International Conference on Inventive Computation Technologies (ICICT). IEEE. 2022. P. 452–456. DOI: https://doi.org/10.1109/ICICT54344.2022.9850965

6. Tang W., Han Y., Ai T., Li G., Yu B., Yang X. Yggdrasil: Reducing Network I/O Tax with (CXL-Based) Distributed Shared Memory. Proceedings of the 53rd International Conference on Parallel Processing. 2024. P. 597–606. DOI: https://doi.org/10.1145/3673038.3673138

7. Tanenbaum A., Wetherall D. Computer networks. Pearson, 2021. 944 p.

8. Kurose J., Ross K. Computer Networking: A Top-Down Approach, Global Edition. Pearson Education; 2018. 856 p.

9. TigerVNC. URL: https://tigervnc.org/ (дата звернення: 25.03.2026).

10. Киричек Г. Г., Пестов О. Д., Тягунова, М. Ю. Система віддаленого керування об'єктами критичної інфраструктури. *Системи та технології*. 2024, 68 (2). С. 63–70. DOI: https://doi.org/10.32782/2521-6643-2024-2-68.7

11. Yggdrasil Network. URL: https://yggdrasil-network.github.io/ (дата звернення: 25.03.2026).

DOI https://doi.org/10.36059/978-966-397-621-1-64

Морозюк А. В.,
студент ІІ курсу магістратури факультету інформаційних технологій Хмельницького національного університету
м. Хмельницький, Україна

КІБЕРФІЗИЧНА СИСТЕМА ПРОЦЕСУ НАВІГАЦІЇ ПРИ ВИЗНАЧЕННІ НЕСПРАВНИХ ВУЗЛІВ ТЕЛЕКОМУНІКАЦІЙНОЇ МЕРЕЖІ

Розвиток сучасних телекомунікаційних мереж супроводжується стрімким зростанням їх складності: типова корпоративна або операторська мережа охоплює сотні взаємопов'язаних вузлів різного призначення. Це маршрутизатори, комутатори, шлюзи безпеки, сервери прикладних сервісів, віртуальні машини та контейнеризовані компоненти. Тому будь-яке, навіть локальне порушення нормального функціонування вузла здатне спричинити каскадну деградацію сервісів, фінансові втрати та зниження рівня доступності критичних ресурсів [1].

Забезпечення стійкості та безперебійної роботи телекомунікаційних мереж особливої актуальності набуло натепер – в сучасних умовах воєнних загроз. Періодичні відключення електроенергії, підвищене

навантаження на мережі та цілеспрямовані кібератаки створюють додаткові ризики виникнення збоїв і ускладнюють їх оперативне виявлення. У зв'язку з цим особливого значення набуває впровадження інтелектуальних та автоматизованих систем моніторингу, здатних швидко ідентифікувати несправні вузли, забезпечувати ефективну навігацію до них та підтримувати стабільність функціонування інфраструктури навіть у критичних ситуаціях.

Традиційні підходи до адміністрування мереж значною мірою покладаються на ручний аналіз сповіщень систем моніторингу. А це ускладнює оперативне реагування на несправності та напряму залежить від кваліфікації персоналу. Особливо гостро ця проблема проявляється у ситуаціях каскадних відмов, коли система моніторингу одночасно генерує велику кількість сигналів, серед яких важко виділити першопричину інциденту [2, с. 165]. Саме тому актуальним стає впровадження кіберфізичних систем (КФС), що поєднують програмні та апаратні компоненти для автоматизованого збору, аналізу та обробки телеметричних даних у режимі реального часу.

Кіберфізична система у контексті телекомунікаційних мереж являє собою програмно-апаратний комплекс, у якому цифрова модель середовища формується на підставі телеметричних даних, а прийняті аналітичним модулем рішення здатні впливати на логіку управління фізичною інфраструктурою або на маршрутизацію трафіку [3, с. 161]. Фундаментальна властивість такої системи – замкнений контур «спостереження – аналіз – рішення – вплив» – є принципово відмінною від класичних систем моніторингу, орієнтованих переважно на фіксацію відхилень без автоматизованої локалізації їхнього джерела.

Аналіз існуючих рішень у сфері виявлення та локалізації несправностей показує, що жоден окремий підхід не забезпечує одночасно повноти спостереження, точності визначення першопричини та зручної навігації до проблемного вузла. Централізовані системи моніторингу (Zabbix, Nagios) добре відповідають на запитання «що не працює», але погано – на запитання «де саме виникла першопричина». Системи топологічного аналізу забезпечують структурний контекст, проте залежать від актуальності моделі мережі.

Інтелектуальні методи на базі машинного навчання підвищують прогностичність, однак потребують якісних навчальних даних та розвинених механізмів пояснюваності [4]. У звязку з цим найбільш перспективним є гібридний кіберфізичний підхід, що інтегрує переваги зазначених класів рішень.

Кіберфізична система будується навколо графової моделі мережі $G = (V, E)$, де V – множина вузлів (маршрутизатори, комутатори, сервери), а E – множина зв'язків між ними з вагами, що відображають поточний стан каналів [5]. Графова модель дозволяє не лише зберігати топологічну структуру мережі, а й динамічно оновлювати її відповідно

до зібраної телеметрії: затримки, втрати пакетів, стан інтерфейсів та навантаження на вузли.

Архітектура розробленої системи включає чотири логічні підсистеми. Шар збору даних отримує від вузлів оперативну телеметрію через активні перевірки доступності та пасивний збір журналів. Цифрова модель мережі зберігає відомості про вузли, зв'язки, їхні ролі та історію змін станів. Аналітична підсистема обчислює інтегральну оцінку ризику несправності кожного вузла за формулою:

$$Risk(v) = \alpha \cdot A(v) + \beta \cdot C(v) + \gamma \cdot H(v),$$

де A(v) – прямі аномальні ознаки вузла, C(v) – контекстні ознаки на основі топології та сусідніх подій, H(v) – історичний профіль відхилень, а α, β, γ – вагові коефіцієнти [4]. Навігаційна підсистема формує маршрут перевірки як послідовність переходів по ваговому графу з мінімальною вартістю:

$$Cost(R) = \Sigma\, w(ei) + \Sigma\, p(vj),$$

де w(ei) – стан зв'язку між суміжними вузлами, p(vj) – штраф за проходження через потенційно нестабільний вузол. Для пошуку оптимального маршруту застосовуються класичні алгоритми на графах. Алгоритм Дейкстри [6] забезпечує знаходження найкоротшого шляху в графі з невід'ємними вагами ребер і є основою навігації між вузлами мережі. Алгоритм A* [7] доповнює його евристичною оцінкою вартості, що дозволяє прискорити пошук у великих мережах за рахунок пріоритизації напрямків перевірки з більшою ймовірністю наявності несправності.

Для практичної реалізації та експериментальної перевірки системи слід обрати підхід на базі контейнеризації з використанням Docker [8]. Кожен вузол мережі моделюється як окремий контейнер із визначеними сервісами та мережевими інтерфейсами. Це дозволяє відтворювати різні класи несправностей – повну відмову вузла, деградацію каналу, перевантаження ресурсів – без необхідності використання великої кількості фізичного обладнання. Контейнерне середовище також забезпечує високу повторюваність експериментів та можливість поступового масштабування стенду.

Наявна система моніторингу Zabbix генерує значний обсяг сповіщень під час каскадних відмов, а процес визначення першопричини інциденту потребує ручного аналізу та залучення досвідчених інженерів. Це збільшує час реагування та підвищує залежність від людського фактора.

Апробувати систему необхідно за чотирма типовими сценаріями: повна відмова вузла, деградація каналу зв'язку, перевантаження проміжного комутатора та каскадна відмова з множинними симптомами.

Ефективність системи оцінюватиметься за критеріями точності локалізації першопричини, часу реакції від появи симптомів до формування навігаційного висновку, стійкості до неповноти телеметричних даних та масштабованості при збільшенні кількості вузлів [2, с. 1537].

Таким чином, розробка кіберфізичної системи навігації при визначенні несправних вузлів телекомунікаційної мережі є актуальною науково-практичною задачею. Запропонований підхід, що поєднує графову модель мережі, інтегральну оцінку ризику та алгоритмічну навігацію у контейнеризованому середовищі, дозволяє подолати обмеження існуючих рішень і забезпечити автоматизоване визначення несправного вузла без залежності від людського фактора. Результати мають безпосередню практичну цінність для підприємств галузі телекомунікацій [3, с. 165].

Список використаних джерел:

1. Tanenbaum A. S., Wetherall D. J. Computer Networks. 5th ed. Boston : Pearson, 2011. 960 p.
2. Steinder M., Sethi A. S. A Survey of Fault Localization Techniques in Computer Networks. *Science of Computer Programming*. 2004. Vol. 53, No. 2. P. 165–194.
3. Baheti R., Gill H. Cyber-physical systems. The Impact of Control Technology / ed. T. Samad, A. M. *Annaswamy. IEEE Control Systems Society*. 2011. P. 161–166.
4. Boutaba R., Salahuddin M. A., Limam N., Ayoubi S., Shahriar N., Estrada-Solano F., Caicedo O. M. A Comprehensive Survey on Machine Learning for Networking: Evolution, Applications and Research Opportunities. *Journal of Internet Services and Applications*. 2018. Vol. 9, No. 16.
5. Barabasi A.-L. Network Science. Cambridge: Cambridge University Press, 2016. 476 p.
6. Dijkstra E. W. A note on two problems in connexion with graphs. *Numerische Mathematik*. 1959. Vol. 1. P. 269–271.
7. Hart P. E., Nilsson N. J., Raphael B. A Formal Basis for the Heuristic Determination of Minimum Cost Paths. *IEEE Transactions on Systems Science and Cybernetic*s. 1968. Vol. 4, No. 2. P. 100–107.
8. Merkel D. Docker: Lightweight Linux Containers for Consistent Development and Deployment. *Linux Journal.* 2014. No. 239.
9. Cherrared S., Imadali S., Fabre E., Gossler G., Grida Ben Yahia I. A Survey of Fault Management in Network Virtualization Environments: Challenges and Solutions. *IEEE Transactions on Network and Service Management*. 2019. Vol. 16, No. 4. P. 1537–1551.
10. Lee E. A., Seshia S. A. Introduction to Embedded Systems: A Cyber-Physical Systems Approach. 2nd ed. MIT Press, 2017. 592 p.