УДК 004.056.5:621.398 URL: https://ptsj.bmstu.ru/catalog/icec/insec/1106.html

БИОМЕТРИЧЕСКИЕ СИСТЕМЫ АУТЕНТИФИКАЦИИ НА ОСНОВЕ ЭЛЕКТРОКАРДИОГРАММЫ: АНАЛИЗ УЯЗВИМОСТЕЙ И МЕТОДЫ ПОВЫШЕНИЯ НАДЕЖНОСТИ

Г.Б. Чибанов chibanovgb@student.bmstu.ru
Е.В. Глинская glinskaya@bmstu.ru
SPIN-код: 5430-3023

МГТУ им. Н.Э. Баумана, Москва, Российская Федерация

Рассмотрено современное направление развития биометрических технологий — системы аутентификации на основе электрокардиограммы (ЭКГ). Данный метод привлекает внимание исследователей благодаря уникальности электрической активности сердца каждого человека и относительной устойчивости этой характеристики к подделке по сравнению с традиционными биометрическими параметрами (отпечатки пальцев, радужная оболочка, голос). Вместе с тем практическое применение ЭКГ-аутентификации сопряжено с рядом уязвимостей. В статье рассмотрены основные угрозы безопасности, включая возможность искусственного воспроизведения сигналов, влияние шумов и артефактов при съеме данных, снижение точности при изменении физиологического состояния пользователя, а также риски компрометации биометрических шаблонов при хранении и передаче. Проанализированы современные методы повышения надежности систем ЭКГ-аутентификации. К ним относятся: применение алгоритмов адаптивной фильтрации и многоканальной обработки сигналов, использование методов машинного обучения для выделения устойчивых признаков, криптографическая защита биометрических шаблонов, а также интеграция с дополнительными факторами аутентификации. Отдельное внимание уделено концепции многоуровневой защиты, где ЭКГ используется как один из элементов комплексной биометрической системы, обеспечивающей баланс между удобством использования и уровнем безопасности. Сделан вывод, что перспективность ЭКГ-аутентификации напрямую зависит от развития методов защиты от атак воспроизведения, повышения помехоустойчивости при регистрации сигналов, а также от внедрения современных криптографических протоколов для защиты биометрических данных. Таким образом, комбинирование физиологических характеристик с поведенческими и традиционными факторами аутентификации представляет собой наиболее эффективный подход к созданию надежных и практичных систем идентификации пользователей.

Ключевые слова: биометрия, аутентификация, электрокардиограмма, криптографическая защита, атаки воспроизведения, помехоустойчивость, машинное обучение, мультифакторная аутентификация

Введение. В условиях стремительного развития информационных технологий и роста количества киберугроз проблема надежной аутентификации пользователей выходит на первый план. Традиционные методы, основанные на паролях и токенах, демонстрируют низкую устойчивость к современным

 ISSN 2541-8009

атакам, включая фишинг, подбор паролей и компрометацию учетных данных. В этой связи все более широкое распространение получают биометрические системы, использующие уникальные физиологические или поведенческие характеристики человека для подтверждения личности.

Одним из наиболее перспективных направлений в области биометрии является аутентификация на основе электрокардиограммы (ЭКГ). Электрическая активность сердца формирует уникальный для каждого человека сигнал, который сложно подделать или воспроизвести в естественных условиях [1].

Преимущества и недостатки систем аутентификации на основе ЭКГ. Использование электрокардиограммы в качестве биометрического признака обладает рядом существенных преимуществ по сравнению с традиционными методами аутентификации.

1. *Уникальность сигнала*. Электрическая активность сердца формируется на основе анатомических и физиологических особенностей организма. Даже у однояйцевых близнецов ЭКГ имеет различия, что делает данный параметр индивидуальным и высоконадежным идентификатором личности [2].

2. Высокая скрытность и защита от несанкционированного копирования. В отличие от отпечатков пальцев или изображения лица, ЭКГ невозможно незаметно считать у пользователя. Это значительно усложняет задачу злоумышленникам и снижает риск утечки биометрических данных [3].

3. Устойчивость к подделке. Большинство традиционных биометрических признаков можно воспроизвести с помощью фотографий, 3D-моделей или аудиозаписей [4]. Для подделки ЭКГ необходимы специализированные медицинские устройства и точные данные, что делает подобные атаки гораздо менее вероятными [5].

4. Непрерывность и возможность динамической аутентификации. ЭКГ можно регистрировать в реальном времени в течение всего периода использования системы. Это открывает возможность непрерывной (постоянной) аутентификации, когда личность пользователя подтверждается не только при входе в систему, но и на протяжении всей сессии работы. Такой подход повышает уровень защиты от сценариев, связанных с захватом уже активной сессии [6].

5. Сочетание анатомических и функциональных характеристик. В отличие от статичных признаков (отпечатков пальцев, радужной оболочки), ЭКГ отражает и функциональные процессы организма. Это делает идентификатор более сложным и менее подверженным простой имитации.

Несмотря на указанные преимущества, практическая реализация систем ЭКГ-аутентификации сталкивается с рядом проблем. Наиболее существенными являются низкая помехоустойчивость сигнала, зависимость качества

распознавания от физиологического состояния пользователя (стресс, усталость, физическая нагрузка), а также возможность реализации атак воспроизведения с использованием заранее записанных биосигналов. Дополнительные риски связаны с безопасностью хранения и передачи биометрических шаблонов, так как их компрометация может привести к необратимой утечке данных, в отличие от паролей, которые можно изменить.

Технология регистрации и обработка ЭКГ-сигнала. Регистрация электрокардиограммы осуществляется с помощью контактных или бесконтактных датчиков. Наиболее распространены контактные электроды, устанавливаемые на кожу пользователя. В современных системах активно используются упрощенные схемы съема с минимальным количеством каналов (1–3), что позволяет интегрировать технологию в портативные устройства — смарт-часы, фитнес-браслеты, смартфоны. Также ведутся исследования по применению емкостных и оптических датчиков, позволяющих регистрировать ЭКГ без прямого контакта с кожей, что повышает удобство и снижает вероятность отказов при идентификации [7].

Предобработка сигналов. Полученный сигнал ЭКГ подвержен влиянию шумов и артефактов, вызванных движением пользователя, помехами электросети и нестабильным контактом электродов. Для повышения точности аутентификации применяют алгоритмы цифровой фильтрации:

– фильтры нижних и верхних частот для подавления шумов;

– адаптивные фильтры для устранения артефактов движения;

– нормализация сигнала для учета индивидуальных особенностей амплитуды и частоты сердечного ритма [8].

Выделение признаков. Для формирования биометрического шаблона необходимо выделить устойчивые характеристики сигнала [9]. Наиболее часто применяют:

– морфологические признаки (длительность интервалов PQ, QRS, QT, амплитуда зубцов);

– динамические признаки, отражающие временные изменения сердечного ритма;

– спектральные признаки, полученные с помощью преобразования Фурье или вейвлет-анализа;

– признаки, формируемые нейросетевыми моделями, обученными на больших выборках данных.

Комбинация различных типов признаков повышает устойчивость системы к шумам и физиологическим колебаниям.

Формирование биометрического шаблона. После выделения признаков создается биометрический шаблон — уникальный цифровой профиль поль-

 ISSN 2541-8009

зователя. Для повышения безопасности применяются криптографические методы: шифрование шаблонов, использование хэш-функций и схемы fuzzy commitment, позволяющие аутентифицировать пользователя без хранения исходного биометрического сигнала [10].

Заключение. Биометрические системы аутентификации на основе электрокардиограммы (ЭКГ) представляют собой перспективное направление развития технологий информационной безопасности. Уникальные характеристики сердечного сигнала обеспечивают высокую степень индивидуальности, скрытность и устойчивость к подделке по сравнению с традиционными биометрическими признаками. Дополнительным преимуществом является возможность реализации непрерывной аутентификации, что значительно повышает защищенность от захвата активной сессии.

Вместе с тем практическое применение ЭКГ-аутентификации связано с рядом ограничений и уязвимостей. Ключевыми проблемами являются чувствительность сигнала к шумам и физиологическим изменениям организма, возможность атак воспроизведения с применением предварительно записанных биосигналов, а также риски, связанные с хранением и передачей биометрических шаблонов. Эти факторы требуют разработки дополнительных мер защиты и совершенствования алгоритмов обработки данных.

Литература

[1] Jain A.K., Ross A., Nandakumar K. *Introduction to Biometrics*. Springer, 2011.

[2] Labati R.D., Muñoz E., Piuri V., Sassi R., Scotti F. *Heartprint: ECG biometric recognition*. *Biometric Recognition*. Springer, 2017, pp. 331–343.

[3] Хусаинов Ф.Ф., Гилязов Т.Ф. Методы биометрической идентификации личности на основе сигналов электрокардиограммы. *Известия Казанского государственного технического университета им. А.Н. Туполева*, 2019, т. 23, № 2, с. 45–53.

[4] Сивцов С.А., Соловьев А.Н. Биометрическая аутентификация на основе электрокардиографических сигналов. *Научно-технический вестник информационных технологий, механики и оптики*, 2020, т. 20, № 3, с. 423–431.

[5] Agrafioti F., Hatzinakos D., Anderson A.K. ECG pattern analysis for emotion detection. *IEEE Transactions on Affective Computing*, 2012, vol. 3 (1), pp. 102–115.

[6] Odinaka I., Lai P.-H., Kaplan A. D., O’Sullivan J.A., Sirevaag E.J., Rohrbaugh J.W. ECG biometrics: A robust short-time frequency analysis. *IEEE Transactions on Information Forensics and Security*, 2012, vol. 7 (6), pp. 1687–1698.

[7] Plataniotis K.N., Hatzinakos D. ECG biometric recognition in identity management. *IEEE Signal Processing Magazine*, 2015, vol. 32 (6), pp. 95–102.

[8] Biel L., Pettersson O., Philipson L., Wide P. ECG analysis: A new approach in human identification. *IEEE Transactions on Instrumentation and Measurement*, 2001, vol. 50 (3), pp. 808–812.

[9] Martinez J.P., Almeida R., Olmos S., Rocha A.P., Laguna P. A wavelet-based ECG delineator: Evaluation on standard databases. *IEEE Transactions on Biomedical Engineering*, 2004, vol. 51 (4), pp. 570–581.

[10] ISO/IEC 30107-1:2023. *Information technology — Biometric presentation attack detection. Part 1: Framework.* URL: https://www.iso.org/obp/ui/en/#iso:std:iso-iec:30107:-1:ed-2:v1:en (accessed October 15, 2025).

Поступила в редакцию 21.11.2025

Чибанов Георгий Борисович — студент кафедры «Информационная безопасность», МГТУ им. Н.Э. Баумана, Москва, Российская Федерация.

Глинская Елена Вячеславовна — старший преподаватель кафедры «Информационная безопасность», МГТУ им. Н.Э. Баумана, Москва, Российская Федерация.

Научный руководитель — Басараб Михаил Алексеевич, доктор физико-матема тических наук, заведующий кафедрой «Информационная безопасность», МГТУ им. Н.Э. Баумана, Москва, Российская Федерация.

Ссылку на эту статью просим оформлять следующим образом:
Чибанов Г.Б., Глинская Е.В. Биометрические системы аутентификации на основе электрокардиограммы (ЭКГ): анализ уязвимостей и методы повышения надежности. *Политехнический молодежный журнал*, 2026, № 03 (104). URL: https://ptsj.bmstu.ru/catalog/icec/insec/1106.html

 ISSN 2541-8009

ELECTROCARDIOGRAM (ECG)-BASED BIOMETRIC AUTHENTICATION SYSTEMS: VULNERABILITY ANALYSIS AND SECURITY ENHANCEMENT METHODS

G.B. Chibanov chibanovgb@student.bmstu.ru
E.V. Glinskaya glinskaya@bmstu.ru
SPIN-code: 5430-3023

Bauman Moscow State Technical University, Moscow, Russian Federation

This article examines a current trend in biometric technology development: electrocardiogram (ECG)-based authentication systems. This method has attracted the attention of researchers due to the unique electrical activity of each person's heart and the relative resistance of this characteristic to counterfeiting compared to traditional biometric parameters (fingerprints, iris, voice). However, the practical application of ECG authentication is associated with a number of vulnerabilities. Key security threats are discussed, including the possibility of artificial signal reproduction, the influence of noise and artifacts during data collection, decreased accuracy due to changes in the user's physiological state, and the risks of compromising biometric templates during storage and transmission. Modern methods for improving the reliability of ECG authentication systems are analyzed. These include the use of adaptive filtering algorithms and multichannel signal processing, the use of machine learning methods to extract stable features, cryptographic protection of biometric templates, and integration with additional authentication factors. Special attention is given to the concept of multi-layered security, where ECG is used as one element in a comprehensive biometric system that balances ease of use and security. Based on the analysis, it is concluded that the future of ECG authentication directly depends on the development of methods for protecting against replay attacks, improving noise immunity during signal recording, and implementing modern cryptographic protocols for protecting biometric data. Combining physiological characteristics with behavioral and traditional authentication factors is considered the most effective approach to creating reliable and practical user identification systems.

Keywords: biometrics, authentication, electrocardiogram, cryptographic protection, replay attacks, noise immunity, machine learning, multifactor authentication

Received 21.11.2025

Chibanov G.B. — Student of Department of Information Security, Bauman Moscow State Technical University, Moscow, Russian Federation.

Glinskaya E.V. — Senior Lecturer at the Department of Information Security, Bauman Moscow State Technical University, Moscow, Russian Federation.

Scientific advisor — Basarab M.A., Dr. of Phys. and Math. Sci., Head of Department of Information Security, Bauman Moscow State Technical University, Moscow, Russian Federation.

Please cite this article in English as:
Chibanov G.B., Glinskaya E.V. Electrocardiogram (ECG)-based biometric authentication systems: vulnerability analysis and security enhancement methods. *Politekhnicheskiy molodezhnyy zhurnal*, 2026, no. 03 (104). (In Russ.). URL: https://ptsj.bmstu.ru/catalog/icec/insec/1106.html

 ISSN 2541-8009