

ANALYSIS OF FAULT TOLERANCE ALGORITHMS IN MULTISEGMENT NETWORKS

Тkachov Vitalii, Mikhnov Yevgen

Kharkiv National University of Radio Electronics, Kharkiv, Ukraine

Fault tolerance is a determining factor in the effective operation of multi-segment networks of medical institutions, which directly affects the stability of the provision of medical services. In modern conditions of high network load and potential threats, in particular, unauthorized access to medical data and power outages, there is a need to implement solutions capable of minimizing the risks of network infrastructure failures [1]. Such factors as delays in data transmission, a significant volume of information flows and disruptions in energy supply can negatively affect the timeliness and quality of medical care.

The purpose of the study is a comprehensive analysis of the factors that contribute to the occurrence of network failures, as well as an assessment of methods of ensuring fault tolerance of multi-segment networks of medical institutions, which will increase the reliability of data transmission, optimize the use of network resources, and protect the confidentiality of information. Achieving this goal involves the implementation of a comprehensive approach that includes load balancing and virtualization of network components aimed at ensuring high performance and security of the network infrastructure [2]. The results of scientific research in this direction indicate that the introduction of overlay networks allows for efficient distribution of network traffic under conditions of limited physical infrastructure, reducing the risk of overload and ensuring high stability and scalability of the system. The use of server clusters, implemented with the help of software, ensures uniform load distribution, effective backup of critical data and creation of alternative routes to maintain network stability in case of component failures [3, 4]. Thus, the application of these methods increases the fault tolerance of the infrastructure and ensures the necessary level of performance and security of the network system, especially under conditions of limited physical resources and possible power outages.

References

1. T. Vitalii, B. Anna, H. Kateryna and D. Hrebenuk, «Method of Building Dynamic Multi-Hop VPN Chains for Ensuring Security of Terminal Access Systems,» 2020 IEEE PIC S&T, Kharkiv, Ukraine, 2020, pp. 613-618, doi: 10.1109/PICST51311.2020.9467953.
2. Огляд методів балансування навантаження в хмарних системах / Р.М. Минайленко, В.А. Резніченко, О.К. Коноплицька-Слободенюк, Л.І. Поліщук // Конструювання, виробництво та експлуатація сільськогосподарських машин: загальнодерж. міжвід. наук.-техн. зб. – Кропивницький: ЦНТУ, 2021. – Вип. 51. – С. 188-194.
3. Malik, S. et al. «Intelligent Load-Balancing Framework for Fog-Enabled Communication in Healthcare.» *Electronics*, vol. 11, no. 4, 2022.
4. Kuchuk, N., Kovalenko, A., Tkachov, V., Rosinskiy, D., & Kuchuk, H. (2021). Predicting traffic anomalies in container virtualization. *Computer and Information Systems and Technologies*.