

## INFORMATION SECURITY THREATS MODELING FOR MEDICAL INFORMATION SYSTEMS

Gorbunov N.A (ITMO University)

Scientific adviser – senior lecturer, Kuleshova V.O. (ITMO University)

**Introduction.** Threat modeling is necessary for medical institutions that use an information security system in accordance with the information security requirements for personal data information systems, government information systems and critical information infrastructure. Accordingly, medical institutions need to comply with the requirements of regulators when developing an information security threat model for medical information systems.

**Main part.** An information security threat model for medical information systems should be developed in accordance with:

- methodological document "Methodology for assessing threats to information security", approved by the FSTEC of Russia at 05.02.2021 [1]. This document is based on an expert approach and combines the definition of current threats with a risk-based approach. The methodology describes options for placing protected systems in cloud infrastructures, which is relevant when adapting to real medical information systems;
- information security threat databank recommendations [2]. This is an electronic database describing the conditions that could lead to unauthorized access and illegal activities relating to information processed by medical information systems;
- methodological recommendations for the development of regulatory legal acts that define threats to the security of personal data. These recommendations are relevant for the processing of personal data in personal data information systems, approved by the 8th Center of the FSB of Russia (№ 149/7/2/6-432 at 31.03.2015) [3]. It describes the necessity of using cryptographic information protection tools to ensure the security of information processed by medical information systems, including users' personal data.

**Conclusions.** Guided by the requirements presented in the regulatory and methodological documentation described above, the information security threat model for medical information systems will meet the requirements of regulatory authorities (FSTEC and FSB), and will also correspond to real information security threats.

### References:

1. Methodology for assessing threats to information security [Electronic resource] URL: <https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/2170-metodicheskij-dokument-utverzhdjen-fstek-rossii-5-fevralya-2021>.
2. Data bank of information security threats FSTEC [Electronic resource] URL: <https://bdu.fstec.ru/threat>.
3. Guidelines for the development of regulatory legal acts that define threats to the security of personal data that are relevant when processing personal data in personal data information systems operated in the course of the relevant activities, approved by the leadership of the 8th Center of the FSB of Russia (№ 149/7/2/6-432 at 31.03.2015) [Electronic resource] URL: [https://sps-ib.ru/\\_media/npa:fsb149-7-2-6-432\\_31.03.2015.pdf](https://sps-ib.ru/_media/npa:fsb149-7-2-6-432_31.03.2015.pdf).