**Пример оформления статьи**

**Обнаружение аномалий в промышленном IoT с использованием графовых нейронных сетей**

1.2.1 «Искусственный интеллект и машинное обучение» (физ.-мат.)

**Авторы:** Иванов И.В.1, Петрова А.С.2

1Московский физико-технический институт (национальный исследовательский университет), Долгопрудный, Россия; e-mail: ivanov.iv@mipt.ru; ORCID: 0000-0000-0000-0001  
2Санкт-Петербургский политехнический университет Петра Великого, Санкт-Петербург, Россия; e-mail: petrova.as@spbstu.ru; ORCID: 0000-0000-0000-0002

**Аннотация**

Работа посвящена обнаружению аномалий в потоках данных промышленного интернета вещей (IIoT), где сенсоры образуют динамически меняющийся граф технологического процесса. Предлагается метод на основе временных графовых нейронных сетей с контрастивной предподготовкой и адаптивным порогом принятия решений. Модель объединяет топологию оборудования и временные зависимости, а также учитывает смену режимов работы. На синтетико-реальных наборах данных предприятия (150 узлов, 220 ребер, 180 суток телеметрии) предложенный подход превзошёл базовые методы (Isolation Forest, LSTM-автоэнкодер, GCN) по ROC-AUC на 6–12 % и по F1 на 8–10 %. Показана робастность к пропускам, дрейфу распределений и ложным срабатываниям при перезапусках оборудования. Обсуждаются ограничения, требования к внедрению и интеграция с системами мониторинга.

**Ключевые слова:** промышленный IoT; обнаружение аномалий; графовые нейронные сети; контрастивное обучение; временные ряды; киберфизические системы.

**Список литературы**

1. Liu F. T., Ting K. M., Zhou Z.-H. Isolation Forest // *ICDM*. 2008. P. 413–422.
2. Chandola V., Banerjee A., Kumar V. Anomaly detection: A survey // *ACM Computing Surveys*. 2009. Vol. 41, No. 3. Article 15. DOI: 10.1145/1541880.
3. You J. et al. Graph Contrastive Learning with Augmentations // *NeurIPS*. 2020.
4. dos Santos M. et al. Explainable AI for Anomaly Detection in Industry 4.0 // *Sensors*. 2022. 22(3): 987. DOI: 10.3390/s22030987.
5. Кузнецов С. В., Фролов П. А. Методы обнаружения аномалий в киберфизических системах // *Информационные технологии*. 2023. Т. 29, № 4. С. 55–68. DOI: 10.0000/it.2023.29.4.55.

Пример цитирования в тексте: «…как показано в [4,5], интеграция GNN повышает устойчивость…».

**Industrial IoT Anomaly Detection with Graph Neural Networks**

**Authors:** Ivanov I.V.1; Petrova A.S.2

1Moscow Institute of Physics and Technology (National Research University), Dolgoprudny, Russia; e-mail: ivanov.iv@mipt.ru; ORCID: 0000-0000-0000-0001

2Peter the Great St. Petersburg Polytechnic University, St. Petersburg, Russia; e-mail: petrova.as@spbstu.ru; ORCID: 0000-0000-0000-0002

**Abstract**

We address anomaly detection in industrial IoT streams where sensors form a time-varying process graph. We propose a temporal graph neural network with contrastive pretraining and an adaptive decision threshold. The model captures equipment topology and temporal dependencies, handling regime changes. On semi-real datasets (150 nodes, 220 edges, 180 days), our method outperforms baselines (Isolation Forest, LSTM autoencoder, GCN) by 6–12% ROC-AUC and 8–10% F1. Robustness to missing values, distribution drift, and restart artifacts is demonstrated. We discuss limitations, deployment requirements, and integration with monitoring systems.

**Keywords:** industrial IoT; anomaly detection; graph neural networks; contrastive learning; time series; cyber-physical systems.