

РАЗРАБОТКА АЛГОРИТМА БЕЗОПАСНОГО ВЗАИМОДЕЙСТВИЯ ИНТЕРНЕТА ВЕЩЕЙ И ИНФОРМАЦИОННЫХ СИСТЕМ МЕДИЦИНСКИХ УЧРЕЖДЕНИЙ

Снетков И.С. (Университет ИТМО)

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

В данном исследовании рассматриваются проблемы безопасности устройств Интернета вещей в медицине. Существующие протоколы аутентификации не отвечают требованиям, которые выставляются перед Интернетом вещей в медицине. Предлагается алгоритм аутентификации Интернета вещей в беспроводных медицинских сенсорных сетях, а также оценивается его эффективность.

Введение. В сфере медицины вопрос обеспечения безопасности устройств Интернета вещей стоит наиболее остро. Данные устройства осуществляют мониторинг состояния пациентов, сбор и систематизацию данных в период лечения и восстановления. Однако Интернет вещей не обладает такими большими вычислительными мощностями, как персональные компьютеры, из-за чего возникают сложности в обмене ключами шифрования и конфиденциальной информацией. В данной работе рассмотрена проблематика этой темы, проанализированы существующие решения и их недостатки, а также выбрано наиболее эффективное из них с точки зрения противодействия атакам на устройства Интернета вещей в медицине.

Основная часть. В данной работе рассматривается взаимодействие устройств Интернета вещей в беспроводных медицинских сенсорных сетях. Данные сети представляют собой группу подключенных датчиков, узлов, которые занимаются мониторингом и обнаружением. Для подключения этих узлов к сети используются различные протоколы аутентификации, но не все из них решают проблемы, связанные с малой вычислительной мощностью устройств Интернета вещей.

В связи с этим были проанализированы существующие решения в этой области, выделены требования к протоколам, такие как секретность, целостность, анонимность и т.п., достоинства и недостатки предлагаемых протоколов аутентификации. Рассмотрены различные угрозы безопасности и атаки «человек посередине», DOS-атаки и т. д., применимые в данной сфере, и выделены наиболее эффективные решения по обеспечению безопасной передачи конфиденциальной информации между Интернетом вещей и медицинскими информационными системами при помощи методов формального анализа безопасности.

Выводы. В ходе проделанной работы были рассмотрены проблемы обеспечения безопасности Интернета вещей в медицине, а также представлено наиболее эффективное с точки зрения противодействия угрозам информационной безопасности решение. Полученные результаты позволяют улучшить существующие протоколы аутентификации в сфере данных устройств, и таким образом обеспечить защищенность передаваемой конфиденциальной информации в беспроводных медицинских сенсорных сетях.

Список использованных источников:

1. Anwar Nouredine Bahache, Nouredine Chikouche, Fares Mezrag. Authentication Schemes for Healthcare Applications Using Wireless Medical Sensor Networks: A Survey. SN Computer Science (2022) 3: 382.

2. B. D. Deebak, Fadi Al-Turjman (2021) Secure-user sign-in authentication for IoT-based eHealth systems. *Complex & Intelligent Systems*.
3. Vu Khanh Quy, Nguyen Van Hau, Dang Van Anh, Le Anh Ngoc. Smart healthcare IoT applications based on fog computing: architecture, applications and challenges. *Complex & Intelligent Systems* (2022) 8:3805–3815.
4. Khaled H. Almotairi (2022) Application of internet of things in healthcare domain. *J. Umm Al-Qura Univ. Eng.Archit.*

Снетков И.С. (автор)

Подпись

Коржук В.М. (научный руководитель)

Подпись