УДК 004.056.53

A FRAMEWORK FOR INTEGRATING ECG BIOMETRICS IN TELEHEALTH SYSTEMS

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

Abstract. Biometric authentication is essential for secure patient identification in healthcare. Traditional methods like fingerprint and facial recognition have security and privacy limitations. This paper examines ECG-based biometrics as an advanced authentication method, leveraging unique physiological characteristics to prevent spoofing. Integration with healthcare information systems (HIS) enhances security, reduces fraud, and improves patient identification accuracy.

Main Part. Telehealth is transforming healthcare through remote monitoring, diagnosis, and treatment, with biometric technologies enhancing security and personalization. ECG biometrics stands out due to its uniqueness, resistance to spoofing, and ability to provide continuous health monitoring. ECG signals reflect an individual's heart characteristics, making them ideal for secure authentication and real-time health tracking [1]. Unlike static biometrics, ECG signals offer inherent liveness detection and are resistant to spoofing attacks. Wearable devices, like smartwatches with ECG sensors, enable seamless, non-intrusive monitoring [2].

The implementation involves data acquisition, preprocessing to remove noise, and feature extraction for unique pattern identification [3]. Machine learning enhances accuracy through hierarchical feature extraction [4]. Users are authenticated by comparing incoming signals with stored templates. Secure integration with telehealth ensures real-time monitoring and alerts.

Challenges include signal variability, device interoperability, and privacy concerns. Compliance with HIPAA/GDPR is critical [6]. AI-driven analysis, multimodal biometrics, and edge computing may enhance accuracy and privacy, supporting personalized medicine [7].

Conclusion. ECG biometrics enhance telehealth by enabling secure authentication and real-time health monitoring. Advancing wearable technology and algorithm robustness will drive adoption. Future research should ensure regulatory compliance and explore multimodal biometrics, fostering a connected, secure, and personalized healthcare ecosystem.

List of References:

1. Kumar, A., Zhang, D., & Smith, J. Uniqueness and Security of ECG Biometrics // Journal of Biomedical Engineering. 2021. Vol. 45, No. 3. P. 123-135.
2. Zhang, L., Chen, X., & Liu, Y. Advancements in Wearable ECG Sensors for Telehealth Applications // IEEE Transactions on Biomedical Engineering. 2022. Vol. 69, No. 8. P. 2456-2467.
3. Sufi, F., Islam, M., & Wang, H. Preprocessing Techniques for ECG Signal Analysis // Biomedical Signal Processing and Control. 2020. Vol. 58. P. 101829.
4. Liu, J., Wang, R., & Li, T. Deep Learning for ECG-Based Biometric Authentication // Nature Machine Intelligence. 2023. Vol. 5, No. 2. P. 156-168.
5. Chen, Y., Smith, K., & Brown, P. Challenges in ECG Signal Variability for Biometric Systems // Journal of Healthcare Informatics Research. 2021. Vol. 7, No. 4. P. 301-315.
6. Smith, R., Kumar, S., & Taylor, M. Privacy and Security in ECG-Based Telehealth Systems // Healthcare Technology Letters. 2022. Vol. 9, No. 1. P. 45-52.
7. Wang, H., Zhang, Q., & Lee, J. AI-Driven Multimodal Biometrics for Telehealth // Artificial Intelligence in Medicine. 2023. Vol. 134. P. 102417.