

Сидорович Максим Анатольевич

кандидат технических наук, старший преподаватель кафедры «Автоматизированные, телекоммуникационные и электротехнические системы», Дальневосточный государственный университет путей сообщения, город Хабаровск. ORCID: 0000-0002-0194-0921. SPIN-код: 4246-5303. AuthorID: 1039754.

Электронный адрес: msidorovich60@gmail.com

Maksim A. Sidorovich

Ph.D. of Technical Sciences, Senior Lecturer at the Department of Automated, Telecommunications, and Electrical Engineering Systems, Far Eastern State Transport University, Khabarovsk. ORCID: 0000-0002-0194-0921. SPIN code: 4246-5303. AuthorID: 1039754.

E-mail address: msidorovich60@gmail.com

Шматок Виталий Андреевич

аспирант, старший преподаватель кафедры «Цифровая индустрия и защита информации», Дальневосточный государственный университет путей сообщения, город Хабаровск. ORCID: 0009-0005-3439-7530. SPIN-код: 8635-1719. AuthorID: 1342911.

Электронный адрес: vit.shmatok@gmail.com

Vitaly A. Shmatok

Postgraduate, Senior Lecturer at the Department of Digital Industry and Information Security, Far Eastern State Transport University, Khabarovsk. ORCID: 0009-0005-3439-7530. SPIN code: 8635-1719. AuthorID: 1342911.

E-mail address: vit.shmatok@gmail.com

Пономарчук Юлия Викторовна

кандидат физико-математических наук, доцент кафедры «Цифровая индустрия и защита информации», Дальневосточный государственный университет путей сообщения, город Хабаровск. ORCID: 0000-0002-2531-030X. SPIN-код: 2787-1092. AuthorID: 125721

Электронный адрес: yulia.ponomarchuk@gmail.com.

Yulia V. Ponomarchuk

Ph.D. of Physico-mathematical Sciences, Docent at the Department of Digital Industry and Information Security, Far Eastern State Transport University, Khabarovsk. ORCID: 0000-0002-2531-030X. SPIN code: 2787-1092. AuthorID: 125721.

E-mail address: yulia.ponomarchuk@gmail.com.

О ПРИМЕНЕНИИ КИБЕРИММУННОГО ПОДХОДА
И ФЕДЕРАТИВНОГО ОБУЧЕНИЯ К ОБЕСПЕЧЕНИЮ
КИБЕРБЕЗОПАСНОСТИ ИНТЕЛЛЕКТУАЛЬНЫХ
ТРАНСПОРТНЫХ СИСТЕМ

Аннотация. В статье рассматривается применение федеративного обучения для обеспечения кибериммунитета телекоммуникационных систем транспортной ПоТ-инфраструктуры с целью детектирования аномалий и сбоев. Предложена архитектура классификатора на основе ансамблей деревьев принятия

О применении кибериммунного подхода и федеративного обучения
к обеспечению кибербезопасности интеллектуальных транспортных систем

решений для локального анализа сигнатур кибератак на оконечных узлах. Применение одноуровневого механизма федеративного обучения позволяет интеллектуальным модулям обмениваться весами моделей напрямую, что повышает устойчивость системы к несбалансированности и искажениям данных. Эффективность однорангового подхода со взвешенным усреднением подтверждена экспериментально на наборе данных об атаках на IoT-инфраструктуру. Предлагаемая распределенная модель обучения показала улучшение метрик Accuracy и F1 по сравнению с централизованной моделью и одноранговой моделью обучения.

Ключевые слова: детектирование аномалий, беспроводные сети, системы промышленного интернета вещей, машинное обучение, кибериммунитет, федеративное обучение, распределенное обучение, решающие деревья, IoT.

Для цитирования: Сидорович М.А. Шматок В.А., Пономарчук Ю.В. О применении кибериммунного подхода и федеративного обучения к обеспечению кибербезопасности интеллектуальных транспортных систем // Вестник Российского нового университета. Серия: Сложные системы: модели, анализ и управление. 2026. № 3. С. 196–205. DOI: 10.18137/RNU.V9187.26.03.P.196

ON THE APPLICATION OF THE CYBERIMMUNE APPROACH
AND FEDERATED LEARNING TO ENSURING CYBERSECURITY
OF INTELLIGENT TRANSPORTATION SYSTEMS

Abstract. The paper discusses the application of federated learning to enhance the cyber immunity of telecommunications systems within the transport IIoT infrastructure, focusing on the detection of anomalies and failures. It proposes a classifier architecture based on decision tree ensembles for the local analysis of cyberattack signatures at edge nodes. Implementing a single-tier federated learning mechanism enables intelligent modules to directly exchange model weights, thereby boosting the system's resistance to data imbalances and distortions. The efficacy of the peer-to-peer approach, which utilizes weighted averaging, has been validated through experiments on a dataset of IoT infrastructure attacks. The suggested distributed learning model outperforms both centralized and single-shot learning models in terms of Accuracy and F1 metrics.

Keywords: anomaly detection, wireless networks, industrial Internet of Things systems, machine learning, cyberimmunity, federated learning, distributed learning, decision trees, IoT.

For citation: Sidorovich M.A., Shmatok V.A., Ponomarchuk Yu.V. (2026) On the application of cyberimmune approach and federated learning to ensuring the cybersecurity of intelligent transport systems. *Vestnik of Russian New University. Series: Complex Systems: Models, Analysis and Management*. No. 3. Pp. 196–205. DOI: 10.18137/RNU.V9187.26.03.P.196 (In Russian).

В настоящее время растет влияние факторов, связанных с эффективностью работы управляющих систем, на безопасность движения поездов. Также отмечается важность мониторинга и оценки состояния объектов инфраструктуры (строения пути, элементов систем энергоснабжения, сетей телекоммуникаций), своевременная диагностика их предостказных состояний [1]. Сбор технологических данных при администрировании и управлении транспортными средствами и системами открывает широкие возможности для внедрения технологий искусственного интеллекта и машинного обучения, что позволяет оптимизировать технологические процессы и эффективно управлять как материальными,

так и трудовыми ресурсами. С внедрением технологий промышленного интернета вещей (Industrial Internet of Things, IIoT), занимающих в настоящее время значимое место в обеспечении связности объектов инфраструктуры и транспортных средств, отрасль железнодорожного транспорта стоит перед задачей создания и использования распределенных систем для сбора, передачи, хранения и обработки информации [1; 2]. Несмотря на повсеместное внедрение интеллектуальных киберфизических систем (КФС), недостаточно проработаны аспекты комплексной защиты интеллектуальных транспортных систем (ИТС) от специализированных кибератак, нацеленных на вывод инфраструктуры из строя, нарушение графика движения, сбой аппаратного и программного обеспечения узлов телекоммуникаций.

В условиях цифровизации транспортные средства и инфраструктура становятся всё более уязвимыми объектами критической информационной инфраструктуры (КИИ) [2]. Железнодорожный транспорт является стратегической отраслью, и в вопросах кибербезопасности законодательством РФ ему отведена особая роль в соответствии с распоряжением Правительства РФ от 22.06.2022 № 1661-р, федеральными законами ФЗ № 193 [3], № 194-ФЗ [4] и внутренними нормативными актами.

В странах Европы, где применяется единая система управления поездами (ERTMS/ETCS), исследователи указывают на подверженность объектов железнодорожной инфраструктуры актам незаконного вмешательства в их работу [5]. Это требует строгого соблюдения требований безопасности и конфиденциальности, а также применения механизмов защиты, таких как криптография, использование защищенных каналов связи, инструментов обеспечения целостности и отказоустойчивости [6].

Традиционные средства защиты объектов КИИ характеризуются значительной сложностью организации для противодействия атакам широкого спектра на промышленные системы IoT. Интеграция устаревших сетей автоматизированных систем управления технологическими процессами (АСУ ТП) с современными вычислительными и сетевыми технологиями значительно расширила возможности реализации атак, сделав эти системы более уязвимыми [7]. Несмотря на существующие меры безопасности, злоумышленники постоянно осуществляют попытки нанесения ущерба управлению транспортными процессами, а исследователи определяют риски и разрабатывают новые подходы к защите таких систем [8]. Анализ рисков и вызовов, связанных с масштабным внедрением технологий IIoT в инфраструктуру городского транспорта, показывает существенные угрозы для кибербезопасности интеллектуальных транспортных систем [9].

Рассматривая сегмент железнодорожных систем управления движением поездов, которые состоят из многоуровневых интеграций различных подсистем и интерфейсов с целью всеобъемлющего контроля над транспортными процессами, можно отметить следующие особенности. Телекоммуникационные системы являются гетерогенными и распределенными на основе кабельных каналов и радиосвязи. Например, с целью обеспечения голосовой связи могут использоваться протоколы на основе аналоговых и цифровых сигналов. При этом для обеспечения транспортной безопасности необходимо обеспечить заданный уровень качества обслуживания и информационной безопасности в реальном времени. Часто подобные системы функционируют в условиях городской или промышленной среды, следовательно, подвержены широкому спектру преднамеренных и непреднамеренных воздействий.

О применении кибериммунного подхода и федеративного обучения
к обеспечению кибербезопасности интеллектуальных транспортных систем

Если тяжело предсказать сценарии вторжения, а также сбои аппаратного и программного обеспечения в распределенных гетерогенных телекоммуникационных системах, одним из путей обеспечения защищенности является внедрение систем обнаружения вторжений на основе разрабатываемых механизмов кибериммунитета. Кибериммунология – наука об общих закономерностях формирования, накопления и применения кибериммунитета для упреждающей защиты КФС от кибератак. Под кибериммунитетом понимается определенная невосприимчивость КФС к деструктивным информационно-техническим воздействиям [10], которая достигается путем диагностирования состояния и самовосстановления в реальном времени по аналогии с процессами иммунной системы защиты живого организма.

На примере КФС на транспорте рассмотрим архитектуру системы ПоТ на участке железной дороги, которая должна быть интегрирована в микропроцессорную систему управления станцией (МПСУС). МПСУС оснащается штатным устройством кибербезопасного мониторинга (УКБМ), которое обладает предобученным кибериммунитетом и обновляет его путем модификации соответствующего программного обеспечения в зависимости от изменяющихся условий коммуникации.

Архитектура системы ПоТ на участке железной дороги представлена на Рисунке 1.

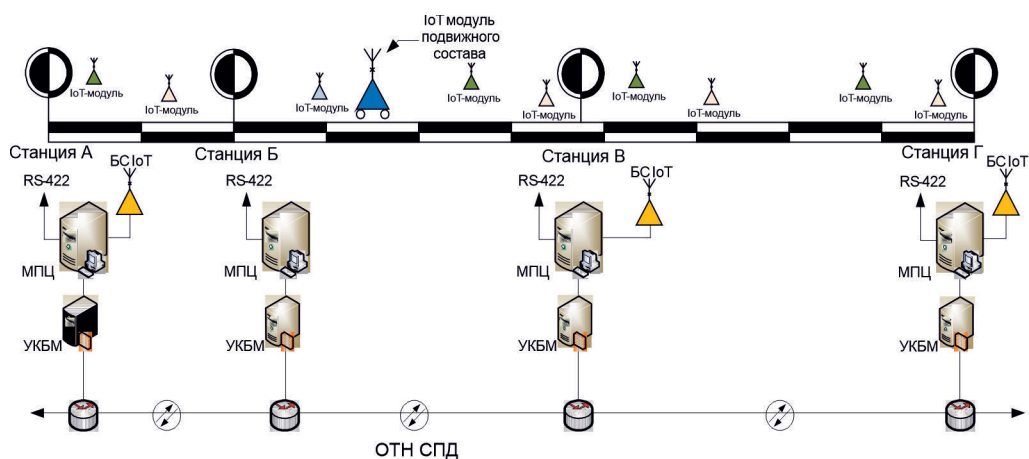


Рисунок 1. Архитектура системы ПоТ на участке железной дороги:

БС ПоТ – базовая станция сети ПоТ; УКБМ – устройство кибербезопасного мониторинга;

МПСУС – система управления на железнодорожной станции;

ОТН СПД – сеть передачи данных оперативно-технологического назначения

При применении подходов кибериммунитета сама структура КИИ позволяет использовать разрозненные узлы защиты и для обучения модулей искусственного интеллекта. Таким образом, появляется возможность внедрить федеративное обучение (FL). Для оценки возможности применения подходов кибериммунитета для систем управления и диагностирования состояния объектов инфраструктуры железных дорог на станциях использован набор данных ML-EdgeIoT [11]. Выбор этого набора обусловлен его вхождением в процент самых цитируемых публикаций, индексируемых в базах данных Web of Science (WoS) по количеству цитирований. Рассмотрим результативность обучения си-

стемы детектирования атак как составного элемента приобретенного кибериммунитета на представленном выше наборе данных и архитектуре, приведенной на Рисунке 1. Для детектирования выделен набор атак, представленный в Таблице 1.

В ходе исследования возможности детектирования представленных в Таблице 1 атак было сформировано подмножество на 10 тыс. экземпляров, которое разделено поровну между классами «норма» и «атака». В последнем записи равномерно распределены по атакам всех типов в равной пропорции. Из подмножества 30 % использовалось для тестирования. Для анализа применимости различных алгоритмов проведено их тестирование в программной среде MatLab 2021b с использованием дополнительного пакета программ Classifier Learner для первичного выявления наилучших подходов машинного обучения для детектирования атак на МПСУС. Для оценки качества детектирования использовались стандартные классификаторы пакета Classification Learner: деревья решений (Tree), машины опорных векторов (SVM) и ансамблевые методы (Ensemble). Для проведения оценки качества детектирования и классификации атак использована метрика Accuracy, которую можно интерпретировать как отношение суммы истинно положительных и истинно отрицательных выявленных атак к общему объему данных. Тестирование проводилось на 30 % данных от сформированного подмножества.

Таблица 1

Ключевые сценарии атак

Тип	Полное наименование	Суть атаки
DDoS	Distributed Denial of Service	Распределённая атака типа отказа в обслуживании, цель – перегрузить сервер или канал связи трафиком до полной недоступности для легитимных пользователей
Password	Подбор пароля	Попытки получить привилегированный доступ к системе путём перебора комбинаций пароля легального устройства или пользователя
Vulnerability scanner	Сканер уязвимостей	Автоматизированный поиск известных уязвимостей в защите систем и сервисов перед проведением основной атаки
Uploading	Несанкционированная загрузка	Загрузка вредоносных файлов на легальное устройство через плохо защищённые механизмы отправки данных
Backdoor	Бэкдор («чёрный ход»)	Скрытый механизм удалённого доступа, который устанавливается в систему после её первоначального взлома для сохранения контроля
Port Scanning	Сканирование портов	Поиск открытых сетевых портов на серверах жертвы для определения доступных сервисов и потенциальных точек входа
MITM	Man-in-the-Middle	Перехват канала связи между двумя сторонами для кражи или подмены данных
Fingerprinting	Фингерпринтинг (снятие отпечатка)	Сбор технической информации об операционной системе (ОС), браузере и сетевом оборудовании цели для подготовки более проработанной атаки

О применении кибериммунного подхода и федеративного обучения
к обеспечению кибербезопасности интеллектуальных транспортных систем

Результаты компьютерного эксперимента представлены на Рисунке 2, где опущены выводы классификаторов на основе машины опорных векторов (SVM) вследствие низкой эффективности, составившей 6,5 % (Accuracy). Следует отметить гораздо большую долю правильных ответов классификаторов на основе решающих деревьев.

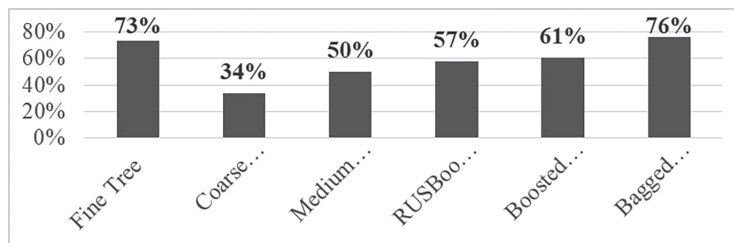


Рисунок 2. Результаты тестирования классификаторов атак по метрике Accuracy на основе решающих деревьев

Для архитектуры КФС (см. Рисунок 1), рассматривалась одноранговая (P2P) архитектура системы FL. При условии унификации оборудования узлов такой подход позволяет отказаться от использования центрального сервера-агрегатора и существенно снизить объем передаваемого трафика за счет обмена весами моделей только между непосредственными соседями в сети.

Усреднение весовых коэффициентов классификаторов, расположенных на соседних узлах сети, позволяет агрегировать обновления параметров модели, полученных от соседних устройств, для создания улучшенной модели. Для этого реализуется обучение на локальных клиентских устройствах (узлах), где каждый клиент независимо обучает свою модель на локальных данных. В данном случае в роли клиентских узлов выступает МПСУС. Агрегация опыта с локальных узлов в рамках сегмента сети подразумевает, что после локального обучения веса моделей с разных клиентов передаются на сервер или главе кластера. Для P2P-сетей наиболее распространенными являются два подхода: равномерный, когда каждое устройство имеет одинаковую значимость своих весовых коэффициентов, и средневзвешенный (Weighted Federated Averaging), рекомендуемый для децентрализованных систем. Вычисления среднего значения весовых коэффициентов в соответствии с последним подходом проводились по формуле

$$W_i^{t+1} = \sum_{j \in N_i} \frac{n_j}{\sum_{k \in N_i} n_k} W_j^{(t)},$$

где W_i^{t+1} – новые веса модели узла i ; N_i – множество, включающее узел i и всех его активных соседей, у которых он запрашивает веса; $W_j^{(t)}$ – текущие веса модели, полученные от соседа j ; n_j – количество образцов данных (объем набора данных) на узле j ; $\sum_{k \in N_i} n_k$ – суммарное количество данных на узле i и всех его соседей [12].

Для оценки эффективности применения подходов FL предложена следующая последовательность этапов исследования. Первый этап оценки предполагал равномерное распределение подмножества данных объема 6700 записей по 10 узлам МПСУС. Сформированная выборка характеризуется соотношением классов «норма» и «атака» как 78 % к

22 % от общего объема данных. Внутри подкласса «атака» представлены все типы, приведенные в Таблице 1, при этом они распределены равномерно.

Модель классификатора представлена ансамблем деревьев решений (Bagging tree), глубина ансамбля ограничена 15 деревьями для предотвращения переобучения. Тестирование проводилось на выборке 3300 записей с аналогичными соотношениями. По итогам эксперимента модель с простым усреднением весовых коэффициентов незначительно уступила подходу со средним взвешенным FedAvg (на 1 % по метрике Accuracy). Второй этап оценки предполагал реалистичное (неравномерное, Non-IID) распределение данных об атаках между 10 МПСУС согласно нормальному распределению. Также неравномерно распределены записи об атаках в объеме данных, что больше соответствует специфике территориально-распределенных МПСУС.

Распределение обучающей выборки представлено на Рисунке 3. На оси абсцисс указаны идентификаторы узлов, по оси ординат – объемы обучающей выборки, приходящиеся на каждый узел, по правой оси – доли записей об атаках также для каждого узла.

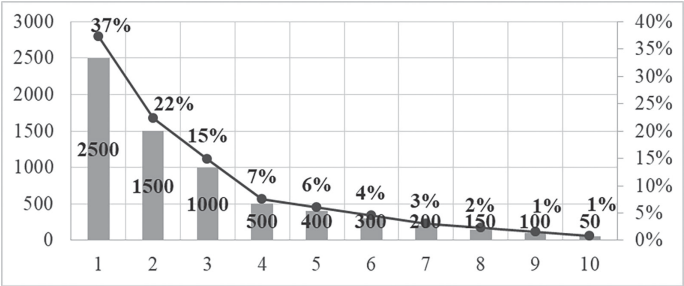


Рисунок 3. Распределение данных и атак по узлам в P2P-системе федеративного обучения

При нормальном распределении данных P2P-система на основе федеративного обучения со средним арифметическим уступила в точности детектирования атак средневзвешенной модели на 14,8 % (Ассигасу). Результаты эксперимента представлены на Рисунке 4.

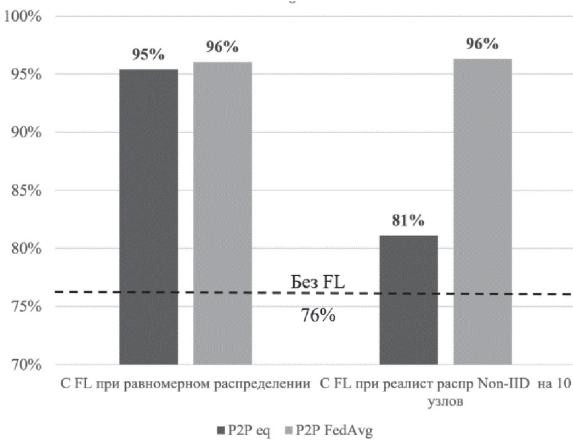


Рисунок 4. Результаты сравнения P2P-классификатора атак по метрике Ассигасу

О применении кибериммунного подхода и федеративного обучения
к обеспечению кибербезопасности интеллектуальных транспортных систем

Результаты тестирования по метрике F1 представлены в Таблице 2. Они показывают преимущество приобретённого кибериммунитета при средневзвешенном вычислении весов даже при учете несбалансированности данных.

Таблица 2

Результаты федеративного обучения моделей с различным усреднением весов

Тип P2P-системы	Равномерное распределение данных, %	Реалистичное распределение данных между узлами, %
Вычисления на основе среднего арифметического (eq)	97,7	87,4
Вычисления на основе среднего взвешенного FedAvg	97,9	97,6

Использование модели FL FedAvg при неравномерном распределении данных и записей об атаках по узлам демонстрирует лучшие показатели метрик F1 и Accuracy, чем P2P-модель, основанная на среднем арифметическом. Предлагаемый в статье метод открывает перспективы для дальнейшей выработки стратегий защиты железнодорожных IoT-систем с помощью приобретённого кибериммунитета.

Реализация данных направлений имеет важное значение для развития технологий диагностики состояния и управления подвижным составом, обеспечения баланса между высокой точностью моделей и отказоустойчивостью распределенной системы. Исследования в данной области открывают перспективы в области эффективного обучения и адаптации классификаторов для применения в распределенных гетерогенных сетях IoT.

Литература

1. Безродный Б.Ф. Особенности кибербезопасности АСУ ТП на железнодорожном транспорте // Системы безопасности: технический журнал. 2020. № 6. С. 34–35.
2. О безопасности критической информационной инфраструктуры Российской Федерации : Федеральный закон от 26.07.2017 № 187-ФЗ // Собрание законодательства РФ. 2017. № 31. Ст. 4745.
3. О внесении изменений в отдельные законодательные акты Российской Федерации в связи с принятием Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации» : Федеральный закон от 26.07.2017 № 193-ФЗ // Собрание законодательства РФ. 2017. № 31. Ст. 4790.
4. О внесении изменений в Закон Российской Федерации «О защите прав потребителей» : Федеральный закон от 07.07.2025 № 194-ФЗ // Официальный интернет-портал правовой информации [Электронный ресурс]. URL: <http://pravo.gov.ru> (дата обращения: 19.06.2026).
51. López-Aguilar P, Batista E, Martínez-Ballesté A, Solanas A. (2022) Information Security and Privacy in Railway Transportation: A Systematic Review // Sensors. Vol. 22, no. 7698. DOI: 10.3390/s22207698
6. Панин Д.Н., Бобков Е.О., Балашова Е.А. Анализ кибератак на критическую информационную инфраструктуру с IoT-технологиями // Автономия личности. 2020. № 2 (22) [Электронный ресурс]. URL: <https://cyberleninka.ru/article/n/analiz-kiberatak-na-kriticheskuyu-informatsionnuyu-infrastrukturu-s-iot-tehnologiyami> (дата обращения: 21.05.2026).
7. Кириллова А.Д. Оценка рисков информационной безопасности АСУ ТП промышленных объектов с использованием методов когнитивного моделирования : автореф. дис. ... канд. техн. наук. Уфа, 2023. 17 с.

8. Шамсутдинов Р.Р. Интеллектуальная система мониторинга информационной безопасности промышленного интернета вещей с использованием механизмов искусственных иммунных систем : дис. ... канд. техн. наук. Уфа, 2023. 139 с.
9. Smart Cities Need Smart IoT Security [Электронный ресурс]. URL: <https://asimily.com/blog/smart-cities-need-smart-iot-security> (дата обращения: 19.08.2026).
10. Жук Р.В. Методика и алгоритмы определения актуальных угроз информационной безопасности в информационных системах персональных данных : дис. ... канд. техн. наук. Краснодар, 2021. 156 с.
11. Ferrag M.A., Friha O., Hamouda D. [et al.]. ML-EdgeIIoT-dataset [Электронный ресурс]. URL: <https://www.kaggle.com/datasets/mohamedamineferrag/edgeiiotset-cyber-security-dataset-of-iiot> (дата обращения: 19.06.2026).
12. Luqman A., Luqman A., Mahesh R., Chattopadhyay A. (2025) Efficient Model Propagation for Peer-to-Peer Federated Learning using Minimum Spanning Tree and Gossip Networks [Электронный ресурс]. URL: <https://cyberleninka.ru/article/n/analiz-kiberatak-na-kriticheskuyu-informatsionnuyu-infrastrukturu-s-iot-tehnologiyami> (дата обращения: 21.05.2026).

References

1. Bezrodny B.F. (2020) Features of cybersecurity of industrial control systems on railway transport. *Security Systems: Technical Journal*. No. 6. Pp. 34–35. (In Russian).
2. On the security of the critical information infrastructure of the Russian Federation: Federal Law No. 187-FZ of July 26, 2017. *Collection of Legislation of the RF*. 2017. No. 31. Art. 4745. (In Russian).
3. On amendments to certain legislative acts of the Russian Federation in connection with the adoption of the Federal Law “On the Security of the Critical Information Infrastructure of the Russian Federation”: Federal Law No. 193-FZ of July 26, 2017. *Collection of Legislation of the RF*. 2017. No. 31. Art. 4790. (In Russian).
4. On amendments to the Law of the Russian Federation “On Protection of Consumer Rights”: Federal Law No. 194-FZ of 07.07.2025 [Electronic resource]. Available at: URL: <http://pravo.gov.ru> (accessed: 19.06.2026). (In Russian).
5. López-Aguilar P., Batista E., Martínez-Ballesté A., Solanas A. (2022) Information Security and Privacy in Railway Transportation: A Systematic Review. *Sensors*. Vol. 22, no. 7698. DOI: 10.3390/s22207698
6. Panin D.N., Bobkov E.O., Balashova E.A. (2020) Analysis of cyberattacks on critical information infrastructure with IoT technologies. *Autonomy of Personality*. No. 2 (22) [Electronic resource]. Available at: <https://cyberleninka.ru/article/n/analiz-kiberatak-na-kriticheskuyu-informatsionnuyu-infrastrukturu-s-iot-tehnologiyami> (accessed: 21.05.2026). (In Russian).
7. Kirillova A.D. (2023) Risk assessment of information security of industrial control systems for industrial objects using cognitive modeling methods: Abstract of a Ph.D. Thesis of Engineering Sciences. Ufa, 17 p. (In Russian).
8. Shamsutdinov R.R. (2023) Intelligent system for monitoring information security of the industrial internet of things using artificial immune system mechanisms: Ph.D. Thesis of Engineering Sciences. Ufa, 139 p. (In Russian).
9. Smart Cities Need Smart IoT Security [Electronic resource]. Available at: <https://asimily.com/blog/smart-cities-need-smart-iot-security> (accessed: 19.08.2026).
10. Zhuk R.V. (2021) Methodology and algorithms for determining current threats to information security in personal data information systems: Ph.D. Thesis of Engineering Sciences. Krasnodar, 156 p. (In Russian).

О применении кибериммунного подхода и федеративного обучения
к обеспечению кибербезопасности интеллектуальных транспортных систем

11. Ferrag M.A., Friha O., Hamouda D. [et al.]. ML-EdgeIIoT-dataset [Electronic resource]. Available at: <https://www.kaggle.com/datasets/mohamedamineferrag/edgeiiotset-cyber-security-dataset-of-iiot-iiot> (accessed: 19.06.2026).

12. Luqman A., Luqman A., Mahesh R., Chattopadhyay A. (2025) Efficient Model Propagation for Peer-to-Peer Federated Learning using Minimum Spanning Tree and Gossip Networks [Electronic resource]. Available at: <https://cyberleninka.ru/article/n/analiz-kiberatak-na-kriticheskuyu-informatsionnuyu-infrastrukturu-s-iiot-tehnologiyami> (accessed: 21.05.2026).

Поступила в редакцию: 20.07.2026

Received: 20.07.2026

Поступила после рецензирования: 25.08.2026

Revised: 25.08.2026

Принята к публикации: 11.09.2026

Accepted: 11.09.2026