УДК 004.056

Семиряков Дмитрий Андреевич, студент кафедры информатики и вычислительной техники, Сургутский государственный университет, г. Сургут

МЕТОДЫ БИОМАРКИРОВАНИЯ ЗАЩИЩАЕМЫХ ОБЪЕКТОВ

Аннотация

В статье рассматриваются современные методы биомаркирования защищаемых объектов, их роль в обеспечении информационной и физической безопасности. Проанализированы существующие подходы к идентификации и аутентификации пользователей, включая электронные подписи, речевые подписи и комплексные биометрические методы. Особое внимание уделено мультимодальным системам, объединяющим визуальные, аудиальные и психофизиологические данные для формирования надежного биомаркера. Рассматриваются принципы обработки и интеграции биометрической информации, включая спектральный анализ голосовых и сердечных сигналов, а также методы внедрения биомаркера в структуру защищаемого объекта. Подчеркивается значение анализа вариабельности сердечного ритма и состояния нервной системы для оценки достоверности действий. Обсуждаются области применения биомаркирования, включая защиту документов, контроль состояния операторов и выявление фактов принуждения. Сделан вывод о высокой перспективности данного направления и возможностях дальнейшего совершенствования с использованием технологий искусственного интеллекта и современных методов обработки данных.

Ключевые слова: биомаркирование, защищаемые объекты, биометрия, психофизиологические параметры, мультимодальные системы, безопасность, идентификация, аутентификация.

Abstract

The article examines modern methods of biomarking protected objects and their role in ensuring information and physical security. Existing approaches to user identification and authentication, including electronic signatures, voice signatures, and comprehensive biometric methods, are analyzed. Special attention is given to multimodal systems that combine visual, audio, and psychophysiological data to form a reliable biomarker. The principles of processing and integrating biometric information, including spectral analysis of voice and heart rate signals, as well as methods of embedding biomarkers into the structure of the protected object, are discussed. The importance of heart rate variability and nervous system state analysis for assessing action authenticity is emphasized. Applications of biomarking, such as

document protection, operator state monitoring, and coercion detection, are considered. The article concludes on the high prospects of this field and the potential for further improvement using artificial intelligence technologies and modern data processing methods.

Keywords: biomarking, protected objects, biometrics, psychophysiological parameters, multimodal systems, security, identification, authentication.

Введение

В современных условиях стремительного развития информационных технологий и увеличения количества угроз как в киберпространстве, так и в физической среде, особую актуальность приобретает задача надежной идентификации и аутентификации субъектов доступа к защищаемым объектам [1][2]. Традиционные методы защиты, такие как пароли, пластиковые карты, токены и даже криптографические ключи, уже не обеспечивают необходимого уровня безопасности, поскольку могут быть украдены, переданы третьим лицам или скомпрометированы в результате различных атак. В связи с этим активно развивается направление, связанное с использованием биометрических и психофизиологических характеристик человека, получившее название биомаркирования [1][3].

Биомаркирование представляет собой более широкое понятие по сравнению с классической биометрией. Если биометрия в основном используется для установления личности человека, то биомаркирование позволяет не только идентифицировать субъекта, но и подтвердить достоверность его действий, оценить его текущее состояние и выявить возможные аномалии поведения [7][8]. Это особенно важно в системах, где требуется не просто подтверждение личности, а гарантия того, что действие выполнено добровольно, осознанно и в нормальном психофизиологическом состоянии.

Теоретические основы биомаркирования

С научной точки зрения биомаркирование можно рассматривать как процесс формирования уникального цифрового отпечатка, основанного на

совокупности биометрических параметров человека, который интегрируется в защищаемый объект или сопровождает процесс выполнения значимого действия. Такой отпечаток формируется на основе физиологических и поведенческих характеристик, обладающих свойствами уникальности, устойчивости во времени и измеримости.

К числу наиболее значимых характеристик относятся геометрия лица, особенности голосового сигнала, параметры сердечного ритма, а также динамические показатели, такие как движения, мимика и особенности взаимодействия с устройствами [9][10][12]. Важным аспектом является то, что данные параметры сложно подделать в совокупности, особенно если система использует несколько источников информации одновременно.

Для иллюстрации особенностей обработки визуальных биометрических данных рассмотрим распределение яркости пикселей инфракрасного изображения лица, представленное на рисунке 1.

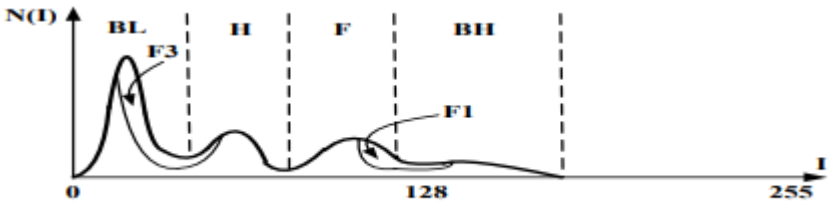

Figure 1: Typical histogram of pixel distribution of thermal image by brightness

Рисунок 1 – Гистограмма распределения яркости инфракрасного изображения лица. [1]

Как видно из рисунка 1, исходное изображение характеризуется неравномерным распределением яркости, при котором значительная часть пикселей относится к фону и малозначимым областям. Это усложняет выделение информативных признаков, необходимых для формирования надежного биомаркера.

Биомаркирование опирается на многослойную модель, включающую идентификационный уровень, функциональный уровень и контекстный уровень. Идентификационный уровень отвечает за установление личности пользователя, функциональный — за оценку его текущего состояния (например, уровень стресса или усталости), а контекстный уровень учитывает

условия, в которых выполняется действие, включая внешнюю среду и поведенческие особенности. Такое объединение различных типов данных позволяет значительно повысить надежность систем безопасности.

Анализ существующих методов подтверждения подлинности

На протяжении длительного времени основным способом подтверждения подлинности документов и действий являлась электронная подпись. Она основана на использовании криптографических алгоритмов и позволяет обеспечить юридическую значимость электронных документов. Однако, несмотря на свои преимущества, электронная подпись имеет ряд существенных недостатков. В частности, безопасность системы полностью зависит от сохранности закрытого ключа. В случае его компрометации злоумышленник получает возможность выполнять действия от имени владельца без каких-либо дополнительных проверок.

Альтернативой является речевая подпись, которая основана на анализе голосового сигнала человека. Голос содержит большое количество уникальных характеристик, связанных как с анатомическими особенностями речевого аппарата, так и с индивидуальными привычками речи. Преобразование голосового сигнала в спектральное представление позволяет выделить устойчивые признаки, пригодные для идентификации. Однако данный метод также имеет ограничения, связанные с влиянием шумов, качеством записи и изменениями состояния человека.

Наиболее перспективным направлением является биометрическая подпись, или биоподпись, которая объединяет в себе несколько типов данных [7][10]. Она может включать не только голос или изображение лица, но и параметры сердечного ритма, дыхания и другие физиологические показатели. Такой подход позволяет перейти от простой проверки личности к комплексной оценке достоверности действия.

Комплексные методы биомаркирования

Современные системы биомаркирования строятся на принципе мультимодальности, то есть использовании сразу нескольких источников биометрической информации [7][11]. Это позволяет компенсировать недостатки отдельных методов и значительно повысить устойчивость системы к атакам.

В рамках комплексного подхода формируется биомаркер, включающий контекстную информацию документа, биометрические характеристики пользователя и его психофизиологические параметры. Контекстная информация может содержать ключевые элементы документа, такие как сумма, дата или тип операции. Биометрическая часть включает голос и изображение лица, а психофизиологическая — параметры сердечного ритма, дыхания и двигательной активности.

Особое значение имеет анализ вариабельности сердечного ритма, который позволяет оценить состояние нервной системы человека [12][14]. Известно, что сердечный ритм не является строго периодическим и изменяется под воздействием различных факторов, включая стресс и физическую нагрузку. Анализ частотных компонентов сигнала позволяет выделить индивидуальные особенности, которые могут использоваться как дополнительный уровень защиты.

Методы обработки и интеграции данных

Получение биометрических данных осуществляется с использованием различных технических средств, включая видеокамеры, микрофоны, инфракрасные датчики и носимые устройства [10][15]. После сбора данные проходят этап предварительной обработки, включающий фильтрацию шумов, нормализацию и выделение информативных признаков.

Одним из наиболее эффективных способов представления биометрической информации является спектральный анализ. Например, голосовой сигнал может быть преобразован в спектрограмму, которая отражает распределение энергии по частотам во времени. Аналогично,

сигналы сердечного ритма могут быть представлены в виде спектра, что позволяет выделить характерные частотные компоненты.

Интеграция биомаркера в защищаемый объект осуществляется путем внедрения полученных данных в структуру документа или системы [7][10]. При этом используется принцип тесной связи между содержимым объекта и биометрическими параметрами. Любое изменение объекта приводит к нарушению этой связи, что позволяет обнаружить попытку подделки.

На рисунке 2 представлено сравнение параметров биометрических данных до и после предварительной обработки и интеграции в объект. Видно, как применение фильтрации, нормализации и спектрального анализа позволяет выделить информативные признаки и повысить надежность биомаркера.

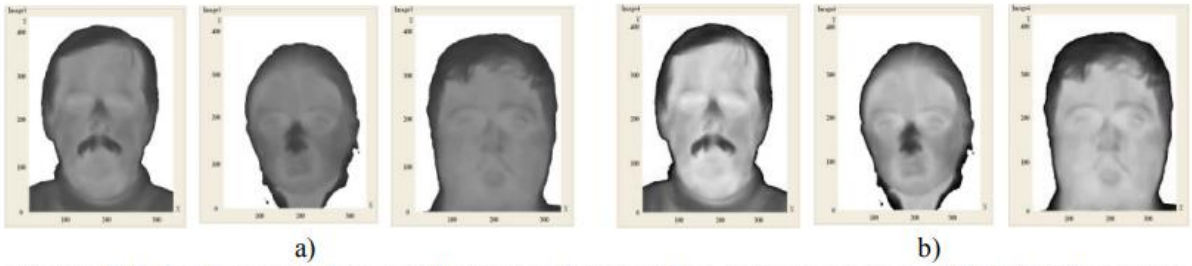

Figure 7: Laboratory approbation of the proposed approach: a - typical examples of the initial thermal image of a person's face; b - improvement of the contrast of images on the basis of the proposed approach

Рисунок 2 – Сравнение параметров до и после обработки [1]

Области применения

Методы биомаркирования находят применение в различных областях, включая защиту документов, обеспечение безопасности критически важных объектов и мониторинг состояния операторов. В системах электронного документооборота биомаркирование позволяет не только подтвердить авторство документа, но и установить условия, в которых он был подписан [7][10][11].

В системах управления сложными техническими объектами биомаркирование используется для контроля состояния операторов. Это особенно важно в таких областях, как транспорт, энергетика и промышленность, где ошибка человека может привести к серьезным

последствиям. Анализ биометрических данных позволяет своевременно выявить признаки усталости, стресса или других неблагоприятных состояний.

Кроме того, биомаркирование может использоваться для выявления фактов принуждения. Известно, что психофизиологическое состояние человека изменяется под воздействием внешнего давления. Эти изменения могут быть зафиксированы и использованы для определения того, было ли действие выполнено добровольно.

Заключение

Таким образом, биомаркирование представляет собой перспективное направление в области обеспечения безопасности, позволяющее существенно повысить надежность систем защиты. В отличие от традиционных методов, оно основывается на использовании уникальных характеристик человека и учитывает не только его личность, но и текущее состояние и поведение. Комплексный подход, включающий анализ различных типов данных, обеспечивает высокую устойчивость к атакам и делает подделку практически невозможной.

Развитие технологий искусственного интеллекта и средств обработки данных открывает новые возможности для совершенствования методов биомаркирования. В дальнейшем можно ожидать появления более точных, быстрых и удобных систем, которые будут широко использоваться как в государственных, так и в коммерческих структурах.

Список литературы

1. Electronic Signatures in Global and National Commerce Act (Public Law 106–229, June 30, 2000). URL: https://www.govinfo.gov/content/pkg/PLAW-106publ229/pdf/PLAW-106publ229.pdf (дата обращения: 31.03.2026)
2. Федеральный закон РФ №63-ФЗ «Об электронной подписи», 06.04.2011. URL: https://iecp.ru/docs/legislation/fz-63.pdf (дата обращения: 31.03.2026)

3. Uniform Electronic Transactions Act, 2021. URL: https://en.wikipedia.org/wiki/Uniform_Electronic_Transactions_Act (дата обращения: 31.03.2026)
4. Alyushin M. V., Kolobashkina L. V., Rozhanskaya Y. N. Measurement of static and dynamic bio-parameters of a person in remote systems for current psycho-emotional and functional state monitoring // Proceedings of IEEE ERGO. – St. Petersburg, Russia, 2018. – P. 161–165. (дата обращения: 31.03.2026)
5. Kiss G., Sztahó D., Vicsi K., Golemis A. Connection between body condition and speech parameters – especially in the case of hypoxia // Proceedings of the 5th IEEE Conference on Cognitive Infocommunications (CogInfoCom). – Vietri sul Mare, Italy, 2014. – P. 333–336. (дата обращения: 31.03.2026)
6. Alyushin M. V., Kolobashkina L. V., Parakhin V. R., Dvoryankin S. V. Obtaining reliable biometric information in the analysis of vibration images of the operator's face // XXIII International Conference on Soft Computing and Measurements (SCM). – St. Petersburg, Russia, 2020. – P. 265–268. (дата обращения: 31.03.2026)
7. Bevilacqua F., Engström H., Backlund P. Changes in heart rate and facial actions during a gaming session with provoked boredom and stress // Entertainment Computing. – 2018. – Vol. 24. – P. 10–20. (дата обращения: 31.03.2026)
8. Calvo M. G., Lang P. J. Gaze patterns when looking at emotional pictures: motivationally biased attention // Motivation and Emotion. – 2004. – Vol. 28, No. 3. – P. 221–243. (дата обращения: 31.03.2026)
9. Ruiz-Padial E., Sollers J. J., Vila J., Thayer J. F. The rhythm of the heart in the blink of an eye: emotion-modulated startle magnitude covaries with heart rate variability // Psychophysiology. – 2003. – Vol. 40, No. 2. – P. 306–313. (дата обращения: 31.03.2026)
10. Alyushin A. M., Alyushin M. V, Kolobashkina L. V. Laboratory approbation of a new approach for contrast enhancement of human face thermal image based on selective multifunction pixel brightness conversion function // Procedia Computer Science. – 2018. – Vol. 123. – P. 1–6. (дата обращения: 31.03.2026)

11. Safonov I., Gartseev I. An approach for benchmarking of activity recognition // 11th Int. Conf. Pattern Recognition and Image Analysis. – Samara, Russia, 2013. – Vol. 2. – P. 457–460. (дата обращения: 31.03.2026)
12. Malik M., Camm A. J. Heart rate variability and clinical cardiology // British Heart Journal. – 1990. – Vol. 63, No. 6. – P. 343–354. (дата обращения: 31.03.2026)
13. Poh M.-Z., McDuff D. J., Picard R. W. Non-contact, automated cardiac pulse measurements using video imaging and blind source separation // Optics Express. – 2010. – Vol. 18, No. 10. – P. 10762–10774. (дата обращения: 31.03.2026)
14. Nkurikiyeyezu K., Massé F., Gagnon J.-F. Multimodal biometric system for operator state monitoring in critical environments // Sensors. – 2019. – Vol. 19, No. 23. – P. 5200. (дата обращения: 31.03.2026)
15. Patel S., Park H., Bonato P., Chan L., Rodgers M. A review of wearable sensors and systems with application in rehabilitation // Journal of NeuroEngineering and Rehabilitation. – 2012. – Vol. 9. – P. 21. (дата обращения: 31.03.2026)