ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
КАФЕДРА КОМП'ЮТЕРНОЙ ІНЖЕНЕРІЇ

КВАЛІФІКАЦІЙНА РОБОТА

на тему: **"Дослідження методів пошуку та усунення несправності в сучасних комп'ютерних мережах"**

на здобуття освітнього ступеня магістра
зі спеціальності ___123__Комп'ютерна інженерія_____
(код, найменування спеціальності)

освітньо-професійної програми Комп'ютерні системи та мережі
(назва)

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____ Владислав Гнядий__
(підпис) *Ім'я, ПРІЗВИЩЕ здобувача*

Виконав здобувач вищої освіти гр. КСДМ -61
Владислав Гнядий _
Ім'я, ПРІЗВИЩЕ

Керівник к.т.н., доцент Вячеслав Черевик
науковий ступінь, вчене звання Ім'я, ПРІЗВИЩЕ

Рецензент: _____
науковий ступінь, вчене звання Ім'я, ПРІЗВИЩЕ

Київ 2024

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Кафедра Комп'ютерної інженерії
Ступінь вищої освіти магістр
Спеціальність 123 Комп'ютерна інженерія
Освітньо-професійна програма _____

ЗАТВЕРДЖУЮ
Завідувач кафедрою Комп'ютерної інженерії
_____Наталія Лащевська
Ім'я, ПРІЗВИЩЕ
« » _____ 202 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

_____ Гнядий Владислав Юрійович _____
(прізвище, ім'я, по батькові здобувача)

1. Тема кваліфікаційної роботи: **"Дослідження методів пошуку та усунення несправності в сучасних комп'ютерних мережах"**
керівник кваліфікаційної роботи Вячеслав Черевик к.т.н., доцент
(Ім'я, ПРІЗВИЩЕ, науковий ступінь, вчене звання)
затверджені наказом Державного університету інформаційно-комунікаційних технологій від « 19 » жовтня 2023 р. № 145.
2. Строк подання кваліфікаційної роботи «8» січня 2024 р.
3. Вихідні дані до кваліфікаційної роботи:
3.1 Вимоги до кваліфікаційної роботи магістра з актуальних завдань спеціальності.
3.2 Нормативні матеріали (стандарти).
3.3 Технічні вимоги.
3.4 Науково-технічна література з питань, пов'язаних з темою роботи.
4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
4.1 Аналіз методів пошуку та усунення несправності в комп'ютерних мережах
4.2 Використання штучного інтелекту для вдосконалення методів пошуку та усунення несправностей у комп'ютерних мережах
4.3 Практичні рекомендації з пошуку та усунення несправностей у комп'ютерних мережах.
5. Перелік ілюстративного матеріалу: презентація

6. Дата видачі завдання«19» жовтня 2023 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1	Підбір науково-технічної літератури	20.10.2023	викононо
2	Аналіз завдання	21.10.2023	викононо
3	Пошук підходів до вирішення завдання.	01.11.2023	викононо
4	Написання розділів роботи.	01.12.2023	викононо
5	Формування висновків.	03.12.2023	викононо
6	Оформлення пояснювальної записки.	04.12.2023	викононо
7	Підготовка демонстраційних матеріалів.	05.12.2023	викононо
8	Попередній захист роботи	06.12.2023	викононо
1.	Пред’явлення роботи в деканат	08.01.2024	викононо

Здобувач(ка) вищої освіти _____ Владислав Гнядий
(підпис) *Ім’я, ПРІЗВИЩЕ)*

Керівник кваліфікаційної роботи _____ _Вячеслав Черевик
(підпис) *Ім’я, ПРІЗВИЩЕ)*

РЕФЕРАТ

Текстова частина кваліфікаційної роботи на здобуття освітнього ступеня магістра: 68 стор., 21 рис., 5 табл., 34 джерела.

Мета роботи – проведення аналізу та пошуку варіантів побудови систем діагностики несправносте в комп’ютерних мережах з метою підвищення надійності їх функціонування.

Об’єкт дослідження – впровадження сучасних методів пошуку та усунення несправностей в комп’ютерних мережах.

Предмет дослідження – комп’ютерні мережі.

Короткий зміст роботи. Дослідження присвячене аналізу та порівняльному дослідженню різних методів пошуку та усунення несправностей у сучасних комп'ютерних мережах. У ході дослідження було розглянуто існуючі підходи до виявлення та виправлення проблем, що виникають у мережній інфраструктурі. Було проаналізовано переваги та недоліки кожного методу, а також оцінено їх ефективність у вирішенні різних типів несправностей, таких як відмови обладнання, проблеми маршрутизації, порушення безпеки тощо. В результаті дослідження було виділено найбільш ефективні та оптимальні методи пошуку та усунення несправностей, які можуть бути використані у сучасних комп'ютерних мережах. Це дослідження є корисним ресурсом для фахівців з мережевої інфраструктури, адміністраторів мереж та інших зацікавлених осіб, які прагнуть налагодити стабільну роботу комп'ютерних мереж та мінімізувати час простою мережевих пристроїв.

КЛЮЧОВІ СЛОВА: КОМП’ЮТЕРНІ МЕРЕЖА, ДІАГНОСТИКА, НЕСПРАВНІСТЬ.

ABSTRACT

The text part of the qualification work for obtaining the master's degree: 68 pages, 21 figures, 5 tables, 34 sources.

The purpose of the work is to conduct an analysis and search for options for building systems for diagnosing malfunctions in computer networks in order to increase the reliability of their operation.

The object of the research is the introduction of modern methods of finding and eliminating faults in computer networks.

The subject of research is computer networks.

Brief content of the work. The study is devoted to the analysis and comparative study of various methods of finding and eliminating faults in modern computer networks. In the course of the study, the existing approaches to identifying and correcting problems arising in the network infrastructure were considered. The advantages and disadvantages of each method were analyzed and their effectiveness in solving different types of faults such as hardware failures, routing problems, security breaches, etc. was evaluated. As a result of the study, the most effective and optimal methods of finding and eliminating faults that can be used in modern computer networks were selected. This study is a useful resource for network infrastructure professionals, network administrators, and other interested parties who seek to establish stable operation of computer networks and minimize downtime of network devices.

KEY WORDS: COMPUTER NETWORK, DIAGNOSTICS, FAILURE.

Скорочення

CNN	Convolutional Neural Networks
CSMA/CD	Carrier Sense Multiple Access with Collision Detection
IT	Information Technology
IP	Internet Protocol
HTTP	HyperText Transfer Protocol
LSTM	Long Short-Term Memory Networks
MAC	Media Access Control
MLP	Multilayer Perceptron
RNN	Recurrent Neural Networks
SSH	Secure Shell
OSI	Open Systems Interconnection
TCP	Transmission Control Protocol
ЗНМ	Згорткова нейронна мережа
КМ	Комп’ютерна мережа
КС	Комп’ютерна система
ШІ	Штучний інтелект
ШНМ	Штучна нейронна мережа

ЗМІСТ

Стр.

Вступ

Сучасні комп'ютерні мережі стають все більшими і складнішими, включаючи сотні та тисячі пристроїв, віртуальних серверів та хмарних ресурсів. Це призводить до зростання кількості можливих точок відмови та несправностей у мережі. Дослідження методів пошуку та усунення несправностей є необхідним для забезпечення надійності та безпеки роботи сучасних мереж.

Несправності в мережах можуть призвести до простоїв, зниження продуктивності або навіть втрати даних. Це може позначитися на продуктивності бізнесу, виробленні прибутку та якості обслуговування. Ефективні методи пошуку та усунення несправностей дозволять скоротити час реакції на проблеми та мінімізувати втрати.

Сучасні мережі можуть включати різні види пристроїв, протоколів та сервісів, такі як віртуалізація, хмарні обчислення, мобільний доступ та Інтернет речей (IoT). Несправності в таких складних середовищах можуть бути складними для виявлення та вирішення. Дослідження методів пошуку та усунення несправностей дозволить адаптувати існуючі методи та розробити нові підходи для таких складних мережевих сценаріїв.

З розвитком технологій штучного інтелекту та машинного навчання стало можливим застосування алгоритмів та методів для автоматизації пошуку та усунення несправностей у комп'ютерних мережах. Це відкриває нові можливості для покращення ефективності та точності діагностики та відновлення в мережах.

Всі ці фактори свідчать про необхідність та актуальність дослідження методів пошуку та усунення несправностей у сучасних комп'ютерних мережах. Це допоможе підвищити надійність, продуктивність та безпеку мереж, а також покращити якість обслуговування та знизити втрати часу та ресурсів.

Сучасні комп'ютерні мережі є складними та динамічними системами. Тому пошук та усунення несправностей у таких мережах є завданням з високим рівнем складності. В останні роки проводилося безліч досліджень та публікацій, присвячених розробці ефективних методів пошуку та усунення несправностей у комп'ютерних мережах.

Однією з основних тем дослідження є розробка методів виявлення несправностей у мережі. Для цього використовуються різні алгоритми, такі як протоколи Internet Control Message Protocol (ICMP), SNMP (Simple Network Management Protocol) і т.д.

Було запропоновано нові підходи до виявлення несправностей на основі аналізу трафіку, використання машинного навчання та аналізу даних.

Крім того, дослідження також фокусуються на розробці методів усунення несправностей комп'ютерних мереж. Одним із методів є використання резервування та відмовостійкості. Нові алгоритми резервування дозволяють швидко перемикатися на резервні канали у разі несправності основного каналу. Також було запропоновано методи автоматичного відновлення мережі, які дозволяють усунути несправності без участі адміністратора.

Інший напрямок досліджень пов'язане з поліпшенням продуктивності пошуку та усунення несправностей. Одним із підходів є використання оптимізації на основі ігрової теорії. Також проводяться дослідження використання штучного інтелекту та аналітичних методів, щоб зробити процес пошуку та усунення несправностей у мережі більш ефективним та автоматизованим.

Деякі дослідження також фокусуються на усуненні причин несправностей, а не лише на їхньому виявленні. Це включає дослідження, пов'язані з усуненням програмних помилок, поліпшенням апаратних компонентів мережі і

Мета роботи – проведення аналізу та пошуку варіантів побудови систем діагностики несправностей в комп’ютерних мережах з метою підвищення надійності їх функціонування.

Для досягнення поставленої мети необхідно вирішити такі задачі:

− провести аналіз використання сучасних методів пошуку та усунення несправності в комп’ютерних мережах;

− обґрунтувати вибір інструментів для діагностики несправностей в комп’ютерних мережах;

− розробити методику діагностики несправностей мереж;

− провести оцінку впливу системи діагностики на ефективність функціонування локальних мереж.

Об’єкт дослідження – впровадження сучасних методів пошуку та усунення несправностей в комп’ютерних мережах.

Предмет дослідження – комп’ютерні мережі

Для досягнення поставленого завдання використовувалися наукові методи системного аналізу, синтезу, моделювання, виміру, експерименту.

Результати даного дослідження дозволять покращити ефективність та надійність роботи комп'ютерних мереж, а також скоротити час та витрати на обслуговування та ремонт. Попередні дослідження в цій галузі фокусувалися на конкретних типах несправностей або протоколах, що використовуються в мережах, проте дане дослідження буде проводитися з урахуванням усіх можливих типів несправностей і різних протоколів, що робить його унікальним і значущим для застосування в реальних мережевих середовищах.

1 Аналіз методів пошуку та усунення несправності в комп’ютерних мережах

Діагностика комп'ютерної мережі є важливою складовою обслуговування та підтримки мережі. Розуміння основних понять та визначень допомагає фахівцям ефективно виявляти та усувати проблеми, забезпечуючи надійність та стабільність роботи комп’ютерной мережі

Комп'ютерна мережа одна із основних об'єктів діагностики у сучасних інформаційних технологіях. Діагностика комп'ютерної мережі – це процес виявлення та аналізу проблем у мережній інфраструктурі, з метою забезпечення її ефективної роботи в процесі експлуатації.

Основні поняття та визначення, що використовуються при пошуку та усунення несправності в комп’ютерних мережах, включають.

Комп'ютерна мережа **-** система взаємодіючих комп'ютерів та інших пристроїв, об'єднаних за допомогою мережевих з'єднань. Комп'ютерна мережа дозволяє обмінюватися інформацією та ресурсами між пристроями, що робить її невід'ємною частиною сучасного інформаційного суспільства.

Мережеві пристрої - апаратні пристрої, які використовуються для встановлення та підтримки з'єднань у комп'ютерній мережі. Прикладами мережевих пристроїв є маршрутизатори, комутатори, мости та маршрутизатори.

Протоколи - правила та стандарти, що визначають спосіб передачі даних та встановлення зв'язку між пристроями у комп'ютерній мережі. Протоколи забезпечують надійність та безпеку передачі даних, а також дозволяють різним пристроям взаємодіяти один з одним.

IP-адреса - унікальний ідентифікатор, присвоєний кожному пристрою в комп'ютерній мережі, щоб він міг бути ідентифікований і пов'язаний з іншими пристроями. IP-адреса складається з чотирьох чисел, розділених точками, і дозволяє маршрутизаторам та іншим мережним пристроям визначити, куди направити дані.

Пінг - програмний засіб, який використовується для перевірки доступності та затримки передачі даних між двома пристроями в мережі. Команда ping відправляє

невеликий пакет даних від одного пристрою до іншого та засікає час, за який пакет повертається. Це допомагає виявити можливі проблеми мережі, такі як втрата пакетів або висока затримка.

Порти - номери, які використовуються для визначення певних процесів або служб на пристрої в комп'ютерній мережі. Кожен мережевий протокол має певні порти певних типів комунікації. Наприклад, порт 80 використовується для з'єднань HTTP, а порт 22 - для SSH-з'єднань.

Трафік- передача даних у комп'ютерній мережі. Трафік може бути вихідним (що надсилається) або вхідним (приймається). Моніторинг та аналіз трафіку дозволяють виявляти можливі вузькі місця чи проблеми у роботі мережі.

Надійність - властивість об'єкта зберігати у часі в установлених межах значення всіх параметрів, які характеризують здатність виконувати потрібні функції в заданих режимах та умовах застосування, технічного обслуговування, зберігання та транспортування" [1].

Несправність - стан об'єкта, за яким він нездатний виконувати хоч би одну із заданих функцій об'єкта [1].

Незначна несправність - несправність, що непорушує жодної з потрібних функцій об'єкта [1].

Значна несправність - несправність, що порушує хоча б одну з потрібних функцій об'єкта [1].

Часткова несправність - несправність, що викликає нездатність об'єкта виконувати частину потрібних функцій [1].

Повна несправність - несправність, що характеризується повною нездатністю об'єкта виконувати усі потрібні функції [1].

Критична несправність - несправність, що може призвести до травмування людей, значних матеріальних збитків чи інших неприйнятних наслідків несправність через перевантаження [1].

Несправність через зношування - стан, коли об'єкт або система втрачає свою ефективність та працездатність через фізичне зношування, відпрацювання ресурсу або старіння її елементів. Ця несправність може бути наслідком нормального процесу експлуатації, коли об'єкт втрачає свою початкову якість та

функціональність з часом. Типовим прикладом є зношені деталі машин або електронних пристроїв, які вимагають заміни частин для подальшої працездатності. Також старіння може призводити до зміни властивостей матеріалів, що впливає на здатність системи виконувати свої функції. [ ].

Конструкційна несправність ситуація, коли в процесі побудови комп'ютерної мережі виявляються недоліки або помилки в її структурі або конфігурації. Це може включати неправильний розміщення кабелів або активного обладнання, некоректне підключення пристроїв до мережі, невірні налаштування IP-адрес і т.д. Несправність у побудові комп'ютерної мережі може призводити до проблем з підключенням до мережі, низької швидкості передачі даних, помилок в роботі пристроїв, втрати пакетів даних і інших негативних наслідків. Виправлення таких несправностей може вимагати проведення додаткових робіт з побудови мережі, перевірки налаштувань і, в деяких випадках, заміни несправних компонентів.

Стабільна несправність- стан, коли мережа функціонує неправильно або незадовільно протягом тривалого періоду часу. Несправність може виникати з різних причин, таких як нестабільний зв'язок між комп'ютерами, недостатня пропускна здатність, недостатнє обладнання або програмне забезпечення, помилки в конфігурації мережі тощо.

Прихована несправність - ситуація, коли в комп'ютерній мережі виникає помилка або помилкова поведінка, яка не виявляється або не обнаружується користувачами чи адміністраторами. Це може створити проблеми в роботі мережі, включаючи зниження продуктивності, втрату даних, проблеми з безпекою тощо. Приховані несправності можуть бути спричинені різними факторами, такими як помилки в конфігурації, несумісність обладнання, проблеми з програмним забезпеченням чи недостатній моніторинг та керування мережею.

Маскована несправність - ситуація, коли певний комп'ютер або устаткування в мережі виявляють ознаки несправності, але намагаються приховати цю інформацію від інших пристроїв або користувачів мережі. Це може бути зроблено шляхом приховання або приглушення повідомлень про помилки, очищення журналів подій або інших заходів, які допомагають маскувати проблему.

Пошкодження - подія, яка полягає у порушенні справного стану об'єкта коли зберігається його працездатність [1]

Відмова - Подія, яка полягає у втраті об'єктом здатності виконувати потрібну функцію, тобто у порушенні працездатного стану об'єкта [1].

Збій - самоусувна відмова або одноразова відмова, яку незначним втручанням усуває оператор [1].

Колізія в комп'ютерной мережі - ситуація, коли два або більше пристроїв в одній мережі намагаються передати дані через спільний канал одночасно. Результатом колізії є конфлікт, через який дані можуть бути втрачені або пошкоджені. Для вирішення колізій в мережах використовуються різні протоколи контролю доступу, такі як CSMA/CD (Carrier Sense Multiple Access with Collision Detection) у мережах Ethernet.

Аномалія в комп'ютерной мережі - порушення чи ненормальне явище, яке відхиляється від очікуваної роботи мережі. Це може бути проблема зі з'єднанням, помилка в передачі даних, атака зловмисника або інша несправність, яка впливає на нормальну роботу мережі. Аномалії можуть спричинити зниження швидкості мережі, втрату даних або недоступність мережевих ресурсів. Для виявлення та вирішення аномалій в мережах застосовуються спеціальні інструменти і технології, такі як системи моніторингу, виявлення вторгнень та аналізу поведінки мережі.

1.2 Класифікація несправностей КМ. Ознаки несправності.

Несправності, що негативно впливають на якість роботи комп’ютерної мережі необхідно поділять на наступні групи: явні мережні дефекти, що адресуються, явні мережні дефекти, приховані мережеві дефекти, явні вузькі місця, приховані вузькі місця [3].

Явні адресовані дефекти мережі - це конкретні проблеми або помилки в комп'ютерній мережі, які негативно позначаються на її якості роботи. Ці дефекти можуть бути причиною зниження продуктивності, непрацездатності або неправильної роботи мережі.

Деякі приклади явних адресованих мережевих дефектів:

- помилки з'єднання: це включає проблеми з підключенням комп'ютера або пристрою до мережі, відсутність або нестабільне з'єднання;
- перевантаження мережі: коли мережа не може обробити всі дані, що передаються, і робить роботу повільною або зупиняє передачу даних зовсім;
- втрата пакетів даних: деякі пакети даних можуть бути втрачені під час передачі, що може призвести до неповної або неправильної передачі інформації;
- конфлікти IP-адрес: якщо два або більше пристрої використовують одну і ту ж IP-адресу, виникають конфлікти, які можуть призвести до збоїв у роботі мережі;
- неправильне налаштування маршрутизатора або комутатора: неправильні установки можуть призвести до неправильного напрямку трафіку або некоректної роботи мережних пристроїв;
- проблеми безпеки: несанкціонований доступ, зловмисники, шкідливі програми та інші загрози можуть негативно впливати на роботу мережі та безпеку даних.

Всі ці дефекти можуть призвести до зниження продуктивності, значних затримок, втрати даних або просто відсутності роботи мережі. Тому їх регулярне виявлення та виправлення є важливим аспектом підтримки високої якості роботи комп'ютерної мережі.

Явні мережеві дефекти - це проблеми або несправності в комп'ютерній мережі, які прямо помітні і негативно впливають на критерій якості її роботи.

Всі ці явні мережеві дефекти негативно впливають на якість роботи комп'ютерної мережі, оскільки вони можуть викликати затримки передачі даних, втрату зв'язку, низьку пропускну здатність або інші збої в мережі. Тому вирішення цих проблем є важливим для забезпечення належної функціональності мережі.

Явні мережеві дефекти можуть бути викликані різними факторами, наприклад:

- перевантаження мережних пристроїв: коли мережні пристрої, такі як маршрутизатори або комутатори, працюють на межі своїх можливостей, це може призвести до затримок обробки пакетів даних або втрат пакетів;

− неправильне налаштування мережі: неправильно настроєні параметри мережі, такі як IP-адреси, підмережі або шлюзи, можуть призвести до відмови в підключенні або неможливості досягти потрібного вузла мережі;

− погане з'єднання або неякісні кабелі: дротики або роз'єми можуть бути пошкоджені або нецілісні, що призводить до втрати сигналу або втручання в передачу даних;

− втрати пакетів: неякісні або перевантажені мережні канали можуть призвести до втрат пакетів, що впливає на продуктивність та швидкість передачі даних;

− відсутність мережних заходів безпеки: відсутність оновлень програмного забезпечення, міжмережевих екранів або інших заходів безпеки може призвести до вразливостей у мережі та потенційних атак.

Явні вузькі місця в комп'ютерній мережі - це точки або компоненти мережі, які є вузькими місцями в пропускній здатності або продуктивності мережі і явно вибиваються із загального контексту роботи мережі. Ці вузькі місця можуть викликати затримку, втрату пакетів даних або зниження продуктивності мережі. Всі ці явні вузькі місця можуть негативно впливати на критерій якості роботи комп'ютерної мережі, такий як пропускна здатність, затримка та надійність. Якщо ці вузькі місця не усуваються або вирішуються неадекватно, мережа може працювати неправильно або неефективно.

Наддаймо деякі приклади явних вузьких місць у мережі:

− вузький канал зв'язку. Якщо мережа використовує вузький канал зв'язку, то пропускна здатність мережі суттєво обмежена, і це може призвести до затримок та втрати пакетів даних;

− недостатня пропускна спроможність маршрутизаторів. Якщо пропускна спроможність маршрутизаторів недостатня для обробки всіх пакетів даних, мережа може стати повільною та нестабільною;

− ненадійні підключення до мережі. Якщо підключення до мережі часто вимикаються або мають низьку надійність, це може негативно позначитися на роботі мережі;

– перевантажені сервери. Якщо сервери в мережі перевантажені великою кількістю запитів і не можуть швидко їх обробити, це може призвести до уповільнення і можливої втрати даних.

Приховані вузькі місця в комп'ютерній мережі - це місця або елементи, які негативно впливають на її якість роботи, але важко виявляються або ідентифікуються за допомогою звичайних методів тестування та моніторингу. Ці вузькі місця можуть виникати через неправильну конфігурацію або налаштування мережевих пристроїв, нестачу пропускної здатності, низьку продуктивність обладнання, збоїв та помилок у роботі програмного забезпечення, проблеми з безпекою або фізичні перешкоди в передачі сигналу.

Наявність прихованих вузьких місць може призвести до зниження швидкості передачі даних, затримок в мережі, деградації якості голосового та відеозв'язку, збільшення кількості пакетів з помилками та втрат даних, зниження надійності та доступності мережевих сервісів.

Для виявлення та усунення прихованих вузьких місць у комп'ютерній мережі може знадобитися проведення спеціалізованого аналізу мережного трафіку, тестування та моніторинг продуктивності з використанням спеціальних інструментів, а також аудит мережної інфраструктури та налаштування мережевих пристроїв.

До завдань діагностування локальних мереж не входить розгляд роботи прикладного мережевого ПЗ. Однаке помилки налаштування прикладного ПЗ або неефективні самі алгоритми роботи можуть бути причиною занадто великого часу реакції сервера на запит користувача. Тому в завдання діагностування комп'ютерних локальних мереж повинна бути включено завдання задача визначення середовища несправності - локальна мережа або мережеве прикладне ПЗ.

Мережні несправності можна класифікувати відповідно до рівня моделі OSI, яка є стандартом для опису мережевих протоколів і сервісів. Модель OSI складається з семи рівнів, кожен з яких відповідає за певну функціональність мережі. Класифікація мережних несправностей відповідно до рівня моделі OSI допомагає ідентифікувати причину проблеми та визначати шляхи вирішення. Кожен

рівень має свої типові проблеми, що дозволяє спростити процес діагностики та відновлення мережі.

Фізичний рівень. На цьому рівні відбувається передача найнижчого рівня сигналів через фізичну мережу. Мережні несправності на цьому рівні можуть включати:

- пошкодження кабелю;
- переривання підключення;
- переривання з'єднання;
- проблеми з живленням;
- втрати сигналу;
- погана якість сигналу.

Канальний рівень. На цьому рівні відбувається передача бітів між пристроями. Мережні несправності на цьому рівні можуть включати:

- збої в декодуванні бітів;
- помилки передачі даних;
- колізії;
- повторна передача;
- відсутність аутентифікації;
- перевантаження каналу.

Мережевий рівень. На цьому рівні відбувається маршрутизація пакетів через мережу. Мережні несправності на цьому рівні можуть включати:

- некоректну маршрутизацію;
- втрату пакетів або неправильне перекладання IP-адрес;
- невідома IP-адреса;
- невідомий маршрут;
- недоступність мережевих вузлів;
- ндосяжність мережевих служб.

Транспортний рівень. На цьому рівні забезпечується надійна передача даних між кінцевими пристроями. Мережні несправності на цьому рівні можуть включати:

- втрату пакетів;
- погану якість з'єднання або відсутність підтвердження доставки;

- помилки при передачі даних;
- адресаційні помилки;
- перевантаження транспортного протоколу.

Сеансовий рівень. На цьому рівні відбувається керування з'єднаннями і сеансами між пристроями. Мережні несправності на цьому рівні можуть включати:

- втрату з'єднання;
- невідповідність між сеансами;
- помилки в установленні з'єднання;
- повторне встановлення з'єднання.

Рівень представлення. На цьому рівні відбувається перетворення та кодування даних для передачі через мережу. Мережні несправності на цьому рівні можуть включати:

- неправильне кодування даних;
- некоректну інтерпретацію даних;
- помилки при упаковуванні або розпаковуванні даних;
- невідповідність формату даних.

Додатковий рівень. На цьому рівні відбувається передача додаткової функціональності і сервісів, таких як шифрування, аутентифікація та управління мережею. Мережні несправності на цьому рівні можуть включати:

- невідповідність протоколів вищих рівні;
- неправильну реалізацію додаткових протоколів;
- проблеми зі стійкістю мережі;
- некоректний доступ до ресурсів;
- помилки у додатках.

Основні несправності відповідно до рівня моделі OSI зведені в табл. 1.1.

Таблиця 1.1 – Класифікація мережевих несправностей відповідно до рівня моделі OSI

Фізичний рівень	Несправності та помилки в кабельній (з'єднувачі, розщеплені пари, обриви, замикання некоректна довжина лінії), повторювачів, концентраторів або портів, наведення, насичення смуги пропускання, відмови

Канальний рівень	Помилки CRC, колізії та фрагментація кадрів (у Ethernet), помилки лінії, помилки пакета, очищення кільця та аварійна сигналізація (у Token Ring), проблеми у мостах та комутаторах (затримки, відкидання пакетів, спотворення даних), широкомовні шторми
Мережевий рівень	Помилки CRC датаграми чи поля корисного навантаження, проблеми адресації підмереж, проблеми маршрутизації (затримки, відкидання пакетів, спотворення даних), широкомовні шторми
Транспортний рівень	Повторні транспортні пересилки, надмірна фрагментація або відкидання пакетів (поверх IP), розмір сегмента, що пересилається, розмір приймального вікна та його перевищення (в TCP)
Сеансовий рівень	Узгодження MTU блоку або буфера, пошук ресурсів за логічними іменами, реєстрація ресурсів за іменами, повторне встановлення з'єднань.
Рівень представлення	Несумісність версій протоколів, заміна кодових таблиць ASCII на EBCDIC, некоректні відомості у базі даних MIB протоколу SNMP
Додатковий рівень	Зациклювання запитів, перекриття запитів на читання або запис файлів, тривалий пошук ресурсів! уповільнена обробка даних клієнтом або сервер недостатнє заповнення пакетів даними, низька пропускна здатність між кінцевими вузлами мережі.

2.3 Методи усунення несправностей в комп’ютерної мережі

У цьому розділі ми представляємо огляд деяких методів усунення неполадок і класифікувати ці методи відповідно до їх основних алгоритмів, включаючи активні методи, пасивні методи та гібридні методи.

Активні методи використовують зондуючі пакети в мережевих системах для аналізу та моніторингу системи. Пасивні методи просто відстежують мережевий трафік, щоб виявити і знайдіть проблеми. Такий підхід не підвищує накладні витрати системи. Гібридні методи використовують як активні зонди, так і аналіз мережевого трафіку для виявлення та пошуку проблем.

На рисунку 1.1 надані методи усунення неполадок в КМ.

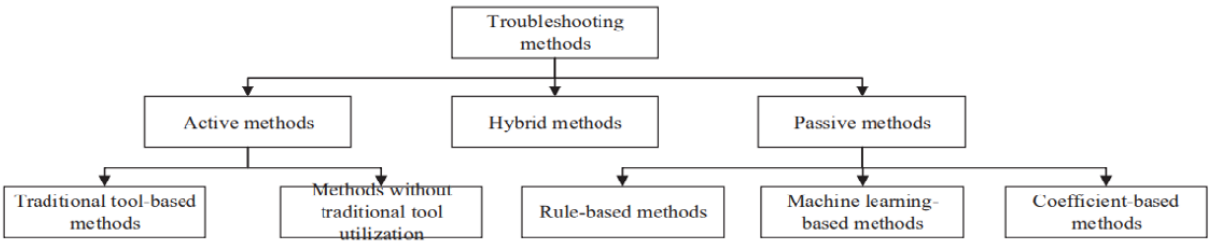

Рис. 1.1 - Методи усунення неполадок в КМ

Активні методи поділяються на:

− ***традиційні методи***, засновані на інструментах. Коли мережеві системи демонструють ненормальну поведінку, IT-фахівці адміністратори використовують деякі інструменти усунення несправностей, такі як ping, трасування, tcpdump або nmap для визначення проблеми з мережею. Використання цих інструментів просто і вимагає мінімального часу обробки. Однак ці інструменти не можуть визначити місце виникнення проблем із мережею. Для деяких випадках ping може надати час туди і назад і втрата пакетів, перевірка доступності хоста до іншого хости або мети, але він не може виявити основні причини, коли закінчився час виконання запитів;

− ***методи без використання традиційних інструментів***. Цей метод використовує зондуючі пакети через мережні системи для отримання інформації та оцінки заходів щодо виявлення проблем із мережею. У [6] автори відтворюють тестові пакети, щоб визначити місцезнаходження мережевих збоїв, таких як втрата пакетів, переупорядкування пакетів та навантаження. Необхідно налаштувати маршрутизатор та протестувати алгоритми вибору пакетів. Цей метод дозволяє виявити та проводити пошук проблеми з мережею, такі як: неправильно налаштований брандмауер правило, навантаження мережі, порушення пріоритетів тощо.

Тим не менш, методи зондування повинні надіслати тестові пакети для аналізу та оцінки. Це неефективно, коли тестові пакети губляться з якихось причин. Крім того, це також збільшує пропускну здатність каналу під час передачі тестових пакетів у мережевих системах.

Пасивні методи поділяються на:

– ***методи, що ґрунтуються на правилах***. Даний метод використовує конфігурацію маршрутизатора та інтелектуальний аналіз асоціативних правил, який вивчає взаємозв'язок вхідних даних та визначає правила, використовуючи деякі заходи аналізу, щоб усунути неправильну конфігурацію роутера. Понад те, необхідно реалізувати інтелектуальний аналіз правил асоціації виявлення несправності. Методи, що ґрунтуються на правилах, не потрібні тестові пакети, але при цьому є суттєві недоліки в компромісі між часом використання та точності. Коли набір правил великий, точність буде високою, але це потребує більше часу обробки. Тому його нелегко реалізувати у реальному часі;

– ***методи, що базуються на машинному навчанні***. Машинне навчання також використовує статистичні методи навчання даних для прийняття рішення. Вони реалізують дерево рішень (машинний алгоритм навчання) для усунення неправильної конфігурації у локальній мережі;

– ***коефіцієнтні методи***. Крім перерахованих вище методів, існують інші підходи, включаючи коефіцієнт узгодженості або коефіцієнт кореляції для виявлення та усунення збоїв у каналі. Більше того, часто застосовують коефіцієнт кореляції для вирішення проблеми втрати пакетів та завантаження ЦП маршрутизатора у разі втрати зв'язку в каналі.

Гібридний метод використовує активні зонди, трасуючи рівня пакетів в мережі, і реалізує кореляційний аналіз для усунення несправностей при перевантаженості мережі. Активні зонди реалізуються за допомогою передачі на сервер для протоколювання пропускної спроможності прикладного рівня. При цьому необхідно використовувати системні виклики в додатках і забезпечити зіставлення правил виявлення проблем у додатках. Крім того, цей метод також підтримує трасування, що генеруються в Linux.

Гібридні методи можуть поєднувати переваги як активних методів, так і пасивних для поліпшення якості мережі, збільшення продуктивності, виявлення нових типів мереж.

На практиці найчастіше використовую наступні методи диагностики комп’ютерних мереж:

– метод діагностики “знизу вгору” згідно моделі OSI;

- метод аналізу журналів логів на хостах и серверах мережі;
- метод аналізу метрік систем моніторінга мереж Zabbix, Nagio;
- інстументальні методи диагностики.

Метод діагностики несправностей у комп'ютерних мережах “знизу нагору” заснований на моделі OSI (Open Systems Interconnection).

При діагностиці "знизу вгору" діагностика починається з фізичного рівня і поступово необхідно рухатися до вищих рівнів. Цей метод допомагає виявити та усунути несправності в мережі

Розглянемо цей метод. На кожному з рівнів моделі виконуються такі дії:

а) на фізичному рівні (Layer 1):

− перевірка фізичного підключення. Переконайтеся, що кабелі правильно підключені та не пошкоджені;

− використовуйте кабельні тестери для перевірки цілісності мережних кабелів.

б) на канальному рівні (Layer 2):

− перевірка налаштування комутаторів та маршрутизаторів. Переконайтеся, що порти знаходяться у правильному стані (увімкнені, активні);

− перевірка таблиці MAC-адрес;

в) на мережевому рівні (Layer 3):

− перевірка налаштування IP-адрес. Переконайтеся, що пристрої мережі мають правильні IP-адреси та маски підмережі;

− використовуйте інструменти, такі як ping та traceroute, щоб перевірити зв'язність та маршрутизацію;

г) на транспортному рівні (Layer 4):

− перевірка налаштування портів та протоколів (наприклад, TCP або UDP);

− використовуйте інструменти, такі як telnet або netstat, щоб перевірити відкриті порти та з'єднання;

д) на сеансовому, презентаційному та прикладному рівні (Layers 5-7):

− перевірка налаштування програм та служб. Переконайтеся, що вони працюють правильно.

Метод аналізу журналів логів на хостах та серверах мережі є важливим методом для виявлення та усунення несправностей мережі. Аналіз логів допоможе виявити приховані проблеми, пов'язані з мережею, програмами або конфігурацією пристроїв.

Розглянемо цей спосіб. На кожному з чотирьох кроків (1 - 4) виконуються такі дії:

1. Збір логів:

− почніть зі збору логів з хостів (клієнтських комп'ютерів) та серверів. Це може бути системні логи, логи додатків, логи безпеки та інші;

− логи містять інформацію про події, помилки, попередження та дії, що відбуваються на пристроях;

2. Аналіз логів:

− використовуйте інструменти для аналізу логів, таких як grep, awk, sed або спеціалізовані програми;

− шукайте ключові слова, пов'язані із проблемою. Наприклад, помилки, збої, недоступність;

3. Звертайте увагу на:

− тимчасові позначки. Подивіться, коли відбулися події. Це допоможе виявити часові залежності;

Типи подій - помилки, попередження, інформаційні повідомлення можуть дати вам уявлення про проблеми.

− зв'язок із мережею. перевірте, чи є події, пов'язані з мережею (наприклад, втрата зв'язку, DNS-проблеми);

4. Реагуйте на проблеми:

− якщо ви виявите помилки або несправності, приступайте до їх усунення;

− при аналізі логів звертайте увагу до симптоми, щоб визначити суть проблеми.

Метод аналізу метрік систем моніторингу мереж Zabbix, Nagios передбачає проведення моніторингу мережі. Моніторинг комп'ютерної мережі — це процес

постійного відстеження мережі на наявність повільних або несправних компонентів. Він включає перевірку стану метрик, у тому числі метрик якості надання сервісу.

Zabbix та Nagios – це популярні системи моніторингу, які дозволяють відстежувати різні параметри мережі, такі як доступність хостів, завантаження серверів, використання ресурсів та інші метрики.

Zabbix та Nagios збирають дані про стан пристроїв та сервісів у мережі. Ці метрики можуть включати в себе інформацію про продуктивність, доступність, навантаження та інші аспекти. Аналіз цих метрик дозволяє виявити потенційні проблеми, такі як високе завантаження серверів, мережні затримки, відмови в обслуговуванні та інші несправності мережі.

Інструментальні методи діагностики та пошуку несправностей у комп'ютерних припускають використання програмно-апаратних засобів таких як:

− ***аналізатори трафіку*** (або сніфери) - це програми або пристрої, призначені для перехоплення та аналізу мережного трафіку як свого, так і чужого;

− ***сніфери*** - можуть аналізувати тільки те, що проходить через їх мережеву картку. Вони дозволяють виявляти паразитний, вірусний і кільцевий трафік, а також перехоплювати незашифровані дані користувача, такі як паролі;

− ***сканери портів*** – ці інструменти сканують мережні порти на пристроях для виявлення відкритих або вразливих портів. Це допомагає у виявленні потенційних вразливостей та захисту мережі;

− ***аналізатори продуктивності*** – вони дозволяють вимірювати пропускну здатність мережі, затримку та інші параметри продуктивності. Це корисно для оптимізації мережі та виявлення вузьких місць;

− ***кабельні тестери*** – використовуються для перевірки фізичної цілісності мережевих кабелів. Вони допомагають виявити несправності у кабелях;

− ***мультиметри*** - хоча вони не є специфічними інструментами для мереж, мультиметри використовуються для вимірювання напруги, опору та інших параметрів мережного обладнання.

Необхідно підкреслити, що всі ці методи допомагають виявляти та усувати проблеми у комп'ютерних мережах, забезпечуючи надійніше функціонування мережевої інфраструктури загалом.

1.4 Вимоги до сучасних систем діагностики комп’ютерних мереж

До сучасних систем діагностики комп’ютерних мереж пред’являються такі вимогі.

Забезпечення швидкодії. Система повинна оперативно знаходити та усувати несправності, мінімізуючи час простою мережі.

Швидкодія системи є однією з головних вимог до систем діагностики комп'ютерних мереж. Це означає, що система має бути здатна швидко та ефективно виконувати свої завдання, включаючи виявлення та аналіз проблем у мережі.

Швидкодія також важлива для обробки великих обсягів даних, що супроводжують мережеві операції. Деякі системи діагностики можуть працювати з великою кількістю пристроїв та мережевих з'єднань, і їм потрібна висока швидкість обробки даних, щоб забезпечити ефективність роботи.

Крім того, швидкодія системи діагностики комп'ютерних мереж також важлива для швидкого доступу до результатів діагностики. Оператори мережі вимагають швидкого зворотного зв'язку та миттєвого доступу до інформації про стан мережі та виявлені проблеми. Це допомагає вжити оперативних заходів для виправлення проблем та запобігання можливим збоям.

Загалом швидкодія системи діагностики комп'ютерних мереж є важливою вимогою, яка забезпечує ефективність роботи мережі, мінімізує час простою та максимізує продуктивність мережі.

Забезпечення надійності. Система повинна бути надійною і не призводити до нештатних ситуацій або додаткових несправностей у процесі пошуку та усунення проблем. Це означає, що система має працювати стабільно та без збоїв як у процесі діагностики, так і у звичайному режимі роботи.

Для отримання надійності потрібно забезпечити:

– ***стійкість до збоїв***. Система має бути захищена від можливих технічних збоїв, таких як збої живлення або апаратні збої. Для цього часто використовуються резервні та резервовані компоненти, а також механізми автоматичного відновлення;

- ***відмовостійкість.*** У разі збоїв або неполадок в одній частині системи вона повинна бути здатна продовжувати роботу без втрати головного функціоналу. Це досягається шляхом використання механізмів резервування, стійких до відмови алгоритмів і дуплікації компонентів;
- ***моніторинг та автоматичне усунення помилок***. Система повинна безперервно моніторити стан комп'ютерної мережі та автоматично реагувати на помилки, що виникають. Це може включати механізми автоматичного відновлення, автоматичне перемикання на резервні канали зв'язку, а також оповіщення системного адміністратора про проблеми, що виникли;
- ***швидкість роботи та продуктивність***. Система повинна забезпечувати швидке та ефективне виконання діагностики комп'ютерної мережі. Це потребує оптимізації алгоритмів та використання високопродуктивного обладнання.
- ***гнучкість і масштабованість***. Система повинна бути гнучкою та масштабованою, щоб підтримувати різні типи комп'ютерних мереж та масштабуватись у разі збільшення їх розміру.
- ***захист від зовнішніх загроз***. Система діагностики комп'ютерних мереж має бути захищена від шкідливих програм, хакерських атак, фішингу та інших зовнішніх загроз. Для цього використовуються засоби захисту, такі як фаєрволи, антивірусні програми та системи аутентифікації.
- ***відповідність стандартам та регуляторним вимогам***. Система повинна відповідати застосовним стандартам та регуляторним вимогам у сфері інформаційної безпеки та якості обслуговування.

Забезпечення необхідної автоматизації. Система повинна мати можливість автоматичного виявлення та локалізації несправностей, спрощуючи та прискорюючи процес їх усунення.

Система автоматизації повинна забезпечити:

- автоматичне виявлення та ідентифікація пристроїв у мережі;
- своечасні овідомлення про збої та проблеми в мережі;
- моніторинг завантаження мережі;
- моніторинг доступності та відгуку мережних пристроїв;
- моніторинг безпеки мережі;

- глибокий аналіз трафіку;
- централізоване управління;
- гнучкість налаштування та адаптації під потреби конкретної мережі;
- − звітність та аналітику.

Забезпечення масштабованості. Система має бути гнучкою і здатною працювати з різними типами мереж, включаючи дротові та бездротові, а також мережі різного масштабу, від малих офісних мереж до великих корпоративних мереж.

Забезпечення необхідної централізації управління. Система повинна забезпечувати централізоване керування та контроль за несправностями у комп'ютерних мережах, дозволяючи операторам оперативно реагувати на проблеми.

Забезпечення сумісності. Система повинна бути сумісною з різними виробниками мережного обладнання та операційними системами, щоб бути універсальною та застосовною у різних мережевих середовищах.

Забезпечення необхідного ступеня безпеки. Система повинна бути захищеною від несанкціонованого доступу, щоб забезпечити безпеку мережі в процесі пошуку та усунення несправностей.

1 Розвиток методів пошуку і усунення несправностей в комп'ютерних мережах

2.1 Загальна модель вирішення проблеми пошуку несправностей

У процесі пошуку несправностей у мережному середовищі має застосовуватись системний підхід. Якщо пошук несправностей ведеться безсистемно, то можуть непродуктивно витрачатися цінні тимчасові та матеріальні ресурси, а іноді при цьому становище навіть погіршується. У процесі усунення порушень у роботі мережі необхідно визначити конкретні ознаки несправності, виявити всі потенційні проблеми, якими можуть бути викликані ці ознаки, а потім систематично усувати всі можливі причини проблем (від найбільш ймовірних до найменш ймовірних) до тих пір, поки всі ознаки несправності не зникнуть.

На рис. 2.1 показано структурну схему загальної моделі вирішення проблеми пошуку несправностей. Ця схема не є жорсткою схемою пошуку несправностей в об'єднаній мережі, а може бути лише основою, на якій формується конкретний процес усунення порушень у роботі, що відповідає конкретному мережному середовищу.

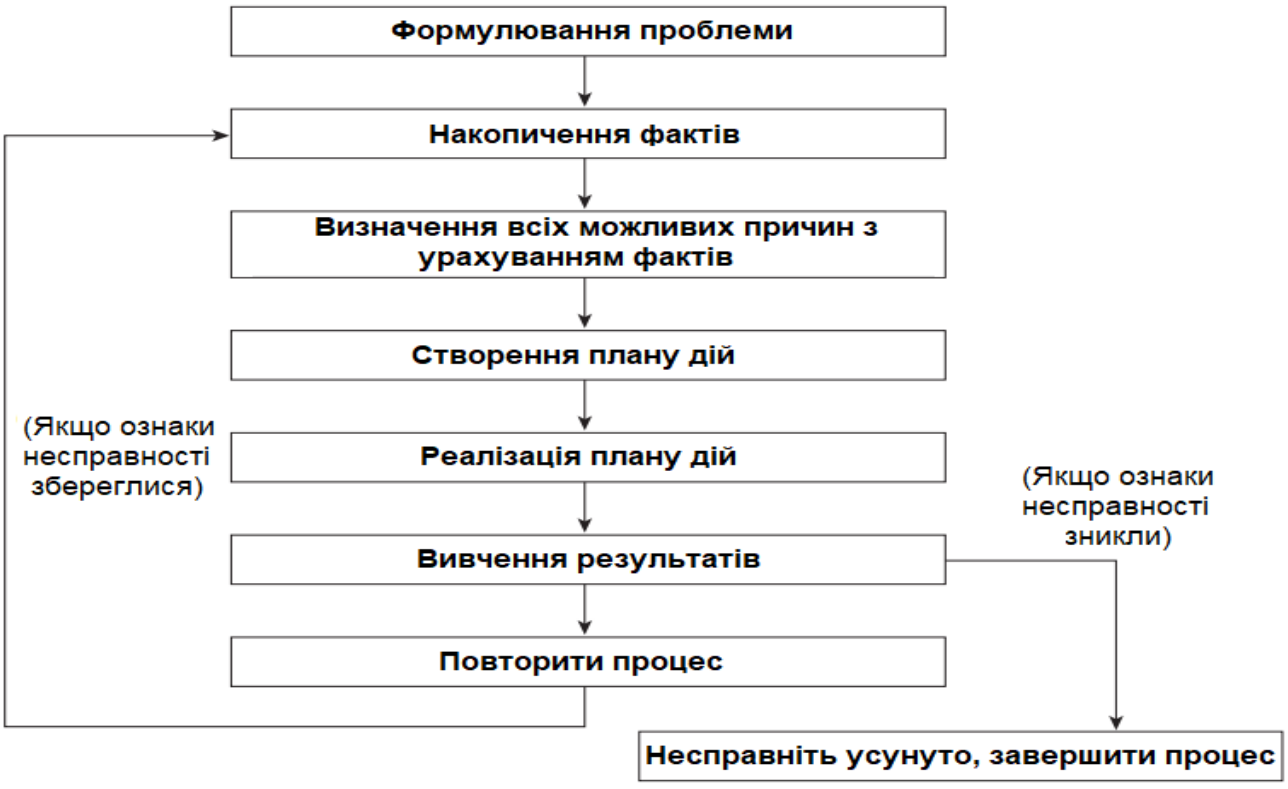

Рис. 2.1. Общая модель решения проблемы поиска неисправностей

Нижче описано конкретні етапи процесу пошуку несправностей, загальна блок-схема якого наведена на рис. 2.1.

Крок 1. Під час аналізу порушення роботи у мережі чітко сформулюйте проблему. Проблема має бути визначена як набір ознак несправностей і можливих причин.

У процесі аналізу проблеми необхідно визначити загальні ознаки несправності, а потім встановити, якими причинами могли бути викликані ці ознаки. Наприклад, припустимо, що хост не відповідає на запити до служб, що надходять від клієнтів (ознака несправності). Можливими причинами цього може бути неправильне настроювання конфігурації хоста, несправні інтерфейсні плати або відсутність необхідних команд у конфігурації маршрутизатора.

Крок 2. Зберіть факти, які дозволять точніше встановити можливі причини.

Необхідно провести опитування всіх зацікавлених користувачів, мережевих адміністраторів, керівників та інших фахівців, а також зібрати інформацію з таких джерел, як системи управління мережею, трасування аналізаторів протоколу, ознайомитися з результатами виконання команд діагностики маршрутизатора або прочитати документацію до застосованої версії програмного забезпечення. забезпечення.

Крок 3. Вивчіть можливі проблеми з урахуванням зібраних фактів. Накопичена вами інформація дозволить виключити деякі потенційні проблеми зі списку підозрюваних. Наприклад, отримані дані можуть свідчити, що апаратне забезпечення працює нормально. Це дозволить зосередитись на порушеннях у роботі програмного забезпечення. За будь-якої можливості потрібно прагнути звузити коло потенційних проблем, щоб можна було розробити ефективний план дій.

Крок 4. Підготуйте план дій, що охоплює всі потенційні проблеми, що залишилися. Почніть із найбільш ймовірної несправності та розробіть план, який передбачає усунення лише однієї конкретної причини.

Якщо план дій спрямований на усунення лише однієї причини, він дозволить знайти потрібне вирішення конкретної проблеми. Намагаючись одночасно усунути відразу кілька причин, також можна вирішити проблему, але при цьому складно

визначити, яка саме дія призвела до усунення ознак несправності, тому при повторному виникненні такої ж проблеми в майбутньому пошук розв'язання доведеться розпочати з самого початку.

Крок 5. Здійсніть план дій, ретельно виконуючи кожен етап і перевіряючи, чи вдалося усунути ознаки несправності.

Крок 6. Після внесення кожної зміни обов'язково проконтролюйте результати. Як правило, для цього повинен застосовуватися той же метод збору даних, як і на кроці 2 (зокрема, при цьому знову залучайте до такої роботи заінтересованих фахівців та використовуйте діагностичні інструментальні засоби).

Крок 7. Проаналізуйте отримані результати, щоб визначити, чи вирішена проблема. У разі позитивної відповіді процес пошуку несправності закінчується.

Крок 8. Якщо проблему не вирішено, розробіть план дій щодо усунення наступної менш ймовірної проблеми зі списку. Поверніться до кроку 4, знову вносите по одній зміні і повторюйте процес, доки проблема не буде вирішена.

2.2 Використання штучного інтелекту для вдосконалення методів пошуку та усунення несправностей у комп'ютерних мережах

2.2.1 Методика побудови штучної нейромережевої моделі диагностикі комп'ютерних мереж

Основні етапи методики побудови штучної нейромережевої моделі діагностики та усунення несправностей у комп'ютерних мережах включають:

- аналіз даних на початковому етапі постановки задачі та вибору моделі (архітектури) ШНМ;
- аналіз та перетворення даних для побудови більш ефективної процедури налаштування ШНМ;
- вибір алгоритму навчання ШНМ;
- тестування та донавчання ШНМ;
- аналіз точності нейромережевого рішення для діагностики;

− ухвалення рішення про технічний стан мережі на основі отриманих результатів.

Розглянемо зміст кожного з етапів методики побудови штучної нейромережевої моделі діагностики та усунення несправностей у комп'ютерних мережах.

***На етапі діагностики та усунення несправностей у комп'ютерних мережах з використанням нейронних мереж (ІНП) аналіз даних включає такі пункти*:**

1. Збір даних: збираються дані про параметри роботи комп'ютерної мережі, такі як пропускна здатність, затримка, втрата пакетів та інші метрики. Ці дані можна отримати за допомогою мережевих пристроїв, моніторингових інструментів або інших методів.

2. Підготовка даних. Зібрані дані проходять попередню обробку, яка може включати фільтрацію шумів, нормалізацію та масштабування значень, поділ на навчальну та перевірочну вибірки та інші операції для забезпечення якісного навчання ІНС.

3. Аналіз даних. На даному етапі проводиться статистичний аналіз даних, виявляються особливості та закономірності в роботі мережі, ідентифікуються типи та природа виникнення несправностей. Також аналізуються залежності між різними параметрами та визначаються причини виникнення несправностей.

4. Постановка задачі та вибір моделі ІНС. На основі проведеного аналізу даних формулюються задачі, які ІНС повинна вирішувати, наприклад, класифікація типів несправностей або прогнозування їх виникнення. Потім вибирається відповідна модель ІНС, яка може бути, наприклад, багатошаровим персептроном, нейронною згортковою мережею або рекурентною нейронною мережею.

Аналіз та перетворення даних для побудови ефективної процедури налаштування ШНМ полягає в наступних кроках:

1. Збір даних. Зберіть усі доступні та необхідні дані, пов'язані з проблемою, яку ви хочете вирішити за допомогою нейронної мережі. Це можуть бути дані про вхідні змінні, вихідні змінні, історичні дані та інші супутні дані.

2. Очищення даних. Перевірте дані на наявність пропущених значень, викидів та помилок. Проведіть процедури очищення даних, щоб усунути ці недосконалості. Це може включати видалення або заміну відсутніх значень, фільтрацію викидів та виправлення помилок.

3. Нормалізація даних. Перетворіть дані, щоб вони були у відповідному форматі для використання в ІНС. Нормалізація може включати масштабування або стандартизацію даних, щоб рівні значень були придатними для використання нейронною мережею.

4. Створення навчальної вибірки та тестової вибірки. Розділіть дані на навчальну вибірку та тестову вибірку. Навчальна вибірка буде використовуватися для навчання ІНС, а тестова вибірка використовуватиметься для перевірки продуктивності нейронної мережі нових даних.

5. Проектування структури ШНМ. Визначте структуру та параметри вашої нейронної мережі, такі як кількість прихованих шарів, кількість нейронів у кожному шарі, функції активації тощо. буд. Це може бути зроблено шляхом застосування експериментації та оптимізації процесу навчання.

6. Навчання ШНМ. Використовуйте навчальну вибірку для навчання ІНС. Це може бути виконано шляхом визначення цільової функції та застосування алгоритмів оптимізації, таких як градієнтний спуск або зворотне розповсюдження помилки. Навчання може зайняти деякий час, залежно від складності проблеми та обсягу даних.

7. Оцінка продуктивності. Після навчання ШНМ перевірте його продуктивність на тестовій вибірці. Використовуйте вибрані метрики, щоб оцінити ефективність ІНС та визначити, чи відповідає вона вашим вимогам.

8. Тонка настройка та оптимізація. У разі недостатньої продуктивності ІНС може знадобитися тонка настройка та оптимізація. Це може включати зміну структури мережі, зміну параметрів навчання або застосування інших методів оптимізації.

9. Перевірка на нових даних. Після налаштування ШНМ перевірте її продуктивність на нових даних, які раніше не використовувалися під час навчання

або тестування. Це допоможе оцінити, наскільки добре ШНМ узагальнює свої знання на нові ситуації.

10. Ітеративний процес. Процес налаштування ІШНМ може бути ітеративним, що вимагає повторного застосування кроків 6-9 для досягнення найкращих результатів.

Вибір алгоритму навчання штучної нейронної мережі *(ШНМ)* залежить від ряду факторів, включаючи тип завдання, доступні дані, доступні обчислювальні ресурси та обмеження, а також переваги та досвід дослідника. Ось деякі з найпоширеніших алгоритмів навчання ШНМ:

1. Зворотне поширення помилки (Backpropagation). Це один із найпоширеніших алгоритмів навчання ШНМ. Він заснований на градієнтному спуску і дозволяє навчати ШНМ із кількома шарами. Поворотне поширення помилки вимагає великих обсягів даних навчання і може бути чутливим до початкових умов.

2. Генетичні алгоритми. Ці алгоритми ґрунтуються на принципах природного відбору та генетики. Вони досліджують простір можливих рішень, використовуючи операції схрещування та мутації, щоб створити нові покоління мереж та вибрати найкращі рішення. Генетичні алгоритми можуть бути ефективними у пошуку оптимальних архітектур ІНС.

3. Метод опорних векторів (Support Vector Machines, SVM). Цей метод використовується завдання класифікації. SVM будує роздільну гіперплощину у просторі ознак для поділу різних класів даних. SVM можуть працювати добре з невеликими обсягами даних та можуть забезпечити хорошу узагальнюючу здатність.

4. Згорткові нейронні мережі (Convolutional Neural Networks, CNN). Ці мережі особливо добре підходять для обробки зображень та відео. Вони використовують згорткові шари виявлення локальних ознак і пулінг шари зменшення розмірності даних. CNN дозволяють автоматично отримувати ієрархічні характеристики, що робить їх ефективними для обробки складних даних з просторовою структурою.

Тестування та доучування штучних нейронних мереж - це процеси, пов'язані з оцінкою та покращенням роботи мереж.

Тестування штучної нейронної мережі включає перевірку її точності та ефективності на тестових даних або реальних завданнях. Під час тестування аналізуються результати роботи мережі, порівнюються з очікуваними та робляться висновки про її якість та здатність вирішувати завдання.

Доучування штучної нейронної мережі це процес оптимізації роботи мережі шляхом зміни її параметрів або архітектури після початкового навчання. Під час доучування мережі використовуються реальні дані, щоб покращити її результати або адаптувати її до нових умов.

Обидва процеси мають важливе значення для створення ефективних та надійних штучних нейронних мереж. Вони допомагають підвищити якість роботи мереж, покращити їх точність та пристосувати до нових умов чи завдань.

Для оценки точности модели нейросетевого решения необходимо разделить набор данных на обучающую, тестовую и проверочную выборки. Обучающая выборка используется для тренировки модели, тестовая выборка для оценки ее точности, а проверочная выборка - для проверки и настройки параметров модели.

Для оцінки точності моделі нейромережевого рішення необхідно розділити набір даних на навчальну, тестову та перевірочну вибірки. Навчальна вибірка використовується для тренування моделі, тестова вибірка для оцінки її точності, а перевірна вибірка - для перевірки та налаштування параметрів моделі.

На підставі отриманих результатів з використанням штучної нейронної мережі можна сформулювати такі ***рішення щодо технічного стану комп'ютерної мережі:***

1. Виявлення аномалій та помило. Штучна нейронна мережа може виявити незвичайні та неправильні патерни в роботі мережі, такі як незвичайний трафік, помилки передачі даних або незвичайні події. Результати нейронної мережі можуть бути використані для прийняття рішень про внесення змін до мережі, щоб запобігти можливим збоям та проблемам.

2. Прогнозування відмов та несправностей. Використовуючи історичні дані та навчену штучну нейронну мережу, можна прогнозувати можливі відмови та

несправності в мережі. Це дозволяє вжити проактивних заходів для запобігання проблемам, провести запобіжні роботи або замінити дефектне обладнання.

3. Оптимізація продуктивності. Штучна нейронна мережа може визначити оптимальні налаштування та конфігурації мережі для досягнення максимальної продуктивності. Наприклад, на основі отриманих результатів можна ухвалити рішення про ребаланс навантаження між пристроями або використання певних протоколів для підвищення швидкості передачі даних.

4. Поліпшення безпеки. Штучна нейронна мережа може розпізнавати атаки та спроби несанкціонованого доступу до мережі. Результати нейронної мережі можуть бути використані для реалізації заходів безпеки, таких як блокування IP-адрес, оновлення антивірусних програм або посилення автентифікації.

5. Автоматична діагностика та усунення проблем. На підставі передбачуваних даних та результатів штучної нейронної мережі можна автоматично визначити та усунути проблеми в комп'ютерній мережі. Це може бути особливо корисно у випадках, коли ручне виявлення та вирішення проблем потребує великих ресурсів та часу.

Підбивши підсумок, штучна нейронна мережа дозволяє ефективно аналізувати та обробляти дані про стан комп'ютерної мережі, що сприяє прийняттю важливих рішень для забезпечення стабільної та надійної роботи мережі.

2.2 Вибір моделі штучних нейронних мереж

Залежно від конкретного завдання та доступних даних для діагностики комп'ютерних мереж можуть застосовуватися такі моделі штучних нейронних мереж або їх комбінації.

1. Багатошаровий перцептрон (Multilayer Perceptron, MLP). Це найпоширеніша модель нейронної мережі, що складається з кількох шарів нейронів. Вона може бути використана для виявлення аномалій, моніторингу мережі та класифікації несправностей.

2. Згорткові нейронні мережі (Convolutional Neural Networks, CNN). Ця модель найчастіше використовується для обробки зображень, але також може бути

використана для діагностики комп'ютерних мереж, особливо для аналізу мережевого трафіку.

3. Рекурентні нейронні мережі (Recurrent Neural Networks, RNN). Ця модель ідеально підходить для аналізу послідовних даних, наприклад тимчасових рядів трафіку в комп'ютерних мережах. Вона може використовуватися для прогнозування та виявлення аномалій у мережах.

4. Мережі довготривалої пам'яті (Long Short-Term Memory Networks, LSTM). Це досить особливий тип рекурентних нейронних мереж, який призначений для роботи з послідовними даними і здатний вловлювати довгострокові залежності. Він може бути корисним для діагностики комп'ютерних мереж, особливо при аналізі тривалих рядів.

5. Мережа Хопфілда. Нейронні мережі Хопфілда можуть бути використані для діагностики комп'ютерних мереж, прогнозування станів мережі та виявлення аномалій у роботі мережі

Розглянемо умови застосування кожної з наведеної моделі штучного інтелекту в реальних умовах для діагностики комп'ютерних мереж.

Модель багатошарового перцептрону (MLP) в першу чергу може бути використана для діагностики станів, виявлення аномалій та моніторингу мережі, а також класифікації даних.

Для діагностики станів MLP повинна бути навчена на історичних даних про стани мережі (наприклад, параметри продуктивності, завантаження, затримка і т. д.) та їх проблеми, щоб визначити правильний стан мережі. Потім модель може бути використана для діагностики стану поточного мережі на основі поточних показників.

При виявлення аномалій MLP має бути навчена на нормальних показниках мережі та використовуватися для виявлення аномалій у реальному часі. Якщо поточний показник відрізняється від передбаченого значення MLP, це може вказувати на можливі проблеми або аномалії в мережі.

Моніторинг мережі MLP може стежити за показниками продуктивності мережі та реагувати на будь-які зміни. Наприклад, якщо MLP виявляє падіння

продуктивності або збільшення затримки, це може ігналізувати проблеми в мережі, які вимагають уваги.

MLP може бути використана для класифікації даних, пов'язаних із мережею. Наприклад, модель може бути навчена для розпізнавання різних типів мережного трафіку (наприклад, веб-трафік, потокове відео, ігровий трафік тощо), що може бути корисним для оптимізації продуктивності та забезпечення

Згорткові нейронні мережі (ЗНМ) використовуються для аналізу мережного трафіку та діагностики комп'ютерних мереж. Застосування ЗНМ дозволяє автоматично розпізнавати певні шаблони та ознаки поведінки мережного трафіку, що може допомогти у виявленні аномалій, атак та небажаної поведінки в мережі.

Важливо, що використання ЗНМ для аналізу мережного трафіку вимагає великого обсягу розмічених даних для навчання та налаштування моделі. Це також вимагає високої обчислювальної потужності та спеціалізованих алгоритмів для ефективної обробки та аналізу мережевого трафіку.

Наведемо варіанти використання ЗНМ для аналізу мережевого трафіку:

− ідентифікація типів мережного трафіку. ЗНМ можуть навчатися на різних типах мережного трафіку, таких як веб-трафік, поштовий трафік, потокове відео і т. д. Це дозволяє автоматично класифікувати мережевий трафік за типами та виявляти відхилення у поведінці трафіку;

− виявлення атак та аномалій. ЗНМ можуть бути навчені на мережевому трафіку, що містить нормальну поведінку та відомі атаки. Це дозволяє ідентифікувати аномалії та виявляти невідомі атаки у реальному часі;

− класифікація загроз. Навчання ЗНМ на наборі даних, що містить різні типи відомих загроз, дозволяє класифікувати нові загрози на основі їх ознак і виявляти їх у мережевому трафіку;

− оптимізація мережевих ресурсів. ЗНМ можуть допомогти в оптимізації використання мережевих ресурсів, наприклад, шляхом розпізнавання та класифікації типів трафіку, обсягів споживаних ресурсів та визначення оптимальних налаштувань для мережних пристроїв;

− прогнозування навантаження та запобігання перевантаженням. ЗНМ можна навчити прогнозувати навантаження на мережу на основі історичних даних, що

дозволяє запобігати перевантаженню та вживати заходів щодо масштабування мережевої інфраструктури.

При використанні рекурентних нейронних мереж (RNN) для діагностики комп'ютерних мереж, прогнозування станів мережі та виявлення аномалій необхідно виконати такі етапи.

− підготовка даних. Необхідно зібрати та підготувати дані про стан комп'ютерних мереж. Це повинно включати інформацію про навантаження на мережу, пропускну здатність, рівень пакетної втрати, затримки та інші параметри.

− підготовка навчального набору даних. Необхідно створити навчальний набір даних, який містить історичні дані про стан мережі та відомі аномалії чи прогнози. Зазвичай такий набір складається із послідовності часових рядів;

− проектування рекурентної нейронної мережі. Необхідно визначити архітектуру рекурентної нейронної мережі, яка може обробляти часові ряди та враховувати залежності між попередніми та поточними станами мережі. Наприклад, LSTM (Long Short-Term Memory) мережі часто використовують для обробки послідовностей даних;

− навчання моделі. Необхідно використовувати навчальний набір даних для навчання нейронної рекурентної мережі. У ході навчання модель налаштовуватиметься на відомі патерни та залежності в даних;

− оцінка моделі. Перевіряється ефективність моделі, використовуючи перевірочний набір даних. Оцінюється точність та надійність моделі, виявляються аномалії та прогнозується стан мережі;

− валідація та налаштування моделі. Якщо модель не досягає необхідного рівня точності, буде проведено валідацію та налаштування параметрів моделі. Це може включати зміну архітектури мережі, зміну гіперпараметрів або зміну підходу до навчання;

− використання моделі для діагностики мережі. Після успішної оцінки та налаштування моделі її використовують для діагностики комп'ютерних мереж. Модель виконуватиме прогнозування станів мережі та виявлення аномалій на основі нових даних про стан мережі.

Нейронні мережі довгострокової пам'яті (LSTM, Long Short-Term Memory) можуть бути використані для діагностики комп'ютерних мереж, прогнозування станів мережі та виявлення аномалій. При використанні LSTM необхідно мати добре підготовлений набір даних для навчання LCTM, який містить представницькі приклади нормальної та аномальної поведінки мережі. Також варто відзначити, що LSTM може використовуватися як один з інструментів для діагностики мережі, і його результати можуть бути використані разом з іншими методами та алгоритмами для більш точного аналізу.

Наведемо варіанти використання LSTM для діагностики комп'ютерних мереж.

− діагностика поточного стану комп'ютерної мережі. LSTM може бути навчена на історичних даних про різні параметри мережі (наприклад, трафік, затримку, втрату пакетів) та їх відповідні діагнози (наприклад, служба сповіщення про збій, проблема з маршрутизатором). Потім система може використовувати навчену LSTM для аналізу поточних даних мережі та надання діагностичної інформації про можливі проблеми.

− прогнозування станів мережі. LSTM може бути навчена на історичних даних про стани мережі у певні моменти часу, таких як пропускна здатність, завантаження та кількість підключених пристроїв. Потім LSTM можна використовувати для прогнозування майбутніх станів мережі. Це може допомогти адміністраторам мережі вживати превентивних заходів або планувати ресурси заздалегідь.

− виявлення аномалій у мережі. LSTM може бути навчена на нормальних паттерна поведінки мережі. Потім система може використовувати навчену LSTM для аналізу поточних даних мережі та виявлення аномальних ситуацій, таких як мережеві атаки, незвичайні патерни трафіку або поведінка користувача. Це дозволяє швидко виявляти потенційні небезпеки без необхідності попереднього знання конкретних ознак аномалій.

Нейронні мережі Хопфілда на практиці при діагностиці комп'ютерних мереж можуть використовуватись в такий спосіб.

− діагностика поточного стану комп'ютерної мережі. Створюється нейронна мережа Хопфілда, яка буде навчена з урахуванням нормального функціонування комп'ютерної мережі. Потім подаються на вхід цієї мережі поточні дані про стан

мережі та спостерігаються результати, які надасть система моніторингу мережі. Якщо результати спостереження відрізняються від очікуваних, це може свідчити про можливі проблеми у мережі;

− прогнозування станів мережі. Проводиться навчання нейронної мережі Хопфілда на історичних даних про стани мережі та відповідні результати або події, що відбулися згодом. Потім подавайте на вхід поточні дані про стан мережі та спостерігайте, які результати надасть мережа. Це дозволяє робити прогнози у тому, які події можуть статися у майбутньому з урахуванням поточного стану мережі;

− виявлення аномалій у роботі мережі. Якщо нейронна мережа Хопфілда навчена на нормальному функціонуванні роботи в мережі, то вхідні дані про поточний стан робота можуть бути подані на вхід цієї мережі. Якщо мережа видасть результат, який відрізняється від нормального функціонування (наприклад, якщо вхідні дані не відповідають відомим патернам), це вказує на аномалію чи проблему роботи мережі.

Необхідно відзначити, що нейронна мережа Хопфілда може досить швидко вчитися і забезпечувати хорошу узагальнюючу здатність, але вона не є ідеальною і має свої обмеження. У деяких випадках може знадобитися комбінування з іншими методами машинного навчання та алгоритмами.

В таблиці 2.1 надані варіанти використання ШНМ для діагностики комп'ютерних мереж

Таблиця 2.1 - Варіанти використання ШНМ

Варіант використання /вид **ШНМ**	**MLP**	**CNN**	**RNN**	**LSTM**
Виявлення несправностей та аномалій	+	+	+	+
Класифікації несправностей	+	-	-	-
Моніторинг мережі	+	-	-	-
Аналізу мережевого трафіку	-	+	-	-
Прогнозування несправностей	-	-	+	+

Відповідно до таблиці ми можемо зробити висновок, що ні одна з моделей ШНМ не дозволяє виконати весь спектр діагностики комп'ютерної мережі. Відповідно до таблиці ми можемо зробити висновок, що ні одна з моделей ШНМ не дозволяє виконати весь спектр діагностики комп'ютерної мережі. Тому на практиці для вирішення завдань діагностики використовують комбінацію моделей ШНМ.

2.2 Використання пакету Matlab для створення рекуррентної моделі штучної нейронної мережі для прогнозування стану комп'ютерної мережі в майбутньому

Широке використання комп'ютерних систем та мереж, конкуренція на ринку комп'ютерних засобів зумовлюють зростання вимог до їх надійності. З погляду надійності комп'ютерна мережа є відновлюваний технічний об'єкт. Ефективне функціонування комп'ютерних систем збору, обробки та передачі інформації передбачає безвідмовну роботу кожної складової комп’ютерної мережі. Існує необхідність аналізу та своєчасного попередження виходу з ладу компонентів комп’ютерної мережі. Існуючи підходи щодо прогнозування відмов комп’ютерних систем пов’язані з аналізом статистичних даних та метриками вірогідності. Можливим альтернативним способом контрою працездатності обладнання є використання нейронних мереж. При вирішенні завдань з використанням нейронної мережі підбирають стандартну конфігурацію нейромережі, але з урахуванням складності та особливості завдання добір існуючих конфігурацій може бути проблематичним.

Якщо ж завдання не може бути зведено до жодного з відомих типів нейромережі, доводиться вирішувати складну проблему синтезу нової конфігурації. Для визначення структури моделі нейронної мережі потрібно розв'язати кілька завдань:

− провести аналіз існуючих нейронних мереж; розробити основні критерії відбору нейронних мереж для побудови моделі;

− визначити основні характеристики визначення якості моделі на основі нейронної мережі.

Отже складність вирішення задачі використання нейронної мережі в першу чергу пов’язана з необхідністю побудови адекватної моделі мережі [2].

Проблематика побудови топології нейронної мережі прогнозування пов’язана з необхідністю селекції значимих факторів, що впливають на обладнання в процесі

експлуатації. Іншим обмеженням при застосуванні нейронної мережі є необхідність збору і аналізу даних для формування навчальної вибірки.

Відповідно до запропонованого варіанту загальної класифікації факторів впливу на працездатність обладнання є фактори з позиції умов застосування обладнання, якості використання та умов експлуатації [11,12].

Зміст дослідження. Розглядаються найбільш важливі фактори впливу з позиції умов застосування, якості та умов роботи. Проведений аналіз зв'язків обладнання у якості як окремих елементів, так і системи в цілому. Сформовані вирази, які описують залежності між параметрами для одного об'єкту дослідження та параметрами об'єктів одного типу при різних умовах застосування.

Для формування вектору вхідних параметрів при побудові і використанні нейронної мережі прогнозування відмов здійснювався вибір наступних показників роботи мережного обладнання:

- загальний час напрацювання, даний параметр передбачає збір даних про загальне напрацювання всіх компонентів мережі;

- час напрацювання мережі після заміни або відновлення окремих її елементів, необхідно здійснювати збір напрацювання для кожного окремого елементу;

- кількість циклів включення-вимикання мережного обладнання та циклів зміни станів, реалізація збору та аналізу даної інформації передбачає використання спеціально розробленого програмного забезпечення. Необхідність врахування загальної кількості циклів включення-вимикання об'єкту пов'язана з появою перехідних процесів в електричних колах та напівпровідниках в результаті зміни їх стаціонарних станів в результаті включення або вимикання;

- коефіцієнт циклічності відмов, вираз для отримання коефіцієнту передбачає проведення аналізу спектральної щільності та періодичності виходів з ладу обладнання комп'ютерної мережі;

- кількість компонентів мережі з різними ваговими коефіцієнтами.

Всі необхідні показники роботи мережного обладнання були зібрані з серверу моніторингу Zabbix компанії Materialize. Мережа компанії включає 15 серверів, 275 робочих станцій та декілька комутаторів та маршрутизаторів.

На основі аналізу вектору вхідних параметрів, проведено побудову та навчання нейронної мережі в програмному середовищі Matlab.

З використанням програми Matlab було створено 3 нейронні мережі (табл. 2.2):

- мережа загальної регресії 15,32,18;
- багатошаровий перцептрон 15,15,15;
- багатошаровий перцептрон 15,15,0.

Таблиця 2.2 – Результати досліджування нейронних мереж

№ п/п	Тип мережі	Помилка, обчислена на навчальній множині даних	Помилка, обчислена на тестовій множині даних	Кількість вхідних нейронів	Кількість нейронів у прихованому шарі 1	Кількість нейронів у прихованому шарі 2
1	Мережа загальної регресії	0,15	0,23	15	32	18
2	Багатошаровий перцептрон	0,21	0,24	15	15	15
4	Багатошаровий перцептрон	0,27	0,29	15	15	0

Оцінюючи дані таблиці 2.2 необхідно зазначити, що штучна нейромережа загальної регресії демонструє дуже малу помилку як на навчальної множини, та и помилку на тестовій множині.

3 Практичні рекомендації з пошуку та усунення відмов у комп'ютерних середовищах

3.1 Процес пошуку та усунення несправностей в комп’ютерних мережах

Проблеми з комп’ютерної мережею поділяються на прості або складні та можуть виникати внаслідок поєднання несправностей мережевого обладнання, програмного забезпечення або підключення. IT-спеціаліст повинен розробити послідовний та логічний метод діагностики мережевих несправностей шляхом поетапного їх усунення.

Спочатку для оцінки масштабу несправностей визначається, скільки мережевих пристроїв зазнали проблеми. Якщо в мережі не працює один пристрій діагностика починається з нього. Якщо проблема з декількома пристроями, процес усунення несправностей в мережі починається з серверного приміщення, де ці пристрої об'єднуються.

Процес пошуку та усунення несправностей складається з 6 кроків, які наведені на рисунку 3.1[14].

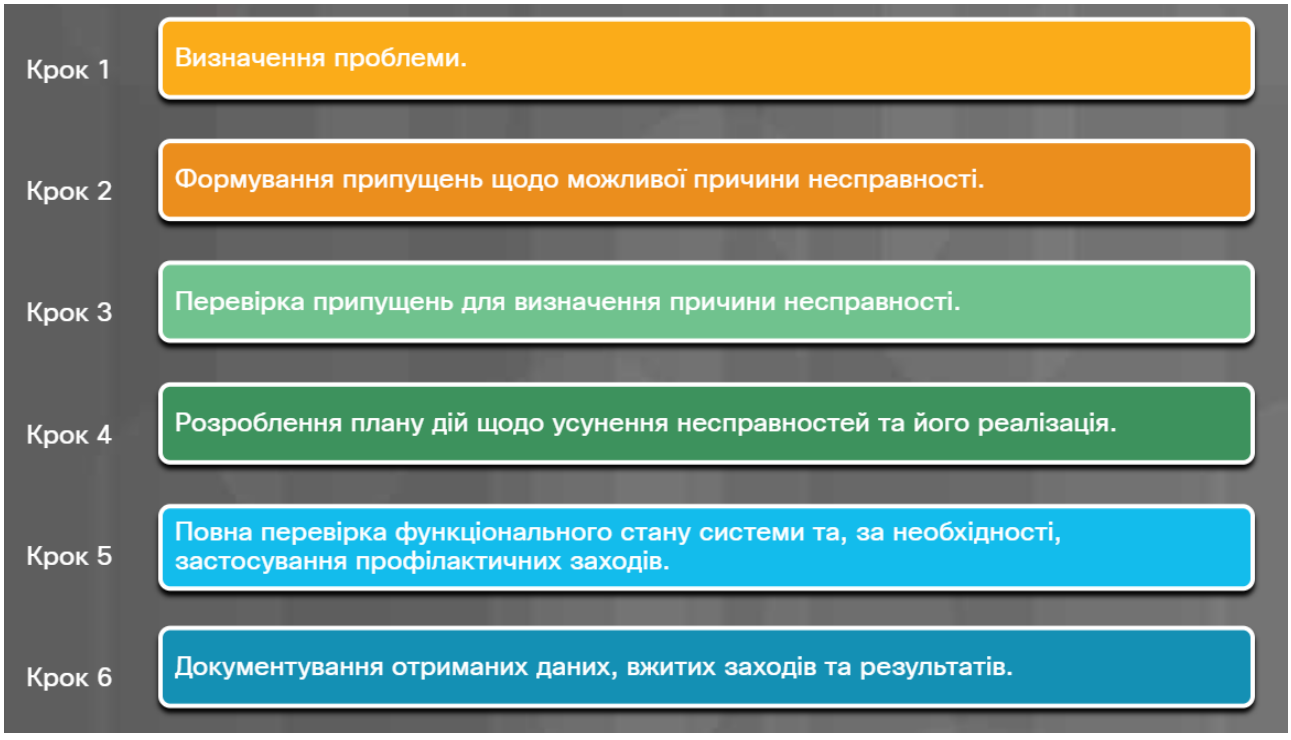

Рис. 3.1 – Основні кроки процес пошуку та усунення несправностей в комп’ютерних мережах

Визначимо зміст кожного із 6 кроків процесу діагностики мережевих несправностей.

Перший крок - визначення проблеми. Він включає збирання інформації від замовника. У процесі діалогу рекомендується використовувати заздалегідь підготовлений список відкритих і закритих питань, наведений на рисунку 3.2.

Крок 1. Визначення проблеми.	
Відкриті запитання	• Які проблеми виникли з вашим пристроєм? • Яке програмне забезпечення було встановлене на вашому пристрої нещодавно? • Що ви робили, коли була виявлена несправність? • Яке повідомлення про помилку ви отримали? • Який тип підключення до мережі використовує пристрій?
Закриті запитання	• Чи користувався хтось інший вашим пристроєм нещодавно? • Чи видно в мережі спільні файли або принтери? • Чи змінювали ви нещодавно свій пароль? • Чи можете ви отримати доступ до Інтернету? • На даний момент ви в мережі? • Чи виникла ця проблема ще в когось? • Чи мали місце зміни в оточенні чи інфраструктурі мережі?

Рис. 3.2 - Визначення проблем з мережевими пристроями

Другі крок. Формування припущень щодо можливої причини несправності

Після розмови із замовником ви можете формувати припущення щодо можливої причини несправності. На рисунку3.3 наведено перелік деяких поширених ймовірних причин проблем з мережею.

Крок 2. Формування припущень щодо можливої причини несправності.	
Поширені причини несправностей мереж	• Ненадійні кабельні з'єднання • Невірно встановлена мережева карта • ISP не надає доступу до Інтернету • Низький рівень сигналу бездротової мережі • Невірна IP адреса • Існує проблема з DNS сервером • Існує проблема з DHCP сервером

Рис. 3.3 - Формування припущень щодо можливої причини несправності

Перевірка припущень для визначення причини несправності (рис. 3.4.)

Після формування припущень про те, що не так, перевірте їх для визначення причини проблеми. Після виявлення точної причини несправності необхідно визначити дії щодо її усунення. У наведеному вище переліку зазначені швидкі

процедури, які можна використовувати для визначення точної причини проблеми або навіть її усунення. Якщо швидка процедура дозволяє виправити проблему, можна перевірити повну функціональність системи. Якщо швидка процедура не усуває проблему, можливо, буде потрібно детальніше вивчення проблеми, щоб встановити точну причину.

Крок 3. Перевірка припущень для визначення причини несправності.	
Кроки для визначення причини	• Перевірте, чи всі кабелі коректно підключені. • Від'єднайте і знову підключіть кабелі та з'єднувачі. • Перезавантажте комп'ютер або мережевий пристрій. • Увійдіть під обліковим записом іншого користувача. • Відновіть або повторно увімкніть мережеве з'єднання. • Зверніться до адміністратора мережі • Виконайте команду ping до основного шлюзу • Перевірте, чи є доступ до віддаленої веб-сторінки, наприклад http://www.cisco.com.

Рис. 3.4 - Перевірка припущень для визначення причини несправності

Розроблення плану дій для вирішення проблеми та впровадження рішення. Визначивши точну причину проблеми, розробіть план дій для її усунення та реалізуйте його. На рисунку3.5 наведено перелік джерел, за допомогою яких можна зібрати додаткову інформацію для вирішення проблеми.

Крок 4. Розроблення плану дій щодо усунення несправностей та його реалізація.	
Якщо на попередньому кроці не досягнуто рішення проблеми, то для її усунення потрібний подальший аналіз ситуації.	• Журнали обліку ремонтних робіт служби підтримки. • Інші технічні фахівці. • Збірники запитань, що часто ставляться виробнику (FAQs). • Технічні веб-сайти. • Групи новин. • Інструкції з використання комп'ютера. • Інструкції з використання пристроїв. • Онлайн-форуми. • Пошук в мережі Інтернет.

Рис. 3.5 - Розроблення плану дій щодо усунення несправностей та його реалізація.

Повна перевірка функціонального стану системи та застосування профілактичних заходів. Після усунення проблеми перевірте повну функціональність системи і, якщо це можливо, здійсніть профілактичні заходи. На рисунку 3.6 наведений перелік дій для перевірки рішення.

Крок 5. Повна перевірка функціонального стану системи та, за необхідності, застосування профілактичних заходів.	
Повна перевірка функціонального стану системи та, за необхідності, застосування профілактичних заходів.	• За допомогою команди **ipconfig /all** виведіть інформацію про IP адреси усіх мережевих адаптерів. • За допомогою команди **ping** перевірте мережеве з'єднання. За вказаною адресою буде надісланий пакет та буде відображена відповідь. • Перевірте, чи може пристрій отримати доступ до авторизованих ресурсів, таких як сервери електронної пошти компанії та Інтернет. • Перевірте виконання додаткових команд або попросіть керівника про допомогу з іншими утилітами тестування.

Рис. 3.5 - Повна перевірка функціонального стану системи та застосування профілактичних заходів

Документування отриманих даних, вжитих заходів та результатів. Завершальним етапом процедури пошуку й усунення несправностей є документування отриманих даних, вжитих заходів і результатів, як показано на рисунку 3.6.

Крок 6. Документування отриманих даних, вжитих заходів та результатів.	
Документування отриманих даних, вжитих заходів та результатів.	• Обговоріть реалізоване рішення із замовником. • Отримайте підтвердження щодо усунення несправності у замовника. • Надайте замовнику всю необхідну документацію. • Задокументуйте усі дії, вжиті для усунення несправності, у замовленні на обслуговування і в журналі техніка. • Задокументуйте всі компоненти, що використовувалися під час ремонту. • Зазначте час, витрачений на усунення несправностей.

Рис. 3.6 - Документування отриманих даних, вжитих заходів та результатів

Наведнмо деяки поширені проблеми функціонування мережі та способи їх усунення (таб. 3.1, 3.1).

Таблиця 3.1 - Поширені проблеми функціонування мережі та способи їх усунення

Визначення проблеми	Ймовірні причини	Можливі рішення
Світлодіодні індикатори мережевої карти не світяться.	Мережевий кабель від'єднаний або пошкоджений.	Повторно під'єднайте або замініть кабель мережевого з'єднання з комп'ютером.
Світлодіодні індикатори мережевої карти не світяться.	Мережева карта пошкоджена.	Замініть мережеву карту.
Користувач не може використовувати SSH для доступу до віддаленого пристрою.	Віддалений пристрій не налаштований для доступу по SSH.	Налаштуйте віддалений пристрій для доступу по SSH.
Користувач не може використовувати SSH для доступу до віддаленого пристрою.	SSH не дозволений від даного користувача або певної мережі.	Надайте доступ SSH від даного користувача або мережі.
Пристрій не може виявити бездротовий маршрутизатор.	Бездротовий маршрутизатор/точка доступу налаштований з іншим протоколом 802.11.	Налаштуйте бездротовий маршрутизатор/точку доступу з протоколом 802.11, сумісним з протоколом даного пристрою.
Пристрій не може виявити бездротовий маршрутизатор.	SSID не транслюється.	Налаштуйте широкомовну транляцію SSID на бездротовому маршрутизаторі.
Пристрій не може виявити бездротовий маршрутизатор.	Бездротова мережева карта у пристрої відключена.	Увімкніть бездротову мережеву карту у пристрої.
Комп'ютер з Windows має IPv4 адресу 169.254.x.x.	Мережевий кабель від'єднаний.	Приєднайте знову мережевий кабель.
Комп'ютер з Windows має IPv4 адресу 169.254.x.x.	Маршрутизатор вимкнений або з'єднання порушене.	Переконайтесь, що маршрутизатор увімкнений і підключений належним чином до мережі. Потім відмініть та оновіть IP адресу на комп'ютері.
Комп'ютер з Windows має IPv4 адресу 169.254.x.x.	Мережева карта пошкоджена.	Замініть мережеву карту.
Віддалений пристрій не відповідає на запит ping.	Міжмережевий екран Windows вимикає ping за замовчуванням.	Встановіть на міжмережевому екрані дозвіл на виконання команди ping.

Таблиця 3.2 - Поширені проблеми функціонування мережі та способи їх усунення

Визначення проблеми	Ймовірні причини	Можливі рішення
Віддалений пристрій не відповідає на запит ping.	Віддалений пристрій налаштований не відповідати на запити ping.	Налаштуйте віддалений пристрій на відповідь на запити ping.
Користувач може отримати доступ до локальної мережі, але не може отримати доступ до Інтернету.	Невірно вказана або не налаштована адреса шлюзу.	Переконайтеся, що мережевій карті призначено правильну адресу шлюзу.
Користувач може отримати доступ до локальної мережі, але не може отримати доступ до Інтернету.	ISP не надає доступу до Інтернету.	Зателефонуйте провайдеру (ISP), щоб повідомити про проблему.
Мережа є повністю функціональною, але бездротовий пристрій не може під'єднатися до неї.	Функції і компоненти бездротового зв'язку пристрою вимкнені.	Увімкніть функції і компоненти бездротового зв'язку пристрою.
Мережа є повністю функціональною, але бездротовий пристрій не може під'єднатися до неї.	Пристрій знаходиться поза межами покриття бездротової мережі.	Підійдіть ближче до бездротового маршрутизатора/точки доступу.
Мережа є повністю функціональною, але бездротовий пристрій не може під'єднатися до неї.	Діють завади, створені іншими бездротовими пристроями, що використовують той самий діапазон частот.	Налаштуйте бездротовий маршрутизатор на інший канал.
Локальні ресурси, такі як спільні файли чи принтери, недоступні.	Можлива низка проблем: неякісне прокладання кабелів, комутатор або маршрутизатор не функціонують, міжмережевий екран блокує трафік, служба DNS не працює.	З'ясуйте масштаб проблеми, спробувавши підключитися з іншого хоста.

Рис. 3.8 - Поширені проблеми функціонування мережі та способи їх усунення

Причини несправностей у роботі мережі можуть бути пов'язані зі збоями обладнання, програмного забезпечення або налаштувань, а також поєднанням цих факторів. Деякі з цих проблем доведеться вирішувати частіше за інші.

3.5 Використання логування для діагностики стану комп'ютерної мережі

Если в работе компьютера, сервера или сетевого возникла неизвестная ошибка, IT-специалисти в первую очередь смотрят логи. Лог это специальный текстовый файл о событиях в компьютерной системе, который хранится на каждом компьютере или сервере. Это стандартная хронология событий и их источников появления, ошибок и причин, по которым произошли эти события. Анализировать логи можно также с помощью специального ПО (Elasticsearch, Logstash и Kibana).

На рис. 3.7 представлен фрагмент лога ПК.

```
Apr 08 13:09:12 rnode22.itgold.io telegraf[1772]: 2021-04-08T10:09:12Z E! [agent] Error writing to outputs.influxdb: could not write any address
Apr 08 13:09:17 rnode22.itgold.io telegraf[1772]: 2021-04-08T10:09:17Z E! [inputs.exec] Error in plugin: exec: command timed out for command '/opt/freeton/scripts/ton-node>
Apr 08 13:09:20 rnode22.itgold.io CRON[471027]: pam_unix(cron:session): session closed for user root
Apr 08 13:09:22 rnode22.itgold.io sshd[472958]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=93.145.61.6  user=root
Apr 08 13:09:22 rnode22.itgold.io telegraf[1772]: 2021-04-08T10:09:22Z W! [outputs.influxdb] Metric buffer overflow; 2 metrics have been dropped
Apr 08 13:09:22 rnode22.itgold.io telegraf[1772]: 2021-04-08T10:09:22Z E! [outputs.influxdb] When writing to [http://127.0.0.1:8086]: failed doing req: Post "http://127.0.>
Apr 08 13:09:22 rnode22.itgold.io telegraf[1772]: 2021-04-08T10:09:22Z E! [agent] Error writing to outputs.influxdb: could not write any address
Apr 08 13:09:23 rnode22.itgold.io sshd[472958]: Failed password for root from 93.145.61.6 port 43554 ssh2
Apr 08 13:09:24 rnode22.itgold.io sshd[472958]: Received disconnect from 93.145.61.6 port 43554:11: Bye Bye [preauth]
Apr 08 13:09:24 rnode22.itgold.io sshd[472958]: Disconnected from authenticating user root 93.145.61.6 port 43554 [preauth]
Apr 08 13:09:29 rnode22.itgold.io sshd[472965]: Invalid user astro from 178.128.61.211 port 56946
Apr 08 13:09:29 rnode22.itgold.io sshd[472965]: pam_unix(sshd:auth): check pass; user unknown
Apr 08 13:09:29 rnode22.itgold.io sshd[472965]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=178.128.61.211
Apr 08 13:09:31 rnode22.itgold.io sshd[472965]: Failed password for invalid user astro from 178.128.61.211 port 56946 ssh2
Apr 08 13:09:32 rnode22.itgold.io telegraf[1772]: 2021-04-08T10:09:32Z E! [outputs.influxdb] When writing to [http://127.0.0.1:8086]: failed doing req: Post "http://127.0.>
Apr 08 13:09:32 rnode22.itgold.io telegraf[1772]: 2021-04-08T10:09:32Z E! [agent] Error writing to outputs.influxdb: could not write any address
Apr 08 13:09:34 rnode22.itgold.io sshd[472965]: Received disconnect from 178.128.61.211 port 56946:11: Bye Bye [preauth]
Apr 08 13:09:34 rnode22.itgold.io sshd[472965]: Disconnected from invalid user astro 178.128.61.211 port 56946 [preauth]
Apr 08 13:09:37 rnode22.itgold.io sshd[472969]: Invalid user b from 213.59.135.87 port 49690
Apr 08 13:09:37 rnode22.itgold.io sshd[472969]: pam_unix(sshd:auth): check pass; user unknown
Apr 08 13:09:37 rnode22.itgold.io sshd[472969]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=213.59.135.87
Apr 08 13:09:40 rnode22.itgold.io sshd[472969]: Failed password for invalid user b from 213.59.135.87 port 49690 ssh2
Apr 08 13:09:40 rnode22.itgold.io sshd[472969]: Received disconnect from 213.59.135.87 port 49690:11: Bye Bye [preauth]
Apr 08 13:09:40 rnode22.itgold.io sshd[472969]: Disconnected from invalid user b 213.59.135.87 port 49690 [preauth]
Apr 08 13:09:42 rnode22.itgold.io telegraf[1772]: 2021-04-08T10:09:42Z E! [outputs.influxdb] When writing to [http://127.0.0.1:8086]: failed doing req: Post "http://127.0.>
Apr 08 13:09:42 rnode22.itgold.io telegraf[1772]: 2021-04-08T10:09:42Z E! [agent] Error writing to outputs.influxdb: could not write any address
Apr 08 13:09:52 rnode22.itgold.io telegraf[1772]: 2021-04-08T10:09:52Z E! [outputs.influxdb] When writing to [http://127.0.0.1:8086]: failed doing req: Post "http://127.0.>
Apr 08 13:09:52 rnode22.itgold.io telegraf[1772]: 2021-04-08T10:09:52Z E! [agent] Error writing to outputs.influxdb: could not write any address
Apr 08 13:09:52 rnode22.itgold.io sshd[472976]: Invalid user mk from 111.231.201.210 port 35542
Apr 08 13:09:52 rnode22.itgold.io sshd[472976]: pam_unix(sshd:auth): check pass; user unknown
Apr 08 13:09:52 rnode22.itgold.io sshd[472976]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=111.231.201.210
Apr 08 13:09:53 rnode22.itgold.io sshd[472978]: Invalid user grep from 193.34.8.49 port 49106
Apr 08 13:09:53 rnode22.itgold.io sshd[472978]: pam_unix(sshd:auth): check pass; user unknown
Apr 08 13:09:53 rnode22.itgold.io sshd[472978]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=193.34.8.49
Apr 08 13:09:55 rnode22.itgold.io sshd[472976]: Failed password for invalid user mk from 111.231.201.210 port 35542 ssh2
Apr 08 13:09:55 rnode22.itgold.io sshd[472978]: Failed password for invalid user grep from 193.34.8.49 port 49106 ssh2
Apr 08 13:09:55 rnode22.itgold.io sshd[472978]: Received disconnect from 193.34.8.49 port 49106:11: Bye Bye [preauth]
Apr 08 13:09:55 rnode22.itgold.io sshd[472978]: Disconnected from invalid user grep 193.34.8.49 port 49106 [preauth]
```

Рис. 3.7 – Логі ПК

Запись логов называется логированием. Логирование позволяет ответить на вопросы, что происходило в системе, при каких обстоятельствах и когда. Без использования логов IT-специалисту сложно понять, из-за чего произошла ошибка в системе, если она возникает только периодически и только в определенных условиях функционирования. Чтобы облегчить задачу системным

администраторам, в лог в обязательном порядке записывается информация не только об ошибках в системе, но и о возможных причинах их возникновения. Администратор ищет причины возникновения неисправностей, сбоев в устройствах системы и недоступности сайтов в системе

Таким образом, постоянный анализ логов — один из основных инструментов в работе системных и сетевых администраторов.

Он помогает обнаружить источники многих сетевых неисправностей, выявить конфликты в сетевых протоколах, отследить события, связанные с перегрузкой сети. Благодаря тщательному анализу логов найденные ошибки в сети их можно быстро исправить.

Логи должны записываться во время работы каждого ИТ-компонента.

Практически все устройств сетевой инфраструктуры обеспечивают передачу информации по регистрации в системе событий в специальную базу syslog-сервер. Syslog-регистрация событий используется для управления серверами и приложениями, а также для проведения мониторинга по сбоям и неисправностям в сети. Уровень подробностей в отчетах задается в настройках (раздел словесного наполнения). Для IT-специалиста доступны варианты от регистрации событий от критически важных событий до регистрации всех, в том числе даже незначительных. По степени важности логи можно разделить на:

- ***критические*** (Fatal/critical error) – состояние сети, когда нужно срочно принять меры по устранению неисправности;
- ***предупреждения*** (Warning) – необходимо обратить внимание на ситуацию в сети;
- ***ошибки*** (Not critical error), которые не влияют на работу сети;
- ***информация от различных сервисов*** (Initial information).

Все типы логов перечислены в документе RFC 3164. Отправляемые логи, включают в себя события и ошибки в сети

Syslog-сервер при соответствующей настройке будет выдавать отчеты об ошибках, событиях и необычных операциях (рис 3.10). От сетевого администратора требуется правильно настроить выделенный коммутатор, указав ему IP-адрес sys.log- сервера. В списке событий sys.log- сервера будут регистрироваться записи о

всех сетевых операциях, а syslog-сервер будет сам установленному расписанию формировать и отправлять отчеты. Сетевому администратору необходимо будет просмотреть и изучить как текущие сообщения, так и sys.log-сообщения за требуемый период. Syslog-регистрация – один из лучших методов диагностики при проблемахв сети.

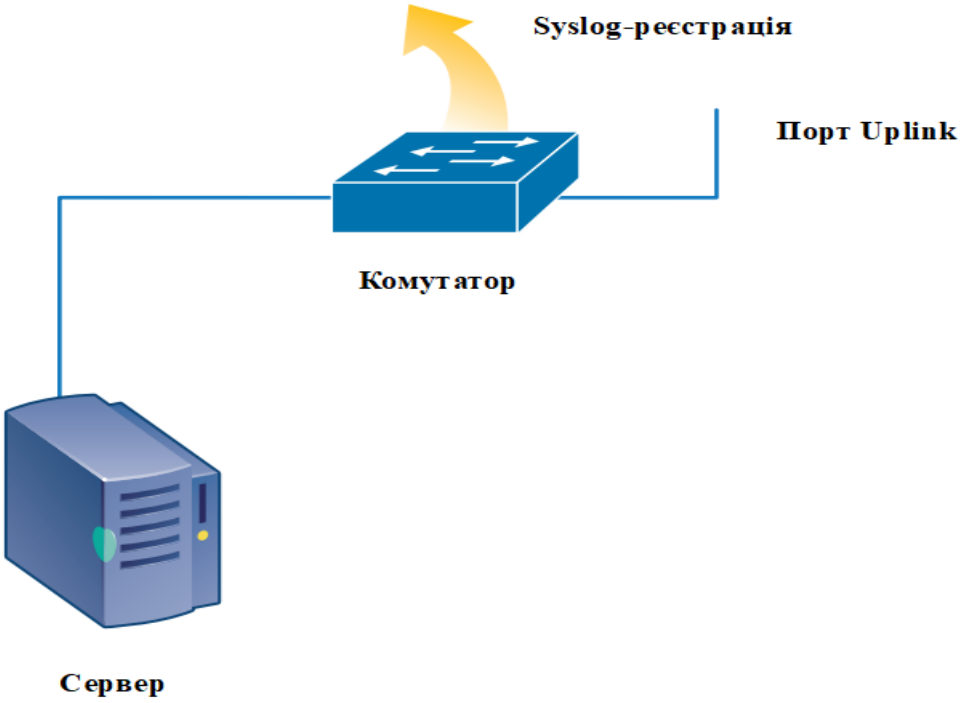

Рисунок 3.8 – Реєстрація подій на Syslog-сервері

Syslog-сервер генерирует в том числе достаточно большое количество бесполезных сообщений. В огромном количестве сообщений бывает крайне сложно обнаружить источник возникшей неиспрвности и тем более и в процессе прогнозирования поведения системы искать источники будущих проблем. Большое количество сообщений, не имеющих достаточно важного значения и необходимость искать среди них нужное привели к появлению специальных syslog-утилит. С помощью таких утилит возникает возможность сортировки и группировки сообщений, а также возможность поиска по заданным критериям.

Обратимся к некоторым системам мониторинга логов. Такие системы мониторинга включают, как правило, четыре компонента: сборщики данных или коллекторы, хранилища, системы визуализации и алертинг.

В таблице 3.3 представлен список основных компонент системам мониторинга логов [15].

Таблице 3.3 - Компоненты системи мониторинга логов

Сборщики логов	Хранилища логов	Системы визуализации
Fluent bit	Elasticsearch.	Grafana
Promtail	ClickHouse	DataLens
Filebeat	Manticore Search	Kibana
Elastic Agent	Grafana Loki	Apache Superset
Fluentd	HDFS	Redash
Vector	Kafka	Metabase
Logstash	PostgreSQL	Apache Superset

Каждый из этих сервисов мониторинга логов имеет свои достоинства и свои недостатки. Выбор остается за потребителем.

Рассмотрим наиболее популярный коллектор логов Fluent bit. У этого коллектора очень малое потребление вычислительных ресурсов и отличная производительность. С версии 2.2.0 он уже поддерживает не только логи, но и метрики, что делает его активным агентом сбора телеметрии от компьютерных систем в целом (рис. 3.9) [16].

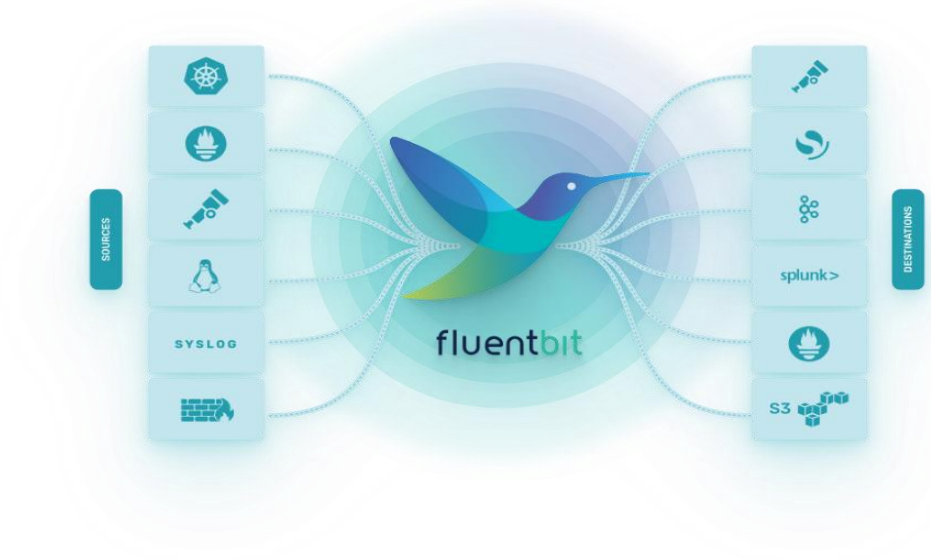

Рис. 3.9 - Коллектор логов Fluent bit

Fluent Bit — це добре масштабований та надшвидкий сервер збирання та пересилки лог-журналів і метрик. Це кращий вибір, в тому числі, для хмарних і контейнерних середовищ.

3.3 Використання метрик систем моніторингу для діагностики стану комп'ютерних мереж

На прикладі використання системи моніторингу комп'ютерних мереж Zabbix розглянемо можливості використання метрик, що формуються у системі для діагностики мережі.

Zabbix контролюйте всю мережеву інфраструктуру, збираючи будь-які метрики з будь-яких джерел. Ось далеко не повний перелік джерел, для яких формуються метрики:

− мережні пристрої;

− хмарні сервіси, контейнери, віртуальні машини;

− моніторинг операційних систем;

− лог-файли;

− бази даних;

− додатки;

− сервіси;

− IoT сенсори;

− моніторинг веб-сторінок;

− моніторинг кінцевих точок HTTP/HTTPS;

− підтримуючи всіх стандартних для галузі протоколів;

− збір даних із зовнішніх кінцевих точок API/

Zabbix забезпечує миттєве виявлення проблем у комп'ютерних мережах. У системі моніторингу не потрібно відстеження метрик вручну. Визначаючи гнучкі пороги для метрик за допомогою Zabbix ви можете автоматично виявляти стан проблеми у вхідному потоці даних:

− високопродуктивне виявлення проблем у режимі реального часу;

− гнучкі можливості визначення;

− розділяйте стани вирішення проблем та самі проблеми;

− кілька рівнів значущості;

− аналіз вихідних даних;

− захист від схлопування;

− виявлення аномалій;

− прогнозування проблем;

− виявлені проблеми можна класифікувати за допомогою тегів для розумних оповіщень;

− експорт виявлених проблем подій у режимі реального часу в сторонні системи (Elastic, Splunk тощо).

Zabbix надає гнучкі розумні можливості визначення порогових значень. Хоча поріг спрацьовування може бути простим ("більше, ніж X"), користувач може використовувати всі можливості підтримуваних функцій та операторів для статистичного аналізу історичних даних.

Zabbix дозволяє отримувати сповіщення про критичні проблеми в мережі за допомогою таких систем оповіщення як:

− VictorOPS;

− Opsgenie;

− Pagerduty;

− SIGNL4;

− Email;

− SMS для надійних оповіщень з використанням USB-модемів;

− Онлайн SMS-шлюзи.

Визначаючи різні повідомлення для різних каналів передачі повідомлень, можна використовувати шаблони за замовчуванням або створити і налаштувати свій власний шаблон:

− налаштовуйте повідомлення залежно від типу проблеми та ролі одержувача повідомлень;

− доповнюйте повідомлення будь-якою інформацією про час виконання та інвентар;

− надсилайте заплановані PDF звіти для поглибленого та довгострокового аналізу даних.

Zabbix дозволяє налагоджувати зібрані метрики різними можливими способами. Визначаючи панелі інструментів на основі віджетів, що відображають необхідну інформацію, система забезпечує:

− великий вибір різноманітних віджетів;

− просте розміщення та масштабування віджетів за допомогою функції drag and drop;

− кожен віджет легко налаштовується відповідно до ваших потреб;

− відображення метрик, проблем інфраструктури на панелі керування;

− доступ до метриків, проблем, звітів та карт одним натисканням кнопки.

Масштабування інфраструктури за допомогою Zabbix дозволяє збирати мільйони показників із сотень тисяч пристроїв, сервісів та додатків. Проксі-сервери Zabbix легко розвертаються та забезпечують необмежену вертикальну масштабованість. Рекомендації щодо масштабування передбачають:

− делегування збору метрик проксі-серверам Zabbix;

− розгортання необмеженої кількості проксі-серверів Zabbix;

− Моніторинг тисяч віддалених локацій, дочірніх структур компанії, центрів обробки даних;

− розгортання проксі-серверів Zabbix із пакетів, контейнерів або хмарних образів;

− зниження мережевих навантажень - трафік між центральним бекендом сервера Zabbix та проксі-серверами стискається.

3.4 Вплив системи діагностики несправностей на ефективність функціонування комп’ютерних мереж

Вплив системи діагностики несправностей на ефективність функціонування комп'ютерних мереж може бути досліджений з використанням різних критеріїв якості роботи комп'ютерної мережі, таких як надійність мережі, доступність мережі, час виявлення несправностей та відновлення працездатності мережі, кількість відмов, ефективність використання ресурсів та витрати на обслуговування.

Система діагностики несправностей відіграє важливу роль у виявленні та запобіганні несправностям у комп'ютерних мережах. Вплив цієї системи може бути оцінений з урахуванням характеристик пасивного обладнання (Sp), таких як кабелі, роз'єми, патч-панелі, активного мережевого обладнання (Sa), що включає мережні

плати, комутатори, маршрутизатори, системні ресурси сервера та робочих станцій (Ssys), а також конфігураційних та мережевих налаштувань мережевої операційної системи (Snos).

Таким чином, загальний критерій оцінки впливу системи діагностики несправностей на ефективність функціонування комп'ютерних мереж може мати вигляд [ ]:

$$Cr = \varphi(S_p\{x_1, x_2, \ldots x_k\}, (S_a\{x_1, x_2, \ldots x_l\}, (S_{sys}\{x_1, x_2, \ldots x_m\}, (S_{nos}\{x_1, x_2, \ldots x_n\}$$

де: $S_p\{x_1, x_2, \ldots x_k\}$ - сукупність характеристик пасивного обладнання;

$S_a\{x_1, x_2, \ldots x_l\}$ - сукупність характеристик активного мережевого обладнання (мережові плати, комутатори, маршрутизатори);

$S_{sys}\{x_1, x_2, \ldots x_m\}$ - сукупність характеристик системних ресурсів сервера та робочих станцій;

$S_{nos}\{x_1, x_2, \ldots x_n\}$ - сукупність конфігураційних та мережевих налаштувань мережевої операційної системи.

Основний критерій якості роботи комп'ютерної мережі – надійність. Вона визначається ймовірністю безвідмовної роботи, тобто ймовірністю відсутності збоїв та простоїв у мережі. Система діагностики несправностей дозволяє виявити та усунути потенційні несправності до їх виникнення, що підвищує надійність мережі.

Інший важливий критерій – доступність мережі. Вона визначається часом реакцію запит користувача, тобто швидкістю відповіді мережі на запити. Система діагностики несправностей допомагає швидко виявити та виправити можливі проблеми, такі як затримки мережі або перевантаження, що покращує доступність мережі.

Ще один критерій - час виявлення несправності та відновлення працездатності мережі. Чим швидше система діагностики виявляє несправність та відновлює працездатність мережі, тим менше часу можуть витратити користувачі на очікування і тим ефективніше працюватиме комп'ютерна мережа.

Кількість відмов – ще один важливий критерій. Система діагностики несправностей може допомогти у запобіганні відмовам та скоротити їх кількість, що підвищить ефективність функціонування комп'ютерної мережі.

Ефективність використання ресурсів може бути підвищена завдяки системі діагностики несправностей. Вона допомагає виявити та виправити проблеми, пов'язані з неефективним використанням ресурсів, наприклад, навантаженнями на певному сегменті мережі або неправильним налаштуванням мережевого обладнання.

Нарешті витрати на обслуговування комп'ютерної мережі можуть бути скорочені завдяки системі діагностики несправностей. Вона допомагає виявити та усунути проблеми в мережі, що знижує кількість викликів до технічної підтримки та час, витрачений на обслуговування.

Таким чином, система діагностики несправностей має значний вплив на ефективність функціонування комп'ютерних мереж, що можна оцінити з використанням різних критеріїв якості роботи мережі.

Висновки

Аналіз методів пошуку та усунення несправності в сучасних комп’ютерних мережах (КМ) показав необхідність пошуку новітніх підходів до діагностики стану мережі та вибору інструментів для підвищення надійності функціонування мережевого обладнання.

В магістерської роботі надані об’єкти і параметри моніторингу та діагностики мереж, визначені основні ознаки несправностей комп'ютерних мереж та запропоновано модель вирішення проблеми пошуку та усунення несправностей .

В роботі показано, що застосування традиційних методів діагностики мережевих несправностей дає суб'єктивну оцінку стану мережі, яка залежить від рівня підготовки ІТ-фахівця. В даному випадку рекомендовано використовувати методи штучного інтелекту для вирішення проблем диагностики стану КМ.

Запропонована у роботі модель процесу діагностики мереж надає можливість сформулювати вимоги щодо її реалізації у складі ШНМ моніторингу стану комп'ютерної мережі. Основне завдання діагностики із застосуванням ШІ зводиться до вибору типу мережі, навчання та визначення параметрів архітектури ШНМ.

В цілому, використання потужних інструментів моніторингу та діагностики підвищує ефективності функціонування мереж на 20-30% залежно від масштабу мережі та засобів які використовуються для моніторингу та діагностики.

Перелік джерел посилання

1. ДСТУ 2860-94 Надійність техніки. Терміни та визначення.

2. ДСТУ 2861-94 Надійність техніки. Основні положення.

3. Бабіч А.В. Введення у діагностику комп'ютерних мереж. -ХНУРЕ, 2010, 126 с.

4. 11. Хайкін С. Нейронні мережі та навчальні машини. Prentice Hall. Нью-Йорк. 2019.

5. 12. Schmidhuber J. (2015). Deep Learning in Neural Networks: An Overview // Neural Networks. 144 2021.

6. C. Cerin, C. Coti, P. Delort, F. Diaz, M. Gagnaire, Q. Gaumer, N. Guillaume, J. Lous, S. Lubiarz, J. Raffaelli et al., "Downtime statistics of current cloud solutions," International Working Group on Cloud Computing Resiliency, Tech. Rep, 2018.

7. G. Gheorghe, T. Avanesov, M.-R. Palattella, T. Engel, and C. Popoviciu, "Sdn-radar: Network troubleshooting combining user experience and sdn capabilities," in Network Softwarization (NetSoft), 2015 1st IEEE Conference on. IEEE, 2017, pp. 1–5.

8. H. Zeng, P. Kazemian, G. Varghese, and N. McKeown, "A survey on network troubleshooting," Technical Report Stanford/TR12-HPNG-061012, Stanford University, Tech. Rep., 2019.

9. Dhamdhere, R. Teixeira, C. Dovrolis, and C. Diot, "Netdiagnoser: Troubleshooting network unreachabilities using endto-end probes and routing data," in Proceedings of the 2017 ACM CoNEXT conference. ACM, 2021, p. 18.

10. R. Fonseca, G. Porter, R. H. Katz, S. Shenker, and I. Stoica, "X-trace: A pervasive network tracing framework," in Proceedings of the 4th USENIX conference on Networked systems design & implementation. USENIX Association, 2017, pp. 20–20.

11. Anand and A. Akella, "Netreplay: a new network primitive," ACM SIGMETRICS Performance Evaluation Review, vol. 37, no. 3, pp. 14–19, 2020.

12. H. Zeng, P. Kazemian, G. Varghese, and N. McKeown, "Automatic test packet generation," in Proceedings of the 8th international conference on Emerging networking experiments and technologies. ACM, 2018, pp. 241–252

13. S. Traverso, E. Tego, E. Kowallik, S. Raffaglio, A. Fregosi, M. Mellia, and F. Matera, “Exploiting hybrid measurements for network troubleshooting,” in Telecommunications Network Strategy and Planning Symposium (Networks), 2014 16th International. IEEE, 2019, pp. 1–6.

14. K.-C. Leung, V. O. Li, and D. Yang, “An overview of packet reordering in transmission control protocol (tcp): problems, solutions, and challenges,” IEEE transactions on parallel and distributed systems, vol. 18, no. 4, pp. 522–535, 2017.

15. Mahimkar, J. Yates, Y. Zhang, A. Shaikh, J. Wang, Z. Ge, and C. T. Ee, “Troubleshooting chronic conditions in large ip networks,” in Proceedings of the 2008 ACM CoNEXT Conference. ACM, 2018, p. 2.

16. J. Sommers, P. Barford, N. Duffield, and A. Ron, “Improving accuracy in end-to-end packet loss measurement,” in ACM SIGCOMM Computer Communication Review, vol. 35, no. 4. ACM, 2015, pp. 157–168.

17. N. Duffield, “Network tomography of binary network performance characteristics,” IEEE Transactions on Information Theory, vol. 52, no. 12, pp. 5373–5388, 2016.

18. S. Kandula, D. Katabi, and J.-P. Vasseur, “Shrink: A tool for failure diagnosis in ip networks,” in Proceedings of the 2015 ACM SIGCOMM workshop on Mining network data. ACM, 2015, pp. 173–178.

19. H. X. Nguyen and P. Thiran, “Using end-to-end data to infer lossy links in sensor networks,” in IEEE Infocom 2021, no. CONF, 2021.

20. R. Karimazad and A. Faraahi, “An anomaly-based method for ddos attacks detection using rbf neural networks,” in Proceedings of the International Conference on Network and Electronics Engineering, vol. 11, 2019, pp. 44–48.

21. W. Wang, M. Zhu, X. Zeng, X. Ye, and Y. Sheng, “Malware traffic classification using convolutional neural network for representation learning,” in Information Networking (ICOIN), 2017 International Conference on. IEEE, 2017, pp. 712–717.

22. [D. Tran, H. Mac, V. Tong, H. A. Tran, and L. G. Nguyen, “A lstm based framework for handling multiclass imbalance in dga botnet detection,” Neurocomputing, vol. 275, pp. 2401– 2413, 2018.

23. Cisco, “Technical notes of ciso,” in https://www.cisco.com/c/en/us/support/docs/routers/10000- series-routers/15095-highcpu.html, 2016.

24. P. Kazemian, G. Varghese, and N. McKeown, “Header space analysis,” Ph.D. dissertation, Stanford University, 2019.

25. N. Feamster and H. Balakrishnan, “Detecting bgp configuration faults with static analysis,” in Proceedings of the 2Nd Conference on Symposium on Networked Systems Design & Implementation-Volume 2. USENIX Association, 2005, pp. 43–56.

26. F. Le, S. Lee, T. Wong, H. S. Kim, and D. Newcomb, “Detecting network-wide and router-specific misconfigurations through data mining,” IEEE/ACM transactions on networking, vol. 17, no. 1, pp. 66–79, 2019.

27. B. Agarwal, R. Bhagwan, T. Das, S. Eswaran, V. N. Padmanabhan, and G. M. Voelker, “Netprints: Diagnosing home network misconfigurations using shared knowledge.” in NSDI, vol. 9, 2019, pp. 349–364.

28. V. Muthumanikandan and C. Valliyammai, “A survey on link failures in software defined networks,” in Advanced Computing (ICoAC), 2015 Seventh International Conference on. IEEE, 2015, pp. 1–5.

29. ONOS, “Open network operating system,” in https://wiki.onosproject.org/display/ONOS/Wiki+Home, 2017

30. Y. Zhuang, E. Gessiou, S. Portzer, F. Fund, M. Muhammad, I. Beschastnikh, and J. Cappos, “Netcheck: Network diagnoses from blackbox traces.” in NSDI, 2014, pp. 115–128.

31. N. M. Kalibhat, S. Varshini, C. Kollengode, D. Sitaram, and S. Kalambur, “Software troubleshooting using machine learning,” in 2017 IEEE 24th International Conference on High Performance Computing Workshops (HiPCW). IEEE, 2017, pp. 3–10.

32. Jayaraj, T. Venkatesh, and C. S. R. Murthy, “Loss classification in optical burst switching networks using machine learning techniques: improving the performance of tcp,” IEEE Journal on Selected Areas in Communications, vol. 26, no. 6, 2018.

33. Mestres, A. Rodriguez-Natal, J. Carner, P. Barlet-Ros, E. Alarcon, M. Sol ´ e, V. Munt ´ es-Mulero, D. Meyer, S. Barkai, . J. Hibbett et al., “Knowledge-defined

networking,” ACM SIGCOMM Computer Communication Review, vol. 47, no. 3, pp. 2–10, 2017.

34. Dethise, M. Chiesa, and M. Canini, “Prelude: Ensuring inter-domain loop-freedom in sdn-enabled networks” arXiv preprint arXiv:1806.09566, 2018.