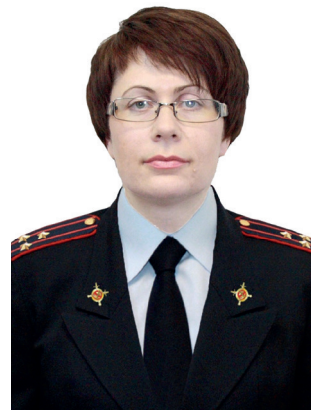


Научная статья
УДК 343.98



НЕКОТОРЫЕ АСПЕКТЫ ПРИМЕНЕНИЯ СИСТЕМ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА ПРИ ПРОТИВОДЕЙСТВИИ ЭКОНОМИЧЕСКИМ ПРЕСТУПЛЕНИЯМ

Владимир Владимирович Баранов¹, Марина Владимировна Лелетова²,

^{1,2} Академия управления МВД России
Москва, Россия,

¹ de_la_sergio@mail.ru, ² leletova@list.ru

Аннотация

Введение: экономические преступления представляют собой деяния, посягающие на экономические интересы общества и государства. В настоящее время практически все экономические преступления, так или иначе, совершаются с использованием информационно-телекоммуникационных технологий (далее – ИТТ).

Материалы и методы: в исследовании применены общенаучные (анализ, синтез) и специальные юридические методы (формально-юридический, сравнительно-правовой метод и др.). В частности:

- анализ нормативно-правовой базы Российской Федерации позволил определить правовые границы и условия использования ИИ в правоохранительной деятельности;
- системный анализ использовался для комплексного изучения возможностей и ограничений применения искусственного интеллекта при противодействии экономическим преступлениям;
- компаративный анализ отечественного опыта позволил выявить наиболее успешные практики и технологии, которые могут быть внедрены в работу органов внутренних дел Российской Федерации.

В совокупности они позволили обеспечить должный анализ проблемных вопросов применения отдельных специальных мер противодействия экономическим преступлениям, совершаемым с использованием ИТТ.

Обзор литературы: авторы учли вклад Е.В. Батуриной, Ю.В. Гаврилина, М.В. Лелетовой, Н.Э. Мартыненко, А.В. Парфенова, Т.В. Пинкевич, А.Н. Позднякова, Г.Г. Саркисян, П.В. Севастьянова, Б.А. Торопова, А.Ф. Дятловой, М.В. Свириной, А.Х. Малаева, Р.Т. Тугуз, А.К. Жаровой, Е.Е. Шемелкина в рассмотрение отдельных аспектов применения специальных мер по противодействию экономическим преступлениям, совершаемым с использованием ИТТ.

Результаты исследования: для повышения эффективности борьбы с экономическими преступлениями, в том числе, совершаемыми с использованием информационно-телекоммуникационных технологий, представляется необходимым использовать возможности систем искусственного интеллекта и аналитических систем.

При организации данной деятельности рассматриваемые системы способны решать разнообразные задачи, необходимые для предупреждения, выявления и расследования экономических преступлений. При этом представляется недостаточным урегулирование вопросов, связанных с функционированием систем ИИ, техническим и правовым описанием процесса их использования в настоящее время в России.

Обсуждение и заключение: внедрение методологии работы систем искусственного интеллекта позволит повысить эффективность предупреждения и выявления экономических преступлений, сократить время их расследования, минимизировать влияние человеческого фактора и снизить коррупционные риски при осуществлении данной деятельности. В конечном итоге, интеграция технологий искусственного интеллекта в деятельность правоохранительных органов способна существенно укрепить экономическую безопасность Российской Федерации и обеспечить устойчивость социально-экономического развития России.

Ключевые слова: системы искусственного интеллекта; экономические преступления; противодействие; предупреждение; мониторинг финансовых операций; Big Data; этика и безопасность данных

© Баранов В.В., Лелетова М.В., 2026

Для цитирования: Баранов В.В., Лелетова М.В. Некоторые аспекты применения систем искусственного интеллекта при противодействии экономическим преступлениям // Вестник Казанского юридического института МВД России. 2026. Т. 17. № 3 (65). С. 64 – 70.

Scientific article

UDC 343.98

SOME ASPECTS OF THE APPLICATION OF ARTIFICIAL INTELLIGENCE SYSTEMS IN COUNTERING ECONOMIC CRIMES

Vladimir Vladimirovich Baranov¹, Marina Vladimirovna Leletova²,

^{1,2} Academy of Management of the Ministry of Internal Affairs of Russia, Moscow, Russia,

¹ de_la_sergio@mail.ru, ² leletova@list.ru

Abstract

Introduction: economic crimes are acts that infringe on the economic interests of society and the state. Currently, virtually all economic crimes are committed, in one way or another, using information and telecommunications technologies (ITT).

Materials and Methods: the study utilized general scientific methods (analysis, synthesis) and specialized legal methods (formal legal, comparative legal, etc.).

In particular:

- An analysis of the Russian Federation's regulatory framework allowed us to determine the legal boundaries and conditions for the use of AI in law enforcement;
- A systems analysis was used to comprehensively study the potential and limitations of using artificial intelligence to combat economic crimes;
- A comparative analysis of domestic experience allowed us to identify the most successful practices and technologies that can be implemented in the work of Russian law enforcement agencies.

Taken together, these methods provided a thorough analysis of the problematic issues involved in the application of specific measures to combat economic crimes committed using artificial intelligence.

Literature review: the authors took into account the contribution of E.V. Baturina, Yu.V. Gavrilina, M.V. Leletova, N.E. Martynenko, A.V. Parfenova, T.V. Pinkevich, A.N. Pozdnyakova, G.G. Sargsyan, P.V. Sevastyanova, B.A. Toropova, A.F. Dyatlova, M.V. Svirina, A.H. Malaeva, R.T. Tuguz, A.K. Zharova, E.E. Shemelkina in considering certain aspects of the application of special measures to combat economic crimes committed using ITT.

Results: to improve the effectiveness of the fight against economic crimes, including those committed using information and telecommunications technologies, it is necessary to utilize the capabilities of artificial intelligence and analytical systems.

When organizing these activities, these systems are capable of solving a variety of tasks necessary for the prevention, detection, and investigation of economic crimes. However, the regulation of issues related to the functioning of AI systems and the technical and legal description of their use currently appears insufficient in Russia.

Discussion and Conclusions: the implementation of artificial intelligence systems will improve the effectiveness of preventing and detecting economic crimes, reduce investigation time, minimize the impact of human error, and reduce corruption risks in these activities. Ultimately, the integration of artificial

intelligence technologies into law enforcement can significantly strengthen the economic security of the Russian Federation and ensure the sustainability of Russia's socioeconomic development.

Keywords: artificial intelligence systems; economic crimes; counteraction; prevention; financial transaction monitoring; Big Data; ethics and data security

© Baranov V.V., Leletova M.V., 2026

For citation: Baranov V.V., Leletova M.V. Some Aspects of the Application of Artificial Intelligence Systems in Countering Economic Crimes. Bulletin of the Kazan Law Institute of MIA of Russia. 2026;17(3):64-70. (In Russ.).

Введение

Экономические преступления представляют собой деяния, посягающие на экономические интересы общества и государства. В настоящее время практически все экономические преступления, так или иначе, совершаются с использованием информационно-телекоммуникационных технологий (далее – ИТТ).

Обзор литературы

В разное время изучению проблем противодействия экономическим преступлениям, совершаемым с использованием ИТТ, посвящали свои исследования Е.В. Батурина [1]; Ю.В. Гаврилин, Н.Э. Мартыненко, А.В. Парфенов, Т.В. Пинкевич, А.Н. Поздняков., Г.Г. Саркисян, П.В. Севастьянов, Б.А. Торопов [2]; С.А. Грачев, А.Ю. Ушаков [3]; А.Ф. Дятлова, М.В. Свирина [4], М.В. Лелетова [5], А.Х. Малаев [6]; Р.Т. Тугуз [7]; А.К. Жарова, Е.Е. Шемелкин и др. Однако до настоящего времени остается множество проблемных вопросов, связанных с повышением эффективности противодействия экономическим преступлениям, особенно в условиях цифровизации.

Материалы и методы

В исследовании применены общенаучные (анализ, синтез) и специальные юридические методы (формально-юридический, сравнительно-правовой метод и др.).

Результаты исследования

Были рассмотрены отдельные специальные меры по противодействию экономическим преступлениям, совершаемым с использованием ИТТ.

1. Создание специализированной цифровой платформы для противодействия преступлениям, совершаемым с ИТТ. Предусмотрено Концепцией государственной системы противодействия противоправным деяниям, совершаемым с помощью информационно-коммуникационных технологий

(распоряжение Правительства РФ от 30.12.2024 № 4154-р)¹.

Возможности данной платформы заключаются в оперативной взаимной передаче информации между правоохранительными органами и Центральным банком, кредитными организациями, операторами связи и др.

2. Мониторинг и ограничение доступа к противоправным ресурсам в информационно-телекоммуникационных сетях, включая интернет.

Федеральный закон № 41-ФЗ «О создании государственной информационной системы противодействия правонарушениям, совершаемым с использованием информационных и коммуникационных технологий, и о внесении изменений в отдельные законодательные акты Российской Федерации», позволяет использовать указанную систему для оперативного предупреждения, выявления и пресечения правонарушений и преступлений, совершаемых с использованием ИТТ.

3. Развитие партнёрских отношений между институтами обеспечения безопасности, компаниями, общественностью и правоохранительными органами, в том числе для обмена информацией о новых угрозах и методах защиты от экономических преступлений, совершаемых с использованием ИТТ².

4. Повышение осведомлённости участников экономической деятельности о существующих рисках и уязвимостях, которые могут стать причиной или создать условия для совершения экономических преступлений.

5. Использование машинного обучения, искусственного интеллекта и аналитических систем для обнаружения угроз, предотвращения кибератак и обеспечения быстрой реакции на них.

Для реализации данных мер противодействия совершению экономических преступлений в настоящее время в России разработаны отечественные информационно-аналитические системы,

¹ Об утверждении Концепции государственной системы противодействия противоправным деяниям, совершаемым с использованием информационно-коммуникационных технологий: распоряжение Правительства Российской Федерации от 30.12.2024 № 4154-р. URL: <https://base.garant.ru/1569180/> (дата обращения: 07.06.2025).

² Например, Минцифры разрабатывает платформу «ТелекомЦентр» для борьбы с киберугрозами. Она будет объединять усилия государства, банков, бизнеса, операторов связи, владельцев соцсетей и разработчиков мобильных приложений по обмену информацией о киберинцидентах и мошеннических действиях. Запуск проекта запланирован на конец 2026 года. URL: <https://www.computerra.ru/300505/mintsifry-sozdaet-novuyu-platformu-dlya-borby-s-kiberprestupnostyu> (дата обращения: 10.05.2025).

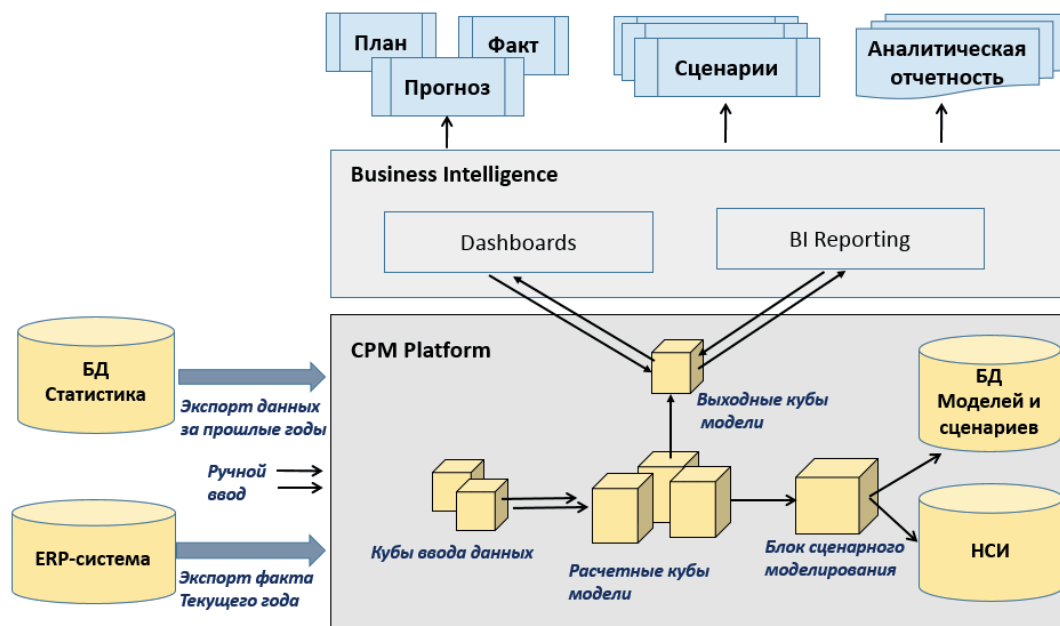


Рис. 1. Функциональная структура информационно-аналитической системы «Граф»

использующие искусственный интеллект. Кратко опишем их возможности.

1. Автоматизированная информационно-аналитическая система (АИАС) МВД России «СОРМ» (система оперативно-розыскных мероприятий).

АИАС использует технологии анализа больших данных и методы машинного обучения для оперативного выявления и анализа финансовых схем, мошенничеств с использованием сети Интернет и ИТТ.

2. Платформа «Сбербанк Аналитика» (Sber AI)

Платформа применяет методы искусственного интеллекта и предиктивной аналитики для:

- обнаружения аномалий в финансовых операциях: анализ транзакционной активности позволяет выявлять подозрительные операции и схемы обналичивания средств;

- идентификации мошеннических схем: использование графовой аналитики помогает выявлять связи между участниками преступных групп и схемы их взаимодействия;

- противодействия отмыванию денежных средств: анализ цифровых следов и поведенческих паттернов позволяет обнаруживать и пресекать попытки легализации незаконных доходов.

Эти технологии позволяют банку и правоохранительным органам эффективно выявлять и пресекать финансовые преступления, обеспечивая безопасность клиентов и финансовой системы в целом¹.

3. Наиболее значимым примером является разработанная в России система VIS (Visual Investigation System) – специализированный программный комплекс, предназначенный для визуального анализа и моделирования информационных связей в ходе оперативно-розыскной и следственной деятельности.

Функциональные возможности VIS включают: автоматический импорт данных из бухгалтерских программ (например, 1С), Excel-таблиц, банковских реестров и других источников; построение интерактивных графов с отображением связей между физическими и юридическими лицами, банковскими счетами, финансовыми потоками; фильтрацию по критериям риска, масштабируемость отображаемых структур; интеграцию с базами данных МВД и других ведомств РФ; поддержку русского языка и соответствие процессуальным нормам российского уголовного судопроизводства.

4. Система «FindFace Security» (ООО «НТехЛаб»)

Разработана российской компанией NtechLab для автоматического поиска и идентификации лиц. Использует нейросетевые технологии для автоматического поиска и идентификации лиц, причастных к экономическим преступлениям, в том числе к мошенничеству в сети Интернет.

5. Информационно-аналитическая система «Граф» (рисунок 1).

Позволяет визуализировать и анализировать сложные финансовые схемы, выявлять связи

¹ О сотрудничестве Сбербанка и МВД по борьбе с дипфейками. URL: https://safe.cnews.ru/news/line/2024-12-18_sber_i_mvd_rossii_budut (дата обращения: 10.06.2025).



Рис. 2. Основные ключевые функции информационно-аналитической системы Росфинмониторинга «Финансовый мониторинг»

между лицами, счетами и транзакциями, в том числе в сети Интернет, с использованием ИИ и алгоритмов анализа данных.

Система применяет различные графовые алгоритмы для анализа:

А) определение близости между объектами: используются метрики, такие как число общих соседей, индекс Адамика-Адара и другие, для оценки степени связи между субъектами,

Б) группировка связанных информационных объектов для выявления потенциальных преступных схем,

В) на основе имеющихся сведений система может предполагать и визуализировать возможные связи между объектами,

Г) обнаружение аномалий и подозрительных операций, характерных для преступных схем,

Д) возможность объединения информации из различных баз данных и информационных систем для дополнения имеющейся информации,

Е) применение алгоритмов машинного обучения для прогнозирования потенциальных угроз [1].

6. Платформа «Центр мониторинга и реагирования на инциденты информационной безопасности» (ЦМРИИБ) Банка России.

Центр известный как ФинЦЕРТ, представляет собой ключевую структуру, обеспечивающую

кибербезопасность финансового сектора страны. Центр осуществляет постоянный мониторинг информационного пространства для выявления потенциальных угроз и происшествий в финансовой сфере; обеспечивает взаимодействие между участниками финансового рынка и государственными органами, способствуя оперативному обмену данными о выявленных угрозах; выявляет и предотвращает кибератаки на организации¹.

7. Информационно-аналитическая система Росфинмониторинга «Финансовый мониторинг» (рисунок 2).

Использует технологии систем искусственного интеллекта и анализа больших данных для выявления подозрительных транзакций, отмывания денег и финансирования экстремизма, совершаемых с применением информационно-телекоммуникационных сетей².

Обсуждение и заключение

Для осуществления отдельных специальных мер противодействия совершению экономических преступлений, в том числе с использованием ИТТ, необходимо внедрение в деятельность правоохранительных органов отечественных информационно-аналитических систем.

При организации данной деятельности системы искусственного интеллекта способны решать разнообразные задачи, необходимые для преду-

¹ Основные направления развития финансовых технологий на 2025–2027 годы. URL: https://www.cbr.ru/Content/Document/File/166399/onfintech_2025-27.pdf (дата обращения: 10.06.2025); О тенденциях и направлениях применения ИИ в информационной безопасности – In4Security. URL: <https://in4security.com/news/tpost/gdftp0ilbz1-o-tendentsiyah-i-napravleniyah-primeneni> (дата обращения: 10.06.2025).

² Росфинмониторинг внедрит в свою работу анализ больших данных и ИИ. URL: <https://x-compliance.ru/publications/podft/rosfinmonitoring-vnedrit-v-svou-rabotu-analiz-bolshih-dannyh-i-ii> (дата обращения: 10.06.2025).

преждения, выявления и расследования экономических преступлений.

В статье проведено краткое описание возможностей указанных систем. Выявлено, что несмотря на различные возможности, функции, задачи и методы, используемые рассмотренными информационно-аналитическими системами, их все в той или иной степени можно использовать при реализации специальных мер по противодействию экономическим преступлениям, совершаемым с использованием ИТТ.

Умелое и правильное применение данных систем, безусловно, способно повысить эффективность борьбы с экономическими преступлениями.

Для этого необходима подготовка и переподготовка кадров правоохранительных органов в целях выработки компетенций в области искусственного интеллекта и цифровых технологий.

Также представляется необходимым дальнейшее развитие систем искусственного интеллекта для противодействия экономическим преступлениям, разработка вопросов, связанных с их функционированием, техническим и правовым описанием процесса их использования в настоящее время в правоохранительной деятельности России.

Максимально полное внедрение систем искусственного интеллекта в деятельность правоохранительных органов для противодействия экономическим преступлениям позволит повысить эффективность данного противодействия. В конечном итоге, интеграция технологий искусственного интеллекта в деятельность правоохранительных органов способна существенно укрепить экономическую безопасность Российской Федерации и обеспечить устойчивость социально-экономического развития России.

СПИСОК ИСТОЧНИКОВ

1. Батурина Е.В. «Информационно-аналитическая система мониторинга теневого безналичного денежного потока: основные элементы, авторский алгоритм» // Вестник университета. Санкт-Петербург. 2019. № 7. С. 144–151.
2. Гаврилин Ю.В., Лелетова М.В., Мартыненко Н.Э., Парфенов А.В., Пинкевич Т.В., Поздняков А.Н., Саркисян Г.Г., Севастьянов П.В., Торопов Б.А. Организация противодействия преступлениям, совершаемым с использованием информационно-телекоммуникационным технологий: учебник. Часть 1. Москва, 2024.
3. Грачев С.А., Лелетова М.В., Ушаков А.Ю. Расследование преступлений в сфере экономической деятельности Нижний Новгород, 2018.
4. Дятлова А.Ф., Свирина М.В. Технологии искусственного интеллекта в сфере экономической безопасности // Вестник Московского университета МВД России. 2024. № 2. С. 227–232. <https://doi.org/10.24412/2073-0454-2024-2-227-232>. EDN: SVRPND.
5. Лелетова М.В. Профилактическая деятельность подразделений экономической безопасности и противодействия коррупции: проблемы теории и практики // Гуманитарные и политико-правовые исследования. 2024. № 4 (27). С. 25–32.
6. Малаев А.Х. Применение цифровых технологий и искусственного интеллекта при предупреждении экстремистских и террористических преступлений // Пробелы в российском законодательстве. 2023. Т. 16. № 4. С. 263–267.
7. Тугуз Р.Т. Искусственный интеллект как инструмент борьбы с преступностью // Актуальные проблемы научных исследований: теоретический и практический аспекты: сборник статей международной научно-практической конференции. Уфа, 2023. С. 44–48.
8. Жарова А.К., Шемелкин Е.Е. Особенности подготовки сотрудников оперативных подразделений, специализирующихся на противодействии преступлениям, совершенным с использованием информационно-телекоммуникационных технологий // Научный Лидер. 2024. № 36 (186). URL: <https://scilead.ru/article/7042-osobennosti-podgotovki-sotrudnikov-operativni>.

REFERENCES

1. Baturina E.V. «Informacionno-analiticheskaya sistema monitoringa tenevogo beznalichnogo denezhnogo potoka: osnovnye elementy, avtorskiy algoritm» // Vestnik universiteta. Sankt-Peterburg. 2019. № 7. S. 144–151.
2. Gavrilin Yu.V., Leletova M.V., Martynenko N.E., Parfenov A.V., Pinkevich T.V., Pozdnyakov A.N., Sarkisyan G.G., Sevast'yanov P.V., Toropov B.A. Organizaciya protivodejstviya prestupleniyam, sovershaemym s ispol'zovaniem informacionno-telekommunikacionnym tekhnologij: uchebnik. Chast' 1. Moskva, 2024.

3. Grachev S.A., Leletova M.V., Ushakov A.Yu. Rassledovanie prestuplenij v sfere ekonomicheskoy deyatel'nosti Nizhnij Novgorod, 2018.
4. Dyatlova A.F., Svirina M.V. Tekhnologii iskusstvennogo intellekta v sfere ekonomicheskoy bezopasnosti // Vestnik Moskovskogo universiteta MVD Rossii. 2024. № 2. S. 227–232. <https://doi.org/10.24412/2073-0454-2024-2-227-232>. EDN: SVRPND.
5. Leletova M.V. Profilakticheskaya deyatel'nost' podrazdelenij ekonomicheskoy bezopasnosti i protivodejstviya korrupcii: problemy teorii i praktiki // Gumanitarnye i politiko-pravovye issledovaniya. 2024. № 4 (27). S. 25–32.
6. Malaev A.H. Primenenie cifrovyyh tekhnologij i iskusstvennogo intellekta pri preduprezhdenii ekstremistskikh i terroristicheskikh prestuplenij // Probely v rossijskom zakonodatel'stve. 2023. T. 16. № 4. S. 263–267.
7. Tuguz R.T. Iskusstvennyj intellekt kak instrument bor'by s prestupnost' // Aktual'nye problemy nauchnyh issledovanij: teoreticheskij i prakticheskij aspekty: sbornik statej mezhdunarodnoj nauchno-prakticheskoy konferencii. Ufa, 2023. S. 44–48.
8. Zharova A.K. Shemelkin E.E. Osobennosti podgotovki sotrudnikov operativnyh podrazdelenij, specializiruyushchih'sya na protivodejstvii prestupleniyam, sovershennym s ispol'zovaniem informacionno-telekommunikacionnyh tekhnologij // Nauchnyj Lider. 2024. № 36 (186). URL: <https://scilead.ru/article/7042-osobennosti-podgotovki-sotrudnikov-operativni>.



Информация об авторах:

Баранов Владимир Владимирович, кандидат юридических наук, доцент, доцент кафедры информационных технологий Академии управления МВД России, e-mail: de_la_sergio@mail.ru

Лелетова Марина Владимировна, кандидат юридических наук, доцент, доцент кафедры уголовной политики Академии управления МВД России. e-mail: leletova@list.ru

Авторы прочитали и одобрили окончательный вариант рукописи.

Information about the authors:

Baranov Vladimir V., Candidate of Legal Sciences, Associate Professor, Associate Professor at the Department of Information Technologies, Academy of Management of the Ministry of Internal Affairs of Russia, e-mail: de_la_sergio@mail.ru

Leletova Marina V., Candidate of Legal Sciences, Associate Professor, Associate Professor at the Department of Criminal Policy, Academy of Management of the Ministry of Internal Affairs of Russia, e-mail: leletova@list.ru

The authors have read and approved the final version of the manuscript.

Заявленный вклад авторов

Баранов Владимир Владимирович – постановка проблемы и концепция исследования; поиск аналитических материалов в официальных источниках; формирование выводов исследования; окончательное утверждение версии для публикации.

Лелетова Марина Владимировна – сбор, анализ, интерпретация полученных данных; подготовка первоначального варианта текста; описание результатов исследования; осуществление критического анализа и доработка текста.

Статья получена: 29.05.2026.

Статья принята к публикации: 30.09.2026.

Статья опубликована онлайн: 30.09.2026.

Против размещения полнотекстовой версии статьи в открытом доступе в сети Интернет не возражаем.