**УДК 004.056.5**

# Риск- ориентированный подход при выявлении уязвимостей информационной безопасности медицинских информационных систем

**Горбунов Н.А** (Университет ИТМО)

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

**Введение.** Выявление уязвимостей информационной безопасности медицинских информационных систем (далее -МИС) является обязательным для медицинских учреждений (далее -МУ), которые применяют систему защиты информации в соответствии с требованиями информационной безопасности, предъявляемым к субъектам критической информационной инфраструктуры. Таким образом, МУ необходимо применять риск-ориентированный подход при выявлении уязвимостей.

**Основная часть.**

Риск- ориентированный подход заключается в том, что необходимо выстроить систему, основанную на принятии решений в области безопасности, ориентированных на учет степени риска. Риск измеряет возможность воздействия опасности на технологический процесс и значимость последствий такого воздействия.

К основным преимуществам риск-ориентированного подхода относят:

активное применение метода риск-менеджмента, в ходе которого усилия направлены на снижение вероятности неблагоприятного результата и минимизацию его последствий, если он все-таки произойдет. МУ заранее выявляет опасности, которые могут возникнуть в ходе эксплуатации МИС, и принимает меры по ликвидации. Оно руководствуется желанием свести последствия сомнительных нарушение безопасности к нулю;

изучение уязвимых мест МИС, недочетов в мероприятиях. С этой целью могут проводиться специальные стресс-тесты, в ходе которых предприятие проверяет МУ на устойчивость возможным рискам и скорость реагирования на угрозу. Исследуется, насколько быстро и успешно учреждение противодействует угрозам информационной безопасности;

проведение конференций и совещаний с целью планирования деятельности организации. Это означает, что учреждение не только действует по ситуации, но и прогнозирует возможные варианты развития рисков и вырабатывает способы по их регулированию;

высшее руководство активно участвуют в контроле над безопасностью МУ, проверке отделов учреждения на их способность быстро противодействовать угрозам.

К возможным недостаткам риск-ориентированного подхода можно отнести несколько проблем, которые могут возникнуть во время его применения:

неправильный выбор при рассмотрении множества сомнительных операций. Когда от внимания службы безопасности могут ускользнуть самые рискованные процессы, а общие усилия будут брошены на менее опасные процессы. Данная ситуация особенно актуальна для больших учреждений, где находится большой объем МУ.

Риск-ориентированный подход основывается на следующих принципах:

действия контролирующего органа согласованы с действующим законодательством, решения по защите МУ объективны и применяются на основании руководящих документов;

регулярно проводятся переоценки риска, учитываются новые уязвимости, применяются инновационные методы противодействия атакам. Все это требует МУ своевременного, должного реагирования на атаки и уязвимости, которое невозможно без совершенствования деятельности;

основные усилия субъекта брошены на наиболее рискованные типы уязвимостей. В то же время уязвимостей, по которым степень угрозы минимальна, проверяются в последнюю очередь;

используемые критерии значимости, а также оценка доступны широкой общественности и прописаны в нормативно-правовых актах и других юридических источниках;

усилия МУ соответствуют угрозам — нет перегибов, когда на минимально рискованные МУ тратятся максимальные ресурсы субъекта, и наоборот.

Риск-ориентированный подход совмещает в себе следующие мероприятия, без проведения которых он несостоятелен:

превентивный контроль — преждевременное обнаружение рисков от уязвимостей. Профилактические меры очень важны, поскольку для МИС должна быть создана такая среда, которая минимизирует появление атак. Должна проводиться надлежащая работа с сотрудниками причастными к обработке информации в МИС;

оценивание организации деятельности МУ, насколько эффективно он противостоит возможным рискам и способен ли их заблаговременно обнаружить. Сюда же относится устойчивость субъекта, насколько учреждение подвержено рискам и способно ли минимизировать негативные последствия для его деятельности;

постоянное улучшение контроля над рискованными МИС, изучение новых методов эксплуатации уязвимостей. МИС должны быть готов к предотвращению и нейтрализации новых атак.

**Выводы.**

Руководствуясь риск-ориентированным подходом для МИС при выявлении уязвимостей информационной безопасности будет, модель угроз для МУ 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