*УДК 621.391*

# ПІДВИЩЕННЯ ВІДМОВОСТІЙКОСТІ ЕЛЕМЕНТІВ СУЧАСНИХ ІНФОКОМУНІКАЦІЙНИХ МЕРЕЖ ІЗ ЗАСТОСУВАННЯМ ПРОТОКОЛІВ РЕЗЕРВУВАННЯ ШЛЮЗУ ЗА ЗАМОВЧУВАННЯМ

О.С. ЄРЕМЕНКО, А. МЕРСНІ
*Харківський національний університет радіоелектроніки*

***Abstract*** *– The article is devoted to the Network Layer means to ensure resilience during designing an infocommunication system that can counteract faults and failures. A review of the default gateway redundancy protocols concept and analysis of recent developments to overcome fault tolerance challenges in the Software-Defined Networks (SDN) control plane are conducted. In addition, an approach to the use of default gateway redundancy protocols in the existing Software-Defined Network architecture is proposed. Therefore, within the approach, the redundancy of the virtual controller is organized based on the current protocol implemented in traditional IP networks, and the SDN switch interacts with the virtual controller. This mechanism aims to reduce the amount of circulating overhead (control traffic), and the backup controller's organization increases the control plane's reliability. Whereas in hybrid and hierarchical SDN networks with border routers, the GLBP mechanism can be applied, which increases the reliability of the controller connected to the data plane. In addition, there are several scenarios where the controller that manages the operation of the SDN data plane may have multiple backup controllers to switch in case of failure, or a controller pool is used to manage each network that makes up the SDN data plane. It also highlights promising future areas for research and development to improve Software-Defined Network resilience, which contributes to the emergence of new solutions. Thus, future research directions are seen in proposing mathematical flow-based models of fault-tolerant interaction of the control plane and the data plane based on redundancy. At the same time, setting the problem in an optimization form with the implementation of load balancing will help to use available network resources effectively.*

***Анотація*** *– Статтю присвячено засобам мережного рівня щодо забезпечення відмовостійкості під час проєктування інфокомунікаційної системи, що здатна протидіяти несправностям і відмовам. Проведено огляд концепції протоколів резервування шлюзу за замовчуванням та аналіз останніх розробок щодо подолання проблем відмовостійкості в площині управління програмно-конфігурованих мереж. Крім того, запропоновано підхід до використання протоколів резервування шлюзу за замовчуванням в існуючій архітектурі програмно-конфігурованої мережі. Отже, у межах підходу організовано резервування віртуального контролера, що базується на існуючому протоколі, реалізованому в традиційних IP-мережах, а SDN комутатор взаємодіє з віртуальним контролером. Такий механізм спрямований на зменшення обсягу циркулюючого службового навантаження (трафіку управління), а організація резервного контролера підвищує надійність площини управління. Тоді як у гібридних та ієрархічних SDN мережах з прикордонними маршрутизаторами, можна використовувати механізм протоколу GLBP, що виконує функцію підвищення надійності контролера, з'єднаного з площиною даних. Крім того, існує можливість декількох сценаріїв, коли контролер, що керує роботою площини даних SDN, може мати кілька резервних контролерів для перемикання у разі відмови, або використовується пул контролерів для управління кожною мережею, що складає площину даних SDN. Також висвітлюються перспективні майбутні напрямки для досліджень і розробок щодо вдосконалення відмовостійкості програмно-конфігурованих мереж, що сприяють появі нових рішень. Отже, майбутні напрямки досліджень вбачаються у пропонуванні математичних потокових моделей відмовостійкої взаємодії площини управління та площини даних на основі резервування. Водночас постановка задачі в оптимізаційній формі з реалізацією балансування навантаження допоможе ефективно використовувати наявні мережні ресурси.*

## Вступ

Сучасні інфокомунікаційні мережі (ІКМ) мають вирішальне значення для зростання та розповсюдження цифрового суспільства. Їхнє широке використання створило нові можливості для розвитку інноваційних архітектур і новітніх мережних стандартів. Програмно-конфігуровані мережі (Software-Defined Network, SDN) – це лише один з прикладів новітніх технологій індустрії побудови інфокомунікаційних мереж,

що надає багато переваг та удосконалень під час проєктування та розгортання на відміну від традиційних мереж.

Однак практичне використання SDN обмежується існуючими проблемами забезпечення необхідного рівня відмовостійкості елементів таких мереж, що є критичним під час надійної комунікації площини даних і керування. Водночас стійкість мережі відноситься до її здатності надавати та підтримувати належний рівень якості обслуговування у разі різноманітних збоїв і відмов у процесі функціонування [1, 2]. Тому більшість сучасних мереж повинні забезпечувати механізми швидкого відновлення як у площині даних, так і в площині управління з метою відповідності високим вимогам щодо стійкості, надійності, якості обслуговування (Quality of Service, QoS) та резервування.

Таким чином, у даній статті зосереджено увагу на засобах мережного рівня щодо забезпечення відмовостійкості під час проєктування інфокомунікаційної системи, що здатна протидіяти несправностям і відмовам. Крім того, пропонується новий підхід до відмовостійкості контролерів SDN шляхом використання механізмів протоколів резервування шлюзу за замовчуванням (First Hop Redundancy Protocols, FHRPs) з базовою архітектурою SDN. FHRP мають у складі декілька протоколів і використовуються для подолання втрат трафіку між відправником (джерелом) і отримувачем потоків даних.

За місцем реалізації відповідно до багаторівневої архітектури сучасних ІКМ задачі відмовостійкої маршрутизації можуть розв'язуватись як на рівні доступу, так і на рівні ядра ІКМ або транспортної мережі (рис. 1) [2].

На рівні доступу задача відмовостійкої маршрутизації зводиться до захисту шлюзу за замовчуванням, тобто маршрутизатора, до якого комутується та чи інша мережа доступу. Це можливо організувати, коли мережі доступу комутуються одночасно до декількох приграничних маршрутизаторів, інтерфейси яких конфігуруються відповідним протоколом як віртуальний шлюз за замовчуванням [24-27]. Для підвищення доступності приграничних маршрутизаторів у разі відмови основного шлюзу протокол в автоматичному режимі здійснює перемикання потоків на резервний шлюз. Крім того, балансування навантаження за декількома інтерфейсами віртуального маршрутизатора здатне підвищити доступність і надійність з'єднання, однак така функціональність властива не всім протоколам (табл. 1) [24, 27].

Отже, решта статті структурована наступним чином: перший розділ присвячено огляду концепції протоколів резервування шлюзу за замовчуванням. У другому розділі обговорено особливості концепції технології SDN та проведено аналіз існуючих підходів і рішень відмовостійких SDN архітектур. Тоді як у четвертому розділі запропоновано декілька майбутніх напрямків щодо забезпечення відмовостійкості контролерів SDN.

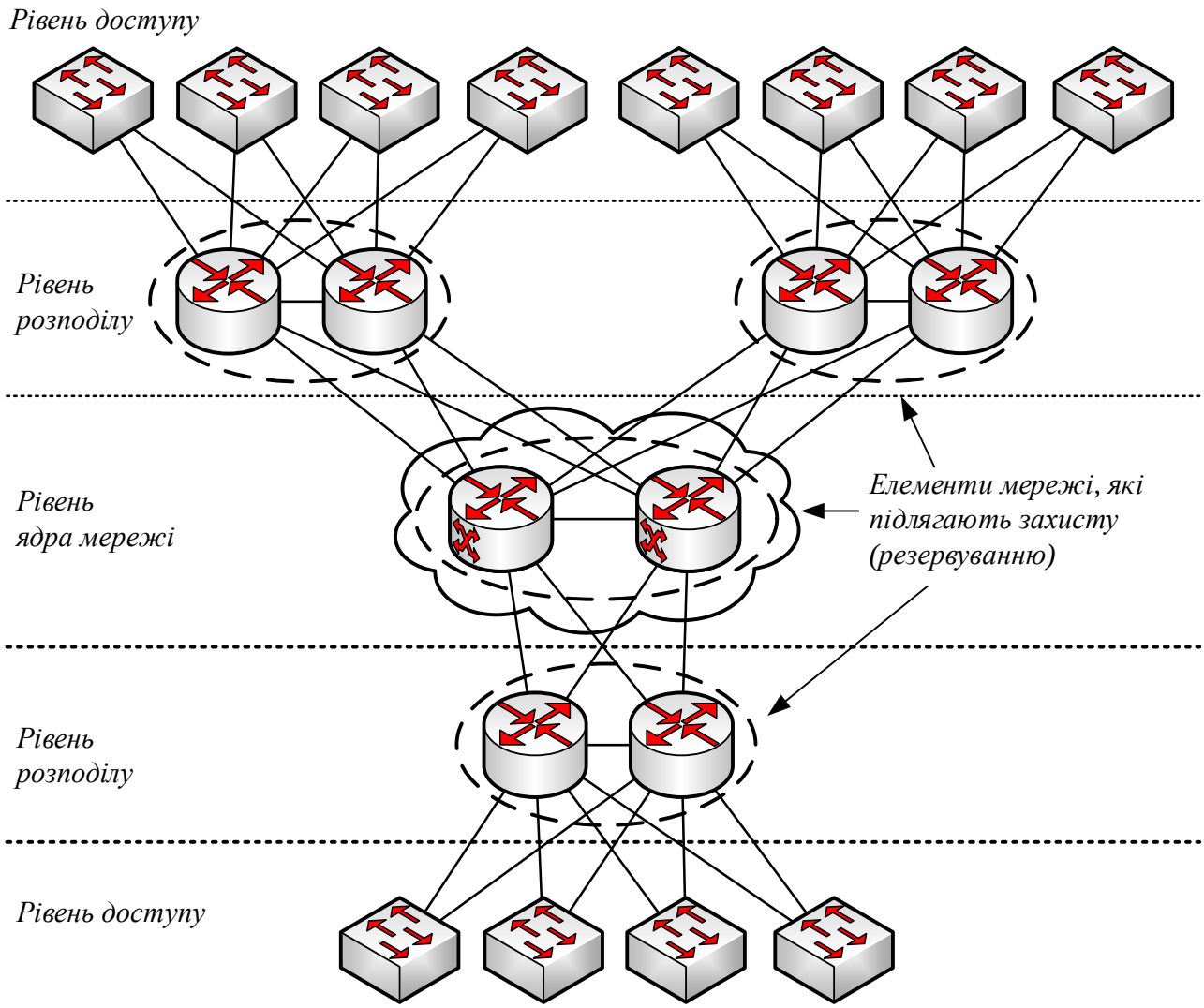


*Рис.* 1. Багаторівнева архітектура забезпечення відмовостійкості ІКМ

## І. Огляд основних протоколів резервування шлюзу за замовчуванням – FHRP

Історично основною проблемою, з якою стикаються інфокомунікаційні мережі, було усунення збоїв і відмов у мережі, викликаних рядом факторів, як-от людські або ненавмисні помилки, проблеми інформаційної безпеки, відмови каналів зв'язку, збої програмного забезпечення та обладнання тощо.

Зі зростанням попиту на інфокомунікаційні послуги та прискореним розвитком інформаційного суспільства підтримка більш стійких мереж до таких відмов залишається найбільш бажаним фактором у всьому світі. Дійсно, використання механізмів резервування в ІКМ – це ефективні засоби підвищення доступності, продуктивності мережі та зменшення відмов, відомих як єдина точка збою (Single Point of Failure, SPOF), тобто таких дефектів у проєктуванні, налаштуванні чи реалізації системи або компонента, що може призвести до виходу з ладу всієї системи. Проблему SPOF може

бути усунено шляхом дублювання та додавання каналів зв'язку або інших мережних компонентів з метою встановлення альтернативних резервних систем (обладнання, вузлів, каналів, маршрутів тощо) та збереження функціонування мережі у разі збою.

Одна з основних технологій резервування – це реалізація резервування шлюзу за замовчуванням. Основна проблема з точки зору необхідності резервування шлюзу полягає в тому, що коли маршрутизатор або лінія зв'язку відмовляють, доступ до зовнішньої мережі втрачається. В результаті виникає необхідність у розгортанні альтернативного резервного маршрутизатора з метою запобігання відключення мережі шлюзу. Крім того, протоколи FHRP зазвичай мають відповідний функціонал, що дозволяє спростити кінцевим пристроям налаштування та використання декількох шлюзів, а також автоматично передавати хостам дані на резервний маршрутизатор, не вимагаючи внесення змін до конфігурації вручну. Тому ці протоколи долають обмеження шлюзу за замовчуванням і надають безвідмовне обслуговування. Отже, до групи протоколів FHRP відносять наступні (Табл. 1) [3,4]:

- Hot Standby Router Protocol (HSRP);
- Virtual Router Redundancy Protocol (VRRP);
- Gateway Load Balancing Protocol (GLBP);
- Common Address Redundancy Protocol (CARP);
- Extreme Standby Router Protocol (ESRP);
- Routed Split multi-link trunking (R-SMLT);
- NetScreen Redundancy Protocol (NSRP);
- Chassis Cluster Redundant Ethernet.

У наступних підрозділах описано основні характеристики та вдосконалення найбільш часто використовуваних протоколів групи FHRP.

**HSRP**

Hot Standby Router Protocol – протокол резервування, розроблений компанією Cisco, що налаштовує маршрутизатори як членів групи та призначає віртуальну IP-адресу (Virtual IP Address, VIP) та віртуальну MAC-адресу, що використовується кінцевими пристроями для зв'язку з маршрутизатором-шлюзом [3]. Для HSRP групи маршрутизатор з найбільшим пріоритетом позначається як активний маршрутизатор і відповідає за переадресацію трафіку. Тоді як маршрутизатор з другим найвищим пріоритетом обирається як резервний маршрутизатор, що візьме на себе відповідальність за маршрутизацію пакетів у разі збою активного маршрутизатора або при виконанні заздалегідь визначених критеріїв і завдань. Усі інші маршрутизатори в HSRP групі перебувають у стані прослуховування [4].

HSRPv2 – найновіша версія протоколу, призначена для усунення недоліків стандартної версії протоколу, HSRPv1. Вона була розширена для підтримки IPv6 та використання мілісекундних `hello` таймерів. В результаті він забезпечує більшу стабільність і швидший час відновлення після відмов [5].

Ще однією перевагою HSRPv2 є те, що він надсилає `hello` пакети, використовуючи нову багатоадресну IP-адресу 224.0.0.102 замість адреси багатоадресної розсилки

224.0.0.2, що використовувалася HSRPv1. Ця нова адреса дозволяє активувати обробку протоколом Cisco Group Management Protocol (CGMP) в еквівалентний для HSRP час. HSRPv2 збільшує діапазон номерів груп до 4095, а не лише до 255, як у HSRPv1. Таким чином, розширений діапазон дозволяє номеру групи на підінтерфейсах відповідати номеру VLAN [6].

*Таблиця* 1. Порівняння протоколів резервування шлюзу за замовчуванням [2]

| Характеристика | HSRP | VRRP | GLBP | CARP |
|---|---|---|---|---|
| Застосування | Cisco Proprietary | IEEE Standard | Cisco Proprietary | Not a standard (BSD based OS) |
| Стандарт | RFC 2281 | RFC 5798 | Ні | Ні |
| Рівень моделі OSI | Мережний | Мережний | Канальний | Мережний |
| Балансування навантаження | Не підтримується | Підтримується | Підтримується | Підтримується |
| IPv6 | Підтримується | Підтримується | Підтримується | Підтримується |
| Переваги | – легка конфігурація;<br>– низьке навантаження мережі службовим трафіком. | – спрощене управління мережею;<br>– висока адаптованість;<br>– низьке навантаження мережі службовим трафіком;<br>– балансування навантаження;<br>– мінімізація обчислювальних витрат. | – ефективне використання мережних ресурсів;<br>– висока доступність;<br>– автоматичне балансування навантаження;<br>– низькі витрати на адміністрування;<br>– ефективне проектування рівня доступу. | – відкрита альтернатива HSRP і VRRP;<br>– резервування для брандмауерів та маршрутизаторів;<br>– балансування навантаження. |
| Недоліки | – неефективний для передачі трафіку реального часу;<br>– слабкий рівень безпеки;<br>– пропрієтарний протокол Cisco. | – слабкий рівень безпеки (не містить жодного типу автентифікації). | – пропрієтарний протокол Cisco;<br>– висока складність управління мережею. | – несумісність з чинними стандартами;<br>– слабкий рівень безпеки. |

**VRRP**

Virtual Redundancy Protocol – відмовостійкий open-source протокол, стандартизований Internet Engineering Task Force (IETF) [7]. Він використовується для забезпечення безперервного та надійного обслуговування мережею. У групі VRRP активний маршрутизатор, який керує VIP-шлюзом, називається головним (master) маршрутизатором, тоді як усі інші маршрутизатори VRRP є резервними маршрутизаторами. Віртуальна IP-адреса може бути фізичною (реальною) IP-адресою інтерфейсу.

Оригінальний VRRPv2 був опублікований у RFC 3768 і призначений лише для підтримки IPv4. Однак, остання версія VRRPv3, яка детально описана в RFC 5798, підтримує обидві версії IPv4 та IPv6 [7]. Перевага використання VRRPv3 полягає у тому, що він дозволяє швидше переключатися на резервні пристрої у разі відмови, ніж стандартні механізми виявлення сусідніх пристроїв (neighbor discovery) IPv6. VRRPv3 дозволяє резервному маршрутизатору стати master-маршрутизатором за лічені секунди без використання службового трафіку та участі хоста. [8] Ще однією перевагою застосування VRRPv3 є покращення процесу резервування у мережі шляхом використання декількох пристроїв як шлюзів за замовчуванням, що виключає виникнення єдиної точки відмови.

**CARP**

Common Address Redundancy Protocol – не запатентована альтернатива Cisco HSRP та VRRP, розроблена OpenBSD. Це протокол резервування шлюзу, який використовується для підвищення доступності мережі та забезпечення безперебійних послуг. Це безпечний протокол, що використовує алгоритм HMAC (Hash-based message authentication code) SHA-1 (Secure Hash Algorithm 1) і може бути розгорнутий у мережах Pv4 та IPv6 [9]. Протокол використовується серед групи пристроїв, які мають однакову IP-адресу в одній мережі. Ця група хостів відома як група резервування (redundancy group). Усередині групи один хост обирається як master, а решта стають резервними. Зі свого боку master хост – це той, кому належить спільна IP-адреса та обслуговує будь-який трафік, спрямований на нього, наприклад, запити ARP. У будь-який момент хост може бути членом декількох груп [10].

Кожен вузол у CARP вимагає трьох аргументів для коректної роботи. Перші два – база сповіщень advertisement base (`advbase`) та advertisement skew (`advskew`). Обидва впливають на час, протягом якого передається сповіщення [11]. Змінна `advskew` використовується для вибору master хоста з групи резервування з обмеженням, яке полягає в тому, що чим менше значення `advskew`, тим вищий пріоритет стати master хостом. Змінна `advbase` використовується для визначення часу в секундах, протягом якого надсилається сповіщення CARP. Третій параметр – це пароль, який використовується для перевірки сповіщення [12].

**NSRP**

NetScreen Redundancy Protocol – це протокол резервування маршрутизатора, що належить компанії Juniper Networks та забезпечує прозоре відновлення після відмови

та балансування навантаження. Довгий час NSRP називали High Availability (HA). Попередня версія NSRP була реалізована в більш ранніх поколіннях NetScreen, наприклад, NS-100, який не підтримує ScreenOS 4.0 або пізнішої версії. Ця версія має обмежені функціональні можливості та потребує використання додаткових команд для налаштування HA. Випуск другої версії NSRP реалізовано в ScreenOS 3.1. Налаштування HA часто називають конфігурацією NSRP або «NSRP operation» [13].

**GLBP**

Gateway Load-Balancing Protocol – ще один Cisco-пропрієтарний протокол резервування. Він дозволяє розподіляти навантаження пакетів серед множини резервних маршрутизаторів. GLBP гарантує можливість балансування навантаження для кількох маршрутизаторів шлюзів з однаковою IP-адресою, але з різними MAC-адресами. У GLBP усі маршрутизатори працюють як активні з метою запобігання руйнування всієї системи. Він підвищує продуктивність мережі, забезпечуючи балансування навантаження та IP резервування [3, 4, 6].

Таким чином, найбільш суттєвими недоліками наявних рішень щодо відмовостійкої IP-маршрутизації вважаються такі:

– не враховується потоковий характер мережного трафіку;
– обмежені можливості для балансування навантаження з необхідністю адміністративної конфігурації;
– відсутність узгодженого рішення взаємопов'язаних завдань вибору шлюзу за замовчуванням і маршрутизації у транспортній мережі.

Наприклад, як показано в [24], для забезпечення балансування навантаження за інтерфейсами шлюзів за замовчуванням можуть використовуватися такі механізми: Round Robin та Weighted (зважене) в GLBP, Host-dependent у GLBP та VRRP.

Метод Round Robin передбачає рівномірне балансування навантаження за всіма інтерфейсами віртуального шлюзу, що є прийнятним рішенням лише у разі приблизно однакової доступності приграничних маршрутизаторів транспортної мережі. В іншому випадку доцільно використовувати зважене балансування навантаження, у якому трафік, що надходить від мереж доступу, розподіляється між інтерфейсами віртуального маршрутизатора пропорційно їх адміністративній вазі. Третій механізм (host-dependent) реалізує псевдобалансування, коли певний віртуальний інтерфейс шлюзу для однієї мережі доступу є основним інтерфейсом, а для іншої мережі доступу – резервним. Таким чином, для забезпечення нерівномірного балансування навантаження між приграничними маршрутизаторами транспортної мережі з різною доступністю необхідно адміністративно проводити додаткову конфігурацію обладнання.

Ці механізми балансування значно знижують швидкість реакції мережі на можливі збої та обмежують функціональність мережних рішень для захисту шлюзів (резервування). Крім того, навіть у разі оптимізації балансування навантаження для захисту шлюзу відсутня гарантія, що після вибору шлюзу за замовчуванням у транспортній мережі є маршрут, який має необхідну пропускну здатність для

забезпечення QoS. Це пов'язано з тим, що відомі рішення захисту шлюзу за замовчуванням не узгоджуються з рішеннями маршрутизації в транспортній мережі та вирішуються послідовно та незалежно один від одного.

## II. Аналіз рішень щодо відмовостійкості SDN

Як було зазначено вище, SDN – технологія, в якій існуюча структура традиційних мереж перетворюється на концепцію, де площини передачі даних та управління розділені. Крім того, SDN забезпечує віртуалізацію мережних функцій вузлів, що мінімізує залежність від апаратного забезпечення. Також слід додати, що загальний підхід SDN орієнтований на автоматизацію, що дозволяє постачальникам послуг та операторам мереж швидше розвиватися та зменшувати капітальні та операційні витрати. Він також дозволяє контролювати мережні операції та забезпечує загальне управління комунікаційними процесами [14, 15, 16].

Фундаментальна архітектура SDN складається з трьох площин: застосунків, управління та даних [15]. Зі свого боку Northbound Application Programming Interfaces (APIs) з'єднують площини застосунків та управління. Крім того, взаємодія площини управління та передачі даних організовано за допомогою Southbound APIs. Площина даних містить вузли передачі даних, відомі як SDN комутатори. Площина управління, яку часто називають «мозком», є ключовим компонентом архітектури SDN, де знаходиться контролер. Дійсно, SDN контролер керує процесом передачі потоків даних і надсилає інформацію щодо прийняття рішень на площину даних.

У більшості випадків управління площиною даних організовується за допомогою протоколу Open Flow (OF), який широко використовується для безпечної передачі даних і стандартизований Open Networking Foundation. Він застосовується для встановлення зв'язку між площиною управління та площиною даних [15, 16, 17].

Проте, незважаючи на багато згаданих вище переваг, традиційні засади побудови SDN мають істотний недолік у разі використання єдиного SDN контролера [15]. В результаті цього функціонування мережі сильно залежить від продуктивності одного контролера, що є непридатним для будь-якого застосунку, що вимагає високий рівень надійності. Отже, рекомендується використовувати кілька контролерів (пул) замість централізованого контролера, що виконує управління всією мережею, з метою запобігання виникнення проблеми єдиної точки збою в SDN контролерах.

Багато сучасних досліджень присвячено вивченню проблеми вдосконалення та розробки нових рішень щодо відмовостійкості у SDN. Отже, проведемо короткий аналіз проведених та опублікованих досліджень останніх років (Табл. 2) [15-24]. У роботі [16] було запропоновано підхід до боротьби з відмовами каналів зв'язку у площині даних – Controlled based Robust Network (CORONET). Він базується на платформі NOX, що дозволяє взаємодіяти з Open Flow комутаторами. Тоді як у [18] запропоновано концепцію BOND, що представляє собою гнучкий механізм відновлення після відмов у програмно-конфігурованих мережах. Ідея полягає у призначенні правил резервування комутаторам, а не резервним маршрутам під час урахування потреб того

чи іншого потоку, що передається. Потім використовується глобальна хеш-таблиця для прискорення відновлення після відмови. Ефективність BOND була доведена експериментально та продемонстрована з використанням реальних топологій.

Зі свого боку автори [19] запропонували ефективний метод FTLink для відмовостійкості каналів зв'язку в SDN. Відповідно до методу створюються резервні канали зв'язку у разі невдачі основного з'єднання. FTLink генерує відповідну таблицю для правил резервування, що підтримується через контролер.

Розподілений контролер SDN відповідно до концепції Візантійської відмовостійкості (Byzantine Fault Tolerant, BFT) був розроблений у [20]. Запропонований прототип здатний протидіяти Візантійським помилкам як у площині даних, так і в площині управління. Він поєднує в собі два існуючих вразливих до Візантійських помилок контролера SDN з відкритим вихідним кодом та відповідне програмне забезпечення для реплікації Візантійського кінцевого автомата.

*Таблиця* 2. Рішення щодо відмовостійкості площини управління SDN

| Посилання | Рішення |
|---|---|
| [15] | Запропоновано розподілену відмовостійку архітектуру програмно-конфігурованої мережі (FT-SDN) з вибором робочого резервного контролера на основі відстані та затримок у разі виходу з ладу основного контролера. |
| [21] | Для мережі розподілених контролерів запропоновано механізм Load Balancing and Fault Tolerance (LBFT). Даний підхід виявляє збій головного (основного) контролера і намагається перенести управління комутаторами, пов'язаними з головним контролером, на резервні контролери. |
| [22] | Механзім Automatic Failure Recovery for OpenFlow (AFRO) запропоновано для виявлення несправностей та автоматичного відновлення OpenFlow контролерів. |
| [23] | Запропоновано Byzantine Fault-Avoidance (BFA) як відмовостійку архітектуру, що поєднує стек програмного забезпечення для управління хмарами OpenStack (nova) з реалізацією SDN (neutron). |
| [24] | Зпропоновано платформу MORPH, толерантну до недоступності та відмов типу Byzantine, що виявляє та локалізує дефектні екземпляри контролера та відповідно змінює площину управління. |

У таблиці 2 наведено існуючі рішення щодо забезпечення відмовостійкості SDN саме в площині управління. Однак, запропоновані рішення мають суттєві обмеження. Дійсно, деякі технологічні рішення стосуються лише відмов каналів передачі даних, наприклад, CORONET, BOND та FTLink. Тоді як AFRO, FT-SDN, LBFT, MORPH орієнтовані саме на відмови у площині управління SDN. Проте, з розвитком архітектури SDN стають очевидними додаткові категорії відмов і збоїв. Отже, необхідні ретельні оцінки та постійне вдосконалення відповідних технологічних рішень, пов'язаних з аспектом загально системної відмовостійкості програмно-конфігурованих мереж.

## III. Пропозиції щодо удосконалення рішень відмовостійкості SDN

Завдяки постійному вдосконаленню існуючих механізмів відмовостійкості в сучасних мережах SDN (наприклад, Hybrid SDN, SD-WAN тощо) можливо сформулювати вимоги до потенційних технологічних рішень для підвищення відмовостійкості таких мереж. Дійсно, більшість рішень покращують традиційну стійкість IP/MPLS, використовуючи відмовостійку маршрутизацію та механізми швидкої перемаршрутизації (Fast ReRoute тощо). Тим не менше, багато розробників та дослідників намагалися адаптувати ці рішення у межах SDN [25].

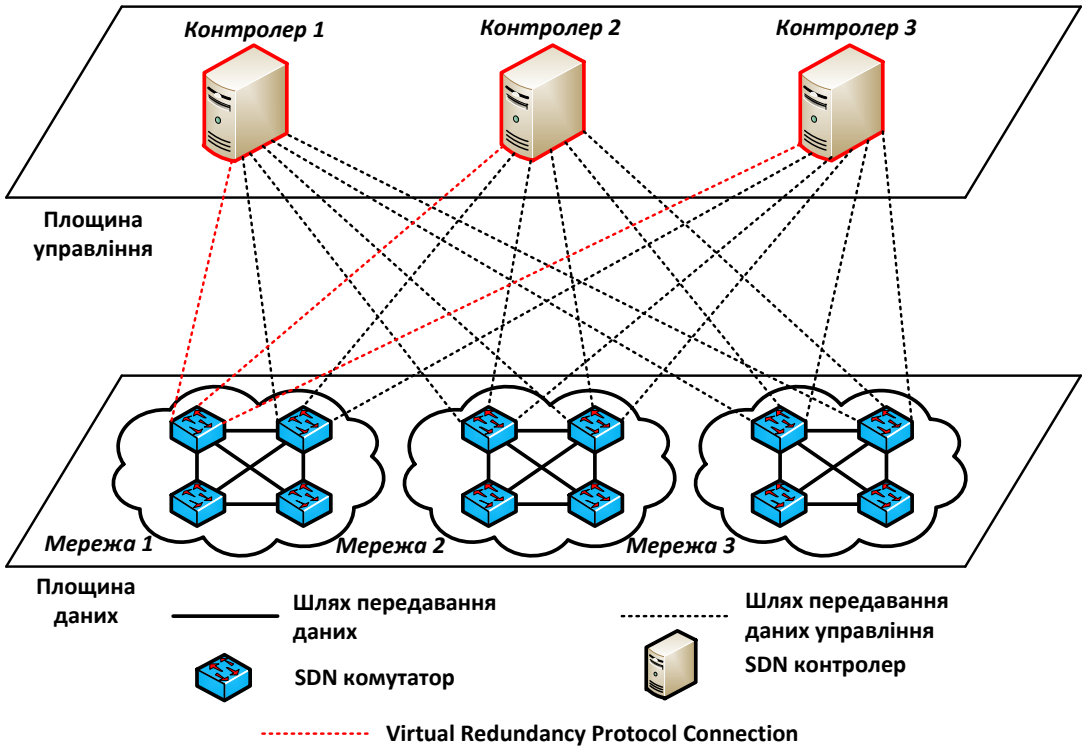


*Рис.* 2. Приклад відмовостійкої SDN архітектури

Однак, надійність мережі загалом залежить від надійності контролерів і площини управління. Ефективне проєктування площини управління повинне забезпечувати узгодженість між пристроями передачі та управління та усіма підмережами у разі збоїв елементів мережі.

Одним із перспективних напрямків є використання підходу так званого резервування віртуального контролера (рис. 2). Цей підхід базується на існуючому протоколі VRRP, реалізованому в традиційних IP-мережах [17]. У цьому випадку комутатор SDN взаємодіє з віртуальним контролером. Такий механізм спрямований на зменшення обсягу циркулюючого службового навантаження (трафіку управління), а організація резервного контролера підвищує надійність площини управління.

Крім того, якщо в гібридних та ієрархічних SDN мережах є приграничні маршрутизатори, можна використовувати механізм GLBP. У цьому разі протокол GLBP виконує функцію підвищення надійності контролера, з'єднаного з площиною даних. Тут

можливо декілька сценаріїв. По-перше, контролер, що керує роботою площини даних SDN, може мати кілька резервних контролерів для перемикання у разі відмови. По-друге, може існувати пул контролерів для управління кожною конкретною мережею, що складає площину даних SDN. У такому випадку, якщо один контролер виходить з ладу, інший (резервний) контролер починає обслуговувати декілька мереж разом.

Загалом, аналіз сучасних підходів [26-35] дозволяє сформулювати такі вимоги щодо забезпечення відмовостійкості площини управління SDN:

- адаптивна реакція на можливі відмови контролера, усуваючи їх негативний вплив на загальне функціонування SDN;
- використання віртуального та функціонального резервування для захисту контролерів мережі;
- застосування балансування навантаження між контролерами;
- сегментація мережі для локалізації трафіку та зменшення навантаження на контролери;
- забезпечення узгодженості та ефективності механізмів управління та захисту елементів площини даних.

## Висновки

У статті проведено аналіз сучасних рішень щодо відмовостійкості площини управління SDN. Крім того, зроблено огляд рішень FHRP як найважливішого компонента відмовостійкості інфокомунікаційної мережі та резервування шлюзу. Крім того, запропоновано стратегію адаптації механізмів FHRP, зокрема VRRP та GLBP, до існуючих архітектур SDN для захисту площини управління та забезпечення необхідного рівня її відмовостійкості.

Однак, відомо, що ефективність протоколу головним чиином залежить від відповідного математичного апарату, на якому він базується. Отже, як майбутні напрямки досліджень вбачається пропозиція потокової математичної моделі відмовостійкої взаємодії площини управління та площини даних на основі резервування. Така модель має враховувати особливості ієрархії архітектур SDN. Водночас постановка технологічного завдання у формі оптимізаційної задачі та реалізація механізмів балансування навантаження допоможуть ефективно використовувати наявні мережні ресурси.

### Список літератури

1. *Barreiros, M., Lundqvist, P.* (2016), QOS-Enabled Networks: Tools and Foundations, 2nd edition. Wiley Series on Communications Networking & Distributed Systems, Wiley, 254 p.

2. *Лемешко, О. В., Єременко, О. С., Невзорова, О. С.* (2020), Потокові моделі та методи маршрутизації в інфокомунікаційних мережах: відмовостійкість, безпека, масштабованість, Харків: ХНУРЕ, 308 с.

3. *Lemeshko, O., Yeremenko, O., Yevdokymenko, M., Shapovalova, A., Hailan, A.M., Mersni, A.* (2019), "Cyber Resilience Approach Based on Traffic Engineering Fast ReRoute with Policing", 10th

IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS), P. 117-122, **DOI**: https://doi.org/10.1109/IDAACS.2019.8924294

4. *Shahriar, F., Fan, J.* (2020), "Performance Analysis of FHRP in a VLAN Network with STP", 2020 IEEE 3rd International Conference on Electronics Technology (ICET), P. 814-818. **DOI**: https://doi.org/10.1109/ICET49382.2020.9119624

5. *Anwar, U., Teng, J., Umair, H. A., Sikander, A.* (2019), "Performance Analysis and Functionality Comparison of FHRP Protocols," 2019 IEEE 11th International Conference on Communication Software and Networks (ICCSN), P. 111-115. **DOI**: https://doi.org/10.1109/ICCSN.2019.8905333

6. *Odom, W.* (2019), CCNA 200-301 Official Cert Guide, Volume 2, Cisco Press.

7. *Headquarters, A.* (2018), First Hop Redundancy Protocols Configuration Guide, Cisco IOS Release 15.1 M&T.

8. *Hinden, R.* (2004), "Virtual Router Redundancy Protocol (VRRP)", RFC 3768, Internet Engineering Task Force (IETF).

9. *Nadas, S.* (2010), "Virtual router redundancy protocol (vrrp) version 3 for IPv4 and IPv6", RFC 5798, Internet Engineering Task Force (IETF).

10. *Koch, F., Hansen, K. T.* (2006), "Redundancy Performance of Virtual Network Solutions", 2006 IEEE Conference on Emerging Technologies and Factory Automation, P. 328-332. **DOI**: https://doi.org/10.1109/ETFA.2006.355395

11. *Nur, R., Saharuna, Z., Irmawati, I., Irawan I., Wahyuni, R.* (2018), "Gateway Redundancy Using Common Address Redundancy Protocol (CARP)", International Journal of Information Technology and Electrical Engineering (IJITEE), vol. 2, no. 3, pp. 71-77.

12. *Denis, F.* (2013), "UCARP". [Online], https://github.com/jedisct1/ UCarp, access date: 03-Apr-2017.

13. *Danhieux, P.* (2004), "CARP-The Free Fail-over Protocol", GSEC, Practical v1.4b, SANS Institute, P. 1-16.

14. Juniper Networks ScreenOS Release Notes, July 2018, Juniper Networks, Inc.

15. *Sujitha, S., Priya, K.P., Pragathi, B.* (2016), "Fault Tolerant SDN Controller: A Survey," International Journal of Advanced Research, P. 186-191.

16. *Das, R. K., Pohrmen, F. H., Maji A. K., Saha, G.* (2020), "FT-SDN: a fault-tolerant distributed architecture for software defined network," Wireless personal communications, No. 114(2), P. 1045-1066. **DOI**: https://doi.org/10.1007/s11277-020-07407-x

17. *Hyojoon, Kim, Schlansker, M., Santos, J. R., Tourrilhes, J., Turner, Y., Feamster, N.* (2012), "CORONET: Fault tolerance for Software Defined Networks," 2012 20th IEEE International Conference on Network Protocols (ICNP), P. 1-2. **DOI**: https://doi.org/10.1109/ICNP.2012.6459938

18. *Sidki, L., Ben-Shimol, Y., Sadovski, A.* (2016), "Fault tolerant mechanisms for SDN controllers," 2016 IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN), P. 173-178. **DOI**: https://doi.org/10.1109/NFV-SDN.2016.7919494

19. *Li, Q., Liu, Y., Zhu, Z., Li, H, Jiang, Y.* (2019), "BOND: Flexible failure recovery in software defined networks," Computer Networks, No. 149, P. 1-12. **DOI**: https://doi.org/10.1016/j.comnet.2018.11.020

20. *Hu, T., Yi, P., Lan, J., Hu, Y., Sun, P.* (2020), "FTLink: Efficient and flexible link fault tolerance scheme for data plane in Software-Defined Networking", Future Generation Computer Systems, No. 111, P. 381-400. **DOI**: https://doi.org/10.1016/j.future.2019.11.015

21. *ElDefrawy, K., Kaczmarek, T.* (2016), "Byzantine Fault Tolerant Software-Defined Networking (SDN) Controllers", 2016 IEEE 40th Annual Computer Software and Applications Conference (COMPSAC), P. 208-213. **DOI**: https://doi.org/10.1109/COMPSAC.2016.76

22. *Mahjoubi, A., Zeynalpour, O., Eslami, B., Yazdani, N.* (2019), "LBFT: Load Balancing and Fault Tolerance in distributed controllers", 2019 International Symposium on Networks, Computers and Communications (ISNCC), P. 1-6. **DOI**: https://doi.org/10.1109/ISNCC.2019.8909087

23. *Kuźniar, M., Perešíni, P., Vasić, N., Canini, M., Kostić, D.* (2013), "Automatic failure recovery for software-defined networks," Second ACM SIGCOMM workshop on Hot topics in software defined networking, P. 159-160. **DOI**: https://doi.org/10.1145/2491185.2491218

24. *Sakic, E., Đerić, N., Kellerer, W.* (2018), "MORPH: An Adaptive Framework for Efficient and Byzantine Fault-Tolerant SDN Control Plane", IEEE Journal on Selected Areas in Communications, No. 36(10), P. 2158-2174. **DOI**: https://doi.org/10.1109/JSAC.2018.2869938

25. *Ahmed, N. O., Bhargava, B.* (2020), "From Byzantine Fault-Tolerance to Fault-Avoidance: An Architectural Transformation to Attack and Failure Resiliency", IEEE Transactions on Cloud Computing, No. 8(3), P. 847-860. **DOI**: https://doi.org/10.1109/TCC.2018.2814989

26. *Kim, G., Kim, K.* (2016), "A study on the adaptation of the firefly algorithm for the synchronization between multiple controllers in SDN environment," 2016 International Conference on Information Networking (ICOIN), P. 308-311. **DOI**: https://doi.org/10.1109/ICOIN.2016.7427082

27. *Tomovic, S., Radusinovic, I.* (2018), "A new traffic engineering approach for QoS provisioning and failure recovery in SDN-based ISP networks", 2018 23rd International Scientific-Professional Conference on Information Technology (IT), P. 1-4. **DOI**: https://doi.org/10.1109/SPIT.2018.8350854

28. *Li, J., Wang, Y., Li, W., Qiu, X.* (2017), "Sharing data store and backup controllers for resilient control plane in multi-domain SDN," 2017 IFIP/IEEE Symposium on Integrated Network and Service Management (IM), P. 476-482. **DOI**: https://doi.org/10.23919/INM.2017.7987315

29. *Lemeshko, O., Yeremenko, O., Tariki, N.* (2017), "Solution for the default gateway protection within fault-tolerant routing in an IP network", International journal of electrical and computer engineering systems, No. 8(1), P. 19-26. **DOI**: https://doi.org/10.32985/ijeces.8.1.3

30. *Yeremenko, O., Tariki, N., Hailan, A. M.* (2016), "Fault-tolerant IP routing flow-based model", 2016 13th International Conference on Modern Problems of Radio Engineering, Telecommunications and Computer Science (TCSET), P. 655-657. **DOI**: https://doi.org/10.1109/TCSET.2016.7452143

31. *Lemeshko, O. V., Yeremenko, O. S., Tariki, N., Hailan, A. M.* (2016), "Fault-tolerance improvement for core and edge of IP network", 2016 XIth International Scientific and Technical Conference Computer Sciences and Information Technologies (CSIT), P. 161-164. **DOI**: https://doi.org/10.1109/STC-CSIT.2016.7589895

32. *Yeremenko, O., Tariki, N., Vavenko, T.* (2016), "Default gateway protection scheme in fault-tolerant IP routing", 2016 Third International Scientific-Practical Conference Problems of Infocommunications Science and Technology (PIC S&T), P. 223-226. **DOI**: https://doi.org/10.1109/INFOCOMMST.2016.7905389

33. *Lemeshko, O., Yevdokymenko, M., Yeremenko, O., Mersni, A., Segeč, P., Papán, J.* (2019), "Quality of Service Protection Scheme under Fast ReRoute and Traffic Policing Based on Tensor Model of Multiservice Network", 2019 International Conference on Information and Digital Technologies (IDT), P. 288-295. **DOI**: https://doi.org/10.1109/DT.2019.8813675

34. *Nevzorova, O., Lemeshko, O., Mersni, A., Hailan, A. M., Ali, A. S., Harkusha, S.* (2019), "Improved Two-Level Method of Multicast Routing in MPLS-TE Network," 2019 IEEE 2nd Ukraine Conference on Electrical and Computer Engineering (UKRCON), P. 846-850. **DOI**: https://doi.org/10.1109/UKRCON.2019.8879965

35. *Mersni, A., Ilyashenko, A., Vavenko, T.* (2017), "Complex optimality criterion for load balancing with multipath routing in telecommunications networks of nonuniform topology," 2017 14th International Conference The Experience of Designing and Application of CAD Systems in Microelectronics (CADSM), P. 100-104. **DOI**: https://doi.org/10.1109/CADSM.2017.7916095