УДК 004.056.5
DOI: 10.26102/2310-6018/2026.54.3.011

Конфиденциальный обмен данными о киберугрозах между государственными учреждениями с использованием FEGB-Net

А.А.С. Арм✉, Е.В. Ляпунцова

Национальный исследовательский технологический университет МИСИС, Москва, Российская Федерация

Резюме. Правительственные сети все чаще становятся объектами скоординированных кибератак, использующих сходства в инфраструктуре и методах работы различных ведомств. Хотя раннее обнаружение в одной организации может послужить важным сигналом для остальных, эффективный обмен информацией об угрозах часто ограничен законами о суверенитете и конфиденциальности данных. В данной статье представлено расширение федеративной ансамблевой графовой сети (FEGB-Net), которое позволяет государственным ведомствам обмениваться данными об угрозах, с выполнением требований конфиденциальности. Предложенный подход извлекает поведенческие сигнатуры угроз из локально обученных моделей графовых нейронных сетей, защищает эти сигнатуры с помощью методов дифференциальной приватности и использует их для межведомственного обнаружения угроз в реальном времени. Экспериментальная оценка с использованием набора данных CICIDS2017 показывает, что точность обнаружения остается сопоставимой с точностью при работе в изолированном (не федеративном) режиме, однако время обнаружения скоординированных атак сокращается до 88,5 %. Анализ показывает ε-дифференциальную приватность с $\varepsilon = 2{,}0$, что ограничивает возможности атак логического вывода до методов, близких к случайному перебору. Эти результаты показывают, что возможность совместной защиты может быть достигнута без ущерба для конфиденциальности данных и суверенитета.

Ключевые слова: федеративное обучение, обмен данными об угрозах, графовые нейронные сети, дифференциальная приватность, государственная кибербезопасность.

Для цитирования: Арм А.А.С., Ляпунцова Е.В. Конфиденциальный обмен данными о киберугрозах между государственными учреждениями с использованием FEGB-Net. *Моделирование, оптимизация и информационные технологии.* 2026;14(3). URL: https://moitvivt.ru/ru/journal/article?id=2189 DOI: 10.26102/2310-6018/2026.54.3.011

Privacy-preserving threat intelligence sharing across government agencies using FEGB-Net

A.A.S. Arm✉, E.V. Lyapuntsova

National Research University of Technology "MISIS", Moscow, the Russian Federation

Abstract. Government networks are increasingly targeted by coordinated cyberattacks that exploit similarities in infrastructure and operational practices across agencies. Although early detection at one organization could provide valuable warnings to others, effective threat intelligence sharing is often constrained by data sovereignty and privacy regulations. This paper presents an extension of the federated ensemble graph-based network (FEGB-Net) framework that enables privacy-preserving threat intelligence sharing across government agencies. The proposed approach extracts compact behavioral threat signatures from locally trained federated graph neural network models, protects these signatures using differential privacy, and supports real-time cross-agency threat matching. Experimental evaluation using the CICIDS2017 dataset demonstrates that detection accuracy remains comparable to isolated operation, while coordinated attack detection time is reduced by up to 88.5 %. Privacy analysis confirms

that ε-differential privacy with $\varepsilon = 2.0$ limits membership inference attacks to near-random success. The results show that collaborative defense can be achieved without compromising data privacy or sovereignty.

Keywords: federated learning, threat intelligence sharing, graph neural networks, differential privacy, government cybersecurity.

For citation: Arm A.A.S., Lyapuntsova E.V. Privacy-preserving threat intelligence sharing across government agencies using FEGB-Net. *Modeling, Optimization and Information Technology.* 2026;14(3). (In Russ.). URL: https://moitvivt.ru/ru/journal/article?id=2189 DOI: 10.26102/2310-6018/2026.54.3.011

Введение

Киберугрозы, направленные на государственную инфраструктуру, эволюционировали от отдельных инцидентов до скоординированных атак, нацеленных на множество ведомств [1, 2]. Когда вредоносная активность обнаруживается одной организацией, другие правительственные структуры могут оставаться в неведении до тех пор, пока аналогичные атаки не повторятся локально, что снижает эффективность реагирования и увеличивает операционные риски. Хотя обмен информацией об угрозах мог бы значительно повысить ситуационную осведомленность, правовые и нормативные требования часто ограничивают централизованный сбор данных и обмен сетевым трафиком[1,2].

Федеративное обучение является многообещающей альтернативой, позволяющей проводить совместное обучение моделей без раскрытия конфиденциальных данных [3], [4]. В этой парадигме модели обучаются локально, и передаются только агрегированные обновления. Федеративная ансамблевая графовая сеть (FEGB-Net), первоначально предложенная в [5], сочетает федеративное и ансамблевое обучение с графовыми нейронными сетями для достижения точного обнаружения аномалий в распределенных системах.

Однако стандартное федеративное обучение неявно встраивает полученные знания в глобальные параметры модели, которые не могут быть напрямую опрошены аналитиками безопасности. Данная статья расширяет возможности FEGB-Net за счет обеспечения явного обмена информацией об угрозах с сохранением конфиденциальности. Поведенческие сигнатуры угроз извлекаются из обученных моделей, защищаются с помощью дифференциальной приватности и используются для межведомственного обнаружения угроз в реальном времени. Это расширение устраняет разрыв между совместным обучением и оперативным реагированием на угрозы.

Связанные работы. Федеративное обучение широко изучалось как сохраняющая конфиденциальность альтернатива централизованному машинному обучению, с применениями в сетевой безопасности и проблемах обнаружения вторжений [3, 4]. Предыдущие работы показали, что федеративные подходы могут достигать сравнимой точности обнаружения при сохранении чувствительных данных локально. Однако большинство существующих методов сосредоточены на улучшении локальной точности обнаружения, а не на обеспечении явного обмена информацией об угрозах.

Графовые нейронные сети продемонстрировали высокую эффективность при моделировании сетевого трафика, фиксируя структурные взаимосвязи между объектами

[1] European Parliament, Council of the European Union. *Document 32016R0679. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).* European Union. URL: https://eur-lex.europa.eu/eli/reg/2016/679/oj (дата обращения: 16.12.2025).

[2] National Institute of Standards and Technology (NIST). *Framework for Improving Critical Infrastructure Cybersecurity. Version 1.1.* URL: https://doi.org/10.6028/NIST.CSWP.04162018 (дата обращения: 16.12.2025).

[6, 7]. Системы обнаружения вторжений (IDS) на основе графов превосходят традиционные модели, основанные на признаках, особенно в случае сложных, многоуровневых атак. Тем не менее, большинство графовых подходов предполагает централизованную работу с данными, что ограничивает их применимость в государственных структурах.

Платформы обмена информацией об угрозах, такие как MISP и STIX[3], предоставляют стандартные инструменты для обмена индикаторами компрометации [8]. Однако эти платформы требуют раскрытия явных артефактов угроз, что может противоречить требованиям конфиденциальности в государственных сетях.

Дифференциальная приватность дает формальные гарантии защиты от утечек информации, оценивая влияние отдельных записей на общие выходные данные [9, 10]. Хотя дифференциальная приватность уже применялась к распределенному обучению, ее использование для защиты общедоступной информации об угрозах остается ограниченным. Эта работа интегрирует методы дифференциальной приватности непосредственно в процесс обмена информацией об угрозах.

Материалы и методы

Предлагаемая система построена на основе распределенной архитектуры, в которой каждое участвующее ведомство развертывает независимый экземпляр FEGB-Net [5] в рамках своей локальной инфраструктуры. Сетевой трафик обрабатывается локально, преобразуется в графовые представления и используется для обучения моделей обнаружения аномалий в соответствии с установленными принципами координации федеративного обучения [3, 4]. Внутренние данные о трафике никогда не покидают границы ведомства.

Центральный координационный сервер необходим для федеративного агрегирования и обновления защищенной базы сигнатур угроз. Сервер не имеет доступа к локальным сетевым данным и журналам. Когда аномальное поведение превышает заданный порог достоверности, генерируется и передается компактная сигнатура угрозы. Другие ведомства могут сравнивать свои локальные наблюдения с уже имеющимися сигнатурами, чтобы распознать аналогичные угрозы на ранней стадии. Полученная архитектура проиллюстрирована на Рисунке 1.

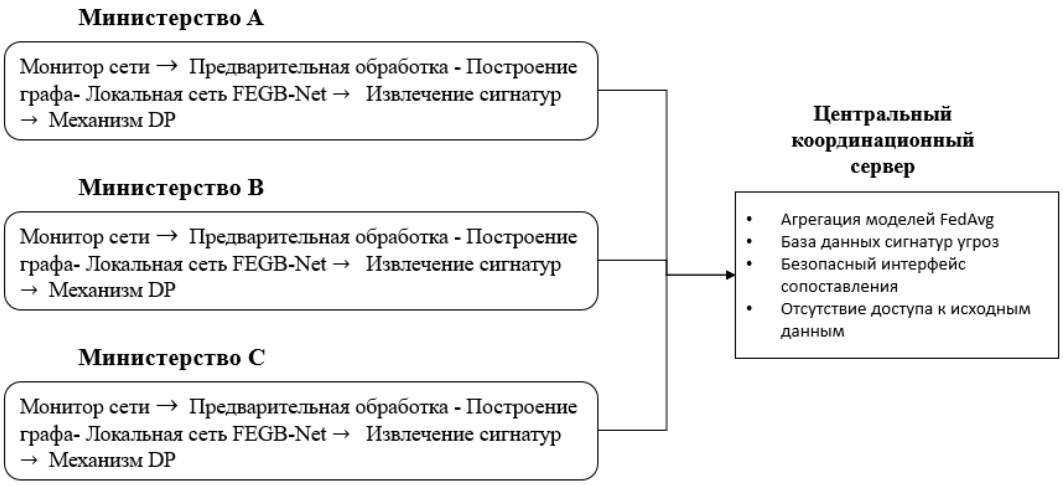

Рисунок 1 – Системная архитектура федеративного обмена информацией об угрозах
Figure 1 – System architecture for federated threat intelligence sharing

[3] Piazza R., Ratliff E., Relitz S., Studer Ch. *STIX Version 2.1 Errata 01*. OASIS Open. URL: https://docs.oasis-open.org/cti/stix/v2.1/stix-v2.1.html (дата обращения: 16.12.2025).

В рамках предложенной архитектуры используется модель «честного, но любопытного» координационного сервера. Несмотря на применение ε-дифференциальной приватности для защиты публикуемых сигнатур, сохраняются потенциальные риски косвенного вывода информации через анализ частотных и временных метаданных [11]. Для усиления модели доверия перспективным направлением является расширение архитектуры механизмами защищенной агрегации (secure aggregation) и многосторонних вычислений (SMPC) [12]. Исследование этих расширений является предметом будущей работы.

Выделение сигнатур угроз. При обнаружении аномальной активности выбираются узлы с высокими показателями аномальности и их соседи, формируя аномальный подграф. Каждый узел представляется последним слоем графовой нейронной сети [6, 7]. Эти слои встраивания объединяются с использованием модифицированного механизма внимания, для получения сигнатуры фиксированной длины.

Процесс агрегирования определяется следующим образом:

$$s = \sum_{i \epsilon V_a} \alpha_i h_i^{(L)}, \quad (1)$$

где V_a – множество аномальных узлов, $\alpha_i h_i^{(L)}$ – слой встраивания, α_i – весы механизма внимания.

Этот подход фиксирует как структурные, так и поведенческие характеристики обнаруженных атак, при этом используя сравнительно небольшой объем данных при передаче.

Полный процесс выделения сигнатур описан в Алгоритме 1.

Алгоритм 1. Извлечение сигнатуры угрозы

Ввод:	*Обученная модель FEGB-Net M, граф G, порог аномалии θ*
Вывод:	*Расширенная сигнатура угрозы* $s_{enriched}$
1	*Вычислить уровни аномалий для всех узлов графа G, используя M*
2	*Выбрать узлы с уровнями, превышающими θ*
3	*Построить аномальный подграф*
4	*Извлечь узловые встраивания*
5	*Применить агрегирование на основе механизма внимания*
6	*Нормализовать агрегированный вектор*
7	*Объединить метаданные*
8	*Получить расширенную сигнатуру* $s_{enriched}$

Порог аномальности θ определяется путем максимизации F1-меры на валидационной выборке, обеспечивая баланс между чувствительностью и уровнем ложноположительных срабатываний. В диапазоне $\theta \in [0{,}6;\ 0{,}8]$ изменение FPR не превышает 0,5 %, что подтверждает устойчивость метода. Для учета различий в профилях трафика различных ведомств перспективным является использование адаптивной настройки порога (например, на основе скользящего перцентиля), что позволяет дополнительно снизить число ложных оповещений при межведомственном обмене [13].

Защита методами дифференциальной приватности. Для предотвращения утечек информации из общедоступных сигнатур угроз, перед их отправкой применяются методы дифференциальной приватности. К каждому параметру сигнатуры добавляется шум, отобранный по распределению Лапласа, что обеспечивает гарантии ε-дифференциальной приватности, как показано в [9]. Теоретические основы и методы учета конфиденциальности следуют стандартным формулировкам [9, 10].

$$\frac{P(M(D)\in S}{P(M(\grave{D})\in S} \leq e^{\varepsilon}. \quad (2)$$

Внедрение шума Лапласа:

$$\tilde{s} = s + Lap(0, {}^{2}_{\varepsilon}). \quad (3)$$

В данном исследовании было выбрано значение $\varepsilon = 2{,}0$ для обеспечения баланса между защитой данных и операционной эффективностью. Оно обеспечивает высокую устойчивость к атакам логического вывода, при этом сохраняя возможность различать сигнатуры угроз.

Сопоставление угроз в реальном времени. На Рисунке 2 продемонстрировано изменение скорости обнаружения скоординированных атак при использовании общего доступа к сигнатурам угроз. В работе показано, что обмен данными об угрозах приводит к более чем 8-микратному приросту скорости реагирования.

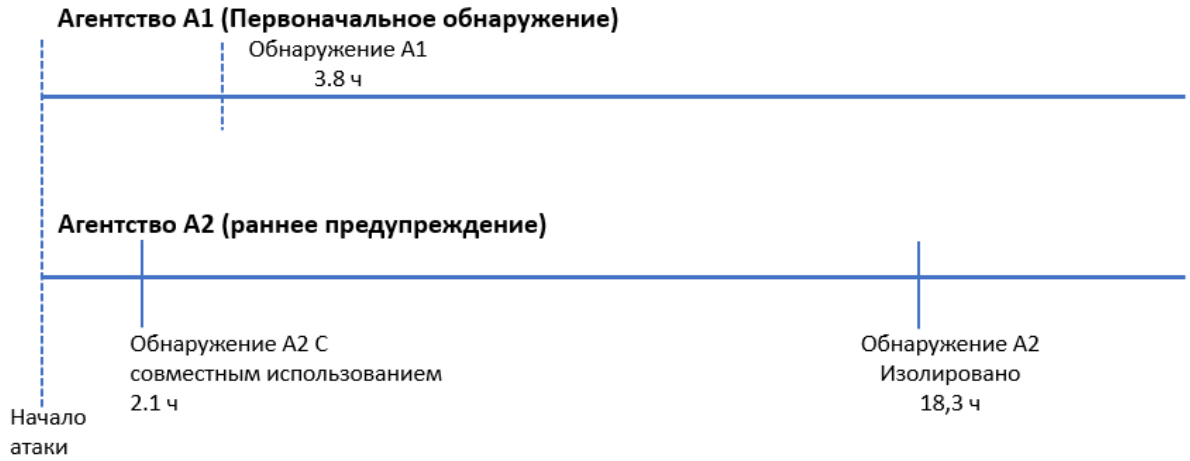

Рисунок 2 – Хронологическая таблица, иллюстрирующая раннее обнаружение скоординированных атак с использованием общих сигнатур угроз

Figure 2 – Timeline illustrating early detection of coordinated attacks using shared threat signatures

Сигнатуры угроз сравниваются с использованием косинусного сходства между нормализованными векторами:

$$sim(s1, s2) = \frac{s1.s2}{\|s1\|.\|s2\|}. \quad (4)$$

Порог сходства определяет, будет ли вызвано оповещение. Для обеспечения масштабируемости используется поиск приблизительных ближайших соседей с помощью иерархического маленького мира (HNSW) [14], что позволяет получить логарифмическую сложность поиска и задержку запроса порядка миллисекунды для больших баз данных угроз.

Когда показатель сходства превышает пороговое значение, генерируется оповещение, дополненное контекстной информацией, такой как ведомство-источник, время обнаружения, значение косинусного сходства и предполагаемый тип атаки.

Экспериментальная установка и оценка. Эксперименты проводились на наборе данных CICIDS2017 [15], который содержит около 2,8 миллиона сетевых потоков, собранных за пять дней, и включает в себя различные типы атак, такие как DDoS атаки, ботнеты, сканирования портов и веб-атаки. Набор данных был временно разделен между тремя моделируемыми государственными учреждениями, чтобы отразить независимые операционные среды.

Следует отметить, что в экспериментах использовалось временное разделение набора CICIDS2017, обеспечивающее лишь умеренную гетерогенность данных. В реальных межведомственных условиях распределения могут быть существенно non-IID, что способно повлиять на агрегацию и устойчивость сопоставления сигнатур при концептуальном дрейфе. Для повышения робастности системы могут применяться методы персонализированного федеративного обучения и адаптивной калибровки моделей [16]. Экспериментальная проверка на более гетерогенных данных рассматривается как направление дальнейших исследований.

Чтобы оценить эффективность обмена информацией об угрозах, использовались синтетические сценарии скоординированных атак, включающие в себя DDoS-атаку, APT-атаку и заражение программой-вымогателем. Предложенная система сравнивалась с изолированной FEGB-Net [5], централизованной FEGB-Net, федеративным усреднением с многослойными персептронами [4] и обменом угроз с помощью MISP вручную [8].

Результаты и обсуждение

Предложенная система достигла точности обнаружения, сравнимой с изолированной FEGB-Net [5], в то же время оставаясь достаточно близко к показателям централизованного обучения (Таблица 1). Это подтверждает, что обмен информацией об угрозах не ухудшает возможности локального обнаружения.

Таблица 1 – Сравнение эффективности обнаружения на CICIDS2017
Table 1 – Detection Performance Comparison on CICIDS2017

Метод	**Accuracy (%)**	**Precision (%)**	**Recall (%)**	**F1-Score (%)**	**AUC-ROC**	**FPR (%)**
Изолированная FEGB-Net	97,1	96,5	95,9	96,2	0,980	2,4
Централизованная FEGB-Net	97,8	97,2	96,8	97,0	0,985	1,9
FedAvg (MLP)	91,3	89,7	90,1	89,9	0,925	6,8
MISP (вручную)	94,2	93,1	92,8	92,9	0,955	4,7
Предлагаемая система	97,3	96,8	96,2	96,5	0,982	2,2

Основные преимущества проявились в сценариях скоординированных атак (Таблица 2). Доступ к данным об угрозах сократил время обнаружения до 88,5 % при DDoS атаках и позволил на ранней стадии локализовать многоэтапные APT-атаки. В сценариях с программами-вымогателями ранние предупреждения сократили скорость распространение вируса на 76 % и в некоторых случаях полностью предотвратили заражение.

Таблица 2 – Результаты обнаружения скоординированных атак
Table 2 – Coordinated Attack Detection Results

Тип атаки	Ведомство	Время обнаружения (изолированная модель)	Время обнаружения (предложенная модель)	Улучшение	Влияние
DDoS-атака	A1	4,2 часа	3,8 часа	На 9,5% быстрее	Раннее предупреждение
	A2	18,3 часа	2,1 часа	На 88,5% быстрее	Выигрыш 16,2 часа
APT-атака	A1	Не обнаружено	6,1 часа	Н/Д	Атака обнаружена

Таблица 2 (продолжение)
Table 2 (continued)

	A2	48+ часов	8,7 часов	На 81,9% быстрее	Остановлена до эскалации
	A3	72+ часов	Предотвращена	100%	Без потерь данных
Программа-вымогатель	A2	10 узлов	10 узлов	Н/Д	Нулевой пациент
	A1	50 узлов	12 узлов	Снижение на 76%	Сохранено 38 узлов
	A3	30 узлов	0 узлов	100% предотвращено	Полное блокирование

В отличие от платформ класса MISP, ориентированных на обмен статическими индикаторами компрометации, коммерческие EDR/XDR-системы реализуют автоматизированную корреляцию событий в централизованной облачной инфраструктуре с типичной задержкой порядка секунд. Предлагаемая федеративная архитектура обеспечивает миллисекундный уровень сопоставления сигнатур за счет использования индекса HNSW [15], при этом не требуя передачи исходного трафика в централизованные хранилища. Такой подход особенно актуален для государственных инфраструктур, где действуют ограничения, связанные с суверенитетом данных [17].

Анализ защиты конфиденциальности (Таблица 3) показывает, что $\varepsilon = 2{,}0$ ограничивает атаки логического вывода на определение принадлежности почти случайным успехом, что согласуется с теорией дифференциальной приватности [9, 10]. Исследования абляции подтверждают важность агрегации на основе механизма внимания и временных характеристик для сохранения индивидуальных различий сигнатур.

Таблица 3 – Анализ защиты конфиденциальности
Table 3 – Privacy protection analysis

Параметры конфиденциальности	**Процент успешных атак (%)**	**95% доверительный интервал**	**Уровень утечки данных**
Нет DP ($\varepsilon = \infty$)	78,3	[76,9; 79,7]	Высокая
$\varepsilon = 5{,}0$	64,1	[62,8; 65,4]	Умеренная
$\varepsilon = 2{,}0$ (предложенное значение)	56,2	[55,1; 57,3]	Низкая
$\varepsilon = 1{,}0$	52,8	[51,8; 53,8]	Очень низкая
Случайный базовый уровень	50,0	[49,1; 50,9]	Н/Д

Заключение

В данной статье демонстрируется практическая возможность обмена информацией об угрозах с выполнением требований конфиденциальности в государственных сетях. Расширенная версия FEGB-Net [5] с поддержкой извлечения поведенческих сигнатур, защиты методами дифференциальной приватности и сопоставления данных угроз в реальном времени, позволяет осуществлять более раннее обнаружение и предотвращение скоординированных атак.

Результаты экспериментов подтверждают, что эффективный обмен данными может быть достигнут с минимальными затратами и гарантией конфиденциальности.

Предложенный подход открывает жизнеспособный путь к объединению усилий в сфере кибербезопасности и государственном управлении, при этом удовлетворяя важнейшим правовым и операционным требованиям, предъявляемым данными областями.

СПИСОК ИСТОЧНИКОВ / REFERENCES

1. Ndubuisi A.F. Strengthening national cybersecurity policies through coordinated threat intelligence sharing and real-time public-private collaboration frameworks. *International Journal of Science and Research Archive.* 2023;8(2):812–831. https://doi.org/10.30574/ijsra.2023.8.2.0299
2. Alaeifar P., Pal Sh., Jadidi Z., Hussain M., Foo E. Current approaches and future directions for cyber threat intelligence sharing: A survey. *Journal of Information Security and Applications.* 2024;83. https://doi.org/10.1016/j.jisa.2024.103786
3. McMahan B., Moore E., Ramage D., Hampson S., Arcas B.A. Communication-efficient learning of deep networks from decentralized data. In: *Proceedings of the 20th International Conference on Artificial Intelligence and Statistics, AISTATS 2017, 20–22 April 2017, Fort Lauderdale, FL, USA.* PMLR; 2017. P. 1273–1282.
4. Li T., Sahu A.K., Zaheer M., et al. Federated optimization in heterogeneous networks. In: *Proceedings of the Third Conference on Machine Learning and Systems, MLSys 2020, 02–04 March 2020, Austin, TX, USA.* MLSys Proceedings; 2020. URL: https://proceedings.mlsys.org/paper_files/paper/2020/file/1f5fe83998a09396ebe6477d9475ba0c-Paper.pdf
5. Арм А.А.С., Ляпунцова Е.В. Новая гибридная модель обнаружения аномалий с использованием ансамблевого машинного обучения и федеративных графовых нейронных сетей для обеспечения сетевой безопасности. *Моделирование, оптимизация и информационные технологии.* 2025;13(2). https://doi.org/10.26102/2310-6018/2025.49.2.044
   Arm A.A.S., Lyapuntsova E.V. A novel hybrid anomaly detection model using federated graph neural networks and ensemble machine learning for network security. *Modeling, Optimization and Information Technology.* 2025;13(2). (In Russ.). https://doi.org/10.26102/2310-6018/2025.49.2.044
6. Wu Z., Pan Sh., Chen F., et al. A comprehensive survey on graph neural networks. *IEEE Transactions on Neural Networks and Learning Systems.* 2021;32(1):4–24. https://doi.org/10.1109/TNNLS.2020.2978386
7. Kipf Th.N., Welling M. *Semi-supervised classification with graph convolutional networks*. arXiv. URL: https://arxiv.org/abs/1609.02907 [Accessed 17th December 2025].
8. Wagner C., Dulaunoy A., Wagener G., Iklody A. MISP: The design and implementation of a collaborative threat intelligence sharing platform. In: *WISCS '16: Proceedings of the 2016 ACM on Workshop on Information Sharing and Collaborative Security, 24 October 2016, Vienna, Austria.* New York: ACM; 2016. P. 49–56. https://doi.org/10.1145/2994539.2994542
9. Dwork C., Roth A. The algorithmic foundations of differential privacy. *Foundations and Trends® in Theoretical Computer Science.* 2014;9(3–4):211–487. https://doi.org/10.1561/0400000042
10. Mironov I. Rényi differential privacy. In: *2017 IEEE 30th Computer Security Foundations Symposium (CSF), 21–25 August 2017, Santa Barbara, CA, USA.* IEEE; 2017. P. 263–275. https://doi.org/10.1109/CSF.2017.11
11. Melis L., Song C., De Cristofaro E., Shmatikov V. Exploiting unintended feature leakage in collaborative learning. In: *2019 IEEE Symposium on Security and Privacy (SP), 19–*

23 May 2019, San Francisco, CA, USA. IEEE; 2019. P. 691–706. https://doi.org/10.1109/SP.2019.00029

12. Bonawitz K., Ivanov V., Kreuter B., et al. Practical secure aggregation for privacy-preserving machine learning. In: *CCS '17: Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, 30 October – 03 November 2017, Dallas, TX, USA.* New York: ACM; 2017. P. 1175–1191. https://doi.org/10.1145/3133956.3133982
13. Sculley D., Holt G., Golovin D., et al. Hidden technical debt in machine learning systems. In: *Advances in Neural Information Processing Systems 28: Annual Conference on Neural Information Processing Systems 2015, 07–12 December 2015, Montreal, Quebec, Canada.* 2015. P. 2503–2511.
14. Sharafaldin I., Lashkari A.H., Ghorbani A.A. Toward generating a new intrusion detection dataset and intrusion traffic characterization. In: *Proceedings of the 4th International Conference on Information Systems Security and Privacy, 22–24 January 2018, Funchal, Madeira, Portugal.* SciTePress; 2018. P. 108–116. https://doi.org/10.5220/0006639801080116
15. Malkov Yu.A., Yashunin D.A. Efficient and robust approximate nearest neighbor search using hierarchical navigable small world graphs. *IEEE Transactions on Pattern Analysis and Machine Intelligence.* 2020;42(4):824–836. https://doi.org/10.1109/TPAMI.2018.2889473
16. Tan A.Z., Yu H., Cui L., Yang Q. Towards personalized federated learning. *IEEE Transactions on Neural Networks and Learning Systems*. 2023;34(12):9587–9603. https://doi.org/10.1109/TNNLS.2022.3160699
17. Von Scherenberg F., Hellmeier M., Otto B. Data sovereignty in information systems. *Electronic Markets.* 2024;34(1). https://doi.org/10.1007/s12525-024-00693-4

ИНФОРМАЦИЯ ОБ АВТОРАХ / INFORMATION ABOUT THE AUTHORS

Арм Ажи Азиз Салих, аспирант, Национальный исследовательский технологический университет «МИСИС», Москва, Российская Федерация.
e-mail: arm.azhi@yandex.com
ORCID: 0000-0002-7361-042X

Azhi A. S. Arm, Postgraduate, National Research University of Technology "MISIS", Moscow, the Russian Federation.

Ляпунцова Елена Вячеславовна, доктор технических наук, профессор, Национальный исследовательский технологический университет «МИСИС», Москва, Российская Федерация.
e-mail: liapuntsova.ev@misis.ru
ORCID: 0000-0002-3420-3805

Elena V. Lyapuntsova, Doctor of Engineering Sciences, Professor, National Research University of Technology "MISIS", Moscow, the Russian Federation.

Статья поступила в редакцию 19.01.2026; одобрена после рецензирования 13.03.2026; принята к публикации 23.03.2026.

The article was submitted 19.01.2026; approved after reviewing 13.03.2026; accepted for publication 23.03.2026.