

7. UNESCO. AI Competency Framework for Teachers. Paris : UNESCO, 2024. 60 p. URL: <https://unesdoc.unesco.org/ark:/48223/pf0000391104> (дата звернення: 20.08.2026).

8. Finnish National Agency for Education. Support for Digital Competence [Електронний ресурс]. Helsinki : Finnish National Agency for Education. URL: <https://www.oph.fi/en/education-and-qualifications/support-digital-competence> (дата звернення: 20.08.2026).

9. Education Estonia. Digital Competence [Електронний ресурс]. Tallinn : Education Estonia. URL: <https://www.educationestonia.org/digital-competence/> (дата звернення: 20.08.2026).

10. Education Estonia. eKool [Електронний ресурс]. Tallinn : Education Estonia. URL: <https://www.educationestonia.org/organisation/ekool-as/> (дата звернення: 20.08.2026).

DOI <https://doi.org/10.36059/978-966-397-651-8-31>

МЕРЕЖЕВА ВІДМОВСТІЙКІСТЬ ЯК ЧИННИК СТІЙКОСТІ ОСВІТИ

Киричек Галина Григорівна

*кандидат технічних наук, доцент,
доцент кафедри комп'ютерних систем та мереж
Національний університет «Запорізька політехніка»
м. Запоріжжя, Україна*

Тягунова Марія Юрївна

*кандидат технічних наук, доцент,
декан факультету комп'ютерних наук та технологій
Національний університет «Запорізька політехніка»
м. Запоріжжя, Україна*

Карнаух Дмитро Миколайович

*аспірант
Національний університет «Запорізька політехніка»
м. Запоріжжя, Україна*

Сучасний заклад вищої освіти (ЗВО) є цифровою екосистемою, у якій освітні, адміністративні та наукові процеси залежать від надійності інформаційно-комунікаційної інфраструктури, а комп'ютерна мережа забезпечує доступ до ключових цифрових сервісів і ресурсів. В умовах

воєнного стану стійкість освітньої та наукової діяльності значною мірою залежить від безперервної роботи цифрових сервісів, інформаційних ресурсів і мережевої інфраструктури [1]. При цьому зростання масштабів мереж ЗВО, використання хмарних платформ, мобільних пристроїв і віртуалізації підвищує вимоги до надійності, пропускну здатності, масштабованості та захищеності [2]. Відмови мережевого обладнання, каналів передачі даних або порушення конфігурацій можуть призводити до втрати доступу до систем дистанційного навчання, електронних бібліотек, хмарних сервісів та платформ комунікації [3-4]. Метою дослідження є підвищення стійкості цифрової інфраструктури ЗВО шляхом застосування механізмів мережевого резервування та оптимізації параметрів відмовостійкості. Об'єктом дослідження є цифрова мережева інфраструктура ЗВО та процеси забезпечення її безперервного функціонування.

Порушення функціонування мережевої інфраструктури може спричиняти каскадне поширення відмов між взаємопов'язаними компонентами цифрового середовища [5]. Вихід з ладу одного з критичних елементів: мережевого шлюзу, маршрутизатора, комутатора, каналу доступу до Інтернету, сервера або точки бездротового доступу, може призвести до недоступності інформаційних ресурсів і сервісів, зокрема систем дистанційного навчання, платформ відеоконференцій та хмарних ресурсів [6]. Тому забезпечення стійкості цифрової освітньої інфраструктури має ґрунтуватися на комплексному застосуванні методів, які доповнюють одне одного: резервуванні мережевого та серверного обладнання, дублюванні каналів зв'язку, сегментації мережі, застосуванні механізмів автоматичного перемикавання на резервні компоненти та організації оперативного відновлення після відмов. Такий підхід дає змогу локалізувати вплив окремих несправностей, запобігати їх поширенню на критичні сервіси та підтримувати безперервність інформаційного обміну [7].

Одним із ключових механізмів підвищення відмовостійкості є застосування протоколів резервування першого переходу (FHRP, First Hop Reservation Protocol), зокрема HSRP, VRRP та GLBP, які забезпечують доступність шлюзу в разі відмови маршрутизатора [8]. Для мереж на базі обладнання Cisco доцільним є застосування HSRP, який забезпечує використання віртуальної IP-адреси у якості шлюзу за замовчуванням і застосовує автоматичне перемикавання на резервний маршрутизатор при відмові активного. Застосування такого механізму в мережі ЗВО сприяє збереженню доступу студентів і викладачів до цифрових та мережевих ресурсів без необхідності зміни налаштувань кінцевих пристроїв [9].

Для оцінювання ефективності резервування побудовано модель мережі в Cisco Packet Tracer із двома маршрутизаторами R1 і R2, комутаторами, кінцевими пристроями та VLAN, налаштованими для роботи HSRP. Експеримент передбачав відмову активного маршрутизатора R1 на 10-й секунді, фіксацію часу перемикання і кількості втрачених ICMP-пакетів [10]. При цьому за стандартних таймерів середній час перемикання дорівнював 12,1 с, а кількість втрат становила 1,6 пакета (табл. 1). Використання оптимізованих таймерів HSRP 1/3 дозволило скоротити середній час до 3,2 с, зберігаючи кількість втрачених пакетів на низькому рівні, що становило близько 1-2 за подію.

Таблиця 1

Порівняння результатів роботи HSRP

Показник	Стандартні таймери HSRP	Оптимізовані таймери HSRP 1/3
Середній час failover, с	12,1	3,2
Середня кількість втрачених ICMP-пакетів	1,6	≈1,2
Характер відновлення	Автоматичний	Автоматичний
Відносне скорочення часу перемикання	–	≈73,6
Придатність для критичних сервісів	Середня	Вища

Отже, зміна параметрів протоколу дозволила суттєво скоротити період недоступності мережевого шлюзу. Розраховане скорочення часу становить приблизно 73,6 %, що є важливим результатом з позиції забезпечення безперервності цифрових сервісів. Порівняння п'яти експериментальних запусків (рис.1) демонструє суттєву різницю між стандартними та оптимізованими параметрами HSRP.

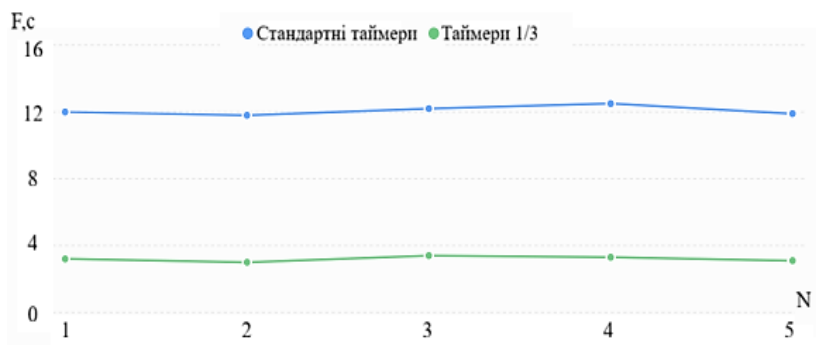


Рис. 1. Порівняння часу автоматичного перемикавання

Для стандартної конфігурації значення failover становили 12,0; 11,8; 12,2; 12,5 та 11,9 с. Для таймерів 1/3 відповідні значення були 3,2; 3,0; 3,4; 3,3 та 3,1 с. Це показує не лише скорочення середнього часу відновлення, а й збереження достатньо стабільного характеру роботи протоколу. Для цифрового освітнього середовища така властивість є принципово важливою, оскільки короткочасна втрата мережевого доступу може бути менш критичною, ніж тривала або непередбачувана недоступність сервісу.

У роботі розглянуто мережеву відмовостійкість як складову стійкості освітнього середовища та обґрунтовано доцільність резервування критичних мережевих компонентів, зокрема шлюзів за замовчуванням. Практичне дослідження виконано шляхом моделювання відмовостійкої мережі в середовищі Cisco Packet Tracer із використанням протоколу HSRP. Отримані результати підтверджують доцільність використання мережевого резервування та оптимізації параметрів HSRP для підвищення стійкості цифрової інфраструктури, забезпечення безперервності освітньої та наукової діяльності в умовах воєнного стану. Результати дослідження свідчать про доцільність комплексного забезпечення стійкості цифрової інфраструктури ЗВО шляхом резервування критичних мережевих компонентів і каналів зв'язку та оптимізації параметрів мережевих протоколів. Логічна сегментація мережі за допомогою VLAN підвищує керованість і сприяє локалізації порушень, а резервування інформаційних ресурсів забезпечує збереження навчальних матеріалів, електронних курсів і конфігурацій обладнання. Отже, стійкість освітнього середовища має формуватися комплексно на фізичному, мережевому, інформаційному, програмному та організаційному рівнях. Перспективним напрямом подальших досліджень є розроблення комплексної моделі стійкої цифрової

інфраструктури закладу вищої освіти, яка поєднуватиме мережеве резервування, альтернативні канали доступу, бездротові технології, хмарні сервіси та механізми автоматичного відновлення критичних освітніх ресурсів.

Література

1. Kirichek G., Tymoshenko V., Rudkovskyi O., Hrushko S. Decentralized System for Run Services. In: CMIS. 2019. P. 860-872. URL: <https://ceur-ws.org/Vol-2353/paper68.pdf>
2. 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: 10.1088/1402-4896/ad07b9
3. 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: 10.1007/978-981-99-1312-1_14
4. 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: 10.3390/su16103928
5. ALI H., M. Dynamic Fast Convergence Improvement using Predictive Network Analysis. *Int. J. Comput. Digit. Syst*, 2024, 16, 1-16
6. Tiahunova M. Y, Kyrychek H. H, Bohatyrova T O., Moshynets D. D. System and method of automatic collection of objects in the room. In CEUR Workshop Proceedings, 2021. Vol 3077. P. 174–186
7. Huang W., Chen Y., Hee J. STP technology: An overview and a conceptual framework. *Information & management*, 2006, 43(3), 263-270. DOI: 10.1016/j.im.2004.06.001
8. 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: 10.21928/uhdjst.v8n1y2024.pp20-30
9. 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
10. Киричек Г.Г., Школовий В.В. Забезпечення відмовостійкості та надійності мереж передачі даних. *Вчені записки ТНУ імені В.І. Вернадського. Серія: Технічні науки*. 2026. Том 37 (76) № 1. Ч. 2. С. 128-134. DOI: 10.32782/2663-5941/2026.1.2/17