Approaches to secure biomedical informatics systems and networks

Ion Bolun, Alexei Arina

Technical University of Moldova, ion.bolun@isa.utm.md, arina.alexei@tse.utm.md,
ORCID: 0000-0003-1961-7310, 0000-0003-4138-957X, https://utm.md/

Keywords: sensitive information; cyber-attack; impact; healthcare; medical devices

Abstract. A significant part of medical information, but especially that related to patient records, is very sensitive confidential information. A health care facility is at risk of becoming completely unable to activate as needed if data from patient i-records are altered or can no longer be accessed. Unfortunately, in 2023, according to [1], the healthcare sector bears the brunt of cybercrime activity, accounting for 14.2% off all attacks targeting critical infrastructure.

The cyber security peculiarities of biomedical informatics systems (HISs) and networks (HINs) are systematized. Based on these particularities and on some statistical data, the acuteness of HISs/HINs' security is estimated. Cyber security standards [2] in the field, briefly described in the paper, facilitate the orientation in the multitude of aspects and requirements of cyber security in various practical situations. Also, some specific solutions [3] for securing HISs/HINs are described. They can serve to define cyber security modalities in concrete cases. The requirements of cyber security and, respectively, the implementation of the respective informatics means in informatics applications, systems and biomedical networks to comply with them depend on each specific case.

References

[1] European Repository of Cyber Incidents, https://www.swp-berlin.org/en/swp/ about-us/organization/swp-projects/european-repository-on-cyber-incidents-eurepoc (accessed 07.07.2024).

[2] Official Journal of the European Union, L 117, Vol. 60, 5 May 2017. – 333 p.
Jet-Stream Cloud, https://jet-stream.com/jet-stream-cloud/ (accessed 14.07.2024).