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

КВАЛІФІКАЦІЙНА РОБОТА

на тему: «Дослідження методів виявлення та усунення несправностей у мережевому обладнанні з використанням штучного інтелекту»

на здобуття освітнього ступеня бакалавра
зі спеціальності 123 Комп'ютерної інженерії
(код, найменування спеціальності)
освітньо-професійної програми Комп'ютерна інженерія
(назва)

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

_____ *Валерія ШВЕЦЬ*
(підпис) *Ім'я, ПРІЗВИЩЕ здобувача*

Виконала: здобувачка вищої освіти гр. КІД-41
Валерія ШВЕЦЬ
Ім'я, ПРІЗВИЩЕ
Керівник: Ігор БУЧЕНКО
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 123 Комп'ютерної інженерії

Ступінь вищої освіти бакалавр

Спеціальність 123 Комп'ютерної інженерії

Освітньо-професійна програма Комп'ютерна інженерія

ЗАТВЕРДЖУЮ
Завідувач кафедрою Наталія ЛАЩЕВСЬКА
_____Ім'я, ПРІЗВИЩЕ
«_____» _____ 2024р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Швець Валерія Святославівна
(прізвище, ім'я, по батькові здобувача)

1. Тема кваліфікаційної роботи: Дослідження методів виявлення та усунення несправностей у мережевому обладнанні з використанням штучного інтелекту
керівник кваліфікаційної роботи Ігор БУЧЕНКО,
(Ім'я, ПРІЗВИЩЕ, науковий ступінь, вчене звання)
затверджені наказом Державного університету інформаційно-комунікаційних технологій від «27» лютого 2024р. № 36
2. Строк подання кваліфікаційної роботи «3» червня 2024р.
3. Вихідні дані до кваліфікаційної роботи: Інформація про конфігурації мережевих пристроїв, опис використовуваного мережевого обладнання
4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
1. Розділ 1. Огляд існуючих підходів до виявлення та усунення несправностей у мережевому обладнанні
2. Розділ 2. Дослідження існуючих методів виявлення несправностей в мережевому обладнанні з використанням штучного інтелекту
3. Розділ 3. Порівняльний аналіз методів усунення несправностей з використанням .штучного інтелекту
1. Перелік ілюстративного матеріалу: *презентація*
2. Дата видачі завдання «27» лютого 2024р. № 36

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1	Збір даних	28.02-22.03.2024	Виконано
2	Обробка матеріалу	23.03-05.04.2024	Виконано
3	Розробка теоретичної частини	06.04-10.04.2024	Виконано
4	Дослідження існуючих підходів до виявлення та усунення несправностей у мережевому обладнанні	11.04-30.04.2024	Виконано
5	Аналіз методів усунення несправностей з використанням штучного інтелекту	01.05-03.05.2024	Виконано
6	Висновки за результатами аналізу	04.05-08.05.2024	Виконано
7	Розробка презентації	09.05-11.05.2024	Виконано
8	Передзахист	14.05-17.05.2024	Виконано
9	Здача в деканат	23.05-1.06.2024	Виконано

Здобувач(ка) вищої освіти _____ Валерія ШВЕЦЬ
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Керівник кваліфікаційної роботи _____ Ігор БУЧЕНКО
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

РЕФЕРАТ

Текстова частина кваліфікаційної роботи на здобуття освітнього ступеня бакалавра: 41 стор., 5 рис., 2 табл., 30 джерел.

Мета роботи – дослідження і вивчення ефективності методів на основі ШІ у виявленні та усуненні несправностей мережевого обладнання, зокрема, порівняння їх швидкості, точності та ресурсоємності з традиційними підходами, а також визначення оптимальних стратегій використання ШІ для підвищення продуктивності та надійності роботи мережевого обладнання.

Об'єкт дослідження – процес виявлення та усунення несправностей у мережевому обладнанні з використанням штучного інтелекту.

Предмет дослідження – методи і способи виявлення та усунення несправностей в мережевому обладнанні з використанням штучного інтелекту.

Короткий зміст роботи: Сучасні інформаційні інфраструктури стають дедалі складнішими та масштабнішими. Збільшення кількості підключених пристроїв, швидкості передачі даних і обсягу інформації підвищує ймовірність виникнення різних несправностей і проблем в мережі. У сучасних динамічних мережах традиційні методи усунення несправностей недостатньо ефективні. Використання штучного інтелекту може стати важливим фактором у досягненні цих цілей. Штучний інтелект може автоматично аналізувати великі обсяги даних і виявляти складні взаємозв'язки між параметрами мережі.

Крім того, ШІ дозволяє застосовувати прогностичний підхід до управління мережею, що дає змогу передбачати та уникати можливих несправностей.

КЛЮЧОВІ СЛОВА: ВИЯВЛЕННЯ НЕСПРАВНОСТЕЙ, МЕРЕЖЕВЕ ОБЛАДНАННЯ, ШТУЧНИЙ ІНТЕЛЕКТ, МЕРЕЖЕВІ ПРОБЛЕМИ, АЛГОРИТМИ УСУНЕННЯ НЕСПРАВНОСТЕЙ.

ЗМІСТ

ВСТУП

Стрімкий розвиток сучасних технологій вимагає постійного вдосконалення мережевого обладнання для стабільної та ефективної роботи інформаційних систем. Перш за все, важливо відзначити, що мережеве обладнання є основою сучасних інформаційних технологій, а його ефективна робота є необхідним елементом для безперебійного функціонування бізнес-процесів і надання якісних послуг користувачам. Однак постійні технологічні інновації значно ускладнюють роботу мереж, підвищуючи ймовірність виникнення різноманітних збоїв, що призводять до переривання надання інформаційних послуг. Крім того, стандартні підходи до виявлення несправностей, такі як ручний аналіз журналів подій або використання простих систем, заснованих на правилах, можуть бути не повністю ефективними в сучасних динамічних мережах. У таких випадках важливими стають методи, які можуть адаптуватися до змін у середовищі та виявляти нові типи несправностей, що можуть виникнути.

У цьому контексті все більшого значення набуває використання штучного інтелекту (ШІ) як ефективного інструменту виявлення та усунення несправностей мережевого обладнання. Сучасні підходи до управління мережевим обладнанням спрямовані на автоматизацію процесу моніторингу, аналізу та управління мережами, підвищення ефективності та надійності. Штучний інтелект може автоматично аналізувати великі обсяги даних і виявляти складні взаємозв'язки між параметрами мережі, що дозволяє швидко реагувати на потенційні проблеми та запобігати їх виникненню.

Основною метою досліджень у цій галузі є розробка та вдосконалення методів використання штучного інтелекту для виявлення та усунення несправностей мережевих пристроїв. Це включає розробку нових алгоритмів машинного навчання, інтелектуальних систем і програмних рішень, спрямованих на підвищення ефективності діагностики та усунення несправностей мережевих пристроїв. Дослідження в цій галузі також стикаються з етичними питаннями та

питаннями безпеки. Наприклад, використання штучного інтелекту для моніторингу мереж може призвести до порушення приватності та безпеки даних, якщо не приділяти достатньої уваги заходам безпеки та конфіденційності. Також існує ризик атак штучного інтелекту, коли зловмисники намагаються створити штучні збої в роботі мережі, щоб завдати їй шкоди. Тому при розробці та впровадженні методів виявлення та усунення несправностей мережевих пристроїв на основі штучного інтелекту необхідно враховувати не лише технічні, а й етичні, правові та безпекові аспекти. Це забезпечить ефективність і надійність таких методів у реальних умовах експлуатації мережі.

У дослідженні будуть детально розглянуті різні підходи до виявлення та усунення несправностей мережевих пристроїв з використанням штучного інтелекту, а також порівняно їх ефективність та придатність для практичного застосування. Такий аналіз дозволить зробити висновки щодо найкращих стратегій використання штучного інтелекту для покращення управління мережевим обладнанням та забезпечення стабільної роботи інформаційних систем.

РОЗДІЛ 1. ОГЛЯД ІСНУЮЧИХ ПІДХОДІВ ДО ВИЯВЛЕННЯ ТА УСУНЕННЯ НЕСПРАВНОСТЕЙ У МЕРЕЖЕВОМУ ОБЛАДНАННІ

1.1 Загальні принципи мережевого обладнання

В наш час мережеве обладнання повинно мати можливість масштабування від невеликих локальних мереж до великих глобальних мереж і забезпечувати необхідну пропускну здатність і швидкість передачі даних. Масштабованість мережевого обладнання визначає його здатність ефективно функціонувати і задовольняти потреби мережі в міру зростання її розмірів, обсягу даних і кількості користувачів. Загальні принципи для мережевого обладнання визначають основні вимоги та правила побудови та функціонування комп'ютерних мереж. Ці принципи включають масштабованість, яка дозволяє розширювати мережу за необхідності; надійність, яка забезпечує безперебійну роботу системи; продуктивність, яка забезпечує ефективну обробку даних; безпеку, яка захищає мережу від загроз; управління, яке дозволяє ефективно управляти ресурсами; різні компоненти; сумісність, що забезпечує зв’язок між різними компонентами та ефективне використання ресурсів для максимізації продуктивності системи. [3]

Щоб забезпечити масштабованість та ефективність мережі, є кілька важливих аспектів, які слід враховувати при проєктуванні та розробці мережі. По-перше, необхідно враховувати збільшення кількості підключених пристроїв, таких як комп'ютери, телефони й датчики, щоб забезпечити безперервну роботу мережі навіть при високому навантаженні; другий аспект – пропускна здатність, яка повинна забезпечувати достатню пропускну здатність для ефективної передачі даних і враховувати збільшення обсягів даних. По-друге, ефективні механізми маршрутизації та комутації важливі для уникнення перевантажень і забезпечення низьких затримок. Управління та моніторинг також відіграють важливу роль, дозволяючи операторам ефективно керувати своїми мережами навіть у великих

масштабах. Гнучкість і масштабованість обладнання дозволяє йому швидко реагувати на мінливі вимоги і технологічний прогрес. Надійність також є важливим фактором, оскільки великі мережі схильні до різноманітних проблем. Нарешті, системи управління трафіком і безпеки забезпечують стабільну і безпечну роботу мережі навіть при великих обсягах даних і активності.

Щоб уникнути збоїв і забезпечити безперервну роботу мережі, обладнання має бути високонадійним. У цьому допомагає резервування, механізми виявлення та усунення несправностей, а також регулярне технічне обслуговування. Надійність мережевого обладнання – важливий фактор для забезпечення безперебійної роботи мережі.

Між тим, забезпечення надійності мережевого обладнання є важливим аспектом та вимагає систематичного підходу до його обслуговування. Регулярні перевірки, своєчасне оновлення програмного забезпечення та підтримка від виробника є ключовими елементами цього процесу. Резервування апаратного забезпечення та мережевих з'єднань знижує ризик збоїв і забезпечує безперебійну роботу; резервні джерела живлення, такі як ДБЖ і генератори, гарантують, що мережа залишатиметься активною навіть під час перебоїв в електропостачанні. Системи моніторингу та автоматизації допомагають швидко виявляти проблеми та вирішувати їх автоматично. Конфігурації резервного копіювання гарантують швидке відновлення мережі після збою. Ефективні системи захисту від кібер-вірусів забезпечують безпеку мережі. Тестування обладнання перед розгортанням допомагає уникнути проблем, пов'язаних з неякісним обладнанням та програмним забезпеченням.

Мережеве обладнання відіграє важливу роль у забезпеченні ефективної комунікації, а його продуктивність безпосередньо пов'язана із якістю цієї комунікації. Це означає, що мережеве обладнання повинно мати достатню пропускну здатність і швидкість передачі даних. Оптимізована маршрутизація та управління трафіком відіграють ключову роль у забезпеченні ефективного використання мережевих ресурсів. Сюди входять й такі аспекти, як затримка і продуктивність обробки пакетів. Ефективне використання ресурсів і застосування

методів прискорення може допомогти максимізувати продуктивність обладнання та забезпечити стабільну роботу мережі.

Захист мережевого обладнання – складний процес, що вимагає комплексного підходу та уваги до деталей. Основна мета – захистити мережу від різних загроз, таких як несанкціонований доступ, зловмисні атаки та витік конфіденційної інформації. А це означає, що важливо використовувати різні механізми безпеки, такі як автентифікація, авторизація та шифрування даних. Автентифікація дозволяє підтвердити особу користувача, тоді як авторизація визначає права доступу до ресурсів. Шифрування даних є ключовим для забезпечення конфіденційності інформації, що передається мережею, та запобігання несанкціонованому доступу. Однак безпека мережевого обладнання включає не лише цифрові, але й фізичні аспекти. Наприклад, важливо забезпечити фізичну безпеку самого обладнання, щоб несанкціоновані особи не могли отримати фізичний доступ до нього. Регулярне оновлення програмного забезпечення та виправлення виявлених вразливостей також є важливими кроками. Паралельно з цим, моніторинг та виявлення загроз є ефективними для виявлення потенційних загроз та своєчасного реагування на них. Таким чином, забезпечення високого рівня безпеки мережевого обладнання є складним і багатогранним процесом, для успішної реалізації якого необхідне поєднання технічних, організаційних і людських ресурсів.

Керування мережевими пристроями схоже на роботу пілота в кабіні літака, який відповідає за те, щоб все працювало безперебійно та ефективно. Це включає в себе широкий спектр завдань, від налаштування пристроїв до моніторингу їхнього стану та відстеження різних показників продуктивності. Одним з найважливіших аспектів управління є застосування політик безпеки для забезпечення мережевої безпеки за допомогою брандмауерів, VPN тощо. Управління також включає автоматизацію процесів, що допомагає швидко реагувати на зміни та впроваджувати нові функції. Механізми резервного копіювання, за наявності, допомагають швидко відновити мережу у випадку збою. Загалом, ефективне управління мережевим обладнанням є запорукою успіху надійної мережі, яка відповідає потребам бізнесу та безпеки.

Сумісність мережевого обладнання – важливий аспект забезпечення його коректної роботи в мережевому середовищі та взаємодії з іншим обладнанням і компонентами. Для цього потрібно, щоб різні пристрої могли конектитись один з одним і працювати разом відповідно до загальних правил. Фізична сумісність означає, що різні пристрої мають сумісні роз'єми та інтерфейси для встановлення з'єднання один з одним. Сумісність програмного забезпечення дозволяє йому взаємодіяти з операційною системою пристрою та іншими програмами в мережі. Сумісність мережевих протоколів і стандартів гарантує, що пристрої правильно взаємодіють і обмінюються даними відповідно до встановлених правил і форматів. Забезпечення сумісності між пристроями має важливе значення для підтримки стабільної та ефективної роботи мережі, а також спрощує розгортання та управління мережевими компонентами.

Ефективне використання ресурсів мережевого обладнання є важливою стратегією для забезпечення оптимальної продуктивності та надійності. Це ефективний розподіл ресурсів, таких як пропускна здатність, обчислювальна потужність і пам'ять, для досягнення максимальної продуктивності при мінімальних витратах. Для досягнення цієї мети використовуються різні стратегії, включаючи віртуалізацію ресурсів, формування трафіку, оптимізацію трафіку, моніторинг та аналіз, а також оптимізацію мережевої архітектури. Такий підхід допомагає забезпечити ефективну та стабільну роботу мережі.

Ці принципи є ключовими для розгортання стабільної та надійної мережі, яка забезпечує оптимальну продуктивність і відповідає потребам користувачів. Розуміння і застосування цих принципів допоможе створити мережеве середовище, яке забезпечує надійний і ефективний зв'язок і обмін даними. [2]

До того ж, все мережеве обладнання можна розділити на пасивне та активне. Активне мережеве обладнання відповідає за управління потоком даних та перетворення сигналів і потребує живлення. До активного обладнання належать комутатори та маршрутизатори. Таке обладнання характеризується певним "інтелектом".

Рисунок 1.1 – Приклад активного обладнання(комутатор)

Пасивне обладнання не має "інтелекту" і не потребує живлення. Їхнє основне завдання – розподіляти сигнали та знижувати їхні рівні до необхідних значень. Пасивне обладнання має просту конструкцію і легко встановлюється в систему. До пасивного обладнання належать патч-панелі, розетки, оптичні розгалужувачі та кабельні системи. [1]

Рисунок 1.2 – Приклад пасивного обладнання(кабельні системи, розетки, оптичні розгалужувачі)

1.2 Поняття несправності в мережевому обладнанні

Збої в роботі мережевого обладнання можуть виникати з різних причин, що призводить до порушення нормальної роботи мережі та зниження її продуктивності. Це може бути викликано технічними проблемами, помилками програмного забезпечення, вірусами, зловмисними атаками, фізичними пошкодженнями або іншими аномаліями. Прикладами можуть бути втрата зв'язку, надмірна пропускна здатність, помилки протоколу, проблеми з безпекою та перебої в електропостачанні. Виявлення та виправлення таких несправностей є важливим для безперебійної роботи мережі та підтримки її ефективності. Для цього потрібен комплекс заходів з діагностики, моніторингу, аналізу, профілактики та безпеки.

Втрата зв'язку між пристроями в мережі може бути викликана різними факторами, починаючи від технічних проблем і закінчуючи програмними аномаліями. Наприклад, фізичні проблеми з підключенням, такі як пошкоджені кабелі або неправильно підключені роз'єми, можуть призвести до розриву зв'язку. Неправильна конфігурація пристрою або конфлікти мережевих протоколів також можуть спричинити збої зв'язку. Щоб своєчасно виявляти і вирішувати такі проблеми, необхідно систематично проводити моніторинг і аналіз мережі.

Наступна можлива причина несправностей – перевищення пропускної здатності мережі, що відбувається, коли обсяг переданої інформації перевищує пропускну здатність. Це може бути викликано низкою факторів, включаючи постійне зростання трафіку через збільшення кількості користувачів, додатків і сервісів, або погане планування мережі. Цій проблемі можна запобігти, якщо вжити таких заходів, як використання високошвидкісного обладнання, балансування навантаження та оптимізація трафіку. Також важливо регулярно відстежувати обсяги трафіку, передбачати потреби в пропускній здатності мережі та своєчасно реагувати на зростання обсягів даних.

Помилки мережевого протоколу також можуть спричинити низку проблем, включаючи переривання зв'язку, низьку продуктивність і перебої в роботі мережі.

Ці помилки можуть виникати з різних причин, починаючи від неправильної конфігурації протоколу і закінчуючи проблемами з пропускною здатністю і безпекою. Неправильно налаштовані параметри протоколу, такі як маршрутизація, налаштування VLAN і пропускної здатності, можуть призвести до конфліктів і проблем зі з'єднанням. Крім того, неоптимальне використання пропускної здатності може спричинити перевантаження мережі, помилки конфігурації – зациклення трафіку і переповнення, конфлікти IP-адрес і вразливості протоколів також можуть викликати проблеми, що призводять до втрати зв'язку і атак на мережеве обладнання. Для виявлення та усунення таких помилок важливо здійснювати моніторинг мережі, шукати аномалії та вживати заходів для запобігання їм у майбутньому. Також важливо постійно оновлювати програмне забезпечення та дотримуватися найкращих практик при налаштуванні мережевого обладнання.

Проблеми з електроживленням можуть становити серйозну загрозу для стабільності та надійності мережі. Вони можуть бути спричинені перебоями в електропостачанні, раптовими стрибками напруги, шумами на лініях електропередач або збоями у внутрішній електричній мережі. Наприклад, збій в електропостачанні може перервати живлення мережевого обладнання, що призведе до порушення зв'язку. Раптові стрибки напруги можуть пошкодити обладнання або спричинити його несправність. Аномальні сигнали на лініях електропередач можуть вплинути на якість живлення мережевого обладнання та викликати збої в роботі. Несправності у внутрішній електричній мережі, такі як перегрів проводів або перевантаження ланцюгів, також можуть спричинити збої живлення мережевого обладнання. Нарешті, несправна батарея в джерелі резервного живлення або неправильно налаштована система автоматичного резервування можуть призвести до втрати надійності мережі передачі в разі відключення електроенергії. Для забезпечення безперебійної роботи електромережі та підтримки її ефективності важливо виявляти та усувати несправності електропостачання. Для цього використовуються різні методи діагностики, моніторингу та аналізу, а також профілактичні та запобіжні заходи.

1.3 Штучний інтелект у сфері технічного обслуговування

Штучний інтелект (ШІ) широко використовується в технічному обслуговуванні для поліпшення діагностики, прогнозування несправностей, планування технічного обслуговування і ремонтів; ШІ можна використовувати для підвищення ефективності технічного обслуговування, скорочення часу простою обладнання і зниження витрат на ремонт і обслуговування. Він також може допомогти підвищити надійність і доступність обладнання, що має вирішальне значення для бізнес-процесів багатьох компаній.

Використання штучного інтелекту для прогнозування відмов мережевого обладнання є важливою стратегією підвищення надійності та безперервності мережевої інфраструктури. Машинне навчання та методи аналізу даних можна використовувати для завчасного прогнозування можливих відмов обладнання та вжиття заходів для запобігання або мінімізації їхнього впливу. Для досягнення цієї мети використовуються такі методи, як аналіз великих даних, категоризація пристроїв за ризиком несправностей, виявлення патернів аномалій та інтеграція з системами моніторингу. Підвищення ефективності управління мережею і зниження ризику в надзвичайних ситуаціях є основними перевагами такого підходу. [4]

Для усунення несправностей мережевого обладнання зі штучним інтелектом використовуються різноманітні методи машинного навчання та аналізу даних для виявлення, класифікації та прогнозування можливих проблем. Використання алгоритмів штучного інтелекту, таких як нейронні мережі та алгоритми класифікації, дозволяє автоматично аналізувати великі обсяги даних про стан мережі, трафік і поведінку пристроїв. Це дозволяє виявляти аномалії та потенційні проблеми, які можуть вплинути на продуктивність і надійність. Створення систем моніторингу, які автоматично аналізують дані і навчаються виявляти несправності, є одним з підходів до діагностики. Такі системи надають операторам мережі попередження про можливі несправності та рекомендації щодо вирішення проблем

до того, як це вплине на продуктивність або якість обслуговування. Штучний інтелект також може застосовуватися для вирішення конкретних діагностичних завдань, таких як виявлення несправностей в обладнанні та складних мережевих конфігураціях, прогнозування тривалості життя обладнання та розробка оптимальних стратегій технічного обслуговування і ремонту. Використання штучного інтелекту для діагностики несправностей може допомогти підвищити надійність, знизити витрати на обслуговування і поліпшити якість обслуговування користувачів мережі. [5]

Планування технічного обслуговування мережевого обладнання на основі штучного інтелекту є важливим кроком в управлінні мережею для оптимізації робочого процесу та забезпечення надійності. Штучний інтелект використовується для аналізу даних моніторингу стану обладнання та прогнозування потреб у технічному обслуговуванні; алгоритми ШІ можуть виявляти аномалії та прогнозувати ймовірність виходу обладнання з ладу, допомагаючи таким чином розробляти стратегії технічного обслуговування для запобігання збоїв. Штучний інтелект може планувати профілактичні заходи, визначати найкращий час для їх проведення та мінімізувати вплив на роботу мережі. Автоматизований аналіз даних дозволяє ефективно розподіляти мережеві ресурси і забезпечує оптимальну роботу. Штучний інтелект також допомагає оцінити операційний вплив запланованих змін у конфігурації мережі, що дозволяє приймати обґрунтовані рішення щодо впровадження змін. Прогнози навантаження і ресурсів дозволяють планувати розвиток мережі і вносити необхідні зміни заздалегідь. Використання штучного інтелекту для сервісного планування мережевого обладнання дозволяє підвищити ефективність управління мережею, забезпечити надійність і доступність мережевих сервісів, а також знизити витрати на обслуговування і ремонт. [6]

Автоматизація процесів обслуговування мережевого обладнання є важливим аспектом вдосконалення управління мережею за допомогою штучного інтелекту. Цей підхід використовується для автоматизації різних етапів обслуговування, від планування робіт до моніторингу та діагностики. Штучний інтелект може вирішувати такі завдання, як моніторинг та аналіз даних, виявлення та діагностика

несправностей, оптимізація ресурсів, прогнозування навантаження на мережу та автоматизоване управління. Ці методи допомагають підвищити ефективність і надійність мережевої інфраструктури. Одним з важливих аспектів автоматизації є можливість автоматичного реагування на мережеві аномалії та несправності, що дозволяє операторам своєчасно реагувати на потенційні проблеми та уникати відключень мережі. Штучний інтелект також використовується для автоматизації планування та виконання завдань з профілактичного обслуговування та ремонту, що допомагає забезпечити безперебійну роботу мережі та уникнути витрат через непередбачувані відключення. Загалом, автоматизація технічного обслуговування на основі штучного інтелекту виявилася ефективним інструментом для організацій, які бажають забезпечити ефективну та безперебійну роботу своїх мереж. [7]

Штучний інтелект відіграє важливу роль у розробці рекомендацій щодо усунення несправностей мережевого обладнання, що є важливим аспектом забезпечення безперебійної роботи мережі. Ці рекомендації ґрунтуються на використанні різних методів і підходів до аналізу даних і діагностики: першим кроком є розробка системи моніторингу та діагностики. Ці системи відстежують стан мережі та обладнання і використовують алгоритми штучного інтелекту для виявлення потенційних несправностей. Наступним важливим кроком є прогнозування несправностей. Це досягається за допомогою алгоритмів машинного навчання для прогнозування майбутніх відмов обладнання та розробки превентивних стратегій. Ще одним важливим аспектом є автоматичне виявлення та усунення несправностей. Системи можуть бути налаштовані на автоматичне виявлення проблем і надання рекомендацій щодо їх усунення або автоматичного виправлення. Щоб підвищити ефективність процесу усунення несправностей, важливо проаналізувати причину проблеми. Використовуйте штучний інтелект для аналізу даних і виявлення першопричин несправностей. Також важливо оптимізувати процес відновлення після усунення несправностей. Це включає автоматичне відновлення конфігурацій, балансування трафіку та інші операції. Нарешті, важливим аспектом є створення бази знань. Накопичуючи дані про несправності та їхнє усунення, можна створити базу знань для вдосконалення

систем ШІ та запобігання майбутнім проблемам. Всі ці аспекти допомагають ШІ підвищити ефективність і надійність мережевого обладнання, скорочуючи час, витрати і ризик збоїв.

Використання штучного інтелекту для прогнозування життєвого циклу обладнання в мережевій системі є важливим кроком у забезпеченні ефективного управління ресурсами та планування технічного обслуговування. У цьому процесі є кілька ключових етапів. Першим кроком є збір та аналіз історичних даних про життєвий цикл обладнання, включаючи дані про поломки, ремонт, технічне обслуговування та знос. Ці дані аналізуються за допомогою алгоритмів машинного навчання для виявлення закономірностей поведінки обладнання в часі. На основі зібраних даних розробляються прогнозні моделі, які можуть передбачити майбутні поломки та термін служби обладнання. Будуть розглянуті різні методи машинного навчання, включаючи нейронні мережі, дерева рішень і методи кластеризації. Важливим аспектом є врахування факторів впливу, таких як умови експлуатації, навантаження на мережу та робоче середовище. Це може зробити прогнози більш точними та адаптивними. Важливу роль у цьому процесі відіграє постійний моніторинг та оновлення моделі. Нові дані використовуються для постійного оновлення та вдосконалення моделі, а також для врахування змін в умовах експлуатації та технологіях. На основі прогнозів моделі розробляються стратегії планування ресурсів і технічного обслуговування, такі як ремонт і профілактичне обслуговування. Це дозволяє оптимізувати витрати та підтримувати надійність мережі на оптимальному рівні. [8]

1.4 Попередні дослідження та роботи в області виявлення та усунення несправностей

Результати попередніх досліджень і робіт в області діагностики несправностей мережевого обладнання показують, що досягнутий значний прогрес

у використанні різних методів і прийомів для підвищення надійності, доступності та продуктивності мережі. Ці дослідження охоплюють такі ключові аспекти: методи моніторингу та аналізу даних, спрямовані на збір та обробку інформації про стан мережі з метою виявлення потенційних проблем та аномалій; розробка алгоритмів для автоматизації процесу виявлення та прогнозування несправностей мережевого обладнання використання машинного навчання та аналітики даних; методів діагностики та прогнозування, заснованих на використанні інтелектуальних систем для виявлення причин збоїв і прогнозування потенційних майбутніх відмов; автоматизованого пошуку та усунення несправностей мережевого обладнання; підвищення надійності, доступності та продуктивності мережевого обладнання. використання різних методів і технологій для підвищення надійності, доступності та продуктивності мережевого обладнання.

У сфері усунення несправностей мережевого обладнання існують різні методи моніторингу та аналізу даних, спрямовані на ефективне виявлення та вирішення проблем. Дослідницькі зусилля зосереджені на розробці алгоритмів та інструментів, які контролюють стан мережевого обладнання та аналізують зібрані дані для виявлення аномалій і прогнозування можливих збоїв. Ці методи включають моніторинг різних компонентів обладнання, використання журналів подій для виявлення аномальної поведінки, моніторинг мережевого трафіку, використання датчиків і систем Інтернету речей, а також застосування методів штучного інтелекту і машинного навчання для аналізу великих обсягів даних і прогнозування несправностей. Окремо або в поєднанні ці методи можна використовувати для ефективного моніторингу та аналізу мережевого обладнання, а також для виявлення та усунення потенційних несправностей. [9]

Дослідження в галузі усунення несправностей мережевого обладнання зосереджені на розробці та вдосконаленні методів машинного навчання та аналізу даних. Ці методи спрямовані на автоматизацію процесу виявлення та вирішення проблем у мережевих системах. Використання таких підходів має важливе значення для підвищення надійності та ефективності мережевих інфраструктур. Ключові напрямки досліджень включають класифікацію несправностей на основі

алгоритмів машинного навчання, прогнозування несправностей обладнання на основі аналізу великих даних, виявлення аномалій мережевого обладнання, планування технічного обслуговування з використанням моделей машинного навчання, а також аналіз журналів подій і системних параметрів. Дослідження в цій галузі спрямовані на створення надійних та ефективних інструментів для автоматичного моніторингу, виявлення та усунення несправностей мережевого обладнання для забезпечення більш стабільної та продуктивної роботи мережевих систем. [10]

Методи діагностики та прогнозування, засновані на машинному навчанні та аналізі даних, активно досліджуються в галузі усунення несправностей мережевого обладнання. Метою даного дослідження є розробка ефективних методів виявлення та вирішення проблем мережевих систем. Використання таких підходів є ключовим для забезпечення стабільності та продуктивності мережевих інфраструктур. Різноманітні діагностичні та прогностичні методи виявлення несправностей мережевого обладнання дозволяють ефективно виявляти, аналізувати та вирішувати проблеми. Вони включають моніторинг стану обладнання, аналіз журналів подій, використання датчиків і детекторів, прогнозування несправностей, виявлення аномалій і аналіз даних мережевого трафіку. Ці методи дозволяють розробляти стратегії запобігання несправностям і ефективно контролювати стан мережевого обладнання. [11]

Дослідження в галузі автоматизації процесів пошуку та усунення несправностей в мережевому обладнанні активно розвивають автоматизовані системи, які використовують методи штучного інтелекту для управління та усунення проблем. Цей напрямок включає в себе цілий ряд інструментів і методів, спрямованих на швидке і ефективне виявлення, діагностику та усунення несправностей. Системи моніторингу та управління можуть автоматично виявляти аномалії, повідомляти адміністратора про проблему, виконувати автоматичні дії для вирішення проблеми або запускати сценарії відновлення. Використання системи віддаленого управління обладнанням дозволяє здійснювати дистанційну діагностику та управління мережевим обладнанням, навіть у разі несправності

ключового каналу зв'язку. Автоматизована діагностика і виправлення помилок передбачає розробку програм і скриптів, які самостійно виявляють і усувають типові несправності без участі адміністраторів. Крім того, використання автоматизованих систем для планування та виконання регламентних робіт спрощує процес резервного копіювання, оновлення програмного забезпечення та інших процедур технічного обслуговування. Автоматизоване відновлення послуг дозволяє швидко та ефективно реагувати на несправності та проблеми, наприклад, автоматично перенаправляти трафік у разі виходу з ладу первинної лінії зв'язку. Інтелектуальні системи управління з використанням штучного інтелекту та аналізу даних забезпечують автоматичне усунення несправностей та оптимізацію роботи мережевого обладнання. [12]

Дослідження в області інтелектуальних систем управління мережевим обладнанням (ІСУМО) спрямовані на створення систем, здатних адаптуватися до мінливих умов, виявляти і усувати несправності. Використання штучного інтелекту та автоматизації спрямоване на покращення продуктивності мережі, забезпечення високої доступності, підвищення ефективності та забезпечення безпеки. Основні аспекти та принципи ІСУМО включають моніторинг та аналіз стану мережі, автоматизоване управління трафіком, виявлення та усунення несправностей, оптимізацію ресурсів, мережеву безпеку та інші. Дослідження в цій галузі спрямовані на розробку інтелектуальних алгоритмів і методів, які дозволяють системам управління мережевим обладнанням приймати розумні та оптимальні рішення. [13]

РОЗДІЛ 2. ДОСЛІДЖЕННЯ ІСНУЮЧИХ МЕТОДІВ ВИЯВЛЕННЯ НЕСПРАВНОСТЕЙ В МЕРЕЖЕВОМУ ОБЛАДНАННІ З ВИКОРИСТАННЯМ ШТУЧНОГО ІНТЕЛЕКТУ

2.1 Аналіз існуючих методів виявлення несправностей в мережевому обладнанні

Аналіз існуючих методів виявлення несправностей в мережевому обладнанні важливий для забезпечення стабільності та надійності роботи мережі. Розглянемо деякі з найпоширеніших методів.

Метод моніторингу мережі використовує спеціальне програмне забезпечення для безперервного моніторингу стану мережевої інфраструктури. Цей метод дозволяє системі моніторингу автоматично виявляти аномалії та проблеми, які можуть виникнути в мережі. Відстежуючи різні параметри мережі, такі як пропускна здатність, втрата пакетів і затримка даних, програмне забезпечення може швидко виявляти проблеми і надавати інформацію мережевому менеджеру для подальшого аналізу і виправлення. Цей метод є ключовим для підтримки стабільної та ефективної мережевої інфраструктури, оскільки він може швидко реагувати на будь-які проблеми та забезпечувати безперебійну передачу даних.

Тестування зв'язку – це метод, який використовується для перевірки стабільності та ефективності зв'язку між різними вузлами мережі. Процес використовує спеціальні інструменти для об'єктивної оцінки якості з'єднання та виявлення можливих проблем. Тестування зв'язку активно завантажує вузли мережі та перевіряє наявність таких проблем, як перервані з'єднання, заблоковані мережеві шляхи та фізичні або логічні збої. Процес включає в себе надсилання пакетів даних між вузлами та аналіз відповідей для визначення часу відгуку, втрати пакетів і стабільності з'єднання. Тестування з'єднання допомагає виявити потенційні проблеми мережі та вжити відповідних заходів для їх вирішення. Таким

чином, мережеві адміністратори можуть підвищити надійність мережі та забезпечити безперебійну передачу даних між вузлами. [14]

SNMP (Simple Network Management Protocol – простий протокол керування мережею) – це стандарт, який використовується для моніторингу та керування мережевим обладнанням. SNMP дозволяє мережевим адміністраторам віддалено контролювати мережеве обладнання та керувати ним з централізованої системи управління мережею (NMS). (NMS) для віддаленого моніторингу та керування мережевим обладнанням. Аналізуючи ці дані, можна виявити потенційні проблеми і вжити відповідних заходів. Використовується як інструмент для моніторингу та діагностики мережевих пристроїв в різних комп'ютерних мережах, включаючи локальні мережі, корпоративні мережі та глобальні мережі. [15]

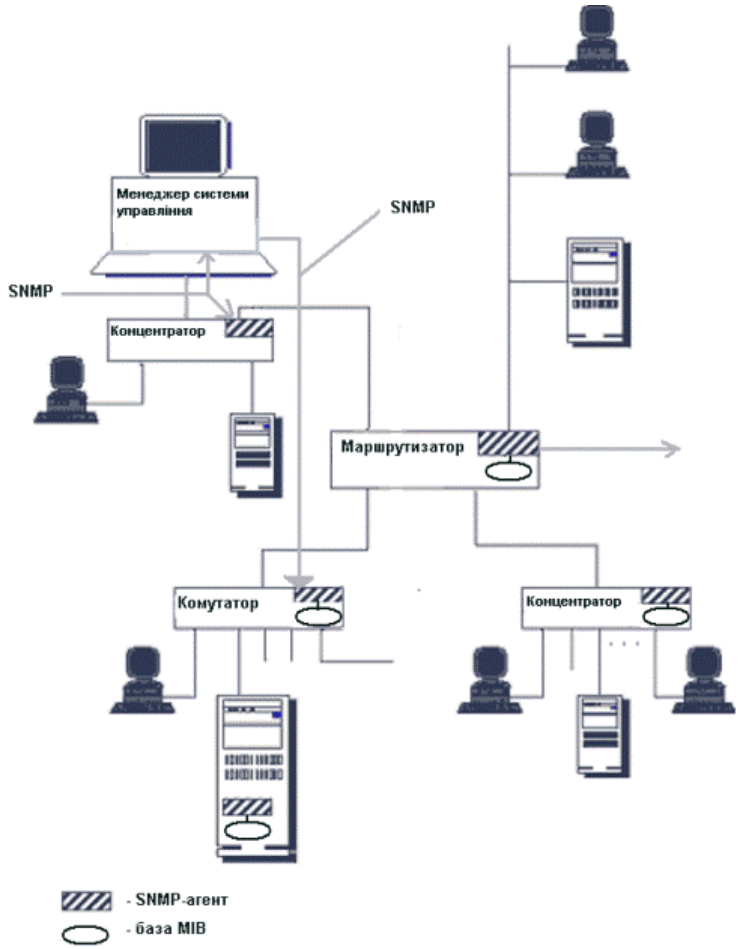


Рисунок 2.1 – Типова структура системи управління

Використання тривог і автоматичних повідомлень є важливою складовою систем моніторингу та управління мережевим обладнанням. Цей метод передбачає налаштування системи оповіщення, яка автоматично виявляє проблеми та

аномальні стани в мережевому обладнанні та надсилає повідомлення менеджерам і відповідальним особам для подальшого аналізу та вирішення. Системи оповіщення можуть бути налаштовані на виявлення різних типів проблем, таких як перевищення максимально допустимих значень параметрів, втрата зв'язку з певним обладнанням, недоступність послуг та інші незвичайні події. При виникненні таких подій система автоматично генерує тривоги і надсилає повідомлення адміністратору різними каналами зв'язку, такими як електронна пошта, SMS, спеціальні додатки та інші засоби зв'язку. Таким чином, проблеми з мережевим обладнанням можна швидко виявити і вжити заходів, скоротивши час простою мережі і підтримуючи стабільність і надійність мережевої інфраструктури завдяки швидкому вирішенню проблем. [16]

Аналіз журналів подій є важливою складовою систем моніторингу та діагностики мережевого обладнання. Цей метод передбачає систематичне вивчення журналів подій, в яких зберігається інформація про всі події та дії, що відбуваються на мережевому обладнанні. Аналізуючи журнали подій, можна виявити різні аномалії, помилки і попередження, які вказують на проблеми з мережевим обладнанням. До них відносяться операційні помилки, відмова в обслуговуванні, мережеві атаки, незвичайна активність або інші події, що вказують на переривання нормальних режимів роботи. Для ефективного аналізу журналів подій часто використовують спеціалізовані програмні засоби, що дозволяють автоматизувати процес збору, фільтрації та аналізу даних журналів. Такі інструменти допомагають виявити і класифікувати різні проблеми і ризики, які можуть виникнути в мережевому середовищі. Аналіз журналів подій є важливим кроком у забезпеченні безпеки, надійності та ефективності мережевої інфраструктури. Це дозволяє швидко виявляти і вирішувати потенційні проблеми, скорочуючи час простою мережі і забезпечуючи її стабільну роботу. [17]

Спосіб використання машинного навчання та аналізу даних в контексті мережевої інфраструктури полягає в застосуванні різних алгоритмів машинного навчання для аналізу великих обсягів даних, зібраних з мережі. Метод спрямований на виявлення несправностей, аномалій і небезпечних ситуацій, які можуть

виникнути в мережевому середовищі. Алгоритми машинного навчання використовуються для автоматизації аналізу та обробки великих обсягів структурованих і неструктурованих даних, включаючи інформацію про трафік, стан мережевого обладнання, журнали подій та інші параметри мережі. Цей метод дозволяє системам моніторингу та управління мережею виявляти закономірності та залежності в даних, що може допомогти виявити аномальну активність або незвичну поведінку в мережі. Наприклад, алгоритми машинного навчання можуть виявляти аномальні мережеві пакети, аномальне використання ресурсів, мережеві атаки та інші потенційно небезпечні події. Однією з головних переваг цього підходу є його здатність до самонавчання та адаптації до змін у мережевому середовищі. Моделі машинного навчання можна вдосконалювати та оптимізувати з часом на основі нових даних та досвіду. [18]

Комплексний моніторинг та усунення несправностей мережевого обладнання стає все більш важливим питанням у сучасному технологічному середовищі. У цьому контексті використання різних методів є ефективним підходом. Оскільки кожен з цих методів має свої переваги і обмеження, важливо вибрати метод, який найкраще відповідає конкретним потребам і характеристикам мережевої інфраструктури. Комбінація цих методів може бути використана для більш ефективного і надійного моніторингу та усунення несправностей мережевого обладнання.

2.2 Використання штучного інтелекту для виявлення несправностей

Використання штучного інтелекту (ШІ) для виявлення несправностей в мережевому обладнанні відкриває можливості автоматизації та оптимізації процесу діагностики і вирішення проблем.

Аналіз великих даних за допомогою штучного інтелекту є важливою складовою сучасних систем моніторингу мережевого обладнання. Цей підхід

дозволяє обробляти великі обсяги інформації з різних джерел, включаючи моніторинг стану мережі, журнали подій і дані датчиків. Штучний інтелект використовується для автоматизації аналізу цих даних з метою виявлення аномалій і несправностей, які важко виявити неозброєним оком або традиційними методами. Цей процес аналізу великих обсягів даних вимагає використання різних алгоритмів машинного навчання, таких як класифікація, кластеризація, аналіз правил асоціацій і глибоке навчання ШІ може автоматично виявляти складні закономірності в даних і встановлювати зв'язки між різними параметрами мережі. встановлювати, таким чином допомагаючи виявити проблеми на ранній стадії. Прикладом такого підходу є аналіз журналів подій мережевого обладнання для виявлення незвичних змін у поведінці системи, які вказують на проблему або можливу загрозу безпеці. Інший приклад - аналіз даних мережевого трафіку для виявлення незвичайних патернів, що вказують на атаки або несправності в мережі. [19]

Машинне навчання – це галузь штучного інтелекту, яка використовує алгоритми та статистичні моделі, щоб робити припущення на основі великих обсягів даних і навчати системи покращувати їх без явного програмування. У контексті управління мережею машинне навчання використовується для аналізу структури мережі та виявлення аномалій, відхилень і потенційних несправностей. Такий підхід дозволяє системі автоматично виявляти несправності та аномалії, які можуть свідчити про проблеми з мережевим обладнанням або інфраструктурою. Наприклад, алгоритми машинного навчання можуть аналізувати дані про трафік, стан інтерфейсу, завантаження процесора та інші показники для виявлення несправностей у режимі реального часу. Крім того, машинне навчання можна використовувати для прогнозування можливих несправностей і планування профілактичних заходів. Алгоритми можуть аналізувати історичні дані про несправності та стан мережі, виявляти закономірності, які можуть передувати несправності, і вживати відповідних заходів, щоб уникнути несправності. Машинне навчання може автоматизувати процес аналізу та управління мережею, скорочуючи час і зусилля, необхідні для виявлення проблем, й забезпечуючи надійність мережевого обладнання. [20]

Розпізнавання образів – це метод, який використовується у штучному інтелекті для виявлення спільних рис або шаблонів у даних. У контексті управління мережею цей підхід використовується для аналізу мережевого трафіку і поведінки пристроїв з метою виявлення потенційних несправностей. Алгоритми розпізнавання образів можуть автоматично виявляти загальні закономірності, які вказують на ненормальну або нерегулярну активність у мережі. Наприклад, вони можуть виявити надмірне використання пропускної здатності, несподівані зміни в поведінці пристроїв або інші відхилення від типових мережевих шаблонів. Такий підхід дозволяє системам моніторингу автоматично виявляти потенційні проблеми без необхідності ручного аналізу великих обсягів даних. Розпізнавання шаблонів уможливлює швидке та ефективне усунення несправностей мережі, що дозволяє швидко вирішувати потенційні проблеми, забезпечуючи безперебійну роботу мережевого обладнання. [21]

Системи самонавчання – це розробка інтелектуальних систем, здатних навчатися на нових даних і досвіді з метою виявлення несправностей в мережевому обладнанні. Такий підхід дозволяє системі адаптуватися до мінливих умов і отримувати більш точні та актуальні результати виявлення проблем. Системи самонавчання базуються на алгоритмах машинного навчання, таких як нейронні мережі, глибокі нейронні мережі, алгоритми класифікації та кластеризації даних. Ці системи використовують нові дані про стан мережі та досвід раніше виявлених несправностей для покращення своєї роботи та точності виявлення проблем. Основною перевагою систем, що самонавчаються, є їх здатність адаптуватися до нових ситуацій і отримувати більш точні результати з часом. Системи, що самонавчаються, можуть автоматично виявляти нові типи несправностей і аномальну активність. [22]

Прогнозування відмов – це процес використання методів інтелектуального аналізу даних на основі історичних даних для визначення ймовірності відмов мережевого обладнання та розробки стратегій запобігання цим проблемам. Цей метод використовується для прогнозування можливих відмов або несправностей мережевого обладнання на основі аналізу минулих інцидентів та їх характеристик.

Шляхом обробки великої кількості історичних даних про несправності, включаючи дату, час, тип проблеми, параметри обладнання та інші фактори, можна розробити прогнозні моделі для оцінки ймовірності виникнення подібних проблем у майбутньому. Прогнозування відмов важливо для менеджерів мережі Це пов'язано з тим, що воно дозволяє їм вживати превентивних заходів для уникнення потенційних проблем і гарантувати, що мережа залишається працездатною. [23]

Автоматизоване прийняття рішень – це процес розробки систем, які можуть автоматично аналізувати дані та вживати відповідних заходів для усунення несправностей мережевого обладнання без необхідності втручання людини. Метод заснований на використанні штучного інтелекту, машинного навчання та алгоритмів автоматизації для автоматичного аналізу даних про стан мережі та реагування на виявлені аномалії та проблеми. Автоматизовані системи прийняття рішень можуть бути реалізовані в програмному забезпеченні та інтегровані в систему управління мережею (NMS) або безпосередньо в мережеве обладнання. Такий підхід дозволяє системі автоматично вживати заходів для вирішення проблем без затримок, які можуть виникнути при втручанні людини, тим самим скорочуючи час реагування на проблеми і уникаючи потенційних збоїв. [24]

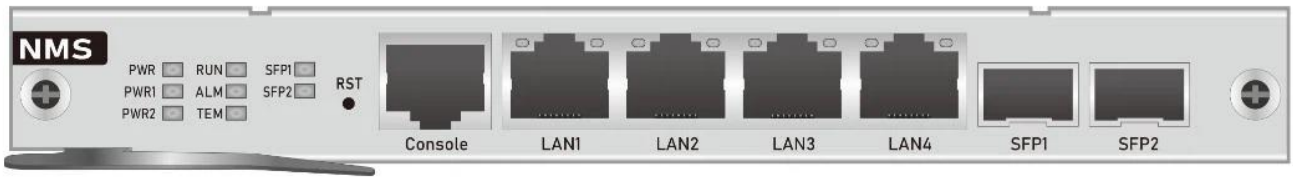


Рисунок 2.2 – NMS (Система Керування Мережею)

Використання штучного інтелекту (ШІ) для виявлення несправностей в мережевому обладнанні відкриває можливість більш точного і швидкого реагування на проблеми, що призводить до скорочення часу простою мережі, підвищення надійності і поліпшення якості обслуговування користувачів. Завдяки такому підходу системи моніторингу мережі можуть автоматично виявляти аномалії і несправності швидше, ніж це може зробити людина, аналізуючи великі обсяги даних і використовуючи розуміння мережевих патернів. Це дозволяє операторам мереж швидше реагувати на проблеми і вживати необхідних заходів

для їх вирішення, що, в свою чергу, зменшує час простою мережі і підвищує загальну ефективність мережі. Більш точне і швидке реагування на проблеми також може допомогти підвищити надійність мережі. Це пов'язано з тим, що можливість автоматичного виявлення та усунення несправностей означає, що в разі виникнення критичної проблеми можна уникнути значних витрат часу і ресурсів. Крім того, забезпечення кращого користувацького досвіду допомагає підтримувати задоволеність клієнтів і підвищує конкурентоспроможність операторів на ринку. [25]

2.3 Методи усунення несправностей з використанням штучного інтелекту

Використання штучного інтелекту для усунення несправностей мережевого обладнання може охоплювати широкий спектр стратегій і методів, спрямованих на ефективне і автоматизоване вирішення проблем. Ці методи включають в себе не тільки інструменти для пошуку несправностей, але і різні підходи до вирішення проблем, завдяки чому проблеми можуть бути вирішені швидко, а час і ресурси не витрачаються даремно. Системи штучного інтелекту можуть реалізовувати методи автоматичного виявлення аномалій мережевого трафіку і програмного забезпечення, а також механізми автоматичного ремонту на основі заздалегідь визначених алгоритмів і сценаріїв. Крім того, такі системи можуть використовувати методи машинного навчання для адаптивного вдосконалення алгоритмів у режимі реального часу на основі нових даних і досвіду; підходи на основі ШІ можуть розробляти ймовірнісні моделі для прогнозування можливих збоїв, щоб можна було вжити превентивних заходів вжити превентивних заходів до того, як виникне несправність, зменшуючи вплив негативних подій на продуктивність мережі. Цей підхід також включає аналіз журналів подій і статистичні методи для виявлення закономірностей збоїв і їх взаємозв'язку з різними факторами.

Розробка автоматизованих систем управління несправностями - це створення програмних засобів, які можуть спонтанно реагувати на виявлені аномалії та проблеми мережевого обладнання без втручання людини. Ці системи дозволяють враховувати виявлені несправності, застосовувати відповідні процедури і автоматично виконувати необхідні дії для вирішення проблеми. Спеціалізовані програмні рішення, що відповідають за автоматичне управління несправностями, можуть бути налаштовані на виявлення широкого спектру проблем, від перевантаження мережі до конкретних аномалій в окремих пристроях. При виявленні несправностей ці системи можуть автоматично визначити причину і вжити відповідних заходів для вирішення проблеми. Завдяки автоматизованим системам управління несправностями більшість рутинних завдань, пов'язаних з діагностикою та усуненням проблем, можна виконувати без втручання людини. Це значно скорочує час реагування в разі виникнення проблеми і дозволяє підтримувати мережеве обладнання в робочому стані з мінімальними людськими ресурсами. Такі системи також можуть зберігати дані про виявлені несправності для подальшого аналізу та вдосконалення процесів усунення несправностей. [26]

Системи самодіагностики є важливим елементом забезпечення надійності та ефективності мережевого обладнання, й ІТ-індустрія гостро потребує розробки алгоритмів, здатних виявляти та ідентифікувати несправності в самому обладнанні. Ці системи використовують різні методи, включаючи перевірку працездатності обладнання, аналіз робочих параметрів, моніторинг мережевого трафіку та виявлення аномальних патернів. Ці алгоритми дозволяють обладнанню реагувати на проблеми в режимі реального часу, підвищуючи надійність мережі та скорочуючи час простою. При виявленні несправності система може вжити відповідних заходів для її усунення, наприклад, автоматично перезапустити операції, надіслати повідомлення адміністратору або виконати програмовані дії для резервного копіювання обладнання.

Розробка та впровадження саморегулюючих систем передбачає створення технологічних рішень, які дозволяють системам автоматично адаптуватися до різних умов і змін у навколишньому середовищі. Ці системи мають здатність не

лише виявляти можливі проблеми та відхилення, а й надавати автоматизовані відповіді на них, щоб забезпечити безперебійне функціонування без необхідності втручання оператора. Такий підхід сприяє оптимізації процесів управління мережею, зменшенню часу простою та підвищенню рівня надійності мережевих систем. Він дозволяє системам оперативно реагувати на зміни у середовищі та забезпечувати ефективне функціонування, що відповідає вимогам сучасних високотехнологічних мереж.

Прогностичний аналіз – це використання даних про минулі події та застосування методів прогнозування для оцінки ймовірності майбутніх подій. В контексті управління мережею це означає аналіз історичних даних про несправності, переривання і відмови мережевого обладнання для прогнозування подібних ситуацій в майбутньому. Аналізуючи ці дані і використовуючи відповідні алгоритми прогнозування, можна визначити ймовірність виникнення певної несправності або відмови в мережі. Після визначення цих ймовірностей можна вжити превентивних заходів для вирішення потенційних проблем. Профілактичні заходи включають проактивне обслуговування обладнання, розгляд можливості модернізації або заміни мережевих елементів і впровадження додаткових заходів безпеки. Такий предиктивний аналіз дозволяє менеджерам мережі заздалегідь передбачити і підготуватися до потенційних проблем, тим самим зменшуючи час простою мережі і підвищуючи її надійність.

Кореляційний аналіз – це метод, який використовується для виявлення взаємозв'язків між різними параметрами мережі та визначення причинно-наслідкових зв'язків, які можуть призвести до несправностей або проблем. Аналіз ґрунтується на спостереженні за змінами одного параметра і їх можливим впливом на інші параметри мережі. Кореляційний аналіз розглядає взаємозв'язок між різними факторами, такими як пропускна здатність, навантаження на мережу і час відгуку. Потім він розглядає, як зміна одного з цих параметрів впливає на інші. Наприклад, збільшення навантаження на мережу може призвести до зниження швидкості передачі даних або збільшення часу відгуку. Виявивши такі взаємозв'язки, мережеві менеджери можуть бути попереджені про потенційні

проблеми і вжити коригувальних заходів, що зменшить час простою мережі і забезпечить більш ефективну роботу.

Системи попередження про несправності – це програмні або апаратні засоби, розроблені та впроваджені для прогнозування можливих несправностей мережевого обладнання та надання операторам мережі своєчасної інформації про ці проблеми з метою запобігання серйозних наслідків. Ці системи аналізують різні параметри мережі, такі як пропускна здатність, час відгуку і навантаження на обладнання, щоб виявити зміни, які вказують на можливу несправність. Наприклад, збільшення часу відгуку або зменшення пропускної здатності вказує на можливу проблему в мережі. При виявленні таких змін система попередження про несправності надсилає певні повідомлення або сигнали оператору мережі, який може вжити відповідних заходів для запобігання серйозним проблемам. Це може включати перевірку обладнання, коригування параметрів мережі або, де це можливо, автоматичне усунення несправностей. Такі системи дозволяють операторам реагувати на проблеми до того, як вони призведуть до серйозного зниження продуктивності або недоступності мережі, а також підтримувати стабільність і ефективність мережі в умовах непередбачуваних подій.

2.4 Етапи виявлення та усунення несправностей

Несправне мережеве обладнання може спричинити серйозні проблеми, в тому числі зниження продуктивності, втрату даних і перерву в роботі. Однак досягнення в галузі штучного інтелекту і технологій аналізу даних відкрили нові можливості для виявлення і усунення несправностей мережевого обладнання. Використання штучного інтелекту дозволило розробити системи, які не тільки виявляють аномалії та несправності, але й автоматизують процес усунення

несправностей, дозволяючи швидше реагувати на проблеми та мінімізувати час простою мережі. Тому опишемо основні етапи усунення несправностей мережевого обладнання за допомогою штучного інтелекту. Розглянемо кожен етап, а також визначимо ключові аспекти та методи, що використовуються для забезпечення оптимального функціонування такої системи. [27]

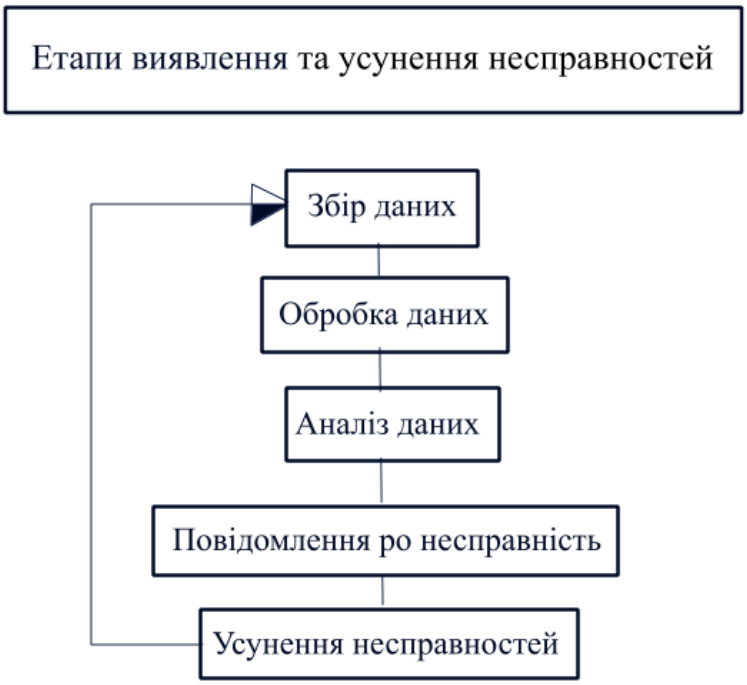


Рисунок 2.3 – Етапи усунення несправностей

На першому етапі усунення несправностей мережевого обладнання система збирає дані. Це важливий крок в отриманні інформації про стан різних аспектів мережі та її обладнання. Система збирає різноманітні дані, включаючи стан інтерфейсу, використання ресурсів, активність користувачів і журнали подій. Ці дані можуть бути зібрані з різних джерел, таких як простий протокол управління мережею (SNMP), який дозволяє контролювати і керувати мережевими пристроями, а також системи моніторингу, які виявляють і записують мережеву активність. Збір даних є фундаментальним етапом, оскільки якість і кількість отриманих даних визначає ефективність подальшого аналізу і прийняття рішень системою. Завдяки систематичному збору та зберіганню різних типів інформації система готується до наступного етапу аналізу та виявлення можливих несправностей мережевого обладнання.

Після дані обробляються. Цей процес включає низку важливих операцій, спрямованих на підготовку даних для подальшого аналізу. По-перше, дані фільтруються для перевірки на наявність аномалій, помилок і непотрібної інформації, яка може спотворити результати аналізу. Далі відбувається агрегація, коли великі обсяги даних групуються за певними параметрами або об'єднуються для полегшення подальшого аналізу. Потім проводиться нормалізація для забезпечення однорідності масштабу, одиниць виміру та формату даних. Це уніфікує дані і робить їх придатними для подальшого порівняння та аналізу. Нарешті, дані можуть бути перетворені або оброблені, наприклад, із застосуванням математичних і статистичних методів, для того, щоб витягти корисну інформацію. Загалом, обробка даних є важливим етапом в усуненні несправностей мережевого обладнання. Це пов'язано з тим, що вона допомагає забезпечити точність, чистоту і надійність даних, що має вирішальне значення для ефективного функціонування системи пошуку та усунення несправностей.

Наступний етап - аналіз даних. На цьому етапі використовуються алгоритми машинного навчання та інтелектуального аналізу даних для виявлення аномалій і відхилень від нормальних патернів, які можуть свідчити про несправності в мережевому обладнанні. У цьому процесі використовуються різноманітні методи, включаючи класифікацію, кластеризацію та аналіз часових рядів. Алгоритми машинного навчання використовуються для того, щоб система могла вчитися на історичних даних і розрізняти типові та аномальні моделі поведінки. Наприклад, методи класифікації можуть визначити, чи належить певна подія до типового режиму роботи, чи є аномальною. Кластерний аналіз дозволяє згрупувати події за схожістю і виявити незвичайні патерни або несправності, які можуть бути приховані в загальних даних. Аналіз часових рядів може виявити аномалії на основі змін у часі певних параметрів мережі, таких як швидкість передачі даних або навантаження на обладнання. Ці методи можуть допомогти системам виявити підозрілі зміни і швидко та ефективно відреагувати на них. Як правило, цей етап, на якому використовуються алгоритми машинного навчання та аналізу даних, є ключовим при усуненні несправностей мережевого обладнання. Це пов'язано з тим,

що аномалії можна виявити і відреагувати на них безпосередньо і автоматично, забезпечуючи таким чином ефективну роботу мережі.

При виявленні несправності система автоматично генерує повідомлення або оповіщення, що містить інформацію про виявлену аномалію. Ці повідомлення можуть бути надіслані адміністратору мережі або оператору мережі для подальшого аналізу та усунення несправностей. Повідомлення можуть містити інформацію про тип і характер несправності, а також інформацію про час і місце виникнення проблеми в мережі. Це дозволяє операторам мереж швидко реагувати на виявлені проблеми та вживати відповідних заходів для їх вирішення. Крім того, система може надавати додаткові рекомендації щодо можливих дій для вирішення проблеми або, де це можливо, автоматично запускати процес усунення несправностей. Це забезпечує ефективне та швидке реагування на проблеми та скорочує час, необхідний для їх вирішення, підвищуючи таким чином доступність та надійність мережі.

Після цього настає час для автоматичного або рекомендованого усунення несправностей. На цьому етапі після виявлення несправності система може автоматично вжити заходів для її усунення або надати рекомендації щодо подальших дій оператору мережі. У разі автоматичного усунення несправностей система може вжити необхідних заходів без втручання оператора мережі. Це включає, наприклад, перезапуск обладнання, переналаштування параметрів або автоматичне видалення несправного обладнання з мережі. Автоматичне усунення несправностей вирішує нові проблеми швидко і ефективно, зменшуючи необхідність втручання оператора мережі. У разі предиктивного усунення несправностей система надає оператору мережі конкретні рекомендації щодо подальших дій для вирішення проблеми. Це можуть бути, наприклад, інструкції щодо виконання певних операцій або перевірки певних параметрів. Оператори мережі можуть використовувати ці рекомендації для ефективного та швидкого усунення несправностей і підтримки належного функціонування мережі. Обидва підходи сприяють підвищенню ефективності та надійності мережі і зменшенню часу простою, що, в свою чергу, покращує загальну продуктивність і якість

обслуговування користувачів.

Нарешті, після усунення несправностей система продовжує моніторинг мережі, щоб перевірити ефективність контрзаходів і виявити нові аномалії та несправності. Моніторинг стану мережі безперервно відстежує різні параметри мережевого обладнання, такі як пропускна здатність, використання ресурсів і завантаження каналів передачі даних. Система безперервно перевіряє ці параметри та аналізує дані, щоб виявити будь-які незвичні ознаки потенційних проблем або збоїв. Перевірка та моніторинг дозволяє системі керувати станом мережі після усунення несправностей і негайно реагувати на подальші відхилення. Це важливо для забезпечення безперебійного функціонування мережі та надання якісних послуг користувачам. Крім того, моніторинг дозволяє системі визначати ефективність заходів з усунення несправностей і вносити будь-які необхідні корективи в стратегію управління мережею, щоб максимізувати продуктивність і надійність.

РОЗДІЛ 3. ПОРІВНЯЛЬНИЙ АНАЛІЗ МЕТОДІВ УСУНЕННЯ НЕСПРАВНОСТЕЙ З ВИКОРИСТАННЯМ ШТУЧНОГО ІНТЕЛЕКТУ

3.1 Оцінка ефективності методів усунення несправностей з використанням штучного інтелекту

Оцінка ефективності методів усунення несправностей на основі ШІ є важливим кроком на шляху до підвищення надійності та продуктивності мережевого обладнання. З цією метою використовуються різні метрики та методи оцінки для визначення ефективності виявлення, усунення та попередження несправностей. [28]

У сучасних мережевих інфраструктурах використання штучного інтелекту для усунення несправностей має вирішальне значення. Розглянемо деякі способи використання цього підходу й порівняємо їх за точністю виявлення несправностей.

Системи машинного навчання для виявлення аномалій мають високу чутливість до несправностей, але можуть страждати від хибнопозитивних або хибнонегативних результатів, залежно від якості моделі та даних. Системи самодіагностики, з іншого боку, мають високу специфічність, але їхня ефективність залежить від точності власних алгоритмів виявлення несправностей. Системи автоматичного прийняття рішень і запобігання несправностям також можуть мати високу чутливість і специфічність при правильному налаштуванні, але їх ефективність залежить від якості прогнозуючих моделей і алгоритмів усунення несправностей. Загалом, вибір методів усунення несправностей на основі ШІ повинен ґрунтуватися на характеристиках конкретної мережевої інфраструктури та якості вхідних даних.

Для деяких систем важлива можливість усунення несправностей у режимі реального часу. Оцінка продуктивності системи в режимі реального часу допомагає переконатися, що система ефективно функціонує в реальних мережевих умовах.

Системи машинного навчання мають обмежену продуктивність в реальному часі, оскільки їм потрібно обробляти великі обсяги даних і виконувати складні обчислення. Вони також потребують значних обчислювальних ресурсів і часу для навчання моделей і аналізу даних, що може ускладнити їх використання в реальному часі. Системи самодіагностики, вбудовані безпосередньо в обладнання, зазвичай забезпечують високу продуктивність в режимі реального часу. Вони можуть негайно реагувати на виявлення несправностей і виконувати діагностику в польових умовах без затримок. Автоматизоване прийняття рішень також ефективне в режимі реального часу, особливо якщо воно базується на заздалегідь визначених алгоритмах і правилах пошуку та усунення несправностей. Однак ефективність такого підходу може залежати від складності та глибини аналізу, який необхідно виконати для прийняття правильних рішень в режимі реального часу. На закінчення важливо відзначити, що кожен з розглянутих методів має свої переваги і обмеження з точки зору продуктивності в реальному часі. Системи самодіагностики та автоматизованого прийняття рішень можуть бути ефективними в режимі реального часу, оскільки вони негайно реагують на виявлення несправностей, тоді як системи машинного навчання можуть вимагати більше обчислювальних ресурсів і часу для аналізу даних. Найбільш ефективний метод слід обирати, виходячи з конкретних потреб і обмежень мережевої інфраструктури.

Системи машинного навчання, системи самодіагностики та автоматизованого прийняття рішень мають різні витрати на інтеграцію та експлуатацію. Інтеграція систем машинного навчання є дорогою у розробці та впровадженні. Це пов'язано з необхідністю розробки складних алгоритмів, підготовки та очищення великих обсягів даних, а також вибору та налаштування моделей машинного навчання. Крім того, зазвичай потрібно стримувати операційні витрати на підтримку та оновлення моделей з плином часу. Системи самодіагностики часто базуються на стандартизованих діагностичних алгоритмах і процедурах і тому можуть мати нижчі витрати на інтеграцію, ніж системи машинного навчання. Витрати на розробку і впровадження можуть бути низькими, але також існують витрати, пов'язані з підтримкою і оновленням системи.

Автоматизоване прийняття рішень також може бути дорогим у розробці та інтеграції, особливо якщо це стосується складних бізнес-процесів і систем. Однак за умови ефективного впровадження вона може зменшити операційні витрати за рахунок автоматизації процесів і прийняття більш якісних рішень.

Ці системи також відрізняються своєю здатністю адаптуватися і вдосконалюватися в мінливому мережевому середовищі. Системи машинного навчання мають великий потенціал у своїй здатності адаптуватися і вдосконалюватися. Вони можуть вчитися на нових даних і досвіді та автоматично адаптуватися до змін у мережевому середовищі. Крім того, вони можуть покращувати свою продуктивність з часом, постійно оновлюючи свої моделі машинного навчання. Системи самодіагностики також можуть мати здатність до адаптації, але зазвичай обмежуються стандартними алгоритмами діагностики. Ці системи можуть виявляти та ідентифікувати певні типи несправностей, але мають обмежену здатність до автоматичного вдосконалення або адаптації до нових ситуацій. Автоматизовані системи прийняття рішень зазвичай приймають рішення на основі заздалегідь визначених правил і параметрів, тому їхня здатність до адаптації може бути обмеженою. Однак вони можуть бути оновлені для врахування нових правил і критеріїв. Таким чином, системи машинного навчання мають найбільшу здатність до адаптації та вдосконалення, за ними йдуть системи самодіагностики та системи автоматичного прийняття рішень, які можуть мати обмежену здатність до адаптації, але все ще можуть оновлюватися та вдосконалюватися. [29]

Зробимо порівняльний аналіз трьох методів усунення несправностей на основі ШІ, заснованих на різних характеристиках, включаючи точність виявлення несправностей, час відгуку, продуктивність в реальному часі, інтеграцію та експлуатаційні витрати, а також здатність адаптуватися і вдосконалюватися, що представимо в таблиці нижче.

Таблиця 3.1 – Порівняльний аналіз трьох методів усунення несправностей

Характеристика	Системи машинного навчання	Системи самодіагностики	Автоматизоване прийняття рішень
Точність виявлення несправностей	Висока	Висока	Висока
Продуктивність в умовах реального часу	Обмежена	Висока	Висока
Вартість інтеграції та експлуатації	Висока	Низька	Висока
Здатність до адаптації та вдосконалення	Висока	Обмежена	Обмежена

3.2 Порівняння швидкодії та точності методів усунення несправностей з використанням штучного інтелекту

Швидкість і точність методів усунення несправностей на основі ШІ є ключовим фактором при виборі найкращого методу для розгортання для конкретної мережевої інфраструктури.

Швидкість. Системи машинного навчання можуть вимагати багато часу і ресурсів, оскільки їм потрібно обробляти великі обсяги даних і виконувати складні обчислення для навчання моделей і аналізу інформації. Однак після навчання моделі можуть працювати швидше і виявляти несправності. Системи самодіагностики, вбудовані безпосередньо в обладнання, зазвичай працюють швидше і можуть негайно реагувати на виявлення несправностей без затримок, пов'язаних з передачею даних на зовнішній сервер для аналізу. Системи автоматичного прийняття рішень швидкі, якщо вони не вимагають складних операцій аналізу і базуються на заздалегідь визначених правилах і алгоритмах прийняття рішень. [30]

Точність. Системи машинного навчання можуть бути дуже точними у виявленні несправностей, особливо якщо вони навчені на великих обсягах різноманітних даних і мають здатність виявляти складні закономірності та аномалії. Системи самодіагностики, засновані на стандартизованих діагностичних алгоритмах, також можуть бути високоточними, оскільки вони спеціалізуються на певних типах несправностей і можуть негайно визначити їхні причини. Системи автоматичного прийняття рішень є більш точними, якщо вони базуються на правилах, які точно визначають несправності та їх наслідки.

Час реакції. Важливо визначити час, необхідний системі для виявлення та усунення несправності. Швидка реакція мінімізує вплив несправності на мережу і підтримує продуктивність. Системам машинного навчання зазвичай потрібен час для навчання моделей на великих обсягах даних, що може затримати реакцію на нові несправності. Однак, якщо модель вже навчена та оптимізована, можлива швидка реакція на виявлення аномалій. Системи самодіагностики, де алгоритми вбудовані безпосередньо в обладнання, виявляють несправності "на льоту" і тому можуть реагувати негайно. Системи автоматичного прийняття рішень також можуть реагувати швидко, оскільки вони можуть автоматично вживати коригувальні дії відповідно до заздалегідь визначених алгоритмів. Таким чином, системи самодіагностики та системи автоматичного прийняття рішень мають перевагу над системами машинного навчання з точки зору швидкого реагування.

Таблиця 3.2 – Порівняльний аналіз трьох методів усунення несправностей

Характеристика	Системи машинного навчання	Системи самодіагностики	Автоматизоване прийняття рішень
Швидкість	Низька	Висока	Висока
Час реакції	Низький	Високий	Високий
Точність	Обмежена	Обмежена	Обмежена

3.3 Порівняння стабільності та інтегрування методів усунення несправностей з використанням штучного інтелекту

Стабільність. Системи машинного навчання мають довгу історію використання в різних галузях, включаючи мережеве обладнання. Їх надійність і стабільність можуть варіюватися в залежності від складності моделі та її чутливості до мінливих умов. Системи машинного навчання використовуються для прогнозування несправностей, виявлення аномалій і управління мережевими ресурсами. Однак на їхню надійність і стабільність можуть впливати кілька факторів. По-перше, складність моделей машинного навчання призводить до високого рівня абстракції, що ускладнює їх розуміння та налагодження. Це може вплинути на їхню здатність стабільно працювати в мережевих середовищах, де можуть виникати різноманітні складні дані та змінні умови. Другий фактор - це чутливість моделей машинного навчання до мінливих умов. У мережевому середовищі мінливість може бути високою, оскільки навантаження, структура мережі та використовувані протоколи постійно змінюються. Це може вплинути на здатність моделі адаптуватися до нових умов і забезпечувати стабільну роботу. Таким чином, системи машинного навчання мають потенціал для ефективного використання для управління мережевим обладнанням, але їх надійність і стабільність можуть бути піддані ретельній перевірці через їх складність і чутливість до мінливих умов.

Системи самодіагностики також мають довгу історію використання, особливо в промисловому застосуванні. Оскільки вони використовують стандартизовані алгоритми і протоколи, вони, як правило, вважаються дуже стабільними. Стандартизовані алгоритми дозволяють системам самодіагностики ефективно виявляти та аналізувати несправності, що сприяє їх стабільності. Ці алгоритми ретельно тестуються і оптимізуються для забезпечення надійного виявлення несправностей і визначення несправностей. Крім того, завдяки використанню стандартизованих протоколів, системи самодіагностики можуть

бути ефективно інтегровані з існуючим обладнанням і мережами, забезпечуючи сумісність і стабільну роботу в різних середовищах. Таким чином, системи самодіагностики мають певну стабільність, засновану на використанні стандартизованих алгоритмів і протоколів, що робить їх ефективним і надійним засобом виявлення несправностей в мережевому обладнанні.

Автоматизоване прийняття рішень вже використовується в різних галузях. Їх стабільність може залежати від якості визначених правил та алгоритмів. Якщо правила та алгоритми чітко визначені і добре адаптовані до конкретної ситуації, автоматизовані системи можуть працювати дуже стабільно і надійно. Такі системи зазвичай мають вбудовані механізми для виявлення непередбачуваних ситуацій та винятків і можуть реагувати на них належним чином. Однак, якщо правила та алгоритми недостатньо чітко визначені або не враховують усіх можливих варіацій ситуацій, це може призвести до нестабільності та ненадійності автоматизованих систем прийняття рішень. Отже, стабільність автоматизованої системи прийняття рішень залежить від якості визначених правил та алгоритмів і вимагає ретельної розробки та тестування для забезпечення надійної роботи в різних умовах.

Інтеграція з існуючими системами. Системи машинного навчання відомі тим, що вимагають значних зусиль для інтеграції з існуючими системами. Це часто пов'язано з необхідністю заздалегідь підготувати і очистити вхідні дані, вибрати або розробити відповідні моделі машинного навчання і налаштувати їх для роботи в конкретному середовищі. Підготовка даних передбачає обробку та форматування наявних даних, щоб зробити їх готовими для подальшого аналізу та використання моделлю. Очищення даних може включати видалення пропусків, заповнення відсутніх даних та інші операції для забезпечення якості вхідних даних для моделі. Далі необхідно вибрати або розробити відповідну модель машинного навчання для вирішення конкретної проблеми виявлення несправностей. Це передбачає вибір алгоритмів, налаштування гіперпараметрів, а також оцінку і вибір найкращої моделі з декількох альтернатив. Інтеграція з існуючими системами може вимагати спеціальних знань мережевої інфраструктури та програмного забезпечення, а також додаткового часу для налагодження і тестування. Однак, якщо інтеграція

виконана правильно, системи машинного навчання можуть працювати ефективно і точно виявляти несправності.

На відміну від систем машинного навчання, системи самодіагностики, як правило, легше інтегрувати з існуючими системами. Однією з причин цього є те, що вони часто безпосередньо інтегровані в апаратне або програмне забезпечення і тому можуть використовуватися без додаткової інтеграції. Ці системи можуть використовувати стандартизовані протоколи та інтерфейси для зв'язку з іншими компонентами мережі. Це означає, що їх можна легко інтегрувати з існуючими системами без значних зусиль з боку користувача. Оскільки вони інтегровані безпосередньо в обладнання, вони можуть працювати як частина існуючої інфраструктури без необхідності встановлення додаткових компонентів або програмного забезпечення. Це робить системи самодіагностики привабливими для використання в різних галузях промисловості, де важлива швидкість і простота інтеграції з існуючими системами.

Автоматизовану систему прийняття рішень можна легко інтегрувати з існуючими системами за умови, що її робочі правила та алгоритми чітко визначені та зрозумілі. Такі системи можуть взаємодіяти з іншими системами в мережі за допомогою стандартизованих протоколів та інтерфейсів. Однак може знадобитися подальша робота з інтеграції, якщо системі потрібно розробити складні алгоритми прийняття рішень або адаптувати їх до конкретного середовища. Налаштування таких складних алгоритмів та їх належна інтеграція з існуючими системами може вимагати спеціальних знань і часу. Тому, хоча автоматизоване прийняття рішень має потенціал для ефективної інтеграції з існуючими системами, це може бути більш складним процесом, якщо необхідно розробити складні алгоритми прийняття рішень або налаштувати їх для конкретних застосувань.

Таблиця 3.3 – Порівняльний аналіз трьох методів усунення несправностей

Характеристика	Системи машинного навчання	Системи самодіагностики	Автоматизоване прийняття рішень
Стабільність	Варіабельна	Висока	Залежить від якості визначених правил та алгоритмів
Інтеграція	Вимагає значних зусиль для інтеграції	Легко інтегруються.	Легко інтегруються

ВИСНОВКИ

У роботі розглядаються різні підходи до виявлення та усунення несправностей мережевих пристроїв за допомогою штучного інтелекту (ШІ). Основна мета – визначити найбільш ефективні методи, які поєднують швидкий час реагування з високою точністю. Загальний огляд мережевого обладнання та концепції несправностей у цій галузі забезпечує контекст для подальших досліджень. Велику увагу приділено використанню штучного інтелекту в технічному обслуговуванні, оскільки він може бути застосований для автоматизації процесів виявлення несправностей і ремонту. Один з ключових висновків цього дослідження полягає в тому, що штучний інтелект може значно полегшити цей процес, надаючи автоматизовані методи пошуку та усунення несправностей. Системи машинного навчання можуть ефективно обробляти великі обсяги даних і виявляти складні закономірності та аномалії. Системи самодіагностики та автоматизованого прийняття рішень, з іншого боку, можуть негайно реагувати на виявлені несправності, мінімізуючи час, необхідний для вирішення проблем.

Порівняння систем машинного навчання, систем самодіагностики та автоматизованого прийняття рішень з точки зору стабільності та інтеграції з існуючими системами дозволяє зробити кілька висновків. Системи машинного навчання мають потенціал для ефективного управління мережевими пристроями, але їх надійність і стабільність викликають сумніви через складність їх моделей і чутливість до зміни умов. На противагу цьому, системи самодіагностики та автоматизованого прийняття рішень видаються стабільними, оскільки вони використовують стандартизовані алгоритми і протоколи та легко інтегруються з існуючими системами. Таким чином, вибір найкращого методу усунення несправностей залежить від конкретних вимог і характеристик мережі, а також від наявності ресурсів для інтеграції та конфігурації системи.

Використання штучного інтелекту для прогнозування потенційних збоїв мережевого обладнання визнано важливою стратегією підвищення надійності та

відмовостійкості мережевої інфраструктури. Машинне навчання та методи аналізу даних можна використовувати для прогнозування потенційних збоїв і вжиття заходів для уникнення або пом'якшення їхніх наслідків. Це досягається шляхом аналізу великих обсягів даних, класифікації ризиків, виявлення відхилень від нормальних шаблонів та інтеграції з системами моніторингу. Підвищення ефективності управління мережею та зменшення ризиків у критичних ситуаціях вважаються основними перевагами цього підходу.

Аналіз існуючих методів виявлення та ремонту несправностей показує широкий спектр підходів, що використовуються в цій галузі. Існують різноманітні стратегії, починаючи від систем машинного навчання і закінчуючи самодіагностикою та автоматизованими системами прийняття рішень, кожна з яких має свої переваги та обмеження.

Особливу увагу приділено порівняльному аналізу швидкості та точності цих методів. З'ясовано, що системи машинного навчання є дуже точними, але навчання моделей займає багато часу. Водночас системи самодіагностики та автоматизованого прийняття рішень можуть реагувати швидше, але їх точність може залежати від стандартизованих алгоритмів діагностики.

Можна зробити висновок, що вибір найбільш ефективного методу усунення несправностей залежить від балансу між часом реагування і точністю виявлення. Також враховуються специфічні потреби та обмеження мережевої інфраструктури. Успішне впровадження такої системи вимагає врахування цих факторів і вибору найбільш підходящого підходу, що забезпечує найкращі результати в конкретних умовах.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Все, що вам потрібно знати про мережеве обладнання. Макснет – Гігабітний інтернет-провайдер та оператор зв'язку для дому та бізнесу. URL: https://maxnet.ua/blog/vse-chto-vam-nuzhno-znat-o-setevom-oborudovanii/ (дата звернення: 07.05.2024).

2. Ukrinform. Як правильно вибрати мережне обладнання. Укрінформ – актуальні новини України та світу. URL: https://www.ukrinform.ua/rubric-other_news/3395359-ak-pravilno-vibrati-merezne-obladnanna.html (дата звернення: 07.05.2024).

3. Воробієнко П. П., Нікітюк Л. А., Резніченко П. Телекомунікаційні та інформаційні мережі : Підруч. для ВНЗ / ред. І. Пономаренко. Київ : САММІТ-Кн., 2010. 708 с. URL: https://duikt.edu.ua/ua/lib/1/category/2316/view/472.

4. Поперешняк С. В., Вєчерковська А. С. ЦИФРОВІЗАЦІЯ КОМП'ЮТЕРНИХ СИСТЕМ НА ОСНОВІ ШТУЧНОГО ІНТЕЛЕКТУ. Systems and Technologies. 2023. Т. 66, № 2. С. 50–56. URL: https://doi.org/10.32782/2521-6643-2023.2-66.6 (дата звернення: 09.05.2024).

5. Research of software solutions for forecasting electricity generation and consumption in Ukraine that are based on machine learning methods / I. P. Sinitsyn et al. PROBLEMS IN PROGRAMMING. 2023. No. 3. P. 99–108. URL: https://doi.org/10.15407/pp2023.03.099 (дата звернення: 09.05.2024).

6. Jittawiriyanukoon C., Srisarkun V. Simulation for predictive maintenance using weighted training algorithms in machine learning. International Journal of Electrical and Computer Engineering (IJECE). 2022. Т. 12, № 3. С. 2839. URL: https://doi.org/10.11591/ijece.v12i3.pp2839-2846 (дата звернення: 09.05.2024)

7. Prachi. Network Intrusion Detection Using Machine-Learning Techniques. International Journal of Data Mining And Emerging Technologies. 2017. Т. 7, № 1. С. 23. URL: https://doi.org/10.5958/2249-3220.2017.00004.0 (дата звернення: 09.05.2024).

8. Machine Learning for Networking: Workflow, Advances and Opportunities / M. Wang та ін. IEEE Network. 2018. Т. 32, № 2. С. 92–99. URL: https://doi.org/10.1109/mnet.2017.1700200 (дата звернення: 06.05.2024).

9. Yang R., Zhong M. Fault Diagnosis Method Based on Recurrent Convolutional Neural Network. Machine Learning-Based Fault Diagnosis for Industrial Engineering Systems. Boca Raton, 2022. С. 11–25. URL: https://doi.org/10.1201/9781003240754-2 (дата звернення: 09.05.2024).

10. Network Support Data Analysis for Fault Identification Using Machine Learning / S. Basheer та ін. International Journal of Software Innovation. 2019. Т. 7, № 2. С. 41–49. URL: https://doi.org/10.4018/ijsi.2019040104 (дата звернення: 09.05.2024).

11. Computer Networking. Mathematics and Computers in Simulation. 1978. Vol. 20, no. 2. P. 128. URL: https://doi.org/10.1016/0378-4754(78)90036-8 (date of access: 09.05.2024).

12. Claise B., Wolter R. Network Management: Accounting and Performance Strategies. Pearson Education, Limited, 2007. 672 с.

13. Bejtlich R. The Tao of Network Security Monitoring: Beyond Intrusion Detection. Addison-Wesley Professional, 2004. 832 с.

14. Géron A. Hands-On Machine Learning with Scikit-Learn, Keras, and TensorFlow: Concepts, Tools, and Techniques to Build Intelligent Systems. O'Reilly Media, Incorporated, 2022.

15. Yang L. Research on Application of Artificial Intelligence Based on Big Data Background in Computer Network Technology. IOP Conference Series: Materials Science and Engineering. 2018. Т. 392, № 6. С. 062185. URL: https://doi.org/10.1088/1757-899x/392/6/062185 (дата звернення: 09.05.2024).

16. Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications / A. Al-Fuqaha та ін. IEEE Communications Surveys & Tutorials. 2015. Т. 17, № 4. С. 2347–2376. URL: https://doi.org/10.1109/comst.2015.2444095 (дата звернення: 09.05.2024).

17. Moseley L. G. Introduction to machine learning. Engineering Applications of Artificial Intelligence. 1988. Т. 1, № 4. С. 334. URL: https://doi.org/10.1016/0952-1976(88)90057-7 (дата звернення: 09.05.2024).

18. Motohashi Y., Fujimaki R. Development of Predictive Analytics Solution using Machine Learning. IEEJ Transactions on Electronics, Information and Systems. 2016. Т. 136, № 3. С. 249–252. URL: https://doi.org/10.1541/ieejeiss.136.249 (дата звернення: 05.05.2024).

19. Automated remote decision-making algorithm as a primary triage system using machine learning techniques / D. Kim та ін. Physiological Measurement. 2021. Т. 42, № 2. С. 025006. URL: https://doi.org/10.1088/1361-6579/abe524 (дата звернення: 09.05.2024).

20. Skulimowski A. M. J., Bañuls V. A. AI Alignment of Disaster Resilience Management Support Systems. Artificial Intelligence and Soft Computing. Cham, 2021. P. 354–366. URL: https://doi.org/10.1007/978-3-030-87897-9_32 (date of access: 09.05.2024).

21. Беляченко В. В., Бобров С. В., Утюшев М. К. Управління ризиками створення елементів автоматизованих систем управління. Збірник наукових праць Центру воєнно-стратегічних досліджень НУОУ імені Івана Черняховського. 2021. № 3-70. С. 101–106. URL: https://doi.org/10.33099/2304-2745/2020-3-70/101-106 (дата звернення: 04.05.2024).

22. Subramanian M. Network Management: Principles and Practices. Prentice Hall, 2010. 695 p.

23. Lin C.-Y. Information Technology for Project Management Automation. Best Practices. 2001. С. 477–484. URL: https://doi.org/10.1201/9781420000160.ch42 (дата звернення: 07.05.2024).

24. A Machine Learning Approach to Improving Dynamic Decision Making / G. Meyer та ін. Information Systems Research. 2014. Т. 25, № 2. С. 239–263. URL: https://doi.org/10.1287/isre.2014.0513 (дата звернення: 09.05.2024).

25. NLFFT: A Novel Fault Tolerance Model Using Artificial Intelligence to Improve Performance in Wireless Sensor Networks / V. K. Menaria та ін. IEEE Access.

2020. Т. 8. С. 149231–149254. URL: https://doi.org/10.1109/access.2020.3015985 (дата звернення: 09.05.2024).

26. Elkadeem M. R., Alaam M. A., Azmy A. M. Improving performance of underground MV distribution networks using distribution automation system: A case study. Ain Shams Engineering Journal. 2018. Т. 9, № 4. С. 469–481. URL: https://doi.org/10.1016/j.asej.2016.04.004 (дата звернення: 06.05.2024).

27. Artificial-Intelligence-Driven Customized Manufacturing Factory: Key Technologies, Applications, and Challenges / J. Wan та ін. Proceedings of the IEEE. 2020. С. 1–22. URL: https://doi.org/10.1109/jproc.2020.3034808 (дата звернення: 09.05.2024).

28. Fault and performance management in multi-cloud virtual network services using AI: A tutorial and a case study / L. Gupta та ін. Computer Networks. 2019. Т. 165. С. 106950. URL: https://doi.org/10.1016/j.comnet.2019.106950 (дата звернення: 06.05.2024).

29. Tackling Faults in the Industry 4.0 Era–A Survey of Machine-Learning Solutions and Key Aspects / A. Angelopoulos та ін. Sensors. 2019. Т. 20, № 1. С. 109. URL: https://doi.org/10.3390/s20010109 (дата звернення: 06.05.2024).

30. Wang X., Li X., Leung V. C. M. Artificial Intelligence-Based Techniques for Emerging Heterogeneous Network: State of the Arts, Opportunities, and Challenges. IEEE Access. 2015. Т. 3. С. 1379–1391. URL: https://doi.org/10.1109/access.2015.2467174 (дата звернення: 06.05.2024).

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ

(Презентація)

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
Навчально-науковий інститут Інформаційних технологій
Кафедра Комп'ютерної інженерії

КВАЛІФІКАЦІЙНА РОБОТА
НА ЗДОБУТТЯ ОСВІТНЬОГО СТУПЕНЯ БАКАЛАВРА

на тему: «Дослідження методів виявлення та усунення несправностей у мережевому обладнанні з використанням штучного інтелекту»

Виконала студентка групи КІД-41
Швець Валерія Святославівна

Керівник кваліфікаційної роботи:
Бученко Ігор Анатолійович,
старший викладач кафедри КІ

Київ – 2024

Мета роботи – дослідження і вивчення ефективності методів на основі ШІ у виявленні та усуненні несправностей мережевого обладнання, зокрема, порівняння їх швидкості, точності та ресурсоємності з традиційними підходами, а також визначення оптимальних стратегій використання ШІ для підвищення продуктивності та надійності роботи мережевого обладнання.

Об'єкт дослідження – процес виявлення та усунення несправностей у мережевому обладнанні з використанням штучного інтелекту.

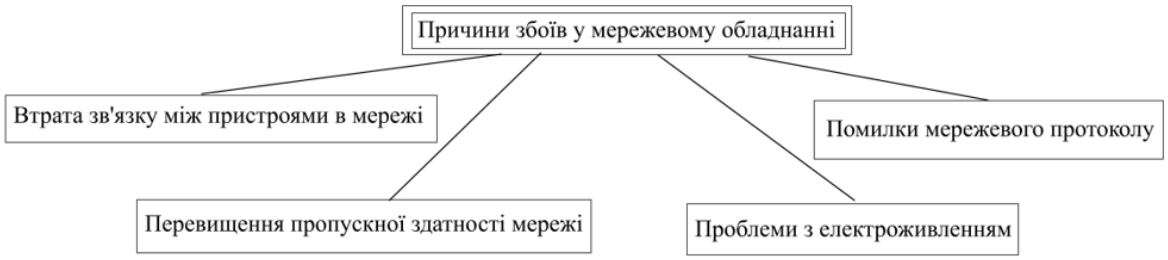
Предмет дослідження – методи і способи виявлення та усунення несправностей в мережевому обладнанні з використанням штучного інтелекту.

Актуальність обраної теми

Сучасні інформаційні інфраструктури стають все більш складними та масштабними. Збільшення кількості підключених пристроїв, швидкості передачі даних і обсягу інформації підвищує ймовірність виникнення різних несправностей і проблем в мережі.

Використання штучного інтелекту може стати ключовим фактором у досягненні цих цілей. Штучний інтелект може автоматично аналізувати великі обсяги даних і виявляти складні взаємозв'язки між параметрами мережі. У сучасних динамічних мережах традиційні методи усунення несправностей недостатньо ефективні. Використання штучного інтелекту в процесі усунення несправностей може підвищити ефективність цих процесів за рахунок автоматизації аналізу даних, виявлення аномалій і прогнозування можливих проблем з мережевим обладнанням.

Збої в мережевому обладнанні

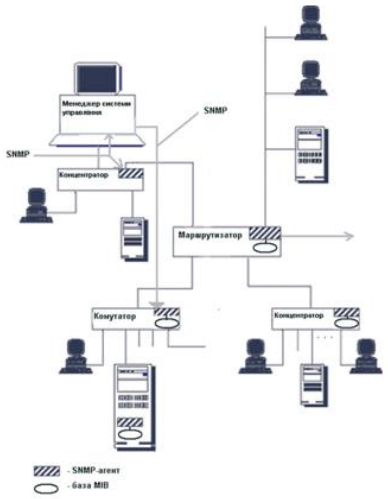


Штучний інтелект у сфері технічного обслуговування

- поліпшення діагностики
- прогнозування несправностей
- планування технічного обслуговування і ремонтів
- скорочення часу простою обладнання
- автоматизація процесів обслуговування мережевого обладнання
- прогнозування життєвого циклу обладнання

5

Типова структура системи управління



6

Етапи усунення несправностей

7

Порівняльний аналіз методів усунення несправностей

Характеристика	Системи машинного навчання	Системи самодіагностики	Автоматизоване прийняття рішень
Точність виявлення несправностей	Висока	Висока	Висока
Продуктивність в умовах реального часу	Обмежена	Висока	Висока
Вартість інтеграції та експлуатації	Висока	Низька	Висока
Здатність до адаптації та вдосконалення	Висока	Обмежена	Обмежена

8

Порівняльний аналіз методів усунення несправностей

Характеристика	Системи машинного навчання	Системи самодіагностики	Автоматизоване прийняття рішень
Швидкість	Низька	Висока	Висока
Час реакції	Низький	Високий	Високий
Точність	Обмежена	Обмежена	Обмежена

Порівняльний аналіз методів усунення несправностей

Характеристика	Системи машинного навчання	Системи самодіагностики	Автоматизоване прийняття рішень
Стабільність	Варіабельна	Висока	Залежить від якості визначених правил та алгоритмів
Інтеграція	Вимагає значних зусиль для інтеграції	Легко інтегруються.	Легко інтегруються

ВИСНОВКИ

У роботі розглянуто різні підходи до виявлення та усунення несправностей мережевих пристроїв за допомогою штучного інтелекту (ШІ). Основною метою було визначення найбільш ефективних методів, які поєднують швидкий час реагування з високою точністю. Велику увагу приділено використанню штучного інтелекту в технічному обслуговуванні, оскільки він може бути застосований для автоматизації процесів виявлення несправностей і ремонту. Один з ключових висновків цього дослідження полягає в тому, що штучний інтелект може значно полегшити цей процес, надаючи автоматизовані методи пошуку та усунення несправностей. Системи машинного навчання можуть ефективно обробляти великі обсяги даних і виявляти складні закономірності та аномалії. Системи самодіагностики та автоматизованого прийняття рішень, з іншого боку, можуть негайно реагувати на виявлені несправності, мінімізуючи час, необхідний для вирішення проблем.

ПРОДОВЖЕННЯ ВИСНОВКІВ

Порівняння систем машинного навчання, систем самодіагностики та автоматизованого прийняття рішень з точки зору стабільності та інтеграції з існуючими системами дозволяє зробити кілька висновків. Системи машинного навчання мають потенціал для ефективного управління мережевими пристроями, але їх надійність і стабільність викликають сумніви через складність їх моделей і чутливість до зміни умов. На противагу цьому, системи самодіагностики та автоматизованого прийняття рішень видаються стабільними, оскільки вони використовують стандартизовані алгоритми і протоколи та легко інтегруються з існуючими системами. Таким чином, вибір найкращого методу усунення несправностей залежить від конкретних вимог і характеристик мережі, а також від наявності ресурсів для інтеграції та конфігурації системи.