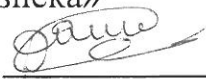


Міністерство освіти і науки України
Державний університет «Житомирська політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки

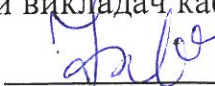
ПОЯСНЮВАЛЬНА ЗАПИСКА

до випускної кваліфікаційної роботи бакалавра
на тему: «Проект системи моніторингу для виявлення
та аналізу кіберзагроз в захищеній мережі на основі
Zabbix»

Виконала: студентка 4-го курсу групи КБ-20-1
спеціальності 125 «Кібербезпека»

 Дар'я БОБЕР

Керівник: старший викладач кафедри КІ та КБ

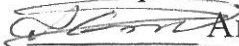
 Ігор ФАЛЬКОВСЬКИЙ

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

 Олена ГОЛОВНЯ

Житомир – 2024

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
5 березня 2024 р.

ЗАВДАННЯ

на випускню кваліфікаційну роботу бакалавра

Студентка: Бобер Дар'я Володимирівна

Тема роботи: «Проект системи моніторингу для виявлення та аналізу кіберзагроз в захищеній мережі на основі Zabbix»

затверджена Наказом університету від 5 березня 2024 р. № 98/с

Термін здачі студентом закінченої роботи 9 червня 2024 р.

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

1. Предметом дослідження є система моніторингу Zabbix, питання безпеки системи моніторингу Zabbix, питання застосування системи Zabbix у мережах різних розмірів, можливості системи моніторингу Zabbix для проведення моніторингу мереж.
2. Об'єктом дослідження є процес моніторингу кіберзагроз у захищених інформаційних системах за допомогою Zabbix.

Обладнання та програмне забезпечення:

1. Маршрутизатори Cisco 3945 та Cisco 3660
2. Комутатори Cisco 2960
3. Ubuntu 22.04
4. Kali Linux
5. Топологія мережі
6. Гіпервізор Oracle VirtualBox
7. Мережевий емулятор GNS3

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

Розділ	Консультант	Дата	
		Завдання видав	Завдання прийняв
1	Шелуха О. О.	01.03.2024 <i>Шелуха</i>	05.03.2024 <i>Дар'я</i>
2	Шелуха О. О.	20.04.2024 <i>Шелуха</i>	14.04.2024 <i>Дар'я</i>
3	Шелуха О. О.	17.05.2024 <i>Шелуха</i>	15.05.2024 <i>Дар'я</i>

Студентка

Керівник

Дар'я
Шелуха

Дар'я Бобер

Ігор ФАЛЬКОВСЬКИЙ

Календарний план

№ з/п	Назви етапів випускної кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Постановка завдання	01.03.2024	Виконано
2	Розробка плану роботи	25.03.2024	Виконано
3	Пошук інформації щодо реалізації системи моніторингу	12.04.2024	Виконано
4	Пректування загальної топології	20.04.2024	Виконано
5	Розробка IP-адресації та вибір необхідного обладнання	01.05.2024	Виконано
6	Аналіз технологій захисту мережі	06.05.2024	Виконано
7	Налаштування пристроїв мережі	14.05.2024	Виконано
8	Тестування налаштованої мережі на проникнення	25.05.2024	Виконано
9	Налаштування засобів захисту	05.06.2024	Виконано
10	Написання пояснювальної записки	10.06.2024	Виконано
11	Отримання відгуку та рецензії	24.06.2024	Виконано

Студентка

Керівник

Дар'я
Шелуха

Дар'я Бобер

Ігор ФАЛЬКОВСЬКИЙ

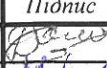
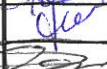
АНОТАЦІЯ

Випускна кваліфікаційна робота бакалавра представляє з себе проект системи моніторингу для виявлення та аналізу кіберзагроз в захищеній мережі на основі Zabbix. Кваліфікаційна робота містить опис проектування, розробки та налаштування мережі з Zabbix-системою. Пояснювальна записка складається зі вступу, трьох розділів, висновків, списку використаної літератури та додатків. Текстова частина викладена на 55 сторінках друкованого тексту. Пояснювальна записка містить 3 додатки на 11 сторінках. Список використаних джерел містить 22 найменування і займає 2 сторінки. В роботі наведено 54 рисунки та 5 таблиць. Загальний обсяг роботи – 76 сторінок.

Метою роботи є розробка системи моніторингу для виявлення та аналізу кіберзагроз у захищеній мережі на основі Zabbix, що забезпечить своєчасне виявлення та реагування на потенційні загрози, підвищуючи рівень безпеки інформаційних ресурсів організації.

В ході роботи визначено основні завдання для розробки системи моніторингу для виявлення та аналізу кіберзагроз у захищеній мережі на основі Zabbix. Спроектовано загальну топологію мережі та локальні підмережі, розроблено схему аде-сації пристроїв з урахуванням можливості розширення, здійснено вибір обладнання. Побудовано модель загроз мережі. Проведено налаштування мережі у від-повідності до проекту та перевірено правильність функціонування налаштованих протоколів. Проведено тестування на проникнення, після чого налаштовано засоби захисту від атак.

Ключові слова: ЗАХИСТ МЕРЕЖІ, СИСТЕМИ МОНІТОРИНГУ, ТЕСТУ-ВАННЯ, КІБЕРЗАГРОЗА, ШИФРУВАННЯ, ZABBIX, PROXY, АГЕНТ.

					ККІКБ.КР.Б – 125 – 01 – ПЗ				
Змн.	Арк.	№ докум.	Підпис	Дата	Проект системи моніторингу для виявлення та аналізу кіберзагроз в захищеній мережі на основі Zabbix	Літ.	Арк.	Аркушів	
Розроб.		Бобер Д. В.		24.06.24					
Керівник		Фальковський І. Г.		24.06.24			4	75	
Реценз.		Головня О. С.		24.06.24		ФІКТ, Гр. КБ-20-1			
Н. контр.		Фальковський І. Г.		24.06.24					
Затверд.		Єфіменко А.А.		24.06.24					

ANNOTATION

The final qualification work of the bachelor is a project of a monitoring system for the detection and analysis of cyber threats in a protected network based on Zabbix. The qualification work contains a description of the design, development and configuration of the network with the Zabbix system. The explanatory note consists of an introduction, three sections, conclusions, a list of references and appendices. The text part is laid out on 55 pages of printed text. The explanatory note contains 3 appendices on 11 pages. The list of used sources contains 22 names and occupies 2 pages. The work contains 54 figures and 5 tables. The total volume of the work is 76 pages.

The purpose of the work is to develop a monitoring system for the detection and analysis of cyber threats in a protected network based on Zabbix, which will ensure timely detection and response to potential threats, increasing the level of security of the organization's information resources.

In the course of the work, the main tasks for the development of a monitoring system for the detection and analysis of cyber threats in a protected network based on Zabbix were determined. The general topology of the network and local subnets were designed, the device adhesion scheme was developed taking into account the possibility of expansion, the selection of equipment was made. A model of network threats has been built. The network was configured in accordance with the project and the correct functioning of the configured protocols was checked. Penetration testing has been performed, after which attack defenses have been configured.

Keywords: NETWORK PROTECTION, MONITORING SYSTEMS, TESTING, CYBER THREAT, ENCRYPTION, ZABBIX, PROXY, AGENT.

		Бобер Д. В.			ККИКБ.КР.Б – 125 – 01 – ПЗ	Арк.
		Фальковський І. Г.				5
Змн.	Арк.	№ докум.	Підпис	Дата		

ЗМІСТ

ВСТУП	8
РОЗДІЛ 1 ТЕОРЕТИЧНІ ТА ПРИКЛАДНІ АСПЕКТИ ЗАСТОСУВАННЯ ZABBIX ДЛЯ ПОБУДОВИ СИСТЕМИ МОНІТОРИНГУ ПРИСТРОЇВ КОМП'ЮТЕРНОЇ МЕРЕЖІ.....	9
1.1 Принципи побудови та функціональні можливості системи моніторингу Zabbix.....	9
1.2 Використання Zabbix-проху для розподіленого моніторингу.....	17
1.3 Питання безпеки системи моніторингу Zabbix	20
1.4 Існуючі аналоги систем моніторингу.....	22
Висновки до першого розділу	24
РОЗДІЛ 2 ПРОЕКТУВАННЯ ПІДСИСТЕМИ МОНІТОРИНГУ КОМП'ЮТЕРНОЇ МЕРЕЖІ ІЗ ЗАСТОСУВАННЯ ZABBIX ТА АНАЛІЗ ПРОБЛЕМ БЕЗПЕКИ	26
2.1 Проектування підсистеми моніторингу та комп'ютерної мережі.....	26
2.2 Аналіз загроз підсистеми моніторингу	31
2.3 Побудова моделі загроз підсистеми моніторингу	32
Висновки до другого розділу	34
РОЗДІЛ 3 НАЛАГОДЖЕННЯ ТА ДОСЛІДЖЕННЯ СИСТЕМИ ЗАХИСТУ ПІД- СИСТЕМИ МОНІТОРИНГУ МЕРЕЖНОЇ ІНФРАСТРУКТУРИ.....	36
3.1 Вибір мережевого обладнання.....	36
3.2 Налагодження комп'ютерної мережі та підсистеми моніторингу	38
3.2 Дослідження рівня захищеності мережі	51
3.4 Налагодження засобів захисту та дослідження стійкості системи моніто- ринг	54
Висновки до третього розділу.....	59
ВИСНОВКИ.....	61
СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ	63
ДОДАТКИ.....	65

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ПЗ – програмне забезпечення

ОС – операційна система

БД – база даних

ЦП – центральний процесор

ОП – оперативна пам'ять

DHCP – Dynamic Host Configuration Protocol

EIGRP – Enhanced Interior Gateway Routing Protocol

SNMP – Simple Network Management Protocol

PSK – Pre-Shared Key

		Бобер Д. В.			ККІКБ.КР.Б – 125 – 01 – ПЗ	Арк.
		Фальковський І. Г.				7
Змн.	Арк.	№ докум.	Підпис	Дата		

ВСТУП

Актуальність теми. Сучасні інформаційні системи постійно стикаються з кіберзагрозами. Зростає необхідність забезпечення надійного захисту від збільшення кількості та складності кіберзагроз. З розвитком технологій та збільшенням обсягів переданих даних, організації все частіше стикаються з проблемами зломів, витоків інформації та інших форм кіберзлочинності. Ефективна система моніторингу дозволяє оперативно виявляти та реагувати на такі загрози, мінімізуючи потенційні збитки.

Метою кваліфікаційної роботи є розробка системи моніторингу для виявлення та аналізу кіберзагроз у захищеній мережі на основі Zabbix, що забезпечить своєчасне виявлення та реагування на потенційні загрози, підвищуючи рівень безпеки інформаційних ресурсів організації.

Визначена мета обумовлює наступні завдання:

- Дослідження сучасних методів та технологій моніторингу кіберзагроз.
- Розробка архітектури системи моніторингу
- Налаштування Zabbix для збору, обробки та аналізу даних про кіберзагрози та проблеми.
- Проведення тестування розробленої системи та аналіз її ефективності.

Об'єктом дослідження є процес моніторингу кіберзагроз у захищених інформаційних системах за допомогою Zabbix.

Предметом дослідження є система моніторингу Zabbix, питання безпеки системи моніторингу Zabbix, питання застосування системи Zabbix у мережах різних розмірів, можливості системи моніторингу Zabbix для проведення моніторингу мереж.

У процесі виконання кваліфікаційної роботи було розроблено проект системи моніторингу захищеної мережі з використанням системи Zabbix, досліджено її можливості, реалізовано рішення безпеки та проведено тестування стійкості мережі.

		Бобер Д. В.			ККІКБ.КР.Б – 125 – 01 – ПЗ	Арк.
		Фальковський І. Г.				8
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 1 ТЕОРЕТИЧНІ ТА ПРИКЛАДНІ АСПЕКТИ ЗАСТОСУВАННЯ ZABBIX ДЛЯ ПОБУДОВИ СИСТЕМИ МОНІТОРИНГУ ПРИСТРОЇВ КОМП'ЮТЕРНОЇ МЕРЕЖІ

1.1 Принципи побудови та функціональні можливості системи моніторингу Zabbix

Zabbix – це рішення для розподіленого моніторингу корпоративного класу з відкритим вихідним кодом. Zabbix з'явився в 1998 році, як внутрішній проект в латвійському банку. Існуючі на той час рішення були дорогими та складними у використанні, що робило їх недоступними для багатьох організацій. 7 квітня 2001 року систему було випущено публічно під ліцензією GPL, перша стабільна версія – 1.0 від 23 березня 2004. Її розробила латвійська компанія Zabbix SIA, яка була заснована 2005 року та повністю керує дорожньою картою (roadmap) продукту. Це безкоштовний продукт. Останній стабільний реліз – 7.0. Zabbix створено Олексієм Владишевим, який на даний момент є генеральним директором компанії Zabbix SIA в місті Рига та займається розвитком продукту та компанії. Основний напрямок діяльності Zabbix включає розробку програмного забезпечення з відкритим кодом, яке призначене для моніторингу мереж і додатків. Компанія також надає широкий спектр професійних послуг, адаптованих до специфічних потреб кожного клієнта. До них відносяться впровадження, інтеграція, індивідуальна розробка, консультування та різноманітні навчальні програми. [1]

Zabbix – це розподілена система моніторингу з централізованим веб-інтерфейсом, через який здійснюється управління, основними характеристиками якої є:

- централізований веб-інтерфейс;
- підтримка різних ОС;
- широка підтримка агентів для більшості Unix-подібних ОС та Windows;
- налаштування системи є простим і зрозумілим;
- моніторинг може здійснюватися за допомогою протоколів SNMP

		Бобер Д. В.			ККІКБ.КР.Б – 125 – 01 – ПЗ	Арк.
		Фальковський І. Г.				9
Змн.	Арк.	№ докум.	Підпис	Дата		

(v1, v2, v3), IPMI, JMX, ODBC, SSH, HTTP(S), TCP/UDP та Telnet;

- завдяки API, реалізованому для багатьох мов програмування, Zabbix легко інтегрується з іншими системами;
- є можливість створення власних елементів та графіків.

Zabbix — це популярна система моніторингу та управління, яка підтримує широкий спектр операційних систем. Це дозволяє використовувати Zabbix у різних середовищах, залежно від потреб і можливостей організації. Основні операційні системи, на яких може функціонувати Zabbix, включають: Alma Linux, Debian, Rocky Linux, Debian (arm64), Oracle Linux, Red Hat Enterprise Linux, OpenSUSE Leap, SUSE Linux Enterprise Server, Raspberry Pi OS, Ubuntu, Ubuntu (arm64), CentOS.

Архітектура Zabbix складається з трьох основних компонентів:

- веб-сервер;
- сервер БД;
- сервер Zabbix.

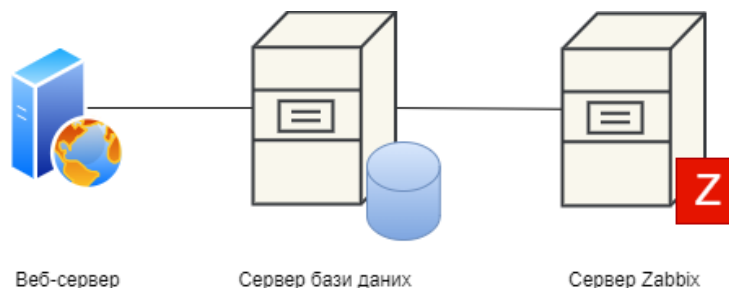


Рисунок 1.1. – Архітектура Zabbix системи

Для моніторингу великого оточення варто використовувати виділені сервери для спрощення подальшого розширення, забезпечити конфігурацію з високою доступністю та реалізувати конфігурацію з високою відмовостійкістю. Сервер Zabbix не дуже вимогливий до продуктивності ЦП, але вимагає великого обсягу пам'яті. [2]

Основними завданнями моніторингу є:

- відстеження стану мережевого обладнання, серверів та робочих станцій;
- визначення працездатності мережевих сервісів;

		Бобер Д. В.			ККІКБ.КР.Б – 125 – 01 – ПЗ	Арк.
		Фальковський І. Г.				10
Змн.	Арк.	№ докум.	Підпис	Дата		

- перевірка середовища передачі даних та якості послуг;
- агрегування зібраної інформації в БД.

Системи моніторингу бувають двох типів: Pull-системи та Push-системи. В Pull-системі сервер моніторингу сам проводить опитування вузлів в мережі, а в Push-системі вузли надсилають всю інформацію на сервер. Zabbix є представником Pull-системи, але водночас має функціонал Push-системи. Тобто, було розроблено агент, який може бути встановлено на клієнта, і цей агент передаватиме всю інформацію на сервер.

Елемент Zabbix характеризується ідентифікатором, типом даних і хостом. Ідентифікатор складається з імені та ключа елемента. Разом з хостом вони використовуються для ідентифікації серед тисяч інших елементів, що є в системі моніторингу. Тип даних необхідний для того, щоб Zabbix знав, як саме зберігати елемент, як його візуалізувати.

Пасивний елемент – це елемент, який вимагає, щоб сервер сам визначав інтервал і надсилав запити агенту про необхідність отримання даного елемента. Сервер ініціює мережеве з'єднання та закриває його, а агент просто приймає вхідні запити.



Рисунок 1.2. – Пасивний елемент

Ситуація протилежна у випадку активного елемента. Агент запитує у сервера інтервал і дані, які йому потрібно отримати. Після чого, агент планує порядок виконання вимірювань і ініціює з'єднання з сервером, щоб надіслати результати. В даному випадку агент має знати до якого сервера звертатися.

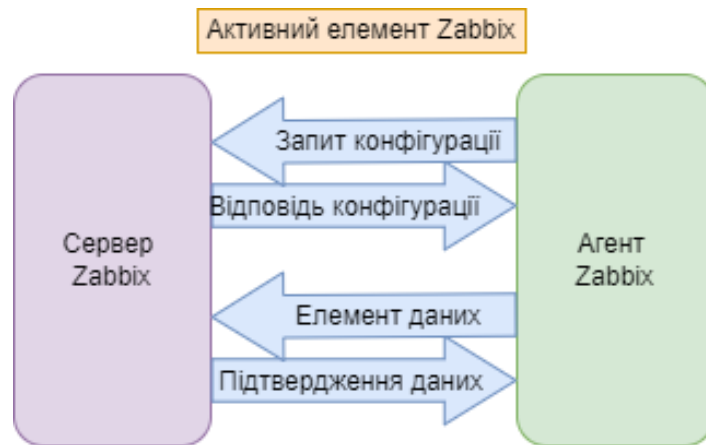


Рисунок 1.3. – Активний елемент

Основна різниця між пасивними та активними елементами полягає в ініціаторі мережевих з'єднань та можливості керування інтервалами між вимірами. У випадку з пасивними елементами можна встановлювати різні інтервали в залежності від часу доби та дня тижня. Наприклад, доступність сервера автентифікації користувачів можна перевіряти щохвилини під час робочих годин, а в неробочий час – кожні десять хвилин. Активні елементи, навпаки, виконують вимірювання з фіксованими інтервалами. [3]

У розширеній інфраструктурі Zabbix існують ще дві важливі складові:

- агенти Zabbix;
- проксі-сервери Zabbix.

Централізований сервер Zabbix з'єднаний з кількома проксі-серверами, зазвичай по одному на кожную підмережу. Сервер Zabbix отримує дані від проксі-серверів, які, у свою чергу, отримують дані від підключених агентів Zabbix. Всі ці дані зберігаються у виділеній БД, а доступ до них здійснюється через веб-інтерфейс. Веб-інтерфейс реалізовано за допомогою PHP, а сервер, проксі-сервери і агенти написані на мові С. [4]

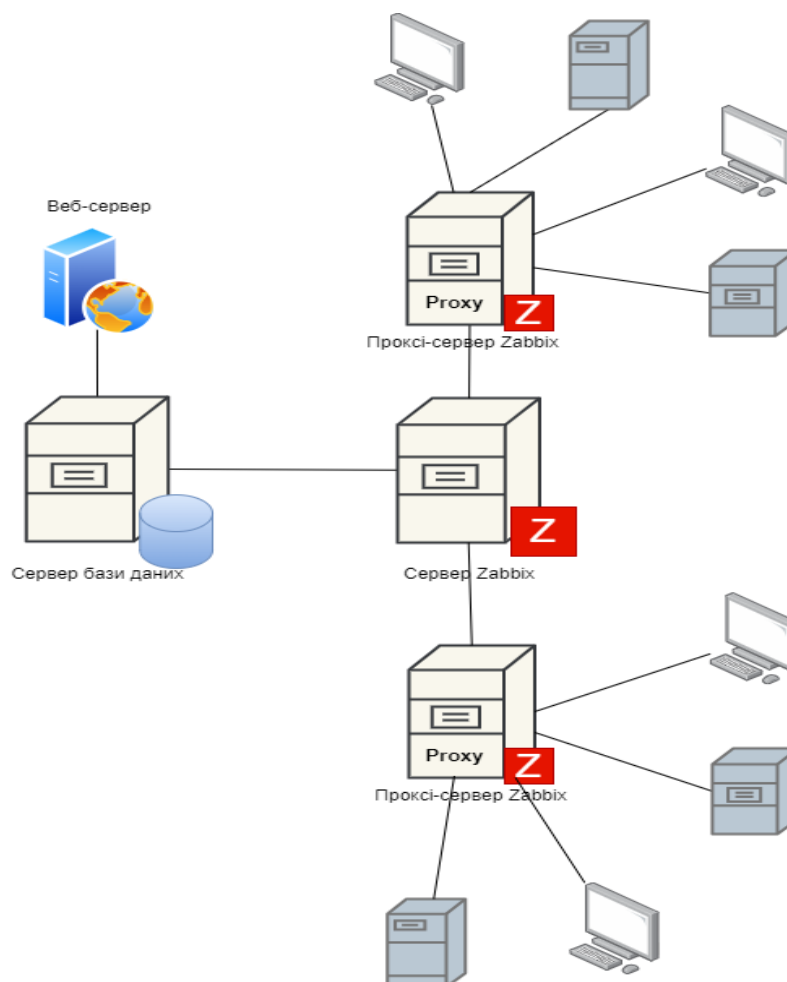


Рисунок 1.4. – Додаткові компоненти Zabbix

Графіки в Zabbix можна класифікувати на дві основні категорії: прості та нестандартні. Прості графіки в Zabbix дуже легкі для налаштування, оскільки вони відображають лише числові показники без складних налаштувань. Ці графіки призначені для простого відображення та моніторингу окремих метрик. Однак для більш складних потреб, наприклад, для спостереження за кількома параметрами одночасно, особливо корисною стає функція ситуаційних графіків, яка з'явилася у версії Zabbix 2.4. Такий підхід значно полегшує інтерпретацію даних і дозволяє швидко аналізувати пов'язані метрики.

Також у Zabbix існує доступний потужний інструмент для відображення географічної інформації, який дозволяє створювати деталізовані картографічні представлення інфраструктури. Карти в Zabbix це графічні візуалізації мережевих компонентів, серверів та їх зв'язків. Особливістю цього інструменту є його повна динамічність: на карті можна відображати активні попередження, повідомлення та тригери з використанням різних символів, кольорів і міток.

		Бобер Д. В.			ККІКБ.КР.Б – 125 – 01 – ПЗ	Арк.
		Фальковський І. Г.				13
Змн.	Арк.	№ докум.	Підпис	Дата		

Це дозволяє створювати дуже інформативні візуальні представлення. На карті можна розміщувати такі елементи, як;

- хости;
- групи хостів;
- тригери;
- зображення;
- карти.

Ручне налаштування кожного окремого компонента для кожного підконтрольного хоста є надзвичайно складним завданням. У великих середовищах з сотнями або тисячами об'єктів моніторингу практично неможливо вручну створити всі необхідні елементи даних, графіки та тригери. Механізм шаблонів в Zabbix дозволяє визначити різноманітні набори елементів, тригерів і графіків для застосування до будь-якої кількості хостів. При цьому існує можливість керування змінами у кожному конкретному випадку. Додатковою корисною особливістю шаблонів є функція автоматичного виявлення. Вона дозволяє визначати набір правил, які дозволяють Zabbix автоматично виявляти нові хости в мережі. [5]

Дуже важливим компонентом Zabbix-системи є сповіщення. Zabbix надає розширену систему сповіщень, яка дозволяє оперативно отримувати інформацію про стан системи і вчасно реагувати на проблеми. Основні складові системи сповіщень включають три складові. Це тригери, які викликаються при виконанні певних умов, визначених в налаштуваннях моніторингу, таких як перевищення порогу використання ресурсів або відсутність відповіді від сервера. Дії налаштовуються для виконання певних дій після спрацювання тригера. Це може включати відправлення електронних листів, SMS-повідомлень, викликів API, запусків сценаріїв тощо. Та способи доставки сповіщень, такі як електронна пошта, SMS, Jabber, SNMP трапи, звичайні програми, внутрішні оповіщення тощо. Zabbix може інтегруватися з різними зовнішніми системами сповіщень через API або зовнішні інтеграційні модулі. Це дозволяє реалізувати різноманітні сценарії доставки сповіщень в залежності від потреб. [6]

		Бобер Д. В.			ККІКБ.КР.Б – 125 – 01 – ПЗ	Арк.
		Фальковський І. Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		14

Способів встановлення Zabbix є декілька: [7]

- встановлення з попередньо скомпільованих пакетів спрощує процедуру оновлення;
- встановлення з вихідного коду забезпечує можливості компіляції лише необхідних компонентів, встановлення в різних версіях Linux та контролю за оновленнями;
- завантаження готового рішення; образ має налаштований Zabbix-сервер, базу даних MySQL та веб-інтерфейс, та доступний в таких форматах: vmdk (VMWare/Virtualbox), OVF (Open Virtualisation Format), CD iso, Образ HDD/flash, Preload ISO, Xen guest.

Моніторинг через SSH виконується Zabbix-сервером без участі агента, що може бути дуже зручним у певних ситуаціях. Це особливо корисно, оскільки дозволяє виконувати віддалені команди на пристроях, де встановлення агента Zabbix неможливе. Така можливість може бути використана у випадках, коли немає змоги встановити агента Zabbix, наприклад:

- для моніторингу пристроїв, на які не можна встановити додаткове програмне забезпечення;
- для моніторингу пристроїв з незвичайною або закритою операційною системою.

Для забезпечення моніторингу через SSH, Zabbix-сервер повинен бути скомпільований з підтримкою SSH2. Мінімально потрібна бібліотека libssh2 версії 1.0.0. Моніторинг через SSH підтримує два види автентифікації:

- з використанням імені користувача та пароля;
- з використанням файлу ключа.

Варто зазначити, що протокол SSH може вносити затримки та уповільнювати процес моніторингу. [8]

SNMP (Simple Network Management Protocol) є простим протоколом керування мережею, який функціонує на основі запитів і використовується для моніторингу мережевих пристроїв, таких як комутатори, маршрутизатори, де-

		Бобер Д. В.			ККІКБ.КР.Б – 125 – 01 – ПЗ	Арк.
		Фальковський І. Г.				15
Змн.	Арк.	№ докум.	Підпис	Дата		

які брандмауери та сховища даних. Існують три основні версії цього протоколу, кожна з яких має свої особливості та відмінності: [9]

- SNMPv1;
- SNMPv2;
- SNMPv3.

Далі наведено основні відмінності між SNMPv1, SNMPv2 та SNMPv3.

SNMPv1:

- найстаріша версія протоколу, яка не забезпечує безпеки, оскільки не використовує шифрування;
- для підтвердження зв'язку між моніторинговим хостом та пристроєм використовується лише спільнота (community);
- спільнота SNMP налаштовується на пристрої та використовується агентом для отримання метрик;
- має обмеження у вигляді 32-розрядних лічильників і вважається застарілою.

SNMPv2:

- також не використовує шифрування і для ідентифікації використовує лише ім'я спільноти (community name);
- може використовувати 64-розрядні лічильники, що є покращенням у порівнянні з SNMPv1.

SNMPv3:

- забезпечує шифрування зв'язку між мережевим пристроєм та Zabbix-сервером або Zabbix-проксі, а також дозволяє використовувати імені користувача та пароль для ідентифікації;
- значно безпечніший, але водночас складніший у налаштуванні та підтримці, оскільки вимагає створення користувачів і встановлення багатьох параметрів, таких як ім'я контексту (context name), ім'я безпеки (security name), рівень безпеки (security level) тощо;
- потребує постійної підтримки цієї конфігурації на всіх контрольованих середовищах та пристроях;

		Бобер Д. В.			ККІКБ.КР.Б – 125 – 01 – ПЗ	Арк.
		Фальковський І. Г.				16
Змн.	Арк.	№ докум.	Підпис	Дата		

- завдяки шифруванню та автентифікації є повільнішим. Потрібно бути обережним при налаштуванні параметрів, щоб уникнути помилок, оскільки це може призвести до того, що деякі елементи не підтримуватимуться на хостах або інтерфейс SNMP буде постійно переходити між станами "працює" та "не працює".

Інтерфейс IPMI є апаратною специфікацією, незалежною від конкретної операційної системи або BIOS. Однією з головних переваг IPMI є його доступність навіть тоді, коли система вимкнена. Це забезпечується завдяки наявності окремого апаратного модуля з низьким енергоспоживанням у кожному пристрої з підтримкою IPMI, який не залежить від основного апаратного або програмного середовища. Наразі IPMI підтримується більшістю виробників серверів і реалізується у вигляді карт управління, таких як HP ILO, IBM RSA, Sun SSP, DELL RDAC. [10]

1.2 Використання Zabbix-proxu для розподіленого моніторингу

Zabbix – це потужна програма для моніторингу, яка має здатність керувати тисячами елементів даних у конфігурації з одним сервером. Проте, коли потрібно моніторити тисячі хостів у мережах зі складною топологією або з географічно розподіленими елементами, єдиного серверу може бути недостатньо. Також часто зустрічаються мережі з сегментами, де діють суворі правила безпеки, які не дозволяють двостороннього зв'язку між довільними вузлами і, відповідно, не дозволяють серверу Zabbix взаємодіяти з усіма агентами у таких сегментах. Різним підрозділам компанії може знадобитися незалежність у керуванні їх підмережами, або може бути відсутнє надійне підключення до мережі. У таких випадках потрібно організувати накопичення даних моніторингу та їх асинхронну передачу для подальшої обробки. Завдяки можливостям розподіленого моніторингу Zabbix може ефективно використовуватися в різних ситуаціях. [11]

Сервер Zabbix-проксі – це додатковий компонент системи Zabbix, який розташовується між основним сервером і агентами Zabbix. Подібно до основного сервера, проксі-сервери збирають інформацію про роботу вузлів і зберігають її в БД.

		Бобер Д. В.			ККІКБ.КР.Б – 125 – 01 – ПЗ	Арк.
		Фальковський І. Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		17

Проксі-сервери, як і агенти, не мають веб-інтерфейсу і керуються безпосередньо центральним сервером. Вони не займаються аналізом зібраних даних. Zabbix-проксі простий та легкий інструмент, що допомагає зняти частину навантаження з центрального сервера, впорядкувати потік даних моніторингу через мережу.

Zabbix-проксі повинен працювати на машині, відокремленій від основного сервера. Він не має користувацького інтерфейсу та не виконує складних запитів або обчислень, тому йому не потрібен потужний процесор або жорсткий диск з високою пропускнуою здатністю. Малопотужний комп'ютер часто є найкращим вибором. Такі характеристики проксі-сервера забезпечують можливість розширення та розподілу архітектури моніторингу без значних фінансових витрат та низької складності дій.

У випадку, коли за одним проксі-сервером закріплено сотні хостів з тисячами параметрів, що підлягають моніторингу, замість використання більш потужного комп'ютера, частіше кращим рішенням є розподіл хостів на групи із використанням декількох проксі-серверів. Перевагами в такому підході є рівномірний розподіл навантаження, зменшення ризику втрати значної кількості даних через можливу відмову проксі-сервера.

Для Zabbix-проксі можна використовувати невеликі машини. Перевагами їх використання є те, що вони дешевші, простіше розгортаються, більш надійні, дуже економно споживають електроенергію. Та у випадку, коли мережа поділена на сегменти за географічним принципом, краще, щоб проксі-сервери мали достатньо ємну БД. Причиною є те, що зв'язок з центральним сервером може бути втрачено на тривалий час. Проксі-сервер повинен мати можливість зберігати дані в таких ситуаціях. [12]

Варто враховувати декілька ключових факторів при визначенні періоду, протягом якого проксі-сервер повинен зберігати дані, коли втрачено зв'язок з центральним сервером. Це кількість хостів та обсяг даних, які потрібно зберігати у БД проксі-сервера. Отже, якщо проксі-сервер працює в локальній мережі, доцільно буде використати легку та продуктивну БД, наприклад SQLite. В інших випадках

		Бобер Д. В.			ККІКБ.КР.Б – 125 – 01 – ПЗ	Арк.
		Фальковський І. Г.				18
Змн.	Арк.	№ докум.	Підпис	Дата		

краще обирати інші типи БД, які можуть надійно зберігати інформацію протягом тривалого часу, наприклад MySQL чи PostgreSQL.

Zabbix проху-сервери можуть працювати в двох режимах: [13]

- активний;
- пасивний.

У режимі за замовчуванням (активному) проксі-сервер ініціює всі з'єднання з сервером Zabbix, щоб отримати конфігураційну інформацію про об'єкти, що моніторяться, і надсилати зібрані дані для подальшої обробки. Активний проксі-сервер зменшує навантаження на основний сервер, оскільки Zabbix-серверу потрібно лише чекати запити на отримання оновленої конфігурації або нових даних моніторингу. Проте, проксі-сервери часто використовуються для моніторингу закритих мереж або сегментів з суворими обмеженнями на вихідний трафік. У таких випадках ініціювати з'єднання з боку проксі-сервера може бути складно через політику безпеки або інші причини. У таких ситуаціях простіше і безпечніше ініціювати з'єднання з закритими мережами ззовні, що робить пасивний проксі-сервер більш підходящим.

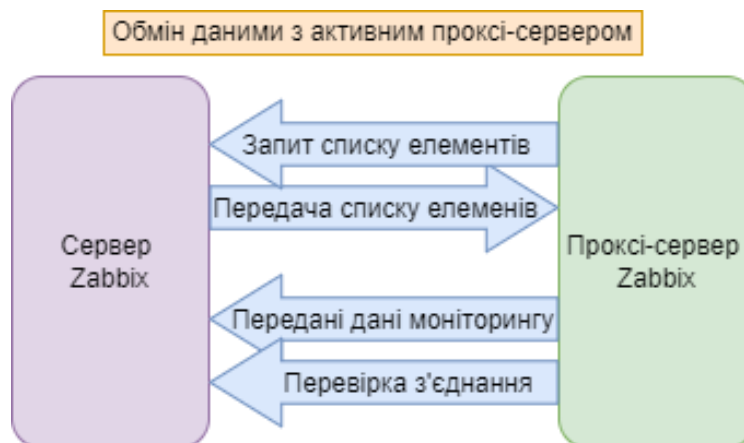


Рисунок 1.5. – Обмін даними з активним проксі-сервером

У пасивному режимі центральний сервер періодично з'єднується з проксі, щоб відправити зміни до конфігурації та отримати дані моніторингу. В іншому, пасивний та активний режими роботи проксі-серверів не відрізняються.

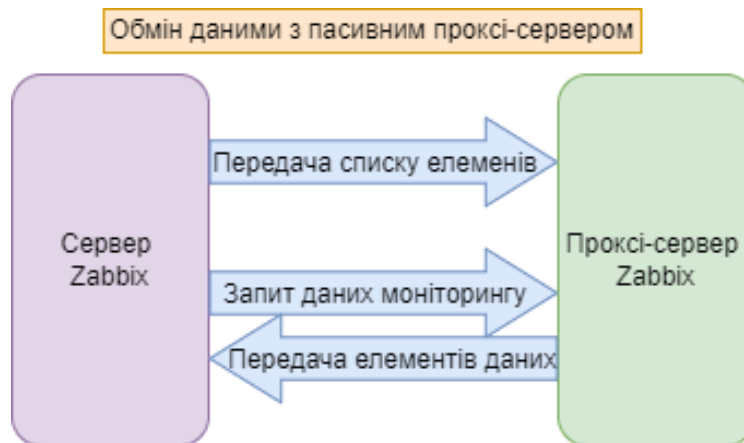


Рисунок 1.6. – Обмін даними з пасивним проксі-сервером

В залежності від політики конкретних мереж, можна одночасно використовувати і активні, і пасивні проксі-сервери, що дозволяє ефективно моніторити всі сегменти мережі.

1.3 Питання безпеки системи моніторингу Zabbix

Раніше, одним із небагатьох недоліків архітектури Zabbix була відсутність вбудованих засобів безпеки на рівні протоколу. Хоча веб-інтерфейс і Zabbix API можна було захистити за допомогою стандартних засобів SSL, не існувало простого і стандартного рішення для захисту взаємодії між такими пристроями, як Zabbix-сервер, агент та проксі-сервер.

І хоча прості дані моніторингу або конфігурації можуть і не вимагати особливого захисту, їх підробка може призвести до неправильних висновків. Попри відсутність стандартних заходів для вирішення цієї проблеми, існувало кілька можливих рішень: [14]

- відмова від конфігурації мережі
- ізолювання мережі
- прості тунелі:
 - *протокол SSH*
 - *програма Stunnel*
- використання повноцінної VPN

Шифрування стало однією з довгоочікуваних функцій для Zabbix. Раніше розглядалися різні варіанти його впровадження: від автентифікації за попереднім секретним ключем (PSK) до повної підтримки TLS і Kerberos. Згодом було вирішено реалізувати підтримку шифрування на основі TLS. Стала доступною можливість налаштування всіх з'єднань між сервером Zabbix, проксі та агентами на використання шифрування. Це дозволило використовувати Zabbix у середовищах, де було потрібно запровадити шифрування даних між хостами. Zabbix підтримує зашифрований зв'язок між своїми компонентами за допомогою протоколу безпеки транспортного рівня (TLS) версій 1.2 та 1.3. Також підтримуються методи шифрування на основі сертифіката та попереднього ключа. [15]

Шифрування є необов'язковим і може бути налаштоване для окремих компонентів. Тобто, одні проксі-сервери та агенти можуть використовувати шифрування на основі сертифікатів, інші можуть застосовувати шифрування на основі попереднього спільного ключа чи взагалі мати незашифроване з'єднання. Zabbix-сервер та проксі-сервери можуть використовувати різне шифрування для різних хостів.

Zabbix-демони використовують один порт для обробки як зашифрованих, так і незашифрованих вхідних з'єднань. Для додавання шифрування не потрібно відкривати нові порти на брандмауерах.

Шифрування Zabbix має певні обмеження:

- Приватні ключі зберігаються у вигляді звичайного тексту у файлах, доступних компонентам Zabbix під час запуску.
- Попередньо спільні ключі вводяться у зовнішній інтерфейс Zabbix і зберігаються в базі даних Zabbix як звичайний текст.
- Вбудоване шифрування не забезпечує захист комунікацій між інтерфейсом Zabbix і сервером Zabbix.
- Кожне зашифроване з'єднання наразі відкривається через повне рукостискання TLS;
- Додавання шифрування збільшує час перевірки елементів і дій, залежно від затримки мережі;
- Виявлення мережі не підтримує шифрування.

		Бобер Д. В.			ККІКБ.КР.Б – 125 – 01 – ПЗ	Арк.
		Фальковський І. Г.				21
Змн.	Арк.	№ докум.	Підпис	Дата		

- Шифрування потрібно налаштовувати окремо для кожного хоста та проксі-сервера, оскільки за замовчуванням з'єднання є незашифрованими.

Шифрування підтримує:

- сертифікати;
- спільні ключі PSK.

Є можливість використання кількох типів шифрування для вхідних підключень. Сертифікати вважаються більш безпечними, оскільки використовують асиметричне шифрування, тобто використовують пару ключів. PSK має симетричне шифрування, але його легше налаштувати.

Починаючи з версії 5.0, з'явилася можливість шифрування з'єднання з базою даних. Для цього використовуються сертифікати. Підтримується для таких БД, як:

- MySQL;
- PostgreSQL.

1.4 Існуючі аналоги систем моніторингу

Zabbix є потужною платформою для моніторингу мережі та серверів, однак існує багато альтернатив, які пропонують різні можливості та підходи до моніторингу. Нижче наведені деякі з популярних аналогів Zabbix. [16]

Nagios — це одна з найстаріших та найвідоміших систем моніторингу. Вона надає гнучкі можливості для моніторингу серверів, мережевих пристроїв та інфраструктури. Основні можливості включають моніторинг служб, ресурсів системи (наприклад, процесор, пам'ять, дисковий простір), та оповіщення про проблеми.

Перевагами є:

- велика кількість плагінів та модулів;
- гнучка та масштабована архітектура;
- сильна спільнота користувачів та підтримка.

Недоліки:

- складність у налаштуванні для новачків;

		Бобер Д. В.			ККІКБ.КР.Б – 125 – 01 – ПЗ	Арк.
		Фальковський І. Г.				22
Змн.	Арк.	№ докум.	Підпис	Дата		

- обмежений веб-інтерфейс.

Prometheus — це система моніторингу та оповіщення, розроблена компанією SoundCloud. Вона відома своєю здатністю збирати та зберігати метрики як часові ряди, використовуючи HTTP pull модель. Prometheus часто використовується для моніторингу контейнеризованих середовищ та інфраструктури на основі мікросервісів.

Переваги:

- висока масштабованість;
- підтримка складних запитів за допомогою PromQL;
- легкість інтеграції з контейнерами (наприклад, Kubernetes).

Недоліки:

- може бути складною для новачків через специфічну модель запитів та збору даних;
- вимагає додаткових інструментів для повного стеку моніторингу (наприклад, Grafana для візуалізації).

PRTG Network Monitor — це комерційний інструмент моніторингу мережі, який надає візуальні звіти та оповіщення в реальному часі. Він використовує сенсори для збору даних з різних мережевих пристроїв і служб.

Перевагами є:

- зручний та інтуїтивно зрозумілий інтерфейс користувача;
- вбудована підтримка різних типів сенсорів;
- можливість налаштування за допомогою мобільних додатків.

Недоліки:

- висока вартість ліцензій;
- можливі обмеження у масштабованості для великих середовищ.

SolarWinds Network Performance Monitor (NPM) — це ще один потужний інструмент для моніторингу мережі, який пропонує багатофункціональні можливості для відстеження продуктивності та доступності мережевих пристроїв і служб.

		Бобер Д. В.			ККІКБ.КР.Б – 125 – 01 – ПЗ	Арк.
		Фальковський І. Г.				23
Змн.	Арк.	№ докум.	Підпис	Дата		

Переваги:

- розширені можливості візуалізації та звітності;
- інтеграція з іншими продуктами SolarWinds для повного стеку IT-моніторингу;
- інтуїтивно зрозумілий інтерфейс.

Недоліки:

- висока вартість;
- може вимагати значних ресурсів для розгортання та підтримки.

Icinga — це форк Nagios, який пропонує покращений веб-інтерфейс та API для інтеграції з іншими інструментами. Він забезпечує гнучкі можливості моніторингу та оповіщення, подібні до Nagios.

Перевагами є:

- покращений веб-інтерфейс;
- підтримка сучасних API;
- сумісність з плагінами Nagios.

Недоліки:

- може вимагати значних зусиль для налаштування;
- деякі функції все ще знаходяться на стадії розвитку.

Вибір інструменту для моніторингу залежить від конкретних вимог вашої організації, включаючи розмір інфраструктури, технічні вимоги, бюджет та досвід команди. Кожен з наведених інструментів має свої переваги та недоліки, тому важливо ретельно оцінити їх перед впровадженням.

Висновки до першого розділу

Система Zabbix містить в собі наступні компоненти: сервер, база даних, веб-інтерфейс, агент, потік даних, що передаються між сервером моніторингу та вузлами моніторингу. Основне завдання проксі-сервера – збір даних. Акти-

		Бобер Д. В.			ККІКБ.КР.Б – 125 – 01 – ПЗ	Арк.
		Фальковський І. Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		24

вний проксі-сервер зменшує навантаження на основний сервер. Та попри невелике збільшення навантаження на центральний сервер, пасивні проксі-сервери дозволяють моніторити закриті мережі та їх сегменти. Можна одночасно використовувати і активні, і пасивні проксі-сервери. Для роботи обрано пасивні агенти, оскільки зручні для систем, де потрібно мінімізувати використання ресурсів.

SNMPv3 є найбезпечнішою версією, але вимагає більшої уваги та точності при налаштуванні. Для простоти та швидкості можна використовувати SNMPv2, але варто пам'ятати про відсутність шифрування. Використання SNMPv1 сьогодні не рекомендується через його обмеження та недостатню безпеку. Тому, для роботи було обрано SNMPv3, оскільки він найбільше гарантує безпеку.

Сертифікати і PSK використовуються для забезпечення безпеки з'єднання між агентами, проксі-серверами та сервером моніторингу. Обрано PSK, оскільки він простіший у використанні та налаштуванні.

		Бобер Д. В.			ККІКБ.КР.Б – 125 – 01 – ПЗ	Арк.
		Фальковський І. Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		25

РОЗДІЛ 2 ПРОЕКТУВАННЯ ПІДСИСТЕМИ МОНІТОРИНГУ КОМП'ЮТЕРНОЇ МЕРЕЖІ ІЗ ЗАСТОСУВАННЯ ZABBIX ТА АНАЛІЗ ПРОБЛЕМ БЕЗПЕКИ

2.1 Проектування підсистеми моніторингу та комп'ютерної мережі

При створенні сучасних корпоративних мереж варто дотримуватися таких основних принципів, як ієрархія, модульність та відмовостійкість. Трирівнева архітектура мережі, розроблена компанією Cisco повністю відповідає вимогам відмовостійкості, модульності та ієрархічності. [17]

Трирівнева структура включає такі рівні:

- рівень ядра забезпечує зв'язність між обладнанням рівня розподілу та іншими ресурсами мережі.
- рівень розподілу, який є проміжним між рівнем доступу і ядром, він займається маршрутизацією трафіку абонентів.
- рівень доступу включає обладнання, до портів якого безпосередньо підключені абоненти.

Мережу було спроектовано за допомогою графічного редактора Draw.io. Схема спроектованої мережі зображена на рисунку 2.1.

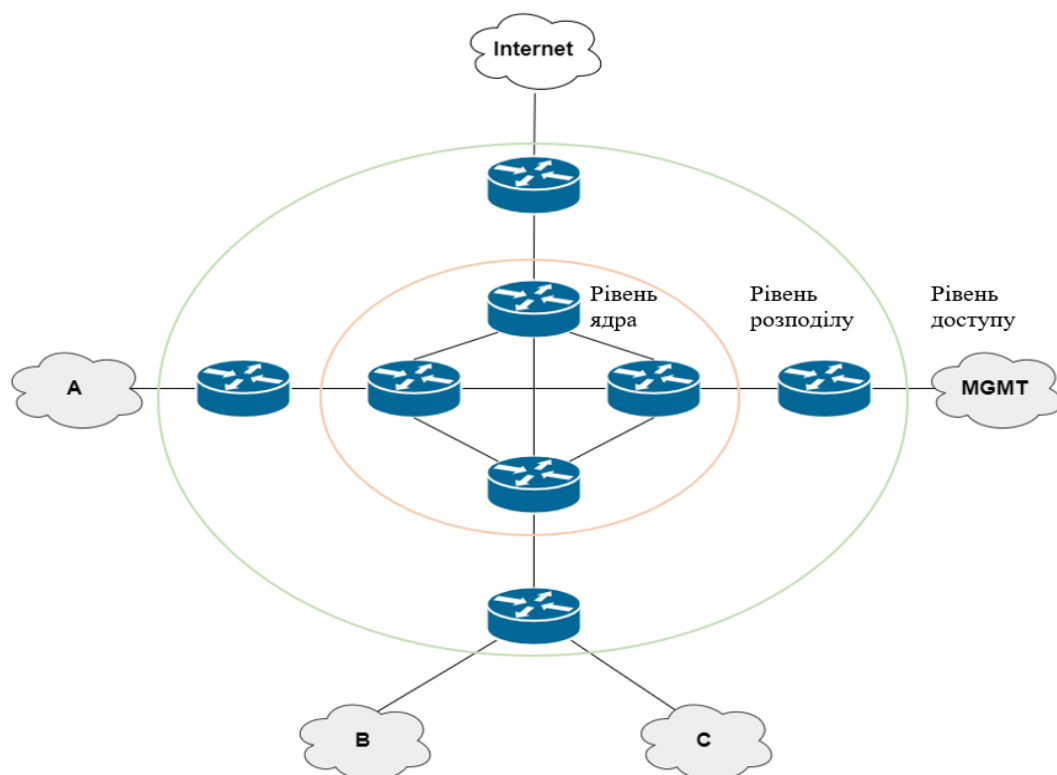


Рисунок 2.1. – Загальна топологія мережі

		Бобер Д. В.			ККІКБ.КР.Б – 125 – 01 – ПЗ	Арк.
		Фальковський І. Г.				26
Змн.	Арк.	№ докум.	Підпис	Дата		

Рівень ядра має 4 маршрутизатори, які з'єднані між собою високошвидкісними каналами зв'язку вита пара Gigabit Ethernet. На одному з маршрутизаторів реалізовано вихід в глобальну мережу.

Рівень розподілу представлено 3 маршрутизаторами, що під'єднані до ядра мережі. З'єднання з ядром мережі виконано за допомогою витой пари Gigabit Ethernet. Одна з локальних мереж являється мережею для моніторингу за допомогою Zabbix.

Рівень доступу складається з кінцевого устаткування користувачів та комутаційного обладнання.

Загалом у мережі використано 8 маршрутизаторів та 4 комутатори. Мережа складається з 4 підмереж.

На маршрутизаторі R-9-1-7 реалізовано вихід в глобальну мережу, рисунок 2.2. У своєму складі підмережа представлена 1 маршрутизатором та Інтернет-хмарою.



Рисунок 2.2. – Загальний вигляд доступу до WAN

Від маршрутизатора R-9-1-6 виходить підмережа А, рисунок 2.3. У своєму складі підмережа А має 20 ПК та один комутатор для підключення. У комутаторі задіяно 21 порт (20 портів на ПК + 1 порт на підключення до маршрутизатора), вільними залишається ще 3 порти.

		Бобер Д. В.			ККІКБ.КР.Б – 125 – 01 – ПЗ	Арк.
		Фальковський І. Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		27

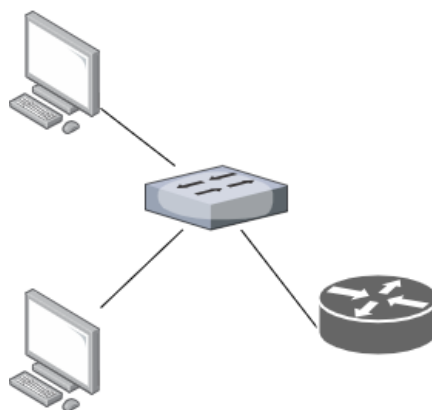


Рисунок 2.3. – Загальний вигляд підмережі А

Від маршрутизатора R-9-1-7 виходять 2 підмережі В та С, рисунок 2.4. Мережа В має у своєму складі 140 ПК і для їх підключення використовує 7 комутаторів на 24 порти. До кожного з комутаторів підключено по 20 ПК та один порт у кожному з комутаторів використовується для підключення до маршрутизатора R-9-2-8. Таким чином у комутаторах залишаються вільні порти. Мережа С є аналогічною мережі В.

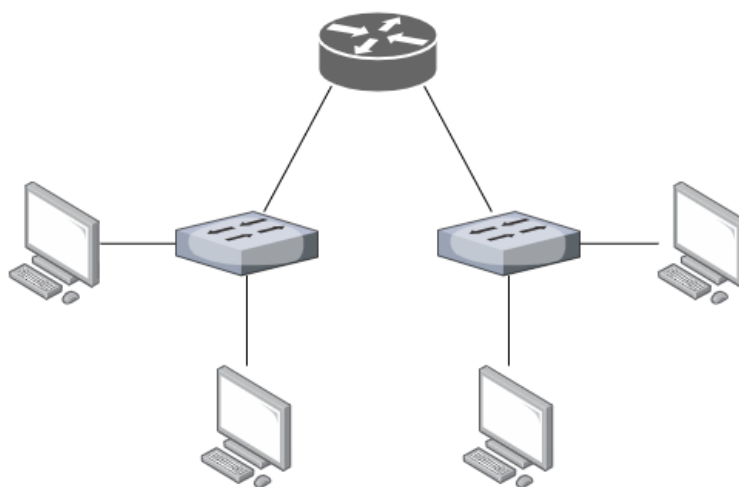


Рисунок 2.4. – Загальний вигляд підмереж В та С

Від маршрутизатора R-9-1-8 виходить 1 підмережа MGMT, рисунок 2.5. Дана мережа використовується для моніторингу мережі. Мережа MGMT представлена 1 комутатором та 1 сервером для Zabbix-моніторингу.

		Бобер Д. В.			ККІКБ.КР.Б – 125 – 01 – ПЗ	Арк.
		Фальковський І. Г.				28
Змн.	Арк.	№ докум.	Підпис	Дата		

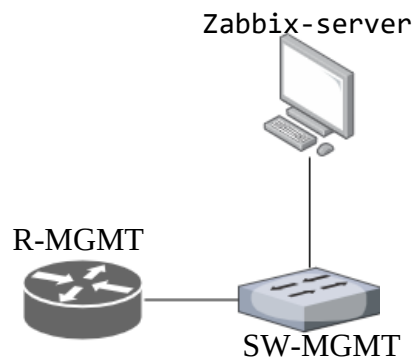


Рисунок 2.5. – Загальний вигляд підмережі MGMT

Під час проектування топології мережі важливо правильно розробити систему IP-адресації. Для рівня ядра мережі розподіл адрес по діапазону проводився таким чином, щоб використати мінімальну кількість IP-адрес, забезпечивши при цьому потреби підключених вузлів. Розрахунок приведено нижче:

R-9-1-1 – R-9-1-2: 192.168.1.0 /30
 R-9-1-2 – R-9-1-3: 192.168.1.4 /30
 R-9-1-3 – R-9-1-4: 192.168.1.8 /30
 R-9-1-4 – R-9-1-1: 192.168.1.12 /30
 R-9-1-1 – R-9-1-3: 192.168.1.16 /30
 R-9-1-2 – R-9-1-4: 192.168.1.20 /30

Для зв'язку між рівнем ядра та рівнем розподілу було використано 11 підмереж:

R-9-1-2 – R-9-1-6: 192.168.2.0 /30
 R-9-1-4 – R-9-1-5: 192.168.3.0 /30
 R-9-1-3 – R-MGMT: 192.168.4.0 /30
 R-9-1-1 – R-9-1-7: 192.168.5.0 /30

Розрахунок IP адрес для підмереж наведений у таблицях 2.1 – 2.4.

Таблиця 2.1 – Адресація підмережі А

Призначення	IP-адреса
Адреса мережі	192.168.6.0
Маска мережі	255.255.255.224/27
Інвертована маска	0.0.0.31

Мінімальна адреса	192.168.6.1
Максимальна адреса	192.168.6.30
Широкомовна адреса	192.168.6.31
Шлюз по замовчуванню	192.168.6.30
Діапазон адрес майбутніх ПК	192.168.6.1 – 20
Діапазон адрес комутаторів	192.168.6.21
Діапазон вільних адрес	192.168.6.22 – 29

Таблиця 2.2 – Адресація підмережі В

Призначення	IP-адреса
Адреса мережі	192.168.7.0
Маска мережі	255.255.255.0/24
Інвертована маска	0.0.0.255
Мінімальна адреса	192.168.7.1
Максимальна адреса	192.168.7.254
Широкомовна адреса	192.168.7.255
Шлюз по замовчуванню	192.168.7.254
Діапазон адрес майбутніх ПК	192.168.7.1 – 140
Діапазон адрес комутаторів	192.168.7.141 – 147
Діапазон вільних адрес	192.168.7.148 – 253

Таблиця 2.3 – Адресація підмережі С

Призначення	IP-адреса
Адреса мережі	192.168.8.0
Маска мережі	255.255.255.0/24
Інвертована маска	0.0.0.255
Мінімальна адреса	192.168.8.1
Максимальна адреса	192.168.8.254
Широкомовна адреса	192.168.8.255

Шлюз по замовчуванню	192.168.8.254
Діапазон адрес майбутніх ПК	192.168.8.1 – 140
Діапазон адрес комутаторів	192.168.8.141 – 147
Діапазон вільних адрес	192.168.8.148 – 253

Таблиця 2.4 – Адресація підмережі MGMT

Призначення	IP-адреса
Адреса мережі	192.168.9.0
Маска мережі	255.255.255.248/29
Інвертована маска	0.0.0.7
Мінімальна адреса	192.168.9.1
Максимальна адреса	192.168.9.6
Широкомовна адреса	192.168.9.7
Шлюз по замовчуванню	192.168.9.6
Діапазон адрес майбутніх ПК	192.168.9.1
Діапазон адрес комутаторів	192.168.9.2
Діапазон вільних адрес	192.168.9.3 – 5

2.2 Аналіз загроз підсистеми моніторингу

Аналіз загроз для підсистеми моніторингу включає детальний огляд протоколів і технологій, які налаштовані на мережевих пристроях, та перевірку потенційних вразливостей і можливих атак. У спроектованій топології передбачено налаштування наступних протоколів:

- протокол маршрутизації EIGRP;
- протокол керування мережами SNMP;
- протокол прикладного рівня DHCP.

Найпоширенішою атакою на SNMP в контексті використання Zabbix є атака на основі SNMP Community String Attack. Цей тип атаки використовує відсутність належної автентифікації в SNMPv1 і SNMPv2. Тому для моніторингу мережевих

		Бобер Д. В.			ККІКБ.КР.Б – 125 – 01 – ПЗ	Арк.
		Фальковський І. Г.				31
Змн.	Арк.	№ докум.	Підпис	Дата		

пристроїв за допомогою Zabbix краще використовувати SNMPv3, який забезпечує шифрування та автентифікацію, значно підвищуючи рівень безпеки в порівнянні з SNMPv1 і SNMPv2.

Протокол прикладного рівня DHCP (Dynamic Host Configuration Protocol) є критично важливим компонентом сучасних мереж, оскільки він автоматизує процес призначення IP-адрес пристроям. Однак, DHCP піддається різноманітним загрозам та атакам. Виведення його з ладу відріже локальні підмережі від мережі. Найпоширеніші можливі атаки на DHCP-сервер:

- DHCP Spoofing: зловмисник може налаштувати свій пристрій, як фальшивий DHCP-сервер і видавати себе за легітимний сервер;
- DHCP Starvation: вона використовує безліч запитів з різних MAC-адрес для вичерпання пулу доступних IP-адрес, що призводить до того, що нові пристрої не можуть отримати IP-адреси. [18]

Метою атаки Fake EIGRP Neighbors є перевантаження ЦП маршрутизатора з допомогою пакетів привітання EIGRP. В майбутньому це може призвести до атаки відмови в обслуговуванні. Атака EIGRP Blackhole порушує мережевий трафік шляхом спрямування трафіку до чорної діри. Атака переповнення таблиці маршрутизації навантажує ЦП і ОП маршрутизатора за допомогою заповнення таблиці маршрутизації численними помилковими маршрутами. [19]

Для моніторингу було використано систему Zabbix, яка за замовчуванням здійснює передачу своїх зібраних даних на сервер як звичайний текст. Це дозволяє будь-якому мережевому sniffers збирати дані. Також це не забезпечує цілісність даних, та не гарантує, що дані не буде змінено під час передачі.

2.3 Побудова моделі загроз підсистеми моніторингу

Сучасні інформаційно-комунікаційні системи стикаються з численними загрозами інформаційної безпеки, кількість яких зростає разом із розвитком технологій. Загрози можуть походити як із зовнішніх, так і з внутрішніх джерел, і мати руйнівні наслідки. Атаки можуть паралізувати системи або призвести до витоку

		Бобер Д. В.			ККІКБ.КР.Б – 125 – 01 – ПЗ	Арк.
		Фальковський І. Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		32

конфіденційної інформації, що негативно впливає на довіру клієнтів до постачальників. Для забезпечення стабільної роботи мережі важливо на етапі проектування ретельно проаналізувати всі можливі загрози. Ефективним методом є графічне моделювання, яке дозволяє наочно визначити вразливі елементи системи, їхній взаємозв'язок та потенційні загрози.

Моделювання ризиків є безперервним процесом, спрямованим на виявлення та мінімізацію загроз шляхом застосування відповідних заходів. Перевага цього підходу полягає в можливості розуміння реальних атак, встановлення зв'язків між компонентами системи, визначення сценаріїв та ймовірностей експлуатації вразливостей, а також оцінки впливу атак на систему. Результати моделювання дозволяють скласти повний перелік можливих загроз для мережі, оцінити основні процеси, бази даних та користувачів на стійкість до різного роду загроз, визначити критичність кожного елемента.

Загрози можна класифікувати на:

- об'єктивні: атаки з боку користувачів мережі, хакерів та інших злоумисників;
- суб'єктивні: природні явища та катастрофи.

		Бобер Д. В.			ККІКБ.КР.Б – 125 – 01 – ПЗ	Арк.
		Фальковський І. Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		33

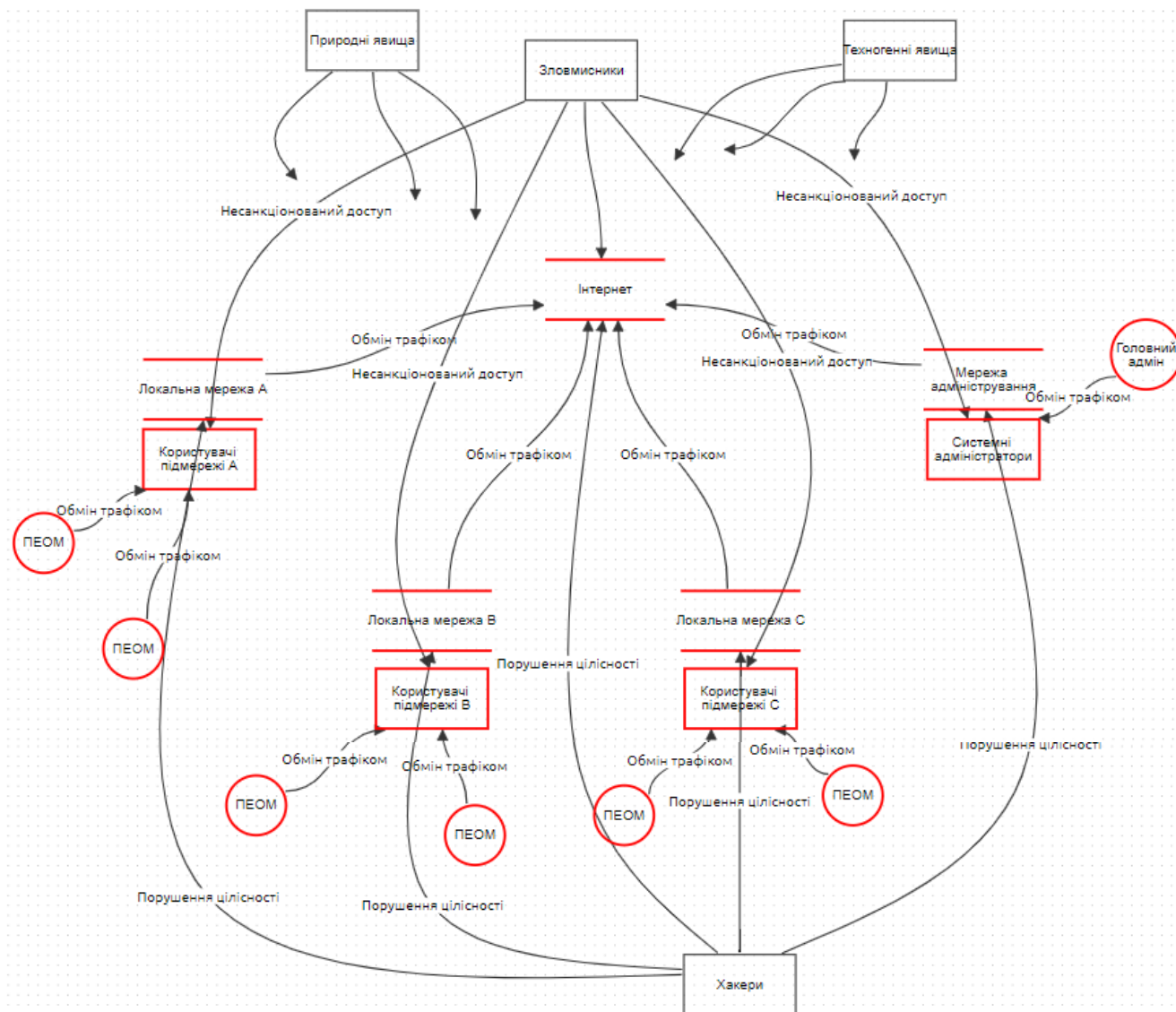


Рисунок 2.6 – Модель загроз мережі організації

Висновки до другого розділу

В першому підрозділі було спроектовано загальну топологію мережі та локальні ділянки з використанням редактору Draw.io. Також розроблено схему адресації мережі, враховуючи можливість розширення. Можливість розширення для підмережі адміністрування необхідно для додавання виділених серверів, у випадку збільшення мережі та кількості елементів, що моніторяться.

У другому підрозділі було проведено аналіз можливих загроз мережі. Враховано протоколи, що використовуються у спроектованій мережі. Для кожного протоколу представлено найпоширеніші варіанти можливих проблем і атак.

В третьому підрозділі створено модель загроз мережі з використанням OWASP Threat Dragon. Визначено та класифіковано загрози за природою їх виникнення та виявлено найбільш критичні ділянки мережі.

		Бобер Д. В.			ККІКБ.КР.Б – 125 – 01 – ПЗ	Арк.
		Фальковський І. Г.				35
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 3 НАЛАГОДЖЕННЯ ТА ДОСЛІДЖЕННЯ СИСТЕМИ ЗАХИСТУ ПІДСИСТЕМИ МОНІТОРИНГУ МЕРЕЖНОЇ ІНФРАСТРУКТУРИ

3.1 Вибір мережевого обладнання

Маршрутизатор виконує функцію пересилки пакетів даних між різними сегментами мережі, забезпечуючи її розширення, високу швидкість передачі та обробки даних. Для реалізації проекрованої комп'ютерної мережі було вирішено використовувати обладнання Cisco Systems, Inc. При виборі моделі маршрутизатора важливо враховувати його здатність до маршрутизації в складних глобальних мережах. Пристрій повинен бути сучасним, мати достатню кількість портів, забезпечувати надійну роботу та легке розширення мережі, а також працювати на необхідній швидкості. [20]

На рівні ядра необхідний маршрутизатор, що підтримує Gigabit Ethernet, EIGRP та SNMP. Оптимальним варіантом є маршрутизатор CISCO3945/K9. Це пристрій, що забезпечує високу надійність, захист, продуктивність і масштабованість зі швидкістю до 350 Мбіт/с. (Рис. 3.1)



Рисунок 3.1 – Маршрутизатор CISCO3945/K9

Переваги CISCO3945/K9 включають модульну конфігурацію з великою кількістю слотів розширення під EHWIC модулями, сумісність з WIC/VWIC/HWIC, слоти для модулів SM, підтримка цифрових модулів обробки сигналів (DSP) для голосових і відео функцій, а також можливість установки WLAN-контролера для

		Бобер Д. В.			ККІКБ.КР.Б – 125 – 01 – ПЗ	Арк.
		Фальковський І. Г.				36
Змн.	Арк.	№ докум.	Підпис	Дата		

управління до 25 точок доступу Cisco Unified Access Point. Маршрутизатор має до чотирьох вбудованих гігабітних мережевих інтерфейсів і підтримку процесорного модуля SPE (Service Performance Engine). На ньому встановлено універсальне ПЗ Cisco IOS Release 15.0 M, з усіма функціями доступними в одній прошивці, окремі елементи якої відкриваються за потреби.

Для рівня розподілу та доступу потрібен маршрутизатор, схожий за функціоналом на той, що використовується на рівні ядра, але за нижчою ціною. Оптимальним вибором є маршрутизатор Cisco 3660, який підтримує SNMP та EIGRP протоколи, забезпечуючи належний захист. (Рис. 3.2)



Рисунок 3.2 – Маршрутизатор Cisco 3660

Cisco 3660 – це гнучка платформа з широким спектром мережевих модулів, сумісних з Cisco 1600, 1700, 2600 та 3600, що знижує витрати на підтримку мережі та навчання фахівців. Основні переваги включають резервне джерело живлення та можливість гарячої заміни модулів, що підвищує надійність і ефективність роботи. Маршрутизатор має шість слотів розширення для мережевих модулів, два слоти Advanced Integration Module (AIM), один консольний порт, один додатковий (AUX) порт та два слоти PCMCIA для зберігання програмного забезпечення та конфігурацій. Він доступний з одним або двома портами Fast Ethernet, забезпечуючи гарячу заміну мережевих модулів та резервних джерел живлення. Cisco 3660 є оптимальним рішенням для надійної та гнучкої роботи мережі на рівні розподілу та доступу.

Комутатори серії Cisco Catalyst 2960 забезпечують фіксовану конфігурацію з портами Fast Ethernet і Gigabit Ethernet, а також розширені LAN сервіси для підп-

		Бобер Д. В.			ККІКБ.КР.Б – 125 – 01 – ПЗ	Арк.
		Фальковський І. Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		37

риємств початкового рівня та віддалених офісів. Вони підтримують передачу голосу, даних та відео з безпечним доступом і масштабованим управлінням, що відповідає зростаючим потребам бізнесу.



Рисунок 3.3 – Комутатор Cisco WS-C2960-24TT-L

Cisco Catalyst 2960 підтримують інтелектуальні функції, такі як створення складних списків контролю доступу та розширена безпека. Вони мають гігабітні аплінки, що можуть бути мідними або з використанням SFP-модулів для різних середовищ (Cisco 1000BASE-0, 1000BASE-ZX, 100BASE-FX, 100BASE-LX, CWDM SFP). Інші особливості включають підтримку QoS, покроковий Rate Limiting, ACL на основі MAC або IP адрес, UDP/TCP портів, мультикаст сервіси, регулювання швидкості передачі на кожному порту з кроком 64 кбіт, Link Aggregation для швидкісних з'єднань, транкові з'єднання за допомогою тегів 802.1q, підтримку до 255 VLAN на комутатор та до 4000 VLAN ID. Управління здійснюється через Cisco Network Assistant, що підтримує широкий спектр моделей комутаторів від Cisco Catalyst 2960 до Cisco Catalyst 4506.

3.2 Налаштування комп'ютерної мережі та підсистеми моніторингу

Спершу в мережі було налаштовано адресацію інтерфейсів маршрутизаторів. Як приклад далі наведено налаштування на маршрутизаторі R-9-2-1:

```
R-9-1-1(config)#int f0/0
R-9-1-1(config-if)#description Link-To-R-9-1-7
R-9-1-1(config-if)#ip add 192.168.5.1 255.255.255.252
R-9-1-1(config-if)#no shut
R-9-1-1(config-if)#exit
R-9-1-1(config)#int f0/1
R-9-1-1(config-if)#description Link-To-R-9-1-2
```

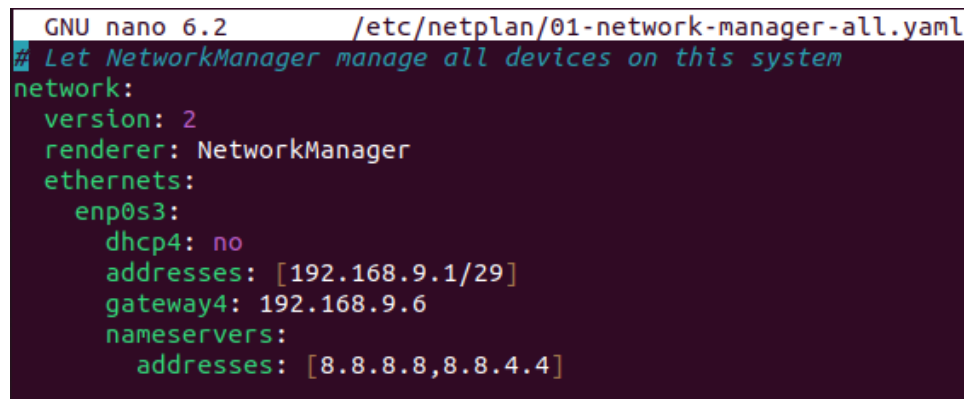
		Бобер Д. В.			ККІКБ.КР.Б – 125 – 01 – ПЗ	Арк.
		Фальковський І. Г.				38
Змн.	Арк.	№ докум.	Підпис	Дата		

```

R-9-1-1(config-if)#ip add 192.168.1.5 255.255.255.252
R-9-1-1(config-if)#no shut
R-9-1-1(config-if)#exit
R-9-1-1(config)#int f1/0
R-9-1-1(config-if)#description Link-To-R-9-1-4
R-9-1-1(config-if)#ip add 192.168.1.13 255.255.255.252
R-9-1-1(config-if)#no shut
R-9-1-1(config-if)#exit
R-9-1-1(config)#int f2/0
R-9-1-1(config-if)#description Link-To-R-9-1-3
R-9-1-1(config-if)#ip add 192.168.1.17 255.255.255.252
R-9-1-1(config-if)#no shut
R-9-1-1(config-if)#exit

```

Налаштування на одній з робочих станцій з ОС Ubuntu 22.04



```

GNU nano 6.2 /etc/netplan/01-network-manager-all.yaml
# Let NetworkManager manage all devices on this system
network:
  version: 2
  renderer: NetworkManager
  ethernets:
    enp0s3:
      dhcp4: no
      addresses: [192.168.9.1/29]
      gateway4: 192.168.9.6
      nameservers:
        addresses: [8.8.8.8,8.8.4.4]

```

Рисунок 3.4 – Налаштування IP-адресації на ПК

```

student@student-VirtualBox:~$ ls /etc/netplan/
01-network-manager-all.yaml
student@student-VirtualBox:~$ sudo nano /etc/netplan/01-network-manager-all.yaml
[sudo] пароль до student:
student@student-VirtualBox:~$ sudo netplan apply
student@student-VirtualBox:~$ ip addr show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group defau
lt qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP g
roup default qlen 1000
    link/ether 08:00:27:73:c4:25 brd ff:ff:ff:ff:ff:ff
    inet 192.168.9.1/29 brd 192.168.9.7 scope global noprefixroute enp0s3
        valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fe73:c425/64 scope link
        valid_lft forever preferred_lft forever
student@student-VirtualBox:~$

```

Рисунок 3.5 – Перевірка налаштування IP-адресації на ПК

Маршрутизатори рівня розподілу було налаштовано як DHCP-сервери за допомогою наступних команд:

R-9-1-6(config)#ip dhcp pool Lan-A

R-9-1-6(dhcp-config)#network 192.168.6.0 255.255.255.224

R-9-1-6(dhcp-config)#default-router 192.168.6.30

R-9-1-6(dhcp-config)#domain-name bober.local

R-9-1-6(dhcp-config)#dns-server 8.8.8.8

R-9-1-6(dhcp-config)#exit

```

GNU nano 6.2 /etc/netplan/01-network-manager-all.yaml *
# Let NetworkManager manage all devices on this system
network:
  version: 2
  renderer: NetworkManager
  ethernets:
    enp0s3:
      dhcp4: true

```

Рисунок 3.6 – Налаштування отримання DHCP-адреси

		Бобер Д. В.			ККІКБ.КР.Б – 125 – 01 – ПЗ	Арк.
		Фальковський І. Г.				40
Змн.	Арк.	№ докум.	Підпис	Дата		

```

student@student-VirtualBox:~$ sudo nano /etc/netplan/01-network-manager-all.yaml
[sudo] пароль до student:
student@student-VirtualBox:~$ ip addr show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:73:c4:25 brd ff:ff:ff:ff:ff:ff
    inet 192.168.6.1/27 brd 192.168.6.31 scope global dynamic noprefixroute enp0s3
        valid_lft 86291sec preferred_lft 86291sec
    inet6 fe80::a00:27ff:fe73:c425/64 scope link
        valid_lft forever preferred_lft forever
student@student-VirtualBox:~$

```

Рисунок 3.7 – Успішне отримання DHCP-адреси

В мережі було налаштовано протокол EIGRP. Далі наведено приклад налаштувань на маршрутизаторі R-9-2-5:

```

R-9-1-5(config)#router eigrp 1
R-9-1-5(config-router)#no auto-summary
R-9-1-5(config-router)#network 192.168.3.0 0.0.0.3
R-9-1-5(config-router)#network 192.168.7.0 0.0.0.255
R-9-1-5(config-router)#network 192.168.8.0 0.0.0.255
R-9-1-5(config-router)#passive-interface f0/1
R-9-1-5(config-router)#passive-interface f1/0
R-9-1-5(config-router)#exit

```

У відповідності до розробленої у розділі 2 схеми всі компоненти системи моніторингу розміщено на одному віртуальному сервері. Далі показано налаштування Zabbix-сервера.

```

student@student-VirtualBox:~$ sudo apt update
[sudo] пароль до student:
В кеші:1 http://ua.archive.ubuntu.com/ubuntu jammy InRelease
Отр:2 http://ua.archive.ubuntu.com/ubuntu jammy-updates InRelease [128 kB]
Отр:3 http://ua.archive.ubuntu.com/ubuntu jammy-backports InRelease [127 kB]
Отр:4 http://security.ubuntu.com/ubuntu jammy-security InRelease [129 kB]
Отр:5 http://ua.archive.ubuntu.com/ubuntu jammy-updates/main amd64 Packages [1734 kB]
Отр:6 http://ua.archive.ubuntu.com/ubuntu jammy-updates/main i386 Packages [643 kB]

```

Рисунок 3.8 – Оновлення системи

		Бобер Д. В.			ККІКБ.КР.Б – 125 – 01 – ПЗ	Арк.
		Фальковський І. Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		41

Було проведено встановлення необхідних залежностей з використанням наступних команд:

```
sudo apt install apache2 libapache2-mod-php
```

```
sudo apt install mysql-server
```

```
sudo apt install php php-mbstring php-gd php-xml php-bcmath php-ldap php-mysql
```

```
student@student-VirtualBox:~$ wget https://repo.zabbix.com/zabbix/7.0/ubuntu/pool/main/z/zabbix-release/zabbix-release_7.0-1+ubuntu22.04_all.deb
--2024-06-20 19:40:25-- https://repo.zabbix.com/zabbix/7.0/ubuntu/pool/main/z/zabbix-release/zabbix-release_7.0-1+ubuntu22.04_all.deb
Визначення імені repo.zabbix.com (repo.zabbix.com)... 178.128.6.101, 2604:a880:2:d0::2062:d001
Встановлення з'єднання з repo.zabbix.com (repo.zabbix.com)|178.128.6.101|:443..
. з'єднано.
HTTP-запит надіслано, очікуємо на відповідь... 200 OK
Довжина: 6012 (5,9K) [application/octet-stream]
Зберігаємо до 'zabbix-release_7.0-1+ubuntu22.04_all.deb'

zabbix-release_7.0- 100%[=====] 5,87K --.-KB/s за 0s

2024-06-20 19:40:25 (564 MB/s) - 'zabbix-release_7.0-1+ubuntu22.04_all.deb' збережено [6012/6012]

student@student-VirtualBox:~$ sudo dpkg -i zabbix-release_7.0-1+ubuntu22.04_all.deb
Вибір раніше не обраного пакунку zabbix-release.
(Читання бази даних ... на дану мить встановлено 185247 файлів та каталогів.)
Приготування до розпакування zabbix-release_7.0-1+ubuntu22.04_all.deb ...
Розпакування zabbix-release (1:7.0-1+ubuntu22.04)...
Налаштовування zabbix-release (1:7.0-1+ubuntu22.04) ...
```

Рисунок 3.9 – Встановлення репозиторію Zabbix

```
student@student-VirtualBox:~$ sudo apt install zabbix-server-mysql zabbix-front
end-php zabbix-apache-conf zabbix-sql-scripts zabbix-agent
Зчитування переліків пакунків... Виконано
Побудова дерева залежностей... Виконано
Зчитування інформації про стан... Виконано
Буде встановлено такі додаткові пакунки:
 fonts-dejavu fonts-dejavu-extra fping libevent-2.1-7 libmodbus5
 libmysqlclient21 libodbc2 libopenipmi0 libsnmp40 php-curl php8.1-curl snmpd
Пропоновані пакунки:
 odbc-postgresql tdsodbc snmptrapd zabbix-nginx-conf
```

Рисунок 3.10 – Встановлення Zabbix

		Бобер Д. В.			ККІКБ.КР.Б – 125 – 01 – ПЗ	Арк.
		Фальковський І. Г.				42
Змн.	Арк.	№ докум.	Підпис	Дата		

```

student@student-VirtualBox:~$ sudo mysql -uroot -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 9
Server version: 8.0.37-0ubuntu0.22.04.3 (Ubuntu)

Copyright (c) 2000, 2024, Oracle and/or its affiliates.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> create database zabbix character set utf8mb4 collate utf8mb4_bin;
Query OK, 1 row affected (0,10 sec)

mysql> create user zabbix@localhost identified by 'password';
Query OK, 0 rows affected (0,05 sec)

mysql> grant all privileges on zabbix.* to zabbix@localhost;
Query OK, 0 rows affected (0,01 sec)

mysql> set global log_bin_trust_function_creators = 1;
Query OK, 0 rows affected, 1 warning (0,01 sec)

mysql> quit;
Bye

```

Рисунок 3.11 – Створення початкової бази даних

```

student@student-VirtualBox:~$ zcat /usr/share/zabbix-sql-scripts/mysql/server.s
ql.gz | mysql --default-character-set=utf8mb4 -uzabbix -p zabbix
Enter password:
student@student-VirtualBox:~$ sudo mysql -uroot -p
[sudo] пароль до student:
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 13
Server version: 8.0.37-0ubuntu0.22.04.3 (Ubuntu)

Copyright (c) 2000, 2024, Oracle and/or its affiliates.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

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

mysql> quit;

```

Рисунок 3.12 – Імпортування початкової схеми та даних

		Бобер Д. В.			ККІКБ.КР.Б – 125 – 01 – ПЗ	Арк.
		Фальковський І. Г.				43
Змн.	Арк.	№ докум.	Підпис	Дата		

```
GNU nano 6.2 /etc/zabbix/zabbix_server.conf *
# DBUser=

DBUser=zabbix

### Option: DBPassword
# Database password.
# Comment this line if no password is used.
#
# Mandatory: no
# Default:
DBPassword=password
```

Рисунок 3.13 – Налаштування бази даних для сервера Zabbix

```
student@student-VirtualBox:~$ sudo nano /etc/zabbix/zabbix_server.conf
student@student-VirtualBox:~$ sudo systemctl restart zabbix-server zabbix-agent
apache2
student@student-VirtualBox:~$ sudo systemctl enable zabbix-server zabbix-agent a
pache2
Synchronizing state of zabbix-server.service with SysV service script with /lib/
systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable zabbix-server
Synchronizing state of zabbix-agent.service with SysV service script with /lib/s
```

Рисунок 3.14 – Запуск процесів Zabbix

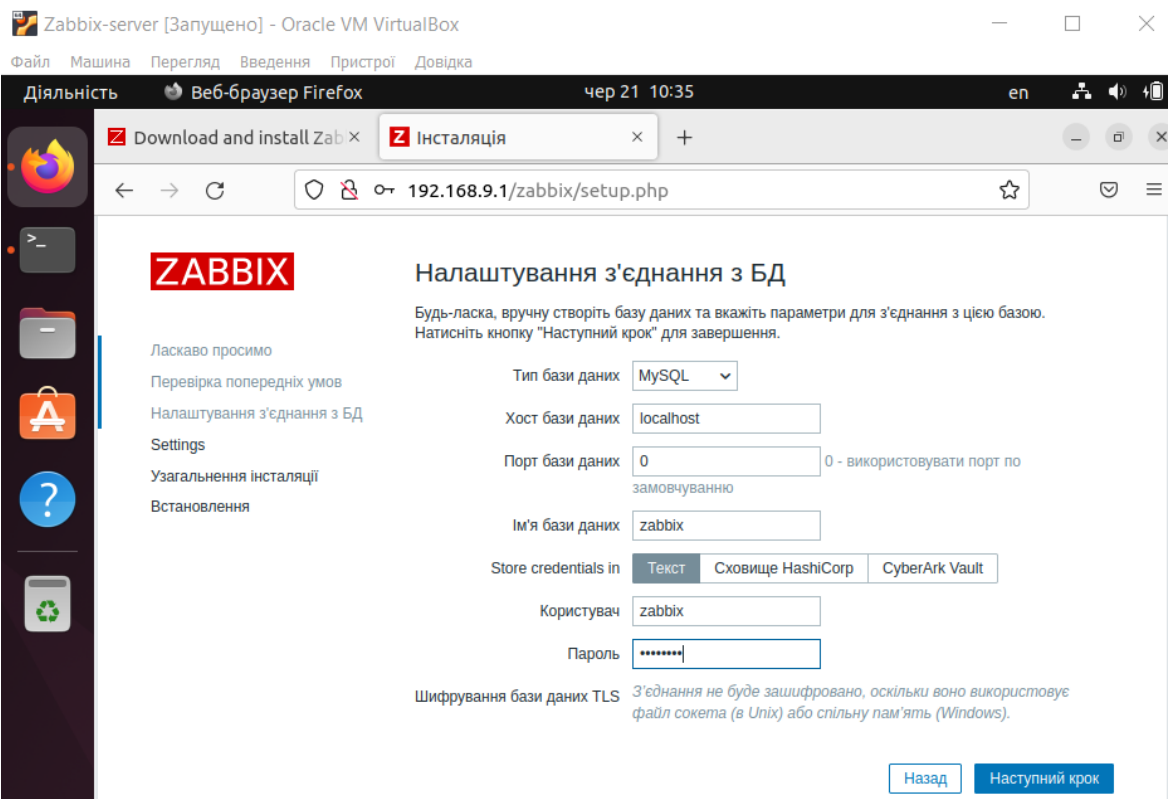


Рисунок 3.15 – Налаштування з'єднання з БД

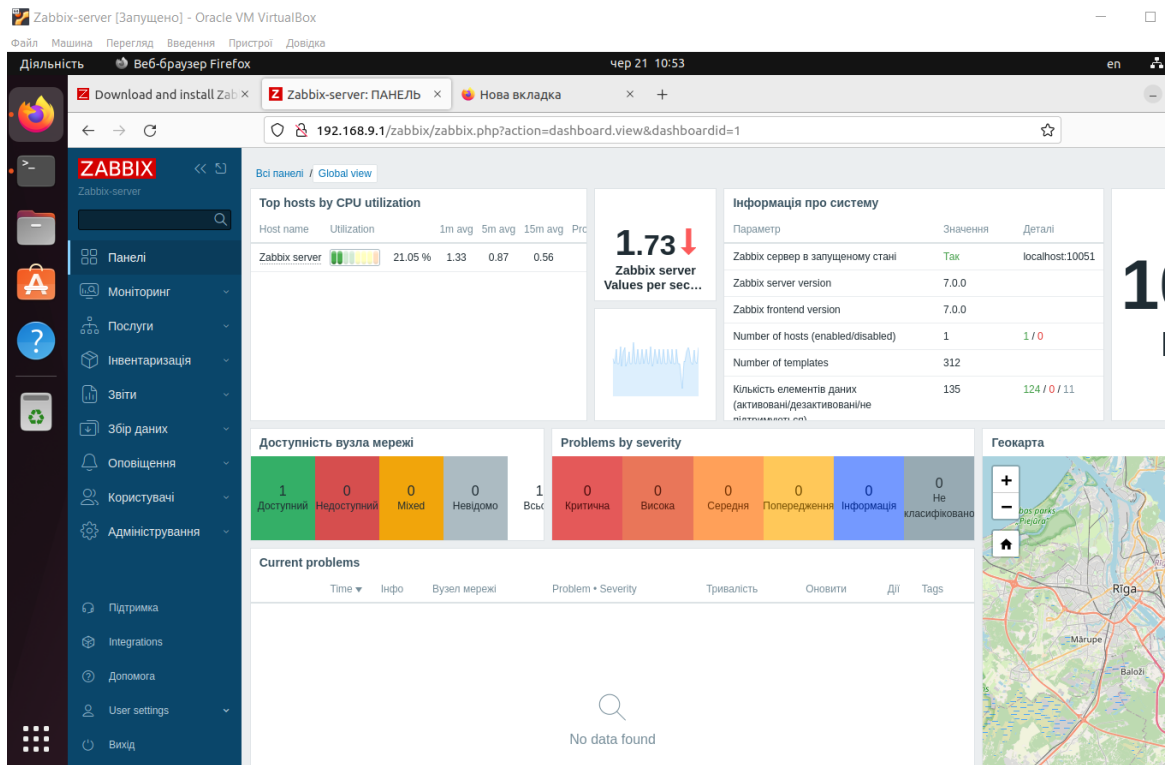


Рисунок 3.16 – Панель налаштованого Zabbix

Далі було проведено налаштування агентів Zabbix. Налаштування SNMPv3 на мережевому обладнанні. Наведено приклад налаштувань на маршрутизаторі R-MGMT:

```
R-MGMT(config)#snmp-server group Admin v3 priv read snmpzabbix
```

```
R-MGMT(config)#snmp-server user adminzabbix Admin v3 auth md5
adminzabbix3 priv des adminzabbix3
```

```
R-MGMT(config)#snmp-server view adminrw iso included
```

		Бобер Д. В.			ККІКБ.КР.Б – 125 – 01 – ПЗ	Арк.
		Фальковський І. Г.				45
Змн.	Арк.	№ докум.	Підпис	Дата		

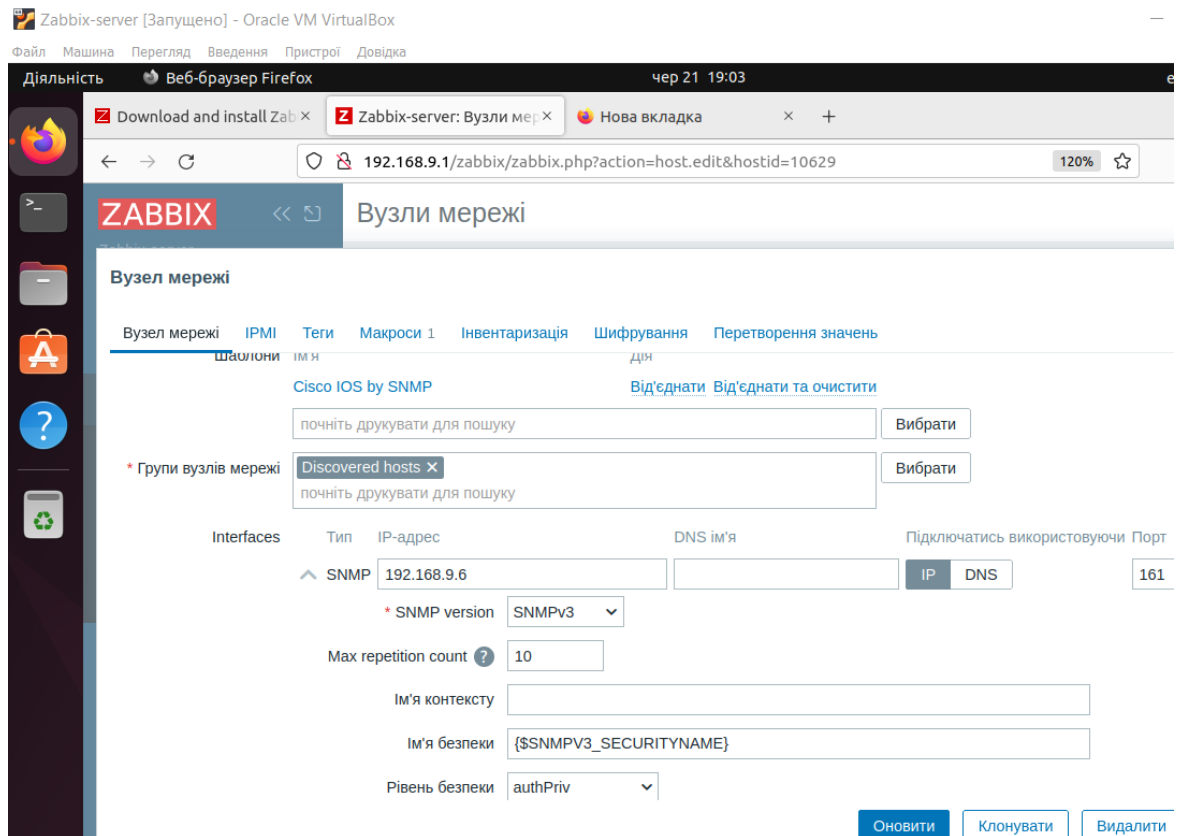


Рисунок 3.17 – Додавання вузла мережі

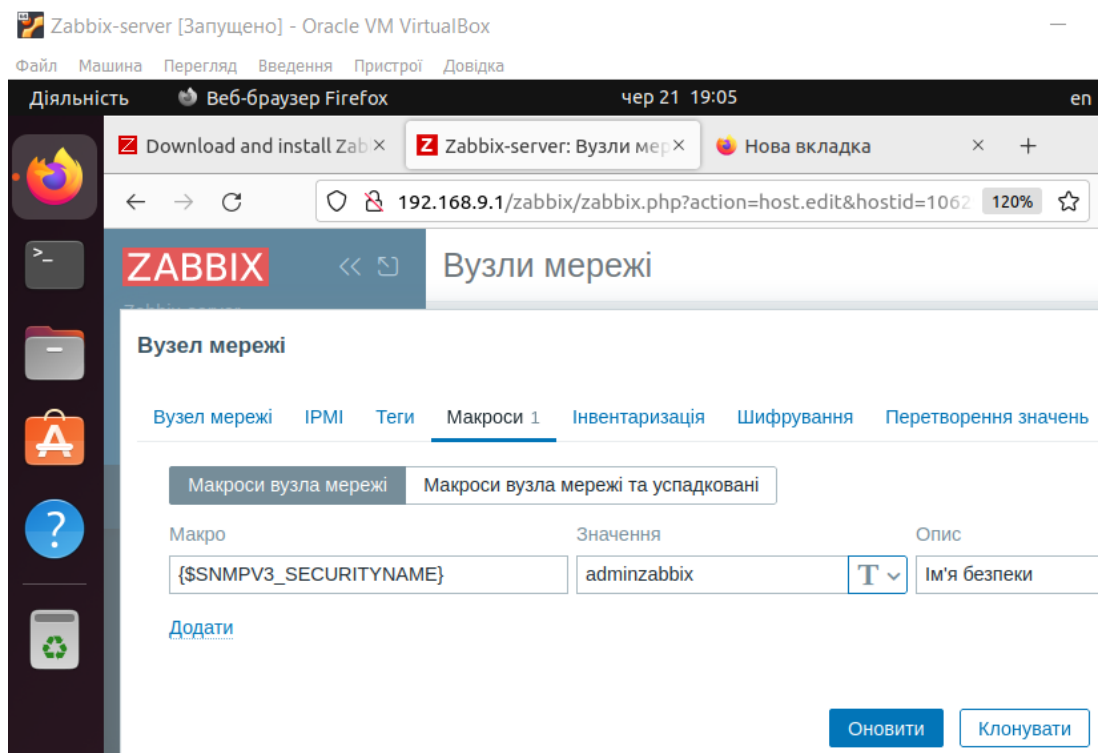


Рисунок 3.18 – Налаштування макросів

		Бобер Д. В.			ККІКБ.КР.Б – 125 – 01 – ПЗ	Арк.
		Фальковський І. Г.				46
Змн.	Арк.	№ докум.	Підпис	Дата		

```

student@student-VirtualBox:~$ wget https://repo.zabbix.com/zabbix/7.0/ubuntu/pool/main/z/zabbix-release/zabbix-release_7.0-1+ubuntu22.04_all.deb
--2024-06-21 16:53:14-- https://repo.zabbix.com/zabbix/7.0/ubuntu/pool/main/z/zabbix-release/zabbix-release_7.0-1+ubuntu22.04_all.deb
Визначення імені repo.zabbix.com (repo.zabbix.com)... 178.128.6.101, 2604:a880:2:d0::2062:d001
Встановлення з'єднання з repo.zabbix.com (repo.zabbix.com)|178.128.6.101|:443..
. з'єднано.
HTTP-запит надіслано, очікуємо на відповідь... 200 OK
Довжина: 6012 (5,9K) [application/octet-stream]
Зберігаємо до 'zabbix-release_7.0-1+ubuntu22.04_all.deb'

zabbix-release_7.0- 100%[=====] 5,87K ---KB/s за 0s

2024-06-21 16:53:16 (1,31 GB/s) - 'zabbix-release_7.0-1+ubuntu22.04_all.deb' збережено [6012/6012]

student@student-VirtualBox:~$ sudo dpkg -i zabbix-release_7.0-1+ubuntu22.04_all.deb
[sudo] пароль до student:
Вибір раніше не обраного пакунку zabbix-release.
(Читання бази даних ... на дану мить встановлено 183924 файли та каталоги.)
Приготування до розпакування zabbix-release_7.0-1+ubuntu22.04_all.deb ...
Розпакування zabbix-release (1:7.0-1+ubuntu22.04)...
Налаштовування zabbix-release (1:7.0-1+ubuntu22.04) ...
student@student-VirtualBox:~$

```

Рисунок 3.19 – Встановлення Zabbix-агента

```

student@student-VirtualBox:~$ sudo apt install zabbix-agent
Зчитування переліків пакунків... Виконано
Побудова дерева залежностей... Виконано
Зчитування інформації про стан... Виконано
Буде встановлено такі додаткові пакунки:
  libmodbus5
НОВІ пакунки, які будуть встановлені:
  libmodbus5 zabbix-agent
оновлено 0, встановлено 2 нових, 0 відмічено для видалення і 506 не оновлено.

```

Рисунок 3.20 – Встановлення Zabbix-агента

```

student@student-VirtualBox:~$ systemctl restart zabbix-agent
student@student-VirtualBox:~$ systemctl enable zabbix-agent
Synchronizing state of zabbix-agent.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable zabbix-agent

```

Рисунок 3.21 – Перезапуск Zabbix-агента

```

GNU nano 6.2 /etc/zabbix/zabbix_agentd.conf *
# Server=

Server=192.168.9.1

### Option: ListenPort
# Agent will listen on this port for connections from
#

```

Рисунок 3.22 – Налаштування Zabbix-агента

		Бобер Д. В.			ККІКБ.КР.Б – 125 – 01 – ПЗ	Арк.
		Фальковський І. Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		47

```
student@student-VirtualBox:~$ sudo systemctl status zabbix-agent
● zabbix-agent.service - Zabbix Agent
   Loaded: loaded (/lib/systemd/system/zabbix-agent.service; enabled; vendor preset: enabled)
   Active: active (running) since Fri 2024-06-21 18:21:24 EEST; 1min 11s ago
     Main PID: 5438 (zabbix_agentd)
    CGroup: /systemd/system/zabbix-agent.service
            └─ 5438 /usr/sbin/zabbix_agentd
```

Рисунок 3.23 – Перевірка статусу агента

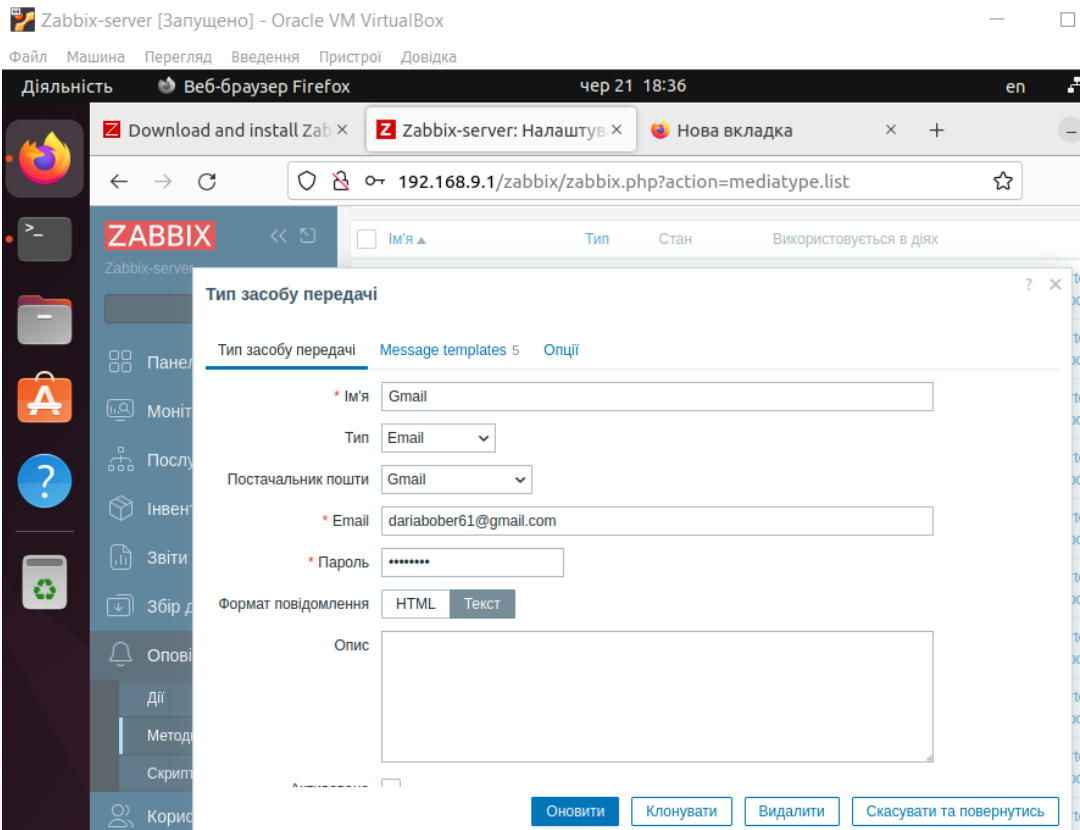


Рисунок 3.24 – Налаштування Zabbix-сповіщень

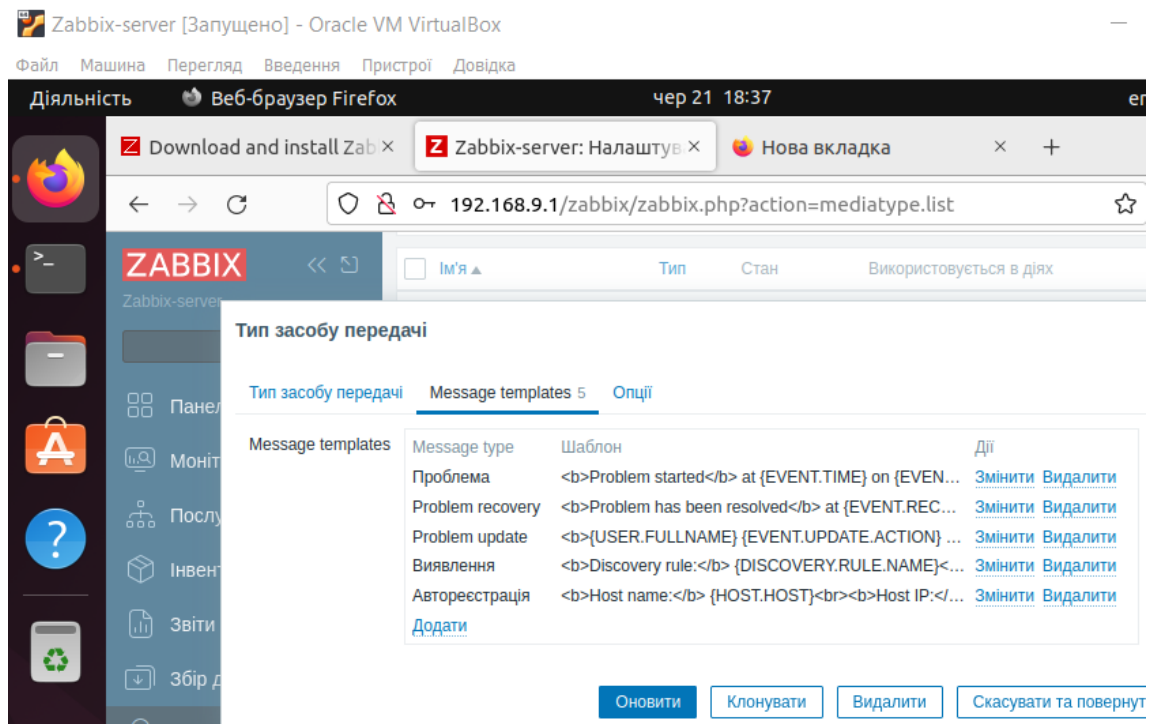


Рисунок 3.25 – Налаштування Zabbix-сповіщень

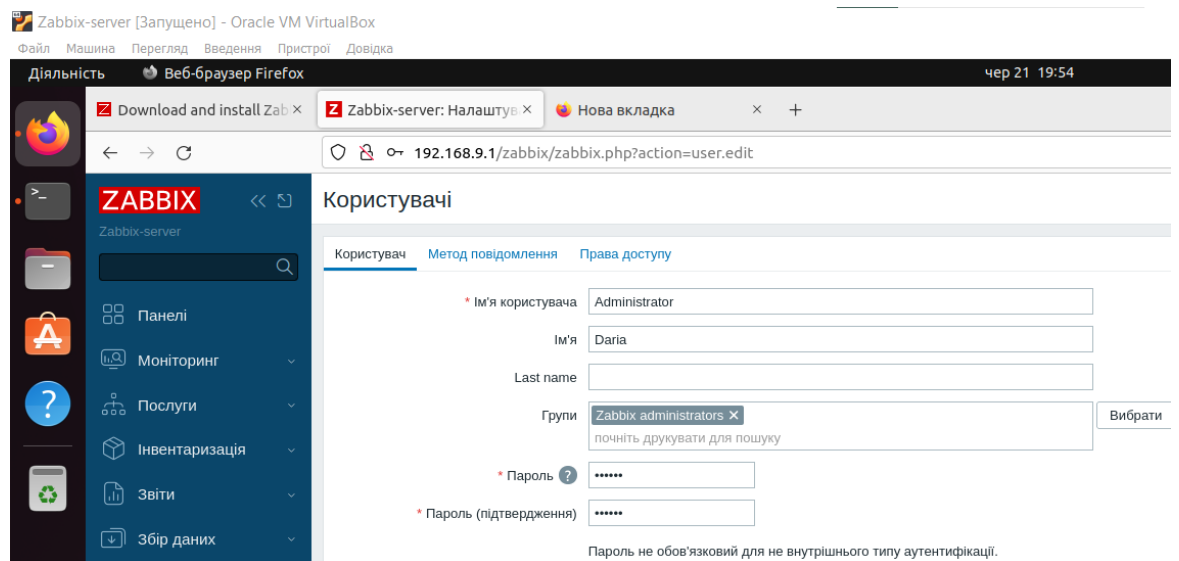


Рисунок 3.26 – Створення користувача

		Бобер Д. В.			ККІКБ.КР.Б – 125 – 01 – ПЗ	Арк.
		Фальковський І. Г.				49
Змн.	Арк.	№ докум.	Підпис	Дата		

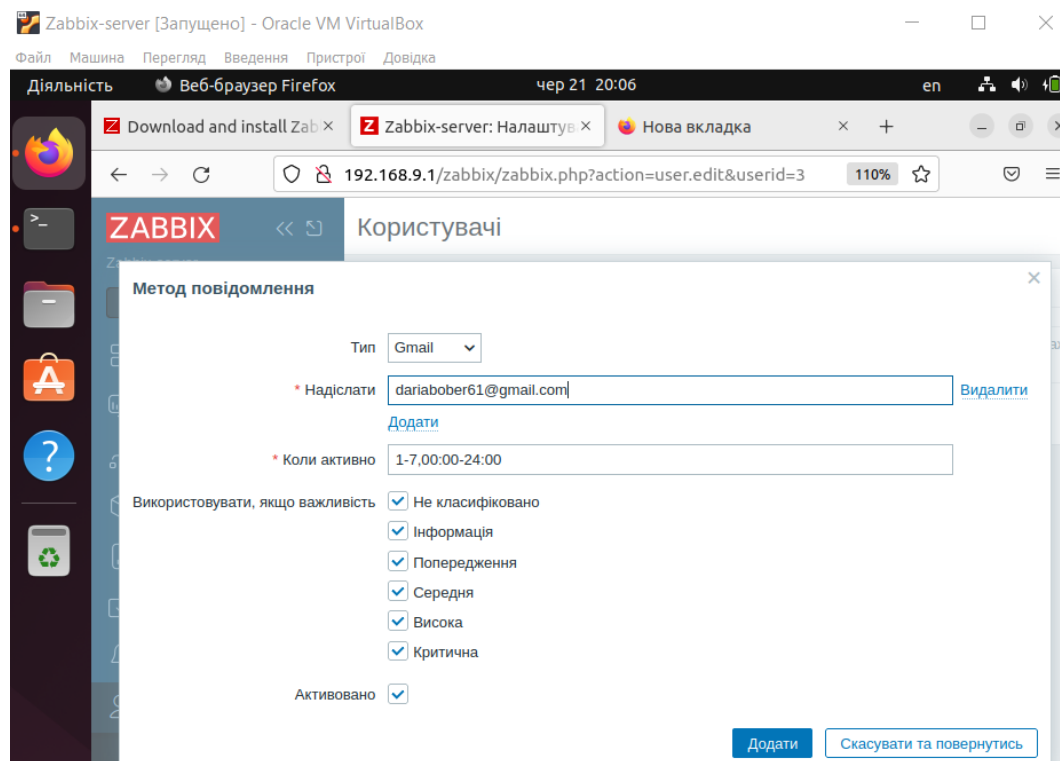


Рисунок 3.27 – Налаштування сповіщень для створеного користувача

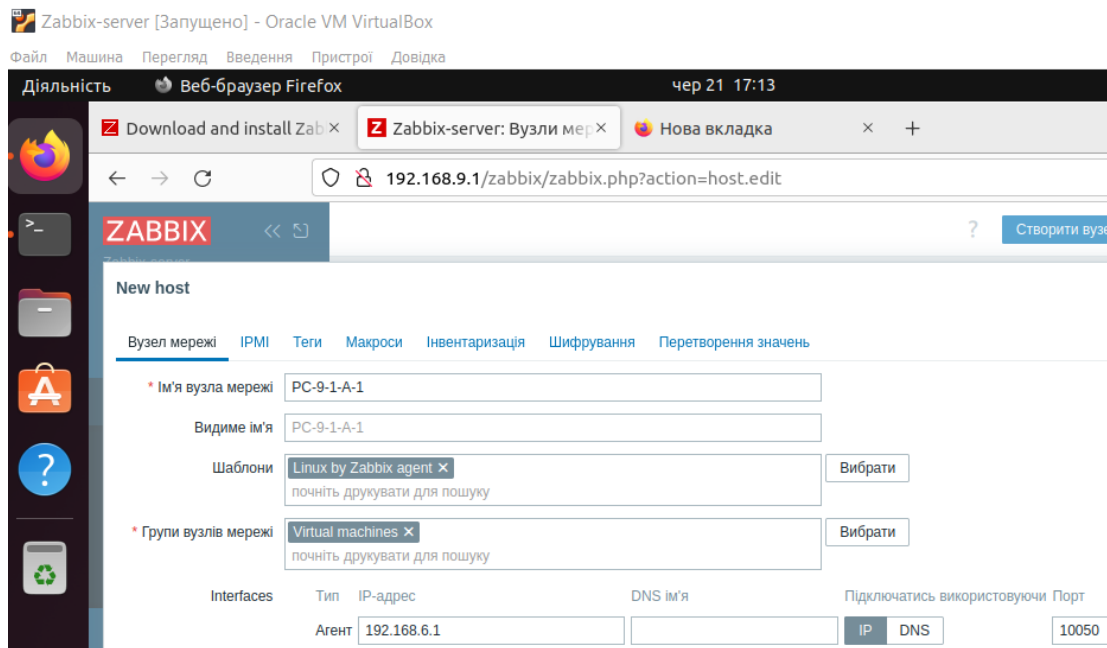


Рисунок 3.28 – Додавання вузла мережі

		Бобер Д. В.			ККІКБ.КР.Б – 125 – 01 – ПЗ	Арк.
		Фальковський І. Г.				50
Змн.	Арк.	№ докум.	Підпис	Дата		

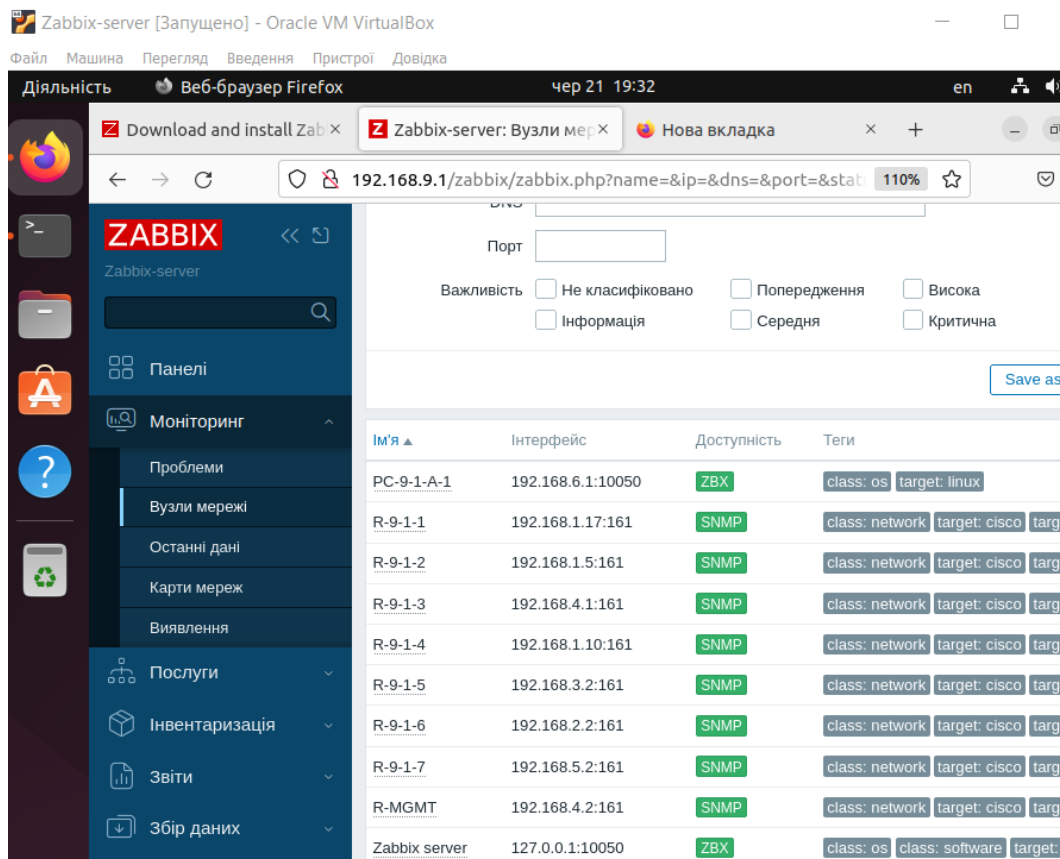


Рисунок 3.29 – Перевірка доступності пристроїв

3.2 Дослідження рівня захищеності мережі

Kali Linux - це дистрибутив операційної системи на основі Debian, спеціально розроблений для тестування на проникнення та дослідження безпеки. Включає широкий спектр інструментів, що допомагають фахівцям з інформаційної безпеки оцінювати захищеність мереж і систем. Цей розділ описує, як використовувати Kali Linux для перевірки мереж на наявність вразливостей і підвищення їх безпеки.

Kali Linux містить сотні інструментів для тестування на проникнення, включаючи:

- інструмент nmap для сканування мереж, який дозволяє виявити активні хости, відкриті порти, сервіси та операційні системи на цільових пристроях, використовується для збору інформації про мережу та її структуру;

- аналізатор мережевих протоколів Wireshark, що дозволяє досліджувати трафік у реальному часі, корисний для виявлення підозрілої активності та аналізу безпеки мережевого зв'язку;
- платформа Metasploit для розробки, тестування та використання експлойтів, яка дозволяє виявляти вразливості у системах та перевіряти ефективність засобів захисту;
- комплект інструментів для тестування безпеки бездротових мереж Aircrack-ng, включаючи перехоплення трафіку та злом WEP/WPA-ключів;
- потужний інструмент для злому паролів John the Ripper, що підтримує різні формати хешів і алгоритми;
- інтегрована платформа для тестування безпеки веб-додатків Burp Suite, яка надає інструменти для аналізу та маніпуляції HTTP запитів, виявлення вразливостей та виконання автоматизованих сканувань.

Kali Linux є незамінним інструментом для фахівців з кібербезпеки, що дозволяє проводити всебічні дослідження захищеності мереж і систем та має безліч інших інструментів тестування. Використовуючи широкий спектр вбудованих інструментів, можна ефективно виявляти та усувати вразливості, забезпечуючи надійну безпеку інформаційних ресурсів.

Для реалізації атаки DHCP Server Spoofing було підключено фальшивий DHCP-сервер. Досліджено стан робочих станцій та комунікаційних пристроїв під час проведення атаки. Перевірено можливість проведення інформаційного обміну під час та після проведення атаки. Вказано виявлені ознаки, які свідчать про факт атаки. Атаку реалізовано з використанням Ettercap з віртуальної машини Kali-Linux. Дану віртуальну машину було під'єднано до підмережі А. [22]

		Бобер Д. В.			ККІКБ.КР.Б – 125 – 01 – ПЗ	Арк.
		Фальковський І. Г.				52
Змн.	Арк.	№ докум.	Підпис	Дата		

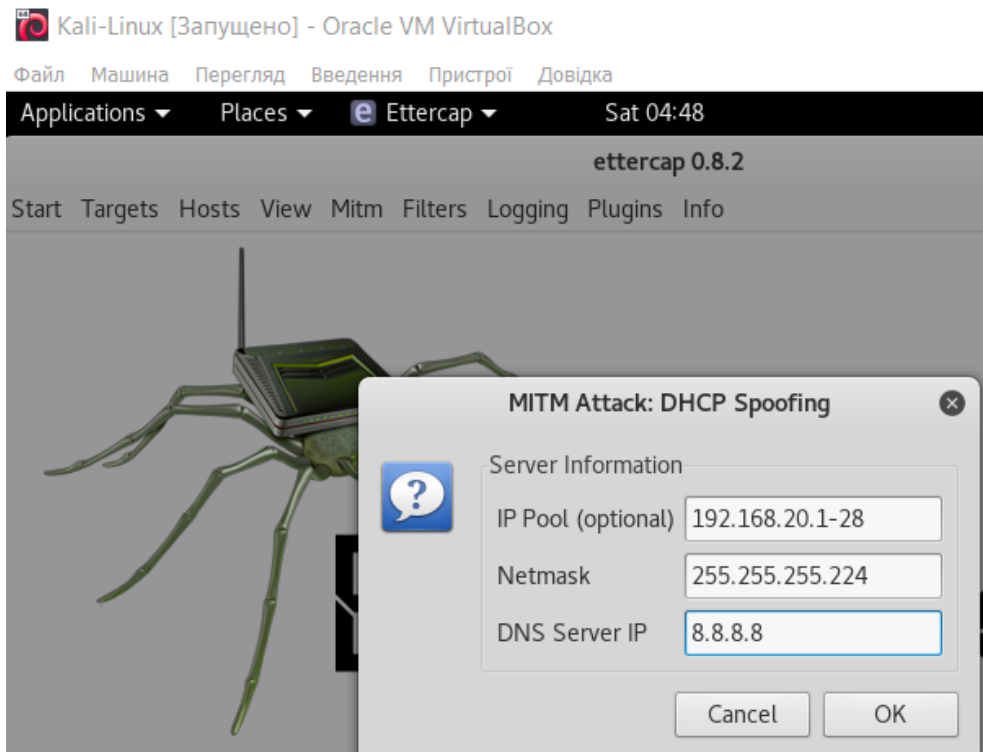


Рисунок 3.30 – Реалізація атаки DHCP Server Spoofing



Рисунок 3.31 – Реалізація атаки DHCP Server Spoofing

		Бобер Д. В.			ККІКБ.КР.Б – 125 – 01 – ПЗ	Арк.
		Фальковський І. Г.				53
Змн.	Арк.	№ докум.	Підпис	Дата		

```

PC-9-1-A-2 - PuTTY
ip dhcp -r
DORA IP 192.168.20.1/27 GW 192.168.6.30

```

Рисунок 3.32 – Налаштування динамічної IP-адресації на одній з робочих станцій

3.4 Налаштування засобів захисту та дослідження стійкості системи моніторинг

Аутентифікація пакетів протоколу маршрутизації EIGRP з використанням алгоритму MD5 забезпечує перевірку та підтвердження достовірності інформації про маршрути, що передається між маршрутизаторами. Цей процес полягає в створенні цифрових підписів за допомогою спільного ключа, який використовується для шифрування інформації перед відправкою. Отримуючи дані, інший маршрутизатор може перевірити цей підпис, щоб підтвердити їхню відповідність надісланим даним. Такий підхід гарантує, що тільки дійсні маршрутизатори з відомим ключем можуть надсилати та отримувати маршрутні дані, що мінімізує ризик введення недейсних даних маршрутизації у мережу і зменшує можливість атак. [21]

```

R-9-1-1(config)#key chain EIGRP_KEY
R-9-1-1(config-keychain)#key 1
R-9-1-1(config-keychain-key)#key-string kb201
R-9-1-1(config-keychain-key)#exit
R-9-1-1(config-keychain)#exit
R-9-1-1(config)#int f0/0
R-9-1-1(config-if)#ip authentication mode eigrp 1 md5
R-9-1-1(config-if)#ip authentication key-chain eigrp 1 EIGRP_KEY
R-9-1-1(config-if)#exit
R-9-1-1(config)#int f0/1
R-9-1-1(config-if)#ip authentication mode eigrp 1 md5
R-9-1-1(config-if)#ip authentication key-chain eigrp 1 EIGRP_KEY
R-9-1-1(config-if)#exit
R-9-1-1(config)#int f1/0

```

		Бобер Д. В.			ККІКБ.КР.Б – 125 – 01 – ПЗ	Арк.
		Фальковський І. Г.				54
Змн.	Арк.	№ докум.	Підпис	Дата		

```

R-9-1-1(config-if)#ip authentication mode eigrp 1 md5
R-9-1-1(config-if)#ip authentication key-chain eigrp 1 EIGRP_KEY
R-9-1-1(config-if)#exit
R-9-1-1(config)#int f2/0
R-9-1-1(config-if)#ip authentication mode eigrp 1 md5
R-9-1-1(config-if)#ip authentication key-chain eigrp 1 EIGRP_KEY
R-9-1-1(config-if)#exit

```

Проведено налагодження засобів захисту від атак на сервіси протоколу DHCP на комунікаційних пристроях мережі. Запустили на виконання відповідні атаки. Перевірено можливість проведення інформаційного обміну та досліджено стан робочих станцій та комунікаційних пристроїв під час та після проведення атаки.

```

SW-9-1-A#conf t
SW-9-1-A(config)#int range e0/0
SW-9-1-A(config-if-range)#ip dhcp snooping trust
SW-9-1-A(config-if-range)#ip dhcp snooping limit rate 256
SW-9-1-A(config-if-range)#exit

```

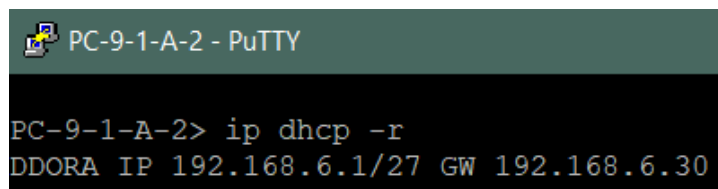


Рисунок 3.33 – Налагодження динамічної IP-адресації на одній з робочих станцій

		Бобер Д. В.			ККІКБ.КР.Б – 125 – 01 – ПЗ	Арк.
		Фальковський І. Г.				55
Змн.	Арк.	№ докум.	Підпис	Дата		

```

SW-9-1-A - PuTTY
SW-9-1-A#show ip dhcp snooping
Switch DHCP snooping is disabled
Switch DHCP gleaning is disabled
DHCP snooping is configured on following VLANs:
none
DHCP snooping is operational on following VLANs:
none
DHCP snooping is configured on the following L3 Interfaces:

Insertion of option 82 is enabled
  circuit-id default format: vlan-mod-port
  remote-id: aabb.cc00.0100 (MAC)
Option 82 on untrusted port is not allowed
Verification of hwaddr field is enabled
Verification of giaddr field is enabled
DHCP snooping trust/rate is configured on the following Interfaces:

Interface                Trusted    Allow option    Rate limit (pps)
-----
Ethernet0/0              yes       yes             256
Custom circuit-ids:

```

Рисунок 3.34 – Виконання команди show ip dhcp snooping

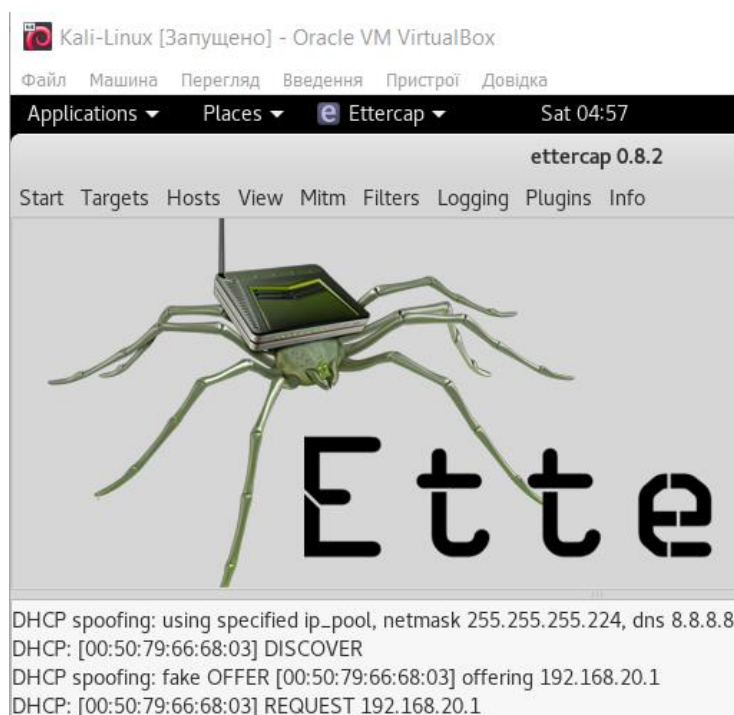


Рисунок 3.35 – Захист пристроїв від атаки

PSK (Pre-Shared Key) Encryption є важливим аспектом забезпечення безпеки при передачі даних у системі моніторингу Zabbix. Використання PSK дозволяє шифрувати трафік між Zabbix-сервером, агентами та проксі-серверами, забезпечуючи конфіденційність та цілісність даних. PSK Encryption у Zabbix є ефективним

способом захисту передаваних даних між серверами, агентами та проксі-серверами. Використання PSK значно підвищує рівень безпеки, забезпечуючи захист конфіденційності та цілісності даних в системі моніторингу. [22]

```
student@student-VirtualBox:~$ sudo sh -c "openssl rand -hex 32 > /etc/zabbix/zabbix_agentd.psk"
[sudo] пароль до student:
student@student-VirtualBox:~$ cat /etc/zabbix/zabbix_agentd.psk
> ^C
student@student-VirtualBox:~$ cat /etc/zabbix/zabbix_agentd.psk
9e3da10827d7b3c876773bc7cf1d65d6e14ec7e54abdd5a63420a55f6148dcbe
```

Рисунок 3.36 – Генерування PSK

```
GNU nano 6.2 /etc/zabbix/zabbix_agentd.conf *
#           psk           - connect using TLS and a pre-shared key
#           cert          - connect using TLS and a certificate
#
# Mandatory: yes, if TLS certificate or PSK parameters are defined (even for 'b
# Default:
# TLSConnect=unencrypted
TLSConnect=psk
### Option: TLSAccept
#           What incoming connections to accept.
#           Multiple values can be specified, separated by comma:
#           unencrypted - accept connections without encryption
#           psk         - accept connections secured with TLS and a pre-sh
#           cert        - accept connections secured with TLS and a certifi
#
# Mandatory: yes, if TLS certificate or PSK parameters are defined (even for 'b
# Default:
# TLSAccept=unencrypted
TLSAccept=psk
```

Рисунок 3.37 – Редагування конфігураційного файлу

```
GNU nano 6.2 /etc/zabbix/zabbix_agentd.conf *
### Option: TLSPSKIdentity
#           Unique, case sensitive string used to identify the pre-shared key.
#
# Mandatory: no
# Default:
TLSPSKIdentity=PSK 001
### Option: TLSPSKFile
#           Full pathname of a file containing the pre-shared key.
#
# Mandatory: no
# Default:
TLSPSKFile=/etc/zabbix/zabbix_agent.psk
```

Рисунок 3.38 – Редагування конфігураційного файлу

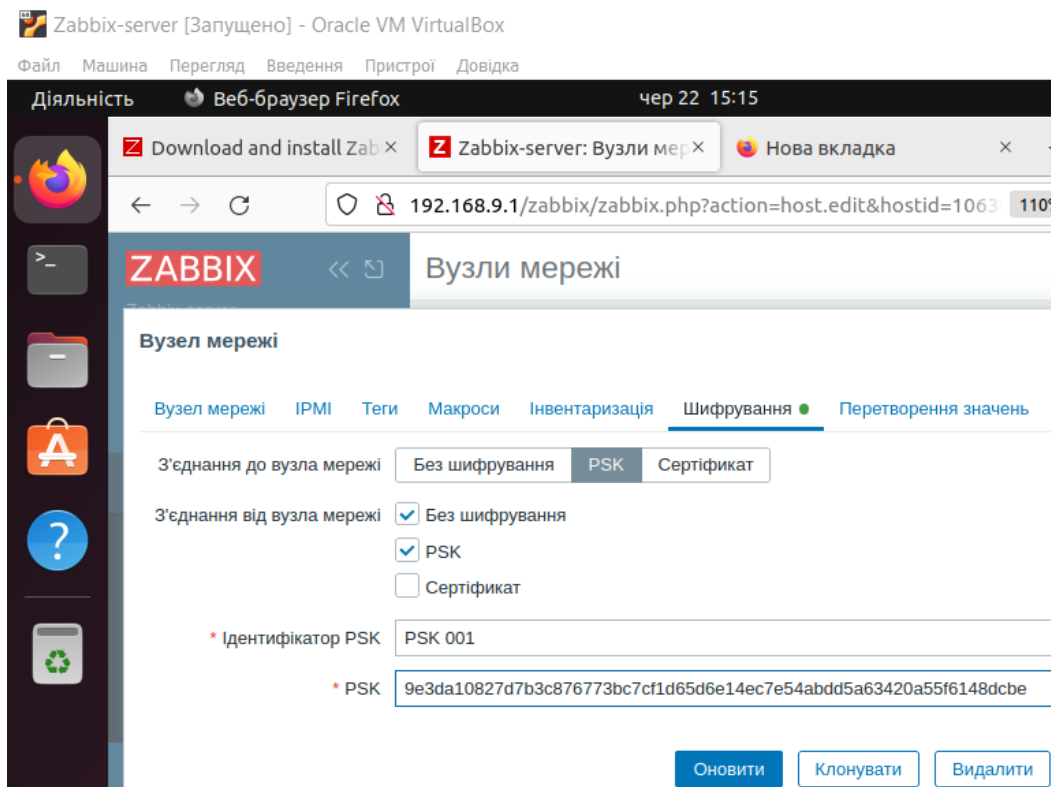


Рисунок 3.39 – Додавання шифрування на основному сервері

```
student@student-VirtualBox:~$ sudo systemctl status zabbix-agent
● zabbix-agent.service - Zabbix Agent
   Loaded: loaded (/lib/systemd/system/zabbix-agent.service; e
   Active: active (running) since Fri 2024-06-21 18:21:24 EEST
   Main PID: 5438 (zabbix_agentd)
```

Рисунок 3.40 – Перевірка статусу агента

		Бобер Д. В.			ККІКБ.КР.Б – 125 – 01 – ПЗ	Арк.
		Фальковський І. Г.				58
Змн.	Арк.	№ докум.	Підпис	Дата		

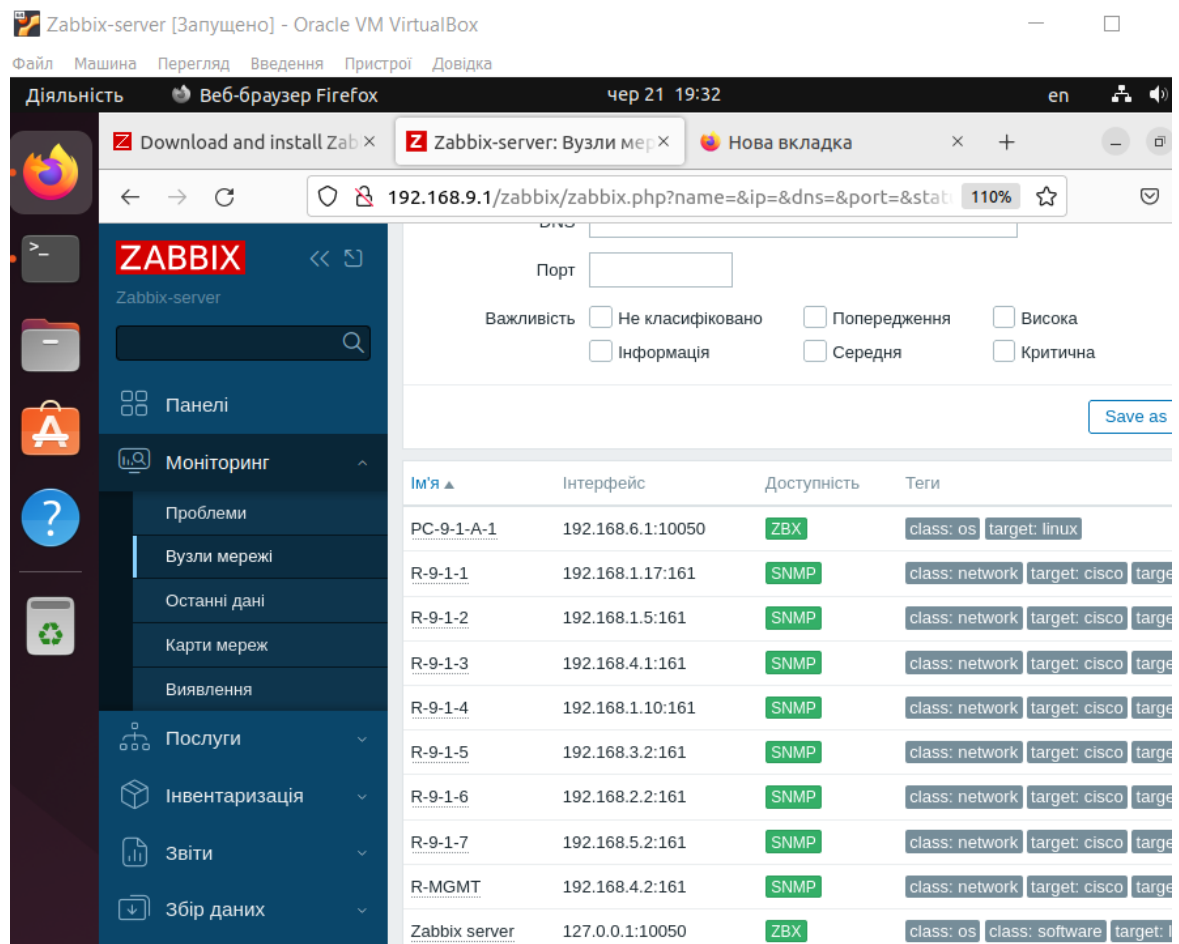


Рисунок 3.41 – Перевірка доступності пристроїв

Висновки до третього розділу

У першому підрозділі проаналізовано мережне обладнання, яке відповідає вимогам проекту мережі. Вибрано маршрутизатори та комутатори від компанії Cisco.

У другому підрозділі налаштовано параметри IP-адресації, DHCP-серверів, було налаштовано Zabbix-сервери, SNMP-агенти та Zabbix-агенти, а також маршрутизацію за протоколом EIGRP. Перевірено правильність функціонування налаштувань.

У третьому підрозділі проведено аналіз основних проблем безпеки налаштованої мережі. Проведено тестування на проникнення та виявлення можливих інцидентів кібербезпеки.

		Бобер Д. В.			ККІКБ.КР.Б – 125 – 01 – ПЗ	Арк.
		Фальковський І. Г.				59
Змн.	Арк.	№ докум.	Підпис	Дата		

У четвертому підрозділі налаштовано засоби захисту від атак на протоколи та механізми мережі. Повторно здійснено спроби атаки для перевірки правильності налаштувань та функціонування безпекових рішень.

		Бобер Д. В.			ККІКБ.КР.Б – 125 – 01 – ПЗ	Арк.
		Фальковський І. Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		60

ВИСНОВКИ

В результаті виконання випускної кваліфікаційної роботи було проведено проектування системи моніторингу захищеної мережі для виявлення та аналізу кіберзагроз в захищеній мережі на основі Zabbix з використанням емулятора GNS3. Досліджено особливості функціонування та безпеки системи моніторингу Zabbix. Обґрунтування актуальності теми оцінює важливість Zabbix-системи.

У першому розділі розглянуто основні теоретичні аспекти функціонування та захисту системи моніторингу Zabbix, також проведено порівняння з іншими системами моніторингу. Проаналізувавши зібрану інформацію було обрано такі інструменти: Zabbix-сервер, компоненти якого знаходяться на одній робочій машині, пасивний Zabbix-агент, SNMP версії 3. Також було обрано шифрування PSK між Zabbix-сервером та Zabbix-агентом.

В другому розділі було спроектовано загальну топологію мережі та локальні підмережі з використанням редактору Draw.io. Також розроблено схему адресації мережі, враховуючи можливість розширення. Проведено аналіз можливих загроз мережі з урахуванням використовуваних протоколів. Основними загрозами визначено вразливість SNMP Community String Attack, атаки на DHCP, можливі атаки перевантаження ЦП та ОП маршрутизатора, збирання даних Zabbix сторонніми користувачами. Створено модель загроз мережі за допомогою OWASP Threat Dragon.

У третьому розділі проаналізовано мережне обладнання, яке відповідає вимогам проекту мережі. Вибрано маршрутизатори CISCO3945/K9, Cisco 3660 та комутатори Cisco Catalyst 2960. Налаштовано параметри IP-адресації, DHCP-серверів, було налаштовано Zabbix-сервери, SNMP-агенти та Zabbix-агенти, а також маршрутизацію за протоколом EIGRP. Проведено аналіз основних проблем безпеки налаштованої мережі. Проведено дослідження рівня захищеності мережі, здійснивши атаку DHCP Server Spoofing. У четвертому підрозділі налаштовано засоби захисту від атак на протоколи та механізми мережі, а саме: автентифікацію пакетів протоколу маршрутизації EIGRP з використанням алгоритму MD5, налагодження засобів захисту від атак на сервіси протоколу DHCP на комунікаційних пристроях мережі, налагоджено використання PSK дозволяє шифрувати трафік між Zabbix-

		Бобер Д. В.			ККІКБ.КР.Б – 125 – 01 – ПЗ	Арк.
		Фальковський І. Г.				61
Змн.	Арк.	№ докум.	Підпис	Дата		

сервером, Zabbix-агентами Повторно реалізовано спробу атаки DHCP Server Spoofing, перевірено доступність Zabbix-агента.

В ході виконання кваліфікаційної роботи було розроблено проект системи моніторингу захищеної мережі з використанням Zabbix, досліджено її можливості, реалізовано заходи безпеки та проведено тестування стійкості мережі.

		Бобер Д. В.			ККІКБ.КР.Б – 125 – 01 – ПЗ	Арк.
		Фальковський І. Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		62

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Zabbix :: The Enterprise-Class Open Source Network Monitoring Solution.
Zabbix :: The Enterprise-Class Open Source Network Monitoring Solution.
URL: <https://www.zabbix.com/>
2. Professionelles Monitoring mit Zabbix | IT-Administrator Magazin. Online | IT-Administrator Magazin. URL: <https://www.it-administrator.de/Monitoring-mit-Zabbix>
3. Zabbix Agent: Active vs. Passive - Zabbix Blog. Zabbix Blog. URL: <https://blog.zabbix.com/zabbix-agent-active-vs-passive/9207/>
4. Zabbix supervision on a remote infrastructure with proxy and PSK-based encryption · Brendan Abolivier. Brendan Abolivier. URL: <https://brendan.abolivier.bzh/zabbix-proxy-encryption/>
5. 2 Active agent autoregistration. Zabbix :: The Enterprise-Class Open Source Network Monitoring Solution. URL: https://www.zabbix.com/documentation/current/en/manual/discovery/auto_registration
6. 5 Receiving problem notification. Zabbix :: The Enterprise-Class Open Source Network Monitoring Solution. URL: <https://www.zabbix.com/documentation/current/en/manual/quickstart/notification>
7. Zabbix Tutorial for Beginners: A Step-by-Step Guide. Best Monitoring Tools. URL: <https://bestmonitoringtools.com/zabbix-tutorial-for-beginners-a-step-by-step-guide/>
8. SSH Monitoring with Zabbix - regify WIKI. Welcome to regify wiki - regify WIKI. URL: https://wiki.regify.com/index.php?title=SSH_Monitoring_with_Zabbix
9. Zabbix: Monitor Cisco Switch or Router with SNMP template. Best Monitoring Tools. URL: <https://bestmonitoringtools.com/how-to-monitor-cisco-switch-or-router-with-zabbix/>

		Бобер Д. В.			ККІКБ.КР.Б – 125 – 01 – ПЗ	Арк.
		Фальковський І. Г.				63
Змн.	Арк.	№ докум.	Підпис	Дата		

- 10.4 IPMI checks. Zabbix :: The Enterprise-Class Open Source Network Monitoring Solution. URL: <https://www.zabbix.com/documentation/current/en/manual/config/items/itemtypes/ipmi>
- 11.Proxy:: The Enterprise-Class Open Source Network Monitoring Solution. URL: <https://www.zabbix.com/documentation/current/en/manual/concepts/proxy>
- 12.Deploying a Zabbix proxy | Packt Hub. Packt Hub. URL: <https://hub.packtpub.com/deploying-zabbix-proxy/>
- 13.Cyber Gateway - Zabbix Proxy Active Passive. URL: <https://cyber-gateway.net/nfo/37934-zabbix-proxy-active-passive>
- 14.Vacche A. D. Mastering Zabbix - Second Edition. Packt Publishing, Limited, 2015.
- 15.17 Encryption. Zabbix :: The Enterprise-Class Open Source Network Monitoring Solution. URL: <https://www.zabbix.com/documentation/current/en/manual/encryption>
- 16.Gratas B. Top 9 Zabbix Alternatives in 2023: Find the Best Monitoring Tool. URL: <https://blog.invgate.com/zabbix-alternative>
- 17.Ієрархічна модель мережі від Cisco. URL: <https://www.telesphera.net/blog/model-mereghi-vid-cisco.html>
- 18.DHCP attack definition â□□ Glossary. NordVPN. URL: <https://nordvpn.com/uk/cybersecurity/glossary/dhcp-attack/>
- 19.Threat Modeling | HackTricks. HackTricks | HackTricks. URL: <https://book.hacktricks.xyz/v/ua/generic-methodologies-and-resources/threat-modeling>
- 20.Cisco: Software, Network, and Cybersecurity Solutions. Cisco. URL: <https://www.cisco.com/site/ca/en/index.html>
- 21.How to configure EIGRP Authentication. NetworkLessons.com. URL: <https://networklessons.com/eigrp/how-to-configure-eigrp-authentication>
- 22.Enable PSK Encryption for Zabbix Agents - Zabbix Tutorials. SBCODE Tutorials. URL: <https://sbcode.net/zabbix/agent-psk-encryption/>

		Бобер Д. В.			ККІКБ.КР.Б – 125 – 01 – ПЗ	Арк.
		Фальковський І. Г.				64
Змн.	Арк.	№ докум.	Підпис	Дата		

ДОДАТКИ

		Бобер Д. В.			ККІКБ.КР.Б – 125 – 01 – ПЗ	Арк.
		Фальковський І. Г.				65
Змн.	Арк.	№ докум.	Підпис	Дата		

Детальна схема побудованої мережі в GNS3

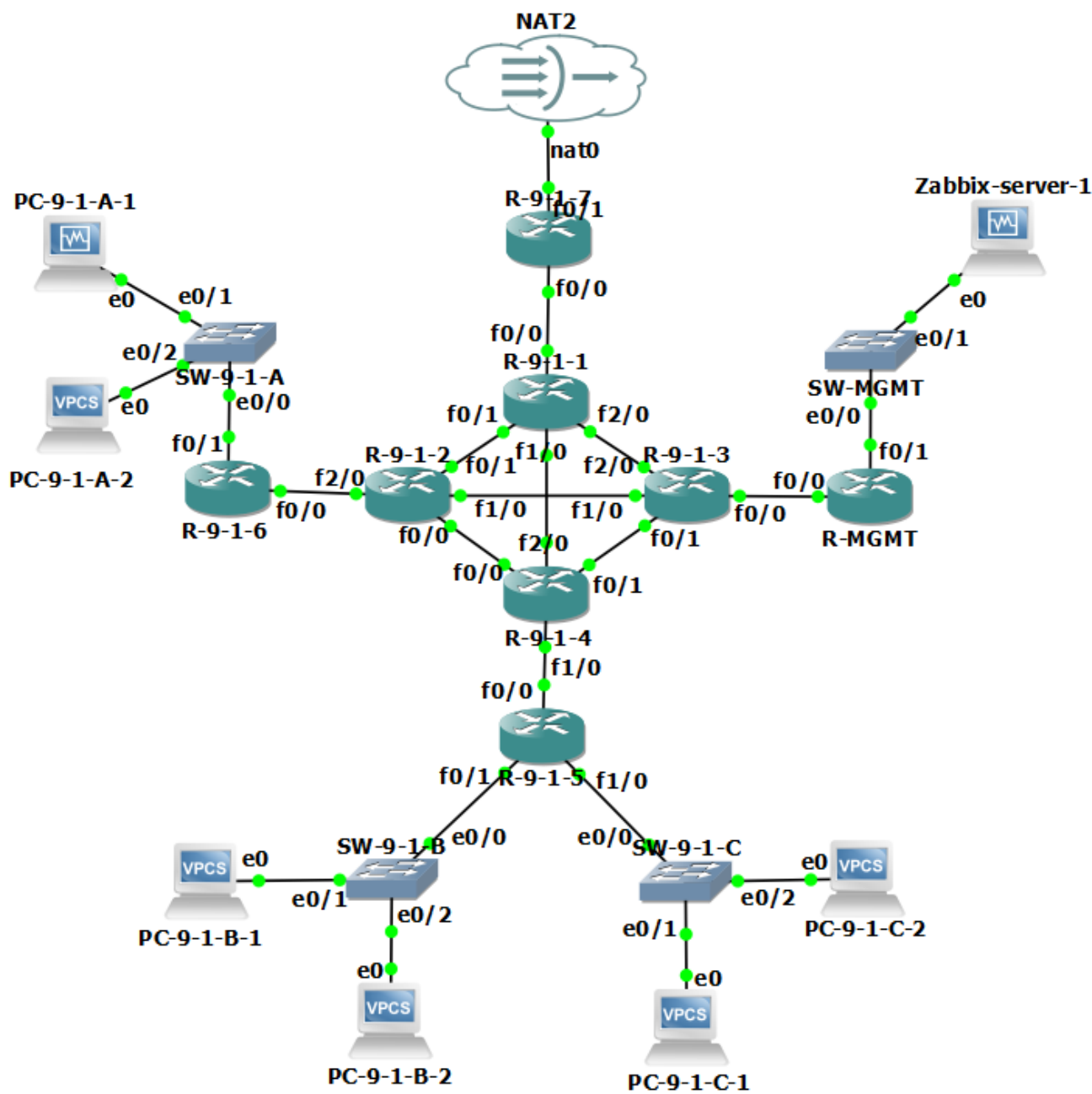


Рисунок А.1 – Схема побудованої мережі в емуляторі GNS 3

ОС, на яких можливо розгорнути Zabbix

Частота оновлень	Документація	Складність встановлення	Поширеність	Вартість	Стабільність	Засновник	ОС
Регулярно	Докладна	Середня	Висока	Безкоштовна	Висока	CloudLinux	Alma Linux
6 місяців	Добра	Середня	Висока	Безкоштовна	Висока	Red Hat	CentOS
Регулярно	Відмінна	Середня	Висока	Безкоштовна	Дуже висока	The Debian Project	Debian
Регулярно	Відмінна	Середня	Середня	Безкоштовна	Дуже висока	The Debian Project	Debian(arm64)
1 рік	Відмінна	Легка	Висока	Безкоштовна	Висока	Проект OpenSUSE	OpenSUSE Leap
Регулярно	Докладна	Середня	Середня	Безкоштовна	Висока	Oracle	Oracle Linux
Регулярно	Добра	Легка	Середня	Безкоштовна	Висока	Raspberry Pi Foundation	Raspberry Pi OS
3 роки	Відмінна	Середня	Висока	Комерційна	Дуже висока	Red Hat	Red Hat Enterprise Linux
6 місяців	Відмінна	Середня	Середня	Безкоштовна	Висока	Rocky Enterprise Software Foundation	Rocky Linux
2 – 3 роки	Відмінна	Середня	Середня	Безкоштовна	Дуже висока	Novell	SUSE Linux Enterprise Server
6 місяців	Відмінна	Легка	Висока	Безкоштовна	Висока	Canonical Ltd	Ubuntu
6 місяців	Відмінна	Легка	Середня	Безкоштовна	Висока	Canonical Ltd	Ubuntu (arm64)

Лістинг конфігураційних файлів всіх пристроїв мережі

```

R-9-1-1#sh running-conf
Building configuration...
Current configuration : 1926 bytes
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
hostname R-9-1-1
boot-start-marker
boot-end-marker
no aaa new-model
memory-size iomem 5
no ip icmp rate-limit unreachable
ip cef
no ip domain lookup
ip auth-proxy max-nodata-conns 3
ip admission max-nodata-conns 3
multilink bundle-name authenticated
key chain EIGRP_KEY
  key 1
    key-string kb201
archive
  log config
  hidekeys
ip tcp synwait-time 5
interface FastEthernet0/0
  description Link-To-R-9-1-7
  ip address 192.168.5.1 255.255.255.252
  ip authentication mode eigrp 1 md5
  ip authentication key-chain eigrp 1 EIGRP_KEY
  duplex auto
  speed auto
interface FastEthernet0/1
  description Link-To-R-9-1-2
  ip address 192.168.1.1 255.255.255.252
  ip authentication mode eigrp 1 md5
  ip authentication key-chain eigrp 1 EIGRP_KEY
  duplex auto
  speed auto
interface FastEthernet1/0
  description Link-To-R-9-1-4
  ip address 192.168.1.13 255.255.255.252
  ip authentication mode eigrp 1 md5
  ip authentication key-chain eigrp 1 EIGRP_KEY
  duplex auto
  speed auto
interface FastEthernet2/0
  description Link-To-R-9-1-3
  ip address 192.168.1.17 255.255.255.252
  ip authentication mode eigrp 1 md5
  ip authentication key-chain eigrp 1 EIGRP_KEY
  duplex auto
  speed auto
router eigrp 1
  network 192.168.1.0 0.0.0.3
  network 192.168.1.12 0.0.0.3
  network 192.168.1.16 0.0.0.3
  network 192.168.5.0 0.0.0.3
  no auto-summary
ip forward-protocol nd
no ip http server
no ip http secure-server
snmp-server group Admin v3 priv read snmpzabbix
snmp-server view adminrw iso included
no cdp log mismatch duplex
control-plane
line con 0
  exec-timeout 0 0
  privilege level 15
  logging synchronous
line aux 0
  exec-timeout 0 0

```

		Бобер Д. В.			ККІКБ.КР.Б – 125 – 01 – ПЗ	Арк.
		Фальковський І. Г.				68
Змн.	Арк.	№ докум.	Підпис	Дата		

```

privilege level 15
logging synchronous
line vty 0 4
login
end

R-9-1-2#sh running-conf
Building configuration...
Current configuration : 1924 bytes
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
hostname R-9-1-2
boot-start-marker
boot-end-marker
no aaa new-model
memory-size iomem 5
no ip icmp rate-limit unreachable
ip cef
no ip domain lookup
ip auth-proxy max-nodata-conns 3
ip admission max-nodata-conns 3
multilink bundle-name authenticated
key chain EIGRP_KEY
key 1
  key-string kb201
archive
log config
hidekeys
ip tcp synwait-time 5
interface FastEthernet0/0
description Link-To-R-9-1-4
ip address 192.168.1.21 255.255.255.252
ip authentication mode eigrp 1 md5
ip authentication key-chain eigrp 1 EIGRP_KEY
duplex auto
speed auto

```

```

interface FastEthernet0/1
description Link-To-R-9-1-1
ip address 192.168.1.2 255.255.255.252
ip authentication mode eigrp 1 md5
ip authentication key-chain eigrp 1 EIGRP_KEY
duplex auto
speed auto
interface FastEthernet1/0
description Link-To-R-9-1-3
ip address 192.168.1.5 255.255.255.252
ip authentication mode eigrp 1 md5
ip authentication key-chain eigrp 1 EIGRP_KEY
duplex auto
speed auto
interface FastEthernet2/0
description Link-To-R-9-1-6
ip address 192.168.2.1 255.255.255.252
ip authentication mode eigrp 1 md5
ip authentication key-chain eigrp 1 EIGRP_KEY
duplex auto
speed auto
router eigrp 1
network 192.168.1.0 0.0.0.3
network 192.168.1.4 0.0.0.3
network 192.168.1.20 0.0.0.3
network 192.168.2.0 0.0.0.3
no auto-summary
ip forward-protocol nd
no ip http server
no ip http secure-server
snmp-server group Admin v3 priv read snmpzabbix
snmp-server view adminrw iso included
no cdp log mismatch duplex
control-plane
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous

```

		Бобер Д. В.			ККИКБ.КР.Б – 125 – 01 – ПЗ	Арк.
		Фальковський І. Г.				69
Змн.	Арк.	№ докум.	Підпис	Дата		

```

line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
line vty 0 4
login
end
R-9-1-3#sh running-conf
Building configuration...
Current configuration : 1923 bytes
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
hostname R-9-1-3
boot-start-marker
boot-end-marker
no aaa new-model
memory-size iomem 5
no ip icmp rate-limit unreachable
ip cef
no ip domain lookup
ip auth-proxy max-nodata-conns 3
ip admission max-nodata-conns 3
multilink bundle-name authenticated
key chain EIGRP_KEY
key 1
  key-string kb201
archive
log config
hidekeys
ip tcp synwait-time 5
interface FastEthernet0/0
description Link-To-R-MGMT
ip address 192.168.4.1 255.255.255.252
ip authentication mode eigrp 1 md5
ip authentication key-chain eigrp 1 EIGRP_KEY
duplex auto

```

```

speed auto
interface FastEthernet0/1
description Link-To-R-9-1-4
ip address 192.168.1.9 255.255.255.252
ip authentication mode eigrp 1 md5
ip authentication key-chain eigrp 1 EIGRP_KEY
duplex auto
speed auto
interface FastEthernet1/0
description Link-To-R-9-1-2
ip address 192.168.1.6 255.255.255.252
ip authentication mode eigrp 1 md5
ip authentication key-chain eigrp 1 EIGRP_KEY
duplex auto
speed auto
interface FastEthernet2/0
description Link-To-R-9-1-1
ip address 192.168.1.18 255.255.255.252
ip authentication mode eigrp 1 md5
ip authentication key-chain eigrp 1 EIGRP_KEY
duplex auto
speed auto
router eigrp 1
network 192.168.1.4 0.0.0.3
network 192.168.1.8 0.0.0.3
network 192.168.1.16 0.0.0.3
network 192.168.4.0 0.0.0.3
no auto-summary
ip forward-protocol nd
no ip http server
no ip http secure-server
snmp-server group Admin v3 priv read snmpzabbix
snmp-server view adminrw iso included
no cdp log mismatch duplex
control-plane
line con 0
exec-timeout 0 0
privilege level 15

```

		Бобер Д. В.			ККІКБ.КР.Б – 125 – 01 – ПЗ	Арк.
		Фальковський І. Г.				70
Змн.	Арк.	№ докум.	Підпис	Дата		

```

logging synchronous
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
line vty 0 4
login
end

R-9-1-4#sh running-conf
Building configuration...
Current configuration : 1927 bytes
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
hostname R-9-1-4
boot-start-marker
boot-end-marker
no aaa new-model
memory-size iomem 5
no ip icmp rate-limit unreachable
ip cef
no ip domain lookup
ip auth-proxy max-nodata-conns 3
ip admission max-nodata-conns 3
multilink bundle-name authenticated
key chain EIGRP_KEY
key 1
  key-string kb201
archive
log config
hidekeys
ip tcp synwait-time 5
interface FastEthernet0/0
description Link-To-R-9-1-2
ip address 192.168.1.22 255.255.255.252
ip authentication mode eigrp 1 md5

```

```

ip authentication key-chain eigrp 1 EIGRP_KEY
duplex auto
speed auto
interface FastEthernet0/1
description Link-To-R-9-1-3
ip address 192.168.1.10 255.255.255.252
ip authentication mode eigrp 1 md5
ip authentication key-chain eigrp 1 EIGRP_KEY
duplex auto
speed auto
interface FastEthernet1/0
description Link-To-R-9-1-5
ip address 192.168.3.1 255.255.255.252
ip authentication mode eigrp 1 md5
ip authentication key-chain eigrp 1 EIGRP_KEY
duplex auto
speed auto
interface FastEthernet2/0
description Link-To-R-9-1-1
ip address 192.168.1.14 255.255.255.252
ip authentication mode eigrp 1 md5
ip authentication key-chain eigrp 1 EIGRP_KEY
duplex auto
speed auto
router eigrp 1
network 192.168.1.8 0.0.0.3
network 192.168.1.12 0.0.0.3
network 192.168.1.20 0.0.0.3
network 192.168.3.0 0.0.0.3
no auto-summary
ip forward-protocol nd
no ip http server
no ip http secure-server
snmp-server group Admin v3 priv read snmpzabbix
snmp-server view adminrw iso included
no cdp log mismatch duplex
control-plane
line con 0

```

		Бобер Д. В.			ККИКБ.КР.Б – 125 – 01 – ПЗ	Арк.
		Фальковський І. Г.				71
Змн.	Арк.	№ докум.	Підпис	Дата		

```

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

```

R-9-1-5#sh running-conf

Building configuration...

Current configuration : 2059 bytes

version 12.4

service timestamps debug datetime msec

service timestamps log datetime msec

no service password-encryption

hostname R-9-1-5

boot-start-marker

boot-end-marker

no aaa new-model

memory-size iomem 5

no ip icmp rate-limit unreachable

ip cef

no ip dhcp use vrf connected

ip dhcp excluded-address 192.168.7.148

192.168.7.254

ip dhcp excluded-address 192.168.8.148

192.168.8.254

ip dhcp pool Lan-B

network 192.168.7.0 255.255.255.0

default-router 192.168.7.254

dns-server 8.8.8.8

domain-name bober.local

ip dhcp pool Lan-C

network 192.168.8.0 255.255.255.0

default-router 192.168.8.254

dns-server 8.8.8.8

domain-name bober.local

no ip domain lookup

ip auth-proxy max-nodata-conns 3

ip admission max-nodata-conns 3

multilink bundle-name authenticated

key chain EIGRP_KEY

key 1

key-string kb201

archive

log config

hidekeys

ip tcp synwait-time 5

interface FastEthernet0/0

description Link-To-R-9-1-4

ip address 192.168.3.2 255.255.255.252

ip authentication mode eigrp 1 md5

ip authentication key-chain eigrp 1 EIGRP_KEY

duplex auto

speed auto

interface FastEthernet0/1

description Link-To-B

ip address 192.168.7.254 255.255.255.0

duplex auto

speed auto

interface FastEthernet1/0

description Link-To-C

ip address 192.168.8.254 255.255.255.0

duplex auto

speed auto

interface FastEthernet2/0

no ip address

shutdown

duplex auto

speed auto

router eigrp 1

passive-interface FastEthernet0/1

passive-interface FastEthernet1/0

		Бобер Д. В.			ККІКБ.КР.Б – 125 – 01 – ПЗ	Арк.
		Фальковський І. Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		72

```

network 192.168.3.0 0.0.0.3
network 192.168.7.0
network 192.168.8.0
no auto-summary
ip forward-protocol nd
no ip http server
no ip http secure-server
snmp-server group Admin v3 priv read snmpzabbix
snmp-server view adminrw iso included
no cdp log mismatch duplex
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

```

```

R-9-1-6#sh running-conf
Building configuration...
Current configuration : 1780 bytes
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
hostname R-9-1-6
boot-start-marker
boot-end-marker
no aaa new-model
memory-size iomem 5
no ip icmp rate-limit unreachable
ip cef
no ip dhcp use vrf connected

```

```

ip dhcp excluded-address 192.168.6.22
192.168.6.30
ip dhcp pool Lan-A
network 192.168.6.0 255.255.255.224
default-router 192.168.6.30
domain-name bober.local
dns-server 8.8.8.8
no ip domain lookup
ip auth-proxy max-nodata-conns 3
ip admission max-nodata-conns 3
multilink bundle-name authenticated
key chain EIGRP_KEY
key 1
key-string kb201
archive
log config
hidekeys
ip tcp synwait-time 5
interface FastEthernet0/0
description Link-To-R-9-1-2
ip address 192.168.2.2 255.255.255.252
ip authentication mode eigrp 1 md5
ip authentication key-chain eigrp 1 EIGRP_KEY
duplex auto
speed auto
interface FastEthernet0/1
description Link-To-A
ip address 192.168.6.30 255.255.255.224
duplex auto
speed auto
interface FastEthernet1/0
no ip address
shutdown
duplex auto
speed auto
interface FastEthernet2/0
no ip address
shutdown

```

		Бобер Д. В.			ККІКБ.КР.Б – 125 – 01 – ПЗ	Арк.
		Фальковський І. Г.				73
Змн.	Арк.	№ докум.	Підпис	Дата		

```

duplex auto
speed auto
router eigrp 1
  passive-interface FastEthernet0/1
  network 192.168.2.0 0.0.0.3
  network 192.168.6.0 0.0.0.31
  no auto-summary
ip forward-protocol nd
no ip http server
no ip http secure-server
snmp-server group Admin v3 priv read snmpzabbix
snmp-server view adminrw iso included
no cdp log mismatch duplex
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

```

```

R-9-1-7#sh running-conf
Building configuration...
Current configuration : 1719 bytes
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
hostname R-9-1-7
boot-start-marker
boot-end-marker
no aaa new-model
memory-size iomem 5

```

```

no ip icmp rate-limit unreachable
ip cef
no ip domain lookup
ip auth-proxy max-nodata-conns 3
ip admission max-nodata-conns 3
multilink bundle-name authenticated
key chain EIGRP_KEY
  key 1
    key-string kb201
archive
  log config
  hidekeys
ip tcp synwait-time 5
interface FastEthernet0/0
  description Link-To-R-9-1-1
  ip address 192.168.5.2 255.255.255.252
  ip authentication mode eigrp 1 md5
  ip authentication key-chain eigrp 1 EIGRP_KEY
ip nat inside
ip virtual-reassembly
duplex auto
speed auto
interface FastEthernet0/1
  description Link-To-Nat
  ip address dhcp
  ip nat outside
  ip virtual-reassembly
duplex auto
speed auto
interface FastEthernet1/0
  no ip address
  shutdown
duplex auto
speed auto
interface FastEthernet2/0
  no ip address
  shutdown
duplex auto

```

		Бобер Д. В.			ККИКБ.КР.Б – 125 – 01 – ПЗ	Арк.
		Фальковський І. Г.				74
Змн.	Арк.	№ докум.	Підпис	Дата		

```

speed auto
router eigrp 1
 redistribute static
 network 192.168.5.0 0.0.0.3
 network 192.168.122.0
 no auto-summary
 ip forward-protocol nd
 ip route 0.0.0.0 0.0.0.0 192.168.122.1
 no ip http server
 no ip http secure-server
 ip nat inside source list 1 interface FastEthernet0/1
 overload
 access-list 1 permit any
 snmp-server group Admin v3 priv read snmpzabbix
 snmp-server view adminrw iso included
 no cdp log mismatch duplex
 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

R-MGMT#sh running-conf
Building configuration...
Current configuration : 1732 bytes
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
hostname R-MGMT
boot-start-marker

```

```

boot-end-marker
no aaa new-model
memory-size iomem 5
no ip icmp rate-limit unreachable
ip cef
no ip domain lookup
ip domain name bober.local
ip auth-proxy max-nodata-conns 3
ip admission max-nodata-conns 3
multilink bundle-name authenticated
key chain EIGRP_KEY
 key 1
  key-string kb201
username admin secret 5
$1$efw2$iqvZH2b8wx6Q/UmvUWtej/
archive
 log config
  hidekeys
ip tcp synwait-time 5
ip ssh version 2
interface FastEthernet0/0
 description Link-To-R-9-1-3
 ip address 192.168.4.2 255.255.255.252
 ip authentication mode eigrp 1 md5
 ip authentication key-chain eigrp 1 EIGRP_KEY
 duplex auto
 speed auto
interface FastEthernet0/1
 description Link-To-MGMT
 ip address 192.168.9.6 255.255.255.248
 duplex auto
 speed auto
interface FastEthernet1/0
 no ip address
 shutdown
 duplex auto
 speed auto
interface FastEthernet2/0

```

		Бобер Д. В.			ККИКБ.КР.Б – 125 – 01 – ПЗ	Арк.
		Фальковський І. Г.				75
Змн.	Арк.	№ докум.	Підпис	Дата		

```

no ip address
shutdown
duplex auto
speed auto
router eigrp 1
  passive-interface FastEthernet0/1
  network 192.168.4.0 0.0.0.3
  network 192.168.9.0 0.0.0.7
  no auto-summary
ip forward-protocol nd
no ip http server
no ip http secure-server
snmp-server group Admin v3 priv read snmpzabbix
snmp-server view adminrw iso included
no cdp log mismatch duplex
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 local
  transport input ssh
line vty 5 15
  login local
  transport input ssh
end

```

		Бобер Д. В.			ККІКБ.КР.Б – 125 – 01 – ПЗ	Арк.
		Фальковський І. Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		76