Автоматизация и моделирование в проектировании и управлении. 2024. № 1 (23). С. 58-64.
ISSN 2658-3488 print, ISSN 2658-6436 online
Automation and modeling in design and management. 2024. № 1 (23). P. 58-64.

Управление в организационных системах

Научная статья
Статья в открытом доступе
УДК 004.056.53
doi: 10.30987/2658-6436-2024-1-58-64

МЕТОДИКА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ТРАНЗАКЦИЙ НА ОСНОВЕ ИСПОЛЬЗОВАНИЯ АНТИФРОД-СИСТЕМЫ

Любовь Евгеньевна Батюкова[1], Татьяна Владимировна Карлова[2]
[1] Московский государственный технологический университет «СТАНКИН», г. Москва, Россия
[2] Институт конструкторско-технологической информатики Российской академии наук, г. Москва, Россия
[1] lyubabatyukova@yandex.ru
[2] karlova-t@yandex.ru

Аннотация. *Целью данной научной работы является предложение методики обеспечения безопасности транзакций в коммерческих структурах с использованием антифрод-системы. Статья посвящена анализу актуальных проблем в сфере информационной безопасности в финансовом секторе, а именно применению антифрод-систем, призванных верно определять нелегитимные платежные операции для их своевременного предотвращения. Рассмотрен вопрос целесообразности использования машинного обучения в антифрод-системах как инструмента, отвечающего за повышение точности выполнения проверок в процессах работы с большими данным. Новизна исследования заключается в предложении схемы взаимодействия подсистем антифрод-механизмов с использованием ручной проверки экспертом, что подходит для организаций, которым необходимо вручную просматривать каждый установленный случай Интернет-мошенничества. Результатом работы являются рекомендации для подготовки к выбору антифрод-системы, схемы взаимодействия подсистем антифрод-программы.*

Ключевые слова: антифрод, машинное обучение, информационная безопасность, интернет транзакции
Для цитирования: Батюкова Л.Е., Карлова Т.В. Методика обеспечения безопасности транзакций на основе использования антифрод-системы // Автоматизация и моделирование в проектировании и управлении. 2024. №1 (23). С. 58-64. doi: 10.30987/2658-6436-2024-1-58-64.

Original article
Open Access Article

METHODOLOGY FOR ENSURING THE TRANSACTION SECURITY BASED ON USING AN ANTI-FRAUD SYSTEM

Lyubov E. Batyukova[1], Tatyana V. Karlova[2]
[1]Moscow State University of Technology «STANKIN», Moscow, Russia
[2]Institute for Design-Technological Informatics of the Russian Academy of Sciences, Moscow, Russia
[1] lyubabatyukova@yandex.ru
[2] karlova-t@yandex.ru

Abstract. *The aim of this scientific work is to propose a methodology for ensuring the security of transactions in commercial structures using an anti-fraud system. The article is devoted to analyzing the current problems in the field of information security in the financial sector, namely the use of anti-fraud systems designed to correctly identify illegitimate*

payment transactions for their timely prevention. The paper considers the feasibility question using machine learning in anti-fraud systems as a tool responsible for increasing the accuracy of checks while working with big data. The novelty of the study lies in proposing a scheme for the subsystem interaction of anti-fraud mechanisms using an expert's manual verification, which is suitable for organizations that need to manually review each identified case of the Internet fraud. The work results in recommendations for preparing for the selection of an anti-fraud system, and a scheme for the subsystem interaction of the anti-fraud program.

Keywords: antifraud, machine learning, information security, Internet transactions

For citation: Batyukova L.E., Karlova T.V. Methodology for Ensuring the Transaction Security Based on Using an Anti-Fraud System. Automation and modeling in design and management, 2024, no. 1 (23). pp. 58-64. doi: 10.30987/2658-6436-2024-1-58-64.

Введение

Рост цифровизации способствует не только развитию технологий и удобству управления всеми сферами общественной жизни, но и увеличивает риск мошеннических действий в Интернете, что побуждает многие организации к тщательному продумыванию вопроса безопасности. Наиболее стандартным решением проблемы мошенничества в сфере информационных технологий являются антифрод-системы, призванные выявлять нелегитимные операции в финансовых, телекоммуникационных и других коммерческих структурах. В статье предложена методика поддержки защиты от мошеннических транзакций на основе использования антифрод-системы с применением инструментов машинного обучения, позволяющая вовремя оказывать противодействие Интернет-злоумышленникам в корпоративном бизнесе.

Постановка задачи обеспечения защиты от несанкционированных действий в коммерческом секторе

В 2022 году объем украденных средств злоумышленниками составил 14,2 млрд рублей, что больше почти на 5 %, по сравнению с показателями 2021 года. Основной объем похищенных средств приходится на взлом мобильных приложений банка или личных кабинетов. Около 20 % были украдены посредством оплаты товаров и услуг в Интернете. Наименьший процент приходится на использование банкоматов без согласия клиента. Статистика показывает, что количество мошеннических транзакций растет ежегодно. Это обусловлено, в первую очередь, увеличением рынка безналичных платежей. Кроме того, большой проблемой с точки зрения безопасности, является сервис мгновенных переводов, благодаря которому за несколько секунд можно перевести крупные суммы денежных средств преступнику.

Рис. 1. Процентное распределение похищенных денежных средств в 2022 году
Fig. 1. Percentage distribution of stolen funds in 2022

Возврат денежных средств жертвам мошенников при этом составил только 4,4 % от общей украденной суммы. Такой низкий процент объясняется тем, что мошенники в

большинстве случаев используют приемы социальной инженерии, суть которых заключается в том, что пострадавший, находясь под психологическим воздействием, добровольно переводит мошенникам деньги, либо сообщает им банковские сведения, там самым предоставляя доступ в личный кабинет банка или приложения.

Такая статистика побуждает банки, интернет-магазины, государственные учреждения прилагать усилия по безопасности своих клиентов. Основным способом борьбы с мошенниками в сфере информационных технологий являются системы мер по предотвращению и борьбе с мошенничеством – антифрод-системы.

Подготовка к внедрению антифрод-системы

Экономическая целесообразность внедрения антифрод-систем в банковских и коммерческих предприятиях, как правило, не подвергается сомнению. Инструменты для противодействия мошенничеству в финансовом секторе способны значительно снизить ущерб организаций и их клиентов от нелегитимных операций. Для того, чтобы определиться с финальным способом защиты компаниям необходимо ответить на массу вопросов.

Первый вопрос заключается в выборе типа антифрод-системы: транзакционный или сессионный. Транзакционные антифрод-системы характеризуются автоматической проверкой конкретной транзакции, в ходе которой происходит оценка рисков с целью защиты системы от мошенничества. Примером может служить оплата покупки или перевод денег другому человеку. В данном случае система оценивает транзакцию по определенным параметрам и выносит решение о ее блокировке, отправке ответственному в качестве подозрительного действия, либо успешном пропуске транзакции.

Немало важным преимуществом антифрод-системы является предотвращение мошеннических платежей, до того как они были совершены. Для этого используются сессионные антифрод-инстурменты, выявляющие нетипичное поведение пользователя приложения или сайта. Системы сессионного типа концентрируются на проверке действий пользователя во время конкретной активности, т.е. система оценивает действия как стандартное поведение пользователя или нетипичное. В качестве атипичного поведения может быть расценена нехарактерная траектория движения курсора или изменение скорости набора текста. При большом количестве отклонений от стандартного поведения пользователя система выносит решение о блокировке. Кроме того, существует смешанный транзакционно-сессионный тип антифрод-системы, сочетающий черты обоих типов.

Второй вопрос заключается в выборе поставки антифрод-системы. Существует возможность облачного решения, отличительной особенностью которого является значительно более короткая скорость подключения, при этом информация передается в зашифрованном виде с помощью хэширования. Есть вариант локального размещения у заказчика, для этого со стороны компании необходима полноценная инфраструктура для функционирования антифрод-системы, а также специалисты, которые обеспечат работу систему. Затраты для компании в данном случае выше, но преимущество заключается в возможности самостоятельно контролировать информацию.

Важным фактором при выборе антифрод-системы является необходимость использования истории данных. Транзакции или данные хранятся в базе данных, и чем больше параметров и правил используется при проверке, тем сильнее нагрузка на базу, что обеспечивает спад ее производительности. Поэтому для увеличения скорости работы антифрод-системы используют технологию рестроспективности.

При выборе антифрода нужно учесть необходимость работы с внешними источниками данных. Для банковской сферы важно иметь возможность взаимодействовать с внешними источниками данных, в частности, для проверки черных списков Банка России, что позволит обладать актуальной информацией по списку лиц, уличенных в мошеннических действиях. Организациям, планирующим внедрение антифрод-системы, необходимо понимать частоту обновления программы. Чтобы правила соответствовали актуальным видам угроз, важно использовать свежие данные о мошенничестве.

Целесообразность использования машинного обучения в антифрод-системе

Современные антифрод-системы помимо стандартных правил содержат в себе модуль машинного обучения. Этот модуль способен создать профиль пользователя на основе статистических данных и оценивать его действия как типичные или нетипичные. На основе статистических и ретроспективных данных составляется некий портрет клиента – образ его стандартных действий при совершении транзакции. В случае если система видит, что совершаемые действия нехарактерны для пользователя, то маркирует платеж как подозрительный.

Основными причинами, способствующими применению машинного обучения в антифрод-системах, способствуют следующие факторы:

1. Создание системы правил требует больших временных затрат аналитиков: необходимо собрать все возможные данные о транзакции, преобразовать и обработать их, провести анализ для максимально верной оценки веса каждого параметра. В ходе данного процесса некоторые данные могут быть не упущены. Кроме того, базовых атрибутов вроде суммы и времени транзакции бывает недостаточно для поиска закономерностей. Поэтому из имеющихся данных аналитики формируют дополнительные сложносоставные атрибуты, что может повысить вероятность ошибки. Очевидный плюс машинного обучения в данном случае заключается в том, что блок машинного обучения в данном случае становится неким страхующим звеном, при помощи которого можно покрыть те области, которые недоступны для анализа статическими правилами. Также Machine Learning позволит сократить ручной труд и повысить объективность оценки риска.

2. Данные в любой организации могут меняться с течением времени: создаются новые продукты, меняющие стиль поведения пользователей, появляются новые данные, старые данные теряют актуальность. Машинное обучение позволит вовремя обнаружить изменение в данных и сократить затраты на обновление правил. Таким образом, столкнувшись с какими-либо изменениями в данных компаниям необязательно сразу создавать новую систему правил.

3. Работа с большими данными также способствует использованию машинного обучения. Как правило, когда речь идет о транзакциях в финансовом секторе, их число может превышать миллионы. Методы Machine learning эффективны при больших объёмах поступающей информации, так как снижается время на разбор операций для ручного анализа. Также решения на базе машинного обучения совершенствуются со временем, по мере обработки новых данных и обучении новой выборки.

4. Экспертами было отмечено, что использование машинного обучения способствуют уменьшению ложноположительной ошибки, т.е. снижает риск неверного решения о блокировке транзакции, которая не является фродом. Например, пользователь совершает действия, которые похожи на мошеннические, однако в случае если для конкретного клиента это стандартная ситуация, то антифрод-система, благодаря данным машинного обучения, не разметит транзакцию как фрод. Также машинное обучение помогает в обратном случае: когда транзакция, с точки зрения локальных фильтров, не является подозрительной, но по нехарактерным для пользователя действиям понятно, что это злоумышленник. В этом случае антифрод обычно приостанавливает операцию для более детального разбора. Чем меньше вероятность ложноположительной ошибки, тем меньше трудозатрат на проверку и дальнейшие разбирательства с пользователем, которые могут повлиять на репутацию компании. Кроме того, в правилах сложно учитывать внезапные сезонные всплески или органические изменения поведения, которые алгоритмы машинного обучения способны находить и учитывать.

5. Машинное обучение использует более сложные и современные инструменты анализа, чем те, что используется в системе правил. Алгоритмы способны находить аномальные паттерны, которые сложно обнаружить ручным трудом специалистов. Результат работы машинного обучения совсем не обязательно будет определяющим – в правилах антифрода есть множество статичных критериев, по которым принимается решение. Тем не менее, результаты этой дополнительной проверки позволяют существенно повысить точность обнаружения мошенника.

На рис.2 представлена схема взаимодействия подсистем анифрод-сервиса.

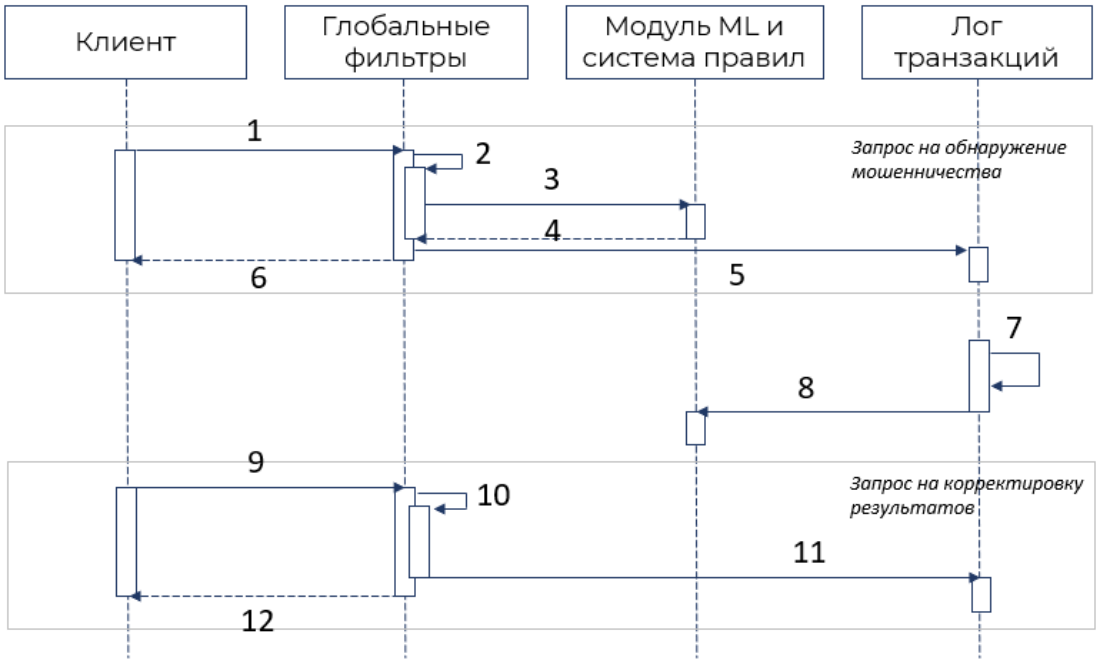

Рис. 2. Взаимодействие подсистем антифрод-сервиса
Fig. 2. Interaction of antifraud service subsystems

На первом шаге происходит отправка запроса с информацией о платеже от пользователя.

На втором шаге запрос подвергается проверке через глобальные фильтры и валидность введенных платежных данных.

Далее при положительном вердикте на шаге *2* запрос проверяется через внутреннюю систему правил, разработанную специально для организации под ее характерные особенности. Также на третьем шаге модуль машинного обучения выносит решение на основе данных.

В результате на четвертом этапе выносится вердикт о статусе транзакции: успешно или заблокировано.

Финальный результат сохраняется в базе данных для дальнейшего обучения модели и возможности использования исторических данных для будущего анализа.

На шестом шаге пользователь получает ответ об исходе транзакции.

Далее происходит переобучение модели, обновление обучающей выборки.

Остальные (*9 – 12*) шаги опциональны: клиент в случае несогласия с вынесенным вердиктом может инициировать отправку запроса в техническую поддержку, где эксперт повторно анализирует результат на более глубоком уровне и принимает финальное решение о разблокировке или сохранении текущего статуса платежа.

На рис. 3 предложена схема взаимодействия подсистем с учетом дополнительной ручной проверки экспертом.

В данном случае добавлен еще один блок – проверка экспертом. В результате на четвертом этапе выносится вердикт о статусе транзакции: успешно или заблокировано до проверки специалистом. В случае, если подозрений о фроде нет, успешный статус транзакции отображается клиенту. Однако если система распознала операцию как фрод, то информация уходит к специалисту, который погружается в полученную от предыдущих блоков информацию (шаг *7*) и принимает финальное решение. Результат проверки экспертом также сохраняется в хранилище транзакций и направляется пользователю, совершившему транзакцию. Дальнейшие шаги аналогичны процессу, изображенному на рис. 2.

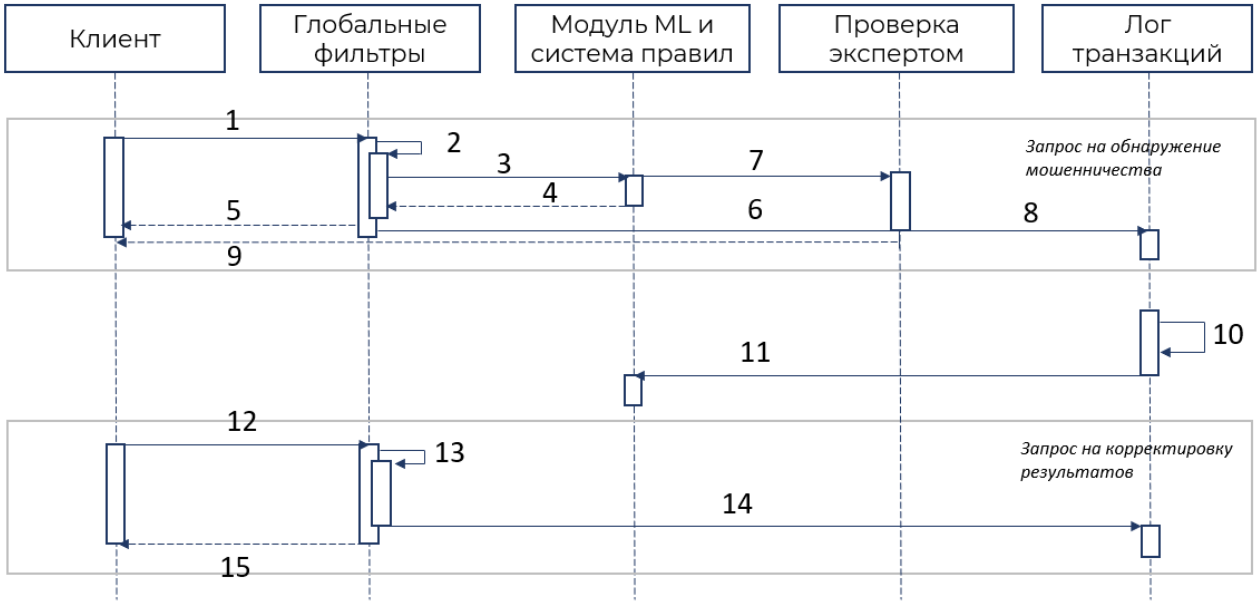

Рис. 3. Взаимодействие подсистем антифрод-сервиса с участием эксперта
Fig 3. Interaction of anti-fraud service subsystems with the participation of an expert

Заключение

Для обеспечения защиты от мошеннических транзакций в информационной среде следует использовать антифрод-системы. На рынке существует множество предложений программного обеспечения с функционалом защиты от цифровых мошеннических действий. Организациям, внедряющим антифрод-систему, необходимо ответить на ряд вопросов перед принятием решения о покупке существующего на рынке коробочного решения или собственной разработке сервиса по обнаружению подозрительных транзакций.

Одним из факторов принятия решения будет выступать необходимость использования блока машинного обучения (МО). Последнее необходимо для увеличения точности нахождения подозрительных транзакций и сокращения числа ложноположительных ошибок. Другие преимущества МО заключаются в адаптивности к динамическому изменению внешних данных, использовании современных и сложных методов анализа данных, возможность применять расширенный аналитический функционал, недоступный при применении обычных статистических правил.

На основе данных о специфике организаций, их требований к полноте и тщательности анализа транзакционных операций на признаки фрода, предложены схемы взаимодействия всех подсистем антифрод-программы.

Список источников:

1. Окошкин А. Что интересует компании перед выбором антифрода: 10 главных вопросов. Anti-Malware. 2021.
2. Аминева Ю. Обзор систем противодействия банковскому мошенничеству (антифрод). Anti-Malware. 2019.
3. Сарычев Д. Выбор Анифрода, системы противодействия мошенничеству в финансовой сфере. Anti-Malware. 2021.
4. Ahramovich A. Machine Learning for fraud detection: essentials, use cases, and guidelines. Itransition. 2023.
5. Количество случаев хищения денег с банковских счетов сократилось впервые за 7 лет: итоги 2022 года, Банк России: официальный сайт. 2023. https://cbr.ru/press/event/?id=14544

References:

1. Okoshkin A. What Companies are Interested in Before Choosing an Antifraud: 10 Main Questions. Anti-Malware; 2021.
2. Amineva Yu. Review of Systems for Combating Bank Fraud (Anti-Fraud). Anti-Malware; 2019.
3. Sarychev D. Choice of Anifrod, a System for Combating Fraud in the Financial Sector. Anti-Malware; 2021.
4. Ahramovich A. Machine Learning for Fraud Detection: Essentials, Use Cases, and Guidelines. Itransition; 2023.
5. The Number of Cases of Theft of Money From Bank Accounts Has Decreased for the First Time in 7 Years: Results of 2022, Bank of Russia [Internet]. 2023. Available from: https://cbr.ru/press/event/?id=14544

6. Россияне сдали мошенникам рекордные ₽14млрд. РБК. 2023.
7. Копнин А.А., Соколова Е.В., Долгополов А.А. Методика обеспечения безопасности банковских интернет-транзакций на основе анифрод системы // International journal of professional science. 2022. №10.
8. Аксенов В.А. Роль и значение программного комплекса «Антифрод» как меры специально-криминологического характера в предупреждении мошенничества, совершенного с использованием информационно-телекоммуникационных технологий // Вестник Московского университета МВД России. 2021. №6 С.16-20.
9. Ивлиева Н.В. Актуальные проблемы противодействия хищениям денежных средств с банковских счетов физических лиц // Научный портал МВД России. 2019. №3 (47).
10. Ларионова С.Л., Ряховский Е.Э. Усовершенствование алгоритмов антифрод-системы на основе использования методов graph representation learning и сетей cyclegan // Инновации и инвестиции. 2021. №6.
11. Шавалаев Б.Э. Банковские меры противодействия преступлениям в сфере информационных технологий // Вестник Казанского юридического института МВД России. 2020. №2 (40).
12. Медведева М.Б., Васин М.М. Проблемы защиты от мошенничества в операциях с платежными картами в системе КБО физических лиц и развитие ее законодательного обеспечения // Финансовые рынки и банки. 2019. №1.
13. Радионова М.В., Корзухин А.А., Саушев Н.А. Математические методы оценки финансовых транзакций на предмет мошенничества // Вестник ПГУ. Серия: Экономика. 2021 №1.

6. Russians Handed Over a Record ₽14 Billion to scammers. RBC. 2023.
7. Kopnin A.A., Sokolova E.V., Dolgopolov A.A. Methodology for ensuring the security of banking Internet Transactions Based on an Antifraud System. International Journal of Professional Science. 2022;10.
8. Aksenov V.A. The Role and Significance of the Anti-Fraud Suite as a Special Criminological Measure to Prevent Fraud Committed Through the Use of Information and Telecommunication Technologies. Bulletin of the Moscow University of the Ministry of Internal Affairs of Russia. 2021;6:16-20.
9. Ivlieva N.V. Actual Problems of Counteraction to Embezzlement of Money From Bank Accounts of Individuals. Scientific Portal of the Russia Ministry of the Interior. 2019;3(47).
10. Larionova S.L., Ryakhovsky E.E. Improvement of Anti-Fraud System Algorithms Based on the Use of Graph Representation Learning Methods and CycleGAN. Innovations and Investments. 2021;6.
11. Shavalaev B.E. Banking Measures to Combat Information Technology Crimes. Bulletin of the Kazan Law Institute of the Ministry of Internal Affairs of Russia. 2020;2(40).
12. Medvedeva M.B., Vasin M.M. Problems of Protection Against Fraud in Operations with Payment Cards in the CBS System for Individuals and the Development of its Legislative Support. Financial Markets and Banks. 2019;1.
13. Radionova M.V., Korzukhin A.A., Saushev N.A. Mathematical Methods for Assessing Financial Transactions for Fraud. Vestnik PGU. Series: Economics. 2021;1.

Информация об авторах:

Любовь Евгеньевна Батюкова
аспирант Московского государственного технологического университета «СТАНКИН»

Татьяна Владимировна Карлова
доктор социологических наук, кандидат технических наук, профессор Институт конструкторско-технологической информатики Российской академии наук

Information about the authors:

Lyubov Evgenievna Batyukova
Postgraduate student at Moscow State University of Technology «STANKIN».

Tatyana Vladimirovna Karlova
Doctor of Sociological Sciences, Candidate of Technical Sciences, Professor of the Institute for Design-Technological Informatics of the Russian Academy of Sciences

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 11.02.2024; одобрена после рецензирования 28.02.2024; принята к публикации 03.03.2024.

The article was submitted 11.02.2024; approved after reviewing 28.02.2024; accepted for publication 03.03.2024.

Рецензент – Малаханов А.А., кандидат технических наук, доцент, Брянский государственный технический университет.

Reviewer – Malakhanov A.A., Candidate of Technical Sciences, Associate Professor, Bryansk State Technical University.