УДК 621.391

ДОСЛІДЖЕННЯ ПОКАЗНИКІВ НАДІЙНОСТІ ФРАГМЕНТУ ЛОКАЛЬНОЇ ІНФОКОМУНІКАЦІЙНОЇ МЕРЕЖІ

О.С. ЄРЕМЕНКО, В.О. ЛЕМЕШКО, В.О. КУРЕНКО
Харківський національний університет радіоелектроніки

Abstract *– Based on the analysis, it is established that to ensure and improve the reliability of information and communication networks (ICN), it is necessary to comprehensively involve the functionality of all layers of the Open Systems Interconnection reference model. The solutions of individual layers should be implemented systematically in different parts of the network and when protecting (backing up) different types of network elements - routers, links, and paths. The Cisco Packet Tracer simulator was used to design a reliable local information and communication network. At the level of the local network, which operated using Ethernet technology, the structural reliability was increased by introducing additional links between switches to create a strongly connected topology. The use of the STP protocol, namely its PVST+ and Rapid PVST versions, made it possible to ensure quick response to network failures of its elements - routers and communication links between them. The HSRP fault-tolerant routing protocol was configured to ensure access to WAN services. The results of the ICN testing confirmed its high reliability level during network uptime and in the face of possible failures. The article analyzes the reliability level of several network topologies. The analysis focused on the impact of the reliability level of individual links and structural redundancy on the probability of fault-free operation of connections between different network switches. The analysis results confirmed that introducing redundancy in the network topology increases ICN structural reliability. The obtained quantitative results allow us to justify the choice of a particular topology to ensure a given level of structural reliability. Based on the results, it is possible to develop recommendations for choosing a specific network topology depending on the state of the switches, their ports, and the requirements for the reliability level of the ICN in general.*

Анотація *– На основі проведеного аналізу встановлено, що для забезпечення та підвищення надійності інфокомунікаційних мереж (ІКМ) потрібно комплексно залучати функціонал всіх рівнів еталонної моделі взаємодії відкритих систем. Рішення окремих рівнів повинні реалізовуватись системно на різних ділянках мережі та при захисті (резервуванні) різних типів мережних елементів – маршрутизаторів, каналів та шляхів. За допомогою симулятора Cisco Packet Tracer спроєктована надійна локальна інфокомунікаційна мережа. На рівні локальної мережі, яка функціонувала з використання технології Ethernet, підвищення структурної надійності забезпечувалось на підставі введення додаткових каналів між комутаторами для створення сильнозв'язної топології. Використання протоколу STP, а саме його версій PVST+ та Rapid PVST, дозволило забезпечити швидке реагування мережі на відмови її елементів – маршрутизаторів та каналів зв'язку між ними. Для забезпечення відмовостійкого доступу до сервісів глобальної мережі у розділі було налаштовано протокол відмовостійкої маршрутизації HSRP. Результати тестування ІКМ підтвердили високий рівень її надійності як при безвідмовній роботі мережі, так і в умовах можливих відмов. У статті проведено аналіз рівня надійності множини мережних топологій. Аналіз стосувався впливу рівня надійності окремих каналів та структурної надлишковості на ймовірності безвідмовної роботи з'єднань між різними комутаторами мережі. Результати аналізу підтвердив, що введення надлишковості у топологію мережі призводить до підвищення рівня структурної надійності ІКМ. Отримані кількісні результати дозволяють обґрунтувати вибір тієї чи іншої топології ІКМ для забезпечення заданого рівня її структурної надійності. Ґрунтуючись на отриманих результатах, можна розробити рекомендації щодо вибору тієї чи іншої мережної топології в залежності від стану комутаторів, його портів та вимог щодо рівня надійності ІКМ взагалі.*

Вступ

Сучасна інфокомунікаційна мережа – це складна система технічних засобів та програмного забезпечення, людей та та споруд, які використовуються для передавання та приймання різних видів даних. Вони можуть об'єднувати кінцеві пристрої користувачів (комп'ютери, смартфони тощо), пристрої інтернету речей (Internet of Things, IoT), сервери та інші електронні засоби. Варто зазначити, що відповідно до моделі OSI (Open System Interconnection), функціонал інфокомунікаційні мережі розглядаються на декількох рівнях, кожен з яких відповідає за розв'язання певних задач щодо

передачі та обробки інформації за допомогою відповідних протоколів та механізмів управління трафіком [1-5].

Однією з важливих властивостей ІКМ є надійність. Під надійністю розуміють властивість мережі виконувати задані функції і підтримувати значення встановлених експлуатаційних показників протягом певного часу в заданих межах, що відповідає умовам використання та технічного обслуговування. Надійність є складовою такого більш загального терміну, як стійкість по відношенню до внутрішніх факторів, що впливають на ІКМ, наприклад, відмов та збоїв комунікаційного обладнання. У свою чергу надійність проявляє себе через такі властивості, як безвідмовність, відмовостійкість, довговічність, збереженість та ремонтопридатність (рис. 1) [6-12].

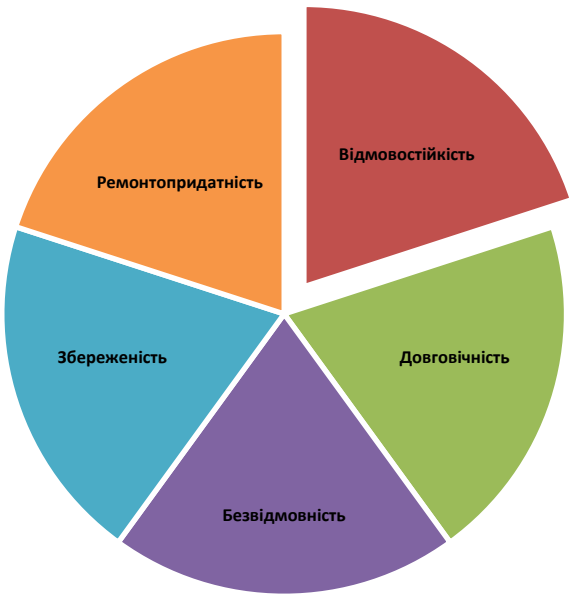

Рис. 1. Складові надійності

Безвідмовність – це властивість об'єкта виконувати функції протягом певного інтервалу часу. Довговічність – це властивість об'єкта виконувати необхідні функції до переходу у граничний стан при встановленій системі технічного обслуговування та ремонту. Ремонтопридатність – це властивість об'єкта бути пристосованим до підтримання та відновлення стану, в якому він здатний виконувати потрібні функції за допомогою технічного обслуговування та ремонту. Збережуваність – це властивість об'єкта зберігати значення параметрів, що характеризують здатність об'єкта виконувати необхідні функції. Відмовостійкість – це властивість об’єкту зберігати показники своєї ефективності на заданому рівні в умовах відмов комунікаційного обладнання [4-8]. При цьому під відмовою в ІКМ розуміється подія, після виникнення якої мережа або її елемент втрачає здатність виконувати свої функції із заданими показниками ефективності, наприклад, якості обслуговування (Quality of Service, QoS). До основних причин відмов (рис. 2) можна віднести [4, 5]:

– масштабні техногенні катастрофи, соціально-політичні та економічні чинники;

– людський чинник, пов'язаний з помилками людини-оператора та/або адміністратора мережі під час конфігурації обладнання та оновлення його програмного забезпечення (ПЗ) через його низький рівень кваліфікації, уваги або втому;

– зовнішні шкідливі втручання у роботу мережі з боку зловмисників;

– екологічні проблеми та катаклізми (повені, вулкани, сніжні лавини, селі тощо);

– апаратні збої у роботі мережного обладнання;

– збої мережного програмного забезпечення;

– проблеми з енергоживленням;

– перевантаження мережі.

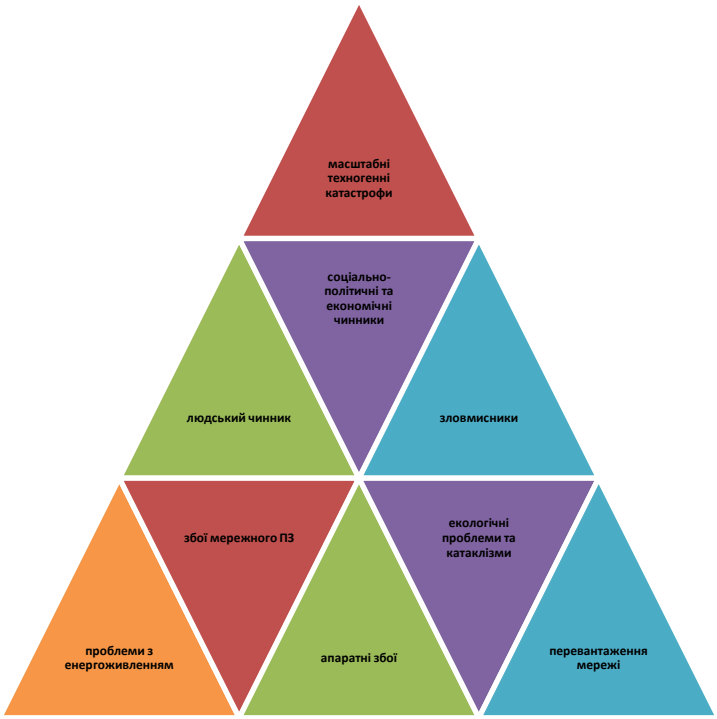

Рис. 2. Основні фактори відмов в ІКМ

Тому актуальним технологічним завданням у області інфокомунікацій є побудова ІКМ, які забезпечують високі значення показників надійності, відмовостійкості та якості обслуговування (Quality of Resilience, QoR). У даній статті пропонується дослідження, пов'язане із порівняльним аналізом рівня надійності локальної ІКМ для різних варіантів її структурної побудови.

I. Огляд та аналіз технологічних засобів підвищення надійності інфокомунікаційних мереж

Забезпечення високого рівня надійності ІКМ є складною задачею, що вимагає на практиці залучення цілісної системи технологічних рішень, які логічно відносяться до

різних рівнів моделі OSI. Відомо, що модель OSI — це концептуальна модель, що використовується для організації процесу передачі даних в інформаційних та комунікаційних системах, у тому числі і ІКМ. Ця модель складається з семи рівнів (рис. 3), кожен з яких відповідає за певну функціональність у процесі комунікації між пристроями [1, 2].

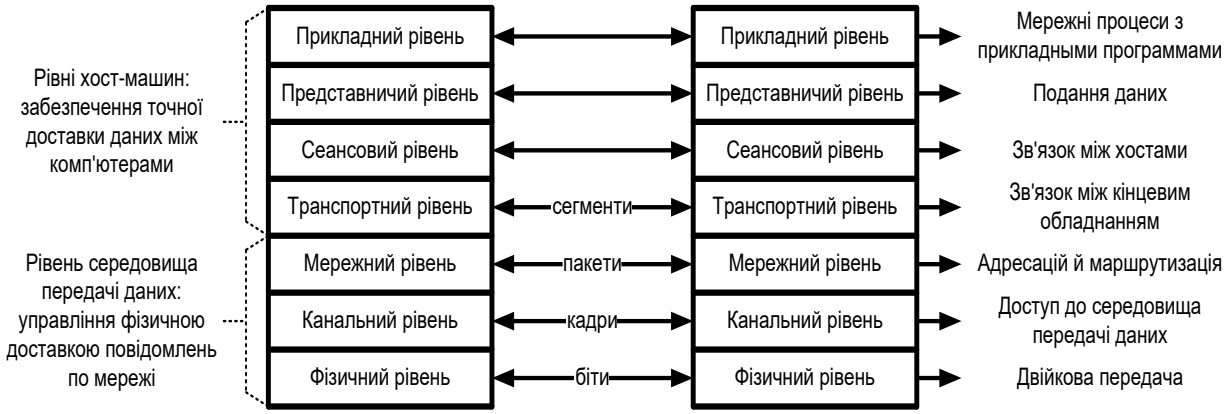

Рис. 3. Рівні моделі OSI

Функціональність трьох верхніх рівнів моделі OSI, як правило, реалізується засобами операційних систем кінцевих пристроїв (хост-машин). Ці рівні відповідають за забезпечення точної та безпомилкової (надійної) доставки даних між цими пристроями на базі мережних застосунків – множини сервісних протоколів (HTTP, FTP, SNMP тощо). Нижні чотири рівні називаються технологічно залежними, бо напряму залежать від типу комунікаційної технології, яка використовується в ІКМ. На цих рівнях також використовуються засоби забезпечення надійної передачі інформації на рівні сигналів (фізичний рівень), кадрів (канальний рівень), пакетів (мережний рівень) та сегментів (транспортний рівень).

Фізичний рівень – це нижній рівень моделі OSI, який відповідає за доставку даних (бітів) у фізичному середовищі передачі. Також фізичний рівень відповідає за електромагнітну сумісність, а саме за розподіл частот електромагнітного спектра, визначення потужності сигналу, аналогової смуги пропускання тощо. Надійність фізичного рівня є запорукою стабільного функціонування всієї мережі та мінімізації ризиків втрати даних чи відмов у роботі мережі. Це стосується забезпечення безпомилкової роботи апаратного забезпечення, кабельної інфраструктури та інших фізичних компонентів мережі.

Надійність фізичного рівня перш за все залежить від якості апаратного забезпечення та типу середовища, яке обрано для передачі. Використання високоякісних компонентів, які мають низький рівень відмов, дозволяє убезпечити мережу від бітових поломок та спотворень сигналів. Встановлення апаратури від надійних постачальників з якісним сервісним обслуговуванням також зменшує ймовірність виникнення проблем [1, 2]. На випадок аварійних ситуацій необхідно подбати про резервні канали

зв'язку та протоколи аварійного відновлення мережі. Необхідно також піклуватись про встановлення систем моніторингу стану апаратного забезпечення та кабельної інфраструктури, щоб вчасно реагувати на можливі несправності та мати змогу запобігти потенційному ускладненню проблеми.

Для забезпечення надійності також важливий вибір середовища передачі. До них належать мідний кабель, оптичне волокно та радіоефір (для безпроводових технологій). Кожен с цих типів середовищ передачі має свої переваги та недоліки щодо забезпечення надійної передачі інформації. Основною перевагою мідних кабелів над іншими середовищами передачі є висока міцність, що робить мідні кабелі захищеними від зовнішніх фізичних впливів. Окрім цього передача інформації по мідному кабелю гарантує досить високу швидкість зв'язку. Також значущою перевагою мідних кабелів можна назвати їх доступність та низьку вартість. До недоліків мідних кабелів, відносять обмежену довжину ділянок для передачі даних. Також до недоліків мідних кабелів відносять їх надмірну вагу та габарити, що ускладнює їх використання в деяких ситуаціях.

До переваг оптичних волокон відносять пропускну здатність, завдяки чому вони забезпечують високу швидкість передачі даних. Також однією з переваг оптичних волокон є низька вразливість до електромагнітних завад. Оптичні волокна майже не піддаються впливу електромагнітних хвиль, що робить їх обгрунтованим вибором для середовищ навіть з високим рівнем електромагнітного шуму. До недоліків оптичних мереж відносять їх відносно високу вартість. Оптичні волокна можуть бути значно дорожчими в установці та обслуговуванні порівняно зі звичайними мідними кабелями. Також оптичні кабелі вразливі до пошкоджень. Вони можуть пошкодитися під час установки або експлуатації, що призведе до відмов та втрати даних.

До переваг безпроводових технологій відносять відсутність проводової інфраструктури, а також мобільність (портативність) користувачів та їхніх кінцевих пристроїв. Завдяки безпроводовим рішенням ним можна підключатися до мережі практично з будь-якого місця в зоні покриття. До недоліків безпроводових ІКМ відносять їхню нижчу пропускну здатність у порівнянні з проводовими аналогами, наприклад, оптичними мережами. Також до недоліків безпроводових мереж відносять їх чутливість до зовнішніх впливів – завад та зловмисників, що у фінальному підсумку суттєво впливає на надійність надання сервісів з боку ІКМ.

Тому різні середовища передачі та комунікаційне обладнання знаходить своє використання на різних ділянках мережі – локальних мереж, доступу, розподілу інформації, глобальних мереж, хмар тощо в залежності від умов функціонування ІКМ та вимог щодо надійності, пропускної здатності, безпеки та мобільності.

Важливу роль у забезпеченні надійності ІКМ відіграють технології канального рівня OSI. Канальний рівень моделі OSI відповідає за організацію каналу зв'язку та передачу даних (у вигляді кадрів/фреймів) між вузлами, що перебувають в одній підмережі. Канальний рівень в залежності від типу використаної технології може забезпечувати надійну доставку кадрів між сусідніми пристроями. Якщо функцію надійної доставки кадрів технологія не підтримує, то ця функція перекладається на протоколи

біль високих рівнів, наприклад, на протокол транспортного рівня TCP (Transmission Control Protocol) [1, 2]. Протоколи канального рівня працюють над виявленням і виправленням помилок та керуванням потоком даних. Для забезпечення надійності канального рівня застосовуються контрольні суми, щоб виявляти пошкоджені пакети даних, а для відновлення втрачених даних за необхідності можуть застосовуватися коди Хеммінга або Ріда-Соломона.

Для надійної передачі інформації на канальному рівні велика увага приділяється побудові та використанню надійних мережних топологій (структур), створених множиною комутаторів. Для підвищення надійності та продуктивності локальних мереж (Local Area Network, LAN) для зв'язків між Ethernet-комутаторами можуть використовуватися кратні з'єднання або надлишкові канали.

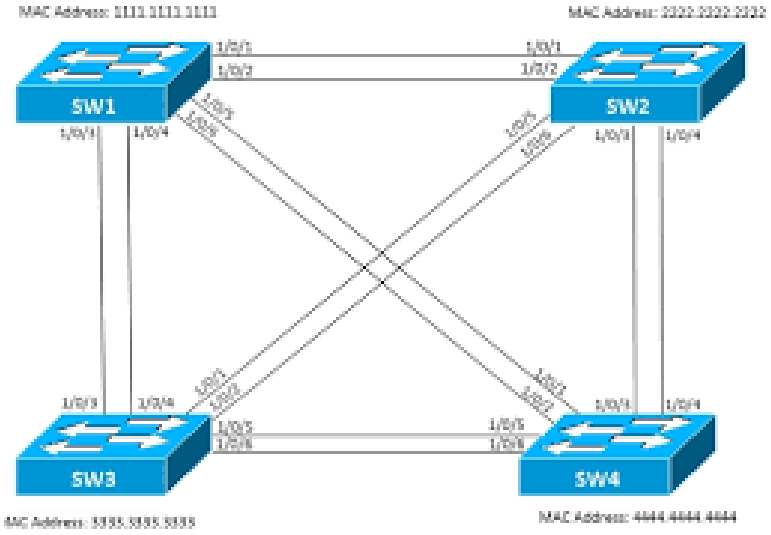

Рис. 4. Приклад створення локальної мережі з надлишковими зв'язками

Проте для запобігання та усунення петель кадрів у локальних мережах, що використовують технологію Ethernet, потрібно застосовувати протокол побудови остового дерева STP (Spanning Tree Protocol). Протокол STP створює остове дерево для передачі даних, забезпечуючи єдиний шлях між будь-якими двома комутаторами в мережі, що дозволяє усунути надлишкові шляхи і петлі. STP використовує алгоритм, що ґрунтується на мінімальному ідентифікаторі мосту (Bridge ID), щоб вибрати кореневий міст (Root Bridge), який буде основою дерева.

До переваг STP відносять його гнучкість до змін топології, а також покращення керованості трафіку у складних щодо зв'язності комутаторів мережних структурах. До недоліків протоколу STP відносять необхідність його налаштування, повільне відновлення після відмови зв'язку у разі використання стандартного STP, а також вразливість до дій зловмисника [13]. Взагалі протокол STP та його численні модифікації ефективно адаптуються під різні ситуації та практиці. У разі несправності обладнання або

зміни топології STP забезпечить відмовостійкість мережі, автоматично перебудує дерево мережі, не впливаючи при цьому на безперервність її роботи. До основних модифікацій цього протоколу відносять такі [13]:

- STP (стандарт IEEE 802.1D) – це оригінальна версія протоколу, який створює одне дерево для уникнення петель кадрів;

- RSTP (Rapid Spanning Tree Protocol) – це вдосконалена версія оригінального STP, яка забезпечує більш швидке відновлення мережі після відмови того чи іншого зв'язку (каналу) між комутаторами локальної мережі. RSTP здатний підвищити швидкість адаптації (збіжності) до декількох секунд на відміну від оригінального STP;

- PVST+ (Per VLAN Spanning Tree Plus) дозволяє кожній VLAN мати своє власне дерево, що позитивно впливає на балансування навантаження, але водночас вимагає більшої обчислювальної потужності комутаторів;

- MSTP (Multiple Spanning Tree Protocol), описаний у стандарті IEEE 802.1s (в подальшому включений у стандарт IEEE 802.1Q-2003) і також дозволяє створювати в одній мережі декілька незалежних дерев, що значно полегшує управління трафіком у великих LAN. Різні VLAN (Virtual Local Area Network) можуть використовувати різні дерева для балансування навантаження та забезпечення ефективного використання доступного мережного (канального) ресурсу. MSTP на відміну від PVST+ передбачає конфігурування необхідної кількості екземплярів, незалежно від числа VLAN на комутаторі;

- SPB (Shortest Path Bridging) є певною альтернативою сімейству протоколів Spanning Tree, які дозволяють використовувати тільки одне дерево (маршрут) пересилання кадрів до кореневого комутатора (root bridge) і блокують будь-які альтернативні шляхи. SPB активно використовує всі наявні маршрути між комутаторами, які мають однакову вартістю (equal cost multipathing). STP має швидку збіжність, а також вищі значення відмовостійкості та пропускної здатності, так як використовує ресурс всіх наявних шляхів між заданою парою комутаторів та балансує між ними навантаження.

Мережний рівень моделі OSI, що відповідає за адресацію мереж та пристроїв, а також за маршрутизацію пакетів від відправника до одержувача через одну або кілька підмереж. Для цього можуть використовуватись адреси IPv4 та IPv6. Також мережний рівень відповідає за фрагментацію, тобто розбиття великих пакетів на менші фрагменти для передачі через мережі, що мають обмеження на розмір пакетів, а також за збирання цих фрагментів на стороні отримувача [1, 2]. Надійність мережного рівня забезпечується на підставі адаптивної зміни маршрутів, коли певний мережний елемент відмовить. Стандартні протоколи IP-маршрутизації, такі як RIP (Routing Information Protocol), EIGRP (Enhanced Interior Gateway Routing Protocol), OSPF (Open Shortest Path First), IS-IS (Intermediate System to Intermediate System), BGP (Border Gateway Protocol), здатні адаптуватись до зміни стану мережі, виявляти проблемні маршрутизатори та канали та розраховувати маршрути, які не містять елементів мережі які відмовили [3].

Протоколи дистанційно-векторної маршрутизації оновлюють маршрути через певний період часу, який складає десятки секунд, 30 або 90 с для RIP та IGRP відповідно. Протоколи стану каналів, наприклад, OSPF та IS-IS, та оновлюють маршрути за вимогою, тобто при виявленні проблемної ситуації в ІКМ. При визначенні оптимального маршруту велике значення відводиться формуванню та використанню маршрутних метрик, але тільки протоколи IGRP/EIGRP та IS-IS у явному вигляді можуть враховувати при розрахунку метрик надійність інтерфейсів маршрутизаторів.

Додатковим засобом підвищення відмовостійкості ІКМ на мережному рівні OSI є використання технології швидкої перемаршрутизації (Fast ReRoute, FRR). Забезпечується відмовостійкість в межах FRR на підставі введення у ІКМ надлишковості на основі розрахунку, зберігання та наступного використання відразу і основного шляху (шляхів), і резервних. При FRR може забезпечуватись захист (резервування) вузла (маршрутизатора), каналу або маршруту взагалі [4, 5]. Прикладом подібного рішення у IP-мережі є протокол EIGRP [4, 5]. Він дозволяє визначати та зберігати у таблиці топології основні та резервні маршрути. При цьому час на перемикання трафіку з основного маршруту та резервний може складати 40-60 мс. За замовчуванням протокол EIGRP підтримує схему ненавантаженого («холодного») резерву, коли метрика основного шляху менша за метрику резервного. Проте у цьому протоколі закладена можливість використання і схеми навантаженого («гарячого») резерву, коли пакети одночасно передаються і за основним, і за резервними маршрутами, навіть якщо їхня метрика неоднакова.

У свою чергу, для захисту приграничних маршрутизаторів, інтерфейси яких для локальних мереж виконуються роль шлюзу за замовчуванням, використовуються протоколи відмовостійкої маршрутизації сімейства FHRP (First Hop Redundancy Protocol). Мета протоколів FHRP – це забезпечення відмовостійкості та надійності ІКМ на основі підвищення доступності доступність та безперервність інфокомунікаційних послуг. Функціональність протоколів FHRP дозволяє майже миттєво автоматично (без втручання адміністратора мережі) перемикати і навіть балансувати трафік з локальної мережі між множиною приграничних маршрутизаторів.

Прикладами протоколів відмовостійкої маршрутизації є такі рішення [4, 5]:

- Virtual Router Redundancy Protocol (VRRP);
- Hot Standby Router Protocol (HSRP);
- Gateway Load Balancing Protocol (GLBP);
- Common Address Redundancy Protocol (CARP).

Протоколи VRRP та HSRP не підтримують балансування навантаження між множиною приграничних маршрутизаторів, а протокол GLBP підтримує, що дозволяє реалізувати додатково схему захисту із «гарячим» резервуванням.

Транспортний рівень моделі OSI відповідає за забезпечення швидкої та надійної передачі сегментів між двома кінцевими пристроями (хостами) мережі, забезпечуючи цілісність і послідовність даних. З цією метою в IP-мережах використовуються два основних протоколи [1, 2, 13]:

- TCP (Transmission Control Protocol) – протокол управління передачею, який забезпечує надійну та гарантовану передачу сегментів у правильному порядку;

- UDP (User Datagram Protocol) – протокол датаграм користувача, який не забезпечує надійну передачу сегментів.

Протокол UDP використовується переважно для управління мультимедійними потоками, які не є чутливими до втрат пакетів. Але мультимедійним пакетам важливо забезпечити мінімальну затримку та джитер. Протокол TCP забезпечує більш надійну, навіть гарантовану доставку сегментів за UDP, так як на основі підтверджень контролює доставку сегментів та повторно надсилає втрачені сегменти.

TCP розбиває великі файли на сегменти для передачі та знову збирає їх на приймаючій стороні. Якщо сегмент загублений або пошкоджений під час передачі, TCP автоматично повторно пересилає його. Перед передачею даних TCP встановлює з'єднання між відправником і приймачем через процес трьохетапного рукостискання. Це дозволяє двом сторонам синхронізувати свої параметри і гарантувати готовність до передачі даних. Також протокол TCP відповідає за контроль потоку, тобто регулювання швидкості передачі даних, щоб уникнути перевантаження мережі та приймача. Також TCP використовує контрольні суми для перевірки цілісності даних. Пошкоджені сегменти повторно запитуються і пересилаються. TCP використовується в додатках, де важлива надійність і цілісність даних.

II. Опис налаштування фрагменту надійної ІКМ

Нехай відповідно до вихідних даних на проєктування надійна локальна мережа компанії охоплює чотири офіси (табл. 2.1), які розміщені на різних поверхах однієї будівлі, та повинна мати відмовостійкий доступ до глобальної мережі та її сервісів. Кожен з офісів містив по 20 персональних комп'ютерів (ПК). У загальному випадку замість деяких ПК могли бути налаштовані інші пристрої – хости мережі (локальні сервери, мережні принтери тощо). Налаштування віртуальних локальних мереж не передбачалося.

Таблиця 1. Характеристики офісів

Офіс	Кількість ПК	Діапазон IP-адрес	Шлюз за замовчуванням	Комутатор
A	20 (з 1 по 20)	192.168.1.1 – 192.168.1.20	192.168.1.253	Switch1
B	20 (з 21 по 40)	192.168.1.21 – 192.168.1.40		Switch2
C	20 (з 41 по 60)	192.168.1.41 – 192.168.1.60	192.168.1.254	Switch3
D	20 (з 61 по 80)	192.168.1.61 – 192.168.1.80		Switch4

Попередньо було виконано статичний розподіл IP-адрес між персональними комп'ютерами та іншими пристроями локальної мережі (рис. 5). IP-адреса мережі була спільною для всіх пристроїв – 192.168.1.0/24, що дозволяє суттєво нарощувати кількість ПК в ній, приблизно до 250. Бо з 256 доступних IP-адрес дві адреси виділенні на адреси мережі (192.168.1.0/24) та широкомовного розсилання пакетів

(192.168.1.255/24); дві IP-адреси треба виділити на фізичні інтерфейси пригранічних маршрутизаторів (Router1 та Router2); дві IP-адреси треба зарезервувати на IP-адреси двох віртуальних шлюзів за замовчуванням, створених за допомогою протоколу відмовостійкої маршрутизації HSRP.

Взаємодія між ПК кожного з офісів відбувається через відповідний комутатор (табл. 1): Switch1 – Switch4. Комутаторами виступали пристрої Cisco WS-C2960-24TT, у яких вистачало кількості портів для під'єднання необхідного числа ПК того чи іншого офісу та з'єднання між собою (рис. 5).

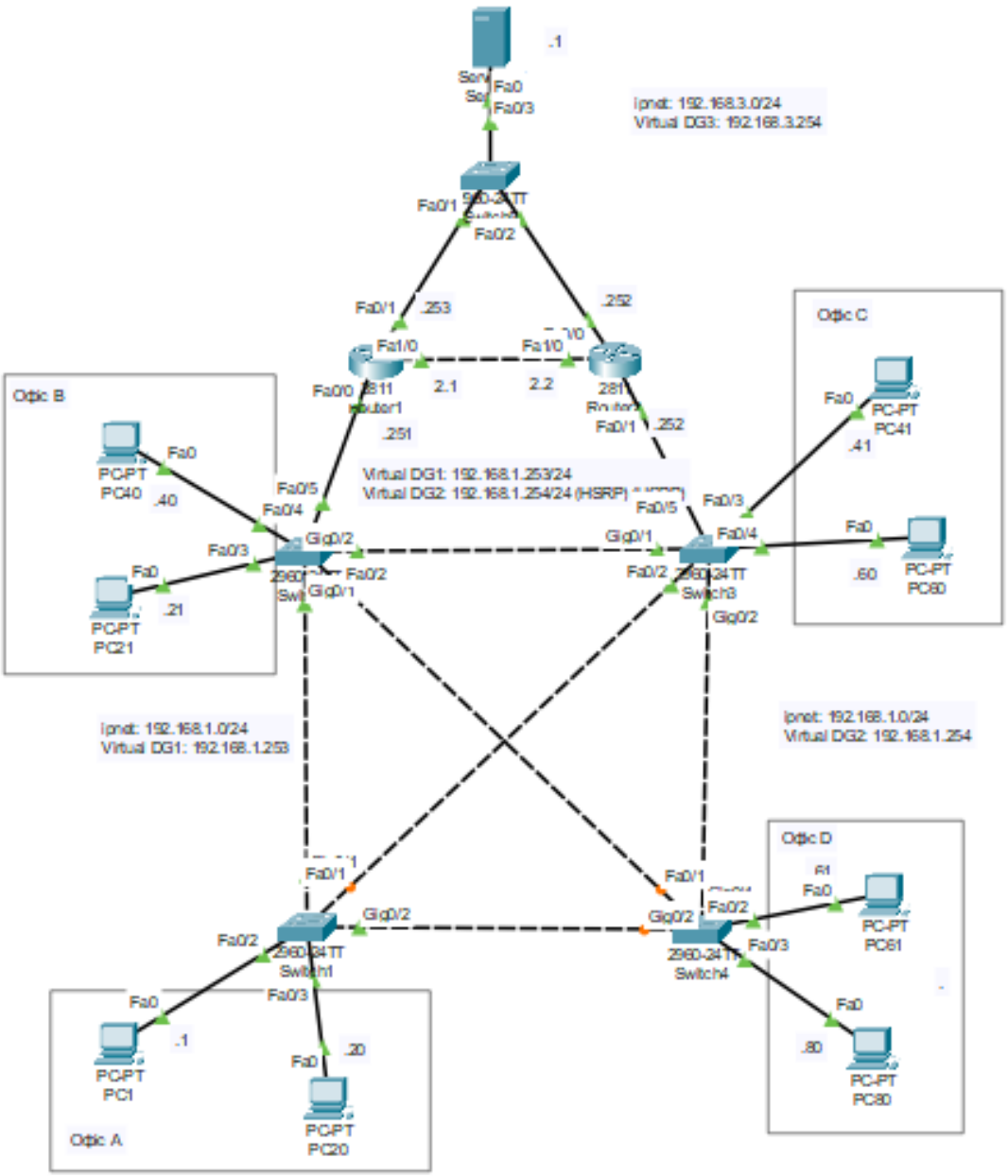

Рис. 5. Схема мережі, яка досліджувалась

Для доступу ПК до глобальної мережі та її сервісів використовувалися два маршрутизатора Cisco 2811 (табл. 1), які мали достатню кількість інтерфейсів для під'єднання комутаторів проєктованої локальної мережі, для взаємодії між собою та для з'єднання з пристроями інших мереж. Роль пристроїв віддаленої мережі покладалась на комутатор Switch5 та сервер Server0 (рис. 5). Ця мережа мала IP-адресу 192.168.3.0/24. Сервер Server0 (рис. 5) також був під'єднаний через комутатор Switch5 до маршрутизаторів за відмовостійкою схемою.

Для забезпечення максимальної надійності локальної мережі розглядалися різноманітні схеми з'єднання комутаторів. На рис. 5 представлена повнозв'язна схема мережі, коли кожен з комутаторів був з'єднаний з усіма іншими комутаторами локальної мережі. Показники надійності порівнювальних схем щодо варіантів з'єднання комутаторів мережі досліджувались у наступному розділі статті. На обраних комутаторах за замовчуванням було активовано версію протоколу STP – PVST+. Цей протокол забезпечував високу конвергенцію рішень щодо побудови остова на схемі мережі (рис. 5) з врахуванням метрик та пріоритетів портів. Кореневим комутатором було налаштовано комутатор Switch2 через його ключове положення по відношенню до інших комутаторів (офісів) та маршрутизаторів (рис. 6). Всі порти цього комутатора знаходяться у режимі FWD, тобто можуть передавати кадри (рис. 6 б).

```
Switch1#sh spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32769
             Address     000D.BD88.0332
             Cost        4
             Port        25(GigabitEthernet0/1)
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
             Address     0060.5C58.9824
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/2            Desg FWD 19        128.2    P2p
Fa0/3            Desg FWD 19        128.3    P2p
Fa0/1            Altn BLK 19        128.1    P2p
Gi0/2            Desg FWD 4         128.26   P2p
Gi0/1            Root FWD 4         128.25   P2p
```

а) Switch1

```
Switch2#sh span
Switch2#sh spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32769
             Address     000D.BD88.0332
             This bridge is the root
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
             Address     000D.BD88.0332
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/4            Desg FWD 19        128.4    P2p
Fa0/2            Desg FWD 19        128.2    P2p
Fa0/3            Desg FWD 19        128.3    P2p
Fa0/5            Desg FWD 19        128.5    P2p
Gi0/1            Desg FWD 4         128.25   P2p
Gi0/2            Desg FWD 4         128.26   P2p
```

б) Switch2

```
Switch3#sh spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32769
             Address     000D.BD88.0332
             Cost        4
             Port        25(GigabitEthernet0/1)
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
             Address     0030.A34D.0158
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/3            Desg FWD 19        128.3    P2p
Fa0/2            Desg FWD 19        128.2    P2p
Fa0/4            Desg FWD 19        128.4    P2p
Fa0/5            Desg FWD 19        128.5    P2p
Gi0/2            Desg FWD 4         128.26   P2p
Gi0/1            Root FWD 4         128.25   P2p
```

в) Switch3

```
Switch4#sh spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32769
             Address     000D.BD88.0332
             Cost        8
             Port        25(GigabitEthernet0/1)
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
             Address     00D0.583C.2C41
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Gi0/1            Root FWD 4         128.25   P2p
Gi0/2            Altn BLK 4         128.26   P2p
Fa0/2            Desg FWD 19        128.2    P2p
Fa0/1            Altn BLK 19        128.1    P2p
Fa0/3            Desg FWD 19        128.3    P2p
```

г) Switch4

Рис. 6. Перегляд характеристик комутаторів локальної мережі та їхньої ролі у побудованому остові

Для прикладу на рис. 6 показано стан комутатора Switch4, у якому частина портів при побудові остова була вимкнена (блокована, BLK). Проте кожен з цих портів є альтернативним до використання (Altn), тобто може швидко увімкнутись при побудові оновленого остова у випадку відмови того чи іншого елемента локальної мережі. Таким чином, відповідно до результатів перевірки стану локальної мережі вона працює використовує остов Switch1-Switch2- Switch3-Switch4. У випадку відмови, наприклад, порту G0/2 на Switch3, за яким він з'єднується з Switch4, остов мережі перебудується на новий варіант: Switch4-Switch1- Switch2-Switch3, що можна відстежити за зміною стану комутаторів Switch3 та Switch4 (рис. 7).

```
Switch3#sh spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32769
             Address     000D.BD88.0332
             Cost        4
             Port        25(GigabitEthernet0/1)
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
             Address     0030.A34D.0158
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/3            Desg FWD 19        128.3    P2p
Fa0/2            Desg FWD 19        128.2    P2p
Fa0/4            Desg FWD 19        128.4    P2p
Fa0/5            Desg FWD 19        128.5    P2p
Gi0/1            Root FWD 4         128.25   P2p
```

а) Switch3

```
Switch4#sh spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32769
             Address     000D.BD88.0332
             Cost        8
             Port        26(GigabitEthernet0/2)
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
             Address     00D0.583C.2C41
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Gi0/2            Root FWD 4         128.26   P2p
Fa0/2            Desg FWD 19        128.2    P2p
Fa0/1            Altn BLK 19        128.1    P2p
Fa0/3            Desg FWD 19        128.3    P2p
```

б) Switch4

Рис. 7. Перегляд характеристик комутаторів Switch3 та Switch4 та їхньої ролі у оновленому остові

За допомогою протоколу STP досягається підтримка багатозв'язних топологій для локальних мереж, які працюють відповідно до технології Ethernet та її численних модифікацій. Продемонстровано, що під час відмови елемента (каналу) мережі, протокол PVST+ автоматично (без втручання адміністратора мережі) відновив працездатність мережі. Це відбулося шляхом побудови оновленого остова мережі, тобто без використання мережного елементу, який відмовив. Процес оновлення займає близько десяти секунд. Для підвищення часу реакції мережі на відмови доцільно використовувати ще одну модифікацію протоколу STP, а саме Rapid PVST на кожному комутаторі локальної мережі. Експериментально встановлено, що час оновлення остову знизився приблизно в три рази, що дозволяє пропорційно знизити рівень втрат кадрів, що передаються мережею. Для підвищення надійності та пропускної здатності мережі одночасно необхідно використовувати на комутаторах агрегування портів. У цьому випадку надмірність у мережу вводиться на рівні підвищення кратності зв'язків (каналів) між комутаторами (рис. 8) за наявності вільних портів.

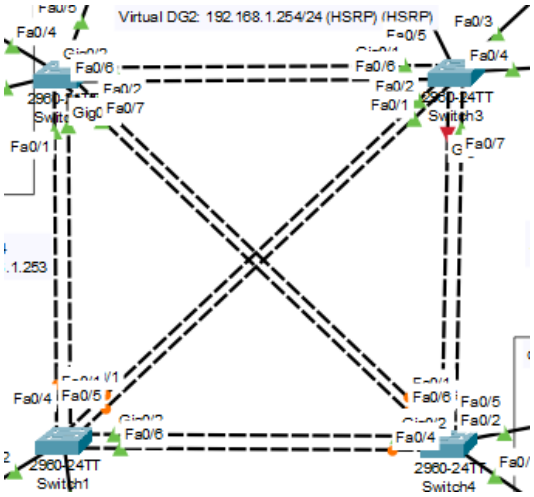

Рис. 8. Фрагмент локальної мережі з агрегуванням портів на комутаторах

Для забезпечення відмовостійкого доступу ПК локальної мережі до сервісів глобальної мережі пропонується реалізувати схему захисту шлюзу за замовчуванням. Для цього в межах схеми (рис. 5) потрібно використовувати не один, а два (а за необхідністю і більше) приграничних маршрутизаторів, до яких під'єднуються комутатори локальної мережі. Саме інтерфейси цих приграничних маршрутизаторів (Router1 та Router2) мають виконувати функції шлюзу за замовчуванням при налаштуванні IP-адресації на ПК локальної мережі. Тому у роботі запропоновано локальну мережу з'єднувати з приграничними маршрутизаторами не через один комутатор, а через два (Switch2 та Switch3), що вже підвищить надійність мережі, так як ПК отримають доступ до глобальної мережі навіть у випадку відмови одно з цих комутаторів (рис. 5).

При подальшому підвищенні відмовостійкості доступу ПК до глобальної мережі можуть використовуватися декілька стандартних рішень. Перше рішення полягає у тому, щоб частина ПК, наприклад, офісів A та B, використовувала як шлюз за замовчуванням IP-адресу відповідного інтерфейсу (Fa0/0) маршрутизатора Router1, а інша частина ПК, наприклад, офісів C та D, з цією метою використовувала інтерфейс Fa0/1 маршрутизатора Router2 (рис. 5). Подібне рішення досить просте в реалізації, проте у випадку відмови одно з маршрутизаторів блокованою все ж залишиться певна кількість ПК. У наведеному випадку – це ПК двох офісів: або A та B, або C та D.

Друге рішення базується на використанні протоколів відмовостійкої маршрутизації сімейства FHRP – VRRP, HSRP або GLBP, які аналізувалися у першому розділі даної роботи. Особливістю використання кожного з цих протоколів є те, що потрібно провести на приграничних маршрутизаторах, інтерфейси яких об'єднуються в віртуальний шлюз за замовчуванням, додаткові налаштування. Після цього на кожному ПК локальної мережі потрібно налаштувати як шлюз за замовчуванням IP-адресу віртуальний шлюзу, попередньо сконфігурованого на приграничних маршрутизаторах. У цьому випадку протоколи VRRP та HSRP [4, 5] будуть направляти пакети від усіх ПК локальної мережі на маршрутизатор, який виконує функції основного шлюзу. А при

його відмові – на маршрутизатор, який виконує функції резервного. Тобто у такому разі балансування (розподіл) навантаження між приграничними маршрутизаторами підтримуватися не буде. Протокол GLBP складніший у налаштуванні та підтримується лише на Cisco-маршрутизаторах. Однак він підтримує декілька схем балансування навантаження.

У даній роботі відмовостійкий доступ буде забезпечено з використанням протоколу HSRP з додатковими налаштуваннями для підтримки штучного балансування пакетів між приграничними маршрутизаторами. З цією метою були проведено ряд налаштувань. На рис. 2.5 показано результати налаштування IP-адрес на інтерфейсах маршрутизаторів Router1 та Router2, як наведено на рис. 9.

```
Router1#sh ip inter bri
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/0        192.168.1.251   YES manual up                    up
FastEthernet0/1        192.168.3.253   YES manual up                    up
FastEthernet1/0        192.168.2.1     YES manual up                    up
Vlan1                  unassigned      YES unset  administratively down down
Router1#
```

а) Router1

```
Router2#sh ip inter bri
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/0        192.168.3.252   YES manual up                    up
FastEthernet0/1        192.168.1.252   YES manual up                    up
FastEthernet1/0        192.168.2.2     YES manual up                    up
Vlan1                  unassigned      YES unset  administratively down down
```

б) Router2

Рис. 9. Результати налаштування IP-адрес на інтерфейсах маршрутизаторів Router1 та Router2

Далі на кожному з маршрутизаторів налаштовувалось три standby-групи. Перша і друга standby-групи створювалися на інтерфейсах Router1 та Router2, які знаходилися у підмережі 192.168.1.0/24, а третя – у підмережі 192.168.3.0/24. На рис. 10 показано приклад налаштування першої та другої standby-групи на маршрутизаторах Router1 та Router2.

```
Router1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router1(config)#inter fa0/0
Router1(config-if)#standby version 2
Router1(config-if)#standby 1 ip 192.168.1.253
Router1(config-if)#
%HSRP-6-STATECHANGE: FastEthernet0/0 Grp 1 state Init -> Init

Router1(config-if)#standby 1 priority 120
Router1(config-if)#
%HSRP-6-STATECHANGE: FastEthernet0/0 Grp 1 state Speak -> Standby

%HSRP-6-STATECHANGE: FastEthernet0/0 Grp 1 state Standby -> Active

Router1(config-if)#standby 1 preempt
Router1(config-if)#standby 2 ip 192.168.1.254
Router1(config-if)#
%HSRP-6-STATECHANGE: FastEthernet0/0 Grp 2 state Init -> Init

Router1(config-if)#standby 2 priority 50
%HSRP-6-STATECHANGE: FastEthernet0/0 Grp 2 state Speak -> Standby

%HSRP-6-STATECHANGE: FastEthernet0/0 Grp 2 state Standby -> Active

Router1(config-if)#standby 2 preempt
Router1(config-if)#
%HSRP-6-STATECHANGE: FastEthernet0/0 Grp 2 state Speak -> Standby
```

а) Router1

```
Router2(config)#inter fa0/1
Router2(config-if)#standby version 2
Router2(config-if)#standby 1 192.168.1.253
                             ^
% Invalid input detected at '^' marker.

Router2(config-if)#standby 1 ip 192.168.1.253
Router2(config-if)#
%HSRP-6-STATECHANGE: FastEthernet0/1 Grp 1 state Init -> Init

Router2(config-if)#standby 1 pri
%HSRP-6-STATECHANGE: FastEthernet0/1 Grp 1 state Spea
Router2(config-if)#standby 1 priority 50
Router2(config-if)#standby 1 preempt
Router2(config-if)#standby 2 ip 192.168.1.254
Router2(config-if)#
%HSRP-6-STATECHANGE: FastEthernet0/1 Grp 2 state Init -> Init

Router2(config-if)#standby 2 priority 120
Router2(config-if)#standby 2 preempt
Router2(config-if)#
 %HSRP-6-STATECHANGE: FastEthernet0/1 Grp 2 state Standby -> Active
```

б) Router2

Рис. 10. Налаштування standby-груп на маршрутизаторах Router1 та Router2

Пріоритети на інтерфейсах маршрутизаторів Router1 та Router2 задавались таким чином, щоб Router1 був основним (Active) шлюзом за замовчуванням для тих ПК (табл. 1), у яких як шлюз вказувалась віртуальна адреса 192.168.1.253 (перша standby-група). Цей же маршрутизатор Router2 був резервним (Standby) шлюзом за замовчуванням для тих ПК (табл. 1), у яких як шлюз вказувалась віртуальна адреса 192.168.1.254 (друга standby-група). Пріоритет інтерфейсу F0/1 на маршрутизаторі Router2 мав вище значення (120), а ніж інтерфейсу F0/0 на маршрутизаторі Router1 для другої standby-групи, тому у цій групі саме Router2 був основним (Active), а Router1 – резервним (Standby). Це можна перевірити за даними наведеними на рис. 11.

```
Router1#sh standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State    Active          Standby         Virtual IP
Fa0/0       1    120 P Active   local           192.168.1.252   192.168.1.253
Fa0/0       2    50  P Standby  192.168.1.252   local           192.168.1.254
Fa0/1       3    50  P Standby  192.168.3.252   local           192.168.3.254
Router1#
```

а) Router1

```
Router2#sh standby bri
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State    Active          Standby         Virtual IP
Fa0/0       3    120 P Active   local           192.168.3.253   192.168.3.254
Fa0/1       1    50  P Standby  192.168.1.251   local           192.168.1.253
Fa0/1       2    120 P Active   local           192.168.1.251   192.168.1.254
Router2#
```

б) Router2

Рис. 11. Перевірка стану налаштувань standby-груп на маршрутизаторах Router1 та Router2

Більш деталізована інформації про стан налаштувань standby-груп на маршрутизаторах Router1 та Router2 представлено на рис. 12.

```
Router1#sh standby
FastEthernet0/0 - Group 1 (version 2)
  State is Active
    7 state changes, last state change 00:21:45
  Virtual IP address is 192.168.1.253
  Active virtual MAC address is 0000.0C9F.F001
    Local virtual MAC address is 0000.0C9F.F001 (v2 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 1.029 secs
  Preemption enabled
  Active router is local
  Standby router is 192.168.1.252
  Priority 120 (configured 120)
  Group name is hsrp-Fa0/0-1 (default)
FastEthernet0/0 - Group 2 (version 2)
  State is Standby
    10 state changes, last state change 00:27:43
  Virtual IP address is 192.168.1.254
  Active virtual MAC address is 0000.0C9F.F002
    Local virtual MAC address is 0000.0C9F.F002 (v2 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 2.626 secs
  Preemption enabled
  Active router is 192.168.1.252, priority 120 (expires in 8 sec)
    MAC address is 0000.0C9F.F002
  Standby router is local
  Priority 50 (configured 50)
  Group name is hsrp-Fa0/0-2 (default)
FastEthernet0/1 - Group 3
  State is Standby
    9 state changes, last state change 00:35:33
  Virtual IP address is 192.168.3.254
  Active virtual MAC address is 0000.0C07.AC03
    Local virtual MAC address is 0000.0C07.AC03 (v1 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 0.585 secs
  Preemption enabled
  Active router is 192.168.3.252, priority 120 (expires in 7 sec)
    MAC address is 0000.0C07.AC03
  Standby router is local
  Priority 50 (configured 50)
  Group name is hsrp-Fa0/1-3 (default)
Router1#
```

а) Router1

```
Router2#sh standby
FastEthernet0/0 - Group 3
  State is Active
    3 state changes, last state change 00:35:00
  Virtual IP address is 192.168.3.254
  Active virtual MAC address is 0000.0C07.AC03
    Local virtual MAC address is 0000.0C07.AC03 (v1 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 1.551 secs
  Preemption enabled
  Active router is local
  Standby router is 192.168.3.253, priority 50 (expires in 6 sec)
  Priority 120 (configured 120)
  Group name is hsrp-Fa0/0-3 (default)
FastEthernet0/1 - Group 1 (version 2)
  State is Standby
    5 state changes, last state change 00:25:49
  Virtual IP address is 192.168.1.253
  Active virtual MAC address is 0000.0C9F.F001
    Local virtual MAC address is 0000.0C9F.F001 (v2 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 1.497 secs
  Preemption enabled
  Active router is 192.168.1.251
  Standby router is local
  Priority 50 (configured 50)
  Group name is hsrp-Fa0/1-1 (default)
FastEthernet0/1 - Group 2 (version 2)
  State is Active
    5 state changes, last state change 00:27:09
  Virtual IP address is 192.168.1.254
  Active virtual MAC address is 0000.0C9F.F002
    Local virtual MAC address is 0000.0C9F.F002 (v2 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 0.447 secs
  Preemption enabled
  Active router is local
  Standby router is 192.168.1.251, priority 50 (expires in 8 sec)
  Priority 120 (configured 120)
  Group name is hsrp-Fa0/1-2 (default)
Router2#
```

б) Router2

Рис. 12. Деталізована перевірка стану standby-груп на маршрутизаторах Router1 та Router2

На рис. 11 та 12 зазначено, що на інтерфейсах маршрутизаторів Router1 (F0/1) та Router2 (F0/0) також було налаштовано третю standby-групу. Вона використовувалась для підвищення відмовостійкості підключення серверу Server0 до глобальної мережі (рис. 5). У цьому випадку Router2 виконував функцію основного (Active) шлюзу за замовчування, а маршрутизатор Router2 – резервного (Standby). Взагалі протоколи IP-маршрутизації для даної схеми (рис. 5) мережі налаштовувати не потрібно. Проте для передачі пакетів між маршрутизаторами можна додатково налаштувати статичні маршрути (рис. 13).

```
Router2(config)#
Router2(config)#ip route 192.168.1.0 255.255.255.0 192.168.2.1
Router2(config)#
```

Рис. 13. Приклад налаштування статичного маршруту від маршрутизатора Router2 до мережі 192.168.1.0/24 через маршрутизатор Router1

Статичний маршрут, налаштований на рис. 13 є резервним рішенням на той випадок, коли відмовить інтерфейс на F0/1 маршрутизатора Router2, а пакети від сервера Server0 до ПК мережі 192.168.1.0/24 передавати потрібно. Якщо зазначений інтерфейс буде працездатний, то пакети будуть передаватись через нього, а не за статич-

ним маршрутом. Причина полягає у тому, що статичний маршрут має адміністративну відстань 1, що є більшим значенням за 0, яке відповідає адміністративній відстані рішення «directly connected».

У роботі проводилось тестування мережі з метою аналізу рівня її надійності та відмовостійкості при виході з ладу елементів ІКМ. На рис. 14 продемонстровано результати успішної перевірки працездатності з'єднання між першим ПК (офіс А) та сервером Server0. Всі чотири пакети, які використовувались у ході тестування, були успішно передані та отримано підтвердження про їхню доставку.

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.3.1

Pinging 192.168.3.1 with 32 bytes of data:

Reply from 192.168.3.1: bytes=32 time<1ms TTL=127
Reply from 192.168.3.1: bytes=32 time=1ms TTL=127
Reply from 192.168.3.1: bytes=32 time<1ms TTL=127
Reply from 192.168.3.1: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.3.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>tracert 192.168.3.1

Tracing route to 192.168.3.1 over a maximum of 30 hops:

  1    0 ms      0 ms      0 ms      192.168.1.251
  2    0 ms      0 ms      0 ms      192.168.3.1

Trace complete.

C:\>
```

Рис. 14. Результати успішної перевірки працездатності з'єднання між першим ПК (офіс А) та сервером Server0

Відповідно до проведених налаштувань (рис. 2.7) для ПК офісу А як шлюз за замовчуванням виступав віртуальний шлюз з IP-адресою 192.168.1.253, тобто маршрутизатор Router1. Саме його фізичний інтерфейс F0/0 з IP-адресою 192.168.1.251 було використано під час виконання команди tracert (рис. 14).

При перевірці працездатності з'єднання між вісімдесятим ПК (офіс D) та сервером Server0 було встановлено (рис. 15), що всі чотири пакети були успішно передані за маршрутом, який проходив через Router2. Ці результати підтверджують факт балансування навантаження між приграничними маршрутизаторами при передачі пакетів від ПК локальної мережі.

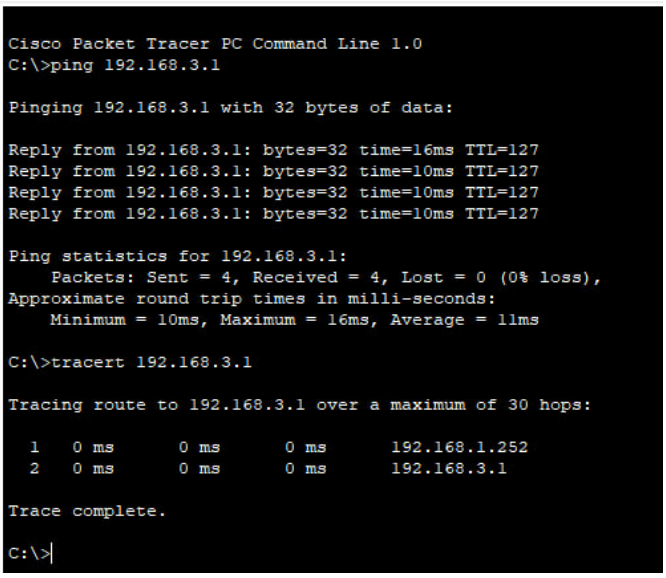

Рис. 15. Результати успішної перевірки працездатності з'єднання між вісімдесятим ПК (офіс D) та сервером Server0

На рис. 16 продемонстровано результати успішної перевірки працездатності з'єднання між першим ПК (офіс A) та сервером Server0 у разі відмови інтерфейсу F0/0 на маршрутизаторі Router1. Всі чотири пакети, які використовувались у ході тестування, були успішно передані. Пакети передавались через резервний маршрутизатор Router2, через його інтерфейс F0/1. Саме цей маршрутизатор перебирав на себе функції Active-маршрутизатора.

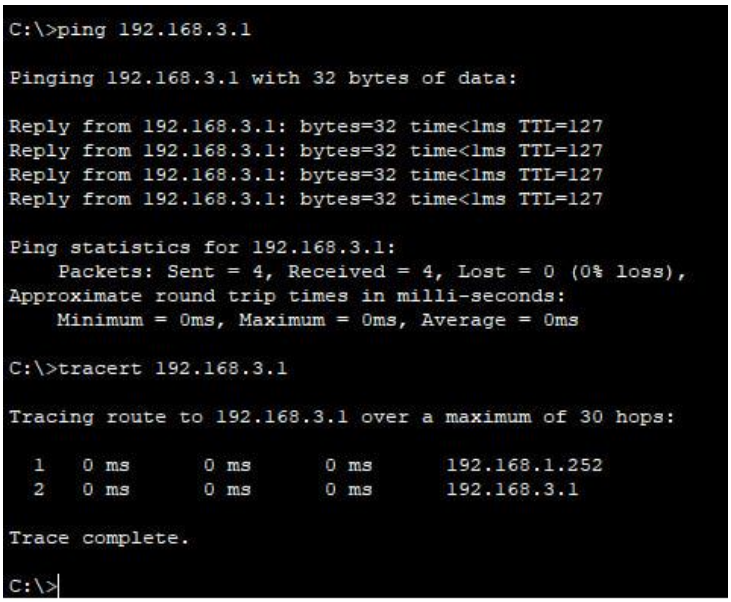

Рис. 16. Результати успішної перевірки працездатності з'єднання між першим ПК (офіс A) та сервером Server0 у разі відмови інтерфейсу F0/0 на маршрутизаторі Router1

Аналогічна ситуація спостерігалася у разі відмови інтерфейсу F0/1 на маршрутизаторі Router2. Пакети від вісімдесятого ПК (офіс D) успішно передавались через резервний шлюз – маршрутизатор Router1 (рис. 17). Підтвердження у зворотному напрямку до вісімдесятого ПК передавались через Router2 та Router1 за допомогою попередньо налаштованого статичного маршруту (рис. 13).

```
C:\>ping 192.168.3.1

Pinging 192.168.3.1 with 32 bytes of data:

Reply from 192.168.3.1: bytes=32 time<1ms TTL=126
Reply from 192.168.3.1: bytes=32 time<1ms TTL=126
Reply from 192.168.3.1: bytes=32 time<1ms TTL=126
Reply from 192.168.3.1: bytes=32 time<1ms TTL=126

Ping statistics for 192.168.3.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>tracert 192.168.3.1

Tracing route to 192.168.3.1 over a maximum of 30 hops:

  1    0 ms      0 ms      0 ms      192.168.1.251
  2    0 ms      0 ms      0 ms      192.168.3.1

Trace complete.
```

Рис. 17. Результати успішної перевірки працездатності з'єднання між вісімдесятим ПК (офіс D) та сервером Server0 у разі відмови інтерфейсу F0/1 на маршрутизаторі Router2

III. Аналіз показників структурної надійності різних мережних рішень

Математична модель розрахунку показників структурної надійності інфокомунікаційної мережі

У процесі аналізу різних підходів до оцінки рівня структурної надійності ІКМ була обрана математична модель, яка представлена у роботах [15-18]. Використання цієї моделі дозволяє проаналізувати різні мережні топології, які містять як нескладні послідовні та паралельні з'єднання елементів ІКМ, так і більш складні т.з. містки. Нехай V – кількість каналів зв'язку в ІКМ загалом;

p_i – імовірність безвідмовної роботи i-го каналу ІКМ ($i = \overline{1,V}$);

q_i – імовірність відмови i-го каналу ІКМ ($i = \overline{1,V}$).

Тоді для кожного каналу зв'язку ІКМ буде справедливою така формула:

$$p_i + q_i = 1 \ (i = \overline{1,V}). \quad (1)$$

Розглянемо приклади мережних топологій локальної ІКМ, яка проєктувалась у другому розділі. На рис. 18 зображену схему, де комутатори К1, К2, К3 та К4 з'єднані за принципом остова послідовно. Біля кожного каналу вказано його умовний номер.

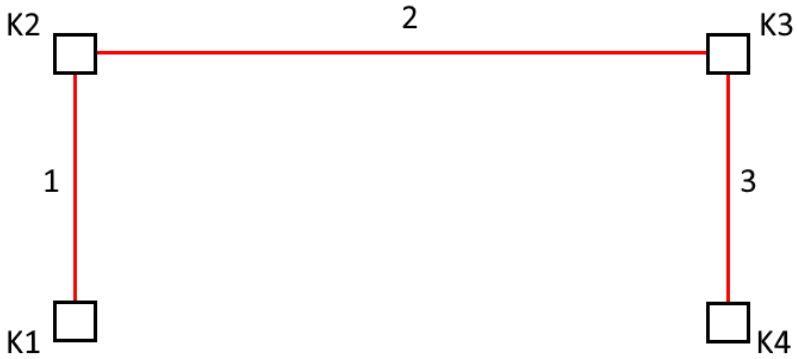

Рис. 18. Топологія ІКМ з послідовним з'єднанням комутаторів

Для розрахунку ймовірності безвідмовної роботи з'єднання комутаторів К1 та К4 (P_{1-4}) можна використати формулу:

$$P_{1-4} = p_1 p_2 p_3 \ . \tag{2}$$

Тоді ймовірність відмови з'єднання між комутаторами К1 та К4 (Q_{1-4}) можна розрахувати відповідно до формули:

$$Q_{1-4} = 1 - P_{1-4}. \tag{3}$$

Для розрахунку ймовірності безвідмовної роботи з'єднання комутаторів К1 та К2 (P_{1-2}) можна використати формулу:

$$P_{1-2} = p_1. \tag{4}$$

Ймовірність відмови з'єднання між комутаторами К1 і К2 (Q_{1-2}) можна розраховувати відповідно до формули:

$$Q_{1-2} = 1 - P_{1-2}. \tag{5}$$

Для розрахунку ймовірності безвідмовної роботи з'єднання комутаторів К1 і К3 (P_{1-3}) можна використати формулу:

$$P_{1-3} = p_1 p_2. \tag{6}$$

Тоді ймовірність відмови з'єднання між комутаторами К1 і К3 (Q_{1-3}) можна розрахувати відповідно до формули:

$$Q_{1-3} = 1 - P_{1-3}. \tag{7}$$

На рис. 19 зображену схему, де комутатори К1, К2, К3 та К4 з'єднані за топологією "кільце". Біля кожного каналу також вказано його умовний номер.

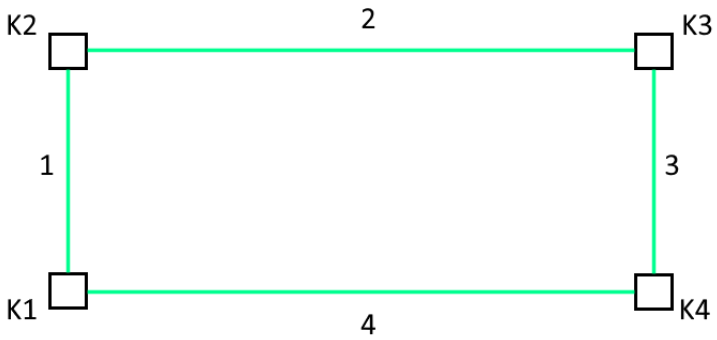

Рис. 19. Топологія ІКМ, де комутатори з'єднано за схемою "кільце"

У цьому випадку для розрахунку ймовірності відмови з'єднання між комутаторами К1 та К2 (Q_{1-2}) можна використати формулу:

$$Q_{1-2} = q_1(1 - p_4p_3p_2). \tag{8}$$

Тоді ймовірність того, що з'єднання між комутаторами К1 та К2 працездатне (P_{1-2}), можна розрахувати відповідно до формули:

$$P_{1-2} = 1 - Q_{1-2}. \tag{9}$$

Для розрахунку ймовірності відмови з'єднання між комутаторами К1 та К3 (Q_{1-3}) (рис. 19) можна використати формулу:

$$Q_{1-3} = (1 - p_1p_2)(1 - p_4p_3). \tag{10}$$

Для мережної топології, представленої на рис. 19, ймовірність безвідмовної роботи з'єднання між комутаторами К1 та К3 (P_{1-3}) можна розрахувати відповідно до формули:

$$P_{1-3} = 1 - Q_{1-3}. \tag{11}$$

Для розрахунку ймовірності відмови з'єднання між комутаторами К1 та К4 (Q_{1-4}) можна використати таку формулу:

$$Q_{1-4} = q_4(1 - p_1p_2p_3). \tag{12}$$

Тоді ймовірність безвідмовної роботи з'єднання між комутаторами К1 та К4 (P_{1-4}) можна розрахувати наступним чином:

$$P_{1-4} = 1 - Q_{1-4}. \quad (13)$$

На рис. 20 зображену схему, де комутатори К1, К2, К3 та К4 з'єднано за комірчастою топологією. На цій схемі додано ще один канал, тобто рівень структурної надлишковості підвищився у порівнянні з топологіями, представленими на рис. 18 та 19.

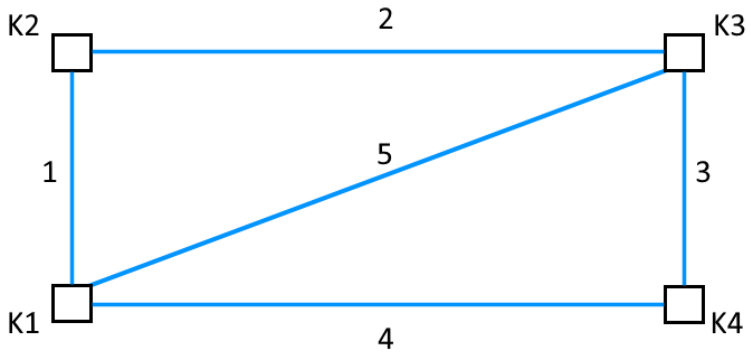

Рис. 20. Топологія ІКМ, де комутатори з'єднано за комірчастою схемою

У цьому випадку для розрахунку ймовірності відмови з'єднання між комутаторами К1 та К2 (Q_{1-2}), можна використати формулу:

$$Q_{1-2} = q_1(1 - p_2(1 - q_5(1 - p_4p_3))). \quad (14)$$

Для розрахунку ймовірності відмови з'єднання між комутаторами К1 та К3 (Q_{1-3}) доцільно використати формулу:

$$Q_{1-3} = (1 - p_1p_2)(1 - p_5)(1 - p_4p_3). \quad (15)$$

Для схеми (рис. 20) ймовірність відмов з'єднання між комутаторами К1 та К4 (Q_{1-4}) визначається згідно формули:

$$Q_{1-4} = q_4(1 - p_3(1 - q_5(1 - p_1p_2))). \quad (16)$$

На рис. 21 зображену схему, де комутатори К1, К2, К3 та К4 з'єднано за повнозв'язною топологією з використанням шести каналів зв'язку.

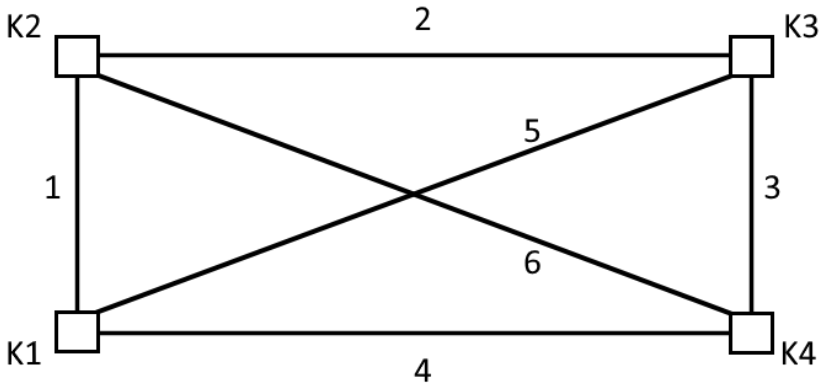

Рис. 21. Топологія ІКМ, де комутатори з'єднано за повнозв'язною схемою

Для цієї топології ймовірність безвідмовної роботи з'єднання комутаторів К1 і К2 (P_{1-2}) можна визначити за формулою:

$$P_{1-2} = p_4(1 - q_1(1 - (1 - q_5q_3)(1 - q_2q_6))) + q_4(1 - q_5(1 - p_5p_2)(1 - p_3p_6)). \quad (17)$$

Для обчислення ймовірності безвідмовної роботи з'єднання комутаторів К1 та К3 (P_{1-3}) треба використати формулу:

$$P_{1-3} = p_6(1 - q_5(1 - (1 - q_1q_4)(1 - q_2q_3))) + q_6(1 - (1 - p_1p_2)(1 - p_5)(1 - -p_4p_3)), \quad (18)$$

Для розрахунку ймовірності безвідмовної роботи з'єднання комутаторів К1 і К4 (P_{1-4}) можна використати вираз:

$$P_{1-4} = p_2(1 - (1 - (1 - q_5q_1)(1 - q_3q_6))q_4) + q_2(1 - q_4(1 - p_5p_3)(1 - p_1p_6)), \quad (19)$$

Нехай ймовірності безвідмовної роботи каналів зв'язку представлені у табл. 2. Тоді з використанням математичної моделі (1)-(19) розраховані показники надійності для кожної з розглянутих мережних топологій. Результати розрахунків представлені у табл. 3.2. Отримані результати розрахунків підтвердили адекватність математичних виразів (3.2)-(3.19). Мережні топології з вищим рівнем структурної надлишковості забезпечували вищі показники надійності ІКМ (рис. 3.2).

Таблиця 2. Ймовірності безвідмовної роботи каналів зв'язку

Номер каналу (i)	1	2	3	4	5	6
p_i	0,9	0,99	0,8	0,998	0,85	0,98

Таблиця 3. Показники надійності для різних мережних топологій

Тип з'єднання комутаторів / номер топології	K1 – K2	K1 – K3	K1 – K4
топологія 1 (рис. 18)	0,9000	0,8910	0,7128
топологія 2 (рис. 19)	0,9790	0,9780	0,9994
топологія 3 (рис. 20)	0,9960	0,9967	0,9996
топологія 4 (рис. 21)	0,9970	0,9996	1,0000

Результати дослідження та порівняльний аналіз рівня надійності різних мережних топологій

У роботі проводилось дослідження та порівняльний аналіз рівня надійності різних мережних топологій (рис. 18 – 21), які можуть бути реалізовані на схемі мережі, запропонованої у другому розділі (рис. 5). Аналіз стосувався впливу рівня надійності окремих каналів та структурної надлишковості на ймовірності безвідмовної роботи з'єднань між різними комутаторами мережі. Формули (1)-(19) були запрограмовані у середовищі MATLAB (рис. 22). З його ж допомогою були побудовані необхідні графічні залежності.

```
clc
clear all
%calculation releability
j=0;
for p0=0.75:0.0001:0.9999
j=j+1;
pi(j)=p0;
%p=[0.9; 0.99; 0.8; 0.998; 0.85; 0.98];%probabilitys sucsess
p=pi(j)*ones(6,1);
q=1-p;%probability no sucsess

%Red - 1
%1_4
P_1_4(1,j)=p(1)*p(2)*p(3);%probability sucsess path
Q_1_4(1,j)=1-P_1_4(1,j);%probability no sucsess path

%1_2
P_1_2(1,j)=p(1);%probability sucsess path
Q_1_2(1,j)=1-P_1_2(1,j);%probability no sucsess path

%1_3
P_1_3(1,j)=p(1)*p(2);%probability sucsess path
Q_1_3(1,j)=1-P_1_3(1,j);%probability no sucsess path

%Green -2
%1_2
Q_1_2(2,j)=q(1)*(1-p(4)*p(3)*p(2));%probability no sucsess path
P_1_2(2,j)=1-Q_1_2(2,j);%probability sucsess path

%1_3
Q_1_3(2,j)=(1-p(1)*p(2))*(1-p(4)*p(3));%probability no sucsess path
P_1_3(2,j)=1-Q_1_3(2,j);%probability sucsess path

%1_4
Q_1_4(2,j)=q(4)*(1-p(1)*p(2)*p(3));%probability no sucsess path
P_1_4(2,j)=1-Q_1_4(2,j);%probability sucsess path
```

а)

```
%blue -3
%1_2
Q_1_2(3,j)=q(1)*(1-p(2)*(1-q(5)*(1-p(4)*p(3))));%probability no sucsess path
P_1_2(3,j)=1-Q_1_2(3,j);%probability sucsess path

%1_3
Q_1_3(3,j)=(1-p(1)*p(2))*(1-p(5))*(1-p(4)*p(3));%probability no sucsess path
P_1_3(3,j)=1-Q_1_3(3,j);%probability sucsess path

%1_4
Q_1_4(3,j)=q(4)*(1-p(3)*(1-q(5)*(1-p(1)*p(2))));%probability no sucsess path
P_1_4(3,j)=1-Q_1_4(3,j);%probability sucsess path

%Dark -4
%1_2
P_1_2(4,j)=p(4)*(1-q(1)*(1-(1-q(5)*q(3))*(1-q(2)*q(6))))+q(4)*(1-q(5)*(1-p(5)*p(2))*(1-p(3)*p(6)));
Q_1_2(4,j)=1-P_1_2(4,j);%probability no sucsess path

%1_3
P_1_3(4,j)=p(6)*(1-q(5)*(1-(1-q(1)*q(4))*(1-q(2)*q(3))))+q(6)*P_1_3(3,j);%probability sucsess path
Q_1_3(4,j)=1-P_1_3(4,j);%probability no sucsess path

%1_4
P_1_4(4,j)=p(2)*(1-(1-(1-q(5)*q(1))*(1-q(3)*q(6)))*q(4))+q(2)*(1-q(4)*(1-p(5)*p(3))*(1-p(1)*p(6)));
Q_1_4(4,j)=1-P_1_4(4,j);%probability no sucsess path

['1-2       1-3       1-4']
RED=[P_1_2(1,j) P_1_3(1,j) P_1_4(1,j)]
GREEN=[P_1_2(2,j) P_1_3(2,j) P_1_4(2,j)]
BLUE=[P_1_2(3,j) P_1_3(3,j) P_1_4(3,j)]
DARK=[P_1_2(4,j) P_1_3(4,j) P_1_4(4,j)]


GG_1_2(2,j)=100*(P_1_2(2,j)-P_1_2(1,j))/P_1_2(1,j);
GG_1_2(3,j)=100*(P_1_2(3,j)-P_1_2(1,j))/P_1_2(1,j);
GG_1_2(4,j)=100*(P_1_2(4,j)-P_1_2(1,j))/P_1_2(1,j);
```

б)

Рис. 22. Перша (а) та друга (б) частина коду програми у середовищі MATLAB

У процесі дослідження припускалося, що ймовірності безвідмовної роботи всіх каналів локальної ІКМ однакові та змінюються, наприклад, у діапазоні від 0,75 до 0,9999. Аналізувалися показники надійності з'єднань між усіма парами комутаторів для різних мережних конфігурацій (рис. 18 – 21). Топологія 1 (рис. 18) відповідала остову мережі, всі інші топології були засновані на введенні певної структурної надлишковості. Топологія 2 (рис. 19) забезпечувала між кожною парою комутаторів два

можливі шляхи передачі кадрів (один основний та один резервний). Топології 3 та 4 (рис. 20 та рис. 21) засновані на подальшому підвищенні структурної надлишковості мережі.

На рис. 23 представлені результати розрахунку ймовірності безвідмовної роботи з'єднань в залежності від зміни ймовірності безвідмовної роботи окремих каналів зв'язку.

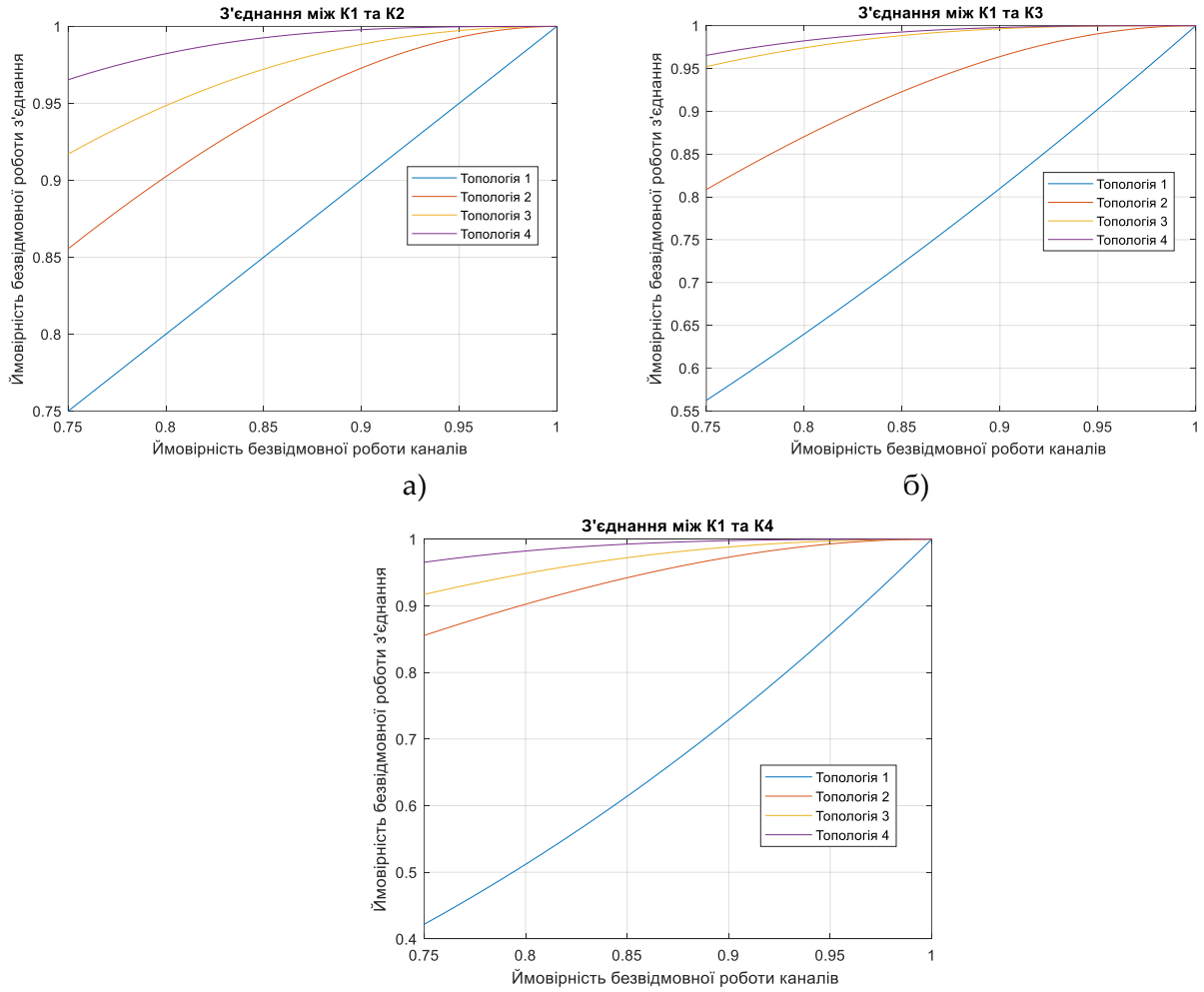

Рис. 23. Результати розрахунку ймовірності безвідмовної роботи з'єднань в залежності від зміни ймовірності безвідмовної роботи окремих каналів зв'язку

На рис. 24 представлені залежності відсотку покращення рівня надійності з'єднань від використаної мережної топології з надлишковістю у порівнянні з остовою топологією (топологією 1). Аналіз залежностей, представлених на рис. 23 та 24 показав, що як і передбачалося, введення надлишковості у топологію мережі призводить до підвищення рівня структурної надійності ІКМ. На підвищення рівня надійності впливали такі основні фактори:

- ймовірність безвідмовної роботи каналів зв'язку мережі;
- кількість каналів у з'єднанні між обраною парою комутаторів мережі.

Найбільший виграш спостерігався за умов використання каналів зв'язку з відносно невисокою ймовірністю безвідмовної роботи (0,75÷0,9). У цьому випадку підвищити рівень надійності з'єднань вдавалось від 10-30% (рис. 24 а) до 35-130% (рис. 24 в). Саме для повнозв'язної топології (рис. 21) для з'єднань, які містили максимальну кількість каналів, забезпечувалось максимальне зростання надійності.

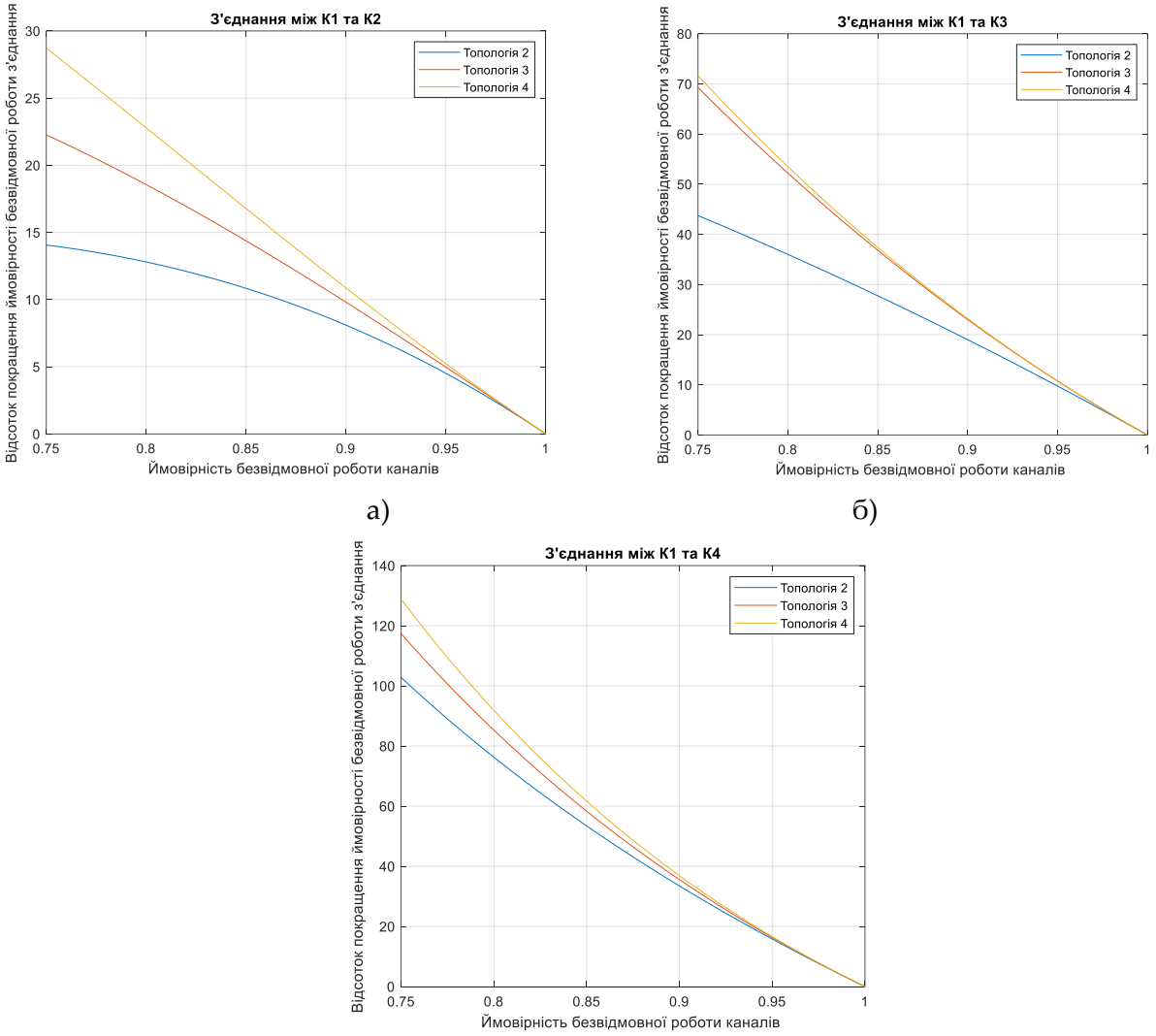

Рис. 24. Залежності відсотку покращення рівня надійності з'єднань від використаної мережної топології з надлишковістю у порівнянні з остовою топологією (топологією 1)

Якщо канали зв'язку мережі мали високу ймовірність безвідмовної роботи (0,9÷0,9999), то виграш дещо знижувався і складав від 5% до 18% (рис. 24). Знову ж таки, максимально підвищити надійність вдалося для з'єднань, які містили максимальну кількість каналів (рис. 24 в). Це і визначає область рекомендованого використання топологій з надлишковістю. Отримані та представлені на рис. 23 та 24 результати досліджень дозволяють кількісно оцінити вплив на показники надійності мережі та з'єднань рівня надійності окремих каналів та структурної надлишковості. Ґрунтуючись на

отриманих результатах можна розробити рекомендації щодо вибору тієї чи іншої мережної топології в залежності від стану комутаторів, його портів та вимог щодо рівня надійності ІКМ взагалі.

Наприклад, якщо при проєктуванні мережі потрібно забезпечити ймовірність відмовостійкої роботи з'єднань між будь-якою парою комутаторів на рівні 0,95 на вище (при $p_i = 0{,}7$), то потрібно використовувати повнозв'язну мережу (рис. 21). Як показано на рис. 23 тільки її використання гарантує виконання висунутих вимог для проаналізованих варіантів з'єднання комутаторів. Якщо ж при проєктуванні мережі потрібно, щоб ймовірність відмовостійкої роботи мережі складала не нижче 0,9, то доцільно використовувати топологію 3 (рис. 20). У випадку, коли вимоги до рівня надійності мережі є високими, наприклад, коли ймовірність відмовостійкої роботи мережі має складати не нижче 0,99, то потрібно не тільки обгрунтовано обрати ту чи іншу мережну топологію, але й попіклуватись про підвищення рівня надійності окремих каналів зв'язку. Ця задача вже пов'язана із заміною (оновленням) комутаторів (модулів портів на них), а також перевіркою стану або умов фізичних з'єднань між ними.

Висновки

1. На підставі проведено аналізу встановлено, що надійність є однією з основних властивостей сучасних ІКМ. Рівень надійності сильно впливає на якість наданих мережею сервісів та може кількісно оцінюватись за множиною показників. До подібних показників відносять ймовірність безвідмовної роботи, ймовірність відмови, частоту відмов, інтенсивність відмов, середній час напрацювання до відмови, коефіцієнт готовності та багато інших. 2. Встановлено, що забезпечення надійності ІКМ є складною проблемою, вирішення якої потребує використання сил та засобів всіх рівнів моделі OSI – від фізичного до прикладного. Протоколи та механізми кожного з цих рівнів відповідають за успішне вирішення окремих задач щодо забезпечення надійності ІКМ при передачі інформації.

2. Проведено якісний аналіз функціональних можливостей засобів фізичного, канального, мережного та транспортного рівнів OSI щодо забезпечення надійності ІКМ. Зазначено, що кожен рівень долучений до вирішення цієї важливої проблеми. Її вирішення має відбуватись на принципах системності та взаємозв'язку з іншими властивостями та показниками ІКМ – якості обслуговування, безпеки тощо. Більш детальна увага була акцентована на можливостях канального та мережного рівня, які базуються на забезпеченні надійності ІКМ шляхом використання протоколів STP, IP-маршрутизації, швидкої перемаршрутизації та відмовостійкої маршрутизації. Для підвищення надійності та відмовостійкості ІКМ ці рішення повинні реалізовуватись у комплексі на різних ділянках мережі та при захисті (резервуванні) різних типів мережних елементів – маршрутизаторів, каналів та шляхів.

3. За допомогою симулятора Cisco Packet Tracer спроєктована надійна локальна інфокомунікаційна мережа, яка охоплює чотири офіси, що містили по 20 персональних комп'ютерів кожний. До структури ІКМ входили чотири комутатори, два пригранічних маршрутизатори. Сервіси глобальної мережі моделювались за допомогою серверу Server0 (рис. 5). Надійність та відмовостійкість мережі забезпечувалась на декількох рівнях.

4. На рівні локальної мережі, яка функціонувала з використання технології Ethernet, підвищення структурної надійності забезпечувалось на підставі введення надлишковості – додаткових зв'язків (каналів) між комутаторами для створення сильнозв'язної топології. Використання протоколу STP, а саме його версій PVST+ та Rapid PVST, дозволило забезпечити швидке реагування мережі на відмови її елементів – маршрутизаторів та каналів зв'язку між ними. У розділі продемонстровано приклади роботи протоколу PVST+ при безвідмовній роботі мережі (рис. 6) та в умовах можливих відмов (рис. 7). Підтверджена ефективність роботи мережі при відмові одного з портів комутатора. Показано, що протокол PVST+ досить швидко побудував оновлений працездатний остов. Оновлене рішення не включало елемент, який відмовив. Додатково з протоколом PVST+ для підвищення надійності та пропускної здатності мережі рекомендується застосувати агрегування портів на комутаторах (рис. 8) при нарощуванні кратності зв'язків (каналів) між комутаторами.

5. Для забезпечення відмовостійкого доступу до сервісів глобальної мережі у розділі було реалізовано такі рішення:

- використано не один, а два пригранічних маршрутизаторів, які виконували функції шлюзу за замовчуванням для ПК локальної мережі (рис. 5);

- налаштовано протокол відмовостійкої маршрутизації HSRP з додатковим штучним балансуванням (розподілом) навантаження між пригранічними маршрутизаторами, що дозволяє також підвищити швидкість передачі пакетів до глобальної мережі (рис. 9 – 13).

6. Проведено тестування мережі та підтверджено високий рівень її надійності як при безвідмовній роботі мережі (рис. 14, рис. 15), так і в умовах можливих відмов (рис. 16, рис. 17). Протокол HSRP дозволив підвищити відмовостійкість доступу до глобальної мережі шляхом захисту шлюзу за замовчуванням. Завдяки функціоналу протоколу HSRP мережа автоматично перенаправляє пакети з основного (Active) пригранічного маршрутизатора, який відмовив, до резервного (Standby). Час реакції на відмову визначався таймерами протоколу, наведеними на рис. 12. Таймер Hello, який за замовчуванням складає 3 с, забезпечує виявлення факту відмови мережного обладнання. Таймер Hold Time (10 с) визначає період заміни основного (Active) пригранічного маршрутизатора, який відмовив, на резервний (Standby). Для зменшення часу реагування на відмови у мережі рекомендується таймер Hello зменшувати, наприклад, до 1 с, як це реалізовано у протоколі VRRP.

7. У процесі аналізу різних підходів до оцінки рівня структурної надійності ІКМ була обрана математична модель, яка представлена у роботах [15-18]. Використання цієї моделі дозволяє проаналізувати різні мережні топології, які містять як нескладні

послідовні та паралельні з'єднання елементів ІКМ, так і більш складні т.з. містки. Було розраховано ймовірності безвідмовної роботи з'єднання та ймовірність відмови з'єднання між різними комутаторами. Також з використанням математичної моделі (1)-(19) розраховані показники надійності для кожної з розглянутих мережних топологій. Результати розрахунків представлені у табл. 3. Отримані результати розрахунків підтвердили адекватність математичних виразів (1)-(19).

8. Було проведено дослідження та порівняльний аналіз рівня надійності різних мережних топологій (рис. 18 – 21), запропонованої у другому розділі (рис. 5). Аналіз стосувався впливу рівня надійності окремих каналів та структурної надлишковості на ймовірності безвідмовної роботи з'єднань між різними комутаторами мережі. Математична модель та приклади розрахунку ймовірності безвідмовної роботи того чи іншого з'єднання між різними комутаторами мережі (рис. 18 – 21). Формули (1)-(19) були запрограмовані у середовищі MATLAB (рис. 22). З його ж допомогою були побудовані необхідні графічні залежності.

9. Аналіз залежностей, представлених на рис. 23 та 24 показав, що як і передбачалося, введення надлишковості у топологію мережі призводить до підвищення рівня структурної надійності ІКМ. На підвищення рівня надійності впливали такі фактори, як ймовірність безвідмовної роботи каналів зв'язку мережі; кількість каналів у з'єднанні між обраною парою комутаторів мережі. Найбільший виграш спостерігався за умов використання каналів зв'язку з відносно невисокою ймовірністю безвідмовної роботи (0,75÷0,9). У цьому випадку підвищити рівень надійності з'єднань вдавалось від 10-30% (рис. 24 а) до 35-130% (рис. 24 в). Саме для повнозв'язної топології (рис. 21) для з'єднань, які містили максимальну кількість каналів, забезпечувалось максимальне зростання надійності.

10. Отримані та представлені на рис. 23 та 24 результати досліджень дозволяють кількісно оцінити вплив на показники надійності мережі та з'єднань рівня надійності окремих каналів та структурної надлишковості. Ґрунтуючись на отриманих результатах, можна розробити рекомендації щодо вибору тієї чи іншої мережної топології в залежності від стану комутаторів, його портів та вимог щодо рівня надійності ІКМ взагалі.

Список літератури

1. *Лемешко, О. В., Поповський, В. В., Лошаков, В. А. та ін., за ред. Поповського В. В.* (2010), Багатоканальний електрозв'язок та телекомунікаційні технології: підручник у 2-х ч. Ч. 1. Харків: ТОВ "Компанія СМІТ", 470 с.

2. *Лемешко, О. В., Лошаков, В. А., Поповський, В. В. та ін.; за заг. ред. проф. Поповського В. В.* (2010), Багатоканальний електрозв'язок та телекомунікаційні технології: підручник у 2-х частинах. Ч. 2. Харків: ТОВ "Компанія СМІТ", 482 с.

3. *Medhi, D., Ramasamy, K.* (2018), Network Routing (Algorithms, Protocols, and Architectures), 2nd edition, Elsevier Inc, 1018 p.

4. *Лемешко, О. В., Єременко, О. С., Невзорова, О. С.* (2020), Потокові моделі та методи маршрутизації в інфокомунікаційних мережах: відмовостійкість, безпека, масштабованість, Харків: ХНУРЕ, 308 с. **DOI**: https://doi.org/10.30837/978-966-659-282-1.

5. *Лемешко, О. В., Єременко, О. С., Євдокименко, М. О., Шаповалова, А. С., Слейман, Б.* (2022), Моделювання та оптимізація процесів безпечної та відмовостійкої маршрутизації в телекомунікаційних мережах: Монографія. Х.: ХНУРЕ, 198 с. **DOI**: https://doi.org/10.30837/978-966-659-378-1.

6. *Васілевський, О. М., Поджаренко, В. О.* (2010), Нормування показників надійності технічних засобів. Вінниця: ВНТУ, 130 с.

7. ДСТУ 2861-94 (1994), Державний стандарт України. Надійність техніки. Аналіз надійності. Основні положення. Київ: Держстандарт, 16 с.

8. *Журахівський, А. В., Казанський, С. В., Матеєнко, Ю. П., Пастух, О. Р.* (2017), Надійність електроенергетичних систем і електричних мереж: підручник. Київ: КПІ ім. Ігоря Сікорського, Вид-во «Політехніка», 456 с.

9. ДСТУ 2506-94 (1995), Державний стандарт України. Засоби обчислювальної техніки. Відмовостійкість і живучість. Загальні технічні вимоги. Київ: Держстандарт, 4 с.

10. *Коренівська, О. Л., Бенедицький, Б. В.* (2020), Надійність, експлуатація та ремонт радіоелектронної та телекомунікаційної техніки. Житомир: Житомирська політехніка, 181 с.

11. *Бобало, Ю. Я., Волочій, Б. Ю., Лозинський, О. Ю. та ін.* (2013), Математичні моделі та методи аналізу надійності радіоелектронних, електротехнічних та програмних систем. Львів: Видавництво Львівської політехніки, 301 с.

12. *Абрамова, А. О.* (2022), Розрахунок ймовірності безвідмовної роботи системи на основі моделі типу «міцність-навантаження». Київ: КПІ ім. Ігоря Сікорського, 37 с.

13. *Lammle, T.* (2020), Cisco CCNA Certification, 2 Volume Set: Exam 200-301 1st Edition. Sybex, 1296 p.

14. *Boesch, F. T.* (1988), "A survey and introduction to network reliability theory", Proceedings of the IEEE International Conference on Communications, - Spanning the Universe, No. 2, Philadelphia, PA, USA, 12–15 June, P. 678–682. **DOI**: https://doi.org/10.1109/ICC.1988.13649.

15. *Pai, K.-J., Chang, R.-S., Wu, R.-Y., Chang, J.-M.* (2019), "Three Completely Independent Spanning Trees of Crossed Cubes with Application to Secure-Protection Routing", Proceedings of the 2019 IEEE 21st International Conference on High Performance Computing and Communications; IEEE 17th International Conference on Smart City; IEEE 5th International Conference on Data Science and Systems (HPCC/SmartCity/DSS), Zhangjiajie, China, 10-12 August, P. 1358–1365. **DOI**: https://doi.org/10.1109/HPCC/SmartCity/DSS.2019.00189.

16. *Lobur, M., Shcherbovskykh, S., Stefanovych, T.* (2016), "Reliability modeling of bridge structure system with load-sharing taking into account", Proceedings of the 2016 XII International Conference on Perspective Technologies and Methods in MEMS Design (MEMSTECH), Lviv, Uktaine, 20–24 April, P. 87–89. **DOI**: https://doi.org/10.1109/MEMSTECH.2016.7507525.

17. *Lemeshko, O., Yeremenko, O., Mersni, A., Gazda, J.* (2022), "Improvement of Confidential Messages Secure Routing over Paths with Intersection in Cyber Resilient Networks", Proceedings of the 2022 XXVIII International Conference on Information, Communication and Automation Technologies (ICAT), Sarajevo, Bosnia and Herzegovina, 16-18 June, P. 1–6. **DOI**: https://doi.org/10.1109/ICAT54566.2022.9811191.

18. *Лемешко, О. В., Єременко, О. С., Євдокименко, М. О., Коваленко, Т. М.* (2021), "Методика розрахунку ймовірності компрометації конфіденційних повідомлень при безпечній маршрутизації в інфокомунікаційних мережах з використанням шляхів, які перетинаються", Проблеми телекомунікацій, No. 2(29). С. 15–27. **DOI**: https://doi.org/10.30837/pt.2021.2.02.