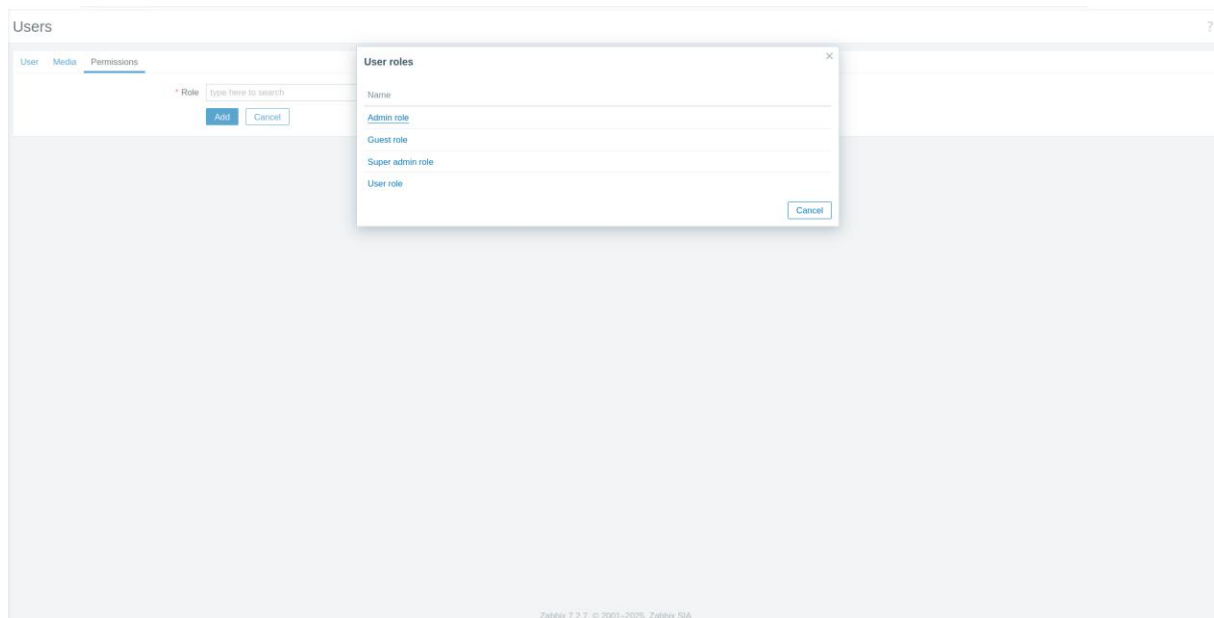


Рисунок 3.11 – Меню вибору стандартних ролей користувача

Users

User Media Permissions

* Role

User type

Group	Type	Permissions
All groups	Hosts	None
All groups	Templates	None

Permissions can be assigned for user groups only.

Access to UI elements

Dashboards

Monitoring

Services

Inventory

Reports

Data collection

Alerts

Access to services

Read-write access to services

Read-only access to services

Access to modules

Access to API

Access to actions

Рисунок 3.12 – Гнучке налаштування ролей користувача

3.2 Встановлення та налаштування системи Zabbix Agent на робочі станції

Для збору інформації з мережевих пристроїв і серверів у системі моніторингу Zabbix використовується Zabbix Agent — спеціальний програмний модуль, який встановлюється на клієнтські машини. Агент відповідає за збір різноманітних показників: стану процесора, пам'яті, дискових ресурсів, мережевих інтерфейсів, а також інших параметрів, що важливі для моніторингу.

Процес встановлення Zabbix Agent включає наступні етапи:

- Завантаження відповідної версії агента, що сумісна з операційною системою клієнта (Linux, Windows тощо).
- Інсталяція пакету агента за допомогою стандартних менеджерів пакетів або інсталяційних файлів.
- Налаштування конфігураційного файлу агента, у якому вказується IP-адреса або доменне ім'я сервера Zabbix, а також параметри, які слід моніторити.
- Запуск служби агента і додавання відповідного хоста в панелі керування Zabbix сервера для початку збору даних.

Коректна установка і налаштування Zabbix Agent є ключовою умовою для отримання повної і достовірної інформації про стан мережевих пристроїв і серверів, що дозволяє системі моніторингу працювати ефективно та своєчасно інформувати про будь-які відхилення чи проблеми[14].

OS DISTRIBUTION	OS VERSION	HARDWARE	ZABBIX VERSION	ENCRYPTION	PACKAGING
Windows	Any	amd64	7.2	OpenSSL	MSI
Linux		i386	7.0 LTS	No encryption	Archive
macOS			6.2		
AIX			6.0 LTS		
FreeBSD			5.4		
OpenBSD			5.2		
Solaris			5.0 LTS		
			4.4		
			4.2		
			4.0 LTS		
			3.0 LTS		

Рисунок 3.13 – Можливий вибір ОС для встановлення Zabbix Agent

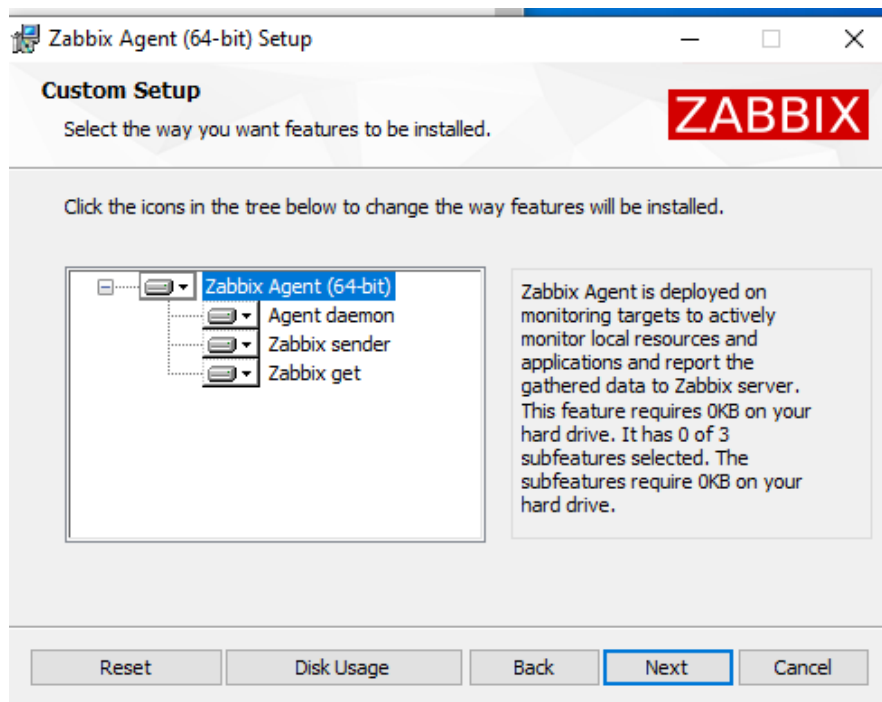


Рисунок 3.14 – Встановлення Zabbix Agent на робочу станцію

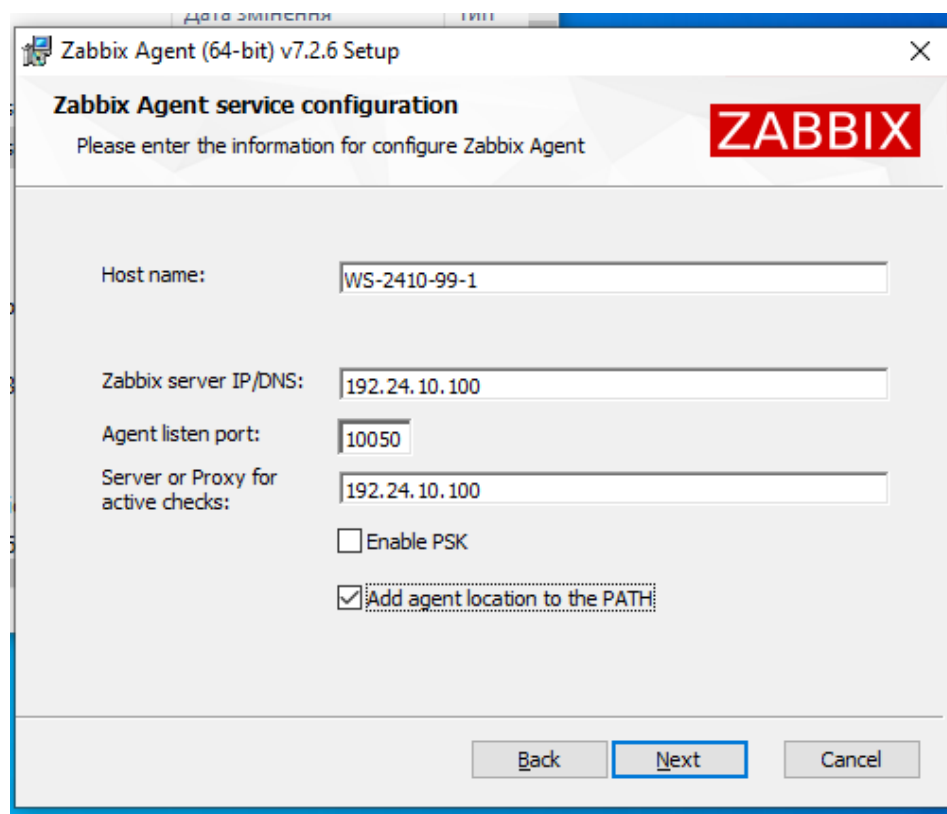


Рисунок 3.15 – Встановлення Zabbix Agent на робочу станцію

Для забезпечення збору даних з клієнтських пристроїв було налаштоване підключення Zabbix Agent до сервера моніторингу Zabbix. На кожному агенті у конфігураційному файлі вказано адресу сервера Zabbix, що дозволяє агенту передавати зібрану інформацію на центральний сервер. Сервер, у свою чергу,

		Нероденко Д.О			ККІКБ.КР.Б – 125 – 10 – ПЗ	Арк.
		Покотило О.А				
Змн.	Арк.	№ докум.	Підпис	Дата		51

налаштовано на прийом і обробку цих даних, що забезпечує своєчасне відстеження стану пристроїв і сервісів у мережі[2].

Крім того, у системі моніторингу було активовано функцію автоматичного виявлення нових пристроїв у мережі за допомогою ICMP ping. Цей механізм дозволяє періодично сканувати задані підмережі та ідентифікувати активні вузли, що полегшує адміністрування мережі і швидке додавання нових пристроїв до системи моніторингу без необхідності ручного втручання.

Завдяки цим налаштуванням система Zabbix отримала можливість не лише моніторити існуючі ресурси, а й автоматично виявляти і інтегрувати нові пристрої, що значно підвищує ефективність управління мережею.

The screenshot shows the Zabbix web interface for configuring a new host. The 'Host' tab is active, displaying various configuration fields. The 'Host name' and 'Visible name' are both set to 'WS-2410-99-1'. Under 'Templates', 'Zabbix agent' is selected. In the 'Host groups' section, 'Virtual machines' is chosen. The 'Interfaces' table shows one interface of type 'Agent' with IP address '192.24.99.101'. The 'Connect to' section has 'IP' and 'DNS' buttons, with 'Port' set to '10050'. The 'Default' radio button is set to 'Remove'. There is an 'Add' link below the interfaces table. The 'Description' field is empty. The 'Monitored by' section has 'Server', 'Proxy', and 'Proxy group' buttons, with 'Server' selected. The 'Enabled' checkbox is checked. At the bottom right, there are buttons for 'Update', 'Clone', 'Delete', and 'Cancel'.

Рисунок 3.16 – Підключення Zabbix Agent до Zabbix серверу

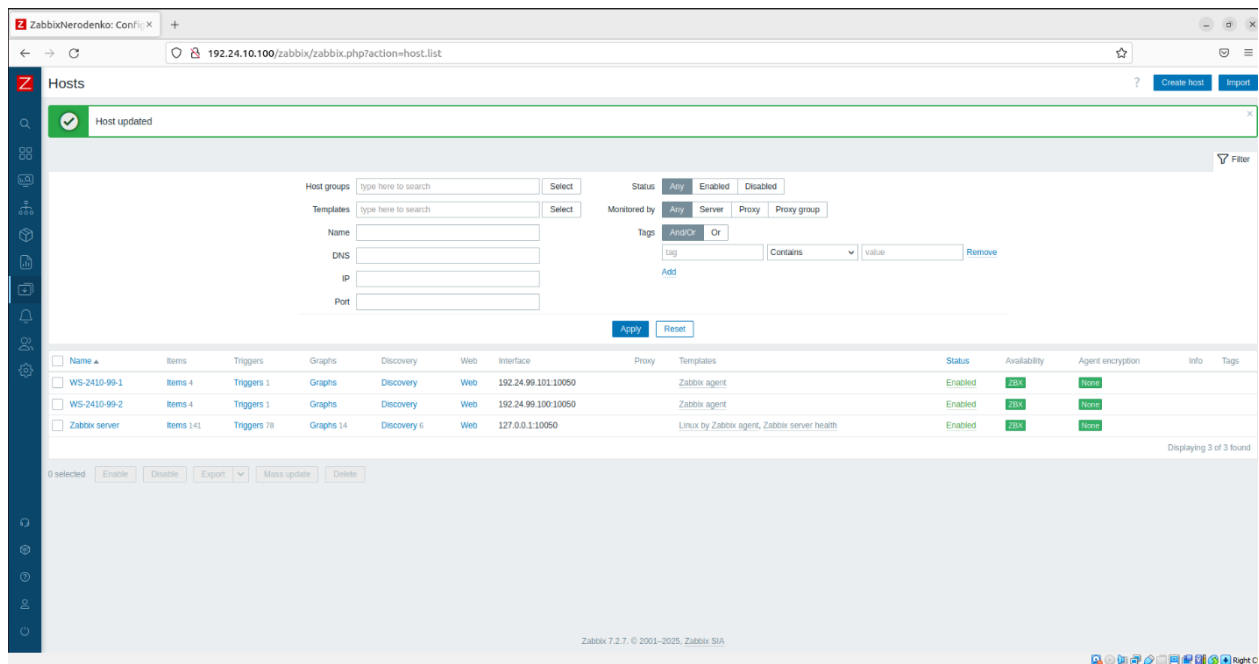


Рисунок 3.17 – Підключенні Zabbix агенти до Zabbix серверу та сам агент Zabbix серверу

Discovery rule

* Name:

Discovery by: ☒ Server ☐ Proxy

* IP range:

* Update interval:

Maximum concurrent checks per type: ☐ One ☐ Unlimited ☒ Custom

* Checks:

Type	Actions
ICMP ping	Edit Remove
Add	

Device uniqueness criteria: ☒ IP address

Host name: ☒ DNS name ☐ IP address

Visible name: ☒ Host name ☐ DNS name ☐ IP address

Enabled: ☒

Рисунок 3.18 – Налаштування ICMP виявлення робочих станцій в локальній мережі проекту

Discovery rule CheckNewWSByPing x Filter			
type here to search			
Apply Reset			
Discovered device	Monitored host	Uptime/Downtime	ICMP ping
CheckNewWSByPing (16 devices)			
192.24.10.1 (static.1k.dscga.com)		00:11:01	12h 19m 23s
192.24.10.100 (static.100k.dscga.com)		00:10:27	12h 18m 32s
192.24.10.101 (static.101k.dscga.com)		00:10:27	12h 18m 32s
192.24.10.102 (static.102k.dscga.com)		00:10:27	12h 18m 32s
192.24.20.1		00:09:33	12h 17m 38s
192.24.20.101		00:08:13	12h 14m 9s
192.24.20.102		00:08:13	12h 14m 9s
192.24.30.1		00:06:18	12h 9m 14s
192.24.30.101		00:04:53	12h 5m 51s
192.24.30.102		00:04:53	12h 5m 51s
192.24.40.1 (192-24-40-1.nftctelecom.com)		00:02:58	12h 59s
192.24.40.101 (192-24-40-101.nftctelecom.com)		00:02:22	11h 37m 55s
192.24.40.102 (192-24-40-102.nftctelecom.com)		00:02:22	12h 17s
192.24.99.1 (192-24-99-192-24-99-1.cpe.sparklight.net)		00:01:29	11h 59m 17s
192.24.99.100 (192-24-99-192-24-99-100.cpe.sparklight.net)	WS-2410-99-2	00:00:46	9h 34m 19s
192.24.99.101 (192-24-99-192-24-99-101.cpe.sparklight.net)	WS-2410-99-1	09:34:19	11h 36m 30s

Рисунок 3.19 – Результат виявлення за допомогою ICMP пінгу

Можна також побачити що Zabbix автоматично підписує робочі станції з Zabbix агентом.

Також було встановлено робочу машину на Linux OS (Ubuntu) а також було поставлено Zabbix агент.

```
root1111@root1111-virtual-machine:~$ sudo su
[sudo] password for root1111:
root@root1111-virtual-machine:/home/root1111# wget https://repo.zabbix.com/zabbix/7.2/release/ubuntu/pool/main/z/zabbix-release/zabbix-release_latest_7.2+ubuntu22.04_all.deb
# dpkg -i zabbix-release_latest_7.2+ubuntu22.04_all.deb
--2025-06-16 12:27:18-- https://repo.zabbix.com/zabbix/7.2/release/ubuntu/pool/main/z/zabbix-release/zabbix-release_latest_7.2+ubuntu22.04_all.deb
Resolving repo.zabbix.com (repo.zabbix.com)... 178.128.6.101, 2604:a880:2:d0::2062:d001
Connecting to repo.zabbix.com (repo.zabbix.com)|178.128.6.101|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 7288 (7,1K) [application/octet-stream]
Saving to: 'zabbix-release_latest_7.2+ubuntu22.04_all.deb'

zabbix-release_latest_ 100%[=====>] 7,12K --.-KB/s in 0s

2025-06-16 12:27:19 (2,96 GB/s) - 'zabbix-release_latest_7.2+ubuntu22.04_all.deb' saved [7288/7288]

root@root1111-virtual-machine:/home/root1111# dpkg -i zabbix-release_latest_7.2+ubuntu22.04_all.deb
```

Рисунок 3.20 – Встановлення Zabbix агенту на робочу станцію з ОС Linux

```
root@root1111-virtual-machine:/home/root1111# apt install zabbix-agent2
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
 chromium-codecs-ffmpeg-extra gstreamer1.0-vaapi i965-va-driver intel-media-va-driver
 libaacs0 libaom3 libass9 libavcodec58 libavformat58 libavutil56 libbdplus0 libblas3
 libbluray2 libbs2b0 libchromaprint1 libcodec2-1.0 libdav1d5 libflite1 libgme0 libgsm1
 libgstreamer-plugins-bad1.0-0 libigdgmm12 libilv-0-0 libllvm15 libmfx1 libmysofa1
 libnorm1 libopenmpt0 libpgm-5.3-0 libpostproc55 librabbitmq4 librubberband2
 libserd-0-0 libshine3 libsnappy1v5 libsord-0-0 libsratom-0-0 libsrtp1.4-gnutls
 libssh-gcrypt-4 libswresample3 libswscale5 libudfread0 libva-drm2 libva-wayland2
 libva-x11-2 libva2 libvdpau1 libvidstab1.1 libx265-199 libxvidcore4 libzing2 libzmq5
 libzvbi-common libzvbi0 mesa-va-drivers mesa-vdpau-drivers pocketsphinx-en-us
 va-driver-all vdpau-driver-all
Use 'sudo apt autoremove' to remove them.
The following NEW packages will be installed:
 zabbix-agent2
0 upgraded, 1 newly installed, 0 to remove and 208 not upgraded.
Need to get 5 558 kB of archives.
After this operation, 18,9 MB of additional disk space will be used.
Get:1 https://repo.zabbix.com/zabbix/7.2/stable/ubuntu jammy/main amd64 zabbix-agent2 amd
64 1:7.2.7-1+ubuntu22.04 [5 558 kB]
Fetched 5 558 kB in 11s (493 kB/s)
Selecting previously unselected package zabbix-agent2.
(Reading database ... 199629 files and directories currently installed.)
Preparing to unpack .../zabbix-agent2_1%3a7.2.7-1+ubuntu22.04_amd64.deb ...
Unpacking zabbix-agent2 (1:7.2.7-1+ubuntu22.04) ...
Setting up zabbix-agent2 (1:7.2.7-1+ubuntu22.04) ...
Created symlink /etc/systemd/system/multi-user.target.wants/zabbix-agent2.service → /lib/
systemd/system/zabbix-agent2.service.
Processing triggers for man-db (2.10.2-1) ...
root@root1111-virtual-machine:/home/root1111# systemctl restart zabbix-agent2
root@root1111-virtual-machine:/home/root1111# systemctl enable zabbix-agent2
Synchronizing state of zabbix-agent2.service with SysV service script with /lib/systemd/s
ysd/sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable zabbix-agent2
root@root1111-virtual-machine:/home/root1111# systemctl status zabbix-agent2
● zabbix-agent2.service - Zabbix Agent 2
   Loaded: loaded (/lib/systemd/system/zabbix-agent2.service; enabled; vendor preset:
   Active: active (running) since Mon 2025-06-16 13:13:50 EEST; 21s ago
   Main PID: 162355 (zabbix_agent2)
   Tasks: 7 (limit: 4554)
   Memory: 4.1M
```

Рисунок 3.21 – Встановлення Zabbix агенту на робочу станцію з ОС Linux

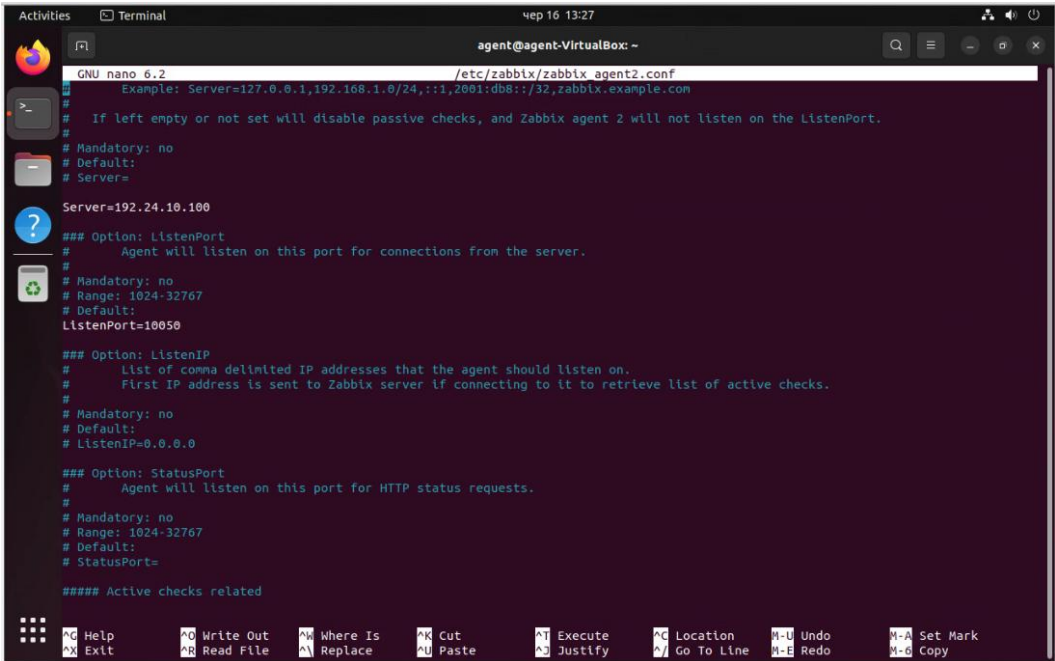


Рисунок 3.22 – Налаштування конфігураційного файлу Zabbix агенту на робочій станції з ОС Linux

Рисунок 3.23 – Налаштування хосту за допомогою SNMPv2

Name	Interface	Availability	Tags	Status	Latest data	Problems	Graphs	Dashboards	Web
Mainrouter	192.24.10.1:161	SNMP	class: network target: cisco target: cisco-ios	Enabled	Latest data 138	Problems	Graphs 13	Dashboards 1	Web
WS-2410-99-1	192.24.99.101:10050	Zabbix	class: software target: zabbix-agent	Enabled	Latest data 4	Problems	Graphs	Dashboards 1	Web
WS-2410-99-2	192.24.99.100:10050	Zabbix	class: software target: zabbix-agent	Enabled	Latest data 4	Problems	Graphs	Dashboards 1	Web
WS-2410-99-3U	192.24.99.102:10050	Zabbix	class: software target: zabbix-agent	Enabled	Latest data 4	Problems	Graphs	Dashboards 1	Web
Zabbix server	127.0.0.1:10050	Zabbix	class: os class: software target: linux +++	Enabled	Latest data 141	Problems	Graphs 14	Dashboards 4	Web

Рисунок 3.24 – Результат налаштування хосту за допомогою SNMPv2

3.3 Приклади та аналіз результатів моніторингу

Важливим компонентом моніторингу є стабільність самої системи моніторингу, в даному випадку — Zabbix. При створенні віртуальної машини на ОС Linux Ubuntu 22.04 системі було виділено 4096 МБ оперативної пам'яті, 128 МБ відеопам'яті, два ядра процесора та 20 ГБ на жорсткому диску для операційної системи і збереження необхідної інформації.

При навантаженні з 4-ма Zabbix Agent, SNMP-опитуванні, перевірці доступу до глобальної мережі через ICMP ping до IP-адреси 8.8.8.8, а також виявленні нових робочих станцій, серверів та інших мережевих пристроїв, система споживає до 25% ресурсів. При надмірному навантаженні на Zabbix сервер, максимальне використання процесора більше 65%.

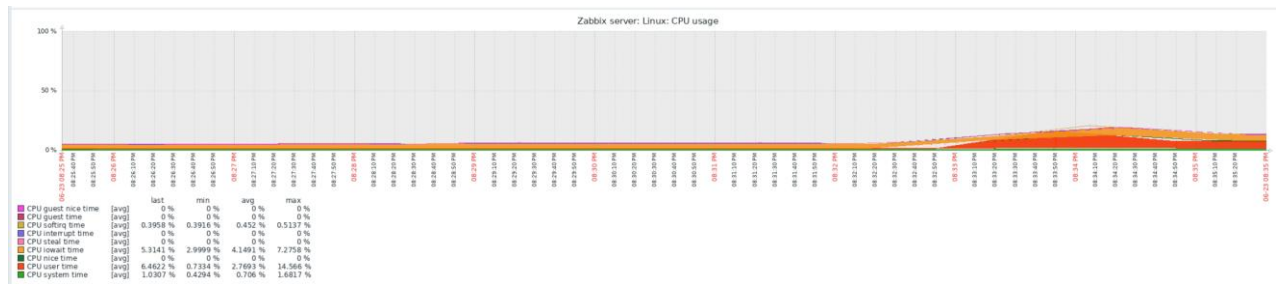


Рисунок 3.25 – Графік використання процесора сервером при ненадмірному навантаженні

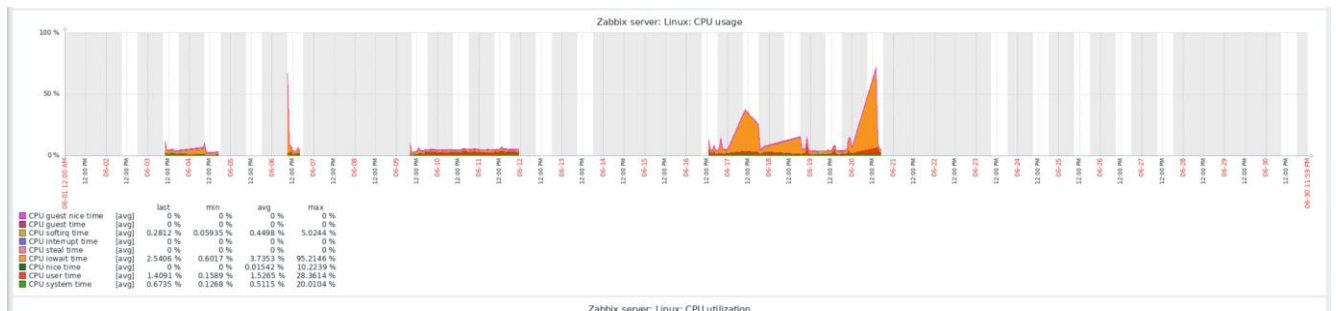


Рисунок 3.26 – Графік використання процесора сервером за місяць

Водночас, система також потребує значних ресурсів оперативної пам'яті. Зокрема, під час виконання численних запитів і обробки великої кількості даних, обсяг використаної оперативної пам'яті може досягати до 3.5 ГБ оперативної пам'яті включно з пам'яттю що використовує система, що також впливає на загальну продуктивність системи.

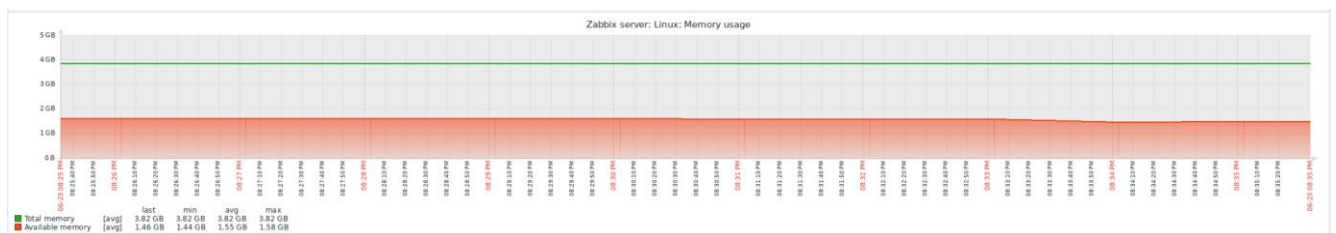


Рисунок 3.27 – Графік використання оперативної пам'яті сервером при ненадмірному навантаженні

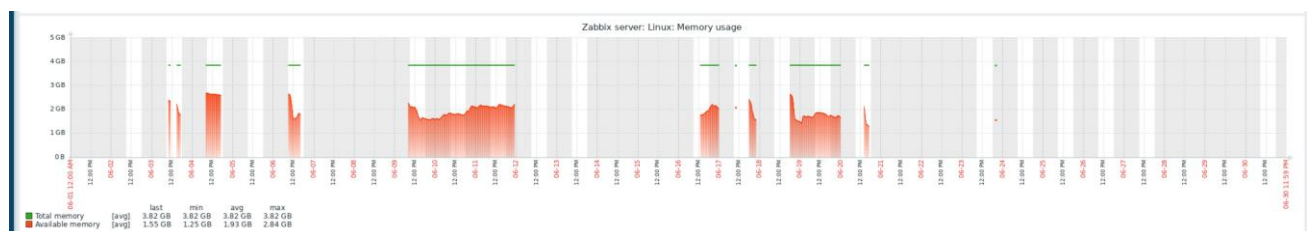


Рисунок 3.28 – Графік використання оперативної пам'яті сервером за місяць

Як можна побачити з скріншоту з місячним аналізом графіку споживання оперативної пам'яті забікс сервер споживає не так багато оперативної пам'яті і її графік стабільніший ніж графік використання процесору.

Одною із ключових важливих речей в роботі серверу моніторингу це навантаження системи. На цьому графіку відображено загальне навантаження на Zabbix-сервер протягом певного часу, що дає змогу оцінити ефективність використання ресурсів та стабільність роботи системи. Всі значення знаходяться в межах нормальних параметрів, що свідчить про відсутність перевантажень у системі.

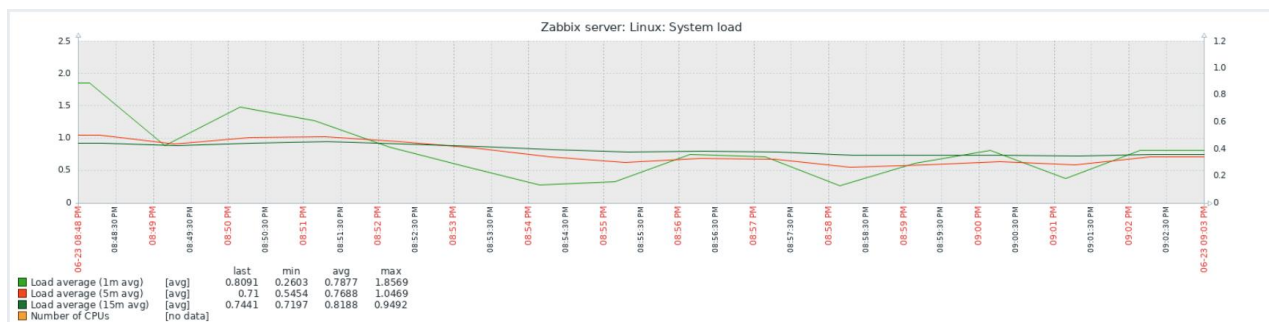


Рисунок 3.29 – Графік навантаження системи за останні 15 хвилин часу.

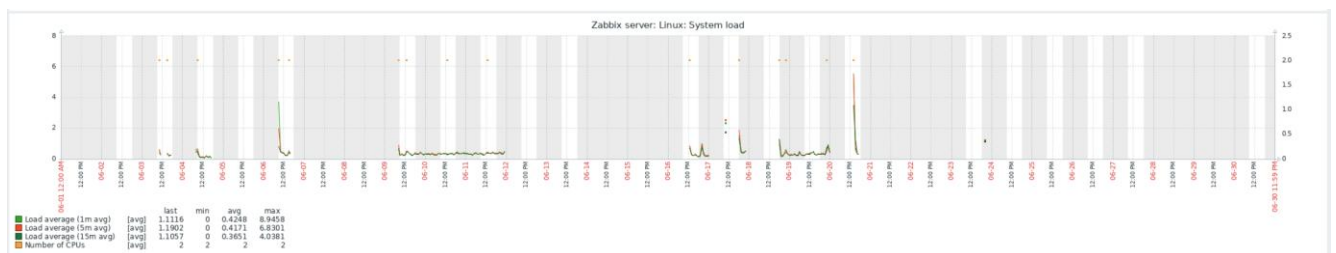


Рисунок 3.30 – Графік навантаження системи за останній місяць

Судячи з графіку за цей місяць система була завантажена найбільше між 20.06 та 21.06 в цей час відбувалася симуляція роботи робочих станцій та мережі в цілому.

Наступним важливим параметром системи є тип накопичувачів даних. У рамках цього проекту використовувався звичайний жорсткий диск, який не забезпечує достатньо високої швидкості читання та запису. Це призводить до деяких проблем з продуктивністю сервера. Одним із суттєвих покращень, яке можна впровадити, є заміна звичайного жорсткого диска на диск типу Seagate IronWolf з 7200 обертами та швидкістю передачі даних до 210 МБ/с. Така заміна буде особливо корисною, якщо Zabbix-сервер розміщується на гіпервізорі типу 1 (гіпервізор на фізичному обладнанні, такому як сервер).

		Нероденко Д.О			ККІКБ.КР.Б – 125 – 10 – ПЗ	Арк.
		Покотило О.А				58
Змн.	Арк.	№ докум.	Підпис	Дата		

У разі розміщення Zabbix-сервера на звичайній робочій станції, оптимальним варіантом може бути використання SATA SSD або SSD M.2, що дозволить значно покращити швидкість обробки даних, зменшуючи затримки при моніторингу та підвищуючи загальну продуктивність системи. Така заміна також дозволить зменшити енергоспоживання та знизити рівень шуму, що є важливим для робочих станцій.

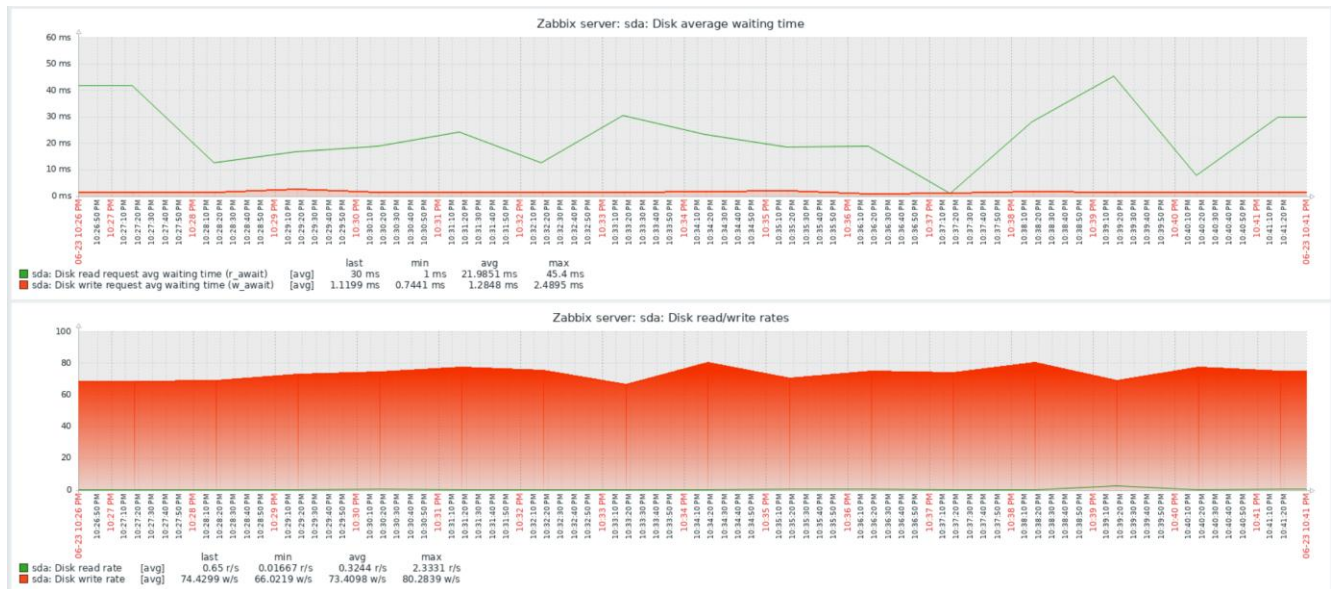


Рисунок 3.31 – Графік середній час очікування та швидкості читання і запису на диск. за останні 15 хвилин часу



Рисунок 3.32 – Графік середній час очікування та швидкості читання і запису на диск. за останній місяць

		Нероденко Д.О			Арк.
		Покотило О.А			59
Змн.	Арк.	№ докум.	Підпис	Дата	

Як вже зазначалося, через невідходящий тип накопичувального пристрою робота віртуальної робочої станції, на якій встановлено Zabbix-сервер, стикається з певними проблемами у функціонуванні через низьку швидкість зчитування. Це призводить до затримок у зборі та обробці даних, що знижує ефективність моніторингу мережі.

З метою покращення продуктивності було запропоновано замість традиційного жорсткого диска (HDD) використовувати спеціалізовані серверні жорсткі диски, SSD або NVMe накопичувачі, що забезпечать значно вищу швидкість доступу до даних. Це дозволить значно зменшити час відповіді при роботі з великими обсягами інформації та забезпечить стабільну і безперебійну роботу сервера, що є критично важливим для моніторингових систем у реальному часі.

У процесі налаштування моніторингу за допомогою технології Zabbix було розглянуто можливість автоматичного збору та аналізу даних про стан мережі та її компонентів. Однак, для забезпечення ефективного управління інфраструктурою, необхідно не тільки збирати дані, а й оперативно отримувати інформацію про критичні події, які можуть статися за відсутності адміністратора на робочому місці. Враховуючи це, важливо налаштувати систему для надсилання сповіщень про виникнення важливих робочих станцій або серверів.

Zabbix надає широкі можливості для інтеграції з різними платформами для сповіщень, що дозволяє адміністратору своєчасно отримувати інформацію про виникнення проблем у мережі.

Серед доступних платформ для надсилання сповіщень в Zabbix можна виділити такі:

Email, Discord, Gmail, Jira, MSTEams, Office365, Slack, SMS, Telegram;

Це основні і відомі для звичайного користувача платформи для отримання сповіщень.

		Нероденко Д.О			ККІКБ.КР.Б – 125 – 10 – ПЗ	Арк.
		Покотило О.А				
Змн.	Арк.	№ докум.	Підпис	Дата		60

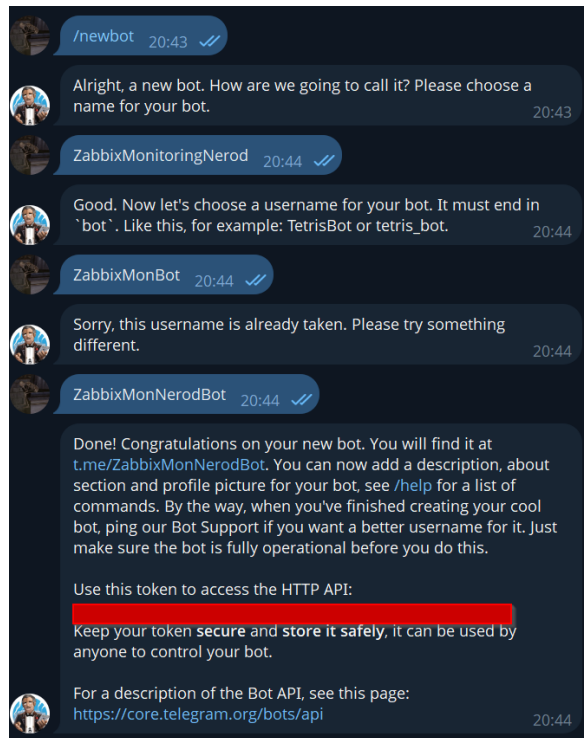


Рисунок 3.35 – Створення боту для сповіщень за допомогою іншого боту в якому нам надається API токен для майбутнього налаштування сповіщень



Рисунок 3.36 – Створений бот для сповіщень

Далі нам потрібен наступний бот для того щоб коректно підв'язати створеного боту до Zabbix.

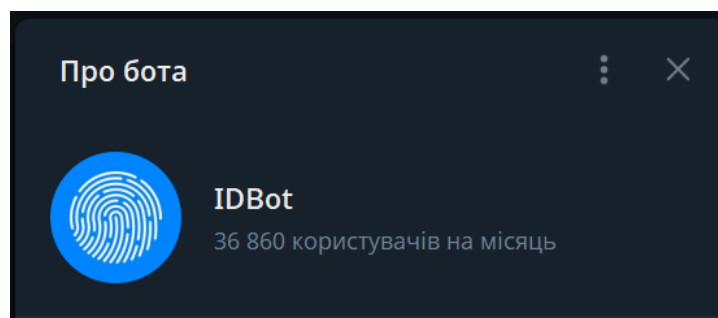


Рисунок 3.37 – Бот для підключення

		Нероденко Д.О			ККІКБ.КР.Б – 125 – 10 – ПЗ	Арк.
		Покотило О.А				
Змн.	Арк.	№ докум.	Підпис	Дата		62

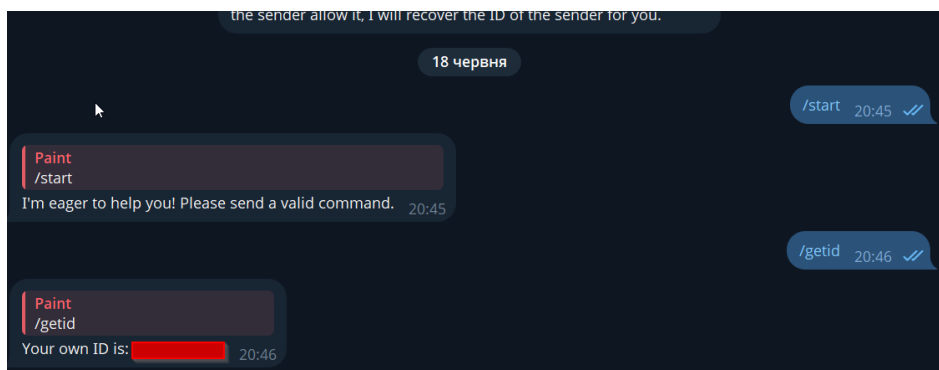


Рисунок 3.38 – Отримання айді свого чату для налаштування відправки сповіщень через телеграм боту

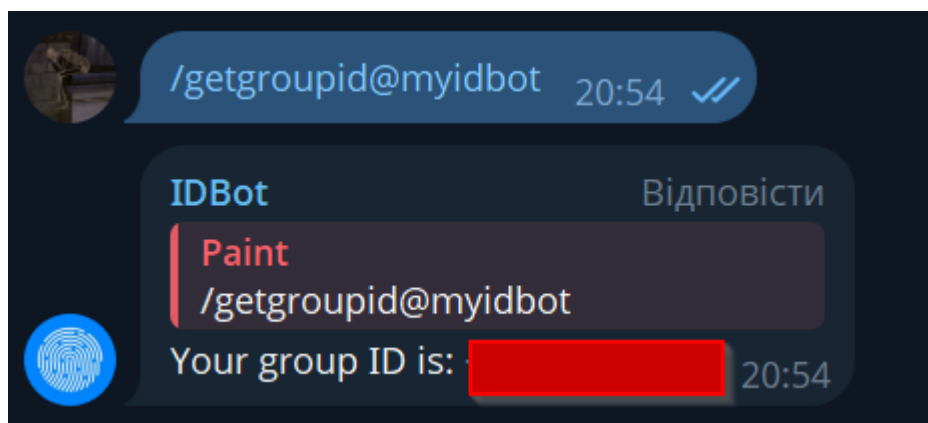


Рисунок 3.39 – Отримання групового айді для налаштування відправки сповіщень через телеграм боту

Перед налаштуванням сповіщень від Zabbix доцільно забезпечити захист Telegram-бота. Одним із важливих кроків є додавання секретного ключа в повідомлення, який підтверджує, що сповіщення надійшло від справжнього, офіційного Telegram-бота. Оскільки відправка повідомлень здійснюється через API-токен, який надається при створенні бота, цей токен є основним механізмом доступу до вашого бота. Важливо зберігати цей токен у безпечному місці і не надавати його стороннім особам. Тому доцільно використовувати захищене зберігання токена, наприклад, через змінні середовища або конфігураційні файли з належними правами доступу. Окрім того, важливою частиною захисту Telegram-бота є логування подій, що відбуваються при його використанні, що дозволяє відслідковувати всі операції та своєчасно реагувати на потенційні загрози.

Далі потрібно продовжити налаштування вже на самому Zabbix сервері а саме налаштувати сповіщення Telegram.

		Нероденко Д.О			ККІКБ.КР.Б – 125 – 10 – ПЗ	Арк.
		Покотило О.А				
Змн.	Арк.	№ докум.	Підпис	Дата		63

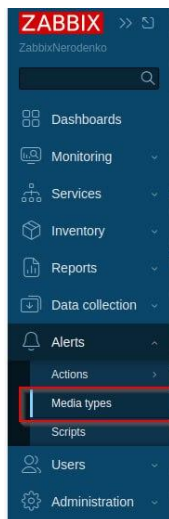


Рисунок 3.40 – Налаштування боту для сповіщень

☐	Mattermost	Webhook	Disabled	Report not supported items, Report not supported low level discovery rules, Report problems to Zabbix administrators, Report unknown triggers	Test
☐	MS Teams	Webhook	Disabled	Report not supported items, Report not supported low level discovery rules, Report problems to Zabbix administrators, Report unknown triggers	Test
☐	MS Teams Workflow	Webhook	Disabled	Report not supported items, Report not supported low level discovery rules, Report problems to Zabbix administrators, Report unknown triggers	Test
☐	Office365	Email	Disabled	Report not supported items, Report not supported low level discovery rules, Report problems to Zabbix administrators, Report unknown triggers	SMTP server: "smtp.office365.com", email: "zabbix@example.com"
☐	Office365 relay	Email	Disabled	Report not supported items, Report not supported low level discovery rules, Report problems to Zabbix administrators, Report unknown triggers	SMTP server: "example-com.mail.protection.outlook.com", email: "zabbix@example.com"
☐	Opsgenie	Webhook	Disabled	Report not supported items, Report not supported low level discovery rules, Report problems to Zabbix administrators, Report unknown triggers	Test
☐	OTRS CE	Webhook	Disabled	Report not supported items, Report not supported low level discovery rules, Report problems to Zabbix administrators, Report unknown triggers	Test
☐	PagerDuty	Webhook	Disabled	Report not supported items, Report not supported low level discovery rules, Report problems to Zabbix administrators, Report unknown triggers	Test
☐	Pushover	Webhook	Disabled	Report not supported items, Report not supported low level discovery rules, Report problems to Zabbix administrators, Report unknown triggers	Test
☐	Redmine	Webhook	Disabled	Report not supported items, Report not supported low level discovery rules, Report problems to Zabbix administrators, Report unknown triggers	Test
☐	Rocket.Chat	Webhook	Disabled	Report not supported items, Report not supported low level discovery rules, Report problems to Zabbix administrators, Report unknown triggers	Test
☐	ServiceNow	Webhook	Disabled	Report not supported items, Report not supported low level discovery rules, Report problems to Zabbix administrators, Report unknown triggers	Test
☐	SIGNAL4	Webhook	Disabled	Report not supported items, Report not supported low level discovery rules, Report problems to Zabbix administrators, Report unknown triggers	Test
☐	Slack	Webhook	Disabled	Report not supported items, Report not supported low level discovery rules, Report problems to Zabbix administrators, Report unknown triggers	Test
☐	SMS	SMS	Disabled	Report not supported items, Report not supported low level discovery rules, Report problems to Zabbix administrators, Report unknown triggers	GSM modem: "Idvity50"
☐	SolarWinds Service Desk	Webhook	Disabled	Report not supported items, Report not supported low level discovery rules, Report problems to Zabbix administrators, Report unknown triggers	Test
☐	SysAid	Webhook	Disabled	Report not supported items, Report not supported low level discovery rules, Report problems to Zabbix administrators, Report unknown triggers	Test
☐	Telegram	Webhook	Enabled	Report not supported items, Report not supported low level discovery rules, Report problems to Zabbix administrators, Report unknown triggers	Test
☐	TOPdesk	Webhook	Disabled	Report not supported items, Report not supported low level discovery rules, Report problems to Zabbix administrators, Report unknown triggers	Test
☐	VictorOps	Webhook	Disabled	Report not supported items, Report not supported low level discovery rules, Report problems to Zabbix administrators, Report unknown triggers	Test
☐	Zammad	Webhook	Disabled	Report not supported items, Report not supported low level discovery rules, Report problems to Zabbix administrators, Report unknown triggers	Test
☐	Zendesk	Webhook	Disabled	Report not supported items, Report not supported low level discovery rules, Report problems to Zabbix administrators, Report unknown triggers	Test

Рисунок 3.41 – Налаштування боту для сповіщень

Media type

Media type
Message templates 10
Options

Name Telegram
Type Webhook

Parameters

alert_message	{ALERT.MESSAGE}	Remove
alert_subject	{ALERT.SUBJECT}	Remove
api_chat_id	1	Remove
api_parse_mode	<PLACE_PARSE_MODE>	Remove
api_token	2	Remove
event_nseverity	{EVENT.NSEVERITY}	Remove
event_severity	{EVENT.SEVERITY}	Remove
event_source	{EVENT.SOURCE}	Remove
event_tags	{EVENT.TAGS.JSON}	Remove
event_update_nseverity	{EVENT.UPDATE.NSEVERITY}	Remove
event_update_severity	{EVENT.UPDATE.SEVERITY}	Remove
event_update_status	{EVENT.UPDATE.STATUS}	Remove
event_value	{EVENT.VALUE}	Remove

Add

Script const CLogger = function(serviceName) {
Timeout 30s

Update Clone Delete Cancel

Рисунок 3.42 – Налаштування боту для сповіщень

- В поле ID чату вставляємо токен який ми отримали при виконанні команди, дивитися рисунок 3.31.
- Цей API токен ми отримали при створенні боту, дивитися рисисунок 3.35.

Test media type "Telegram"

Media type test successful.

alert_message: Alarm!

alert_subject: Test.Subj

api_chat_id: [REDACTED]

api_parse_mode: <PLACE PARSE MODE>

api_token: [REDACTED]

event_nseverity: {EVENT.NSEVERITY}

event_severity: {EVENT.SEVERITY}

event_source: 1

event_tags: []

event_update_nseverity: {EVENT.UPDATE.NSEVERITY}

event_update_severity: {EVENT.UPDATE.SEVERITY}

event_update_status: {EVENT.UPDATE.STATUS}

event_value: {EVENT.VALUE}

Response: { "tags": { "telegram_msg_id": "4899655069": 9 } }

Response type: JSON

Test Cancel

Рисунок 3.43 – Тестування боту для сповіщень

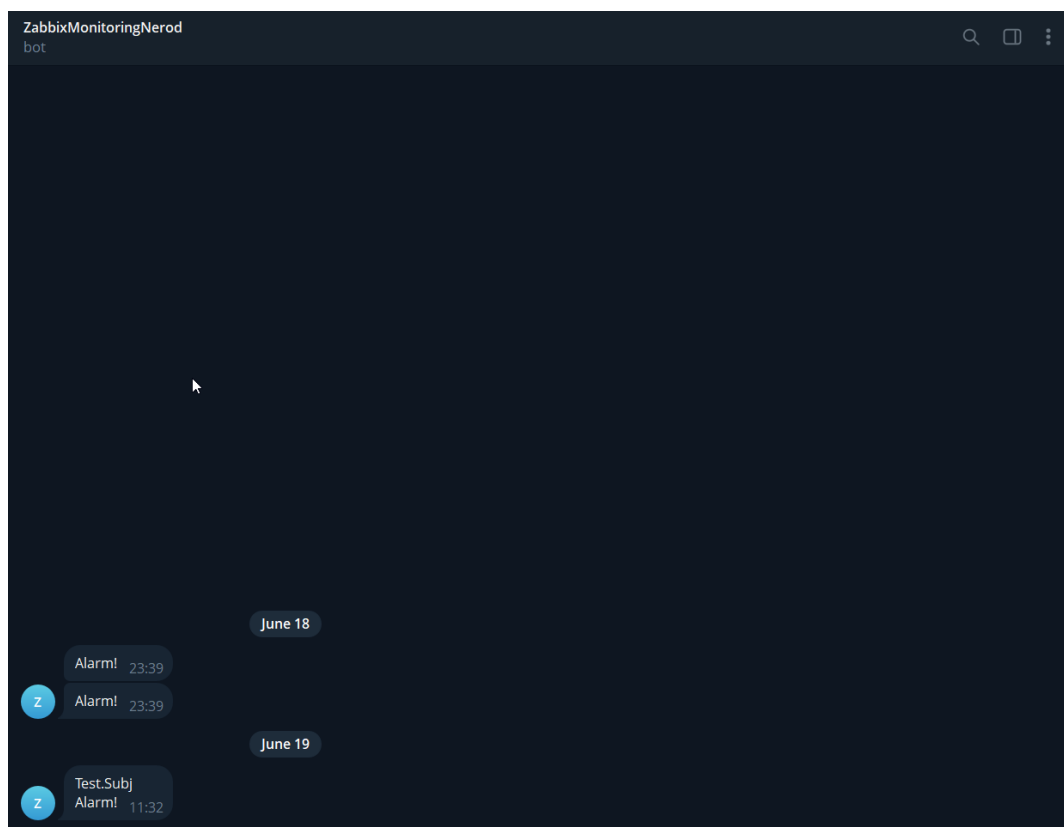


Рисунок 3.44 – Тестування боту успішне

		Нероденко Д.О			ККІКБ.КР.Б – 125 – 10 – ПЗ	Арк.
		Покотило О.А				
Змн.	Арк.	№ докум.	Підпис	Дата		65

Далі налаштовуємо сповіщення до певних груп та юзерів.

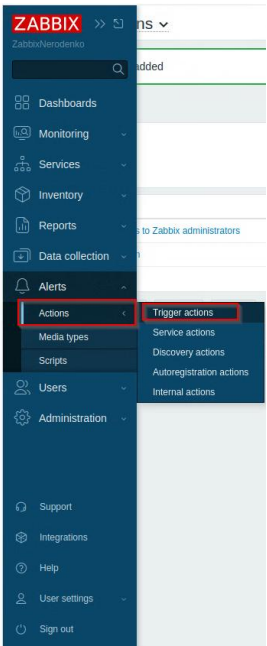


Рисунок 3.45 – Налаштування сповіщень та отримувачів

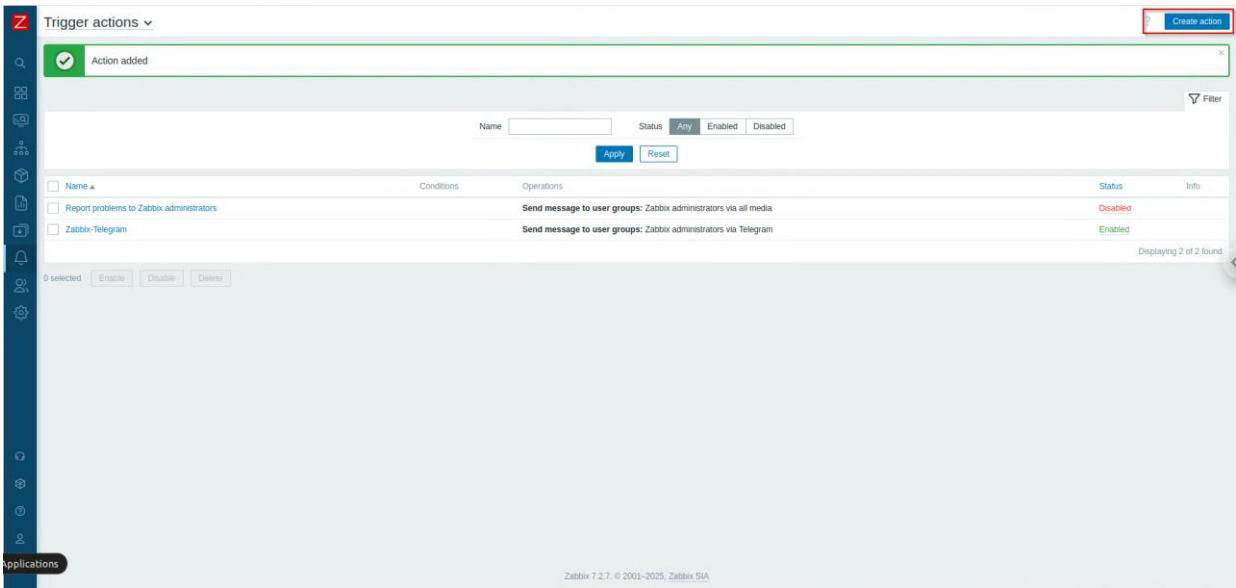


Рисунок 3.46 – Створення дії

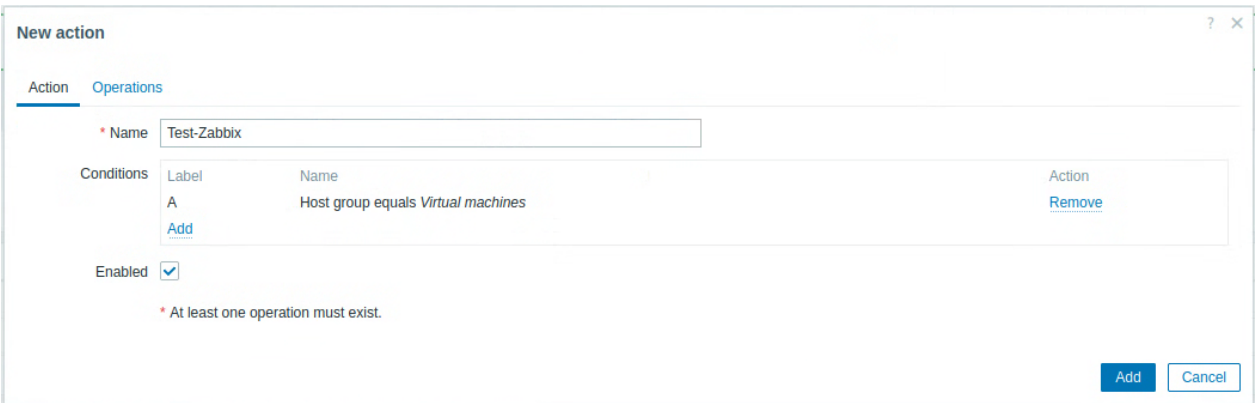


Рисунок 3.47 – Налаштування дії

Operation details

Operation

Send message

Steps

1 - 1

(0 - infinitely)

Step duration

0

(0 - use action default)

At least one user or user group must be selected.

Send to user groups

Zabbix administrators

type here to search

Select

Send to users

TestTelegram

type here to search

Select

Send to media type

Telegram

Custom message

Conditions

Label

Name

Action

Add

Add

Cancel

Рисунок 3.48 – Налаштування груп отримувачів а також юзерів які будуть отримувати сповіщення

Trigger actions

Action added

Name

Report problems to Zabbix administrators

Zabbix-Telegram

0 selected

Enable

Disable

Delete

New action

Default operation step duration

1m

Operations

Steps

Details

Start in

Duration

Actions

1

Send message to users: TestTelegram via Telegram

Send message to user groups: Zabbix administrators via Telegram

Add

Recovery operations

Details

Actions

Add

Update operations

Details

Actions

Add

Pause operations for symptom problems

☒

Pause operations for suppressed problems

☒

Notify about canceled escalations

☒

At least one operation must exist.

Add

Cancel

Рисунок 3.49 – Налаштування дії

Media

Type

Telegram

Send to

When active

1-7,00:00-24:00

Use if severity

☒ Not classified
 ☒ Information
 ☒ Warning
 ☒ Average
 ☒ High
 ☒ Disaster

Enabled

☒

Add

Cancel

Рисунок 3.50 – Налаштування доступу сповіщень користувачеві Admin

		Нероденко Д.О			ККІКБ.КР.Б – 125 – 10 – ПЗ	Арк.
		Покотило О.А				67
Змн.	Арк.	№ докум.	Підпис	Дата		

Для перевірки було створено перевірку з'єднання локальної мережі з глобальною мережею шляхом пінгу 8.8.8.8 або google.com.

Рисунок 3.51 – Створена перевірка з'єднання

Зараз проблем немає з перевіркою але якщо ми вимкнемо доступ до глобальної мережі шляхом вимкнення порту G3/0(підключення NAT) на MainRouter або змінимо адресу в перевірці то нас повідомлять про те що немає зв'язку з глобальною мережею.

Рисунок 3.52 – Симуляція недоступності до глобальної мережі

		Нероденко Д.О			ККІКБ.КР.Б – 125 – 10 – ПЗ	Арк.
		Покотило О.А				
Змн.	Арк.	№ докум.	Підпис	Дата		68

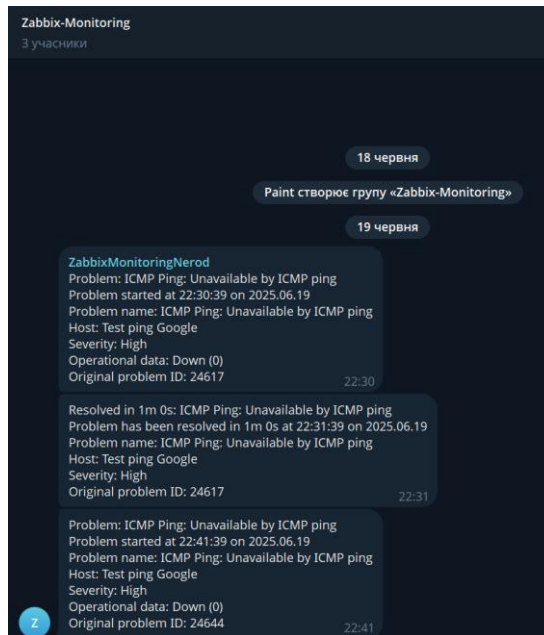


Рисунок 3.53 – Сповіщення про те що немає зв’язку з глобальною мережею

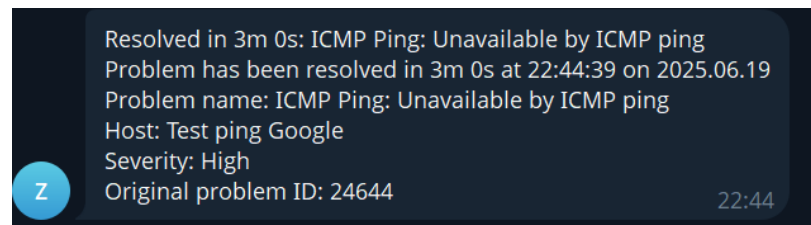


Рисунок 3.54 – Сповіщення про вирішення проблеми з мережею

Задля наглядності я вирішив ввімкнути робочі станції так як проблеми з робочими станціями теж надсилаються в чат телеграм ботом[13].

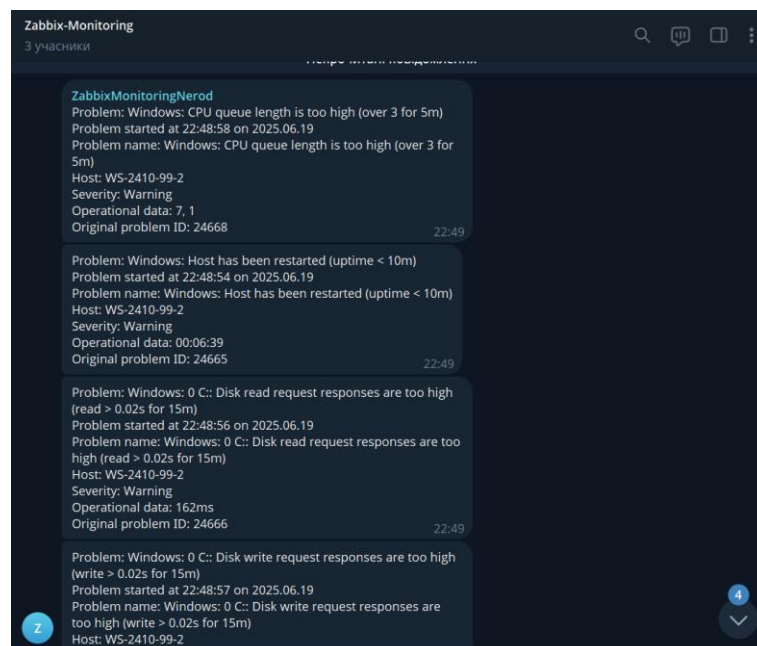


Рисунок 3.55 – Сповіщення про проблеми з робочими станціями

		Нероденко Д.О			ККІКБ.КР.Б – 125 – 10 – ПЗ	Арк.
		Покотило О.А				69
Змн.	Арк.	№ докум.	Підпис	Дата		

Після отримання сповіщення про проблему, наприклад, спрацювання тригера на високий рівень завантаження процесора або недостатнє місце на жорсткому диску, та надсилання відповідного повідомлення в Telegram, адміністратор повинен виконати наступні кроки:

Перевірити, який обсяг даних займає диск, використовуючи інструменти для аналізу дискового простору. Для систем на базі Linux можна використовувати команди `df` або `du`. У випадку з Windows адміністратор може звернутися до Провідника або скористатися утилітами для аналізу диска, такими як TreeSize або CCleaner, які точно вкажуть, які файли займають найбільше місця.

Після визначення причини заповнення диска адміністратор має кілька варіантів для вирішення проблеми:

- Перенесення великих або застарілих файлів на інші диски чи пристрої.
- Очищення застарілих або непотрібних файлів для звільнення простору.
- Замінити поточний диск на диск з більшою ємністю (хоча цей варіант є складнішим для екстреного виконання, тому рекомендується вибирати перші два варіанти).

Після виконання зазначених дій адміністратор отримає підтвердження про вирішення проблеми та звільнення місця на диску.

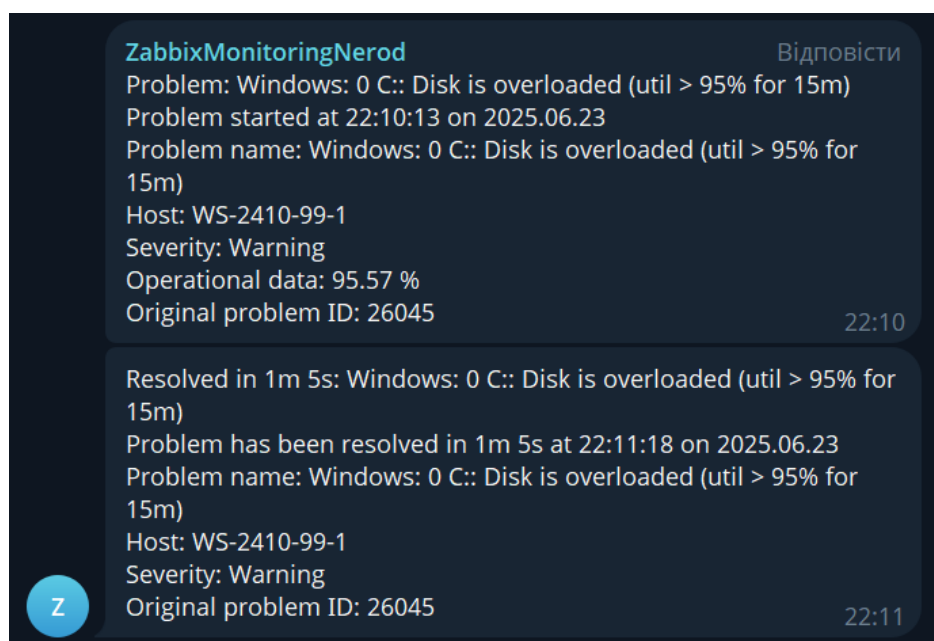


Рисунок 3.56 – Приклад сповіщення про нестачу місця на комп’ютері або сервері та вирішення цієї проблеми

		Нероденко Д.О			ККІКБ.КР.Б – 125 – 10 – ПЗ	Арк.
		Покотило О.А				70
Змн.	Арк.	№ докум.	Підпис	Дата		

Проаналізувавши сповіщення, можна швидко зрозуміти його зміст. Розглянемо сповіщення про помилку (рис. 3.56, перше повідомлення).

Перш за все, ми бачимо назву проблеми — Windows 0 C:: Disk is overloaded, а також інформацію про те, що диск заповнений більше ніж на 95%. Такий лаконічний запис дозволяє адміністратору швидко визначити суть проблеми та вжити необхідних заходів для її вирішення.

Час початку проблеми в даному випадку — 23.06.2025 о 22:10:13. Цей пункт є важливим для ведення документації щодо поломок або надзвичайних ситуацій, якщо така документація ведеться в організації.

Наступний пункт у повідомленні є аналогічним до першого — він містить назву хосту, на якому сталася проблема, в нашому випадку це WS-2410-99-1.

Severity (рівень критичності) вказує на ступінь серйозності проблеми, що дає змогу оцінити важливість інциденту.

ID проблеми — це унікальний ідентифікатор, що допомагає відстежувати конкретне сповіщення.

Тепер розглянемо сповіщення про вирішення цієї проблеми (рис. 3.56, друге повідомлення).

Перше, що ми бачимо — це час вирішення проблеми. У нашому випадку, проблема була вирішена за 1 хвилину 5 секунд. Далі йде назва проблеми.

Також зазначено, за який час була вирішена проблема та дата і час вирішення: 23.06.2025 о 22:11:18.

Знову ж таки, повторюється інформація про хост, на якому проблема була вирішена, рівень критичності та ID помилки.

Отже, сповіщення через Zabbix та Telegram-бота дозволяють адміністратору оперативно отримувати чітку інформацію про виникнення проблем і швидко реагувати на них, що значно підвищує ефективність моніторингу і управління системою.

		Нероденко Д.О			ККІКБ.КР.Б – 125 – 10 – ПЗ	Арк.
		Покотило О.А				
Змн.	Арк.	№ докум.	Підпис	Дата		71

Висновок до третього розділу

У третьому розділі розглянуто практичне застосування технологій моніторингу мережі в комп'ютерних мережах, що є важливим етапом забезпечення стабільної роботи і безпеки інформаційних систем.

Одним з основних аспектів розділу стало застосування системи Zabbix, яка є одним із найбільш потужних і популярних інструментів для моніторингу мереж. Важливим етапом стало описання процесу встановлення та налаштування Zabbix Server, Zabbix Agent і SNMPv2, що дозволяє забезпечити збір, обробку та аналіз мережевих даних у реальному часі. Особливу увагу було приділено автоматичному виявленню нових пристроїв у мережі за допомогою ICMP ping, що дозволяє значно спростити процес адміністрування та інтеграції нових елементів мережі в систему моніторингу.

Система Zabbix за допомогою детального налаштування сповіщень через Telegram, здатна своєчасно інформувати адміністраторів про проблеми, які можуть виникнути в мережі, наприклад, про вимкнення важливих робочих станцій або серверів. Це дозволяє зменшити час реагування на проблеми і забезпечує надійність роботи мережі. Використання такого підходу до моніторингу дає змогу не лише підтримувати працездатність мережі, а й гарантувати її безпеку, своєчасно реагуючи на загрози, що можуть з'явитися в процесі її функціонування. Також було проаналізовано повідомлення про проблеми з робочою станцією та дії які має зробити адміністратор задля її усунення.

		Нероденко Д.О			ККІКБ.КР.Б – 125 – 10 – ПЗ	Арк.
		Покотило О.А				
Змн.	Арк.	№ докум.	Підпис	Дата		72

ВИСНОВКИ

У кваліфікаційній роботі було розглянуто проєкт підсистеми моніторингу мережі на базі технології Zabbix, яка є одним із найпопулярніших інструментів для моніторингу комп'ютерних мереж. Метою роботи було розробити систему, здатну централізовано збирати та аналізувати дані про стан мережевої інфраструктури в реальному часі, що є важливим етапом для забезпечення стабільної роботи інформаційних систем.

Зосереджено увагу на використанні Zabbix як основного інструменту моніторингу. Ця система забезпечує ефективний збір та аналіз даних, що дозволяє оперативно реагувати на проблеми та підвищити надійність мережі.

Особливу увагу було приділено проектуванню мережі з використанням сучасних технологій, таких як VLAN, RSTP, TRUNK і NAT, що дозволяють створити надійну та безпечну мережеву інфраструктуру, зменшити навантаження на окремі сегменти мережі і підвищити її безпеку.

Практична частина роботи зосереджена на налаштуванні Zabbix для моніторингу мережі, включаючи етапи встановлення серверу та агентів, налаштування SNMPv2 для моніторингу мережевих пристроїв та автоматичне виявлення нових пристроїв через ICMP ping. Також було реалізовано налаштування сповіщень, що дозволяють оперативно інформувати адміністраторів про виникнення проблем у мережі.

Розроблена підсистема моніторингу також сприяє автоматизації процесів виявлення і усунення несправностей, що значно знижує час простою мережі та підвищує ефективність роботи організації. У майбутньому можна розглянути можливість інтеграції цієї системи з іншими інструментами для ще більшого розширення функціоналу моніторингу та управління інфраструктурою.

В результаті виконаної роботи було підтверджено важливість застосування сучасних технологій моніторингу для забезпечення стабільної роботи та безпеки мереж. Розроблене рішення є адаптованим до різних типів організацій і може використовуватися для покращення управління інфраструктурою, що сприяє підвищенню стабільності та безпеки мережі.

		Нероденко Д.О			ККІКБ.КР.Б – 125 – 10 – ПЗ	Арк.
		Покотило О.А				73
Змн.	Арк.	№ докум.	Підпис	Дата		

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Zabbix Посібник [Електронний ресурс] – Режим доступу: <https://www.zabbix.com/documentation/current/en/manual>
2. Monitor Linux with Zabbix agent [Електронний ресурс] – Режим доступу: https://www.zabbix.com/documentation/current/en/manual/guides/monitor_linux
3. Zabbix: What It Is and How to Use It [Електронний ресурс] – Режим доступу: <https://alexhost.com/faq/zabbix-what-it-is-and-how-to-use-it/>
4. Top 10 Network Monitoring Tools for 2025: Enhance Your Network Performance [Електронний ресурс] – Режим доступу: <https://uptrace.dev/tools/network-monitoring-tools>
5. The Best Network Monitoring Software and Tools [Електронний ресурс] – Режим доступу: <https://www.comparitech.com/net-admin/network-monitoring-tools/>
6. What is network monitoring? [Електронний ресурс] – Режим доступу: <https://www.techtarget.com/searchnetworking/definition/network-monitoring>
7. Network Monitoring [Електронний ресурс] – Режим доступу: <https://www.fortinet.com/resources/cyberglossary/network-monitoring>
8. What is network monitoring? [Електронний ресурс] – Режим доступу: <https://www.ibm.com/think/topics/network-monitoring>
9. Таненбаум Е., Везеролл Д. Комп'ютерні мережі. — 5-е вид., Київ: Діалектика, 2014. — 960 с. [Електронний ресурс]
10. Поняття VLAN, Trunk та протоколи VTP і DTP: [Електронний ресурс] – <https://surl.li/uhnjdj>
11. David Bombal., GNS3 Talks: Use the NAT node to connect GNS3 to the Internet easily! [Електронний ресурс] – <https://www.youtube.com/watch?v=2zeoC2Q4mW0>
12. Roei Hazout ., Rapid Spanning Tree Protocol (RSTP) [Електронний ресурс] – [https://www.ioriver.io/terms/rapid-spanning-tree-protocol#:~:text=Rapid%20Spanning%20Tree%20Protocol%20\(RSTP\)%20is%2](https://www.ioriver.io/terms/rapid-spanning-tree-protocol#:~:text=Rapid%20Spanning%20Tree%20Protocol%20(RSTP)%20is%2)

		Нероденко Д.О			ККІКБ.КР.Б – 125 – 10 – ПЗ	Арк.
		Покотило О.А				74
Змн.	Арк.	№ докум.	Підпис	Дата		

[0a%20network%20protocol%20used,convergence%2C%20stability%2C%20and%20efficiency.](#)

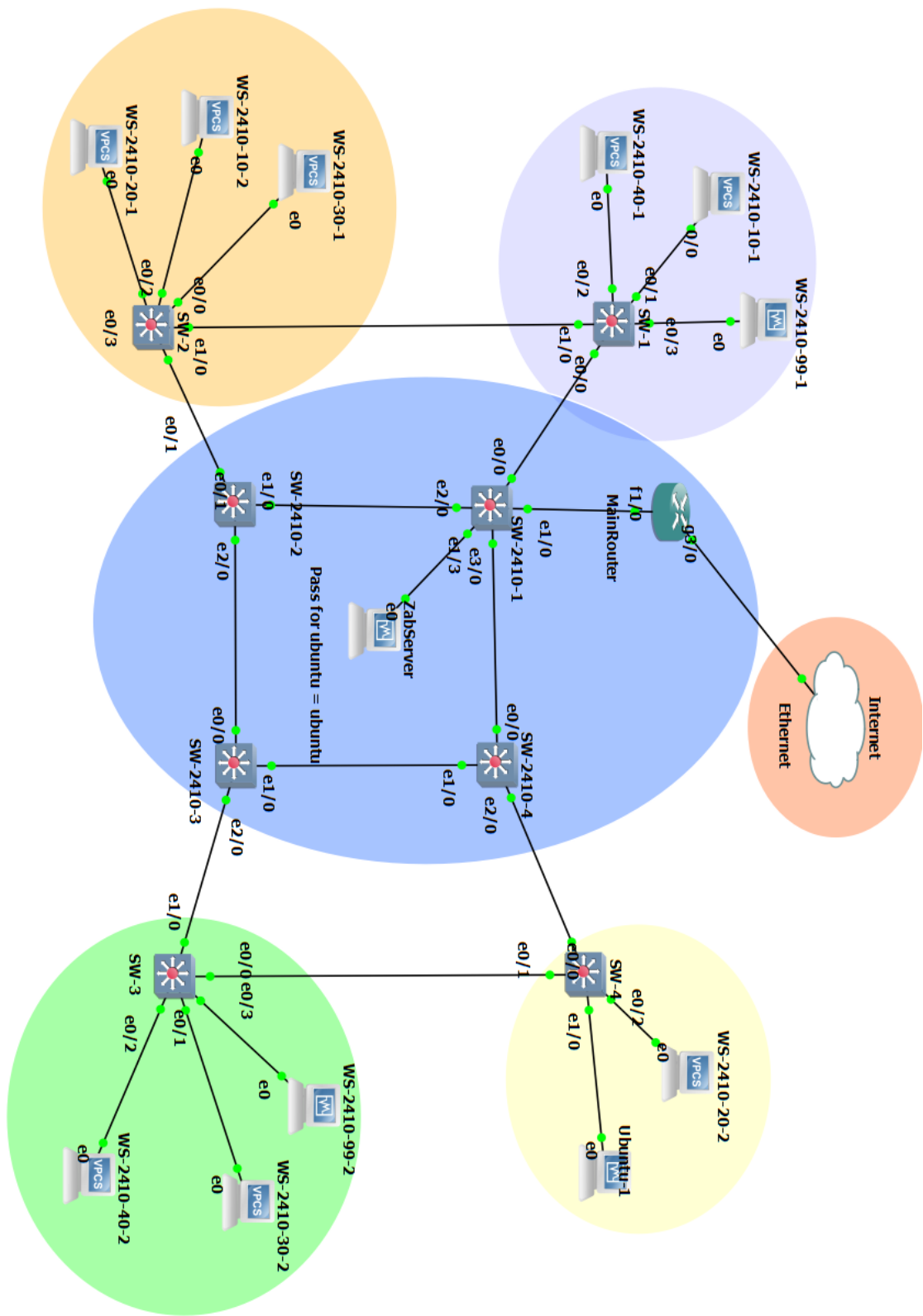
13. Zabbix + Telegram [Електронний ресурс] – Режим доступу: https://www.zabbix.com/integrations/telegram?utm_source=chatgpt.com
14. Zabbix Documentation [Електронний ресурс] – Режим доступу: <https://www.zabbix.com/documentation/current/en/>
15. Zabbix Network Monitoring [Електронний ресурс] – Режим доступу: https://books.google.com.ua/books?hl=ru&lr=&id=xgjVDQAAQBAJ&oi=fnd&pg=PP1&dq=Zabbix&ots=zSDflnL2jm&sig=msYHukS6CJW93MGQI4nJpOZS99U&redir_esc=y#v=onepage&q&f=true
16. ToTatCa: Zabbix - How to Send Zabbix Alerts to Telegram - Step-by-Step Guide [Електронний ресурс] – Режим доступу: <https://www.youtube.com/watch?v=mEV9TRMl6rk&t=325s>
17. Zabbix integration [Електронний ресурс] – Режим доступу: <https://www.zabbix.com/integrations>
18. НАЛАГОДЖЕННЯ ТА ДОСЛІДЖЕННЯ РОБОТИ ПРОТОКОЛУ RIPv2+ У МЕРЕЖІ НА БАЗІ КОМУТАТОРІВ CISCO [Електронний ресурс] – Режим доступу: <https://learn.ztu.edu.ua/mod/resource/view.php?id=240766>
19. Software Configuration Guide - Configuring VLAN Trunks [Електронний ресурс] – Режим доступу: https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst_digital_building_series_switches/software/15-2_5_ex/configuration_guide/b_1525ex_consolidated_cdb_cg/b_1525ex_consolidated_cdb_cg_chapter_0110101.pdf
20. Андрій Єфіменко., Лекція №14 налаштування NAT: [Електронний ресурс] – Режим доступу: <https://drive.google.com/file/d/1zW-bPFXGPAeJtyiH9ZXtYsHYmzWswrvs/view>

		Нероденко Д.О.			ККІКБ.КР.Б – 125 – 10 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		75

ДОДАТКИ

		Нероденко Д.О			ККІКБ.КР.Б – 125 – 10 – ПЗ	Арк.
		Покотило О.А				
Змн.	Арк.	№ докум.	Підпис	Дата		76

Повна схема мережі



		Нероденко Д.О		
		Покотило О.А		
Змн.	Арк.	№ докум.	Підпис	Дата

!	!	encapsulation dot1Q 30
!	!	ip address 192.24.30.1
!	!	255.255.255.0
!	!	ip nat inside
!	!	ip virtual-reassembly
!	!	!
!	!	interface FastEthernet1/0.40
upgrade fpd auto	archive	encapsulation dot1Q 40
version 12.4	log config	ip address 192.24.40.1
service timestamps debug	hidekeys	255.255.255.0
datetime msec	!	ip nat inside
service timestamps log	!	ip virtual-reassembly
datetime msec	!	!
no service password-	!	interface FastEthernet1/0.99
encryption	!	encapsulation dot1Q 99
!	ip tcp synwait-time 5	ip address 192.24.99.1
hostname MainRouter	!	255.255.255.0
!	!	ip nat inside
boot-start-marker	!	ip virtual-reassembly
boot-end-marker	!	!
!	interface FastEthernet0/0	interface FastEthernet1/1
logging message-counter	no ip address	no ip address
syslog	shutdown	ip nat inside
!	duplex half	ip virtual-reassembly
no aaa new-model	!	duplex auto
ip source-route	interface FastEthernet1/0	speed auto
no ip icmp rate-limit	no ip address	!
unreachable	ip nat inside	interface FastEthernet2/0
ip cef	ip virtual-reassembly	no ip address
!	duplex auto	shutdown
!	speed auto	duplex half
!	!	!
!	interface FastEthernet1/0.10	interface GigabitEthernet3/0
ip name-server 8.8.8.8	encapsulation dot1Q 10	ip address dhcp
no ipv6 cef	ip address 192.24.10.1	ip nat outside
!	255.255.255.0	ip virtual-reassembly
multilink bundle-name	ip nat inside	negotiation auto
authenticated	ip virtual-reassembly	!
!	!	ip forward-protocol nd
!	interface FastEthernet1/0.20	no ip http server
!	encapsulation dot1Q 20	no ip http secure-server
!	ip address 192.24.20.1	!
!	255.255.255.0	!
!	ip nat inside	ip nat inside source list 1
!	ip virtual-reassembly	interface GigabitEthernet3/0
!	!	overload
!	interface FastEthernet1/0.30	!

		Нероденко Д.О			ККІКБ.КР.Б – 125 – 10 – ПЗ	Арк.
		Покотило О.А				78
Змн.	Арк.	№ докум.	Підпис	Дата		

access-list 1 permit any	!	!
no cdp log mismatch duplex	hostname SW-1	interface Ethernet0/0
!	!	switchport trunk allowed
!	boot-start-marker	vlan 10,20,30,40,99
!	boot-end-marker	switchport trunk encapsula-
!	!	tion dot1q
!	!	switchport mode trunk
snmp-server community	logging discriminator EX-	!
public RO	CESS severity drops 6 msg-	interface Ethernet0/1
!	body drops EXCESSCOLL	switchport access vlan 10
control-plane	logging buffered 50000	switchport mode access
!	logging console discrimina-	spanning-tree portfast edge
!	tor EXCESS	!
!	!	interface Ethernet0/2
!	no aaa new-model	switchport access vlan 40
!	!	switchport mode access
!	!	spanning-tree portfast edge
!	!	!
gatekeeper	!	interface Ethernet0/3
shutdown	!	switchport access vlan 99
!	no ip icmp rate-limit un-	switchport mode access
!	reachable	spanning-tree portfast edge
line con 0	!	!
exec-timeout 0 0	!	interface Ethernet1/0
privilege level 15	!	switchport trunk allowed
logging synchronous	no ip domain-lookup	vlan 10,20,30,40,99
stopbits 1	no ip cef	switchport trunk encapsula-
line aux 0	no ipv6 cef	tion dot1q
exec-timeout 0 0	!	switchport mode trunk
privilege level 15	!	!
logging synchronous	!	interface Ethernet1/1
stopbits 1	spanning-tree mode rapid-	!
line vty 0 4	pvst	interface Ethernet1/2
login	spanning-tree extend system-	!
!	id	interface Ethernet1/3
End	!	!
	vlan internal allocation pol-	interface Ethernet2/0
	icy ascending	!
	!	interface Ethernet2/1
SW-1:	ip tcp synwait-time 5	!
!	!	interface Ethernet2/2
! Last configuration change	!	!
at 00:14:00 UTC Fri May 23	!	interface Ethernet2/3
2025	!	!
!	!	interface Ethernet3/0
version 15.2	!	!
service timestamps debug	!	interface Ethernet3/1
datetime msec	!	!
service timestamps log	!	interface Ethernet3/2
datetime msec	!	!
no service password-encryp-	!	interface Ethernet3/3
tion	!	!
service compress-config	!	!

		Нероденко Д.О			ККІКБ.КР.Б – 125 – 10 – ПЗ	Арк.
		Покотило О.А				
Змн.	Арк.	№ докум.	Підпис	Дата		5

interface Vlan1	!	logging synchronous
no ip address	!	line aux 0
shutdown	!	exec-timeout 0 0
!	!	privilege level 15
ip forward-protocol nd	control-plane	logging synchronous
!	!	line vty 0 4
!	!	login
no ip http server	line con 0	!
no ip http secure-server	exec-timeout 0 0	!
!	privilege level 15	
End		
SW-2:		
!	no ipv6 cef	spanning-tree portfast edge
! Last configuration change	!	!
at 00:15:44 UTC Fri May 23	!	interface Ethernet0/3
2025	!	switchport access vlan 20
!	spanning-tree mode pvst	switchport mode access
version 15.2	spanning-tree extend system-	spanning-tree portfast edge
service timestamps debug	id	!
datetime msec	!	interface Ethernet1/0
service timestamps log	vlan internal allocation pol-	switchport trunk allowed
datetime msec	icy ascending	vlan 10,20,30,40,99
no service password-encryp-	!	switchport trunk encapsula-
tion	ip tcp synwait-time 5	tion dot1q
service compress-config	!	switchport mode trunk
!	!	!
hostname SW-2	!	interface Ethernet1/1
!	!	!
boot-start-marker	!	interface Ethernet1/2
boot-end-marker	!	!
!	!	interface Ethernet1/3
!	!	!
logging discriminator EX-	!	interface Ethernet2/0
CESS severity drops 6 msg-	!	!
body drops EXCESSCOLL	!	interface Ethernet2/1
logging buffered 50000	!	!
logging console discrimina-	!	interface Ethernet2/2
tor EXCESS	interface Ethernet0/0	!
!	switchport access vlan 30	interface Ethernet2/3
no aaa new-model	switchport mode access	!
!	spanning-tree portfast edge	interface Ethernet3/0
!	!	!
!	interface Ethernet0/1	interface Ethernet3/1
!	switchport trunk allowed	!
!	vlan 10,20,30,40,99	interface Ethernet3/2
no ip icmp rate-limit un-	switchport trunk encapsula-	!
reachable	tion dot1q	interface Ethernet3/3
!	switchport mode trunk	!
!	!	interface Vlan1
!	interface Ethernet0/2	no ip address
no ip domain-lookup	switchport access vlan 10	shutdown
no ip cef	switchport mode access	!

		Нероденко Д.О			<i>ККИКБ.КР.Б – 125 – 10 – ПЗ</i>	Арк.
		Покотило О.А				6
Змн.	Арк.	№ докум.	Підпис	Дата		

interface Vlan99	!	line aux 0
no ip address	!	exec-timeout 0 0
!	!	privilege level 15
ip forward-protocol nd	control-plane	logging synchronous
!	!	line vty 0 4
!	!	login
no ip http server	line con 0	!
no ip http secure-server	exec-timeout 0 0	!
!	privilege level 15	end
!	logging synchronous	

		Нероденко Д.О			ККІКБ.КР.Б – 125 – 10 – ПЗ	Арк.
		Покотило О.А				5
Змн.	Арк.	№ докум.	Підпис	Дата		

SW-3:

!
! Last configuration change
at 23:38:17 UTC Thu May
22 2025
!
version 15.2
service timestamps debug
datetime msec
service timestamps log
datetime msec
no service password-encryp-
tion
service compress-config
!
hostname SW-3
!
boot-start-marker
boot-end-marker
!
!
logging discriminator EX-
CESS severity drops 6 msg-
body drops EXCESSCOLL
logging buffered 50000
logging console discrimina-
tor EXCESS

!
no aaa new-model
!
!
!
!
no ip icmp rate-limit un-
reachable
!
!
!
no ip domain-lookup
no ip cef
no ipv6 cef
!
!
spanning-tree mode rapid-

vlan internal allocation pol-
icy ascending
!

ip tcp synwait-time 5
!
!
!
!
!
!
!
!
interface Ethernet0/0
switchport trunk allowed
vlan 10,20,30,40,99
switchport trunk encapsula-
tion dot1q
switchport mode trunk
!
interface Ethernet0/1
switchport access vlan 30
switchport mode access

spanning-tree portfast edge
!
interface Ethernet0/2
switchport access vlan 40
switchport mode access
spanning-tree portfast edge
!
interface Ethernet0/3
switchport access vlan 99
switchport mode access
spanning-tree portfast edge
!
interface Ethernet1/0
switchport trunk allowed
vlan 10,20,30,40,99
switchport trunk encapsula-
tion dot1q
switchport mode trunk
!
interface Ethernet1/1
switchport trunk allowed
vlan 10,20,30,40,99
switchport trunk encapsula-
tion dot1q
switchport mode trunk
!
interface Ethernet1/2
switchport access vlan 10
switchport mode access
spanning-tree portfast edge
!
interface Ethernet1/3
switchport access vlan 20
switchport mode access
spanning-tree portfast edge
!
interface Ethernet2/0
switchport access vlan 30
switchport mode access
spanning-tree portfast edge
!
interface Ethernet2/1
switchport access vlan 40
switchport mode access
spanning-tree portfast edge
!
interface Ethernet2/2
switchport access vlan 99
switchport mode access
spanning-tree portfast edge
!
interface Ethernet2/3
switchport access vlan 10
switchport mode access
spanning-tree portfast edge
!
interface Ethernet3/0
switchport access vlan 20
switchport mode access
spanning-tree portfast edge
!
interface Ethernet3/1
switchport access vlan 30
switchport mode access
spanning-tree portfast edge
!
interface Ethernet3/2
switchport access vlan 40
switchport mode access
spanning-tree portfast edge
!
interface Ethernet3/3
switchport access vlan 99
switchport mode access
spanning-tree portfast edge
!
interface Vlan1
no ip address
shutdown
!
interface Vlan99
ip address 192.24.99.5
255.255.255.0
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
!
!
!
!
control-plane
!
!
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
line vty 0 4
exec-timeout 0 0
privilege level 15
logging synchronous

Просте розроблення системи моніторингу мережі на базі технології Zabbix					ФІКТ, Гр. КБ-21-2		
Змні	Арк.	№ докум.	Підпис	Дата	Лім. стор.	Арк.	Аркушів
Розроб.	Нероденко Д.О						
Керівник	Покотило О.А						
Реценз.	Головня О.С						
Н. контр.	Покотило О.А						
Затверд.	Єфіменко А.А.						

!	!	interface Ethernet1/1
!	vlan internal allocation pol-	duplex full
End	icy ascending	!
SW-4:	!	interface Ethernet1/2
!	ip tcp synwait-time 5	duplex full
! Last configuration change	!	!
at 15:34:04 UTC Tue Jun 3	!	interface Ethernet1/3
2025	!	switchport access vlan 99
!	!	switchport mode access
version 15.2	!	duplex full
service timestamps debug	!	spanning-tree portfast edge
datetime msec	!	!
service timestamps log	!	interface Ethernet2/0
datetime msec	!	duplex full
no service password-encryp-	!	!
tion	!	interface Ethernet2/1
service compress-config	!	duplex full
!	!	!
hostname SW-4	interface Ethernet0/0	interface Ethernet2/2
!	switchport trunk allowed	duplex full
boot-start-marker	vlan 10,20,30,40,99	!
boot-end-marker	switchport trunk encapsula-	interface Ethernet2/3
!	tion dot1q	duplex full
!	switchport mode trunk	!
logging discriminator EX-	duplex full	interface Ethernet3/0
CESS severity drops 6 msg-	!	duplex full
body drops EXCESSCOLL	interface Ethernet0/1	!
logging buffered 50000	switchport trunk allowed	interface Ethernet3/1
logging console discrimina-	vlan 10,20,30,40,99	duplex full
tor EXCESS	switchport trunk encapsula-	!
!	tion dot1q	interface Ethernet3/2
no aaa new-model	switchport mode trunk	duplex full
!	duplex full	!
!	!	interface Ethernet3/3
!	interface Ethernet0/2	duplex full
!	switchport access vlan 20	!
!	switchport mode access	interface Vlan1
no ip icmp rate-limit un-	duplex full	no ip address
reachable	spanning-tree portfast edge	shutdown
!	!	!
!	interface Ethernet0/3	interface Vlan99
!	switchport access vlan 99	no ip address
no ip domain-lookup	switchport mode access	!
no ip cef	duplex full	ip forward-protocol nd
no ipv6 cef	spanning-tree portfast edge	!
!	!	!
!	interface Ethernet1/0	no ip http server
!	switchport access vlan 99	no ip http secure-server
spanning-tree mode rapid-	switchport mode access	!
pvst	duplex full	!
spanning-tree extend system-	spanning-tree portfast edge	!
id	!	!

		Нероденко Д.О.			ККІКБ.КР.Б – 125 – 10 – ПЗ	Арк.
		Покотило О.А				
Змн.	Арк.	№ докум.	Підпис	Дата		5

!	no ip icmp rate-limit un-	switchport trunk allowed
control-plane	reachable	vlan 10,20,30,40,99
!	!	switchport trunk encapsula-
!	!	tion dot1q
line con 0	!	switchport mode trunk
exec-timeout 0 0	no ip domain-lookup	!
privilege level 15	no ip cef	interface Ethernet1/1
logging synchronous	no ipv6 cef	!
line aux 0	!	interface Ethernet1/2
exec-timeout 0 0	!	!
privilege level 15	spanning-tree mode rapid-	interface Ethernet1/3
logging synchronous	pvst	switchport access vlan 10
line vty 0 4	spanning-tree extend system-	switchport mode access
login	id	spanning-tree portfast edge
!	!	!
!	!	interface Ethernet2/0
End	vlan internal allocation pol-	switchport trunk allowed
SW-2410-1:	icy ascending	vlan 10,20,30,40,99
!	!	switchport trunk encapsula-
! Last configuration change	ip tcp synwait-time 5	tion dot1q
at 23:39:02 UTC Thu May	!	switchport mode trunk
22 2025	!	!
!	!	interface Ethernet2/1
version 15.2	!	!
service timestamps debug	!	interface Ethernet2/2
datetime msec	!	switchport trunk allowed
service timestamps log	!	vlan 10,20,30,40,99
datetime msec	!	switchport trunk encapsula-
no service password-encryp-	!	tion dot1q
tion	!	switchport mode trunk
service compress-config	!	!
!	!	interface Ethernet2/3
hostname SW-2410-1	!	!
!	interface Ethernet0/0	interface Ethernet3/0
boot-start-marker	switchport trunk allowed	switchport trunk allowed
boot-end-marker	vlan 10,20,30,40,99	vlan 10,20,30,40,99
!	switchport trunk encapsula-	switchport trunk encapsula-
!	tion dot1q	tion dot1q
logging discriminator EX-	switchport mode trunk	switchport mode trunk
CESS severity drops 6 msg-	!	!
body drops EXCESSCOLL	interface Ethernet0/1	interface Ethernet3/1
logging buffered 50000	switchport access vlan 10	!
logging console discrimina-	switchport trunk allowed	interface Ethernet3/2
tor EXCESS	vlan 10,20,30,40,99	!
!	switchport mode access	interface Ethernet3/3
no aaa new-model	spanning-tree portfast edge	switchport access vlan 99
!	!	switchport mode access
!	interface Ethernet0/2	spanning-tree portfast edge
!	!	!
!	interface Ethernet0/3	interface Vlan1
!	!	no ip address
	interface Ethernet1/0	shutdown

		Нероденко Д.О.			ККІКБ.КР.Б – 125 – 10 – ПЗ	Арк.
		Покотило О.А				
Змн.	Арк.	№ докум.	Підпис	Дата		6

```
!
!
logging discriminator EX-
CESS severity drops 6 msg-
body drops EXCESSCOLL
logging buffered 50000
logging console discrimina-
tor EXCESS
!
no aaa new-model
!
!
!
!
!
no ip icmp rate-limit un-
reachable
!
!
!
no ip domain-lookup
no ip cef
no ipv6 cef
!
!
!
spanning-tree mode rapid-
pvst
spanning-tree extend system-
id
!
vlan internal allocation pol-
icy ascending
!
ip tcp synwait-time 5
!
!
!
!
!
!
!
!
!
!
!
interface Ethernet0/0
 switchport trunk allowed
 vlan 10,20,30,40,99
```

```

switchport trunk encapsula-
tion dot1q
switchport mode trunk
!
interface Ethernet0/1
!
interface Ethernet0/2
!
interface Ethernet0/3
!
interface Ethernet1/0
switchport trunk allowed
vlan 10,20,30,40,99
switchport trunk encapsula-
tion dot1q
switchport mode trunk
!
interface Ethernet1/1
!
interface Ethernet1/2
!
interface Ethernet1/3
!
interface Ethernet2/0
switchport trunk allowed
vlan 10,20,30,40,99
switchport trunk encapsula-
tion dot1q
switchport mode trunk
!
interface Ethernet2/1
!
interface Ethernet2/2
switchport trunk allowed
vlan 10,20,30,40,99
switchport trunk encapsula-
tion dot1q
switchport mode trunk
!
interface Ethernet2/3
!
interface Ethernet3/0
!
interface Ethernet3/1
!
interface Ethernet3/2
!
interface Ethernet3/3
!
interface Vlan1
no ip address
shutdown

```

		Нероденко Д.О.			ККІКБ.КР.Б – 125 – 10 – ПЗ	Арк.
		Покотило О.А				7
Змн.	Арк.	№ докум.	Підпис	Дата		

```

!
interface Vlan99
  no ip address
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
!
!
!
!
!
!
control-plane
!
!
line con 0
  exec-timeout 0 0
  privilege level 15
  logging synchronous
line aux 0
  exec-timeout 0 0
  privilege level 15
  logging synchronous
line vty 0 4
  login
!
!
End
SW-2410-3:
!
! Last configuration change
at 23:38:22 UTC Thu May
22 2025
!
version 15.2
service timestamps debug
datetime msec
service timestamps log
datetime msec
no service password-encryp-
tion
service compress-config
!
hostname SW-2410-3
!
boot-start-marker
boot-end-marker
!
!

```

```

logging discriminator EX-
CESS severity drops 6 msg-
body drops EXCESSCOLL
logging buffered 50000
logging console discrimina-
tor EXCESS
!
no aaa new-model
!
!
!
!
no ip icmp rate-limit un-
reachable
!
!
!
no ip domain-lookup
no ip cef
no ipv6 cef
!
!
!
spanning-tree mode rapid-
pvst
spanning-tree extend system-
id
!
vlan internal allocation pol-
icy ascending
!
ip tcp synwait-time 5
!
!
!
!
!
!
!
!
!
!
interface Ethernet0/0
  switchport trunk allowed
vlan 10,20,30,40,99
  switchport trunk encapsula-
tion dot1q
  switchport mode trunk

```

```

!
interface Ethernet0/1
!
interface Ethernet0/2
!
interface Ethernet0/3
!
interface Ethernet1/0
  switchport trunk allowed
vlan 10,20,30,40,99
  switchport trunk encapsula-
tion dot1q
  switchport mode trunk
!
interface Ethernet1/1
!
interface Ethernet1/2
!
interface Ethernet1/3
!
interface Ethernet2/0
  switchport trunk allowed
vlan 10,20,30,40,99
  switchport trunk encapsula-
tion dot1q
  switchport mode trunk
!
interface Ethernet2/1
!
interface Ethernet2/2
  switchport trunk allowed
vlan 10,20,30,40,99
  switchport trunk encapsula-
tion dot1q
  switchport mode trunk
!
interface Ethernet2/3
!
interface Ethernet3/0
!
interface Ethernet3/1
!
interface Ethernet3/2
!
interface Ethernet3/3
!
interface Vlan1
  no ip address
  shutdown
!
interface Vlan99
  no ip address

```

		Нероденко Д.О.			ККІКБ.КР.Б – 125 – 10 – ПЗ	Арк.
		Покотило О.А				8
Змн.	Арк.	№ докум.	Підпис	Дата		

```

!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
!
!
!
!
!
control-plane
!
!
line con 0
  exec-timeout 0 0
  privilege level 15
  logging synchronous
line aux 0
  exec-timeout 0 0
  privilege level 15
  logging synchronous
line vty 0 4
  login
!
!
End
SW-2410-4:
!
! Last configuration change
at 23:38:32 UTC Thu May
22 2025
!
version 15.2
service timestamps debug
datetime msec
service timestamps log
datetime msec
no service password-encryp-
tion
service compress-config
!
hostname SW-2410-4
!
boot-start-marker
boot-end-marker
!
!
logging discriminator EX-
CESS severity drops 6 msg-
body drops EXCESSCOLL
logging buffered 50000

```

```
logging console discriminator EXCESS
!
no aaa new-model
!
!
!
!
!
no ip icmp rate-limit unreachable
!
!
!
no ip domain-lookup
no ip cef
no ipv6 cef
!
!
!
spanning-tree mode rapid-pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
ip tcp synwait-time 5
!
!
!
!
!
!
!
!
!
!
!
!
interface Ethernet0/0
 switchport trunk allowed vlan 10,20,30,40,99
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface Ethernet0/1
!
interface Ethernet0/2
```

```

!
interface Ethernet0/3
!
interface Ethernet1/0
    switchport trunk allowed
vlan 10,20,30,40,99
    switchport trunk encapsula-
tion dot1q
    switchport mode trunk
!
interface Ethernet1/1
!
interface Ethernet1/2
!
interface Ethernet1/3
!
interface Ethernet2/0
    switchport trunk allowed
vlan 10,20,30,40,99
    switchport trunk encapsula-
tion dot1q
    switchport mode trunk
!
interface Ethernet2/1
!
interface Ethernet2/2
    switchport trunk allowed
vlan 10,20,30,40,99
    switchport trunk encapsula-
tion dot1q
    switchport mode trunk
!
interface Ethernet2/3
!
interface Ethernet3/0
!
interface Ethernet3/1
!
interface Ethernet3/2
!
interface Ethernet3/3
!
interface Vlan1
    no ip address
    shutdown
!
interface Vlan99
    no ip address
!
ip forward-protocol nd
!
!

```

		Нероденко Д.О.			<i>ККІКБ.КР.Б – 125 – 10 – ПЗ</i>	Арк.
		Покотило О.А				9
Змн.	Арк.	№ докум.	Підпис	Дата		

```

no ip http server
no ip http secure-server
!
!
!
!
!
control-plane
!
!
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
line vty 0 4
login
!
!
end

```

		Нероденко Д.О.			ККІКБ.КР.Б – 125 – 10 – ПЗ	Арк.
		Покотило О.А				10
Змн.	Арк.	№ докум.	Підпис	Дата		