УДК 004.056:621.391

МЕТОДИ ВІДМОВОСТІЙКОЇ МАРШРУТИЗАЦІЇ В ІНФОКОМУНІКАЦІЙНІЙ МЕРЕЖІ З БАЛАНСУВАННЯМ НАВАНТАЖЕННЯ НА ОСНОВІ МЕТРИК РИЗИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Міланка І.Ю.
e-mail: ihor.milanka@nure.ua.
Харківський національний університет радіоелектроніки, каф. ІКІ
м. Харків, Україна

Ensuring the robustness and security of infocommunication networks has become a vital challenge in today's dynamic environment. Conventional routing techniques prioritize Quality of Service (QoS) but frequently neglect cybersecurity vulnerabilities, leaving networks exposed to potential threats. This study examines a fault-tolerant routing method that incorporates security metrics based on risk assessment while maintaining balanced network utilization. The proposed solution optimizes traffic flow by factoring in the reliability of network components alongside cybersecurity risks. Adopting this approach strengthens network stability and security, enabling efficient data transmission even in challenging circumstances. The outcomes of this research offer valuable insights for advancing secure and resilient network infrastructure.

У сучасних інфокомунікаційних мережах підтримання відмовостійкості та ефективного розподілу навантаження є вкрай важливими для забезпечення безперервної роботи та високого рівня якості обслуговування (QoS). Разом із цим, зростання кількості кіберзагроз диктує необхідність врахування параметрів інформаційної безпеки у процесах маршрутизації. У представлених тезах розглядаються підходи до відмовостійкої маршрутизації з урахуванням балансування навантаження, які включають до аналізу метрики ризиків інформаційної безпеки.

Забезпечення надійності та безпеки інфокомунікаційних мереж є одним із основних викликів сучасності. Хоча традиційні методи маршрутизації здебільшого орієнтовані на підтримання якості обслуговування (QoS), вони часто недостатньо враховують аспекти інформаційної безпеки, що створює потенційні вразливості у мережі. Включення метрик ризиків інформаційної безпеки у процес маршрутизації сприяє підвищенню загальної стійкості мережі перед кіберзагрозами.

Розглянемо сучасні підходи, які об'єднують у собі елементи відмовостійкості, балансування навантаження та забезпечення інформаційної безпеки, спрямовані на підвищення ефективності та стабільності мережевих систем.

Один із таких підходів – потокова модель безпечної маршрутизації. Ця модель ґрунтується на засадах Traffic Engineering і розширює їх за рахунок інтеграції параметрів мережевої безпеки. Вона враховує низку

критичних факторів, таких як рівень ризиків інформаційної безпеки для маршрутизаторів і каналів зв'язку, ймовірність експлуатації вразливостей у протоколах та обладнанні, а також можливі загрози витоку даних. Завдяки цьому підходу забезпечується зважений компроміс між якістю обслуговування (QoS) та рівнем безпеки мережі, що дозволяє ефективно розподіляти навантаження між ресурсами, оптимізуючи їх використання й одночасно мінімізуючи ризики[1].

Ще одну групу інноваційних рішень складають моделі швидкої перемаршрутизації. Ці моделі орієнтовані на оперативне перенаправлення трафіку в разі виникнення відмов чи інших позаштатних ситуацій, при цьому зберігаючи високі показники QoS та дотримуючись вимог інформаційної безпеки. Ключовим інструментом їхньої реалізації виступають тензорні методи аналізу, які дозволяють глибоко досліджувати структуру мережі та швидко приймати оптимальні рішення щодо переналаштування маршрутів. Завдяки використанню цих моделей значно скорочуються затримки в обробці трафіку, підвищується адаптивність мережевої інфраструктури, а також покращується її стійкість до зовнішніх загроз і технічних збоїв[2].

Таким чином, обидва підходи спрямовані на забезпечення високого рівня надійності та безпеки сучасних комп'ютерних мереж, досягнення балансу між продуктивністю й захистом даних, а також створення більш гнучкої й інтелектуальної екосистеми управління трафіком.

Під час організації балансування навантаження важливо ретельно враховувати параметри надійності різних складових мережі, оскільки саме від них залежить загальна ефективність роботи системи.

Ключовою частиною цього процесу є впровадження проактивних стратегій відмовостійкої маршрутизації. Ці підходи сприяють оптимальному розподілу навантаження як на рівні транспортної мережі, так і на рівні доступу до ресурсів. Увага при цьому приділяється надійності критично важливих компонентів, таких як прикордонні маршрутизатори, які виконують важливу роль у структурі системи. Завдяки такому підходу забезпечується підвищення стійкості мережі до можливих збоїв, мінімізуються ризики порушень у роботі та створюються умови для стабільного й безперебійного обслуговування навіть за наявності технічних або непередбачуваних проблем[3].

Інтеграція метрик ризиків інформаційної безпеки у процеси відмовостійкої маршрутизації та балансування навантаження є важливим кроком для підвищення надійності та безпеки інфокомунікаційних мереж. Запропоновані підходи успішно поєднують якість обслуговування (QoS) із необхідним рівнем захисту, що має вирішальне значення для сучасних мережевих інфраструктур.

Список використаних джерел:

1. Євдокименко, М. О., Шаповалова, А. С., Шаповал, М. М. (2020), “Потокова модель маршрутизації з урахуванням ризиків інформаційної безпеки за допомогою базових метрик критичності вразливостей”, Проблеми телекомунікацій, No. 1(26), С. 48-62. URL:http://pt.nure.ua/wp-content/uploads/2021/03/201_yevdokimenko_security.pdf.

2. Євдокименко М. О. Теоретичні основи відмовостійкої маршрутизації чутливого до затримок та втрат трафіка в телекомунікаційних мережах з використанням тензорних моделей і методів. URL:https://uacademic.info/ua/document/0521U100030?utm_source=chatgpt.com.

3. 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. DOI: https://doi.org/10.30837/978-966-659-282-1.