УДК 004.056.5

Моделирование угроз информационной безопасности медицинских информационных систем

Горбунов Н.А (Университет ИТМО)
Научный руководитель – доцент, кандидат технических наук, Коржук В.М.
(Университет ИТМО)

Введение. Моделирование угроз является обязательным для медицинских учреждений, которые применяют систему защиты информации в соответствии с требованиями информационной безопасности, предъявляемым к информационным системам персональных данных, государственным информационным системам или субъектам критической информационной инфраструктуры. Таким образом, медицинским учреждениям необходимо соблюдать требования регуляторов при разработке модели угроз безопасности информации для медицинских информационных систем.

Основная часть. Модель угроз безопасности информации для медицинских информационных систем должна быть разработана в соответствии с:
- методическим документом «Методика оценки угроз безопасности информации», утвержденным ФСТЭК России 05.02.2021 [1]. Данный документ основывается на экспертном подходе и сочетает в себе определение актуальных угроз с риск ориентированным подходом. В методике описаны варианты размещения защищаемых систем в облачных инфраструктурах, что является актуальным при адаптации на реальные медицинские информационные системы;
- рекомендациями банка данных угроз безопасности информации [2]. Это электронная база данных с описанием условий, которые могли бы стать причиной несанкционированного доступа и осуществления неправомерных действий со сведениями, обрабатываемыми медицинскими информационными системами;
- методическими рекомендациями по разработке нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности, утвержденным руководством 8 Центра ФСБ России (№ 149/7/2/6-432 от 31.03.2015) [3]. Здесь представлен порядок необходимости применения средств криптографической защиты информации для обеспечения безопасности сведений, обрабатываемыми медицинскими информационными системами, в том числе персональных данных пользователей.

Выводы. Руководствуясь требованиями, представленными в описанными выше нормативно-методическим документацией, модель угроз безопасности информации для медицинских информационных систем будет удовлетворять требованиям регулирующих органов (ФСТЭК и ФСБ), а также будет соответствовать реальным угрозам информационной безопасности.

Список использованных источников:

1. Методика оценки угроз безопасности информации [Электронный ресурс] URL: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/2170-metodicheskij-dokument-utverzhden-fstek-rossii-5-fevralya-2021.
2. Банк данных угроз безопасности информации ФСТЭК РФ [Электронный ресурс] URL: https://bdu.fstec.ru/threat.
3. Методические рекомендациями по разработке нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности, утвержденным руководством 8

Центра ФСБ России (№ 149/7/2/6-432 от 31.03.2015) [Электронный ресурс] URL: https://sps-ib.ru/_media/npa:fsb149-7-2-6-432_31.03.2015.pdf