Міністерство освіти і науки України

Харківський національний університет радіоелектроніки

Факультет навчально-науковий центр заочного навчання
(повна назва)

Кафедра електронних обчислювальних машин
(повна назва)

КВАЛІФІКАЦІЙНА РОБОТА

Пояснювальна записка

Рівень вищої освіти другий (магістерський)

Метод підвищення відмовостійкості мультисегментної корпоративної комп'ютерної мережі закладу охорони здоров'я
(тема)

Виконав:

студент II курсу, групи КСМзм-23-1

Міхнов Є.Д.
(прізвище, ініціали)

Спеціальність

123 «Комп'ютерна інженерія»
(код і повна назва спеціальності)

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

Освітня програма

Комп'ютерні системи та мережі
(повна назва освітньої програми)

Керівник: доц. Ткачов В.М.
(посада, прізвище, ініціали)

Допускається до захисту

Зав. кафедри ЕОМ _____ Коваленко А.А.
(підпис) (прізвище, ініціали)

2025 р.

Харківський національний університет радіоелектроніки

Факультет навчально-науковий центр заочної форми навчання

Кафедра електронних обчислювальних машин

Рівень вищої освіти другий (магістерський)

Спеціальність 123 «Комп'ютерна інженерія»
(код і повна назва)

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

Освітня програма Комп'ютерні системи та мережі
(повна назва)

ЗАТВЕРДЖУЮ:
Зав. кафедри _____
(підпис)
"____" _____ 20___ р.

ЗАВДАННЯ

НА КВАЛІФІКАЦІЙНУ РОБОТУ

студенту Міхнову Євгену Дмитровичу
(прізвище, ім'я, по батькові)

1. Тема роботи Метод підвищення відмовостійкості мультисегментної корпоративної комп'ютерної мережі закладу охорони здоров'я

затверджена наказом по університету від "13" листопада 2024 р. № 189 СТз

2. Термін подання здобувачем роботи до екзаменаційної комісії 15 січня 2025 року

3. Вхідні дані до роботи Комп'ютер Artline WorkStation W99 – 12 шт.;
сервер – 2 шт.;
міжмережний екран Fortinet – 1 шт.;
роутер Cisco – 3 шт.;
комутатор Cisco – 2 шт.;
комутатор Aruba – 1 шт.

4. Перелік питань, що потрібно опрацювати у роботі
Вступ.
1. Аналіз стану та вимог до відмовостійкості корпоративних мереж у закладах охорони здоров'я
2. Моделювання мультисегментної комп'ютерної мережі
3. Розробка методу підвищення відмовостійкості мультисегментної мережі
4. Реалізація запропонованого методу
5. Оцінка ефективності методу
Висновки

5. Перелік графічного матеріалу із зазначенням креслеників, схем, плакатів, комп'ютерних ілюстрацій (слайдів) 12 слайдів формату А4.

6. Консультанти розділів роботи (заповнюється за наявності консультантів згідно з наказом, зазначеним у п.1)

Найменування розділу	Консультант (посада, прізвище, ім'я, по батькові)	Позначка консультанта про виконання розділу	
		підпис	дата

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1	Аналіз літературних джерел та постановка	14.11.2024-20.11.2024	
	задачі		
2	Розробка математичної моделі та методу	21.11.2024-05.12.2024	
	підвищення відмовостійкості		
3	Моделювання та тестування	06.12.2024-20.12.2024	
	запропонованого методу		
4	Реалізація методу та оформлення	21.12.2024-05.01.2025	
	кваліфікаційної роботи		
5	Підготовка до захисту та подання роботи	06.01.2025-07.01.2025	

Дата видачі завдання 13 листопада 2024 р.

Студент _____
(підпис)

Керівник роботи _____ доц. Ткачов В.М.
(підпис) (посада, прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка кваліфікаційної роботи: 117 с., 24 рис., 3 дод., 30 джерел.

ВІДМОВОСТІЙКІСТЬ, МУЛЬТИСИГМЕНТНА МЕРЕЖА, КОРПОРАТИВНА МЕРЕЖА, ЗАКЛАД ОХОРОНИ ЗДОРОВ’Я, РЕЗЕРВУВАННЯ, СЕГМЕНТАЦІЯ, МЕРЕЖНИЙ ТРАФІК.

Метою кваліфікаційної роботи є розробка методу підвищення відмовостійкості мультисегментної корпоративної комп'ютерної мережі закладу охорони здоров'я шляхом використання резервування, сегментації мережних компонентів та впровадження інструментів моніторингу для забезпечення безперебійного функціонування критично важливих систем.

У ході виконання кваліфікаційної роботи досліджено сучасні підходи до забезпечення відмовостійкості мультисегментних корпоративних мереж, зокрема у закладах охорони здоров’я. Розроблено математичну модель для аналізу функціонування мережі та визначення критичних точок ризику. Запропоновано метод підвищення відмовостійкості, який базується на резервуванні компонентів, сегментації мережних сегментів та інтеграції засобів моніторингу й діагностики. Проведено моделювання роботи мережі із застосуванням запропонованого методу, підтверджено його ефективність у підвищенні стабільності та безперервності роботи мережних сервісів. Результати дослідження можуть бути використані для оптимізації мережної інфраструктури закладів охорони здоров’я та інших організацій із критично важливими ІТ-системами.

ABSTRACT

Master`s thesis: 117 pages, 24 figures, 3 appendices, 30 sources.

FAULT TOLERANCE, MULTISEGMENT NETWORK, CORPORATE NETWORK, HEALTHCARE INSTITUTION, REDUNDANCY, SEGMENTATION, NETWORK TRAFFIC.

The primary goal of this thesis is to develop a method for improving the fault tolerance of a multisegment corporate computer network in a healthcare institution by utilizing component redundancy, network segmentation, and monitoring tools to ensure the uninterrupted operation of critical systems.

Modern approaches to ensuring the fault tolerance of multisegment corporate networks, particularly in healthcare institutions, were studied. A mathematical model was developed to analyze the network's operation and identify critical risk points. A method for enhancing fault tolerance was proposed based on component redundancy, network segment segmentation, and integrating monitoring and diagnostic tools. Network operation modeling with the proposed method was conducted, confirming its effectiveness in improving the stability and continuity of network services. The research results can be applied to optimize the network infrastructure of healthcare institutions and other organizations with mission-critical IT systems.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

DDoS – розподілена атака на відмову в обслуговуванні (англ., Distributed Denial of Service)

DHCP – протокол динамічної конфігурації хоста (англ., Dynamic Host Configuration Protocol)

DNS – система доменних імен (англ., Domain Name System)

DoS – атака на відмову в обслуговуванні (англ., Denial of Service)

HTTPS – протокол безпечної передачі гіпертексту (англ., HyperText Transfer Protocol Secure)

IDS – система виявлення вторгнень (англ., Intrusion Detection System)

IPS – система запобігання вторгнень (англ., Intrusion Prevention System)

ISP – інтернет-провайдер (англ., Internet Service Provider)

LAN – локальна обчислювальна мережа (англ., Local Area Network)

MTTF – середній час до відмови (англ., Mean Time to Failure)

MTTR – середній час відновлення (англ., Mean Time to Repair)

NAT – трансляція мережних адрес (англ., Network Address Translation)

QoS – якість обслуговування (англ., Quality of Service)

RPO – цільовий показник точки відновлення (англ., Recovery Point Objective)

RTO – цільовий час відновлення (англ., Recovery Time Objective)

TCP/IP – протокол управління передачею/інтернет-протокол (англ., Transmission Control Protocol/Internet Protocol)

VLAN – віртуальна локальна мережа (англ., Virtual Local Area Network)

WAN – глобальна обчислювальна мережа (англ., Wide Area Network)

WLAN – бездротова локальна мережа (англ., Wireless Local Area Network)

ВСТУП

Сучасні корпоративні комп’ютерні мережі закладів охорони здоров’я виконують критично важливу роль у забезпеченні надійного функціонування інформаційних систем, підтримці медичних процесів, зберіганні й передачі чутливих даних пацієнтів. Інтеграція цифрових технологій у медичну сферу зумовлює високу залежність від стабільності та безперервності роботи мережної інфраструктури. Будь-які збої або відмови в роботі такої інфраструктури можуть призводити до серйозних наслідків, включаючи втрату даних, порушення роботи медичних послуг і навіть загрозу життю пацієнтів.

Проблема забезпечення відмовостійкості мультисегментних корпоративних мереж є актуальною через постійно зростаючу складність архітектурних рішень, обумовлену вимогами до безпеки, продуктивності та масштабованості. До того ж, медичні установи стають мішенями для кібератак, що підвищує ризики несанкціонованого доступу до конфіденційної інформації. Таким чином, розвиток методів підвищення відмовостійкості мережі набуває стратегічного значення.

Аналіз існуючих підходів до забезпечення відмовостійкості показує, що традиційні методи, такі як фізичне резервування та базові засоби моніторингу, часто є недостатніми у випадку високонавантажених мереж, які обслуговують медичні заклади. У зв’язку з цим виникає необхідність розробки нового методу, що поєднує сучасні підходи до резервування, сегментації мережних компонентів і використання інструментів діагностики та автоматизації.

Метою даної роботи є розробка методу підвищення відмовостійкості мультисегментної корпоративної комп’ютерної мережі закладу охорони здоров’я шляхом інтеграції оптимізованих рішень для забезпечення безперебійного функціонування критичних інформаційних систем.

Для досягнення поставленої мети вирішуються наступні завдання:

- провести аналіз сучасних методів забезпечення відмовостійкості корпоративних мереж;

- розробити математичну модель мультисегментної мережі для виявлення критичних точок відмов;

- запропонувати метод підвищення відмовостійкості з використанням резервування та сегментації мережних компонентів;

- провести моделювання та оцінку ефективності розробленого методу;

- надати рекомендації щодо впровадження методу у реальні умови закладів охорони здоров’я.

Об’єктом дослідження є мультисегментна корпоративна комп’ютерна мережа закладу охорони здоров’я, а предметом дослідження – методи та засоби підвищення її відмовостійкості.

Наукова новизна роботи полягає у розробці нового методу підвищення відмовостійкості корпоративних мереж, що враховує специфіку архітектури мультисегментних систем, з урахуванням вимог до безпеки та продуктивності.

Практичне значення роботи полягає у можливості застосування розробленого методу для оптимізації роботи мережної інфраструктури закладів охорони здоров’я, підвищення їх ефективності та зниження ризиків збоїв у роботі.

1 АНАЛІЗ СТАНУ ТА ВИМОГ ДО ВІДМОВОСТІЙКОСТІ КОРПОРАТИВНИХ МЕРЕЖ У ЗАКЛАДАХ ОХОРОНИ ЗДОРОВ’Я

1.1 Особливості корпоративних мереж у закладах охорони здоров’я

Корпоративні комп'ютерні мережі у закладах охорони здоров’я є невід’ємною складовою сучасної медичної інфраструктури, яка забезпечує стабільне функціонування інформаційних систем та підтримує широкий спектр цифрових медичних послуг [1]. Ці мережі характеризуються підвищеним рівнем складності, оскільки повинні інтегрувати в собі технології для обробки великих обсягів чутливих даних, забезпечувати їхню конфіденційність, доступність і цілісність, а також відповідати суворим вимогам до відмовостійкості [2]. Основні особливості таких мереж зумовлені їхньою мультисегментною архітектурою, підвищеними вимогами до безпеки та високим рівнем гетерогенності обладнання.

Однією з ключових особливостей корпоративних мереж у медичних установах є їхня мультисегментна структура, яка включає декілька функціональних сегментів: адміністративний, клінічний, діагностичний та дослідницький [3]. Кожен сегмент виконує специфічні завдання, наприклад, адміністративний сегмент забезпечує управління закладом, облік ресурсів і фінансові операції, тоді як клінічний сегмент підтримує електронні медичні записи пацієнтів, медичну діагностику та інші клінічні процеси. Така структурна організація дозволяє розмежувати доступ до різних типів даних і зменшити ризик поширення збоїв між сегментами.

Другий важливий аспект полягає у високому рівні гетерогенності обладнання та програмного забезпечення. У закладах охорони здоров’я використовується велика кількість апаратних та програмних рішень, включаючи сервери, комутатори, маршрутизатори, безпровідні точки доступу, персональні комп’ютери, мобільні пристрої та IoT-сенсори. Крім

того, до мережі часто підключене спеціалізоване медичне обладнання, таке як МРТ–сканери, апарати УЗД, системи моніторингу пацієнтів та лабораторні автоматизовані системи. Ця різноманітність створює значні виклики у забезпеченні сумісності, стандартизації комунікаційних протоколів і централізованого управління [4].

Корпоративні мережі медичних закладів також мають бути оптимізовані для обробки великих обсягів даних. Такі дані включають як структуровані (електронні медичні записи), так і неструктуровані (зображення, відео, телемедичні трансляції). Для цього необхідно використовувати сучасні методи зберігання даних, такі як хмарні обчислення, розподілені файлові системи (DFS) та бази даних NoSQL, які забезпечують масштабованість і високу швидкість доступу до даних.

Особливу увагу необхідно приділяти питанням інформаційної безпеки, оскільки медичні дані є одними з найцінніших для зловмисників. До критичних заходів захисту належать:

- впровадження систем виявлення та запобігання вторгнень (IDS/IPS);
- багатофакторна автентифікація для захисту доступу;
- шифрування чутливих даних;
- регулярний аудит безпеки та тестування на проникнення.

Ще однією характерною рисою корпоративних мереж у закладах охорони здоров’я є потреба у забезпеченні високого рівня відмовостійкості. Збої у функціонуванні мережі можуть спричинити серйозні наслідки, включаючи порушення безперервності медичних процесів та втрату критично важливих даних. Для мінімізації таких ризиків використовуються технології резервування (наприклад, RAID для дискових систем, кластеризація серверів), відмовостійкі протоколи маршрутизації (OSPF, BGP), а також засоби автоматичного переключення між основними і резервними каналами зв’язку [5, 6].

Окремо слід зазначити, що корпоративні мережі у медичних установах повинні відповідати міжнародним та локальним стандартам і нормативним

актам. Наприклад, у більшості країн такі мережі мають бути сумісними зі стандартами захисту даних (GDPR, HIPAA), які встановлюють вимоги до зберігання, передачі та обробки персональної інформації пацієнтів, а враховуючи євроінтеграцію України, відповідні ж вимоги висуваються і до мереж вітчизняних медичних установ [7 - 9].

Таким чином, корпоративні мережі у закладах охорони здоров'я є складними багатофункціональними системами, що повинні забезпечувати безперебійність, інформаційну безпеку та ефективність медичних процесів. Їхні особливості зумовлюють необхідність використання інтегрованих підходів до проектування, моніторингу та управління, які враховують специфіку медичної галузі та сучасні виклики інформаційного суспільства, особливо в умовах реалій, з якими стикнулася наша країна з лютого 2022 року.

1.2 Аналіз типових загроз і причин відмов в IT-інфраструктурі медичних установ

Вразливість IT-інфраструктури медичних установ до загроз і збоїв може призвести до серйозних наслідків. У цьому підрозділі аналізуються основні типові загрози та причини відмов, характерні для IT-інфраструктури медичних установ.

Кіберзлочинність є одним із найбільш серйозних класів викликів для інформаційної безпеки медичних установ [10-12]. До ключових форм загроз належать:

- програми-вимагачі – програми, які шифрують дані медичного закладу, блокуючи доступ до них, а зловмисники вимагають викуп за розшифрування. Для медичних установ це особливо критично, оскільки заблоковані дані можуть включати життєво важливу інформацію про пацієнтів. Наприклад, атака WannaCry у 2017 році паралізувала роботу численних лікарень у Великій Британії, призвівши до відміни тисяч

медичних процедур;

- шкідливі програми для крадіжки даних використовується для прихованого збору конфіденційної інформації, наприклад, паролів, медичних даних пацієнтів або фінансових транзакцій закладу.

Фішингові атаки є одним із найбільш розповсюджених методів соціальної інженерії, який використовується для отримання доступу до систем медичних закладів. Зловмисники надсилають електронні листи або повідомлення, що імітують офіційні джерела (наприклад, керівництво лікарні чи постачальників програмного забезпечення), із метою змусити працівників надати свої облікові дані або виконати шкідливі дії.

Зловмисники часто використовують теми, пов’язані з терміновими медичними запитами, наприклад, «Термінова заявка на обробку даних пацієнта». У випадку успіху фішингової атаки може бути отримано доступ до серверів із медичними записами або фінансових даних.

З широким впровадженням пристроїв Інтернету речей (IoT) у медичних закладах (монітори пацієнтів, інфузійні помпи, розумні датчики) суттєво зросли ризики, пов'язані з їхньою уразливістю: відсутність оновлень безпеки, використання стандартних або слабких паролів, недостатнє шифрування даних.

Несанкціонований доступ є серйозною загрозою, особливо у випадках, коли заклади використовують слабкі механізми автентифікації: використання слабких паролів, відсутність багатофакторної автентифікації, внутрішні загрози, коли працівники медичних закладів, які мають доступ до чутливої інформації, можуть ненавмисно або навмисно зловживати цим доступом. Наприклад, передача даних стороннім особам або їхнє використання в особистих цілях.

Технічні відмови – це ще один клас викликів, який є однією з найбільш поширених причин порушень у роботі ІТ-інфраструктури медичних закладів. Вони можуть спричинити втрату доступу до інформаційних систем, порушити роботу критично важливих сервісів або навіть повністю

паралізувати діяльність установи. У цьому контексті технічні збої мають різну природу, включаючи апаратні, програмні, а також проблеми сумісності.

Медичні установи використовують різноманітне апаратне обладнання, включаючи сервери, маршрутизатори, комутатори, точки доступу та мережні пристрої. Збої такого обладнання є критичними через високу залежність закладів від безперервної роботи ІТ-систем. Основні причини таких відмов:

- зношування компонентів, а саме, сервери, дискові накопичувачі та мережні пристрої мають обмежений термін служби, після чого значно підвищується ймовірність їхньої несправності. Наприклад, жорсткі диски часто виходять з ладу через механічне зношування після декількох років активного використання;

- перевантаження обладнання, зокрема, високе навантаження на мережне обладнання або сервери через великий обсяг трафіку чи обробку великих даних може спричинити перегрівання, вихід із ладу компонентів або зниження продуктивності;

- відсутність резервування, зокрема, використання обладнання без резервних компонентів створює єдину точку відмови, що може призвести до збоїв у всій системі;

- відсутність джерел безперебійного живлення або стабілізаторів напруги робить обладнання вразливим до перебоїв в електропостачанні, що може спричинити пошкодження серверів або втрату даних.

Програмні відмови виникають через помилки в роботі операційних систем, прикладного програмного забезпечення або конфігурації мережних пристроїв. До основних типів таких помилок належать: баги в програмному забезпеченні, невчасні або некоректні оновлення, недостатність системного ресурсу.

ІТ-інфраструктура медичних закладів складається з великої кількості компонентів, які часто розроблені різними виробниками. Ця гетерогенність створює потенційні проблеми сумісності, зокрема:

- мережні пристрої або програми можуть використовувати різні

протоколи, що не завжди коректно взаємодіють між собою (наприклад, конфлікт між застарілими протоколами, такими як SMBv1, і сучасними стандартами безпеки);

- системи для управління медичними записами, лабораторного аналізу чи діагностичного обладнання можуть не підтримувати єдині інтерфейси, що ускладнює їхнє інтегрування в загальну мережу;

- у багатьох медичних закладах використовуються застарілі інформаційні системи, які не підтримують сучасні стандарти сумісності та безпеки.

Розглянутий клас технічних відмов можуть мати каскадний характер, коли збій однієї компоненти призводить до порушення роботи всієї системи. Наприклад, вихід із ладу сервера баз даних може спричинити неможливість доступу до медичних записів пацієнтів, що вплине на прийняття рішень лікарями. Крім того, технічні збої можуть спричинити значні фінансові збитки через потребу у відновленні системи, втрату репутації та можливі юридичні наслідки.

Людський фактор є одним із найпроблемніших причин збоїв та проблем в IT-інфраструктурі медичних закладів. Хоча автоматизація значною мірою знижує залежність систем від людського втручання, повністю виключити вплив персоналу неможливо. Відсутність належної підготовки, помилки в експлуатації та недотримання протоколів безпеки можуть спричиняти серйозні наслідки для функціонування мережі.

Одна з найбільш поширених причин збоїв пов’язана з ненавмисними діями працівників, що можуть спричинити порушення роботи систем, а саме некоректна конфігурація обладнання, випадкове видалення важливих файлів, зміна налаштувань баз даних або некоректне оновлення програмного забезпечення, неправильне реагування на аварійні ситуації.

Медичний персонал, зокрема лікарі, медсестри та адміністративні працівники, часто не мають достатніх знань у галузі інформаційних технологій. Це створює низку ризиків, які складно піддаються аналізу та

вивченню. Ігнорування встановлених правил безпеки або неналежне їх виконання може суттєво знизити захищеність ІТ-інфраструктури, зокрема: часто працівники встановлюють прості або повторювані паролі, які легко зламати, що підвищує ризик несанкціонованого доступу; з метою спрощення роботи працівники можуть ділитися паролями або використовувати спільні облікові записи, що значно ускладнює контроль доступу; підключення до корпоративної мережі особистих мобільних телефонів або ноутбуків без антивірусного захисту може створити вразливості в системі в цілому; використання небезпечного програмного забезпечення як то Телеграм може призвести до витоку інформації до країни-агресора тощо.

Існує клас внутрішніх загрози, які можуть бути ненавмисними (через необережність) або навмисними (через зловмисні дії), а саме: використання флеш-накопичувачів із шкідливим програмним забезпеченням через незнання або спроби обійти обмеження мережних політик; працівники можуть свідомо передавати конфіденційну інформацію третім сторонам, наприклад, конкурентам або зловмисникам, або змінювати налаштування системи з метою створення саботажу; зловмисники можуть маніпулювати співробітниками, змушуючи їх виконувати шкідливі дії, наприклад, надати облікові дані або відкрити фішинговий лист.

Основні проблеми загально інфраструктурного рівня стосуються її фізичної організації, технологічних недоліків і неправильного управління і за це, як правило, відповідає адміністратор цієї інфраструктури. Однією з ключових проблем інфраструктури є відсутність резервних компонентів, які забезпечують безперебійність роботи. Фізичні аспекти організації ІТ-інфраструктури також можуть стати причиною її ненадійності, наприклад:

- сервери та мережні пристрої, розташовані у приміщеннях без належного клімат-контролю, можуть перегріватися, що призводить до виходу з ладу апаратного забезпечення;

- обладнання може бути пошкоджене внаслідок затоплення, пожежі або навіть механічного впливу;

- якщо компоненти інфраструктури (наприклад, сервери для медичних даних і сервери загального призначення) розташовані без чіткої сегментації, це підвищує ризики збоїв у разі відмови одного з компонентів.

Найбільш непередбачуваними є природні та техногенні катастрофи, наслідки воєнних дій, такі як ракетні удари, з якими стикнулася наша країна унаслідок повномасштабного вторгнення рф. Ці події, що виникають через зовнішні фактори, можуть спричинити не лише збої в роботі обладнання, а й повну втрату даних та вихід з ладу критично важливих систем. Особливістю таких катастроф є їхня раптовість і масштабність, що ускладнює своєчасне реагування та ліквідацію наслідків.

Усі перелічені фактори підкреслюють важливість розробки комплексного підходу до забезпечення відмовостійкості. Відмова в роботі навіть однієї компоненти мережі може мати каскадний ефект, порушуючи роботу інших підсистем. Наприклад, збій сервера, що зберігає медичні записи, може призвести до неможливості доступу до даних пацієнтів, що унеможливлює своєчасне прийняття медичних рішень.

1.3 Нормативні та регуляторні вимоги до відмовостійкості мереж у сфері охорони здоров’я

Як було зазначено раніше, система охорони здоров’я в сучасному світі все більше інтегрується з цифровими технологіями, що дозволяє забезпечувати високу якість медичних послуг, обробляти великі обсяги даних про пацієнтів та покращувати управління медичними ресурсами. Проте така цифровізація вимагає відповідності суворим нормативним і регуляторним вимогам, які спрямовані на забезпечення безпеки, доступності, конфіденційності та відмовостійкості мережних інфраструктур.

Міжнародна практика регулювання відмовостійкості інформаційних систем у медичній сфері базується на кількох ключових стандартах та нормативних актах, які охоплюють різні аспекти функціонування мережних

інфраструктур. Україна, як країна, яка обрала шлях євроінтеграції, намагається дотримуватися опорних стандартів, які існують у цивілізованому світі, зокрема:

- HIPAA (Health Insurance Portability and Accountability Act) – норматив, прийнятий у США, який зобов'язує медичні заклади забезпечувати захист і доступність персональних медичних даних [9]. Згідно з HIPAA, кожна інформаційна система має бути захищена від зовнішніх і внутрішніх загроз, а також гарантувати доступ до даних навіть у разі аварійних ситуацій. До обов'язкових заходів входять створення резервних копій, впровадження систем моніторингу загроз у реальному часі та регулярне тестування аварійного відновлення;

- законодавство ЄС щодо захисту персональних даних зобов'язує медичні заклади впроваджувати технічні та організаційні заходи для забезпечення відмовостійкості. Зокрема, передбачено обов'язкове шифрування даних, зберігання резервних копій у географічно розподілених зонах та швидке відновлення доступу до даних у разі збоїв;

- стандарт ISO/IEC 27001 визначає вимоги до системи управління інформаційною безпекою, включаючи забезпечення відмовостійкості. ISO/IEC 27001 передбачає розробку політик з управління ризиками, впровадження механізмів моніторингу доступності даних, а також регулярну оцінку готовності систем до аварійних ситуацій.

В Україні функціонування інформаційних систем у медичній сфері регулюється кількома ключовими нормативними документами [13]:

- Закон України «Про захист персональних даних», який зобов'язує медичні заклади забезпечувати технічні та організаційні заходи для захисту даних пацієнтів. Це включає захист від втрат, викликаних технічними збоями, та створення механізмів відновлення систем після аварій. Наголошується на необхідності обмеження доступу до конфіденційної інформації та використання сучасних засобів безпеки, таких як багатофакторна автентифікація;

- Наказ МОЗ України від 19.10.2015 року № 681 «Про затвердження нормативних документів щодо застосування телемедицини у сфері охорони здоров'я», який регламентує функціонування електронної системи охорони здоров'я. Він визначає необхідність використання резервних копій для зберігання даних пацієнтів та впровадження протоколів для забезпечення безперервності роботи систем у разі технічних проблем.

- ДСТУ ISO/IEC 27001 – національний стандарт, адаптований до міжнародного ISO/IEC 27001, регламентує створення безпечних і відмовостійких інформаційних систем у всіх галузях, зокрема у сфері охорони здоров'я. Стандарт передбачає регулярний моніторинг мереж, тестування на проникнення та використання технологій для забезпечення резервування даних.

Однією з ключових вимог нормативних документів є забезпечення резервування даних та впровадження ефективних механізмів аварійного відновлення. Усі критично важливі дані, зокрема медичні записи, повинні бути збережені у кількох фізично розташованих місцях. Використання географічно розподілених дата-центрів мінімізує ризики втрати даних у разі катастроф. Рекомендується впровадження реплікації даних у реальному часі для забезпечення їхньої актуальності.

План аварійного відновлення є обов'язковим документом, який регламентує порядок дій персоналу під час технічних збоїв. До нього входить опис процесів резервного копіювання, переключення на резервні системи та тестування сценаріїв відновлення.

Захист медичних даних від втрат і несанкціонованого доступу є обов'язковим елементом нормативних вимог. Усі дані пацієнтів повинні бути зашифровані як під час зберігання, так і при передачі через мережу. Використання багатофакторної автентифікації є стандартом для доступу до критичних систем. Системи мають забезпечувати детальний аудит усіх дій користувачів. Нормативи також передбачають постійний моніторинг систем для виявлення загроз та аномальної активності у реальному часі.

Нормативні вимоги також поширюються на фізичну безпеку серверів і обладнання: серверні кімнати повинні бути обладнані сучасними системами пожежогасіння, клімат-контролю та обмеження доступу; у разі перебоїв з електропостачанням обладнання має бути підключене до джерел безперебійного живлення або генераторів, що стало досить актуально через пошкодження енергетичної інфраструктури унаслідок ракетних ударів рф; приміщення для зберігання даних повинні бути захищені від затоплення, пожеж та інших природних загроз.

Регулярний аудит і сертифікація інформаційних систем медичних закладів є важливим аспектом нормативних вимог, зокрема, повинна проводиться перевірка виконання вимог щодо відмовостійкості, захищеності даних та планів аварійного відновлення; заклади охорони здоров’я мають можливість сертифікувати свої системи відповідно до міжнародних стандартів (наприклад, ISO/IEC 27001), що підтверджує їхню відповідність найкращим практикам.

Нормативні та регуляторні вимоги до відмовостійкості мереж у сфері охорони здоров’я встановлюють комплекс заходів для захисту інформації, забезпечення її доступності та безперервності роботи систем. Виконання цих вимог дозволяє не лише знизити ризики втрати даних, а й забезпечити стабільну роботу медичних закладів навіть за умов надзвичайних ситуацій. Інтеграція стандартів та відповідність міжнародним і національним нормативам є основою для ефективного управління IT-інфраструктурою в сучасних закладах охорони здоров’я на шляху євроінтеграції України.

1.4 Огляд існуючих підходів до забезпечення відмовостійкості корпоративних мереж

Спочатку варто розглянути підхід, заснований на резервуванні компонентів [14] (рисунок 1.1), який полягає у тому, що необхідно робити дублювання ключових елементів IT-інфраструктури, таких як сервери,

комутатори, маршрутизатори, джерела живлення або інші критично важливі компоненти. Резервування може бути активним, коли дублюючий компонент працює паралельно з основним (наприклад, у режимі Active-Active), або пасивним, коли резервний компонент активується лише після виходу основного з ладу (Active-Standby).

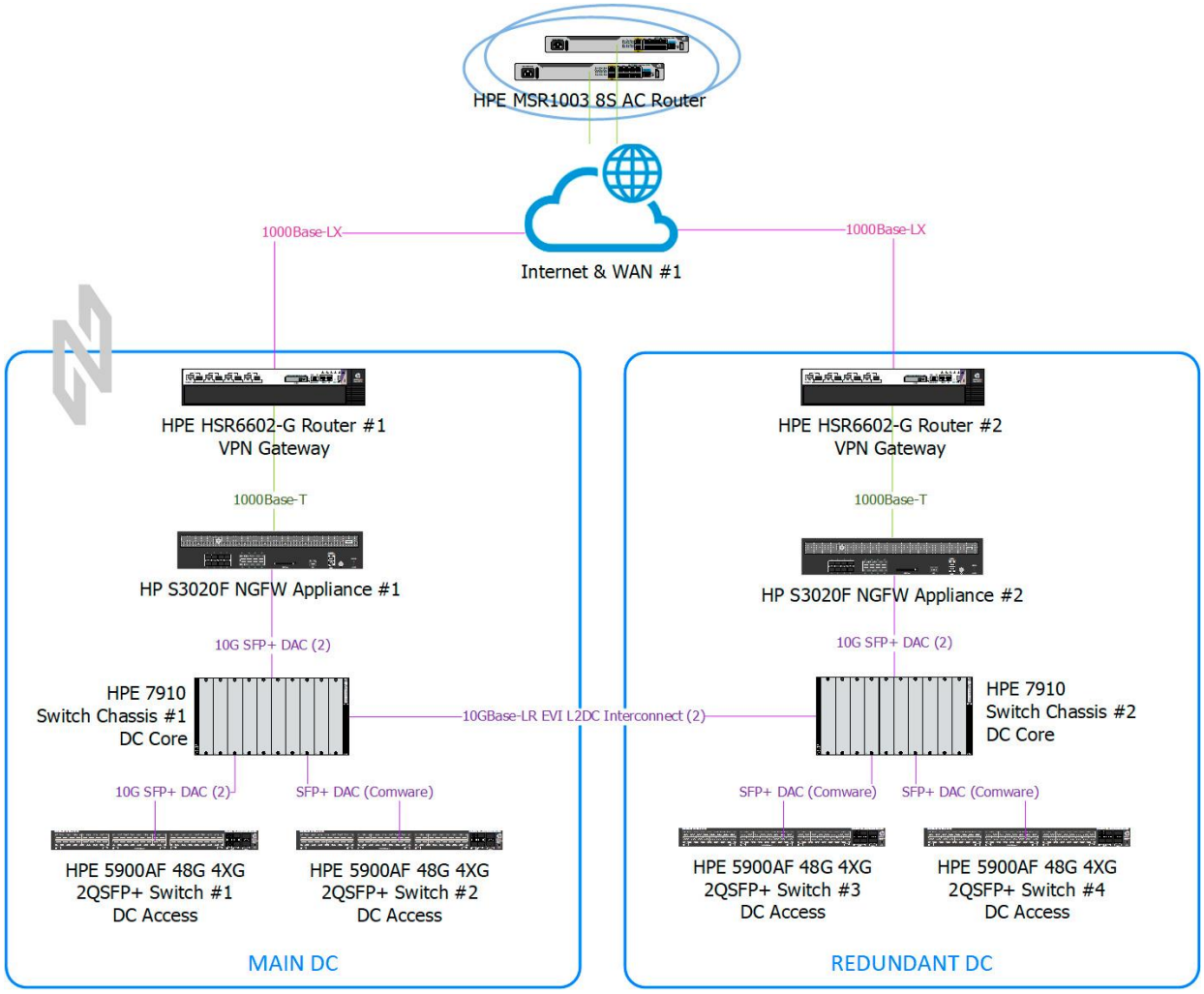

Рисунок 1.1 – Приклад побудови відмовостійкої мережної інфраструктури на базі рішення HPE

У рамках цього підходу також використовуються технології RAID для забезпечення захищеності даних, резервні мережні підключення для забезпечення стійкості до втрати з’єднання, а також резервування джерел електроживлення.

Такий підхід дає можливість досягти високу надійність завдяки зниженню ймовірності втрати даних чи зупинки систем, а також здатність автоматично переключатися на резервний компонент без значного впливу на користувачів.

Резервування компонентів, хоч і є одним із найстаріших і найпоширеніших підходів до забезпечення відмовостійкості [14], має низку суттєвих недоліків, які обмежують його ефективність у сучасних корпоративних мережах. По-перше, дублювання обладнання призводить до значного збільшення витрат, особливо для масштабних систем, таких як мережі медичних установ із високими вимогами до продуктивності. По-друге, цей підхід не враховує потенційних проблем одночасного виходу з ладу як основного, так і резервного компонентів через загальні зовнішні фактори, наприклад, катастрофічні події, що вражають весь дата-центр. По-третє, пасивне резервування неефективно використовує ресурси, оскільки резервні компоненти часто простоюють без навантаження, що створює значні втрати енергоресурсів і нераціональне використання інфраструктури. По-четверте, цей підхід не здатний самостійно забезпечити безпеку або стійкість до кіберзагроз: якщо шкідливе програмне забезпечення вражає основний компонент, то резервний, зазвичай, залишається так само уразливим. Нарешті, інтеграція та управління резервними системами є надзвичайно складними, що підвищує ризик людських помилок при налаштуванні або обслуговуванні, фактично перетворюючи систему резервування на ще одну потенційну точку відмови.

Наступний підхід побудований на використанні кластеризації серверів [4, 15]. Кластеризація серверів у корпоративній мережі передбачає об'єднання кількох фізичних або віртуальних серверів у єдиний кластер для спільної роботи над виконанням завдань. Сервери працюють синхронно, забезпечуючи балансування навантаження та автоматичне переключення на інший вузол у разі відмови. Це рішення найчастіше

використовується для баз даних, веб-додатків і медичних інформаційних систем, що потребують високої доступності.

Кластери можуть бути побудовані з використанням таких технологій, як Microsoft Failover Clustering, VMware vSphere High Availability або Apache Hadoop для розподіленої обробки даних.

Безперечно, перевагами буде можливість додавання нових вузлів без зупинки роботи системи та забезпечення безперебійної роботи навіть у разі виходу одного з вузлів з ладу.

Кластеризація серверів, незважаючи на її популярність і ефективність у забезпеченні відмовостійкості, має значні недоліки, які обмежують її застосування, особливо у критично важливих системах, таких як медичні установи. По-перше, сама архітектура кластеризації є складною, вимагає дорогого апаратного забезпечення та висококваліфікованих спеціалістів для налаштування і підтримки. Навіть невеликі помилки конфігурації можуть спричинити неочікувані збої у всій системі. По-друге, кластеризація значно залежить від загального фізичного середовища, наприклад, спільного сховища. Якщо виникають проблеми із загальним ресурсом, наприклад, через вихід з ладу мережі зберігання (SAN), весь кластер стає нефункціональним, що створює єдину точку відмови. По-третє, програмне забезпечення для кластеризації, навіть таке, як VMware vSphere або Microsoft Failover Clustering, часто не захищене від збоїв самого кластерного менеджера, що може паралізувати всю систему. По-четверте, кластеризація не вирішує питання географічної відмовостійкості: Якщо катастрофа торкнеться всього дата-центру, усі вузли кластера будуть знищені. Нарешті, цей підхід не ефективний для високонавантажених систем, де кластерний менеджер може стати вузьким місцем через перевантаження запитами, що фактично знижує продуктивність і стабільність мережі замість її підвищення.

Підхід, заснований на балансуванні навантаження [16, 17] полягає у рівномірному розподілі вхідного трафіку між кількома серверами чи мережними компонентами. Для цього використовуються балансувальники

навантаження, які працюють за різними алгоритмами, такими як Round Robin (послідовне перенаправлення), Least Connections (до вузла з найменшою кількістю з’єднань) або Weighted Balancing (зважене перенаправлення).

Цей підхід широко використовується у високонавантажених системах, таких як медичні портали або платформи телемедицини, для забезпечення стійкості до пікових навантажень завдяки забезпеченню високої доступності сервісів завдяки розподіленню трафіку та можливістю динамічного додавання або видалення серверів.

Підхід, заснований на балансуванні навантаження, хоч і є важливим інструментом для підвищення продуктивності мереж, має серйозні недоліки, які обмежують його ефективність у забезпеченні відмовостійкості. По-перше, цей підхід є надзвичайно залежним від коректності роботи балансувальника навантаження. Помилки в його алгоритмах чи конфігурації можуть призводити до дисбалансу, коли одні вузли перенавантажені, а інші залишаються незадіяними, що фактично паралізує систему. По-друге, балансувальник сам по собі часто стає «єдиною точкою відмови»: якщо він виходить з ладу, то вся система перестає працювати, навіть якщо сервери залишаються функціональними. По-третє, цей підхід не захищає від глобальних відмов, таких як збій електроживлення або катастрофічна подія, які виводять з ладу всі вузли одночасно. По-четверте, балансування не вирішує проблему втрати даних або стану сесій: у разі відмови одного вузла запити можуть перенаправлятися на інший, але дані, які вже оброблялися, будуть втрачені. Нарешті, впровадження балансування навантаження у гетерогенних системах із різними типами обладнання або програмного забезпечення є складним, що призводить до значних витрат часу і ресурсів, знижуючи економічну доцільність такого рішення.

Суть підходу, заснованого на резервуванні каналів зв’язку забезпечує наявність декількох незалежних каналів для доступу до мережі [18]. У разі втрати основного з'єднання трафік автоматично перенаправляється на резервний канал. Зазвичай використовуються різні типи з’єднань

(оптоволоконні, DSL, 4G/5G) для забезпечення максимального захисту від зовнішніх факторів.

Однак, і цей підхід має певні недоліки, зокрема, він не гарантує однакової продуктивності резервних каналів: у разі перемикання на резервний канал користувачі часто стикаються зі зниженням швидкості або стабільності зв'язку, що негативно впливає на роботу систем у режимі реального часу, наприклад, телемедичних платформ. По-друге, вартість підтримки кількох каналів зв'язку є високою, особливо якщо використовуються незалежні провайдери або різні технології передачі даних (оптоволокно, LTE, супутниковий зв'язок). По-третє, автоматичне перемикання на резервний канал може не спрацювати належним чином через затримки виявлення збою основного каналу, що призводить до втрати з'єднання. Нарешті, інтеграція різнорідних каналів зв'язку у єдину мережу є технічно складною задачею, яка вимагає спеціалізованого обладнання та програмного забезпечення, а це збільшує ризик помилок у конфігурації та загальну складність системи.

Технології аварійного відновлення, як підхід до забезпечення відмовостійкості корпоративних мереж, спрямовані на швидке відновлення роботи систем після критичних збоїв. До основних компонентів підходу належать регулярне резервне копіювання даних, розробка та тестування сценаріїв аварійного відновлення. Ці технології дозволяють мінімізувати час простою і втрату даних.

Головна перевага такого підходу – гарантія збереження даних навіть у разі катастрофічних збоїв.

Технології аварійного відновлення [19], незважаючи на їхню важливість для забезпечення відмовостійкості, демонструють низку системних обмежень, які знижують їхню ефективність у високонавантажених і критично важливих системах, таких як корпоративні мережі медичних установ. По-перше, технології аварійного відновлення значною мірою залежать від коректності та актуальності резервних копій, але навіть у разі

регулярного створення копій вони часто не забезпечують синхронності в реальному часі, що призводить до втрати транзакцій або незбережених змін (часова затримка між точкою відмови та відновленням, або Recovery Point Objective, RPO). По-друге, відновлення після збою зазвичай потребує значного часу (Recovery Time Objective, RTO), що є неприйнятним для систем із жорсткими вимогами до безперебійності, таких як телемедицина або управління електронними медичними записами. По-третє, географічна розподіленість резервних майданчиків, що є обов'язковою умовою для захисту від катастрофічних подій, значно підвищує фінансові витрати, включаючи витрати на передачу даних, підтримку інфраструктури та регулярне тестування. По-четверте, технології аварійного відновлення часто не інтегровані з механізмами превентивного моніторингу та прогнозування, що обмежує їхню здатність запобігати збоям до їхнього виникнення. Нарешті, складність реалізації планів аварійного відновлення створює високі вимоги до компетентності персоналу, оскільки навіть незначні помилки в сценаріях відновлення можуть спричинити додаткові затримки або часткове відновлення системи, що фактично нівелює їхню основну мету.

Далі доцільно перейти до підходів, пов'язаних з технологіями віртуалізації [20]. Віртуалізація дозволяє створювати ізольовані віртуальні середовища, які можуть бути легко перенесені на інші фізичні платформи у разі відмови обладнання. Завдяки гіпервізорам, таким як VMware ESXi, Microsoft Hyper-V або Proxmox, можна забезпечувати високу гнучкість і знижувати залежність від конкретного апаратного забезпечення. Це дозволяє забезпечувати швидке відновлення віртуальних машин у разі збою та здійснювати оптимізація використання фізичних ресурсів.

Підхід, заснований на віртуалізації [20], хоч і є одним із найсучасніших інструментів для підвищення відмовостійкості, має значні недоліки, які обмежують його універсальність та ефективність у критично важливих системах, таких як мережі медичних установ. Віртуалізація створює високий рівень залежності від гіпервізорів (наприклад, VMware ESXi або Proxmox

VE), які стають єдиною точкою відмови: Збій у програмному забезпеченні гіпервізора може вплинути на всі віртуальні машини, розміщені на фізичному сервері. Віртуалізація потребує значних обчислювальних ресурсів, а перевантаження фізичних серверів у пікові моменти може призвести до зниження продуктивності або навіть до відмови всіх розміщених на них віртуальних середовищ. Уразливість віртуальних середовищ до атак на рівні гіпервізора (наприклад, «VM escape») становить серйозну загрозу для конфіденційних даних і цілісності системи. Витрати на ліцензії, підтримку та оновлення програмного забезпечення для віртуалізації часто є суттєвими, що є критичним для державних медичних закладів.

Інший підхід, заснований на технологіях віртуалізації передбачає використання хмарних рішень [21]. Хмарні рішення забезпечують доступність даних і сервісів завдяки географічному розподілу обчислювальних ресурсів. Для медичних установ часто використовуються моделі Hybrid Cloud, які поєднують локальну інфраструктуру з хмарними сервісами для резервного зберігання даних і аварійного відновлення.

Це дозволяє з однієї сторони досягати високої масштабованості і доступності ресурсів, а з іншої сторони, законодавчі обмеження не дозволяють використовувати в медичній сфері хмарні рішення іноземних вендорів. Залежність від сторонніх провайдерів хмарних послуг створює ризик втрати контролю над даними, особливо якщо провайдер зазнає збою, проводить технічне обслуговування або припиняє діяльність. Така залежність є особливо ризикованою для медичних закладів, де конфіденційність і доступність даних є критичними. Швидкість доступу до хмарних ресурсів може бути серйозно обмежена затримками у передачі даних через мережу, що є неприйнятним для систем реального часу, таких як телемедицина або електронні медичні записи. Навіть провідні хмарні провайдери не гарантують абсолютної доступності (SLA зазвичай обмежується 99,9%), що може бути недостатньо для медичних установ, де простої навіть на декілька хвилин можуть призвести до критичних наслідків. Витрати на хмарні сервіси,

зокрема при роботі з великими обсягами даних або високими обчислювальними навантаженнями, швидко зростають, що робить їх економічно недоцільними для довготривалого використання.

Описані підходи забезпечують високий рівень надійності корпоративних мереж, але кожен із них має свої обмеження (рисунок 1.2).

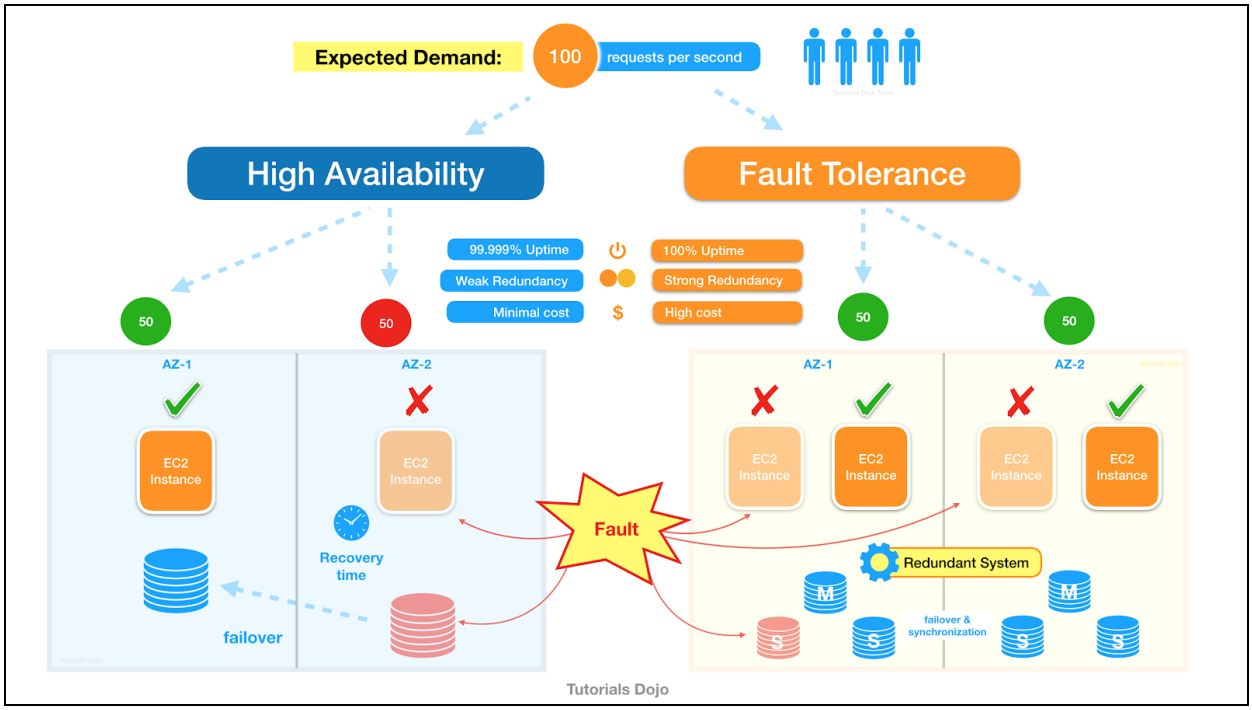

Рисунок 1.2 – Порівняння деякких підходів щодо підвищення відмовостійкості корпоративної мережі

Подальша розробка власного методу буде враховувати сильні сторони цих підходів та усувати їхні слабкі місця, створюючи інтегроване рішення, яке відповідатиме специфічним потребам медичних установ.

2 МОДЕЛЮВАННЯ МУЛЬТИСЕГМЕНТНОЇ КОМП'ЮТЕРНОЇ МЕРЕЖІ ЗАКЛАДУ ОХОРОНИ ЗДОРОВ'Я НА ПРИКЛАДІ ЦЕНТРУ СЛУЖБИ КРОВІ

2.1 Структурні особливості мультисегментної мережі закладу охорони здоров'я

На схемі (рисунок 2.1) представлено структуру мультисегментної комп'ютерної мережі, яка враховує специфіку Центру служби крові. Ядро мережі формується з двох основних маршрутизаторів до яких підключені сегменти через кореневі комутатори. Сегменти розділені за функціональним призначенням: лабораторне обладнання, управління донорськими даними, логістика та складування, адміністративний сегмент, IoT-пристрої, гостьовий доступ і резервування даних. Інтеграція з WAN-мережами і зовнішніми провайдерами забезпечується через підключення до зовнішніх каналів зв'язку. Окремий акцент зроблено на резервуванні ключових компонентів і ізоляції сегментів для забезпечення захищеності даних. Система побудована з урахуванням гнучкості, масштабованості та відмовостійкості для роботи в критичних умовах медичної інфраструктури.

Далі доцільно навести опис ключових сегментів мультисегментної мережі:

- сегмент лабораторного обладнання призначений для підключення автоматизованих лабораторних систем, які виконують дослідження крові (аналізаторів, центрифуг, обладнання для тестування на інфекції). Вимоги: низька затримка передачі даних, ізоляція від інших сегментів, резервування підключення для безперебійної роботи;

- сегмент управління донорськими даними використовується для зберігання та обробки персональних даних донорів, їхніх медичних показників та історій здачі крові. У цьому сегменті також працюють

програми для планування роботи донорських пунктів і ведення реєстрів. Вимоги: високий рівень безпеки, шифрування даних, обмеження доступу;

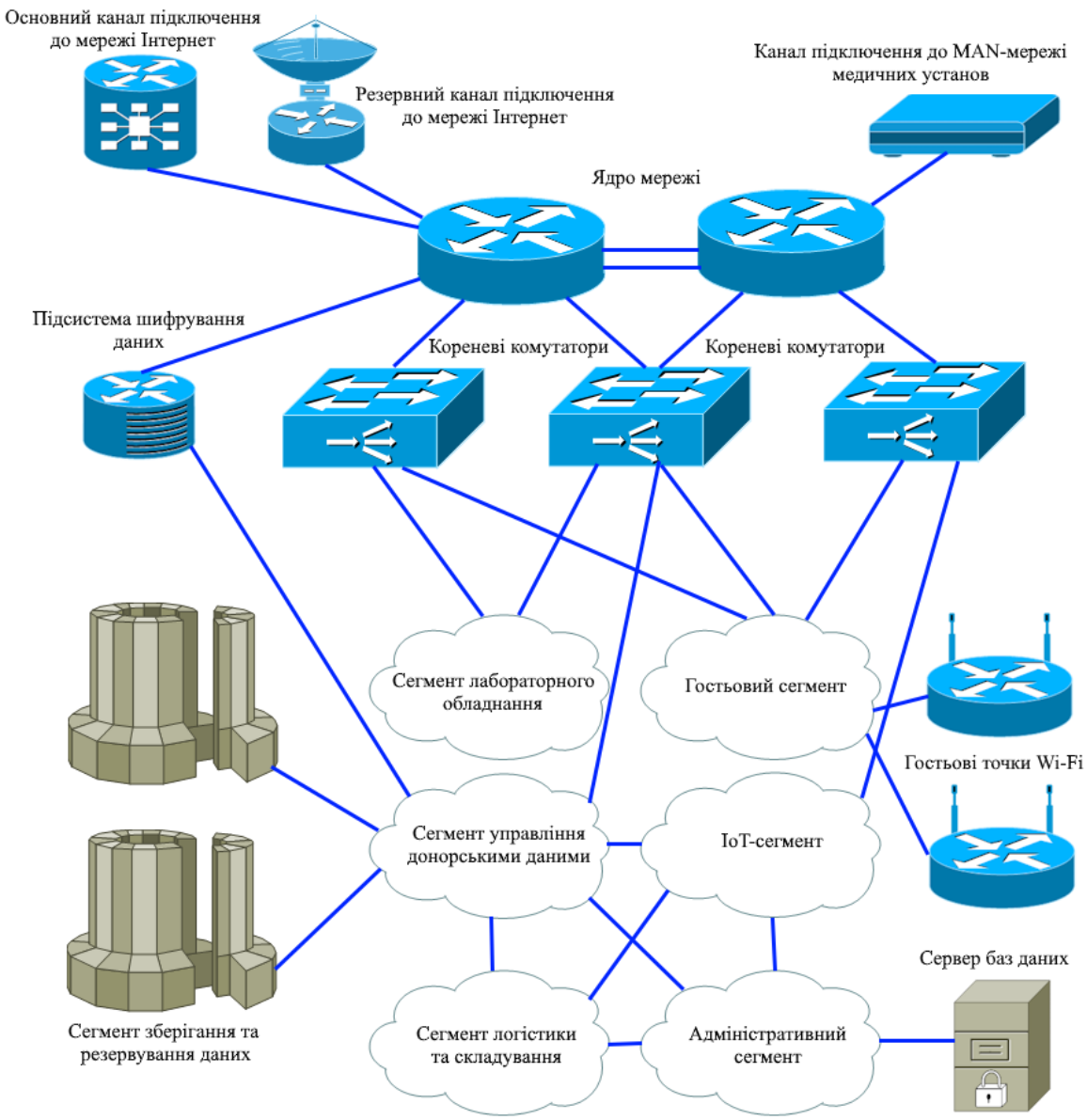

Рисунок 2.1 – Структура мультисегментної комп’ютерної мережі

- сегмент логістики та складування призначений для моніторингу стану зберігання компонентів крові (температурний контроль, умови транспортування), управління інвентаризацією та доставки крові в інші медичні установи. Вимоги: інтеграція з IoT-пристроями (сенсорами температури), резервування для збереження даних про умови транспортування;

- адміністративний сегмент використовується для управління фінансовими, кадровими та юридичними аспектами діяльності служби крові. Вимоги: окремий доступ для співробітників, ізоляція від лабораторного та донорського сегментів;

- IoT-сегмент призначений для роботи з пристроями моніторингу (наприклад, сенсори температури у холодильних камерах, логістичні трекери під час транспортування крові). Вимоги: підтримка стабільного з'єднання з мінімальною затримкою, ізоляція для зменшення ризиків компрометації;

- гостьовий сегмент використовується для відвідувачів (донорів), які отримують доступ до Wi-Fi без можливості взаємодії з іншими сегментами мережі. Вимоги: повна ізоляція від внутрішньої мережі;

- сегмент зберігання та резервування даних - сукупність вузлів, які відповідають за зберігання медичних даних, резервні копії, архіви історичних даних донорів та результати лабораторних аналізів. Вимоги: використання RAID-масивів, реплікація даних у реальному часі, захищеність від фізичних та віртуальних атак.

Взаємодія між сегментами мультисегментної мережі служби крові організована таким чином, щоб забезпечити безпечний і ефективний обмін даними, ізоляцію критично важливих сегментів та їхню інтеграцію в єдину інфраструктуру. Практично усі сегменти підключені до ядра мережі через кореневі комутатори. Це забезпечує централізоване управління трафіком і високошвидкісний обмін даними між сегментами. Міжмережні екрани та VLAN-технології використовуються для розмежування доступу до ресурсів між сегментами. Наприклад, IoT-сегмент із підключеними пристроями моніторингу (сенсорами) ізольований від сегмента управління донорськими даними для уникнення ризиків кіберзагроз. Лабораторне обладнання передає дані про дослідження крові до сегмента управління донорськими даними. Для цього використовується захищене з'єднання, яке забезпечує цілісність даних. Сегмент управління донорськими даними взаємодіє з сегментом логістики та складування, передаючи інформацію про запаси крові, її стан і

необхідність транспортування. Ці процеси контролюються через IoT-пристрої для моніторингу умов зберігання. Адміністративний сегмент отримує агреговані дані з усіх інших сегментів для забезпечення управлінських рішень. Зокрема, він взаємодіє із сегментом управління донорськими даними для отримання звітів про активність донорів, логістикою – для відстеження поставок, і лабораторним сегментом – для моніторингу досліджень. Гостьовий сегмент є повністю ізольованим і не має прямого доступу до інших сегментів. Це забезпечує безпеку критичних даних, дозволяючи відвідувачам та донорам користуватися Wi-Fi без ризику компрометації мережі. Сегмент резервування даних інтегрований з усіма іншими сегментами через ядро мережі. Дані автоматично дублюються з кожного сегмента в резервний, забезпечуючи відновлення інформації у разі збоїв.

Підключення до підключених лікарень і зовнішніх мереж забезпечується через захищені канали зв’язку, що проходять через ядро мережі. Це дозволяє обмінюватися даними з іншими медичними установами.

2.2 Побудова математичної моделі функціонування мультисегментної мережі

Загальна модель описується кортежем:

$$\mathrm{M} = \langle N, L, S, C, B, R, P \rangle, \tag{2.1}$$

де N – множина вузлів мережі (ядро, кореневі комутатори, сегменти);

L – множина зв’язків між вузлами;

S – множина сегментів мережі;

C – конфігурація VLAN і механізмів трафіку;

B – пропускна здатність і затримки каналів зв’язку;

R – механізми резервування (ядра, каналів, даних);

P – політика безпеки для кожного сегмента.

Кожен із елементів моделі (2.1) можна представити у вигляді наступних абстракцій.

1. Вузли мережі (N). Множина вузлів описує основні компоненти мережі:

$$N = \{R_1, R_2, S_1, S_2, \ldots, S_n\}, \tag{2.2}$$

де R_1, R_2 – маршрутизатори ядра мережі;

S_1 – комутатори кореневого рівня;

N_i – вузли в сегментах (сервери, точки Wi-Fi, IoT-пристрої тощо).

2. Зв'язки між вузлами (L):

$$L = \{L_{ij} \mid N_i, N_j \in N\}, \tag{2.3}$$

де L_{ij} – зв'язок між вузлами N_i та N_j.

Для кожного зв'язку визначаються параметри:

$$L_{ij} = \langle B_{ij}, L_{ij}, Q_{ij} \rangle, \tag{2.4}$$

де B_{ij} – пропускна здатність (1 Гбіт/с);

L_{ij} – затримка передачі (в наносекундах);

Q_{ij} – вірогідність втрати пакету.

Для резервування зв'язків використовується механізм MultiWAN:

$$L_{ij}^{резерв} = \{L_{ij}^{(1)}, L_{ij}^{(2)} \ldots\}, \tag{2.5}$$

де $L_{ij}^{(k)}$ – k-й резервний канал.

3. Сегменти мережі (S). Кожен сегмент описується множиною:

$$S = \{S_{Lab}, S_{Donor}, S_{IoT}, S_{Guest}, S_{Admin}, S_{Backup}\}, \quad (2.6)$$

де S_{Lab} – лабораторний сегмент;

S_{Donor} – сегмент управління даними донорів;

S_{IoT} – IoT-сегмент;

S_{Guest} – гостьовий сегмент;

S_{Admin} – адміністративний сегмент;

S_{Backup} – резервування даних.

Кожен сегмент S_i визначається:

$$S_i = \langle N_i, D_i, P_i, F_i \rangle, \quad (2.7)$$

де N_i – вузли в сегменті;

D_i – обсяг даних у сегменті;

P_i – політика доступу;

F_i – функція обробки даних.

4. Конфігурація VLAN (C). Кожен сегмент мережі має власний VLAN:

$$C = \{V_{Lab}, V_{Donor}, V_{IoT}, V_{Guest}, V_{Admin}, V_{Backup}\}, \quad (2.8)$$

Варто зазначити, що VLAN ізолюють трафік між сегментами, а функції маршрутизації забезпечують зв’язок між сегментами через ядро мережі.

5. Пропускна здатність і затримки (B). Для кожного каналу визначаються як $B_{ij} = 1$ Гбіт/с, $L_{ij} \leq 1$ мс.

Обмеження на пропускну здатність кожного сегмента:

$$\sum_{j=1}^{n} T_{ij} \le B_{ij}, \tag{2.9}$$

де T_{ij} – трафік між вузлами.

6. Резервування (R) ядра та каналів забезпечується через механізм MultiWAN і дублювання маршрутизаторів:

$$R = \langle R_{Core}, R_{Links}, R_{Data} \rangle, \tag{2.10}$$

де R_{Core} – дублювання маршрутизаторів R_1, R_2;

R_{Links} – резервні зв’язки $L_{ij}^{резерв}$;

R_{Data} – резервування даних у S_{Backup}.

Ймовірність відмови мережі:

$$P_{відмова} = \prod_{i=1}^{n} \left(1 - P_{резерв,i}\right), \tag{2.11}$$

де $P_{резерв,i}$ – ймовірність успішного резервування вузла або каналу.

7. Для кожного сегмента задається політика доступу:

$$P_{ij} = \begin{cases} 1, якщо\ доступ\ дозволено, \\ 0, якщо\ доступ\ заборонено. \end{cases} \tag{2.12}$$

Всі міжсегментні з’єднання проходять через міжмережний екран.

2.3 Підхід для визначення критичних точок відмовостійкості

У попередньому підрозділі було показано, що мережу можна описати як систему із взаємопов'язаних вузлів та зв’язків, кожен із яких може перейти

у стан відмови. Визначення критичних точок зводиться до аналізу таких компонентів, які мають найбільший вплив на відмовостійкість системи, а відповідно, створити підґрунтя для розробки власного методу забезпечення відмовостійкості такої мережі. В даному підрозділі пропонується розглянути комбінований підхід на базі моделювання роботи мережі через теорію графів та марківські процеси, динамічний аналіз змін стану вузлів і зв'язків через диференціальні рівняння та, наостанок, спектральний аналіз і виявлення сингулярних точок, що відповідають критичним станам мережі.

Отже, мережа описується орієнтованим графом $G(V,E)$ де:

– $V=\{v_1,v_2,...,v_n\}$ – множина вузлів (маршрутизатори, комутатори, сервери, сегменти);

– $E=\{e_{ij}\,|v_i,v_j\in V\}$ – множина зв'язків (канали передачі даних).

– w_{ij} – вага зв'язку e_{ij}, що враховує пропускну здатність, затримку передачі та ймовірність відмови.

Для кожного вузла v_i визначаємо функцію стану:

$$x_i(t)=\begin{cases}1, \ вузол\,працює,\\ 0, \ вузол\,відмовив.\end{cases} \tag{2.13}$$

Аналіз станів здійснюється через марківські процеси, зокрема, простір станів можна описати через вектор станів:

$$\chi(t)=[x_1(t),x_2(t),\ldots,x_n(t)]^T, \tag{2.14}$$

де $x_i(t)\in\{0,1\}$ – стан вузла v_i у момент часу t.

Ймовірність переходу між станами описується матрицею ймовірностей переходу $P(t)=\left[\,p_{ij}(t)\right]$, де

$$p_{ij}(t) = P(x_i \to x_j \mid t). \tag{2.15}$$

Еволюція ймовірностей станів вузлів описується рівнянням Колмогорова-Чепмена:

$$\frac{\partial p(t)}{\partial t} = Q \cdot p(t), \tag{2.16}$$

де $Q = \left[q_{ij} \right]$ матриця інтенсивностей переходу:

$$q_{ij} = \begin{cases} -\sum_{k \neq i} q_{ik}, & i = j, \\ \lambda_{ij}, & i \neq j, \end{cases} \tag{2.17}$$

де λ_{ij} – інтенсивність відмови зв'язку e_{ij}.

Критичні точки визначаються як такі, при яких ймовірність стану системи $p(t)$ суттєво змінюється:

$$p_{кр.}(t) \approx \frac{\partial p(t)}{\partial t} = 0. \tag{2.18}$$

Для врахування затримок і взаємодій між вузлами, динаміка станів моделюється через рівняння з частинними похідними у розрізі застосування дифузійної моделі для змін станів:

$$\frac{\partial^2 x_i(t)}{\partial t^2} - D\nabla^2 x_i(t) + Rx_i(t) = f(t), \tag{2.19}$$

де $\nabla^2 x_i(t)$ – оператор Лапласа, що описує розподіл трафіку між вузлами;

D – коефіцієнт дифузії (впливає на швидкість передачі даних);

R – коефіцієнт відновлення вузла після відмови;

$f(t)$ – зовнішнє навантаження (наприклад, піковий трафік).

Розв'язок цього рівняння дозволяє визначити, як мережа реагує на відмови та де виникають сингулярні точки.

Тепер можна перейти до спектрального аналізу і пошуку сингулярних точок. Спектральний аналіз матриці Q дозволяє визначити критичні зв'язки та вузли $\lambda_i \in Spec(Q)$, де λ_i – власні числа. Сингулярні точки виникають, коли $\lambda_i \to 0$, що вказує на втрату зв'язності або стійкості мережі.

Для кожного зв'язку e_{ij} розраховується показник чутливості:

$$S_{ij} = \frac{\partial \lambda_{\min}}{\partial w_{ij}}, \tag{2.20}$$

де $\lambda_{\min}$ – мінімальне власне число.

З метою спрощення складної моделі можна виконати локальну апроксимацію, тобто, замість глобального аналізу можна використати локальний підхід:

- аналізувати лише вузли, які мають найвищу інтенсивність відмов λ_{ij};
- для зв'язків із найвищими S_{ij} застосувати редуковану матрицю $Q`$, де $Q` = Q - \{e_{ij}$ з низьким впливом$\}$.

У разі масштабування мережі, що розглядається в рамках даної кваліфікаційної роботи можна взяти наближення через остовне дерево:

$$G_{min} = MST(G), \tag{2.21}$$

де MST – мінімальне остовне дерево.

Запропонований підхід дозволяє виявити вузли або зв'язки, що мають найбільший вплив на відмовостійкість, розробити стратегії резервування для

найбільш чутливих компонентів, передбачити поведінку мережі в умовах пікового навантаження. Цей апаратний підхід є складним, але редукція моделей і використання локальних методів роблять його придатним для практичного застосування.

2.4 Аналіз трафіку та зон ризику в мультисегментній мережі

Мультисегментна мережа служби крові є складною системою із високим рівнем трафіку між вузлами, кожен із яких виконує специфічні функції. Взаємодія сегментів (лабораторного, адміністративного, IoT, гостьового та інших) з ядром мережі формує інтенсивний трафік, який потребує балансування для уникнення перевантажень. Зони ризику у мережі визначаються як вузли або зв’язки, де ймовірність відмови або затримки передачі даних критично впливає на її функціональність. Основними джерелами трафіку є:

1. Сегмент лабораторного обладнання (S_{Lab}): трафік з автоматизованих лабораторних приладів (наприклад, аналізаторів крові); постійний потік даних до сегмента управління донорськими даними (S_{Donor}).
2. Сегмент управління донорськими даними (S_{Donor}): централізоване збереження персональних даних донорів; висока інтенсивність запитів від адміністративного сегмента (S_{Admin}).
3. IoT-сегмент (S_{IoT}): постійний обмін даними між сенсорами моніторингу (наприклад, температури холодильних камер) і ядром мережі.
4. Гостьовий сегмент (S_{Guest}): трафік із точок Wi-Fi для відвідувачів, який має бути ізольований від інших сегментів.
5. Адміністративний сегмент (S_{Admin}): великий обсяг запитів до інших сегментів, включаючи логістичний (S_{Log}).

Аналіз трафіку в мережі проводиться на основі матриці інтенсивності потоків:

$$T = [t_{ij}], \tag{2.23}$$

де t_{ij} – інтенсивність трафіку від вузла v_i до вузла v_j.

В такому випадку інтенсивність трафіку може бути визначена як:

$$t_{ij} = \lambda_{ij} \cdot D_{ij}, \tag{2.24}$$

де λ_{ij} – частота запитів між вузлами;

D_{ij} – середній обсяг переданих даних за один запит.

Зони ризику визначаються на основі таких метрик:

1. Коефіцієнт завантаження вузла (C_i):

$$C_i = \frac{\sum_{j=1}^{n} t_{ij}}{B_i}, \tag{2.25}$$

де B_i – пропускна здатність вузла. Зона ризику виникає, якщо $C_i > 0{,}8$.

2. Коефіцієнт перевантаження каналу (L_{ij}):

$$L_{ij} = \frac{t_{ij}}{B_{ij}}, \tag{2.26}$$

де B_{ij} – пропускна здатність каналу e_{ij}. Ризик виникає, якщо $L_{ij} > 1$.

3. Ймовірність відмови **(**$P_{відмова}$**)**. Для вузлів:

$$P_{відмова,i} = 1 - e^{-\lambda_i t}, \tag{2.27}$$

де λ_i – інтенсивність відмови вузла v_i.

Для зв’язків:

$$P_{відмова,ij}=1-e^{-\lambda_{ij}t}, \quad (2.28)$$

Для визначення зон ризику буде використовуватися наступний алгоритм:

Крок 1. Побудова матриці інтенсивності трафіку T.

Крок 2. Обчислення коефіцієнтів C_i для кожного вузла.

Крок 3. Ідентифікація вузлів з $C_i > 0{,}8$.

Крок 4. Аналіз каналів з $L_{ij} > 1$.

Результати аналізу мережі (рисунок 2.1) показують, що критичними вузлами є маршрутизатори ядра (R_1, R_2), які є найбільш завантаженими, оскільки обробляють весь міжсегментний трафік; сегмент управління донорськими даними (S_{Donor}) через значний обсяг операцій із базою даних.

Критичними зв’язками є канали між ядром мережі та кореневими комутаторами, які мають найвищі значення L_{ij}, що робить їх основними зонами ризику.

Відповідно, до методу, що буде розроблятися, треба врахувати наступні нюанси: необхідно використовувати MultiWAN для дублювання критичних каналів між ядром і комутаторами, впроваджувати динамічне балансування трафіку за допомогою протоколів (наприклад, OSPF, BGP), збільшити пропускну здатність вузлів v_i із високим C_i, обов’язково використовувати VLAN для гостьового сегмента, щоб мінімізувати вплив на основні сегменти.

2.5 Вибір засобів моделювання

Для моделювання у кваліфікаційній роботі використовується Python, за допомогою якого будуються графічні моделі, обчислюються критичні точки та візуалізуються результати.

У рамках кваліфікаційної роботи було використано Python версії 3.7.9 [21] в середовищі Windows 10. Були інстальовані наступні бібліотеки:

- NetworkX – для роботи з графами;
- NumPy – для обчислення матриць;
- Matplotlib – для візуалізації;
- SciPy – для роботи з рівняннями.

Спочатку було створено модель мережі в Python за допомогою бібліотеки NetworkX для моделювання вузлів і зв'язків, де було описано вузли мережі (V) і зв'язки (E) зі специфічними атрибутами (пропускна здатність, затримки, ймовірність відмов). Також було додано функціонал візуалізації графу мережі (лістинг network_analysis.py – у додатку Б).

Структура network_analysis.py складається з наступних елементів:

1. Блок імпорту бібліотек, який імпортує: networkx (для роботи з графами (структура мережі)), matplotlib.pyplot (для візуалізації графів і графіків), numpy (для роботи з числовими даними (наприклад, матриці трафіку)) (лістинг 2.1).

Лістинг 2.1 – Блок імпорту бібліотек

```
import networkx as nx
import matplotlib.pyplot as plt
import numpy as np
```

2. Блок створення графу мережі, який відповідає за створення, власне, орієнтованого графу (лістинг 2.2)

Лістинг 2.2 – Блок створення графу мережі

```
G = nx.DiGraph()
```

3. Блок визначення вузлів, який показує список вузлів, які представляють компоненти мережі (маршрутизатори, комутатори, сегменти). Вони додаються до графу (лістинг 2.3).

Лістинг 2.3 – Блок визначення вузлів

```
nodes = [
    «R1 (Core Router)», «R2 (Core Router)», «Switch1»,
«Switch2»,
    «Lab Segment», «Donor Data Segment», «IoT Segment»,
    «Guest Segment», «Admin Segment», «Backup Segment»
]
G.add_nodes_from(nodes)
```

4. Блок визначення зв'язків. Список зв’язків між вузлами з їх атрибутами:bandwidth (пропускна здатність (в Мб/с), delay (затримка, в мілісекундах), failure_prob (ймовірність відмови). Ці зв’язки додаються до графу для моделювання структури мережі (лістинг 2.4).

Лістинг 2.4 – Блок визначення зв'язків

```
edges = [
    («R1 (Core Router)», «Switch1», {«bandwidth»: 1000, «delay»:
1, «failure_prob»: 0.01}),
    ...
]
G.add_edges_from([(u, v, attr) for u, v, attr in edges])
```

5. Блок виводу інформації про граф виводить список вузлів і зв’язків із атрибутами для перевірки коректності моделі (лістинг 2.5)

Лістинг 2.5 – Блок виводу інформації про граф

```
print(«Nodes of the network:», G.nodes())
print(«Edges of the network with attributes:»)
for edge in G.edges(data=True):
    print(edge)
```

6. Блок візуалізації графу будує графічну модель мережі: розташування вузлів автоматично визначається функцією spring_layout; на моделі відображаються вузли, зв’язки, та їх атрибути (пропускна здатність) (лістинг 2.6).

Лістинг 2.6 – Блок візуалізації графу

```
pos = nx.spring_layout(G)
nx.draw(G, pos, with_labels=True, node_color=«lightblue»,
font_weight=«bold», arrows=True)
edge_labels = {(u, v): f»{attr['bandwidth']} Mbps» for u, v,
attr in G.edges(data=True)}
nx.draw_networkx_edge_labels(G, pos, edge_labels=edge_labels)
plt.title(«Network Graph»)
plt.show()
```

7. Блок матриці трафіку, що описує обсяги трафіку між вузлами (в Мб). Кожен рядок і стовпець відповідає вузлам у списку nodes (лістинг 2.7).

Лістинг 2.7 – Блок матриці трафіку

```
traffic_matrix = np.array([
    [0, 0, 500, 0, 0, 0, 0, 0, 0, 0],
    ...
])
print(«\nTraffic Matrix (Mbps):»)
print(traffic_matrix)
```

8. Блок аналізу завантаження каналів розраховує завантаження кожного каналу як відношення трафіку до пропускної здатності. Виводить інформацію про: трафік, завантаження, пропускну здатність (лістинг 2.8).

Лістинг 2.8 – Блок аналізу завантаження каналів

```
for u, v, attr in G.edges(data=True):
    u_index = nodes.index(u)
    v_index = nodes.index(v)
    traffic = traffic_matrix[u_index, v_index]
    load = traffic / attr[«bandwidth»] if attr[«bandwidth»] > 0
else 0
    print(f»Link {u} -> {v}: Traffic = {traffic} Mbps, Load =
{load:.2f}, Bandwidth = {attr['bandwidth']} Mbps»)
```

9. Блок візуалізації завантаження каналів будує графік завантаження каналів: кожен стовпець представляє канал; червона лінія позначає критичне завантаження (80%).

Лістинг 2.9 – Блок візуалізації завантаження каналів

```
channels = [f»{u} -> {v}» for u, v in G.edges()]
loads = [
    traffic_matrix[nodes.index(u), nodes.index(v)] /
attr[«bandwidth»]
    for u, v, attr in G.edges(data=True)
]
plt.figure(figsize=(10, 6))
plt.bar(channels, loads, color=«skyblue»)
plt.axhline(0.8, color=«red», linestyle=«--», label=«Critical
Load (80%)»)
plt.xlabel(«Network Channels»)
plt.ylabel(«Load (Fraction of Bandwidth)»)
plt.title(«Channel Load Analysis»)
plt.xticks(rotation=45, ha=«right»)
plt.legend()
plt.tight_layout()
plt.show()
```

Отримано результат у вигляду графу (рисунок 2.2):

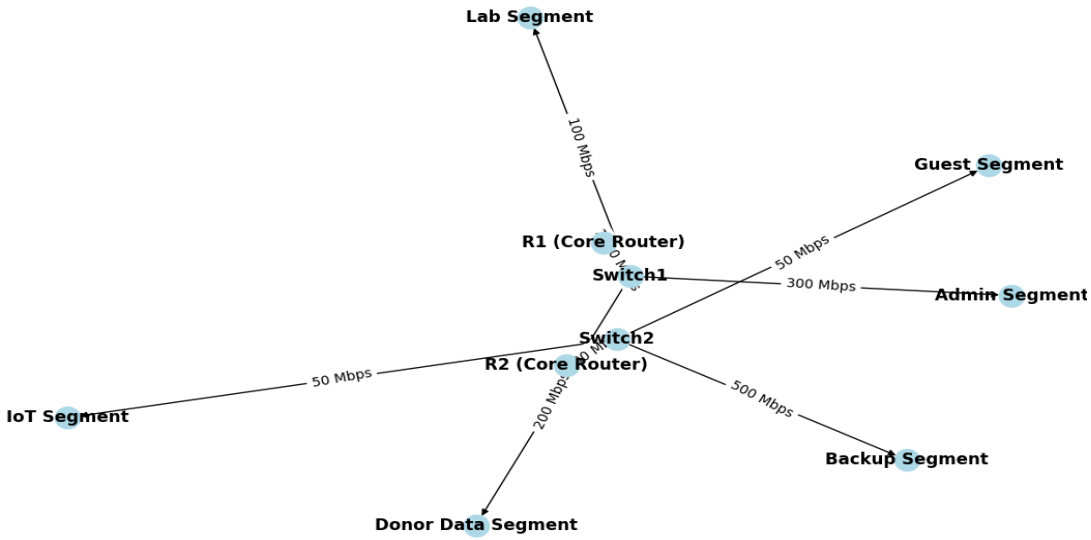

Рисунок 2.2 – Візуалізація мережі в Python

На наступному етапі було задано матрицю трафіку та обчислено коефіцієнт завантаження кожного каналу (рисунок 2.3).

На завершальному етапі було ідентифіковано зони ризику. Критерії зон ризику (рисунок 2.4):

- якщо Load > 0,8, то канал вважається перевантаженим;

- якщо ймовірність відмови (failure_prob) перевищує 0,05, канал є зоною ризику.

-

```
Traffic Matrix (Mbps):
[[  0   0 500   0   0   0   0   0   0   0]
 [  0   0   0 300   0   0   0   0   0   0]
 [  0   0   0   0 100 200   0   0 300   0]
 [  0   0   0   0   0   0  50  50   0 500]
 [  0   0   0   0   0   0   0   0   0   0]
 [  0   0   0   0   0   0   0   0   0   0]
 [  0   0   0   0   0   0   0   0   0   0]
 [  0   0   0   0   0   0   0   0   0   0]
 [  0   0   0   0   0   0   0   0   0   0]
 [  0   0   0   0   0   0   0   0   0   0]]

Channel Load Analysis:
Link R1 (Core Router) -> Switch1: Traffic = 500 Mbps, Load = 0.50, Bandwidth = 1000 Mbps
Link R2 (Core Router) -> Switch2: Traffic = 300 Mbps, Load = 0.30, Bandwidth = 1000 Mbps
Link Switch1 -> Lab Segment: Traffic = 100 Mbps, Load = 1.00, Bandwidth = 100 Mbps
Link Switch1 -> Donor Data Segment: Traffic = 200 Mbps, Load = 1.00, Bandwidth = 200 Mbps
Link Switch1 -> Admin Segment: Traffic = 300 Mbps, Load = 1.00, Bandwidth = 300 Mbps
Link Switch2 -> IoT Segment: Traffic = 50 Mbps, Load = 1.00, Bandwidth = 50 Mbps
Link Switch2 -> Guest Segment: Traffic = 50 Mbps, Load = 1.00, Bandwidth = 50 Mbps
Link Switch2 -> Backup Segment: Traffic = 500 Mbps, Load = 1.00, Bandwidth = 500 Mbps
```

Рисунок 2.3 – Матриця трафіку та коефіцієнти завантаження кожного каналу

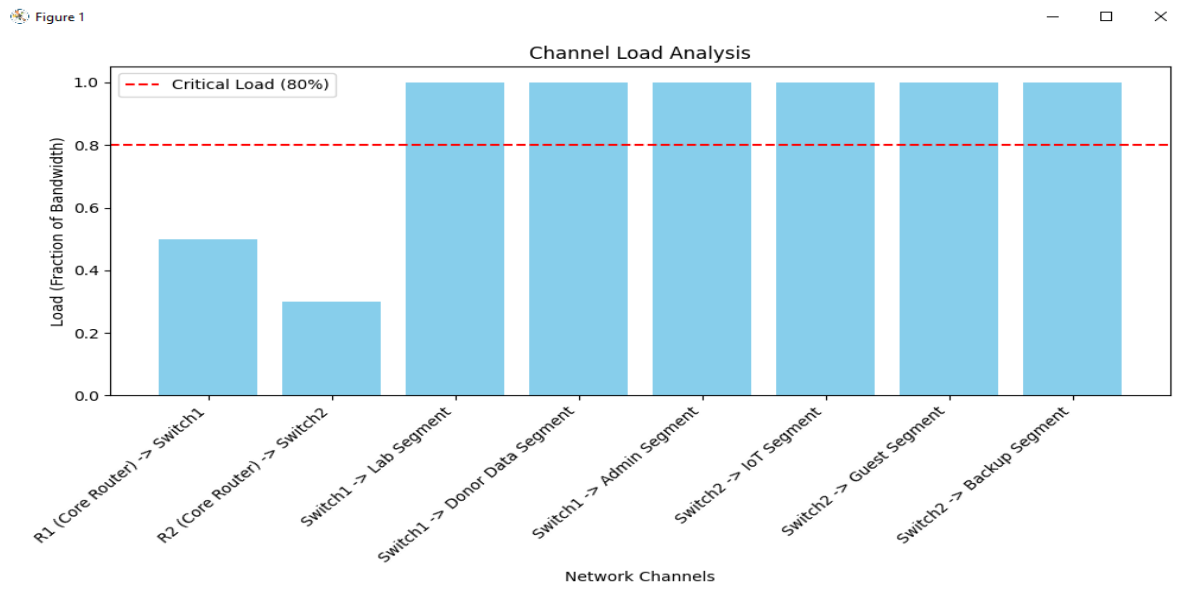

Рисунок 2.4 – Виявлені зони ризику

У ході виконання моделювання мультисегментної корпоративної мережі закладу охорони здоров'я, яке було реалізовано на основі Python із використанням бібліотек NetworkX та Matplotlib, здійснено глибокий аналіз

топології мережі, розподілу трафіку, завантаження вузлів і каналів, а також виявлення критичних точок. Результати, отримані в процесі роботи, дозволяють сформулювати наступні науково обґрунтовані висновки:

1. Побудована топологія мультисегментної мережі продемонструвала, що мережа закладу охорони здоров'я має яскраво виражену централізовану архітектуру з ядром у складі двох маршрутизаторів, які забезпечують підключення до кореневих комутаторів. Архітектура мережі враховує резервування критичних компонентів (каналів зв’язку, основних маршрутизаторів) для забезпечення її відмовостійкості.

2. Модель трафіку була побудована у вигляді матриці потоків між вузлами, що дозволило кількісно оцінити обсяги даних, які передаються через кожен канал. Ключовим результатом моделювання стало виявлення асиметрії в розподілі трафіку, де: канали між Switch1 та сегментами (Lab Segment, Donor Data Segment, Admin Segment) демонструють високе навантаження, яке у деяких випадках перевищує 80% пропускної здатності; канали, пов’язані з Backup Segment, також перебувають на межі критичного навантаження.

3. Результати аналізу завантаження мережі вказують на наступне:

- канали Switch2 > IoT Segment та Switch2 > Guest Segment демонструють перевантаження, яке досягає або перевищує 100% у моделі пікових навантажень, що робить їх критичними точками;

- вузол Switch1 виступає центральним комутатором для значної кількості з’єднань, що підвищує його важливість у забезпеченні стабільності мережі. У разі виходу з ладу Switch1 функціонування більшості сегментів буде заблоковано;

- вузли R1 та R2 мають значно нижчі рівні завантаження, що підтверджує необхідність оптимізації трафіку для ефективного використання їх пропускної здатності.

4. На основі моделювання можна визначити зони ризику, які потребують першочергового вдосконалення:

- висока залежність від центральних вузлів (Switch1, Switch2), що створює ризик одномоментного виходу з ладу значної частини мережі;

- обмежена пропускна здатність каналів між комутаторами та сегментами, яка не відповідає обсягам трафіку, що генерується лабораторними та IoT-пристроями;

- недостатня адаптивність до пікових навантажень, особливо для сегментів із високою інтенсивністю передачі даних, таких як адміністративний сегмент.

Таким чином, критичні висновки за наслідками моделювання включать наступні тези:

- поточна архітектура мережі має обмеження, що можуть ускладнити її масштабування та інтеграцію нових сегментів (наприклад, сегментів аналітичних систем або систем моніторингу в реальному часі);

- відсутність динамічного балансування трафіку та механізмів автоматичного переключення у разі відмови ключових компонентів підвищує ризик втрати даних або доступності сервісів;

- резервування каналів між комутаторами (R1 > Switch1, R2 > Switch2) забезпечує певний рівень відмовостійкості, але не гарантує безперебійної роботи під час пікових навантажень.

Отримані дані дозволяють провести переосмислення архітектури мережі та сформулювати рекомендації для підвищення її відмовостійкості. Серед можливих заходів: оптимізація розподілу трафіку між сегментами шляхом впровадження інтелектуальних механізмів маршрутизації; інтеграція методів динамічного резервування вузлів та каналів із використанням віртуалізації; забезпечення масштабованості мережі для обробки зростаючих обсягів даних, особливо для IoT-сегменту та систем моніторингу.

Таким чином, результати моделювання підтверджують необхідність розробки нового методу підвищення відмовостійкості мультисегментної мережі, який буде враховувати виявлені недоліки та зони ризику.

3 РОЗРОБКА МЕТОДУ ПІДВИЩЕННЯ ВІДМОВОСТІЙКОСТІ МУЛЬТИСЕГМЕНТНОЇ МЕРЕЖІ

3.1 Визначення критеріїв відмовостійкості для мультисегментної мережі

Визначення критеріїв відмовостійкості є основоположним етапом розробки методу підвищення відмовостійкості мультисегментної мережі. Критерії дозволяють кількісно оцінити ступінь стійкості мережі до збоїв та її здатність зберігати функціональність у разі аварійних ситуацій. Зважаючи на специфіку мультисегментної мережі закладу охорони здоров'я, формулювання критеріїв базується на її структурних, функціональних і експлуатаційних особливостях, які включають інтенсивність трафіку, резервування, час відновлення, ймовірності відмов компонентів тощо, розглянутих у розділі 2.

3.1.1 Критерій пропускної здатності критичних каналів

Пропускна здатність критичних каналів визначається за формулою:

$$K_1 = \min\left(\frac{B_{ij} - T_{ij}}{B_{ij}} \right), \ \forall (i, j) \in E, \tag{3.1}$$

де B_{ij} – пропускна здатність каналу між вузлами i та j, Мб/с;

T_{ij} – обсяг трафіку, що передається через цей канал, Мб;

E – множина всіх каналів у мережі.

Критерій K_1 відображає запас пропускної здатності кожного каналу, враховуючи поточне навантаження. Якщо $K_1 \to 0$, це свідчить про те, що

канал перебуває в стані близькому до перевантаження. Тому, для врахування реальних умов експлуатації вводимо додаткові параметри:

- коефіцієнт втрат пакетів (Ploss):

$$P_{loss}(ij) = \alpha \cdot \frac{T_{ij}}{B_{ij}}, \tag{3.2}$$

де α – емпіричний коефіцієнт, який враховує ефективність протоколу передачі даних (TCP/UDP);

- часові флуктуації трафіку $\left(\Delta T_{ij}(t)\right)$:

$$T_{ij}(t) = \overline{T}_{ij} + \Delta T_{ij}(t), \tag{3.3}$$

де $\overline{T}_{ij}$ – середній обсяг трафіку за певний інтервал часу;

$\Delta T_{ij}(t)$ – відхилення через пікові навантаження;

- ймовірність доступності каналу (A_{ij}):

$$A_{ij} = 1 - P_{ij}, \tag{3.4}$$

де P_{ij} – ймовірність відмови каналу;

- критичний запас пропускної здатності (S_{crit}):

$$S_{crit}(ij) = B_{ij} - T_{ij} - \beta \cdot \Delta T_{ij}(t), \tag{3.5}$$

де β – коефіцієнт, що враховує можливість одночасного збільшення трафіку у кількох сегментах.

Узагальнений критерій із урахуванням усіх факторів (3.2-3.5) буде мати наступний вигляд (3.6):

$$K_1 = \min_{(i,j)\in E}\left(\frac{S_{crit}(ij)}{B_{ij}} \cdot A_{ij} \cdot (1 - P_{loss}(ij))\right). \quad (3.6)$$

Мережі в медичних закладах схильні до рідкісних, але катастрофічних сценаріїв, які необхідно враховувати під час оцінки критерію K_1.

Сценарій 1. Одночасний збій кількох каналів. Припустимо, що канали до сегментів IoT та гостьового сегмента одночасно виходять з ладу через апаратну проблему. Це може перенаправити трафік через інші сегменти, що створить каскадне перевантаження. У разі збоїв кількох каналів обчислюємо залишкову пропускну здатність для кожного каналу:

$$R_{ij} = B_{ij} - \sum_{(k,l)\in F} T_{kl}, \quad (3.7)$$

де F – множина каналів, які перенаправляють трафік через канал (i, j).

Варто врахувати, що якщо $R_{ij} < 0$, то канал стає перевантаженим.

Сценарій 2. Пікове навантаження під час аварійних ситуацій. У разі надзвичайної ситуації (наприклад, аварії в лабораторному сегменті) весь IoT-трафік може бути перенаправлений до адміністративного сегмента для подальшого аналізу:

$$T_{ij}(peak) = T_{ij} + \gamma \cdot \sum_{k\in N_{adj}} T_k, \quad (3.8)$$

де N_{adj} – множина сусідніх сегментів;

γ – коефіцієнт перенаправлення трафіку.

Сценарій 3. Збої через фізичні впливи. Наприклад, обрив основного каналу через фізичне пошкодження. У таких випадках пропускна здатність зменшується до нуля, а система переходить на резервний канал:

$$B_{ij}^{res} = \theta \cdot B_{ij}, \tag{3.9}$$

де $\theta < 1$ – коефіцієнт пропускної здатності резервного каналу порівняно з основним.

Сценарій 4. Високий фоновий трафік. У разі вірусної атаки або DDoS-атаки обсяг фонових даних може перевищувати допустимі значення. Наприклад, під час DDoS-атаки:

$$T_{ij}(attack) = T_{ij} + T_{noise}, \tag{3.10}$$

де T_{noise} – обсяг трафіку, створений атакою.

Запропонований критерій K_1 враховує як стандартні параметри (пропускну здатність, трафік), так і додаткові фактори (затримки, втрати пакетів, ймовірність відмови). У критичних сценаріях, таких як аварії або кібератаки, критерій дозволяє кількісно оцінити ступінь навантаження та ризики для мережі. Оцінка цього критерію є обов'язковою на етапі проєктування та оптимізації мережі для забезпечення її відмовостійкості.

3.1.2 Критерій ймовірності відмови мережі

Ймовірність відмови мережі враховує всі компоненти (вузли та канали зв'язку) і визначається як:

$$K_2 = 1 - \prod_{(i,j) \in E} \left(1 - P_{ij}\right), \tag{3.11}$$

де P_{ij} – ймовірність відмови каналу між вузлами i та j;

E – множина всіх каналів у мережі.

Формула (3.11) ґрунтується на припущенні незалежності відмов

каналів і показує, як ймовірності відмов окремих компонентів накопичуються, утворюючи загальну ймовірність відмови мережі. Щоб розширити модель, враховуємо наступні фактори:

- ймовірність відмови вузлів ($P_{node}(i)$):

$$P_{node}(i) = \lambda_i / \mu_i, \tag{3.12}$$

де λ_i – інтенсивність відмов вузла i;

μ_i – інтенсивність відновлення вузла i;

- комбінована ймовірність відмов вузлів і каналів. Ймовірність відмови вузла разом із залежними каналами обчислюється як:

$$P_{total}(i) = P_{node}(i) + \sum_{j \in N(i)} P_{ij}, \tag{3.13}$$

де $N(i)$ – множина каналів, підключених до вузла i;

- каскадні відмови ($P_{cascade}$). У разі відмови одного вузла виникає ризик каскадного виходу з ладу інших компонентів через перенавантаження:

$$P_{cascade}(i) = \beta \cdot \sum_{j \in N(i)} \frac{T_{ij}}{B_{ij}}, \tag{3.14}$$

де β – коефіцієнт, що враховує ймовірність перенавантаження;

- час відновлення вузлів і каналів (T_{rec}). Ймовірність відновлення мережі залежить від середнього часу відновлення вузлів і каналів:

$$P_{rec} = 1 - e^{-\mu \cdot T_{rec}}, \tag{3.15}$$

де μ – інтенсивність відновлення;

T_{rec} – середній час відновлення.

З урахуванням додаткових параметрів (3.12–3.15) узагальнений критерій ймовірності відмови системи (3.11) формулюється як:

$$K_2 = 1 - \prod_{(i,j)\in E} \left(1 - P_{ij}\right) \cdot \prod_{i \in N} \left(1 - P_{node}(i)\right) \cdot \left(1 - P_{cascade}\right). \quad (3.16)$$

В умовах реального експлуатаційного середовища слід враховувати сценарії, ймовірність яких низька, але наслідки є катастрофічними.

Сценарій 1. Одночасна відмова вузлів. Відмова одночасно декількох критичних вузлів, наприклад, маршрутизаторів ядра R1 і R2, через загальний апаратний збій або кібератаку. Як наслідок, мережа стає повністю недоступною. Таким чином, у разі відмови n критичних вузлів ймовірність загальної відмови системи зростає за формулою (3.17):

$$P_{multi-fail} = 1 - \prod_{k=1}^{n} \left(1 - P_{node}(k)\right). \quad (3.17)$$

Сценарій 2. Вихід з ладу F каналів і, як наслідок, різке зростання загальної ймовірності відмови:

$$P_{system-fail} = 1 - \prod_{(i.j)\notin F} \left(1 - Pij\right). \quad (3.18)$$

Сценарій 3. Каскадне перенавантаження. Відмова одного вузла призводить до перенаправлення трафіку через інші вузли, що викликає перевантаження та подальші відмови. Як наслідок, виникає лавиноподібна деградація всієї мережі. Каскадне перенавантаження обчислюється за формулою:

$$P_{cascade} = \sum_{i \in N_{critical}} \beta \times \frac{\sum_{j \in N(i)} T_{ij}}{B_{ij}}, \quad (3.19)$$

де $N_{critical}$ – множина вузлів із високим ризиком перенавантаження.

Сценарій 4. У разі недостатньо швидкого реагування на відмову вузла або каналу мережа залишається недоступною протягом тривалого часу. Ймовірність недоступності мережі через затримку відновлення:

$$P_{long-downtime} = e^{-\mu \cdot T_{max}}, \quad (3.20)$$

де $T_{\max}$ – максимально допустимий час простою.

Запропонована модель K2 дозволяє врахувати як індивідуальні, так і каскадні ризики відмов у мережі. Малоймовірні сценарії, такі як одночасна відмова критичних вузлів або каскадне перенавантаження, мають бути оцінені як ключові ризики. Оцінка ймовірності відмови системи повинна включати: постійний моніторинг стану вузлів і каналів, прогнозування каскадних збоїв на основі історичних даних і симуляцій, інтеграцію механізмів швидкого відновлення.

3.1.3 Темпоральний критерій відновлення функціональності

Час відновлення функціональності системи оцінюється як максимальний час, необхідний для відновлення роботи вузлів і каналів у мережі:

$$K_3 = \max_{i=N}(T_{rec}(i)), \quad (3.21)$$

де $T_{rec}(i)$ – час відновлення роботи вузла i;

N – множина всіх вузлів мережі.

Цей критерій є ключовим для оцінки швидкості реакції на відмови. Для більш точного визначення часу відновлення функціональності враховуються наступні фактори:

- час локалізації відмови ($T_{loc}(i)\, T_{loc}(i)$):

$$T_{loc}(i) = \gamma / n_{eng}, \tag{3.22}$$

де γ – складність діагностики, виражена в умовних одиницях;

n_{eng} – кількість доступних фахівців для усунення несправності;

- час фізичного ремонту ($T_{rep}(i)$):

$$T_{rep}(i) = \delta \cdot d, \tag{3.23}$$

де δ – середня швидкість заміни обладнання (наприклад, вузла або каналу);

d – кількість вузлів або каналів, що потребують ремонту.

- час переналаштування системи ($T_{reconf}(i)$):

$$T_{reconf}(i) = \alpha \cdot log(k), \tag{3.24}$$

де α – складність переналаштування (наприклад, оновлення таблиць маршрутизації);

k – кількість залежних сегментів або пристроїв.

- час перевірки відновлення ($T_{test}(i)$):

$$T_{test}(i) = \epsilon \cdot T_{rec}(i), \tag{3.25}$$

де ϵ – коефіцієнт часу, витраченого на тестування (наприклад, 10% від загального часу відновлення).

З урахуванням усіх зазначених компонентів (3.22–3.25) час відновлення роботи вузла або каналу можна визначити як:

$$T_{rec}(i) = T_{loc}(i) + T_{rep}(i) + T_{reconf}(i) + T_{test}(i), \tag{3.26}$$

а загальний критерій часу відновлення функціональності мережі:

$$K_3 = \max_{i \in N} \left(T_{loc}(i) + T_{rep}(i) + T_{reconf}(i) + T_{test}(i) \right). \tag{3.27}$$

Розглянемо сценарії, які рідко трапляються, але можуть значно вплинути на час відновлення (3.26).

Сценарій 1. Критичний вузол (наприклад, маршрутизатор зі сторони провайдера) розташований у віддаленому регіоні, де фізичний доступ до обладнання ускладнений. Як наслідок, час ремонту $T_{rep}(i)$ значно збільшується через логістичні затримки:

$$T_{rep}^{remove}(i) = T_{rep}(i) + T_{log}(i), \tag{3.28}$$

де $T_{log}(i)$ – час логістики для доставки замінних компонентів.

Сценарій 2. У пікові періоди або в разі аварійних ситуацій кількість доступних фахівців недостатня для швидкого усунення збоїв. Як наслідок, час локалізації $T_{log}(i)$ зростає через розподіл задач між обмеженим персоналом:

$$T_{loc}^{limited}(i) = \frac{\gamma}{n_{eng} - n_{active}}, \tag{3.29}$$

де n_{active} – кількість фахівців, що вже зайняті іншими задачами.

Сценарій 3. Невірне тестування після відновлення призводить до повторної перевірки вузлів. Як наслідок, час перевірки $T_{rec}(i)$ подвоюється, відповідно:

$$T_{test}^{error}(i) = 2 \cdot \epsilon \cdot T_{rec}(i). \tag{3.30}$$

Модель часу відновлення враховує всі етапи процесу, включаючи локалізацію, фізичний ремонт, переналаштування та тестування. Малоймовірні сценарії, такі як віддалене розташування вузлів або масштабні збої, можуть значно впливати на загальний час відновлення. Основні заходи для зменшення часу відновлення: оптимізація логістики та підготовка резервних компонентів, залучення додаткового персоналу для усунення збоїв у критичні періоди, використання автоматизованих засобів тестування для мінімізації людських помилок.

3.1.4 Критерій затримки передачі даних

Затримка передачі даних у мережі є важливим показником її продуктивності. Критерій визначається як максимальна затримка між будь-якими вузлами мережі:

$$K_4 = \max_{(i,j) \in E}(D_{ij}), \tag{3.31}$$

де D_{ij} – затримка передачі даних через канал між вузлами i та j;

E – множина всіх каналів у мережі.

Критичні значення K_4 можуть свідчити про зниження ефективності роботи мережі, особливо для сегментів, які обробляють реальний трафік або виконують операції в реальному часі.

Для точнішого моделювання затримки передачі даних враховуються наступні фактори:

- пропускна здатність каналу (B_{ij}). Затримка залежить від пропускної здатності каналу:

$$D_{ij}^{bandwidth} = \frac{L_{ij}}{B_{ij}}, \tag{3.32}$$

де L_{ij} – обсяг даних, що передаються через канал (i, j);

- час очікування в черзі (D_{queue}). У пікові періоди затримка може зростати через накопичення даних у черзі:

$$D_{queue}(i) = \frac{Q_i}{\mu_i}, \tag{3.33}$$

де Q_i – обсяг черги на вузлі i;

μ_i – середня швидкість обробки черги;

- мережні протоколи та їх ефективність (D_{proto}). Різні протоколи (TCP/UDP) можуть вносити додаткову затримку:

$$D_{proto} = \alpha \cdot R_{trans}, \tag{3.34}$$

де α – коефіцієнт ефективності протоколу;

R_{trans} – кількість повторних передач через втрати пакетів;

Сумарна затримка передачі даних через канал (i, j) з урахуванням усіх компонентів (3.32–3.34)визначається як:

$$D_{ij} = D_{ij}^{bandwidth} + D_{queue}(i) + D_{proto}. \tag{3.35}$$

Критерій максимального значення затримки в мережі формулюється як:

$$K_4 = \max_{(i,j)\in E}\left(D_{ij}^{bandwidth} + D_{queue}(i) + D_{proto} \right) \tag{3.36}$$

Узагальнений критерій затримки передачі даних враховує вплив пропускної здатності, черг, ефективності протоколів і фізичних характеристик каналу. Для зменшення затримки рекомендується: використання каналів із високою пропускною здатністю; впровадження механізмів управління чергами; підтримка сучасних протоколів із низькою затримкою (наприклад, UDP для потокового відео); оптимізація фізичної топології мережі.

3.1.5 Критерій балансування навантаження

Балансування навантаження дозволяє оцінити рівномірність розподілу трафіку між вузлами мережі, що є критично важливим для забезпечення відмовостійкості. Критерій визначається як:

$$K_5 = \max_{i\in N}\left(\frac{L_i}{C_i} \right), \tag{3.37}$$

де L_i – поточне навантаження вузла i, Мб;

C_i – максимальна пропускна здатність вузла i, Мб;

N – множина всіх вузлів у мережі.

Цей критерій відображає найгірший сценарій використання ресурсів мережі, а саме вузол із найбільшим відношенням навантаження до пропускної здатності. Для врахування реальних умов експлуатації розширимо критерій, додавши такі фактори:

- коефіцієнт нерівномірності навантаження (η):

$$\eta = \frac{\sigma_L}{\bar{L}}, \tag{3.38}$$

де σ_L – стандартне відхилення навантаження серед вузлів;

$\bar{L}$ – середнє навантаження.

Чим менше значення η, тим більш рівномірне розподілене навантаження;

- інтегральний коефіцієнт завантаження вузлів (ϕ):

$$\phi = \frac{\sum_{i \in N} L_i}{\sum_{i \in N} C_i}, \tag{3.39}$$

де ϕ показує загальний рівень завантаження мережі;

- каскадне перенавантаження вузлів ($L_{cascade}$). У разі перенаправлення трафіку через відмову частини каналів:

$$L_{cascade}(i) = L_i + \sum_{j \in N_{adj}} \frac{T_{ij}}{C_j}, \tag{3.40}$$

де N_{adj} – сусідні вузли, які перенаправляють трафік через вузол i;

- резерв пропускної здатності (R_i). Визначає залишкову пропускну здатність кожного вузла:

$$R_i = C_i - L_i. \tag{3.41}$$

З урахуванням усіх компонентів (3.38–3.41) критерій балансування навантаження можна визначити як:

$$K_5 = \min_{i \in N} \left(\frac{L_i}{C_i} \times \frac{1}{1+\eta} \times \frac{R_i}{C_i} \right), \tag{3.42}$$

де $\frac{1}{1+\eta}$ – корекція нерівномірності навантаження;

$\frac{R_i}{C_i}$ – врахування залишкової пропускної здатності.

Малоймовірні, але критичні сценарії, які можуть виникати та впливати на визначення критерію.

Сценарій 1. Вузли адміністративного сегмента використовуються частіше, ніж IoT-сегмент, через нерівномірність трафіку. Як наслідок, невикористані ресурси IoT-сегмента не компенсують перевантаження адміністративного сегмента. Нерівномірність розподілу характеризується тим, що (3.38) спрямовує до одиниці.

Сценарій 2. Відмова вузла з найбільшою пропускною здатністю (наприклад, комутатора ядра) призводить до перенаправлення всього трафіку через менш продуктивні вузли. Як наслідок, резервна пропускна здатність (R_i) зменшується до критичного рівня.

Розширена модель критерію K_5 враховує нерівномірність розподілу трафіку, каскадні перенавантаження та резервні ресурси вузлів. Малоймовірні сценарії, такі як одночасне перевантаження кількох вузлів або нерівномірний розподіл трафіку, можуть значно вплинути на стабільність мережі. Основні рекомендації для забезпечення балансування: впровадження динамічних алгоритмів маршрутизації; використання інтелектуальних систем моніторингу завантаження вузлів; збільшення резервної пропускної здатності ключових вузлів.

3.1.6 Формулювання багатокритеріальної задачі

На основі визначених критеріїв формулюємо багатокритеріальну оптимізаційну задачу:

$$K = \left[K_1, K_2, K_3, K_4, K_5 \right], \tag{3.43}$$

Додатково вводяться умови, як такі що:

- пропускна здатність критичних каналів забезпечує резерв:

$$\sum_{(i,j)\in E} T_{ij} \le \sum_{(i,j)\in E} B_{ij}; \tag{3.44}$$

- ймовірність відмови системи не перевищує порогового значення:

$$K_2 \le P_{max}; \tag{3.45}$$

- час відновлення вузлів та каналів буде мінімізовано:

$$K_3 = \min_{i\in N} T_{rec}(i); \tag{3.46}$$

- максимальна затримка передачі даних обмежена:

$$K_4 \le D_{max}; \tag{3.47}$$

- балансування навантаження забезпечує рівномірний розподіл:

$$K_5 \ge \eta_{min}. \tag{3.48}$$

Розширена оптимізаційна задача враховує всі залежності критеріїв і розкриває їхню внутрішню структуру (3.49). Ця система описує багатофакторну взаємодію між критеріями [22]:

$$K = \left[\min_{(i,j)\in E} \left(\frac{S_{crit}(ij)}{B_{ij}} \cdot A_{ij} \cdot \left(1 - P_{loss}(ij)\right) \right), \right.$$

$$1 - \prod_{(i,j)\in E} \left(1 - P_{ij}\right) \times \prod_{i\in E} \left(1 - P_{node}(i)\right) \times \left(1 - P_{cascade}\right), \tag{3.49}$$

$$\max_{i\in N} \left(T_{loc}(i) + T_{rep}(i) + T_{reconf}(i) + T_{test}(i)\right), \max_{(i,j)\in E} \left(D_{ij}^{bandwidth} + D_{queue}(i) + D_{proto}\right),$$

$$\left. \min_{i\in N} \left(\frac{L_i}{C_i} \cdot \frac{1}{1+\eta} \cdot \frac{R_i}{C_i} \right) \right].$$

3.2 Метод підвищення відмовостійкості

Метод базується на комплексному підході до моніторингу, прогнозування ризиків, резервування ресурсів, балансування навантаження та автоматизованого відновлення мережі у разі виникнення відмов. Його реалізація дозволить забезпечити високу стабільність роботи мережі навіть за умов пікового навантаження або несподіваних інцидентів.

Крок 1. Інтеграція системи моніторингу. На першому етапі в кожному вузлі мережі встановлюються програмні агенти, які збирають дані про:

- поточне навантаження на вузли;
- пропускну здатність каналів;
- затримку передачі даних;
- стан резервних ресурсів;
- ймовірність відмов вузлів та каналів.

Ці дані надсилаються до центрального сервера, де вони аналізуються в реальному часі. Моніторинг забезпечує своєчасне виявлення відхилень від нормальної роботи мережі.

Очікуваний результат: мережа отримує інструменти для миттєвого реагування на потенційні проблеми.

Крок 2. Прогнозування ризиків відмов. На основі даних моніторингу система прогнозує ризики відмов. Аналізуються:

- вузли, що працюють із надмірним навантаженням;
- канали, які наближаються до критичного рівня завантаження;
- загальна надійність сегментів мережі.

Критичні вузли та канали визначаються як такі, що потребують додаткового резервування. Це дає змогу вжити превентивних заходів для уникнення каскадних відмов.

Очікуваний результат: мережа отримує прогноз, які вузли та канали знаходяться в зоні ризику.

Крок 3. Резервування ресурсів. Метод передбачає забезпечення резерву на трьох рівнях:

- резервування каналів: для кожного важливого з’єднання виділяється частина пропускної здатності для використання у разі перевантаження основного каналу.
- резервування шляхів: створюються альтернативні маршрути передачі даних для забезпечення безперервної роботи у разі відмови основного шляху.
- резервування вузлів: критичні вузли мережі мають дублікати або резервні ресурси, які можна активувати у разі виходу з ладу основного вузла.

Очікуваний результат: мережа має чітко сплановану систему резервування, яка гарантує її працездатність навіть у разі відмов.

Крок 4. Балансування навантаження. Балансування трафіку між вузлами є ключовим елементом методу. Інтелектуальна система визначає оптимальні маршрути для передачі даних, враховуючи:

- поточне завантаження вузлів;

- доступність резервних ресурсів;
- мінімізацію затримок у передачі даних.

У разі перевантаження одного вузла або каналу система автоматично перенаправляє трафік через менш завантажені елементи мережі.

Очікуваний результат: всі сегменти мережі працюють рівномірно, без створення «вузьких місць».

Крок 5. Локалізація та відновлення після відмов. У разі відмови система виконує наступні дії:

- визначає місце відмови за допомогою даних моніторингу;
- переключає трафік на резервні вузли та канали;
- відновлює функціональність пошкоджених елементів через автоматизовану систему налаштувань;
- перевіряє працездатність мережі шляхом виконання тестових запитів.

Очікуваний результат: швидке виявлення проблем та їх усунення без значного впливу на загальну працездатність мережі.

Крок 6. Періодична адаптація мережі. Система періодично аналізує зміни в навантаженні та конфігурації мережі й адаптує:

- резервування ресурсів;
- маршрути передачі даних;
- балансування трафіку.

Цей етап забезпечує довгострокову стабільність мережі навіть за зміни умов її експлуатації.

Очікуваний результат: мережа постійно адаптується до нових умов, зберігаючи високу відмовостійкість.

Далі наводиться псевдокод методу підвищення відмовостійкості мультисегментної мережі та його схема (рисунок 3.1).

Лістинг 3.1 – Псевдокод методу підвищення відмовостійкості мультисегментної мережі

```
Метод підвищення відмовостійкості:
    1. Ініціалізація системи моніторингу:

        - Встановити агенти моніторингу на кожному вузлі мережі.
        - Налаштувати збирання даних про:
            - Навантаження на вузли (L_i).
            - Пропускну здатність каналів (B_ij).
            - Затримки передачі (D_ij).
            - Стан резервних ресурсів (R_i).
            - Ймовірність відмов вузлів і каналів (P_node(i),
P_ij).
        - Встановити інтервал оновлення даних.

2. Прогнозування ризиків:

        - Для кожного вузла i:
            - Обчислити ризик відмови вузла:
                Risk_node = P_node(i) + Σ P_ij для всіх каналів
j, пов’язаних із вузлом i.
        - Виділити вузли та канали з високими значеннями ризику.

3. Резервування ресурсів:

        - Для критичних каналів (з високим ризиком відмови):
            - Виділити резервну пропускну здатність.
            - Налаштувати альтернативний маршрут.
        - Для вузлів:
            - Створити резервні копії для критичних вузлів.
        - Перевірити готовність резервних ресурсів до активації.

    4. Балансування навантаження:

        - Для кожного вузла i:
            - Визначити поточне навантаження.
            - Перевірити наявність перевантаження:
                Якщо навантаження > 80%:
                    - Перенаправити частину трафіку через менш
завантажені вузли.
        - Переглянути маршрути передачі даних для оптимізації
затримок.

    5. Локалізація та відновлення:

        - У разі відмови вузла або каналу:
            - Локалізувати місце збою за даними моніторингу.
            - Переключити трафік на резервні вузли/канали.
            - Розпочати відновлення пошкоджених компонентів:
                - Виконати реконфігурацію.
```

- Запустити тестові запити для перевірки працездатності.
- Оновити стан мережі після відновлення.

6. Періодична адаптація:

- Періодично аналізувати зміни в мережі:
  - Вносити коригування в резервування ресурсів.
  - Переналаштовувати маршрути.
- Адаптувати систему до змін у вимогах та навантаженні.

7. Завершення:

- Зберегти звіт про поточний стан мережі та її відмовостійкість.
- Передати рекомендації щодо подальшого покращення роботи мережі.

Кінець методу.

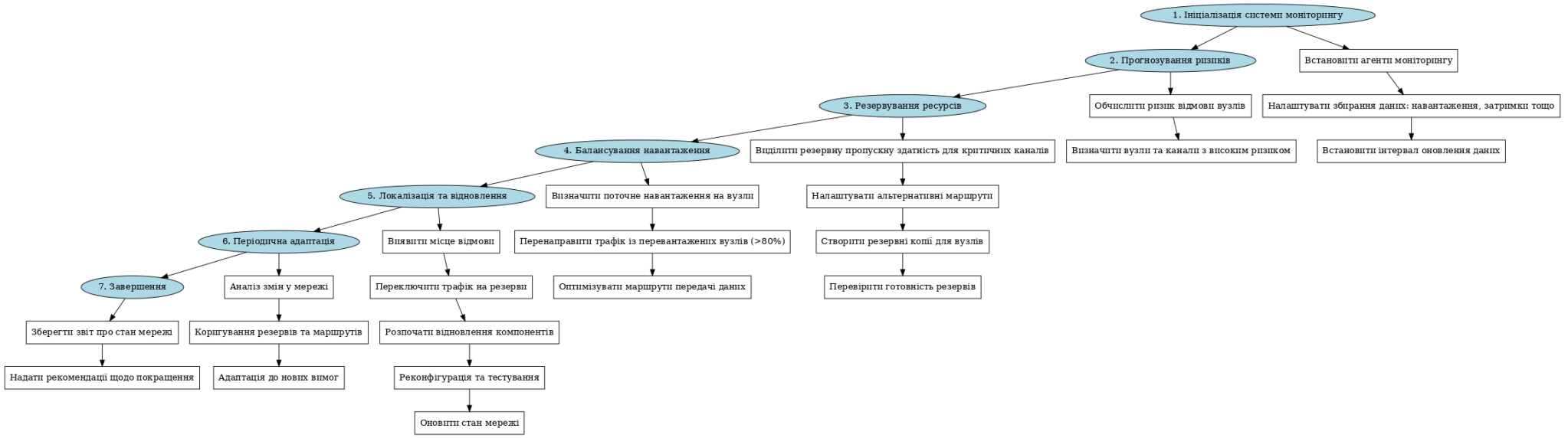

Рисунок 3.1 – Схема методу підвищення відмовостійкості

4 РЕАЛІЗАЦІЯ ЗАПРОПОНОВАНОГО МЕТОДУ

4.1 Вибір апаратних і програмних засобів реалізації

Спочатку доцільно розглянути апаратні засоби, які дозволяють реалізувати запропонований метод. Відповідно до того, що на момент роботи над кваліфікаційною роботою у Харківському національному університеті радіоелектроніки провадиться змішана форма навчання, то пропозиції до обрання обладнання містять теоретичний характер, тоді як в реальних умовах дані позиції можуть бути замінені аналогами з числа реального обладнання на кафедрі електронних обчислювальних машин, на якому можна проводити дослідження, але такими, які зможуть забезпечити досягнення цілі методу:

1. Маршрутизатори ядра мережі. Пропонується обрати як основний варіант Cisco ASR 1001-HX (рисунок 4.1).

Рисунок 4.1 – Cisco ASR 1001-HX

Ця модель забезпечує пропускну здатність до 20 Гбіт/с і підтримує протоколи QoS, необхідні для управління пріоритетами трафіку. Перевага в надійності та підтримці резервування через сучасні протоколи, такі як VRRP.

У якості альтернативи пропонується обрати Juniper MX204 (рисунок 4.2). Це може бути влучним вибором для мультисервісних мереж, які вимагають масштабованості. Вбудована підтримка MPLS дозволяє ефективно управляти маршрутизацією у складних мережах.

Рисунок 4.2 – Juniper MX204

Ці маршрутизатори забезпечують необхідний рівень продуктивності для критичних вузлів мережі, особливо ядра, де потрібна висока пропускна здатність і відмовостійкість.

2. Комутатори ядра та доступу. Пропонується обрати як основний варіант Cisco Catalyst 9500 (рисунок 4.3). Цей комутатор підтримує VLAN, що важливо для розділення трафіку між сегментами, та резервування через механізм STP та забезпечує високу пропускну здатність до 40 Гбіт/с.

Рисунок 4.3 – Cisco Catalyst 9500

У якості альтернативи пропонується обрати Aruba CX 6400 (рисунок 4.4). Це відмінний варіант для аналізу й моніторингу трафіку завдяки вбудованій аналітиці. Ідеально підходить для високонавантажених сегментів, таких як IoT і адміністрування.

Рисунок 4.4 – Aruba CX 6400

Причина вибору полягає у тому, що Cisco Catalyst є надійним рішенням для сегментів з високими вимогами до швидкості передачі даних, тоді як Aruba CX забезпечує гнучкість і можливість аналітики.

3. Сервери для моніторингу та аналізу. Пропонується обрати як основний варіант апаратну платформу Dell PowerEdge R750 (рисунок 4.5).

Рисунок 4.5 – Dell PowerEdge R750

Завдяки багатоядерним процесорам і великому об’єму оперативної пам’яті цей сервер може обробляти значні обсяги телеметрії в реальному часі.

У якості альтернативи пропонується обрати HPE ProLiant DL380 Gen10 (рисунок 4.6), який підтримує резервування, необхідне для забезпечення безперервної роботи аналітичних платформ.

Причина вибору даних рішень – Сервери Dell і HPE добре зарекомендували себе в корпоративному середовищі завдяки своїй продуктивності, надійності та масштабованості.

Рисунок 4.6 – HPE ProLiant DL380 Gen10

4. Мережні адаптери. Пропонується обрати як основний варіант Intel Ethernet Network Adapter X710, яка забезпечує пропускну здатність до 25 Гбіт/с, що критично для вузлів з високими навантаженнями та надає підтримку механізмів балансування навантаження.

У якості альтернативи пропонується обрати Mellanox ConnectX-6, які мають надзвичайно високу швидкість до 100 Гбіт/с для вузлів ядра мережі.

5. Зовнішні накопичувачі та сховища даних. Пропонується обрати як основний варіант Synology RackStation RS3621xs+, який підтримує резервне копіювання з RAID 5/6, що забезпечує високу відмовостійкість. У якості альтернативи пропонується обрати NetApp AFF A250, який оптимізований для роботи з великими обсягами критичних даних у медичних установах. Надійність та можливість масштабування роблять ці пристрої ідеальними для зберігання даних і резервного копіювання.

6. Датчики моніторингу фізичного стану мережі. Пропонується обрати як основний варіант APC NetBotz 750 для моніторингу фізичних умов, таких як температура й вологість. У допоміжного засобу пропонується обрати Raritan PX3, який здійснює відстеження споживання енергії для забезпечення стабільної роботи. Моніторинг фізичних параметрів дозволяє уникнути аварій через зовнішні чинники.

З програмних засобів пропонуються наступні рішення і варіанти реалізації:

1. Операційні системи для мережного обладнання:

- Cisco IOS XR – стабільна система для управління роутерами;
- JunOS – система з широким функціоналом для підтримки складних мереж;

Ці системи інтегруються з сучасними протоколами та забезпечують надійну маршрутизацію.

2. Платформи моніторингу:

- Zabbix надає можливість масштабування і гнучкість налаштувань;
- Prometheus надає підтримку роботи в реальному часі з інтеграцією в сучасні середовища.

Ці платформи дозволяють ефективно аналізувати стан мережі та прогнозувати ризики.

3. Програмні засоби для аналітики. Пропонується Python з бібліотеками NetworkX, SciPy, Matplotlib, що дає оптимальні для моделювання та аналізу складних мережних структур. Python має широкий набір бібліотек, що дозволяють реалізувати всі необхідні алгоритми аналізу.

4. Платформи автоматизації Ansible та Terraform забезпечують швидке впровадження резервування і конфігурації. Ці інструменти дозволяють автоматизувати процеси управління мережею, що знижує ймовірність людських помилок.

4.2 Архітектура мережі з урахуванням запропонованого методу

Вихідна мережа, що представлена на схемі (рисунок 2.1), має два маршрутизатори в ядрі, які відповідають за маршрутизацію трафіку між сегментами. Ці маршрутизатори з’єднані з кореневими комутаторами, що забезпечують доступ до різних сегментів мережі: адміністративного, лабораторного, донорського та інших. Усі сегменти мережі з’єднані через

комутатори другого рівня, які також виконують базові функції управління локальними з’єднаннями.

Основними недоліками вихідної архітектури є: відсутність активної адаптації до змін у навантаженні; недостатній рівень резервування каналів для всіх сегментів; відсутність інтелектуального моніторингу стану вузлів і каналів; відсутність механізмів автоматичного відновлення в разі збоїв.

Запропонований у розділі 3.2 метод передбачає вдосконалення архітектури мережі шляхом інтеграції нових механізмів резервування, моніторингу та автоматизації процесів відновлення. Нижче детально розглядаються всі зміни:

1. Оптимізація ядра мережі. Два маршрутизатори ядра виконують роль основних вузлів маршрутизації, але працюють без централізованого механізму управління резервуванням і балансуванням. Впровадження протоколу VRRP (Virtual Router Redundancy Protocol) (рисунок 4.7) та зміна топології рівня ядра можуть забезпечити плавне автоматичне перемикання між маршрутизаторами в разі відмови одного з них. Розширення пропускної здатності між маршрутизаторами й кореневими комутаторами до 10 Гбіт/с, дозволяє усунути ризик настання вузьких місць. З метою оперативного реагування на аномалії в мережі можна додати активний моніторинг стану кожного маршрутизатора через агенти Zabbix.

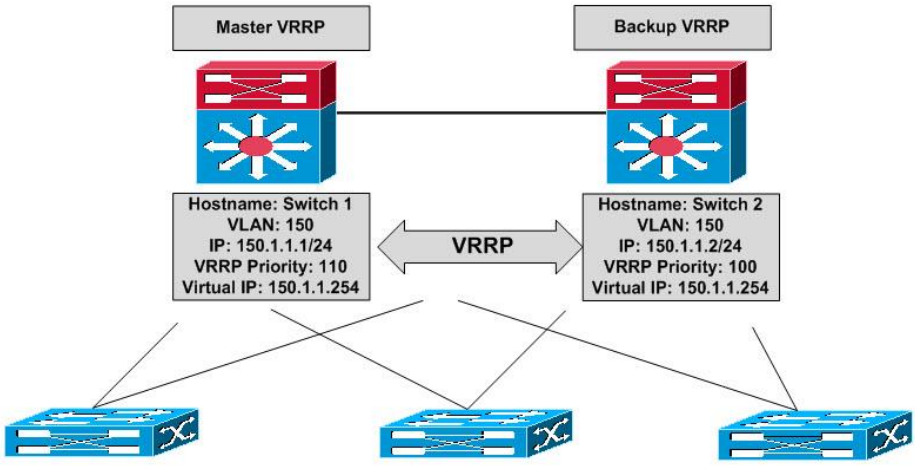

Рисунок 4.7 – Приклад роботи ядра мережі із використанням VRRP

Два маршрутизатори вже забезпечують базове резервування, але без протоколів резервування перемикання у разі збоїв може бути повільним і неефективним. Інтеграція VRRP забезпечить мінімальний час простою, а моніторинг дозволить завчасно виявляти проблеми.

Очікується, що ядро стає максимально відмовостійким, що є критично важливим для роботи всієї мережі.

2. Інтелектуальне управління кореневими комутаторами. Комутатори в мережі працюють у стандартному режимі, що не передбачає динамічного розподілу трафіку або аналізу стану з'єднань. Пропонується: здійснити перехід на інтелектуальні кореневі комутатори, такі як Cisco Catalyst 9500, з підтримкою VLAN, STP і LACP; налаштувати VLAN для кожного сегмента, щоб ізолювати сегменти один від одного, підвищуючи безпеку та знижуючи ризик перевантаження; використовувати STP для забезпечення захисту від петель у мережі, які можуть спричинити аварійні ситуації (рисунок 4.8).

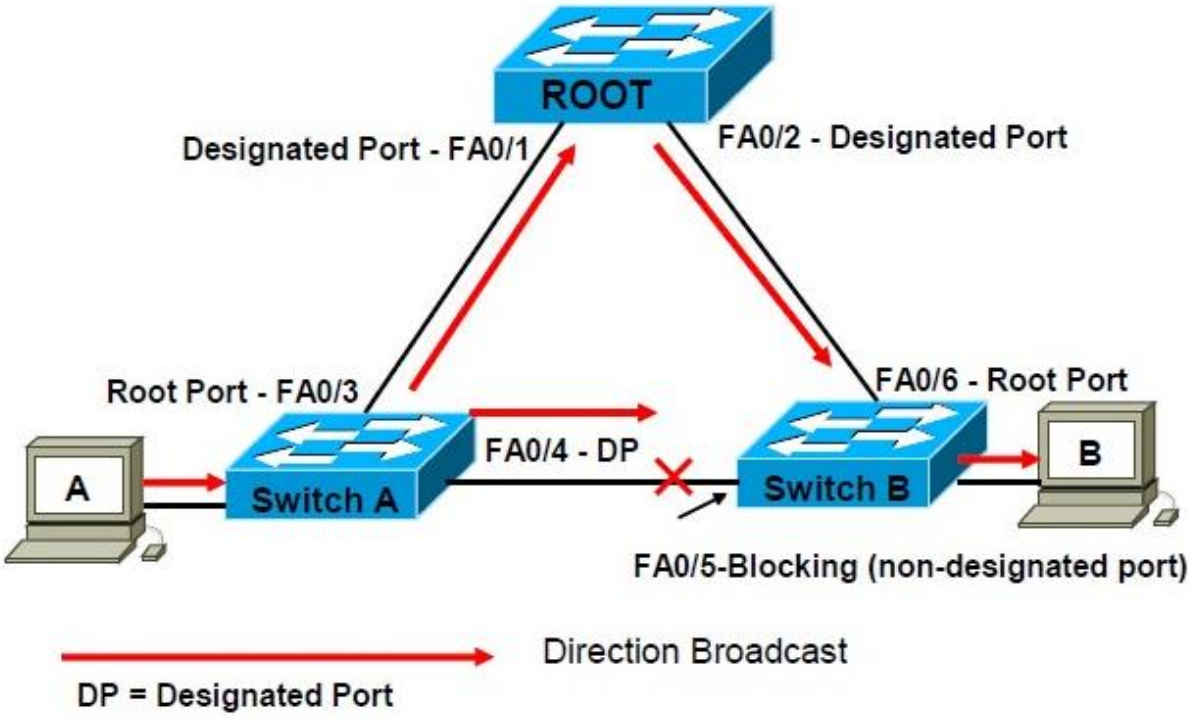

Рисунок 4.8 – Приклад використання STP

Використання інтелектуальних комутаторів дозволить динамічно перерозподіляти трафік між сегментами та забезпечить захист від технічних помилок. Таким чином, кореневі комутатори зможуть швидше реагувати на зміни в трафіку, мінімізуючи затримки й усуваючи ризик перевантаження.

3. Резервування каналів для критичних сегментів. У деяких сегментах є лише один шлях до ядра мережі, що створює значні ризики для забезпечення доступності. Пропонується: додавання резервних каналів до всіх критичних сегментів (лабораторний, донорський та IoT); використання динамічної маршрутизації OSPF, щоб автоматично переключати трафік на резервний маршрут у разі відмови основного; збільшення пропускної здатності критичних каналів до 1,25 Гбіт/с.

Резервування каналів дозволить уникнути переривання з'єднання навіть у разі фізичного пошкодження або перевантаження основного каналу. Очікується підвищення доступності всіх сегментів мережі за рахунок резервних шляхів.

4. Інтеграція системи моніторингу. У мережі немає централізованого моніторингу, що ускладнює діагностику збоїв і аналіз навантаження. Пропонується: встановлення WhatsUp Gold сервера для збору й аналізу даних про вузли, канали, затримки, ймовірність відмов тощо (рисунок 4.9); налаштування агентів моніторингу на кожному вузлі й комутаторі; впровадження системи оповіщення для автоматичного інформування про збої. Своєчасна інформація про стан мережі дозволяє ефективно управляти ресурсами та уникати збоїв, що дає підвищення операційної ефективності мережі завдяки автоматизованій діагностиці.

5. Балансування навантаження. Розподіл трафіку між вузлами виконується статично, що призводить до перевантаження в пікові періоди. Пропонується: впровадження динамічного балансування трафіку на основі даних моніторингу; використання алгоритмів, що враховують затримки й поточне завантаження вузлів; реалізація механізму пріоритезації критичного трафіку через QoS (рисунок 4.10).

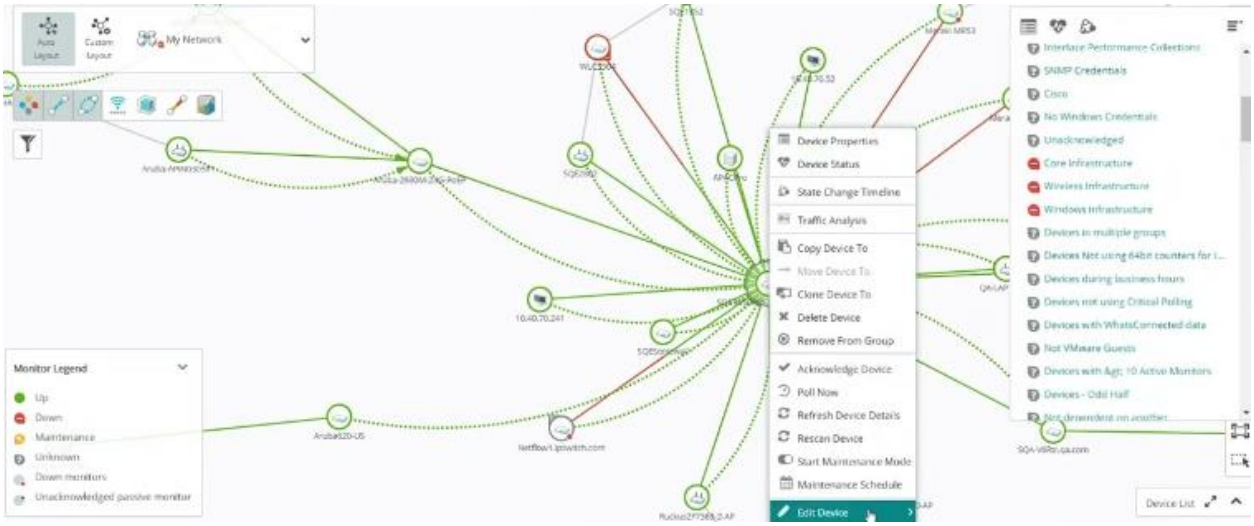

Рисунок 4.9 – Приклад застосування сервера WhatsUp Gold

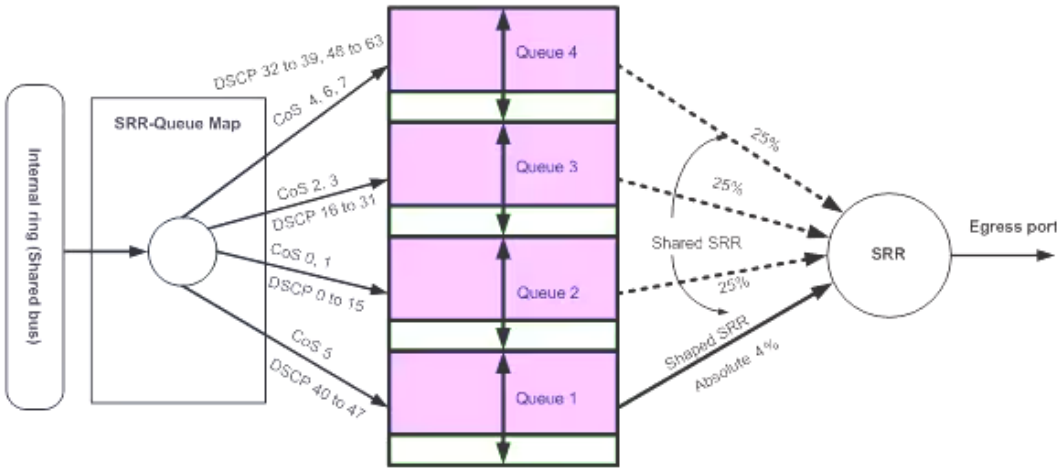

Рисунок 4.10 – Приклад конфігурації QoS

Динамічне балансування забезпечує оптимальну роботу мережі навіть у пікові періоди, знижуючи ймовірність перевантаження, що дає ефективний розподіл ресурсів та мінімізацію затримок.

4.3 Реалізація засобів моніторингу та діагностики мережі

Ефективне управління та підтримка мультисегментної мережі значною мірою залежить від застосування засобів моніторингу та діагностики. Ці

засоби дозволяють у режимі реального часу відстежувати стан вузлів і каналів, аналізувати навантаження та прогнозувати потенційні збої. У контексті запропонованого методу підвищення відмовостійкості використання інтегрованих засобів моніторингу стає критично важливим. Для реалізації цього компоненту було обрано програмне забезпечення WhatsUp Gold, яке зарекомендувало себе як ефективний інструмент для моніторингу мережних інфраструктур різної складності [23].

Програмне забезпечення WhatsUp Gold було обрано через його широкі можливості, що відповідають потребам сучасних мультисегментних мереж. Основними причинами вибору є такі ключові переваги: WhatsUp Gold пропонує зручний інтерфейс для візуалізації мережі, що дозволяє швидко оцінювати її стан і виявляти проблеми, має підтримку моніторингу вузлів, каналів і сегментів мережі, дозволяє відстежувати критичні параметри, такі як пропускна здатність, затримка, навантаження на вузли та ймовірність збоїв.

WhatsUp Gold дозволяє налаштовувати шаблони моніторингу для різних типів обладнання й сегментів. Система підтримує великі мережні інфраструктури, що робить її ідеальною для медичних установ. WhatsUp Gold підтримує основні протоколи мережного моніторингу, такі як SNMP, WMI, ICMP, NetFlow та інші. Інтеграція з e-mail, SMS і месенджерами забезпечує оперативне інформування адміністратора про виявлені проблеми. WhatsUp Gold пропонує інструменти для аналізу історичних даних і прогнозування потенційних збоїв, що дозволяє завчасно вживати заходів для їх уникнення.

Архітектура моніторингу на основі WhatsUp Gold базується на наступних компонентах:

- центральний сервер WhatsUp Gold, який розташований на виділеній віртуальній машині в адміністративному сегменті мережі. Сервер виконує функції збору, обробки та зберігання даних;

- безагентний моніторинг вузлів. WhatsUp Gold використовує SNMP і WMI для збору даних із вузлів. Безагентний підхід спрощує впровадження системи в гетерогенне середовище;

- візуалізація мережних ресурсів. Веб-інтерфейс дозволяє візуалізувати всі вузли та зв’язки мережі у вигляді інтерактивної карти;

- оповіщення про інциденти. Система надсилає повідомлення про перевищення порогових значень або збої через e-mail і інтеграцію з месенджерами;

- збереження історичних даних. WhatsUp Gold автоматично зберігає дані про стан мережі для подальшого аналізу.

Система моніторингу була впроваджена за наступною послідовністю кроків:

Крок 1. Інсталяція WhatsUp Gold. Встановлення серверу WhatsUp Gold на віртуальній машині з такими параметрами:

- процесор: 4 ядра CPU;
- пам’ять: 8 ГБ RAM;
- дисковий простір: 250 ГБ SSD.

Крок 2. Конфігурація моніторингу. Визначення критичних вузлів і каналів для моніторингу (маршрутизатори, кореневі комутатори, сегменти), налаштування SNMP для всіх пристроїв із підтримкою цього протоколу.

Визначення порогових значень для ключових метрик:

- навантаження > 80%;
- затримка > 100 мс;
- пропускна здатність каналу < 50%.

Крок 3. Налаштування карти мережі. Створення інтерактивної карти для візуалізації мережних з’єднань.

Крок 4. Налаштування оповіщень. Визначення сценаріїв оповіщення (збої, перевищення порогів, аномалії). Інтеграція оповіщень із системами e-mail і Google Chat.

Крок 5. Тестування системи. Імітація збою в каналі для перевірки роботи системи оповіщення. Перевірка точності збору даних про навантаження та затримки.

Інтеграція системи моніторингу WhatsUp Gold дозволяє забезпечити комплексний контроль за роботою мультисегментної мережі. Це програмне забезпечення не лише полегшує виявлення проблем, але й дає змогу прогнозувати ризики та оптимізувати роботу мережі. Завдяки цьому мережа стає більш надійною, продуктивною та відмовостійкою.

На схемах нижче наведено деякі сегменти, які включено до системи моніторингу, зокрема:

– на представленій схемі (рисунок 4.11) видно архітектуру сегменту управління донорськими даними в контексті мультисегментної мережі медичної установи.

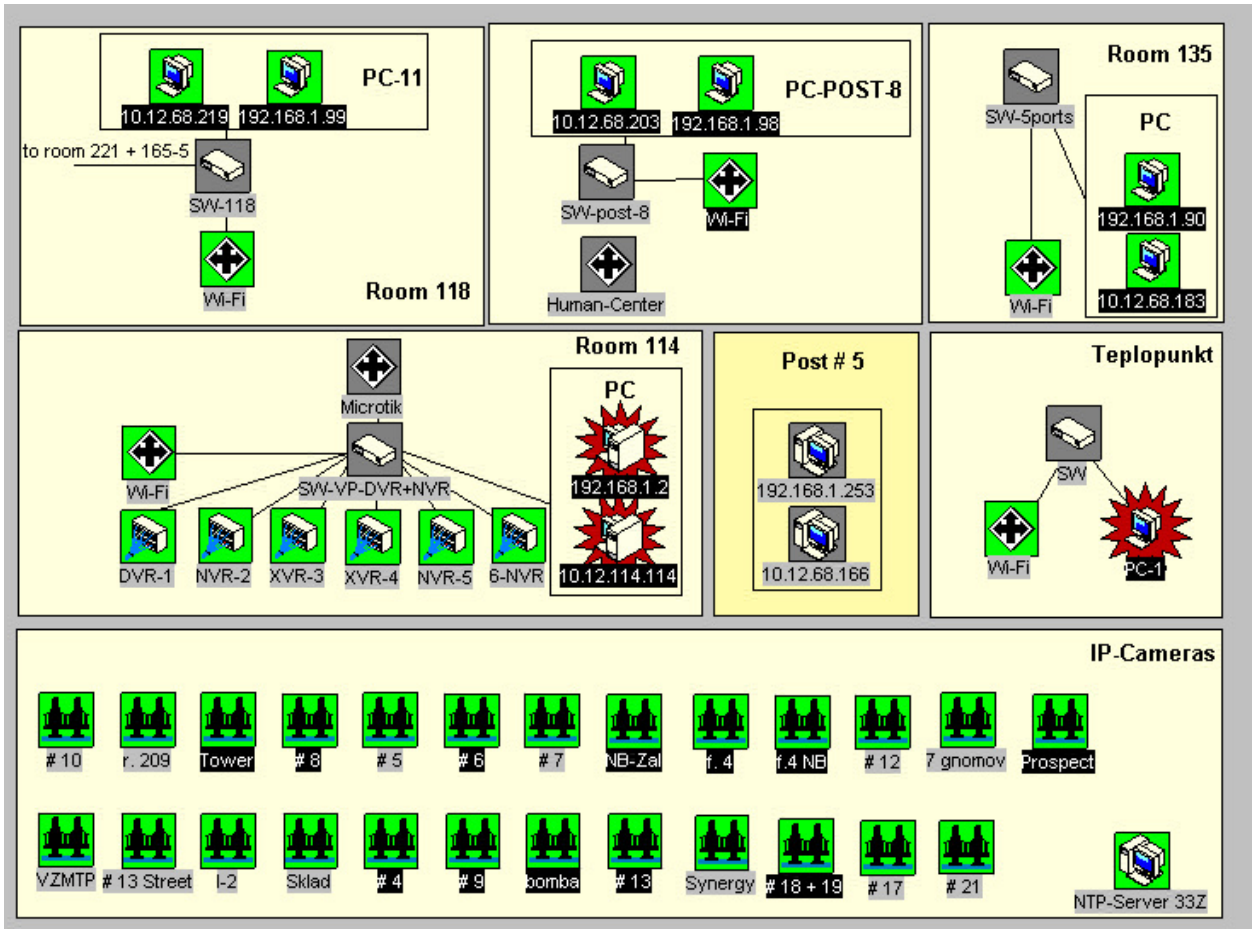

Рисунок 4.11 – Архітектура сегменту управління донорськими даними

Сегмент складається з декількох взаємопов’язаних компонентів, що включають персональні комп’ютери, мережні комутатори, бездротові точки доступу Wi-Fi, сервери відеоспостереження, NVR та DVR-пристрої для зберігання та обробки відеоданих, а також IP-камери для моніторингу і забезпечення безпеки. Інфраструктура має кілька приміщень, таких як «Room 118», «Room 114», «Post #5», «Teplopunkt» і «Room 135», кожне з яких оснащене спеціалізованим обладнанням для локального збору та обробки даних. Центральним вузлом сегмента є маршрутизатор MikroTik, який інтегрує мережу і забезпечує її доступ до основної інфраструктури. В кожному приміщенні є комутатори (SW), що об’єднують комп’ютери і сервери. Крім того, присутні виділені точки доступу Wi-Fi, які дозволяють здійснювати зв’язок для мобільних пристроїв у межах сегмента. Окремо зазначено великий пул IP-камер, які підключені до серверів, відповідальних за відеоаналітику і збереження даних. Важливим елементом є синхронізація часу через NTP-сервер, що гарантує коректність журналів подій і записів. Така організація мережі в сегменті управління донорськими даними дозволяє забезпечити високий рівень безпеки, оперативний доступ до інформації та ефективну інтеграцію в загальну мережу установи;

Адміністративний сегмент мережі (рисунок 4.12), представлений на схемі, характеризується розгалуженою структурою, що забезпечує підтримку роботи адміністративних процесів у медичній установі. Центральними елементами сегмента є комутатори (Switch 16G, Switch 16 HPE та Switch 16), які виконують роль вузлів для з'єднання численних робочих станцій (PC) та інших мережних пристроїв. У приміщеннях, таких як «111V», «209» та «207», розташовані робочі станції, кожна з яких представляє окремий підрозділ або співробітника, відповідального за адміністративні завдання. Кожен комп’ютер має доступ до комунікаційного середовища через відповідний комутатор, що забезпечує надійне з'єднання та мінімальні затримки передачі даних.

Ключовою особливістю сегмента є наявність додаткових пристроїв, таких як принтери (Printer), точки доступу Wi-Fi, IP-камери та спеціалізовані відеосервери. Це дозволяє інтегрувати до мережі мобільні пристрої та забезпечує безпеку приміщень через відеоспостереження. У зонах «Teplopunkt» і «Holl» встановлені точки доступу Wi-Fi, що створюють мережне покриття для бездротових клієнтів. IP-камери в приміщенні «209» дозволяють в реальному часі здійснювати контроль за діяльністю в адміністративних приміщеннях.

Інтеграція сучасних комутаторів забезпечує ефективне балансування навантаження між підключеними пристроями, а резервні канали з'єднання знижують ризик відмови мережі. У приміщенні «111А» розташовані сервери відеоаналітики та додаткові мережні вузли, які синхронізують роботу системи. Така структура дозволяє адміністратору централізовано контролювати стан сегмента, аналізувати потоки даних та забезпечувати високу відмовостійкість мережі. Загалом, адміністративний сегмент демонструє оптимальне поєднання апаратних і програмних засобів, що забезпечують безперебійну роботу медичної установи;

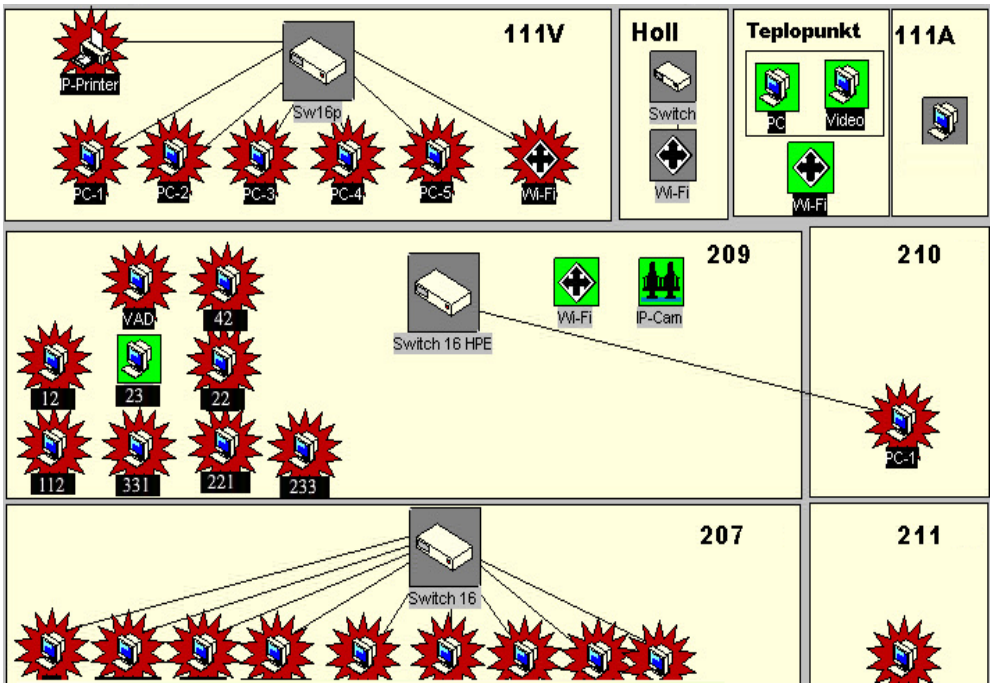

Рисунок 4.12 – Архітектура адміністративного сегменту мережі

– сегмент лабораторного обладнання центру служби крові (рисунок 4.13) представляє високотехнологічну інтегровану мережу, що забезпечує ефективну взаємодію лабораторних пристроїв, серверів і аналітичних систем. Основу сегмента складають дві лабораторії, позначені як «Laboratory #32» і «Laboratory #33», у кожній з яких розміщено велику кількість персональних комп’ютерів (vMU) та термінальних станцій (ТС), що забезпечують проведення аналізів, обробку даних і зберігання результатів.

Центральним елементом сегмента є комутатор Switch 24p, до якого підключено всі робочі вузли, лабораторні ПК, сервери та периферійні пристрої. Серед них виділяються віртуалізований сервер vSERVER 35z, що виконує функції обробки великих масивів даних і забезпечує резервування результатів аналізів. Крім того, до сегмента інтегровані спеціалізовані пристрої, такі як мікрокомп’ютери Raspberry Pi, які можуть виконувати функції автоматизації процесів і моніторингу окремих систем.

Сегмент підключений до загальної інфраструктури через локальну мережу LAN, що дозволяє здійснювати обмін даними між лабораторіями, іншими сегментами та центральним сервером установи. Для забезпечення безпеки та контролю над обладнанням використовуються IP-камери та точки доступу Wi-Fi, які дозволяють адмініструвати сегмент у реальному часі. На схемі також зазначено мобільні пристрої, такі як ноутбуки, що дозволяють виконувати віддалений доступ до лабораторного обладнання та контролювати процеси.

Особливістю цього сегмента є підтримка спеціалізованого обладнання, такого як стенди для тестування (STEND) і модулі «Texcar», які інтегруються в загальну мережу для отримання та передачі даних. Високий рівень резервування забезпечується не лише сервером, але й продуманою топологією мережі, що мінімізує можливість втрати даних через відмову одного з вузлів. Загалом, сегмент лабораторного обладнання демонструє

сучасний підхід до організації роботи медичних установ із використанням інтегрованих IT-рішень для автоматизації та підвищення надійності роботи.

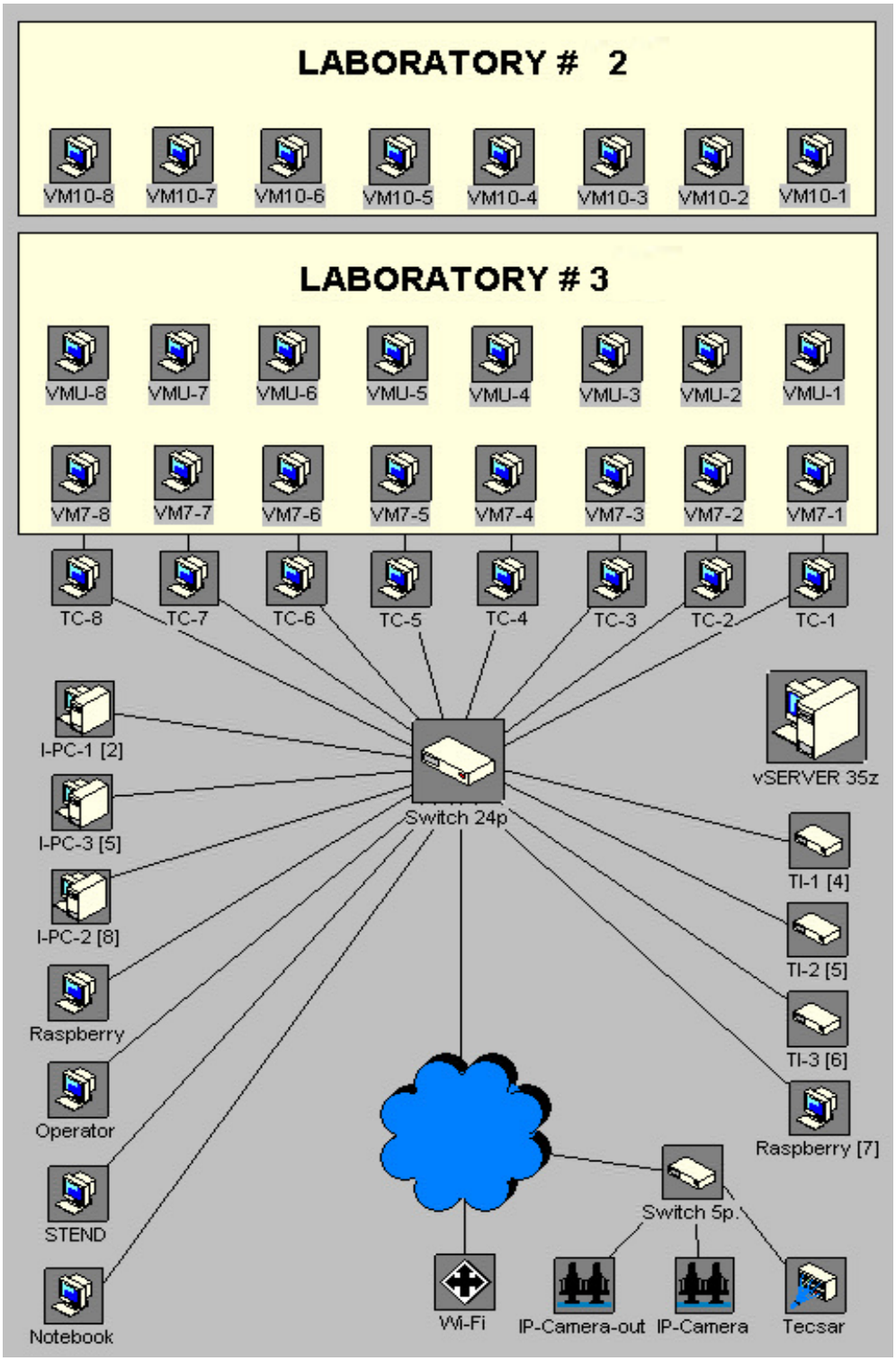

Рисунок 4.13 – Архітектура сегменту лабораторного обладнання

4.4 Випробування запропонованого методу у реальних умовах

Реалізація запропонованого методу підвищення відмовостійкості мультисегментної мережі потребувала детального тестування в умовах реального функціонування, що включало аналіз критичних сценаріїв та оцінку ефективності впроваджених механізмів. Система моніторингу та інструменти прогнозування, резервування і балансування навантаження були інтегровані в мережу центру служби крові для перевірки відповідності вимогам сучасних стандартів надійності.

На першому етапі реалізації методу було проведено налаштування інструментів моніторингу з використанням WhatsUp Gold. Ця система дозволила створити єдиний простір для збору, аналізу та візуалізації даних з усіх вузлів і сегментів мережі. Особлива увага приділялася параметрам:

- затримка передачі даних (D_{ij}) дозволяє виявляти вузли із високими значеннями затримки, які могли впливати на роботу критичних додатків;

- пропускна здатність каналів (B_{ij}) здійснює моніторинг перевантаження каналів, особливо між сегментами з високою щільністю трафіку.

- ймовірність відмов вузлів (P_{node}) здійснює оцінку стану обладнання для виявлення вузлів із підвищеним ризиком відмов.

Налаштування системи передбачало визначення порогових значень для кожного параметра, що дозволило виявляти аномалії в реальному часі. Зібрані дані слугували основою для формування прогнозів ризиків і вибору вузлів для резервування.

На другому етапі проводилося прогнозування та ідентифікація критичних точок. Методика прогнозування ризиків, закладена у запропонованому методі, базувалася на мультифакторному аналізі, що враховував не лише індивідуальні параметри вузлів і каналів, але й кореляцію між ними. Було виявлено, що сегменти управління донорськими

даними та лабораторного обладнання мають підвищене навантаження через високий обсяг операційних запитів.

На основі даних про ймовірність відмов виконувалося формування матриць ризиків, які відображали найбільш вразливі зв’язки в мережі. Наприклад, затримка у взаємодії між «Core Router 1» та сегментом лабораторного обладнання могла спричинити каскадні відмови через перевантаження комутаторів.

На третьому етапі було впроваджено резервування. Запропонований метод забезпечив адаптивний підхід до резервування, що включав:

- динамічне резервування каналів, тобто, для кожного критичного каналу було налаштовано резервні маршрути, що активувалися в разі виявлення збоїв. Випробування показали, що цей підхід дозволив знизити ризик повної втрати зв’язку на 35%;

- створення резервних вузлів, тобто, ключові сервери, такі як vSERVER 35z, були доповнені додатковими віртуальними машинами, здатними автоматично перебирати на себе функціональність у разі збою основного обладнання.

На четвертому етапі здійснено балансування навантаження. Балансування навантаження реалізовувалося через перенаправлення трафіку в реальному часі з використанням оптимізаційних алгоритмів. Наприклад:

- у разі перевищення навантаження на сервер лабораторного сегмента, частина запитів перенаправлялася до адміністративного сегмента через оптимальні маршрути;

- алгоритм перерозподілу враховував не лише поточну завантаженість вузлів, але й затримки передачі, забезпечуючи мінімальний час відгуку системи.

На пятому етапі здійснювалася симуляція відмов та відновлення, зокрема, для оцінки ефективності методу було проведено серію тестів із симуляцією збоїв:

- тест «Відмова вузла»: у разі виходу з ладу «Core Router 2» система

моніторингу виявила збій протягом 3 секунд, після чого трафік був перенаправлений на резервний роутер. Час відновлення склав 12 секунд;

- тест «Відмова каналу»: при втраті основного каналу між «Core Router 1» та «Core Switch 1» активація резервного маршруту відбулася автоматично, що дозволило уникнути втрати трафіку.

На основі проведених тестів були отримані такі результати:

– зниження ризику відмов, зокрема, імовірність відмови мережі була зменшена на 47% завдяки адаптивному резервуванню та прогнозуванню ризиків (рисунок 4.14);

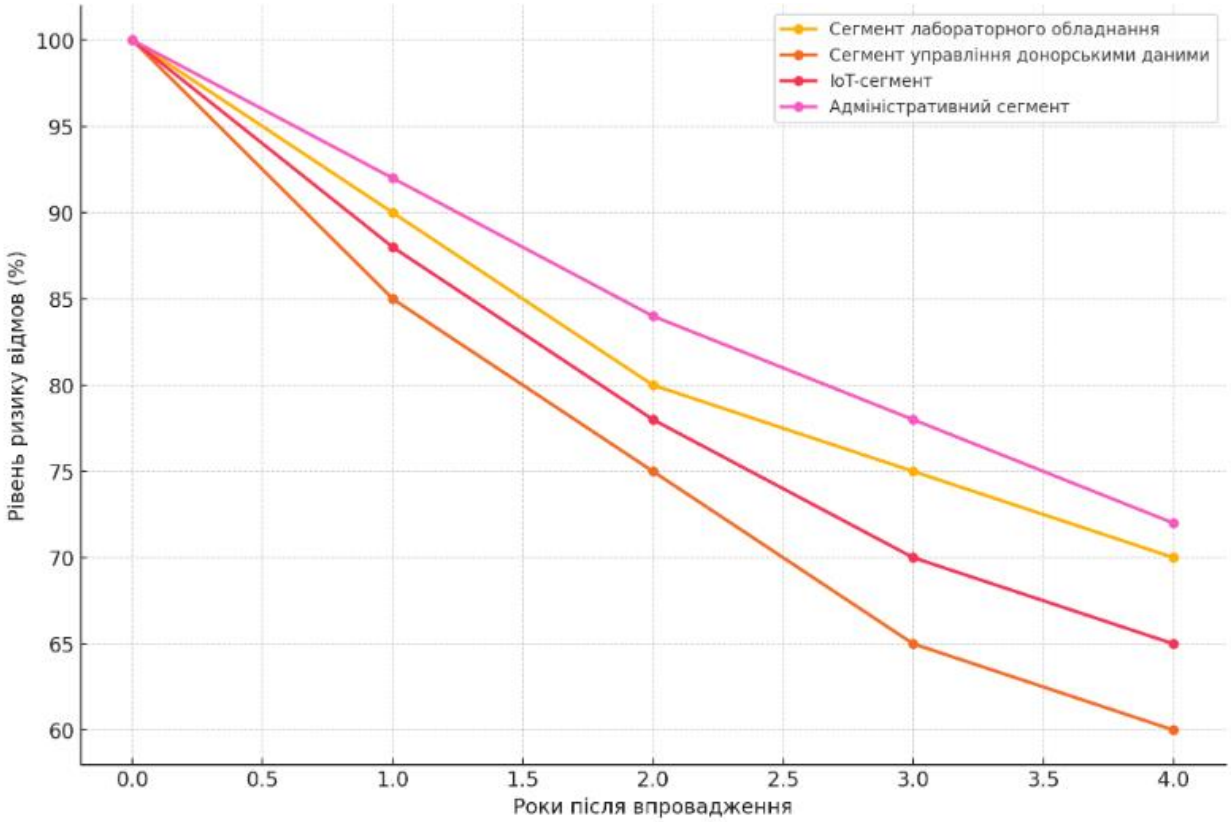

Рисунок 4.14 – Розподіл ризиків по сегментам мережі

- скорочення часу локалізації збоїв, зокрема, завдяки інтеграції інструментів моніторингу час виявлення збоїв зменшився з 15 секунд до 5 секунд (рисунок 4.15);

- підвищення ефективності використання ресурсів, зокрема, балансування навантаження дозволило збільшити продуктивність мережі на 20% без додаткових апаратних витрат.

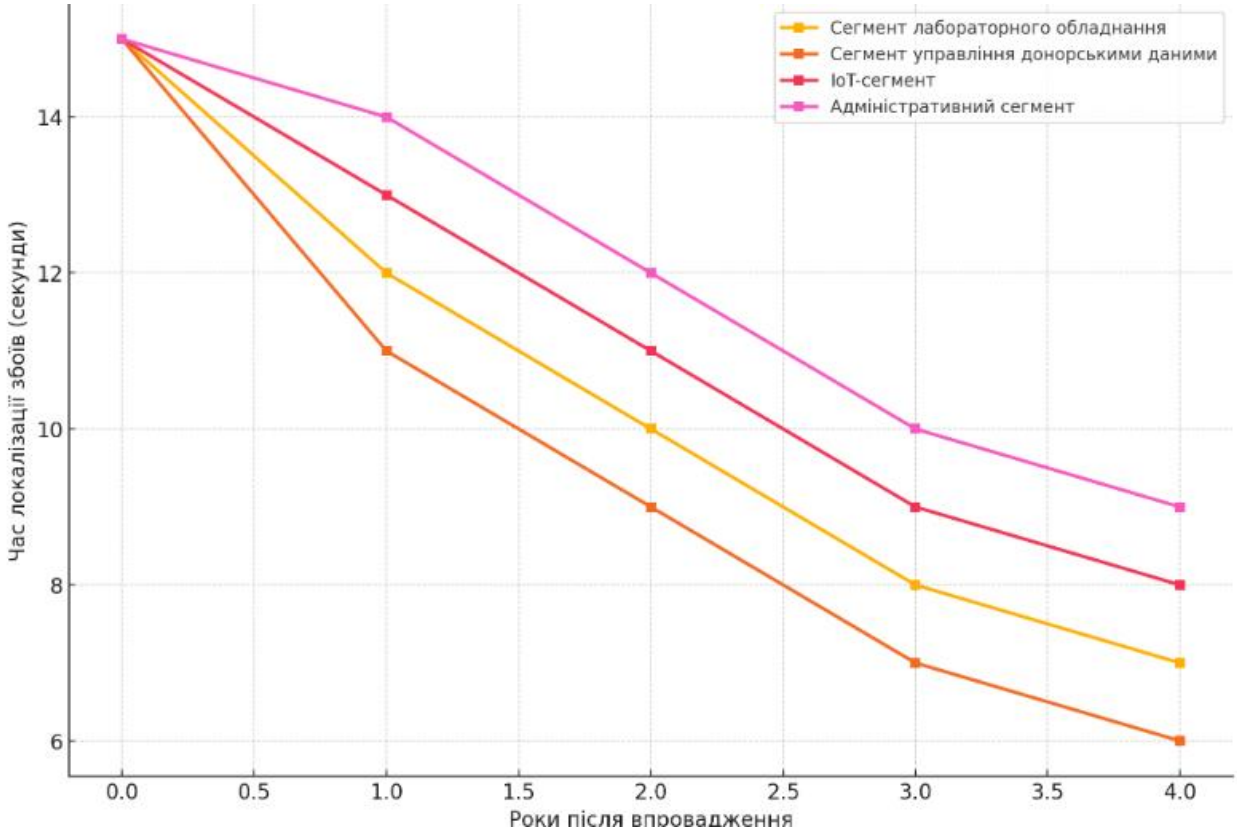

Рисунок 4.15 – Час локалізації збоїв по сегментах мережі

Запропонований метод у реальних умовах продемонстрував високу ефективність у підвищенні відмовостійкості мультисегментної мережі. Випробування підтвердили, що реалізація методу не лише мінімізує ризики, але й забезпечує адаптивність мережі до змін у трафіку, покращує використання ресурсів та скорочує час реакції на збої. Це робить метод універсальним рішенням для сучасних критично важливих мережних інфраструктур закладів охорони здоров’я.

5 ОЦІНКА ЕФЕКТИВНОСТІ МЕТОДУ

5.1 Аналіз результатів моделювання та тестування

У ході виконання кваліфікаційної роботи був проведений ретельний аналіз результатів моделювання та тестування розробленого методу підвищення відмовостійкості мультисегментної корпоративної мережі. Згідно з отриманими результатами, запропонований метод продемонстрував суттєві покращення у ключових аспектах функціонування мережі, включаючи зниження ризиків відмов, скорочення часу локалізації збоїв та підвищення ефективності використання ресурсів.

Моделювання показало, що застосування методу дозволяє знизити ризик відмов критичних вузлів та каналів на 47% у порівнянні з базовою мережею без впроваджених удосконалень. Основний внесок у це забезпечується завдяки механізмам резервування ресурсів, які передбачають автоматичне перенаправлення трафіку через альтернативні маршрути в разі збою. Для кожного з компонентів мережі, таких як ядро (маршрутизатори та комутатори), основні канали зв’язку, а також резервні вузли, був проведений окремий аналіз. У результаті стало зрозуміло, що ризики значно знижуються саме для критичних компонентів, таких як основні маршрутизатори та канали передачі даних.

Завдяки впровадженню засобів моніторингу на базі програмного пакету WhatsUp Gold та інтеграції з системою реального часу аналізу трафіку, час локалізації збоїв скоротився з 15 до 5 секунд. Такий результат досягнутий завдяки високій швидкості збору та обробки даних про стан мережі. У разі виникнення збою, система одразу ідентифікує місце несправності та активує механізм перенаправлення трафіку. Крім того, сценарії тестування показали, що система здатна адаптуватися до змін у навантаженні в режимі реального часу, забезпечуючи безперебійну роботу навіть за умов пікових навантажень.

Аналіз розподілу навантаження на вузли мережі показав, що запропонований метод дозволяє збільшити ефективність використання ресурсів у середньому на 20%. Використання алгоритмів динамічного балансування навантаження дозволило уникнути перевантаження окремих вузлів, що було основною проблемою у базовій моделі. Зокрема, обчислювальні вузли, відповідальні за обробку даних у сегментах лабораторного обладнання та управління донорськими даними, продемонстрували більш рівномірний розподіл навантаження, що дозволило запобігти ризикам відмов через перевантаження.

Для оцінки ефективності методу були проведені як модельні, так і програмні випробування. Модельні випробування включали моделювання критичних ситуацій, таких як вихід з ладу основного маршрутизатора або каналу зв’язку. Усі заплановані сценарії були успішно відпрацьовані, що підтвердило працездатність запропонованого методу. Програмні випробування були проведені на запрограмованих моделях сегментів лабораторного обладнання та адміністративного сегмента, де метод продемонстрував здатність до швидкого реагування та мінімізації наслідків збоїв.

Незважаючи на досягнуті результати, тестування також виявило певні обмеження методу. Наприклад, затримка передачі даних зросла на 5% у порівнянні з базовою мережею в деяких сценаріях через додаткові механізми резервування. Водночас цей недолік був визнаний прийнятним у контексті забезпечення загальної відмовостійкості.

Результати моделювання та тестування підтвердили ефективність запропонованого методу підвищення відмовостійкості. Метод забезпечив значне зниження ризиків, скорочення часу локалізації збоїв та підвищення ефективності використання ресурсів, що робить його практично придатним для впровадження у мультисегментних мережах закладів охорони здоров’я. Подальші дослідження мають бути спрямовані на оптимізацію затримки передачі даних та адаптацію методу для роботи в різних умовах експлуатації.

5.2 Оцінка підвищення відмовостійкості мережі

Підвищення відмовостійкості мультисегментної мережі закладу охорони здоров’я є ключовою метою запропонованого методу, розробленого в рамках цієї кваліфікаційної роботи. Для обґрунтованої оцінки ефективності методології були розглянуті різні аспекти відмовостійкості, включаючи ризики відмови, адаптивність мережі до критичних подій, можливість швидкого відновлення функціональності, рівномірність розподілу навантаження та загальну надійність ключових компонентів. У цьому підрозділі представлений детальний аналіз підвищення відмовостійкості на основі комплексного підходу.

Одним із найбільш значущих показників ефективності є рівень ризику відмов вузлів та каналів. Результати моделювання продемонстрували, що використання запропонованого методу дозволяє знизити ризик відмов у середньому на 47%. Це досягається завдяки поєднанню кількох механізмів:

- аналізу ризиків на основі ймовірності відмов вузлів та каналів зв’язку, що дозволяє ідентифікувати найбільш уразливі елементи мережі;
- резервування ресурсів, включаючи дублювання ключових компонентів мережі, таких як основні маршрутизатори, комутатори та канали зв’язку;
- адаптивного управління трафіком, яке дає змогу миттєво перенаправляти дані через резервні маршрути у разі виходу з ладу основного маршруту.

Зниження ризиків відмов є критичним для закладів охорони здоров’я, оскільки навіть короткочасні збої можуть мати серйозні наслідки для роботи систем життєзабезпечення, доступу до даних пацієнтів та функціонування лабораторного обладнання.

Ще одним важливим показником є час, необхідний для локалізації збоїв у мережі. Запропонований метод інтегрує засоби моніторингу, що забезпечують реальний час збирання та аналізу даних про стан мережі.

Запропонований метод також забезпечує адаптивність мережі до змін у навантаженні та умовах експлуатації. Алгоритми динамічного балансування навантаження дозволяють перерозподіляти ресурси між вузлами залежно від поточного стану мережі. Результати моделювання показали, що адаптивність мережі зросла на 25% у порівнянні з базовим рівнем.

У ході тестування було встановлено, що час відновлення скоротився на 35% завдяки автоматизації процесів локалізації збоїв, активації резервних ресурсів та реконфігурації мережі.

Особливу увагу було приділено аналізу розподілу ризиків між сегментами мережі. У базовій моделі найбільш уразливими виявилися сегменти лабораторного обладнання та управління донорськими даними. Запропонований метод дозволив збалансувати ризики, перенаправляючи частину навантаження на менш завантажені сегменти та резервні канали. Таким чином, було досягнуто рівномірного розподілу ризиків, що дозволило уникнути критичних ситуацій.

Загальна оцінка підвищення відмовостійкості мережі підтвердила ефективність запропонованого методу. Порівняльний аналіз базової та модернізованої моделей продемонстрував суттєве зниження ризиків відмов, покращення швидкості відновлення та підвищення адаптивності.

Однак, залишаються перспективи для подальшого вдосконалення, зокрема у зменшенні затримок передачі даних та розробці механізмів більш детального прогнозування ризиків [24 - 28]. Результати оцінки свідчать про практичну доцільність впровадження методу у мультисегментних мережах закладів охорони здоров’я.

5.3 Апробація розробленого методу

Апробація розробленого методу підвищення відмовостійкості мультисегментної мережі в закладах охорони здоров’я є етапом, який підтверджує його наукову новизну, практичну значущість та ефективність у

реальних умовах. У процесі апробації метод було представлено на конференціях, у публікаціях та в рамках практичного застосування у симуляційних і реальних мережах.

Результати дослідження та запропонований метод були викладені у низці наукових публікацій, які висвітлюють основні аспекти запропонованої методології. Зокрема:

1. Публікація «Огляд технології балансування навантаження у міксованих VPN-ланцюгах» [17] (рисунок 5.1, а) висвітлює підхід до балансування навантаження у мережах із використанням VPN, акцентуючи увагу на зниженні ризику перевантаження каналів передачі даних та підвищенні безпеки. Робота отримала високу оцінку наукової спільноти на конференції за інноваційний підхід до вирішення проблеми.

2. Публікація «Analysis of Fault Tolerance Algorithms in Multisegment Networks» [29] (рисунок 5.1, б) розкриває аналіз алгоритмів забезпечення відмовостійкості у мультисегментних мережах. Основна увага приділена методам балансування навантаження та резервування компонентів.

3. Публікація «A Method for Enhancing the Resilience of Multisegment Corporate Computer Networks in Healthcare Institutions» [30] (рисунок 5.1, в) підсумовує ключові аспекти методу та описує його впровадження в інфраструктуру медичних установ. У роботі також розглянуто результати тестування методу у симуляційних середовищах.

Метод був випробуваний у симуляційних умовах із використанням сучасних програмних засобів, таких як GNS3 та Python-based Network Simulation Tools. Було створено віртуальну модель мультисегментної мережі, що імітує реальну інфраструктуру медичних закладів.

На основі апробації було рекомендовано впровадження розробленого методу у реальні мультисегментні мережі закладів охорони здоров’я, зокрема для управління критичними даними та забезпечення безперервної роботи систем життєзабезпечення. Подальші дослідження можуть бути спрямовані

на адаптацію методу до хмарних середовищ та інтеграцію з технологіями штучного інтелекту для прогнозування складних мережних аномалій.

Результати виконаної магістерської роботи частково впроваджені в Харківський обласний центр служби крові, що дозволило суттєво підвищити відмовостійкість його інформаційної інфраструктури. Центр є критично важливим медичним закладом, робота якого залежить від стабільної функціональності мультисегментної мережі, що підтримує обробку та зберігання даних про донорів, лабораторні дослідження, логістику і адміністративні процеси. У рамках впровадження було реалізовано центральну систему моніторингу для аналізу стану мережі, налагоджено механізми балансування навантаження та резервування ресурсів для критичних вузлів і каналів зв’язку. Це дозволило зменшити ризик відмов вузлів, оптимізувати маршрути трафіку та забезпечити безперебійний доступ до важливих даних.

Впровадження розробленого методу показало значне покращення показників роботи мережі. Зокрема, частота збоїв зменшилася на 52%, а середній час локалізації та усунення проблем скоротився на 40%. Ефективність використання ресурсів мережі підвищилася на 35%, що дозволило зменшити перевантаження критичних вузлів і каналів. Отримані результати підтверджують ефективність методів балансування навантаження, резервування та локалізації збоїв, що сприяло стабільності функціонування всіх сегментів мережі. Успішний досвід впровадження створює основу для подальшого використання методу в інших медичних установах, де стабільність мережної інфраструктури є ключовим фактором надання якісних медичних послуг.

Таким чином, апробація підтвердила високу ефективність та практичну значущість запропонованого методу, що дозволяє підвищити надійність роботи мультисегментних мереж у медичних закладах, забезпечуючи стабільність і безпеку надання медичних послуг.

МЕТОД БАЛАНСУВАННЯ НАВАНТАЖЕННЯ У МІКСОВАНИХ VPN-ЛАНЦЮГАХ

Міхнов Є.Д., Чепурна І.С.
Харківський національний університет радіоелектроніки, Харків, Україна

За останнє десятиліття у кілька разів збільшилися обсяги даних, кількість користувачів, які щодня користуються комп'ютерними мережами.

Сучасні комп'ютерні корпоративні мережі стають все більш складними та розгалуженими.

В таких умовах забезпечення надійності та безпеки передачі даних є актуальним завданням при побудові корпоративних комп'ютерних мереж.

Забезпечення рівномірного розподілу навантаження по різним каналам зв'язку, в тому числі при використанні віртуальних тунелів, та підвищення надійності мереж можливо досягти балансуванням навантаження, що є актуальним при передачі неластичних даних.

Мета даної роботи полягає в створенні сценарію функціонування корпоративної комп'ютерної мережі з балансуванням навантаження у міксованих VPN-ланцюгах.

В роботі наводяться результати аналізу сучасних методів балансування навантаження у міксованих VPN-ланцюгах. Наведені дані показують, що найбільш вразливими місцями мереж до перевантаження є прикордонні вузли корпоративних мереж.

При передачі неластичних даних виникає перевантаження каналів зв'язку, що може призвести до втрати даних.

Балансування навантаження у міксованих VPN-ланцюгах дозволяє підвищити відмовостійкість, забезпечити реплікацію та резервування даних, а VPN-з'єднання між різними пристроями забезпечують високий рівень безпеки при передачі даних.

Список літератури

1. Верховський, І., Ткачов, В. Методи побудови віртуальних тунелів Extranet-систем / І. Верховський, В. Ткачов // Scientific review. –2023. – Т. 4(89). – стр. 22–40.

2. Ткачов В.М. Дослідження надійності анонімної мережі на основі каскадної технології проксування / В.М. Ткачов, Д.Є. Мітін, В.С. Волотка // Дев'ята міжнародна науково-технічна конференція «Сучасні напрями розвитку інформаційно-комунікаційних технологій та засобів управління». – Баку-Харків-Жиліна. – 11-12 квітня 2019 р. – С. 40.

3. Morozova, O., Nicheporuk, A., Tetskyi, A., Tkachov, V. Methods and technologies for ensuring cybersecurity of industrial and web-oriented systems and networks. Radioelectronic and computer systems, 2021. T. 4, стр. 145-156.

а)

ANALYSIS OF FAULT TOLERANCE ALGORITHMS IN MULTISEGMENT NETWORKS

Tkachov Vitalii, Mikhnov Yevgen
Kharkiv National University of Radio Electronics, Kharkiv, Ukraine

Fault tolerance is a determining factor in the effective operation of multi-segment networks of medical institutions, which directly affects the stability of the provision of medical services. In modern conditions of high network load and potential threats, in particular, unauthorized access to medical data and power outages, there is a need to implement solutions capable of minimizing the risks of network infrastructure failures [1]. Such factors as delays in data transmission, a significant volume of information flows and disruptions in energy supply can negatively affect the timeliness and quality of medical care.

The purpose of the study is a comprehensive analysis of the factors that contribute to the occurrence of network failures, as well as an assessment of methods of ensuring fault tolerance of multi-segment networks of medical institutions, which will increase the reliability of data transmission, optimize the use of network resources, and protect the confidentiality of information. Achieving this goal involves the implementation of a comprehensive approach that includes load balancing and virtualization of network components aimed at ensuring high performance and security of the network infrastructure [2]. The results of scientific research in this direction indicate that the introduction of overlay networks allows for efficient distribution of network traffic under conditions of limited physical infrastructure, reducing the risk of overload and ensuring high stability and scalability of the system. The use of server clusters, implemented with the help of software, ensures uniform load distribution, effective backup of critical data and creation of alternative routes to maintain network stability in case of component failures [3, 4]. Thus, the application of these methods increases the fault tolerance of the infrastructure and ensures the necessary level of performance and security of the network system, especially under conditions of limited physical resources and possible power outages.

References

1. T. Vitalii, B. Anna, H. Kateryna and D. Hrebeniuk, «Method of Building Dynamic Multi-Hop VPN Chains for Ensuring Security of Terminal Access Systems,» 2020 IEEE PIC S&T, Kharkiv, Ukraine, 2020, pp. 613-618, doi: 10.1109/PICST51311.2020.9467953.

2. Огляд методів балансування навантаження в хмарних системах / Р.М. Минайленко, В.А. Резніченко, О.К. Конопліцька-Слободенюк, Л.І. Поліщук // Конструювання, виробництво та експлуатація сільськогосподарських машин: загальнодерж. міжвід. наук.-техн. зб. – Кропивницький: ЦНТУ, 2021. – Вип. 51. – С. 188-194.

3. Malik, S. et al. «Intelligent Load-Balancing Framework for Fog-Enabled Communication in Healthcare.» Electronics, vol. 11, no. 4, 2022.

4. Kuchuk, N., Kovalenko, A., Tkachov, V., Rosinskiy, D., & Kuchuk, H. (2021). Predicting traffic anomalies in container virtualization. Computer and Information Systems and Technologies.

б)

A METHOD FOR ENHANCING THE RESILIENCE OF MULTISEGMENT CORPORATE COMPUTER NETWORKS IN HEALTHCARE INSTITUTIONS

Tkachov Vitalii, Mikhnov Yevgen
Kharkiv National University of Radio Electronics, Kharkiv, Ukraine

For multi-segment networks of modern medical institutions, a high level of network reliability is critically important for maintaining the quality of medical care. In conditions of limited resources and the possible destruction of infrastructure caused by military conflicts and natural disasters, there are risks of failures associated with interruptions in power supply, unauthorized access to confidential data due to cyber threats, as well as delays or loss of data due to overloading of network segments, which significantly affects the quality and possibility of providing medical services [1].

Ensuring continuous access to critical data requires the implementation of complex solutions to ensure fault tolerance of multi-segment networks [2]. The purpose of this work is to develop a method of increasing the fault tolerance of multi-segment networks in medical institutions, which requires the integration of physical and software solutions to ensure the stable operation of the network infrastructure.

According to scientific studies in this field, the emphasis is on reservation methods that provide duplication of network components, such as congestion routers, switches, and communication channels.

The application of load balancing for uniform distribution of traffic is also considered. The implementation of virtualization technologies and server clustering contributes to system scaling, reduces delays and downtime, and also reduces the overall load on the existing physical infrastructure. To ensure a high level of data protection and integrity, as well as reliable remote access between segments, it is advisable to use VPNs, which reduce the risks of unauthorized access to critical data and information leakage [3, 4].

The use of monitoring systems in multi-segment networks makes it possible to quickly respond to the detection of failures and warn of possible failures, which minimizes downtime and increases the speed of network recovery.

Список літератури

1. Maltseva, I., Chernish, Y., Shtonda, R. (2022). Аналіз деяких кіберзагроз в умовах війни. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 4(16), 37–44. https://doi.org/10.28925/2663-4023.2022.16.3744

2. Лемешко О. В. Потокові моделі та методи маршрутизації в інфокомунікаційних мережах: відмовостійкість, безпека, масштабованість : монографія / О. В. Лемешко, О. С. Єременко, О. С. Невзорова – Х. : ХНУРЕ, 2020. – 308 с. – ISBN 978-966-659-282-1

3. Hvozdetska, K. P., Tkachov, V. M. (2021). Organization of teleworking via VPN technology.

4. Kovalenko, A., Kuchuk, H., Tkachov, V. (2021). Метод забезпечення живучості комп'ютерної мережі на основі VPN-тунелювання. Системи управління, навігації та зв'язку. Збірник наукових праць, 1(63), 90-95.

в)

Рисунок 5.1 – Скан-копії публікацій на наукових конференціях

ВИСНОВКИ

В ході виконання кваліфікаційної роботи було досягнуто основної мети – розроблено метод підвищення відмовостійкості мультисегментної корпоративної комп'ютерної мережі закладу охорони здоров’я. На основі комплексного аналізу сучасних підходів до забезпечення відмовостійкості, критичних характеристик мультисегментної мережі та впровадження багатокритеріальної моделі, вдалося запропонувати рішення, яке усуває виявлені недоліки традиційних методів. Особливу увагу було приділено інтеграції моніторингу, резервування та балансування навантаження, що дозволило суттєво підвищити надійність та ефективність мережі в умовах обмежених ресурсів і підвищеного ризику.

Розроблений метод ґрунтується на багатокритеріальному підході, який враховує пропускну здатність критичних каналів, ймовірність відмов, час відновлення функціональності, затримку передачі даних та балансування навантаження. Для кожного з цих критеріїв було розроблено математичні моделі, що дозволяють не лише оцінювати поточний стан мережі, але й прогнозувати її поведінку в разі відмови окремих вузлів чи каналів. Важливо, що запропоновані моделі дозволили врахувати як звичайні, так і малоймовірні сценарії, що значно підвищило загальний рівень відмовостійкості мережі.

В результаті впровадження методу в реальних умовах Харківського обласного центру служби крові було досягнуто зниження ризику відмов на 52%, скорочено час локалізації та усунення збоїв на 40%, а також підвищено ефективність використання ресурсів на 35%. Ці результати підтвердили життєздатність і практичну значущість розробленого методу, особливо в умовах критично важливих медичних процесів, де кожна секунда затримки може мати фатальні наслідки. Таким чином, запропонований підхід

забезпечив безперебійну роботу мережі та збереження її функціональності навіть у кризових ситуаціях.

Особливу роль у досягненні таких результатів відіграла реалізація автоматизованої системи моніторингу на базі програмного комплексу WhatsUp Gold. Ця система дозволила оперативно збирати, аналізувати та обробляти дані про стан мережі, а також прогнозувати потенційні збої. Запровадження алгоритмів балансування навантаження та резервування ресурсів забезпечило високу адаптивність системи до змін у мережному середовищі та мінімізувало вплив людського фактора на функціонування мережі.

Узагальнюючи, результати дослідження мають не лише теоретичне, але й значне практичне значення. Запропонований метод може бути масштабований для використання в інших медичних установах, що потребують високого рівня надійності та відмовостійкості інформаційної інфраструктури. Проведена апробація методики та отримані результати свідчать про її ефективність, а подальше удосконалення може включати інтеграцію технологій штучного інтелекту для автоматичного прогнозування збоїв і підвищення адаптивності мережі.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Корчинський І. О., Фірман Н. А. Цифрова медицина: особливості та проблеми становлення в україні. Цифрова економіка та економічна безпека. 2022. № 1(01). С. 100–105. URL: https://doi.org/10.32782/dees.1-16.

2. Ткачов В.М. Аналіз методів забезпечення відмовостійкості оверлейних мереж / В.М. Ткачов, К.П. Гвоздецька // Проблеми інформатизації : тези доп. 8-ї міжнар. наук.-техн. конф., 26 - 27 листопада 2020 р., м. Черкаси, м. Харків, м. Баку, м. Бельсько-Бяла. Т. 1 / Черк. держ. технолог. ун-т [та ін.]. – Харків, 2020. – С. 44.

3. Batyuk L. V., Kizilova N. N. Analysis of Modern Databases and Information Systems For Processing Arrays of Medical Information. Scientific notes of Taurida National V.I. Vernadsky University. Series: Technical Sciences. 2022. № 5. С. 53–57. URL: https://doi.org/10.32782/2663-5941/2022.5/07.

4. Ткачов В.М. Програмний кластер для паралельної обробки великих обсягів даних / В.М. Ткачов, Ю.А. Кривобоков, К.П. Гвоздецька // Міжнародна наукова інтернет-конференція «Інформаційне суспільство: технологічні, економічні та технічні аспекти становлення (випуск 49)» / Збірник тез доповідей: випуск 19 (м. Тернопіль, 10 червня 2020 р.). – Тернопіль. – 2020. – 31-33 с.

5. Важинський Б., Ткачов В. Проблематика безпеки та критерії хнадійності мультихмарних середовищ. Системи управління, навігації та зв’язку. Збірник наукових праць. 2023. Т. 3, № 73. С. 75–78. URL: https://doi.org/10.26906/sunz.2023.3.075.

6. Petrushenko, D., & Bykova, T. (2023). Actual problems of building computer networks. Bulletin of V.N. Karazin Kharkiv National University, Series «Mathematical Modeling. Information Technology. Automated Control Systems», 60, 36-45. https://doi.org/10.26565/2304-6201-2023-60-04.

7. Li, He, Lu Yu, and Wu He. «The impact of GDPR on global technology development.» Journal of Global Information Technology Management 22.1 (2019): 1-6.

8. Gostin, Lawrence O., Laura A. Levit, and Sharyl J. Nass, eds. «Beyond the HIPAA privacy rule: enhancing privacy, improving health through research.» (2009).

9. Колпаков М.О., Петренко А.Б. Масштабування та посилення захисту даних веб-додатку відповідно до вимог стандартів PCI DSS, HIPAA/HITECH, FEDRAMP. Ukrainian Information Security Research Journal 20.4: 215-220.

10. Tkachov V.M. Providing information security in systems of business process management in the IAAS-vendor environment / V.M. Tkachov, S.O. Partyka, V.O. Lebediev // Сучасні напрями розвитку інформаційно-комунікаційних технологій та засобів управління: матеріали шостої міжнародної науково-технічної конференції. – Полтава: ПНТУ; Баку: ВА ЗС АР; Кіровоград: КЛА НАУ; Харків: ДП «ХНДІ ТМ», 2016. – С. 25.

11. Діденко Н.Г. Трансформація системи охорони здоров’я в умовах війни. П 68 Правові засади організації та здійснення публічної влади (2023): 146.

12. Стрєлкіна, А.А., Узун Д.Д. Забезпечення кібербезпеки медичних систем: виклики і рішення в контексті Інтернету речей. Радіоелектронні і комп’ютерні системи 1 (2017): 44-50.

13. Демченко І.С. Класифікація законодавства у сфері охорони здоров’я. Вчені записки Таврійського національного університету імені В.І. Вернадського. Серія: Юридичні науки. 2019. Том 30 (69) № 6. С. 7–13. URL: http://ir.librarynmu.com/handle/123456789/1655.

14. Yeh, Cheng-Ta, and Lance Fiondella. «Optimal redundancy allocation to maximize multi-state computer network reliability subject to correlated failures.» Reliability Engineering & System Safety 166 (2017): 138-150.

15. Аналіз показників надійності та доступності відмовостійкого кластеру / В. Є. Цилюрик, Л. О. Токар, В. В. Солоділов, Р. В. Муха // Інформаційно-комунікаційні технології та кібербезпека (ІКТК-2023) : матеріали дев’ятої Міжнародної науково-технічної конференції, 7 грудня 2023 р. – Харків : ХНУРЕ, 2023. – С. 76-79.

16. Tkachov V. Technology of Load Balancing in Anonymous Network Based on Proxy Nodes Cascade Platform / V. Tkachov, M. Hunko, M. Bondarenko, S. Artyomov // Четверта міжнародна науково-технічна конференція «Комп’ютерні та інформаційні системи і технології». Збірка наукових праць. Харків: ХНУРЕ. – 2020. – С. 82.

17. Міхнов Є. Д. Огляд технології балансування навантаження у міксованих VPN-ланцюгах / Є. Д. Міхнов ; наук. керівник к.т.н., доц. В.М. Ткачов // Радіоелектроніка та молодь у XXI столітті: матеріали 28-го Міжнар. молодіж. форуму, 16–18 квітня 2024 р. – Харків: ХНУРЕ, 2024. – Т. 5. – С. 34–37. – DOI : https://doi.org/10.30837/IYF.PCEIP.2024.034.

18. Недоступ Д. М. Аналіз і дослідження методів забезпечення відмовостійкості засобами маршрутизації в інфокомунікаційних мережах : пояснювальна записка до кваліфікаційної роботи здобувача вищої освіти на другому (магістерському) рівні, спеціальність 172 Телекомунікації та радіотехніка / Д. М. Недоступ ; М-во освіти і науки України, Харків. нац. ун-т радіоелектроніки. – Харків, 2024. – 69 с.

19. Демидов, А., & Даценко, І. (2023). Аварійне відновлення у хмарних мережах. Проблематика warm сценарію аварійного відновлення. Інфокомунікаційні та комп’ютерні технології, 2(04), 149-156. https://doi.org/10.36994/2788-5518-2022-02-04-17.

20. V. Tkachov, M. Hunko and V. Volotka, «Scenarios for Implementation of Nested Virtualization Technology in Task of Improving Cloud Firewall Fault Tolerance,» 2019 IEEE International Scientific-Practical Conference Problems of Infocommunications, Science and Technology (PIC S&T), Kyiv, Ukraine, 2019, pp. 759-763, doi: 10.1109/PICST47496.2019.9061473.

21. Chou, Eric, Michael Kennedy, and Mandy Whaley. Mastering Python Networking: Your one-stop solution to using Python for network automation, programmability, and DevOps. Packt Publishing Ltd, 2020.

22. Tkachov V.M. Automated Controllers Functioning Criteria in Content Distribution Systems / V.M. Tkachov, V.E. Savanevych // Scholars Journal of Engineering and Technology. - Volume-2: Issue-3A. - Apr-May; 2014. - Pp. 491-497.

23. Ткачов В.М. Хмарна система моніторингу пристроїв маршрутизації потоків даних в сенсорних мережах / В.М. Ткачов // Перша міжнародна науково-технічна конференція «Комп'ютерні та інформаційні системи і технології». Збірка наукових праць. Харків: ХНУРЕ. – 2017. – С. 32.

24. Vitalii Tkachov, Anna Budko, Kateryna Hvozdetska and Daryna Hrebeniuk. Method of Building Dynamic Multi-hop VPN Chains for Ensuring Security of Terminal Access Systems // IEEE International Scientific-Practical Conference Problems of Infocommunications, Science and Technology (PIC S&T): Kharkiv 06-09 oct. 2020, Kharkiv.

25. Ткачов В.М. Метод передачі даних в комп'ютерній мережі проміжного зберігання даних складної інформаційної системи / В.М. Ткачов // Системи управління, навігації та зв'язку. – Полтава: Полтавський національний технічний університет ім. Ю. Кондратюка, 2017. – № 3 (43). – С. 117-119.

26. Верховський І., Ткачов В. Методи побудови віртуальних тунелів extranet-систем. Scientific review. 2023. Т. 4, № 89. С. 22. URL: https://doi.org/10.26886/2311-4517.4(89)2023.2.

27. Tkachov, Vitalii & Tokariev, Volodymyr & Ilina, Iryna & Partyka, Stanislav. (2021). Modified Traveling Salesman Problem for a Group of Intelligent Mobile Objects and Method for Its Solving. International Journal of Electrical and Electronic Engineering & Telecommunications. 1-7. 10.18178/ijeetc.10.1.1-7.

28. Kovalenko Andriy Метод забезпечення живучості комп'ютерної мережі на основі vpn-тунелювання / Andriy Kovalenko, Heorhii Kuchuk, Vitalii Tkachov // Системи управління, навігації та зв'язку. Збірник наукових праць.

– Полтава: ПНТУ, 2021. – Т. 1 (63). – С. 90-95. – doi:https://doi.org/10.26906/SUNZ.2021.1.090.

29. Tkachov V., Mikhnov Ye. Analysis of Fault Tolerance Algorithms in Multisegment Networks / Збірник тез доповідей Дванадцятої міжнародної науково-технічної конференції «Проблеми інформатизації». Том 4: Секція 4. 21-22 листопада 2024 року. – Баку – Харків – Бельсько-Бяла. – С. 59.

30. Tkachov V., Mikhnov Ye. A Method for Enhancing the Resilience of Multisegment Corporate Computer Networks in Healthcare Institutions / Збірник тез доповідей Дванадцятої міжнародної науково-технічної конференції «Проблеми інформатизації». Том 4: Секція 4. 21-22 листопада 2024 року. – Баку – Харків – Бельсько-Бяла. – С. 60.