DOI 10.37882/2223-2966.2026.03.01

ОБЛЕГЧЁННАЯ САМОКОНТРОЛИРУЕМАЯ ЭКГ-АУТЕНТИФИКАЦИЯ ДЛЯ IOT-ДАТЧИКОВ С ОГРАНИЧЕННЫМИ ВЫЧИСЛИТЕЛЬНЫМИ РЕСУРСАМИ

LIGHTWEIGHT SELF-SUPERVISED ECG AUTHENTICATION FOR RESOURCE-CONSTRAINED IOT EDGE SENSORS

M. Azab
A. Sila
V. Korzhuk

Summary. This paper proposes a lightweight ECG biometric authentication framework for wearable IoT devices using CNN-based feature extraction and self-supervised contrastive learning. The approach enables effective training using unlabeled ECG signals and improves cross-dataset generalization. The model achieved 99.15% accuracy on the PTB dataset and maintained over 98.5% accuracy on MIT-BIH and ECG-ID datasets without retraining. Model optimization through pruning and quantization reduced computational requirements with minimal performance loss, achieving 98.67% accuracy. The findings demonstrate the feasibility of deploying robust ECG authentication on resource-limited IoT edge platforms.

Keywords: electrocardiogram authentication, contrastive learning, IoT devices.

Азаб Мохамед Абдалла Эльсайед
Аспирант, Университет ИТМО, Санкт-Петербург
mohamed.a.azab@itmo.ru
Сила Анастасия Станиславовна
Университет ИТМО, Санкт-Петербург
cstfokina@gmail.com
Коржук Виктория Михайловна
Доцент, Университет ИТМО, Санкт-Петербург
vmkorzhuk@itmo.ru

Аннотация. В статье представлен облегчённый метод биометрической аутентификации пользователей по ЭКГ для носимых IoT-устройств. Подход основан на извлечении признаков с использованием сверточных нейронных сетей и самоконтролируемого контрастивного обучения, что позволяет использовать большие объёмы неразмеченных данных и повышает устойчивость модели. На базе PTB достигнута точность 99,15 %, а при тестировании на базах MIT-BIH и ECG-ID точность превысила 98,5 % без дополнительного обучения. Применение методов квантования и прореживания уменьшило вычислительную нагрузку при сохранении точности 98,67 %. Полученные результаты подтверждают возможность внедрения предложенного метода в IoT-датчики с ограниченными вычислительными ресурсами.

Ключевые слова: аутентификация по электрокардиосигналу, контрастивное обучение, устройства интернета вещей.

Введение

Биометрическая аутентификация широко применяется в киберфизических системах благодаря высокой надёжности и удобству использования. Традиционные биометрические признаки, включая отпечатки пальцев, распознавание лица, радужной оболочки глаза и голоса, используются для подтверждения личности пользователя при входе в систему [1]. Однако большинство систем применяют одноразовую аутентификацию, что может привести к несанкционированному доступу во время бездействия пользователя. Методы непрерывной аутентификации позволяют повысить уровень безопасности за счёт постоянной проверки личности пользователя [2]. По сравнению с паролями биометрические методы обеспечивают более высокий уровень защиты и удобства.

Носимые устройства Интернета вещей (IoT) позволяют пассивно и непрерывно собирать физиологические сигналы, что делает их перспективными для реализации непрерывной аутентификации [3, 4]. Среди физиологических биометрических признаков электрокардиосигнал (ЭКГ) обладает высокой индивидуальностью, универсальностью и устойчивостью к подделке [5]. Кроме того, ЭКГ-данные широко доступны для научных исследований [6]. Методы глубокого обучения, особенно сверточные нейронные сети (CNN), эффективно извлекают информативные признаки из ЭКГ-сигналов для задач аутентификации [7]. Однако большинство существующих систем аутентификации по ЭКГ используют ограниченные наборы данных и тестируются на тех же данных, что снижает их обобщающую способность [8–9]. Дополнительные сложности связаны с масштабируемостью, изменчивостью ЭКГ-сигналов, высокими требованиями к точности и ограниченными вычислительными ресурсами носимых устройств [14].

В данной работе предложен облегчённый метод аутентификации по ЭКГ для IoT-устройств, основанный на самоконтролируемом контрастивном обучении и использовании CNN-энкодера для автоматического извлечения признаков. Для повышения эффективности внедрения применяются методы оптимизации модели, включая квантование и прореживание, что позволяет обеспечить высокую точность аутентификации при ограниченных вычислительных ресурсах.

Литературный обзор

В данном разделе рассматриваются современные методы биометрической аутентификации по ЭКГ и подходы к извлечению признаков на основе сверточных нейронных сетей. Методы аутентификации по ЭКГ обычно подразделяются на фидуциальные, нефидуциальные и гибридные в зависимости от используемых признаков [10]. Фидуциальные методы используют характерные точки сигнала ЭКГ (волны P, Q, R, S и T) для извлечения временных и амплитудных признаков. Например, Tantawi и соавт. применили вейвлет-разложение интервалов RR и достигли точности 97,7 % на базе PTB, однако метод требовал ручного выбора признаков и не позволял выявлять неизвестных пользователей [8]. Аналогично, Yang и соавт. реализовали систему аутентификации на основе фидуциальных признаков на платформе Raspberry Pi, но получили сравнительно высокий уровень ошибок — 8,67 % [11]. Нефидуциальные методы извлекают признаки ЭКГ без определения характерных точек сигнала и обычно используют методы цифровой обработки сигналов. Hejazi и соавт. применили дискретное вейвлет-преобразование и классификатор SVM, достигнув точности 94,54 % на небольшом наборе данных, однако метод требовал сложной предварительной обработки [12]. Agrafioti и соавт. использовали автокорреляцию и линейный дискриминантный анализ совместно с методом ближайших соседей, достигнув точности 92,3 %, но столкнулись с ограничениями производительности и масштабируемости [13]. Huang и соавт. разработали IoT-систему сбора данных с точностью F1 около 97 %, однако отсутствие встроенного механизма инференса ограничивает практическое применение.

Методы на основе CNN значительно повысили эффективность аутентификации по ЭКГ за счёт автоматического извлечения информативных признаков. Hammad и соавт. использовали CNN совместно с классификатором QG-MSVM и достигли точности 98,66 % [11]. Ghazarian и соавт. обучили CNN на крупном наборе данных ЭКГ, продемонстрировав высокую точность идентификации, но выявили потенциальные риски конфиденциальности [14]. Метод Deep-ECG обеспечил точность 100 % на небольших наборах данных [13]. Однако большинство существующих систем демонстрируют слабую обобщающую способность и высокую вычислительную сложность, что ограничивает их применение в носимых устройствах [8–13].

Контрастивное обучение является перспективным методом самоконтролируемого обучения, позволяющим уменьшить зависимость от размеченных данных и повысить устойчивость моделей [9]. Архитектуры MoCo и SimCLR показали высокую эффективность при обучении признаковых представлений путём сравнения схожих и различающихся выборок [12]. Современные исследования успешно применяют контрастивное обучение для анализа ЭКГ и повышения качества классификации [13]. Несмотря на это, многие существующие системы остаются ограниченными по масштабируемости и вычислительной эффективности [14]. С учётом указанных ограничений в данной работе предложен облегчённый метод аутентификации по ЭКГ на основе CNN и контрастивного обучения, направленный на повышение обобщающей способности и снижение вычислительной сложности для внедрения в IoT-устройства.

Материалы и методы

В данном разделе представлен метод биометрической аутентификации по ЭКГ на основе сверточной нейронной сети, включающий два основных этапа: обучение и аутентификацию. На этапе обучения неразмеченные ЭКГ-сигналы проходят предварительную обработку и подаются в модель контрастивного обучения, которая формирует признаковые векторы с использованием CNN-энкодера. Параметры энкодера обновляются посредством оптимизации функции потерь. Этап аутентификации включает предварительную обработку данных, извлечение признаков, вычисление сходства и принятие решения. При регистрации пользователей формируются уникальные признаковые векторы, которые сохраняются в базе данных. При попытке входа формируется новый вектор признаков, который сравнивается с сохранёнными векторами с использованием коэффициента корреляции Пирсона. Общая схема обучения и аутентификации представлена на Рис. 1 и Рис. 2.

Предварительная обработка данных направлена на удаление шумов и сегментацию ЭКГ-сигналов. Сигналы, полученные с носимых датчиков, могут содержать дрейф базовой линии, мышечные шумы и сетевые помехи, которые устраняются с помощью полосового фильтра. После фильтрации выполняется сегментация сигналов. В работе рассматриваются три метода сегментации: сегментация между R-пиками, сегментация между P— и T-пиками и сегментация без определения пиков. Метод R2R использует обнаружение R-пиков, но может приводить к ошибкам при неточном определении пиков. Метод P2T обеспечивает выделение полного сердечного цикла, однако увеличивает вычислительную сложность. Метод NPD использует фиксированные временные окна без обнаружения пиков, что снижает вычислительную сложность и сохраняет непрерывность сигнала. Примеры сегментации представлены на Рисунке 3.

Извлечение признаков выполняется с использованием одномерной сверточной нейронной сети, предназначенной для анализа временных характеристик ЭКГ-сигналов. Архитектура сети включает несколько сверточных слоёв с функцией активации ReLU и слои подвыборки, за которыми следует полносвязный слой

Рис. 1. Обучение на основе контрастивного подхода

Рис. 2. Блок-схема процессов регистрации и аутентификации пользователя

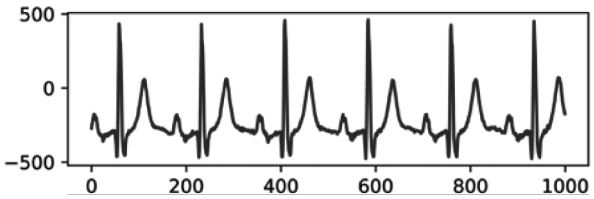

Рис. 3. Сегментация сигнала

для формирования высокоразмерных признаковых векторов. Архитектура энкодера представлена на Рисунке 4. Полученные векторы признаков представляют уникальные биометрические характеристики пользователей и сохраняются при регистрации.

Аутентификация выполняется путём сравнения вектора признаков входного ЭКГ-сигнала с сохранёнными в базе данных. Для оценки сходства используется коэффициент корреляции Пирсона, который позволяет эффективно сравнивать временные сигналы и не зависит от масштаба данных. Если значение коэффициента превышает заданный порог, пользователь считается успешно аутентифицированным.

Для повышения масштабируемости системы и уменьшения зависимости от размеченных данных используется контрастивное обучение. В работе применяются две архитектуры: сиамская модель и триплетная модель. Сиамская модель сравнивает пары сегментов ЭКГ и обучает модель уменьшать расстояние между похожими сигналами и увеличивать расстояние между различными сигналами. Триплетная модель расширяет этот подход, используя якорный, положительный и отрицательный образцы для повышения различимости признаков. Процесс обучения триплетной модели представлен на Рисунке 5. Использование данных архитектур позволяет повысить обобщающую способность модели и обеспечить эффективное внедрение системы в IoT-устройства.

Результаты

В работе использованы три общедоступные базы данных ЭКГ. База PTB Diagnostic ECG Database (PTBDB) [12] применялась для обучения и основной оценки модели. Она содержит 549 записей ЭКГ от 290 испытуемых, записанных с использованием 12 отведений с частотой дискретизации 1000 Гц. Из этой базы формировались признаковые векторы зарегистрированных пользователей. Для проверки обобщающей способности модели использовались две ранее неизвестные базе обучения базы данных. MIT-BIH Arrhythmia Database (MITDB) [13] содержит 48 записей ЭКГ от 47 испытуемых с частотой дискретизации 360 Гц. ECG-ID Database (ECGIDDB) [14] включает 310 записей от 90 испытуемых с частотой дискретизации 500 Гц. Использование различных баз дан-

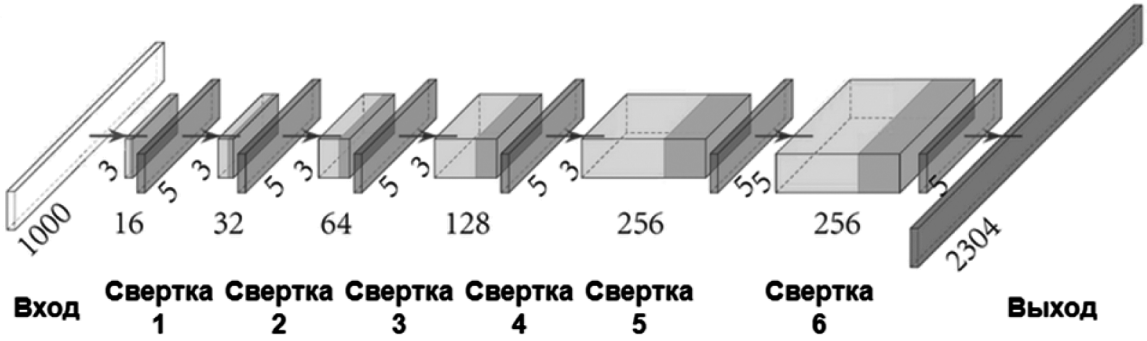

Рис. 4. Сегментация сигнала

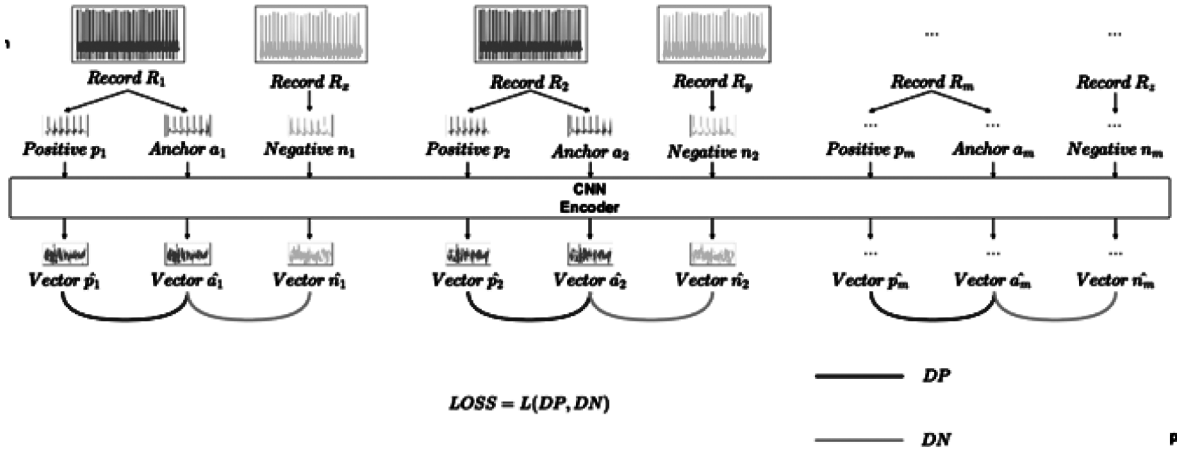

Рис. 5. Рабочий процесс триплетного контрастивного обучения за одну эпоху

ных позволило оценить устойчивость системы к различным условиям регистрации сигналов и шумам.

Эксперименты показали, что триплетная модель контрастивного обучения превосходит сиамскую модель по всем метрикам качества. Метод сегментации P2T обеспечил наивысшую точность благодаря сохранению полного сердечного цикла. Метод R2R показал несколько меньшую точность из-за возможного нарушения структуры сердечных циклов при сегментации. Метод NPD продемонстрировал конкурентоспособные результаты, несмотря на случайный характер сегментации, что свидетельствует о способности нейронной сети извлекать информативные признаки.

Таблица 1.

Сравнение методов сегментации и обучающих архитектур на базе PTBDB

Сегментация	Обучение	Точность (%)	Полнота (%)	Точность (%)
NPD	Siamese	96.33	98.7	97.53
NPD	Triplet	98.52	99.78	99.15
R2R	Siamese	95.81	96.37	96.1
R2R	Triplet	97.06	98.04	97.56
P2T	Siamese	98.04	97.67	97.85
P2T	Triplet	99.28	99.04	99.16

Модель, обученная на базе PTBDB, была протестирована на базах MITDB и ECGIDDB без изменения параметров модели. Полученные результаты показали высокую точность аутентификации на ранее неизвестных данных. Метод сегментации NPD показал наилучшие результаты и высокую устойчивость к различиям условий регистрации сигналов. Кроме того, данный метод снижает вычислительную сложность за счёт отсутствия этапа обнаружения пиков, как показано в Таблице 2.

Таблица 2.

Сравнение методов предобработки и тестовых наборов данных

Сегментация	Набор данных	Точность (%)	Полнота (%)	Точность (%)
NPD	MITDB	98.24	99.09	98.67
NPD	ECG	98.32	99.21	98.77
R2R	MITDB	92.45	94.34	93.45
R2R	ECGIDDB	92.9	95.03	94.02
P2T	MITDB	94.06	95.28	94.7
P2T	ECGIDDB	95.3	97.68	96.52

Выбор порогового значения существенно влияет на показатели FAR и FRR. Эксперименты показали, что

оптимальный диапазон порога обеспечивает баланс между безопасностью и удобством использования системы. Для оценки дискриминационной способности системы были построены ROC-кривые. Все методы сегментации продемонстрировали высокие значения площади под ROC-кривой (AUC) на базе PTBDB, при этом метод NPD показал наилучшую обобщающую способность, как показано на Рис. 6 и 7.

Для внедрения системы в IoT-устройства были применены методы оптимизации модели, включая квантование и прореживание. Квантование позволило уменьшить размер модели и ускорить инференс при минимальном снижении точности. Прореживание дополнительно уменьшило вычислительную сложность при сохранении высокой точности. Результаты экспериментов подтверждают возможность применения предложенной модели в ресурсно-ограниченных встроенных системах, показано на Рис 8.

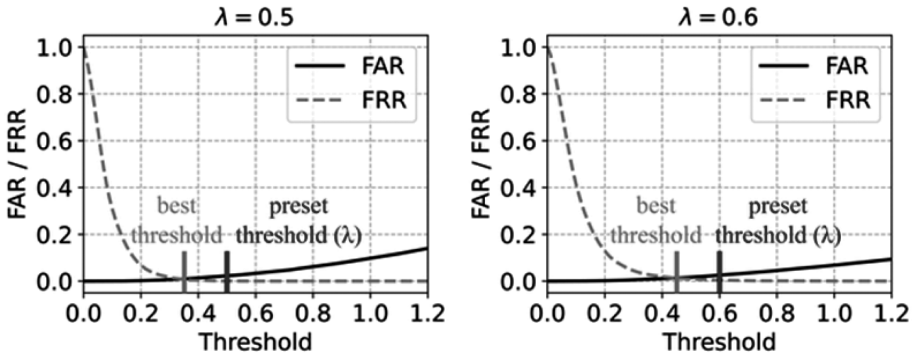

Рис. 6. Зависимость FAR и FRR от порогового значения

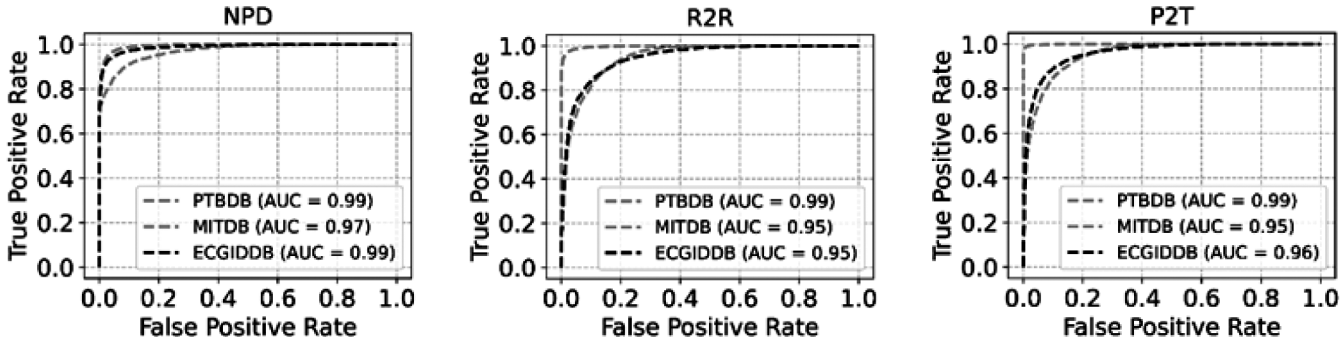

Рис. 7. ROC-кривые различных методов предобработки на наборах данных

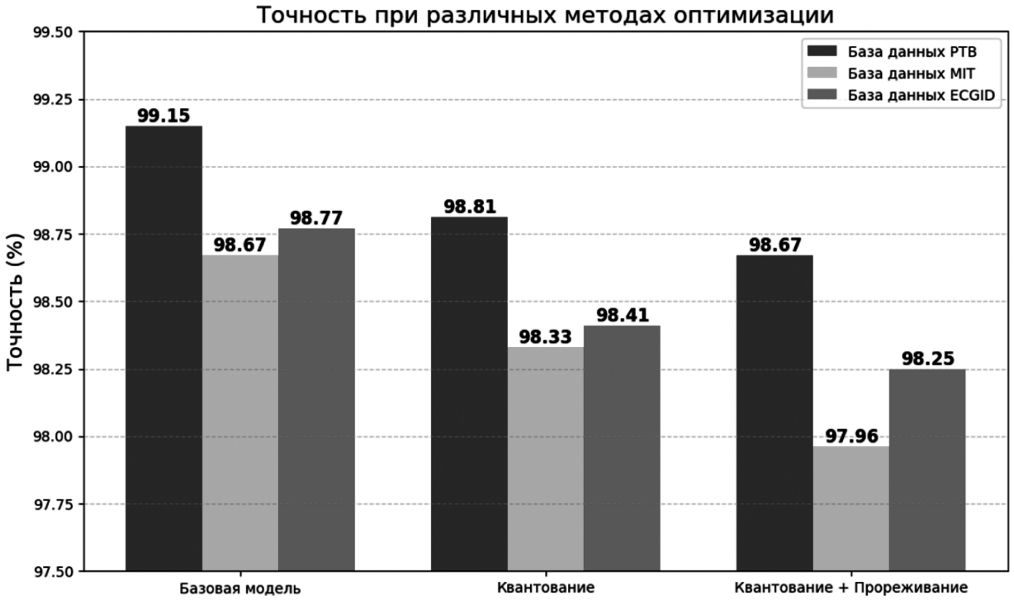

Рис. 8. Точность при различных методах оптимизации

Заключение

В работе предложена облегчённая система биометрической аутентификации по ЭКГ, основанная на сверточных нейронных сетях и самоконтролируемом контрастивном обучении. Разработанный метод обеспечивает высокую точность и устойчивость к вариациям сигналов. Применение квантования и прореживания позволило снизить вычислительную сложность и энергопотребление, обеспечив возможность внедрения системы в IoT-устройства. Использование закодированных биометрических признаков повышает уровень защиты персональных данных. Перспективным направлением дальнейших исследований является повышение устойчивости модели и разработка мультимодальных биометрических систем.

ЛИТЕРАТУРА

1. Тантави М.М., Реветт К., Салем А., Толба М.Ф. Метод извлечения признаков на основе вейвлет-преобразования для биометрического распознавания по ЭКГ // Signal, Image and Video Processing. — 2015. — Т. 9. — С. 1271–1280.
2. Хаммад М., Лю И., Ванг К. Мультимодальная биометрическая аутентификация на основе сверточных нейронных сетей с использованием ЭКГ и отпечатков пальцев // IEEE Access. — 2018. — Т. 7. — С. 26527–26542.
3. Лабати Р.Д., Пьюри В., Скотти Ф. Deep-ECG: сверточные нейронные сети для биометрической идентификации по ЭКГ // Pattern Recognition Letters. — 2019. — Т. 126. — С. 78–85.
4. Хазратифард М., Горбани А., Кешаварзиан П. Ансамблевая сиамская нейронная сеть для аутентификации пользователей по ЭКГ в интеллектуальных медицинских системах // Sensors. — 2023. — Т. 23, № 10. — С. 4727.
5. Сепахванд М., Абдали-Мохаммади Ф. Многоканальное распознавание личности по ЭКГ с использованием временно-частотного представления и морфологических CNN // Biomedical Signal Processing and Control. — 2021. — Т. 68. — Ст. 102766.
6. Хуанг П., Ванг С., Ванг Х. Практическая система конфиденциальной аутентификации по ЭКГ для IoT-здравоохранения // IEEE Internet of Things Journal. — 2019. — Т. 6, № 5. — С. 9200–9210.
7. Газариан А., Чжэн Ц., Струппа Д., Раковски К. Анализ рисков повторной идентификации при использовании алгоритмов глубокого обучения для данных ЭКГ // IEEE Access. — 2022. — Т. 10. — С. 68711–68723.
8. Хэ К., Фан Х., У Ю., Се С., Гиршик Р. Контрастное обучение представлений без учителя с использованием импульсной памяти // Материалы конференции IEEE/CVF Conference on Computer Vision and Pattern Recognition. — 2020. — С. 9729–9738.
9. Чен Т., Корнблит С., Норузи М., Хинтон Д. Простой фреймворк контрастивного обучения представлений // Материалы Международной конференции по машинному обучению. — 2020. — С. 1597–1607.
10. Чен Х., Лян И., Ванг С. CLECG: контрастивное обучение для классификации аритмий по ЭКГ // IEEE Signal Processing Letters. — 2021. — Т. 28. — С. 1993–1997.
11. Вэй Ц.Т., Чжан Ц., Ванг И. Contrastive Heartbeats: самоконтролируемое обучение представлений ЭКГ // Материалы IEEE International Conference on Acoustics, Speech and Signal Processing. — 2022. — С. 1126–1130.
12. Пан Д., Томпкинс У.Дж. Алгоритм обнаружения QRS-комплекса в реальном времени // IEEE Transactions on Biomedical Engineering. — 1985. — С. 230–236.
13. Муди Г.Б., Марк Р.Г. Значение базы данных MIT-BIH для исследований сердечных аритмий // IEEE Engineering in Medicine and Biology Magazine. — 2001. — Т. 20, № 3. — С. 45–50.
14. Ванг Г., Ли З., Чен Л. Низкосложная система биометрической аутентификации по ЭКГ для периферийных IoT-устройств // Материалы IEEE International Conference on Integrated Circuits, Technologies and Applications. — 2020. — С. 145–146.

Журнал «Современная наука: актуальные проблемы теории и практики»