УДК 004.056

АНАЛИЗ СОВРЕМЕННОГО УРОВНЯ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ IOT УСТРОЙСТВ, ПРИМЕНЯЕМЫХ ПРИ ОСУЩЕСТВЛЕНИИ МЕДИЦИНСКОЙ ДЕЯТЕЛЬНОСТИ

Луценко М.С. (Университет ИТМО),
Научный руководитель – доцент Факультета БИТ, к.т.н. Коржук В.М.
(Университет ИТМО)

Введение. В современном обществе благодаря цифровизации претерпевают положительные изменения все сферы жизнедеятельности человека, в том числе и сфера оказания медицинских услуг [1]. В текущее время, существующие методы защиты цифровых систем медицинских организаций в целом позволяют решать задачи защиты сетевой инфраструктуры, однако, появление новых умных технологий Интернет вещей, совершенствование способов совершения атак на информационные системы со стороны злоумышленников требуют проведения непрерывной работы по актуализации способов и подходов к организации защиты умных цифровых сетей [2]. Анализ научных источников показал, что на данный момент не разрешены правовые отношения между требованиями к защите медицинских персональных данных и врачебной тайны, а также не регламентирован порядок оценки рисков для IoT устройств, применяемых в целях реализации телемедицинской деятельности. Все это обуславливает актуальность проводимого исследования.
Целью работы является выявление современного уровня безопасности IoT устройств посредством анализа уже существующих решений по защите данных для дальнейшего повышения эффективности при проведении оценки рисков информационной безопасности медицинских IoT устройств.

Основная часть. В данной работе решаются следующие задачи:

1. Анализ обобщенной архитектуры медицинских IoT устройств.
2. Изучение беспроводной структуры медицинских IoT устройств.
3. Формирование перечня основных современных проблем безопасности медицинских IoT устройств.
4. Выявление актуальных угроз в сфере применения медицинских IoT устройств.
5. Анализ методов оценки рисков информационной безопасности медицинских IoT устройств и беспроводной передачи данных.

В работе была выявлена степень научной проработанности темы обеспечения безопасности медицинских IoT устройств. Также после детального изучения главных компонентов архитектуры устройств Интернета Вещей была составлена сравнительная таблица основных стандартов беспроводной передачи данных, включающая в себя такие критерии как: виды сигналов, рабочие частоты, вид шифрования и др. Помимо этого на основании статистики распространенных киберинцидентов в сфере безопасности медицинских IoT устройств был сформирован перечень актуальных угроз безопасности из Банка Данных Угроз Безопасности ФСТЭК [3]. Также был проведен анализ актуальных на сегодняшний момент методов оценки рисков, применимых для оценки устройств Интернета Вещей.

Выводы. В результате исследования был определен современный уровень обеспечения информационной безопасности IoT устройств, применяемых в медицинской деятельности, составлена сравнительная таблица актуальных методов оценки рисков. Сравнительный анализ показал, что рассмотренные методы не учитывают особенности функционирования медицинских устройств, однако применение модели зрелости при проведении оценки рисков способно учесть данные особенности, а именно уровень необходимой безопасности в системе. В дальнейшем требуется создать собственную методику оценки рисков, которая будет соответствовать всем требованиям информационной безопасности, применяемым к медицинским IoT устройствам.

Список использованных источников:

1. A Survey of Healthcare Internet of Things (HIoT): A Clinical Perspective [Электронный ресурс]. – URL: https://ieeexplore.ieee.org/document/8863483
2. The cyber-risks of IoT in the medical field [Электронный ресурс]. – URL: https://blog.unguess.io/cybersecurity-medical-iot
3. Банк данных угроз безопасности информации [Электронный ресурс]. – URL: https://bdu.fstec.ru

Луценко М.С. (автор) Подпись

Коржук В.М. (научный руководитель) Подпись