УДК 004.7
DOI https://doi.org/10.32782/2663-5941/2026.1.2/17

Киричек Г.Г.
https://orcid.org/0000-0002-0405-7122
Національний університет «Запорізька політехніка»

Школовий В.В.
https://orcid.org/0009-0007-9986-9273
Національний університет «Запорізька політехніка»

ЗАБЕЗПЕЧЕННЯ ВІДМОВОСТІЙКОСТІ ТА НАДІЙНОСТІ МЕРЕЖ ПЕРЕДАЧІ ДАНИХ

У роботі здійснено комплексний аналіз архітектур корпоративних комп'ютерних мереж із зосередженням уваги на чинниках, що визначають їхню надійність, доступність та безперервність функціонування. Розглянуто типові загрози стабільності мережевої інфраструктури, пов'язані із відмовами мережевих пристроїв, каналів передачі даних і помилками конфігурації, а також проаналізовано сучасні підходи до підвищення відмовостійкості, шляхом використання механізмів резервування. Окрему увагу приділено протоколам першого переходу (First Hop Redundancy Protocols), які забезпечують безперервний доступ кінцевих вузлів до мережі за умов відмови основного шлюзу. З метою оцінювання практичної ефективності обраних рішень спроєктовано та реалізовано експериментальну модель відмовостійкої мережі в середовищі моделювання Cisco Packet Tracer. У рамках дослідження застосовано протокол Hot Standby Router Protocol (HSRP), який надає можливість організувати резервування шлюзів за замовчуванням і автоматичне перемикання трафіку у разі виникнення відмов. Проведено серію експериментів, які включали моделювання роботи мережі без використання механізмів резервування, із застосуванням HSRP зі стандартними значеннями таймерів, а також із використанням оптимізованих параметрів протоколу. Результати моделювання продемонстрували істотне зменшення часу простою мережі та зниження рівня втрат пакетів у сценаріях із використанням HSRP порівняно з базовою конфігурацією без резервування. Найвищі показники стабільності та швидкості відновлення з'єднання досягнуті за умови оптимізації таймерів протоколу, що підтверджує доцільність їх адаптації до конкретних умов експлуатації. Отримані результати свідчать про ефективність застосування протоколів резервування під час проєктування та модернізації корпоративних мереж і можуть бути використані як практичні рекомендації при впровадженні відмовостійкої мережевої інфраструктури у реальних корпоративних системах.

Ключові слова: *надійність мережі, відмовостійкість, резервування шлюзів, HSRP, протоколи першого переходу, мережеве моделювання.*

Постановка проблеми. У сучасних умовах корпоративні комп'ютерні мережі стають фундаментальною основою для функціонування інформаційних систем підприємств, установ і організацій [1]. Вони забезпечують інтеграцію окремих структурних підрозділів у єдиний інформаційно-комунікаційний простір, що створює умови для ефективного обміну даними, централізованого зберігання інформаційних ресурсів і реалізації сервісів різного рівня складності, від офісних прикладних систем до хмарних обчислень і комплексних систем управління ресурсами [7]. Розвинена корпоративна мережа сприяє оперативності прийняття управлінських рішень, координації діяльності територіально розподілених підрозділів та впровадженню сучасних засобів інформаційної та кібербезпеки.

Водночас, розширення масштабів корпоративних мереж, зростання кількості розподілених сервісів, активне використання мобільних пристроїв, технологій віртуалізації та хмарних платформ, визначають підвищені вимоги до їхньої надійності, пропускної здатності, масштабованості та рівня захищеності. За таких умов забезпечення відмовостійкості та безперервності функціонування корпоративних мереж розглядається як

один із пріоритетних напрямів розвитку сучасних інформаційно-комунікаційних технологій. Тому особливе значення набуває застосування механізмів резервування мережевих елементів, зокрема шлюзів за замовчуванням і каналів передачі даних.

Використання відповідних протоколів резервування надає можливість реалізувати автоматичне перемикання трафіку, у разі відмови основних компонентів мережі, що істотно зменшує час простою, знижує рівень втрат пакетів та забезпечує збереження доступності критично важливих сервісів. Актуальність даного дослідження визначається зростанням залежністю сучасних бізнес-процесів від безперебійної і стабільної роботи корпоративної мережевої інфраструктури, а також необхідністю впровадження ефективних рішень для підвищення її надійності та відмовостійкості.

Аналіз останніх досліджень і публікацій. Забезпечення надійності мереж та захист інформації є одним із першочергових завдань у контексті цифрової трансформації та зростання кіберзагроз [3]. Сучасні інформаційні системи повинні не лише протистояти зовнішнім атакам, але й зберігати стійкість під час внутрішніх збоїв та інфраструктурних несправностей [4].

Корпоративні комп'ютерні мережі зазвичай проєктуються за модульним принципом [5], зокрема відповідно до концепції SAFE blueprint, яка передбачає поділ мережевої інфраструктури на функціональні зони Campus Area, Edge Area та Service Provider Area [6]. Зона Campus Area призначена для обслуговування внутрішніх користувачів і забезпечує стабільний обмін даними між підрозділами, тоді як Edge Area відповідає за взаємодію корпоративної мережі із зовнішніми сервісами та віддаленими користувачами.

Чітке зональне розділення мережі спрощує впровадження механізмів логічної сегментації, зокрема VLAN і VRF, що знижує ризик поширення атак та забезпечує ізоляцію критично важливих сервісів [7]. Використання резервування каналів зв'язку, дублювання критичних елементів інфраструктури, протоколів швидкої конвергенції та механізмів failover дозволяє підтримувати неперервність бізнес-процесів навіть у випадку відмов обладнання або зовнішніх атак [8].

Важливою перевагою корпоративних мереж є масштабованість – поетапне розширення інфраструктури без суттєвих змін її архітектури. Модульні мережеві моделі, зокрема Cisco SAFE та зональні архітектури типу Campus–Edge–Data Center, забезпечують нарощування кількості користувачів і сервісів без втрати стабільності та безпеки [9]. Крім того, такі мережі підтримують різні типи трафіку, включно з даними, голосом і відео, а застосування механізмів QoS сприяє пріоритизації критичних сервісів та забезпеченню їх стабільної роботи навіть за умови високого навантаження [3].

Постановка завдання. Метою роботи є реалізація системи забезпечення відмовостійкості корпоративних комп'ютерних мереж із використанням протоколів резервування, а також дослідження відповідних методів і механізмів та оцінювання ефективності їх застосування в сучасних інформаційних системах. Об'єктом дослідження є корпоративна комп'ютерна мережа як інфраструктура передачі, обробки та доступу до даних. Предметом є методи підвищення відмовостійкості мережевої інфраструктури та протоколи резервування шлюзів першого переходу (First Hop Redundancy Protocols, FHRP).

У межах дослідження проведено аналіз архітектур корпоративних комп'ютерних мереж та визначено ключові чинники, які впливають на надійність, доступність і безперервність їх функціонування. Наведено сучасні методи підвищення відмовостійкості мережевої інфраструктури, зокрема механізми резервування та протоколи першого переходу (FHRP). Для перевірки практичної придатності обраних рішень реалізовано модель відмовостійкої корпоративної мережі в середовищі Cisco Packet Tracer із застосуванням протоколу Hot Standby Router Protocol (HSRP) для резервування шлюзів. Проведено моделювання роботи мережі за різних сценаріїв, зокрема без використання механізмів резервування, із застосуванням HSRP зі стандартними параметрами та з оптимізованими значеннями таймерів. Аналіз отриманих результатів за показниками часу відновлення працездатності мережі та рівня втрат пакетів дозволяє оцінити ефективність застосування протоколу HSRP. Результати дослідження використано для обґрунтування доцільності впровадження протоколів резервування під час проєктування та модернізації корпоративних мереж.

Виклад основного матеріалу. З огляду на проведений аналіз протоколів резервування [4-6] стає очевидним, що їх спільною метою є забезпечення безперервного доступу до мережі у разі відмови основного шлюзу [9], водночас кожен із них характеризується специфічними особливостями та перевагами [10]. Основними критеріями порівняння виступають швидкість перемикання на резервний канал, складність конфігурування,

сумісність із наявним мережевим обладнанням, масштабованість та можливість балансування навантаження [11-12]. У таблиці 1 представлено порівняльний аналіз протоколів резервування з урахуванням зазначених характеристик.

На основі проведеного аналізу робимо висновок, що всі розглянуті протоколи FHRP забезпечують безперервний доступ до мережі при відмові шлюзу, проте відрізняються сферами застосування. HSRP є надійним і простим у конфігурації рішенням для мереж на обладнанні Cisco, VRRP забезпечує сумісність у мультивендорних середовищах, а GLBP поєднує резервування та балансування навантаження для високонавантажених Cisco-мереж. Враховуючи орієнтацію дослідження на корпоративні мережі Cisco та необхідність експериментальної оцінки часу перемикання і параметрів відмовостійкості, для практичної реалізації обрано HSRP.

Логічна структура реалізованої мережі відображає принципи побудови відмовостійкої інфраструктури (рис. 1), у якій ключовим механізмом забезпечення безперервності роботи є протокол HSRP. В мережі виділено окремий VLAN 10, призначений для пристроїв користувачів. Використання VLAN дозволяє ізолювати трафік кінцевих станцій і забезпечити коректну роботу HSRP у межах спільного широкомовного домену.

Для забезпечення відмовостійкості мережі виконано конфігурацію протоколу HSRP на маршрутизаторах R1 та R2, а також налаштовано комутатори SW1 і SW2 та кінцеві пристрої PC1 і PC2.

Під час експериментальних досліджень показано, що значення таймерів hello/hold безпосередньо визначають час автоматичного перемикання (failover) HSRP. Стандартні параметри standby timers 3 10 забезпечують оптимальний баланс між швидкістю реакції та обсягом службового трафіку, проте для сервісів із підвищеними вимогами до доступності доцільно застосовувати зменшені значення, наприклад standby timers 1 3.

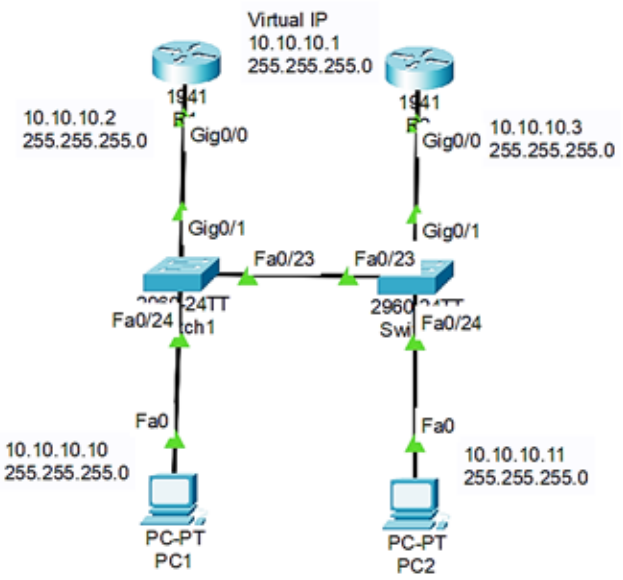

Рис. 1. Логічна схема мережі

Важливо дотримуватися рекомендацій щодо налаштування таймерів: значення мають бути однаковими на всіх маршрутизаторах HSRP-групи; не слід встановлювати інтервали менші за 1 секунду на мережах із повільними або перевантаженими ділянками, щоб уникнути хибних спрацьовувань; а також рекомендується узгоджувати таймери HSRP із параметрами протоколів динамічної маршрутизації для запобігання ситуаціям, коли шлюз уже перемкнувся, а маршрути ще не оновлені.

Для оцінки часу перемикання активного шлюзу імітувалася відмова маршрутизатора R1 у фіксований момент часу (10-та секунда симуляції). У кожному прогоні вимірювалися: момент вимкнення R1; час надходження першого HSRP-повідомлення від резервного маршрутизатора R2; час першої успішної ICMP-відповіді після переключення на резервний шлюз та кількість втрачених ICMP-пакетів під час події (табл. 2).

Середній час автоматичного перемикання склав приблизно 12,1 с, при цьому в середньому

Таблиця 1

Порівняння протоколів резервування

Критерій порівняння	HSRP	VRRP	GLBP
Сумісність із обладнанням	Висока (переважно Cisco)	Середня (різні виробники)	Середня (Cisco та сумісні)
Підтримка балансування навантаження	Низька (один активний маршрутизатор)	Низька (один master маршрутизатор)	Висока (декілька активних маршрутизаторів одночасно)
Складність налаштування	Середня	Середня	Середня
Час відновлення після відмови (failover time)	Дуже швидкий	Швидкий	Швидкий
Масштабованість	Висока	Висока	Висока

втрачалося 1,6 ICMP-пакета. На графіку зміни часу failover (рис. 2) видно, що розкид значень між окремими прогонами не перевищує 0,7 с, що свідчить про стабільність роботи HSRP.

Окремо досліджено процес повернення активної ролі R1 після його відновлення. У цьому сценарії маршрутизатор R2 виконує функції активного шлюзу, а після ввімкнення R1, за умови більш високого пріоритету та активованого preempt, відбувається зворотне перемикання активного шлюзу на R1. Під час експерименту фіксувалися: момент подачі живлення на R1; час появи першого HSRP-повідомлення від R1 після завантаження; час першої успішної ICMP-відповіді після повернення R1 до ролі активного маршрутизатора та кількість втрачених пакетів при перемиканні (табл. 3).

Побудований на основі отриманих даних графік (рис. 3) демонструє незначний розкид значень часу відновлення, що підтверджує передбачуваність роботи механізму preemption в умовах стандартних таймерів за протоколом HSRP.

Середній час від моменту надходження першого HSRP-повідомлення від R1 до відновлення успішних ICMP-відповідей становив близько 7,7 с, при цьому в кожному прогоні спостерігалася втрата лише одного ICMP-пакета, що є прийнятним показником для більшості застосунків, особливо з урахуванням, що процес перемикання залишався повністю прозорим для користувачів. Під час моделювання сценарію відмови активного R1 процедура залишалася незмінною: у фіксований момент часу, на десятій секунді симуляції, активний маршрутизатор вимикався, після чого фіксувалися: час відмови R1; час надходження першого HSRP-повідомлення від R2; час першої успішної ICMP-відповіді після перемикання та кількість втрачених ICMP-пакетів (табл. 4).

На основі даних, середній час перемикання становив приблизно 3,2 с, тобто у 3-4 рази менший, ніж при використанні стандартних таймерів. Кількість втрачених ICMP-пакетів при цьому не перевищувала 1-2 за раз, що можна вважати прийнятним значенням для більшості типів трафіку (рис. 4).

Побудований графік підтверджує, що зменшення таймерів дозволяє досягти стабільного та прогнозованого скорочення часу відновлення активної ролі без суттєвого збільшення кількості втрат пакетів.

Висновки. Аналіз базової конфігурації показав критичну залежність мережі від єдиного маршрутизатора-шлюзу. Використання HSRP зі

Таблиця 2

Вимірювання часу автоматичного перемикання

Прогін	Час вимкнення R1 (s)	Перший HSRP-пакет від R2 (s)	Перший успішний ICMP (s)	Failover time (s)	Втрачено ICMP
1	10.0	12.5	22.0	12.0	2
2	10.0	12.3	21.8	11.8	1
3	10.0	12.7	22.2	12.2	2
4	10.0	12.1	22.5	12.5	2
5	10.0	12.9	21.9	11.9	1
Середнє (прибл.)	-	12.5 ± 0.2	22.08 ± 0.2	12.08 ± 0.2	1.6

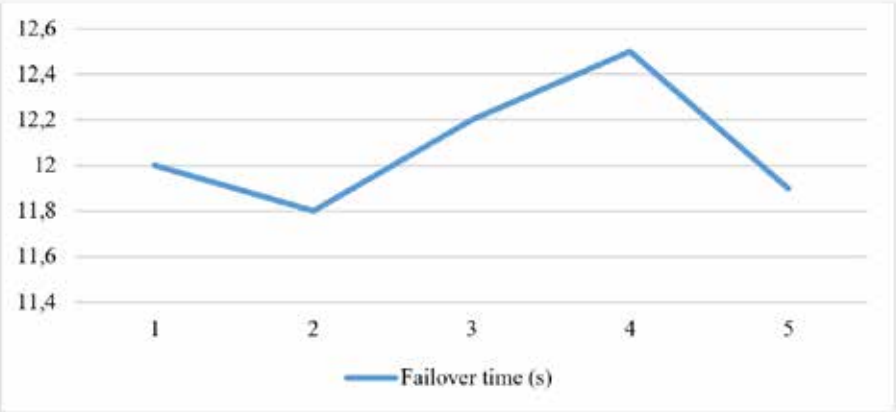

Рис. 2. Графік автоматичного відновлення

Таблиця 3

Вимірювання часу відновлення активної ролі R1

Прогін	Час увімкнення R1	Час появи першого HSRP від R1 після відновлення (s)	Перший успішний ICMP після відновлення (s)	Час від HSRP до пінг (s)	Втрачено ICMP
1	0.1	27.0	35.0	8.0	1
2	0.1	26.8	34.5	7.7	1
3	0.1	27.5	35.6	8.1	1
4	0.1	27.9	35.2	7.3	1
5	0.1	26.9	34.3	7.4	1
Середнє (прибл.)		-	-	7.7 ± 0.2	1

Рис. 3. Графік вимірювання часу відновлення R1

Таблиця 4

Автоматичне перемикання (failover) при таймерах HSRP 1/3

Прогін	Час вимкнення R1 (s)	Перший HSRP-пакет від R2 (s)	Перший успішний ICMP (s)	Failover time (s)	Втрачено ICMP
1	10.0	11.0	13.2	3.2	1
2	10.0	11.1	13.0	3.0	1
3	10.0	10.9	13.4	3.4	2
4	10.0	11.2	13.3	3.3	1
5	10.0	10.8	13.1	3.1	1
Середнє (прибл.)	–	11.0 ± 0.2	13.2 ± 0.2	3.2 ± 0.2	≈1.2

стандартними таймерами дозволило істотно підвищити відмовостійкість системи. Графік зміни часу failover для окремих прогонів демонструє невеликий розкид значень, що свідчить про стабільність роботи протоколу HSRP навіть за зменшених таймерів. Оптимізація параметрів HSRP шляхом зменшення інтервалів hello/hold дозволила скоротити час автоматичного перемикання з приблизно 12,1 с до 3,2 с, зменшити час повернення активної ролі R1 з близько 7,7 с до 2,1 с та зберегти низький рівень втрат ICMP-пакетів (0–2 за подію). Конфігурація з таймерами 1/3 забезпечує значно вищу оперативність реакції на відмову та відновлення вузлів, що робить її доцільною для використання в мережах із жорсткими вимогами до доступності та мінімальних простоїв. Отримані результати підтверджують ефективність застосування протоколів резервування у корпоративних мережах і демонструють, що коректний вибір параметрів HSRP суттєво впливає на показники доступності та якості мережевих сервісів.

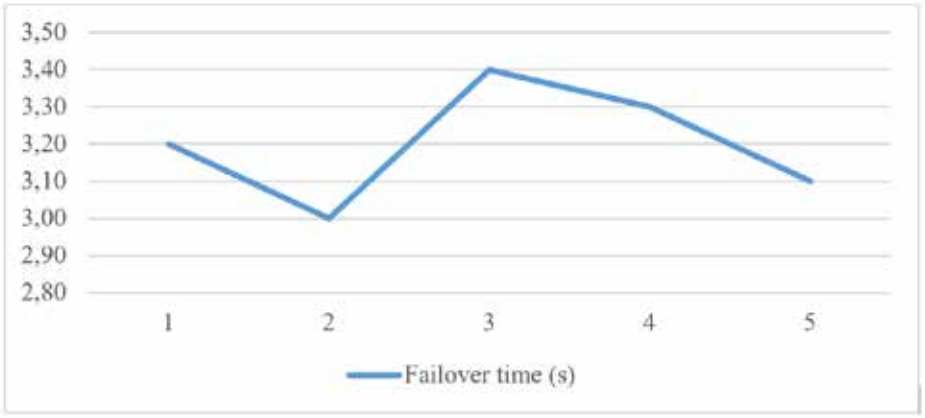

Рис. 4. Графік автоматичного відновлення

Список літератури:

1. Pestov O., Kyrychek H., Tiahunova M. Yggdrasil routing scheme as a basis for large-scale decentralized mesh networks. ICST-2024. *CEUR Workshop*, 2024. Vol. 3790. P. 110–122. URL: https://ceur-ws.org/Vol-3790/paper10.pdf

2. Jia M., Liu A., Narahara T. The integration of dual evaluation and minimum spanning tree clustering to support decision-making in territorial spatial planning. *Sustainability.* 2024. 16(10). 3928. DOI: https://doi.org/10.3390/su16103928

3. Киричек Г.Г., Тягунова М.Ю., Братчиков В.В. Система кешування даних в розгалуженій мікросервісній архітектурі. *Вчені записки Таврійського національного університету ім. В.І. Вернадського. Серія: Технічні науки*. 2024. Том 35 (74) № 1. Ч.1. С. 141-146. DOI: https://doi.org/10.32782/2663-5941/2024.1.1/21

4. Agarwal A., Sharma S., Xavier E. Performance Evaluation of HSRP and GLBP Over OSPF and RIP Routing Protocols. In: International Conference on Signal Processing and Integrated Networks. *Springer Nature Singapore*. 2022. P. 173–186. DOI: https://doi.org/10.1007/978-981-99-1312-1_14

5. Киричек Г. Г. Керування інформаційними потоками на всіх рівнях ієрархії отримання знань. *Радіоелектроніка, інформатика, управління*. 2010. № 1. С. 70–78. DOI: https://doi.org/10.15588/1607-3274-2010-1-13

6. Huang W., Chen Y., Hee J. STP technology: An overview and a conceptual framework. *Information & management*. 2006. 43(3). 263–270. DOI: https://doi.org/10.1016/j.im.2004.06.001

7. Yang L., Zhang D., Li L., He Q. Energy efficient cluster-based routing protocol for WSN using multi-strategy fusion snake optimizer and minimum spanning tree. *Scientific Reports.* 2024. 14(1). 16786.

8. Swaid M., Papakonstantinou S., Kloock-Schreiber D., Gollnick V. Design of a uam ground infrastructure network with respect to maintenance capacity requirements, 2024.

9. ALI H., M. Dynamic Fast Convergence Improvement using Predictive Network Analysis. Int. J. Comput. Digit. Syst, 2024, 16, 1-16.

10. Kosar Z., Zaman S., Ali W., Ullah A. The number of spanning trees in a K5 chain graph. *Physica Scripta.* 2023. 98(12). 125239. DOI: https://doi.org/10.1088/1402-4896/ad07b9

11. Bernardino R. C., Martins C. M., Pereira P. S., Lourenço G. E., Junior P. S. Link redundancy in the process bus according to IEC 61850 ED. 2: experience with RSTP, PRP and HSR protocols. In: IET Conference Proceedings CP800. Stevenage, *UK: The Institution of Engineering and Technology,* 2022. p. 164–169. DOI: https://doi.org/10.1049/icp.2022.0931

12. Abd D. F., Rashid R. A., Othman D. A., Abdulqader H. M. Performance evaluation using spanning tree protocol, rapid spanning tree protocol, per-VLAN spanning tree, and multiple spanning tree. *UHD Journal of Science and Technology,* 2024. 8(1), 20–30. DOI: https://doi.org/10.21928/uhdjst.v8n1y2024.pp20-30

Kyrychek H.H., Shkolovyi V.V. ENSURING RESILIENCE AND RELIABILITY OF DATA TRANSMISSION NETWORKS

The paper provides a comprehensive analysis of corporate computer network architectures, focusing on factors that determine their reliability, availability, and continuity of operation. Typical threats to network infrastructure stability associated with failures of network devices, data transmission channels, and configuration errors are considered, and modern approaches to increasing fault tolerance through the use of

redundancy mechanisms are analyzed. Special attention is paid to First Hop Redundancy Protocols, which provide continuous access of end nodes to the network in case of failure of the main gateway. In order to evaluate the practical effectiveness of the selected solutions, an experimental model of a fault-tolerant network was designed and implemented in the Cisco Packet Tracer simulation environment. The study used the Hot Standby Router Protocol (HSRP), which provides the ability to organize default gateway redundancy and automatic traffic switching in the event of failures. A series of experiments was conducted, which included modeling the network without the use of redundancy mechanisms, using HSRP with standard timer values, and using optimized protocol parameters. The simulation results demonstrated a significant reduction in network downtime and packet loss in scenarios using HSRP compared to the basic configuration without redundancy. The highest stability and connection recovery rates were achieved when the protocol timers were optimized, which confirms the feasibility of adapting them to specific operating conditions. The results obtained indicate the effectiveness of using redundancy protocols during the design and modernization of corporate networks and can be used as practical recommendations when implementing fault-tolerant network infrastructure in real corporate systems.

***Key**words:** network reliability, fault tolerance, gateway redundancy, HSRP, first hop protocols, network modeling.*

Дата першого надходження статті до видання: 12.01.2026
Дата прийняття статті до друку після рецензування: 05.02.2026
Дата публікації (оприлюднення) статті: 08.04.2026