УДК 004.852
DOI: 10.26102/2310-6018/2024.47.4.023

Разработка алгоритма многоклассового классификатора системы федеративного обучения, функционирующей в условиях неполноты классов локальных классификаторов

П.А. Михалев✉, М.А. Куцакин, О.В. Карамыхова

Академия Федеральной службы охраны Российской Федерации, Орёл, Российская Федерация

Резюме. Актуальность исследования обусловлена необходимостью решения задачи обучения моделей многоклассовых классификаторов, используемых в структуре системы федеративного машинного обучения, оперирующей обучающей выборкой данных, которая содержит как общедоступные данные, так и конфиденциальные данные, формирующие скрытые классы. Подобная проблема возникает в условиях обучения классификатора с использованием выборки данных, часть из которых состоит из персональной информации или данных различной степени конфиденциальности. В связи с этим данная статья направлена на исследование особенностей модели гауссовой смеси распределений как способа представления скрытых классов, представляющих конфиденциальные данные, а также обоснование выбора алгоритмического метода нахождения оценок максимального правдоподобия ее параметров. Ведущим методом решения проблемы идентификации параметров скрытых классов является обоснованно выбранная двухэтапная итерационная процедура «ожидание-максимизация» (EM-алгоритм), обеспечивающая усиление связи между пропущенными (конфиденциальными) данными и неизвестными параметрами модели данных, представленной гауссовой смесью распределений. В статье представлена схема разработанного алгоритма многоклассового классификатора системы федеративного машинного обучения, представленная параллельно выполняющимися циклами формирования локальных моделей обучения и их последующего ансамблирования в глобальную модель обучения.

Ключевые слова: федеративное машинное обучение, многоклассовая классификация, конфиденциальные обучающие данные, модель гауссовой смеси распределений, EM-алгоритм.

Для цитирования: Михалев П.А., Куцакин М.А., Карамыхова О.В. Разработка алгоритма многоклассового классификатора системы федеративного обучения, функционирующей в условиях неполноты классов локальных классификаторов. *Моделирование, оптимизация и информационные технологии.* 2024;12(4). URL: https://moitvivt.ru/ru/journal/pdf?id=1731 DOI: 10.26102/2310-6018/2024.47.4.023

Development of a multi-class classifier algorithm for a federated learning system operating in case of incomplete classes of local classifiers

P.A. Mikhalev✉, M.A. Kutsakin, O.V. Karamyhova

Russian Federation Security Guard Service Federal Academy, Oryol, the Russian Federation

Abstract. The relevance of research is due the need to solve the problem of training multi-class classifier models used in federated machine learning system structure operating with a training data set that contains both publicly available data and confidential data that forming hidden classes. A similar problem arises in the context of training a classifier using a training data set, some of which consists of personal information or data of varying degrees of confidentiality. In this regard, this article is aimed at researching the features of the Gaussian mixture model of distributions as a way of representing hidden

classes representing confidential data, as well as justifying the choice of an algorithmic method for finding maximum likelihood estimates of its parameters. The main method for solving the problem of identifying the parameters of hidden classes is a reasonably chosen two-stage iterative expectation-maximization procedure (EM-algorithm), which ensures strengthening the relationship between missing (confidential) data and unknown parameters of the data model represented by a Gaussian mixture of distributions. The article presents a diagram of the developed algorithm of a multi-class classifier for federated machine learning system, represented by parallel cycles of forming local learning models and their ensemble into a global learning model.

Keywords: federated machine learning, multi-class classification, confidential training data, Gaussian mixture model of distributions, EM-algorithm.

For citation: Mikhalev P.A., Kutsakin M.A., Karamyhova O.V. Development of a multi-class classifier algorithm for a federated learning system operating in case of incomplete classes of local classifiers. *Modeling, Optimization and Information Technology*. 2024;12(4). (In Russ.). URL: https://moitvivt.ru/ru/journal/pdf?id=1731 DOI: 10.26102/2310-6018/2024.47.4.023

Введение

Прогресс в таких относительно новых предметных областях, как системы беспилотного транспорта (Vehicular automation), интеллектуальные системы информационной поддержки и поддержки принятия решений (Virtual assistant systems), Интернет вещей (IoT – Internet of Things), а также в иных сферах деятельности основан на все более широком использовании моделей, методов и технологий машинного обучения (МО). К важными классам задач, решаемых с использованием МО, относятся задачи распознавания образов, классификации и кластеризации данных, являющиеся основой задач более высокого уровня, таких, например, как принятие решений об управляющих воздействиях на элементы автоматизированной системы на основе обработки данных об обстановке, в которой она функционирует. При этом, в общем случае, решение задачи классификации данных является основой систем поддержки принятия решения в различных сферах деятельности, таких как медицинская диагностика, информационная безопасность, машиностроительная дефектоскопия и других.

Реализация современных систем МО подразумевает разработку высокопроизводительных и легко масштабируемых центров обработки данных (ЦОД). При этом одной из тенденций развития подобных вычислительных инфраструктур является их распределенная реализация – размещение отдельных компонентов системы МО в логически или территориально распределенных вычислительных кластерах, объединяемых высокоскоростной телекоммуникационной системой (ТКС). В рамках таких распределенных инфраструктур все большее применение находят модели МО с децентрализованной схемой. В ней локальные компоненты системы МО не просто реализуют функции сбора и предварительной обработки данных, но и поддерживают собственные локальные МО (ЛМО), обучающиеся на локально ограниченных наборах данных. При этом для получения глобальной МО (ГМО) решается задача ансамблирования (ensemble) множества ЛМО. Подобный подход в [1, 2] именуется федеративное машинное обучение (federative machine learning), а системы МО на его основе именуются системами федеративного МО (СФМО).

Схема организации СФМО рассмотрена в [3] и пример ее обобщенной структуры, решающей задачу трехклассовой классификации, представлен на Рисунке 1.

Из Рисунка 1 видно, что модели ЛМО параллельно формируются в Worker-узлах СФМО и через ТКС передаются на Master-узел, осуществляющий их ансамблирование в модель ГМО. В дальнейшем полученная модель ГМО передается на Worker-узлы в качестве основы их ЛМО.

К преимуществам подобного подхода к организации СФМО относится не только повышение оперативности процесса обучения моделей, связанное с распараллеливанием процесса формирования ЛМО, но и возможность достаточно простого масштабирования структуры СФМО, требуемая, например, при увеличении числа источников данных, а также повышение точности (accuracy) классификации в рамках ЛМО за счет использования ансамблированного варианта ГМО.

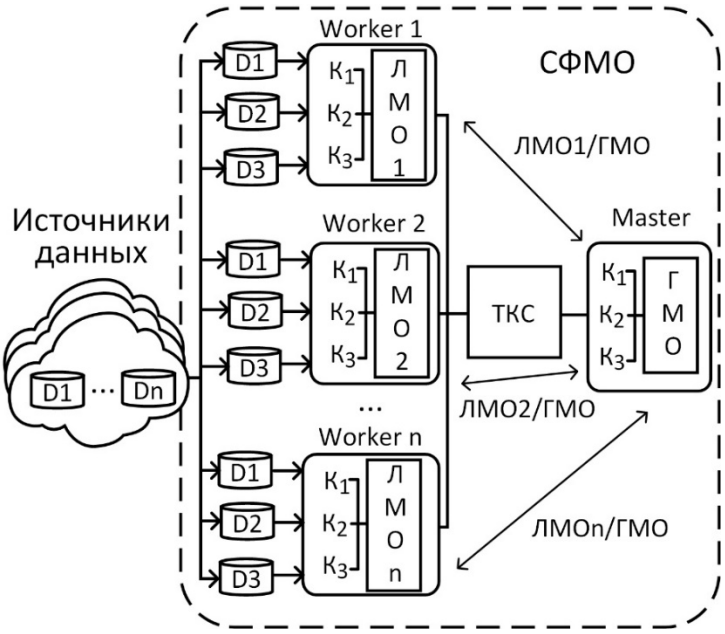

Рисунок 1 – Обобщенная схема системы федеративного машинного обучения для задачи трехклассовой классификации

Figure 1 – Generalized design of a federated machine learning system for a three-class classification problem

В рамках реализации подобной структуры СФМО существует проблема, связанная с неоднородностью данных, представляющих обучающую выборку, поступающих на входы Worker-узлов. В ряде предметных областей, использующих СФМО, некоторые данные могут носить конфиденциальный характер в пределах одного Worker-узла. Например, обучение ЛМО для классификации типа заболевания может осуществляться на основе персональных данных пациентов того учреждения, в котором эксплуатируется конкретный Worker-узел. Следовательно, в рамках задачи формирования локальных классов в ЛМО, часть из них может быть недоступна (скрыта) для других Worker-узлов, что неизбежно сказывается на полноте и точности модели ГМО. Подобная особенность функционирования СФМО иллюстрируется Рисунком 2.

Из Рисунка 2 видно, что классификаторы C^1,…, C^k для формирования моделей $ЛМО_1$,..., $ЛМО_k$ используют обучающую выборку как на основе общедоступных (ОДД) данных, так и данных, локально-конфиденциальных (ЛКД) относительно каждого Worker-узла.

В рамках исследования такая проблема формулируется как проблема формирования многоклассового классификатора (модель ГМО) в условиях неполноты классов локальных классификаторов (модели ЛМО).

В [4] делается формальная постановка этой проблемы, в частности, формализуется представление многоклассового (K-классового) классификатора C_K, как ансамбля локальных бинарных классификаторов, а также обосновывается использование функции кросс-энтропийных потерь [5] (1).

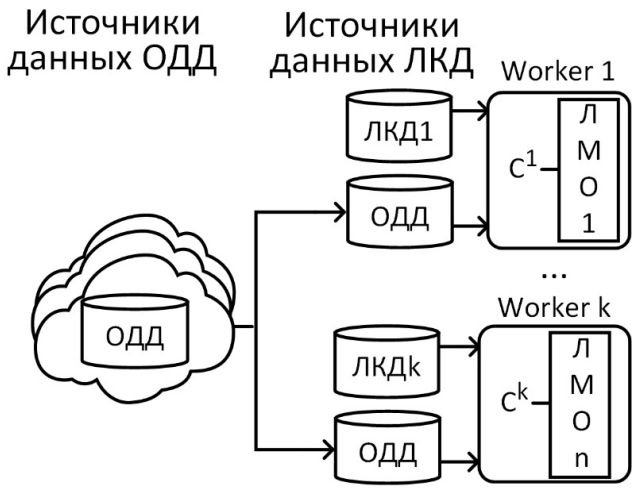

Рисунок 2 – Схема системы федеративного машинного обучения с локальными классификаторами, обучающимися на общедоступных и локально-конфиденциальных данных
Figure 2 – Diagram of a federated machine learning system with local classifiers trained on publicly available and locally confidential data

При этом, в силу наличия ЛКД в обучающих выборках классификаторов $C^1,\ldots, C^k$ делается предположение, что значение множества предикторов классификатора можно получить только путем интегрирования локальной оценки плотности вероятности значения каждого элемента данных обучающей выборки (2).

$$C^K = C^0, C^1, \ldots, C^k = \arg\min_{C^0, C^1, \ldots, C^k} \left\{ -\sum_{j=1}^{L} \sum_{i=1}^{n_j} \sum_{k=0}^{K} 1(y_{ij}=k) \log C^k(x_{ij}) \right\}, \quad (1)$$

$$C^K(X) = \sum_{j=1}^{L} C_j^k(X) \times \frac{f_X^{(j)} p_N^{(j)}}{f_X} = \sum_{j=1}^{L} C_j^k(X) \times \frac{f_X^{(j)} p_N^{(j)}}{\sum_{j=1}^{L} f_X^{(j)} p_N^{(j)}}, \quad (2)$$

где $f_X^{(j)}$ – функция распределения вероятностей предикторов, а $p_N^{(j)}$ – вероятность отнесения данных к конкретному классу. На практике значение $p_N^{(j)}$ можно получить на основе априорных данных о размере обучающей выборки, а для получения значения функции $f_X^{(j)}$, в силу ее вероятностного характера (невозможности использования простых моделей композиционных данных) в [4] предлагается рассмотрение класса моделей смеси распределений.

На основе такого предположения в рамках статьи обосновывается использование модели гауссовой смеси распределений (GMM – Gaussian mixture model) [6] и синтезируется схема алгоритма многоклассового классификатора СФМО, функционирующая в условиях неполноты классов локальных классификаторов.

Материалы и методы

Выбор модели смеси распределений, обеспечивающей адекватное представление функции распределения вероятностей предикторов $f_X^{(j)}$ модели ЛМО, требует рассмотрения особенностей как подобных моделей, так и задачи классификации, решаемой моделью ЛМО.

В [5] модель смеси распределений представляется как вариант распределения вероятностей наблюдений для некоторой обобщенной совокупности с целью определения свойств этой совокупности на основе анализа свойств частных совокупностей (подсовокупностей), входящих в ее состав.

При этом также может быть рассмотрена и обратная задача: получение априори неизвестных (ненаблюдаемых, скрытых) статистических свойств подсовокупностей на основе наблюдений свойств обобщенной совокупности. В силу выдвинутого предположения о том, что использование для обучения моделей ЛМО, обучающих выборок как на основе данных ОДД, так и данных ЛКД, можно представить в виде модели со смешанными распределениями, решение второй задачи возможно применить для разделения оценок значений элементов данных в составе их смеси.

Проведенный анализ источников, связанных с решением такой проблемы [6–8], показал, что в подобных случаях наиболее широко применяется модель гауссовой смеси распределений (GMM), которая обеспечивает представление подсовокупностей, имеющих нормальный закон распределения, внутри обобщенной совокупности.

Такая модель может быть описана тремя типами параметров:

– средними значения компонентов подсовокупности (одномерное представление);

– ковариациями средних значений компонентов подсовокупности (многомерное представление);

– весовыми коэффициентами смеси компонентов подсовокупности.

В общем случае, она может быть представлена взвешенной суммой R компонентов гауссовых плотностей распределения вероятностей:

$$p(x|\lambda) = \sum_{i=1}^{R} w_i \, g(x|\mu_i,\Sigma_i), \quad (3)$$

где x – это многомерный вектор элементов, w_i, i=1, ..., R – смеси весов этих элементов, а $g(x|\mu_i,\Sigma_i)$, i=1, ..., R – многомерная функция, определяющая компоненты гауссовой плотности вероятностей, которая представляется как:

$$g(x|\mu_i,\Sigma_i) = \frac{1}{(2\pi)^{\frac{D}{2}}\left|\Sigma_i\right|_2^{\frac{1}{2}}} \exp\left\{-\frac{1}{2}(x\text{-}\mu_i)'\Sigma_i^{-1}(x\text{-}\mu_i)\right\}, \quad (4)$$

где D – размерность векторного пространства элементов, μ_i – среднее значение вектора, а Σ_i – ковариационная матрица.

При этом параметризация полной модели GMM выполняется на основе средних значений векторов, ковариационных матриц и весов смеси из всех плотностей вероятностей R компонентов:

$$\lambda=\{w_i,\mu_i,\Sigma_i\},\ i=1,\ ...,\ R. \quad (5)$$

Следовательно, для рассматриваемой проблемы (представление ненаблюдаемых классов модели ЛМО) функцию распределения вероятностей предикторов в общем случае можно представить GMM с R компонентами:

$$f_X^{(J)}(X) = \sum_{r=1}^{R} \pi_r^j \, f_{x|z_j=r}(X). \quad (6)$$

Таким образом, задачей, связанной с получением параметров ненаблюдаемых классов моделей ЛМО на основе использования для их представления модели GMM, является оценивание параметров λ (выражение 5) этой модели, и выбор тех из них, которые наиболее полно представляют распределение векторов признаков ненаблюдаемых классов. В [8] выполнено детальное исследование методов оценки параметров GMM, среди которых наиболее известным и, в некотором роде, устоявшимся является метод оценивания максимального правдоподобия (Maximum Likelihood) – поиска таких параметров модели GMM, которые максимизируют ее правдоподобие GMM с учетом используемых элементов. Исходя из выражения 5, для

последовательности R векторов (с учетом их независимости) правдоподобие модели GMM на некотором интервале T определяется как:

$$p(X|\lambda) = \prod_{t=1}^{T} p(x_t|\lambda). \quad (7)$$

Очевидно, в силу нелинейности функции параметров λ получение аппроксимации $p(X|\lambda)$ аналитически невозможно. Поэтому для решения этой задачи широкое распространение получили итеративные методы, которые позволяют, начиная с функции λ (первая итерация), оценить вид новой функции $\bar{\lambda}$, для которого выполняется условие:

$$p\left(X\middle|\bar{\lambda}\right) \geq p(X|\lambda). \quad (8)$$

На следующей итерации полученный вариант $\bar{\lambda}$ становится начальным. Этот цикл повторяется до тех пор, пока не будет достигнут заданный порог сходимости.

Наиболее известной реализацией интерактивных методов является EM-алгоритм [9], состоящий из следующих шагов:

1. Условное ожидание (E (expectation)-шаг).
2. Максимизация (M (maximization)-шаг).

Рассмотрим его использование применительно к задаче оценивания параметров функции вероятности ненаблюдаемых классов модели ЛМО.

На E-шаге рассчитываются условные ожидания отсутствующих данных (ЛКД) с учетом всей совокупности наблюдаемых данных и Θ – оценок параметров модели GMM. При этом условные ожидания ненаблюдаемых данных с учетом наблюдаемых данных и оценок параметров модели GMM вычисляются на основе выражения:

$$Q(\Theta_0|\Theta_n) = E_{Z|x,\Theta_n}[\log L(\Theta,x,z)], \quad (9)$$

где $L(\Theta, x, z)$ – функция правдоподобия, Θ – вектор параметров, Θ_n – оценка параметров модели GMM, x – наблюдаемые данные (смесь данных ОДД и ЛКД), z – ненаблюдаемые данные (ЛКД).

На M-шаге выполняется поиск оценки параметра Θ, которая максимизирует функцию правдоподобия данных E-шага:

$$\Theta^* = \arg_{\Theta} max\, Q\,(\Theta_0|\Theta_n). \quad (10)$$

Таким образом, шаги E и M чередуются с целью обновления некоторой оценки Θ_n неизвестных на каждой итерации оценок параметров Θ.

Альтернативой EM-алгоритма для оценивания параметров модели GMM является метод апостериорного максимума (MAP – maximum a posteriori probability) [10]. Как и EM-алгоритм, метод MAP является двухэтапной итерационной процедурой. Однако, в отличие от шага максимизации в EM-алгоритме, обновленная статистическая оценка Θ_n объединяются с оценками предыдущих параметров смеси данных с помощью коэффициента смешивания, значение которого зависит от данных.

Поскольку специфика данных ЛКД не в полной мере обеспечивает получение апостериорной статистики, которая необходима для выполнения этого шага метода MAP, в исследовании было принято решение использовать EM-алгоритм.

Обобщенная схема разработанного алгоритма многоклассовой классификации системы федеративного обучения, функционирующей в условиях неполноты классов ее ЛМО, объединяющая процедуры, выполняющиеся на уровнях ЛМО и ГМО, представлена на Рисунке 3.

Из Рисунка 3 видно, что множество моделей ЛМО реализуют процедуру формирования локального классификатора $\hat{C}_j^k(X)$. При этом на основе данных ОДД и собственных данных ЛКД реализуются итерации EM-алгоритма, обеспечивающего

получение вероятности отнесения отсутствующих (ненаблюдаемых) данных к тому или иному классу.

На уровне ГМО реализуется цикл ансамблирования параметров множества локального классификатора $\hat{C}_j^k(X)$ с полученными значениями классов данных ЛКД, и получение классификатора $C^K(X)$.

В общем случае подобная схема алгоритма соответствует традиционной схеме алгоритма функционирования системы СФМО (Рисунок 1). При этом, включение в этап формирования классификаторов моделей ЛМО итераций ЕМ-алгоритма, обеспечивающего получение оценок вероятностных характеристик ненаблюдаемых классов данных ЛКД, обеспечивает необходимый уровень полноты классификатора модели ГМО.

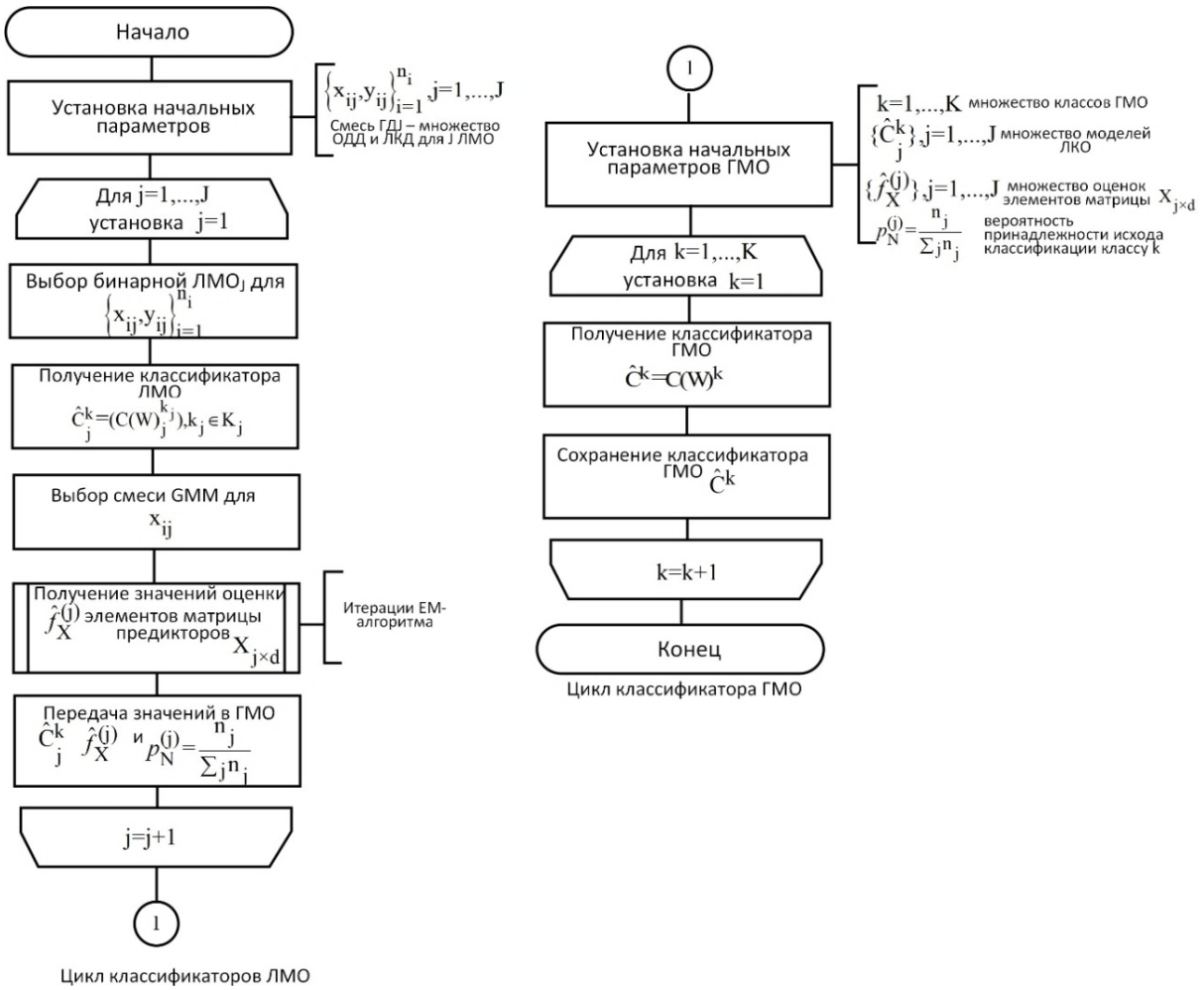

Рисунок 3 – Схема алгоритма многоклассовой классификации системы федеративного обучения, функционирующей в условиях неполноты классов ее ЛМО

Figure 3 – Diagram of a of the algorithm of multi-class classification of the system of federated learning, functioning in case incompleteness of classes its local learning models

Очевидно, что полученные в ходе реализации ЕМ-алгоритма оценки являются прогнозными значениями, что может оказывать влияние на точность классификации модели ГМО. Однако в сравнении с классификацией модели ГМО, функционирующей в условиях неполноты классов, полученное значение точности модифицированного будет превышать возможности традиционного алгоритма за счет формирования полной матрицы классов.

Заключение

Статья посвящена решению проблемы снижения точности многоклассового классификатора глобальной модели обучения в системах федеративного машинного обучения, функционирующих в условиях априорной неполноты классов. Анализ существующих исследований в данной области позволил установить, что одним из путей решения подобной проблемы является представление подмножества значений ненаблюдаемых классов с помощью модели Гауссовой смеси распределений. Для получения значений оценок компонентов гауссовой смеси распределений был обоснованно выбран EM-алгоритм.

На базе представленного выше подхода был разработан модифицированный алгоритм функционирования компонентов системы федеративного машинного обучения, представляющий совокупность параллельно функционирующих алгоритмов локальных моделей обучения, реализующих цикл формирования локальных классификаторов с учетом получения оценок вероятностей ненаблюдаемых классов, а также алгоритма их ансамблирования в модель глобального многоклассового классификатора. Подобное решение обеспечивает повышение точности классификации многоклассовых классификаторов систем федеративного машинного обучения, использующих в обучающих выборках конфиденциальные данные.

Дальнейшие направления исследования направлены на оптимизацию предложенного алгоритма за счет сокращения времени реализации циклов итерационных процедур.

СПИСОК ИСТОЧНИКОВ / REFERENCES

1. Wahab O.A., Mourad A., Otrok H., Taleb T. Federated Machine Learning: Survey, Multi-Level Classification, Desirable Criteria and Future Directions in Communication and Networking Systems. *IEEE Communications Surveys & Tutorials.* 2021;23(2):1342–1397. https://doi.org/10.1109/COMST.2021.3058573
2. Lo S.K., Lu Q., Zhu L., Paik H.-Y., Xu X., Wang C. Architectural Patterns for the Design of Federated Learning Systems. *Journal of Systems and Software*. 2022;191. https://doi.org/10.1016/j.jss.2022.111357
3. Mikhalev P.A., Kutsakin M.A., Mironov O.Yu. On the need for parametric optimization of systems with federated machine learning. In: *Modern Informatization Problems in Simulation and Social Technologies (MIP-2023'SCT): Proceedings of the XXVIII-th International Open Science Conference, 15 November 2022 – 15 January 2023, Yelm, WA, USA.* Yelm: Science Book Publishing House LLC; 2023. pp. 37–41. (In Russ.).
4. Allwein E.L., Schapire R.E., Singer Y. Reducing multiclass to binary: a unifying approach for margin classifiers. *Journal of Machine Learning Research*. 2001;1:113–141.
5. Goodman R., Miller J.W., Smyth P. Objective Functions For Neural Network Classifier Design. In: *1991 IEEE International Symposium on Information Theory, 24–28 June 1991, Budapest, Hungary.* IEEE; 1991. pp. 87. https://doi.org/10.1109/ISIT.1991.695143
6. Galar M., Fernández A., Barrenechea E., Bustince H., Herrera F. An overview of ensemble methods for binary classifiers in multi-class problems: Experimental study on one-vs-one and one-vs-all schemes. *Pattern Recognition*. 2011;44(8):1761–1776. https://doi.org/10.1016/j.patcog.2011.01.017
7. Arı Ç., Aksoy S., Arıkan O. Maximum likelihood estimation of Gaussian mixture models using stochastic search. *Pattern Recognition*. 2012;45(7):2804–2816. https://doi.org/10.1016/j.patcog.2011.12.023

8. Tohka J., Krestyannikov E., Dinov I.D., Graham A.M., Shattuck D.W., Ruotsalainen U. Genetic Algorithms for Finite Mixture Model Based Voxel Classification in Neuroimaging. *IEEE Transactions on Medical Imaging*. 2007;26(5):696–711. https://doi.org/10.1109/TMI.2007.895453
9. Martínez A.M., Vitrià J. Learning mixture models using a genetic version of the EM algorithm. *Pattern Recognition Letters*. 2000;21(8):759–769. https://doi.org/10.1016/S0167-8655(00)00031-3
10. Pernkopf F., Bouchaffra D. Genetic-based EM algorithm for learning Gaussian mixture models. *IEEE Transactions on Pattern Analysis and Machine Intelligence*. 2005;27(8):1344–1348. https://doi.org/10.1109/TPAMI.2005.162

ИНФОРМАЦИЯ ОБ АВТОРАХ / INFORMATION ABOUT THE AUTHORS

Михалев Павел Андреевич, сотрудник, Академия Федеральной службы охраны Российской Федерации, Орёл, Российская Федерация.
e-mail: pavel_057@list.ru

Pavel A. Mikhalev, employee, Russian Federation Security Guard Service Federal Academy, Oryol, the Russian Federation.

Куцакин Максим Алексеевич, кандидат технических наук, сотрудник, Академия Федеральной службы охраны Российской Федерации, Орёл, Российская Федерация.
e-mail: max_kooks@mail.ru

Maksim A. Kutsakin, Candidate of Technical Sciences, employee, Russian Federation Security Guard Service Federal Academy, Oryol, the Russian Federation.

Карамыхова Оксана Викторовна, кандидат педагогических наук, сотрудник, Академия Федеральной службы охраны Российской Федерации, Орёл, Российская Федерация.
e-mail: karamihova82@mail.ru

Oksana V. Karamyhova, Candidate of Pedagogical Sciences, employee, Russian Federation Security Guard Service Federal Academy, Oryol, the Russian Federation.

Статья поступила в редакцию 30.10.2024; одобрена после рецензирования 18.11.2024; принята к публикации 20.11.2024.

The article was submitted 30.10.2024; approved after reviewing 18.11.2024; accepted for publication 20.11.2024.