УДК 004.056 Обзорная статья

https://doi.org/10.32603/2071-8985-2024-17-5-74-82

# Федеративное обучение (FL) – Обзор

**М. Аль-Тамими✉, М. Б. Хассан, С. А. Аббас**

Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В. И. Ульянова (Ленина), Санкт-Петербург, Россия

✉almokhalad44@gmail.com

**Аннотация.** Рассмотрены основные аспекты федеративного обучения (FL) в контексте систем обнаружения вторжений (IDS) в сетях интернета вещей (IoT). Федеративное обучение представляет собой инновационный подход к обучению моделей машинного обучения на распределенных устройствах, минимизирующий необходимость передачи чувствительных данных на центральные серверы. FL классифицируется на горизонтальное, вертикальное и федеративное трансферное обучение и рассматривается их применение в системах IDS. Дополнительно анализируется структура сети FL, включая централизованное и децентрализованное FL. На основе проведенного обзора можно сделать вывод о перспективности использования FL в сетях IoT для повышения конфиденциальности данных и эффективности обнаружения аномалий.

**Ключевые слова:** федеративное обучение, системы обнаружения вторжений, интернет вещей, горизонтальное федерированное обучение, децентрализованное федерированное обучение

**Для цитирования:** Аль-Тамими М., Хассан М. Б., Аббас С. А. Федеративное обучение (FL) – Обзор // Изв. СПбГЭТУ «ЛЭТИ». 2024. Т. 17, № 5. С. 74–82. doi: 10.32603/2071-8985-2024-17-5-74-82.

**Конфликт интересов.** Авторы заявляют об отсутствии конфликта интересов.

Review article

# Federated Learning (FL) – Overview

**M. Al-Tameemi✉, M. B. Hassan, S. A. Abass**

Saint Petersburg Electrotechnical University, Saint Petersburg, Russia

✉ almokhalad44@gmail.com

**Abstract.** Explores the fundamental aspects of federated learning (FL) in the context of intrusion detection systems (IDS) within Internet of Things (IoT) networks. Federated learning presents an innovative approach to training machine learning models on distributed devices, thereby minimizing the need to transmit sensitive data to central servers. We classify FL into horizontal, vertical, and federated transfer learning and examine their application in IDS systems. Additionally, we analyze the network structure of FL, encompassing centralized and decentralized FL. Based on the conducted review, it can be concluded that FL holds promise for enhancing data privacy and anomaly detection efficiency in IoT networks.

**Keywords** federated learning, intrusion detection systems, Internet of Things, horizontal federated learning, decentralized federated learning

**For citation:** Al-Tameemi M., Hassan M. B., Abas S. A. Federated Learning (FL) – Overview // LETI Transactions on Electrical Engineering & Computer Science. 2024. Vol. 17, no. 5. P. 74–82. doi: 10.32603/2071-8985-2024-17-5-74-82.

**Conflict of interest.** The authors declare no conflicts of interest.

**Введение.** Федеративное обучение (Federated Learning, FL) представляет собой инновационный подход к машинному обучению на распределенных устройствах. В отличие от традиционного централизованного подхода, при котором данные собираются на центральном сервере для обучения

модели [1], он позволяет обучать модель на нескольких устройствах, получая обновления модели локально и передавая их для агрегации [2]. Этот подход дает возможность справиться с вызовами, связанными с масштабируемостью, конфиденциальностью и затратами на связь, которые возникают при использовании централизованных методов обучения. FL применяется в различных областях – в медицинских приложениях, финансовой аналитике и мобильных приложениях [3], благодаря своим уникальным характеристикам, которые применяют новые методы обучения, учитывая современные требования к конфиденциальности и масштабируемости. Федеративное обучение предлагает ряд важных преимуществ для приложений в области интернета вещей (IoT):

– улучшение конфиденциальности данных: FL не требует передачи исходных данных на центральный сервер для обучения модели, что минимизирует риск утечки чувствительной информации о пользователях;

– FL помогает снизить задержки в коммуникации и экономить сетевые ресурсы, поскольку данные обрабатываются локально на устройствах;

– повышение качества обучения: привлечение вычислительных ресурсов и разнообразных наборов данных с различных устройств IoT, повышение качества обучения моделей.

Кроме того, FL показывает свою эффективность в обнаружении аномалий на стороне клиента в сетях IoT. Федеративное обучение позволяет обнаруживать аномальное поведение без раскрытия чувствительных данных на центральном сервере. Используя модели машинного обучения на устройствах, оно значительно повышает безопасность и позволяет реагировать на угрозы безопасности, сохраняя конфиденциальность данных пользователей. Федеративное обучение нашло применение в различных областях IoT, в смарт-здравоохранении, смарт-транспорте и т. д., где его использование совместно с системами обнаружения аномалий становится более актуальным.

**IDS на основе федеративного обучения.** С момента своего появления в 2016 г. [4] FL преобразовало множество интеллектуальных приложений, предлагая новые AI-решения с распределенной и конфиденциальной природой. Появление этой новой распределенной технологии искусственного интеллекта имеет потенциал изменить текущие системы с передовыми архитектурами FL. В связи с последними достижениями в мобильной аппаратуре и нарастающими опасениями относительно утечек конфиденциальной информации FL особенно привлекательно для создания распределенных систем, перемещая функции искусственного интеллекта, например обучение данных ИИ, к краю сети с данными. В результате данные пользователя никогда не передаются напрямую третьей стороне, при этом обеспечивается совместное обучение общей глобальной модели, что приносит пользу в плане экономии ресурсов сети и повышения уровня конфиденциальности. FL может стать сильной альтернативой традиционным централизованным подходам и помочь ускорить развертывание услуг и приложений в большем масштабе. Здесь представлена ключевая концепция федеративного обучения и затем описаны некоторые важные его категории, используемые в сетях.

***Основная концепция FL.*** Концепция федеративного обучения в системах обнаружения вторжений (Intrusion Detection Systems, IDS) состоит из двух основных элементов: клиенты данных, например устройства в сети, и агрегирующий сервер, расположенный централизованно (рис. 1). Пусть $K = \{1, 2, 3, \ldots, k\}$ обозначает набор участников, которые используют свои устройства – компьютеры или серверы – для совместной реализации алгоритма FL для выполнения задач обнаружения вторжений. Например, в системе безопасности сети различные устройства могут участвовать в совместном процессе FL для обнаружения и устранения потенциальных угроз безопасности, анализируя совместно шаблоны сетевого трафика.

В современных архитектурах сетевой безопасности федеративное обучение играет ключевую роль в улучшении общей способности обнаружения посредством распределения механизмов обнаружения по нескольким устройствам в сети, снижая таким образом зависимость от одного централизованного сервера. FL позволяет устройствам и агрегирующему серверу совместно обучать общую глобальную модель, сохраняя при этом исходные данные локально на каждом устройстве. В процессе FL каждое участвующее устройство $k$ вносит свой вклад в обучение общей модели, используя свой собственный набор данных $D_k$. После локального обучения модель FL, обученная на каждом устройстве, называется локальной моделью $w_k$. После локального обучения устройства передают свои обновления локальной модели на агрегирующий сервер, который сводит их для построения обобщенной – глобальной $w_G$ модели. Используя распределенное обучение на данных всех устройств, агрегирующий сервер может улучшить точность обнаружения, не нарушая

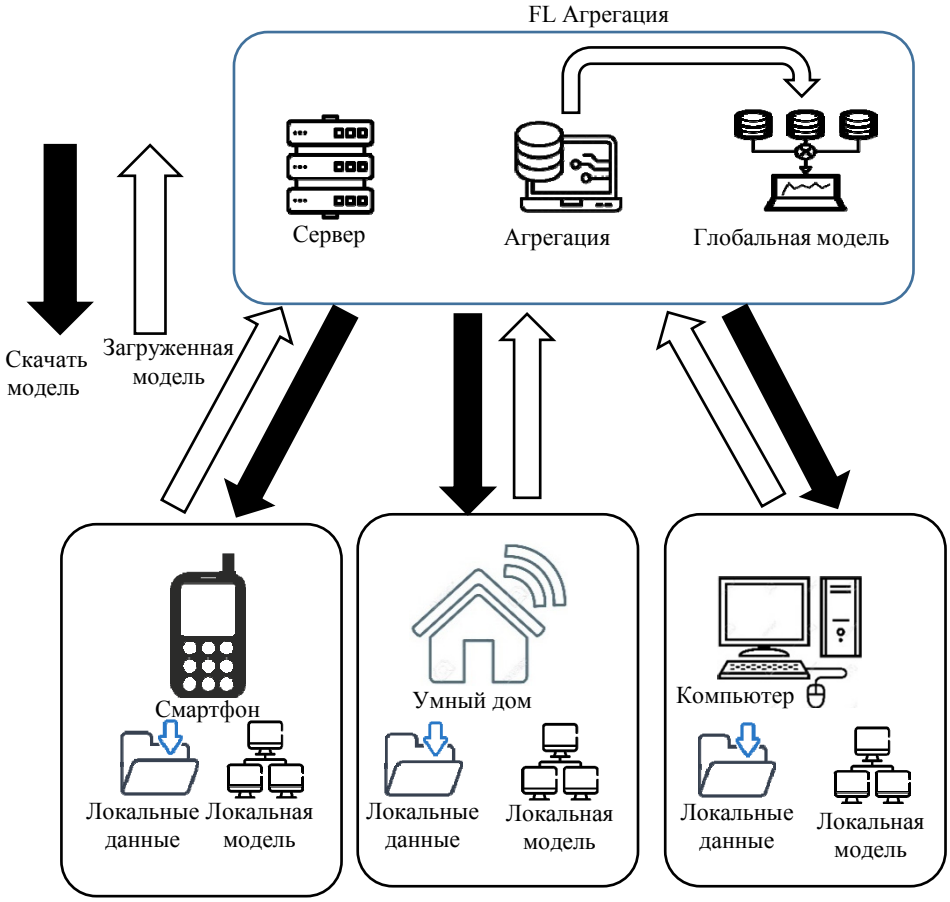


*Рис. 1.* Сетевая архитектура и коммуникационный процесс для Fl-IoT
*Fig 1.* The network architecture and communication process for Fl-IoT

конфиденциальность данных каждого устройства. Как показано на рис. 2, типичный процесс FL в IDS включает в себя следующие основные шаги:

1. *Инициализация системы и выбор устройств*: Агрегатор выбирает задачи IDS – такие, как распознавание человеческой активности, и настраивает параметры обучения, например скорости обучения и количество итераций коммуникации. Также выбирается подмножество устройств IoT для участия в процессе FL. Несколько возможных факторов для выбора включают в себя условия канала и важность локальных обновлений каждого устройства [5].

2. *Распределенное локальное обучение и обновления*. После настройки конфигурации обучения сервер инициализирует новую модель $\left(w_G^0\right)$ и передает ее устройствам IoT для начала распределенного обучения. Каждое устройство $k$ обучает локальную модель, используя собственный набор данных $D_k$, и вычисляет обновление $w_k$, минимизируя функцию потерь $F(k_w)$ [19]

$$w_k^0 = \arg\min_{wk} F(wk),\ k \in K,$$

где функция потерь может отличаться для различных алгоритмов FL [6]. Например, с набором пар ввода/вывода $\{(x_i, y_i)\}^k\ i=1$ функция потерь линейной регрессии FL может быть определена как [19]

$$F(wk) = \frac{1}{2}\sum_{i=1}^{k}\left(x_i^{\mathrm{T}} w_k - y_i\right)^2.$$

Затем каждый клиент $k$ загружает вычисленное обновление $w_k$ на сервер для агрегации.

3. *Агрегация модели и загрузка*. После сбора всех обновлений модели от локальных клиентов сервер сводит их воедино и вычисляет новую версию глобальной модели [19]:

$$w_G = \frac{1}{\sum_{k\in K}|D_k|w_k},$$

решая следующую задачу оптимизации:

$$(P1):\ \min_{w_k \in K}\frac{1}{k}\sum_{k=1}^{k}F\left(w_k\right)$$

при условии: $(C1)\, w_1 = w_2 = \ldots w_k = w_G$ ,

где функция потерь отражает точность алгоритма FL – например, точность задачи классификации объектов на основе FL [7]. Более того, ограничение (C1) гарантирует, что все клиенты и сервер используют одну и ту же обучающую модель для задачи FL после каждого цикла обучения. (P1) – это задача оптимизации, которая минимизирует среднюю функцию потерь каждого устройства $k$ при условии, что все локальные модели равны глобальной модели $w_G$. После вычисления модели сервер транслирует новое глобальное обновление всем клиентам для оптимизации локальных моделей в следующем цикле обучения. Процесс FL повторяется до сходимости глобальной функции потерь или достижения желаемой точности.

***Классификация FL, секционирование данных.*** Основываясь на том, как обучающие данные распределяются по выборке и пространствам признаков, эту категорию можно разделить на три небольших класса, включая горизонтальное, вертикальное FL и федеративное трансферное обучение [8], как показано на рис. 2.

*Горизонтальное федеративное обучение HFL*. Традиционное FL предполагает, что каждая сторона имеет одинаковый набор функций, но разные данные. Недавно был проведен анализ более реалистичного сценария в рамках FL, который предполагает вертикальное распределение различных признаков среди участников [9]. HFL предполагает, что разные стороны имеют одинаковый набор данных, но у каждой стороны есть только непересекающийся поднабор функций. Этот подход привлекает все больше внимания в связи с его потенциалом для расширения участия в различных отраслях – здравоохранении, финансах, банковском деле, – где конфиденциальность играет ключевую роль. Однако, несмотря на это, существующие методы HFL не решают некоторые важные проблемы, что ограничивает их применимость на практике [10].

HFL может стать мощным инструментом для совместного обучения моделей на чувствительных данных без утечки конфиденциальной информации [11]. Однако для его успешного применения необходимо решить некоторые текущие проблемы и разработать эффективные методы агрегации и адаптации.

Существует проблема несбалансированности данных, что означает, что различные типы аномального поведения могут быть представлены в данных неравномерно. Например, количество обычного сетевого трафика может значительно превышать количество атакующего трафика. Несбалансированные данные могут снизить эффективность обнаружения аномалий, так как модель может быть недостаточно обучена на менее представленных классах аномалий.

*Проблема гетерогенности данных*: HFL в системах IDS требует согласованности данных и моделей между различными устройствами, участвующими в процессе обучения. Однако данные от различных устройств могут иметь различные форматы, структуры и характеристики из-за различий в сетевых архитектурах, конфигурациях и типах атак. Эта гетерогенность данных может затруднить эффективное согласование и объединение информации для обучения общей модели IDS.

*Вертикальное федеративное обучение* (*VFL*). VFL представляет собой концепцию коллективного обучения модели на наборе данных, в котором признаки данных разделены между несколькими сторонами [12]. Например, различные организации здравоохранения могут иметь разные данные об одном пациенте. Учитывая чувствительность данных, эти две организации не могут просто объединить свою информацию, не нарушив приватность этого человека. Поэтому машинное обучение должно проводиться коллективно и данные должны храниться на соответствующих площадках [12]. У алгоритмов машинного обучения для вертикально разделенных данных существуют следующие проблемы:

1. Перегрузка коммуникации: VFL требует частой коммуникации между различными сторонами, участвующими в процессе федеративного обучения. Эта коммуникационная нагрузка может быть значительной, особенно при работе с большими наборами данных или большим количеством сторон.

2. Неравномерность и дисбаланс данных: распределение данных среди разных сторон может быть неравномерным, что приводит к проблемам с неравномерностью данных или дисбалансом классов. Это может повлиять на производительность модели федеративного обучения, особенно если эта проблема не будет должным образом рассмотрена в процессе обучения.

3. Риски безопасности и конфиденциальности: в то время как VFL стремится сохранить конфиденциальность, распределяя данные, по-прежнему существуют потенциальные риски безопасности, связанные с обменом обновлениями модели и градиентами между различными сторонами.

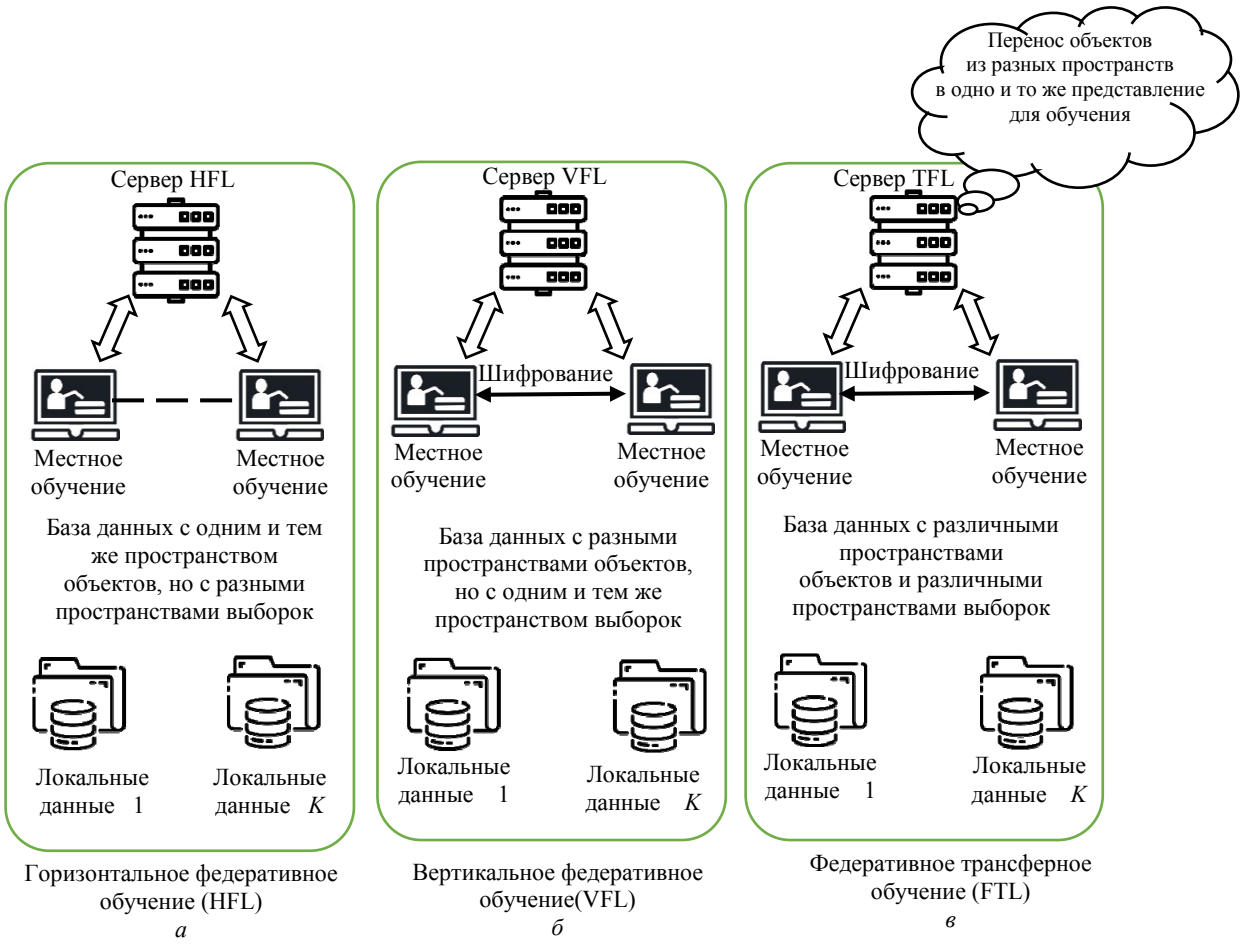


*Рис. 2.* Типы моделей FL с секционированием данных
*Fig. 2.* Types of FL models with data partitioning

*Трансферное федеративное обучение* (*FTL*). Трансферное федеративное обучение представляет собой особый случай федеративного обучения, который отличается как от горизонтального, так и от вертикального федеративного обучения. В контексте федеративного обучения два набора данных различаются в пространстве признаков. Это относится к данным, собранным из предприятий различной, но схожей природы или предприятий, находящихся на больших расстояниях друг от друга. В результате различий в характере бизнеса у этих предприятий есть только ограниченное пересечение в пространстве признаков [12].

Трансферное федеративное обучение направлено на разработку эффективной модели для целевой области и использует знания, полученные из других (исходных) областей. В отличие от горизонтального и вертикального федеративного обучения, где существует обширное пересечение в пространстве признаков или пользователей/образцов между наборами данных, FTL используется, когда пересечение как в пространстве признаков, так и в пространстве образцов невелико (рис. 2).

Методика FTL основана на использовании модели, обученной на образцах и пространстве признаков исходной области. Затем FTL адаптирует эту модель для повторного использования в целевом пространстве таким образом, что модель может быть применена к непересекающимся образцам, используя знания, полученные из непересекающихся признаков исходной области.

***Классификация FL.*** Существуют два значимых типа архитектуры FL: децентрализованная и централизованная [11] (рис. 3).

*Децентрализованное FL*. Истинная децентрализация подразумевает, что алгоритм обучения выполняется на данных, распределенных по нескольким клиентам, и никакие данные никогда не покидают устройства клиента. Другими словами, алгоритм выполняется в рамках данных силохранилищ [13]. Это важный момент, поскольку устраняется необходимость передачи данных в центральное местоположение и избегаются потенциальные риски и затраты, связанные с этим. Обратите внимание, что передача промежуточных моделей или градиентов, вероятно, менее

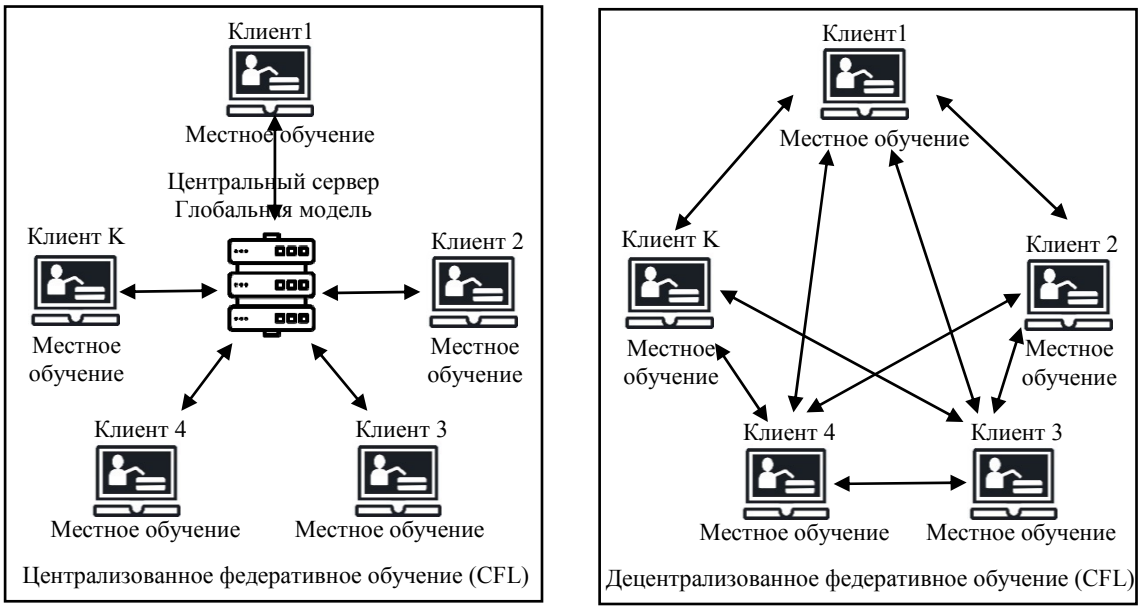


*Рис. 3.* Архитектурный дизайн централизованного и децентрализованного FL
*Fig. 3:* Architectural design of centralized and decentralized FL

рискованна (затратна), чем передача сырых данных, хотя даже в этих случаях передачи можно избежать с помощью вычислений на устройствах (без необходимости сетевого общения) [14]. Более того, децентрализация в своей крайней форме (чистые вычисления на устройствах) может предложить преимущества в области конфиденциальности данных, избегая сценариев, где данные передаются третьим сторонам, которые помогают с обучением, но которым нет необходимости иметь доступ к фактическим сырым данным [15].

*Централизованное FL*. В централизованной архитектуре FL «рабы» (рабочие) только вычисляют градиенты; «мастер» (т. е. параметрический сервер) получает параметры от всех «рабов» и распространяет последние глобальные параметры им обратно для обновления на следующем этапе обучения [16]. Это централизованное обучение требует высокой стоимости коммуникации между «рабами» и сервером. Тем не менее, централизованные архитектуры необходимы для достижения согласованности модели, особенно когда используется параллелизм данных. Существует множество стратегий обновления параметров для поддержания согласованности глобальной модели, относящихся к модели синхронизации между вычислительными узлами [17]. В этом отношении асинхронный параллельный (ASP) и булк синхронный параллельный (BSP) [18] – наиболее распространенные подходы к обновлению параметров в распределенной системе обучения. BSP и ASP обновляют параметры одновременно с получением всех градиентов от группы вычислительных узлов (барьерная синхронизация) и только от одного любого узла (без синхронизации) соответственно. Как правило, BSP относительно медленен из-за времени простоя ожидания, в то время как ASP быстрее, так как он не выполняет никакой синхронизации; в качестве компромисса сходимость в BSP гарантирована, но не определена в ASP [20]. SSP представляет собой промежуточное решение, балансирующее между BSP и ASP, которое выполняет расслабленную синхронизацию.

**Заключение.** Хотелось бы подчеркнуть значимость федеративного обучения в области систем обнаружения вторжений в сетях интернета вещей. FL предоставляет эффективный механизм обучения моделей без необходимости централизованного хранения и обработки данных, что способствует повышению конфиденциальности и снижению затрат на связь. Классификация и анализ различных подходов FL позволяет выявить их преимущества и недостатки в контексте применения в сетях IoT. Дальнейшие исследования в этой области могут помочь оптимизировать методы обнаружения аномалий и повысить общую безопасность в сетях интернета вещей.

## Список литературы

1. A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications / L. Jie, W. Yu, N. Zhang, X. Yang, H. Zang, W. Zhao // IEEE Internet of Things J. 2017. Vol. 4, no. 5. P. 1125–1142. doi: 10.1109/JIOT.2017.2683200.

2. Mehdi M., Al-Fuqaha A. Enabling cognitive smart cities using big data and machine learning: Approaches and challenges // IEEE Communications Magazine. 2018. Vol. 56, no. 2. P. 94–101. doi: 10.1109/MCOM.2018.1700298.

3. Application of machine learning in wireless networks: Key techniques and open issues / S. Yaohua, M. Peng, Y. Zhou, Y. Huang, S. Mao // IEEE Communications Surveys & Tutorials. 2019. Vol. 21, no. 4. P. 3072–3108. doi: 10.1109/COMST.2019.2924243.

4. Communication-efficient learning of deep networks from decentralized data / M. Brendan, E. Moore, D. Ramage, S. Hampson, B. A. Arcas // Artificial intelligence and statistics. 2017. P. 1273–1282. URL: https://proceedings.mlr.press/v54/mcmahan17a?ref=https://githubhelp.com (дата обращения: 24.03.2024).

5. Federated learning in mobile edge networks: A comprehensive survey / L. Wei, Y. Bryan, N. C. Luong, D. T. Hoang, Y. Jiao, Y-C. Liang, Q. Yang, D. Niyato, C. Miao // IEEE Communications Surveys & Tutorials. 2020. Vol. 22, no. 3. P. 2031–2063. doi: 10.1109/COMST.2020.2986024.

6. Federated optimization: Distributed machine learning for on-device intelligence / K., Jakub, H. B. McMahan, D. Ramage, P. Richtárik. doi: 10.48550/arXiv.1610.02527 (дата обращения: 02.04.2024).

7. A joint learning and communications framework for federated learning over wireless networks / C. Mingzhe, Z. Yang, W. Saad, C. Yin, H. V. Poor, S. Cui // IEEE Transactions on Wireless Communications. 2020. Vol. 20, no. 1. P. 269–283. doi: 10.1109/TWC.2020.3024629.

8. Federated machine learning: Concept and applications / Y. Qiang, Y. Liu, T. Chen, Y. Tong // ACM Transactions on Intelligent Systems and Technol. (TIST) 10. 2019, no. 2. P. 1–19. doi: 10.1145/3298981 (дата обращения: 02.04.2024).

9. Privacy-preserving traffic flow prediction: A federated learning approach / L. Yi, J. Q. James, J. Kang, D. Niyato, S. Zhang // IEEE Internet of Things J. 2020. Vol. 7, no. 8. P. 7751–7763. doi: 10.1109/JIOT.2020.2991401.

10. Privacy-preserving asynchronous vertical federated learning algorithms for multiparty collaborative learning / G. Bin, A. Xu, Z. Huo, C. Deng, H. Huang // IEEE Transactions on Neural Networks and Learning Systems. 2021. Vol. 33, no. 11. P. 6103-6115. doi: 10.1109/TNNLS.2021.3072238.

11. Vafl: a method of vertical asynchronous federated learning / C. Tianyi, X. Jin, Y. Sun, W. Yin. doi: 10.48550/arXiv.2007.06081 (дата обращения: 02.04.2024).

12. Sudipan S., Bovolo F., Bruzzone L. Building change detection in VHR SAR images via unsupervised deep transcoding // IEEE Transactions on Geoscience and Remote Sensing. 2020. Vol. 59, no. 3. P. 1917–1929. doi: 10.1109/TGRS.2020.3000296.

13. Christopher B., Fan Z., Andras P. A review of privacy-preserving federated learning for the Internet-of-Things // Federated Learning Systems: Towards Next-Generation AI. P. 21–50. doi: 10.1007/978-3-030-70604-3_2 (дата обращения: 24.03.2024).

14. Zhijin Q., Li G. Y., Ye H. Federated learning and wireless communications // IEEE Wireless Communications. 2021. Vol. 28, no. 5. P. 134–140. doi: 10.1109/MWC.011.2000501.

15. Mathilde R., Pasquin D., Troncoso C. Can decentralized learning be more robust than federated learning? doi: 10.48550/arXiv.2303.03829 (дата обращения: 02.04.2024).

16. Efficient and less centralized federated learning / C. Li, Z. Liu, Z. Wang, A. Shrivastava // In Machine Learning and Knowledge Discovery in Databases. Research Track: European Conf., ECML PKDD. Bilbao, Spain: Springer International Publishing, 2021. P. 1. P. 13–17.

17. A hybrid architecture for federated and centralized learning / A. M. Elbir, S. Coleri, A. K. Papazafeiropoulos, P. Kourtessis, S. Chatzinotas // IEEE Transactions on Cognitive Communications and Networking. 2022. Vol. 8, no. 3: P. 1529–1542. doi: 10.1109/TCCN.2022.3181032.

18. Federated vs. centralized machine learning under privacy-elastic users: A comparative analysis / D. Georgios, K. V. Katsaros, P. Pantazopoulos, V. Sourlas, A. Amditis // In IEEE 19th Intern. Symp. on Network Computing and Appl. (NCA). IEEE, 2020 P. 1–8. doi: 10.1109/NCA51143.2020.9306745Burges/.

19. Burges C. J. C. A tutorial on support vector machines for pattern recognition // Data Mining and Knowledge Discovery. 1998. Vol. 2, no. 2. P. 121–167.

20. Wireless federated learning with hybrid local and centralized training: A latency minimization design / H. Ning, M. Dai, Y. Wu, T. Q. S Quek, X. Shen // IEEE J. of Selected Topics in Signal Proc. 2022. Vol. 17, no. 1: 248–263. doi: 10.1109/JSTSP.2022.3223498.

## Информация об авторах

**Аль-Тамими Мохалад –** аспирант кафедры информационной безопасности СПбГЭТУ «ЛЭТИ».
E-mail: almokhalad44@gmail.com
https://orcid.org/ 0009-0005-5316-1689

**Мубарек Барре Хассан –** аспирант кафедры вычислительной техники СПбГЭТУ «ЛЭТИ».
E-mail: moubarekbarrehassan@gmail.com
https://orcid.org/ 0009-0007-2744-5666

**Саддам Ахмед Аббас** – канд. техн. наук, ассистент кафедры вычислительной техники СПбГЭТУ «ЛЭТИ».
E-mail: saddamabbas077@gmail.com
https://orcid.org/0000-0001-9931-463X

## References

1. A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications / L. Jie, W. Yu, N. Zhang, X. Yang, H. Zang, W. Zhao // IEEE Internet of Things J. 2017. Vol. 4, no. 5. P. 1125–1142. doi: 10.1109/JIOT.2017.2683200.

2. Mehdi M., Al-Fuqaha A. Enabling cognitive smart cities using big data and machine learning: Approaches and challenges // IEEE Communications Magazine. 2018. Vol. 56, no. 2. P. 94–101. doi: 10.1109/MCOM.2018.1700298.

3. Application of machine learning in wireless networks: Key techniques and open issues / S. Yaohua, M. Peng, Y. Zhou, Y. Huang, S. Mao // IEEE Communications Surveys & Tutorials. 2019. Vol. 21, no. 4. P. 3072–3108. doi: 10.1109/COMST.2019.2924243.

4. Communication-efficient learning of deep networks from decentralized data / M. Brendan, E. Moore, D. Ramage, S. Hampson, B. A. Arcas // Artificial intelligence and statistics. 2017. P. 1273–1282. URL: https://proceedings.mlr.press/v54/mcmahan17a?ref=https://githubhelp.com (data obrashhenija: 24.03.2024).

5. Federated learning in mobile edge networks: A comprehensive survey / L. Wei, Y. Bryan, N. C. Luong, D. T. Hoang, Y. Jiao, Y-C. Liang, Q. Yang, D. Niyato, C. Miao // IEEE Communications Surveys & Tutorials. 2020. Vol. 22, no. 3. P. 2031–2063. doi: 10.1109/COMST.2020.2986024.

6. Federated optimization: Distributed machine learning for on-device intelligence / K., Jakub, H. B. McMahan, D. Ramage, P. Richtárik. doi: 10.48550/arXiv.1610.02527 (data obrashhenija: 02.04.2024).

7. A joint learning and communications framework for federated learning over wireless networks / C. Mingzhe, Z. Yang, W. Saad, C. Yin, H. V. Poor, S. Cui // IEEE Transactions on Wireless Communications. 2020. Vol. 20, no. 1. P. 269–283. doi: 10.1109/TWC.2020.3024629.

8. Federated machine learning: Concept and applications / Y. Qiang, Y. Liu, T. Chen, Y. Tong // ACM Transactions on Intelligent Systems and Technol. (TIST) 10. 2019, no. 2. P. 1–19. doi: 10.1145/3298981 (data obrashhenija: 02.04.2024).

9. Privacy-preserving traffic flow prediction: A federated learning approach / L. Yi, J. Q. James, J. Kang, D. Niyato, S. Zhang // IEEE Internet of Things J. 2020. Vol. 7, no. 8. P. 7751–7763. doi: 10.1109/JIOT.2020.2991401.

10. Privacy-preserving asynchronous vertical federated learning algorithms for multiparty collaborative learning / G. Bin, A. Xu, Z. Huo, C. Deng, H. Huang // IEEE Transactions on Neural Networks and Learning Systems. 2021. Vol. 33, no. 11. P. 6103-6115. doi: 10.1109/TNNLS.2021.3072238.

11. Vafl: a method of vertical asynchronous federated learning / C. Tianyi, X. Jin, Y. Sun, W. Yin. doi: 10.48550/arXiv.2007.06081 (data obrashhenija: 02.04.2024).

12. Sudipan S., Bovolo F., Bruzzone L. Building change detection in VHR SAR images via unsupervised deep transcoding // IEEE Transactions on Geoscience and Remote Sensing. 2020. Vol. 59, no. 3. P. 1917–1929. doi: 10.1109/TGRS.2020.3000296.

13. Christopher B., Fan Z., Andras P. A review of privacy-preserving federated learning for the Internet-of-Things // Federated Learning Systems: Towards Next-Generation AI. P. 21–50. doi: 10.1007/978-3-030-70604-3_2 (data obrashhenija: 24.03.2024).

14. Zhijin Q., Li G. Y., Ye H. Federated learning and wireless communications // IEEE Wireless Communications. 2021. Vol. 28, no. 5. P. 134–140. doi: 10.1109/MWC.011.2000501.

15. Mathilde R., Pasquin D., Troncoso C. Can decentralized learning be more robust than federated learning? doi: 10.48550/arXiv.2303.03829 (data obrashhenija: 02.04.2024).

16. Efficient and less centralized federated learning / C. Li, Z. Liu, Z. Wang, A. Shrivastava // In Machine Learning and Knowledge Discovery in Databases. Research Track: European Conf., ECML PKDD. Bilbao, Spain: Springer International Publishing, 2021. P. 1. P. 13–17.

17. A hybrid architecture for federated and centralized learning / A. M. Elbir, S. Coleri, A. K. Papazafeiropoulos, P. Kourtessis, S. Chatzinotas // IEEE Transactions on Cognitive Communications and Networking. 2022. Vol. 8, no. 3: P. 1529–1542. doi: 10.1109/TCCN.2022.3181032.

18. Federated vs. centralized machine learning under privacy-elastic users: A comparative analysis / D. Georgios, K. V. Katsaros, P. Pantazopoulos, V. Sourlas, A. Amditis // In IEEE 19th Intern. Symp. on Network Computing and Appl. (NCA). IEEE, 2020 P. 1–8. doi: 10.1109/NCA51143.2020.9306745Burges/.

19. Burges C. J. C. A tutorial on support vector machines for pattern recognition // Data Mining and Knowledge Discovery. 1998. Vol. 2, no. 2. P. 121–167.

20. Wireless federated learning with hybrid local and centralized training: A latency minimization design / H. Ning, M. Dai, Y. Wu, T. Q. S Quek, X. Shen // IEEE J. of Selected Topics in Signal Proc. 2022. Vol. 17, no. 1: 248–263. doi: 10.1109/JSTSP.2022.3223498.

## Information about the authors

**Mokhalad Al-Tameemi –** postgraduate student of the Department of Information Security of Saint Petersburg Electrotechnical University.
E-mail: almokhalad44@gmail.com
https://orcid.org/ 0009-0005-5316-1689

**Moubarek B. Hassan** – postgraduate student of the Department of Computer Technology of Saint Petersburg Electrotechnical University.
E-mail: moubarekbarrehassan@gmail.com
https://orcid.org/ 0009-0007-2744-5666

**Saddam A. Abass** – Ph. D., Assistant of the Department of Computer Technology of Saint Petersburg Electrotechnical University.
E-mail: saddamabbas077@gmail.com
https://orcid.org/ 0000-0001-9931-463X

Статья поступила в редакцию 28.03.2024; принята к публикации после рецензирования 08.04.2024; опубликована онлайн 24.05.2024.

Submitted 28.03.2024; accepted 08.04.2024; published online 24.05.2024.