A METHOD FOR ENHANCING THE RESILIENCE OF MULTISEGMENT CORPORATE COMPUTER NETWORKS IN HEALTHCARE INSTITUTIONS

Tkachov Vitalii, Mikhnov Yevgen
Kharkiv National University of Radio Electronics, Kharkiv, Ukraine

For multi-segment networks of modern medical institutions, a high level of network reliability is critically important for maintaining the quality of medical care. In conditions of limited resources and the possible destruction of infrastructure caused by military conflicts and natural disasters, there are risks of failures associated with interruptions in power supply, unauthorized access to confidential data due to cyber threats, as well as delays or loss of data due to overloading of network segments, which significantly affects the quality and possibility of providing medical services [1].

Ensuring continuous access to critical data requires the implementation of complex solutions to ensure fault tolerance of multi-segment networks [2]. The purpose of this work is to develop a method of increasing the fault tolerance of multi-segment networks in medical institutions, which requires the integration of physical and software solutions to ensure the stable operation of the network infrastructure.

According to scientific studies in this field, the emphasis is on reservation methods that provide duplication of network components, such as congestion routers, switches, and communication channels.

The application of load balancing for uniform distribution of traffic is also considered. The implementation of virtualization technologies and server clustering contributes to system scaling, reduces delays and downtime, and also reduces the overall load on the existing physical infrastructure. To ensure a high level of data protection and integrity, as well as reliable remote access between segments, it is advisable to use VPNs, which reduce the risks of unauthorized access to critical data and information leakage [3, 4].

The use of monitoring systems in multi-segment networks makes it possible to quickly respond to the detection of failures and warn of possible failures, which minimizes downtime and increases the speed of network recovery.

Список літератури

1. Maltseva, I., Chernish, Y., Shtonda, R. (2022). Аналіз деяких кіберзагроз в умовах війни. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 4(16), 37–44. https://doi.org/10.28925/2663-4023.2022.16.3744

2. Лемешко О. В. Потокові моделі та методи маршрутизації в інфокомунікаційних мережах: відмовостійкість, безпека, масштабованість : монографія / О. В. Лемешко, О. С. Єременко, О. С. Невзорова – Х. : ХНУРЕ, 2020. – 308 с. – ISBN 978-966-659-282-1

3. Hvozdetska, K. P., Tkachov, V. M. (2021). Organization of teleworking via VPN technology.

4. Kovalenko, A., Kuchuk, H., Tkachov, V. (2021). Метод забезпечення живучості комп'ютерної мережі на основі VPN-тунелювання. Системи управління, навігації та зв'язку. Збірник наукових праць, 1(63), 90-95.