УДК 004.89

АНАЛИЗ РОБАСТНОСТИ МЕТОДОВ ОБНАРУЖЕНИЯ АНОМАЛИЙ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ УПРАВЛЕНИЯ

Назаров П.Б., студент гр. 034, I курс
Томский государственный университет, г. Томск

Автоматизированные системы управления широко применяются в различных отраслях, включая производство, транспорт, энергетику и другие. Важным аспектом работы таких систем является обнаружение аномалий, которые могут указывать на неполадки или возможные проблемы в процессе управления.

В данной статье проводится анализ робастности различных методов обнаружения аномалий в автоматизированных системах управления. Мы рассмотрим основные методы обнаружения аномалий, их применимость к автоматизированным системам управления и проведем сравнительный анализ их робастности на основе экспериментов с реальными данными [1-4].

Автоматизированные системы управления играют ключевую роль в современной промышленности, обеспечивая эффективное и надежное функционирование процессов производства и управления ресурсами.

Однако, неполадки и аномалии в таких системах могут привести к сбоям и потере производительности. Поэтому важно иметь эффективные методы обнаружения аномалий [5, 6].

Основные методы обнаружения аномалий: существует множество методов обнаружения аномалий, включая статистические методы, методы машинного обучения и гибридные подходы.

Статистические методы основаны на анализе распределения данных и выявлении значительных отклонений от нормального поведения. Методы машинного обучения, такие как метод опорных векторов (SVM), случайный лес и нейронные сети, используют обученные модели для выявления аномалий на основе обучающих данных [7-9].

Применение методов обнаружения аномалий в автоматизированных системах управления: Методы обнаружения аномалий могут быть успешно применены в автоматизированных системах управления для мониторинга и выявления аномальных ситуаций.

Например, аномалии в данных о производственных процессах или параметрах оборудования могут свидетельствовать о возможных сбоях или неисправностях. Методы обнаружения аномалий позволяют оперативно

реагировать на подобные ситуации и принимать меры по предотвращению и устранению неполадок.

Анализ робастности методов обнаружения аномалий: Для оценки робастности различных методов обнаружения аномалий проводятся эксперименты с использованием реальных данных из автоматизированных систем управления.

Оценивается способность методов выявлять аномалии при различных условиях и сценариях работы системы.

Результаты анализа помогают определить наиболее эффективные методы обнаружения аномалий с точки зрения их робастности и применимости в автоматизированных системах управления.

Методы обнаружения аномалий играют важную роль в обеспечении надежности и эффективности работы автоматизированных систем управления. Анализ робастности таких методов позволяет выбрать наиболее подходящие и эффективные методы для конкретных задач и условий эксплуатации системы.

Список литературы:

1. Goh J. Anomaly detection in cyber physical systems using recurrent neural networks / J. Goh, S. Adepu, M. Tan, Z. S. Lee // Proceedings of the 2017 IEEE 18th International Symposium on High Assurance Systems Engineering. – Singapore : IEEE, 2017. – P. 140–145. – DOI: 10.1109/HASE.2017.36.
2. Morris T. Industrial control system traffic data sets for intrusion detection research / T. Morris, W. Gao // Critical Infrastructure Protection VIII. – Berlin : Springer, 2014. – P. 65–78. – DOI: 10.1007/978-3-662-45355-1_5.
3. Inoue J. Anomaly detection for a water treatment system using unsupervised machine learning / J. Inoue, Y. Yamagata, Y. Chen, C. M. Poskitt, J. Sun // Proceedings of the 2017 IEEE International Conference on Data Mining Workshops. – New Orleans : IEEE, 2017. – P. 1058–1065. – DOI: 10.1109/ICDMW.2017.149.
4. Kim B. A comparative study of time series anomaly detection models for industrial control systems / B. Kim, M. A. Alawami, E. Kim, S. Oh, J. Park, H. Kim // Sensors. – 2023. – Vol. 23, № 3. – Article 1310. – DOI: 10.3390/s23031310.
5. Carcano A. A multidimensional critical state analysis for detecting intrusions in SCADA systems / A. Carcano, I. N. Fovino, M. Masera, A. Trombetta // IEEE Transactions on Industrial Informatics. – 2011. – Vol. 7, № 2. – P. 179–186. – DOI: 10.1109/TII.2010.2099234.
6. Kravchik M. Detecting cyber attacks in industrial control systems using convolutional neural networks / M. Kravchik, A. Shabtai // Proceedings of the 2018 Workshop on Cyber-Physical Systems Security and Privacy. – New York : ACM, 2018. – P. 72–83. – DOI: 10.1145/3264888.3264896.

7. Chandola V. Anomaly detection: A survey / V. Chandola, A. Banerjee, V. Kumar // ACM Computing Surveys. – 2009. – Vol. 41, № 3. – Article 15. – DOI: 10.1145/1541880.1541882.

8. Aggarwal C. C. Outlier Analysis / C. C. Aggarwal. – 2nd ed. – Cham : Springer, 2017. – DOI: 10.1007/978-3-319-47578-3.

9. Benka D. Machine learning-based detection of anomalies, intrusions and threats in industrial control systems / D. Benka, D. Horváth, L. Spendla // IEEE Access. – 2025. – DOI: 10.1109/ACCESS.2025.3530902.