Міністерство освіти і науки України
Національний технічний університет
«Дніпровська політехніка»

Інститут електроенергетики
Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеню магістра

студента *Брюханової Анастасії Олександрівни*

академічної групи *172м-17-1*

спеціальності *172 Телекомунікації та радіотехніка*

спеціалізації[1]

за освітньо-професійною програмою *Телекомунікації та радіотехніка*

на тему ***Вибір методу підвищення відмово стійкості програмно-конфігуруємої (SDN) мережі***

Керівники	**Прізвище, ініціали**	**Оцінка за шкалою**		**Підпис**
		рейтинговою	**інституційною**	
кваліфікаційної роботи	к.т.н., доцент Галушко О.М.			
розділів:				
спеціальний	к.т.н., доцент Галушко О.М.			
економічний	к.е.н., доцент Романюк Н.М.			

Рецензент				

Нормоконтролер	к.ф-м.н., доцент Гусєв О.Ю.			

Дніпро
2018

ЗАТВЕРДЖЕНО:
завідувач кафедри
безпеки інформації та телекомунікацій
_____ д.т.н., проф. Корнієнко В.І.

«_____»_____2018 року

ЗАВДАННЯ
на кваліфікаційну роботу ступеня магістра

студенту ***Брюхановій А.О.*** **академічної групи** *172м-17-1*
(прізвище та ініціали) (шифр)

спеціальності ***172 Телекомунікації та радіотехніка***

спеціалізації[1]

за освітньо-професійною програмою ***Телекомунікації та радіотехніка***

на тему ***Вибір методу підвищення відмовостійкості програмно-конфігуруємої (SDN) мережі***

1 ПІДСТАВИ ДЛЯ ПРОВЕДЕННЯ РОБОТИ

Наказ ректора НТУ «Дніпровська політехніка» від _29.11.2018_№ 2025-л

2 МЕТА ТА ВИХІДНІ ДАНІ ДЛЯ ПРОВЕДЕННЯ РОБІТ

Об'єкт досліджень програмно-конфігуровані мережі.

Предмет досліджень спосіб забезпечення надійності в програмно- конфігурованіій мережі.

Мета вибір методу підвищення відмовостійкості програмно-конфігуруємої мережі як на фізичному так і прикладному рівнях

Вихідні дані для проведення роботи

3 ОЧІКУВАНІ РЕЗУЛЬТАТИ

Наукова новизна *полягає у тому, що одразу пропонуються методи*

забезпечення надійності як програмні, так і фізичні. Запропоновано спосіб побудови для мережі та розраховано капітальні витрати на конкретну мережу.

Практична цінність отриманих результатів полягає в тому, що запропонована структура призводить до можливості масштабувати мережу, перепрограмувати її без втрати надійності передачі даних.

4 ЕТАПИ ВИКОНАННЯ РОБІТ

Найменування етапів робіт	**Строки виконання робіт** (початок-кінець)
Стан питання. Постановка задачі	27.09.2018 – 6.10.2018
Спеціальна частина	7.10.2018 – 15.11.2018
Економічний розділ	16.11.2018 – 24.11.2018

5 РЕАЛІЗАЦІЯ РЕЗУЛЬТАТІВ ТА ЕФЕКТИВНІСТЬ

Економічний ефект За умови значних втрат через слабку надійність мережі і як наслідок втрати клієнтів, витрти на побудову проектованої мережі є цілком доцільними.

7 ДОДАТКОВІ ВИМОГИ

Завдання видано _____ _____
(підпис керівника) (прізвище, ініціали)

Дата видачі:

Дата подання до екзаменаційної комісії:

Прийнято до виконання_____ _____
(підпис студента) (прізвище,ініціали)

РЕФЕРАТ

Пояснювальна записка: 69 с., 23 рис., 11 табл., 4 додатки, 53 джерела.

Об’єкт дослідження: програмно-конфігуруємі мережі.

Предмет дослідження: способи забезпечення надійності в програмно-конфігуруємих мережах.

Мета дипломної роботи: вибрати методи забезпечення надійності (вімовостікості) SDN мережі для архітектурних рішень та на прикладному рівні.

У першому розділі описано і проаналізовано технологію SDN. Наведено детальний опис методів резервування на прикладному рівні та розглянуто посилення надійності з точки зору фізичної реалізації. Сформульовано завдання для дипломної роботи.

У спеціальній частині проведено аналіз впливу резервування на SDN мережу, проведено аналіз існуючих структур архітектури рівня контролю, математично визначена середній час відгуку контролера, запропоновано модифікований спосіб структуризації рівня управління SDN, розглянуто потенційні алгоритми забезпечення відновлення мережі.

В економічному розділі визначено розмір капітальних та експлуатаційних витрат для побудови проектованної мережі.

SDN, DATACENTRE, РЕЗЕРВУВАННЯ, ПЕРЕМАРШРУТИЗАЦІЯ, ВІДНОВЛЕННЯ МЕРЕЖІ.

РЕФЕРАТ

Пояснительная записка: 69 с., 23 рис., 11 табл., 4 приложения, 53 источника.

Объект исследования: программно-конфигурируемых сети.

Предмет исследования: способы обеспечения надежности в программно-конфигурируемых сетях.

Цель дипломной работы: выбрать методы обеспечения надежности SDN сети для архитектурных решений и на прикладном уровне.

В первом разделе описано и проанализировано технологию SDN. Приведено подробное описание методов резервирования на прикладном уровне и рассмотрены усиления надежности с точки зрения физической реализации. Сформулированы задачи для дипломной работы.

В специальной части проведен анализ влияния резервирования на SDN сеть, проведен анализ существующих структур архитектуры уровня контроля, математически определена среднее время отклика контроллера, предложен модифицированный способ структурирования уровня управления SDN, рассмотрены потенциальные алгоритмы обеспечения восстановления сети.

В экономическом разделе определены размер капитальных и эксплуатационных затрат для построения проектованнои сети.

SDN, DATACENTRE, РЕЗЕРВИРОВАНИЕ, ПЕРЕМАРШРУТИЗАЦИЯ, ВОССТАНОВЛЕНИЕ СЕТИ.

ABSTRACT

Explanatory note: 69 p., 23 figures, 11 tables, 4 annexes, 53 sources.

Object of research: software-configuring networks.

Subject of research: ways to ensure reliability in software-configurable networks.

The purpose of the thesis: to choose the methods of ensuring the reliability SDN network for architectural decisions and at the application level.

The first section describes and analyzes SDN technology. A detailed description of redundancy methods at the application level is presented and enhancements in reliability from the point of view of physical implementation are considered. The task for graduation work is formulated.

In the special part the analysis of the effect of the reservation on the SDN network was conducted, an analysis of the existing structures of the control level architecture was performed, the average time of the controller response was mathematically determined, a modified method for structuring SDN management level was proposed, and potential network restoration algorithms were considered.

The economic section defines the size of capital and operating costs for the construction of the projected network.

SDN, DATACENTRE, RESERVATION, INTERMEDIATION, NETWORK RESTORATION.

СПИСОК УМОВНИХ СКОРОЧЕНЬ

SDN – Software Defined Network

ACL – Access Control List

VLAN – Virtual Local Area Network

QoS – Quality of Service

ПЗ – Програмне забезпечення

ЦОД – Центр обробки даних

CSP – Cloud Solution Provider

MPLS – Multiprotocol Label Switching

BFD – Bidirectional Forwarding Detection

API – Application Programming Interface

ЗМІСТ

ВСТУП

У зв'язку з постійним розвитком інформаційних технологій і появою нових технологій (таких як хмарні обчислення та Big Data), вимоги до комп'ютерних мереж зростають, а реалізація ускладнюється. Мережі потребують більшої швидкості передачі даних та вдосконалення інструментів, що використовуються для мережевого управління і моніторингу. Така ситуація призводить до появи нових функціональних і технологічних мереж, з ускладненою інфроструктурою. Старі методи моніторингу і управління не відповідають новим вимогам.

Тому останнім часом зростає популярність программно-конфігуровних мереж SDN (Software-Defined Networks). Самій ідеї мереж SDN вже більше десяти років, але в останні декілька років відомі компанії пропонують нові реалізації, які відкривають більше можливостей. Одною з найпопулярніших є організація мережі SDN зі спільним застосуванням протоколу OpenFlow. Головна перевага представленої технології в тому, що вона працює окремо від мережевих пристроїв і її контроль може здійснюватися операторами за допомогою стандартного сервера.

Проте, як і кожна нова технологія, SDN досі має багато проблем, вирішення яких є актуальною проблемою. Основними є масштабованість і безпека рівня управління.

Мета роботи. Випускна кваліфікаційна робота магістра присвячена дослідженню підвищення надійності мережі SDN для підприємства.

1 СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ

1.1 Аналіз проблеми підвищення надійності

1.1.1 Існуюча архітектура мережі і її недоліки

У класичній мережевій архітектурі завдання побудови маршруту (control plane) і реалізація маршруту (data plane) об'єднані в мережевому пристрої – маршрутизаторі. Управління (control plane) в маршрутизаторі обробляє пакети і приймає рішення, куди їх передати далі (routing). Передача даних (data plane) вирішує проблему транспортування пакету від вхідного порту на певний вихідний (forwarding). Всі ці операції вирішуються закладеними в маршрутизатор протоколами.

Існує безліч протоколів (близько 700), багато з цих протоколів беруть участь у функціонуванні мережі, але при цьому кожен з них може мати різні цілі, виконувати різні завдання, та має свої переваги та недоліки.

Слід зауважити що будь-який протокол може мати кілька програмних реалізацій, наприклад: один і той же протокол реалізований різними компаніями, має різні характеристики. На ефективність взаємодії пристроїв впливає логіка роботи протоколу, якість програмних рішень (реалізацій компаній), а також якість сукупності протоколів (стека або набору протоколів).

Різні протоколи працюють на різних рівнях моделі OSI, тому що реалізувати всі особливості моделі в рамках одного протоколу є неможливим завданням. Саме тому розроблено безліч протоколів, що спрямовані на конкретну функцію, кожен з яких виконує своє завдання на певному рівні моделі OSI, з цього випливає, що мережеві пристрої мають розрізняти так працювати з безліччю протоколів.

Від самого початку комп'ютерні мережі припускали використання трафіку, який істотно відрізняється від трафіку телефонних мереж, більш пізнього мультимедійного трафіку, який є відеозображеннями та мовленням в цифровому вигляді.

Задача передачі різного трафіку мережею створює проблеми пов'язані з різними вимогами до якості обслуговування. Виникає суттєва складність суміщення в одній мережі мультимедійного і традиційного трафіку [3].

Основною характеристикою телекомунікаційної мережі, є її здатність обслуговувати трафік, що до неї надходить, із заданою інтенсивністю при заданій якості інформаційного обміну. Все можна звести до необхідності передачі інформації, представленої у вигляді різного трафіку як можна швидше та з високою надійністю і достовірністю. Останнє має на увазі мінімізацію помилок на стороні прийому, визначаючи тим самим вимоги до обладнання і ПЗ. З огляду на тенденцію до підвищення вимог користувача до швидкості передачі, обсягів та затримок, головним стає завдання підтримки необхідної якості, що може бути здійснено нарощуванням, модернізацією або розподілом мережевих ресурсів шляхом відповідного управління мережею [4].

В існуючій традиційній архітектурі є труднощі:

- статичне (ручне) виділення та перерозподіл мережевих ресурсів;
- окреме налаштування кожного мережевого пристрою;
- складність і ресурсомісткість при впровадженні та зміні мережевих
- конфігурації нових сервісів та інше;
- багатовендорність деяких функцій [5].

Наприклад, щоб додати або видалити окремий пристрій, мережеві адміністратори мають провести коригування в численних комутаторах, маршрутизаторах, брандмауерах, порталах веб-аутентифікації і т.п., адаптувати списки доступу (ACL), VLAN, QoS та інші механізми, що базуються на протоколах, використовуючи для цього інструменти управління на рівні пристроїв. До уваги також повинні бути прийняті топологія мережі, виробники і моделі комутаторів, версії ПЗ. Така складність призводить до відносної статичності мереж, оскільки адміністратори прагнуть мінімізувати ризики, що вноситься сервісом.

Це та ряд інших невідповідностей між потребами ринку і можливостями існуючих мереж привели до пошуку нових підходів щодо організації мережі, одним з яких є програмно-конфігуровані мережі (SDN) [1].

1.1.2 Програмно-конфігуровані мережі.

Програмно-конфігурована мережа (SDN, Software-defined networking) – мережа передачі даних, в якій рівень управління мережею відділений від пристроїв передачі даних і реалізується програмно [6].

Традиційна трирівнева архітектура (доступ - агрегація - ядро) та необхідність робити безліч дій при обробці трафіку в кожному вузлі є занадто надлишковим для інфраструктури з високою ефективністю для організації взаємодії між безліччю серверів та великих ЦОД.

Концепція SDN передбачає:

- відокремленняя управління мережевим обладнанням від управління передачею даних, управління обладнанням повинно бути винесено на окремий комп'ютер, який буде знаходитися під контролем адміністратора мережі;
- перехід від управління окремими екземплярами мережевого обладнання до управління цілої мережі;
- створення інтелектуального програмно-керованого інтерфейсу між мережевим додатком і транспортним середовищем (рис 1.1) [7].

Таким чином, реалізація концепції SDN – розподіл управління мережею (площина управління) та механізму передачі даних (площина даних), перенесення функцій управління в окремі обчислювальні пристрої (переважно хмарні), які називаються SDN-контролерами. Це призводить до зміни традиційної розподіленої моделі маршрутизації централізованою моделлю, перетворює процес управління мережею, що включає створення маршрутів, в процес програмування мережі загалом [8].

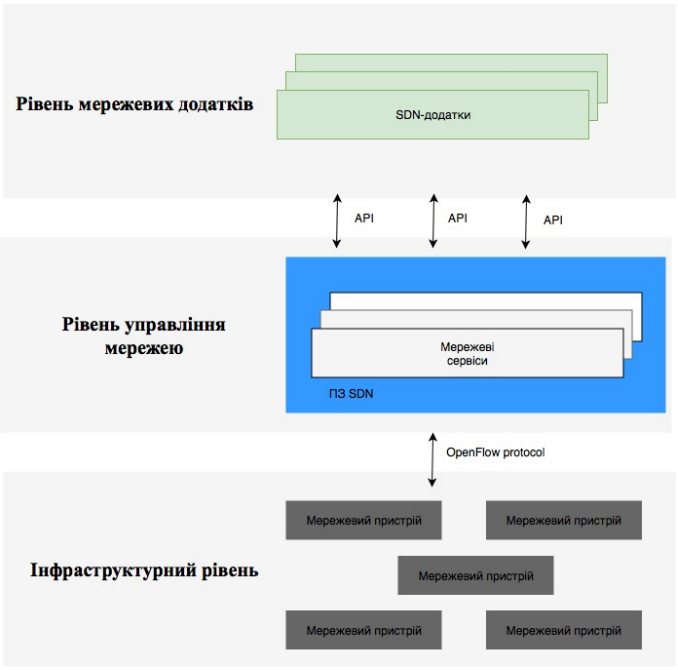


Рисунок 1.1 – Принцип реализації концепції SDN

Теоретично, концепція програмно-конфігурованих мереж має багато переваг, а саме:

- підвищується продуктивність (через прискорення переміщення трафіку);
- знижуються витрати на побудову і супровід мережі (через віртуалізацію управління мережею);
- підвищується зручність управління, безпека та спрощується виконання ряду інших завдань (на централізованому контролері системний адміністратор може спостерігати всю мережу як єдине ціле);
- необмежені можливості з розширення і масштабування мережі в залежності від поставлених завдань [9].

При впровадженні SDN на практиці виникли критичні зауваження від виробників мережевого обладнання, які стурбовані занадто радикальними змінами, що несе в собі нова технологія. Це як висока вартість нового обладнання, так і ризики, що виникають із-за недостатнього тестування цього обладнання. Важливим фактором є також і те, що збільшаться витрати на перенавчання IT спеціалістів, яким доведеться працювати з новими мережами [10]. Але головною підозрою фахівців є те, що централізоване управління

мережею, реалізоване в концепції SDN, є найбільш вразливим місцем даної технології. У разі відсутності зв'язку між контролером SDN і комутаторами мережі, комутатори переходять в дефолтний стан і стають некерованими або зовсім перестають працювати (якщо будь-які налаштування комутатора вимагали постійної роботи контролера). Тобто контролер ПКМ є єдиною точкою відмови.

Для подолання зазначеного недоліку, необхідно враховувати різні механізми забезпечення відмовостійкості мережі. Забезпечення надійності мереж засноване на виявленні відмови і резервування. До того ж в мережах з новими технологіями відновлення має відбутись за час, що не перевищує 50 мс. Сучасною тенденцією в мережах з програмним завданням конфігурації є перенесення підвищення надійності з фізичного на більш високі рівні, навіть до прикладного. Це відповідає переходу від апаратного способу резервування на програмний спосіб [11].

Якщо виконати перехід від резервування на фізичному (апаратному) рівні до резервування на більш високих рівнях моделі OSI, з'являється ряд нових переваг. По-перше, при застосуванні програмних засобів з’являється більше можливостей для резервування, ніж при апаратних. Крім того, операції резервування на вищих рівнях є прозорими щодо нижчих рівнів моделі. Наприклад, якщо після спроби резервування на фізичному рівні (SDH) було зафіксовано негативні результати резервування, то треба виконати додаткове резервування на мережевому рівні, до того ж ця операція має починатися з деякою розрахунковою затримкою, що підвищує час перемикання і досить складно реалізується [12].

Тому резервування в мережах SDN, де рішення про резервування приймається на прикладному рівні (в площині управлінні SDN), а його реалізація виконується в площині даних SDN, суттєво зменшує залежність від резервування на інших рівнях і підвищує швидкість перемикання.

На даний момент до програмно-конфігурованих мереж пред'явлено високі вимоги з надійності (відмовостійкості), а також до характеристик

відновлення після відмови, до того ж відновлення повинно відбуватись непомітно для абонента.

Високий рівень надійності (відмовостійкості) мережі забезпечується завдяки швидкому виявленню пошкоджень та усуненню наслідків від цих ушкоджень, тобто відновлення зв'язку за малий час [13].

Всі механізми забезпечення відмовостійкості мережі можна поділити наступним чином:

- захисне перемикання (або резервування);
- відновлення (або перемаршрутізація).

Процес резервування відбувається шляхом перенаправлення трафіка підготовленим до встановлення з'єднання резервним шляхом. А відновлення відбувається шляхом пошуку нового шляху (перемаршрутізації) після відновлення після відмови.

У кожного з механізмів забезпечення відмовостійкості є свої переваги і недоліки – таблиця 1.1.

Обидва зазначені методи дозволяють забезпечити необхідний користувачу показник готовності з'єднання або показник готовності різних послуг, що йому надаються. В момент вибору мережевого сервісу готовність послуги є більш важливим показником, навіть важливішим за інші QoS-параметри (наприклад такі як затримка, втрата пакетів та інше). Якщо проаналізувати сучасний ринок телекомунікаційних послуг, то можна помітити, що більше половини користувачів очікують 99,9% доступності, тому потрібно забезпечити $К_г$ порядку 0,999999 (для бізнес-сегменту), що відповідає часу простою близько 50 мс [14].

Надійність функціонування мережевої інфраструктури забезпечується шляхом використання алгоритмів резервування і відновлення зв'язку між мережевими вузлами.

Таблиця 1.1 - Переваги і недоліки механізмів забезпечення відмовостійкості мережі

Механізм	Переваги	Недоліки
Захисне перемикання (або резервування)	Швидке відновлення зв’язку	Необхідність додаткової пропускної здатності
Відновлення (або перемаршрутізація)	Оптимізоване використання пропускної здатності мережі	Потребує більше часу на відновлення зв’язку; виникає ризик нестабільності мережі

Наразі є кілька реалізацій технічних рішень щодо забезпечення надійності SDN, використовуючи один або два контроллера SDN, а також при використанні сервера або кластера серверів. Перевагою використання більше ніж одного сервера є те, що при відмові одного сервера переривання зв'язку не буде. Проте використання більше ніж одного контроллера SDN є економічно невигідним для маленьких мереж (втрачається вигода перед традиційними мережами передачі даних).

Беручи до уваги наявні методи забезпечення надійності, а також їх комплексне використання при різних технічних реалізаціях SDN можна оцінити характеристики надійності мережі.

Для досягнення поставленої мети необхідно вирішити завдання, а саме:

- виконати побудову схеми досліджуваної мережі згідно концепції SDN;
- розглянути застосування механізмів забезпечення надійності;
- провести оцінку впливу резервування контролера SDN;
- запропонувати рішення задачі перемаршрутізації;
- зробити основні висновки.

1.2. Аналіз механізмів підвищення надійності

1.2.1 Опис механізмів підвищення надійності

Надійність функціонування мережевої інфраструктури забезпечується шляхом використання алгоритмів резервування і відновлення зв'язку між мережевими вузлами і засобів підвищення надійності самих вузлів, в першу чергу комутаторів. Сьогодні всі серйозні технічні рішення вимагають модулі

управління, які характеризуються надмірністю різних підсистем з можливістю їх швидкої заміни в «гарячому» режимі [15].

При проектуванні мережі необхідно прагнути зменшити як ймовірність відмови, так і вплив відмови. Це непросте завдання, оскільки існує взаємний зв'язок між зниженням імовірності відмови і зниженням ступеня впливу відмови. Сучасні телекомунікаційні мережі - це мережі, що володіють величезною пропускною спроможністю і використовують як правило, волоконно - оптичні лінії зв'язку. Тому завдання забезпечення структурної надійності таких мереж є надзвичайно актуальною [16].

Резервування і відновлення є двома основними підходами, що забезпечують структурну надійність телекомунікаційних мереж при виході з ладу вузлів і ліній зв'язку. Основними вимогами до методів забезпечення надійності є:

- економія пропускної здатності;
- обмеження на комп'ютерні ресурси;
- швидкість заміщення;
- складність передбачуваних методів;
- масштабованість [17].

Зауважимо, що завдання оптимізації будь-якого з показників при наявності обмежень є в більшості випадків складним завданням. Для її вирішення можуть використовуватися різні методи. А саме, метод невизначених множників Лагранжа, методи лінійного та нелінійного цілочисельного лінійного програмування та ін. Однак найчастіше для вирішення поставленого завдання використовують евристичні методи.

Для підвищення надійності телекомунікаційних систем та елементів використовують резервування, що полягає в застосуванні того чи іншого виду надмірності. Види резервування діляться на 4 типи: структурний, інформаційне, тимчасове і програмне. В інформаційному резервування використовує надмірну інформацію. Тимчасове резервування - застосування надмірної часу. Програмне резервування - надлишкових програм [18]. Всі ці види резервування в системі використовуються в цілому або окремо. На

сьогодні в практиці найбільше поширюється вид структурного резервування (рис. 1.2).

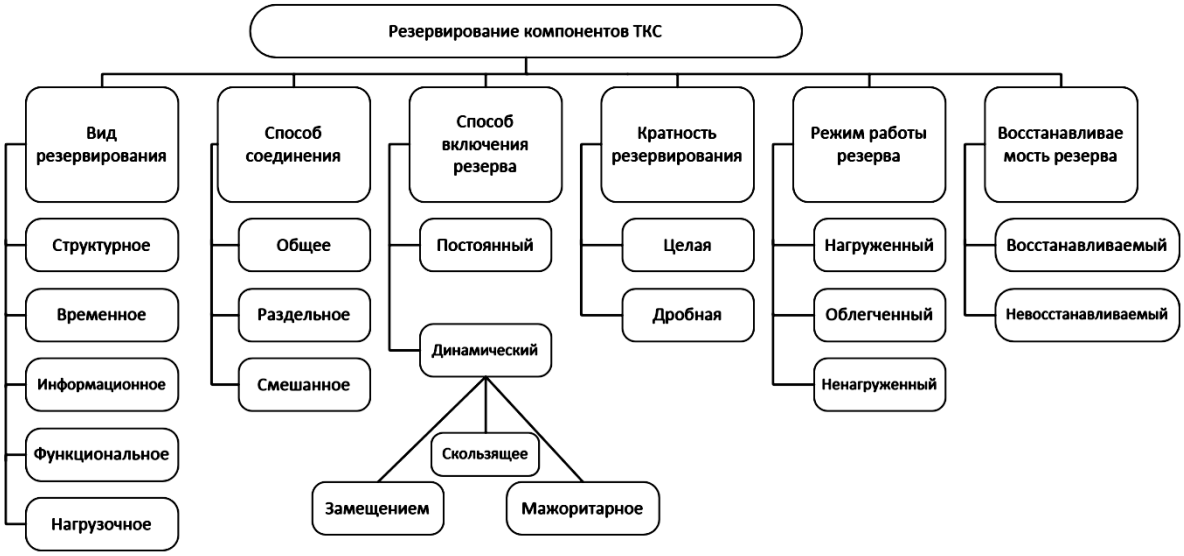


Рисунок 1.2 – Класифікація резервування компонентів телекомунікаційних систем

Види резервування за схемою включення елементів діляться на постійне, роздільне, резервування із заміщенням і на ковзне резервування. При постійному резервуванні резервні елементи працюють разом з основними і це є найбільш надійним методоам з вище перерахованих – рисунок 1.3. При постійному резервуванні при відмові не потрібні особливі для конструкції включення резервних елементів в роботу.

Роздільним резервуванням називається метод підвищення надійності при якому резервуються окремо елементи системи - рис. 1.4.

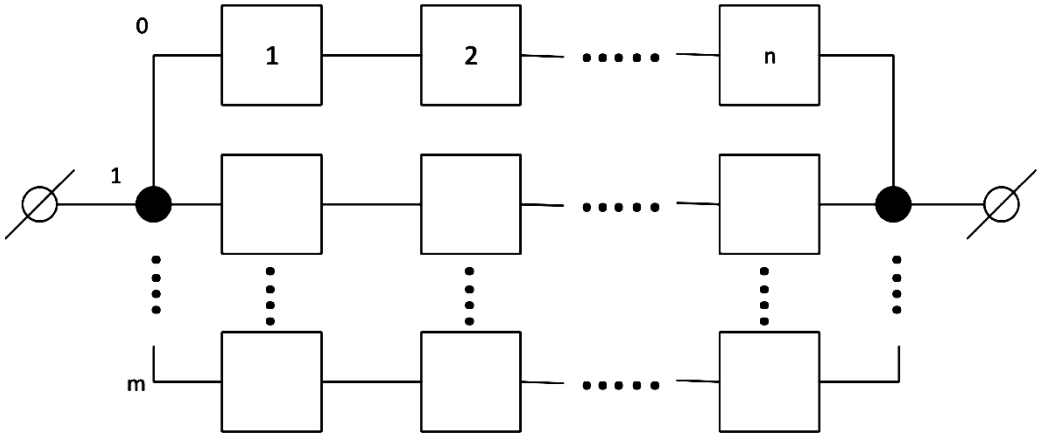


Рисунок 1.3 – Загальне резервування з постійним резервом

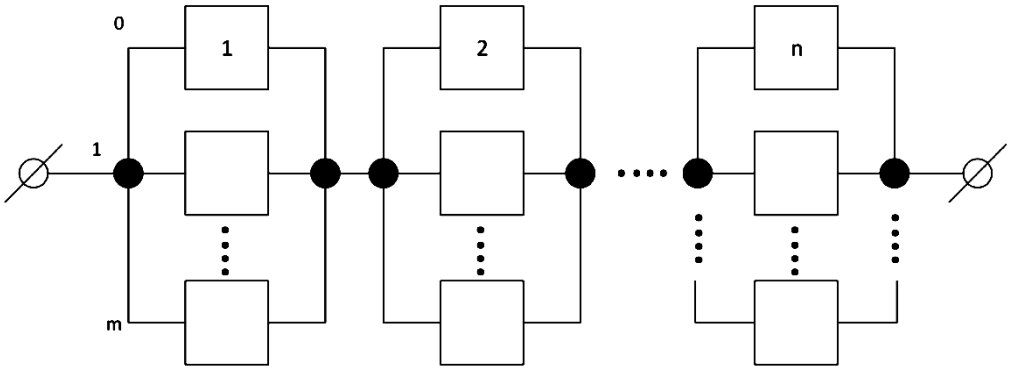


Рисунок 1.4 – Роздільне резервування

При використанні ковзного резервування група основних елементів резервується одним або кількома резервними елементами, власне можливо змінити елемент, який відмовив, із будь-якої групи системи - рис. 1.5.

Завдання включення надмірності полягає в забезпеченні нормального функціонування системи після відмови його елементів. Структурне резервування (або апаратне) передбачає використання системи, елементи яких називаються основними, вводяться додаткові елементи, вузли, пристрої або навіть замість однієї системи передбачається використання кількох однакових систем [18].

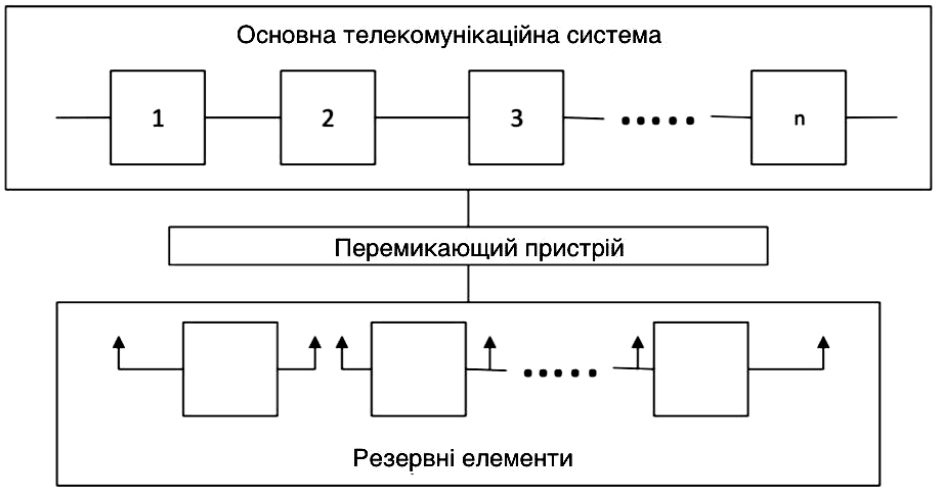
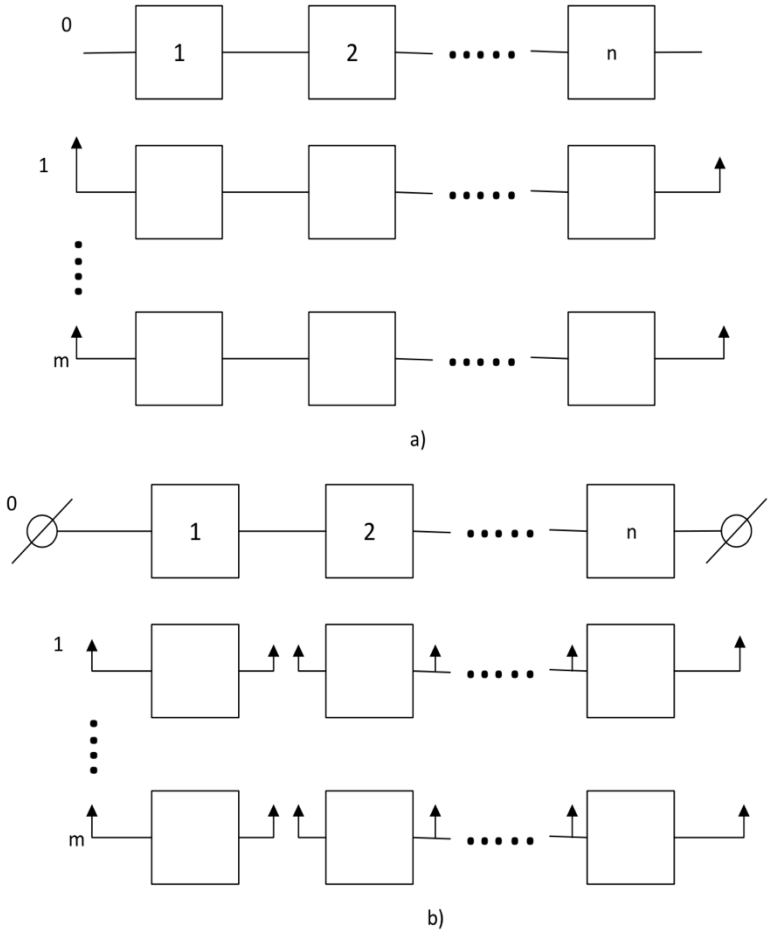


Рисунок 1.5 – Схема ковзного резервування



a) загальне резервування; b) роздільне резервування

Рисунок 1.6 – Резервування з заміщенням резерву

В залежності від режиму роботи розрізняють:

- навантажений резерв - резервний елемент знаходиться в такому ж режимі експлуатації як і основний - приймається, що характеристики

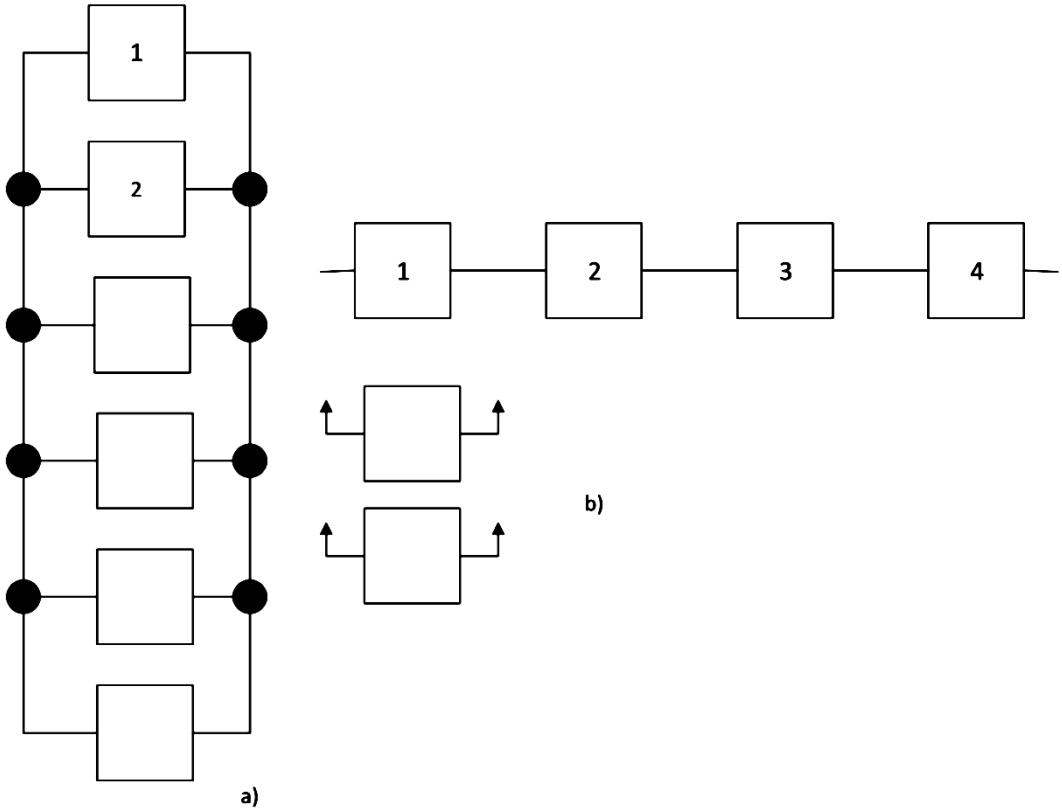
надійності резервних елементів під час їх перебування в резерві та в період використання замість основних, після відмови останніх, залишаються незмінними;

- полегшений резерв - резервний елемент знаходиться в менш завантаженому режимі, ніж основний - передбачається, що характеристики надійності резервних елементів під час їх перебування в якості резерву вищі, ніж під час їх використання замість основних після відмови останніх.

Існує резервування з цілою і дробною кратністю. Для того щоб її розрізняти в схемі указують кратність резервування *m*– рис. 1.7.

Для резервування систем, які складаються з рівних елементів, можна використовувати невелику кількість резервних елементів замість будь-яких основних (ковзне резервування). Незавантажений резерв-резервний елемент практично не несе навантаження. Такий резервний елемент, перебуваючи в резерві, не повинен відмовляти, тобто в цей період має досконалу надійність. У період застосування цього елементу замість основного, після відмови останнього, надійність стає рівною надійністі головного.

Окремим випадком резервування з дробною кратністю є мажоритарне резервування, що часто використовується в пристроях дискретної дії (рис 1.8). При мажоритарному резервуванні, замість одного елемента (канала), під’єднується три ідентичних елемента, виходи, яких подаються до мажоритарного органу *M* (елементу голосування). Якщо всі елементи цієї резервної групи справні, то вхід *M* отримує три ідентичних сигнали і такий саме сигнал надходить у зовнішнє коло від виходу *M*.



а) постійне резервування з кратністю (m = 4/2); b) роздільне резервування з кратністю (m = 2/4)

Рисунок1.7 – Резервування з дробовою кратністю

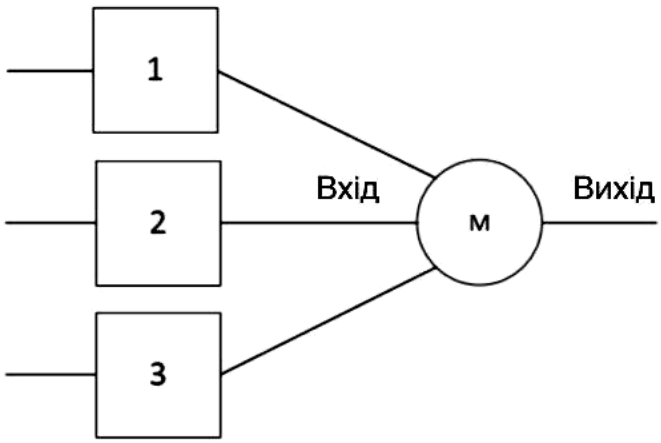


Рисунок 1.8 – Мажоритарне резервування

Якщо один з трьох резервних елементів відмовив, то вхід М отримав два однакових сигнали (TRUE) і один сигнал FALSE. На виході М буде сигнал, що збігається з більшістю сигналів на його вході, тобто мажоритарний орган, здійснює операцію голосування чи вибору за більшістю. Таким чином, умовою безвідмовної роботи при мажоритарному резервуванні є здатність працювати будь-яких двох елементів із трьох і власне мажоритарної системи в заданий проміжок часу [20].

Комбінований резерв – на рис. 1.9 показана група з резервуванням, яка поєднує в собі переваги навантаженого резервування (безперервність роботи) і ненавантаженого резервування (забезпечення значного виграшу в надійності). У цьому випадку два елементи утворюють дублюючу групу (навантажений резерв), а третій належить до ненавантаженого резерву. Цей резерв називається комбінованим.

Всі види структурного резервування можуть застосовуватися в пристроях, що мають призначення управляючих (рис 1.10).

Теоретично введенням надмірності в структуру системи і вибором оптимальних режимів можна створити як завгодно надійну телекомунікаційну систему. Враховуючи всі види резервування, необхідно зробити певний практичний висновок: забезпечити високу надійність за допомогою загального навантаженого резерву не є можливим з економічних причин. Максимальний ефект має дати поелементне резервування [21]. Порівнюючи види резервування з навантаженим і ненавантаженим резервом між собою, можна помітити, що при однакових умовах система з ненавантаженим резервом є надійнішою системи з навантаженим резервом.

Надійність телекомунікаційних систем безпосередньо залежить від методів резервування між мережевими пристроями. Комплекс технічного обладнання та ліній зв'язку, призначеного для формування спеціалізованої передачі джерел інформації, називається трактом інформаційної передачі.

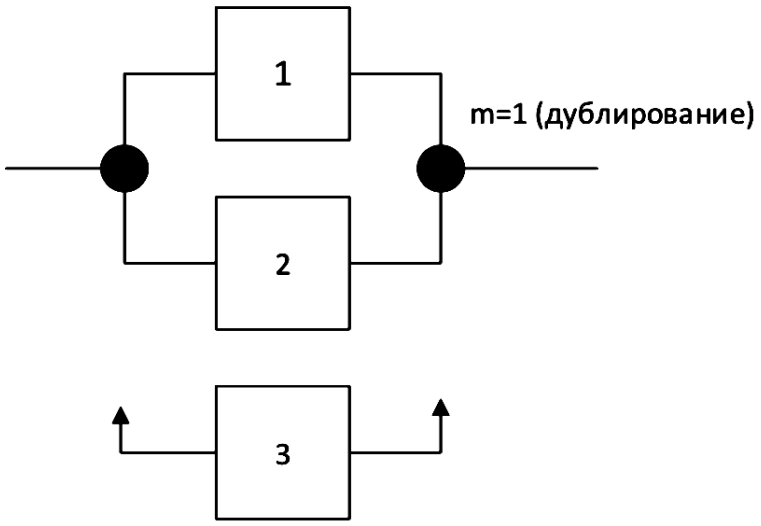


Рисунок 1.9 - Комбінований резерв

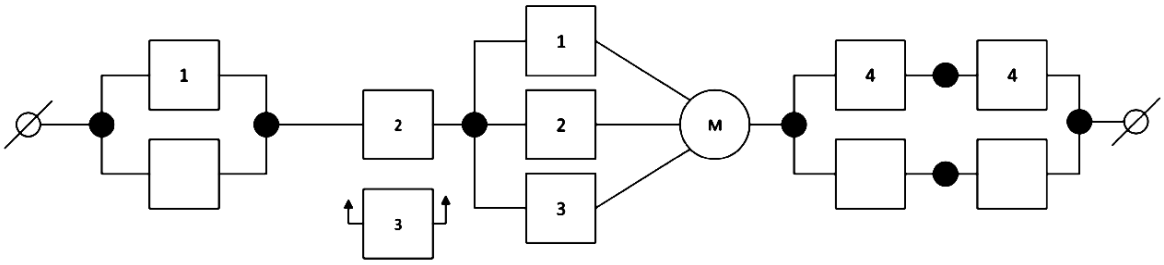


Рисунок 1.10 – Розрахунково-логічна схема структурного резервування

Для визначення ступеню захисту, необхідного для даного сегменту мережі, треба врахувати ймовірність відмови сегмента мережі і очікуваного впливу на трафік (з точки зору часу відновлення та ймовірності втрати пакетів) [22].

Вплив ймовірності відмови в області захисту може бути визначений базуючись на наявній інформації про відмови. Початкове значення ймовірності відмови можна уточнити на основі фактичної статистики даних.

Якщо ймовірність відмови відома, то необхідно проаналізувати, як саме відмова впливає на трафік в мережі, тобто визначити "степінь впливу відмови". Критичний аспектом для оцінки впливу відмови є якість

обслуговування (QoS) трафіка, яке визначається двома компонентами: час, необхідний для відновлення та кількість втрачених пакетів.

Час відновлення T_B визначається циклом відновлення тракту. Варто зауважити, що цей цикл можна задати наступними складовими:

1) час виявлення відмови T_1;

2) час утримання (за необхідності) T_2;

3) час сповіщення (тобто повідомлення на вузол, що відповідає за перемикання) T_3;

4) час для резервування маршруту та сигналізації T_4;

5) час перемикання трафіку T_5 з активного тракту до резервного тракту.

Кількість пакетів, втрачених $N_{ВП}$, пропорційна до часу відновлення T_B та швидкості передачі пакетів R, тобто

$$N_{ВП} = RT_B \tag{1.1}$$

Зменшення часу, що необхідний для виявлення відмови і час перемикання залежить від технології відновлення, яка використовується в конкретній системі. Крім того, час для встановлення резервних трактів (за умови виявлення відмови) залежить від методу маршрутизації та методів сигналізації телекомунікаційної системи.

Зменшити час сповіщень T_3 – напевно, основний аспект при проектуванні методів захисту для мережі. Час сповіщення залежить від часу розповсюдження між вузлами сигналу про відмову T_P і відстані *D(i,a)*, які можна визначити як кількість сегментів мережі (ребер) між вузлом, який виявив відмову (вузол *a*), і вузом, який є відповідальним за перемикання (вузол *i*) [14].

Розглянемо класичні моделі резервування мереж зв'язку (рис. 1.11) і дамо їм стислу характеристику. Фізична топологія мережі складається з вузлів, з'єднаних лініями зв'язку (каналами зв'язку, ланки). Якщо розглядати процес передачі від джерела до одержувача, то вводиться поняття «тракт». Існують первинні (робочі) тракти та резервні. Сегмент тракту, що складається з декількох ланок, прийнято називати «сегментом». Визначення «сегмент» можна розглядати як узагальнення визначень «робочий тракт» та «ланка».

Рисунок 1.11 показує модель захисту ланки. Тут кожна ланка захищена індивідуально (локальний захист). Цей метод має високу обчислювальну ефективність, забезпечує швидку перемаршрутизацію, є простим і масштабованим, але потребує великих мережевих ресурсів.

Захист тракту (рис 1,11b) здійснюється наскрізним шифруванням, тобто на кінцевих пристроях користувачів (іноді такий захист називається глобальним). Тут мережеві ресурси використовуються більш економно, але обчислення тракту від кінця до кінця є більш важким завданням. Для цього захисту є два варіанти:

1) альтернативний тракт, який використовує одну або кілька ланок робочого контуру;

2) альтернативний тракт, що не збігається з основним трактом ні в одній із ланок.

Другий варіант варто розглянути, якщо відмови можуть статися в будь-якій з ланок в основному тракті (тоді для кожного випадка невдачі в першому варінті доведеться шукати альтернативний шлях). В разі відмови будь-якої ланки основного шляху, за умови використання другого варіанту, може бути одразу почато відновлення, без конкретизації де саме сталася проблема. На рисунку 1.11c і 1.11d представлено моделі захисту сегмента (дільнки з кількох ланок). Модель на рисунку 1.11d відрізняється тим, що тут показано захист з "накладенням", це дає змогу забезпечити обхід вузлів, що вийшли з ладу (за винятком вузлів джерела та приймача).

На рисунку 1.11e показано кільцевий захист на основі П-циклів. Суть резервування на основі П-циклів полягає в розміщенні на високо зв’язній топологічній структурі замкнутого контуру або циклу з попереднім розрахунком пропускної спроможності, які можуть застосовуватися в результаті відмови мережі зв'язку [27]. На прикладі моделей, зображених на рисунку 1.11 розглянуто тільки підходи до вибору області захисту (або масштабу захисту). Далі зосередимося на відомих методах використання ресурсів пропускної здатності, таких як 1+1, 1:1, M:N, які можуть

використовуватися як для варіантів захисту трактів, так і для варіантів захисту сегментів або ланок.

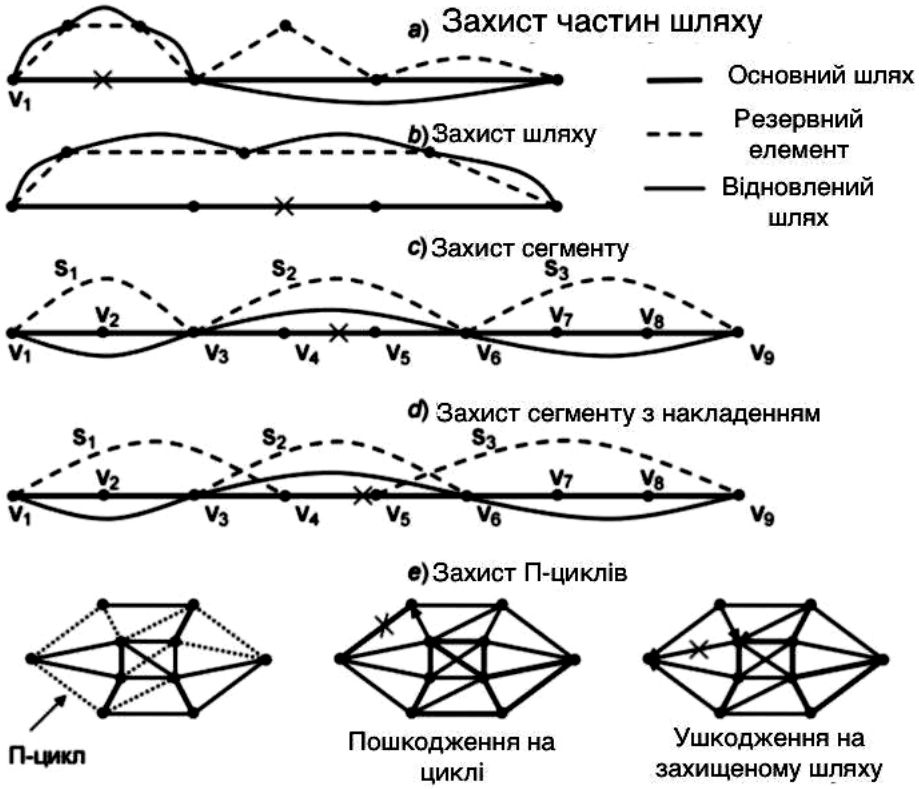


Рисунок 1.11 - Моделі резервування телекомунікаційних систем

Захист тракту 1+1. Дані передаються одночасно робочим та резервним трактами. На етапі прийому виділяється кращий сигнал. Робочий та резервний тракти розділені.

Захист ланки 1+1. Принцип дії такий самий, як у випадку з захистом тракту, але забезпечується сканування лише однієї ланки чи вузла, що має сбій, а не всього тракту.

Захист ланки 1:1. До відмови дані надсилаються лише на робочим трактом. Вторинний трафік може транслюватися резервним трактом. У разі відмови робочої ланки передача вторинного трафіку припиняється і дані передаються резервною ланкою, яка стає робочою. Якщо несправність робочого тракту вирішиться, можливі наступні варіанти:

1) трафік з резервного тракту передається назад на робочий;

2) трафік після усунення несправності залишається на резервному тракті, в той час як робочий виконує функцію резервного.

Перевагою першого варіанту є використання пріоритетним трафіком більш надійного тракту, яким зазвичай є робочий. Недоліком є необхідність перемикання, яке здійснюється пристроєм, що має Kr < 1.

Захист тракту 1:1. Принцип дії такий самий, як і у випадку захисту ланки 1:1, але тут забезпечується обхід всього пошкодженого тракту.

У деяких випадках використовується так званий груповий захист (shared) або захист M:N, що є узагальненням захисту виду 1:1, (M = 1, N = 1).

Захист ланок M:N. Робочий та резервний тракти організовані до відмови (N робочих, M резервних, N ≥ M). У разі відмови на ланці, дані передаються на резервну ланку, але якщо більш ніж M робочих ланок пошкоджено, втрачається вторинний трафік. Найбільш часто використовується варіант M:N, що відповідає випадку, коли M = 1 (1:N) [28].

Захист тракту M:N. Принцип дії такий же, як у випадку захисту ланок, але він забезпечує обхід всього шляху. Цей спосіб резервування є найбільш затребуваним через його низьку вартість та гнучкість. Тим не менш, цей варіант досить складний в оптимізації, особливо якщо є потреба використання механізмів, що враховують пріоритети [29].

Резервні процедури, розглянуті вище, можуть бути використані в поєднанні з процедурами відновлення.

Для боротьби з втратою пакетів в мережі (включаючи мережі SDN) і для знаходження резервних маршрутів використовується механізм перемаршрутизації. Необхідно знайти новий маршрут в мережі, але не перенавантажити ланки резервного тракту. Механізм находження нового шляху подібний до IP-мережі, коли є відмова лінії або коммутаторів.

Час відновлення шляху залежить від алгоритму, що застосовується OpenFlow та складності топології мережі, зазвичай це десятки мілісекунд.

Існує кілька механізмів відновлення.

Відновлення тракту його початковим вузлом. Цей механізм є традиційним і реалізується за допомогою протоколів маршрутизації.

Пошук нового шляху, що обходить елемент, який відмовив. Особливістю є те, що тільки один вузол мережі займається пошуком нового шляху, а саме початковий вузол тракту. У нашій роботі цей механізм не може бути реалізовано, крім тієї умови якщо початковий вузол не є власне контролер SDN.

Захист лінії. Цей захист організовується між двома мережевими пристроями, що безпосередньо з'єднанні між собою лінією зв'язку. Маршрут для обходу знайдено заздалегідь, до того як сталася відмова, і прокладається заздалегідь між цими пристроями таким чином, щоб була можливість обійти лінію зв'язку в разі відмови. Захист лінії є тимчасовим заходом, оскільки після початку використання обхідного шляху, починається процес відновлення. Після відновлення використання тракту для обходу припиняється. Недоліком цього механізму є відсутність гарантій пропускної здатності. Проте цей механізм працює дуже швидко і час перемикання не перевищує 50 мс.

Захист вузла. Цей механізм подібний до механізму захисту лінії, але їх відмінність полягає в тому, що обхідний шлях прокладається таким чином, щоб обійти відмовивший пристрій. Всі інші характеристики схожі на характеристики захисту лінії, цей механізм також є тимчасовим заходом.

Захист шляху. На додаток до основного шляху мережі, прокладається новий шлях, що зв'язує кінцеві пристрої, але проходить через коммутатори та лінії зв'язку, які не беруть участь в основному тракті. Цей механізм є найбільш універсальним, але він повільніший за механізми захисту вузла і захисту лінії [30].

1.3 Опис алгоритмів дослідження та їх обмеження

В наукових роботах з дослідження та забезпечення надійності важливе місце займають статистичні методи дослідження та імовірнісні оцінки надійності. Це зумовлено тим, що події і значення, що використовуються в теорії надійності, як правило, мають випадковий характер. Відмови об'єкта викликані великою кількістю причин, зв’язок між якими не є можливим, так що відмови належать до категорії випадкових подій. Час до того як станеться

відмова може приймати різні значення в певній області можливих значень і належить до категорії випадкових [31].

Розрахунки надійності спрямовані на отримання якісних значень показників надійності досліджуваного об'єкту. Ці розрахунки стали обов'язковим елементом на всіх етапах розробки, створення і використання технічних систем.

Вибір моделі надійності - це комплексне та складне науково-технічне завдання. Воно може бути вирішено методами математичної статистики, якщо є великий статистичний матеріал про відмови досліджуваної системи. Вважаючи новизну SDN і її компонентів, статистичних даних недостатньо для використання методів математичної статистики. У нашому випадку підбір моделі основано на результатах випробувань і фізичних міркувань.

У випадку наближених оцінок, часто використовується експоненційна модель як найбільш зручна з точки зору аналітичних перетворень. Рекомендується використовувати дану модель при виконанні розрахунків надійності за умови відсутності інших вихідних даних, за винятком відмов.

Для опису імовірнісного процесу (оскільки функціонування будь-якої технічної системи являє собою реалізацію імовірнісних процесів), необхідно вказати тип процесу та його чисельні характеристики. Найпоширенішим процесом для опису процесів, що виконуються в системі, є марковський[33].

Необхідною передумовою для марківського процесу є експоненційний розподіл часу до відмови і часу відновлення роботоздатності. Найбільш важливою чисельною характеристикою такого процесу є ймовірність переміщення об'єкту в певний стан протягом зазначеного періоду часу. Знаючи це, ви можете визначити вірогідність кожного можливого стану об'єкта.

Для відновлення в мережі SDN протокол OpenFlow організовує оригінальний метод відновлення [34].

Для відновлення використовується наступний алгоритм. Після виявлення відмови мережевим контролером, цей збій буде зафіксовано і буде складено список трактів LSP, що були зачеплені відмовою. Для кожної нової

відмови мережева модель обчислює обхідний шлях, дійсний в контролері. Виконується алгоритм відновлення CSP, за результатами якого протокол OpenFlow оновлює таблиці коммутації відповідно до обчисленими маршрутами контурів [35].

Для боротьби з втратою пакетів, як зазначалося вище, використовується алгоритм перемаршрутизації. При перемаршрутизації необхідно організувати новий резервний шлях, але не перезавантажити ланки цього нового шляху більше 70%. Вибір граничних умов в області 70% пояснюється збільшенням затримки при збільшенні рівня навантаженності каналу. Після того, як навантаження каналу знаходиться на рівні 70% (рис. 1.12), з'являється затримка. Саме тому цей рівень навантаження вибрано як граничний.

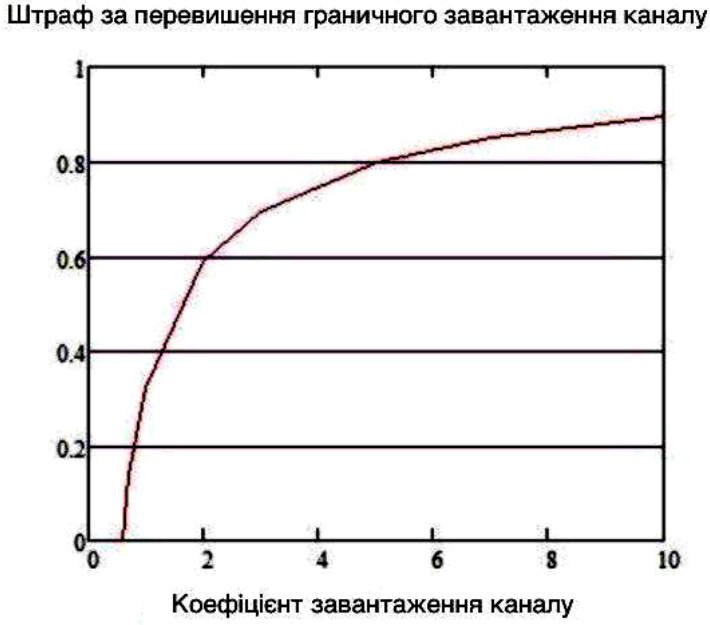


Рисунок 1.12 – Графік залежності затримки в каналі за ступенем його навантаження

У більшості випадків рішення проблеми перемаршрутизації зводиться до проблеми CSP (Constrained Shortest Path) – задачі побудови найкоротших шляхів з урахуванням обмежень. Цей метод знаходить мінімальні значення функції вартості всіх контурів, визначених як сума вартостей всіх трактів мережі *fc(r)* під час виконання обмежень затримки *fD(r)*.

Маршрутизація методом CSP еквівалентна тому, що найкоротший шлях практично можна знайти лише за кількістю стрибків (hop).

Особливість методу CSP є швидка збіжність та висока швидкість, яка дозволяє використовувати його для вирішення проблем в режимі реального часу, тобто під час роботи мережі [36].

Метод CSP, завдяки високій швидкості, можна використовувати як для виявлення обхідних шляхів в реальному часі після виявлення відмови під час експлуатації мережі, так і для попереднього визначення шляху обходу під час проектування мережі. При повному розрахунку надійності необхідно також оцінити надійність управління в мережах SDN, яке виконується контролерами[37].

У сучасних мережах не провадиться маршрутизація на основі потоку. Коли пакет досягає маршрутизатора, він перевіряє пару адрес джерела і призначення пакета з записами таблиці маршрутизації і пересилає його відповідно до попередньо визначених правил (наприклад, протоколом маршрутизації), налаштованими мережевим оператором. З іншого боку, OpenFlow забезпечує гнучкість визначення різних типів потоків, до яких може бути прив'язаний набір дій і правил. Наприклад, один тип потоку може бути перенаправлений з використанням алгоритму маршрутизації з найкоротшим маршрутом, в той час як інші потоки можуть слідувати маршрутами, налаштованим вручну по мережі. Таким чином, кожен потік (тобто пакет) може оброблятися по-різному на мережевому рівні. У OpenFlow ми можемо визначати потоки різними способами. Потоки можуть містити однакові або різні типи пакетів. По суті, потоки можна задавати як комбінацію полів заголовка, але оператор мережі також повинен враховувати обмеження обчислювальної потужності мережевих пристроїв (маршрутизаторів або комутаторів). Щоб уникнути складних розрахунків таблиць потоків, визначення потоку повинні бути правильно і коректно встановлені і, якщо можливо, агреговані. У OpenFlow мережеві пристрої зберігають потоки і пов'язані з ними правила в таблицях потоків, які обробляються як конвеєр. Мета конвеєрної обробки - скоротити час обробки пакетів. OpenQoS використовує парадигму пересилання на основі потоку OpenFlow, щоб ми могли диференціювати дані і мультимедійний трафік. Потоки мультимедіа

можуть бути визначені за допомогою наступних полів або значень заголовка пакета:

- поле заголовка класу трафіку в MPLS,
- поле TOS (Тип обслуговування) IPv4,
- поле класу трафіку в IPv6,
- якщо відомий мультимедійний сервер, IP-адреса джерела,
- номера джерела та / або номера порту призначення.

Бажано визначити потоки відповідно до заголовків пакетів нижнього рівня (L2, L3), оскільки складність розбору пакетів нижче в порівнянні з обробкою до верхніх рівнів (L4). Тому ми пропонуємо визначати мультимедійні потоки, використовуючи поля в MPLS, який розглядається між лінією передачі даних і мережевим рівнем (L2.5) і забезпечує надшвидку комутацію. Але в деяких випадках поля заголовка верхнього рівня також можуть знадобитися для кращого розпізнавання типів пакетів, а OpenFlow дозволяє гнучко визначати потоки, використовуючи поля верхнього рівня (L4) заголовка. Крім того, визначення потоків можуть не покладатися на поточний IP. Будь-яка схема адресації з інформацією про рівень обслуговування може використовуватися для визначення потоків мультимедійного типу. Для розрахунку маршрутів QoS важливо збирати оновлену інформацію про стан глобальної мережі, таку як затримка, смуга пропускання і швидкість втрати пакетів для кожної лінії.

Продуктивність будь-якого алгоритму маршрутизації безпосередньо пов'язана з точністю інформації про стан мережі. У великих мережах збір мережевого стану по всьому світу може бути складним через масштаб мережі. Проблема стає ще більш складною в мережі Інтернеті через повністю розподіленої (hop-by-hop) архітектури. OpenFlow полегшує це завдання, використовуючи централізований контролер. Замість обміну інформацією про стан з усіма іншими маршрутизаторами, OpenFlow безпосередньо відправляє інформацію про локальному стані контролера. Потім контролер збирає інформацію про стан пересилання і відповідним чином обчислює найкращі можливі маршрути.

Вкрай важливо вибрати метрику витрат і обмеження, коли вони обидва характеризують мережеві умови і підтримують вимоги QoS. У мультимедійних додатках типовими індикаторами QoS є втрата пакетів, затримка і зміна затримки (тремтіння). Однак деякі індикатори QoS можуть відрізнятися в залежності від типу програми.

Мережевий контролер SDN є ключовим елементом, оскільки він виконує функції керування елементами мережевої інфраструктури та потоками даних в мережі. Характеристики надійності мережі SDN безпосередньо залежать від відповідних характеристик надійності контролера.

У даній роботі розглядаються тільки методи (механізми) підйому при виникненні відмов в мережі SDN, а сам моніторинг мережі не розглядається. Можна лише зазначити, що моніторинг буде здійснюватися через періодичну організацію в площині передачі даних протокольних сесій BFD (Bidirectional Forwarding Detection). Цей протокол має мало або взагалі не впливає на продуктивність, тому вона забезпечує швидку збіжність. Робота двосторонніх протоколів BFD. На основі того, що супутні пристрої генерують BFD-пакети, а також відповідати на BFD-пакети з сусіднього приладу (пакети-відповіді містять набір функцій, які однозначно характеризують цей пакет [38]). Це гарантує, що потік інформації не буде спрямований в пошкоджену мережеву область. Окрім дослідницької роботи, можна звітувати про інший напрям досліджень в галузі підвищення надійності SDN.

1.4 Підвищення надійності шляхом технічної реалізації

Оскільки SDN є підходом до проектування мереж, то і критерії оцінки використовують, як правило, такі ж як і до інших видів мереж.

Головною вимогою до мережі є виконання мережею її основної функції - забезпечення користувачів потенційною можливістю доступу до ресурсів всіх комп'ютерів, об'єднаних в мережу. Всі інші вимоги - продуктивність, надійність, сумісність, керованість, захищеність, розширюваність і масштабованість - пов'язані з якістю виконання цієї основної задачі.

Хоча всі ці вимоги дуже важливі, часто поняття «якість обслуговування» комп'ютерної мережі трактується більш вузько: в нього включаються тільки дві найважливіші характеристики мережі - продуктивність і надійність.

Незалежно від обраного показника якості обслуговування мережі існують два підходи до його забезпечення. Перший підхід полягає в тому, що мережа гарантує користувачеві дотримання деякої числової величини показника якості обслуговування. Наприклад, мережа може гарантувати користувачу А, що будь-який з його пакетів, посланих користувачеві В, буде затриманий мережею не більше, ніж на 150 мілісекунд. Або, що середня пропускна спроможність каналу між користувачами А і В не буде нижче 5 мегабіт в секунду, при цьому канал буде дозволяти пульсації трафіку в 10 Мбіт на інтервалах часу не більше 2 секунд. Технології framerelay і ATM дозволяють будувати мережі, що гарантують якість обслуговування по продуктивності.

Другий підхід полягає в тому, що мережа обслуговує користувачів відповідно до їх пріоритетів. Тобто якість обслуговування залежить від ступеня привілейованості користувача або групи користувачів, до якої він належить. Якість обслуговування в цьому випадку не гарантується, а гарантується тільки рівень привілеїв користувача. За таким принципом працюють, наприклад, локальні мережі, побудовані на комутаторах з пріоритезацією кадрів.

В рамках цієї роботи основним показником якості розглядається надійність.

Для технічних пристроїв використовуються такі показники надійності, як середній час напрацювання на відмову, імовірність відмови, інтенсивність відмов. Однак ці показники придатні для оцінки надійності простих елементів і пристроїв, які можуть перебувати лише в двох станах - працездатному або непрацездатному. Складні системи, що складаються з багатьох елементів, крім станів працездатності та непрацездатності, можуть мати і інші проміжні стани, які ці характеристики не враховують. У зв'язку з цим для оцінки надійності складних систем застосовується інший набір характеристик.

Готовністю або коефіцієнтом готовності називають проміжок часу, протягом якого система може бути використана. Готовність може бути поліпшена шляхом введення надмірності в структуру системи: ключові елементи системи повинні існувати в декількох екземплярах, щоб при відмові одного з них функціонування системи забезпечували інші.

Крім того, необхідно забезпечити збереження даних, захист їх від спотворення або несуперечливість даних (наприклад, якщо для підвищення надійності на декількох файлових серверах зберігається кілька копій даних, то потрібно постійно забезпечувати їхню ідентичність).

Ще однією характеристикою надійності є відмовостійкість. У мережах під відмовостійкісттю розуміється здатність системи приховати від користувача відмову окремих її елементів. Наприклад, якщо копії таблиці бази даних зберігаються одночасно на декількох файлових серверах, то користувачі можуть просто не помітити відмову одного з них.

Постановка задач дослідження

Основне завдання роботи полягає в визначенні методів для забезпечення надійності мережі побудованою за концепцією SDN.

Для досягнення поставленої мети необхідно вирішити ряд завдань, а саме:

- виконати побудову схеми досліджуваної мережі згідно концепції SDN;
- розглянути застосування механізмів забезпечення надійності;
- провести оцінку впливу резервування контролера SDN;
- запропонувати рішення задачі перемаршрутизації;
- зробити основні висновки і пропозиції щодо подальшого дослідження.

1.5 Висновки до першого розділу

У першому розділі описано і проаналізовано технологію SDN. Наведено детальний опис методів резервування на прикладному рівні та розглянуто посилення надійності з точки зору фізичної реалізації. Сформульовано завдання для дослідження механізмів щодо забезпечення відмовостійкості; приведення алгоритму оптимального розподілу ресурсів для підвищення

надійності мережі зв'язку; зробити оцінку впливу методів забезпечення надійності на якість обслуговування; вибір архітектурного рішення для мережі

2 СПЕЦІАЛЬНА ЧАСТИНА

Предметом дослідження є частина мережі підприємства, яка була перебудована за принципами технології SDN, де використовуються комутатори з малим функціоналом, а всі головні завдання управління, маршрутизації та іншого виконують контролери SDN.

Основна задача підприємства – забезпечення доступу своїм користувачам до конструкторів сайтів та до готових сайтів з даними користувацькими даними.

Усі запроси користувачів йдуть до дата-центру, який обробляє дані та призводить рендер сайту на стороні сервера після чого віддає клієнту необхідні данні.

Було обрано технологію SDN за легкість у масштабуванні та через перспективу перенесення мережі до облачних сервісів, побудованих за принципом віртуалізації мережевих функцій, у майбутньому. Мережа SDN також не є залежною від вендорів обладнання і не має ряду проблем, пов’язанних із сумісністю певних приладів, що необхідні для функціонування складної корпоративної мережі.

Оскільки надійність та час відновлення є ключовими для бізнесу постала задача забезпечення надійності (відмовостійкості).

На рисунку 2.1 представлено узагальнену схему досліджуваної мережі до переходу на SDN.

Забезпечити надійність SDN мережі можна на кількох рівнях: на нижніх рівнях моделі OSI за допомогою інфрастуктури мережі та на прикладному рівні за допомогою спеціальних протоколів відновлення.

В першу чергу варто розглянути інфраструктуру мережі і відштовхуючись від неї розглянути подальші методи забезпечення надійності.

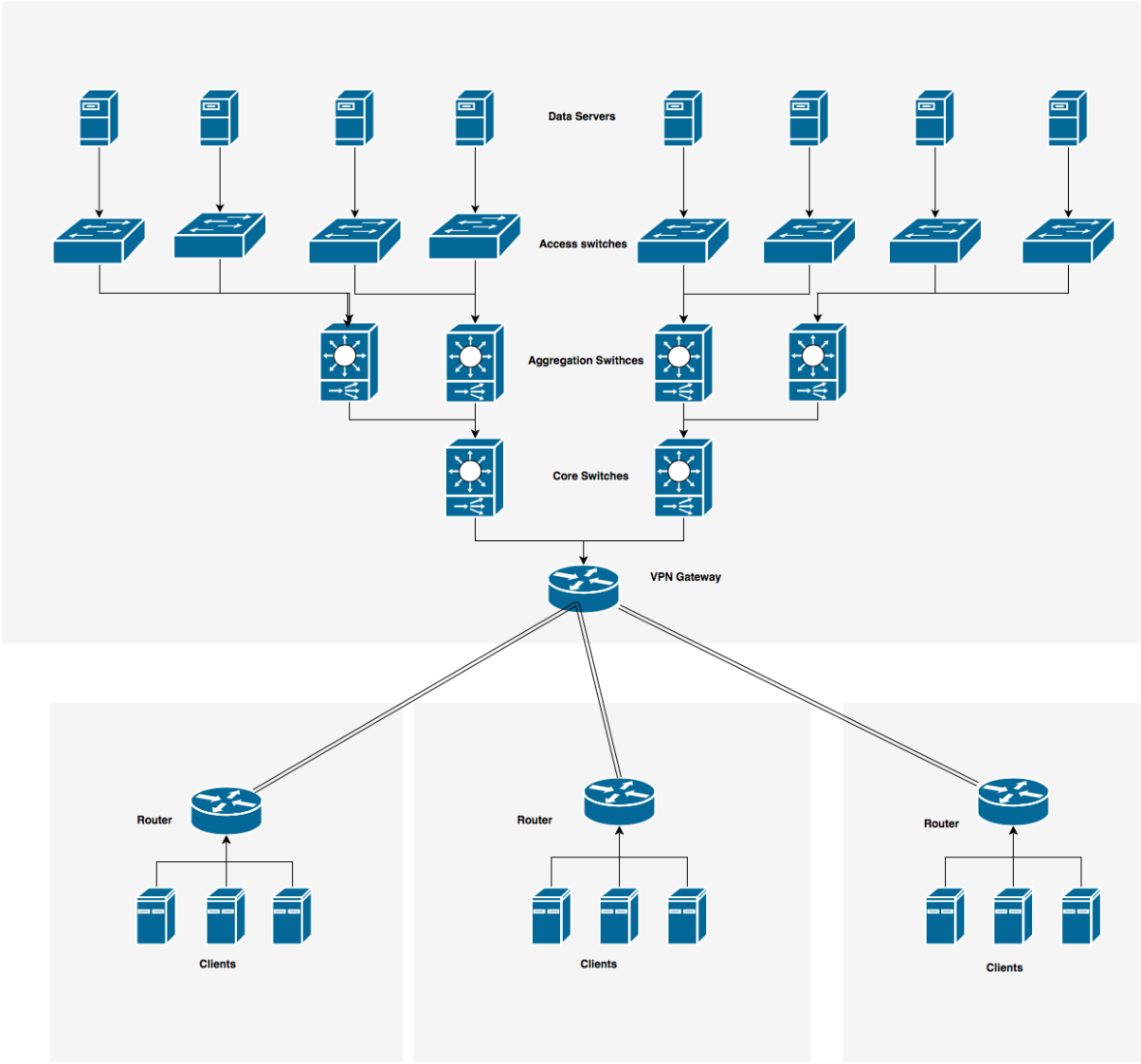


Рисунок 2.1 – Узагальнена структура підприємства

2.1 Модифікація існуючої архітектури

Існують два загальноприйнятих варіанти поліпшення продуктивності рівня управління SDN. Перший – це перенести частину функції управління на інші пристрої в мережі, наприклад, мережеві комутатори. Цей підхід дійсно дозволяє значно зменшити навантаження на центральний вузол, і значно збільшує загальну продуктивність мережі. Проте, комутатори повинні бути побудовані на спеціальній інтегральній схемі і мати центральний процесор. Таким чином, збільшується складність розгортання мережі. Другий підхід полягає в проектуванні особливого розподіленого рівня управління, який передбачає розподілення навантаження між декількома контролерами.

Іншими словами, рівень управління буде працювати як розподілена комп'ютерна система, що колективно обробляє вхідні мережеві запити.

Окрім того, ще одним аспектом, який значно впливає на продуктивність мережі в цілому є взаємодія контролера з OpenFlow комутаторами. Використання декількох потоків і управління завантаженістю шляхів маршрутизації є найбільш ресурсоємкими задачами. Окрім того, багато часу потребує отримання і обробка пакетів з каналу.

Як правило, архітектура рівня управління SDN може бути централізованою і децентралізованою. Децентралізована, в свою чергу, поділяється на два підвиди: локальний і глобальний. Вузли локального виду не бачать мережу в цілому. Кожен вузол обробляє запити тільки від частини вузлів мережі. В свою чергу, вузли в децентралізованих системах глобального виду можуть приймати запити від усіх вузлів мережі. Децентралізовані структури також називають розподіленими структурами.

Для розрахунків масштабованості рівня управління SDN можна Окрім того, ще одним аспектом, який значно впливає на продуктивність мережі в цілому є взаємодія контролера з OpenFlow комутаторами. Використання декількох потоків і управління завантаженістю шляхів маршрутизації є найбільш ресурсоємкими задачами. Окрім того, багато часу потребує отримання і обробка пакетів з каналу.

Як правило, архітектура рівня управління SDN може бути централізованою і децентралізованою. Децентралізована, в свою чергу, поділяється на два підвиди: локальний і глобальний. Вузли локального виду не бачать мережу в цілому. Кожен вузол обробляє запити тільки від частини вузлів мережі. В свою чергу, вузли в децентралізованих системах глобального виду можуть приймати запити від усіх вузлів мережі. Децентралізовані структури також називають розподіленими структурами.

Для розрахунків масштабованості рівня управління SDN можна використовувати метрики масштабованості для розподіленої системи. Масштабованість для розподілених систем базується на продуктивності. Розподілену систему можна назвати масштабованою, якщо продуктивність системи залишається на одному рівні при збільшенні розміру системи. Для рівня управління SDN продуктивність F(N) може бути визначена як:

$$F(N) = \phi(N) * \frac{T(N)}{C(N)} \quad (2.1),$$

де:

N – кількість вузлів в мережі,

φ(N) – пропускна спроможність рівня управління в обробці мережевих запитів,

T(N) – середній час відгуку на кожен запит,

C(N) – вартість розгортання рівня управління (наприклад, вартість одного контролеру).

Таким чином, масштабованість для рівня управління SDN, розмір якої змінюється від N2 до N1 визначається як:

$$\Psi(N_1, N_2) = \frac{F(N_2)}{F(N_1)}. \quad (2.2)$$

В SDN існує декілька типів мережевих запитів, які рівень управління повинен обробляти. Наприклад, запит для спостерігання за станом мережі, оновлення стану мережі, відновлення після збою. Однак ініціювання потоку є головною і основною функціональністю контролеру SDN. Тому основна увага приділяється обробці ініціювання потоку в рівні управління. В децентралізованих структурах локального вигляду та ієрархічних структурах обробка запиту ініціювання потоку може оброблятися декількома контролерами. Необхідно ввести такий структурний параметр, як середня

дистанція контролерів, що визначає яка кількість контролерів в середньому необхідна для обробки запиту ініціювання потоку.

Навантажувальна спроможність контролера визначається центральним процесором, використанням пам'яті і завантаженістю мережі. Як правило, "вузьким місцем" є процесор. Тому будемо приймати до уваги тільки час, який витрачає центральний процесор для обробки одного запиту. Час обробки залежить від топології мережі, використаних алгоритмів маршрутизації і обчислювальної потужності контролера. Часова складність алгоритмів маршрутизації позначається g(V,E), де V – кількість мережевих вузлів, а E – кількість мережевих з'єднань. Тоді ми припустимо, що час обробки підлягає експоненційному розподілу з середнім значенням $\frac{g(V,E)}{K}$, де K – обчислювальна потужність. Тому припустимо, що контролер використовує алгоритм Дейкстри для пошуку найкращого шляху. Складність алгоритму Дейкстри залежить від реалізації, і у загальному випадку складає $O(V^2)$. Для спрощення обчислень, в цій роботі допустимо, що $g(V,E) = V^2$. Оскільки надходження запитів з одного вузла до іншого піддається Пуассонівському розподіленню, а сума незалежних випадкових величин Пуассонівського розподілення представляє собою Пуассонівське розподілення, то сукупність запитів, що надходять до контролера, також піддаються Пуассонівському розподіленню. Таким чином, кожен контролер є моделлю черги M/M/1.

Спочатку визначимо час відгуку контролера в централізованій структурі при кількості вузлів N та базовій середній інтенсивності надходження запитів λ.

$$\lambda_C = N * (N - 1) * \lambda. \quad (2.3)$$

Ця величина має пуассонівський розподіл. Час обробки запиту розподіляється за експоненціальним законом. І середній час обробки запиту $\mu_C(N)$ обернено пропорційний до масштабу мережі N. З цього випливає, що

$$\mu_C = \frac{K}{g(N)}. \quad (2.4)$$

Тоді середній час відгуку контролера при централізованій структурі буде:

$$E\{T_C(N)\} = \frac{1}{\mu_C - \lambda_C}. \quad (2.5)$$

В децентралізованій структурі декілька контролерів. Припустимо, що кількість контролерів буде mD. В першому типі децентралізованної структури кожен контролер має свою локальну мережу. Тому, існують два випадки: коли весь шлях управляється одним контролером, і коли необхідно задіяти декілька контролерів. Схематичне представлення децентралізованої локальної структури можна побачити на рисунку 2.2.

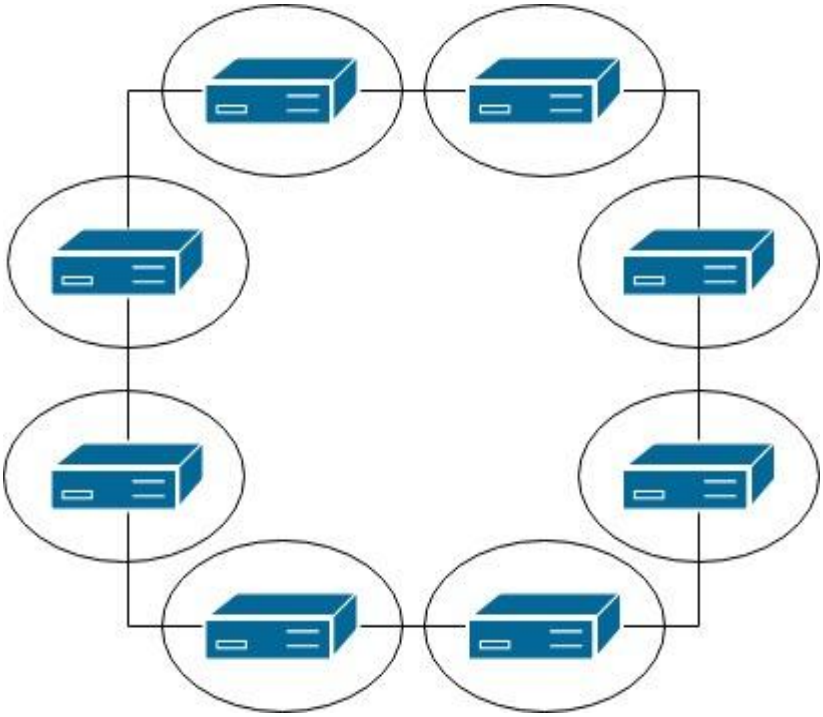


Рисунок 2.2 - Децентралізована локальна структура рівня управління

Глобальний запит поділяється на два запити: на локальний і на ще один локальний або глобальний до іншого контролера. Якщо середня дистанція контролерів d_D, кожен глобальний запит буде поділений на $d_D + 1$ запитів. І час відгуку на глобальний запит буде дорівнювати сумі часу відгуку на локальні

запити. Відповідно до цього, $\frac{N^2}{m_D} - N$ – кількість локальних шляхів, $N^2 - \frac{N^2}{m_D}$ – кількість глобальних шляхів. Тому швидкість прибуття запитів на кожен контролер буде:

$$\lambda_{D,l} = \lambda * \frac{\left(N^2 - \frac{N^2}{m_D}\right) * (d_D + 1) + (\frac{N^2}{m_D} - N)}{m_D}, \quad (2.6)$$

а також кожен контролер повинен керувати топологією з $\frac{N}{m_D} + m_D$ вузлами. Тому середній час обробки запиту:

$$\mu_{D,l} = \frac{K}{g(\frac{N}{m_D} + m_D - 1)}, \quad (2.7)$$

а середній час відгуку контролера:

$$E\{T_{D,l}\} = \frac{1 + \frac{N*(m_D-1)}{(N-1)*m_D} * d_D}{m_{D,l} - \lambda_{D,l}}. \quad (2.8)$$

В другому типі децентралізованної структури, кожен вузол контролеру має повний доступ до мережі. Схематичне представлення децентралізованої глобальної структури можна побачити на рисунку 2.3. Ця властивість дозволяє розрахувати середній час обробки запиту і середній час відгуку контролера за формулами для централізованої структури. Швидкість прибуття запитів на кожен контролер буде:

$$\lambda_{D,g} = \frac{N*(N-1)*\lambda}{m_D} \quad (2.9)$$

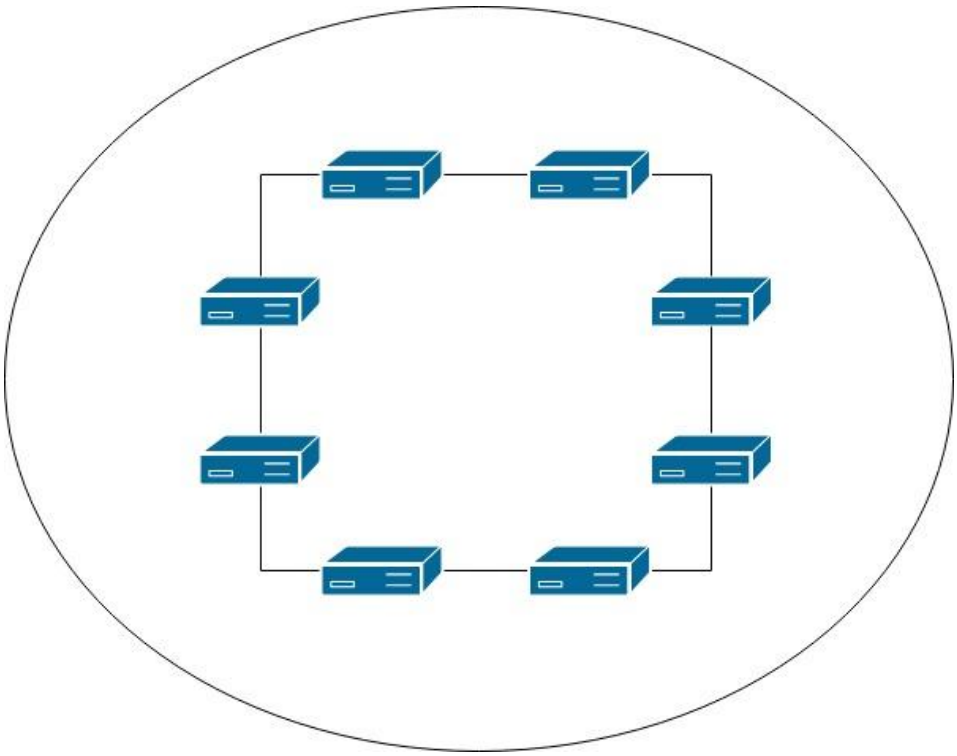


Рисунок 2.3 - Децентралізована глобальна структура рівня управління

Ієрархічна структура, як правило, має 2 рівні. В даній роботі розглядається ієрархічна структура з двома рівнями, оскільки ієрархічна структура з більшою кількістю рівнів може бути розглянута в такий же самий спосіб. Схематичне представлення ієрархічної структури можна побачити на рисунку 2.4.

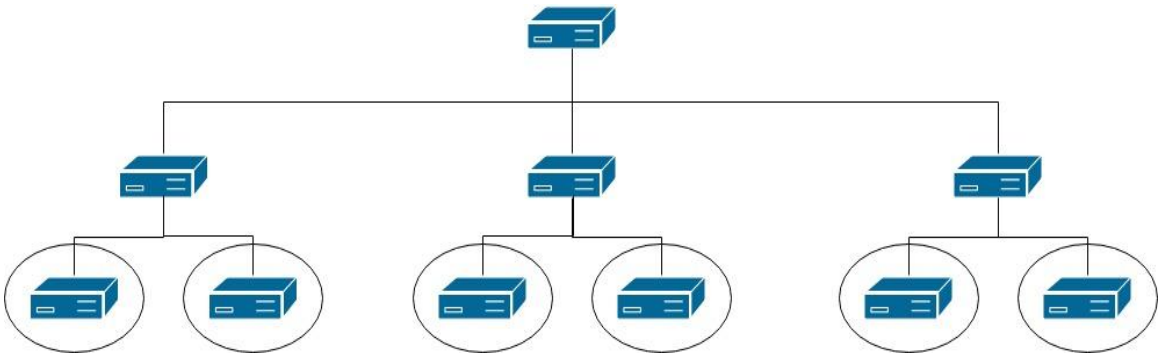


Рисунок 2.4 - Ієрархічна структура рівня управління

В даній структурі рівень управління організовано у вигляді дерева, і вузли розділені на два типи: один корінний вузол і багато листів. Вузли-листя управляють безпосередньо рівнем даних. І видимість кожного вузла-листа

поширюється тільки на певну зону в мережі і управляється коренем дерева. Контролер кожного окремого листа і його локальна мережа абстрагуються коренем, як логічний вузол. Корінь володіє інформацією про ці логічні вузли. Потоки можуть бути двох видів: локальними і глобальними. Початковий хост і хост призначення управляються одним і тим же листовим контролером. Глобальні потоки повністю навпаки. Кожен запит ініціалізації локального потоку буде оброблений тільки одним листовим контролером. В той час як кожен запит ініціалізації глобального потоку буде оброблений кореневим контролером спочатку, а потім розділений на локальні запити, які будуть оброблятися відповідними листовими контролерами.

Припустимо існує m_H листових контролерів і середня дистанція листових контролерів d_H. З цього випливає, що кореневий контролер управляє логічним графом з m_H вузлами. Таким чином, середній час обробки запита кореневим контролером буде:

$$\mu_{H,r} = \frac{K}{g(m_H)}. \tag{2.10}$$

Кожен листовий контролер управляє $\frac{N}{m_H}$хостами. З цього вираховуємо середній час обробки запиту для кожного листового контролера:

$$\mu_{H,l} = \frac{K}{g(\frac{N}{m_H})}. \tag{2.11}$$

Будемо позначати j-ий контролер і-го рівня як $c_{i,j}$. $C_{x,y}$ - позначення множини, до якої входять контролери, які необхідно залучити, щоб обробити запити ініціації потоку $f_{x,y}$. Нехай $I_{x,y(i,j)}$ буде бінарною змінною, що ідентифікує, чи входить $c_{i,j}$ до $C_{x,y}$.

$$I_{x,y}(i,j) = \begin{cases} 1; \text{якщо } c_{i,j} \in C_{x,y} \\ 0; \end{cases} \tag{2.12}$$

Серед N^2 - N потоків $\frac{N^2}{m_D} - N$ локальних потоків і $N^2 - \frac{N^2}{m_D}$ глобальних. Таким чином, можна отримати:

$$\sum_{x=1}^{N} \sum_{y=1,y\neq x}^{N} I_{x,y}(1,1) = N^2 - \frac{N^2}{m_H} \quad (2.13)$$

$$\sum_{x=1}^{N} \sum_{y=1,y\neq x}^{N} \sum_{j=1}^{m_H} I_{x,y}(2,j) = \left(N^2 - \frac{N^2}{m_H}\right) * (d_H + 1) + \frac{N^2}{m_H} - N \quad (2.14)$$

Отже, середня кількість запитів ініціації потоку в кореневому контролері визначається як:

$$\lambda_{H,r} = \lambda * \sum_{x=1}^{N} \sum_{y=1,y\neq x}^{N} I_{x,y}(1,1) = \lambda * (N^2 - \frac{N^2}{m_H}) \quad (2.15)$$

І середній час прибуття запиту до кожного листового контролера буде:

$$\lambda_{H,l} = \lambda * \sum_{x=1}^{N} \sum_{y=1,y\neq x}^{N} \sum_{j=1}^{m_H} \frac{I_{x,y}(2,j)}{m_H} = \lambda * \left(\left(N^2 - \frac{N^2}{m_H}\right) * (d_H + 1)\right) + \\ + \frac{N^2}{m_H} - N \quad (2.16)$$

Нехай T_H - час відгуку на запит ініціалізації потоку. T_H можна розділити на дві частини: час відгуку T_r на кореневому контролері і час відгуку T_l на листовому контролері. Отримуємо $E\{T_H\} = E\{T_r\} + E\{T_l\}$. Нехай $T_{rx,y}$ буде час відгуку на запит ініціації потоку $f_{x,y}$ на кореневому контролері (якщо $f_{x,y}$ це локальний потік, то $T_{rx,y} = 0$). $T_{ci,j}$ - час відгуку для запиту ініціації потоку $c_{i,j}$.

Тож отримуємо:

$$E\{T_r\} = \frac{\sum_{x=1}^{N} \sum_{y=1,y\neq x}^{N} E\{T_{r_{x,y}}\}}{N*(N-1)} = \frac{\sum_{x=1}^{N} \sum_{y=1,y\neq x}^{N} E\{T_{C_{1,1}}\} * I_{x,y}(1,1)}{N*(N-1)} = \frac{N - \frac{N}{m_H}}{N-1} * \frac{1}{\mu_{H,r} - \lambda_{H,r}} \quad (2.17)$$

Якщо $f_{x,y}$ це глобальний потік, запит ініціації генерований $f_{x,y}$ буде

поділений кореневим контролером на $\sum_{j=1}^{m_H} I_{x,y}(2,j)$ локальних запитів. Таким чином, $Tl_{x,y}$ буде дорівнювати найдовшому часу відгуку для локальних запитів.

Якщо fx,y - це локальний потік, вираз Tlx,y залишиться без змін. Оскільки є незалежною однаково розподіленою величиною і має

негативне експоненціальне розподілення з середнім значенням $\frac{1}{\mu_{H,l}-\lambda_{H,l}}$, то

$$P\{Tl_{x,y} < t\} = \prod_{j=1}^{m_j} P\left\{I_{x,y}(2,j) * T_{C_{2,j}} < t\right\} = \left(1 - e^{(\lambda_{H,r}-\mu_{H,r})*t}\right)^{\sum_{j=1}^{m_H} I_{x,y}(2,j)} \quad (2.18)$$

Нехай $d_x = \sum_{j=1}^{m_H} I_{x,y}(2,j)$ Тоді функція щільності ймовірності буде $f_{Tl_{x,y}}(t) = d_{x,y} * (1 - e^{(\lambda_{H,r}-\mu_{H,r})*t})^{d_{x,y}-1} * (\lambda_{H,r} - \mu_{H,r}) * e^{(\lambda_{H,r}-\mu_{H,r})*t}$

Таким чином, середнє значення Tlx,y буде

$$E(Tl_{x,y}) = \int_0^{\infty} f_{Tl_{x,y}}(t) * t\, dt = \frac{d_{x,y}}{\lambda_{H,r}-\mu_{H,r}} * \sum_{i=0}^{d_{x,y}-1} \binom{d_{x,y}-1}{i} * \frac{(-1)^i}{d_{x,y}^2} \leq \frac{\ln d_{x,y}+1}{\lambda_{H,r}-\mu_{H,r}} \quad (2.19)$$

Виходячи з цього, час середньої відповіді контролера в ієрархічній структурі буде

$$E\{T_H\} = \frac{\frac{N-\frac{N}{m_H}}{N-1}}{\mu_{H,r}-\lambda_{H,r}} + \frac{\ln\left(\frac{N-\frac{N}{m_H}}{N-1} * d_H + 1\right)+1}{\mu_{H,l}-\lambda_{H,l}}. \quad (2.20)$$

При розрахунках середнього часу відгуку контролера в різних структурах були отримані результати, наведені в таблиці 2.1. Для розрахунку бралися наступні дані: кількість вузлів N = 100, швидкість прибуття запитів в секунду λ = 10, кількість контролерів в децентралізованих структурах mD = 10 і середня дистанція контролерів dD = 5.

Таблиця 2.1 – Середній час відгуку контролера в різних структурах

Тип структури	Централізована	Децентралізована (локальна)	Децентралізована (глобальна)	Ієрархічна
E, с	$1{,}194*10^{-4}$	$1{,}9*10^{-6}$	$1{,}026*10^{-5}$	$3{,}91*10^{-6}$

Базуючись на результатах досліджень, можна зробити висновок, що найбільш ефективною топологією рівня управління є децентралізована з локальною видимістю мережі. Проте, в даному випадку ми розглядали мережу, де один контролер відповідає за свою підмережу. Це виглядає як об'єднання централізованих мереж. За результатами підрахунків, мережа централізована архітектура рівня контролю найгірше масштабується і має найгірші показники середнього часу відгуку контролера. Окрім того, навантаження на один контролер може бути значним. Тобто, не дивлячись на те, що при децентралізованій локальній архітектурі, кожному контролеру потрібно оброблювати запити зі значно меншої кількості вузлів, ніж в випадку з децентралізованою локальною структурою, все одно можливі випадки, коли навантаження на один контролер в підмережі буде значно більше очікуваного. А це негативно впливає на масштабованість рівня управління і на надійність мережі в цілому, оскільки, при відмовленні одного єдиного контролера, що управляє підмережею, можуть виникнути проблеми.

Значно кращим варіантом буде використання декількох контролерів, замість одного, для управління підмережею. Фактично децентралізувати контроль підмережі. Використовувати для даних цілей децентралізовану локальну або ієрархічну архітектуру занадто складно. Оскільки, в будь-якому випадку організація цих топологій потребує більше ресурсів і часу для налаштування, ніж звичайна глобальна децентралізована архітектура. Окрім того, якщо вузлів в підмережі не так багато, ніякої різниці зі звичною глобальною децентралізованою топологією не буде.

Тому було вирішено поєднати децентралізовану локальну і децентралізовану глобальну структури. На рисунку 2.5 можна побачити схематичне зображення цієї архітектури.

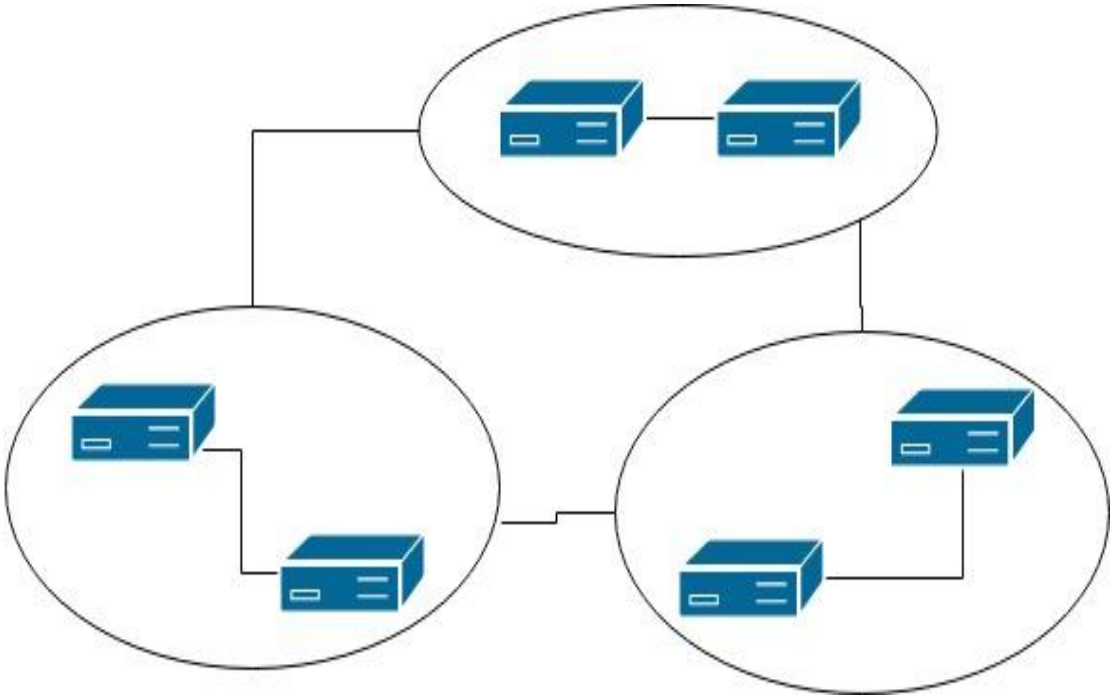


Рисунок 2.5 - Децентралізована гібридна архітектура (локально- глобальна)

$$\lambda_{sub} = \frac{\frac{N}{M}*\left(\frac{N}{M}-1\right)*\lambda}{m_D} \tag{2.21}$$

$$E\{T_c(N)\} = \frac{\frac{N}{M}}{\mu_{sub}-\lambda_{sub}} \tag{2.22}$$

Будемо вважати групу контролерів єдиним цілим. Тому надалі необхідно використовувати формули для розрахунків показників децентралізованої локальної архітектури. Замість кількості фізичних вузлів використовується кількість угрупувань M.

$$\lambda_{main} = \lambda * \frac{\left(M^2-\frac{M^2}{m_D}\right)*(d_D+1)+(\frac{N^2}{m_D}-M)}{m_D}, \tag{2.23}$$

$$\mu_{main} = \frac{K}{g(\frac{M}{m_D}+m_D-1)} \tag{2.24}$$

Звідси середній час відгуку контролера:

$$E\{T_{D,l}\} = \frac{1+\frac{M*(m_D)}{(M-1)*m_D}*d_D}{\mu_{main}-\lambda_{main}} + \frac{\frac{N}{M}}{\mu_{sub}-\lambda_{sub}} \quad (2.25)$$

Як можна побачити в таблиці 2.2, при використанні гібридної децентралізованої структури можна отримати майже в 5 разів менший час відгуку контролера.

Таблиця 2.2 - Середній час відгуку контролера в різних структурах з урахуванням гібридної

Тип структури	Централізована	Децентралізована (локальна)	Децентралізована (глобальна)	Ієрархічна	Децентралізована (гібридна)
E, с	$1{,}194*10^{-4}$	$1{,}9*10^{-6}$	$1{,}026*10^{-5}$	$3{,}91*10^{-6}$	$4{,}7*10^{-7}$

2.2 Захисне перемикання (резервування)

Тож розглянемо окремий SDN контролер для оцінки забезпечення надійності системи[53].

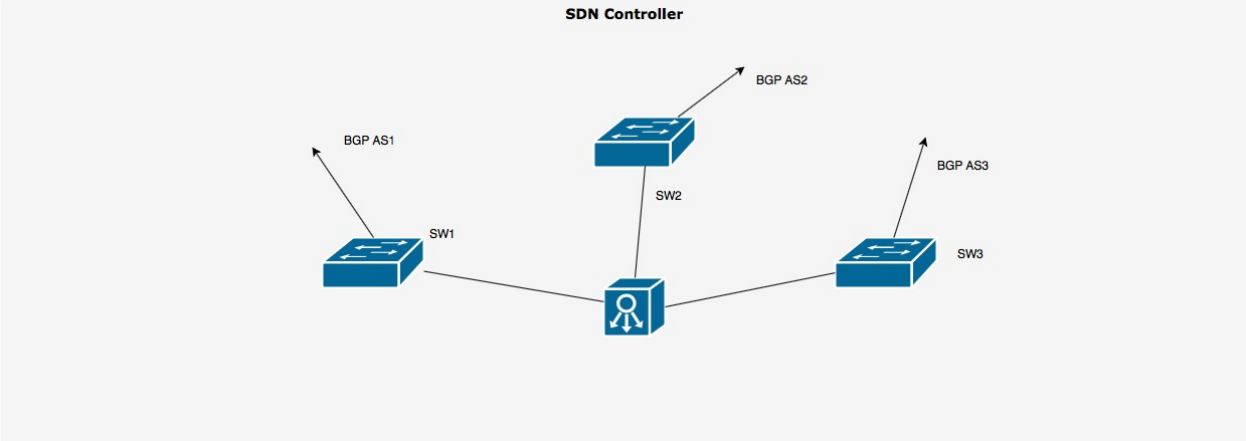


Рисунок 2.7 – Сегмент досліджуванної мережі SDN

Аналіз надійності телекомунікаційних систем проводиться за допомогою аналітичних методів, а також імітаційного і статичного моделювання.

Основою аналітичних методів є теорія випадкових процесів (в нашому завданні - марковських). За допомогою однорідних марковських процесів з кінцевим числом станів описується система при обмеженнях. Час перебування в одному стані розподілено по показовому закону. Даний розподіл можна використовувати лише тоді, коли потоки є найпростішими, тобто мають властивості ординарності, стаціонарності і відсутності післядії.

Випадкові процеси зустрічаються в теорії надійності виходять за межі марковських процесів. Якщо відмовитися від використання експоненціального відмов і відновлень, то це призведе до труднощів складання інтегродиференціальних рівнянь [40].

У справжнім методах розрахунку надійності приймається допущення, що відмови елементів незалежні, і система потрапляє в стан відмови при відмові певного числа елементів.

На рисунку 2.7 представлена схема сегменту досліджуваної мережі. Контролер SDN - це самий технічно складний пристрій мережі, якщо відмовить контролер, то станеться обрив зв'язку з зовнішніми мережами. Для зв'язку з зовнішніми мережами використовуються маршрути через автономні системи BGP [41].

Для дослідження впливу резервування SDN контролера, вводимо допущення при обчисленнях:

- при відмові одного з маршрутів, залишившийся смуги пропускання залишається досить для задоволення підприємства;
- розглянута мережа вважається непрацездатною при відмові контролера SDN, а також при відмові всіх комутаторів;
- при роботі мережі, в один момент часу може відмовити тільки один сервер;
- час відновлення контролера набагато більше часу відновлення комутатора, тому відновлення комутатора відбувається непомітно при одночасному відновленні контролера.

Для даної мережі складемо список станів:

1) відмови відсутні;

2) відмова одного комутатора;

3) відмова двох комутаторів;

4) відновлення комутатора при робочому сервері;

5) відновлення двох комутаторів при робочому сервері;

6) відмова сервера;

7) відмова комутатора і сервера;

8) відмова сервера і двох комутаторів;

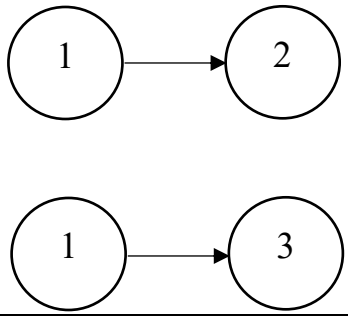
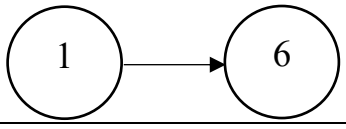
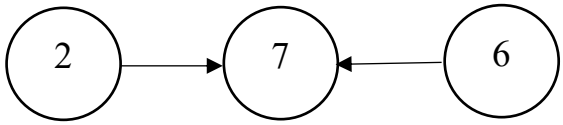
9) відновлення контролера;

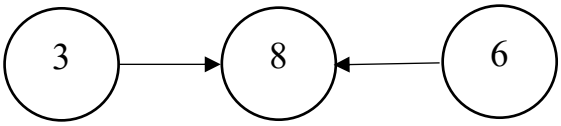
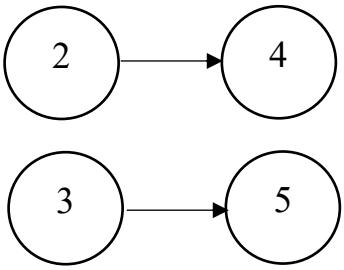
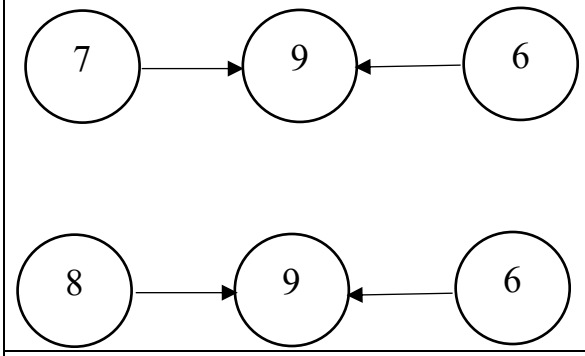
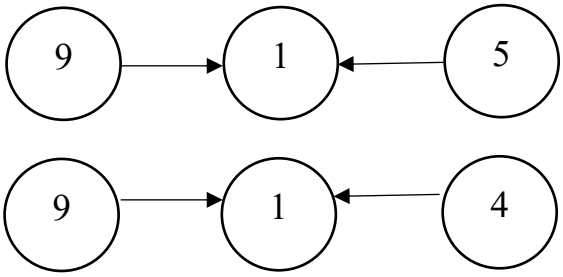
10) контролер з кластера серверів непрацездатний.

При резервуванні система непрацездатна в стані 9 і 10, при відсутності резервування система вважається непрацездатною в станах 6, 7, 8, і 9.

Необхідно скласти таблицю переходів між станами для досліджуваної системи (таблиця 2.3)

Таблиця 2.3 – Переходи між станами досліджуваної системи

Перехід	Опис
	Відбувається відмова комутатора або відмова двох комутаторів, інтенсивності відмови комутаторів рівні
	Відмова сервера
	при відмові сервера або комутатора, відбувається відмова комутатора або сервера

	
	перехід в стан відновлення
	відновлення сервера, при фоновому відновленні комутатора
	ліквідація відмов

Якщо з'єднати всі ці станами отриманими переходами, то вийде граф досліджуваної мережі (рис. 2.8).

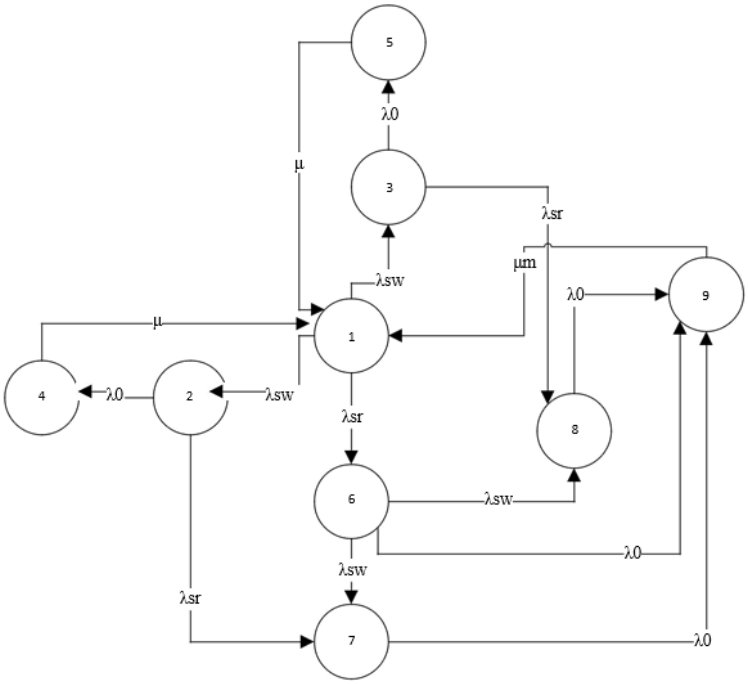


Рисунок 2.8 – Граф стану досліджуваної мережі при відсутності резервування

При використанні резервування контролера SDN з'являється новий стан, при якому система переходить в стан №10 - контролер з кластера серверів непрацездатний.

При використанні нового стану і утворилися логічних переходів між новим станом і вихідними станами системи виходить новий граф станів мережі (рис. 2.9).

Всі переходи між станами відбуваються з заданими в таблиці 2.4 інтенсивностями.

Таблиця 2.4 – значення інтенсивностей переходів між станами для досліджуваної мережі

Позначення	Значення	Опис
λsw	1/516593 $ч^{-1}$	Інтенсивність відмов комутаторів
λsr	1/1700000 $ч^{-1}$	Інтенсивність відмови сервера
λ0	1/0,5 – 1/24 $ч^{-1}$	Інтенсивність виявлення відмов
μ	1/4 $ч^{-1}$	Інтенсивність відновлення комутатора
μm	1/6 $ч^{-1}$	Інтенсивність відновлення контролера

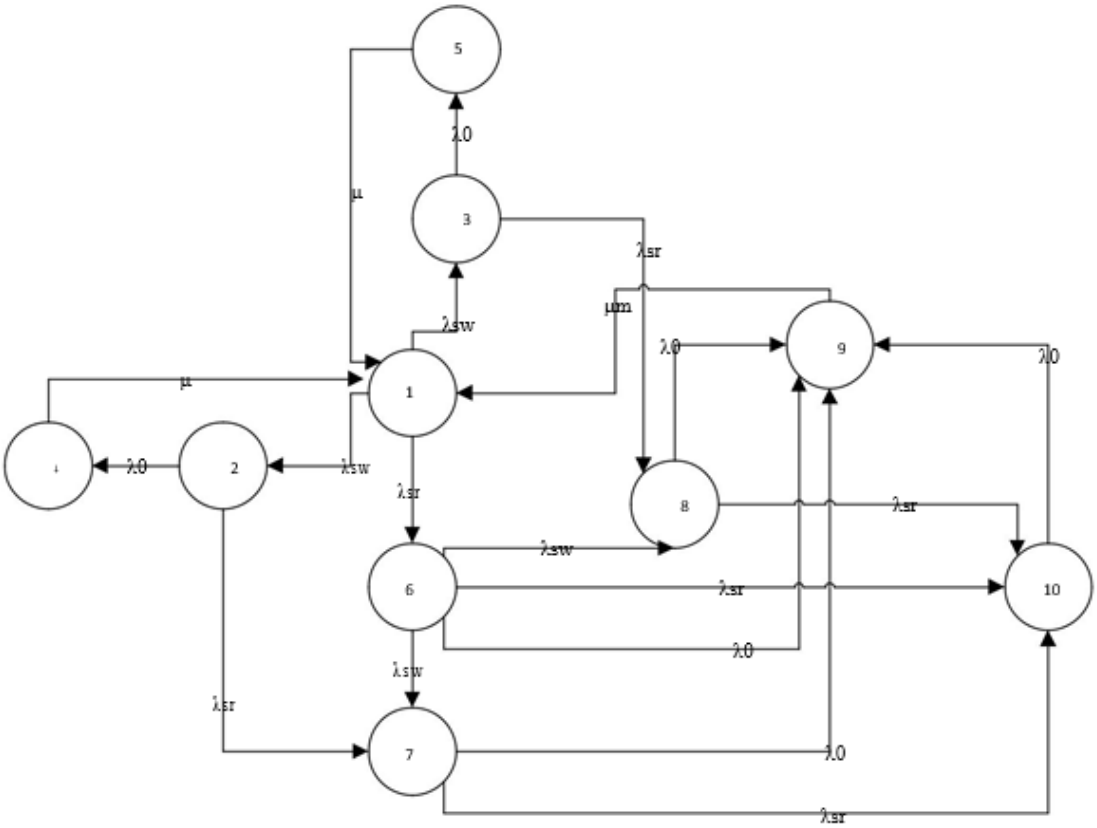


Рисунок 2.9 – Граф станів досліджуваної мережі із застосуванням резервування контролера SDN

Інтенсивності відмов комутаторів і сервера [42] [43].

Складемо рівняння для визначення ймовірностей кожного стану марковського процесу для даної системи без резервування і з застосуванням резервування (диференціальні рівняння А.Н. Колмогорова).

Система диференціальних рівнянь Колмогорова для нерезервованої системи (2.26) Має вигляд

$$\begin{cases} \frac{dP_1(t)}{dt} = -(2\lambda_{sw} + \lambda_{sr})P_1 + \mu P_3 + \mu P_4 + \mu_m P_8 \\ \frac{dP_2(t)}{dt} = \lambda_{sw} P_1 - (\lambda_0 + \lambda_{sr})P_2 \\ \frac{dP_3(t)}{dt} = \lambda_{sw} P_1 - (\lambda_0 + \lambda_{sr})P_3 \\ \frac{dP_4(t)}{dt} = \lambda_0 P_2 - \mu P_4 \\ \frac{dP_5(t)}{dt} = \lambda_0 P_3 - \mu P_5 \\ \frac{dP_6(t)}{dt} = \lambda_{sr} P_1 - (2\lambda_{sw} + \lambda_0)P_6 \\ \frac{dP_7(t)}{dt} = \lambda_{sr} P_2 + \lambda_{sw} P_6 - \lambda_0 P_7 \\ \frac{dP_8(t)}{dt} = \lambda_{sr} P_3 + \lambda_{sw} P_6 - \lambda_0 P_8 \\ \frac{dP_9(t)}{dt} = \lambda_0 P_6 + \lambda_0 P_7 + \lambda_0 P_8 - \mu_m P_9 \end{cases} \quad (2.26)$$

У практиці розрахунків надійності систему рівнянь Колмогорова можна отримати безпосередньо з вигляду графа станів об'єкта.

Рішення системи (2.26) можна отримати за відомими правилами рішення системи диференціальних рівнянь. Однак його можна істотно спростити, якщо врахувати, що розглядається стаціонарний марковський процес, для якого $dP_i(t) = 0$ (ймовірності станів не змінюються з плином часу) [44].

Тоді якщо замінити ліву частину рівнянь на 0 і ввести в систему нормувального умова

$$\sum_{i=0}^{n} P_i = 1 \quad (2.27)$$

Замінюючи в рівняннях Колмогорова ліві частини нульовими значеннями, отримаємо систему лінійних алгебраїчних рівнянь, що описують стаціонарний режим. Така система рівнянь має вигляд:

$$\begin{cases} 0 = -(2\lambda_{sw} + \lambda_{sr})P_1 + \mu P_3 + \mu P_4 + \mu_m P_8 \\ 0 = \lambda_{sw} P_1 - (\lambda_0 + \lambda_{sr})P_2 \\ 0 = \lambda_{sw} P_1 - (\lambda_0 + \lambda_{sr})P_3 \\ 0 = \lambda_0 P_2 - \mu P_4 \\ 0 = \lambda_0 P_3 - \mu P_5 \\ 0 = \lambda_{sr} P_1 - (2\lambda_{sw} + \lambda_0)P_6 \\ 0 = \lambda_{sr} P_2 + \lambda_{sw} P_6 - \lambda_0 P_7 \\ 0 = \lambda_{sr} P_3 + \lambda_{sw} P_6 - \lambda_0 P_8 \\ 0 = \lambda_0 P_6 + \lambda_0 P_7 + \lambda_0 P_8 - \mu_m P_9 \end{cases} \quad (2.28)$$

Як видно з системи (2.28) деякі значення ймовірностей будуть однаковими, отже для спрощення системи необхідно виключити однакові рівняння, а в нормувальній умові (2.27) замінити коефіцієнт. Підсумкова система рівнянь для якої будуть проводитися розрахунки має вигляд:

$$\begin{cases} 0 = \lambda_{sw} P_1 - (\lambda_0 + \lambda_{sr})P_2 \\ 0 = \lambda_0 P_2 - \mu P_4 \\ 0 = \lambda_{sr} P_1 - (2\lambda_{sw} + \lambda_0)P_6 \\ 0 = \lambda_{sr} P_2 + \lambda_{sw} P_6 - \lambda_0 P_7 \\ 0 = \lambda_0 P_6 + \lambda_0 P_7 + \lambda_0 P_8 - \mu_m P_9 \\ P_1 + 2P_2 + 2P_4 + P_6 + 2P_7 + P_9 = 1 \end{cases} \quad (2.29)$$

Підставивши значення інтенсивностей і вирішивши систему рівнянь, отримаємо значення ймовірностей станів системи.

Досліджувану систему лінійних алгебраїчних рівнянь представимо у вигляді матриці і вектора. Матриця коефіцієнтів (2.30) при невідомих можливостях станів системи і вектор вільних членів (2.31).

$$X = \begin{pmatrix} -\lambda_{sw} & \lambda_0 + \lambda_{sr} & 0 & 0 & 0 & 0 \\ 0 & -\lambda_0 & \mu & 0 & 0 & 0 \\ -\lambda_{sr} & 0 & 0 & 2\lambda_{sw} + \lambda_0 & 0 & 0 \\ 0 & -\lambda_{sr} & 0 & -\lambda_{sw} & \lambda_0 & 0 \\ 0 & 0 & 0 & -\lambda_0 & -2\lambda_0 & \mu_m \\ 1 & 2 & 2 & 1 & 2 & 1 \end{pmatrix} \quad (2.30)$$

$$Y = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} \tag{2.31}$$

В результаті роботи функції lsolve (X, Y) отримуємо вектор значень граничних ймовірностей системи.

Таблиця 2.3 - Значення ймовірностей станів системи при різних інтенсивностях виявлення відмов

λ, ч⁻¹ / P_i	0,5	1	2	4	5	10	15	20	24
P_1	0.9999787 55080811	0.9999765 25300732	0.9999720 65770406	0.9999631 4682908	0.9999586 8741808	0.9999363 90959674	0.9999140 95495552	0.9998918 01025647	0.9998739 66165514
P_2	9.6785908 92341742 *10^-7	1.9357132 92823544 *10^-6	3.8714070 43200608 *10^-6	7.7427359 17677192 *10^-6	9.6783710 42307647 *10^-6	1.9356253 54999978 *10^-5	2.9033647 55625712 *10^-5	3.8710553 09425739 *10^-5	3.8710553 09425739 *10^-5
P_3	9.6785908 92341742 *10^-7	1.9357132 92823544 *10^-6	3.8714070 43200608 *10^-6	7.7427359 17677192 *10^-6	9.6783710 42307647 *10^-6	1.9356253 54999978 *10^-5	2.9033647 55625712 *10^-5	3.8710553 09425739 *10^-5	4.6451725 84980608 *10^-5
P_4	7.7428727 13873395 *10^-6	7.7428531 71294175 *10^-6	7.7428140 86401218 *10^-6	7.7427359 17677193 *10^-6	7.7426968 33846117 *10^-6	7.7425014 19999912 *10^-6	7.7423060 15001899 *10^-6	7.7421106 18851476 *10^-6	7.7419543 08301015 *10^-6
P_5	7.7428727 13873395 *10^-6	7.7428531 71294175 *10^-6	7.7428140 86401218 *10^-6	7.7427359 17677193 *10^-6	7.7426968 33846117 *10^-6	7.7425014 19999912 *10^-6	7.7423060 15001899 *10^-6	7.7421106 18851476 *10^-6	7.7419543 08301015 *10^-6
P_6	2.9411082 92252383 *10^-7	5.8821920 81687397 *10^-7	1.1764286 15302545 *10^-6	2.3528180 27201446 *10^-6	2.9409980 3233458* 10^-6	5.8817510 57197453 *10^-6	8.8222590 97588638 *10^-6	1.1762522 17650559 *10^-5	1.4114556 28283036 *10^-5
P_7	5.6932840 87269202 *10^-13	2.2773060 17735746 *10^-12	9.1091631 35140848 *10^-12	3.6436165 05983808 *10^-11	5.6931127 06903878 *10^-11	2.2771689 1786334* 10^-10	5.1234587 03796127 *10^-10	9.1080664 03557052 *10^-10	1.3115264 71032283 *10^-9
P_8	5.6932840 87269202 *10^-13	2.2773060 17735746 *10^-12	9.1091631 35140848 *10^-12	3.6436165 05983808 *10^-11	5.6931127 06903878 *10^-11	2.2771689 1786334* 10^-10	5.1234587 03796127 *10^-10	9.1080664 03557052 *10^-10	1.3115264 71032283 *10^-9
P_9	3.5293436 1458467* 10^-6	3.5293425 76684651 *10^-6	3.5293405 00886445 *10^-6	3.5293363 49297348 *10^-6	3.5293342 73506462 *10^-6	3.5293238 94588615 *10^-6	3.5293135 15731758 *10^-6	3.5293031 3693589* 10^-6	3.5292948 33943107 *10^-6
ΣP	1	1	1	1	1	1	1	1	1

Знаючи значення ймовірностей, знайдемо коефіцієнт готовності, як суму ймовірностей і-х працездатних станів:

$$K_r(t) = \sum_{i=1}^{n} P_i(t) \tag{2.32}$$

де n - число працездатних станів;

$P_i(t)$ - ймовірність і-го робочого стану.

Для системи без використання резервування працездатними вважаються стану: 1, 2, 3, 4, 5. Отже коефіцієнт готовності для нерезервованої системи:

$$K_r(t) = P_1 + P_2 + P_3 + P_4 + P_5 \tag{2.33}$$

З огляду на, що ймовірності деяких станів однакові, спростимо (2.33):

$$K_r(t) = P_1 + 2P_2 + 2P_4 \tag{2.34}$$

Використовуючи результати з таблиці 2.3 знайдемо значення коефіцієнта готовності при різних інтенсивностях виявлення відмов.

Таблиця 2.4 – Коефіцієнт готовності при різних інтенсивностях виявлення відмов

Інтенсивність виявлення відмов λ0, ч-1	Коефіцієнт готовності, Кг
0,5	0.999996176544417
1	0.99999588243366
2	0.999995294212665
4	999994117772751
5	0.999993529553832
10	0.999990588469614
15	0.999987647402695
20	0.999984706353073
24	0.99998235352583

Система диференціальних рівнянь Колмогорова для резервованої системи (2.35):

$$\begin{cases} \frac{dP_1(t)}{dt} = -(2\lambda_{sw} + \lambda_{sr})P_1 + \mu P_3 + \mu P_4 + \mu_m P_8 \\ \frac{dP_2(t)}{dt} = \lambda_{sw}P_1 - (\lambda_0 + \lambda_{sr})P_2 \\ \frac{dP_2(t)}{dt} = \lambda_{sw}P_1 - (\lambda_0 + \lambda_{sr})P_3 \\ \frac{dP_4(t)}{dt} = \lambda_0 P_2 - \mu P_4 \\ \frac{dP_5(t)}{dt} = \lambda_0 P_3 - \mu P_5 \\ \frac{dP_6(t)}{dt} = \lambda_{sr}P_1 - (2\lambda_{sw} + \lambda_0 + \lambda_{sr})P_6 \\ \frac{dP_7(t)}{dt} = \lambda_{sr}P_2 + \lambda_{sw}P_6 - (\lambda_0 + \lambda_{sr})P_7 \\ \frac{dP_8(t)}{dt} = \lambda_{sr}P_3 + \lambda_{sw}P_6 - (\lambda_0 + \lambda_{sr})P_8 \\ \frac{dP_9(t)}{dt} = \lambda_0 P_6 + \lambda_0 P_7 + \lambda_0 P_8 - \mu_m P_9 + \lambda_0 P_{10} \\ \frac{dP_{10}(t)}{dt} = \lambda_{sr}P_6 + \lambda_{sr}P_7 + \lambda_{sr}P_8 - \lambda_0 P_{10} \end{cases} \quad (2.35)$$

Замінюючи в рівняннях Колмогорова ліві частини нульовими значеннями, отримаємо систему лінійних алгебраїчних рівнянь, що описують стаціонарний режим. Для системи (рис. 3.3) така система рівнянь має вигляд:

$$\begin{cases} 0 = -(2\lambda_{sw} + \lambda_{sr})P_1 + \mu P_3 + \mu P_4 + \mu_m P_8 \\ 0 = \lambda_{sw} P_1 - (\lambda_0 + \lambda_{sr})P_2 \\ 0 = \lambda_{sw} P_1 - (\lambda_0 + \lambda_{sr})P_3 \\ 0 = \lambda_0 P_2 - \mu P_4 \\ 0 = \lambda_0 P_3 - \mu P_5 \\ 0 = \lambda_{sr} P_1 - (2\lambda_{sw} + \lambda_0 + \lambda_{sr})P_6 \\ 0 = \lambda_{sr} P_2 + \lambda_{sw} P_6 - (\lambda_{0+}\lambda_{sr})P_8 \\ 0 = \lambda_0 P_6 + \lambda_0 P_7 + \lambda_0 P_8 - \mu_m P_9 + \lambda_0 P_{10} \\ 0 = \lambda_{sr} P_6 + \lambda_{sr} P_7 + \lambda_{sr} P_8 - \lambda_0 P_{10} \end{cases} \quad (2.36)$$

Прибираємо зайві рівняння, замінюємо перше рівняння нормувального умовою, отримуємо систему вигляду (2.37):

$$\begin{cases} 0 = \lambda_{sw} P_1 - (\lambda_0 + \lambda_{sr})P_2 \\ 0 = \lambda_0 P_2 - \mu P_4 \\ 0 = \lambda_{sr} P_1 - (2\lambda_{sw} + \lambda_0 + \lambda_{sr})P_6 \\ 0 = \lambda_{sr} P_2 + \lambda_{sw} P_6 - (\lambda_0 + \lambda_{sr})P_7 \\ 0 = \lambda_0 P_6 + 2\lambda_0 P_7 - \mu_m P_9 + \lambda_0 P_{10} \\ 0 = \lambda_{sr} P_6 + 2\lambda_{sr} P_7 - \lambda_0 P_{10} \\ P_1 + 2P_2 + 2P_4 + P_6 + 2P_7 + P_9 = 1 \end{cases} \quad (2.37)$$

Досліджувану систему лінійних алгебраїчних рівнянь представимо у вигляді матриці і вектора. Матриця коефіцієнтів (2.38) при невідомих можливостях станів системи і вектор вільних членів (2.39).

$$\begin{pmatrix} -\lambda_{sw} & \lambda_0 + \lambda_{sr} & 0 & 0 & 0 & 0 & 0 \\ 0 & -\lambda_0 & \mu & 0 & 0 & 0 & 0 \\ -\lambda_{sr} & 0 & 0 & 2\lambda_{sw} + \lambda_0 + \lambda_{sr} & 0 & 0 & 0 \\ 0 & -\lambda_{sr} & 0 & -\lambda_{sw} & \lambda_0 + \lambda_{sr} & 0 & 0 \\ 0 & 0 & 0 & -\lambda_0 & -2\lambda_0 & \mu_m & -\lambda_0 \\ 0 & 0 & 0 & -\lambda_{sr} & -2\lambda_{sr} & 0 & \lambda_0 \\ 1 & 2 & 2 & 1 & 2 & 1 & 1 \end{pmatrix} \quad (2.38)$$

$$Y = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} \tag{2.39}$$

В результаті роботи функції lsolve (X, Y) отримуємо вектор значень граничних ймовірностей системи.

ми.

Таблиця 2.5 – Значення ймовірностей станів системи при різних інтенсивностях виявлення відмов

λ_0, $ч^{-1}$ / P_i	0.5	1	2	4	5	10	15	20	24
P_1	0.999978755080811	0.999976525300732	0.999972065770406	0.99996314682908	0.99995868741808	0.999936390959674	0.999914095495552	0.999891801025647	0.999873966165514
P_2	9.678590892341742*10^-7	1.935713292823544*10^-6	3.871407043200608*10^-6	7.742735917677192*10^-6	9.678371042307647*10^-6	1.935625354999978*10^-5	2.903364755625712*10^-5	3.871055309425739*10^-5	4.645172584980608*10^-5
P_3	9.678590892341742*10^-7	1.935713292823544*10^-6	3.871407043200608*10^-6	7.742735917677192*10^-6	9.678371042307647*10^-6	1.935625354999978*10^-5	2.903364755625712*10^-5	3.871055309425739*10^-5	4.645172584980608*10^-5
P_4	7.742872713873395*10^-6	7.742853171294174*10^-6	7.742814086401216*10^-6	7.742735917677192*10^-6	7.742696833846119*10^-6	7.742501419999912*10^-6	7.742306015001899*10^-6	7.742110618851476*10^-6	7.741954308301014*10^-6
P_5	7.742872713873395*10^-6	7.742853171294174*10^-6	7.742814086401216*10^-6	7.742735917677192*10^-6	7.742696833846119*10^-6	7.742501419999912*10^-6	7.742306015001899*10^-6	7.742110618851476*10^-6	7.741954308301014*10^-6
P_6	2.941107427222461*10^-7	5.882188621589 84*10^-7	1.176427231281225*10^-6	2.352812491257784*10^-6	2.940989382533247*10^-6	5.881716460204763*10^-6	8.822181259333107*10^-6	1.17623838062337*10^-5	1.411435703983217*10^-5
P_7	5.693281575550584*10^-13	2.277304008412807*10^-12	9.109147060012178*10^-12	3.643603646300351*10^-11	5.693087590533343*10^-11	2.277148825727233*10^-10	5.123390895974683*10^-10	9.10790568139968*10^-10	1.311498699278956*10^-9
P_8	5.693281575550584*10^-13	2.277304008412807*10^-12	9.109147060012178*10^-12	3.643603646300351*10^-11	5.693087590533343*10^-11	2.277148825727233*10^-10	5.123390895974683*10^-10	9.10790568139968*10^-10	1.311498699278956*10^-9
P_9	3.529343614584669*10^-6	3.529342576684652*10^-6	3.529340500886445*10^-6	3.529336349297349*10^-6	3.529334273506462*10^-6	3.529323894588615*10^-6	3.529313515731758*10^-6	3.52930313693589*10^-6	3.529294833943107*10^-6
P_{10}	8.650349452310621*10^-14	3.460137745688239*10^-13	1.384053470088641*10^-12	5.536200854895788*10^-12	8.650303659661937*10^-12	3.460101111747004*10^-11	7.785181709569678*10^-11	1.384024163219997*10^-10	1.992985417020808*10^-10
ΣP_i	1	1	1	1	1	1	1	1	1

Для системи без використання резервування працездатними станами вважаються: 1 - 8. Отже коефіцієнт готовності для нерезервованої системи:

$$K_r(t) = P_1 + P_2 + P_3 + P_4 + P_5 + P_6 + P_7 + P_8 \quad (2.40)$$

З огляду, що ймовірності деяких станів однакові, спростимо (2.40):

$$K_r(t) = P_1 + 2P_2 + 2P_4 + P_6 + 2P_7 \quad (2.41)$$

Використовуючи результати з таблиці 2.5 знайдемо значення коефіцієнта готовності при різних інтенсивностях виявлення відмов.

Таблиця 2.6 – Коефіцієнт готовності при різних інтенсивностях виявлення відмов

інтенсивність виявлення відмов λ0, ч-1	Коефіцієнт готовності, Кг
0,5	0.999996470656299
1	0.999996470657077
2	0.999996470658115
4	0.999996470658114
5	0.999996470657077
10	0.999996470641504
15	0.999996470608632
20	0.99999647055846
24	0.999996470505867

Після отримання чисельних значень коефіцієнтів готовності, можна побудувати графік залежності коефіцієнта готовності від інтенсивності виявлення відмов, при використанні резервування контролера і для нерезервованої системи (рис. 2.10).

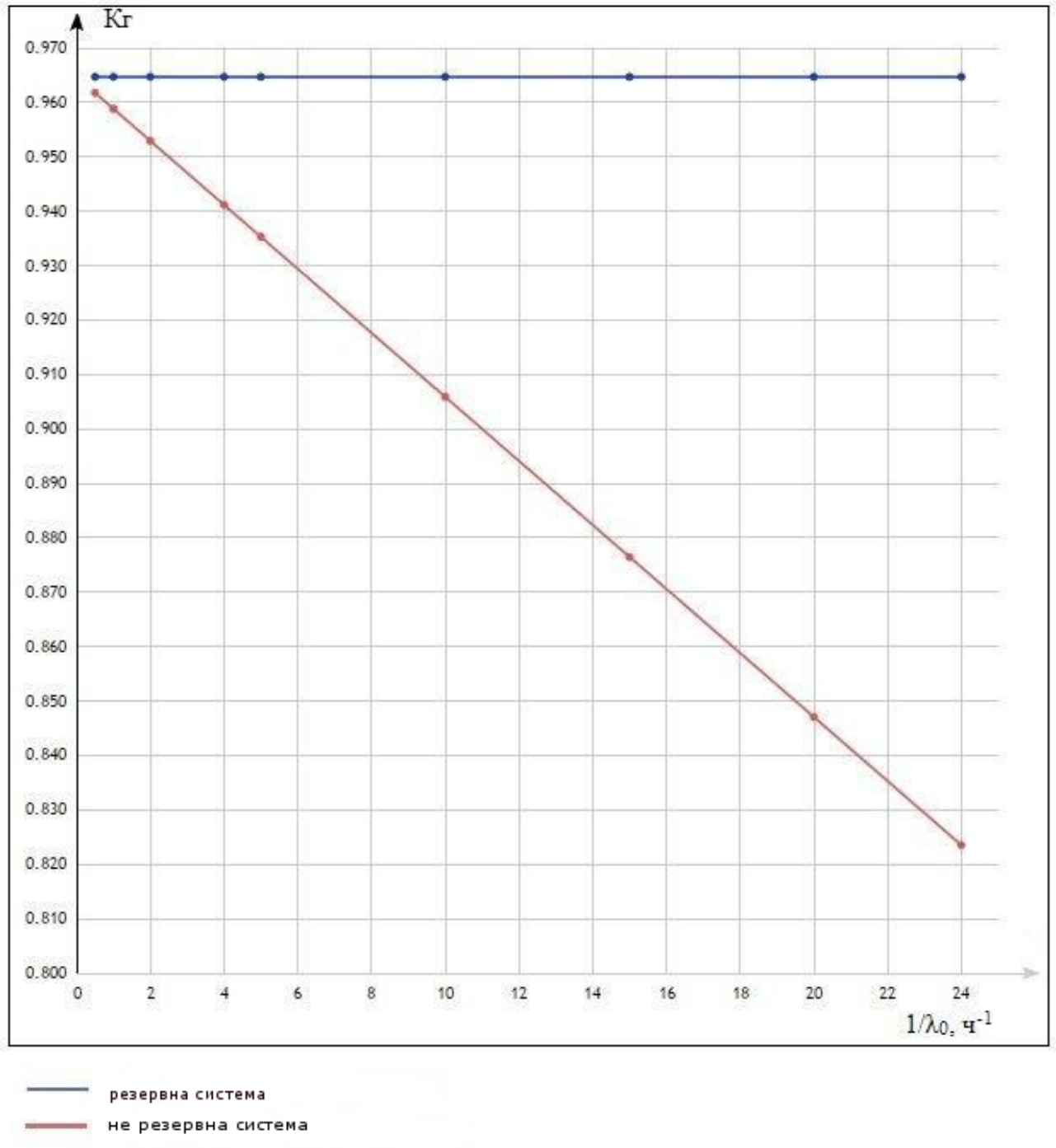


Рисунок 2.10 – Графік залежності коефіцієнта готовності від інтенсивності виявлення відмов

Роблячи висновок по результатам розрахунку і наочному уявленню (рис. 2.10), можна сказати, що:

- при однакових числових значеннях, коефіцієнт готовності при використанні резервування вище ніж у нерезервованої системи;

- при використанні резервування $К_г$ менш залежний від інтенсивності виявлення відмов.

Виходячи з вищеописаних результатів можемо узагальнено зобразити проектовану мережу підприємства наступним чином (рис. 2.11):

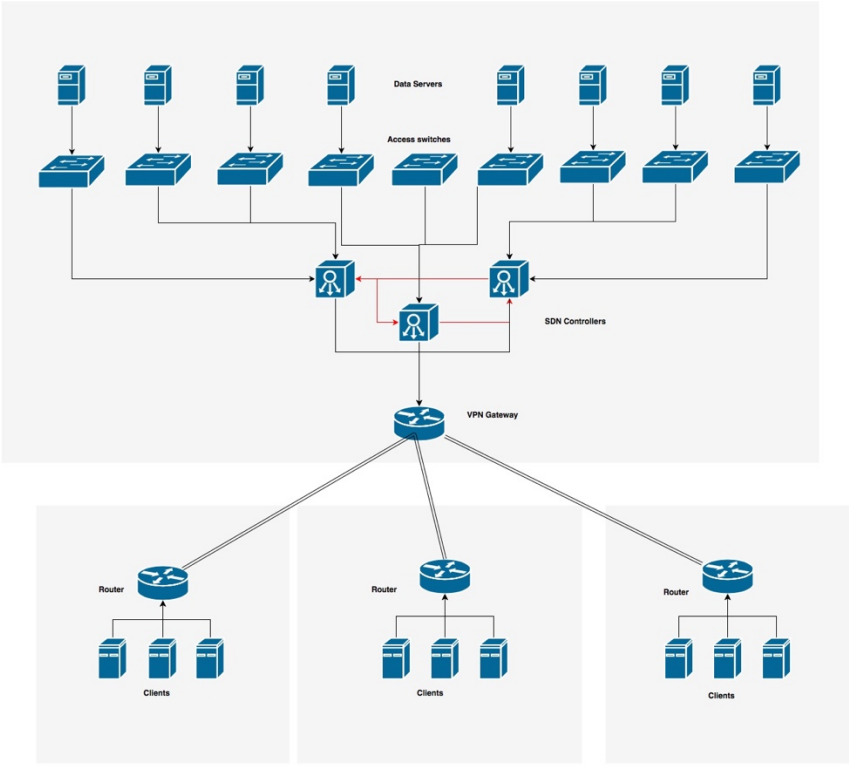


Рисунок 2.11 – Модифікована структура мережі

2.3 Відновлення (перемаршрутизація)

У мережах SDN для підвищення відмовостійкості мережі в площині даних використовують методи відновлення засновані на оригінальному способі відновлення протоколу OpenFlow. Даний метод відновлення заснований на перемаршрутизації, як на основний діючий механізм відкритого протоколу.

Для відновлення використовується алгоритм який фіксує виявлення відмови та складає список трактів порушених цією відмовою (LSP). Для кожної відмови на мережі, керованої контролером, розраховується обхідний шлях. Організовується перемаршрутизація за алгоритмом CSP (Constrained Shortest Path), для робочої частини діючої в контролері мережі.

За результатами роботи алгоритму CSP протокол OpenFlow змінює записи в таблицях комутації в комутаторах підлеглих контролера SDN відповідно до нових розрахованих маршрутів.

Уявімо мережу у вигляді простого спрямованого графа G (N, A), де N-безліч вузлів, а A - безліч всіх дуг (ланок), arc (i, j) - є упорядкована пара, яка виходить з вузла i і надходить на вузол j. Нехай Rst - безліч всіх маршрутів (підмножин A) від початкового вузла s до вузла призначення t. Для будь-якого такого маршруту ми визначаємо вартість F_c і затримки F_D, як

$$\begin{cases} F_c(r) = \sum_{i,j \in r} c_{ij} \\ F_D(r) = \sum_{i,j \in r} d_{ij} \end{cases} \quad (2.42)$$

де c_{ij} і d_{ij} - коефіцієнти вартості і затримок для дуги (i, j).

Тоді проблема CSP може бути сформульована як знаходження:

$$r * = \arg min\{F_c(r) | r \in R_{st}, F_D(r) \leq D_{max}\} \quad (2.43)$$

Таким чином виходить, що пошук нового маршруту r, на підмножині R_{st}, повинен відповідати умовам мінімальної вартості, при затримці що не перевищує максимального заданого значення D_{max}.
Метрика вартості вибирається в такий спосіб:

$$c_{ij} = g_{ij} + d_{ij} \ \forall (i,j) \in A \quad (2.44)$$

де g_{ij} - визначає міру перевантаження трафіку по лінії (i, j), а d_{ij} - міра затримки.

При використанні технології SDN важливо враховувати функції розширення протоколу OpenFlow стандартного контролера, яке забезпечує доставку з використанням OpenQoS. OpenQoS збирає необхідні параметри g_{ij} і d_{ij} , використовуючи використання дороговказу.

Дороговказ – ця функція відповідає за визначення доступності та переадресацію пакетів, використовуючи перемаршрутізацію для розрахунку маршруту. Для цього потрібно збирати дані про сучасний стан мережі.

Розрахунок маршруту – ця функція відповідає за розрахунок і визначення маршрутів для різних типів потоків. Кілька алгоритмів маршрутизації можуть виконуватися паралельно для задоволення вимог до продуктивності і типів різних потоків. В цю функцію поряд з резервуванням послуг вводяться топологія мережі і інформація про управлінні маршрутом [45].

Як вказувалося вище завдання CSP є NP-повною, тому для функції розрахунку маршруту згідно OpenQoS пропонується використовувати алгоритм Lagrigangian Relaxation Aggregated Cost (LARAC), який є поліноміальних алгоритмом часу, який ефективно знаходить хороший маршрут без відхилення від оптимального рішення [46].

Коли функція надання інформації про маршрут оновлює параметри, що вказують QoS, або функція управління топологією виявляє зміна топології, функція обчислення маршруту запускає алгоритм LARAC для вирішення проблеми CSP. Потім контролер оновлює таблиці потоків відповідним чином. Отже, маршрути QoS динамічно встановлюються і здійснюється швидка перемаршрутізація відповідно до встановлених обмежень.

Існують різні алгоритми маршрутизації, які можна використовувати для обчислення маршруту в разі виникнення відмови.

Алгоритм маршрутизації Constrained Bellman-Ford (CBF) виконує пошук по ширині, виявляючи шляху монотонно збільшується затримки при запису і оновленні шляху з найменшою вартістю для кожного вузла, який він відвідує. Він зупиняється, коли перевищується найвище обмеження, або більше немає можливості поліпшити шлях. Так як це розширення використовує затримку замість лічильника переходів, який є безперервною метрикою, таблиця маршрутизації, яка містить записи для всіх можливих затримок, може бути дуже великий, навіть нездійсненного розміру. До того ж, алгоритм CBF має експоненціальний час роботи [47].

Алгоритм Fallback routing передбачає, що в мережі є ранжирування показника. По-перше, алгоритм маршрутизації обчислює найкоротший шлях для першої метрики (тобто вартість), а потім перевіряє, чи може він гарантувати всі інші вимоги QoS. Якщо шлях не вдався, алгоритм намагається знайти інший для наступної метрики, поки не буде знайдений відповідний шлях або маршрутизація завершиться невдало для всіх метрик. Цей алгоритм дуже простий, швидкий і завжди дає відповідне рішення, якщо воно існує, але немає гарантії знайти оптимальний маршрут, і ми нічого не знаємо про якість знайденого шляху [48].

Алгоритм DCA (Delay Constrained Unicast Routing) може вибирати між шляхами найменшої вартості і найменшою затримкою незалежно від вибору попереднього вузла. Цей алгоритм має більш високий, але все ж розумний час роботи, і більш імовірно, що знайде рішення поблизу оптимального, ніж алгоритм Fallback, але жоден з цих алгоритмів не гарантує оптимальності шляху [49].

Існують також алгоритми, засновані на агрегованих витратах, які можуть знайти шлях, що задовольняє обмеженням. Таким алгоритмом є LARAC, який використовує метод релаксації Лангранжа для знаходження оптимального шляху.

Представлений алгоритм агрегованих витрат на основі LARAC - Lagrange Relax заснований на евристиці мінімізації зміненої функції вартості

$$C_\lambda = C + \lambda \cdot \mathrm{d} \tag{2.45}$$

Для цього (фіксованого) λ ми можемо легко обчислити мінімальний шлях (p_λ). Якщо λ = 0 і

$$d(p_\lambda) \leq \Delta_{delay} \tag{2.46}$$

то, ми знайшли оптимальне рішення для початкового завдання.

Якщо

$$d(p_\lambda) > \Delta_{delay} \tag{2.47}$$

то, ми повинні збільшити λ, щоб збільшити домінування затримки в модифікованої функції вартості. Тому ми збільшуємо λ, а оптимальне рішення cλ задовольняє вимогам затримки.

Рішення, що застосовуються до вихідної задачі, можуть, звичайно ж, задовольняти умовам релаксації, тому ми можемо отримати нижню межу вихідної задачі. Якщо знайдений шлях неможливий для умов обмеження, ми збільшуємо його домінування в модифікованої функції вартості, забезпечивши вирішення для підходу до оптимального рішення. Крім того, зменшити різницю між отриманою нижньою межею і оптимумом вихідної задачі. Це і є основа лагранжевой релаксації. Більш детальний опис [50]

За допомогою лагранжевой релаксації ми отримуємо алгоритм, який може знайти оптимальне λ для заданої пари джерел, таким чином, серед агрегованих методів маршрутизації цей алгоритм дає найкраще рішення, яке може бути отримано. Крім того, він дає оцінку для оптимального рішення, хоч у нас і немає гарантії знайти оптимальне рішення, ми завжди отримуємо оцінку рішення, яка показує наскільки вона відрізняється від оптимального рішення.

Вихідний алгоритм LARAC був найкращим серед поліноміальних евристичних алгоритмів, запропонованих до сих пір в літературі. Його вартість найбільш близька до оптимальної вартості, обчисленої за алгоритмом CBF, крім того, вона дає оцінку оптимальності знайдених шляхів.

Можливим подальшим удосконаленням алгоритму LARAC може бути його розширення для обробки двох заданих обмежень при мінімізації третього. Прикладом для цих двох обмежень може бути затримка і число кроків. Потім агрегована функція витрат має містити три тега (вартість, затримка, номер кроку). Наші очікування полягають у тому, що складність алгоритму не збільшиться під час розширення при удосконаленні, як це сталося з алгоритмом CBF [46]

2.4 Висновки до розділу 2

У розділі 2 дипломного проекту було проведено аналіз впливу резервування на SDN мережу, проведено аналіз існуючих структур архітектури рівня контролю, математично визначена середній час відгуку контролера, запропоновано модифікований спосіб структуризації рівня управління SDN, який відрізняється від відомих більшою швидкодією приблизно в 5 разів. Було розглянуто алгоритми CBF та LARAC для відновлення в мережі та проведено аналіз.

3 ЕКОНОМІЧНА ЧАСТИНА

3.1 Розрахунок капітальних витрат

Капітальні витрати – це кошти, призначені для створення і придбання основних фондів і нематеріальних активів, що підлягають амортизації.

В нашому випадку це засоби, витрачені на придбання обладнання фірми, допоміжне обладнання, витрати на виконання монтажних та налагоджувальних робіт.

При визначенні величини проектних капіталовкладень ($К_{пр}$) можна скористатися формулою:

$$К_{пр} = К_{об} + З_{т} + З_{м} + З_{н}, \quad (3.1)$$

де $К_{об}$ – вартість придбання обладнання (засобів автоматизації, програмного забезпечення і т.д.) за проектом;

$З_{м}$ – витрати на монтажні роботи;

$З_{н}$ - витрати на налагоджувальні роботи;

$З_{т}$ – витрати на транспортування.

Витрати на упаковку, транспортування і монтаж (УТМ) визначають як відсоток від вартості обладнання і береться 10% від вартості обладнання [25]

Тоді величина проектних капіталовкладень ($К_{пр}$) визначається формулою:

$$К_{пр} = К_{об} + 0.1 \cdot К_{об}, \quad (3.2)$$

Основне виробниче обладнання проектованої мережі представлено в таблиці 3.1.

Таблиця 3.1 – Витрати на обладнання

Найменування	Кількість	Ціна за од., грн	Сума, грн
SDN контролер HP VAN SDN Controller	3 шт.	13 860	41 580
Ліцензія на вікористання додаткової кількості пристроїв	1 шт.	84 000	84 000
Cisco Catalyst 2960X-48TS-L 48 Port Ethernet Switch	9 шт.	21 240	191 160
Разом			316 740

За формулою 3.2 проектні капіталовкладення складають:

$$К_{пр} = К_{об} + 0.1 \cdot К_{об} = 316740 + 31674 = 348\ 414 \text{ грн}$$

3.2 Розрахунок експлуатаційних витрат

Експлуатаційні витрати - це поточні витрати на експлуатацію та обслуговування об'єкта проектування за певний період (рік), виражені в грошовій формі.

До основних статей експлуатаційних витрат по електротехнічного устаткування відносяться:

- амортизаційні відрахування ($С_а$);
- заробітна плата обслуговуючого персоналу ($С_з$);
- відрахування на соціальні заходи від заробітної плати ($С_с$);
- витрати на технічне обслуговування і поточний ремонт обладнання ($С_т$);
- вартість електроенергії, споживаної об'єктом проектування ($С_э$);
- інші експлуатаційні витрати ($С_{пр}$).

Таким чином, річні експлуатаційні витрати складуть:

$$С = С_а + С_з + С_с + С_т + С_э + С_{пр}, \text{ грн.} \quad (3.3)$$

Розрахунок експлуатаційних витрат ведеться по проектному і базовому варіантів паралельно.

3.2.1 Розрахунок амортизаційних відрахувань

Амортизація об'єкта основних коштів нараховується виходячи з терміну його корисного використання.

Строк корисного використання основних засобів, що визначається за групами, для передавальних пристроїв складає 10 років.

Норма амортизації На при прямолінійній методі постійна протягом всього амортизаційного періоду і дорівнює:

$$На = \frac{Фп}{Фп * Еп} * 100 = \frac{2228,6}{2228,6 * 10} * 100 = 10\%$$

де $Т_п$ – строк корисного використання (амортизаційний період).

Тоді річні амортизаційні відрахування АВ за прямолінійним методом:

$$Са = \frac{Фп * На}{100} = \frac{2228,6 * 10}{100} = 222,86грн$$

3.2.2 Розрахунок річного фонду заробітної плати

Розрахунок річного фонду заробітної плати здійснюється за категоріями персоналу, який обслуговує об'єкт проектування, відповідно до їх чисельності, режиму роботи, годинними тарифними ставками, посадовими окладами, що застосовуються на підприємстві формами і системами оплати праці та преміювання.

Основна заробітна плата працівників - це винагорода за виконану роботу відповідно до встановлених норм праці (норми часу, виробітку, обслуговування, посадові обов'язки).

Додаткова заробітна плата – це винагорода за працю понад установлені норми, за особливі умови праці. До додаткової заробітної плати відносяться премії, пов'язані з виконанням виробничих завдань і функцій, доплати і надбавки, гарантійні і компенсаційні виплати, передбачені чинним законодавством.

Результати розрахунку основної заробітної плати обслуговуючого персоналу представлені у табл. 3.2.

Таблиця 3.2 – Розрахунок річного фонду заробітної плати обслуговуючого персоналу

№ п/п	Найменування професій працівників	Кількість, чол.	Годинна тарифна ставка, грн.	Номінальний річний фонд робочого часу, ч.	Разом, основна зарплата по тарифу, грн.
1.	Адміністратор	1	170,5	1744	297 352
2.	Java розробник	1	310	1744	540640
	Разом	2	-	-	837 992

Додаткова заробітна плата обслуговуючого персоналу визначається в розмірі 10-15% від основної заробітної плати.

Таким чином, загальна величина річного фонду заробітної плати становить:

$$С_з = З_{заг} + З_{доп} = 837\ 992 + 0,1 \cdot 837992 = 921791,2 \text{ грн},$$

де $З_{заг}$, $З_{доп}$ - основна і додаткова заробітна плата відповідно, грн.

3.2.3 Розрахунок відрахувань на соціальні заходи

Відрахування на соціальні заходи (єдиний соціальний внесок) визначаються на підставі встановленого чинним законодавством відсотка від суми основної та додаткової заробітної плати, що на 2017 рік складає 22% [30].

$$С_с = С_з \cdot 0,22 = 921791,2 \cdot 0,22 = 202\ 794 \text{ грн}.$$

3.2.4 Визначення річних витрат на технічне обслуговування і поточний ремонт

Річні витрати на технічне обслуговування і поточний ремонт обладнання включають витрати на матеріали, запасні частини, заробітну плату ремонтним робітникам і можуть визначатися за фактичними даними підприємства.

Витрати з ремонту обладнання є однією з великих статей витрат і в середньому становить 10% [31].

$$С_Т = Фп \cdot 0,1 = 348\ 414 * 0,1 = 34\ 841,4 \text{ грн.}$$

3.2.5. Розрахунок вартості спожитої електроенергії

Вартість електроенергії, споживаної об'єктом проектування протягом року, визначається виходячи з його встановленої потужності, річного фонду робочого часу і тарифів на електроенергію:

$$С_э = W_Г * Ц_Е \quad (3.4),$$

де $W_Г$ - кількість спожитої за рік електроенергії, кВт · год;

$Ц_Е$ - тариф на електроенергію станом на конкретну дату, грн. / кВт · год;

$W_Г$ = 0,0108 кВт·8760 год=94,608 кВт·год.

$Ц_Е$ = 163,754 коп/кВт·год [32].

Витрати на електроенергію складають:

$$С_Е = 94,608 \cdot 163,754 = 154,93 \text{ грн.}$$

3.2.6. Визначення інших витрат

Інші витрати по експлуатації об'єкта проектування включають витрати з охорони праці, на спецодяг та ін. Відповідно до практики, ці витрати визначаються в розмірі 4% від річного фонду заробітної плати обслуговуючого персоналу.

$$С_{пр} = С_з \cdot 0,04 = 921791,2 \cdot 0,04 = 36\ 871,65 \text{ грн.}$$

Таким чином, річні експлуатаційні витрати складуть:

$$С = 348\ 414 + 921791,2 + 202\ 794 + 222,86 + 34\ 841,4 + 36\ 871,65 = 1\ 544\ 936 \text{ грн}$$

3.5 Висновки до третього розділу

В економічному розділі розраховані капітальні витрати, що складають 348 414 грн, а експлуатаційні витрати – 1 544 936 грн.

Проектування SDN мережі є занадто дорогим. Тому витрати на таку мережу можуть бути виправдано, якщо фінансові втрати без її забезпечення будуть більшими. Або якщо традиційна мережа буде занадто складною и буде потребувати не менших витрат.

ВИСНОВКИ

В ході виконання дипломної роботи було представлено основні методи забезпечення відмовостійкості, такі як резервування і перемаршрутізація. Обидва ці методи дозволяють забезпечити необхідний користувачем показник готовності з'єднання або показник готовності різних послуг, що надаються.

При оцінці впливу резервування на надійність мережі SDN, представленої в розділі 2, використовувалися аналітичні методи моделювання засновані на теорії випадкових процесів. Дані методи були застосовані для досліджуваної мережі при відсутності резервування і при резервуванні контролера, зроблені відповідні висновки про вплив резервування на коефіцієнт готовності. Було визначенно, що незалежно від типу резервування система відновлюється за очікуваний час. А найкращим алгоритмом відновлення є LARAC. Також підібрано оптимальну архітектуру мережі. Таким чином було представлено варіанти забезпечення надійності мережі як архітектурними рішеннями, так і прикладними.

В економічному розділі розраховані капітальні витрати, що складають 348 414 грн, а експлуатаційні витрати – 1 544 936 грн.

Проектування SDN мережі є занадто дорогим. Тому витрати на таку мережу можуть бути виправдано, якщо фінансові втрати без її забезпечення будуть більшими. Або якщо традиційна мережа буде занадто складною и буде потребувати не менших витрат.

ПЕРЕЛІК ПОСИЛАНЬ

1. Смелянский Р.Л. Технология программно-конфигурируемых сетей и виртуализация сетевых сервисов: новые возможности для телекоммуникаций// Вестник Связи. 2014. No1. - [Электронный ресурс]. - Режим доступа: http://arccn.ru/media/1132 (20.01.2017)

2. ISO 9001:2015 "Quality management systems - Requirements", IDT, [Электронный ресурс]. - Режим доступа: https://www.iso.org/home.html (22.01.2017) 3. Шлиончак Е.Т. Требования, предъявляемые к современным вычислительным сетям [Электронный ресурс]. - Режим доступа: http://compnets.narod.ru/1-11.html#1.6.5. Поддержка разных видов трафика

4. Легков К. Е., Донченко А. А. Современные требования к показателям

качества информационного обмена в сетях беспроводного доступа специального назначения // T-Comm. 2009. No4. - [Электронный ресурс]. - Режим доступа: http://cyberleninka.ru/article/n/sovremennye-trebovaniya-k-pokazatelyam-kachestva- informatsionnogo-obmena-v-setyah-besprovodnogo-dostupa-spetsialnogo-naznacheniya (15.02.2017).

5. Найденов А. Эволюция в сетях Дата-Центров. Программно- определяемые сети SDN/ «Хабрахабр» - крупнейший в Европе ресурс для IT- специалистов [Электронный ресурс] – Режим доступа: http://habrahabr.ru/company /ibm/blog/211208 (11.01.2017)

6. Будылдина Н.В., Шувалов В.П. Сетевые технологии высокоскоростной передачи данных: [учебное пособие для вузов]/ под ред. ВП. Шувалова. – Москва: Горячая линия – Телеком, 2016г. – 343 с.: ил.

7. SDN&NFV [Электронный ресурс]/ Bellintegrator: Режим доступа: http://www.bellintegrator.ru/services-sdn-nfv.html (10.02.2017)

8. Барсков А. SDN: кому и зачем это надо?/ Журнал сетевых решений/LAN. 2012. No 12. – [Электронный ресурс]. – Режим доступа: https://www.osp.ru/ lan/2012/12/13033012 (12.02.2017)

9. Смелянский Р. Л. Программно-конфигурируемые сети // Открытые системы. СУБД. 2012. No 9. С. 3843. - [Электронный ресурс]. – Режим доступа: http://www.osp.ru/os/2012/09/13032491 (26.02.2017)

10. Панеш А.Х. Достоинства и недостатки программно-конфигурируемых компьютерных сетей // Вестник Адыгейского государственного университета. Серия 4: Естественно-математические и технические науки. 2016. No3 (186). - [Электронный ресурс]. – Режим доступа: http://cyberleninka.ru/article/n/dostoinstva- i-nedostatki-programmno-konfiguriruemyh-kompyuternyh-setey (10.03.2017)

11. Зейбот Р. Резервирование в информационной системе — стандартные решения// Intelligent enterprise. 2010. No11. - [Электронный ресурс]. – Режим доступа: https://www.iemag.ru/platforms/detail.php?ID=16464 (21.02.2017)

12. Aganval S., Kodialam M, Lakshman T.V. Traffic Engineering in Software Defined Networks// 2013 Proceedings IEEE INFOCOM, paper no. 06567024, pp. 2211- 2219

13. Амосов А. Отказоустойчивые ИТ-системы: принципы построения// PC Week/RE. 2016. No7. - [Электронный ресурс]. – Режим доступа: https://www.pcweek.ru/ infrastructure/article/ detail.php?ID=186752 (12.03.2017)

14.Егунов М.М., Шувалов В.П. Резервирование и восстановление в телекоммуникационных сетях// Вестник СибГУТИ. 2012. No2. - [Электронный ресурс]. – Режим доступа: http://vestnik.sibsutis.ru/uploads/1349761574_6392.pdf (11.03.2017)

15. Половко А.М., Гуров С.В. Основы теории надёжности. БХВ – Петербург, 2008. – 560 с.

16. Mukherjee B. «Optical WDM Networks». Springer. 2006. – 956 p.

17. Шувалов В. П., Егунов М. М., Минина Е. А. Обеспечение показателей надежности телекоммуникационных систем и сетей. Москва : Горячая линия – Телеком, 2015. 180 с.

18. Матвеевский В.Р. Надежность технических систем. Учебное пособие – Московский государственный институт электроники и математики. М., 2002 г. – 113 с.

19. Матвеевский В.Р. Надежность технических систем и техногенный риск [Электронный ресурс]. – Режим доступа: http://www.obzh.ru/nad/4-4.html

20. Острейковский В.А. Теория надежности: Учебник для вузов. – М.: Высш.шк.:, 2003. – 463с.

21. Тезисы докладов IX международной научно технической конференции «Энергетика, телекоммуникации и высшее образование в современных условиях». Алматы, 2014. АУЭС, - 344с.

22. Das A., Martel C., Mukherjee B., and Rai S.. «New Approach to Reliable Multipath Provisioning.» J. Opt. Commun. Netw, vol. 3, no 1, January 2011

23. Juran J. M., Godfrey A. B., Hoogstoel R. E., Schilling E. G, Juran's Quality Hhandbook, Fifth Edition. Singapore: McGraw-Hill, 2000, pp. 8.14.

24. Schneiderman A. M., “Optimum Quality Costs and Zero Defects: Are They Contradictory Concepts?” Quality Progress, vol. 19, no. 11, pp. 28-31, Nov 1986

25. Wosinska L., and Chen J., “Reliability Performance Analysis vs. Deployment Cost of Fiber Access Networks,” 7th Int’l. Conf. Optical Internet, 2008

26. Blake S, Black D., Carlson M, Davies E, Wang Z, Weiss W. An Architecture for Differentiated Services // RFC2475, 1998

27. Avizienis A.. Design of fault-tolerant computers. In Proc. 1967 Fall Joint Computer Conf., AFIPS Conf. Proc. Vol. 31, pages 733-743, 2004

28. Cholde P., Jojszyk A. «Reliability Assessment of p-Cycles» // IEEE Global Telecommunication Conference (GlobeCom 2005), st. Lonis, November-December 2005 29. Pan P., Swallow G. and Atlas. «Fast Reroute Extensions to RSVP-TE for LSP

Tunnels», RFC 4090 (Propoused Standart), Internet Engineering Task Force, May 2005 30. Олифер В.Г., Олифер Н.А. - Компьютерные сети. Принципы, технологии,

протоколы (4-е издание): Учебное пособие. – Санкт-Петербург, 2010. – 944с.
31. Вопросы математической теории надежности / Барзилович Е. Ю., Беляев Ю. К., Каштанов В. А. и др.// Под ред. Гнеденко Б. В.— М.: Радио и связь, 1983.—

184 с.
32.Байхельт Ф, Франкен П. Надежность и техническое обслуживание.

Математический подход: пер. с нем.— М.: Радио и связь, 1988.— 392 с.

67

33. Зеленцов Б.П. Моделирование функционирования систем связи на основе марковских процессов: Учебное пособие /СибГУТИ. – Новосибирск, 2012. – 72с.

34. McKeown N., Anderson T., Balakrishnan H., Parulkar G., Peterson L., Rexford J., Shenker S., and Turner J., “OpenFlow: enabling innovation in campus networks,” SIGCOMM Comput. Commun. Rev., vol. 38, no. 2, pp. 69–74, 2008

35. Сергеева Т. П., Тетёкин Н. Н. Методы повышения надежности в сетях SDN // T-Comm. 2014. No6. – [Электронный ресурс]. – Режим доступа:

http://cyberleninka.ru/article/n/metody-povysheniya-nadezhnosti-v-setyah-sdn (25.02.2017)

36. Juttner A., Szviatovski B., Mecs I., and Rajko Z., “Lagrange relaxation based method for the QoS routing problem,” in Proc. IEEE INFOCOM, vol. 2, Apr. 2001, pp. 859–868.

37.Барсков А, SDN: от концепции к решениям// Журнал сетевых решений/LAN. 2015. No9. – [Электронный ресурс]. – Режим доступа: https://www.osp.ru/lan/2015/09/13046914 (12.04.2017)

38. BGP и BFD на Cisco// Cisco Howto. – [Электронный ресурс]. – Режим доступа: http://ciao-cacao.blogspot.ru/2011/12/bgp-bfd.html (11.03.2017)

39. Heller B., Sherwood R., McKeown N. On Reliability-optimized Controller Placement for Software-Defined Networks. Rev., vol. 38, no. 2, pp. 69–74, 2009

40. Половко А.М., Гуров С.В. Основы теории надежности. – 2-е изд., перераб. И доп. –СПб.: БХВ-Петербург, 2006. -704с.:ил.

41. Постников И. Н. Оценка влияния резервирования контроллера SDN на надежность сети // Молодой ученый. — 2016. — No6. — С. 164-168.

42. D-link. Gigabit Stackable Smart Managed Switches [Электронный ресурс]: Электрон. текстовые дан.— D-link, 2015.— Режим доступа: http://www.dlink.com/- /media/Business_Products/DGS/DGS%201510/Datasheet/DGS_1510_Series_ Datasheet_EN_EU.pdf (12.04.2017)

43.HP Performance Brief for External Audiences [Электронный ресурс]: Электрон. текстовые дан.— HP, 2007.— Режим доступа: ftp.hp.com/pub/c-products/servers/benchmarks/dl380_spec2005_062707.pdf (12.04.2017)

44. Яковлев А.В. Надежность информационных систем. Лекционный материал, Муром 2004

45. Семенов Ю.А. Сетевая технология OpenFlow (SDN). – [Электронный ресурс]. – Режим доступа: http://book.itep.ru/4/41/openflow.htm (20.04.2017)

46. Hilmi E., Egilmez S., Tahsin D., Tolga K. and Murat A. OpenQoS: An OpenFlow Controller Design for Multimedia Delivery with End-to-End Quality of Service over Software-Defined Networks //Koc University, Istanbul, Turkey

47. Widyono R., 'The design and evaluation of routing algorithms for realtime channels', Technical Report TR-94-024, University of California at Berkeley, June 1994 48. Lee W.C., et al. 'Multi-Criteria Routing subject to Resource and Performance Constraints', ATM Forum 94-0280, March 1994
49. Salama H.F., Reeves D.S. and Viniotis Y., 'A Distributed Algorithm for Delay-

Constrained Unicast Routing', IEEE Infocom'97, Kobe, Japan, April 1997
50. Ahuja R.K., Magnanti T.L. and Orlin J.B., 'Network Flows' PRENTICE

HALL, Upper Saddle River, New Jersey 07458, 1993.
51. ГОСТ 27.002-89. Надежность в технике. Основные понятия. Термины и

определения.
52. ГОСТ Р 53480-2009. Надежность в технике. Термины и определения.

53. Шувалов В.П. Исследование методов повышения надежности в сетях SDN // 2017

ДОДАТОК А. Відомість матеріалів дипломної роботи

№	Формат	Найменування	Кількість листів	Примітки
Документація				
1	А4	Реферат	3	
2	А4	Список умовних скорочень	2	
3	А4	Зміст	1	
4	А4	Вступ	2	
5	А4	Стан питання. Постановка задачі	28	
6	А4	Спеціальна частина	25	
7	А4	Економічний розділ	6	
8	А4	Висновки	1	
9	А4	Перелік посилань	6	
10	А4	Додаток А	1	
11	А4	Додаток Б	1	
12	А4	Додаток В	1	

ДОДАТОК Б. Відгук керівника економічного розділу

Керівник розділу _____ _____

(підпис) (прізвище, ініціали)

ДОДАТОК В. Відгук керівника дипломної роботи

ВІДГУК

на дипломну роботу

студентки групи 172м-17-1 Брюханової Анастасії Олександрівни

Керівник розділу _____ _____

(підпис) (прізвище, ініціали)

Р Е Ц Е Н З І Я

на дипломну роботу магістра на тему

«*Вибір методу підвищення відмово стійкості програмно-конфігуруємої (SDN) мережі*»

студентки групи 172м-17-1

Брюханової Анастасії Олександрівни

за спеціальністю 172 «Телекомунікації та радіотехніка»

На рецензію дипломна робота магістра представлена пояснювальною запискою на 69 стор., має 23 рисунків, 11 таблиць, 4 додатків, 53 джерел.

Високий рівень надійності мереж забезпечується за рахунок швидкого виявлення пошкоджень і усунення їх наслідків в короткий час. В даний час одним з рішень цих вимог є використання програмно-конфігуруємих мереж.

Мета дипломної роботи вибрати методи забезпечення надійності (вімовостійкості) SDN мережі в значної ступені автором досягнута.

У першому розділі ретельно проаналізовано технологію SDN. Наведено опис методів резервування на прикладному рівні та розглянуто посилення надійності з точки зору фізичної реалізації.

У спеціальній частині автором виконано аналіз існуючих структур архітектури рівня контролю, впливу резервування на SDN мережу, визначено середній час відгуку контролера та запропоновано модифікований спосіб структуризації рівня управління SDN.

В економічному розділі визначено розмір капітальних та експлуатаційних витрат для побудови проектованої мережі.

В якості недоліку можна відмітити те, що для обґрунтування прийнятих рішень використано занадто великий обсяг аналітичних доказів.

В цілому дипломна робота магістра виконана успішно та заслуговує оцінки **«*добре*»,** а її автор Брюханова Анастасія Олександрівна присвоєння їй кваліфікації 2144.2 Інженер в галузі електроніки та телекомунікацій.

Рецензент - професор кафедри ПЗКС
НТУ «Дніпровська політехніка», д.т.н. _____ Мещеряков Л.І.