Міністерство освіти і науки України
Харківський національний університет радіоелектроніки

Факультет інфокомунікацій
(повна назва)

Кафедра інформаційно-мережної інженерії
(повна назва)

КВАЛІФІКАЦІЙНА РОБОТА
Пояснювальна записка

рівень вищої освіти другий (магістерський)

Особливості планування локальної мережі підземної лікарні

(тема)

Виконав:
здобувач 2 року навчання,
групи ІМІм-23-1

Усов О.О.
(прізвище, ініціали)

Спеціальність 172 «Електронні комунікації та радіотехніка»
(код і повна назва спеціальності)

Тип програми освітньо-професійна
(освітньо-професійна або освітньо-наукова)

Освітня програма Інформаційно-мережна інженерія
(повна назва освітньої програми)

Керівник доц. Харченко Н.А.
(посада, прізвище, ініціали)

Допускається до захисту

Зав. кафедри _____ Безрук В.М.
(підпис) (прізвище, ініціали)

2025 р.

Не містить відомостей заборонених до відкритого публікування

Студент _____ / Усов О.О./

Керівник _____ / Харченко Н.А./

Харківський національний університет радіоелектроніки

Факультет інфокомунікацій

Кафедра інформаційно-мережної інженерії

Рівень вищої освіти другий (магістерський)

Спеціальність 172 Електронні комунікації та радіотехніка

Тип програми освітньо-професійна
(код і повна назва)

Освітня програма інформаційно-мережна інженерія
(повна назва)

ЗАТВЕРДЖУЮ:
Зав. кафедри _____
(підпис)
«____»_____ 2024 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

здобувачеві Усову Олександру Олексійовичу
(прізвище, ім'я, по батькові)

1. Тема роботи Особливості планування локальної мережі підземної лікарні

затверджена наказом університету від 28 жовтня 2024 р. № 1148 Ст

2. Термін подання студентом роботи до екзаменаційної комісії 14 січня 2025 р.

3. Вихідні дані до роботи

Провести аналіз особливостей побудови локальних мереж: топологія, адресація, настроювання обладнання. Дослідити питання забезпечення працездатності мережі, основних методів проведення діагностики та організаційно-технічних заходів по підтримці стабільного функціонування мережі. Провести планування локальної мережі лікарні, що розміщується на трьох підземних рівнях. Забезпечити настроювання мережі з розподілом різних пріоритетів для клієнтів та робочого персоналу. Дослідити особливості захисту інформації у таких мережах.

4. Перелік питань, що потрібно опрацювати в роботі

Вступ

1. Сучасні підходи до побудови локальних обчислювальних мереж

2. Проектування і побудова локальної мережі підземної лікарні

3. Логічна організація, перевірка рівня безпеки та працездатності локальної мережі

Висновки

5. Перелік графічного матеріалу із зазначенням креслеників, схем, плакатів, комп'ютерних ілюстрацій (п.5 включається до завдання за рішенням випускової кафедри) _____

Слайди у форматі Power Point (назва та мета роботи, узагальнена схема процесу аналізу збоїв у мережі, основні підходи до побудови локальних мереж, основні методи проведення діагностики та організаційно-технічних заходів у локальній мережі, завдання автоматизації підтримки процесу забезпечення працездатності обчислювальної мережі, методика автоматизації пошуку компонентів мережі, що спричинили порушення її функціонування, загальні принципи побудови локальних мереж, схема розміщення обладнання на першому рівні підземної лікарні, вертикальна підсистема для підземної лікарні, динамічне призначення VLAN на комутаторі, схема тестового стенду для перевірки 802.1x авторизації, висновки)

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Терміни виконання етапів роботи	Примітка
1	Ознайомлення із завданням. Уточнення ТЗ.	28.10.2024	виконано
2	Підбір літератури за темою роботи	27.10-18.11.2024	виконано
3	Сучасні підходи до побудови локальних обчислювальних мереж	19.11-03.12.2024	виконано
4	Проектування і побудова локальної мережі підземної лікарні	04.12-19.12.2024	виконано
5	Логічна організація, перевірка рівня безпеки та працездатності локальної мережі	20.12.2024-07.01.2025	виконано
6	Оформлення презентаційного матеріалу, підготовка до захисту у ЕК	08.01.-13.01.2025	виконано

Дата видачі завдання 28 жовтня 2024 р.

Здобувач _____
(підпис)

Керівник роботи _____ доц. Харченко Н.А.
(підпис) (посада, прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 82 с., 6 рис., 1 табл., 2 додатки, 26 джерел.

Об'єктом дослідження є особливості побудови локальної мережі підземної лікарні.

Мета роботи - аналіз комплексу заходів необхідних для планування та побудови локальної мережі у підземному приміщенні.

Побудова локальних підземних мереж критичних об'єктів, таких як лікарні, є надзвичайно важливим завданням. Одним із ключових аспектів є використання дротових підключень для забезпечення стабільного зв'язку. Також, з точки зору функціонування такі локальні мережі повинні мати високу відмовостійкість і своєчасне виявлення несправностей. Це в свою чергу зобов’язує під час планування звертати увагу на впровадження систем моніторингу стану мережі та приділяти особливу увагу захисту як обладнання так і даних, що передаються. Робота фокусується на дослідженні, проєктуванні, встановленні та налаштуванні інфраструктури локальної мережі в підземній лікарні.

ТОПОЛОГІЯ, АДРЕСАЦІЯ, АВТОМАТИЧНА СИСТЕМА УПРАВЛІННЯ, ОРГАНІЗАЦІЙНО-ТЕХНІЧНІ ЗАХОДИ, ЗАХИСТ ІНФОРМАЦІЇ, 802.1X, VLAN

THE ABSTRACT

Explanatory note: 82 p., 6 fig, 1 tables, 26 sources, 2 app.

The object of the study is the peculiarities of building a local network of an underground hospital.

The purpose of this paper is to analyse the set of measures required for planning and building a local area network in an underground facility.

Building local underground networks for critical facilities such as hospitals is a critical task. One of the key aspects is the use of wired connections to ensure stable communication. Also, in terms of operation, such local networks must have high fault tolerance and timely fault detection. This, in turn, requires that planning should focus on the implementation of network monitoring systems and pay special attention to the protection of both equipment and transmitted data. The work focuses on the research, design, installation, and configuration of the local network infrastructure in an underground hospital.

TOPOLOGY, ADDRESSING, AUTOMATIC CONTROL SYSTEM, ORGANISATIONAL AND TECHNICAL MEASURES, INFORMATION SECURITY, 802.1X, VLAN

ЗМІСТ

С.

ПЕРЕЛІК СКОРОЧЕНЬ

ACL – Access Control List – списки контролю доступу;

CALS – Continuous Acquisition and Life cycle Support – безперервна інформаційна підтримка життєвого циклу виробництва;

IP – Internet Protocol – інтернет протокол;

IPv4 – Internet Protocol version 4 – четверта версія інтернет-протоколу;

RADIUS – Remote Authentication Dial In User Service – мережевий протокол, що забезпечує централізовану аутентифікацію;

RAID – Redundant Array of Independent Disks – надлишковий масив незалежних (самостійних) дисків;

SNMP – Simple Network Management Protocol – простий протокол керування мережею;

UTP – Unshielded Twisted Pair – неекранована кручена пара;

VLAN – Virtual Local Area Network – віртуальна локальна комп'ютерна мережа;

АРМ – автоматизоване робоче місце;

АСУП – автоматична система управління підприємством;

БД – база даних;

ІБ – інформаційна безпека;

КОТЗ – комплекс організаційно-технічних заходів;

ЛОМ – локальна обчислювальна мережа;

ЛПР – людина, що приймає рішення;

МІС – медична інформаційна система;

ОС – операційна система;

СППР – система підтримки прийняття рішень.

ВСТУП

Побудова локальних підземних мереж критичних об'єктів, таких як лікарні, є надзвичайно важливим завданням. Одним із ключових аспектів є використання дротових підключень для забезпечення стабільного зв'язку. Дротові підключення забезпечують високу швидкість передачі даних та стійкість мережі. Для побудови локальних мереж підземних лікарень необхідно використовувати кабелі із захистом від впливу довкілля [1].

Для ефективної побудови та керування мережею одним із головних факторів є планування структурованої кабельної мережі. Адже підземні критичні об’єкти мають свої особливості та вплив на кабельну мережу та мережне обладнання.

Одним із ключових компонентів локальних підземних мереж є сервер, який забезпечує зберігання та обробку даних. Важливо розміщувати сервери в окремих приміщеннях, щоб забезпечити їх захист від впливу зовнішнього середовища та забезпечити доступність. Для забезпечення ефективної роботи локальної мережі необхідно також передбачити систему резервного копіювання даних, щоб забезпечити їх збереження у разі збоїв у роботі мережі або апаратних збоїв [1].

З точки зору функціонування локальна мережа, що розглядається у роботі, повинна мати високу відмовостійкість і своєчасне виявлення несправностей. Це в свою чергу зобов’язує під час планування звертати увагу на впровадження систем моніторингу.

Сучасні автоматизовані системи управління виробництвом побудовані у вигляді розподілених систем, що базуються на обчислювальних мережах, під час експлуатації яких можуть виникати різні порушення роботи їх пристроїв, що роблять мережу непрацездатною. Для повернення обчислювальних мереж розподілених автоматизованих систем у режим штатного функціонування обслуговуючий мережу персонал має провести певні організаційно-технічні

заходи. Процес виявлення самих несправностей і формування комплексу заходів може зайняти значний час і істотно вплинути на функціонування системи автоматизації підприємства в цілому. Часті відмови або тривалі періоди непрацездатного стану мережі можуть призвести до повної втрати працездатності системи автоматизації підприємства. Для підвищення оперативності вжиття заходів, здатних повернути локальну обчислювальну мережу в режим штатного функціонування, необхідне проведення моніторингу мережі, який переважно залежить від людського фактора [2].

Розроблено досить багато варіантів систем моніторингу та централізованого управління мережею. Однак формування єдиного комплексу методик та засобів автоматизації процесу працездатності локальних мереж, що дозволяють знайти порушення у роботі мережних пристроїв та запропонувати оптимальний варіант їх усунення, вивчені у недостатній ступені.

В цілому, побудова локальних підземних мереж критичних об'єктів на базі дротового підключення є складним завданням, але це необхідне забезпечення ефективної роботи медичних установ. Якісне проєктування мережі, використання захищених кабелів та розміщення серверів в окремих приміщеннях допоможуть забезпечити стабільну та надійну роботу мережі. А використання систем моніторингу дозволить вчасно реагувати на несправності.

1 СУЧАСНІ ПІДХОДИ ДО ПОБУДОВИ ЛОКАЛЬНИХ ОБСЛЮВАЛЬНИХ МЕРЕЖ

1.1 Проектування та модернізація корпоративної мережі та способи підвищення її працездатності

Для сучасних підприємств актуальна проблема інтеграції розподілених автоматичних систем управління виробництвом (АСУП) і доступу до них.

Одним із перспективних напрямів розвитку інформаційних технологій стало створення в рамках підприємства єдиного інформаційного простору (або інтегрованого інформаційного середовища), що охоплює всі етапи життєвого циклу виробу. Ідея інформаційної інтеграції життєвого циклу виробу стала базовою при організації підходу, що отримав назву CALS (Continuous Acquisition and Life cycle Support - безперервна інформаційна підтримка життєвого циклу) [2].

Інформаційні потоки у мережі підприємства тісно пов'язані зі технічною складовою його інфраструктури, що представлена сукупністю мережевих пристроїв. Відповідно реорганізація мережі вплине і на зміну структури розподілених АСУП. При чому процес доопрацювання, модернізації та оперативного усунення порушень функціонування розподілених АСУП часто здійснюється на інтуїтивному рівні за допомогою неформалізованих методів, заснованих на практичному досвіді людей-експертів, що не завжди є оптимальним рішенням бо залежить від рівня експертів.

При оперативному усуненні порушень функціонування розподіленої АСУП необхідний глибокий та всебічний аналіз сучасних підходів до побудови, модернізації, оперативного усунення порушень функціонування розподілених середовищ підприємств [3].

Сучасні автоматизовані системи управління виробництвом (АСУП) підприємств будуються з урахуванням структурованої кабельної структури корпоративних мереж. Вони є складними розподіленими системами.

Обслуговуючому персоналу необхідно постійно підтримувати мережу як штатного функціонування. Це досягається шляхом зміни структури мережі або застосування систем, що управляють роботою мереж, що функціонують некоректно. Вплив на проблемні ділянки мереж представлені комплексами організаційно-технічних заходів [3].

1.1.1 Особливості, види та топології мереж

Комп'ютерна мережа – це набір вузлів, пов'язаних комунікаційною системою та забезпечених відповідним програмним забезпеченням, що надає користувачам мережі доступ до ресурсів даної системи [4].

Фізична структура мережі - форма подання інформаційно-обчислювальної мережі як взаємодіючих апаратних засобів [2].

Існують такі основні види мереж: локальні, корпоративні, глобальні.

Локальні обчислювальні мережі - це мережі, призначені для обробки, зберігання та передачі даних, і є кабельною системою об'єкта (будівлі) або групи об'єктів (будівель). На сьогоднішній день важко уявити роботу сучасного офісу без локальної обчислювальної мережі (ЛОМ, LAN – Local Area Network), без інформаційно-обчислювальної мережі зараз не обходиться ні одне підприємство. Призначення локальної інформаційно-обчислювальної мережі – забезпечити доступ до мережних (загальних) ресурсів (комп'ютерів, серверів, факсів, сканерів, принтерів тощо), даних та програм. ЛОМ знаходять широке застосування, як частина інформаційної системи тієї чи іншої фірми [4].

Правильно побудована ЛОМ, що відповідає сучасним стандартам безпеки, дозволяє отримувати доступ до необхідної інформації, забезпечує захист від несанкціонованого доступу до даних, забезпечуючи стабільну інформаційну взаємодію. Локально-обчислювальної мережі характеризують такі показники [3]:

– висока швидкість передачі інформації, велика пропускна спроможність мережі. На сьогодні прийнятна швидкість становить не менше 100 Мбіт/с;

– низький рівень помилок передачі (забезпечується високоякісними каналами зв'язку, насьогодні це дротові з’єднання по звитій парі категорії 5е та вище або оптичний кабель);

– ефективний, швидкодіючий механізм керування трафіком даних у мережі (залежить від мережного обладнання та його настроювання).

Корпоративна мережа – мережа змішаної топології, куди входять кілька локальних обчислювальних мереж, що належать одному підприємству чи корпорації.

Глобальна мережа –обчислювальна мережа, що з'єднує комп'ютери та локальні мережі, географічно віддалені великі відстані один від одного; використовує засоби зв'язку дальньої дії [3].

Під *топологією комп'ютерної мережі* зазвичай розуміється фізичне розташування комп'ютерів мережі один щодо одного та спосіб з'єднання їх лініями зв'язку. Важливо, що поняття топології належить, передусім, до локальних мереж, у яких структуру зв'язків можна легко простежити [3].

Існує три базові топології мережі: шина, зірка, кільце. Найкраще, з точки зору побудови локалььних мереж, зарекомендувала себе зірка. Вона має переваги передусім у можливості масштабування та керуванням трафіком.

1.1.2 Особливості та види мережних технологій

Мережна технологія визначає характеристики безпосередньої передачі в мережі, реалізуючи два нижніх рівня моделі OSI [2].

Ethernet – найпоширеніший стандарт локальних обчислювальних мереж. Під Ethernet зазвичай розуміють будь-який із варіантів цієї технології: Ethernet, Fast Ethernet, Gigabit Ethernet. Всі види стандартів Ethernet використовують той самий метод доступу до середовища передачі даних – метод CSMA/CD – метод колективного доступу з розпізнаванням несучої та виявленням колізій [1].

На сьогоднішній день для побудови мереж переважно застосовують технологію Fast Ethernet або Gigabit Ethernet, що працюютьь зі швидкостями 100 Мбіт/с та 1 Гбіт/с відповідно.

Мережі на цих технологіях мають ієрархічну деревоподібну структуру, побудовану на комутаторах та маршрутизаторах.

1.1.3 Фізична структура мережі та мережеве обладнання

Загалом фізичну структуру локальної обчислювальної мережі можна представити так: мережа ділиться на частини (підмережі), що з'єднані системою високошвидкісних каналів передачі – магістралей. У мережі, для побудови деревоподібної топології, застосовують мережні пристрої, що називають комутаторами, і які здатні ділити частини мережі на сегменти [5].

До кінцевого обладнання відносять комп'ютери та сервери.

Комп'ютер – універсальний вузол мережі, прикладне використання якого визначається програмним забезпеченням та додатковим обладнанням [5].

Сервер - це комп'ютер, що має в мережі більшу активність і значущість порівняно з клієнтськими машинами [5].

До мережного обладнання можна віднести маршрутизатори, комутатори та концентратори.

Концентратор - пристрій, до якого підключаються кабелі від безлічі кінцевих вузлів та комунікаційних пристроїв [5].

Маршрутизатор - пристрій з кількома фізичними інтерфейсами, можливо, різних мережевих технологій, що використовується організації регламентованих зв'язків між логічними підмережами з урахуванням мережної адресної інформації [5].

Комутатор - мережний пристрій, що служить засобом сегментації, та спрямовує дані на відповідний вихідний порт [5].

1.1.4 Сутність процесу забезпечення працездатності обчислювальної мережі

При плануванні локальної мережі можна виділити групу контрольованих ознак, за ознаками яких можна говорити, що мережа буде продуктивна.

Збір, порівняння та аналіз функціональних параметрів мережі є надзвичайно важливими для її працездатності або ж при складанні обґрунтування необхідності модернізації мережі. На ринку є безліч засобів для моніторингу мережі та збору даних, наприклад, програмні засоби Cisco Works, HP OpenView, Insight Manager, Optivity. Вибір конкретного продукту та необхідних досліджуваних параметрів буде залежати від конкретної інфраструктури мережі та від найбільш пріоритетних факторів для особи, яка приймає рішення (ЛПР) при дослідженні мережі.

Обчислювальна мережа працездатна, якщо параметри, що описують її роботу і що показують, що мережа виконує покладені на неї функції, знаходяться в межах, передбачених технічною документацією [7].

Обчислювальна мережа непрацездатна, якщо хоча б один із вищезазначених параметрів виходить за межі, передбачені технічною документацією [7].

У процесі функціонування мережі може порушуватись робота групи пристроїв мережі, тому персонал повинен постійно забезпечувати працездатність обчислювальної мережі. У цей процес входять діагностика роботи мережі з метою виявлення пристроїв, що порушують її функціонування та оперативне усунення збоїв повернення обчислювальної мережі в режим штатного функціонування [8].

У процесі забезпечення працездатності обчислювальної мережі за умови порушення роботи групи пристроїв для повернення мережі в режим штатного функціонування застосовується комплекс організаційно-технічних заходів [9]. До комплексу можуть входити наступні заходи:

– налаштування мережного обладнання;

– перевірка з'єднання кабелю з мережевим пристроєм;

– перепланування для усунення впливу джерел, що спотворюють сигнали на передавальне обладнання;

– «переконфігурація» фрагмента мережі (за рахунок мережного обладнання з іншої частини мережі та заміна ним проблемної складової мережі);

– заміна мережного обладнання;

– додавання мережевих пристроїв.

Недостатньо формалізованим та трудомістким є процес аналізу збоїв у роботі мережі та їх усунення. Збій – ситуація некоректного функціонування мережі. Поняття збою включає фізичну відмову мережного обладнання, збій програмного забезпечення як на кінцевих, так і на проміжних пристроях мережі, некоректне налаштування обладнання, недостатня якість обслуговування [10].

Узагальнена схема процесу аналізу збоїв у мережі та їх усунення зображена на рис. 1.1.

Бачимо, що є ряд етапів, через які повна автоматизація неможлива. Тому на схемі вказана область можливої автоматизації процесу аналізу збоїв у мережі та їх усунення.

У процесі експлуатації локальної мережі внаслідок впливу багатьох чинників у роботі можуть виникнути ситуації, що призводять до порушення її функціонування. При цьому будуть відправлені певні повідомлення у заданому форматі у відповідальний підрозділ. Будь яке вирішення проблеми починається зі збору даних та параметрів функціонування обчислювальної мережі. Збір даних здійснюється наступним чином:

– уточнення факторів порушення функціонування мережі;

– дистанційна або безпосередня діагностика характеристик проблемної ділянки мережі.

Зібрана статистика дозволяє провести аналіз проблеми та її ідентифікацію. Тобто виконується локалізація проблеми та пошук компонентів, які порушують функціонування мережі. Після локалізації проблеми виявляються можливі шляхи її вирішення. З них обирається найбільш обґрунтований варіант.

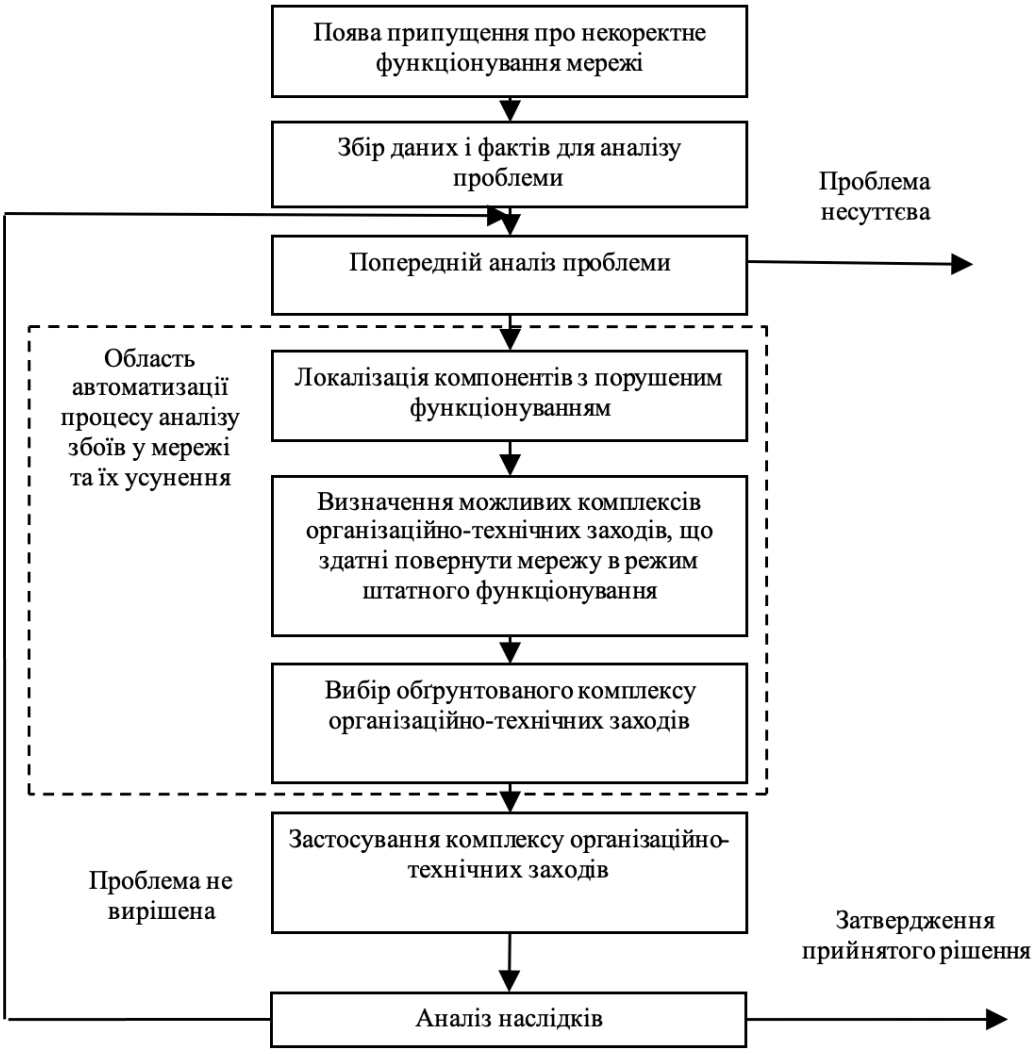

Рисунок 1.1 - Узагальнена схема процесу аналізу збоїв у мережі та їх усунення

Для повернення мережі у стан коректного функціонування конкретного типу мережної складової можна застосувати кілька варіантів організаційно-технічних заходів відповідно до конкретної складової мережі. Критеріями вибору заходів найчастіше стають вартість та трудомісткість виконання даних заходів. У порядку зменшення пріоритету за вказаними критеріями заходи можна розмістити наступним чином: перевірити з'єднання, налаштувати, переконфігурувати (переставити деталь чи весь мережний пристрій з іншої частини мережі в проблемну ділянку), замінити, повністю модернізувати частину мережі.

Однак на вибір заходу впливає важливість складової мережі. Визначення важливості є нечітким параметром. Чим вище значення складової мережі, тим більше знизиться продуктивність мережі при видаленні цієї складової.

Головна мета, яку адміністратор ставить під час пошуку організаційно-технічних заходів щодо усунення проблеми – повернути мережу до працездатного стану. Якщо існує кілька комплексів організаційно-технічних заходів, що повертають мережу в режим штатного функціонування, то їх вибирається один оптимальний з точки зору вартості та часу відновлення функціонування мережі.

Після цього проводиться аналіз роботи мережі після проведення організаційно-технічних заходів. Якщо після їх проведення досі наявні порушення функціонування мережі, то слід провести повторну ідентифікацію проблеми. Якщо порушення відсутні, варіант структури мережі затверджується.

Супровід мережі –це один із способів підтримки працездатності мережі. У разі рішення щодо необхідності вжиття заходів щодо проведення комплексу організаційно-технічних заходів над мережею виникає потреба впровадження системи підтримки прийняття рішень (СППР) у цей процес [11]. СППР - це людино-машинна інформаційна система, що використовується для підтримки дій ЛПР у ситуаціях вибору, коли неможливо чи небажано мати автоматичну систему подання та реалізації всього процесу оцінки та вибору альтернатив. У разі усунення збоїв у процесі функціонування обчислювальних мереж під СППР можна розуміти програмний комплекс, що дає рекомендації особам, які приймають рішення; щодо організації процесу пошуку оптимальної сукупності організаційно-технічних заходів відносно усунення проблем у мережі. СППР може сприяти аналізу та локалізації проблеми, виявленню шляхів вирішення проблеми та вибору обґрунтованого варіанту модернізації або оперативного усунення порушень функціонування мережі [11].

1.2 Основні підходи до побудови локальних мереж

Головною вимогою, що висуваються до мереж, є виконання мережею її основної функції - забезпечення користувачам потенційної можливості доступу до ресурсів всіх комп'ютерів, об'єднаних у мережу [3].

Хоча всі ці вимоги дуже важливі, часто поняття «якість обслуговування» комп'ютерної мережі трактується вужче - до нього включаються лише дві найважливіші характеристики – продуктивність і надійність [12].

Незалежно від обраного показника якості обслуговування мережі існують два підходи щодо його забезпечення. Перший підхід полягає у тому, що мережа (та обслуговуючий її персонал) гарантує користувачеві дотримання деякої числової величини показника якості обслуговування.

Другий підхід полягає в тому, що мережа обслуговує користувачів відповідно до їхніх пріоритетів. Тобто якість обслуговування буде залежати від ступеня привілейованості користувача або групи користувачів, до якої він належить. В цьому випадку якість обслуговування не гарантується, а гарантується лише рівень привілеїв користувача. Тобто мережа намагається якомога якісніше обслуговувати користувача, але нічого при цьому не гарантує.

Потенційно висока продуктивність - це одна з основних властивостей розподілених систем, до яких належать комп'ютерні мережі. Ця властивість забезпечується можливістю розпаралелювання робіт між кількома комп'ютерами чи серверами. На жаль, цю можливість не завжди вдається реалізувати. Існує кілька основних характеристик продуктивності мережі:

- час реакції;
- пропускна спроможність;
- затримка передачі та варіація затримки передачі [13].

Час реакції мережі є інтегральною характеристикою продуктивності мережі з погляду користувача. Загалом час реакції визначається як інтервал часу між виникненням запиту користувача до будь-якої мережної служби та отриманням відповіді на цей запит [13].

Очевидно, що значення цього показника залежить від типу служби, до якої звертається користувач, від того, який користувач і до якого сервера він звертається, а також від поточного стану елементів мережі - завантаженості сегментів, комутаторів і маршрутизаторів, через які проходить запит, завантаженості сервера і т.п.

Тому має сенс використовувати також і середньозважену оцінку часу реакції мережі, усереднюючи цей показник по користувачам, серверам та часу звернення (від якого значною мірою залежить завантаження мережі).

Час реакції мережі зазвичай складається з кількох складових. У загальному випадку в нього входить час підготовки запитів на клієнтському комп'ютері, час передачі запитів між клієнтом та сервером через сегменти мережі та проміжне комунікаційне обладнання, час обробки запитів на сервері, час передачі відповідей від сервера клієнту та час обробки відповідей на клієнтському комп'ютері [11].

Знання часу реакції кожної з мережних складових дає можливість оцінити продуктивність окремих сегментів мережі, виявити вузькі місця та, у разі потреби, виконати модернізацію мережі, підвищуючи, таким чином, її загальну продуктивність.

Пропускна здатність відображає обсяг даних, переданих мережею або її частиною за одиницю часу. Пропускна здатність безпосередньо характеризує якість виконання основної функції мережі транспортування повідомлень - і тому частіше використовується при аналізі продуктивності мережі, ніж час реакції. Пропускна здатність вимірюється або в бітах за секунду, або в пакетах за секунду. Пропускна здатність може бути миттєвою, максимальною та середньою [13].

Середня пропускна здатність обчислюється шляхом розподілу загального обсягу переданих даних на час їх передачі, причому вибирається досить тривалий проміжок часу – година, день чи тиждень [13].

Миттєва пропускна здатність відрізняється від середньої тим, що для усереднення вибирається дуже маленький проміжок часу – наприклад, 10 мс або 1с [13].

Максимальна пропускна здатність – це найбільша миттєва пропускна здатність, зафіксована протягом періоду спостереження. Максимальна пропускна здатність дозволяє оцінити можливості мережі справлятися з піковими навантаженнями, характерними для особливих періодів роботи мережі, наприклад ранкових годин, коли співробітники підприємства майже одночасно реєструються в мережі і звертаються до файлів і баз даних [13].

Пропускну здатність можна вимірювати між двома вузлами або точками мережі, наприклад між клієнтським комп'ютером і сервером, між вхідним і вихідним портами маршрутизатора. Для аналізу та налаштування мережі дуже корисно знати дані про пропускну здатність окремих елементів мережі [13].

Параметр загальної пропускної здатності мережі, що визначається як середня кількість інформації, переданої між усіма вузлами мережі за одиницю часу, теж використовується, але вже як загальна характеристика мережі.

Зазвичай при визначенні пропускної спроможності сегмента або пристрою в даних, що передаються, не виділяються окремі пакети якогось певного користувача, програми або комп'ютера – підраховується загальний обсяг інформації, що передається. Тим не менш, для більш точної оцінки якості обслуговування така деталізація бажана, і останнім часом системи управління мережами все частіше дозволяють її виконувати [14].

Затримка передачі визначається як затримка між моментом надходження пакета на вхід будь-якого мережного пристрою або частини мережі та моментом його появи на виході цього пристрою. Цей параметр продуктивності за змістом близький до часу реакції мережі, але відрізняється тим, що завжди характеризує лише мережні етапи обробки даних, без затримок обробки комп'ютерами мережі. Зазвичай якість мережі характеризують величинами максимальної затримки передачі та варіацією затримки. Не всі типи трафіку чутливі до затримок передачі, принаймні до тих величин затримок, які

характерні для комп'ютерних мереж, – зазвичай затримки не перевищують сотень мілісекунд, рідше – кількох секунд. Такий порядок затримки пакетів, що породжуються файловою службою, службою електронної пошти або службою друку, мало впливають на якість цих служб з точки зору користувача мережі. З іншого боку, такі ж затримки пакетів, що переносять голосові дані або відеозображення, можуть призводити до значного зниження якості інформації, що надається користувачеві - виникнення ефекту «еха» чи завмирання, неможливості розібрати деякі слова, тремтіння зображення тощо [15].

Пропускна здатність та затримки передачі є незалежними один від одного параметрами, тобто мережа може мати низьку пропускну здатність, але вносити мінімальні затримки при передачі кожного пакета.

Однією з початкових цілей створення розподілених систем, до яких належать обчислювальні мережі, було досягнення більшої надійності у роботі порівняно з функціонуванням окремих обчислювальних машин [2].

Важливо розрізняти декілька аспектів надійності. Для технічних пристроїв використовуються такі показники надійності як середній час напрацювання на відмову, ймовірність відмови, інтенсивність відмов. Однак ці показники придатні для оцінки надійності простих елементів та пристроїв, які можуть перебувати лише у двох станах – працездатному чи непрацездатному. Складні системи, що складаються з багатьох елементів, крім станів працездатності та непрацездатності, можуть мати інші проміжні стани, які ці характеристики не враховують. У зв'язку з цим з метою оцінки надійності складних систем застосовується інший набір характеристик [15].

Готовність чи коефіцієнт готовності – частка часу, протягом якого система може бути використана. Готовність може бути покращена шляхом введення надмірності в структуру системи: ключові елементи системи повинні існувати в кількох варіантах реалізації, щоб при відмові одного з них функціонування системи забезпечували інші [15].

Систему можна віднести до високонадійної тоді, коли вона має, як мінімум, високу готовність, але цього недостатньо. Необхідно також забезпечити збереження даних та захист їх від спотворень.

Також повинна підтримуватись узгодженість (несуперечність) даних. Наприклад, при зберіганні кількох копій даних на різних файлових серверах потрібно забезпечити їх ідентичність.

Так як мережа працює на основі механізму передачі пакетів між кінцевими вузлами, то однією з характерних характеристик надійності є можливість доставки пакета вузлу призначення без спотворень. Поряд з цією характеристикою можуть використовуватися й інші показники: ймовірність втрати пакета (з будь-якої причини: через переповнення буфера маршрутизатора, через розбіжність контрольної суми, через відсутність працездатного шляху до вузла призначення і т.д.), ймовірність спотворення окремого біта даних, що визначаютьься як відношення втрачених пакетів до доставлених [12].

Іншим аспектом загальної надійності є безпека – здатність системи захистити дані від несанкціонованого доступу. У розподіленій системі це зробити набагато складніше, ніж у централізованій. У мережах повідомлення передаються лініями зв'язку, які часто проходять через загальнодоступні приміщення, в яких можуть бути встановлені засоби прослуховування ліній. Іншим вразливим місцем можуть бути залишені без нагляду персональні комп'ютери. Крім того, завжди є потенційна загроза злому захисту мережі від неавторизованих користувачів, якщо мережа має виходи у глобальну мережу загального користування [12].

Ще однією характеристикою надійності є стійкість до відмови. У мережах під стійкістю до відмови розуміється здатність системи приховати від користувача відмову окремих її елементів. Наприклад, якщо копії таблиці бази даних зберігаються одночасно на декількох файлових серверах, користувачі можуть просто не помітити відмову одного з них. У відмовостійкій системі відмова одного з її елементів призводить до деякого зниження якості її роботи

(деградації), а не до повного зупинення. Так, при відмові одного з файлових серверів у попередньому прикладі збільшується лише час доступу до бази даних через зменшення ступеня розпаралелювання запитів, але в цілому система продовжуватиме виконувати свої функції [15].

Розширюваність означає можливість порівняно легкого додавання окремих елементів мережі (користувачів, комп'ютерів, додатків, служб), нарощування довжини сегментів мережі та заміни наявної апаратури потужнішою. При цьому важливо, що легкість розширення системи іноді може забезпечуватися в деяких дуже обмежених межах. Наприклад, локальна мережа класичного Ethernet, побудована на основі одного сегмента товстого коаксіального кабелю, має гарну розширюваність, у тому сенсі, що дозволяє легко підключати нові станції. Однак така мережа має обмеження на кількість станцій – їх кількість не повинна перевищувати 30-40. Хоча мережа допускає фізичне підключення до сегменту більшої кількості станцій (до 100), але при цьому найчастіше різко знижується продуктивність мережі. Наявність такого обмеження і є ознакою поганої масштабованості системи при добрій розширюваності [16].

Масштабованість означає, що мережа дозволяє нарощувати кількість вузлів та протяжність зв'язків у дуже широких межах, при цьому продуктивність мережі не погіршується. Для забезпечення масштабованості мережі доводиться застосовувати додаткове комунікаційне обладнання та спеціальним чином структурувати мережу. Наприклад, хорошу масштабованість має багатосегментна мережа, побудована з використанням комутаторів і маршрутизаторів і має ієрархічну структуру зв'язків. Така мережа може включати кілька тисяч комп'ютерів і забезпечувати кожному користувачеві мережі необхідну якість обслуговування [16].

Прозорість мережі досягається в тому випадку, коли мережа представляється користувачам не як безліч окремих комп'ютерів, пов'язаних між собою складною системою кабелів, а як традиційна обчислювальна машина з системою поділу часу. Прозорість може бути досягнута на двох різних рівнях

- на рівні користувача та на рівні програміста. На рівні користувача прозорість означає, що для роботи з віддаленими ресурсами він використовує ті ж команди та звичні йому процедури, що й для роботи з локальними ресурсами. На програмному рівні прозорість полягає в тому, що програма для доступу до віддалених ресурсів потребує тих самих викликів, що й для доступу до локальних ресурсів [17].

Керованість мережі має на увазі можливість централізовано контролювати стан основних елементів мережі, виявляти та вирішувати проблеми, що виникають під час роботи мережі, виконувати аналіз продуктивності та планувати розвиток мережі. В ідеалі засоби управління мережами є системою, що здійснює спостереження, контроль і управління кожним елементом мережі - від найпростіших до найскладніших пристроїв, при цьому така система розглядає мережу як єдине ціле, а не як розрізнений набір окремих пристроїв [17].

Сумісність або інтегрованість означає, що мережа здатна включати найрізноманітніше програмне та апаратне забезпечення, тобто в ній можуть співіснувати різні операційні системи, що підтримують різні стеки комунікаційних протоколів, і працювати апаратні засоби і додатки від різних виробників. Мережа, що складається з різнотипних елементів, називається неоднорідною або гетерогенною, а якщо гетерогенна мережа працює без проблем, вона є інтегрованою. Основний шлях побудови інтегрованих мереж - використання модулів, виконаних відповідно до відкритих стандартів та специфікацій [17].

1.2.1 Специфіка побудови та забезпечення працездатності локальних мереж

Існують стандартні алгоритми та моделі побудови локальних мереж, що залежать від технологій передачі в них інформації. Існує два види моделей побудови мережі. Перша модель збирає локальну мережу із сегментів «за принципом конструктора», орієнтуючись на групу правил. Причому для

взаємодіючих сегментів визначено необхідне мережне устаткування. Тут критерієм виступає допустима довжина кабелю. Мережеве обладнання розташовується так, щоб сигнал якнайменше загасав [18].

Наприклад, при побудові сегментів мережі за технологією Fast Ethernet, необхідно дотримуватися наступних правил:

– сегменти, виконані на електричних кабелях (кручених парах) не повинні бути довшими за 100 метрів;

– сегменти, виконані на оптоволоконних кабелях, не повинні бути довшими за 412 метрів;

– якщо використовуються адаптери із зовнішніми (виносними) трансіверами, то трансіверні кабелі не повинні бути довшими за 50 сантиметрів [18].

При виконанні перелічених правил можна бути впевненим, що мережа буде працездатною і жодних додаткових розрахунків робити не потрібно.

Така модель за параметрами та кількістю правил буде відрізнятися для різних технологій передачі, але в межах кожної технології вони фіксовані, що спрощує планування локальних сегментів.

Друга модель, що застосовується з метою оцінки конфігурації мережі, полягає в точному розрахунку часових характеристик обраної конфігурації мережі. Застосування другої моделі необхідно в тому випадку, коли розмір мережі, що проектується, близький до максимально допустимого. Обчислюється подвійний (круговий) час проходження сигналу по мережі та виконується його порівняння з максимально допустимою величиною.

При цьому обчислення завжди ведуться для найгіршого випадку, для шляху максимальної довжини, який вимагає для свого проходження максимального часу.

При проектуванні локальної мережі можна також використовувати обидві моделі. При цьому слід врахувати всі види технологій передачі в мережі (Ethernet, Fast Ethernet і т.д.) для автоматизації вищезгаданих моделей.

Розуміємо, що не існує універсального методу побудови локальної мережі, та універсальних правил вибору комплексу організаційно-технічних заходів, що застосовуються до мережі, яка некоректно функціонує. Правила, що дозволяють проаналізувати продуктивність мережі, відрізняються в залежності від стандарту побудови мережі. Комплекси організаційно-технічних заходів, що застосовуються для аналізу, теж, зазвичай, вибираються приватно для конкретної мережі підприємства.

1.2.2 Аналіз побудови та забезпечення працездатності корпоративних мереж

При побудові магістралей та сегментів мережі, чи підключенні клієнтів до неї слід враховувати групу умов вибору способів підключення.

Магістральні вузли зв'язку з метою мінімізації витрат найчастіше розміщують у, так званих, точках присутності - вузлах вже існуючих телекомунікаційних мереж (Міські АТС, вузли зв'язку провайдерів, комутаційні вузли та шафи в будинках).

За допомогою добудови центрального вузла (магістралі) можна зібрати в єдину мережу наявні локальні мережі. Або ж можна піти зворотнім шляхом: спочатку побудувати магістраль, а потім вже ставити завдання приєднання до неї локальних мереж та їх проектування.

Для підключення великих абонентів можна використовувати оптоволоконні з'єднання, існуючі електричні кабелі зв'язку, обладнання MetroEthernet, xDSL чи PON [4].

Якщо мережу включається малий населений пункт, то спочатку кабельна інфраструктура слаборозвинена і ненадійна, а створення нової економічно неефективно. Тут потрібно застосовувати бездротові технології зв'язку: технології супутникового доступу та RadioEthernet. На даний момент впровадження якісних систем на основі супутникового доступу та технології RadioEthernet стримується з економічних причин, але їхня роль постійно зростає [4].

Якщо існують користувачі, для яких неможливо або економічно невигідно створювати виділені канали зв'язку, доступ до Інтернету можна організувати з використанням вже наявної телефонної інфраструктури, тобто з використанням технології xDSL. Однак, автори групи робіт, що стосуються проектування мережі, наприклад, виключають цей спосіб як малошвидкісний та якісно невигідний [4].

При побудові локальних мереж, що входять до корпоративної, зараз начастіше використовують поширену технологію Fast Ethernet. Однак слід враховувати, що дана технологія вже не вважається такою швидкою за сучасними мірками, тому, бажано, магістраль мережі проектувати вже на основі технології Gigabit Ethernet.

Основним критерієм оцінки продуктивності є пропускна здатність каналу передачі. За ним, найчастіше оцінюється, зручність роботи з сервісами Інтернет на робочому місці працівника.

Вибраний критерій продуктивності досить зручний та легкий у підрахунках. Важливість цього критерію очевидна – запровадження і підтримка сучасних послуг потребує постійного його збільшення. І це вже досить нетривіальна задача при плануванні нових мереж. Дана методика здатна допомогти в оснащенні підприємств корпоративними мережами, проте вона слабо враховує необхідні рівні обладнання, особливо якщо є потреба у розрахунку параметрів «на майбутнє». Звідси випливає, що ми не зможемо зібрати статистику і в повній мірі оцінити продуктивність роботи підмереж системи. Даний критерій також слабо враховує побудову мережі із резервом потенціалу. Система статична, що в реальному житті майже не існує, бо швидко втрачається її конкурентноспроможність.

У роботах Гостєва В.М. розглядається розробка методів оптимального проектування та оцінки продуктивності магістральної інформаційної інфраструктури регіональних освітніх комплексів. Загальна проблема оптимального проектування мереж передачі даних формулюється в такий спосіб. Для заданих множин є - безліч вузлів комутації, безліч доступних

маршрутизаторів, безліч доступних каналів передачі даних між можливими пунктами розміщення вузлів комутації, а також заданої (прогнозованої) інтенсивності трафіку між вузлами комутації необхідно визначити топологію мереж передачі даних, тип маршрутизатора, що встановлюється в кожному вузлі комутації, тип і тип параметру кожного каналу передачі даних, маршрути передачі між вузлами комутації. В якості основних критеріїв оцінки проекту використовуються вартісні характеристики мереж передачі даних (витрати на обладнання та експлуатаційні витрати) та очікувані часові характеристики передачі даних по мережі – середній та максимальний час затримки пакетів у мережах передачі даних [19].

У процесі формування та аналізу варіантів мереж передачі даних застосовуються аналітичні та імітаційні моделі вузлів комутації, каналів передачі даних, зовнішніх джерел (серверів та робочих станцій), що генерують трафік різних типів (симетричний, несиметричний, з різними розподілами інтервалів часу між надходженням пакетів тощо) [19].

Підхід, в цілому, продуктивний: мережі, побудовані за цією моделлю, будуть ефективно та коректно функціонувати. Вартісний критерій враховуєтсья. А от вимоги до робочих місць виявлені слабо. Тобто економія на певних параметрах при побудові локальних підмереж можуть призвести до неможливості виконання ними функцій, що були закладені апри роботі відділу.

При оцінці мережі пропонуються такі параметри продуктивності системи, але вже на програмному рівні:

– доступність сервісу - відсоток часу, який мережевий додаток готовий надати відповідний сервіс;

– реакція – швидкість, з якою мережевий додаток видає відповідний сервіс [19].

З наведених прикладів бачимо що, предметна область дає широкі можливості вибору критеріїв продуктивності системи. Проблема проектування мереж передачі є складною багатокритеріальною проблемою, для якої досі не знайдено однозначного раціонального рішення.

1.3 Основні методи проведення діагностики та організаційно-технічних заходів у локальній мережі

Діагностика мережі – процес аналізу стану мережі. У функціонуванні корпоративних інформаційних систем виникають незрозумілі, на перший погляд, проблеми, які помітно знижують ефективність роботи такої системи, а в деяких випадках дезорганізують роботу підприємства. Це означає, що певна складова мережі працює некоректно. У процесі діагностики проводиться пошук цих пристроїв чи сегментів, фіксується факт несправності, визначається її місце та вид. До проблемної ділянки застосовується комплекс організаційно-технічних заходів (КОТЗ) [20].

Існує група програмних продуктів, призначених для діагностики мереж. Як приклади можна навести MS Network Monitor, LANalyzer for Windows компанії Novell, FTest та SelFTrend компанії «Пролан» [17].

Діагностика відбувається наступним чином. Система, що здійснює діагностику, за допомогою точок контролю розраховує значення групи ознак, які описують поточний стан мережі. Залежно від сукупності значень ознак, ідентифікується проблема у функціонуванні мережі.

Нехай *СР* – стан мережі, при якому порушено роботу її пристроїв, *р* – ознака, що зчитується та описує стан мережі, *Р* – діапазон значень відповідної ознаки, *n* – кількість зчитуваних ознак, *ш* – кількість станів мережі. Тоді процес виявлення збоїв у роботі мережі можна подати у вигляді таблиці 1.1.

Таблиця 1.1 - Виявлення збоїв у роботі мережі за значеннями зчитуваних ознак

	p_1	…	p_n
CP_1	P_{11}	…	P_{1n}
CP_m	P_{m1}	…	P_{mn}

Багато підходів до діагностики використовують ймовірнісну оцінку стану мережі.

Для моніторингу стану мереж та управління мережними пристроями застосовується модель менеджер-агент. В цьому випадку менеджер це - програмно-апаратні засоби, які збирають інформацію від агентів, виконують її обробку та надання адміністратору мережі. Орієнтуючись на подану інформацію адміністратор за допомогою менеджера може здійснювати керування об'єктами мережі. Агенти розміщуються в керованих елементах мережі. Вони взаємодіють із пристроями та обслуговують базу даних керованих параметрів (MIB). В них знаходяться списки керованих параметрів та їх значення. Менеджер може надіслати агенту запит на інформацію (відбувається зчитування даних з бази) або ж виконати керування об'єктом (запис до бази параметрів).

Управління може бути в тій чи іншій мірі автоматизоване, проте повністю автоматизувати процес повернення мережі у працездатний стан при некоректному функціонуванні неможливо. Підтримка механізму прийняття рішень дозволить повною мірою охопити широкий спектр варіантів. організаційно-технічних заходів щодо конкретної проблемної ситуації [21].

Для діагностики та керування станом мережі часто використовують протокол керування SNMP. Протокол SNMP визначає: механізм взаємодії агента та менеджера, моделі представлення параметрів мережі та механізми роботи з ними. SNMP має команди, здатні зчитувати параметри пристроїв [15].

Іншим способом доступу до параметрів, що описує поточний стан мережі є аналіз стану каналів передачі даних за допомогою аналізатора мережевих протоколів [22].

Він повинен підключатися до сегменту мережі, де виявлено збої, в максимальній близькості до найбільш підозрілих комп’ютерів або сервера.

Якщо мережа має архітектуру з комутатором в якості магістралі, то аналізатор необхідно підключати до портів комутатора, через які проходить

аналізований трафік. Деякі програми мають спеціальні агенти або зонди (probes), що встановлюються на комп'ютерах, підключених до віддалених портів комутатора. Зазвичай агенти (не агенти SNMP) це окремий сервіс, що працює у фоновому режимі на комп'ютері користувача.

Якщо в комутаторі спеціальний порт відсутній, то аналізатор (або агент) слід підключати до портів доменів мережі, що знаходяться в максимальній близькості до найбільш підозрілих станцій або серверу.

Для автоматизації підтримки процесу забезпечення працездатності обчислювальної мережі необхідно розробити зручний пошук пристроїв, робота яких порушена. Розглянемо існуючі підходи до моделювання мереж.

Існують спеціальні, орієнтовані на моделювання обчислювальних мереж програмні системи, в яких процес створення моделі спрощений. Такі програмні системи самі генерують модель мережі на основі вихідних даних про її топологію та протоколи, про інтенсивність потоків запитів між комп'ютерами мережі, протяжність ліній зв'язку, про типи використовуваного обладнання та додатків. Програмні системи моделювання можуть бути вузько спеціалізованими і досить універсальними, що дозволяє імітувати мережі різних типів. Якість результатів моделювання значною мірою залежить від точності вихідних даних мережі, переданих у систему імітаційного моделювання [23].

Приклади існуючих систем: COMNET III (CACI Product), NetMaker XA (Make System), Opnet (MIL3) [23].

Основні етапи роботи систем:

1) збір даних про існуючу мережу. Підтримується група форматів імпорту даних про існуючу мережу;

2) детальне моделювання мережі. За допомогою графічного інтерфейсу користувач збирає мережу із пропонованої групи вузлів, визначаючи її топологію;

3) оцінка продуктивності мережі. Після закінчення моделювання користувач може отримати наступні характеристики продуктивності мережі:

– прогнозовані затримки між кінцевими та проміжними вузлами мережі, пропускні здібності каналів, коефіцієнти використання сегментів, буферів та процесорів;

– піки та спади трафіку як функція часу;

– джерела затримок та вузьких місць мережі.

Звіти подаються у зручній для друку текстовій або графічній формі.

Аналіз підходів до побудови мереж, їх діагностики, можливих організаційно-технічних заходів над мережею та основних підходів до їх оперативного застосування виявив відсутність єдиного комплексу формалізованих методик та інструментальних засобів.

Як було зазначено, процес включає у собі ряд етапів, повна автоматизація яких неможлива. Тому на схемі (рис. 1.2) вказується область можливої автоматизації процесу аналізу збоїв у мережі та їх усунення.

В результаті аналізу підходів до діагностики мереж та можливих організаційно-технічних заходів було виявлено, що для автоматизації підтримки процесу забезпечення працездатності обчислювальної мережі підприємства мають бути вирішені наступні науково-технічні завдання:

1) методика автоматизації вибору обґрунтованого комплексу організаційно-технічних заходів;

2) аналіз наслідків;

3) затвердження прийнятого рішення:

– побудова формалізованої моделі подання мережі для локалізації компонентів з порушеним функціонуванням на основі структурної декомпозиції, що випливає із узагальненої структури;

– побудова чи реорганізація корпоративної мережі за умови деталізації її компонентів на різних рівнях абстракції;

– створення методики пошуку порушень функціонування обчислювальної мережі для локалізації компонентів, робота яких порушена, на основі ситуаційного та лінгвістичного підходів до управління, що використовує

моделі представлення мереж для деталізації компонентів мережі на різних рівнях її абстракції;

– створення методики вибору рекомендацій щодо усунення порушень функціонування обчислювальної мережі для вибору рекомендацій на основі ситуаційного та лінгвістичного підходів до управління з використанням експертних оцінок, а також даних щодо порушень роботи пристроїв мережі, виявлених у результаті застосування методики пошуку порушень функціонування обчислювальної мережі.

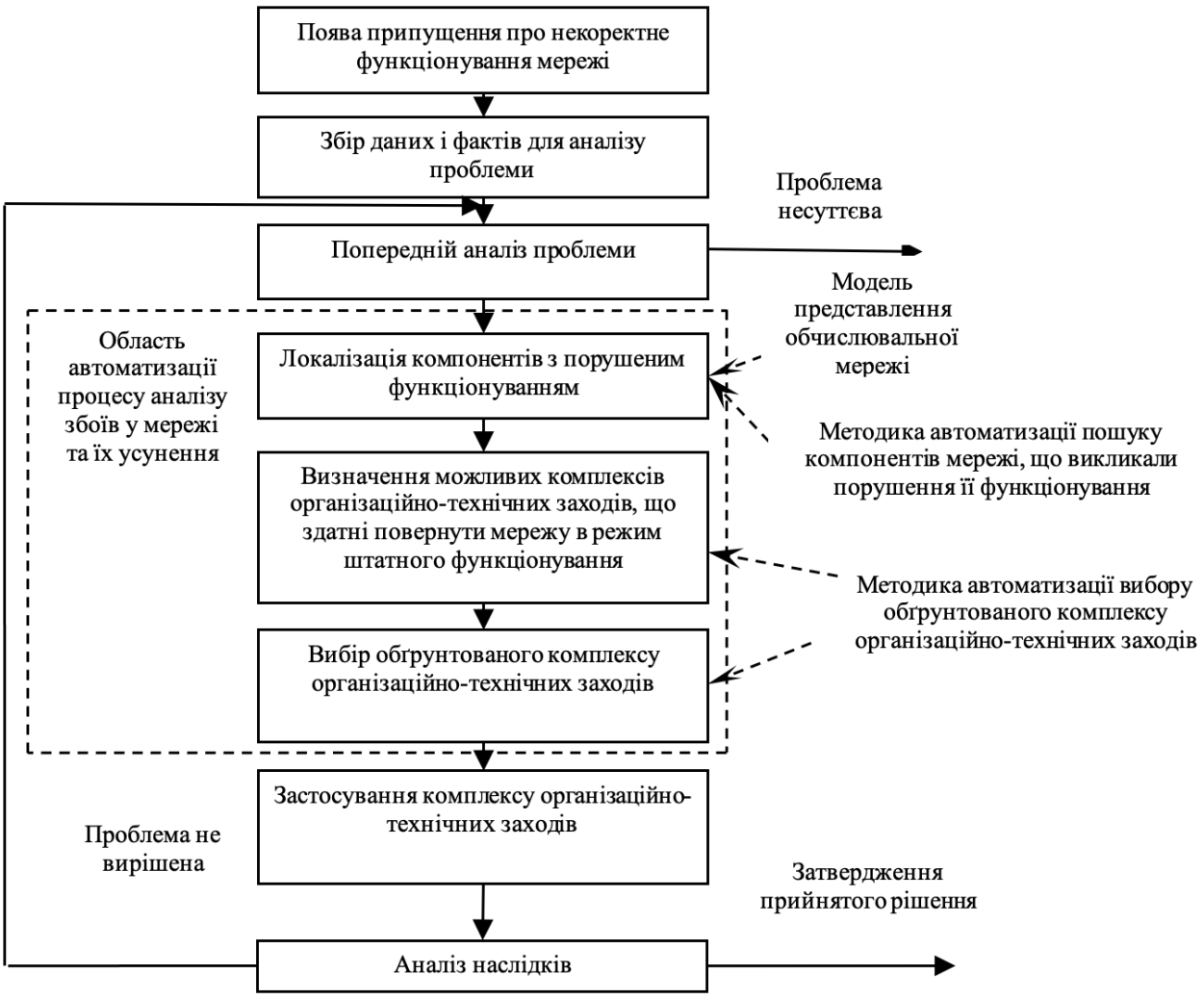

Рисунок 1.2 - Методика автоматизації пошуку компонентів мережі, що спричинили порушення її функціонування

Висновки з першого розділу

Дослідження існуючих топологій мереж, мережевих технологій та стандартів побудови дозволило сформувати уявлення про узагальнену структуру корпоративної мережі. Це дає основу для розробки, побудови та дослідження моделі представлення корпоративної мережі організації.

Було розглянуто процес аналізу збоїв у мережі та їх усунення. Виявлено область його можливої автоматизації. На основі проведених досліджень виявлено систему підтримки прийняття рішень, як найбільш раціональний варіант «радиальної системи», що допомагає вибрати оптимальний комплекс заходів, здатний повернути мережу в режим нормального функціонування.

Аналіз процесу забезпечення працездатності обчислювальної мережі підштовхнув до докладнішого дослідження деяких його складових частин: особливостей модернізації мереж у результаті виявленої некоректної роботи мережі, процесу діагностики та процесу моделювання мереж.

Аналіз підходів до побудови, моделювання та діагностики мереж виявив відсутність єдиного комплексу формалізованих методик та інструментальних засобів автоматизації підтримки процесу забезпечення працездатності обчислювальної мережі.

У зв'язку з цим постало питання про розробку методики автоматизації процесу забезпечення працездатності обчислювальної мережі.

В результаті аналізу підходів до діагностики мереж, виявлення несправностей та аналізу можливих організаційно-технічних заходів було зазначено, що для автоматизації підтримки процесу забезпечення працездатності обчислювальної мережі підприємства мають бути вирішені насамперед науково-технічні завдання.

У сучасних умовах широко використовуються мережеві аналізатори, кабельні сканери, тести кабельних систем, аналізатори протоколів, протоколи моніторингу мережі. Все це дозволяє своєчасно і без затримок визначити слабкі місця в технічній та програмній організації ЛОМ. Тому основним методичним прийомом діагностики мережі є комплексна перевірка всіх складових мережі. У сучасних умовах на першому місці стоїть випереджувальна діагностика, суть

якої полягає в безперервному або тривалому спостереженні за роботою мережі. Тільки планова цілеспрямована діагностика дозволить створити стійку і безперебійну роботу ЛОМ, що створить умови для її безпечної роботи.

2 ПРОЕКТУВАННЯ І ПОБУДОВА ЛОКАЛЬНОЇ МЕРЕЖІ ПІДЗЕМНОЇ ЛІКАРНІ

2.1 Загальні принципи побудови

В цілому, побудова локальних підземних мереж критичних об'єктів на базі проводового підключення є складним завданням, але це необхідне забезпечення ефективної роботи медичних установ. Якісне проектування мережі, використання захищених кабелів та розміщення серверів в окремих приміщеннях допоможуть забезпечити стабільну та надійну роботу мережі [1].

При роботі в підземних умовах важливо мати надійну та швидку локальну мережу, яка дозволить своєчасно та ефективно обробляти дані.

Основу підземної локальної мережі складають сервер, маршрутизатори та комутатори. Сервер є центральним вузлом мережі, на якому зберігаються та обробляються дані. Комутатори і маршрутизатори виконують функцію передачі даних між комп'ютерами мережі. Для забезпечення швидкої та ефективної роботи мережі необхідно вибрати правильний сервер, маршрутизатори та комутатори [1].

Під час проектування та монтажу ЛОМ виконавець повинен вирішити завдання:

– мережа має бути універсальним середовищем передачі: даних, голосу, відео та іншої інформації;

– забезпечувати можливість сумісності з наявним передавальним обладнанням зі швидкостями передачі 10/100 Мбіт/с;

– володіти модульністю та можливістю внесення змін та нарощування;

– допускати одночасне використання будь-яких протоколів передачі;

– використовувати стандартні компоненти та матеріали;

– дозволяти створювати незалежні ділянки у мережі;
– відповідати існуючим стандартам TIA/EIA-568A та ISO11801;
– забезпечувати високу надійність у роботі.

Сервер повинен забезпечувати високу продуктивність та надійність зберігання даних. У підземній лікарні необхідно враховувати умови роботи сервера за екстремальних умов. Сервер повинен бути стійкими до вібрацій та високої вологості. Можна використовувати сервер з RAID-масивами для забезпечення надійності зберігання даних.

Кабелі. При проектуванні локальної мережі в підземній лікарні рекомендується використовувати високошвидкісні кабелі Cat7 серверного підключення. Кабелі Cat7 забезпечують більш високу швидкість передачі даних і мають більшу захищеність від завад і перешкод у порівнянні з більш старими стандартами кабелів. Це особливо важливо для медичної середовища, де надійна і стабільна передача даних критично важлива. Кабелі Cat7 також забезпечують підтримку передачі даних для більшої відстані без втрати якості сигналу [1].

Маршрутизатори. Маршрутизатори грають ключову роль у побудові та в управлінні мережею в підземній лікарні. Вони відповідають за маршрутизацію трафіку між різними мережними сегментами та зв’язок із зовнішніми мережами. При виборі маршрутизаторів для підземної лікарні слід звернути увагу на їх продуктивність, надійність, масштабованість і можливості безпеки. Маршрутизатори повинні підтримувати протоколи маршрутизації, включаючи IPv4 і IPv6, і забезпечувати ефективне управління мережним трафіком [1].

Комутатори. Комутатори використовуються для підключення комп'ютерів, серверів та інших мережевих пристроїв до локальної мережі підземної лікарні. Вони забезпечують комутацію даних, що забезпечує передачу інформації між пристроями в межах однієї мережі. При виборі комутаторів необхідно враховувати кількість портів, необхідну пропускну здатність, підтримку стандарту PoE (Power over Ethernet) для живлення мережевих пристроїв, а також функції безпеки, такі як контроль доступу та

ізоляція портів. Комутатори також повинні забезпечувати низьку підтримку і високу продуктивність для плавної та надійної роботи мережі [1].

Важливо відзначити, що при виборі та розгортанні кабелів, маршрутизаторів і комутаторів в підземній лікарні необхідно дотримуватися відповідних стандартів і регулятивних вимог, встановлених в медичній галузі. У підземній лікарні особлива увага приділяється безпеці даних, надійності та відмовостійкості мережі.

Важливим аспектом при виборі обладнання для підземної лікарні є його сумісність та інтеграція з іншими системами та пристроями, що використовуються у медичному середовищі. Наприклад, маршрутизатори та комутатори повинні підтримувати спільну роботу з медичними інформаційними системами (МІС), системами відеоспостереження, системами керування доступом та іншими системами, які можуть бути необхідні у лікарняному середовищі [1].

Одним із важливих аспектів при побудові локальної мережі у підземній лікарні є організація віртуальних локальних мереж (VLAN). VLAN дозволяють розділяти мережу на логічні групи, керувати трафіком та забезпечувати безпеку даних. Кожна окрема VLAN може бути налаштована для конкретного відділу чи групи користувачів, забезпечуючи їм ізольоване мережеве оточення [1].

Іншим важливим аспектом є резервування та відмовостійкість мережі. У підземній лікарні критично важливо, щоб мережа залишалася працездатною навіть у разі збою в одному з вузлів. Для цього можуть використовуватися дубльовані маршрутизатори, комутатори з підтримкою протоколу Spanning Tree та механізми резервування каналів [1].

Важливим аспектом при побудові є правильне налаштування мережевих налаштувань. Необхідно визначити правильні налаштування IP-адрес, підмереж та шлюзів за замовчуванням для серверів, комутаторів та комп'ютерів у мережі. Це дозволить забезпечити правильну маршрутизацію даних та запобігти конфліктам IP-адрес.

Створення ЛОМ має дозволити надалі:

– організувати ефективний обмін інформацією між ПК робочих місць;

– скоротити кількість необхідної периферійної техніки (друкарські пристрої, принтери та ін) за рахунок її спільного використання;

– створити основу для організації доступу до загальних інформаційних ресурсів;

– створити основу для впровадження корпоративних інформаційних систем, корпоративної поштової системи, а також забезпечити доступ співробітників до сервісів Internet [18].

2.2 Вимоги до структури та функціонування ЛОМ

До ЛОМ пред'являються такі загальні вимоги:

– ЛОМ повинна бути виконана відповідно до вимог вищеперелічених кабельних стандартів, мати всі ознаки ЛОМ: універсальність, структуризація, надмірність;

– потрібно встановлювати ЛОМ з гарантією на пасивні компоненти системи терміном не менше 25 років;

– всі компоненти ЛОМ повинні бути від одного виробника, екранованими та відповідати вимогам категорії 6 та вище (класу Е);

– всі матеріали та телекомунікаційне обладнання повинні відповідати вимогам кабельних стандартів [18].

Вимоги до пасивного обладнання

Для використання в якості пасивного обладнання мережі передачі даних слід вибрати:

– кабеленесучі елементи ЛОМ (лотки, короби, жолоби та їх аксесуари): відомих та визнаних фірм виробників;

– пасивні елементи ЛОМ (патч-панелі, модульні гнізда, шафи та аксесуари): відомих та визнаних фірм виробників;

– кабель: STP (6 категорія і вище, екранований) має не менш ніж 25-річну гарантію виробника.

Вимоги до активного обладнання мережі передачі даних

Інформаційний обмін між активним мережевим обладнанням повинен здійснюватися через єдиний інформаційний простір та використання стандартизованих протоколів і форматів обміну даними. Як основні протоколи канального рівня моделі OSI повинні використовуватися такі протоколи: Gigabit Ethernet, 10 Gigabit Ethernet. Як основний протокол мережного рівня за моделлю OSI повинен використовуватися IP-протокол.

Як сервери для керування корпоративною базою даних, центрального файлового сервера, файлового сервера робочих груп, сервера електронної пошти, web-сервера та сервера резервного копіювання повинні бути використані комп'ютери з характеристиками не нижче, ніж такі:

Процесор - Intel Xeon E7-2860 (2.26 GHz /10-core /24 MB /130 W), Кількість процесорів - 4 шт, максимальна кількість процесорів - до 8 шт, тип пам'яті - DDR3 Registered, максимальна кількість накопичувачів - 8 шт., тип накопичувачів - SFF (2,5') SAS/SATA/SSD Hot Plug, підтримка RAID, мережевий інтерфейс - 4 x 1GigEth.

Уточнення марки та продуктивності серверів має бути здійснено на стадії проектування ЛОМ.

2.3 Побудова структурованої кабельної системи для підземного використання

Одним із ключових елементів структурованої кабельної системи є вибір відповідних кабелів. У підземній лікарні, де є підвищена вологість і можливість пошкодження кабелів при проведенні робіт, необхідно вибирати кабелі, які мають захист від зовнішніх впливів і відповідають необхідним нормам і вимогам [2].

Також необхідно враховувати розташування комутаційних панелей, кабельних лотків та інших елементів кабельної системи у приміщеннях. Оптимальне розміщення елементів дозволить забезпечити більш зручний доступ та обслуговування кабельної системи [2].

Важливою частиною структурованої кабельної системи є також сполучні елементи, такі як розетки та конектори. Вибір з'єднувальних елементів також повинен відповідати вимогам щодо надійності та продуктивності мережі.

Схема підземної лікарні ділиться на 3 рівні, кожен з яких має однакове плануванням для зручності побудови (рис. 2.1). Приблизна кількість крученої пари – 130 метрів на кожен поверх. Використовується кручена пара 6-ої категорії (UTP 6) і технологія Gigabit Ethernet (GbE). Для робочих груп використано топологію «шина» з комутатором. Дана схема розроблена з урахуванням характерних особливостей побудови. Кабелі будуть розташовані уздовж стіни, в спеціально відведених для них каналах [3].

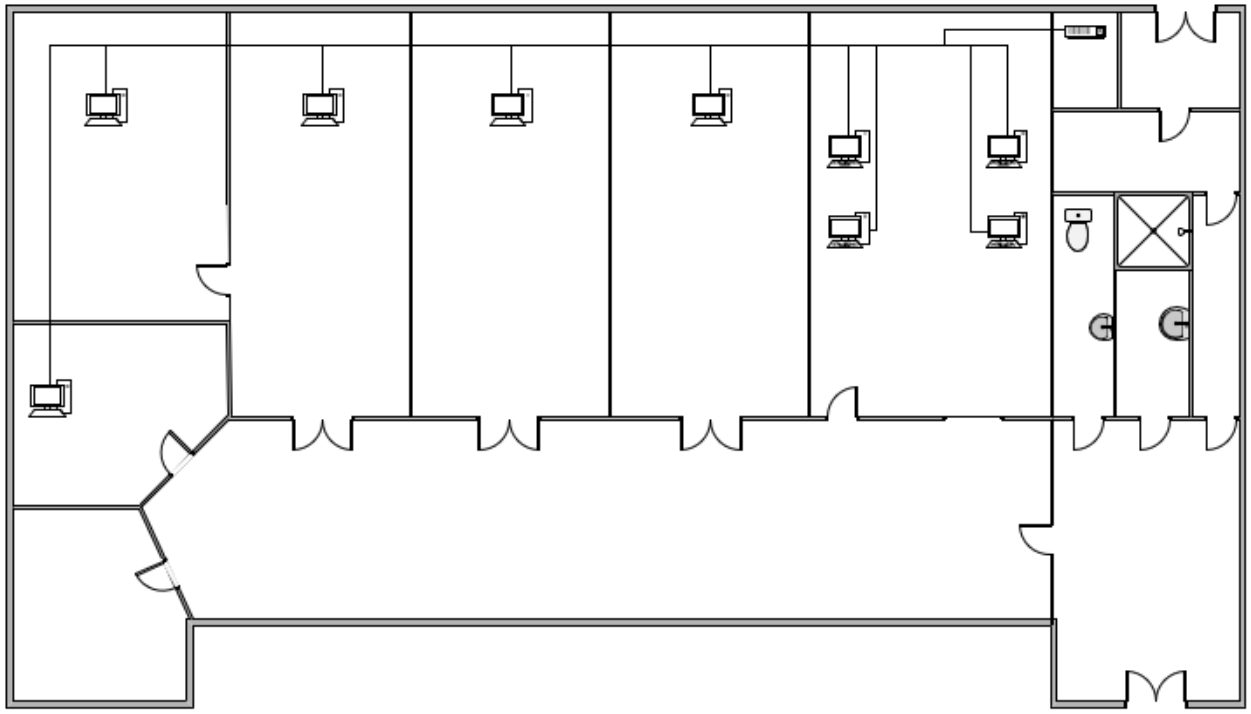

Рисунок 2.1 – Типова організація рівнів

Вертикальна підсистема для підземної лікарні показана на рис. 2.2. Приблизна кількість крученої пари в такій мережі – 403 метри. Використовуються кабелі категорії 7 (Cat7). Використовується технологія Gigabit Ethernet (з урахуванням перспективи розвитку та вимог до швидкості у структурі такого типу). Для побудови підсистеми було використано комутатори та маршрутизатор з декількома портами [3].

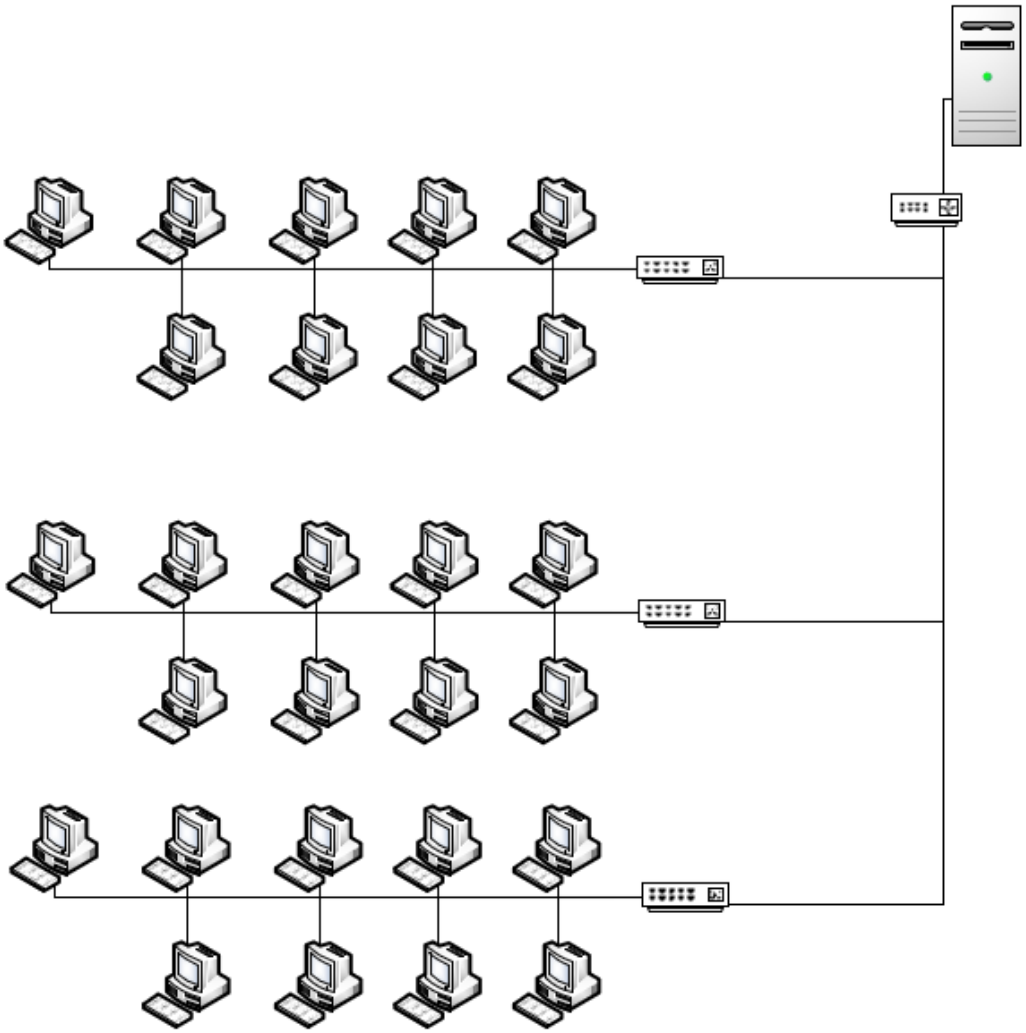

Рисунок 2.2 – Трирівнева організація мережі

Побудова таких мереж вимагає глибокого розуміння потреб та вимог об'єктів, а також застосування передових технологій у галузі мережного зв'язку та безпеки. Забезпечення надійності, ефективності та захищеності цих мереж

гарантує безперебійну роботу критичних систем, захист життя та безпеку людей, а також ефективне використання ресурсів. Побудова локальних підземних мереж для критичних об'єктів є стратегічно важливим завданням, яке сприяє стабільності та розвитку суспільства в сучасному світі, де забезпечення надійного зв'язку є необхідністю. Ці мережі виконують важливу роль у забезпеченні безперебійної роботи критичних систем та обладнання, а також в оперативному реагуванні на надзвичайні ситуації. Отже, побудова локальних підземних мереж для критичних об'єктів є невід'ємною складовою їхньої інфраструктури та забезпечує надійну комунікацію та зв'язок в умовах підземної середовища [3].

3 ЛОГІЧНА ОРГАНІЗАЦІЯ, ПЕРЕВІРКА РІВНЯ БЕЗПЕКИ ТА ПРАЦЕЗДАТНОСТІ ЛОКАЛЬНОЇ МЕРЕЖІ

3.1 Розбиття мережі на підмережі на основі IP-адрес

Для розбиття мережі лікарні на підмережі будемо використовувати наступні адреси підмереж та масок: перший поверх - 192.168.1.0, другий поверх - 192.168.2.0 та третій поверх - 192.168.3.0 із маскою 255.255.255.0.

Кожна підмережа має свою власну адресу підмережі та маску, яка дозволяє керувати комунікацією в межах кожного поверху. Комп'ютери на кожному поверсі підтримують унікальні IP-адреси з відповідної функції адреси підмережі, і шлюзом для них служить IP-адреса комутатора [5].

На рис. 3.1 представлена логічна схема побудованої мережі відповідно до технічного завдання, а також організовано розбиття всієї мережі на VLAN.

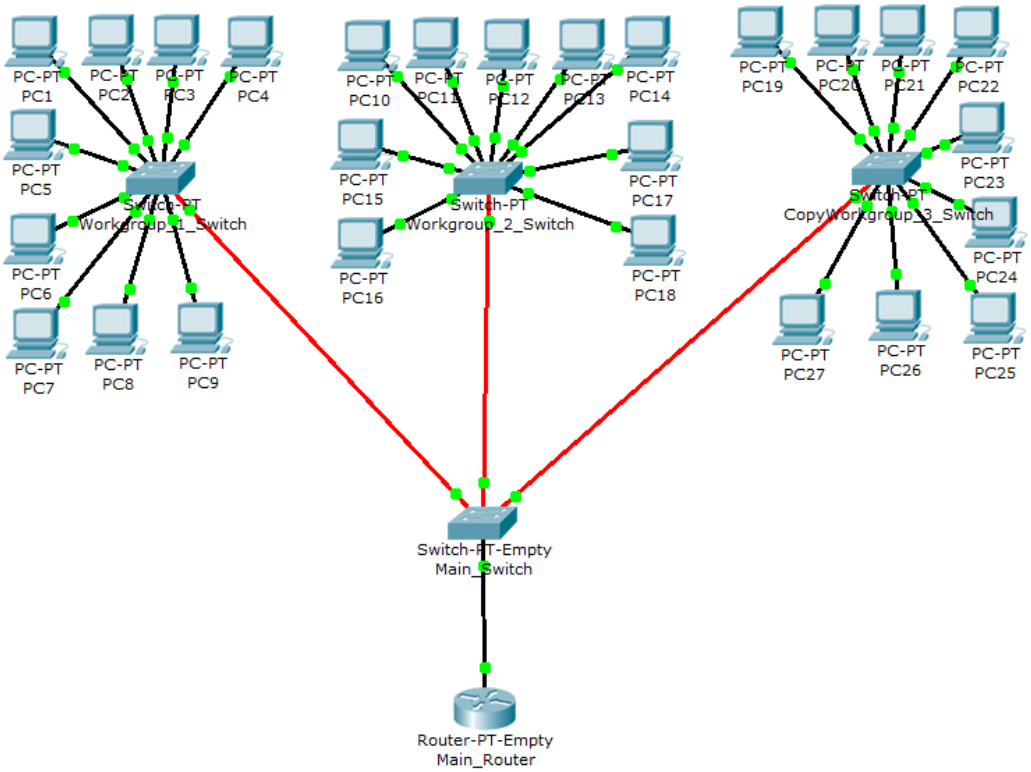

Рисунок 3.1 – Логічна організація мережі

3.2 Особливості захисту інформації у лікарнях

У червні 2019 р. Міністерство охорони здоров'я України оприлюднило для громадського обговорення проект Концепції інформатизації охорони здоров'я. Основою стратегії визнано тактику орієнтованості на пацієнта, що означає безперервне накопичення та зберігання даних з прив'язкою до облікового запису пацієнта в його електронній медичній картці, надання пацієнту, як суб’єкту персональних даних, можливості керувати власними медичними даними й доступом до них. Реалізація цього принципу веде до того, що "медичні дані ходять за пацієнтом" при зміні ним лікаря або закладу, що надає пацієнту медичні послуги [24].

Технологія передбачає пріоритетність електронної форми, тобто при створенні, обміні та зберіганні даних перевага надається електронній формі даних, що обробляються із застосуванням інформаційно-комп'ютерних технологій [24].

Одним із засобів фізичного захисту є системи архівації і дублювання інформації. Актуально як для індивідуальних користувачів так і для корпоративних мереж [24].

Програмні засоби захисту включають антивірусні програми, системи розмежування повноважень, програмні засоби контролю доступу [24].

Щодо захисту медичної інформації, оскільки вона належить до конфіденційної і є об’єктом захисту на законодавчому рівні у відповідності до Закону «Про захист персональних даних» від 01.06.2010 р., № 2297-VI в інформаційній системі медичного закладу об’єктами захисту є [24]:

– інформація в базах даних (БД) систем керування базами даних (СКБД);

– ресурси файлового сервера лікувально-профілактичного закладу;

– резервні копії БД СКБД і архівні копії ресурсів файлового сервера;

– керуюча інформація операційної системи, СКБД, автоматизоване робоче місце (АРМ) адміністратора медичної інформаційної системи (МІС) та адміністратора інформаційної безпеки (ІБ);

– технологічний процес збору, обробки, зберігання та передачі інформації в МІС;

– апаратно-програмний комплекс, що забезпечує роботу МІС.

До МІС висуваються підвищені вимоги щодо достовірності та обмеженості доступу до інформації, технічних заходів захисту даних і програм медичної інформаційної системи, юридичної відповідальності [24].

У відповідності до цього в МІС реалізовано ряд заходів безпеки, які проводяться системно на всіх етапах її діяльності: від проектування і розробки до впровадження і експлуатації, перекривають всі відомі загрози безпеки, орієнтовані на тактичне випередження загроз, при цьому повинні відповідати нормам законодавства і відомчим актам системи охорони здоров'я [24].

Інформаційна безпека забезпечується спеціальними програмними засобами – підсистемою інформаційної безпеки, що виконує такі основні функції [24]:

– організація санкціонованого доступу до даних;

– моніторинг небезпечних подій;

– управління властивостями користувача МІС;

– ведення журналів безпеки.

Описані засоби забезпечення безпеки дозволяють МІС здійснювати необхідний комплекс заходів захисту інформації та програм, що є необхідною умовою придатності МІС до її експлуатації [24].

Відомості, якими оперує медична інформаційна система, є персональними даними та можуть становити лікарську таємницю. Крім того, бази даних МІС всіх рівнів містять критично важливу інформацію, від якої, зокрема, може залежати життя людини, тому ключовим фактором при створенні МІС має стати забезпечення цілісності бази даних і можливість стеження за станом системи та її безпекою [26].

Для забезпечення конфіденційності інформації, яка використовується та контролюється МІС, на сучасному етапі розвитку ІБ застосовують такі дії [26]:

– за допомогою комп'ютерного алгоритму присвоюються букви і цифри паролю; користувач може в будь-який час отримати новий пароль;

– кожен пароль змінюється один раз на шість місяців;

– завідувачі відділеннями видають паролі і визначають рівень повноважень;

– всім користувачам повідомляють про те, що пароль прирівнюється до офіційного підпису і що ні за жодних обставин і нікому він не може бути розкритий [26];

– група обслуговування інформаційної системи видає паролі завідувачам відділень і контролює їх використання;

– доступ до даних може обмежуватися як паролем, так і місцем знаходженням терміналу;

– користувачі автоматично відключаються від системи при зупинці роботи терміналу більш ніж на 5 хв;

– комп'ютерна система зберігає в пам'яті кожен випадок доступу до інформації про пацієнтів з фіксацією особистості, професійної належності, місця, типу отриманої інформації, дати і часу [26];

– кожен співробітник, який використовує МІС, має можливість побачити на дисплеї імена всіх осіб, які переглядали певну персональну електронну медичну картку [26];

– пацієнт може запитати список осіб, які переглядали його медичну картку;

– термінали блокуються в разі введення нелегального пароля кілька разів;

– термінали автоматично виводять на екран попередження, якщо користувач переглядає картку знаменитостей, співробітників лікарні та їхніх родичів [26];

– термінали за випадковим принципом виводять на дисплей попередження про конфіденційність відомостей приблизно на кожен 500-й запит відомостей про пацієнта [26];

– для доступу з домашнього телефону потрібен другий пароль на базі вбудованого в систему, специфічний по відношенню до пацієнта, наприклад, дівоче прізвище матері [26].

3.3 Перевірка рівня безпеки та працездатності локальної обчислювальної мережі

Для забезпечення безпечної роботи мережі в першу чергу було вирішено питання авторизації користувачів. Як основне та найбільш захищене рішення для авторизації користувачів корпоративної мережі передбачено використовувати стандарт 802.1x. Таке рішення дозволяє використовувати єдину прозору схему авторизації користувачів для проводової мережі. Важливим фактором є кроссплатформенність рішення – 802.1x реалізований на всіх популярних операційних системах – як Unix-based, так і Windows, і Linux. Можлива інтеграція авторизації з Active Directory, використовуючи штатні засоби системи Windows Server 2008 – Network Policy and Access Server (NPAS).

В локальній мережі для захисту буде використовуватися ViPNet Office Firewall – це програмний міжмережевий екран, призначений для невеликих та середніх організацій та є сертифікованим міжмережевим екраном з 4-м класом захищеності. Він дозволяє забезпечити захист локальної мережі від будь-яких атак з Інтернету, а також дає можливість гнучкого керування доступом до інтернет-ресурсів та організації віртуальних локальних мереж. Тому в новій ЛОМ спочатку запланували використовувати аналогічну програмну конфігурацію [25].

Використання стандарту 802.1x дозволяє впровадити додаткові сервіси для забезпечення мережевої безпеки – такі як перевірка клієнтських машин на відповідність тим чи іншим вимогам локальних політик, наприклад, наявність

антивірусу. Можливе централізоване призначення VLAN порту користувача в момент авторизації, застосування різних правил фільтрації трафіку при авторизації того чи іншого користувача комутатором чи маршрутизатором [18].

З точки зору користувача – єдиною відмінністю мережі захищеною з використанням протоколу 802.1x є необхідність ввести свій логін та пароль при першому підключенні до мережі.

Необхідно реалізувати схему підключення до дротової мережі, при якій всі користувачі поділяються на кілька груп, залежно від необхідних доступів до корпоративних ресурсів, кожній групі виділяється окремий VLAN (свій, на кожному поверсі), до кожного групового VLAN застосовуються необхідні правила фільтрації трафіку. При підключенні користувальницької станції до проводової мережі, аутентифікатор (тобто комутатор) надсилає запит на надання доступу до мережі для даного користувача до RADIUS-серверу – NPAS – і у разі позитивної відповіді (Access - Accept) додатково отримує від RADIUS-сервера інформацію про групу користувача. Далі трафік користувача позначається відповідною групою VLAN-ідентифікатором, і до трафіку застосовуються необхідні правила фільтрації [18].

Для дотримання корпоративних безпекових політик клієнти з вимкненим 802.1x суплікантом повинні поміщатися в карантинний VLAN, якому заборонено доступ до корпоративних ресурсів.

Всі порти користувацьких комутаторів налаштовані в режимі динамічного призначення VLAN-у в якому буде тегуватися трафік користувача. На комутаторах це може бути зроблено наступним чином:

```
protocols {
dot1x {
authenticator {
authentication-profile-name sl_dot1x;
interface {
all {
supplicant multiple;
```

```
retries 2;
quiet-period 10;
transmit-period 3;
supplicant-timeout 3;
maximum-requests 2;
guest-vlan GUEST;
server-reject-vlan AUTH-FAILED block-interval 120 eapol-block;
server-fail vlan-name GUEST;
}
}
}
```

Тут в секції «all» можлива вказівка різних таймерів протоколу, а також ім'я карантинних VLAN, в які буде поміщений користувач, як реакцію на відповіді сервера авторизації. У приведених налаштуваннях користувач буде поміщений у VLAN з ім'ям GUEST при відключеному супліканті, і у VLAN AUTH-FAILED при відмові авторизації з боку RADIUS-сервера.

У ході роботи було визначено логічні схеми структурних блоків мережної інфраструктури та найбільш раціональні способи підключення кожного з блоків до ядра мережі. Наведено механізм авторизації користувачів проводової мережі. Створено план адресації з урахуванням особливостей мережної інфраструктури – потреба у достатній кількості адрес з використання маршрутизації до рівня доступу. Створено необхідну для реалізації проекту фізичну схему. Розроблена система готова до впровадження та повністю задовольняє поставленим вимогам.

Для перевірки працездатності обраного рішення авторизації користувачів у проводовій мережі, було зібрано стенд із комутатора Juniper EX 4200, віртуалізованого сервера з Windows Server 2008 та тестового комп'ютера з інстальованою ОС Windows 10 (рис. 3.2).

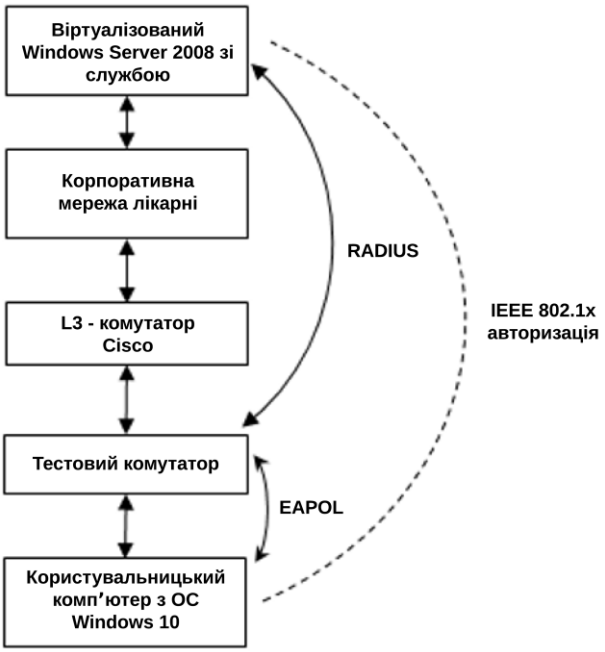

Рисунок 3.2 - Схема тестового стенду для перевірки 802.1x авторизації

Налаштування RADIUS-сервера

Під час тестування використовувався вбудований в ОС Windows 10 802.1x супплікант, «Служба дротового автоналаштування». Необхідна конфігурація з боку сервера аутентифікації (PNAC):

– службу NPS запущено;

– NPS зареєстровано в Active Directory;

– створено шаблон Pre-shared key;

– додано radius-клієнт – тестовий свіч, вказана його адреса та шаблон;

– створені політики авторизації – «RADIUS -сервер для кабельного підключення 802.1x»;

– вибрано метод автентифікації – тестувався PEAP;

– вказано «Параметри керування трафіком» - налаштовані атрибути, які віддаватимуться сервером комутатору при авторизації користувача – необхідно для роботи функції призначення VLAN при авторизації. Необхідні атрибути - Tunnel-Type = VLAN, Tunnel-Medium-Type = 802, Tunnel-Private-Group-ID = test.

Налаштування комутатора

З боку комутатора необхідна конфігурація 802.1x буде простіша. Приведемо налаштування тестового RADIUS-сервера:

```
192.168.1.10 {
port 1812;
secret "$9$hashhashahshashahsh"; ## SECRET-DATA
source-address 192.168.1.250;
}
profile profile1 {
authentication-order radius;
radius {
authentication-server 192.168.1.254;
}
}
```

Також включаємо 802.1x авторизацію в режимі одиночного клієнта на всіх інтерфейсах комутатора:

```
authenticator {
authentication-profile-name profile1;
interface {
all {
supplicant single;
}
}
}
```

Перевірка працездатності

Спочатку, на тестовому комп'ютері користувача служба дротової автонастроювання відключена:

admin@ex4200> show dot1x interface ge-0/0/0 detail

ge-0/0/0.0

Role: Authenticator

Administrative state: Auto

Supplicant mode: Single

Номер retries: 3

Quiet period: 60 seconds

Transmit period: 30 seconds

Mac Radius: Disabled

Mac Radius Restrict: Доступно

Reauthentication: Enabled

Налаштована зміна терміну: 3600 seconds

Supplicant timeout: 30 seconds

Server timeout: 30 seconds

Maximum EAPOL requests: 2

Guest VLAN member: <not configured>

Після включення служби проводового автоналаштування та введення логіна та пароля користувача на тестовому комп'ютері, авторизація пройшла успішно і порт комутатора був переведений у потрібний VLAN:

ge-0/0/0.0

Role: Authenticator

Administrative state: Auto

Supplicant mode: Single

Номер retries: 3

Quiet period: 60 seconds

Transmit period: 30 seconds

Mac Radius: Disabled

Mac Radius Restrict: Доступно

Reauthentication: Enabled

Налаштована зміна терміну: 3600 seconds

Supplicant timeout: 30 seconds

Server timeout: 30 seconds

Maximum EAPOL requests: 2

Guest VLAN member: <not configured>

Supplicant: mail\t.est, BC:AE:C5:EA:FF:FF

Operational state: Authenticated

Backend Authentication state: Idle

Authentcation метод: Радіус

Authenticated VLAN: test

Session Reauth interval: 3600 seconds

Reauthentication due in 2911 seconds

Для роботи декількох пристроїв підключених до одного порту комутатора (наприклад IP-телефону з вбудованим комутатором, через який підключається система користувача) необхідно дозволити підключення декількох користувачів в конфігурації EX 4200:

```
authenticator {
authentication-profile-name profile1;
interface {
all {
  supplicant multiple ;
}
}
}
```

За результатами перевірки на стенді працездатність обраних рішень для побудови локальної обчислювальної мережі та забезпечення виконання корпоративних політик мережної безпеки було підтверджено.

Розроблена система відповідає всім вимогам технічного завдання. Побудована мережева інфраструктура має такі характеристики:

– безпека – за рахунок використання 802.1x авторизації користувачів для доступу до мережі, шифрування даних, що передаються там, де це необхідно, відділення зовнішньої мережі від внутрішньої;

– стійкість та високий рівень доступності – за допомогою резервування ключових вузлів системи та використання протоколів з високою швидкістю збіжності;

– масштабованість – за рахунок розширюваності логічної структури мережі, фізичної системи, що передбачає подальше розширення;

– високий рівень функціональності – за рахунок функціоналу обраного для побудови мережі обладнання та орієнтованості на стандартні протоколи та технології;

– зручність та простота в обслуговуванні – досягається за допомогою однаковості використовуваного обладнання та його конфігурації, автоматизації налаштування обладнання рівня доступу з використанням IEEE 802.1x – конфігурація портів залежно від підключеного користувача, застосування правил фільтрації даних, що передаються.

ВИСНОВКИ

Підземна лікарня є однією з найважливіших інфраструктурних споруд, які можуть забезпечити надійне та ефективне функціонування медичної системи в умовах надзвичайних ситуацій. Однією з ключових складових такої лікарні є локальна дротова мережа, яка грає важливу роль у забезпеченні безперебійної роботи медичного обладнання та ефективної комунікації між медичним персоналом.

Оптимальне розміщення обладнання і прокладання кабелів, а також використання сучасних технологій дозволили досягти максимальної швидкості передачі даних та безперебійного доступу до них, що є важливим для своєчасної діагностики та лікування пацієнтів.

Проведене дослідження дозволило провести комплексний аналіз наукової літератури щодо проблеми проектування та побудови локальних обчислювальних мереж. В результаті аналізу підходів до діагностики мереж, виявлення несправностей та аналізу можливих організаційно-технічних заходів було виявлено, що для автоматизації підтримки процесу забезпечення працездатності локальної обчислювальної мережі підприємства необхідно вирішити комплекс науково-технічних завдань, орієнтованих на створення умов сталої та безперебійної роботи мережі.

У практичній частині дослідження докладно описаний процес проектування та побудови ЛОМ, проведений аналіз технічного завдання якого показав, що орієнтація виконавців замовлення на створення локальної обчислювальної мережі, на забезпечення автоматизації технологічних процесів обробки інформації, дозволить забезпечити швидкий та надійний обмін службовою інформацією. У тому числі документообігу та спільному використанні програмного забезпечення, що використовується у мережі.

Важливою обставиною при введенні локальної обчислювальної мережі в експлуатацію стала можливість використання програмного забезпечення нової

мережі, спрямоване на забезпечення її безпечної роботи та здійснення контролю за доступом до інформаційних ресурсів.

Перевірка рівня безпеки та працездатності локальної обчислювальної мережі, що проводиться з використанням відповідних технологій, описаних у роботі, дозволяє стверджувати, що працездатність обраних рішень для побудови корпоративної локальної обчислювальної мережі та забезпечення виконання корпоративних політик мережної безпеки виконана на належному рівні.

Крім того, в мережі було використано надійні технології мережної безпеки та резервного копіювання даних, що забезпечує захист від можливих кібератак та втрати даних.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Тарнавський Ю.А., Кузьменко І. М. Організація комп'ютерних мереж: підручник: для студ. спеціальності 121 "Інженерія програмного забезпечення" та 122 "Комп'ютерні науки" / КПІ ім. Ігоря Сікорського. – Київ: КПІ ім. Ігоря Сікорського, 2018. – 259 с.

2. Олещенко Л.М. Організація комп'ютерних мереж: конспект лекцій: навч. посіб. для студ. спеціальності 121 "Інженерія програмного забезпечення", спеціалізації "Програмне забезпечення комп'ютерних та інформаційно-пошукових систем" / КПІ ім. Ігоря Сікорського. – Київ: КПІ ім. Ігоря Сікорського, 2018. – 225 с.

3. Попов І.І., Максимов Н.В. Комп'ютерні мережі: навчальний посібник. - М.: ФОРУМ: ІНФРА - М, 2015. – 365 с.

4. Телекомунікаційні системи передавання інформації [Текст] / Климаш М.М. , Колодій Р.С. – Л.: 2018. – 632 с.

5. Загальні принципи організації мереж [Электронный ресурс] - Режим доступу: https://elib.lntu.edu.ua/sites/default/files/elib_upload/123%20%D0%BF%D0%BE%D1%81%D1%96%D0%B1%D0%BD%D0%B8%D0%BA%20%D0%BA%D0%BE%D0%BC%D0%BF'%D1%8E%D1%82%D0%B5%D1%80%D0%BD%D0%B0%20%D1%96%D0%BD%D0%B6%D0%B5%D0%BD%D0%B5%D1%80%D1%96%D1%8F/page36.html.

6. Бартон, М. Обоснование модернизации сети [Электронный ресурс] / М.Бартон // LAN: Корпоративные сети, 2012.

7. Башарін Г.П., Самуйлов К.Є. Сучасний етап розвитку теорії телетрафіку [Текст] // Інформаційна математика. - 2001. - № 1, С. 153 - 166.

8. Основи технічного діагностування Навчально–методичний посібник / Уклад.: А.Я. Жук, Г. П. Малишев – Запоріжжя, 2007. – 114с.

9. Букатов, А.А. Аналіз досвіду створення ефективних регіональних відомчих та міжвідомчих інформаційно-обчислювальних телекомунікаційних мереж. [Текст]/АА Букатов// Вісник комп'ютерних та інформаційних технологій. - М.: Машинобудування, 2006. - №5. С.42-48.

10. Управління процесами серед інформаційного обміну АСУ при відновленні після збоїв. [Текст] / О.М. Савенков, АВ Єрьоменко, СВ Костін, М.А. Сонькін // Вісник комп'ютерних та інформаційних технологій. - М: Машинобудування, 2007. - №10. - С. 35 - 40.

11. О.І. Кушлик-Дивульська, Б.Р. Кушлик. Основи теорії прийняття рішень. – К., 2014. – 94с

12. Оліфер, В.Г., Оліфер, Н.О. Комп'ютерні мережі. Принципи, технології, протоколи: Підручник для вузів. Видання четверте. [Текст] Видавництво: Пітер: 2020. - 1000 с.

13. «Методи забезпечення якості надання телекомунікаційних послуг / К.О. Мамика [Електронный ресурс] – Режим доступу: https://ela.kpi.ua/server/api/core/bitstreams/24f47769-6ec2-4e43-b2af-83f6ffe18bac/content.

14. Технічні засоби автоматизації (Частина 1) / М.В. Лукінюк, В.П. Лисенко, В.Є. Лукін, А.М. Гладкий, С.А. Шворов, А.А. Руденський, А.А. Заверткін.–Ніжин.: Видавець ПП Лисенко М.М., 2017.–569 с.

15. Репин, Г.В. Среда для анализа сетевого трафика на базе инфраструктуры с открытым кодом [Электронный ресурс] / Г.В. Репин, М.Ю. Кузнецов, К.Н. Василенко // Телематика. 2009.

16. КОМП’ЮТЕРНІ МЕРЕЖІ Частина 1 НАВЧАЛЬНИЙ ПОСІБНИК [Електронний ресурс]: навч. посіб. для студ. спеціальності 121 «Інженерія програмного забезпечення» та 126 «Інформаційні системи та технології», спеціалізації «Інженерія програмного забезпечення інформаційно управляючих систем» та «Інформаційне забезпечення робототехнічних систем»/ Б. Ю. Жураковський, І.О. Зенів; КПІ ім. Ігоря Сікорського. – Електронні текстові дані (1 файл: 8,6 Мбайт). – Київ : КПІ ім. Ігоря Сікорського, 2020. – 336 с.

17. Надійність обчислювальних пристроїв, ПК і комп'ютерних систем / Курс лекцій [Електронный ресурс] – Режим доступу: https://elib.lntu.edu.ua/sites/default/files/elib_upload/%D0%95%D0%9D%D0%9C%D0%9A_%D0%9D%D0%B0%D0%B4%D1%96%D0%B9%D0%BD%D1%96%D1%81%D1%82%D1%8C/page6.html.

18. Комп’ютерні мережі : Навчальний посібник / В. Г. Хоменко, М. П. Павленко. – Донецьк : ЛАНДОН-ХХІ, 2011. – 316 с.

19. С.О. Довгий, О.В. Копійка ІТ-інфраструктура як базова складова цифрової трансформації. Монографія – К.: ТОВ «Видавництво «Юстон», 2023. – 458 с.

20. Технічна експлуатація засобів та систем зв’язку: навч. посіб. / Л. М. Сакович та ін.; ІСЗЗІ КПІ ім. Ігоря Сікорського. – Київ, 2021. – 176 с.

21. Ю. А. Тарнавський, І. М. Кузьменко. Організація комп’ютерних мереж. Підручник // Київ: КПІ ім. Ігоря Сікорського; – 2018. – [Електронний ресурс] – Режим доступу: https://ela.kpi.ua/bitstreams/e0a0c843-a57d-4d82-8f42-0eba294bef1f/download

22. Іванов А.В. Практична діагностика мереж. [Електронний ресурс] / А.В. Іванов. - ProLAN, 2009.

23. Проектування систем автоматизації [Текст]: навч. посібник / М.С. Пушкар, С.М. Проценко – Д.: Національний гірничий університет, 2013. – 268 с.

24. Захист медичної інформації – важлива задача сьогодення. [Електронний ресурс] – Режим доступу: https://www.bsmu.edu.ua/blog/2531-zahyst-medychnoi-informacii/

25. Медичні інформаційні системи. [Електронний ресурс] – Режим доступу: https://studfile.net/preview/5280934/page:7/

26. Інформаційні технології в медицині. / За редакцією В.Г. Книгавка. [Електронний ресурс] – Режим доступу: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://repo.knmu.edu.ua/bitstream/123456789/25671/1/%D0%A0%D0%B0%D0%B4%D0%B7%D1%96%D1%88%D0%

B5%D0%B2%D1%81%D1%8C%D0%BA%D0%B0%20%D0%86%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D0%B9%D0%BD%D1%96%20%D1%82%D0%B5%D1%85%D0%BD%D0%BE%D0%BB%D0%BE%D0%B3%D1%96%D1%97%20%D0%B2%20%D0%BC%D0%B5%D0%B4%D0%B8%D1%86%D0%B8%D0%BD%D1%96%20%D0%9F%D1%96%D0%B4%D1%80%D1%83%D1%87.%20%D1%83%D0%BA%D1%80.pdf