

Введение

В сфере защиты информации задачи достоверного распознавания и подтверждения подлинности пользователей сохраняют свою значимость. Несмотря на повсеместное внедрение биометрических технологий (например, дактилоскопической или иридологической верификации), фундаментальным ограничением остается подверженность описываемых подходов для копирования биометрических образцов [1]. В качестве альтернативы предлагаются методы, основанные на динамически изменяющихся психофизиологических параметрах, которые характеризуются низкой латентностью и сложностью принудительной генерации, что повышает устойчивость к ситуациям подмены/имитации.

Основная часть

Исследовательская гипотеза базируется на выдвинутой концепции синергизма характеристик, полученных от центральной (электроэнцефалограмма) и периферической (фотоплетизмограмма) нервной системы человека. Предполагается, что комплексный биометрический дескриптор, сформированный на основе этих показателей, будет обладать повышенной робастностью за счет гибридного подхода при сохранении устойчивости к изменяющимся внешним условиям. На начальном этапе исследования были задействованы методы электроэнцефалографии (ЭЭГ) и электрокардиографии (ЭКГ) ввиду высокой информативности и защищенности данных сигналов. Однако тестирование выявило недостаточную эргономичность подобной схемы: для одновременной регистрации показателей требовалась фиксация минимум шести электродов, что вызывало выраженный дискомфорт при длительном ношении. В качестве решения, обеспечивающего практическую применимость, было предложено использовать нейроинтерфейсный модуль, позволяющий регистрировать сигналы как ЭЭГ, так и ФПГ без существенного ухудшения пользовательского восприятия [2].

Выводы

Целью работы является создание аппаратно-программного комплекса для выявления индивидуальных паттернов на основании анализа сигналов ЭЭГ и ФПГ. Предлагается использовать данное решение в компаниях государственного и корпоративного сектора в качестве нового вида биометрической аутентификации. Дальнейшее развитие проекта состоит в разработке системы непрерывной биометрической аутентификации, которая позволит в режиме реального времени постоянно подтверждать личность испытуемых [3].

Литература

1. Емельянов, А. А. Технические риски предприятия, связанные с цифровой трансформацией / А. А. Емельянов, И. Л. Коршунов // Известия высших учебных заведений. Приборостроение. – 2024. – Т. 67, № 2. – С. 116-121
2. Siam, A. I. Enhanced user verification in IoT applications: a fusion-based multimodal cancelable biometric system with ECG and PPG signals / A. I. Siam, A. A. G. Abualkishik, A. Almazroi [и др.] // The Journal of Supercomputing. – 2024. – Vol. 80, № 5. – P. 6200-6230.
3. Ayeswarya, S. A Comprehensive Review on Secure Biometric-Based Continuous Authentication and User Profiling / S. Ayeswarya, K. John Singh // IEEE Access. – 2024. – Vol. 12. – P. 82996-83021.