

МІНІСТЕРСТВО ФІНАНСІВ УКРАЇНИ
ДЕРЖАВНИЙ ПОДАТКОВИЙ УНІВЕРСИТЕТ

ФАКУЛЬТЕТ ФІНАНСІВ ТА ЦИФРОВИХ ТЕХНОЛОГІЙ
КАФЕДРА КОМП'ЮТЕРНИХ ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ І
СИСТЕМ

КВАЛІФІКАЦІЙНА РОБОТА

на тему: **МОНІТОРИНГ СТАНУ ФУНКЦІОНУВАННЯ КОМП'ЮТЕРНОЇ
МЕРЕЖІ**

Здобувача вищої освіти другого (магістерського) рівня,
II курсу, групи КМІз-21-1, спеціальності 122 «Комп'ютерні науки»,
освітня програма «Інформаційні управляючі системи і технології в економіці»


(підпис)

Мулявки Арсенія Сергійовича
(прізвище, ім'я, по батькові)

Науковий керівник


(підпис)

Погорсловська Ірина Дем'янівна,
к.е.н., доцент
(прізвище, ім'я, по батькові, науковий ступінь,
вчене звання)

Керівник освітньо-
професійної програми


(підпис)

Горбовий Артур Юліанович,
д.т.н., професор
(прізвище, ім'я, по батькові, науковий ступінь,
вчене звання)

Допущено до захисту за рішенням кафедри
протокол від «12» січня 2023 № 6

Завідувач кафедри


(підпис)

Філоненко Михайло Миколайович,
к.ф.-м.н., доцент
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Ірпінь – 2023

Реєстрація № 1

12.01.2023
(дата)



(підпис відповідальної особи)

Результати перевірки

до захисту
(до захисту, на доопрацювання)

12.01.2023
(дата)



(підпис)

Результат захисту

4 (добре)
(оцінка)

13.02.2023
(дата)



(підпис)

Голова комісії:



(підпис)

В.М. Франчук

Члени комісії:



(підпис)

М.М. Філоненко



(підпис)

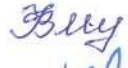
О.В. Редич



(підпис)

Є.В. Котух

БЛАНК ОЦІНЮВАННЯ КВАЛІФІКАЦІЙНОЇ РОБОТИ

Об'єкти контролю	Діапазон оцінки в балах	Фактична кількість балів	Примітки	Дата, П.І.Б.: керівника, голови комісії членів комісії, секретаря, (підписи)
ОЦІНЮВАННЯ КВАЛІФІКАЦІЙНОЇ РОБОТИ КОМІСІЄЮ ПО ЗАХИСТУ				
1. Зміст випускної роботи (якість теоретичного матеріалу, його зв'язок з практичним, вміння представляти матеріал в логічній послідовності, наявність висновків та пропозицій)	від 0 до 30	26		13.02.2023 Франчук В.М.  Філоненко М.М.  Редич О.В.  Котух С.В.  Суховерхня Л.П. 
2. Дотримання вимог щодо оформлення	від 0 до 10	7		
3. Вчасне виконання роботи на всіх етапах у встановлені кафедрою терміни	від 0 до 5	3		
4. Рецензент	від 0 до 5	4		
РАЗОМ БАЛІВ	від 0 до 50	40		

Оцінювання кваліфікаційної роботи науковим керівником - 40 балів.

ПЕРЕВЕДЕННЯ ОЦІНКИ ЗА 100-БАЛЬНОЮ ШКАЛОЮ ДО НАЦІОНАЛЬНОЇ ШКАЛИ ТА ШКАЛИ ЄКТС

Оцінка за 100-бальною шкалою	Оцінка за шкалою ЄКТС	Оцінка за національною шкалою	Дата	П.І.Б.: голови, членів комісії, секретаря, (підпис)
80	B	4 (добре)	13.02.2023	Франчук В.М.  Філоненко М.М.  Редич О.В.  Котух С.В.  Суховерхня Л.П. 

ПРАВИЛА ПЕРЕВЕДЕННЯ ОЦІНОК ДО НАЦІОНАЛЬНОЇ ШКАЛИ ТА ШКАЛИ ЄКТС

Оцінка за 100-бальною шкалою	Оцінка за шкалою ЄКТС	Оцінка за національною шкалою
90-100	A	5 (відмінно)
80-89	B	4 (добре)
70-79	C	
60-69	D	
50-59	E	3 (задовільно)
35-49	FX	2 (незадовільно)

Факультет фінансів та цифрових технологій

Кафедра комп'ютерних та інформаційних технологій і систем

Галузь знань: 12 «Інформаційні технології»

Спеціальність: 122 «Комп'ютерні науки»

Освітня програма: «Інформаційні управляючі системи і технології в економіці»

Затверджую

В.о. завідувача кафедри

 Федотова-Півень І.М.

10. 01. 2022

**Завдання на випускню кваліфікаційну (дипломну) роботу
здобувача вищої освіти**

Мулявки Арсенія Сергійовича

1. Тема випускної кваліфікаційної (дипломної) роботи: **Моніторинг стану функціонування комп'ютерної мережі**

затверджена наказом ректора від 05.01.2022 №4

2. Строк здачі закінченої роботи: 11.01.2023

3. Цільова установка: застосування набутих знань, умінь для здійснення моніторингу комп'ютерної мережі.

Мета роботи: визначення способів та засобів моніторингу стану функціонування комп'ютерної мережі.

Об'єкт дослідження: засоби моніторингу функціонування компонент комп'ютерної мережі.

Предмет дослідження: властивості та характеристики програмно-апаратних засобів моніторингу параметрів комп'ютерної мережі.

4. Вихідні дані до роботи: методи, підходи, програмно-апаратні засоби здійснення моніторингу мережі.

5. Перелік графічного матеріалу: схеми архітектури систем моніторингу, схеми варіантів моніторингу, копії екранів, презентація роботи(.ppt).

6. Зміст випускної кваліфікаційної (дипломної) роботи: Розділ 1. Задачі моніторингу та аналізу параметрів комп'ютерних мереж. 1.1. Моніторинг як засіб аналізу функціонування комп'ютерної мережі. 1.2. Методи моніторингу та аналізу параметрів комп'ютерної мережі. Розділ 2. Аналітичний огляд засобів моніторингу комп'ютерних мереж. 2.1. Архітектура систем моніторингу та механізми моніторингу. 2.2. Програмно-технічні засоби контролю та аналізу стану функціонування комп'ютерних мереж. 2.3. засоби виявлення вторгнень у комп'ютерні системи. Розділ 3. Моніторинг комп'ютерної мережі. 3.1. Контроль наявності вразливостей та помилок конфігурування мережі. 3.2. Визначення завдань та функцій аналізатора протоколів комп'ютерних мереж. 3.3. Відстеження статусу сервісів комп'ютерних мереж.

7. Календарний план виконання роботи

№ п/п	Назва етапів випускної кваліфікаційної (дипломної) роботи	Строк виконання етапів роботи	
		За планом	Фактично
1	2	3	4
1	Вибір теми, підбір літературних джерел, формування структури ДР	24.12.2021	« 24 » 12 2021 р.
2	I. Вступ та I розділ (розкрити сутність і стан дослідження наукової проблематики роботи, після чого навести її загальну характеристику; огляд літератури за темою і вибір конкретних напрямів досліджень)	26.05.2022	« 26 » 05 2022 р.
3	II розділ (аналіз експериментальної частини і методики досліджень)	20.11.2022	« 20 » 11 2022 р.
4	III розділ (проведені теоретичні і (або) експериментальні дослідження та проектні рішення)	30.11.2022	« 30 » 11 2022 р.
5	Висновки	15.12.2022	« 15 » 12 2022 р.
6	Доопрацювання роботи з урахуванням зауважень наукового керівника	10.01.2023	« 10 » 01 2023 р.
7	Отримання відгуку керівника	03.02.2023	« 03 » 02 2023 р.
8	Отримання зовнішньої рецензії	06.02.2023	« 06 » 02 2023 р.

8. Дата видачі завдання 10.01.2022 р.

9. Керівник дипломної роботи  Погореловська І.Д., к.е.н., доцент10. Гарант
освітньо-професійної програми  Горбовий А.Ю., д.т.н., професор11. Завдання до виконання отримав
здобувач вищої освіти  Мулявка А.С.

АНОТАЦІЯ

Моніторинг стану функціонування комп'ютерної мережі

Метою випускної кваліфікаційної (дипломної) роботи є визначення способів та засобів моніторингу стану функціонування комп'ютерної мережі

Завдання, що були вирішені при виконанні роботи:

- визначено задачі та методи моніторингу параметрів комп'ютерних мереж;
- проаналізовано архітектуру систем моніторингу;
- здійснено оцінку можливостей програмно-апаратних засобів контролю наявності вразливостей та помилок конфігурування мережі;
- визначено завдання та функції аналізатора протоколів комп'ютерних мереж;
- проаналізовано можливості систем виявлення вторгнень IDS;
- визначено способи та засоби моніторингу, які забезпечують контроль наявності вразливостей та помилок конфігурування мережі, аналіз протоколів, відстеження статусу сервісів комп'ютерної мережі.

Об'єктом дослідження є засоби моніторингу функціонування компонент комп'ютерної мережі.

Інформаційною базою дослідження є методи, підходи та програмно-апаратні засоби здійснення моніторингу параметрів комп'ютерної мережі, стандарти управління мережевими ресурсами.

За результатами дослідження було сформульовано висновки про необхідність постійного моніторингу стану комп'ютерних мереж з метою контролю наявності вразливостей чи помилок конфігурування мережі, аналізу протоколів та відстеження статусу сервісів, а також запропоновано способи та засоби моніторингу стану функціонування комп'ютерної мережі.

Одержані результати можуть бути використані при формуванні систем моніторингу комп'ютерної мережі, в освітньому процесі при викладанні навчальних дисциплін “Комп'ютерні мережі”, “Технології захисту інформації”.

Дипломна робота містить 56 сторінок, 16 рисунків, 1 таблиця і список використаних джерел з 43 найменувань.

Ключові слова: моніторинг, комп'ютерна мережа, мережеві пристрої, протоколи мереж, аналізатор протоколів, трафік, сніфер, пакети, утіліти, сигнатури, вразливості, вторгнення, аномалії.

Рік виконання дипломної роботи: 2021-2023

Рік захисту роботи: 2023.

SUMMARY

Monitoring of the state of operation of the computer network

The purpose of the final qualification (diploma) work is to determine the methods and means of monitoring the state of computer network functioning

The tasks that were solved during the performance of the work:

- tasks and methods of monitoring parameters of computer networks are defined;
- the architecture of monitoring systems was analyzed;
- assessment of capabilities of software and hardware means of monitoring the presence of vulnerabilities and network configuration errors was carried out;
- the tasks and functions of the computer network protocol analyzer are defined;
- the capabilities of IDS intrusion detection systems were analyzed;
- methods and means of monitoring are defined, which provide control over the presence of vulnerabilities and network configuration errors, analysis of protocols, tracking of the status of computer network services.

The object of the study is the means of monitoring the functioning of computer network components.

The information base of the research is methods, approaches and hardware and software tools for monitoring computer network parameters, network resource management standards.

According to the results of the study, conclusions were drawn about the need for constant monitoring of the state of computer networks in order to control the presence of vulnerabilities or network configuration errors, analysis of protocols and tracking of the status of services, as well as methods and means of monitoring the state of computer network functioning were proposed

The obtained results can be used in the formation of computer network monitoring systems, in the educational process when teaching the educational disciplines “Computer networks”, “Information protection technologies”.

The diploma work contains 56 pages, 16 figures, 1 table, and list of used sources from 43 items.

Keywords: monitoring, computer network, computer systems, network protocols, operating system, routers.

Year of competition of diploma work: 2021-2022.

Year of work protection: 2023.

ЗМІСТ

ВСТУП.....	3
РОЗДІЛ 1. ЗАДАЧІ МОНІТОРИНГУ ТА АНАЛІЗУ ПАРАМЕТРІВ КОМП'ЮТЕРНИХ МЕРЕЖ.....	6
1.1. Моніторинг як засіб аналізу функціонування комп'ютерної мережі.....	6
1.2. Методи моніторингу та аналізу параметрів комп'ютерної мережі.....	8
РОЗДІЛ 2. ОГЛЯД ПРОГРАМНО-ТЕХНІЧНИХ ЗАСОБІВ МОНІТОРИНГУ КОМП'ЮТЕРНИХ МЕРЕЖ.....	11
2.1. Архітектура систем моніторингу та механізми моніторингу.....	11
2.2. Програмно-технічні засоби контролю та аналізу стану функціонування комп'ютерних мереж	14
2.3. Засоби виявлення вторгнень у комп'ютерні системи	21
РОЗДІЛ 3. МОНІТОРИНГ КОМП'ЮТЕРНОЇ МЕРЕЖІ	30
3.1. Контроль наявності вразливостей та помилок конфігурування мережі.....	30
3.2. Визначення завдань та функцій аналізатора протоколів	31
3.3. Відстеження статусу сервісів комп'ютерних мереж.....	33
ВИСНОВКИ.....	44
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ.....	47

ВСТУП

В епоху інформаційних технологій складно уявити сучасну компанію чи організацію, в якій би не функціонувала комп'ютерна мережа, яка являє собою логічне продовження застосування персонального комп'ютера. Локальні мережі все більше стають обов'язковою складовою будь-якої установи. Однак з розвитком сучасних комп'ютерних мереж найбільш актуальними стають проблеми моніторингу та управління їх функціонуванням. Все більше зусиль організацій витрачаються на підтримку оптимального стану функціонування корпоративних локальних мереж, до складу яких входять пристрої різних виробників. Для успішного адміністрування мережі необхідно знати стан кожного її елемента, а також мати можливість змінювати параметри його функціонування.

Моніторинг як спеціально організоване спостереження за станом функціонування комп'ютерної мережі, вимагає знання методів, навичок та умінь оцінити ефективність роботи всіх компонентів мережі з урахуванням їх взаємозв'язків і взаємовпливу.

Проблематика застосування методів і алгоритмів моніторингу мереж детально представлена у роботах Желєзняка В.В., д.т.н., проф. Мясіщева О.А., д.т.н., проф. Ленкова С.В., Сєлюкова Д.О. [1], а також Кривулі Г. Ф., Дзюби І. М., Жуковського А. І [2]. Результати аналізу технологій моніторингу комп'ютерних мереж висвітлюють у своїх роботах Гузій М, Станіславова О, Кадет М. [3]. Можливості прогнозування та діагностики стану комп'ютерних систем у короткостроковій та довгостроковій перспективах розглянуті у роботах Р. Г. Шихалієва, а також В.В. Коренькова і А.В. Ужінського. Корпорація Майкрософт щорічно інвестує більше 1 млрд. доларів США у наукові дослідження і розробку рішень для забезпечення кібербезпеки та моніторингу комп'ютерних мереж.

Актуальність теми: оскільки існує достатньо велика кількість методів, програмно-технічних засобів, підходів для здійснення моніторингу стану

комп'ютерної мережі, то їх аналіз з метою подальшого застосування є актуальним для як наукового пошуку та практичного застосування.

Орієнтуючись на актуальність обраної теми, було визначено мету виконання кваліфікаційної роботи (проєкту), яка полягає у визначенні способів та засобів моніторингу стану функціонування комп'ютерної мережі.

Для досягнення визначеної мети було вирішено наступні завдання:

- визначено задачі та методи моніторингу параметрів комп'ютерних мереж;
- проаналізовано архітектуру систем моніторингу;
- здійснено оцінку можливостей програмно-апаратних засобів контролю наявності вразливостей та помилок конфігурування мережі;
- визначено завдання та функції аналізатора протоколів комп'ютерних мереж;
- проаналізовано можливості систем виявлення вторгнень IDS;
- визначено способи та засоби моніторингу, які забезпечують контроль наявності вразливостей та помилок конфігурування мережі, аналіз протоколів, відстеження статусу сервісів комп'ютерної мережі.

Об'єктом дослідження в даній роботі є засоби моніторингу функціонування компонент комп'ютерної мережі.

Предмет дослідження: властивості та характеристики програмно-апаратних засобів моніторингу параметрів комп'ютерної мережі

Методи дослідження: при написанні дипломної роботи були використані наступні методи: системний аналіз, який застосовувався при роботі з інформаційними ресурсами за темою дослідження; методи порівняння та аналогій були застосовані при дослідженні функціональних систем моніторингу; методи оцінювання застосовувалися при дослідженні характеристик протоколу SNMP; методи групування – при розробці системи моніторингу стану комп'ютерної мережі; за допомогою методу узагальнення були сформовані висновки.

Інформаційною базою дослідження є методи, підходи та програмно-апаратні засоби здійснення моніторингу параметрів комп'ютерної мережі, стандарти управління мережевими ресурсами.

Структура дипломної роботи містить вступ, основну частину, яка складається з трьох розділів, до якої входять 16 рисунків, 1 таблиця, висновки, перелік використаної літератури, що містить 43 джерела.

За результатами дослідження було сформульовано висновки про необхідність постійного моніторингу стану комп'ютерних мереж з метою контролю наявності вразливостей чи помилок конфігурування мережі, аналізу протоколів та відстеження статусу сервісів, а також запропоновано способи та засоби моніторингу стану функціонування комп'ютерної мережі.

Науково-практичне значення одержаних результатів: одержані результати можуть бути використані при діагностиці елементів інфраструктури комп'ютерної мережі, а також в освітньому процесі при викладанні навчальних дисциплін “Комп'ютерні мережі”, “Технології захисту інформації”.

РОЗДІЛ 1. ЗАДАЧІ МОНІТОРИНГУ ТА АНАЛІЗУ ПАРАМЕТРІВ КОМП'ЮТЕРНИХ МЕРЕЖ

1.1. Моніторинг як засіб аналізу функціонування комп'ютерної мережі

Комп'ютерна мережа за своєю суттю є складною системою, до складу якої входить велика кількість різноманітних об'єктів - комп'ютери різних типів, мережеве обладнання (адаптери, концентратори, комутатори, маршрутизатори), лінії зв'язку (кабельні або бездротові), системне, спеціальне та прикладне програмне забезпечення.

Про різноманітність комп'ютерних мереж свідчить також існуюча їх класифікація за різноманітними критеріями, зокрема є глобальні і локальні, з різною топологією ("зірка", "кілеце", "шина", "змішана топологія") та технологією (Ethernet, Token Ring, FDDI, SNA, Internet та ін.) і середовищем передачі (вита пара, коаксіальний кабель, оптоволокну, телефонний кабель, радіозв'язок, супутниковий зв'язок), а також однорангові та клієнт-серверні, з конкурентним, детермінований з опитуванням або маркерним методом доступу до середовища передачі даних (рис.1.1).



Рис.1.1. Різноманітність комп'ютерних мереж.

І, щоб ця громіздка і досить дорога система, яка є важливою частиною інфраструктури будь-якого підприємства, могла найкращим чином працювати, ефективно справлятися з обробкою потоків інформації, необхідно

постійно відслідковувати та аналізувати стан функціонування її компонентів. Тобто, моніторинг мережі є важливим практичним завданням.

Поняття «моніторинг» по своїй сутності й змісту є поліфункціональним і має достатньо велику кількість визначень, зокрема, “постійне спостереження за деяким процесом із метою виявлення його відповідності бажаному результату або вихідному положенню; спеціально організоване систематичне спостереження за станом деяких об'єктів з метою комплексної оцінки і підвищення ефективності функціонування; система збору даних про складне явище, процес, що описуються за допомогою визначених ключових показників із метою оперативної діагностики стану об'єкта дослідження й оцінки його в динаміці та ін” [4].

“Моніторинг (від англ. Monitoring) – це система постійних спостережень, оцінки та прогнозу змін стану будь-якого технічного, природного, соціального та інших об'єктів. В рамках системи спостереження відбувається оцінка, контроль об'єкта, управління станом об'єкта залежно від впливу певних факторів” [5].

Метою моніторингу є отримання якихось закономірностей, а не підтвердження чи спростування гіпотез. Основними характеристиками моніторингу є систематичність, динамічність, націленість на прогноз.

За допомогою моніторингу здійснюються спроби знайти відповіді на питання щодо ефективності роботи певної технології, виділити чинники, які впливають на роботу певного об'єкта.

“Терміном «моніторинг мережі» визначають роботу системи, яка виконує постійне спостереження за комп'ютерною мережею у пошуках повільних або несправних систем і, яка при виявленні збоїв, повідомляє про них мережевого адміністратора. Ці завдання є підмножиною завдань управління мережею” [6].

“Моніторинг мережі - це можливість контролювати і убезпечити робочий процес, який пов'язаний з інтернетом і комп'ютерами” [7].

Варто зазначити, що для безперебійної роботи комп'ютерної мережі адміністраторам доводиться невідлучно за нею стежити, адже моніторинг мережі – це складне завдання, що потребує великих витрат сил і є життєво важливою частиною роботи мережевих адміністраторів.

1.2. Методи моніторингу та аналізу параметрів комп'ютерної мережі

Для вирішення більшої частини проблем, які виникають при функціонуванні КМ, використовують відповідні методи та системи моніторингу, які дозволяють здійснювати проактивний моніторинг доступності, стану й продуктивності компонентів мережі передачі даних, аналізувати й оптимізувати їх завантаження, а також прогнозувати виникнення позаштатних ситуацій.

Проведений аналіз інформаційних ресурсів [8-12] свідчить, що найбільш поширеними методами здійснення моніторингу стану комп'ютерної мережі є активний моніторинг, пасивний моніторинг, моніторинг мережі базований на маршрутизації, моніторинг за аномальною поведінкою.

Суть активного моніторингу полягає у передачі в інформаційну мережу пакетів з метою вимірювання параметрів між двома кінцевими точками комп'ютерної мережі. При цьому вимірюються такі параметри як доступність, маршрут, затримка пакетів, зміна порядку пакетів, втрата пакетів, пропускна здатність каналу. “Базовими інструментами, що здатні допомогти у вимірюванні вищезгаданих параметрів є утиліти: *ping*, що вимірює затримки та втрату пакетів; *traceroute*, яка допомагає визначити топологію мережі; *iperf*, яка вимірює якість пропускної здатності TCP та UDP протоколів, повідомляє про затримку та втрати пакетів” [8]. Недоліком активного моніторингу є те, що згенерований трафік додатково завантажує мережу під час її експлуатації.

Пасивний моніторинг, на відміну від активного моніторингу, не генерує надлишкового трафіку, та вимірює параметри продуктивності лише в одній точці мережі. “Даний метод знайшов застосування у пакетних sniffерах. Результати пасивного моніторингу можуть бути досліджені лише постфактум, при цьому будь-яке додаткове навантаження на мережу відсутнє” [9].

Моніторинг мережі, що базується на маршрутизації зазвичай реалізується мережевими програмно-апаратними засобами.

“Зокрема, використання SNM (Simple Network Management Protocol або простий протокол мережевого управління), який є протоколом прикладного рівня стеку TCP/IP, надає адміністратору мережі можливості керування та контролю роботи пристроїв (комутаторами, маршрутизаторами, серверами, модемами, робочими станціями) та додатками у мережі шляхом обміну інформацією між агентами, що встановлені у мережевих пристроях та менеджерами, що встановлені на станціях керування (Network Management Systems)” [8]. Агенти є програмним забезпеченням, здатним перетворювати дані протоколу SNMP у команди керування пристроями, та навпаки. Станції керування є програмним забезпеченням, що здійснюють моніторинг та контроль за керованими пристроями. Обробка всіх даних, отриманих з агентів, виконується на станціях. Станції керування здатні виконувати базові операції, а саме: *read* – зчитування значень змінних, що знаходяться у пам’яті керованих пристроїв; *write* – змінює значення змінних; *traversal operations* – накопичення інформації щодо доступних змінних керованого пристрою; *trap* – повідомляє систему управління мережею (NMS) про певну подію, що сталася з керованим пристроєм. Водночас SNMP протокол є вразливим, оскільки жодних процедур з аутентифікації користувачів не виконується, що є основним його недоліком.

Для виконання складних функцій управління мережею, для контролю за Інтернет-трафіком призначений стандарт RMON (Remote Monitoring Network або віддалене спостереження мереж), який з’явився у листопаді 1991 року. “RMON включає різні мережеві монітори та системи для обміну інформацією мережевого моніторингу. Даний метод моніторингу є розширенням

Management Information Database (MIB). На відміну від SNMP, коли NMS повинна власноруч надсилати запити на отримання інформації, RMON дозволяє налаштовувати обробники подій, що будуть спрацьовувати за певних критеріїв. Іншою відміною від SNMP є те, що програмно-апаратні агенти RMON збирають та зберігають інформацію самостійно. Агентами можуть

бути мережеві пристрої з вбудованим програмним забезпеченням та комп'ютери, які виконують просту діагностику несправностей та попереджають про можливі відмови. Наприклад, в рамках технології RMON можна зібрати дані про нормальний стан функціонування мережі (виконати так званий baselining) та виставити попереджувальні сигнали, які спряцьовуватимуть при відхиленні режиму роботи мережі від baseline, що може свідчити про неповну справність обладнання. При цьому роль клієнта виконує станція керування, що взаємодіє з агентами з використанням SNMP” [11].

Суть методу *моніторингу за аномальною поведінкою* полягає у виявленні значних відхилень параметрів у порівнянні зі значеннями цих параметрів при стабільному функціонуванні мережі. Для ефективного застосування даного методу, спочатку необхідно зафіксувати контрольні значення важливих параметрів функціонування мережі. “Виявлення аномалій запускає модуль для подальшого аналізу трафіку або спричинює повідомлення для аналітика безпеки” [11].

РОЗДІЛ 2. ОГЛЯД ПРОГРАМНО-ТЕХНІЧНИХ ЗАСОБІВ МОНІТОРИНГУ КОМП'ЮТЕРНИХ МЕРЕЖ

2.1. Архітектура систем моніторингу та механізми моніторингу

Незважаючи на те, що кожна мережа даних по суті унікальна існує загальна ідея, яка широко застосовується в мережі передачі даних. Архітектури щодо надійності, швидкості і надійності передачі даних. Цю архітектуру найкраще характеризує і описує компанія Cisco і її Enterprise Campus 3,0 [12]. “Принцип цієї архітектури – трирівнева ієрархічна мережа з ядром, розподілом і рівнями доступу, яка дозволяє і полегшує майбутнє зростання мереж і значно полегшує маршрутизацію, адресацію і автономію окремих компонентів і блоків мережі” [12]. З точки зору систем моніторингу, одним з найбільш фундаментальних питань є питання їхнього розташування в контрольованій мережі. На думку автора, логічним місцем для його розташування є основний шар, який повинен забезпечити максимальну доступність і в той же час система моніторингу - доступ до всіх шарів елементів мережі.

Коли використовується система моніторингу, потрібно розуміти розмір контрольованої мережі і відповідно до неї повинні вибрати відповідну цьому архітектуру. На даний час використовуються дві архітектури системи моніторингу - централізована і федеративна.

1. Централізована система моніторингу.

Централізована система моніторингу підходять для невеликих мереж без зовнішніх галузей. Система моніторингу використовується там лише з одним сервером, який контролює всю мережу. Якщо необхідно також контролювати зовнішню гілку, у більшості випадків використовується VPN-сайт. Якщо використовується ця архітектура, надзвичайно важливо вибрати відповідне місце системи моніторингу. Логічно, що найкраще місце для його з'єднання в центрі мережі (ядро мережі).

Архітектура з централізованою системою моніторингу зображена на рис. 2.1.

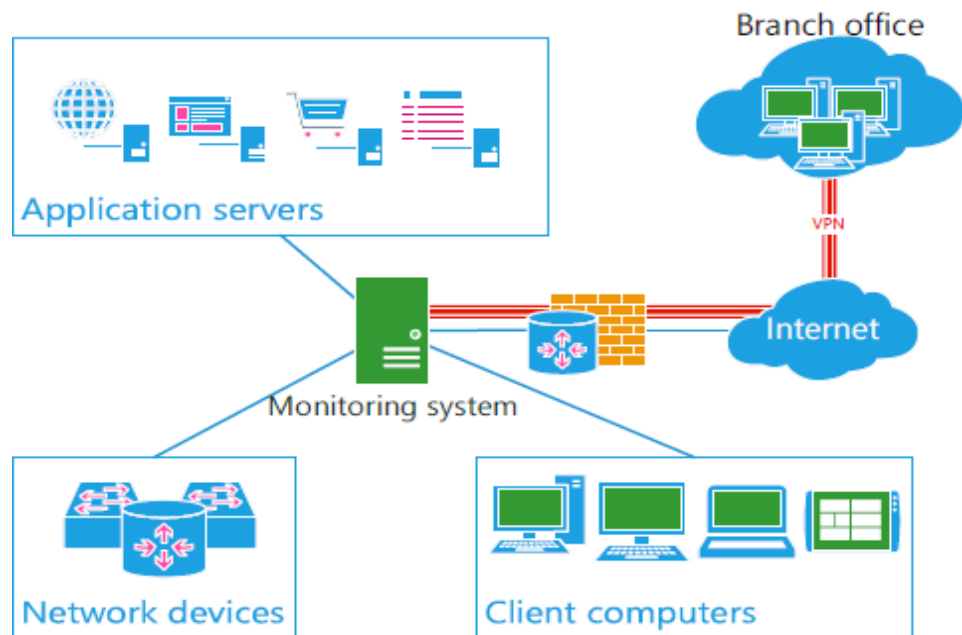


Рис. 2.1. “Архітектура з централізованою системою моніторингу” [12].

Перевагою цієї архітектури є простота та швидкість реалізації. Найбільш ризикованою і найбільш складною точкою її реалізації є чітко визначена концепція системи моніторингу.

2. Система федеративного моніторингу.

Ця архітектура базується на сегментації відстежуваної мережі до менших частин, які контролюються індивідуальною системою моніторингу. Ці менші сервери повідомляють повну інформацію про мережу з їх точки зору на центральний сервер моніторингу. Центральний моніторинг на основі інформації від галузових систем може точно звітувати про постраждалий сегмент мережі. У разі виходу з ладу основної системи моніторингу все ще можливо отримати дані та інформацію від галузових систем. Цей тип архітектури особливо підходить для розгалужених мереж, або, з іншого боку, для постачальників, які можуть використовувати його для спостереження за своїми клієнтами мереж та виходів з основної системи моніторингу, а потім представляти їх в центр моніторингу. Архітектура з федеративною системою моніторингу зображена на рис. 2.2.

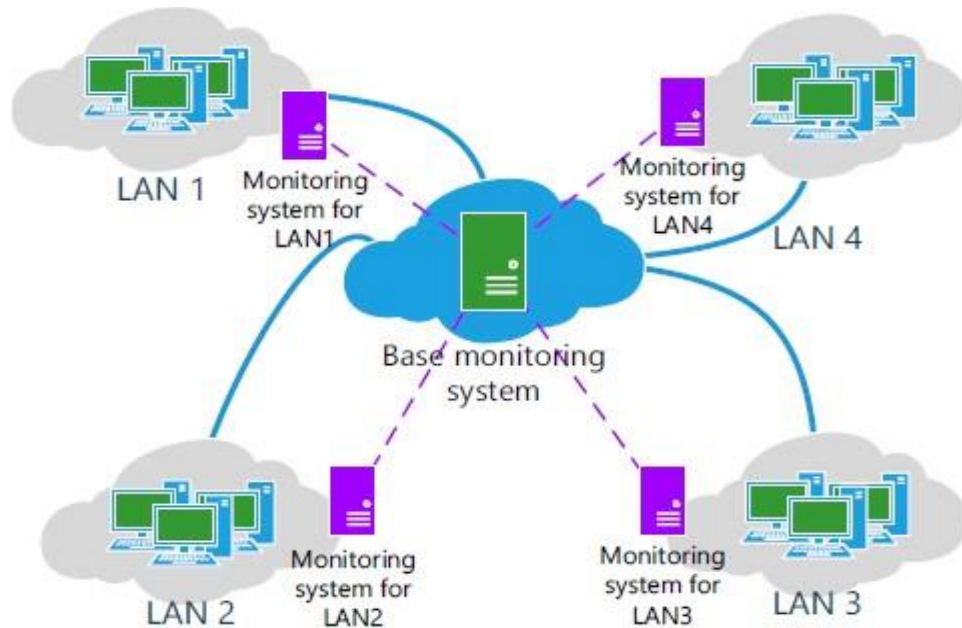


Рис. 2.2. “Архітектура з федеративною системою моніторингу” [12].

Системи моніторингу для збору інформації з контрольованих пристроїв використовують три методи. Перший метод перевіряє пристроїв з використанням стандартних протоколів, таких як ICMP, TCP, SNMP і так далі. Такий спосіб перевірки в більшості випадків не потребує будь-якого великого втручання до конфігурації за винятком дозволу виключень в брандмауері. Це також універсальний метод отримання інформації незалежно від виробників та типу пристрою. Недоліком є певне узагальнення та недоступність деяких спеціалізованих функцій.

Другий варіант - використання SNMP-повідомлення під назвою SNMP пастка. На противагу першому варіанту немає періодичної перевірки з боку системи моніторингу, але контрольований елемент в випадку аварії (помилка, збій порту, RAM заповнений, і так далі) відправить звіт в систему моніторингу, на основі отриманої інформації. “Цей спосіб перевірки у більшості випадків поєднуються з періодичної перевіркою” [11].

Третій варіант, як отримати дані системи моніторингу, - використання спеціального агента для моніторингу пристрою. Агент працює в цільовій системі як додаток, і він взаємодіє з системою моніторингу за принципом

клієнт-сервер. Перевага в тому, що не потрібно використовувати спеціальний мережевий протокол, оскільки ці дані переважно передаються через TCP/IP. Головною перевагою є можливість отримати детальну інформацію про моніторингову систему, а в разі активної системи моніторингу також є можливість керувати станцією, що підлягає моніторингу. Сервери зазвичай контролюються таким способом.

2.2. Програмно-технічні засоби контролю та аналізу стану функціонування комп'ютерних мереж

Проведений аналіз свідчить, що існує декілька класів програмно-технічних засобів, які використовуються для контролю та аналізу стану функціонування комп'ютерних мереж, а саме:

1. “Системи керування комп'ютерною мережею – централізовані програмно-апаратні системи, що збирають дані про стан вузлів та комунікаційних пристроїв мережі, дані про трафік, що циркулює у мережі. Особливістю даних систем є, те що вони в автоматичному або напівавтоматичном режимах виконують дії з керування мережею – увімкнення або відімкнення портів приладів, зміна змісту маршрутизуючих таблиць, правил брандмауерів тощо” [13].

2. Засоби керування системою – виконують функцію, що аналогічні до систем керування мережею, але по відношенню до комунікаційного обладнання. Також вони здатні виконувати найпростіший аналіз мережевого трафіка.

3. Вбудовані системи діагностики та управління – дані системи реалізуються шляхом використання програмних модулів у комунікаційному обладнанні. Вони направлені на виконання функцій діагностики та керування лише над одним пристроєм. На даний час вбудовані системи також виконують роль SNMP-агентів, що постачають дані для систем керування мережею.

4. Аналізатори протоколів – програмні або програмно-апаратні системи, що виконують лише функції моніторингу та аналізу трафіку.

Аналізатор протоколів є самостійним спеціалізованим пристроєм, або

персональним комп'ютером, зазвичай переносним, класу Notebook, оснащений спеціальною мережевою картою і відповідним програмним забезпеченням. Мережева карта і програмне забезпечення, що використовуються повинні відповідати топології мережі.

Аналізатор підключається до мережі як звичайний вузол. “Програмне забезпечення аналізатора складається з ядра, що підтримує роботу мережевого адаптера і декодує одержувані дані, та додаткового програмного коду, що залежить від типу топології досліджуваної мережі. Крім того, поставляється ряд процедур декодування, орієнтованих на певний протокол, наприклад, IPX. До складу деяких аналізаторів може входити також експертна система, яка може видавати користувачеві рекомендації про те, які експерименти слід проводити в даній ситуації, що можуть означати ті чи інші результати вимірювань, як усунути деякі види несправності мережі” [42].

Прикладом широко використовуваного аналізатора мережевих протоколів є система Wireshark. “Wireshark дозволяє побачити, що відбувається у вашій мережі на мікроскопічному рівні, і є стандартом де-факто (і часто де-юре) для багатьох комерційних і некомерційних підприємств, державних установ і навчальних закладів. Розробка Wireshark процвітає завдяки волонтерським внескам мережевих експертів у всьому світі та є продовженням проекту, розпочатого Джеральдом Комбсом у 1998 році” [43].

5. Експертні системи – даний вид систем акумулює знання про виявлення причин аномальної роботи мережі та можливих способах повернення мережі до нормального режиму функціонування. Експертні системи часто реалізуються у вигляді підсистем засобів моніторингу та систем керування мережею. “Функціональною основою складних експертних систем є так звані бази знань, що володіють елементами штучного інтелекту” [9].

Отже, системи моніторингу стану функціонування комп'ютерної мережі повинна містити засоби діагностики, аналізатори протоколів, експертні системи, сканери і тестери, багатофункціональні системи (рис. 2.3).

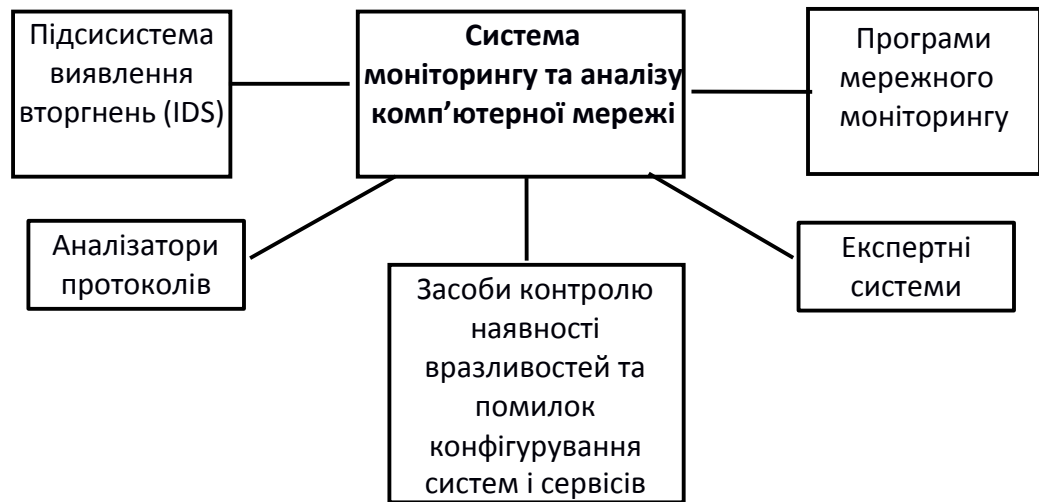


Рис. 2.3. Складові системи моніторингу стану функціонування комп'ютерної мережі

При цьому важливо використовувати якісні інструменти для моніторингу стану функціонування комп'ютерних мереж, які дозволять здійснювати перевірку стану підключення та швидкості передачі даних в мережі на будь-якому апаратному забезпеченні. Недарма в сучасних реаліях розвитку ІТ-індустрії розробники найчастіше використовують технології багатоплатформності – “властивість програмного забезпечення працювати більш ніж на одній програмній (у тому числі – операційній системі) або апаратній платформі; технології, що дозволяють досягти такої властивості. Кросплатформність дозволяє суттєво скоротити витрати на розробку нового або адаптацію існуючого програмного забезпечення” [10].

Сучасний ринок програмного забезпечення пропонує достатньо велику кількість програмних рішень для здійснення ефективного моніторингу стану комп'ютерної мережі, незалежно від операційної системи, на якій вони працюють, зокрема:

1. Система AppDynamics [14] надає комплексне рішення для моніторингу інфраструктури, яке охоплює компоненти сервера, сховища та мережі як у хмарних, так і в гібридних середовищах. Його можна розгорнути локально або використовувати як службу SaaS.

Можливості повного стека моніторингу цього інструменту допомагають співвідносити проблеми продуктивності програми з вузькими місцями інфраструктури низького рівня, прискорюючи тим самим аналіз основних причин і усунення.

2. Система Checkmk [15] побудована на базі Nagios, але сильно дорацьована. Система проста, зручна та функціональна, а поріг входу дуже низький. Розібратися зможе майже будь-хто. Моніторинг виконує на основі агентів та з snmp. Відмінно працює автовиявлення. Достатньо під'єднати хост з агентом і Checkmk сам підбере шаблон, виявить усі відомі йому метрики та почне моніторинг. Має зручний та красивий вебінтерфейс. Після додавання змін необхідно їх підтвердити, до цього вони не застосовуються.

3. Програмний продукт Icinga [16], що спочатку це був форк Nagios. Але з часом їх шляхи сильно розійшлися, тож можна вважати Icinga самостійним продуктом. Причому якісним та повністю безоплатним. У системі є все, що потрібно для здійснення повноцінного моніторингу. Дані може збирати як за допомогою агентів, так і без них. Бекенд написано на C++, вебінтерфейс на PHP. Підтримує MySQL, Oracle Database, PostgreSQL.

4. Програмне забезпечення LibreNMS [17] – форк Observium з більшим функціоналом. Можна запускати в Docker, є інтеграція з Grafana, є можливість зберігати дані в InfluxDB. Система заточена на моніторинг мереж з SNMP. Має підтримку практично всіх популярних мережевих пристроїв, окрім цього, вміє моніторити Windows, Linux, FreeBSD і тому використовує агенти. Працює на базі PHP та MySQL.

5. Система Monit [18] має функціонал схожий на Munin та Monitorix. Система є легкою і з акцентом на моніторинг окремого сервера. Вміє не лише перевіряти, а й виконувати якісь заскриптовані дії. Дані зберігає у БД SQLite. Функціонал системи Monit підійде для тих, хто просто хоче моніторити свій локалхост, отримувати алерти, перезапускати сервіси, коли вони падають, і при цьому витрачати мінімум ресурсів. Дає можливість писати олдскульні конфіги без урахування відступів та дужок.

6. Програмне рішення Monitorix [19] є схожим на Munin-моніторинг — написане теж на основі Perl та RRDtool. Чудово підійде для сервера. Основна позитивна особливість даного інструменту: споживання дуже малої кількості ресурсів. Графіки формуються відразу в png картинки. Крім базових системних та мережевих метрик, підтримує моніторинг найбільш популярного софту такого, як Postfix, Exim, Apache, Nginx, PHP-FPM, ZFS, MySQL, PostgreSQL, Redis тощо.

7. Програмний засіб Monitoror [20] – це проста система моніторингу, що складається лише з одного бінарника та конфігураційного файлу до нього. Окремим конфігом можна налаштувати вебінтерфейс. Використовується формат JSON. Налаштовувати перевірки швидко та просто. Monitoror відрізняє простота парсингу та збирання текстових даних по HTTP з можливістю їх вивести у вигляді плиток на дашборд. Це хороший інструмент для будь-яких чисел, які отримуються з API.

8. Система Munin [21], що написана на Perl, призначена для забезпечення моніторингу окремого сервера (або невеликої групи). Дані зберігаються в RRDtool. Налаштовується дуже просто і швидко. Munin використовують розробники BitrixEnv, які включили його до комплекту свого оточення.

9. Система Nagios [22] є відомою системою моніторингу, яка свого часу була популярнішою за Zabbix, та й з'явилася раніше. Має багато готових плагінів для моніторингу всього та вся. Встановити та налаштувати набагато легше, в порівнянні з Zabbix. Система більше заточена на статуси та стани, а не на графіки, має форк Icinga.

10. Особливість системи моніторингу Netdata [23] є нескладна установка налаштування. Скрипт сам автоматично розгорне сервер на Linux машині. Є можливість використовувати за моделлю SaaS на хмарному сервері розробників. Система функціонує на основі агентів та колекторів, які автоматично реєструють себе на сервері та починають відправляти дані.

11. Система NetXMS [24] є кросплатформною системою моніторингу, що написана на Java. Детальний огляд її характеристики свідчить, що ця система

підтримує усі популярні операційні системи, збирає метрики через SNMP або через агентів. Серверна частина може бути встановлена як на Linux, так і на Windows. Система NetXMS вирізняється великим функціоналом та можливостями, але при цьому є відносно простою у налаштуванні та має низький поріг входу.

12. Система моніторингу Newtelic [25] працює за моделлю SaaS. Достатньо встановити агента на сервер та вказати власний унікальний ключ, а далі агент все зробить сам. Далі необхідно лише зайти в вебінтерфейс і дивитися метрики. Функціонал моніторингу дуже крутий, користуватися зручно. Безплатний тарифний план - 100 GB даних на місяць.

13. Програмне рішення Observium [26] - це система моніторингу з акцентом на SNMP та мережні пристрої. Підтримує популярні ОС, такі як Windows і Linux, дані з яких збираються через агентів. Основний акцент системи — мінімум ручних дій. Все, що підтримується, автоматично виявляється в мережі та ставиться на моніторинг, формуються графіки, будуються дашборди. Працює на базі PHP та MySQL.

14. Система Prometheus [27] - безплатна програма, яка використовується для моніторингу подій та сповіщень. Вона записує показники в режимі реального часу в базу даних часових рядів (з урахуванням високої розмірності), створеної за допомогою моделі витягування HTTP, з гнучкими запитами та сповіщеннями в режимі реального часу. Проєкт написаний на Go і ліцензований Apache 2, вихідний код доступний на GitHub. Є проєктом Cloud Native Computing Foundation разом з Kubernetes і Envoy.

15. Система Sematext Monitoring [28] - повноцінне програмне забезпечення для моніторингу IT-інфраструктури, яке забезпечує видимість локальних і хмарних розгортань в реальному часі. Дозволяє бачити стан справності інфраструктури, відстежуючи програми, сервери, контейнери, процеси, інвентар, події, бази даних тощо. Цей інструмент пропонує комплексне виявлення аномалій та інтеграцію із зовнішніми службами

сповіщень для попередження інфраструктури, такими як PagerDuty, Opsgenie, Splunk On-Call (раніше VictorOps) тощо.

16. Програмний комплекс SolarWinds Server & Application Monitor (SAM), згідно [29], забезпечує поглиблений моніторинг IT-інфраструктури, як локально, так і в хмарі. Цей інструмент пропонує готову підтримку для понад 1200 програм і систем, дозволяє відстежувати компоненти інфраструктури за допомогою WMI, SNMP, Powershell, REST API тощо. Вивчення характеристик показало, що SAM має попередньо визначені конфігурації моніторингу ОС для Windows і Linux, що забезпечує швидшу адаптацію та моніторинг продуктивності.

17. Система The Dude забезпечує моніторинг на базі ОС RouterOS, яка використовується в Mikrotik [30]. Основна її відмінність - простота налаштування та невибагливість у плані ресурсів. The Dude дуже легко встановити та запустити в роботу, не потрібні спеціальні знання та час на вивчення продукту. Базове налаштування просте та інтуїтивне. The Dude вміє автоматично сканувати мережу та додавати до моніторингу всі знайдені пристрої. Це можуть бути як мережні пристрої з передачею даних через SNMP, так і системи Windows, які передають дані через агентів.

18. Система WhatsUp Gold [31] - це рішення для моніторингу мережі, яке можна розширити за допомогою модулів для моніторингу компонентів інфраструктури та програм для моніторингу повного стека. Вивчення функціоналу системи свідчить про те, що він надає широкі можливості моніторингу віртуальної інфраструктури, розміщеної на VMware або Hyper-V. WhatsUp Gold надає інформацію про використання ЦП, пам'яті, диска та мережі хостами та гостями з одного інтерфейсу. Цей інструмент відстежує споживання пропускної спроможності компонентів програми, а також продуктивність мережі.

19. Програмне забезпечення Zabbix [32] — це вільна система моніторингу статусів різноманітних сервісів комп'ютерної мережі, серверів та мережевого обладнання. Вивчення характеристик Zabbix свідчить, що для

зберігання даних використовують БД MySQL, PostgreSQL, SQLite або Oracle Database, вебінтерфейс написаний на PHP. Система підтримує кілька видів моніторингу. Simple checks — може перевіряти доступність і реакцію стандартних сервісів, таких як SMTP або HTTP, без встановлення будь-якого програмного забезпечення на хості, що спостерігається. Zabbix agent — може бути встановлений на UNIX-подібних або Windows-хостах для отримання даних про навантаження процесора, використання мережі, дисковому просторі тощо. External check — виконання зовнішніх програм, також підтримується моніторинг через SNMP.

Отже, інструменти моніторингу інфраструктури перевіряють стан IT-середовища, включаючи продуктивність, пропускну здатність доступності, використання та безпеку. Мають можливість генерувати сповіщення інфраструктури на основі відстежуваних показників і створювати звіти, які дають статистику, незалежно від того, як і де розміщено додаток. Деякі рішення спеціалізуються на конкретних аспектах (наприклад, показники продуктивності), тоді як інші забезпечують моніторинг повного спектра з опціями для налаштування.

2.3. Засоби виявлення вторгнень у комп'ютерні системи

На сьогоднішній день безпека є однією з найбільших проблем майже для всіх мереж у будь-якій галузі, оскільки існує незліченна кількість шкідливих спроб долучитися до приватної інформації, мереж та веб-служб компаній.

Саме тому у комп'ютерній мережі необхідно мати систему виявлення вторгнень (Intrusion Detection System, IDS). “Системи виявлення вторгнень — це системи, які збирають інформацію з різних системних і мережевих джерел, а потім аналізують інформацію про ознаки вторгнення та зловживання” [33]. Через IDS користувачам стає відомо про те, які ризики і загрози вони мають.

IDS, як правило, поділяються на два типи рішень: системи виявлення вторгнення на основі хоста (HIDS) та мережеві системи виявлення вторгнення (NIDS). “HIDS встановлюються на кожному комп'ютері в мережі, щоб аналізувати та контролювати трафік, що надходить до відповідного вузла.

NIDS також відстежує та контролює локальні зміни файлів і можливі зміни через несанкціонований доступ та/або компроміс” [33].

На відміну від цього, NIDS є стратегічно розташованою у різних точках мережі, щоб стежити за трафіком, що йде до мережевих пристроїв і від них. Рішення NIDS часто складається зі збірки взаємодіючих частин: автономний пристрій, апаратні датчики та програмні компоненти є типовими складовими, що входять до NIDS. Ці компоненти дозволяють більше розширити спектр можливостей виявлення вторгнення в мережі у режимі реального часу, ніж при використанні HIDS.

Перш ніж перейти до аналізу можливостей мережевих систем виявлення вторгнень, слід розглянути, як різні типи NIDS виявляють вторгнення.

“NIDS може включати один із двох (або обидва) типів виявлення вторгнення у свої рішення: на підпис (Signature-based) і на основі аномалій (Anomaly-based)” [34]. NIDS на базі підписів відстежує мережевий трафік на наявність підозрілих патернів у пакетах даних – «підписів» відомих шаблонів вторгнення в мережу – для виявлення та усунення нападів та компромісів. Використовуючи перелік відомих типів вторгнень та їх шаблонів даних, NIDS на основі підпису може швидко визначити вторгнення та розпочати відповідний курс дій. NIDS на основі аномалій використовує базову лінію системи в нормальному робочому стані для відстеження наявності незвичної або підозрілої діяльності. Хоча для цього методу потрібен час для налаштування, оскільки для базового сценарію потрібно, щоб NIDS дізналася про вашу модель використання системи. Цей органічний евристичний підхід до виявлення вторгнень може бути більш гнучким та потужним, ніж підхід, що вимагає, щоб шаблон із попередньо існуючим типом вторгнень знаходився в переліку відомих типів вторгнень.

Слід розглянути основні характеристики мережевих систем виявлення вторгнень, зокрема:

- 1) “Програмний комплекс Snort є лідером серед систем з відкритим кодом. Незважаючи на відсутність графічного інтерфейсу або простого

інтерфейсу адміністратора, цей інструмент отримав широке визнання як ефективне рішення мережевої системи виявлення вторгнень для широкого кола сценаріїв та випадків використання” [35]. Крім того, було створила різні інтерфейси для вирішення проблеми відсутності графічного інтерфейсу. Snort використовує як виявлення вторгнення на основі сигнатур, так і методи, що базуються на аномаліях і можуть покладатися на створені користувачами правила або підписи, отримані з баз даних.

2) Програма Suricata, згідно матеріалів [36], є прямим конкурентом Snort і використовує методологію, основу на підписах, безпеку, керовану правилами/політикою, та підхід, що базується на аномаліях, для виявлення вторгнень. Програмне рішення Suricata є сучасною альтернативою галузевому стандартному інструменту Snort, з багатьма можливостями для потоку, прискоренням графічного процесора та численними моделями виявлення статистичних аномалій.

3) Програмне забезпечення Bro IDS за матеріалами сайту [37] використовує виявлення вторгнень на основі аномалій і, як правило, застосовується у поєднанні з Snort, оскільки вони дуже добре доповнюють один одного. Слід зазначити, що Bro насправді є спеціальною мовою для мережевих додатків, в яких написано Bro IDS. Ця технологія особливо ефективна при аналізі трафіку.

4) Програмне забезпечення Security Onion з відкритим кодом, згідно матеріалів сайту [38], є дистрибутивом Linux на базі Ubuntu, призначене для IDS та моніторингу мережевої безпеки (NSM). Ця платформа пропонує комплексне виявлення вторгнень, моніторинг безпеки мережі та управління журналами, об'єднуючи найкраще з Snort, Suricata, Bro, а також інші інструменти, такі як Sguil, Squert, Snorby, ELSA, Xplico та ін. Для випадків, коли необхідно отримати найкраще з вищезазначених інструментів в одному пакеті, варто використовувати Security Onion.

У табл. 2.1 наведено порівняльний аналіз вищезазначених систем.

Сучасні NIDS є розподілені і складаються з декількох компонентів. На рис. 2.4 наведено архітектуру та особливості роботи NIDS на прикладі Snort, яка складається з таких компонентів:

- аналізатор трафіку (sniffer);
- дешифратор пакетів (preprocessor);
- механізм виявлення (detection engine);
- набір правил (ruleset);
- система реєстрації/оповіщення (logger/alerter).

Таблиця 2.1

Порівняльний аналіз існуючих IDS

Назва системи	Переваги	Недоліки
Snort	Дуже простий в установці, запуску та роботі. Велике ком'юніті Snort користувачів, багато підтримуваних ресурсів, доступних в Інтернеті	Поставляється без графічного інтерфейсу, хоча існують додатки, розроблені ком'юніті. Обробка пакетів може бути повільною
Suricata	Може використовувати набори правил Snort. Має розширені функції, такі як багатопоточність і прискорення графічного процесора	Схильні до помилкових спрацьовувань. Системна та мережна ресурсомісткість
Bro IDS	Платформа може бути адаптована до різних випадків використання мережевої безпеки, в доповненні до NIDS	Необхідний певний досвід програмування. Отримання кваліфікації в Bro DSL може потребувати певних зусиль
Security Onion	Комплексний стек безпеки, що складається з декількох провідних рішень із відкритим кодом. Забезпечує простий інструмент налаштування для встановлення всього стеку	Як платформа, що складається з декількох технологій, Security Onion наслідує недоліки кожного

Джерело: складено за матеріалами сайту [38].

Аналізатор трафіку призначений для перехоплення і подальшого аналізу мережево-го трафіку. Перехоплення трафіку здійснюється за допомогою

бібліотеки pcap (libpcap – для Linux, WinPcap – для Windows) звичайним «прослуховуванням» мережевого інтерфейсу.

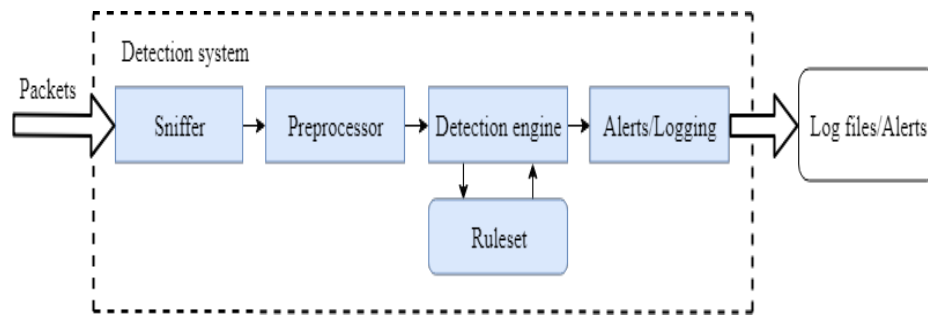


Рис.2.4. “Архітектура Snort” [35].

Дешифратор пакетів готує перехоплені пакети в форму типу даних, які потім можуть бути оброблені механізмом виявлення. Дешифратор пакетів може реєструвати Ethernet, SLIP і PPP-пакети.

Механізм виявлення аналізує і обробляє пакети, подані до нього «дешифратором», ґрунтуючись на правилах Snort (так як система виявлення в Snort працює на основі підписів). Змінні модулі можуть бути включені в механізм виявлення, щоб збільшити функціональні можливості Snort.

Набір правил включає в себе низку підписів (правил), на основі яких орієнтується механізм виявлення, і вже потім вирішує, чи є перехоплений трафік вторгненням.

Система реєстрації/оповіщення дозволяє реєструвати інформацію, зібрану дешифратором пакетів у легкому для читання форматі або повідомляти про виявлені загрози. За замовчуванням файли реєстрації збережені в каталозі /var/log/snort.

Snort має три режими роботи:

“1. Режим пакетного сніфера. В цьому режимі Snort читає і дешифрує всі мережеві пакети і формує дамп до stdout (ваш екран). Для перекладу Snort в режим сніффер використовуйте ключ `-v`.

2. Режим реєстрації пакетів. Цей режим записує пакети на диск і декодує їх в ASCII-формат.

3. Режим виявлення вторгнень. У цьому режимі Snort виступає як повноцінна мережева система виявлення вторгнень” [35].

Саме третій режим відповідає принципам роботи NIDS. При правильному налаштуванні Snort можна досягнути досить високого рівня захисту мережі. Головним критерієм правильного налаштування системи є низка правил для виявлення всіх можливих категорій вторгнень. Для того, щоб цього досягти, використовується великий досвід, отриманий довготривалою експлуатацією системи. За тривалий час свого існування Snort накопичив велике ком'юніті, яке поповнювало перелік правил, і на сьогоднішній час число цих правил перевищує величину в 50 000. Оскільки система є гнучкою і орієнтована на кастомізацію під потреби користувача, то є можливість самостійно розробляти потрібні підписи (правила).

Кожен підпис має поділ на дві частини: заголовок та опції. Заголовок підпису включає дію, протокол, IP-адресу і маски для відправника та отримувача, а також номери портів відправника та отримувача. Опції підпису включають повідомлення та інформацію про те, які частини пакета варто перевірити, аби визначити, чи слід прийняти по відношенню до пакета задану дію.

Нижче наведено приклад підпису:

```
alert tcp any any -> 192.160.0.0/24 111 \ (content:
"| 00 01 86 a5 |"; msg: "mountd access");).
```

Опції підпису вказуються у круглих дужках, слова, за якими слідує двокрапка, є ключовими. При дотриманні усіх вказаних у підписі умов по відношенню до пакета виконується задана підписом дія (генерація попередження у наведеному прикладі).

Заголовок правила має вигляд:

```
<Дія> <Протокол> <Відправник> <Порт> <Напрямок>
<Отримувач> <Порт (ключ: значення)>
```

Заголовок правила містить ключове слово, яке визначає дію, виконувану при співпадінні всіх заданих підписом умов. Дія завжди вказується першою і може бути одним і наведених ключових слів:

1. Alert – сгенерувати сигнал з використанням обраного методу і записати інформацію про пакети в журнальний файл.
2. Log – записати інформацію про пакети в журнальний файл.
3. Pass – ігнорувати пакет.
4. Active – згенерувати сигнал і активізувати інше динамічне правило.
5. Dynamic – правило не виконує жодних дій до його активації за допомогою дії activate в іншому правилі, а при активації виконується як log.

Наступне поле заголовку вказує протокол, який буде відстежуватися. Після протоколу в підписі вказуються адреси і номери портів для даного підпису.

Ключовому слову any будуть відповідати всі адреси IP (0.0.0.0/0). Номери портів можна задавати у вигляді конкретного значення, діапазону, переліку або ключового слова any (будь-який порт). Для портів також підтримується оператор заперечення. Для задання діапазону вказуються верхня та нижня границі, відокремлені двокрапкою (:).

Оператор напрямку → вказує напрямок передачі трафіку для даного підпису. Адреси і порт ліворуч від цього оператора відносяться до відправника, а праворуч – до отримувача пакетів. Можна також створювати двонаправлені підписи за допомогою оператора <>.

У цьому випадку кожна із пар «адреса-порт» буде трактуватися як відправник і отримувач водночас.

Опції правил є найважливішою частиною роботи системи підписів. Для розділення опцій у підписах використовується крапка з комою (;). Ключові слова опцій відділяються від аргументів двокрапкою (:).

Існує чотири основних категорії опцій підписів:

1. Meta-data – інформація про підпис, що не впливає на детектування пакетів і виконуваних по відношенню до них операцій.

2. Payload – опція перегляду поля даних пакета (packet payload).
3. Non-payload – опція перегляду службових полів пакета.
4. Post-detection – опція, яка вказує, що необхідно зробити після виконання заданих для підпису умов.

Для забезпечення зручного користування NIDS потрібен user-friendly інтерфейс користувача. Цю вимогу можна забезпечити за допомогою веб-додатку, що є поширеною практикою на сьогоднішній день. Проте спочатку потрібно спроектувати архітектуру такої системи.

Для даного випадку слід використовувати трирівневу «клієнт-серверну» архітектуру (рис. 2.5). Це архітектурна модель програмного комплексу, що передбачає наявність у ньому трьох компонентів: клієнта, сервера додатків (наша система виявлення) і сервера баз даних (з яким працює сервер додатків).

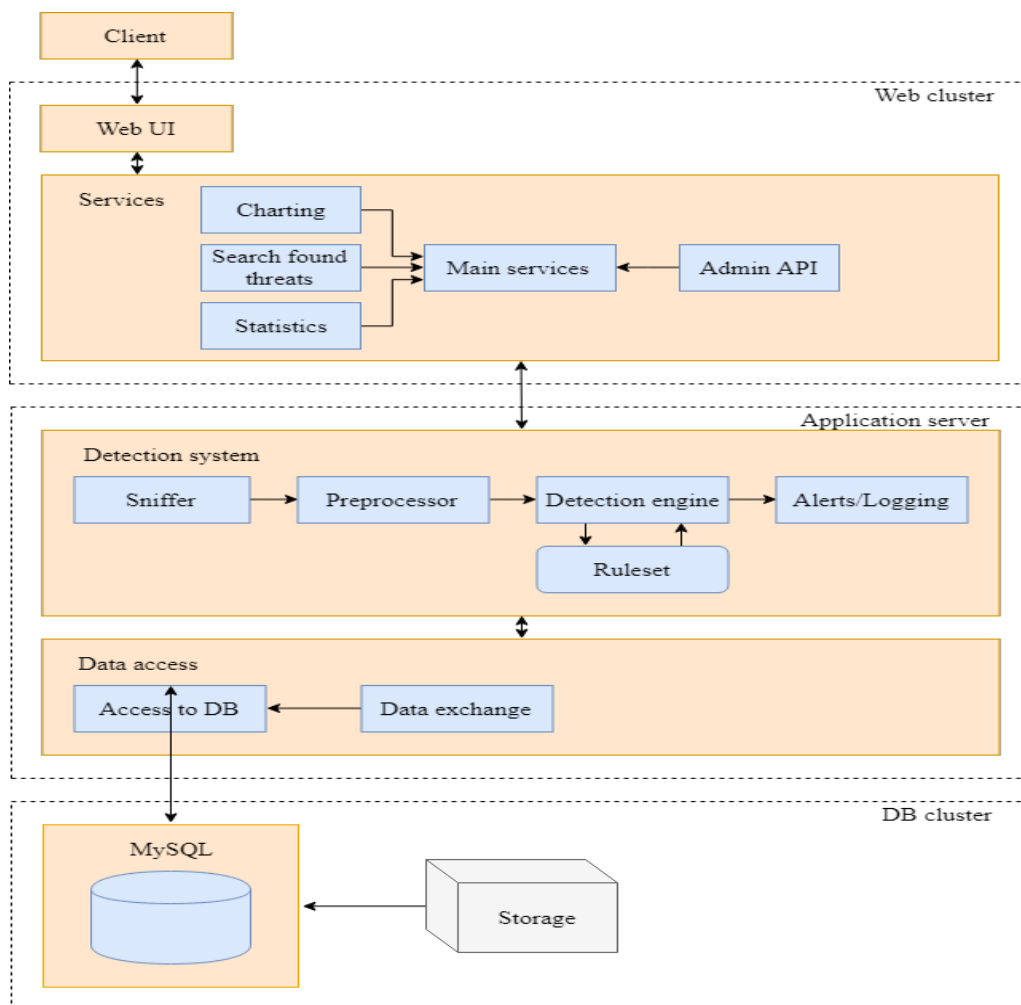


Рис.2.5. «Трирівнева «клієнт-серверна» архітектура мережевої системи виявлення вторгнень» [39]

“У порівнянні з дворівневою «клієнт-серверною» архітектурою або «файл-серверною» архітектурою, трирівнева архітектура забезпечує, як правило, більшу масштабованість (за рахунок горизонтальної масштабованості сервера додатків і мультиплексування з'єднань), кращу можливість конфігурування (за рахунок ізольованості рівнів один від одного)” [39].

РОЗДІЛ 3. МОНІТОРИНГ КОМП'ЮТЕРНОЇ МЕРЕЖІ

3.1. Контроль наявності вразливостей та помилок конфігурування мережі

У даний час діяльність багатьох організацій залежить від стану їх інформаційних систем. При цьому інфраструктура інформаційних систем часто містить вузли та системи, порушення безпеки яких може привести до нанесення збитку для ведення бізнесу в організації.

“Для запобігання випадків порушення безпеки, як правило, після відповідного аналізу формується перелік актуальних загроз і розробляється комплекс заходів щодо їх нейтралізації. В кінцевому підсумку будується система управління інформаційною безпекою, яка включає в себе різні засоби захисту, що реалізують необхідні захисні механізми. До складу даної системи може входити підсистема управління вразливостями, що представляє собою комплекс організаційно-технічних заходів, спрямованих на запобігання використання відомих вразливостей, потенційно існуючих в системі, що захищається або в мережі. Зокрема, в рамках управління вразливостями проводяться такі заходи, як періодичний моніторинг захищеності інформаційних систем і усунення виявлених вразливостей” [40].

Контроль наявності вразливостей та помилок конфігурування мережі є важливою складовою кожної системи моніторингу стану функціонування комп'ютерної мережі, адже це дає змогу мережевим адміністраторам перевірити комп'ютерну мережу на наявність шкідливих об'єктів, таких як комп'ютерні віруси усіх типів, Інтернет-джерела з потенційно-небезпечним контентом, електронні листи зі спамом. Вказані об'єкти можуть завдати шкоди як особистим даним користувача, так і пристрою, на який вони потрапляють.

Нейтралізація шкідливих об'єктів мережі також є необхідним елементом контролю наявності вразливостей. В даному випадку доцільно навести такі способи нейтралізації, а саме:

1. Видалення об'єкта – очищення комп'ютерної мережі від шкідливих об'єктів шляхом його поміщення в корзину з її подальшим очищенням.

2. Поміщення об'єкта на карантин – блокування та зупинка роботи потенційно зараженого об'єкта комп'ютерної мережі для подальшого сканування і подальших дій системи захисту залежно від результатів сканування.

Ще одним важливим і невід'ємним елементом є керування вразливостями. “Керування вразливостями – це безперервний, проактивний і часто автоматизований процес, який забезпечує захист комп'ютерних систем, мереж та корпоративних програм від кібератак і порушень безпеки даних. Тож, це важлива частина загальної програми гарантування безпеки. Визначаючи, оцінюючи й ліквідуючи потенційні слабкі місця в системі безпеки, організації можуть запобігти атакам і, якщо вони все ж трапляться, мінімізувати збитки” [41].

Мета керування вразливостями полягає в тому, щоб зменшити загальний ризик для організації, усунувши якомога більше вразливостей. Це може бути складно, враховуючи кількість потенційних уразливостей і обмеженість ресурсів, доступних для виправлення. Керування вразливостями має бути безперервним процесом відстеження нових загроз і змін середовища.

Важливим елементом також варто назвати “відстеження помилок конфігурування мережі”, оскільки саме від цього елемента залежить ефективність моніторингу стану функціонування комп'ютерної мережі. За допомогою відстеження помилок конфігурування можна визначити помилки, які є присутні у мережі, а також методи і способи їх усунення.

Реалізацію контролю наявності вразливостей та помилок конфігурування мережі можна здійснити за допомогою прикладного програмного забезпечення, що спеціалізується на моніторингу мережі, основні характеристики яких були розглянуті вище.

3.2. Визначення завдань та функцій аналізатора протоколів комп'ютерних мереж

Одним із засобів дослідження комп'ютерної мережі, як вже зазначалося вище, є аналізатор протоколів. “Процес аналізу протоколів включає

захоплення циркулюючих у мережі пакетів, що реалізують той чи інший мережевий протокол, і вивчення вмісту цих пакетів. Ґрунтуючись на результатах аналізу, можна здійснювати обґрунтовану і зважену зміну будь-якого компонента мережі, оптимізацію її продуктивності, пошук і усунення неполадок. Очевидно, що для того, щоб можна було зробити якісь висновки про вплив деякої зміни на мережу, необхідно виконати аналіз протоколів і до, і після внесення змін” [42].

Для проведення аналізу протоколів необхідно виконати шість етапів:

- 1). Захоплення даних. 2). Перегляд захоплених даних. 3). Аналіз даних.
- 4). Пошук помилок. 5). Дослідження продуктивності (Розраховується коефіцієнт використання пропускної здатності мережі або середній час реакції на запит). 6). Докладне дослідження окремих ділянок мережі.

Для проведення аналізу протоколів пропонується застосувати програмний аналізатор Wireshark, що має багатий набір функцій, який включає наступне:

1. Глибока перевірка сотень протоколів, які постійно додаються.
2. Зйомка в реальному часі та офлайн-аналіз.
3. Стандартний трипанельний браузер пакетів.
4. Мультиплатформеність: працює на Windows, Linux, macOS, Solaris, FreeBSD, NetBSD та багатьох інших.
5. Захоплені мережеві дані можна переглядати за допомогою графічного інтерфейсу користувача або за допомогою утиліти TShark у режимі TTY.
6. Найпотужніші фільтри відображення в галузі.
7. Читання/запис багатьох різних форматів захоплених файлів: tcpdump(libpcap), Pcap NG, Catapult DCT2000, Cisco Secure IDS iplog, Microsoft Network Monitor, Network General Sniffer(стиснутий і нестиснутий), Sniffer Pro та NetXray, Network Instruments Observer, NetScreen snoop, Novell LANalyzer, RADCOM WAN/LAN analyzer, Shomiti/Finisar Surveyor, Tekronix K12xx, Visual Networks Visual UpTime, WildPackets EtherPeek/TokenPeek/AiroPeek та багато інших.

8. Файли захоплення, стислі за допомогою gzip, можна розпаковувати на льоту.

9. Живі дані можна читати з Ethernet, IEEE 802.11, PPP/HDLC, ATM, Bluetooth, USB, Token Ring, Frame Relay, FDDI та інших (залежно від платформи).

10. Підтримка дешифрування для багатьох протоколів, включаючи IPsec, ISAKMP, Kerberos, SNMPv3, SSL/TLS, WEP і WPA/WPA2.

11. Правила розфарбовування можна застосувати до списку пакетів для швидкого інтуїтивно зрозумілого аналізу.

12. Вихідні дані можна експортувати в XML, PostScript, CSV або звичайний текст.

3.3. Відстеження статусу сервісів комп'ютерних мереж

Невід'ємною частиною моніторингу стану функціонування комп'ютерної мережі є відстеження статусу сервісів комп'ютерних мереж, оскільки саме статус може дати відповідь на питання працездатності того чи іншого сервісу. Такими сервісами є:

1. Сервіси віддаленого керування комп'ютерами;
2. Сервіси об'єднання віддалених комп'ютерів в одну локальну мережу в межах установи, підприємства, організації.

Як правило, дані сервіси діють завдяки їх підключенню до комп'ютерної мережі, і будь-які помилки конфігурації чи навіть наявність вразливостей можуть зашкодити даній системі.

Для проведення моніторингу КМ за допомогою програми Wireshark доцільно провести 3 кроки: дослідження конфігурації мережі ПК, запуск програми Wireshark і початок збору даних, захоплення і аналіз кадрів бездротової мережі за допомогою програми Wireshark за протоколом ICMP

Крок 1. Дослідження конфігурації мережі ПК.

Для цього необхідно дізнатися IP-адресу комп'ютера і фізичну адресу мережевої плати(NIC), який називається MAC-адресою. Для даної процедури потрібно відкрити вікно командного рядка і ввести команду *ipconfig/all* і

натиснути клавішу вводу. Далі необхідно зафіксувати IP-адресу комп'ютера, його опис і MAC-адресу. В даному випадку буде проведено аналіз бездротової мережі: IP-адреса вузла ПК – 192.168.226.224, IP-адреса шлюзу за замовчуванням – 192.168.226.32. (рис. 3.1).

```

C:\WINDOWS\system32\cmd.exe
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Подключение по локальной сети* 2:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
Description . . . . . : Microsoft Wi-Fi Direct Virtual Adapter #2
Physical Address. . . . . : 2A-E3-47-63-E5-46
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Беспроводная сеть:
Connection-specific DNS Suffix . :
Description . . . . . : Qualcomm Atheros QCA9565 802.11b/g/n WiFi Adapter
Physical Address. . . . . : 28-E3-47-63-E5-46
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::2186:ac2f:9a1d:150e%15(Preferred)
IPv4 Address. . . . . : 192.168.226.224(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Friday, January 20, 2023 10:13:03 PM
Lease Expires . . . . . : Friday, January 20, 2023 11:13:02 PM
Default Gateway . . . . . : 192.168.226.32
DHCP Server . . . . . : 192.168.226.32
DHCPv6 IAID . . . . . : 136897351
DHCPv6 Client DUID. . . . . : 00-01-00-01-24-2B-9D-CF-40-A8-F0-05-3E-9C
DNS Servers . . . . . : 192.168.226.32
NetBIOS over Tcpip. . . . . : Enabled

Tunnel adapter Teredo Tunneling Pseudo-Interface:
Connection-specific DNS Suffix . :
Description . . . . . : Microsoft Teredo Tunneling Adapter
Physical Address. . . . . : 00-00-00-00-00-00-E0
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . : Yes
IPv6 Address. . . . . : 2001:0:284a:364:c22:118f:d12c:a7fd(Preferred)
Link-local IPv6 Address . . . . : fe80::c22:118f:d12c:a7fd%20(Preferred)
Default Gateway . . . . . :
DHCPv6 IAID . . . . . : 335544320
DHCPv6 Client DUID. . . . . : 00-01-00-01-24-2B-9D-CF-40-A8-F0-05-3E-9C
NetBIOS over Tcpip. . . . . : Disabled
  
```

Рис. 3.1. Екранне вікно командного рядка ПК з відображенням даних бездротової мережі.

Крок 2. Запуск програми Wireshark і початок збору даних.

Оскільки варіант «Ethernet» недоступний внаслідок відсутності підключення ПК до локальної мережі, то після запуску Wireshark варто обрати інтерфейс захоплення трафіка і варіант «Бездротова мережа» (рис. 3.2).

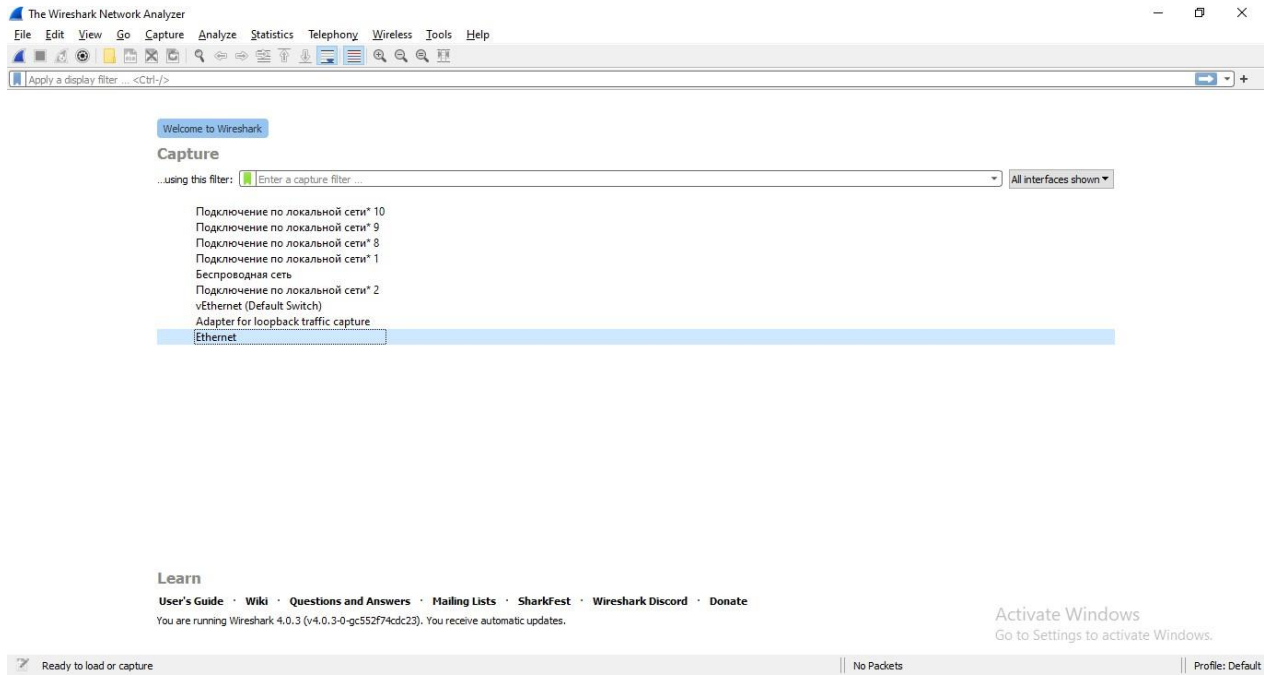


Рис. 3.2. Екранне вікно програмного аналізатора Wireshark.

Для керування інтерфейсом захоплення трафіка натиснути Capture, а далі – Options (рис. 3.3).

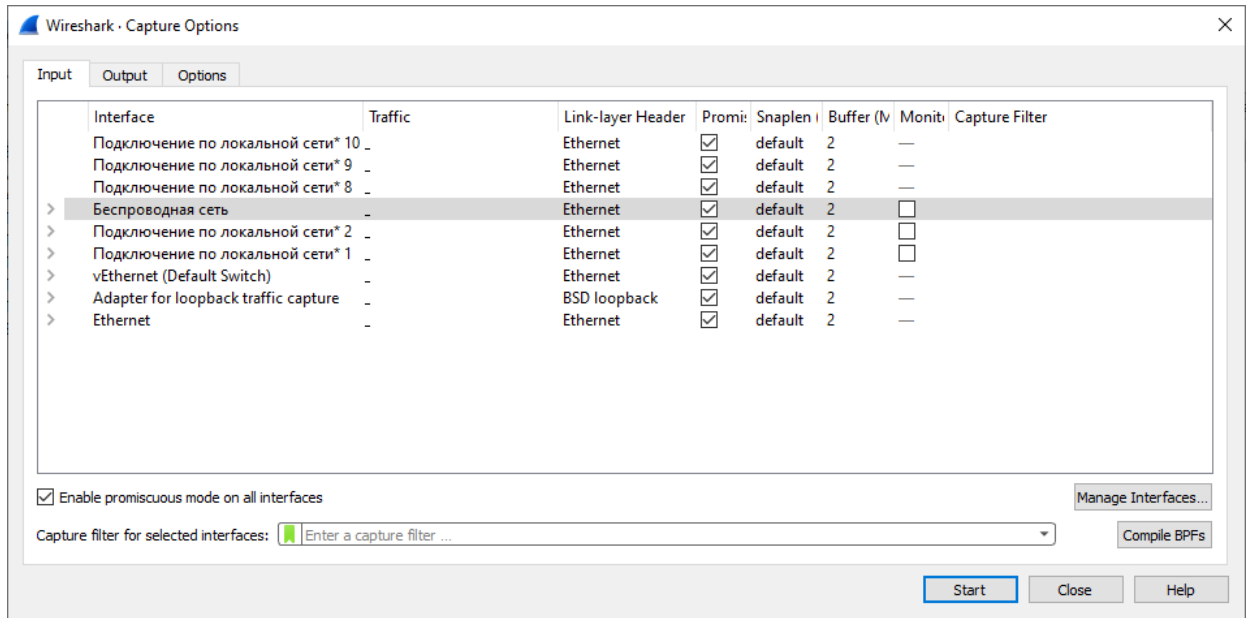


Рис. 3.3. Меню опцій захоплення трафіку.

Далі варто переконатися, що опис відповідає результату, показаному в командному рядку, натиснувши Manage interfaces (рис.3.4).

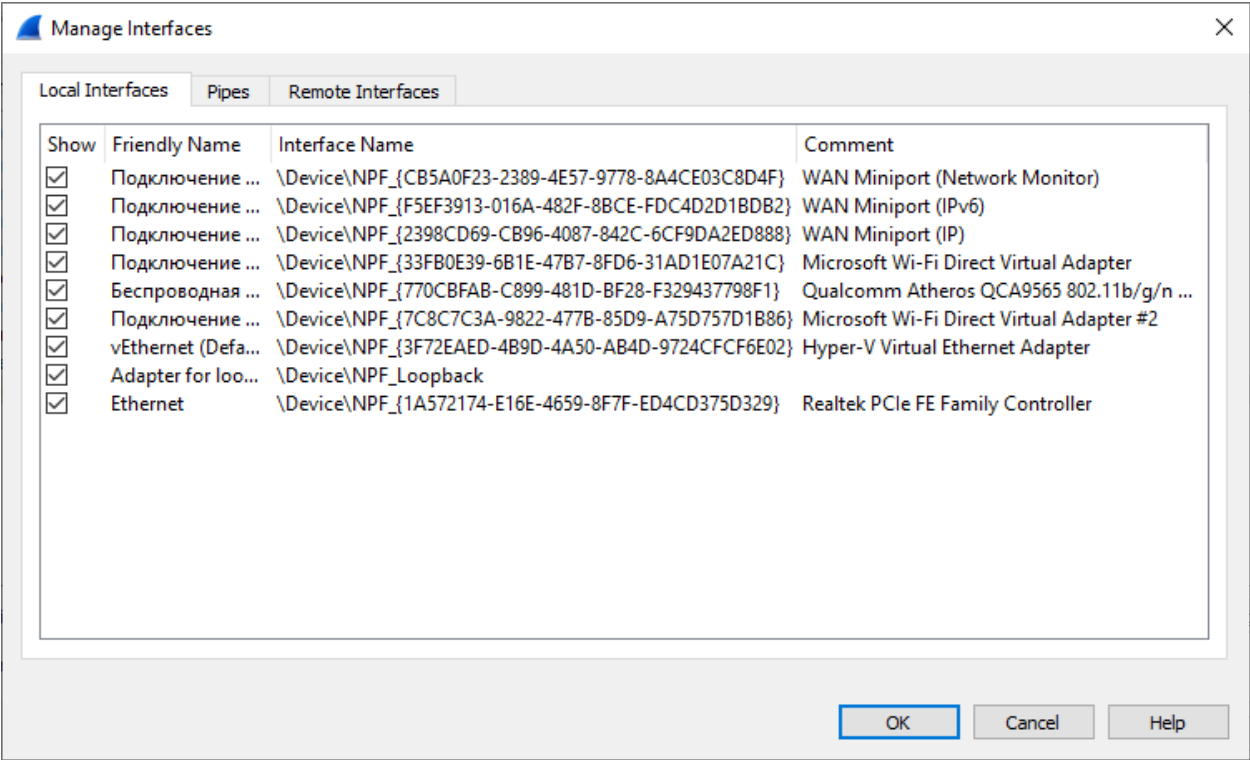


Рис. 3.4. Екранне вікно менеджменту інтерфейсів.

Після підготовки до сканування потрібно натиснути Start, щоб почати процес захоплення даних.

Показаний на рис. 3.5 результат захоплення даних в програмі Wireshark відображаються пакети, що були згенеровані за допомогою команди *ping*, відправленої з вузла ПК на шлюз за замовчуванням. Рядки даних виділяються різноманітними кольорами залежно від протоколу.

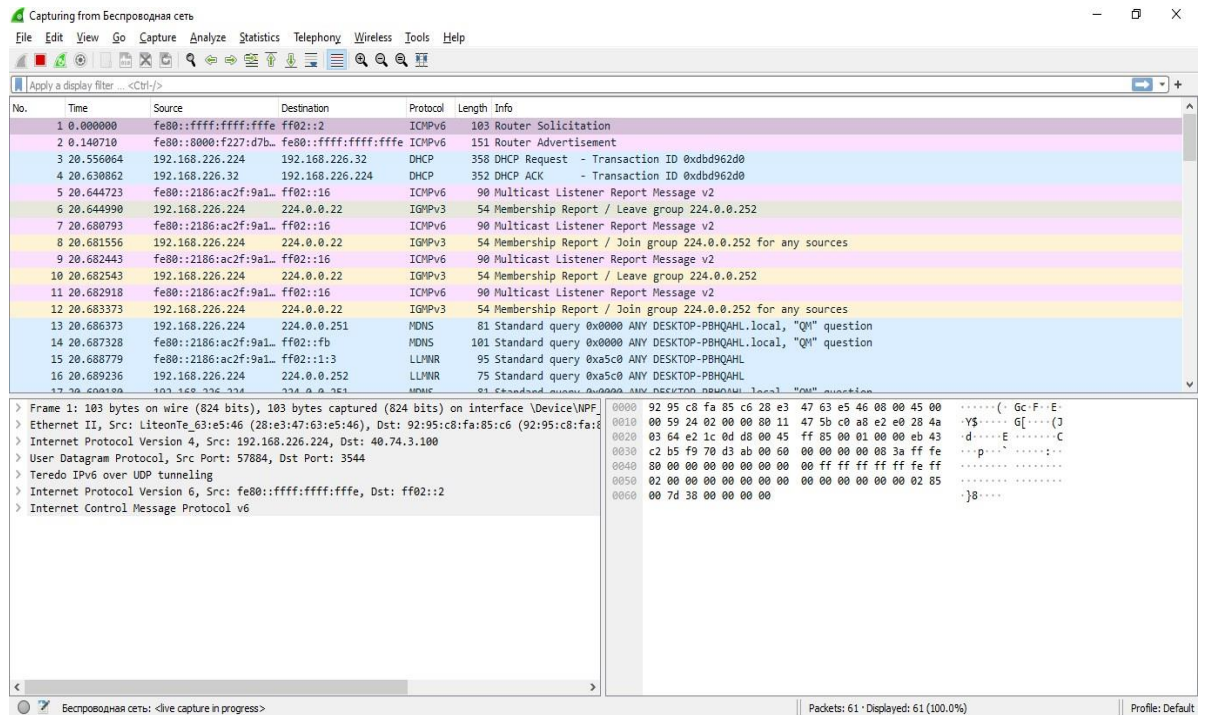


Рис.3.5. Екранне вікно результату захоплення даних бездротової мережі.

Крок 3. Захоплення і аналіз кадрів бездротової мережі за допомогою програми Wireshark за протоколом ICMP.

У рядку фільтр можна ввести одиниці даних будь-якого протоколу, наприклад ICMP. Для початку потрібно повторити крок 1 і назвати IP-адресу шлюзу ПК за замовчуванням: 192.168.226.32. Оскільки ICMP відсутній у списку протоколів, то варто застосувати протокол ICMPv6, для цього в поле фільтру потрібно ввести іcmpv6. При правильному налаштуванні фільтра поле має стати зеленим, якщо поле стало зеленим, варто натиснути кнопку Apply(застосувати), а при неправильному – червоним.

Головне вікно програми Wireshark складається з трьох розділів: панель списку пакетів(зверху), панель відомостей про пакети(знизу зліва), і панель відображення пакету у вигляді послідовності байтів(знизу зправа). Якщо було правильно вибрано інтерфейс для захоплення пакетів в кроці 4, програма Wireshark покаже дані протоколу ICMPv6 на панелі списку пакетів, як показано на рис. 3.6.

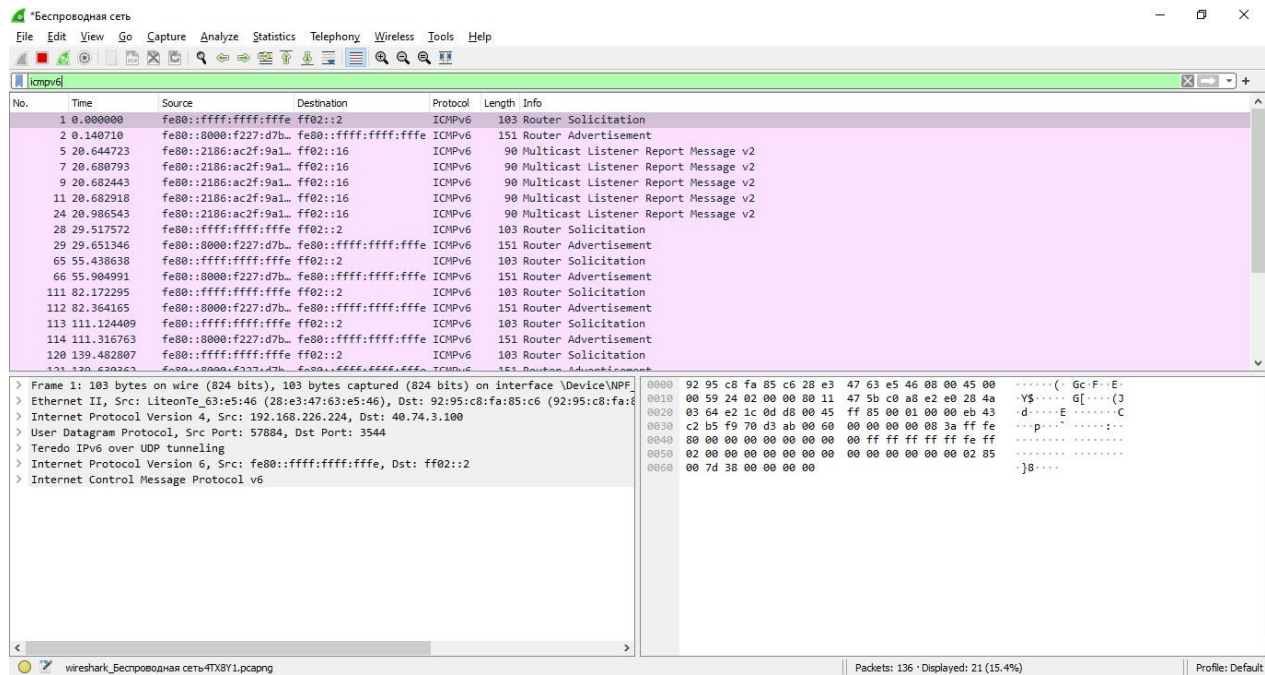


Рис. 3.6. Екранне вікно результату захоплення даних за протоколом ICMPv6.

Також можна виділити частину кадру(в шістнадцятирічній системі і ASCII) на панелі відображення пакету у вигляді послідовності байтів(нижній правий розділ), натиснувши на будь-який рядок у нижньому лівому розділі. Якщо натиснути на рядок «Internet Control Message Protocol v6» в нижньому лівому розділі, то можна побачити, що на панелі відображення пакету буде виділено значення у вигляді послідовності байтів (рис. 3.7), а натиснувши на стрілку рядку «Internet Control Message Protocol v6» або на відображене значення у вигляді послідовності байтів, то можна отримати докладний опис, як це показано на рис. 3.8.

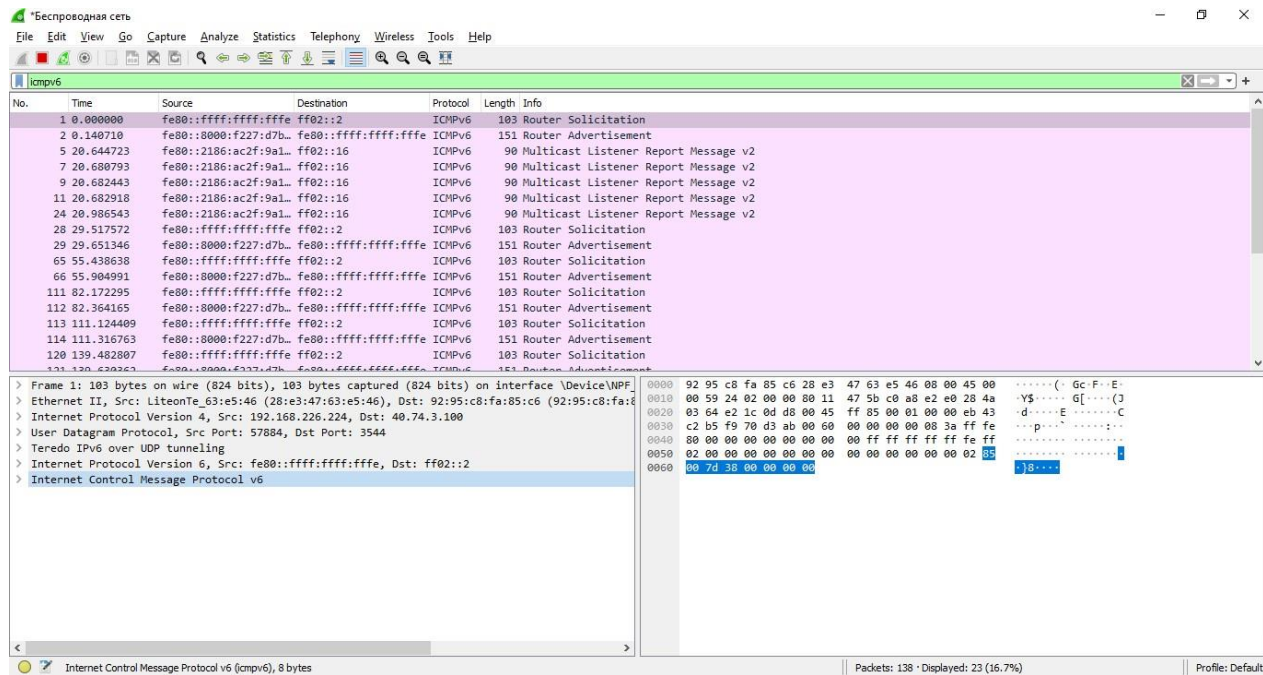


Рис. 3.7. Екранне вікно результату захоплення даних за протоколом ICMPv6 з виділенням рядка «Internet Control Message Protocol v6»

Аналогічний опис також буде і у вище вказаних рядках, що дає змогу мережевому адміністратору побачити загальну картину моніторингу стану функціонування комп'ютерної мережі.

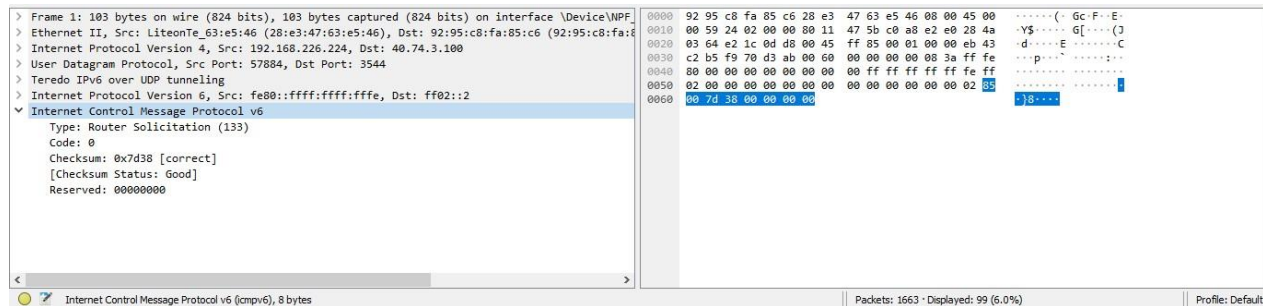


Рис. 3.8. Докладний опис рядка «Internet Control Message Protocol v6».

Окрім одного протоколу, у Wireshark є можливість перехоплювати пакети за декількома протоколами. Наприклад, доцільно спробувати дописати в панель списку пакетів протокол ARP(Address Resolution Protocol), і натиснути кнопку «Apply display filter».

На рис. 3.9 можна побачити, що окрім ICMPv6 також наявні пакети ARP. А якщо натиснути на рядок «Address Resolution Protocol (request)», то можна

побачити еквівалентну послідовність байтів, як в протоколі ICMPv6.

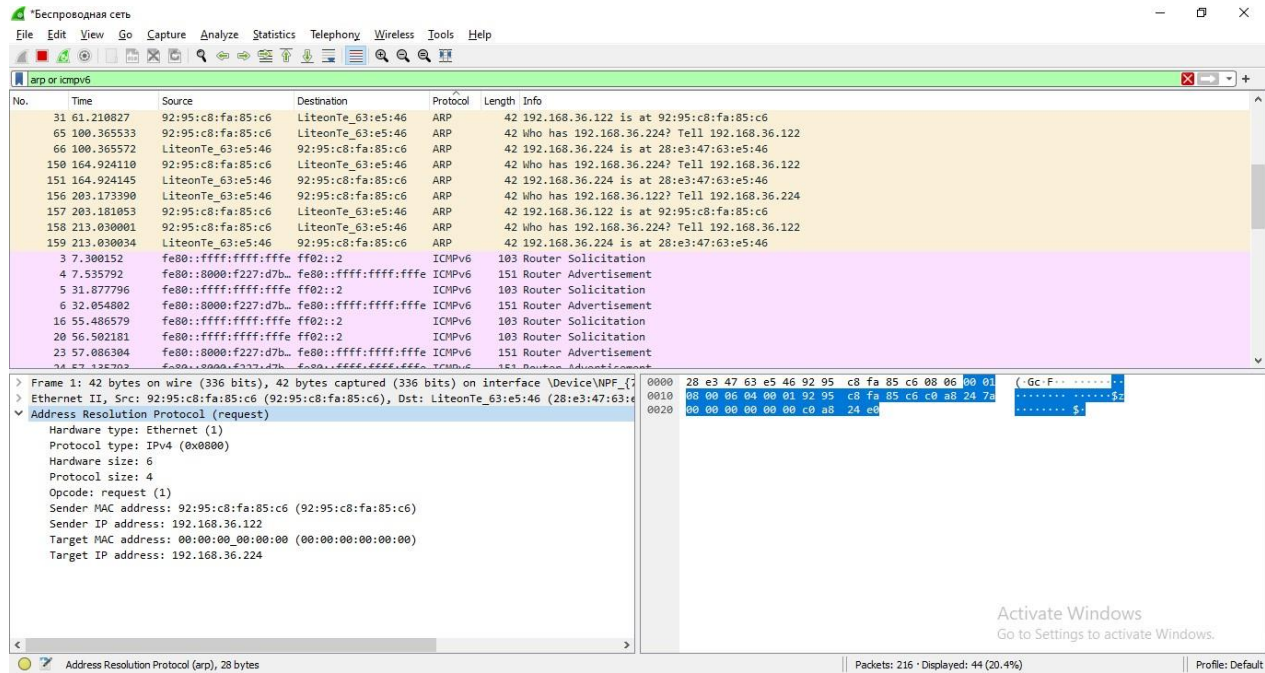


Рис.3.9. Екранне вікно результату захоплення даних за протоколом ICMPv6 і ARP з виділенням рядка «Address Resolution Protocol (request)».

Аналогічно можна додати протокол TCP, і таким чином здійснити захоплення пакетів за трьома протоколами(Рис.3.10).

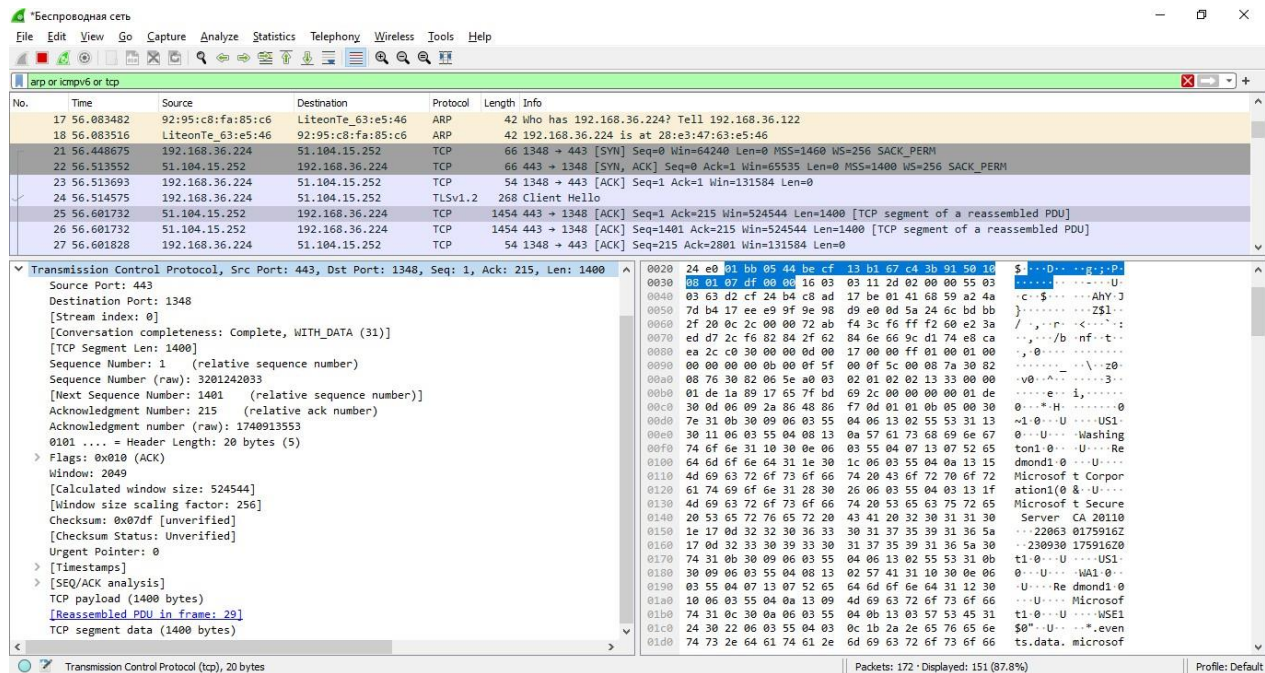


Рис.3.10. Екранне вікно результату захоплення даних за протоколом ICMPv6, ARP і TCP з виділенням рядка «Transmission Control Protocol».

В ході даного дослідження варто запропонувати систему моніторингу КМ, яка забезпечуватиме повний контроль наявності вразливостей та помилок конфігурування мережі, здійснюватиме детальний аналіз протоколів, відстежуватиме статус сервісів комп'ютерної мережі. Також під час її створення варто слідувати усім етапам проєктування і реалізації. Окрім того, варто здійснити підбір технологій створення таких систем, адже саме від них залежить результат створення майбутньої системи моніторингу КМ і як вона функціонуватиме.

Як правило, кожна система моніторингу КМ у своєму складі повинна мати підсистему виявлення вторгнень (IDS), аналізатор протоколів, засоби контролю наявності вразливостей та помилок конфігурування систем і сервісів, експертні системи, програми мережевого моніторингу. Також кожна система моніторингу КМ повинна здійснювати контроль наявності вразливостей та помилок конфігурування мережі, аналізувати кожен протокол і відстежувати статус сервісів комп'ютерних мереж. Також варто зазначити, що система моніторингу КМ повинна мати базу даних, де зберігається інформація про статус функціонування КМ.

Для цього доцільно сформувати такі підсистеми:

1) Підсистема виявлення вторгнень (IDS) – збирають інформацію з різних системних і мережевих джерел, а потім аналізують інформацію про ознаки вторгнення та зловживання. Якщо зібрана інформація про ознаки вторгнення та зловживання підтверджується, то підсистема IDS блокує дане джерело, у випадку виявлення потенційно-небезпечного джерела підсистема поміщає його на карантин.

2) Підсистема аналізу протоколів – аналізує кожен доступний мережевий протокол залежно від типу мережі та пристрою, на якому проводиться аналіз. Прикладом аналізу протоколів є нещодавно проведені перехоплення пакетів у програмі Wireshark.

3) Підсистема відстеження статусу сервісів КМ – дає можливість користувачу стежити за роботоздатністю сервісів комп'ютерних мереж в

режимі реального часу. Така підсистема може являти собою панель приладів, що відображає статус сервісів КМ та її компоненти у вигляді графіків та діаграм.

4) Підсистема контролю наявності вразливостей та помилок конфігурування мережі – дозволяє системі виявляти помилки конфігурації мережі та вразливі місця в мережі при кожному підключенні, також виконує функції антивірусу, і має такі складові:

- Журнал: зберігає попередні результати сканування мережі у хронологічному порядку.

- Карантин: зберігає файли, які можуть нести потенційну загрозу КМ і пристрою, з якого було здійснено сканування мережі, для їх подальшого дослідження.

- Шредер: знищує файли, потенційна загроза яких підтвердилася під час сканування мережі. Також система за вибором користувача може перемістити файли з карантину, загрозу яких було підтверджено під час дослідження у самому карантині.

5) Підсистема налаштувань системи – оптимізує програмні компоненти системи моніторингу КМ, перевіряє наявність оновлень до останніх версій і контролю пристроїв, з яких було здійснено доступ до системи моніторингу КМ. Також дана підсистема здійснює контроль доступу до системи.

З опису останньої підсистеми відомо, що система моніторингу КМ має функціонувати на будь-якому пристрої незалежно від ОС, і повинна мати синхронізацію між пристроями, на яких функціонує дана система. Окрім того, система моніторингу КМ також потребує захисту від несанкціонованого доступу. Для цього під час авторизації до системи доцільно застосувати так звану «двохфакторну автентифікацію». Принцип роботи двофакторної автентифікації полягає в тому, що користувач, авторизуючись до системи, вводить логін і пароль. Далі система генерує одноразовий код з метою підтвердження входу користувача за допомогою SMS-повідомлення на телефон чи повідомлення на електронну пошту, що були вказані під час

реєстрації в системі моніторингу КМ. У випадку авторизації в системі моніторингу КМ зі смартфона, то залежно від характеристик самого смартфона, можна застосувати і біометричний спосіб авторизації. Це може бути вхід в систему за допомогою сканеру відбитків пальців чи системи розпізнавання обличчя залежно від налаштувань. Також передбачено біометричний спосіб підтвердження входу під час двохфакторної автентифікації: після введення логіна і пароля система відправляє повідомлення про авторизацію в системі в мобільний додаток системи моніторингу КМ, далі користувач повинен відкрити дане повідомлення і підтвердити вхід до системи за допомогою сканування відбитку пальця і після цього можна отримати доступ до системи.

Таким чином, ідеальна система моніторингу КМ повинна автоматично і постійно контролювати мережі, оперативно інформувати користувача про проблеми, які виникають, і бути розумною, щоб вказати на проблему та її точне розташування в топології мережі, а також методи і способи усунення даних проблем.

Також система повинна мати можливість виявити наслідки проблеми для решти мережі та служб, які можуть стати недоступними; повинна вести облік змін у мережі, що полегшує пошук причини проблеми через зміну конфігурації; забезпечувати віддалену автентифікацію та авторизацію для адміністратора для доступу до системи моніторингу КМ звідусіль.

ВИСНОВКИ

Сучасний стан розвитку та широке запровадження комп'ютерних мереж в усі галузі економіки зумовлюють важливість питання про підвищення вимог щодо підтримки їх працездатності, до якості і безпеки роботи в мережі та необхідності моніторингу стану їх функціонування. Саме моніторинг комп'ютерної мережі забезпечує можливість контролювати та убезпечити робочий процес, який пов'язаний з інтернетом і комп'ютерами.

Пошук ефективних методів та програмно-технічних засобів для здійснення постійного моніторингу та діагностики роботи мережного устаткування, прикладних програм і мережних сервісів, є визначальним для організації забезпечення кінцевих користувачів якісним доступом до мережесих ресурсів, та свідчить про актуальність обраної для дослідження теми.

При виконанні кваліфікаційної роботи було визначено, що

- для вирішення більшої частини проблем, які виникають при функціонуванні комп'ютерної мережі, використовують відповідні методи та програмно-технічні засоби, які дозволяють здійснювати проактивний моніторинг доступності, стану й продуктивності компонентів мережі, аналізувати й оптимізувати їх завантаження, а також прогнозувати виникнення позаштатних ситуацій.

- за допомогою моніторингу здійснюється пошук відповідей на питання щодо ефективності роботи певної системи чи технології, та визначаються чинники, які впливають на роботу певного об'єкта.

Результати проведеного дослідження за визначеною темою свідчать, що:

- моніторинг стану функціонування комп'ютерної мережі може здійснюватися активним чи пасивним методами, базуватися на маршрутизації чи відслідковувати аномальну поведінку;
- для здійснення аналізу циркулюючих у мережі пакетів, які реалізують той чи інший мережесий протокол, та вивчення вмісту цих пакетів використовуються

аналізатори протоколів, результати роботи яких можуть зумовити пошук помилок та їх усунення, заміну компонентів мережі та оптимізацію продуктивності її роботи.

- при незначних розмірах комп'ютерної мережі архітектура системи моніторингу повинна бути централізована, перевагами якої є простота та швидкість реалізації, а для розгалужених комп'ютерних мереж більше підходить федеративна архітектура систем моніторингу.

- важливою складовою моніторингу, що впливає на його ефективність, є контроль наявності вразливостей та помилок конфігурування мережі, який спрямований на відстеження нових загроз і зміни IT-середовища.

- існує достатньо велика кількість програмних засобів для реалізації контролю наявності вразливостей і помилок конфігурування мережі, серед яких, за результатами аналізу, було обрано для застосування систему Wireshark. За допомогою цієї системи було проведено процедуру захоплення пакетів бездротової мережі, а також захоплення пакетів за протоколом ICMPv6, ARP та TCP.

- для детектування атак у комп'ютерній мережі повинні функціонувати у режимі реального часу системи виявлення вторгнень IDS, яких є два типи - HIDS та NIDS. Кожен тип IDS має свої особливості роботи та використовує різні методи виявлення вторгнення — на основі сигнатур, аномалій, підписів. Для визначення переваг та недоліків найбільш відомих IDS (Bro IDS, Security Onion, Snort, Suricata) було виконано порівняльний аналіз їх функціональних можливостей, за результатами якого можливо здійснювати їх вибір. Повноцінною мережевою системою виявлення вторгнень є програма Snort.

- інструменти моніторингу повинні не лише перевіряти продуктивність, пропускну здатність та безпеку мережі, доступність її елементів, а також генерувати сповіщення на основі відстежуваних показників і створювати звіти.

Комплексне застосування таких методів, засобів та підходів для здійснення постійного моніторингу забезпечує контроль наявності

вразливостей та помилок конфігурування мережі, аналіз протоколів, відстеження статусу сервісів комп'ютерної мережі.

Варто зазначити, що при формуванні комплексної системи моніторингу необхідно слідувати етапам проєктування таких систем, що забезпечить ефективність функціонування всіх складових системи, а також гнучкість та живучість самого технологічного процесу моніторингу.

Необхідно також відзначити, що дослідження засобів моніторингу комп'ютерних мереж є перспективним напрямом розвитку інформаційної інфраструктури та забезпечення надання якісних послуг її абонентам. Незважаючи на ряд проблем, що виникають при впровадженні, застосування методів та засобів моніторингу, за рахунок можливостей перевірки стану функціонування комп'ютерних мереж, включаючи продуктивність, пропускну здатність та безпеку, може забезпечити значне зростання ефективності використання мережного обладнання, знизити кількість критичних збоїв та несанкціонованих дій, що особливо важливо у сучасних умовах.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Желєзняк В.В., Мясіщев О.А., Ленков С.В., Сєлюков Д.О. Аналіз методів та алгоритмів моніторингу обчислювальних мереж. URL: <https://miljournals.knu.ua/index.php/zbirnuk/article/view/293/284> (дата перегляду: 25.09.2022)
2. Кривуля Г. Ф. Комп'ютерні мережі //Енциклопедія Сучасної України: енциклопедія [електронна версія] /ред.: І. М. Дзюба, А. І. Жуковський, М. Г. Желєзняк та ін.; НАН України, НТШ. Київ: Інститут енциклопедичних досліджень НАН України, 2014. Т. 14. URL: <https://esu.com.ua/article-4398> (дата перегляду: 30.09.2022)
3. Гузій М, Станіславова О, Кадет М. Аналіз технологій моніторингу комп'ютерних мереж. Наукоємні технології. No4 (16), URL: <http://jml.nau.edu.ua/index.php/SBT/article/viewFile/5091/5353#:~:text=%D0%A2%D0%B5%D1%80%D0%BC%D1%96%D0%BD%D0%BE%D0%BC%20%D0%BC%D0%BE%D0%BD%D1%96%D1%82%D0%BE%D1%80%D0%B8%D0%BD%D0%B3%20%D0%BC%D0%B5%D1%80%D0%B5%D0%B6%D1%96%20%D0%B2%D0%B8%D0%B7%D0%BD%D0%B0%D1%87%D0%B0%D1%8E%D1%82%D1%8C%20%D1%80%D0%BE%D0%B1%D0%BE%D1%82%D1%83,%D1%94%20%D0%BF%D1%96%D0%B4%D0%BC%D0%BD%D0%BE%D0%B6%D0%B8%D0%BD%D0%BE%D1%8E%20%D0%B7%D0%B0%D0%B2%D0%B4%D0%B0%D0%BD%D1%8C%20%D1%83%D0%BF%D1%80%D0%B0%D0%B2%D0%BB%D1%96%D0%BD%D0%BD%D1%8F%20%D0%BC%D0%B5%D1%80%D0%B5%D0%B6%D0%B5%D1%8E> (дата звернення: 10.10.2022).
4. Задорожна Н.Т., Каплун О.О., Кузнецова Т.В. Підхід до проектування системи моніторингу як складової інформаційних технологій підтримки діяльності органів державного управління. URL: https://core.ac.uk/display/32305432?utm_source=pdf&utm_medium=banner&utm_campaign=pdf-decoration-v1 (дата звернення: 12.10.2022)
5. Моніторинг. URL: https://www.vostok.dp.ua/ukr/infa1/glossary/gl_monitoring/ (дата звернення: 15.10.2022)
6. Моніторинг мережі. URL: <https://www.motadata.com/uk/what-is-network-monitoring/> (дата звернення: 15.10.2022)
7. Internetworking Technology Handbook: User manual /Jackson C. –

Massachusetts : Cisco Systems, 2011. – P. 56 - 67. (дата звернення: 18.10.2022)

8. Cecil A. A Summary of Network Traffic Monitoring and Analysis Techniques / A. Cecil // Computer Systems Analysis. – 2006. – P. 4 – 7. (дата звернення: 20.10.2022)

9. Lowekamp B. Using passive traces of application traffic in a network monitoring systems. / B.B. Lowekamp, M. Zangrilli. – IEEE Computer Society, 2004. – P. 73 – 75. (дата звернення: 23.10.2022)

10. Багатоплатформність. URL: <https://uk.wikipedia.org/wiki/Багатоплатформність> (дата звернення: 30.10.2022)

11. Fry C. Security Monitoring /C. Fry, M. Nystrom – Sebastopol: O'Reily Media, 2009. – P. 40 – 56, 163 – 170. (дата звернення: 05.11.2022)

12. Cisco Systems, Inc., "Enterprise Campus 3.0 Architecture: Overview and Framework," 2008. URL: <http://www.cisco.com/en/US/docs/solutions/Enterprise/Campus/campover.html> (дата звернення: 10.11.2022)

13. J. Case, M. Fedor, M. Schoffstall and J. Davin, "RFC1157: A Simple Network Management Protocol (SNMP)," 5 1990. URL: <http://www.ietf.org/rfc/rfc1157.txt>. (дата звернення: 12.11.2022)

14. AppDynamics. URL: <https://www.appdynamics.com> (дата звернення: 15.11.2022)

15. CheckNMK. URL: <https://checkmk.com> (дата звернення: 15.11.2022)

16. Icinga. URL: <https://icinga.com> (дата звернення: 15.11.2022)

17. LibreNMS. URL: <https://www.librenms.org> (дата звернення: 15.11.2022)

18. Monit. URL: <https://mmonit.com/monit/> (дата звернення: 15.11.2022)

19. Monitorix. URL: <https://www.monitorix.org> (дата звернення: 15.11.2022)

20. Monitoror. URL: <https://monitoror.com> (дата звернення: 15.11.2022)

21. Munin. URL: <https://munin-monitoring.org> (дата звернення: 15.11.2022)

22. Nagios. URL: <https://www.nagios.org> (дата звернення: 15.11.2022)

23. Netdata. URL: <https://www.netdata.cloud> (дата звернення: 15.11.2022)
24. NetXMS . URL: <https://netxms.com> (дата звернення: 15.11.2022)
25. Newrelic. URL: <https://newrelic.com> (дата звернення: 15.11.2022)
26. Observium. URL: <https://www.observium.org> (дата звернення: 15.11.2022)
27. Prometheus. URL: <https://prometheus.io> (дата звернення: 15.11.2022)
28. Sematext monitoring. URL: <https://sematext.com/spm/> (дата звернення: 15.11.2022)
29. SolarWinds. URL: <https://www.solarwinds.com/server-application-monitor> (дата звернення: 15.11.2022)
30. Mikrotik. URL: <https://mikrotik.com/thedude> (дата звернення: 15.11.2022)
31. WhatsUp Gold. URL: <https://www.whatsupgold.com> (дата звернення: 15.11.2022)
32. Zabbix. URL: <https://www.zabbix.com> (дата звернення: 15.11.2022)
33. Top Free Network-Based Intrusion Detection Systems (IDS) for the Enterprise. URL: <https://www.upguard.com/articles/top-free-network-based-intrusion-detection-systems-ids-for-the-enterprise> (дата звернення: 20.11.2022)
34. Open Source Intrusion Detection System using Snort: conf. paper from the 4th International Symposium on Sustainable Development. International Burch University, Faculty of Engineering and Information Technologies. Sarajevo: SOC-1441, 2014. 8 p (дата звернення: 23.11.2022)
35. Snort. URL: <https://www.snort.org> (дата звернення: 25.11.2022)
36. Suricata. URL: <https://suricata.io> (дата звернення: 25.11.2022)
37. Bro IDS. URL: <https://zeek.org> (дата звернення: 25.11.2022)
38. Security Onion. URL: <https://securityonionsolutions.com> (дата звернення: 25.11.2022)
39. Трирівнева клієнт-серверна архітектура. URL: http://immisp.kiev.ua/publications/articles/2018/2018_3/03_2018_Ryndych.pdf (дата звернення: 05.12.2022)

40. Опорний конспект лекцій з дисципліни —”Моніторинг мережевої безпеки” для студентів напряму підготовки —”кібербезпека” освітнього рівня —”магістр”/ Тернопільський національний економічний університет; Уклад. В.В. Яцків, І.З. Якименко—Тернопіль, ФО-П Шпак В., 2019. – 68 с. – URL: http://dspace.wunu.edu.ua/jspui/bitstream/316497/36006/1/Лекції_ММБ.pdf (дата звернення: 10.12.2022)

41. Керування вразливостями. URL: <https://www.microsoft.com/uk-ua/security/business/security-101/what-is-vulnerability-management> (дата звернення: 20.12.2022)

42. Аналізатори протоколів. URL: <https://studfile.net/preview/9239701/page:9/> (дата звернення: 08.01.2023)

43. Wireshark. URL: <https://www.wireshark.org> (дата звернення: 12.01.2023)