UDC 004.056

APPLICATION OF SAFETY AND CYBER SECURITY TECHNOLOGIES IN HEALTHCARE

N. A. Dubrovina[1], V. A. Klymenko[2], O. V. Vysotska[3], L. S. Guryanova[4], V. A. Dubrovina[4]
[1]School of Economics and Management in Bratislava, [2]Kharkiv National Medical University,
[3]National Aerospace University "Kharkiv Aviation Institute",
[4]Kharkiv National Economic University named after S.Kuznets
E-mail: nadija.dubrovina@vsemvs.sk, klymenkoviktoriia@gmail.com, evisotska@ukr.net,
guryanovalidiya@gmail.com, monikavero1979@gmail.com

The given work is devoted to the analysis of problem of safety and cybersecurity in health sector. The main problems of importance of safety and protection against cyberattacks are considered in healthcare. The need criteria for security platform are noted.

As many leading experts from USA and other countries noted that over the past decade, the cyberthreat to the healthcare industry has increased dramatically and cyberattacks in health sector have a negative impact on the security of medical information systems as well as can destroy health and safety of patients [1, 2]. The victims of cyberattacks are large, middle and small healthcare organizations, located worldwide, and involved in E-health or other information systems.

The main purposes of the article are to consider the importance of safety issues and application of cybersecurity technologies in healthcare. The main reasons of these illegal actions are: insurance fraud purposes and collection of payments for health services for patients to obtain financial means for scammers; collection of personal data of medical staff and patients for different scam operations; access to internal information about hospitals or medical center; preparation of fake health note, etc.

American expert of cybersecurity in healthcare Steven Bowcut listed the top cybersecurity challenges facing the healthcare industry.

They are:

1) Patient information is valuable on the darknet;
2) Medical devices often lack adequate security controls;
3) Medical professionals need the ability to access medical data remotely;
4) Insufficient cyber risk training among healthcare workers;
5) Outdated technology used in many healthcare facilities [2].

Unfortunately, only large medical centers create the cyber defense strategy. They have more opportunities in comparison with middle or small healthcare institutions. These large hospitals have security staff, security operations center, use the best technologies against cyber threat.

They use protection of their networks, databases, and endpoints from attack and are responsible for protecting private financial and medical information about their patients and employees. For example, connected devices include patient tracking wristbands, equipment tracking for crash carts, ventilators, portable X-ray machines, and vital-sign monitors are important sources for health care about patients. All of these devices communicate across the hospital network providing doctors with valuable patient information entered into electronic health records. The transmitted data allows doctors to provide more affordable care. Clinicians can work faster and in safer conditions. And each of those devices acts as an entry point for cybercriminals to exploit. This kind of information should be reliably protected against possible cyberattacks or scam operations. Thus, any security platform under consideration for introduction into the medical environment should be thoroughly evaluated against the following criteria: architecture; analytics and reporting; attack response; threat research; device visibility; vulnerability management; integrations; vision; roadmap [1, 2].

The mentioned problem is relatively new for health system in Ukraine, but nowadays it is necessary to take into account new challenges and create reliable tools and platform for E-health system in Ukraine.

Reference:

1. Luna R, Rhine E, Myhra M, Sullivan R, Kruse C. S. Cyber threats to health information systems: A systematic review. Technol Health Care. 2016;24(1):1-9. doi: 10.3233/THC-151102.

2. Cybersecurity in healthcare. – Access mode: https://cybersecurityguide.org/ industries/healthcare. - (Appeal date: 20.08.21).