

УДК 004.056.523

ПРИМЕНЕНИЕ АЛГОРИТМА ДУГЛАСА–ПЕККЕРА В ВОПРОСАХ ОНЛАЙН-АУТЕНТИФИКАЦИИ ИНСТРУМЕНТОВ УДАЛЁННОЙ РАБОТЫ ПРИ ПОДГОТОВКЕ СПЕЦИАЛИСТОВ УКРУПНЁННОЙ ГРУППЫ СПЕЦИАЛЬНОСТЕЙ 10.00.00 «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

А. Г. Уймин¹ [0000-0003-1572-5488], **В. С. Греков**² [0009-0006-4067-4976]

^{1, 2} *Российский государственный университет нефти и газа (Национальный исследовательский университет) имени И.М. Губкина*

¹au-mail@ya.ru, ²grekov.vs.work@gmail.com

Аннотация

В условиях перехода образовательных систем на дистанционное обучение, а также развития тренда на удалённую работу, возникла острая потребность в разработке надежных технологий биометрической идентификации и аутентификации для верификации исполнителей работ в режиме удаленной работы. Такие технологии позволяют обеспечить высокую степень защиты и удобство использования, что делает вопросы их разработки и оптимизации крайне важными.

Проблема заключается в необходимости повышения точности и эффективности систем распознавания движений манипулятора «мышь» без использования специализированных устройств в максимально короткий промежуток времени. Для ее решения требуется эффективная предобработка таких движений, чтобы упростить их траектории, сохранив при этом их ключевые особенности.

В статье предложено использование алгоритма Дугласа–Пеккера для предварительной обработки данных траекторий движений «мыши». Этот алгоритм позволяет значительно уменьшить количество точек в траекториях, упрощая их при сохранении основной формы движений. Данные с упрощенными траекториями затем используются для обучения нейронных сетей.

Экспериментальная часть работы показала, что применение алгоритма Дугласа–Пеккера позволяет сократить количество точек в траекториях на 60%, что приводит к увеличению точности распознавания движений с 70% до 82%. Такое упрощение данных способствует ускорению процесса обучения нейронных сетей и повышению их операционной эффективности.

Проведенное исследование подтвердило эффективность использования алгоритма Дугласа–Пеккера для предварительной обработки данных в задачах распознавания движений «мыши». Полученные результаты могут найти применение в разработке более интуитивно понятных и адаптивных пользовательских интерфейсов.

Предложены также направления для дальнейших исследований, включая оптимизацию параметров алгоритма для различных типов движений и исследование возможности его комбинирования с другими методами машинного обучения.

Ключевые слова: аутентификация, биометрическая идентификация, удалённая работа, дистанционное обучение, алгоритм Дугласа–Пеккера, предобработка данных, нейросеть, HID-устройство, траектория движений «мыши», оптимизация данных.

ВВЕДЕНИЕ

В современном мире цифровые технологии проникают во все аспекты человеческой деятельности, включая образование и трудовую деятельность. С 2019 года, когда в ответ на глобальные вызовы мировые образовательные системы активно начали переходить на дистанционные формы обучения, возникла острая необходимость в разработке и внедрении надежных технологий идентификации и аутентификации. Эти технологии необходимы для обеспечения подлинности выполнения работ и защиты от фальсификации академических достижений, особенно в контексте получения высшего образования в соответствии с укрупненной группой специальностей и направлений (УГСН) 10.00.00 – Информационная безопасность, где лабораторные и практические работы играют ключевую роль в учебном процессе.

В ответ на увеличивающуюся потребность в удаленной аутентификации пользователей особое внимание было уделено разработке методов биометрической идентификации. Прокторинг с использованием видеотрансляций и распознавание HID-устройств (Human Interface Devices) стали наиболее популярными подходами. Среди HID-устройств манипуляторы типа «мышь» выделяются благодаря их устойчивости к попыткам подделки и подмены, что делает их предпочтительным выбором для систем аутентификации. Тем не менее, проблема оптимизации потока входных данных от этих устройств остается актуальной. Во-первых, большой объем данных может привести к переобучению нейронных сетей, являющихся ядром системы распознавания. Во-вторых, высокие требования к пропускной способности сети могут ограничить широкое внедрение технологий биометрической аутентификации в дистанционное образование.

Одним из решений указанных проблем является использование алгоритма Дугласа–Пеккера¹ для предварительной обработки данных траекторий жестов мыши. Этот алгоритм позволяет существенно уменьшить количество точек в траекториях, тем самым упрощая их и сохраняя при этом ключевые особенности движений. Такой подход не только облегчает нагрузку на сетевые и вычислительные ресурсы, но и повышает точность и эффективность последующего распознавания движений с помощью нейронных сетей.

В статье представлен обзор существующих методов аутентификации, проанализирована актуальность проблемы биометрической идентификации в условиях дистанционного образования и работы и обоснован выбор алгоритма Дугласа–Пеккера как оптимального решения для предварительной обработки данных движений «мыши». Особое внимание уделено экспериментальной проверке эффективности предложенного подхода и его потенциалу для повышения надежности и удобства систем дистанционной аутентификации.

¹ https://rosettacode.org/wiki/Ramer-Douglas-Peucker_line_simplification

ОБЗОР ЛИТЕРАТУРЫ

В области биометрической аутентификации и распознавания проведено множество исследований, охватывающих различные аспекты от общих подходов к биометрии до конкретных приложений. В данном обзоре литературы мы рассмотрим научные работы, которые представляют значимый вклад в развитие названной области, начиная от общих обзоров биометрических систем безопасности и заканчивая специфическими методами обработки данных и их применением.

В статье [1] приведён обзор биометрических подходов к аутентификации, охватывающий широкий спектр технологий и подходов. Эта работа служит введением в область биометрической аутентификации, представляя различные методы и их применение.

Обзор, выполненный в [2], представляет собой всесторонний анализ производительности, безопасности и схем защиты шаблонов биометрии в системах аутентификации. Это исследование содержит критический взгляд на существующие подходы и предлагает направления для усиления безопасности биометрических систем.

В работе [3] представлен обширный обзор безопасности биометрической аутентификации, рассмотрены основные концепции и вызовы, стоящие перед системами биометрической аутентификации. Это исследование формирует фундаментальную базу для понимания текущего состояния технологий в области биометрии и подчеркивает важность разработки надежных методов аутентификации.

В [4] проведено исследование уязвимости биометрических систем аутентификации на основе данных с клавиатуры и компьютерной «мыши» перед атаками с использованием техник «черного ящика» и специфических для домена. Это исследование подчеркивает важность разработки устойчивых к атакам систем биометрической аутентификации.

Авторы исследования [5] предлагают обширный обзор методов ненавязчивой активной аутентификации пользователя в биометрии, акцентируя внимание на комфорте пользователя и невмешательстве в его деятельность при обеспечении безопасности.

Далее, в [6, 7] проведён углубленный анализ методов непрерывной аутентификации, использующих биометрические данные. Эти работы акцентируют внимание на важность разработки систем, способных обеспечить постоянную и надежную аутентификацию пользователя в реальном времени.

В области анализа поведенческих биометрических данных, особенно в контексте использования данных компьютерной «мыши», значительный вклад внесли работы [8, 9]. Эти исследования фокусируются на анализе потоковых данных кликов «мыши» как средства для непрерывной аутентификации пользователя.

Исследования [10, 11] дополнительно подчеркивают потенциал поведенческих биометрических данных, полученных с помощью «мыши», для создания надежных систем аутентификации.

Работы [12, 13] иллюстрируют применение машинного и глубокого обучения для анализа динамики движений «мыши», подчеркивая значимость этих подходов для улучшения точности и надежности биометрической аутентификации.

В контексте образовательных технологий исследования [14–16] раскрывают возможности использования биометрической аутентификации для обеспечения честности и подлинности образовательного процесса в дистанционных условиях.

Исследование [17] представляет собой углубленный анализ алгоритма Дугласа–Пеккера, нацеленный на определение оптимальных значений его параметров для систем распознавания онлайн-рукописного ввода. Эта работа значительно обогащает понимание применения алгоритма для упрощения данных, что непосредственно связано с областью биометрической аутентификации.

В статье [18] рассмотрена разработка гибкой системы для отслеживания движений компьютерной «мыши» и оценки поведения, что предоставляет ценные данные для анализа поведенческих биометрий. Это исследование расширяет горизонты использования биометрических данных, полученных с помощью устройств ввода, для аутентификации.

Отметим работы [19, 20], которые специализируются на разработке и анализе инструментов для верификации студентов и предварительной обработки данных с манипуляторов «мышь» для использования в анализе поведенческих биометрий. Эти исследования предлагают конкретные методы и инструменты для улучшения точности и эффективности систем аутентификации в образовательной среде.

Приведенный обзор литературы подчеркивает многоуровневый подход к разработке и внедрению биометрических систем аутентификации, от теоретических основ до конкретных технологических решений, и иллюстрирует широкий спектр исследований, направленных на повышение безопасности, надежности и доступности биометрической аутентификации в различных областях применения.

МАТЕРИАЛЫ И МЕТОДЫ

Для проведения исследования использовались стандартные HID-устройства («мыши»), подключаемые к персональным компьютерам испытуемых. Данные движений «мыши» собирались в реальном времени в ходе выполнения типовых задач, имитирующих действия пользователя в процессах дистанционной работы или обучения. Сбор данных осуществлялся с помощью специально разработанного программного обеспечения RemoteTopology, регистрирующего движения «мыши» с высокой точностью.

Алгоритм Дугласа–Пеккера — это метод уменьшения количества точек в ломаной линии без значительной потери формы. Алгоритм определяет точки, которые можно исключить, минимизируя при этом искажение исходной траектории [17]. В контексте данного исследования алгоритм применялся для упрощения траекторий жестов «мыши» с целью снижения объема данных перед их обработкой нейронными сетями.

Предобработка данных включала несколько этапов:

- Фильтрация шумов и случайных движений, не относящихся к целенаправленным.
- Применение алгоритма Дугласа–Пеккера для уменьшения количества точек в траекториях движений.

- Нормализация данных для унификации входных параметров для обучения нейронных сетей.

В качестве ядра системы распознавания использовались нейронные сети, обученные на данных с упрощенными и неупрощенными траекториями жестов, для сравнения результатов. Подбор архитектуры нейронных сетей, их параметров и гиперпараметров осуществлялся на основе предварительных экспериментов с целью максимизации точности распознавания движений.

Эффективность алгоритма Дугласа–Пеккера оценивалась по следующим критериям:

- Уменьшение объема данных: измерялось процентное сокращение количества точек в траекториях движений после применения алгоритма.
- Точность распознавания жестов: сравнивалась точность идентификации движений нейронными сетями до и после упрощения траекторий.
- Время обучения нейронных сетей: измерялось время, необходимое для обучения сетей на упрощенных и неупрощенных данных.

Эксперименты проводились в контролируемой среде с активным участием группы испытуемых. Участникам были предложены задания, специально разработанные для имитации реальных сценариев использования. Проведение сравнительного анализа результатов обучения нейронных сетей на исходных и обработанных алгоритмом Дугласа–Пеккера данных позволило детально оценить влияние этого метода на эффективность системы биометрической аутентификации, подчеркивая его значимость в реальных сценариях применения.

РЕЗУЛЬТАТЫ

Эксперимент проводился с участием студентов и молодых профессионалов, активно вовлеченных в использование компьютерных технологий в своей повседневной деятельности. Всего было 50 испытуемых, среди кото-

рых 30 мужчин и 20 женщин в возрасте от 18 до 35 лет. Перед началом эксперимента каждому участнику была предоставлена информация о целях исследования, и они дали свое согласие на участие.

Модель нейронной сети была выбрана на основе экспериментальной оценки нескольких архитектур: KNN (k-nearest neighbours, k-ближайших соседей), CNN (convolutional neural networks, свёрточные нейронные сети), RNN (recurrent neural network, рекуррентные нейронные сети).

Результаты эксперимента представлены в таблице 1.

Таблица 1. Результаты эксперимента

Параметр	До применения алгоритма	После применения алгоритма
Среднее количество точек в траектории	1584	634
Средняя точность распознавания, %	70	82
Среднее время обучения, мин	120	84

Результаты демонстрируют значительное улучшение в эффективности системы распознавания жестов «мыши» после применения алгоритма Дугласа–Пеккера. Уменьшение количества точек в траекториях на 60% привело к сокращению времени обучения на 30% и увеличению точности распознавания на 12%.

ОБСУЖДЕНИЕ

Результаты проведенных экспериментов ясно показывают, что применение алгоритма Дугласа–Пеккера для предварительной обработки данных траекторий «мыши» в рамках систем биометрической аутентификации имеет огромные преимущества. Уменьшение объема данных не только облегчает их обработку и сокращает время обучения нейронных сетей, но и

существенно повышает точность распознавания, что крайне важно для эффективности таких систем.

Точность распознавания движений играет ключевую роль в системах онлайн-аутентификации, и увеличение этого показателя на 12% может значительно повлиять на надежность и безопасность процессов идентификации. Это подчеркивает важность выбора подходящих методов предварительной обработки данных при разработке биометрических систем идентификации.

Кроме того, уменьшение времени обучения нейронных сетей также является важным результатом, поскольку позволяет более эффективно использовать вычислительные ресурсы. Это особенно актуально в условиях ограниченных сетевых и временных ресурсов, которые характерны для дистанционного обучения и работы.

Однако важно также обсудить потенциальные ограничения проведенного исследования. Например, необходимо изучить влияние разнообразия жестов и их сложности на эффективность применения алгоритма Дугласа–Пеккера. Также важно рассмотреть возможности дальнейшего улучшения точности распознавания путем оптимизации параметров алгоритма и комбинирования его с другими методами предварительной обработки данных и машинного обучения.

Результаты, приведенные выше, открывают новые горизонты для дальнейших исследований в области биометрической аутентификации и разработки пользовательских интерфейсов, направленных на улучшение взаимодействия между пользователем и системой в условиях дистанционной работы и обучения.

СПИСОК ЛИТЕРАТУРЫ

1. *Yusuf N. et al.* A survey of biometric approaches of authentication // *International Journal of Advanced Computer Research*. 2020. Vol. 10. No. 47. P. 96–104.

2. *Sarkar A., Singh B.K.* A review on performance, security and various biometric template protection schemes for biometric authentication systems // *Multimedia Tools and Applications*. 2020. Vol. 79. No. 37. P. 27721–27776.
3. *Alwahaishi S., Zdrálek J.* Biometric authentication security: an overview // *2020 IEEE International Conference on Cloud Computing in Emerging Markets (CCEM)*. IEEE, 2020. P. 87–91.
4. *López C. et al.* Adversarial attacks against mouse-and keyboard-based biometric authentication: black-box versus domain-specific techniques // *International Journal of Information Security*. 2023. Vol. 22. No. 6. P. 1665–1685.
5. *Thomas P.A., Preetha Mathew K.* A broad review on non-intrusive active user authentication in biometrics // *Journal of Ambient Intelligence and Humanized Computing*. 2023. Vol. 14. No. 1. P. 339–360.
6. *Dahia G., Jesus L., Pamplona Segundo M.* Continuous authentication using biometrics: An advanced review // *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*. 2020. Vol. 10. No. 4. P. e1365.
7. *Ryu R. et al.* Continuous multimodal biometric authentication schemes: a systematic review // *IEEE Access*. 2021. Vol. 9. P. 34541–34557.
8. *Almalki S., Assery N., Roy K.* An empirical evaluation of online continuous authentication and anomaly detection using mouse clickstream data analysis // *Applied Sciences*. 2021. Vol. 11. No. 13. P. 6083.
9. *Almalki S., Chatterjee P., Roy K.* Continuous authentication using mouse clickstream data analysis // *Security, Privacy, and Anonymity in Computation, Communication, and Storage: SpaCCS 2019 International Workshops, Atlanta, GA, USA, July 14–17, 2019, Proceedings 12*. Springer International Publishing, 2019. P. 76–85.
10. *Jorgensen Z., Yu T.* On mouse dynamics as a behavioral biometric for authentication // *Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security*. 2011. P. 476–482.
11. *Sayed B. et al.* Biometric authentication using mouse gesture dynamics // *IEEE systems journal*. 2013. Vol. 7. No. 2. P. 262–274.

12. *Siddiqui N. et al.* Machine and deep learning applications to mouse dynamics for continuous user authentication // *Machine Learning and Knowledge Extraction*. 2022. Vol. 4. No. 2. P. 502–518.
13. *Zhang Y.G. et al.* Trustworthy interaction model: continuous authentication using time–frequency joint analysis of mouse biometrics // *Behaviour & Information Technology*. 2024. P. 1–18.
14. *Fenu G., Marras M., Boratto L.* A multi-biometric system for continuous student authentication in e-learning platforms // *Pattern Recognition Letters*. 2018. Vol. 113. P. 83–92.
15. *Gao Q.* Biometric authentication to prevent e-cheating // *International Journal of Instructional Technology and Distance Learning*. 2012. Vol. 9. No. 2. P. 3–14.
16. *Hernandez-Ortega J. et al.* edBB: Biometrics and behavior for assessing remote education // *arXiv preprint arXiv:1912.04786*. 2019.
17. *Abuzaraida M.A., Jebriel S.M.* The detection of the suitable reduction value of Douglas–Peucker algorithm in online handwritten recognition systems // *2015 IEEE International Conference on Service Operations and Logistics, And Informatics (SOLI)*. IEEE, 2015. P. 82–87.
18. *Fong T. et al.* PyMouseTracks: Flexible Computer Vision and RFID-Based System for Multiple Mouse Tracking and Behavioral Assessment // *eNeuro*. 2023. Vol. 10. No. 5.
19. *Uymin A.* Instruments for student verification and assessment of his emotional and psychological state during remote work // *Norwegian Journal of development of the International Science*. 2022. No. 96. P. 98–101.
20. *Uymin A.* Preprocessing data from the mouse manipulator for use in behavioral biometrics analysis // *Norwegian Journal of Development of the International Science*. 2022. No. 85. P. 53–58.

APPLICATION OF THE DOUGLAS-PEUCKER ALGORITHM IN ONLINE AUTHENTICATION OF REMOTE WORK TOOLS FOR SPECIALIST TRAINING IN HIGHER EDUCATION GROUP OF SCIENTIFIC SPECIALTIES (UGSN) 10.00.00

A. G. Uymin¹ [0000-0003-1572-5488], **V. S. Grekov**² [0009-0006-4067-4976]

^{1,2}*National University of Oil and Gas «Gubkin University»*

¹au-mail@ya.ru, ²grekov.vs.work@gmail.com

Abstract

In today's world, digital technologies are penetrating all aspects of human activity, including education and labor. Since 2019, when, in response to global challenges, the world's educational systems have actively started to shift to distance learning, there has been an urgent need to develop and implement reliable identification and authentication technologies. These technologies are necessary to ensure the authenticity of work and protection from falsification of academic achievements, especially in the context of higher education in accordance with the group of specialties and directions (USGS) 10.00.00 - Information Security, where laboratory and practical work play a key role in the educational process.

The problem lies in the need to optimize the flow of incoming data, which, first, can affect the retraining of the neural network core of the recognition system, and second, impose excessive requirements on the network's bandwidth. To solve this problem, efficient preprocessing of gesture data is required to simplify their trajectories while preserving the key features of the gestures.

This article proposes the use of the Douglas–Peucker algorithm for preliminary processing of mouse gesture trajectory data. This algorithm significantly reduces the number of points in the trajectories, simplifying them while preserving the main shape of the gestures. The data with simplified trajectories are then used to train neural networks.

The experimental part of the work showed that the application of the Douglas–Peucker algorithm allows for a 60% reduction in the number of points in the trajectories, leading to an increase in gesture recognition accuracy from

70% to 82%. Such data simplification contributes to speeding up the neural networks' training process and improving their operational efficiency.

The study confirmed the effectiveness of using the Douglas–Peucker algorithm for preliminary data processing in mouse gesture recognition tasks. The article suggests directions for further research, including the optimization of the algorithm's parameters for different types of gestures and exploring the possibility of combining it with other machine learning methods. The obtained results can be applied to developing more intuitive and adaptive user interfaces.

Keywords: *authentication, biometric identification, remote work, distance learning, Douglas–Peucker algorithm, data preprocessing, neural network, HID devices, mouse gesture trajectories, data optimization.*

REFERENCES

1. Yusuf N. et al. A survey of biometric approaches of authentication // International Journal of Advanced Computer Research. 2020. Vol. 10. No. 47. P. 96–104.
2. Sarkar A., Singh B.K. A review on performance, security and various biometric template protection schemes for biometric authentication systems // Multimedia Tools and Applications. 2020. Vol. 79. No. 37. P. 27721–27776.
3. Alwahaishi S., Zdrálek J. Biometric authentication security: an overview // 2020 IEEE International Conference on Cloud Computing in Emerging Markets (CCEM). IEEE, 2020. P. 87–91.
4. López C. et al. Adversarial attacks against mouse-and keyboard-based biometric authentication: black-box versus domain-specific techniques // International Journal of Information Security. 2023. Vol. 22. No. 6. P. 1665–1685.
5. Thomas P.A., Preetha Mathew K. A broad review on non-intrusive active user authentication in biometrics // Journal of Ambient Intelligence and Humanized Computing. 2023. Vol. 14. No. 1. P. 339–360.
6. Dahia G., Jesus L., Pamplona Segundo M. Continuous authentication using biometrics: An advanced review // Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery. 2020. Vol. 10. No. 4. P. e1365.

7. *Ryu R. et al.* Continuous multimodal biometric authentication schemes: a systematic review // *IEEE Access*. 2021. Vol. 9. P. 34541–34557.
8. *Almalki S., Assery N., Roy K.* An empirical evaluation of online continuous authentication and anomaly detection using mouse clickstream data analysis // *Applied Sciences*. 2021. Vol. 11. No. 13. P. 6083.
9. *Almalki S., Chatterjee P., Roy K.* Continuous authentication using mouse clickstream data analysis // *Security, Privacy, and Anonymity in Computation, Communication, and Storage: SpaCCS 2019 International Workshops, Atlanta, GA, USA, July 14–17, 2019, Proceedings 12*. Springer International Publishing, 2019. P. 76–85.
10. *Jorgensen Z., Yu T.* On mouse dynamics as a behavioral biometric for authentication // *Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security*. 2011. P. 476–482.
11. *Sayed B. et al.* Biometric authentication using mouse gesture dynamics // *IEEE systems journal*. 2013. Vol. 7. No. 2. P. 262–274.
12. *Siddiqui N. et al.* Machine and deep learning applications to mouse dynamics for continuous user authentication // *Machine Learning and Knowledge Extraction*. 2022. Vol. 4. No. 2. P. 502–518.
13. *Zhang Y.G. et al.* Trustworthy interaction model: continuous authentication using time–frequency joint analysis of mouse biometrics // *Behaviour & Information Technology*. 2024. P. 1–18.
14. *Fenu G., Marras M., Boratto L.* A multi-biometric system for continuous student authentication in e-learning platforms // *Pattern Recognition Letters*. 2018. Vol. 113. P. 83–92.
15. *Gao Q.* Biometric authentication to prevent e-cheating // *International Journal of Instructional Technology and Distance Learning*. 2012. Vol. 9. No. 2. P. 3–14.
16. *Hernandez-Ortega J. et al.* edBB: Biometrics and behavior for assessing remote education // *arXiv preprint arXiv:1912.04786*. 2019.
17. *Abuzaraida M.A., Jebriel S.M.* The detection of the suitable reduction value of Douglas–Peucker algorithm in online handwritten recognition systems // *2015 IEEE International Conference on Service Operations and Logistics, And Informatics (SOLI)*. IEEE, 2015. P. 82–87.

18. *Fong T. et al.* PyMouseTracks: Flexible Computer Vision and RFID-Based System for Multiple Mouse Tracking and Behavioral Assessment // *eNeuro*. 2023. Vol. 10. No. 5.

19. *Uymin A.* Instruments for student verification and assessment of his emotional and psychological state during remote work // *Norwegian Journal of development of the International Science*. 2022. No. 96. P. 98–101.

20. *Uymin A.* Preprocessing data from the mouse manipulator for use in behavioral biometrics analysis // *Norwegian Journal of Development of the International Science*. 2022. No. 85. P. 53–58.

СВЕДЕНИЯ ОБ АВТОРАХ



УЙМИН Антон Григорьевич – ст. преподаватель, федеральное государственное автономное образовательное учреждение высшего образования «Российский государственный университет нефти и газа (Национальный исследовательский университет) имени И.М. Губкина»

Anton Grigorievich UYMIN – Senior Lecturer, Federal State Autonomous Educational Institution of Higher Education "Gubkin Russian State University of Oil and Gas (National Research University)".

email: au-mail@ya.ru

ORCID: 0000-0003-1572-5488



ГРЕКОВ Владимир Сергеевич – ассистент, Федеральное государственное автономное образовательное учреждение высшего образования «Российский государственный университет нефти и газа (национальный исследовательский университет) имени И.М. Губкина»

Vladimir Sergeevich GREKOV – Assistant, Federal State Autonomous Educational Institution of Higher Education "Gubkin Russian State University of Oil and Gas (National Research University)".

email: grekov.vs.work@gmail.com

ORCID: 0009-0006-4067-4976

Материал поступил в редакцию 30 марта 2024 г.