УДК 004.056:615.47

А.П. ДУРАКОВСКИЙ, А.Л. ХЛОПОТНИКОВ

Национальный исследовательский ядерный университет «МИФИ», Москва

АНАЛИЗ УГРОЗ И ФАКТОРОВ, ВЛИЯЮЩИХ НА УСТОЙЧИВОСТЬ РОБОТИЗИРОВАННОЙ МЕДИЦИНСКОЙ СИСТЕМЫ

Работа посвящена анализу киберфизических угроз и разработке мер повышения устойчивости роботизированного медицинского комплекса (РМК) da Vinci Si. В ходе исследования решены три основные задачи: анализ архитектуры системы и идентификация угроз, оценка их критичности и разработка комплекса защитных мер. Выявлены неприемлемые риски, требующие немедленного устранения. Предложены технические и организационные меры противодействия угрозам.

Введение

Актуальность исследования обусловлена прямой зависимостью между кибербезопасностью и физической безопасностью пациента при использовании РМК. Критическим фактором риска признана зависимость от проприетарного программного обеспечения и сервисного канала OnSite, что ограничивает возможности независимого аудита безопасности [1]. В работе решены три основные задачи, направленные на комплексный анализ угроз и разработку мер защиты.

Основные проблемы и предлагаемые решения

Три основные задачи. Во-первых, проведен анализ архитектуры РМК da Vinci Si и идентифицированы ключевые угрозы и уязвимости, среди которых доминируют киберфизические риски, связанные с манипуляцией управляющими данными и нарушением доступности каналов связи и визуализации. Критическим фактором риска признана зависимость от проприетарного программного обеспечения и сервисного канала OnSite, что ограничивает возможности независимого аудита безопасности [1].

Во-вторых, выполнена оценка критичности угроз на основе методологии ГОСТ ISO 14971-2021 [2]. Разработаны шкалы для оценки тяжести последствий (S), ориентированной на ущерб здоровью пациента и нарушение основных функциональных характеристик системы, и вероятности реализации угроз (P). Построенная карта рисков показала, что угрозы манипуляции управляющими данными (R=15) и DoS-атаки на

канал визуализации (R=16) относятся к категории неприемлемых рисков, требующих немедленного устранения.

В-третьих, разработан комплекс рекомендаций по минимизации рисков [3]. К техническим мерам отнесены: внедрение аппаратного контроля целостности и доверенной загрузки для защиты от компрометации прошивки; строгая сегментация и изоляция сетевого контура РМК от общебольничной сети для противодействия сетевым атакам; криптографическая защита внутренних коммуникационных шин. К организационным мерам относятся: внедрение строгой политики аутентификации, регламента обновлений и непрерывного обучения персонала. Сформулированы предложения по совершенствованию нормативно-правовой базы, включая интеграцию требований ФСТЭК России и введение обязанности производителей раскрывать спецификации протоколов для независимого аудита [4].

Заключение

Практическая значимость работы заключается в том, что ее результаты могут быть использованы производителями РМК для устранения уязвимостей, медицинскими учреждениями для повышения безопасности эксплуатации и регуляторами при обновлении стандартов кибербезопасности. Реализация предложенных мер позволит существенно повысить устойчивость роботизированных медицинских систем к современным киберфизическим угрозам.

Список литературы

1. Singh, S., Vyas, A., & Bansal, S. (2021). Securing robotic surgical systems: A review of security vulnerabilities and countermeasures. Medical Devices & Sensors, 4(1), e10102. DOI:10.18280/ijsse.130318.

2. ГОСТ ISO 14971-2021. Изделия медицинские. Применение менеджмента риска к медицинским изделиям.

3. Орысюк, Д.А. Робототехника. Биомедицинские приложения робототехнических систем и их проблемы / Д.А. Орысюк, Т.В. Луинда // Молодые ученые - развитию Национальной технологической инициативы (ПОИСК). – 2022. – № 1. – С. 1047-1048. – EDN OXUBSP. (дата обращения: 20.10.2025).

4. Левоневский, Д.К. Модели сценариев функционирования медицинской киберфизической системы в штатных и экстренных ситуациях / Д. К. Левоневский, А. И. Мотиенко // Программная инженерия. – 2022. – Т. 13, № 8. – С. 383-393. – DOI 10.17587/prin.13.383-393. – EDN JQVKXB.