Научная статья
Статья в открытом доступе
УДК 519:004
doi: 10.30987/2658-4026-2024-2-153-158

Мультимодальные нейронные сети в системах информационной безопасности

Дмитрий Владимирович Логвинов[1]✉, Алина Михайловна Шапенская[2], Михаил Юрьевич Рытов[3], Степан Сергеевич Савкин[4]
[1,2,3,4]Брянский государственный технический университет; Брянская область, Брянск, Россия
[1]logvinovdmitriv@gmail.com; https://orcid.org/0009-0004-6399-4396
[2]alinashapenskaya2002@gmail.com; https://orcid.org/0009-0007-8434-5848
[3]rmy@tu-bryansk.ru, https://orcid.org/0000-0001-7533-4353
[4]hanawaro3@gmail.com; https://orcid.org/0009-0000-6368-2967

Аннотация.

В статье освещается значимая роль внедрения мультимодальных нейронных сетей в системы информационной безопасности для повышения эффективности работы при детектировании киберугроз. Использование комбинации нейронных сетей, включая сверточные (CNN), рекуррентные (RNN) и сети с долгой краткосрочной памятью (LSTM), позволяет достигать высокой точности и скорости обнаружения киберугроз. Объединяя различные источники данных, такие как видеонаблюдение, аудиоанализ, биометрическую идентификацию и анализ поведенческих паттернов, эти мультимодальные системы предлагают комплексный и глубокий анализ безопасности, делая их эффективным решением против современных угроз в информационной среде.

***Цель исследования**: анализ и сравнение эффективности различных типов нейросетей, применяемых в информационной безопасности, с особым вниманием к возможностям мультимодальных систем.*

***Задача исследования**: оценка применения различных типов нейросетей в разных сценариях обработки данных, от биометрического распознавания до анализа сетевого трафика.*

***Методы исследования**: теоретический анализ и сравнение сверточных нейронных сетей (CNN), рекуррентных нейронных сетей (RNN) и сетей с долгой краткосрочной памятью (LSTM). Новизна работы заключается в комплексном подходе к анализу мультимодальных систем в контексте современных киберугроз.*

***Результаты исследования**: мультимодальные системы, оснащенные современными нейронными сетями, представляют собой будущее в области информационной безопасности.*

***Выводы**: проведенный анализ подтверждает существенную роль интеграции искусственного интеллекта в системы информационной безопасности, подчеркивая важность мультимодальных систем в создании эффективных, адаптивных и масштабируемых решений для защиты данных и информационных систем в современной цифровой среде.*

Ключевые слова: искусственный интеллект, информационная безопасность, мультимодальные системы, нейронные сети, биометрическое распознавание, анализ сетевого трафика, сверточные нейронные сети, рекуррентные нейронные сети, сети с долгой краткосрочной памятью

Для цитирования: Логвинов Д. В., Шапенская А. М., Рытов М. Ю., Савкин С. С. Мультимодальные нейронные сети в системах информационной безопасности // Эргодизайн. №2 (24). 2024. С. 153-158. http://dx.doi.org/10.30987/2658-4026-2024-2-153-158.

Original article
Open access article

Multimodal Neural Networks in Information Security Systems

Dmitry V. Logvinov[1]✉, Alina M. Shapenskaya[2], Mikhail Y. Rytov[3], Stepan S. Savkin[4]
[1,2,3,4]Bryansk State Technical University; the Bryansk region, Bryansk, Russia
[1]logvinovdmitriv@gmail.com; https://orcid.org/0009-0004-6399-4396
[2]alinashapenskaya2002@gmail.com; https://orcid.org/0009-0007-8434-5848
[3]rmy@tu-bryansk.ru, https://orcid.org/0000-0001-7533-4353
[4]hanawaro3@gmail.com; https://orcid.org/0009-0000-6368-2967

Abstract.

The article highlights the significant role of introducing multimodal neural networks into information security systems to improve operational efficiency in detecting cyber threats. Using a combination of neural networks, including convolutional neural networks (CNN), recurrent neural networks (RNN), and long short-term memory networks (LSTM), it is possible to achieve high accuracy and speed in detecting cyber threats. By combining multiple data sources such as video surveillance, audio analysis, biometric identification, and behavioural pattern analysis, these multi-modal systems offer comprehensive and in-depth security analysis, making them an effective solution against today's threats in the information environment.

The aim of the study is to analyze and compare the effectiveness of various types of neural networks used in information security, with special attention to the capabilities of multimodal systems.

Research objective is to evaluate the use of various types of neural networks in different data processing scenarios, from biometric recognition to network traffic analysis.

Research methods are: theoretical analysis and comparison of convolutional neural networks (CNN), recurrent neural networks (RNN) and long short-term memory networks (LSTM). The novelty of the work lies in an integrated approach to analysing multimodal systems in the context of modern cyber threats.

Research results: multimodal systems equipped with modern neural networks represent the future in the field of information security.

Findings: the analysis confirms the essential role of integrating artificial intelligence into information security systems, emphasizing the importance of multimodal systems in creating effective, adaptive, and scalable solutions for protecting data and information systems in the modern digital environment**.**

Keywords: artificial intelligence, information security, multimodal systems, neural networks, biometric recognition, network traffic analysis, convolutional neural networks, recurrent neural networks, networks with long short-term memory

Для цитирования: Logvinov D.V., Shapenskaya A.M., Rytov M.Yu, Savkin S.S. Multimodal Neural Networks in Information Security Systems // Ergodesign. 2024;2(24): 153-158. http://dx.doi.org/ 10.30987/2658-4026-2024-2-153-158.

В современной эпохе цифровизации, когда информационные технологии (ИТ) стремительно развиваются, вопросы кибербезопасности становятся всё более актуальными. Учитывая стремительный рост исследований в области искусственного интеллекта (ИИ), а в частности нейронных систем, внедрение данных модулей в системы распознования и детектирования киберугроз, позволит радикально изменить традиционные подходы к защите данных и информационных систем (ИС), в особенности для анализа информации из различных источников, таких как видео, аудио, поведенческие паттерны. Для анализа данных из различных типов источников наиболее подходящими являются мультимодальные нейронные сети, поскольку они позволяют комбинировать различные типы нейронных сетей для повышения точности и скорости распознавания киберугроз.

Например, в исследовании «A Novel Multimodal-Sequential Approach Based on Multi-View Features for Network Intrusion Detection» была применен мультимодально-последовательный подход для обнаружения киберугроз в сфере сетевых вторжений (рис. 1) [1]. Данный подход позволил повысить точность обнаружения сетевых атак до 94% при бинарной классификации и до 88% при мультиклассификации, что на 2% и 4% выше по сравнению с другими методами.

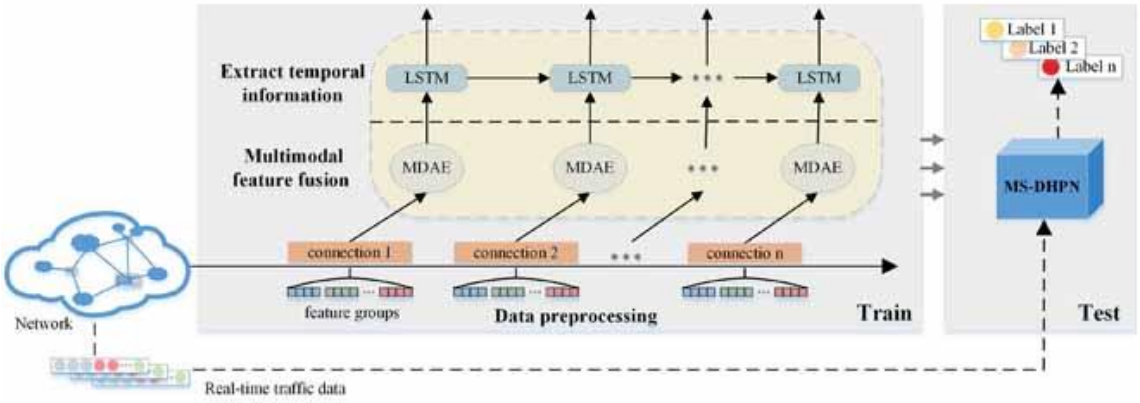

Рис 1. Пример использования мультимодально-последовательного подхода в системе распознавания киберугроз [1]

Fig. 1. An example of using a multimodal-sequential approach in a cyber threat recognition system [1]

На настоящий момент, мультимодально-последовательный подход в виде мультимодальных нейронных сетей (ММНС) применяется в различных отраслях жизнедеятельности человека. Например, для диагностики болезни Альцгеймера, они применяются с механизмом самовнимания, который обрабатывает клинические и генетические результаты исследований, а также изображения мозга для повышения точности диагностики заболевания (рис. 2) [2].

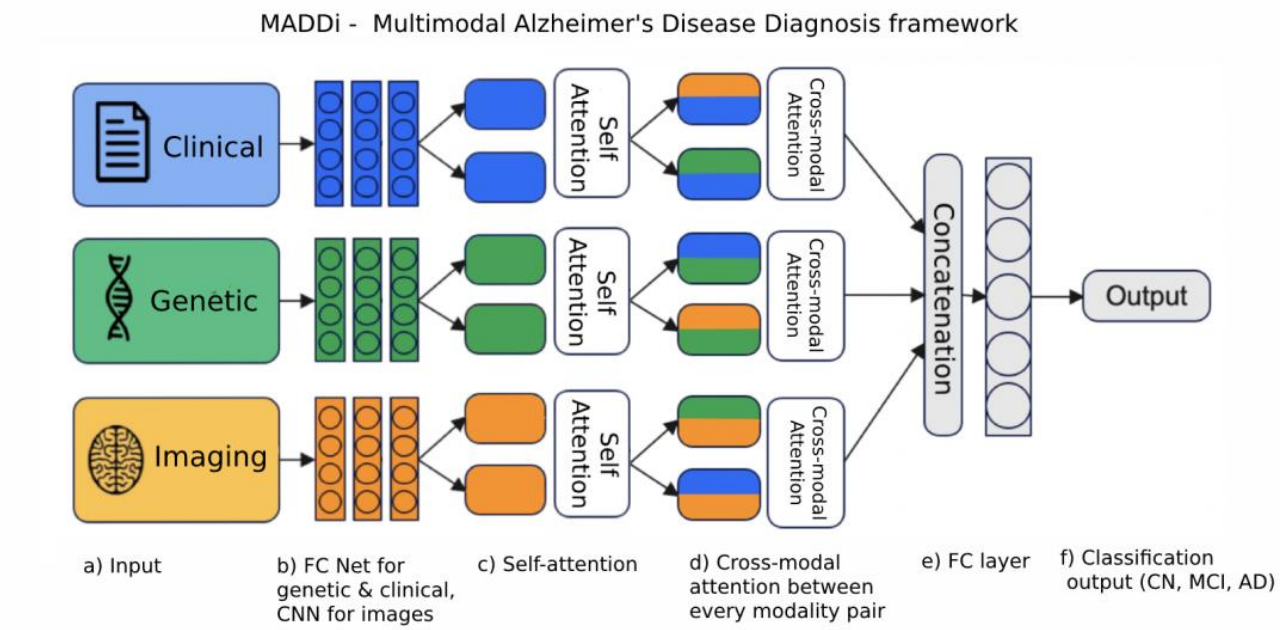

Рис 2. Пример использования мультимодальной системы с механизмом самовнимания для диагностики болезни Альцгеймера [2]

Fig. 2. An example of using a multimodal system with a self-awareness mechanism for the diagnosis of Alzheimer's disease [2]

Проектируя ММНС, необходимо понимать, комбинация каких типов нейронных сетей окажется наиболее подходящей для поставленной задачи, позволяя реализовать гибкую и адаптируемую к непрерывно меняющимся условиям систему. На текущий момент существует 3 основных типа нейронных сетей: сверточные нейронные сети (*CNN*), рекуррентные нейронные сети (*RNN*) и сети с долгой краткосрочной памятью (*LSTM*).

Сеть *CNN* – это тип нейроных сетей, которые оптимизированы для анализа визуальной информации и часто используемый в областях, требующих обработки и распознавания изображений. В основе их работы лежат операции свертки, которые позволяют им извлекать из входных данных важные визуальные особенности, такие как края, углы и текстуры [2]. Это достигается за счет применения фильтров к изображениям, что делает *CNN* высокоэффективными для распознавания образов, видеоанализа и систем биометрической идентификации, которые требуют высокой точности и быстрого анализа, и возможностей классификации изображений.

Сети *RNN* были разработаны для необходимости обработки непрерывных данных, таких как текст и временные ряды, и используют внутренние циклы для сохранения информации о предыдущих входных данных, что позволяет учитывать весь контекст и порядок данных во время обработки [3, 4] и делает их достаточно востребованными для обработки естественного языка, анализа и задач генерации текста, распознавания речи, где важно учитывать порядок и зависимости между словами и символами. Однако с течением времени происходит исчезновение градиентов, что затрудняет обучение и работу *RNN* в течении продолжительного промежутка времени.

Сеть *LSTM* являются улучшенной версией *RNN*, в которой решается проблема исчезающего градиента, что позволяет более эффективно обрабатывать долгосрочные зависимости. Для неё характерно наличие механизмов шлюзования, при помощи которых происходит управление хранением, обновлением и забыванием информации, что позволяет более гибко управлять потоком данных [5]. Эти свойства делают *LSTM* особенно ценными для решения сложных задач обработки естественного языка,

распознавания речи и анализа временных рядов, в которых требуются учет как текущих, так и долгосрочных отношений между элементами данных.

При проектировании ММНС важно понимать, что объединение различных типов нейронных сетей повысит эффективность, но в то же время увеличит время на обучение. В контексте обнаружения аномалий сетевого трафика было обнаружено, что мультимодальная комбинация *CNN* и *LSTM* обладает более высокой способностью обнаруживать аномалии с более высокой точностью, чем их одномодальность.

Приоритеты обнаружения аномалий могут различаться в зависимости от конкретных системных требований. Если стоит цель добиться низкого уровня ложных срабатываний и нет ограничений по временным затратам на обучение, предпочтительным выбором является комбинация сетей *CNN+LSTM*. Модель *CNN+LSTM*-1 показывает точность до 99,126%, а модель *CNN+LSTM*-2 – точность 99,124%, что немного ниже, чем у одномодальных *CNN* и *LTSM*, где точность составила 99,095% и 98,938% соответственно [7].

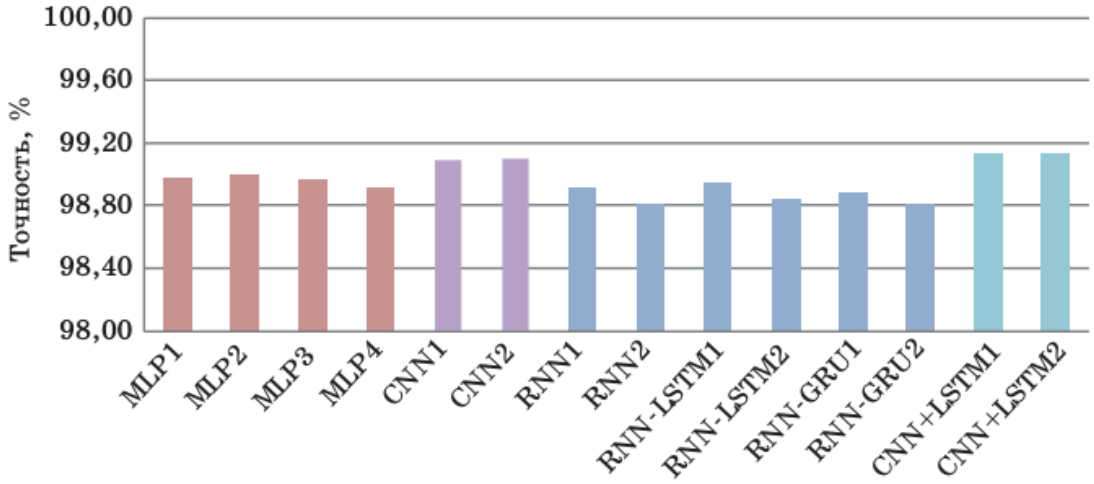

Рис. 3. Сравнение точности одномодальных и мультимодальных нейронных сетей в задаче в задаче детектирования аномалий сетевого трафика *IoT* (Интернет вещей)[7]

Fig. 3. Comparison of the accuracy of single-modal and multimodal neural networks in the problem of detecting anomalies in IoT network traffic (Internet of Things)[7]

Одномодальные нейронные сети по-прежнему эффективны, особенно для задач, где скорость является критическим фактором, хотя их точность уступает мультимодальным нейронным сетям, она все же обеспечивает достаточную эффективность для многих задач.

Также требуется учитывать, что время, необходимое для обучения одномодальной сети или мультимодальной сети с другой комбинацией нейроннх сетей (*RNN+LTSM*), зачастую меньше, чем у мультимодальной сети (*CNN+LTSM*). Это делает другие вариации систем более привлекательными для сценариев, где временные ресурсы на обучение ограничены. Например, для обучения *RNN*-LSTM-1 требуется всего 301,561 секунды, что значительно меньше времени обучения, необходимого для ММНС, таких как *CNN+LSTM*, которое занимает до 1355,819 секунды [7].

Важно подчеркнуть, что выбор между одномодальными и мультимодальными системами, а также их комбинациями должен основываться на конкретных требованиях поставленной задачи. Несмотря на то, что одномодальные нейронные сети достаточно эффективны в определенных задачах, использование ММНС повышает точность распознавания, а также расширяет функциональные возможности для анализа большего вида источников данных. Например, в сфере информационной безопасности, если требуется наибольшая точность распознавания, наиболее подходящими будут мультимодальные сети *CNN+LTSM*, а сети *RNN+LTSM* более подходящие если требуется высокая скорость обучения и достаточная точность.

В контексте информационной безопасности (ИБ) одним из видов эвристической деятельности является противоборство злоумышленникам, связанное с ростом киберпреступлений, в краже и сбыте конфиденциальной информации, в платежных транспортных, банковских системах и т.д. В связи с этим особое значение приобретает

разработка систем искусственного интеллекта, связанные с биометрическими технологиями, устройствами аутентификации в беспроводных сетях, компьютерными системами машинного обучения в сфере информационной безопасности [8].

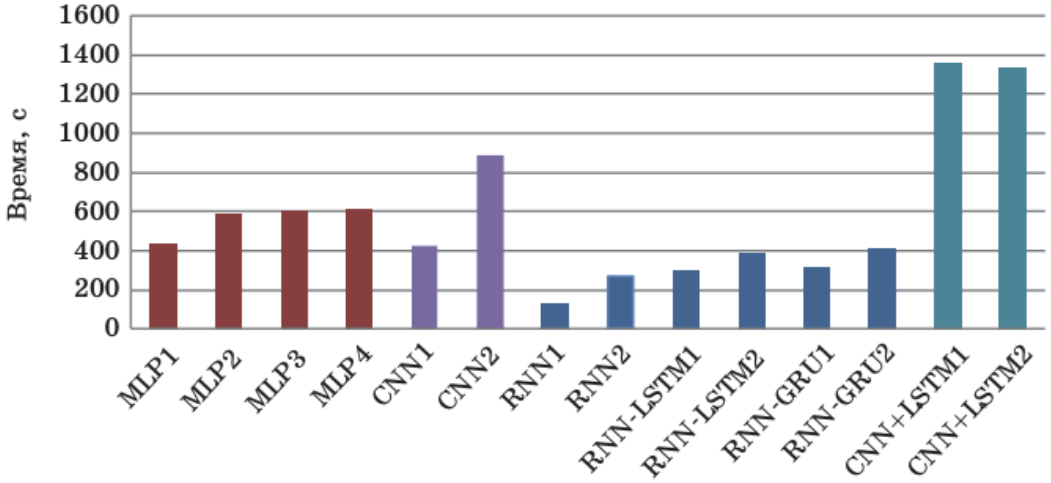

Рис 4. Сравнение времени обучения одномодальных и мультимодальных нейронных сетей в задаче детектирования аномалий сетевого трафика *IoT* [7]

Fig. 4. Comparison of the training time of single-modal and multimodal neural networks in the task of detecting anomalies in IoT network traffic [7]

Таким образом, использование ММНС может существенно повысить качество автоматизации, однако необходимо учитывать, что финальное решение должно приниматься с участием экспертной оценки. Поскольку экспертная оценка позволит произвести критический анализ выводов, сделанных системой, а также определить потенциальные угрозы и неоднозначности, пропущенные системой. Также экспертная оценка позволит объективизировать финальное решение, а также обеспечит соответствие этическим аспектам и требованиям законодательства.

СПИСОК ИСТОЧНИКОВ

1. **Haitao H., Xiaobing S., Hongdou H., Guyu Zh., Ligang H., Jiadong R.** A Novel Multimodal-Sequential Approach Based on Multi-View Features for Network Intrusion Detection. IEEE Access. 2019;7:183207-183221. DOI 10.1109/ACCESS.2019.2959131.
2. **Golovanevsky M., Eickhoff C., Singh R.** Multimodal attention-based deep learning for Alzheimer's disease diagnosis. Journal of the American Medical Informatics Association. 2022;29(12):2014-2022. DOI 10.1093/jamia/ocac168.
3. **Сверточные нейронные сети. Викиконспекты ИТМО.** URL: https://neerc.ifmo.ru/wiki/index.php?title=Сверточные_нейронные_сети (дата обращения:16.01.2024).
4. **Дычков И.Н.** Сверточные нейронные сети // Тенденции развития науки и образования. 2021. № 73-1. С. 38-41. DOI 10.18411/lj-05-2021-08. EDN MQYWDB.
5. **Рекуррентные нейронные сети. Викиконспекты ИТМО.** URL: https://neerc.ifmo.ru/wiki/index.php?title=Рекуррентные_нейронные_сети (дата обращения:18.02.2024).
6. **Долгая краткосрочная память. Викиконспекты ИТМО.** URL: https://neerc.ifmo.ru/wiki/index.php?title=Долгая_краткосрочная_память (дата обращения:23.02.2024).
7. **Гайфулин Д.А., Котенко И.В**. Анализ моделей глубокого обучения для задач обнаружения сетевых аномалий интернета вещей // Информационно-управляющие системы. 2021. № 1(110). С. 28-37. DOI 10.31799/1684-8853-2021-1-28-37. EDN DTPPJY.

REFERENCES

1. **Haitao H., Xiaobing S., Hongdou H., Guyu Zh., Ligang H., Jiadong R.** A Novel Multimodal-Sequential Approach Based on Multi-View Features for Network Intrusion Detection. IEEE Access. 2019;7:183207-183221. DOI 10.1109/ACCESS.2019.2959131.
2. **Golovanevsky M., Eickhoff C., Singh R.** Multimodal Attention-Based Deep Learning for Alzheimer's Disease Diagnosis. Journal of the American Medical Informatics Association. 2022;29(12):2014-2022. DOI 10.1093/jamia/ocac168.
3. **Convolutional Neural Networks. ITMO Wikinotes** [Internet] [cited 2024 Jan 16]. Available from: https://neerc.ifmo.ru/wiki/index.php?title=Convolutional_neural_networks.
4. **Dychkov I.N.** Convolutional Neural Networks. Trends in the Development of Science and Education. 2021;73-1:38-41. DOI 10.18411/lj-05-2021-08.
5. **Recurrent Neural Networks. ITMO Wikinotes.** [Internet] [cited 2024 Feb 18]. Available from: https://neerc.ifmo.ru/wiki/index.php?title=Recurrent_neural_networks.
6. **Long Short-Term Memory. ITMO Wikinotes. [Internet]** [cited 2024 Feb 23]. Available from: https://neerc.ifmo.ru/wiki/index.php?title=Long_short-term_memory.
7. **Gaifulin D.A., Kotenko I.V.** Analysis of Deep Learning Models for Network Anomaly Detection in Internet of Things. Information and Control Systems. 2021;1(110):28-37. DOI 10.31799/1684-8853-2021-1-28-37.

8. **Spasennikov V., Androsov K., Golubeva G.** Ergonomic factors in patenting computer systems for personnel's selection and training. CEUR Workshop Proceedings : 30, Saint Petersburg, 22–25 сентября 2020 года. Saint Petersburg, 2020. P. 1. EDN MRWCZX.

8. **Spasennikov V, Androsov K, Golubeva G.** Ergonomic Factors in Patenting Computer Systems for Personnel's Selection and Training. In: Proceedings of the 30th International Conference on Computer Graphics and Machine Vision GraphiCon-2020; 2020 Sep 22-25; Saint Petersburg: 2020, vol. 2744. p. 1.

Информация об авторах:

Логвинов Дмитрий Владимирович – студент ФГБОУ ВО «Брянский государственный технический университет», тел. 89996212001, E-mail: logvinovdmitriv@gmail.com; ORCID 0009-0004-6399-4396

Шапенская Алина Михайловна – студент ФГБОУ ВО «Брянский государственный технический университет», тел. 89003633385, E-mail: alinashapenskaya2002@gmail.com; ORCID 0009-0007-8434-5848

Рытов Михаил Юрьевич – Брянский государственный технический университет, Кандидат технических наук, доцент, Тел.: +7 (4832) 51-13-77, E-mail: rmy@tu-bryansk.ru

Савкин Степан Сергеевич – студент ФГБОУ ВО «Брянский государственный технический университет», тел. 89092409410, E-mail: hanawaro3@gmail.com; ORCID 0009-0000-6368-2967

Information about the authors:

Logvinov Dmitry Vladimirovich – student of Bryansk State Technical University, ph. 89996212001, E-mail: logvinovdmitriv@gmail.com;

Shapenskaya Alina Mikhailovna – student of Bryansk State Technical University, ph. 89003633385, E-mail: alinashapenskaya2002@gmail.com;

Rytov Mikhail Yurievich – Bryansk State Technical University, Candidate of Technical Sciences, Associate Professor, ph. +7 (4832) 51-13-77, E-mail: rmy@tu-bryansk.ru, the author's international identification numbers: AuthorID: 425093

Savkin Stepan Sergeevich – student of Bryansk State Technical University, ph. 89092409410, E-mail: hanawaro3@gmail.com

Вклад авторов: все авторы сделали эквивалентный вклад в подготовку публикации.
Contribution of the authors: the authors contributed equally to this article.
Авторы заявляют об отсутствии конфликта интересов.
The authors declare no conflicts of interests.
Статья поступила в редакцию 03.06.2024; одобрена после рецензирования 11.06.2024; принята к публикации 14.06.2024. Рецензент –Двилянский А.А.., кандидат технических наук., доцент Академии Федеральной службы охраны РФ, член редакционного совета журнала «Эргодизайн»
The paper was submitted for publication on the 3rd of June, 2024; approved after the peer review on the 11th of June, 2024; accepted for publication on the 14th of June, 2024. Reviewer – Dvilyansky A.A., Candidate Of Technical Sciences, Associate Professor of the Russian Federation Security Guard Service Federal Academy, member of the editorial board of the journal "Ergodesign"..