УДК 004.056

РАЗРАБОТКА МЕТОДИКИ ПРОТИВОДЕЙСТВИЯ УГРОЗАМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ БИОНИЧЕСКИХ ПРОТЕЗОВ В РАМКАХ СИСТЕМЫ МЕДИЦИНСКОГО ИНТЕРНЕТА ВЕЩЕЙ

Крашенинникова М. Е. (Университет ИТМО), **Роговой В.** (Университет ИТМО)

Научный руководитель – доцент, кандидат технических наук Коржук В. М.

(Университет ИТМО)

Аннотация. В текущей работе рассматривается проблема недостаточного уровня защищенности бионических протезов как части системы Iot (Internet of Things). Упор сделан на сетевой уровень модели OSI как на наиболее уязвимый. При разработке методики учитываются ограничения накладываемые системой: ограниченность ресурсов при сохранении статуса объекта КИИ (критической информационной инфраструктуры). Результатом текущей работы является методика противодействия угрозам ИБ бионических протезов, включающая в себя разработку методов аутентификации, шифрования, детектирования вторжений.

Введение. Бионические протезы становятся все более распространенным средством восстановления функций утраченных органов и конечностей. Однако, с ростом количества протезов, подключаемых к медицинскому интернету вещей, а также учитывая тенденции рынка, желание компаний добавлять новые модули и возможности, усложнять систему, возрастает риск угроз информационной безопасности. В текущей работе рассматривается проблема защиты информационной безопасности бионических протезов в рамках системы медицинского интернета вещей.

Основная часть. В ходе исследования было выявлено, что большинство уязвимостей IoMT (Internet of Medical Things) находятся на сетевом уровне. Для решения проблемы информационной безопасности бионических протезов в системе медицинского интернета вещей предлагается использовать подходящие протоколы и методы шифрования и аутентификации для защиты передаваемых данных между протезом и девайсом пользователя. Также необходимо добавление в архитектуру бионического протеза систему детектирования вторжений. Методы, предлагаемые к внедрению в данной работе, удовлетворяют требованиям, выдвигаемым IoMT, например, оптимизированной работы системы (необходимо учитывать свободные ресурсы), не теряя в скорости функционирования. Разработанная методика призвана защитить протезы от потенциальных угроз

информационной безопасности, учитывая, что любое «умное устройство» в рамках медицинского интернета вещей относится к объектам КИИ, следовательно, нуждается в дополнительном внимании со стороны обеспечения ИБ. Таким образом, для защиты бионических протезов в системе медицинского интернета вещей необходимо использовать соответствующие протоколы и методы шифрования, аутентификации и мониторинга.

Выводы. Разработанная методика противодействия угрозам информационной безопасности бионических позволяет повысить уровень защищённости протезов в системе медицинского интернета вещей. Результаты исследования могут быть использованы для практической реализации и внедрения в медицинской практике. Более того, предложенные решения могут применяться для усовершенствования систем информационной безопасности в других областях, которые также используют медицинский интернет вещей.

Список использованных источников:

1. Thomasian N. M., Adashi E. Y. Cybersecurity in the internet of medical things //Health Policy and Technology. – 2021. – Т. 10. – №. 3. – С. 100549.
2. Lacava A. et al. Securing Bluetooth Low Energy networking: An overview of security procedures and threats //Computer Networks. – 2022. – С. 108953.
3. Lu Y., Da Xu L. Internet of Things (IoT) cybersecurity research: A review of current research topics //IEEE Internet of Things Journal. – 2018. – Т. 6. – №. 2. – С. 2103-2115.
4. Inscruction for use. — Текст : электронный // Ottobock : [сайт]. — URL: https://www.ottobock.com/en-us/product/8E70#technical-data (дата обращения: 18.02.2023).

Крашенинникова М. Е. (автор) Подпись

Роговой В. (автор) Подпись

Коржук В. М. (научный руководитель) Подпись