МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЧЕРКАСЬКИЙ ДЕРЖАВНИЙ БІЗНЕС-КОЛЕДЖ
кафедра комп`ютерної інженерії та інформаційних технологій

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

МЕТОДИ МАСШТАБУВАННЯ, ОПТИМІЗАЦІЇ ПРОПУСКНОЇ ЗДАТНОСТІ ТА АНАЛІЗ ДОСТУПНОСТІ КОРПОРАТИВНОЇ МЕРЕЖІ ПІДПРИЄМСТВА

Виконав студент групи: 1К-20
спеціальності: 123 «Комп`ютерна інженерія»
Олександр ЖОВНІР
Керівник: Маргарита МЕДОЛИЗ

Черкаси 2024

АННОТАЦІЯ

кваліфікаційна робота присвячена дослідженню методів масштабування, оптимізації пропускної здатності та аналізу доступності корпоративної мережі підприємства. У роботі розкрито основні можливості корпоративних мереж, описано процес створення таких інформаційних систем. Акцентується увага на важливості ефективного управління мережевими ресурсами для забезпечення безперебійної роботи підприємства. Проаналізовано різні підходи до масштабування та оптимізації пропускної здатності, а також методи діагностики та підвищення доступності мережі. Робота також включає створення програмного інструменту, спрямованого на захист корпоративної мережі.

ABSTRACT

This qualification paper is dedicated to the study of methods for scaling, bandwidth optimization, and availability analysis of an enterprise's corporate network. The work reveals the main capabilities of corporate networks and describes the process of creating such information systems. Emphasis is placed on the importance of effective network resource management to ensure the uninterrupted operation of the enterprise. Various approaches to scaling and bandwidth optimization are analyzed, along with methods for diagnosing and improving network availability. The work also includes the creation of a software tool aimed at protecting the corporate network.

ЗМІСТ

ВСТУП

Одним із ключових напрямів розвитку України є впровадження елементів штучного інтелекту в корпоративні комп'ютерні мережі, що сприятиме пошуку та усуненню неполадок, які виникають у мережах. Основні переваги штучного інтелекту включають швидку обробку та інтероперабельність великих баз даних, проведення аналітичної роботи, а також забезпечення співпраці між різними відділами та гілками комп'ютерних мереж.

Актуальність дослідження. Сьогодні аналіз неполадок у мережах є надзвичайно актуальним через швидкий розвиток технологій та створення нових прикладних мережевих протоколів. Велика кількість комп'ютерів привела до формування інформаційних спільнот та проектування й використання різноманітних інформаційних мереж (локальних, регіональних, глобальних) численними користувачами. Комп'ютери стали глобально використовуватися, стали більш доступними та здатними зберігати великі обсяги інформації [35, с. 99].

Це призвело до можливості зберігання даних на цифрових накопичувачах, що породило задачі зі зберігання, обробки, видалення та обміну цифровими даними. Виникли численні проблеми, пов'язані з автентичністю та анонімністю інформації. Представлене дослідження спрямоване на пошук та усунення неполадок у комп'ютерних мережах за допомогою аналітики на основі штучного інтелекту.

Значні за обсягом дослідження у методиках пошуку та усуненні неполадок в комп’ютерних мережах і оптимізації її пропускної здатності за допомогою аналітики на основі штучного інтелекту проведені у роботах таких вчених, як Б. А. Демида, К. М. Обельовська [24], А. І. Блозва, Ю. В. Матус [2], В. М. Коцовський [14], В. Г. Оліфер, Н. А. Оліфер [20], А. Ю. Філімонов [38], А. В. Назаров, В. П. Мельников, А. І. Купріянов [9].

Мета дослідження полягає в проведенні аналізу методів та розробці програмного продукту щодо оптимізації пропускної здатності, пошуку та

усунення неполадок в комп'ютерних мережах за допомогою аналітики на основі штучного інтелекту.

Завдання дослідження можна сформулювати так:

– провести огляд наукової літератури по темі дослідження;

– описати комп'ютерні мережі, як об'єктів діагностування;

– навести головні підходи до класифікації неполадок мереж та методи їх діагностування;

– перелічити особливості створення сучасних інтелектуальних навчальних систем та навести архітектуру інтелектуальної навчальної системи;

– розглянути призначення і принцип роботи елементів штучного інтелекту для пошуку та усунення неполадок в мережах і оптимізації їх пропускної здатності;

– проаналізувати практику використання Cisco AI Network Analytics для пошуку та усунення неполадок в комп'ютерних мережах та їх комплексного аналізу;

– оцінити перспективи використання штучного інтелекту для пошуку помилок в мережі;

– розробка програмного забезпечення по виявленню шкідливого мережевого трафіку в комп'ютерній мережі.

Об'єкт дослідження – комп'ютерні мережі передачі даних.

Предметом дослідження є засоби пошуку та усунення неполадок в комп'ютерних мережах.

Методb дослідження включала аналіз наукової літератури, узагальнення статистичних даних та порівняння. Теоретичний матеріал був класифікований, а також були розроблені рекомендації.

Для досягнення поставлених завдань був використаний системний підхід, включаючи добір матеріалу, індуктивний та логічний аналіз, спостереження та статистичні методи аналізу літературних даних.

Результати дослідження мають велику теоретичну та практичну цінність. Робота надає систематизований теоретичний матеріал з даного дослідження,

відібраний з великої кількості інформації. Також вона сприяє більш глибокому розумінню даного напрямку дослідження, в порівнянні з попередніми дослідженнями вчених, дисертантів та дослідників в цій галузі.

Структура роботи. Робота складається з 75 листів друкованого тексту, 13 рисунків, 1 таблиці та 3 додатків і налічує 47 джерел використаної літератури.

РОЗДІЛ 1 ТЕОРЕТИЧНІ ОСНОВИ АНАЛІЗУ ТА ДІАГНОСТИКИ КОМП'ЮТЕРНИХ МЕРЕЖ

1.1 Основні поняття і визначення під час маштабування, оптимізації та аналізу доступності комп'ютерних мереж

У сучасному контексті технічної діагностики цифрових пристроїв поняття «діагностика корпоративних комп'ютерних мереж» стосується визначення технічного стану діагностованого об'єкта. Проте, це визначення потребує розширення, оскільки навіть при справному технічному стані окремих компонентів корпоративної мережі може виникнути ситуація, коли загальна якість роботи мережі не задовольняє вимоги користувачів або завдання, що вирішуються в мережі. Відтак, необхідно визначити нові поняття та визначення для комп'ютерної мережі як об'єкта діагностики та дослідження, які будуть використані в цьому дослідженні.

Діагностика корпоративної мережі включає комплекс засобів, методів та алгоритмів, спрямованих на виявлення місця і причин невідповідності стану корпоративної мережі як справного об'єкта діагностики та дослідження, а також на запобігання виникненню таких невідповідностей [37, с. 149]. Справний стан - це стан об'єкта, при якому корпоративна мережа відповідає всім вимогам нормативно-технічної та конструкторської документації.

Щодо корпоративної мережі як об'єкта діагностики та дослідження, такі вимоги включають технічні завдання замовника, вимоги до якості обслуговування користувачів Інтернету та корпоративних мереж (Quality of Service, QoS), встановлені комітетом IETF, угоди про рівень обслуговування (Service Level Agreement, SLA), стандарти де-факто, та відомості про пікові значення характеристик компонентів мережі, отримані в результаті попередньої діагностики [6].

Іншими словами, стан корпоративної мережі як об'єкта діагностики визначається якістю роботи мережі. Якість роботи мережі з точки зору користувача визначається часом реакції прикладного ПЗ сервера на запит

клієнта. У разі фізичної недоступності серверного вузла час реакції прагне до нескінченності. Важливо враховувати, що під терміном «час реакції мережі» у контексті діагностики та оптимізації корпоративної мережі розуміються різні величини, що характеризуються різними показниками:

1. Інтервал часу між запитом користувача до мережевого сервісу на сервері та отриманням відповіді на цей запит. Це включає дослідження всіх компонентів тракту передачі даних, включаючи системні ресурси кінцевих вузлів. Наукові дослідження показують, що цей час не повинен перевищувати 2 секунд. Якщо час реакції більший, користувачі почуваються некомфортно, швидко втомлюються, роблять помилки, і продуктивність праці знижується. Передача інформації, що виконується будь-яким вузлом у відповідь на будь-який запит, повинна займати не більше 100 мс, а у випадку глобальної мережі цей інтервал не має перевищувати 200-250 мс для будь-якої відповіді на будь-який тип запиту вузла [25, с. 112].
2. Інтервал часу між відправленням інформації з мережевого адаптера вузла-джерела до мережевого адаптера вузла-приймача. У цьому випадку досліджується якість каналу передачі даних, і оптимальний час реакції визначається часом, витраченим на передачу кадру мінімальної довжини з урахуванням міжкадрового інтервалу. Для протоколу Ethernet 10 Мб/с цей час має становити 67,2 мкс.

Всі інші критерії, такі як кількість помилок передачі даних, ступінь завантаженості мережевих ресурсів, продуктивність обладнання, є вторинними. Отже, під незадовільною роботою розуміється постійна або часткова відсутність доступу до ресурсів комп'ютерної мережі або великий час реакції прикладного серверного ПЗ на запит клієнта.

Корпоративна мережа як об’єкт діагностування визначається співвідношенням (1.1), що зв’язує критерій якості роботи корпоративної мережі у з факторами, що мають на нього вплив:

$$y = f(S_p\{x_1, x_2 .. x_k\}, S_a\{x_1, x_2 ... x_l\}, S_{sys}\{x_1, x_2 ... x_m\}, S_{nos}\{x_1, x_2 ... x_n\}), \quad (1.1)$$

де y – час реакції прикладного ПЗ сервера на запит клієнта; фактори, що характеризують компоненти корпоративної мережі як об'єкт діагностики та дослідження і впливають на значення критерію якості роботи корпоративної мережі, представлені наступними множинами:

– Sa – сукупність характеристик активного мережевого устаткування (мережеві плати, концентратори, комутатори, маршрутизатори), s {x^x,...^ } «сукупність характеристик системних ресурсів сервера і робочих станцій,

– Sp – сукупність характеристик кабельної системи і іншого пасивного обладнання,

– Snos {x^x,..^] – сукупність конфігураційних і мережевих налаштувань мережевої операційної системи.

Особливістю корпоративної мережі як об'єкта діагностики є те, що навіть при справному технічному стані кожного окремого мережевого компонента, може виникнути ситуація, коли загальна робота мережі не відповідає необхідному рівню якості. Це означає, що з точки зору користувачів та виконуваних мережевих завдань, корпоративної мережі не є справною. Це пояснюється помилками на етапі проектування та розгортання мережі, незбалансованим навантаженням на мережеві компоненти, а також використанням програмного забезпечення з неефективними алгоритмами.

Структурна схема корпоративної мережі як об'єкта діагностики може бути представлена відповідно до компонентного підходу, де кожен з компонентів мережі є сукупністю компонентів першого рівня, кожен з яких, у свою чергу, представлений сукупностями компонентів другого рівня і так далі. Кожен з компонентів кінцевого (нижчого) рівня є потенційним джерелом несправності, тобто може бути причиною загальної незадовільної якості роботи комп'ютерної мережі. Ієрархічне впорядкування, яке характеризує цей підхід, дозволяє створити найбільш повну модель несправностей корпоративної мережі і, отже, підвищити ефективність процесу діагностики.

Як приклад, що ілюструє описаний підхід, представлено фрагмент моделі деякої мережі, що складається з п’яти взаємопов'язаних компонентів: робочої станції, колізійного домену А, комутатора, колізійного домену В і сервера. Кожен колізійний домен може бути представлений концентратором разом з кабельною системою (як у домені А) або лише напівдуплексним з'єднанням між робочою станцією/сервером і комутатором (як у домені В).

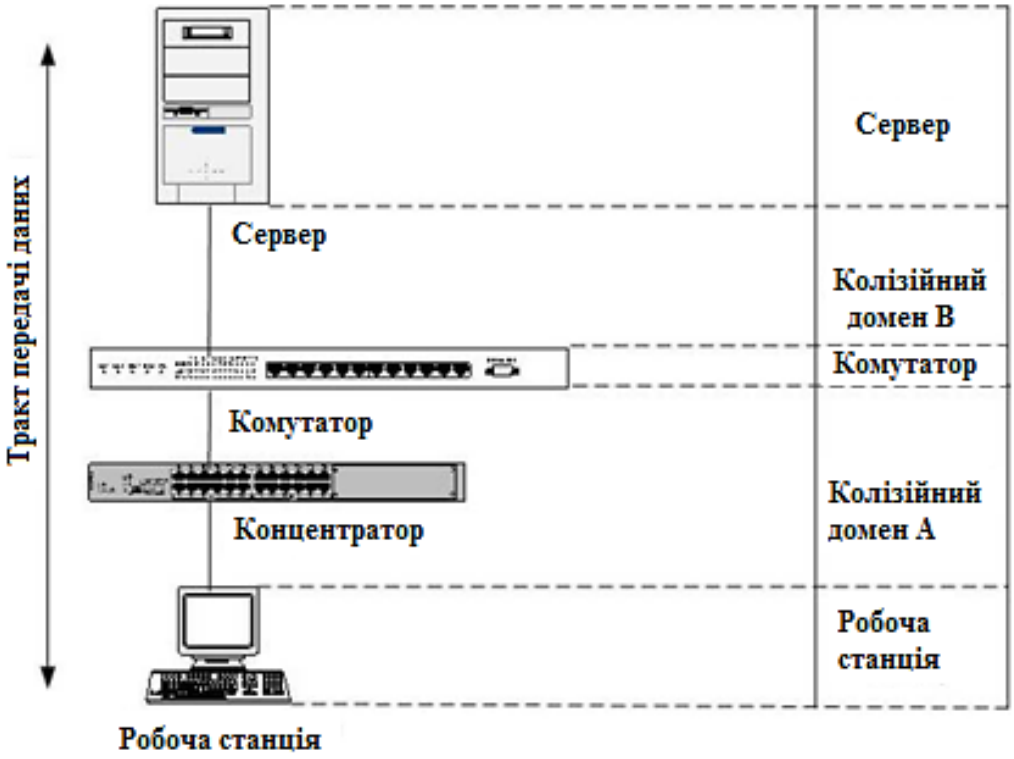


Рисунок 1.1 – Ієрархічний компонентний підхід до подання корпоративної мережі як об’єкта дослідження

Д. Нессер пропонує підходити до дослідження корпоративних мереж через рівневу верифікацію функціонування мережевих протоколів. Це базується на аналізі характеристик і процесів, які дозволяють оцінити коректність роботи мережі або її окремих рівнів. Ці характеристики і процеси можуть бути універсальними для всіх протоколів (наприклад, частка широкомовних передач, дублікати адрес, перекриття запитів і відповідей, повторні передачі, послідовність відкриття сеансу зв’язку, механізми підтримки з'єднання, механізми розсилки повідомлень, повідомлення про помилки в мережі), або

специфічними для певних протоколів (як-от всі типи пакетів ICMP, час життя TCP-пакету, розмір вікна у стеку протоколів TCP/IP) [21, с. 220].

Цей підхід відрізняється своєю складністю та значними тимчасовими витратами, і зазвичай використовується для тонкої оптимізації мережі, коли її загальна якість є задовільною, але необхідно виявити і усунути дефекти, вузькі місця та інші чинники, що знижують її швидкодію.

Для проведення тестування вхідна послідовність призначена для встановлення відповідності технічного стану об'єкта заданим параметрам. У мережі тестування здійснюється як апаратними, так і програмними засобами. Апаратні засоби включають перевірку кабелю за допомогою кабельного сканера, тестера, мультиметра або термінатора для визначення цілісності чи ідентифікації несправностей. Програмні засоби включають команди, як-от ping, для перевірки цілісності кабелю, справності мережевого адаптера або ідентифікації несправностей. Тестування може бути активним, що впливає на роботу мережі, як-от перевірка кабельної системи або стресове тестування, або пасивним, що полягає в спостереженні за мережею та зборі статистичної інформації без втручання в її роботу.

Елементарна перевірка (ЕП) полягає в подачі тесту та спостереженні реакції на нього мережевого компонента або чинника, що характеризує виконувану операцію, з метою виявлення несправності, яка впливає на загальний технічний стан мережі [5]. Реакція – це інформація про технічний стан тестованого компонента, отримана при подачі тесту, яка дозволяє зробити висновки про відповідність або невідповідність об'єкта заданим технічним станам.

Результат елементарної перевірки – це порівняння реакції з еталоном при подачі тесту. Перевірка є позитивною, якщо реакція свідчить про відповідність технічного стану тестованого компонента еталону. Якщо реакція свідчить про невідповідність, результат вважається негативним.

1.2 Класифікація неполадок комп’ютерних мереж

Всі мережеві несправності, які негативно впливають на якість роботи комп'ютерної мережі, поділяються на наступні групи: явні адресовані дефекти, явні мережеві дефекти, приховані мережеві дефекти, явні вузькі місця та приховані вузькі місця.

Адресовані дефекти виникають через недосяжність кінцевих або проміжних вузлів комп'ютерної мережі. Це може статися через фізичні дефекти (некоректний монтаж кабельної системи, відмови повторювачів, концентраторів, зовнішні наведення, відмови мережевих адаптерів) або некоректну конфігурацію мережевого підключення (установка мережевої карти з несумісним протоколом, невірно задана маска підмережі, дубльована IP-адреса) [23, с. 95].

Явні дефекти призводять до спотворення інформації при її передачі мережею. Основними причинами таких спотворень є дефекти пасивного мережевого обладнання, вплив зовнішніх перешкод та деякі несправності приймально-передавальних модулів активного мережевого обладнання. Наприклад, несправності в кабельній системі можуть проявлятися як помилки з'єднання, що фіксуються операційною системою клієнта, або як помилки канального рівня, що перехоплюються аналізатором протоколів і багатофункціональним сканером.

За різними оцінками, частка дефектів пасивного мережевого обладнання становить від 65 до 85%. На відміну від прихованих, явні дефекти легко виявляються за допомогою засобів пасивної діагностики, аналізуючи всі кадри, що проходять мережею, на предмет спотворень. З розвитком мережевих технологій відносна частка явних дефектів знижується, оскільки перехід з коаксіального кабелю на виту пару і оптику підвищує стійкість каналів передачі інформації. Водночас складність активного мережевого обладнання зростає, що підвищує ймовірність прихованих дефектів.

Приховані дефекти уповільнюють роботу комп'ютерної мережі без спотворення кадрів. До таких дефектів належать некоректні налаштування

датчика міжкадрової паузи на мережевій платі, що може призводити до захоплення мережі дефектною мережею або її постійного простою; спотворення інформації після перевірки контрольної суми в активному мережевому обладнанні; дефекти в мікропрограмному забезпеченні комутаторів, що можуть призводити до необґрунтованого видалення інформації з портів або до взаємного блокування портів [13, с. 420].

Вузькі місця у мережі можуть бути явними або прихованими, впливаючи на її пропускну здатність. Вузьке місце визначається найменш продуктивним компонентом мережі, таким як активне обладнання (комутатор, концентратор, маршрутизатор, сервер), програмне забезпечення, параметри налаштування обладнання або програмного забезпечення, а також налаштування мережевої операційної системи.

Приклади прихованих дефектів включають: некоректне налаштування датчика міжкадрової паузи на мережевій платі, що призводить до захоплення мережі дефектною мережею або її простою; спотворення інформації після перевірки контрольної суми в активному мережевому обладнанні; дефекти в мікропрограмному забезпеченні комутаторів, що призводять до видалення інформації з портів або до взаємного блокування портів.

Для забезпечення стабільної та ефективної роботи корпоративної мережі важливо використовувати комплексний підхід до виявлення та усунення як явних, так і прихованих дефектів. Застосування сучасних інструментів для діагностики, таких як аналізатори протоколів і мережеві монітори, а також впровадження передових методів оптимізації та масштабування допоможе підвищити загальну продуктивність та надійність мережевої інфраструктури підприємства.

"Мережева плата погано чує паузу". Одним із поширених дефектів мережевих плат є неправильне налаштування датчика паузи, який перевищує час 9,6 мкс (для Ethernet). Це призводить до того, що станція з такою платою чекатиме довшої паузи, поступаючись каналом іншим станціям, які хочуть передавати дані одночасно. Така "глуха" станція передаватиме інформацію лише

тоді, коли інші станції колізійного домену не мають даних для передачі, що уповільнює її роботу, проте не спричиняє спотворень в інформації.

"Спотворення інформації після перевірки контрольної послідовності CRC". Цей дефект може виникати в будь-якому активному мережевому обладнанні, коли спотворення даних відбувається після їх прийому і перевірки CRC. Наприклад, мережева плата або комутатор можуть прийняти дані, перевірити CRC і передати їх драйверу без виявлення помилок. Проте, через дефекти приймального буфера мережевої плати, дані можуть бути спотворені, що залишиться непоміченим мережею, якщо не виконано додаткову контрольну перевірку на транспортному рівні.

"Приховані дефекти" в мікропрограмному забезпеченні комутаторів. Недоліки в мікропрограмному забезпеченні комутаторів можуть призводити до видалення інформації під час високого навантаження або до взаємного блокування портів. Виробники пасивних діагностичних засобів відреагували на зростання кількості прихованих дефектів, випустивши експертні системи для їх виявлення. Компанія Network General (тепер Network Associates) першою інтегрувала експертні системи в аналізаторі протоколів Sniffer, домінуючи на ринку протягом двох років. Пізніше до них приєдналися компанії Hewlett-Packard з LAN Internetwork Advisor та Wandel & Goltermann (тепер Wavetek Wandel Goltermann) з Mentor. Сьогодні всі серйозні гравці на ринку діагностичних засобів пропонують експертні системи як інтегральний компонент або додаткову опцію для аналізаторів мережевих протоколів, що підвищує ефективність діагностики мережі, але також збільшує вартість обладнання.

Явні вузькі місця включають мережеві ресурси з недостатньою пропускною здатністю, такі як невідповідні прикладні завдання, обмежена продуктивність процесора або дискової підсистеми сервера, низька пропускна здатність комутатора або каналу зв'язку. Вузькі місця явного типу можна виявити, вимірюючи основні системні характеристики компонентів

комп'ютерної мережі та порівнюючи їх, щоб визначити найбільш завантажений компонент.

Приховані вузькі місця включають алгоритми, процеси або параметри налаштування обладнання чи програмного забезпечення, що знижують пропускну здатність мережі. Це можуть бути параметри налаштування, що викликають широкомовні шторми, або параметри прикладного ПЗ, що збільшують частку коротких повідомлень. Також це можуть бути неефективні алгоритми роботи прикладного ПЗ, які знижують пропускну здатність мережі, наприклад, некоректно реалізовані методи пошуку файлів або зациклення запитів. Для виявлення таких вузьких місць пасивні вимірювання недостатні; необхідно проводити додаткові експерименти з впливом на рівень навантаження мережевого трафіку.

Підвищення ефективності роботи прикладного ПЗ не входить до основних завдань діагностування комп'ютерних мереж. Проте неефективні алгоритми або налаштування прикладного ПЗ можуть бути причиною незадовільного часу реакції сервера на запити клієнта. Тому діагностика мереж повинна включати визначення середовища, яке є джерелом несправностей: мережа або прикладне ПЗ.

Дж. Хогдалл пропонує класифікацію мережевих несправностей відповідно до рівнів моделі OSI (Таблиця 1.1).

Таблиця 1.1. – Класифікація мережевих несправностей по Хогдаллу

Фізичний рівень	Фізичний рівень відповідає за фізичні з'єднання між мережевими пристроями та передачу бітів по мережевих середовищах (кабелях, радіохвилях тощо). Несправності на цьому рівні включають: • Переривання кабелів: фізичне пошкодження кабелю, що призводить до втрати зв'язку між пристроями. • Поганий контакт конекторів: нещільне з'єднання кабелю та роз'єму, що викликає інтермітуючі збої. • Електромагнітні перешкоди (EMI): вплив зовнішніх електромагнітних полів, які заважають передачі сигналів. • Застарілі або неякісні кабелі: використання кабелів, які не підтримують необхідну швидкість передачі даних або мають високе загасання сигналу.

Продовження таблиці 1.1.

Канальний рівень	Канальний рівень відповідає за надійне передавання даних між двома вузлами в мережі, виправляючи помилки фізичного рівня. Несправності на цьому рівні включають: • Колізії в мережі: одночасна передача даних декількома вузлами, що призводить до їх зіштовхнення і втрати інформації. • Помилки кадрування: неправильне формування або прийом кадрів даних. • Проблеми з MAC-адресами: дублювання або відсутність коректних MAC-адрес в мережевих пристроях. • Широкомовні шторми: надмірна кількість широкомовних запитів, що перенавантажує мережу.
Мережевий рівень	Мережевий рівень відповідає за маршрутизацію пакетів між різними мережами. Несправності на цьому рівні включають: • Некоректна маршрутизація: неправильні маршрути або таблиці маршрутизації, що призводять до втрати пакетів або неправильного їх направлення. • IP-конфлікти: одночасне використання однієї IP-адреси декількома пристроями. • Перевантаження маршрутизаторів: маршрутизатори не справляються з обсягом трафіку, що призводить до затримок або втрат пакетів. • Проблеми з протоколами маршрутизації: помилки в роботі протоколів OSPF, BGP тощо.
Транспортний рівень	Транспортний рівень забезпечує надійну передачу даних між кінцевими вузлами мережі. Несправності на цьому рівні включають: • Перевантаження портів: надмірна кількість з'єднань, що призводить до затримок або втрат даних. • Проблеми з TCP/UDP: помилки у встановленні або підтримці з'єднань, втрати сегментів, повторні передачі. • Неправильне встановлення вікна TCP: неефективне управління потоком даних, що призводить до затримок або перевантажень.
Сеансовий рівень	Сеансовий рівень відповідає за встановлення, підтримку та завершення сеансів зв'язку між додатками. Несправності на цьому рівні включають: • Розриви сеансів: несподіване завершення або обрив сеансу зв'язку. • Проблеми з синхронізацією: невідповідність у порядку передачі даних між сторонами сеансу. • Неуспішні спроби встановлення сеансів: помилки при спробі встановити нові сеанси зв'язку.
Представницький рівень	Представницький рівень відповідає за перетворення даних для забезпечення сумісності між додатками. Несправності на цьому рівні включають: • Проблеми з кодуванням/декодуванням: неправильне перетворення даних, що призводить до їх спотворення або втрат. • Невідповідність форматів даних: неузгодженість між форматами даних, що використовуються різними додатками. • Помилки в шифруванні/дешифруванні: помилки в процесах шифрування або дешифрування даних, що призводять до їх недоступності або неправильного відображення.

Прикладний рівень	Прикладний рівень забезпечує послуги для кінцевих користувачів та додатків. Несправності на цьому рівні включають: • Неправильна конфігурація додатків: налаштування, що заважають нормальній роботі програм. • Вразливості безпеки: помилки, що дозволяють зловмисникам отримати доступ до мережі або даних. • Проблеми з протоколами прикладного рівня: помилки у функціонуванні протоколів HTTP, FTP, SMTP тощо. Збої в роботі серверів: відмови серверів, що надають послуги додаткам.

Подано детальний опис кожного рівня моделі OSI та відповідних мережевих несправностей дозволяє краще зрозуміти, де можуть виникати проблеми в комп'ютерних мережах та як їх можна діагностувати і вирішувати.

Дж. Хогдалл вказує на перевагу своєї моделі класифікації мережевих дефектів порівняно з компонентним підходом, де основний акцент робиться на місці розташування дефекту. У моделі Хогдалла несправності класифікуються за рівнями моделі OSI, що дозволяє звертати увагу на конкретні функції, які відповідають за кожен рівень мережі. Це спрощує аналіз та виправлення помилок, оскільки він стандартизує причини несправностей.

У цій моделі не вказується конкретний компонент, як носій дефекту. Замість цього, аналіз проводиться на рівнях моделі OSI, де визначаються стандартні набори функцій і протоколів для кожного рівня. Такий підхід дозволяє оперативно виявляти та виправляти несправності, оскільки він дозволяє точно визначити, на якому рівні відбувається проблема та які саме функції або протоколи її стосуються.

1.3 Методи аналізу комп’ютерних мереж

Системи управління мережею (Network Management Systems) є ключовими для ефективного контролю та управління комп'ютерними мережами. Вони забезпечують централізоване збирання і аналіз даних про стан вузлів і пристроїв мережі, а також про трафік, що циркулює в мережі. Окрім моніторингу, вони можуть автоматично або напівавтоматично виконувати дії з управління

мережею, такі як включення і відключення портів пристроїв, зміна параметрів мостів, адресних таблиць, комутаторів і маршрутизаторів. Прикладами таких систем є популярні продукти, такі як HP OpenView, SunNet Manager, IBM NetView [11, с. 75–82].

Засоби управління системою (System Management) виконують схожі функції, але стосуються інших об'єктів. Тут об'єктом управління є програмне та апаратне забезпечення комп'ютерів мережі. Деякі функції цих систем можуть дублюватися з функціями систем управління, наприклад, вони також можуть аналізувати мережевий трафік.

Вбудовані системи діагностики та управління (Embedded Systems) реалізовані у вигляді програмно-апаратних модулів, які встановлюються в комунікаційне обладнання або вбудовані в операційні системи. Вони виконують функції діагностики та управління тільки одним пристроєм і відрізняються від централізованих систем управління. Наприклад, модуль управління концентратором Distributed 5000 автоматично виконує функції автосегментації портів при виявленні несправностей або приписуванні портів внутрішнім сегментам концентратора. Зазвичай вони також виступають у ролі SNMP-агентів, що містять дані про стан пристрою для централізованих систем управління [11, с. 75–82].

Аналізатори протоколів (Protocol Analyzers) призначені для моніторингу та аналізу трафіку в мережі. Вони можуть захоплювати і декодувати пакети різних протоколів, що використовуються в мережі, і відображати їх в зручній формі для фахівця. Це допомагає виявляти та вирішувати проблеми з мережею.

Експертні системи накопичують знання про причини аномальної роботи мережі та можливі шляхи вирішення проблем. Вони можуть бути як окремими підсистемами в системах управління, так і окремими продуктами. Експертні системи допомагають у виявленні та усуненні причин несправностей у мережі.

Багатофункціональні пристрої аналізу та діагностики поєднують функції декількох пристроїв, таких як аналізатори протоколів, кабельні сканери і деякі

можливості програмного забезпечення мережевого управління. Вони корисні для швидкого та зручного аналізу мережі.

Ці різноманітні засоби та системи допомагають адміністраторам мережі ефективно контролювати, управляти та діагностувати мережу для забезпечення її надійності та ефективності.

Знаючи залежність між часом реакції прикладного ПЗ і значеннями спостережуваних параметрів, адміністратор комп'ютерної мережі може визначити максимальні значення параметрів, які допустимі для даної мережі, і ввести їх у вигляді порогів (thresholds) у діагностичний засіб. Якщо значення спостережуваних параметрів перевищують порогові значення, діагностичний засіб інформує адміністратора мережі про це, що свідчить про можливі проблеми в мережі.

Одночасно з цим вимірюються швидкісні характеристики комп'ютерної мережі. Якщо з'ясовується, що швидкість робочих станцій і пропускна здатність комп'ютерної мережі відповідають очікуваним значенням, то роблять висновок про те, що дефектів немає. Якщо ж якісь станції працюють з низькою швидкістю або відключаються від сервера, то роблять висновок про наявність дефектів. При стрес-тестуванні часто використовується швидкість виконання файлових операцій кожною робочою станцією мережі як критерій якості роботи мережі. Цей критерій обраний, оскільки він має високу чутливість до будь-яких дефектів у системі. Інша причина вибору цього критерію полягає в його легкій вимірюваності. Якщо швидкість роботи станції знижується, то, змінюючи умови роботи станції, можна визначити причину цього. Однак при цьому потрібно враховувати, що для проведення таких діагностичних заходів необхідно відсутність робочого трафіку в мережі.

1.4 Засоби аналізу комп'ютерних мереж

Засоби, що застосовуються для діагностування та моніторингу корпоративної мережі, можна розділити на кілька великих класів:

1. Системи управління мережею (Network Management Systems) є важливим інструментом для забезпечення ефективності корпоративних мереж. Прикладами таких систем є HP OpenView, Sun NetManager, IBM NetView, Tivoli. Вони здійснюють контроль за конфігурацією мережі, виявлення та усунення помилок, аналіз продуктивності та безпеки. Управління конфігурацією включає налаштування компонентів мережі та підтримку схеми мережі. Обробка помилок спрощує виявлення та вирішення негараздів в мережі. Аналіз продуктивності допомагає в оцінці часу реакції системи та плануванні розвитку мережі. Управління безпекою включає контроль доступу та збереження цілісності даних. Облік роботи мережі забезпечує реєстрацію та управління використовуваними ресурсами і пристроями.

Системи управління мережею (Network Management Systems) є ключовим компонентом в забезпеченні ефективності корпоративних мереж. Приклади таких систем включають HP OpenView, Sun NetManager, IBM NetView, Tivoli. Ці системи забезпечують контроль за конфігурацією мережі, виявлення та виправлення помилок, аналіз продуктивності та безпеки. Керування конфігурацією включає налаштування компонентів мережі та підтримку схеми мережі. Обробка помилок спрощує виявлення та усунення неполадок в мережі. Аналіз продуктивності допомагає в оцінці часу реакції системи та плануванні розвитку мережі. Керування безпекою включає контроль доступу та збереження цілісності даних. Облік роботи мережі забезпечує реєстрацію та керування використовуваними ресурсами і пристроями [34, с. 57].

2. Засоби управління системою (System Management) виконують функції, подібні до систем управління, але спрямовані на інші об'єкти. Перш за все, вони керують програмним та апаратним забезпеченням комп'ютерів мережі, а також комунікаційним обладнанням. Основні функції засобів управління системою включають:

– Облік використовуваних апаратних і програмних засобів. Система автоматично збирає інформацію про комп'ютери та створює записи в базі даних про апаратні та програмні ресурси. Це дозволяє адміністраторам

швидко з'ясувати, якими ресурсами вони володіють і де вони знаходяться. Наприклад, можна дізнатися, які комп'ютери потребують оновлення драйверів принтерів, а які мають достатньо пам'яті та дискового простору.

– Розподіл і установка програмного забезпечення. Після обстеження адміністратор може створити пакети для розсилки програмного забезпечення, що є ефективним способом зменшення витрат на цю процедуру. Система також може централізовано встановлювати і адмініструвати додатки, які запускаються з файлових серверів, а також дозволяти кінцевим користувачам запускати ці додатки з будь-якої робочої станції мережі.

Прикладами засобів управління системою є продукти, такі як System Management Server від Microsoft або LANDesk Manager від Intel. Типовими представниками засобів управління мережами є системи HP OpenView, SunNet Manager і IBM NetView.

3. Вбудовані системи діагностики та управління (Embedded systems) є важливою складовою сучасних мережних технологій. Вони виконуються у вигляді програмно-апаратних модулів, які встановлюються в комунікаційне обладнання, або у вигляді програмних модулів, вбудованих в операційні системи. Основна їх відмінність від централізованих систем управління полягає у тому, що вони виконують функції діагностики та управління тільки одним пристроєм.

Наприклад, модуль управління концентратором Distributed 5000 може реалізовувати функції автосегментації портів при виявленні несправностей, приписування портів внутрішнім сегментам концентратора. Це означає, що система може автоматично переназначати порти внутрішнім сегментам для підтримки нормального функціонування в разі виявлення несправностей.

Такі вбудовані системи дозволяють підтримувати стабільну роботу мережного обладнання та автоматично реагувати на виникнення проблем, що значно підвищує ефективність управління мережею [34].

4. Аналізатори протоколів (Protocol analyzers) представляють собою важливі інструменти для моніторингу та аналізу трафіку в мережах, включаючи бездротові. Вони можуть бути як програмними, так і апаратно-програмними системами.

При оцінці аналізаторів протоколів важливо враховувати декілька ключових критеріїв, що допомагають вибрати найбільш підходящий аналізатор протоколів для конкретних потреб у моніторингу і управлінні мережею.

1. Можливість декодування мережевих протоколів і підтримка фізичних інтерфейсів. Цей критерій вказує на те, як добре аналізатор може розбирати пакети даних і взаємодіяти з різними типами мережевих інтерфейсів.

2. Якість інтерфейсу програмного забезпечення, включаючи буфер захоплення, фільтри, перемикачі, постфільтраційний пошук і можливість відображення статистичних даних. Ці функції дозволяють користувачеві здійснювати глибокий аналіз трафіку і виявляти проблеми в мережі.

3. Наявність багатоканальності та можливість генерації трафіку. Цей аспект важливий для одночасного моніторингу кількох каналів і тестування мережі на масштабність.

4. Можливість інтеграції з ПК, а також розмір і вага аналізатора. Це важливо для зручності використання та мобільності.

5. Співвідношення ціни і послуг, що надаються. Аналізатор повинен відповідати бюджету користувача і одночасно забезпечувати необхідні функції для ефективного аналізу мережі [31, с. 133].

Обладнання для діагностики та сертифікації кабельних систем має важливе значення для забезпечення надійності і ефективності мережевих інфраструктур. Це обладнання включає чотири основні групи:

1. Мережеві монітори (мережеві аналізатори) є важливими інструментами для діагностики і сертифікації кабельних систем. Вони включають високоточний частотний генератор і вузькосмуговий приймач, наприклад, мережеві аналізатори компанії Hewlett-Packard-HP.

2. Кабельні сканери використовуються для діагностики мідних кабельних систем, дозволяючи визначити довжину кабелю, ступінь загасання, імпеданс і провести оцінку електричних шумів.

3. Багатофункціональні пристрої аналізу та діагностики комбінують функції декількох пристроїв, таких як аналізатори протоколів, кабельні сканери і деякі можливості мережевого управління. Ці пристрої, як Compas компанії Microtestlnc або LANMeter компанії FlukeCorp, є досить недорогими та портативними.

4. Оптичні рефлектометри OTDR (Optical Domain Reflectometer) є інструментами для характеризації втрат потужності оптичного сигналу в оптоволоконних мережах.

5. Візуальні дефектоскопи (VFL, Visual Fault Locators) використовуються для перевірки полярності і виявлення неприпустимих вигинів або обривів кабелю за допомогою інфрачервоного лазера.

6. Рефлектометри MTS 8000 є мультимодульними тестовими платформами для оптоволоконних систем, здатними вимірювати різні характеристики волоконно-оптичних мереж [31, с. 190].

Це лише декілька прикладів обладнання, яке використовується для діагностики і сертифікації кабельних систем, і цей список постійно розширюється та оновлюється, оскільки технології мережевого зв'язку постійно розвиваються.

РОЗДІЛ 2 ІНТЕЛЕКТУАЛЬНІ ТЕХНОЛОГІЇ У МОНІТОРИНГУ ТА ДІАГНОСТИКИ КОМП'ЮТЕРНИХ МЕРЕЖ

2.1 Основні проблеми моніторингу та діагностики комп'ютерних мереж

У контексті масштабування і оптимізації пропускної здатності корпоративної мережі підприємства інтелектуальні інформаційні технології грають важливу роль. Вони дозволяють підприємствам ефективно керувати та оптимізувати використанням мережевих ресурсів, забезпечуючи високу доступність та швидкість обміну даними.

Одним із напрямків оптимізації є використання інтелектуальних агентів для моніторингу та управління мережею. Ці агенти можуть автоматично аналізувати стан мережі, виявляти проблеми та вживати заходів для їх вирішення, що дозволяє підприємствам забезпечувати стабільну роботу мережі.

Крім того, інтелектуальні інформаційні технології дозволяють підприємствам аналізувати доступні дані про використання мережі та прогнозувати потреби в ресурсах. Це дозволяє ефективно розподіляти мережеві ресурси, уникати перевантажень та забезпечувати високу доступність мережі.

Завдяки інтелектуальним інформаційним технологіям підприємства можуть не лише підтримувати стабільну роботу своїх мереж, але й постійно підвищувати їх ефективність та відповідати вимогам сучасного бізнесу.

У цей час насправді дискутують про можливість створення штучного інтелекту. Багато людей вважають, що розробка інтелектуальних інформаційних систем може позбавити людей гідності. У світі сьогодні інтелектуальні інформаційні системи використовуються майже всюди, що створює умови для нового просування. Штучний інтелект дозволяє автоматизувати виробництво, що сприяє підвищенню продуктивності праці. Проте, незважаючи на безліч переваг, він також має свої недоліки, які потребують уважного вирішення людством. Ці недоліки пов'язані з ризиками, що виникають при використанні штучного інтелекту [32, с. 12].

Деякі проблеми виникають через можливу втрату інтересу людей до творчої праці, яка спричинена загальною комп'ютеризацією і використанням машин у мистецтві. Інші, більш серйозні проблеми полягають в тому, що існують програми та машини, які можуть навчатися та адаптуватися до зовнішніх умов. У майбутньому можуть з'явитися машини, які будуть мати такий рівень надійності та пристосованості, що людина не буде потрібна для втручання в процес. Це може призвести до того, що людина втратить свою роль у творчому пошуку рішень.

Інша проблема полягає у тому, що людина може не здати адекватно реагувати на зміни зовнішніх умов. Тому важливо встановити обмеження для автоматизації процесів, особливо в ситуаціях аварій. У сферах, де людина відповідає за керування машиною, важливо завжди правильно діяти в непередбачуваних ситуаціях. Це особливо актуально для ядерної енергетики та транспорту, де навіть невелика помилка може мати жахливі наслідки.

Проблеми з інтелектуальними інформаційними системами потребують постійного втручання людей. Нові проблеми будуть виникати постійно, і цей процес буде безкінечним.

Отже, штучний інтелект в майбутньому матиме велике значення для розвитку людства. Сьогодні на етапі прийняття рішень домінує аналіз інформації в галузі автоматизації управління - обробка початкової інформації та розкладання проблемних ситуацій.

Сучасні інформаційні технології у різних сферах людської діяльності, зростання обсягів інформації та необхідність оперативно реагувати в усіх ситуаціях вимагають пошуку ефективних шляхів вирішення проблем. Найбільш ефективним із них є інтелектуалізація інформаційних технологій.

Інтелектуальні інформаційні технології, як правило, означають інформаційні технології, які мають такі можливості:

– бази знань, що відображають досвід конкретних осіб, груп, суспільства, людства в цілому у вирішенні творчих завдань у визначених галузях діяльності, які традиційно вважаються прерогативою людського

інтелекту (наприклад, погано структуровані завдання, проектування, пояснення, навчання).

- здатність до навчання, перенавчання і, отже, до розвитку.
- можливість пояснювати висновки і рішення, тобто мати механізм пояснень.
- здатність формувати чіткі рішення на основі нечітких, нестрогих, неповних даних.
- наявність моделей мислення на основі баз знань: правил і логічних висновків; аргументації і міркування; розпізнавання і класифікації ситуацій; узагальнення і розуміння [3, с. 175].

Інтелектуальні інформаційні технології вражають своєю універсальністю, охоплюючи практично всі сфери, включаючи управління, проектування, машинний переклад, діагностику, розпізнавання образів та синтез мови. Вони є основою для розподіленого вирішення складних завдань, спільного проектування виробів, створення віртуальних підприємств, моделювання великих виробничих систем, електронної торгівлі, електронної розробки складних комп'ютерних систем, управління системами знань та інформації.

Історія інтелектуальних інформаційних технологій свідчить про постійний розвиток цієї галузі з 60-х років минулого століття. Перший період характеризувався формуванням соціального замовлення на підтримку процесів прийняття рішень і управління, що відбулося через появу перших персептронів, розробку методів евристичного програмування та ситуаційного управління.

У 70-80-х роках з'явилася усвідомленість важливості знань для прийняття адекватних рішень, що призвело до розвитку експертних систем, в яких активно використовується апарат нечіткої математики.

80-90-ті роки характеризувалися появою інтегрованих моделей представлення знань, які поєднували в собі різні види інтелекту, такі як пошуковий, обчислювальний, логічний та образний.

На сьогоднішній день було створено багато систем, що використовують інтелектуальні інформаційні технології. Наприклад, система діагностики

передстартової підготовки ракетно-космічних комплексів, експертна система для діагностики лікарських отруєнь, технологія реінжинірингу бізнес-процесів та конфігурації інформаційної системи підприємства на основі управління знаннями, а також інтелектуальні агенти для виявлення атак в комп'ютерних мережах.

2.2 Особливості створення сучасних інтелектуальних систем з можливостями моніторингу та діагностики

Ethernet хаби і комутатори виконують важливі функції у мережах, забезпечуючи зв'язок між комп'ютерами та іншими мережевими пристроями. Ці пристрої дозволяють комп'ютерам в одному сегменті мережі спілкуватися безпосередньо один з одним.

Хаби працюють на основі простого принципу, приймаючи вхідні пакети через один порт і передаючи їх на всі інші порти. Це дозволяє використовувати режим promiscuous для моніторингу мережі. У порівнянні з хабами, комутатори більш "розумні": вони аналізують MAC-адреси пакетів і пересилають їх тільки на потрібні порти.

Керовані комутатори з підтримкою дзеркалювання портів є ідеальними для мережевого моніторингу, оскільки дозволяють перенаправляти трафік з одних портів на певний порт комутатора. Керування параметрами дзеркалювання залежить від моделі і виробника пристрою [10, с. 25–28].

У маленьких мережах хаби досить поширені через їх доступну вартість, але вони можуть мати обмеження при моніторингу та діагностиці мережі. Хаби відкриті для несанкціонованого моніторингу всередині сегменту мережі, оскільки кожен порт може бути використаний для promiscuous-моніторингу. Деякі «інтелектуальні» хаби можуть не дозволити вести моніторинг всього сегменту мережі.

На апаратному рівні моніторинг і аналіз мережі є важливим етапом контролю за роботою мережі. Для цього розроблено різноманітні програми і

засоби, що працюють автономно. До них входять засоби діагностики, аналізатори протоколів, експертні системи, сканери і тестери. Розуміння основних принципів мережевого моніторингу дозволяє забезпечити прозорість мережі в будь-яких умовах. Прозорість мережі є основою для правильної роботи з програмами мережевого аналізу і моніторингу [10, с. 25–28].

На програмному рівні, сучасні інтелектуальні навчальні системи, розроблені на базі навчальних об'єктів, використовують метадані, які зберігаються в базах знань. Наразі не існує загальновизнаних визначень для термінів "база даних" та "база знань". Ми підтримуємо погляд, що технічної різниці між ними немає. Це пояснюється тим, що багатофункціональні системи управління базами даних, такі як управління об'єктно-орієнтованими, активними та дедуктивними базами даних, підтримують деякі дедуктивні та недедуктивні механізми висновків та засоби структурування, аналогічні базам знань. Якщо є різниця між цими термінами, то вона полягає переважно в тому, наскільки системи підтримують уявлення, структурування та можливість виведення [39, с. 21].

З 1985 по 1995 рік університет Торонто (Канада) розробляв інтелектуальну навчальну систему у рамках проекту KBMS (Knowledge Base Management System). Основною метою цього проекту було створення універсальної архітектури, призначеної для комп'ютерних додатків з інтенсивним розвитком. Ця система мала розширювану, багаторівневу архітектуру, що дозволяла їй працювати як з механізмами виведення загального призначення, так і зі спеціальними механізмами виведення. Спеціальні механізми виведення, такі як механізм просторового мислення або механізм на основі доказової аргументації, вбудовувалися в залежності від потреб спеціальних додатків, тоді як механізми виведення загального призначення були однаковими для всіх додатків.

Багаторівнева архітектура підтримувала проектування коду, засноване на підвищенні рівня абстракції, що дозволяло розбивати загальну задачу проектування ІНС на кілька підзадач. У такій архітектурі використовувався

стандартний інтерфейс для кожного рівня та його компонентів, що дозволяло багаторазово використовувати їх у різних системах.

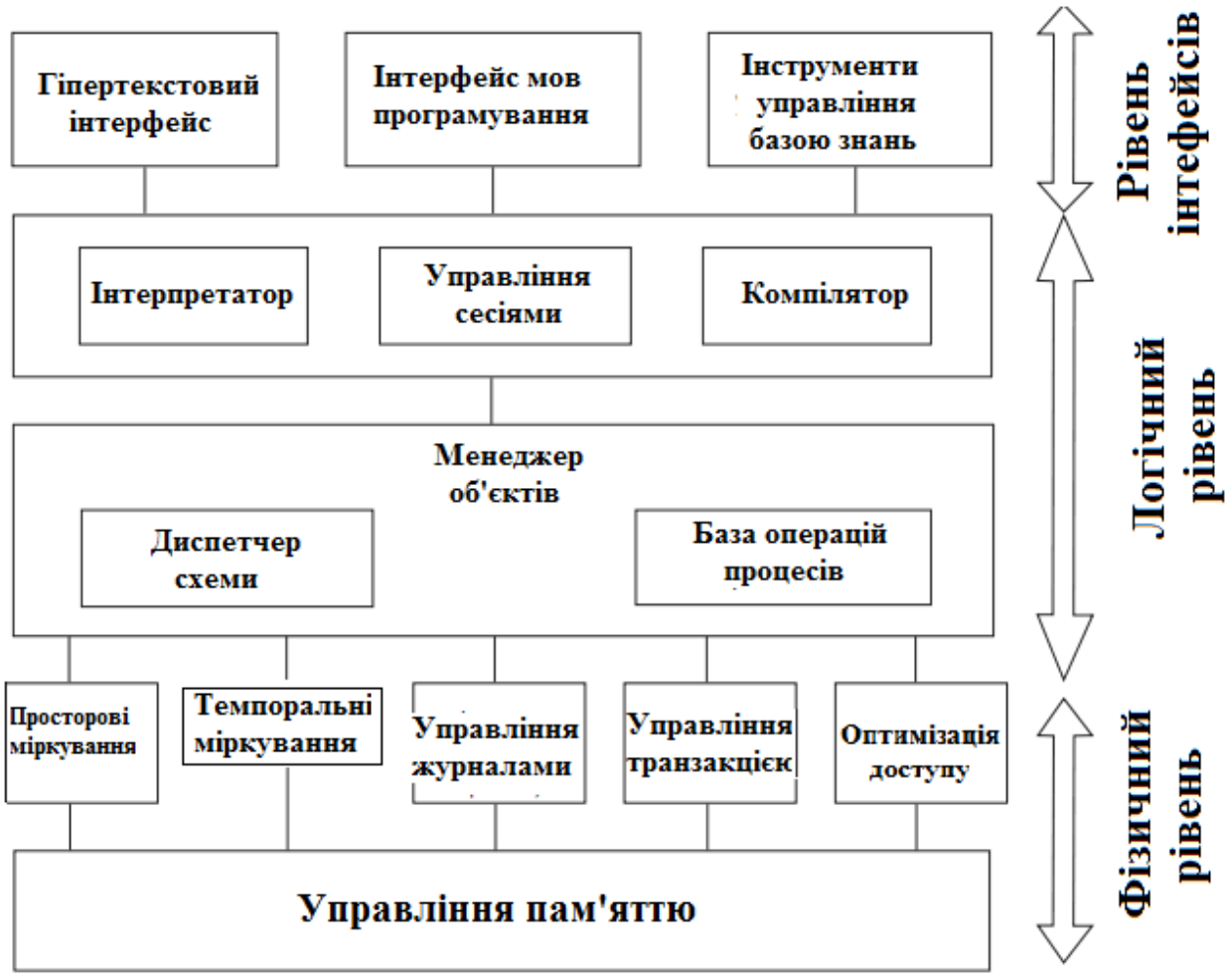


Рисунок 2.1 – Загальна архітектура системи управління

Розроблена архітектура системи управління базою знань (рис. 2.1) складається з трьох рівнів:

1. Рівень інтерфейсів: цей рівень пропонує різноманітні види користувацьких інтерфейсів. Сервіси цього рівня включають гіпертекстовий інтерфейс для взаємодії з користувачем і мовний інтерфейс програмування для виконання додаткових програм, що використовують базу знань. Також на цьому рівні можуть бути інструменти для збору знань, перевірки бази знань, перевірки обмежень, розвитку та обміну знаннями.

2. Логічний рівень: на цьому рівні здійснюються прості операції з вилучення знань і оновлення бази знань. Сервіси цього рівня включають управління класами, включаючи правила і обмеження, і підтримують примітивні операції бази знань.
3. Фізичний рівень: цей рівень відповідає за управління структурами даних для зберігання баз знань, різних показників та іншої допоміжної інформації. Він також управляє індексами, політикою кешування та іншими аспектами фізичного зберігання даних [40].

Рівень інтерфейсів надає різноманітні користувацькі послуги для баз знань. Це включає гіпертекстовий інтерфейс для оперативного взаємодії з користувачем, а також інтерфейс програмування, який дозволяє виконувати додаткові програми з операціями бази знань. Додатково, на цьому рівні можуть бути інструменти для збору знань, перевірки та розвитку бази знань. Служби цього рівня з'єднуються з логічним рівнем за допомогою інтерпретатора мови представлення знань, управління сесіями та компілятора.

Логічний рівень містить інформацію про класифікацію, включаючи правила і обмеження, і підтримує базові операції знань. Його послуги реалізовані поверх фізичного рівня (набору модулів), які включають управління вихідними даними, трасування шляху доступу, планування обробки запитів та блоки міркувань для різних типів обґрунтування (логіка).

Фізичний рівень відповідає за управління структурами даних на диску, індексами та політикою кешування. Його функціональність забезпечується ядром зберігання баз даних, що спеціалізуються на об’єктно-орієнтованих та вкладених реляційних базах даних. Архітектура системи управління знаннями, розроблена в рамках проекту KBMS, знаходить застосування в багатьох додатках інтелектуальних інформаційних технологій, що використовують базу знань [40].

Під час вирішення завдань складної природи система управління базами знань повинна мати можливість концептуального відображення реальності, зберігання та використання високоструктурованих знань. Наявність у проекті

KBMS на рівні інтерфейсів модуля управління базами знань, а також інтерфейсу мов програмування, дозволяє використовувати блоки управління базами знань для розв’язання різноманітних завдань. Однак сучасні програмні додатки є складними, орієнтованими на змінні завдання та методи їх вирішення, що призводить до значних витрат на їх адаптацію та перероблення інтелектуальної системи. Проектування та перероблення є витратними заходами, які вимагають створення власних унікальних модулів управління базами знань. Для зменшення витрат при розробці нових систем, що базуються на знаннях, таких як ІОС, необхідною є наявність готових оболонок для різноманітних інструментів не лише для управління БЗ, але й для вирішення конкретних завдань [40].

Для інтелектуальних інформаційних систем важливим є метод представлення знань. Цей метод дозволяє описувати метадані про навчальні об'єкти та вирішувати такі завдання, як:

- актуалізація знань через процедури навчання;
- перевірка валідності баз знань, моделюючи їх мережами Петрі;
- створення та використання індивідуального середовища навчання та тестування;
- формування послідовності навчальних та тестових об'єктів [40, с. 6].

Дані аспекти грають важливу роль у забезпеченні ефективності та функціональності систем управління знаннями, сприяючи оптимізації процесів навчання та розвитку.

Під час створення інтелектуальних інформаційних систем, які базуються на метаданих навчальних об'єктів (інформація про навчальні об'єкти), важливим аспектом є вибір відповідного методу їх подання. Для застосування індивідуальних навчальних траєкторій запропонований інтегрований метод, який ґрунтується на можливостях представлення структури предметної області та взаємодії сутностей цієї області одна з одною. Інтегрований метод подання знань дозволяє описувати предметну область безліччю описів концепцій. Описи концепцій представляють собою множини вузлів та зважених зв'язків між ними.

Кожен вузол описується такими атрибутами представлення сутності: ім'я, передумова, імена концепцій нижчого рівня, імена концепцій вищого рівня, імена концепцій-асоціацій.

Сучасна інтелектуальна навчальна система є складною розподіленою системою. Компонентами цієї розподіленої системи є безліч суб'єктів навчального процесу, які мають складну поведінку, інтелект і індивідуальні засоби комунікації, що робить непрактичним застосування традиційних формальних методів для їх опису. Тому на сьогоднішній день широко використовується агентно-орієнтований підхід у створенні додатків реальної складності.

2.3 Архітектура інтелектуальної системи з можливостями моніторингу та діагностики

Розробка сучасних інтелектуальних навчальних систем є складним завданням, оскільки вона пов'язана з рядом проблем, які ускладнюють ефективність технологій проектування таких систем. Для подолання цих проблем потрібно визначити конкретні умови і виробити необхідні підходи. Однією з головних умов є розробка ефективної технології проектування інтелектуальних навчальних систем. Для досягнення цієї мети пропонується використовувати методику компонентного проектування, яка є ключовим фактором розвитку будь-яких технологій і ґрунтується на постійно розширюваних бібліотеках типових компонентів, які можна використовувати багато разів. Для цього необхідно вирішити ряд питань, деякі з яких наведено нижче:

– створення бібліотек типових компонентів інтелектуальних систем та уточнення типології таких компонентів (включаючи предметні онтології, фрагменти баз знань, машини виведення та інтерфейсні компоненти);

- розробка засобів комп'ютерної підтримки синтезу інтелектуальних систем з використанням наявних компонентів;
- забезпечення сумісності (інтегрованості) компонентів інтелектуальних систем шляхом уніфікації їх представлення [29, с. 72].

Також важливо мати можливість оновлення бази знань інтелектуальної системи незалежно від оновлення моделей та методів обробки знань, що відрізняється від оновлення засобів технічної реалізації. Це обумовлено тим, що в різних предметних областях можуть змінюватися завдання та рішення. Ці рішення, що є типовими, можуть постійно використовуватися та утворювати бібліотеку багаторазово використовуваних компонентів інтелектуальних навчальних систем.

Інтегрований метод представлення знань дозволяє відобразити реальність у вигляді сутностей та зв'язків між ними. Це дозволяє описати таксономію предметної області та процеси, що виникають у цій області. Архітектура сучасної інтелектуальної навчальної системи показана на рис. 2.2.

Блок для формування та реалізації навчальних планів інтелектуальних навчальних систем дозволяє використовувати персоналізоване середовище навчання, що сприяє розвитку нових компетенцій, враховуючи поточні знання, вміння та навички. Робота з актуальними знаннями та їх відповідність реальності забезпечується блоком для навчання на власному досвіді та успішних рішеннях, де застосовуються методи машинного навчання.

Збільшення обсягу баз знань сучасних інтелектуальних систем, включаючи інтелектуальні навчальні системи, підвищує вимоги до коректності вмісту цих баз. Одним з підходів до валідації баз знань є використання мереж Петрі, які можуть бути складені з безлічі функціональних підмереж і відповідати моделюванню баз знань системи.

Для повноцінної роботи персоналізованого середовища необхідний блок оцінки знань, що відстежує прогрес індивідуальної траєкторії навчання [30, с. 210].

Архітектура інтелектуальної навчальної системи, зображена на рисунку 2.2, включає ядро, що містить систему управління базами знань глобальної інтелектуальної навчальної системи. На рівні інтерфейсів цієї системи знаходиться блок формування і підтримки агентів. Кожен агент інтелектуальної навчальної системи формується за допомогою типових технічних рішень, що можуть використовуватися багаторазово.

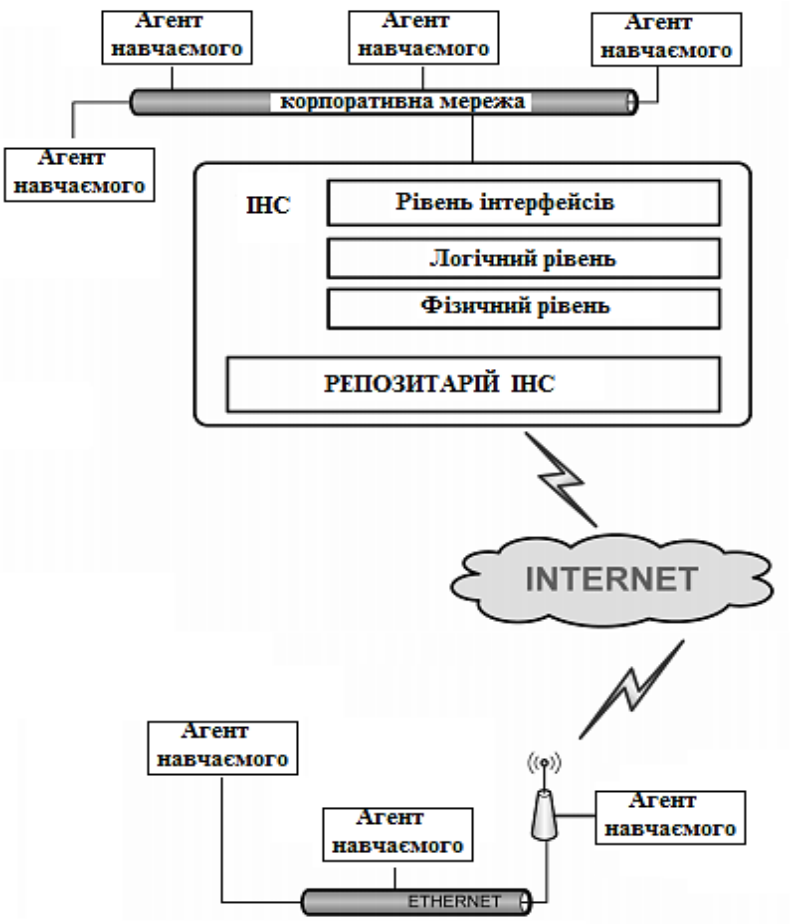


Рисунок 2.2 – Схематичне зображення архітектури інтелектуальних навчальних систем

У створеному агенті використовуються наступні компоненти:

- інтерфейс з персоналізованим середовищем;
- планувальник індивідуальної траєкторії;
- модуль (агент) для оцінки знань на різних етапах формування компетенцій;
- модуль персоналізованого середовища для реалізації індивідуальної траєкторії навчання;

– модуль для створення сховища персоналізованого середовища навчання та його підтримки в актуальному стані.

Для функціонування інтелектуальної навчальної системи можуть знадобитися багаторазово використовувані компоненти для рішення завдань машинного навчання (накопичення досвіду), актуалізації вмісту бази знань системи, розпізнавання типових ситуацій в навчанні та валідації сучасних баз знань.

РОЗДІЛ 3 РОЗРОБКА ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ДЛЯ АНАЛІЗУ МАШТАБУВАННЯ, ОПТИМІЗАЦІЇ ТА АНАЛІЗУ ДОСТУПНОСТІ КОМП'ЮТЕРНИХ МЕРЕЖ

3.1 Призначення і принцип роботи елементів штучного інтелекту для маштабування, оптимізації та аналізу доступності комп'ютерних мереж

Аналіз наукової літератури демонструє, що термін "комп'ютерні мережі" відноситься до засобів, які дозволяють об'єднати комп'ютери за допомогою засобів передачі даних у єдину систему для обробки, зберігання та обміну інформацією. Основна мета цих мереж - забезпечити користувачам доступ до ресурсів усіх комп'ютерів мережі.

Історичною передумовою створення програм на основі штучного інтелекту для пошуку та усунення неполадок у комп'ютерних мережах було виявлення цих неполадок та їх усунення. Застосування різноманітних інструментів, таких як захоплення, декодування та збереження переданих пакетів, дозволяє здійснювати повний аналіз усієї комп'ютерної мережі [27, с. 64].

За допомогою аналізаторів мережі, системні адміністратори та інженери можуть повністю спостерігати за процесом передачі даних у комп'ютерній мережі і виявляти будь-які неполадки вже на першій діагностичній перевірці. Програми на основі штучного інтелекту для виявлення та виправлення таких неполадок мають широкий набір інструментів для розв'язання різних проблем мережі. Ці програми можуть стати потужним засобом у руках досвідченого користувача, але водночас і потенційним джерелом небезпеки, оскільки можуть бути використані для несанкціонованого доступу до конфіденційної інформації.

Програми на основі штучного інтелекту для виявлення та виправлення неполадок у комп'ютерних мережах зазвичай працюють на канальному рівні, використовуючи мережевий адаптер NIC (network interface card). Вони можуть функціонувати в прихованому режимі для захоплення пакетів з трафіку або в діагностичному режимі для виправлення проблем всередині мережі.

Програми на основі штучного інтелекту для виявлення та виправлення неполадок у комп’ютерних мережах працюють в прихованому режимі, що дозволяє їм проходити через фільтри адрес і портів, що використовуються в Ethernet та TCP/IP для ідентифікації даних. Після захоплення пакетів вони зберігають їх у форматі двійкового коду і, за допомогою декодерів, аналізують інформацію для подальшого аналізу.

Для захоплення всіх пакетів, що проходять через мережевий адаптер, програма на основі штучного інтелекту для виявлення та виправлення неполадок мережі повинна підтримувати режим promiscuous mode (безладний режим). Цей режим дозволяє адаптеру перехоплювати всі пакети. Цей режим може бути автоматично активований при запуску програми або встановлюватися вручну.

Вся інформація, що захоплюється, передається декодеру пакетів, який ідентифікує та розподіляє пакети за різними рівнями ієрархії. Залежно від можливостей програми, інформація про пакети може бути подальшим чином аналізована та відфільтрована.

Раніше програми на основі штучного інтелекту для виявлення та виправлення неполадок мережі представляли певну небезпеку, оскільки вони могли використовуватися для несанкціонованого доступу до інформації. Однак зараз, коли мережі зазвичай проектуються з використанням комутаторів, що ускладнює можливість захоплення всієї мережі, ця небезпека є меншою [18, с. 110].

Якщо на будь-якому вузлі мережі є програма на основі штучного інтелекту, яка спеціалізується на виявленні та виправленні неполадок у комп’ютерних мережах, вона може захопити кожен мережевий пакет у мережі, що використовує концентратори. Використання комутаторів ускладнює можливість захоплення всієї мережі, оскільки комутатори працюють на більш високому рівні ізоляції трафіку. Кожен комутатор зберігає адреси підключених пристроїв та визначає шлях передачі даних, що дозволяє зменшити навантаження на мережу порівняно з концентраторами. Пакети даних відправляються до конкретного порту

комутатора, на який підключений отримувач, інші вузли мережі не отримують доступ до цих пакетів.

Ключовим елементом роботи програм на основі штучного інтелекту є корпоративна політика безпеки, яка базується на чотирьох складових: забезпечення безпеки, моніторинг, перевірка та покращення системи. Забезпечення безпеки означає застосування процесів і технологій для забезпечення безпеки. Моніторинг передбачає постійне відслідковування ефективності системи та виявлення порушень. Перевірка включає тестування процесів на адекватність та стійкість. Покращення передбачає розробку нових дизайнів мережі та впровадження нових технологій для підвищення безпеки.

В основі роботи елементів штучного інтелекту лежить корпоративна політика безпеки (Corporate Security Policy), на яку спираються чотири складові:

1. Secure (Забезпечення безпеки), Monitor (моніторинг), Test (перевірка), Improve (покращення системи).
2. Secure – реалізація спроектованих процесів і технологій, спрямованих на забезпечення безпеки.
3. Monitor – процеси і технології безпеки, які потребують моніторингу з метою оцінювання працездатності та ефективності системи безпеки, виявлення та фіксування порушень і вторгнень.
4. Test – фаза тестування, яка включає перевірку процесів на адекватність, стійкість і передбачуваність. Завжди краще самому виявити слабкості в своїй системі безпеки, ніж дозволити це іншим.
5. Improve – розробка нового дизайну мережі, впровадження нових технологій, оновлення обладнання, його ПЗ і конфігурацій.

Незважаючи на всі заходи безпеки, абсолютної безпеки досягти неможливо, оскільки безпека та доступність мережі працюють на протилежних принципах. Існують причини, що ускладнюють захист мережі, і можна їх класифікувати на три групи.

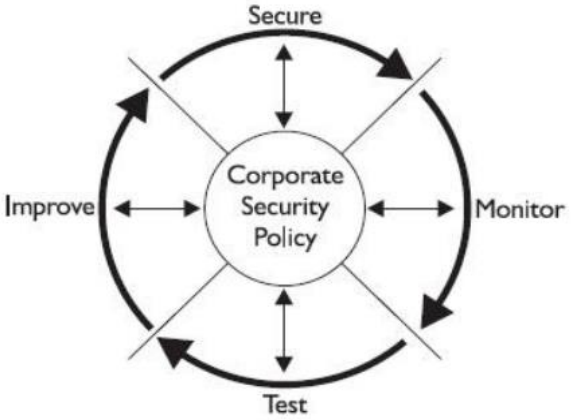


Рисунок 3.1 – Мережева безпека Cisco Security Wheel

Серед основних проблем комп'ютерних мереж, які призводять до зниження продуктивності, можна виокремити наступні: подвійне копіювання даних пакета (з карти мережі в пам'ять ядра, з пам'яті ядра в пам'ять користувача процесу); велика кількість переривань від мережевої карти (по кожному пакету для його копіювання в буфер ядра); часті перемикання між режимами ядра і користувача (по кожному пакету при його копіюванні в пам'ять користувацького процесу); недостатнє використання паралелізму на рівні окремого ядра і процесорів (за замовчуванням всі переривання обробляються одним ядром); проблеми з синхронізацією при доступі до даних з кількох потоків виконання. У випадку, коли отримані дані повинні оброблятися в декілька потоків, виникає ситуація конкуренції за ресурси між цими потоками.

3.2 Практика використання Cisco AI Network Analytics для аналізу неполадок комп’ютерних мереж

Одним з найпопулярніших програмних продуктів для тестування мереж є Cisco AI Network Analytics. Це програмне забезпечення містить емулятор мережевого обладнання Cisco Systems з операційною системою Cisco IOS і інструмент для тестування корпоративних мереж [19, с. 51]. Цей продукт став дуже популярним завдяки необхідності його використання в рамках навчання в програмі Cisco Network Academy.

Cisco AI Network Analytics дозволяє створювати лабораторні роботи за допомогою вбудованого помічника, який допомагає створити еталонну модель, з якою буде порівнюватися конфігурація обладнання, і задати параметри для функціонального тестування, такі як перевірка доступності певного вузла та перевірка коректності встановленого сусідства [43].

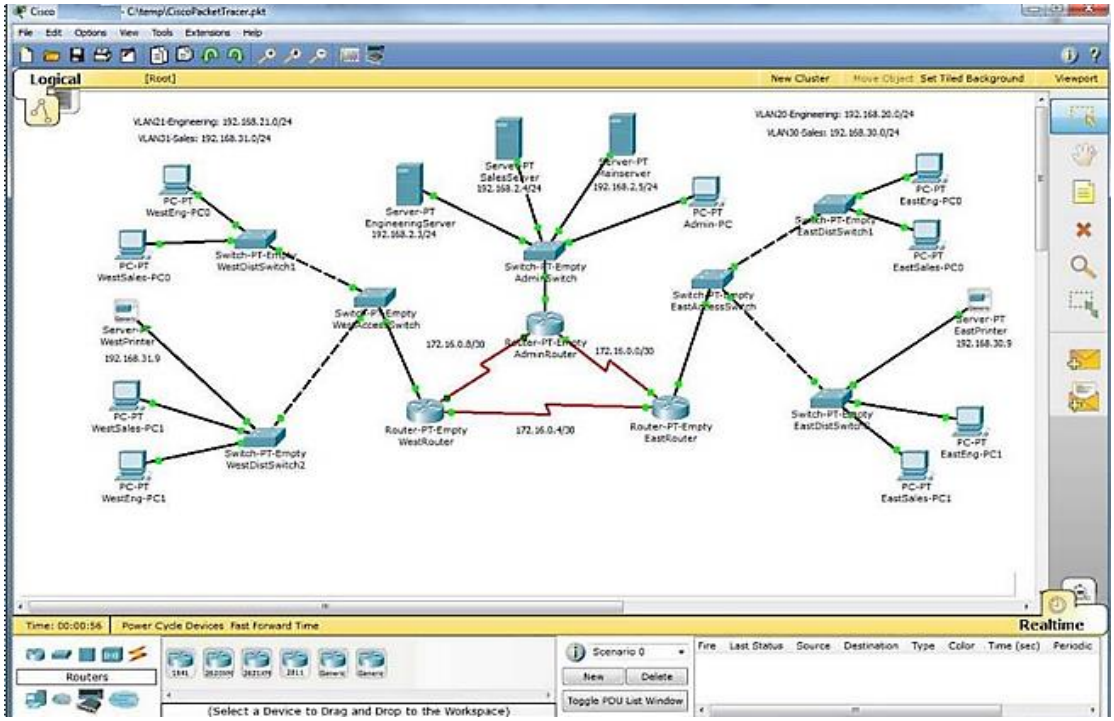


Рисунок 3.2 – Графічна оболонка Cisco AI Network Analytics

Cisco AI Network Analytics емулює лише апаратну і програмну частину певного обладнання. Доступ до повноцінного функціоналу Cisco IOS обмежений, оскільки реалізація функцій операційної системи залежить від розробників цього програмного продукту. Аналізуючи захоплений трафік локальної мережі, можна визначити, що було завантажено на комп'ютер. Наприклад, розглянемо дану процедуру на основі протоколу HTTP і дізнаємося, які зображення були завантажені. Для цього необхідно провести фільтрацію всього трафіку за допомогою фільтру HTTP [42].

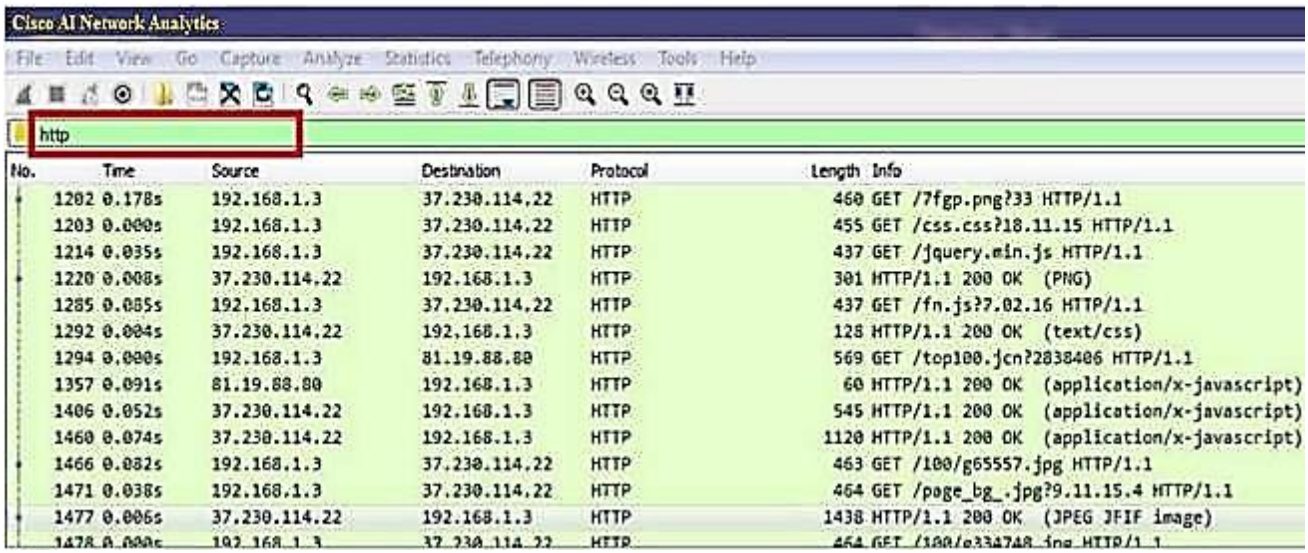


Рисунок 3.3 – Приклад фільтрування трафіку Cisco AI Network Analytics

Після того, як захоплений трафік відфільтрований, він відображає всі пакети, що використовували протокол HTTP. Для знаходження завантажених зображень необхідно перейти на вкладку "export objects" і вибрати HTTP (див. рисунок 3.4). Для експорту завантажених об'єктів можна зберегти або конкретний файл, або всі файли, шляхом збереження їх на робочий стіл. Тим же самим способом можна витягти завантажені ZIP-файли, потокове відео та аудіо.

Наразі комплексним рішенням для проведення аналізу скачаних файлів з мережевих технологій з миттєвою перевіркою виконаного завдання є Cisco AI Network Analytics [47]. Цей програмний продукт дозволяє проводити пошук помилок в комп'ютерній мережі, захоплювати трафік та створювати лабораторні роботи, які можна відразу ж перевірити за готовим шаблоном з використанням функціонального тестування, такого як перевірка з'єднання за допомогою утиліти ping, перевірка установки сусідства в протоколах маршрутизації EIGRP, OSPF, BGP та інші тести.

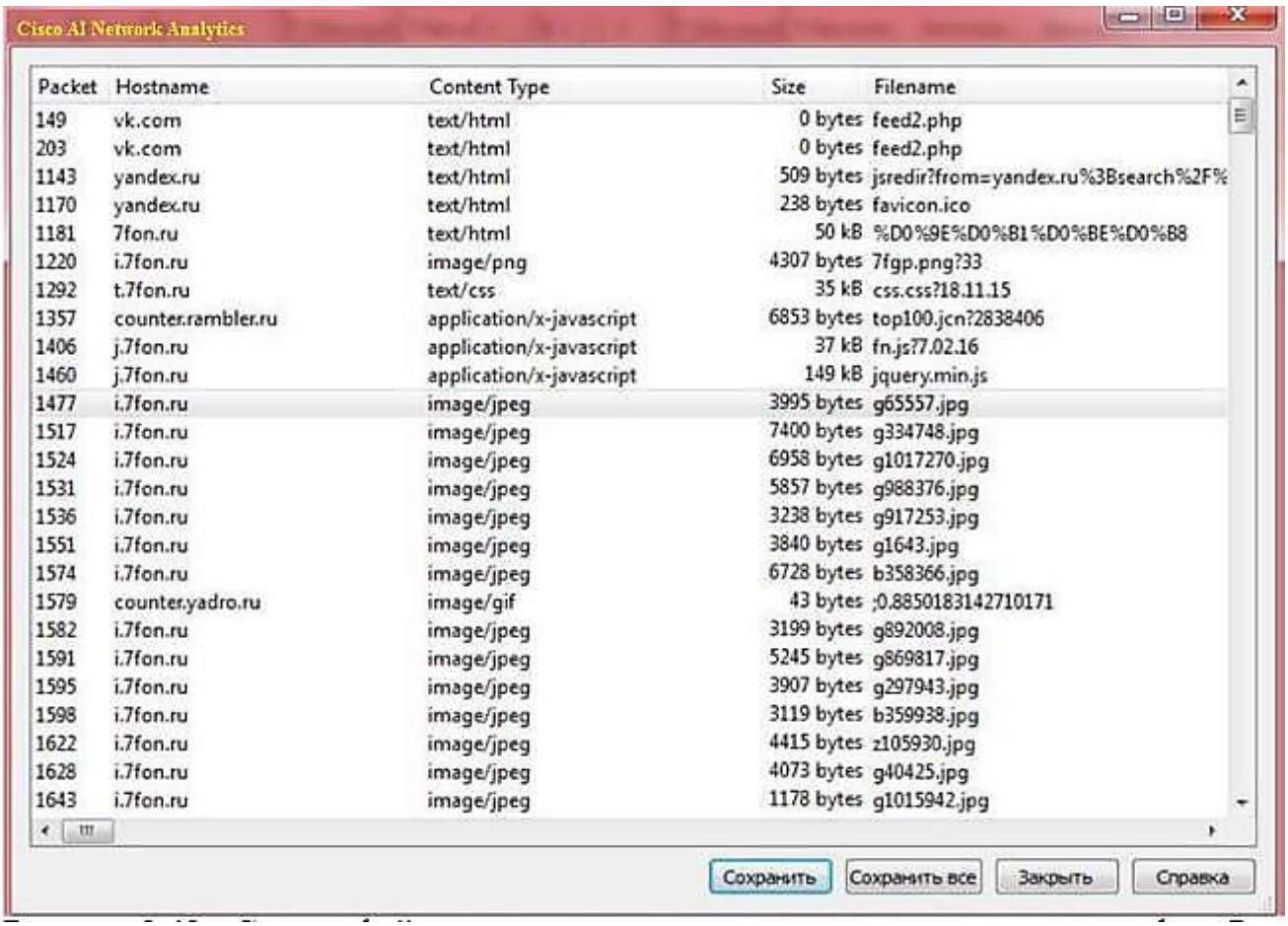


Рисунок 3.4 – Список файлів які можна витягти із захопленого трафіку

Режим візуалізації в Cisco AI Network Analytics дозволяє відслідковувати переміщення даних по мережі, появу і зміну параметрів IP-пакетів при їх проходженні через мережеві пристрої, а також швидкість і шляхи переміщення цих пакетів. Аналіз подій, що відбуваються в мережі, допомагає зрозуміти механізми її роботи і виявляти несправності. Під час аналізу мережевого трафіку локальної мережі за допомогою системного інструменту можна виявити наявність пакетів з помилками або попередженнями [7, с. 15].

Для цього існує спеціальний інструмент, передбачений Cisco AI Network Analytics. Expert Information-журнал в якому відображені помилки, попередження, примітки, викликані мережевими «аномаліями» [45] (рис. 3.5.).

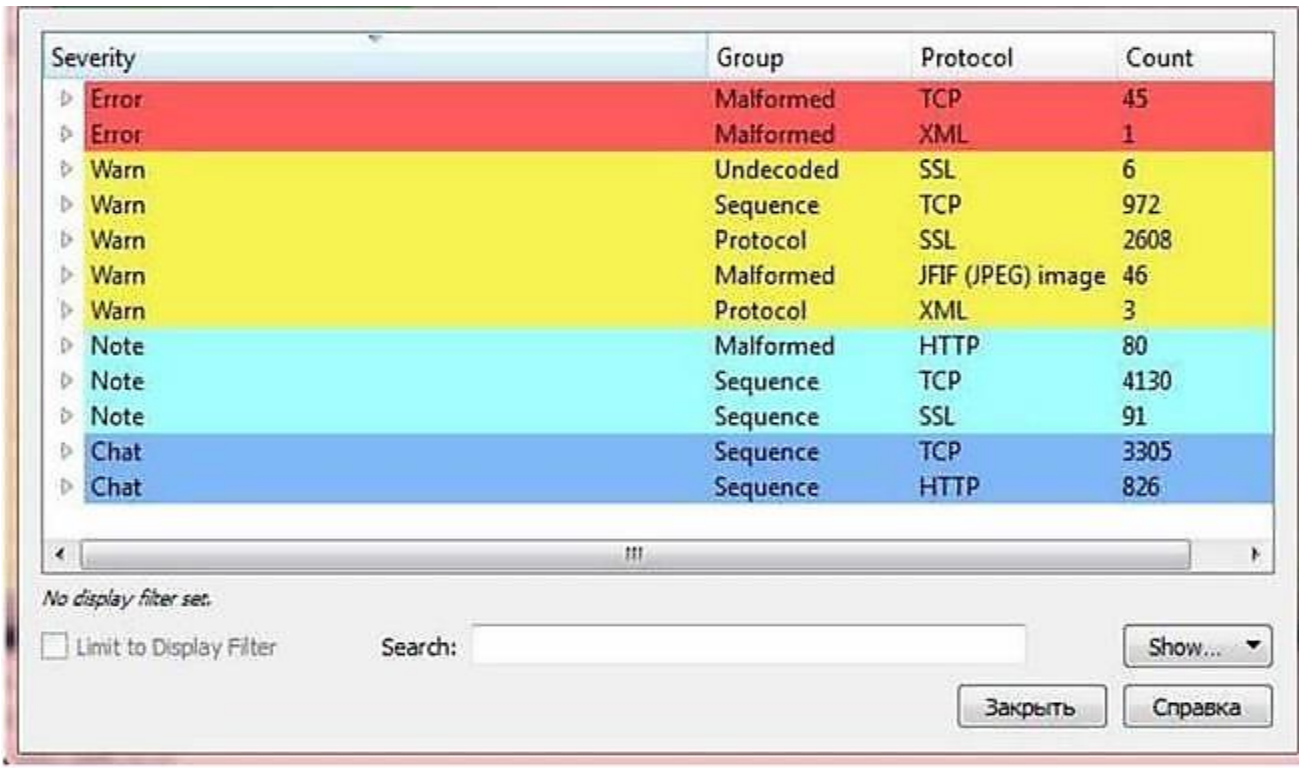


Рисунок 3.5 – Результати пошуку помилок корпоративної мережі за допомогою Cisco AI Network Analytics

Cisco AI Network Analytics має досить зручний інтерфейс, що відображає поведінку мережі. Наявність такого інструменту дозволяє досить швидко виявляти помилки, ніж аналізувати всі пакети вручну. В даному вікні відображена інформація, яка поділена на групи Errors, Warnings, Notes, Chats [44]:

– Errors-помилки, виділені червоним кольором.
– Warnings-попередження, виділені жовтим кольором.
– Notes-примітки, виділені блакитним кольором.
– Chat-чат, виділений синім кольором [8, с. 102].

Для детального опису всіх пошуків та перевірок у текстовому форматі можна використовувати модуль, написаний на мові програмування Python. Наприклад, розглянемо процес аналізу даних для вилучення інформації з локального конфігураційного файлу комп’ютерної мережі за допомогою Cisco AI Network Analytics. У цьому прикладі наведений скрипт на мові Python. Для використання системи необхідно підключити модуль cisco_analyzer, який надає

можливість отримувати звіт про конфігурацію обладнання. Також можливо отримати звіт щодо конкретного сервісу [46]. Приклад створення звіту по сервісу DHCP:

```
import cisco_analyzer def main():
config_filename = «/path / to / config / file»
config = load_config (config_filename)
check = cisco_analyzer. ConfigAnalyzer()
dhcp = check. dhcp (config)
```

DHCP, або протокол динамічного налаштування вузла, є мережевим протоколом, що дозволяє комп’ютерам отримувати IP-адресу та інші параметри для роботи в мережі автоматично. Цей протокол працює за схемою "клієнт-сервер", де комп’ютери запитують конфігурацію у DHCP-сервера. Це уникне необхідності ручного налаштування адрес для кожного комп’ютера і допомагає уникнути помилок.

При аналізі неполадок DHCP важливо враховувати різні можливі причини, такі як проблеми з ПЗ операційної системи, драйверами мережевого адаптера або агентами DHCP-ретрансляції. Однак найбільш поширеною є неправильна конфігурація.

З урахуванням багатьох потенційних проблемних зон при аналізі та виправленні неполадок в корпоративних мережах важливо мати систематичний підхід до виявлення помилок.

1. Вирішення конфліктів IP-адрес. Коли термін оренди IP-адреси клієнта закінчується, DHCP-сервер може намагатись перепризначити цю адресу іншому клієнту. Однак, якщо перепризначення не відбувається, і клієнт перезавантажується, він може використовувати адресу, яка була йому присвоєна раніше. Це може спричинити конфлікт, коли два клієнти намагаються використовувати одну і ту ж IP-адресу.

Команда "show ip dhcp conflict" виводить всі конфліктні адреси, які зареєстровані DHCP-сервером. Для виявлення клієнта, який викликає конфлікт, сервер може використовувати команду ping. Після виявлення конфлікту, адреса

видаляється з пулу адрес і не присвоюється іншому клієнту до тих пір, поки адміністратор не вирішить конфлікт [12, с. 110].

Вихідні дані відображують IP-адреси, DHCP, що конфліктують з сервером. У даних вказаний метод виявлення (detection method) і час виявлення (detection time) конфліктуючих IP-адрес, запропонованих сервером DHCP:

```
R1# show ip dhep conflict
IP address Detection Method Detection time
192.168.10.32 Ping Feb 16 2017 12:28 PM
192.168.10.64 Gratuitous ARP Feb 23 2017 08:12 AM
```

2. Перевірка фізичного з'єднання в комп'ютерній мережі включає в себе перевірку статусу інтерфейсу маршрутизатора, що виступає в якості основного шлюзу для клієнта. Для цього використовується команда "show interfaces interface". Якщо статус інтерфейсу не "up", це може призвести до того, що трафік, включаючи запити DHCP-клієнта, не буде проходити через цей порт.

3. Перевірка зв'язності з використанням статичної IP-адреси може бути корисною при пошуку неполадок в роботі DHCP. Це виконується шляхом налаштування статичної IP-адресації на клієнтській робочій станції. Якщо робоча станція не може отримати доступ до мережевих ресурсів, незважаючи на статично налагоджену IP-адресу, то DHCP не є джерелом проблеми, і необхідно провести перевірку мережевого підключення.

4. Перевірка налаштування порту комутатора включає спробу отримати IP-адресу від DHCP-сервера вручну, відправивши DHCP-запит з пристрою-клієнта у випадку, якщо DHCP-клієнт не може отримати IP-адресу від DHCP-сервера при завантаженні.

5. Діагностика роботи протоколу DHCP в тій же підмережі або VLAN передбачає перевірку, чи працює DHCP коректно в якості DHCP-сервера, коли клієнт знаходиться в тій же підмережі або VLAN. Якщо протокол DHCP працює правильно, але проблема виникає з агентом DHCP-ретрансляції, це може свідчити про проблему з агентом. Якщо неполадки продовжуються, навіть після перевірки роботи DHCP як DHCP-сервера в тій же підмережі або VLAN, проблема, ймовірно, полягає в DHCP-сервері.

Подамо приклад підключення до мережевого обладнання за допомогою протоколу SSH і отримання конфігураційного файлу. Вирішення цієї проблеми може бути представлене таким кодом:

```
import cisco_analyzer
def main():
device = SSH()
auth = ['192.168.0.5', 'root', 'root']
config = device. ssh_connect (auth, 'show running-config')
check = cisco_analyzer. ConfigAnalyzer()
dhcp = check. dhcp (config)
```

Результат звіту для цього прикладу включає наступну інформацію:

- дата створення звіту;
- назва обладнання;
- аутентифікаційні дані, якими виконано підключення до обладнання. Якщо дані були отримані з локального файлу, поле буде порожнім;
- проаналізовані дані. Якщо використовувався аналіз конкретного протоколу або сервісу, звіт буде містити лише ці дані. В іншому випадку будуть відображені всі доступні параметри конфігураційного файлу операційної системи Cisco IOS.

Cisco AI Network Analytics емулює як апаратну, так і програмну частину мережевого обладнання. Це дозволяє створювати копії великих мережевих інфраструктур. Однак емульовані пристрої не підтримують таку велику кількість технологій, які використовуються в реальних великих мережах, та багато функцій, доступних в реальних пристроях, просто відсутні [1, с. 28].

3.3 Програмний рівень виявлення шкідливого мережевого трафіку в комп’ютерній мережі

Завдання оцінки якості обслуговування є важливим у виявленні аномалій в мережевому трафіку проєктованих систем. Мережевий трафік сучасних інформаційних систем має самоподібні властивості, що потребує ефективних методів моделювання процесів трафіку і завантаження в таких мережах.

У даному проєкті планується використання методу статистичного моделювання дробового броунівського руху для виявлення аномалій в мережевому трафіку. Цей метод ґрунтується на властивості стаціонарних приростів у дробовому броунівському русі, що дозволяє побудувати реалізацію руху з заданою проекцією.

Узагальнений Вінерівський процес (дробовий броунівський рух) з індексом Херста H є (0, l) називається гаусівський процес WH (t), t є [6,1] такий, що WH (0) = 0, EWH (t) = 0 і кореляційною функцією:

$$R_H(t,s) = \frac{1}{2}\left(|t|^{2H} + |s|^{2H} - |t-s|^{2H}\right). \qquad (3.1)$$

Якщо H = 1 / 2, то отримаємо стандартний Вінерівський процес.

Вінерівський процес W (t) – це процес з незалежними приростами. Дробовий Броунівський рух WH (t) – це процес зі стаціонарними приростами.

Тоді випадковий процес w (t) = W_H (t + Δ) – W_H (t) з фіксованим Δ є стаціонарним гаусівським процесом з кореляційною функцією.

$$Ew(t+\tau)w(t) = \frac{1}{2}\left(|\tau+\Delta|^{2H} + |\tau-\Delta|^{2H} - 2|\tau|^{2H}\right) \qquad (3.2)$$

і спектральна щільність:

$$g(\lambda) = \frac{A^2}{\pi}\left(\frac{1-\cos(\lambda\Delta)}{|\lambda|^{2H+1}}\right), \lambda \in (-\infty,+\infty) \qquad (3.3)$$

де:

$$A^2 = \left(\frac{2}{\pi}\int_0^{\infty}\frac{1-\cos(\lambda)}{\lambda^{2H+1}}d\lambda\right)^{-1} = \left(-\frac{2}{\pi}\Gamma(-2H)\cos(H\pi)\right)^{-1} \qquad (3.4)$$

Оскільки WH (0) = 0, то будь-яку модель дробового броунівського руху можна зобразити:

$$W_H(t+\Delta) = W_H(t) + w(t) \qquad (3.5)$$

Моделювання дробового броунівського руху включає моделювання гаусівського стаціонарного процесу. Ці методи моделювання стаціонарних

гаусівських процесів були детально вивчені в численних дослідженнях [11, с. 78].

Нехай ξ (t) – дійсний гаусівський стаціонарний випадковий процес з кореляційною функцією R (τ) і спектральною функцією:

$$F(\lambda), \quad R(\tau) = \int_0^{\infty} \cos(\lambda t) dF(\lambda) \tag{3.6}$$

Гаусівський стаціонарний випадковий процес можна представити у вигляді:

$$\xi(t) = \int_0^{\infty} \cos(\lambda t) d\xi_1(\lambda) + \int_0^{\infty} \sin(\lambda t) d\xi_2(\lambda) \tag{3.7}$$

де ξ 1 (t) та ξ2 (t) – центровані і некорельовані випадкові процеси, такі що при 0 < λ1<λ2 має місце:

$$E(\xi_1(\lambda_2) - \xi_1(\lambda_1))^2 = F(\lambda_2) - F(\lambda_1),$$
$$E(\xi_2(\lambda_2) - \xi_2(\lambda_1))^2 = F(\lambda_2) - F(\lambda_1). \tag{3.8}$$

Нехай DΛ – деяке розбиття інтервалу [6, Λ]. Модель випадкового процесу ξ (t) може бути представлена у вигляді:

$$E(\eta_{1i})^2 = E(\eta_{2i})^2 = F(\lambda_{i+1}) - F(\lambda_i). \tag{3.9}$$

Тобто випадковий процес w (t) можна представити у вигляді:

$$w(t) = \int_0^{\infty} \cos(\lambda t) d\xi_1(\lambda) + \int_0^{\infty} \sin(\lambda t) d\xi_2(\lambda). \tag{3.10}$$

Для розбиття/модель випадкового процесу w (t) має вигляд:

$$w_n(t, \Lambda) = \sum_{k=0}^{n-1} (\sin(\lambda_k t) X_k + \cos(\lambda_k t) Y_k), \tag{3.11}$$

де $\{X_k, У_k\}$ – некорельовані субгаусівські випадкові величини з $EX_k = EУ_k = 0$ і

$$E(X_k)^2 = E(Y_k)^2 = \int_{\lambda_k}^{\lambda_{k+1}} g(\lambda) d\lambda. \tag{3.12}$$

Нехай випадковий процес X (t) і всі Xn (t, Λ) належать деякому функціональному простору A (T). Нехай дано два числа: δ > 0 і 0 < ε < 1.

Ця модель дозволяє створити набір методів для покращення виявлення аномалій в мережевому трафіку, який використовує технологію MPLS.

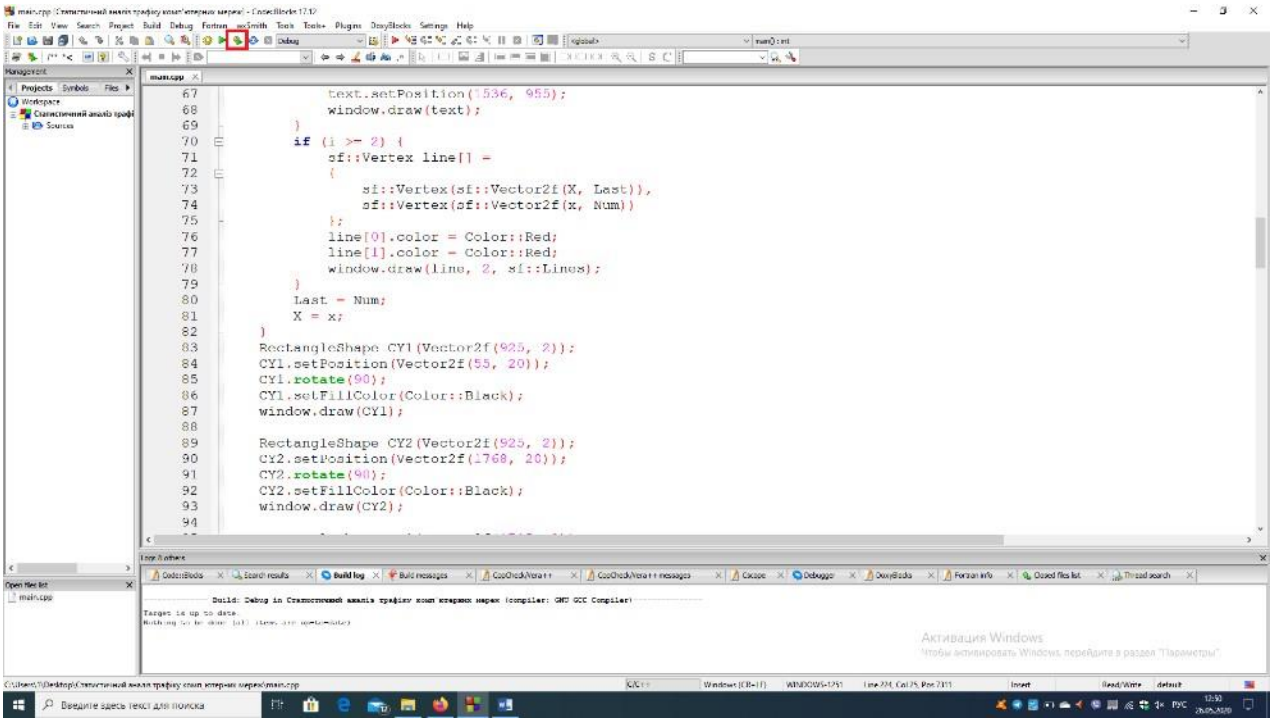


Рисунок 3.6 – Робоче вікно запуску розробленого коду

На основі математичної моделі будемо розробляти програмний код для аналізу трафіку, який надходить на сервер. Для початку роботи з програмою, необхідно завантажити папку "Статистичний аналіз трафіку комп'ютерних мереж". У цій папці відкрийте файл "Статистичний аналіз трафіку комп'ютерних мереж" з розширенням ".cbp" за допомогою IDE "Code::Blocks". Після цього натисніть кнопку для запуску програми і виконайте запуск.

Далі, для продовження дослідження, наведемо програмний код на мові C++, який виконує статистичну обробку трафіку комп'ютерної мережі. У вихідних даних ми маємо 1000 точок трафіку. Лістинг програмного коду для виявлення аномалій в мережевому трафіку проєктованої системи наведений у Додатку Б.

На рисунку 3.7 показано візуалізовані результати оцінки трафіку комп'ютерної мережі, що складається з 1000 точок, за допомогою програмного

коду на мові C++. На цьому рисунку представлена наступна інформація: відносний час отримання пакета, номер пакета, параметри відображення часу, кількість використаних даних трафіку. Конфігурацію інтерфейсу можна легко змінити в меню View.

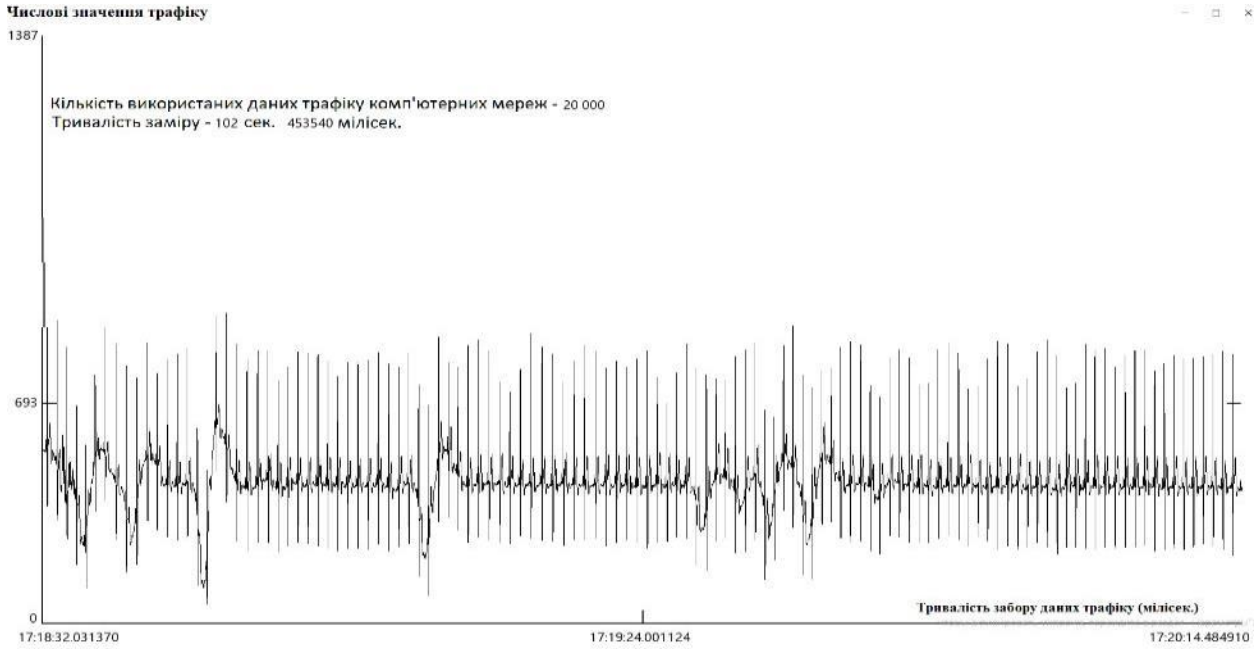


Рисунок 3.7 – Схематичне зображення зміни трафікового навантаження на сервер проєктованої мережі з часом

На рис. 3.7 зображено частину добового трафіку досліджуваної системи, що візуалізована за допомогою програмного коду.

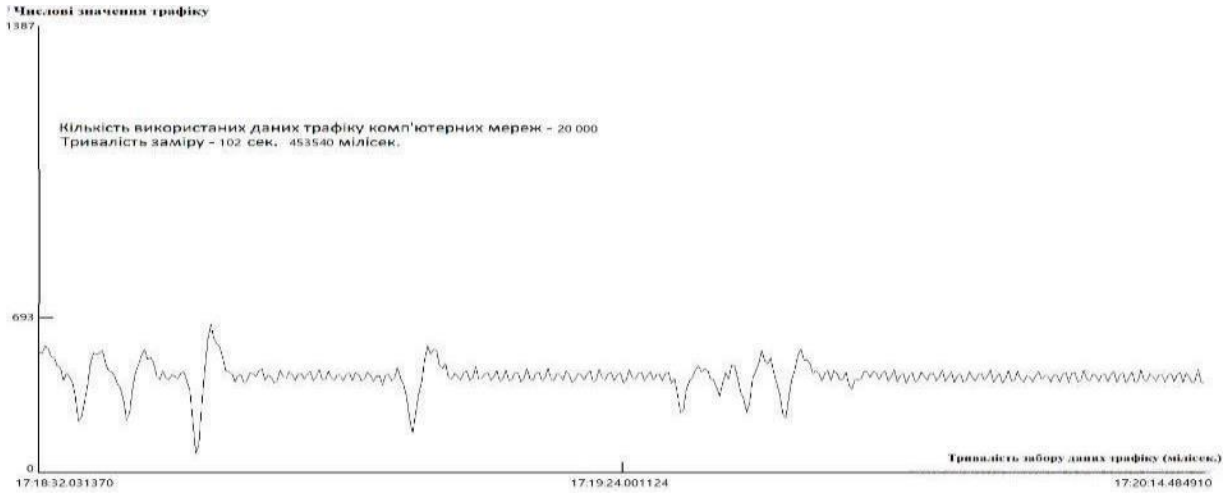


Рисунок 3.8 – Схематичне зображення аномального трафікового навантаження на сервер проєктованої мережі

На рисунку 3.8 показано, що графік зміни середньої кількості пакетів має такий самий характер, як графік сумарного трафіку, але з відзначенням на ньому аномального трафіку, який не відповідає загальним правилам користувацьких запитів (рисунок 3.9).

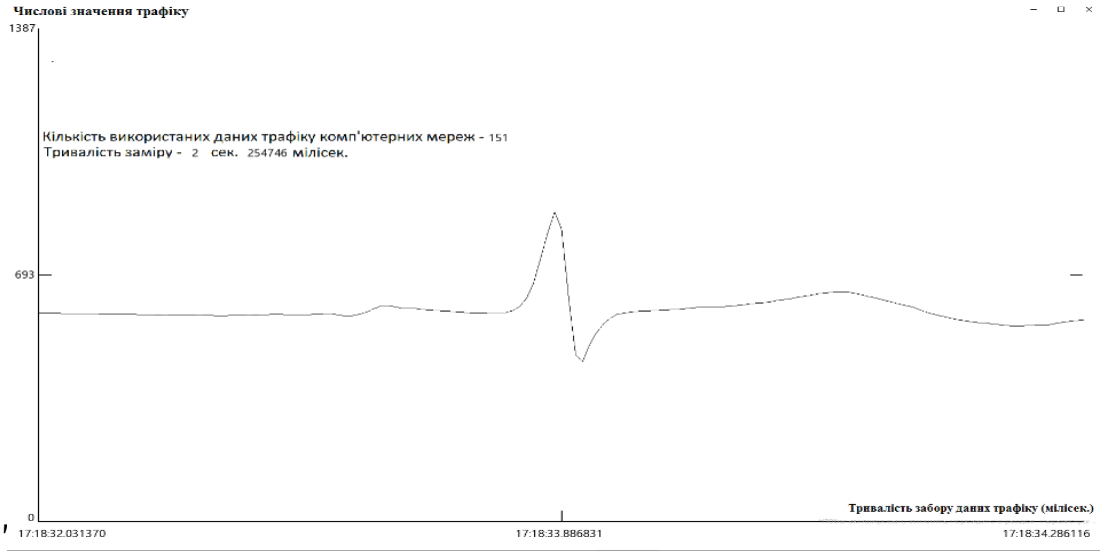


Рисунок 3.9 – Графічний вигляд аномального пікового навантаження на сервер проєктованої мережі під час зміни його інтенсивності

Рисунок 3.9 – Робоче вікно проектованого додатку

Рисунок 3.9 показує, що середній розмір аномальних даних у пакетах мало залежить від завантаження мережі. У той же час встановлено, що характер зміни швидкості передавання пакетів, навпаки, залежить від завантаження мережі.

Отже, аналіз трафіку комп'ютерних мереж виконується за допомогою програмного коду, що моделює різні аспекти мережевого трафіку. Використання методів статистичного моделювання, таких як дробовий броунівський рух, дозволяє ефективно виявляти аномалії в мережевому трафіку. Під час аналізу важливо враховувати зміну середнього розміру пакетів і швидкості передавання в залежності від завантаження мережі.

ВИСНОВКИ

У роботі проведено аналіз основних підходів до класифікації неполадок комп'ютерних мереж та методів їх діагностування, масштабування, оптимізації пропускної здатності та аналізу доступності. Зокрема, розглянуто класифікацію мережевих несправностей за Хогдаллом, яка пропонує структуру для систематизації різних типів проблем.

Досліджено історію розвитку інтелектуальних інформаційних технологій, зокрема їх основні проблеми. Описано засоби діагностування помилок у комп'ютерних мережах, такі як системи управління мережею (HP OpenView, Sun NetManager, IBM NetView, Tivoli), вбудовані системи діагностики та управління, аналізатори протоколів, мережеві монітори, кабельні сканери (Microtest Inc., Fluke Corp., Datacom Technologies Inc., Scope Communication Inc.), а також багатофункціональні пристрої аналізу.

Також описано особливості створення сучасних інтелектуальних навчальних систем, зокрема їх архітектуру. Унікальною особливістю інтелектуальних інформаційних технологій є їх універсальність. Розглянуто призначення та принцип роботи елементів штучного інтелекту для пошуку та усунення неполадок у комп'ютерних мережах.

Отже, у ході дослідження було проведено всебічний аналіз методів масштабування, оптимізації пропускної здатності та аналізу доступності корпоративних мереж. Вивчення основних підходів до класифікації та діагностики мережевих несправностей допомогло виявити критичні моменти, які впливають на стабільність та ефективність роботи мережі. Використання інтелектуальних інформаційних технологій, таких як Cisco AI Network Analytics, дозволило не лише автоматизувати процес виявлення та усунення неполадок, але й значно підвищити точність і швидкість їх вирішення. У практичній частині дослідження описано використання Cisco AI Network Analytics для пошуку та усунення неполадок у комп'ютерних мережах. Показано графічний інтерфейс програми, процес фільтрації трафіку та послідовність роботи із захопленим

трафіком. Оцінено перспективи використання штучного інтелекту для покращення пошуку та усунення неполадок у комп'ютерних мережах.

Проект також містить опис розробки програмного рівня для виявлення шкідливого мережевого трафіку у комп'ютерних мережах за допомогою методу статистичного моделювання дробового броунівського руху для виявлення аномалій у мережевому трафіку. Цей метод використовує властивість стаціонарних приростів у дробовому броунівському русі та створює реалізацію руху з заданою проекцією.

На основі математичної моделі описано розробку програмного коду для аналізу трафіку навантаження на сервер. Для запуску програми необхідно завантажити папку "Статистичний аналіз трафіку комп'ютерних мереж" і відкрити файл "Статистичний аналіз трафіку комп'ютерних мереж" з розширенням ".cbp" за допомогою програми "Code::Blocks IDE". Після цього слід натиснути кнопку для запуску програми та продовжити виконання.

Розробка методів виявлення аномального трафіку за допомогою статистичного моделювання дробового броунівського руху показала високу ефективність у запобіганні та виявленні мережевих загроз. Використання математичних моделей для аналізу мережевого навантаження забезпечило можливість більш точного прогнозування та управління ресурсами мережі.

Отримані результати підтверджують, що інтеграція штучного інтелекту у процеси управління та діагностики мереж є перспективним напрямом, що забезпечує підвищення продуктивності, стабільності та безпеки корпоративних мереж. Рекомендовано продовжувати дослідження в цій галузі з метою розробки нових підходів та інструментів для покращення якості та надійності мережевих інфраструктур.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Адміністрування комп’ютерних мереж та операційних систем. Розробник: к. т. н., доц. Поліщук В. В. Ужгород: 2019. 60 с.
2. Блозва А. І., Матус Ю. В. Комп’ютерні мережі [навчальний посібник] / А. І. Блозва, Ю. В. Матус. Київ: Компрінт, 2017. 821 с.
3. Вілсон Е. Моніторинг та аналіз мереж. Методи виявлення неполадок: [Пер. з англ.]. Ед Вілсон. Київ: Лорі-К, 2011. 476 с.
4. Дороганов В. С. Можливі проблеми, які виникають при створенні штучного інтелекту. *Вісник СумДУ*. Суми, 2017. №5 (99). С. 34–42.
5. ДСТУ ISO / TR 13335–2–2003 Інформаційні технології. Настанови з керування безпекою інформаційних технологій (ІТ). Частина 2. Керування та планування безпеки ІТ.
6. ДСТУ ГОСТ 28147:2009 Системи обробки інформації. Захист криптографічний. Алгоритми криптографічного перетворення.
7. Дуднік А. С. Діагностика персонального комп’ютера. Київ: МАУП, 2019. 21с.
8. Евдокимов А. Ю. Трохи про штучний інтелект. *Вісник СумДУ*. Суми, 2018. № 3. С. 101–104.
9. Експлуатація об’єктів мережевої інфраструктури: Підручник для студ. установ середовищ. проф. освіти. А. В. Назаров, В. П. Мельников, А. І. Купріянов. Київ: Лорі-К, 2014. 538 с.
10. Каллан Робертс. Основні концепції нейронних мереж. Каллан Робертс. Київ: Інтерком, 2013. 287 с.
11. Колесніков А. В. Гібридні інтелектуальні системи. Технологія розробки / А. В. Колесніков. *Вісник СумДУ*. Суми, 2011. 111 с.
12. Комп’ютерні мережі. Навчальний курс: офіційний посібник Microsoft для самостійної підготовки: [Пер. з англ.] / корпорація Майкорософт. Київ: Інтерком, 2018. 522 с.

13.Комп’ютерні мережі. Принципи, технології, протоколи: Підручник для університетів. 2-е видання. / В. Г. Оліфер. Київ: Інтерком, 2018. 864 с.

14.Коцовський В. М. Методи та системи штучного інтелекту: конспект лекцій / В. М. Коцовський. Ужгород, 2016. 76 с.

15.Кулаков Ю. О., Луцький Г. М. Комп’ютерні мережі. Підручник / за ред. Ю. С. Ковтанюка. Київ: Юніор, 2003. 400 с.

16.Лохін В. М. Інтелектуальні системи управління: поняття, визначення, принципи побудови / В. М. Лохін. *Мехатроніка*. 2013. №2. С. 27–35.

17.Маношин Д. А. Програмування штучного інтелекту // Colloquium-journal. 2019. №12 (36). С. 102–110.

18.Морхат П. М. Штучний інтелект: правовий погляд. Київ: Буки Веди, 2017. 257 с.

19.Нікітіна Л. О. Моделі та методи штучного інтелекту у комп’ютерних іграх. / Л. О. Нікітіна, С. О. Нікітін. Харків: Друкарня Мадрид, 2018. 102 с.

20.Оліфер в. г. Комп’ютерні мережі: принципи, технології, протоколи / В. Г. Оліфер, Н. А. Оліфер. 4-е изд. Київ: Інтерком, 2012. 958 с.

21.Оліфер В. Г. Нові технології та обладнання IP мереж / В. Г. Оліфер, Н. А. Оліфер. СПб.: БХВ, 2012. 512 с.

22.Оліфер В. Г. Стратегічне планування мереж масштабу підприємства / В. Г. Оліфер, Н. А. Оліфер. Харків: Центр Інформаційних Технологій, 2010. 680 с.

23.Організація комп’ютерних мереж / Ю. А. Тарнавський, І. М. Кузьменко. Київ: КПІ ім. Ігоря Сікорського, 2018. 259 с.

24.Основи адміністрування LAN у середовищі MS Windows. Навчальний посібник / Б. А. Демида, К. М. Обельовська, В. С. Яковина. Львів: Видавництво Львівської політехніки, 2013. 488 с.

25.Остроух А. В. Основи побудови систем штучного інтелекту для промислових і будівельних підприємств: монографія / А. В. Остроух. Київ: Інтерком, 2008. 280 с.

26.Поняття штучного інтелекту. URL: http: // megalib. com. ua / content / 1956_71_Ponyattya_shtychnogo_intelekty. html. (дата звернення: 1.06.2024).
27.Потапов А. С. Технології штучного інтелекту. Харків: Інтелект, 2010. 218с.
28.Пройдаков Е. М. Сучасний стан штучного інтелекту. *Наукові дослідження.* 2018. №2018. С. 89–96.
29.Пупков К. А. Інтелектуальні системи. К. А. Пупков, в. г. Коньков. Харків: Інтелект, 2013. 148 с.
30.Ретана А. Принципи проектування корпоративних IP мереж. А. Ретана, Д. Слайс, р. Уайт. Харків: Інтелект, 2012. 368 с.
31.Рибіна Г. В. Основи побудови інтелектуальних систем: Навч. посібник / Г. В. Рибіна. Харків: Фінанси та статистика, 2010. 432 с.
32.Рибіна Г. В., Паронджанов С. С. Моделювання процесів взаємодії інтелектуальних агентів у багатоагентних системах. *Штучний інтелект і прийняття рішень.* 2012. № 1. С. 3–15.
33.Рудская Е. Н., Десятниченко Л. В. Штучний інтелект для бізнесу: трансформація ефективних запитів у реальні продажі. *Молодий вчений.* 2015. №8. 121–131 с.
34.Саулин Е. С. Зародження та розвиток штучного інтелекту: характеристика напрямків досліджень. Львів: Видавництво Львівської політехніки, 2016. №18 (82). С. 56–63.
35.Стадніченко С. Ю. Інтелектуальні компоненти для системи автоматизованого моніторингу та діагностики на залізничному транспорті. С. Ю. Стадніченко. *Молодий вчений.* 2012. № 11 (46). С. 98–102.
36.Суркова Н. Е. Методи проектування інформаційних систем. Н. Е. Суркова. Харків: Інтелект, 2015. 201 с.
37.Трембач В. М. Основні етапи створення інтелектуальних навчальних систем. *Програмні продукти і системи,* №3, 2012. С. 148–152.
38.Філімонов А. Ю. Побудова мультисервісних мереж Ethernet: Навчальний посібник. А. Ю. Філімонов. Харків: Інтелект, 2015. 248 с.

39.Шибайкин С. Д., Алексеєв Е. Г. Мови програмування для систем штучного інтелекту. Київ: Лорі-К, 2012. С. 21.

40.Штучний інтелект як технологія створення автоматизованих інтелектуальних систем. URL: https: // er. knutd. edu. ua / bitstr eam / 123456789 / 5044 / 1 / 20160428–29_TEZY_V3_P349. pdf. (дата звернення: 1.06.2024).

41.Штучний інтелект. Підходи і напрямки до розуміння штучного інтелекту. URL: http: // referat-ok. com. ua / informatika / shtuchnii-intelekt. (дата звернення: 1.06.2024).

42.Cisco API Console – Learn more III virl. cisco. com: Cisco API Console, 2015. URL: https: // apiconsole. cisco. com / leam_more (дата звернення: 1.06.2024).

43.Cisco API Console – Welcome to the Cisco API Console. Cisco API Console, 2015. URL: https: // apiconsole. cisco. com (дата звернення: 1.06.2024).

44.Cisco Network Simulator | IT Practice Exams | IT Training | Boson. com, 2015. URL: http: // www. boson. com (дата звернення: 1.06.2024).

45.Cisco Networking Academy: Cisco packet tracer, 2015. URL: https: // www. netacad. com / about-networking-academy / packet-tracer (дата звернення: 1.06.2024).

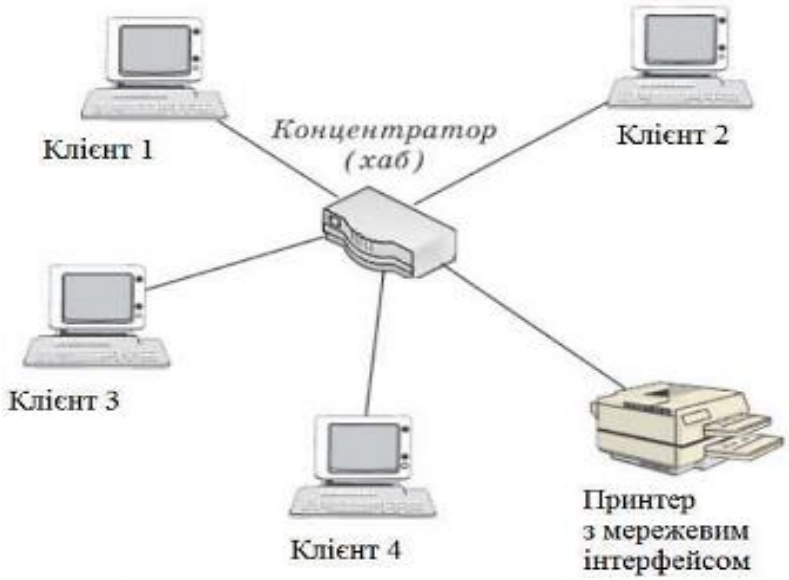
46.NetSim Cisco Network Simulator & Router Simulator. URL: http: // www. boson. com / netsim-cisco-network-simulator (дата звернення: 1.06.2024).

47.OSPF. URL: http: // www. cisco. com / cisco / web / support / RU / 9 / 92 / 92027_1. html (дата звернення: 1.06.2024).

ДОДАТКИ

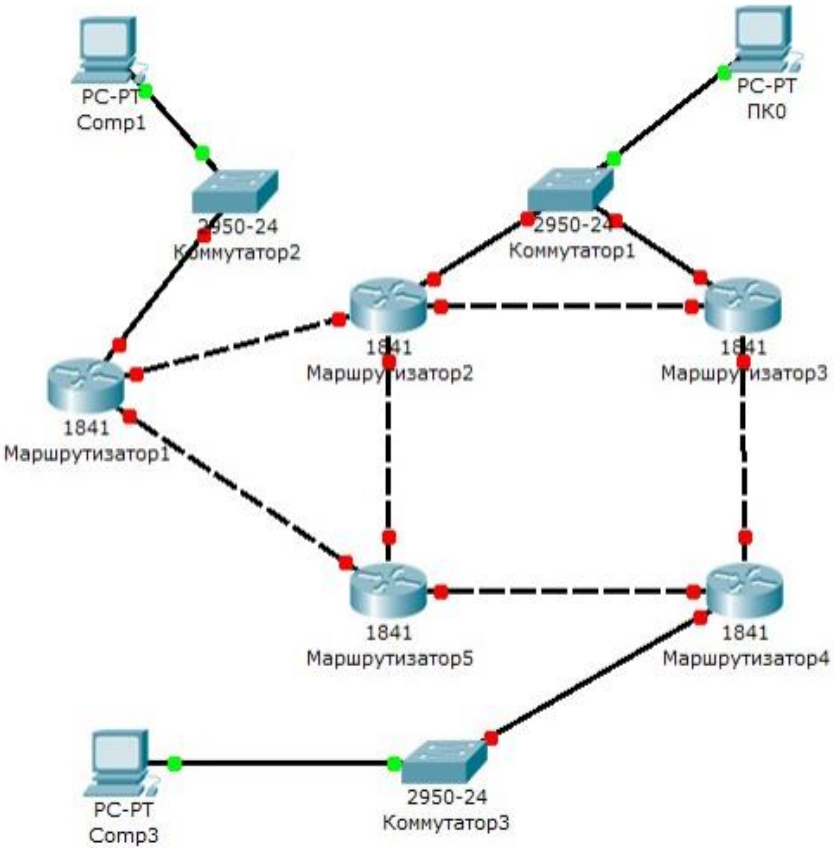
Додаток А

Графічне представлення простої локальної мережі



Додаток Б

Схематичний вигляд комп’ютерної мережі в дослідженні



Додаток В

Зовнішній вигляд обладнання Cisco із елементами штучного інтелекту в комп’ютерній мережі