

УДК 004.932:004.8:004.056

DOI: [10.26102/2310-6018/2026.58.7.003](https://doi.org/10.26102/2310-6018/2026.58.7.003)

Метод блокчейн-консенсусной распределенной классификации изображений

Е.А. Конников¹, Н.Р. Санду², Р.В. Файзуллин²

¹Санкт-Петербургский политехнический университет Петра Великого,
Санкт-Петербург, Российская Федерация

²МИРЭА – Российский технологический университет, Москва, Российская Федерация

Резюме. Предметом исследования являются методы межузловой агрегации обновлений и локальных визуальных представлений в распределенных системах классификации изображений. Цель работы состоит в разработке и экспериментальной проверке метода блокчейн-консенсусной распределенной классификации изображений, ориентированного на повышение устойчивости глобальной модели в условиях неоднородных, шумных и частично вредоносных источников данных. Предлагаемый подход сочетает локальные классовые атласы признаков, аудит-проверку полезности клиентских обновлений, робастную оценку аномальности локальных траекторий и блокчейн-фиксируемое консенсусное взвешивание вклада узлов. Для экспериментальной проверки использованы открытые наборы изображений CIFAR-10 и Olivetti Faces, а сравнение выполнено в сценариях iid_clean, noniid_clean, noniid_noisy и noniid_adversarial. Сопоставление проведено с методами Distributed Mean, Distributed Proximal, Distributed Trimmed Mean и Atlas Consensus по метрикам Accuracy, Macro-F1 и Balanced Accuracy, а также по траекториям сходимости, консенсусным весам и статистической проверке отличий. Показано, что предлагаемый метод не является универсальным лидером на чистых распределениях, однако в целевом вредоносном сценарии обеспечивает лучший результат среди распределенных схем. Полученные результаты подтверждают целесообразность применения блокчейн-консенсусной фильтрации обновлений в задачах распределенной обработки визуальных данных при наличии недоверенных участников и конфликтных межузловых воздействий.

Ключевые слова: блокчейн, распределенная классификация изображений, межузловая агрегация, визуальные данные, неоднородные распределения, вредоносные узлы, робастная агрегация, консенсус, классовый атлас, информационные процессы.

Для цитирования: Конников Е.А., Санду Н.Р., Файзуллин Р.В. Метод блокчейн-консенсусной распределенной классификации изображений. *Моделирование, оптимизация и информационные технологии*. 2026;14(7). URL: <https://moitvvt.ru/ru/journal/article?id=2392> DOI: 10.26102/2310-6018/2026.58.7.003

Method of blockchain-consensus distributed image classification

Е.А. Konnikov¹, N.R. Sandu², R.V. Faizullin²

¹Peter the Great St. Petersburg Polytechnic University, St. Petersburg, the Russian Federation

²MIREA – Russian Technological University, Moscow, the Russian Federation

Abstract. The study focuses on inter-node aggregation methods for model updates and local visual representations in distributed image classification systems. The paper aims to develop and experimentally validate a blockchain-consensus distributed image classification method that improves the robustness of the global model under heterogeneous, noisy, and partially malicious data sources. The proposed approach combines local class atlases, audit-based utility estimation of client updates, robust anomaly scoring of local trajectories, and blockchain-backed consensus weighting of node contributions. The blockchain layer is implemented as a reproducible software ledger for update

provenance and audit logging. The experimental evaluation relies on the open CIFAR-10 and Olivetti Faces datasets in four scenarios: iid_clean, noniid_clean, noniid_noisy, and noniid_adversarial. The method is compared with Distributed Mean, Distributed Proximal, Distributed Trimmed Mean, and Atlas Consensus using Accuracy, Macro-F1, Balanced Accuracy, convergence dynamics, consensus weights, and statistical testing. The results show that the proposed method is not universally superior on clean distributions; however, in the target adversarial scenario it achieves the best performance among distributed schemes. The findings confirm the practical value of blockchain-consensus filtering of node updates for distributed visual data processing.

Keywords: blockchain, distributed image classification, inter-node aggregation, visual data, heterogeneous distributions, malicious nodes, robust aggregation, consensus, class atlas, information processes.

For citation: Konnikov E.A., Sandu N.R., Faizullin R.V. Method of blockchain-consensus distributed image classification. *Modeling, Optimization and Information Technology*. 2026;14(7). (In Russ.). URL: <https://moitvivr.ru/journal/article?id=2392> DOI: 10.26102/2310-6018/2026.58.7.003

Введение

Классификация изображений остается одной из ключевых задач современной информатики и интеллектуальной обработки данных, поскольку лежит в основе систем компьютерного зрения, медицинской диагностики, дистанционного мониторинга, промышленного контроля и цифровой идентификации объектов. При этом развитие прикладных систем визуального анализа приводит к необходимости обработки изображений в распределенной среде, где данные формируются на разных узлах, отличаются по структуре, качеству и объему, а централизованное объединение выборок оказывается организационно, вычислительно или нормативно затрудненным. В данной связи особую научную значимость приобретают методы распределенной классификации изображений, способные одновременно обеспечивать высокое качество распознавания, устойчивость к неоднородности локальных данных и доверенность межузлового взаимодействия.

Исследования по классическим и нейросетевым методам анализа изображений показывают, что сама по себе задача визуальной классификации остается сложной даже в централизованной постановке [1, 2]. В работах по сверточным и адаптивным моделям распознавания подчеркивается, что качество решения зависит не только от мощности модели, но и от предварительной обработки изображений, состава признаков, межклассовой разделимости, полноты обучающих данных и устойчивости алгоритма к шумным или неполным наблюдениям [3, 4]. Отдельные исследования указывают, что на сложных и высоковариативных данных одиночные классификаторы нередко требуют ансамблирования или более сложных схем согласования признаков [5], а использование предобученных сетей и переноса признаков отражает стремление компенсировать дефицит размеченных изображений и ограничения ручного проектирования признакового пространства [6]. Тем самым литература по классификации изображений фиксирует исходный тезис – качество визуального распознавания определяется не только архитектурой модели, но и структурой данных, а значит, при переходе к распределенной постановке данная проблема усиливается.

В международных исследованиях по распределенному обучению для изображений основной акцент переносится на неоднородность локальных выборок, различие числа наблюдений у клиентов, межклиентскую асимметрию классов и несовпадение локальных распределений с глобальной моделью [7, 8]. Обзоры по медицинскому и гистопатологическому анализу изображений показывают, что распределенные схемы обучения особенно востребованы там, где данные трудно централизовать, однако именно в данных областях качество глобальной модели сильнее

всего страдает от неоднородности данных (non-IID), локального смещения признаков, дисбаланса классов и различий между источниками данных [7, 8]. Работы по учету неопределенности, дистилляции, кластеризации и энтропии фиксируют, что для классификации изображений недостаточно просто обмениваться параметрами модели [9, 10]. Требуется согласование локальных визуальных представлений, поскольку разные узлы видят разные фрагменты признакового пространства и формируют неодинаковые межклассовые границы [11, 12].

Наиболее распространенным базовым подходом в распределенной среде остается простое усреднение локальных обновлений, соответствующее семейству FedAvg-подобных методов (алгоритм в рамках федеративного обучения (FL)) и представленное в данной работе как распределенное среднее (Distributed Mean). Однако исследования показывают, что данный класс методов имеет ряд фундаментальных ограничений [13, 14]. Во-первых, простое усреднение не различает полезные и вредоносные обновления, поэтому злонамеренные или низкокачественные узлы могут оказывать чрезмерное влияние на глобальную модель [15, 16]. Во-вторых, при non-IID и количественном перекосе данных глобальная модель начинает смещаться в сторону доминирующих клиентов, а узлы с редкими, но важными визуальными паттернами оказываются недоучтенными [11, 13]. В-третьих, в традиционной постановке сохраняется зависимость от доверенного центрального агрегатора, который становится одновременно уязвимой точкой и организационным ограничением распределенной системы [17, 18]. Следовательно, распределенное среднее является естественным базовым подходом, но с научной точки зрения его недостаточно для устойчивой классификации изображений в недоверенной и неоднородной среде.

Попыткой частично преодолеть данные ограничения стали проксимальные, регуляризационные, дистилляционные и кластеризационные схемы [9, 11]. Проксимальные методы, аналогом которых в данном исследовании выступает проксимальное распределение (Distributed Proximal), уменьшают разброс локальных траекторий за счет дополнительного штрафа на отклонение от глобальной модели, но, как показывают исследования, не решают проблему содержательной валидации вклада и недостаточно эффективны при сильной межузловой неоднородности [13, 14]. Дистилляционные и согласующие методы, напротив, лучше учитывают структуру локальных представлений и межклассовые зависимости, однако в основном решают задачу выравнивания знаний между клиентами, а не задачу доверия к самому участнику распределенной системы [9, 10]. В литературе подчёркиваются такие ограничения данных подходов, как частичная потеря межклассовой информации, забывание редких классов, зависимость от формы локального распределения и отсутствие встроенного механизма фильтрации вредоносных участников [12, 14]. Иными словами, подобные методы улучшают согласование представлений, но не дают полного ответа на вопрос, какие именно локальные обновления следует считать надежными.

Отдельную группу составляют робастные агрегаторы, в частности, методы усеченного усреднения, представленные в работе схемой распределенного усеченного среднего (Distributed Trimmed Mean). Их ключевое преимущество заключается в частичном подавлении экстремальных выбросов и атакующих обновлений, однако анализ литературы показывает, что робастность здесь достигается ценой потери части полезного сигнала [19]. Если уровень усечения выбран недостаточно жестко, метод остается чувствительным к вредоносным узлам. Если же усечение слишком велико, из глобальной модели устраняются не только атакующие, но и редкие информативные обновления, особенно в условиях асимметрии выборок [19]. Для задач классификации изображений это особенно критично, поскольку редкие локальные клиенты могут

содержать уникальные визуальные паттерны, статистически похожие на выбросы, но содержательно ценные для глобального классификатора.

Параллельно развивается направление распределённого обучения на основе блокчейна (blockchain-based distributed learning), в котором блокчейн рассматривается как средство верификации действий узлов, фиксации локальных обновлений и устранения зависимости от доверенного центра [15, 17]. Обзорные и прикладные исследования показывают, что блокчейн может использоваться для обеспечения прозрачности, воспроизводимости и защищенности процесса распределенного обучения, особенно в сценариях, где существует риск злонамеренного поведения клиентов или необходимости доказуемого учёта вклада участников [16, 20]. В работах на основе консенсуса и децентрализованного обучения подчеркивается, что консенсусная логика важна не только как сетевой протокол, но и как вычислительный механизм отбора надежных обновлений [18, 21]. Русскоязычные публикации по цифровой идентификации, смарт-контрактам и киберфизическим системам дополняют данную картину инженерным аспектом – доверие в децентрализованной среде должно быть обеспечено не декларативно, а через проверяемость действий участников, защищенность логики смарт-контрактов и фиксируемость межузловых операций [22, 23].

Несмотря на значительный объем работ, анализ литературы показывает, что предметная область остается фрагментированной. Одни исследования сосредоточены на улучшении качества распределенной классификации изображений при non-IID за счет регуляризации, дистилляции, кластеризации и персонализации [11, 12], другие – на защите распределенного обучения и устранении зависимости от доверенного агрегатора с помощью блокчейн-механизмов [20, 24]. При этом завершённый метод, который одновременно учитывал бы межузловую геометрию визуальных представлений, содержательную полезность локального обновления, робастную аномальность траектории клиента и блокчейн-консенсусную верификацию действий участников, в рассмотренной литературе не представлен. Именно данный разрыв и формирует научную задачу настоящего исследования.

В связи с этим в работе предлагается метод блокчейн-консенсусной распределенной классификации изображений, ориентированный на повышение устойчивости распределенной визуальной классификации в условиях non-IID, шумных и вредоносных узлов. В отличие от распределенного среднего, распределенного проксимального среднего и распределенного усеченного среднего, предлагаемый метод использует не только межузловую агрегацию параметров, но и согласование локальных классовых атласов, оценку полезности обновлений на аудит-выборке, робастную оценку аномальности локальных обновлений и блокчейн-фиксируемое консенсусное взвешивание вклада узлов.

Материалы и методы

Целью работы является разработка и экспериментальная проверка метода блокчейн-консенсусной распределенной классификации изображений, обеспечивающего устойчивую межузловую агрегацию обновлений в условиях неоднородных, шумных и частично вредоносных локальных выборок. Объектом исследования являются процессы распределенной обработки и классификации изображений в многоузловых информационных системах. Предметом исследования являются методы межузловой агрегации параметров моделей и локальных визуальных представлений в условиях неоднородных, шумных и частично вредоносных источников данных. Гипотеза исследования заключается в том, что блокчейн-консенсусная

агрегация обновлений и локальных классовых атласов позволяет повысить устойчивость распределенной классификации изображений по сравнению с простым усреднением, проксимальными и робастными схемами, особенно в сценариях с конфликтными и вредоносными межузловыми воздействиями.

Используемые методы, методики и технологии включают локальную оптимизацию софтмакс-классификатора, формирование классовых атласов признаков, аудит-проверку полезности клиентских обновлений, робастную оценку аномальности траектории и блокчейн-фиксируемое консенсусное взвешивание узлов. Каждый узел передает локальное обновление параметров, локальный классовый атлас признаков, показатели полезности локальной модели и криптографические хэши обновления и атласа. Распределенный реестр используется не для хранения самих изображений, а для фиксации происхождения межузловых обновлений, проверки их качества и расчета консенсусного веса узла. Таким образом, глобальная модель определяется не только объемом локальных данных, но и фактическим вкладом клиента в устойчивое качество классификации. Формальная модель рассматривает систему из K узлов, локальные обучающие выборки, параметризованный softmax-классификатор и раундовую агрегацию обновлений в распределенном журнале.

Для проверки предложенного метода был выполнен вычислительный эксперимент на двух открытых наборах данных, представляющих различные классы задач визуального анализа. В качестве первого набора использовался CIFAR-10, содержащий 60000 цветных изображений размером 32×32 пикселя в 10 классах, из которых 50000 относятся к обучающей, а 10000 к тестовой частям. В качестве второго набора использовался Olivetti Faces, содержащий 400 изображений лиц 40 персон. Изображения были приведены к векторному представлению, стандартизованы и затем понижены по размерности методом главных компонент. Для CIFAR-10 использовалось 48 компонент, для Olivetti Faces – 64 компоненты. В распределенном контуре обучение проводилось на 8 узлах. Для CIFAR-10 использовалось 8 глобальных раундов, для Olivetti Faces – 10. Эксперимент выполнялся на трех независимых сетах: 7, 21 и 84.

Проверялись четыре сценария распределения данных между узлами. Сценарий `iid_clean` задавал равномерное распределение без искажения меток и вредоносных участников. Сценарий `noniid_clean` моделировал неоднородное распределение классов между узлами. Сценарий `noniid_noisy` дополнял неоднородность частичным искажением локальных меток. Сценарий `noniid_adversarial` включал одновременно межузловую неоднородность, шумную разметку, выпадение части узлов и вредоносные обновления. Именно последний сценарий соответствует целевой постановке, в которой блокчейн-консенсусная валидация обновлений должна давать наибольший эффект.

В качестве сравниваемых методов были выбраны: Distributed Mean как базовый метод межузлового усреднения параметров; Distributed Proximal как распределенная проксимальная модификация; Distributed Trimmed Mean как робастная схема агрегации с усечением; Atlas Consensus как метод согласования локальных классовых атласов без блокчейн-компонента полезности; Blockchain Consensus как предлагаемый метод; Centralized Softmax как централизованная верхняя граница качества. При интерпретации результатов основное сравнение выполнялось именно между распределёнными методами, поскольку централизованный классификатор не подвержен распределительным и консенсусным ограничениям.

Для каждого узла на каждом раунде вычислялись полезность локального обновления на общей аудит-выборке, согласованность локального атласа с межузловой геометрией классов и аномальность обновления относительно робастной медианной траектории. Данные показатели использовались для расчета консенсусного веса узла.

Веса, хэши обновлений, хэши атласов и служебные метаданные фиксировались в программной симуляции блокчейн-журнала.

Качество оценивалось по метрикам Accuracy, Macro-F1 и Balanced Accuracy. Дополнительно анализировались траектории сходимости по раундам, распределение консенсусных весов, устойчивость к ухудшению сценария и прирост качества нового метода относительно альтернативных схем. Для проверки статистической состоятельности выполнялся парный критерий Уилкоксона по значениям Macro-F1 на множестве пар dataset, scenario, seed (набор данных, сценарий, начальное значение генератора).

Локальная оптимизация на узле k описывается формулой:

$$\theta_k^{(t+1)} = \operatorname{argmin}_{\theta} (L_k(\theta) + \lambda \|\theta\|_2^2 + \mu \|\theta - \theta^{(t)}\|_2^2), \quad (1)$$

где θ_k – параметры локальной модели узла k , L_k – локальная функция потерь, λ – коэффициент L2-регуляризации, μ – коэффициент проксимального члена, $\theta^{(t)}$ – глобальные параметры на раунде t .

Локальный классовой атлас признаков для класса c определяется формулой:

$$c_{k,c} = \frac{1}{|I_{k,c}|} \sum_{i \in I_{k,c}} x_i, \quad (2)$$

где $|I_{k,c}|$ – множество индексов наблюдений класса c узла k , x_i – векторное представление i -го наблюдения.

Полезность локального обновления на аудит-выборке вычисляется по формуле:

$$u_k^{(t)} = \rho \cdot \operatorname{MacroF1}_k^{\text{audit}} + (1 - \rho) \cdot \operatorname{BalAcc}_k^{\text{audit}}, \quad (3)$$

где $\operatorname{MacroF1}_k^{\text{audit}}$ – макроусредненная мера качества классификации на аудит-выборке, $\operatorname{BalAcc}_k^{\text{audit}}$ – сбалансированная точность на аудит-выборке, ρ – весовой коэффициент.

Аномальность локального обновления относительно медианной траектории определяется формулой:

$$a_k^{(t)} = \frac{\|\Delta\theta_k^{(t)} - \operatorname{med}(\Delta\theta^{(t)})\|_2}{\operatorname{MAD}(\Delta\theta^{(t)}) + \varepsilon}, \quad (4)$$

где $\Delta\theta_k^{(t)}$ – приращение параметров узла k , med – покомпонентная медиана, MAD – медианное абсолютное отклонение, ε – малая константа регуляризации.

Консенсусный вес узла k на раунде t определяется формулой:

$$w_k^{(t)} = \frac{\exp(\alpha u_k^{(t)} + \beta d_k^{(t)} - \gamma a_k^{(t)} + \eta \ln(1+n_k))}{\sum_{j=1}^K \exp(\alpha u_j^{(t)} + \beta d_j^{(t)} - \gamma a_j^{(t)} + \eta \ln(1+n_j))}, \quad (5)$$

где $d_k^{(t)}$ – мера согласованности атласа узла k с межузловой геометрией классов, n_k – объем локальной выборки, $\alpha, \beta, \gamma, \eta$ – настраиваемые коэффициенты.

Глобальное обновление параметров формируется по формуле:

$$\theta^{(t+1)} = \sum_{k=1}^K w_k^{(t)} \theta_k^{(t+1)}. \quad (6)$$

Содержимое блока распределенного журнала на раунде t описывается формулой:

$$B_t = \left(H(B_{t-1}), \{H(\Delta\theta_k^{(t)}), H(A_k^{(t)})\}_{k=1}^K, \{u_k^{(t)}, d_k^{(t)}, a_k^{(t)}, w_k^{(t)}\}_{k=1}^K \right), \quad (7)$$

где H – криптографическая хэш-функция, $A_k^{(t)}$ – локальный классовой атлас узла k , остальные величины определены выше.

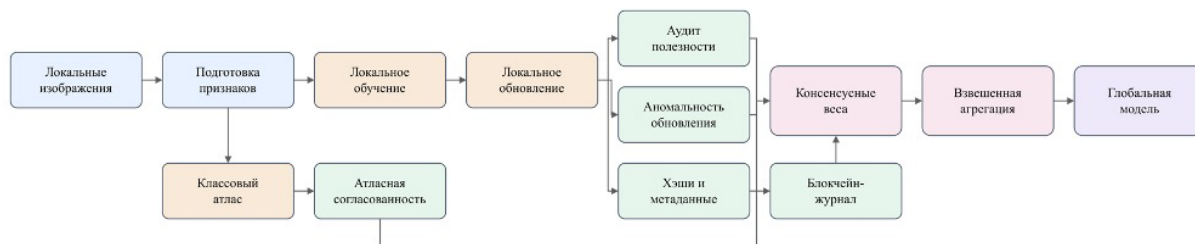


Рисунок 1 – Архитектура метода блокчейн-консенсусной распределенной классификации изображений

Figure 1 – Architecture of the blockchain-consensus distributed image classification method

Результаты

Результаты эксперимента показали, что предлагаемый метод не является безусловным лидером во всех режимах, однако демонстрирует именно тот профиль поведения, который и заявлен в научной гипотезе – преимущество проявляется прежде всего в сложных распределённых сценариях с вредоносными и конфликтующими обновлениями.

На наборе CIFAR-10 в чистом сценарии *iid_clean* лучшие результаты среди распределенных методов показали Distributed Proximal и Distributed Mean с Macro-F1 = 0,3259, тогда как Blockchain Consensus дал Macro-F1 = 0,3216. В сценарии *noniid_clean* лучшим оказался Atlas Consensus с Macro-F1 = 0,3034, а предлагаемый метод показал 0,2698. Аналогичная картина наблюдалась и в *noniid_noisy*, где Atlas Consensus дал 0,2954, а Blockchain Consensus – 0,2514. Однако в сценарии *noniid_adversarial* ситуация изменилась принципиально. Blockchain Consensus стал лучшим распределенным методом с Macro-F1 = 0,2262, превзойдя Atlas Consensus (0,1845), Distributed Proximal (0,1648), Distributed Mean (0,1644) и Distributed Trimmed Mean (0,1572).

На наборе Olivetti Faces в относительно чистых сценариях доминировали традиционные распределенные схемы. В *iid_clean* методы Distributed Mean и Distributed Proximal дали Macro-F1 = 0,9517, а предлагаемый метод – 0,8459. В *noniid_clean* и *noniid_noisy* те же два метода показали 0,9439 и 0,9017 соответственно, в то время как Blockchain Consensus дал 0,7750 и 0,6990. Вместе с тем в сценарии *noniid_adversarial* новый метод продемонстрировал наиболее выраженное преимущество во всем эксперименте: Macro-F1 = 0,6785 против 0,4300 у Atlas Consensus, 0,3795 у Distributed Proximal, 0,3756 у Distributed Mean и 0,2756 у Distributed Trimmed Mean.

Следовательно, на обоих наборах данных предлагаемый метод занял первое место среди распределенных альтернатив именно в целевом вредоносном сценарии. Для CIFAR-10 прирост Macro-F1 относительно Distributed Mean составил +0,0618, относительно Distributed Proximal +0,0614, относительно Atlas Consensus +0,0417, относительно Distributed Trimmed Mean +0,0690. Для Olivetti Faces соответствующие приросты составили +0,3029, +0,2990, +0,2485 и +0,4029.

Результаты по Accuracy и Balanced Accuracy согласуются с поведением Macro-F1. На CIFAR-10 в *noniid_adversarial* новый метод достиг Accuracy = 0,2663, тогда как Atlas Consensus дал 0,2472, Distributed Mean – 0,2380, Distributed Proximal – 0,2383. На Olivetti Faces в том же сценарии Blockchain Consensus дал Accuracy = 0,7208, что заметно выше 0,5042, 0,4292, 0,4333 и 0,3458 у остальных распределенных методов.

Статистическая проверка по совокупности всех сценариев показала, что средний прирост нового метода относительно Distributed Trimmed Mean составил +0,0408 по Macro-F1, однако значение $p = 0,2195$ не позволяет говорить о статистически значимом превосходстве на объединенной совокупности режимов. Это согласуется с общей

структурой результатов. Метод выигрывает не во всех сценариях, а главным образом во вредоносных распределенных условиях, где и должен проявляться эффект блокчейн-консенсусной фильтрации обновлений.

Таблица 1 – Результаты распределенных методов
 Table 1 – Results of distributed methods

Набор данных (dataset)	Сценарий (scenario)	Метод (method_label)	Точность (accuracy)	Макро-F1 (macro_f1)	Сбалансированная точность (balanced accuracy)
cifar10	iid_clean	Distributed Proximal	0,3368	0,3259	0,3368
cifar10	iid_clean	Distributed Mean	0,3368	0,3259	0,3368
cifar10	iid_clean	Atlas Consensus	0,3358	0,3257	0,3358
cifar10	iid_clean	Distributed Trimmed Mean	0,3348	0,3238	0,3348
cifar10	iid_clean	Blockchain Consensus	0,3312	0,3216	0,3312
cifar10	noniid_adversarial	Blockchain Consensus	0,2663	0,2262	0,2663
cifar10	noniid_adversarial	Atlas Consensus	0,2472	0,1845	0,2472
cifar10	noniid_adversarial	Distributed Proximal	0,2383	0,1648	0,2383
cifar10	noniid_adversarial	Distributed Mean	0,2380	0,1644	0,2380
cifar10	noniid_adversarial	Distributed Trimmed Mean	0,2138	0,1572	0,2138
cifar10	noniid_clean	Atlas Consensus	0,3208	0,3034	0,3208
cifar10	noniid_clean	Distributed Proximal	0,3177	0,2919	0,3177
cifar10	noniid_clean	Distributed Mean	0,3173	0,2915	0,3173
cifar10	noniid_clean	Blockchain Consensus	0,2995	0,2698	0,2995
cifar10	noniid_clean	Distributed Trimmed Mean	0,3013	0,2693	0,3013
cifar10	noniid_noisy	Atlas Consensus	0,3230	0,2954	0,3230
cifar10	noniid_noisy	Distributed Proximal	0,3127	0,2762	0,3127
cifar10	noniid_noisy	Distributed Mean	0,3127	0,2755	0,3127
cifar10	noniid_noisy	Distributed Trimmed Mean	0,2873	0,2524	0,2873
cifar10	noniid_noisy	Blockchain Consensus	0,2915	0,2514	0,2915
olivetti_faces	iid_clean	Distributed Mean	0,9542	0,9517	0,9542
olivetti_faces	iid_clean	Distributed Proximal	0,9542	0,9517	0,9542
olivetti_faces	iid_clean	Distributed Trimmed Mean	0,9375	0,9353	0,9375
olivetti_faces	iid_clean	Atlas Consensus	0,9292	0,9261	0,9292

Таблица 1 (продолжение)
 Table 1 (continued)

olivetti_faces	iid_clean	Blockchain Consensus	0,8667	0,8459	0,8667
olivetti_faces	noniid_adversarial	Blockchain Consensus	0,7208	0,6785	0,7208
olivetti_faces	noniid_adversarial	Atlas Consensus	0,5042	0,4300	0,5042
olivetti_faces	noniid_adversarial	Distributed Proximal	0,4333	0,3795	0,4333
olivetti_faces	noniid_adversarial	Distributed Mean	0,4292	0,3756	0,4292
olivetti_faces	noniid_adversarial	Distributed Trimmed Mean	0,3458	0,2756	0,3458
olivetti_faces	noniid_clean	Distributed Mean	0,9500	0,9439	0,9500
olivetti_faces	noniid_clean	Distributed Proximal	0,9500	0,9439	0,9500
olivetti_faces	noniid_clean	Atlas Consensus	0,9417	0,9358	0,9417
olivetti_faces	noniid_clean	Distributed Trimmed Mean	0,8250	0,8017	0,8250
olivetti_faces	noniid_clean	Blockchain Consensus	0,8083	0,7750	0,8083
olivetti_faces	noniid_noisy	Distributed Mean	0,9083	0,9017	0,9083
olivetti_faces	noniid_noisy	Distributed Proximal	0,9083	0,9017	0,9083
olivetti_faces	noniid_noisy	Atlas Consensus	0,9042	0,8909	0,9042
olivetti_faces	noniid_noisy	Distributed Trimmed Mean	0,7667	0,7259	0,7667
olivetti_faces	noniid_noisy	Blockchain Consensus	0,7458	0,6990	0,7458

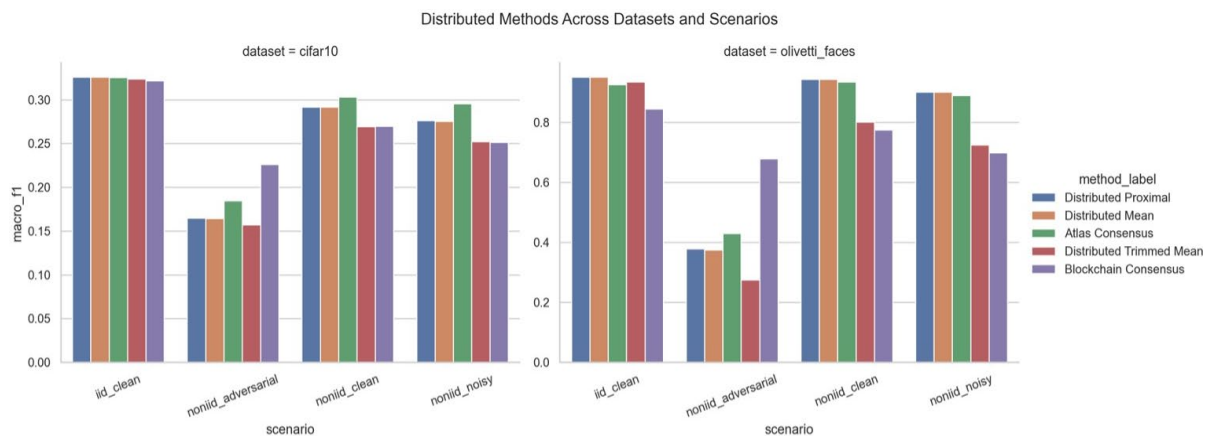


Рисунок 2 – Средние значения макроусредненной меры качества классификации распределенных методов по сценариям и наборам данных

Figure 2 – Mean values of the macro-averaged classification quality metric of distributed methods across scenarios and datasets

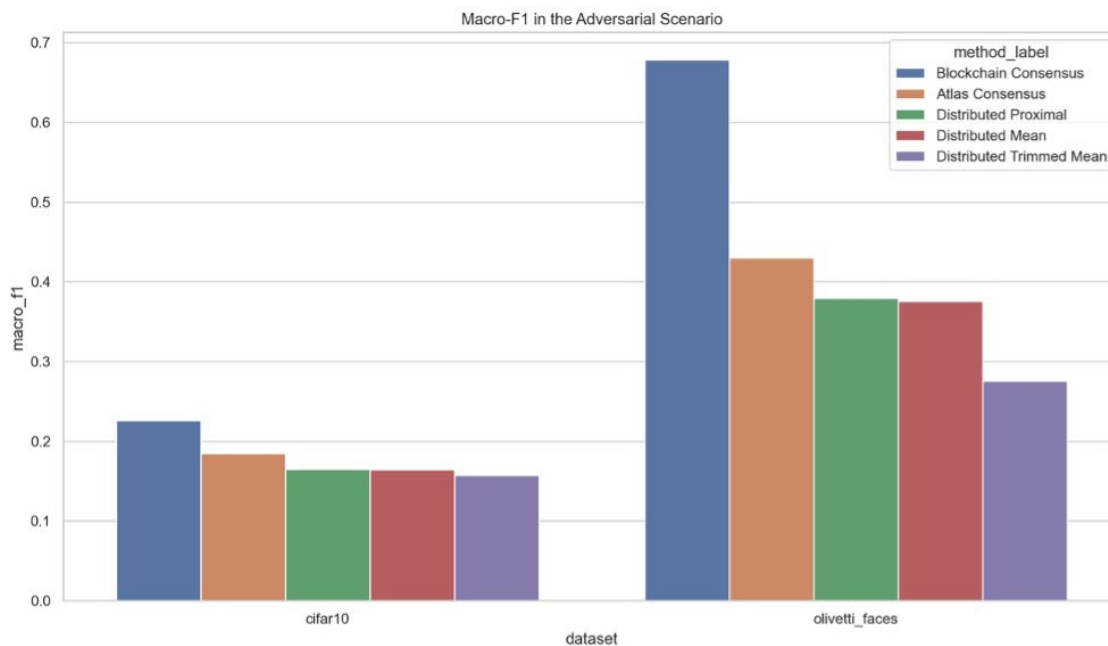


Рисунок 3 – Сравнение методов в сценарии вредоносного распределения
Figure 3 – Comparison of methods in the adversarial distribution scenario

Таблица 2 – Прирост метода Blockchain Consensus в вредоносном сценарии
Table 2 – Gain of the Blockchain Consensus method in the adversarial scenario

Набор данных (dataset)	Базовый метод (baseline_method)	Базовая Macro-F1 (baseline_macro_f1)	Macro-F1 BCCDC (bccdc_macro_f1)	Прирост Macro-F1 (macro_f1_gain)	Базовая точность (baseline_accuracy)	Точность BCCDC (bccdc_accuracy)	Прирост точности (accuracy_gain)
cifar10	Distributed Trimmed Mean	0,1572	0,2262	0,0690	0,2138	0,2663	0,0525
cifar10	Distributed Mean	0,1644	0,2262	0,0618	0,2380	0,2663	0,0283
cifar10	Distributed Proximal	0,1648	0,2262	0,0614	0,2383	0,2663	0,0280
cifar10	Atlas Consensus	0,1845	0,2262	0,0417	0,2472	0,2663	0,0192
olivetti_faces	Distributed Trimmed Mean	0,2756	0,6785	0,4029	0,3458	0,7208	0,3750
olivetti_faces	Distributed Mean	0,3756	0,6785	0,3029	0,4292	0,7208	0,2917
olivetti_faces	Distributed Proximal	0,3795	0,6785	0,2990	0,4333	0,7208	0,2875
olivetti_faces	Atlas Consensus	0,4300	0,6785	0,2485	0,5042	0,7208	0,2167

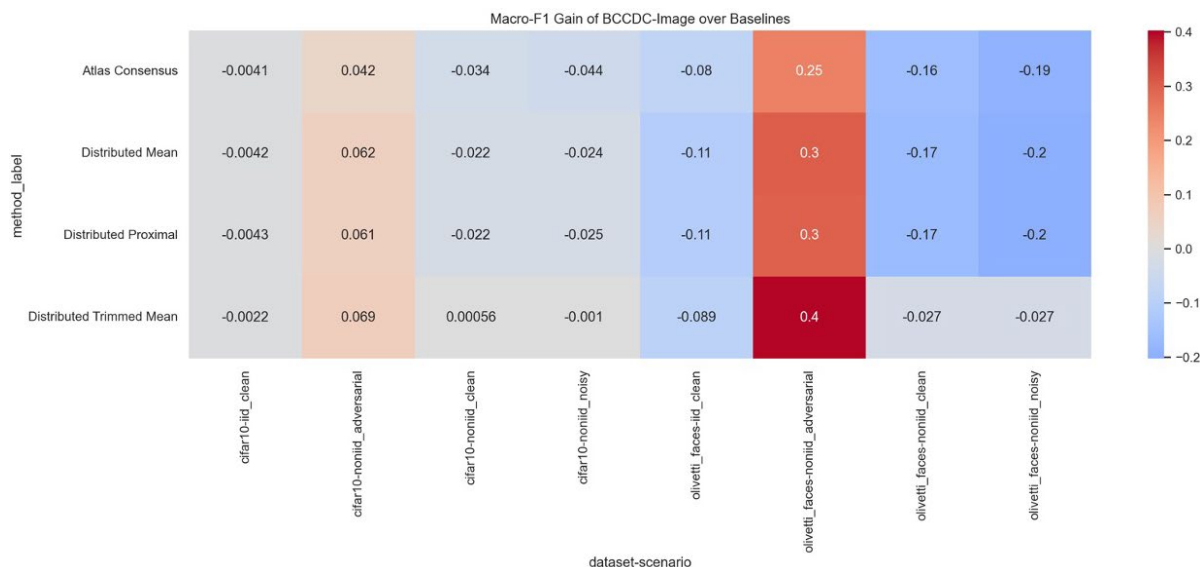


Рисунок 4 – Прирост макроусредненной меры качества классификации метода Blockchain Consensus относительно альтернативных распределенных схем

Figure 4 – Gain of the macro-averaged classification quality metric of the Blockchain Consensus method relative to alternative distributed schemes

Таблица 3 – Статистическая проверка

Table 3 – Statistical testing

Базовый метод (baseline_method)	Среднее приращение Macro-F1 (mean_gain_macro_fl)	Статистика Уилкоксона (wilcoxon_stat)	p-значение (p_value)	Интерпретация (interpretation)
Distributed Mean	-0,0203	103,0	0,9110	Новый метод в среднем не превосходит базовый на всей совокупности сценариев
Distributed Proximal	-0,0210	103,0	0,9110	Новый метод в среднем не превосходит базовый на всей совокупности сценариев
Distributed Trimmed Mean	0,0408	178,0	0,2195	Наблюдается положительный средний прирост, но без статистической значимости
Atlas Consensus	-0,0281	93,0	0,9495	Новый метод в среднем уступает на объединенной совокупности сценариев

Обсуждение

Полученная картина результатов хорошо согласуется с конструкцией метода. В чистых сценариях распределения данных блокчейн-консенсусная фильтрация и дополнительная валидация обновлений не дают выраженного выигрыша, поскольку сами узлы в среднем формируют достаточно согласованные локальные решения. В таких условиях методы простого усреднения или проксимальной коррекции оказываются менее консервативными и потому сохраняют немного более высокое качество.

При переходе к вредоносному сценарию поведение метода меняется. Здесь ключевую роль начинают играть аудит-полезность, межузловая согласованность атласов

и робастная оценка аномальности обновлений. В результате вредоносные и нестабильные участники получают значительно меньшие консенсусные веса, а глобальная модель меньше зависит от искаженных локальных траекторий. Именно этим объясняется заметный прирост на CIFAR-10 и особенно на Olivetti Faces в режиме `noniid_adversarial`.

Важно, что новый метод нельзя интерпретировать как универсальную замену всем существующим распределенным схемам. Эксперимент показывает более узкий и, с научной точки зрения, более убедительный тезис – метод эффективен как специализированный механизм устойчивой агрегации в недоверенной распределенной среде.

Отдельно следует отметить отличие между двумя наборами данных. Для Olivetti Faces выигрыш метода в вредоносном сценарии оказался существенно выше, чем для CIFAR-10. Это может быть связано с тем, что малый объем локальных лицевых подвыборок и большое число классов делают систему особенно чувствительной к ошибочным обновлениям, а значит, польза от консенсусного отбора оказывается более заметной.

К ограничениям текущего эксперимента относятся использование линейного softmax-классификатора после PCA-преобразования, программная симуляция блокчейн-журнала и отсутствие тяжелых сверточных архитектур. Однако данные ограничения не разрушают научной логики работы, поскольку целью эксперимента было сравнение именно схем распределенной агрегации и консенсусной фильтрации обновлений при одинаковом признаковом представлении.

Заключение

В работе предложен метод блокчейн-консенсусной распределенной классификации изображений, ориентированный на устойчивую межузловую агрегацию обновлений в условиях `non-IID`, шумных и вредоносных локальных данных. В отличие от альтернативных схем, метод объединяет согласование локальных классовых атласов, аудит-оценку полезности клиента, робастную оценку аномальности локального обновления и блокчейн-фиксируемое консенсусное взвешивание вклада узлов.

Проведенный эксперимент на наборах CIFAR-10 и Olivetti Faces показал, что предлагаемый метод не является универсальным лидером в чистых сценариях, однако демонстрирует выраженное преимущество в целевом вредоносном режиме `noniid_adversarial`. На обоих наборах данных он занял первое место среди распределенных альтернатив, а наиболее сильный выигрыш был получен на Olivetti Faces, где прирост Macro-F1 относительно альтернативных схем составил от +0,2485 до +0,4029.

Полученные результаты подтверждают, что научная ценность метода состоит не в максимизации качества на идеализированных распределениях, а в снижении деградации распределенной классификации изображений при наличии конфликтных и вредоносных межузловых воздействий. Это позволяет рассматривать предложенный метод как перспективную основу для дальнейшего развития распределенных систем обработки изображений в недоверенной многоузловой среде.

Перспективы дальнейших исследований связаны с переносом консенсусной логики на глубокие сверточные и трансформерные визуальные модели, введением адаптивных порогов допуска узлов и расширением блокчейн-слоя с учетом долговременной репутационной истории клиентов.

СПИСОК ИСТОЧНИКОВ / REFERENCES

1. Кузьмицкий Н.Н. Свёрточная нейросетевая модель в задаче классификации изображений изолированных цифр. *Доклады БГУИР*. 2012;(7):65–71.
Kuzmitsky N.N. Convolutional neural model in a task of classification images of the isolated digits. *Doklady BGUIR*. 2012;(7):65–71. (In Russ.).
2. Фирсов Н.А., Подлипов В.В., Ивлиев Н.А. и др. Ансамбли спектрально-пространственных свёрточных нейросетевых моделей для задачи классификации типов почв на гиперспектральных изображениях. *Компьютерная оптика*. 2023;47(5):795–805. <https://doi.org/10.18287/2412-6179-CO-1260>
Firsov N.A., Podlipnov V.V., Ivliev N.A., et al. Ensembles of spectral-spatial convolutional neural network models for classifying soil types in hyperspectral images. *Computer Optics*. 2023;47(5):795–805. (In Russ.). <https://doi.org/10.18287/2412-6179-CO-1260>
3. Федотов Д.В. Использование свёрточных нейронных сетей для решения задачи автоматического определения возраста. *Актуальные проблемы авиации и космонавтики*. 2015;1(11):377–379.
Fedotov D.V. Using convolutional neural networks for solving problem of automated age estimation. *Actual Problems of Aviation and Cosmonautics*. 2015;1(11):377–379. (In Russ.).
4. Джуманов О.И. Адаптивная нейросетевая система визуализации изображений, распознавания и классификации микрообъектов. *Вестник СибГУТИ*. 2008;(2):76–85.
5. Ташков Д.Ю., Ежов И.Е. Применение нейросетевых алгоритмов распознавания объектов по изображению в системах охранного телевидения. *Альманах Пермского военного института войск национальной гвардии*. 2025;(1):95–106.
Tashkov D.Yu., Ezhov I.E. Application of neural network algorithms for object recognition by image in security television systems. *Almanac of the Perm Military Institute of the National Guard Troops*. 2025;(1):95–106. (In Russ.).
6. Кузнецов А.С., Семёнов Е.Ю., Матросова Л.Д. Кластеризация изображений при использовании предобученных нейронных сетей. *International Journal of Open Information Technologies*. 2019;7(7):42–47.
Kuznetsov A.S., Semenov E.Y., Matrosova L.D. Image clustering using pretrained neural networks. *International Journal of Open Information Technologies*. 2019;7(7):42–47. (In Russ.).
7. Nazir S., Kaleem M. Federated Learning for Medical Image Analysis with Deep Neural Networks. *Diagnostics*. 2023;13(9):1532. <https://doi.org/10.3390/diagnostics13091532>
8. Touhami M., Ahmad Fauzi M.F., Ur Rehman Z., et al. Federated Learning for Histopathology Image Classification: A Systematic Review. *Diagnostics*. 2026;16(1):137. <https://doi.org/10.3390/diagnostics16010137>
9. Lee Sh.-M., Wu J.-L. FedUA: An Uncertainty-Aware Distillation-Based Federated Learning Scheme for Image Classification. *Information*. 2023;14(4):234. <https://doi.org/10.3390/info14040234>
10. Tang J., Ding X., Hu D., et al. FedRAD: Heterogeneous Federated Learning via Relational Adaptive Distillation. *Sensors*. 2023;23(14):6518. <https://doi.org/10.3390/s23146518>
11. Lv Y., Ding H., Wu H., et al. FedRDS: Federated Learning on Non-IID Data via Regularization and Data Sharing. *Applied Sciences*. 2023;13(23):12962. <https://doi.org/10.3390/app132312962>
12. Hsu H.-Y., Keoy K.H., Chen J.-R., et al. Personalized Federated Learning Algorithm with Adaptive Clustering for Non-IID IoT Data Incorporating Multi-Task Learning and

- Neural Network Model Characteristics. *Sensors*. 2023;23(22):9016. <https://doi.org/10.3390/s23229016>
13. Cha N., Chang L. Addressing Non-IID with Data Quantity Skew in Federated Learning. *Information*. 2025;16(10):861. <https://doi.org/10.3390/info16100861>
 14. Khan K. FedEmerge: An Entropy-Guided Federated Learning Method for Sensor Networks and Edge Intelligence. *Sensors*. 2025;25(12):3728. <https://doi.org/10.3390/s25123728>
 15. Ning W., Zhu Y., Song C., et al. Blockchain-Based Federated Learning: A Survey and New Perspectives. *Applied Sciences*. 2024;14(20):9459. <https://doi.org/10.3390/app14209459>
 16. Lee J., Kim W. DAG-Based Blockchain Sharding for Secure Federated Learning with Non-IID Data. *Sensors*. 2022;22(21):8263. <https://doi.org/10.3390/s22218263>
 17. Alghamdi A., Zhu J., Yin G., et al. Blockchain Empowered Federated Learning Ecosystem for Securing Consumer IoT Features Analysis. *Sensors*. 2022;22(18):6786. <https://doi.org/10.3390/s22186786>
 18. Chen Zh., Li D., Zhu J., et al. DACFL: Dynamic Average Consensus-Based Federated Learning in Decentralized Sensors Network. *Sensors*. 2022;22(9):3317. <https://doi.org/10.3390/s22093317>
 19. Zhao S., Zheng X., Chen J. Efficient Adversarial Training for Federated Image Systems: Crafting Client-Specific Defenses with Robust Trimmed Aggregation. *Electronics*. 2025;14(8):1541. <https://doi.org/10.3390/electronics14081541>
 20. Yin X., Wu X., Zhang X. A Trusted Federated Learning Method Based on Consortium Blockchain. *Information*. 2025;16(1):14. <https://doi.org/10.3390/info16010014>
 21. Zhu F., Hu F., Zhao Y., et al. A Secure and Fair Federated Learning Framework Based on Consensus Incentive Mechanism. *Mathematics*. 2024;12(19):3068. <https://doi.org/10.3390/math12193068>
 22. Афанасьева Д.В., Абидарова А.А., Плахина Е.А. Применение технологии «блокчейн» для цифровой идентификации пользователей. *Известия Тульского государственного университета. Технические науки*. 2019;(9):351–354.
Afanasyeva D.V., Abidarova A.A., Plahina E.A. Application of blockchain technology for digital identification of users. *News of the Tula State University. Technical Sciences*. 2019;(9):351–354. (In Russ.).
 23. Тюрин А.В., Тюляндин И.В., Мальцев В.С. и др. Обзор языков для безопасного программирования смарт-контрактов. *Труды Института системного программирования РАН*. 2019;31(3):157–176. (На англ.). [https://doi.org/10.15514/ISPRAS-2019-31\(3\)-13](https://doi.org/10.15514/ISPRAS-2019-31(3)-13)
Tyurin A.V., Tyulyandin I.V., Maltsev V.S., et al. Overview of the Languages for Safe Smart Contract Programming. *Proceedings of the Institute for System Programming of the RAS*. 2019;31(3):157–176. [https://doi.org/10.15514/ISPRAS-2019-31\(3\)-13](https://doi.org/10.15514/ISPRAS-2019-31(3)-13)
 24. Афанасьев М.Я., Фёдоров Ю.В., Крылова А.А. и др. Организация киберфизических производственных систем с использованием технологий блокчейн и смарт-контрактов. *Известия высших учебных заведений. Приборостроение*. 2019;62(3):226–234.
Afanasyev M.Ya., Fedosov Yu.V., Krylova A.A., et al. Organization of cyberphysical production systems using blockchain and smart-contracts technologies. *Journal of Instrument Engineering*. 2019;62(3):226–234. (In Russ.).

ИНФОРМАЦИЯ ОБ АВТОРАХ / INFORMATION ABOUT THE AUTHORS

Конников Евгений Александрович, кандидат экономических наук, доцент Высшей инженерно-экономической школы Института промышленного менеджмента, экономики и торговли, заведующий Научно-исследовательской лабораторией «Политех-Инвест», Санкт-Петербургский политехнический университет Петра Великого, Санкт-Петербург, Российская Федерация.

e-mail: konnikov_ea@spbstu.ru

ORCID: [0000-0002-4685-8569](https://orcid.org/0000-0002-4685-8569)

Evgenii A. Konnikov, Candidate of Economic Sciences, Associate Professor at the Graduate School of Industrial Economics, Institute of Industrial Management, Economics and Trade, Head of the Research Laboratory "Polytech-Invest", Peter the Great St. Petersburg Polytechnic University, St. Petersburg, the Russian Federation.

Санду Никита Романович, аспирант, МИРЭА – Российский технологический университет, Москва, Российская Федерация.

e-mail: sandu.nikita1997@yandex.ru

ORCID: [0009-0009-4067-7458](https://orcid.org/0009-0009-4067-7458)

Nikita R. Sandu, Postgraduate, MIREA – Russian Technological University, Moscow, the Russian Federation.

Файзуллин Ринат Васильевич, кандидат экономических наук, доцент, МИРЭА – Российский технологический университет, Москва, Российская Федерация.

e-mail: fayzullin-rv@ranepa.ru

ORCID: [0000-0002-1179-3910](https://orcid.org/0000-0002-1179-3910)

Rinat V. Faizullin, Candidate of Economic Sciences, Associate Professor, MIREA – Russian Technological University, Moscow, the Russian Federation.

Статья поступила в редакцию 30.04.2026; одобрена после рецензирования 26.06.2026; принята к публикации 07.07.2026.

The article was submitted 30.04.2026; approved after reviewing 26.06.2026; accepted for publication 07.07.2026.