УДК 004.89

ИСПОЛЬЗОВАНИЕ БАЙЕСОВСКИХ СЕТЕЙ ДЛЯ ВЫЯВЛЕНИЯ АНОМАЛИЙ В ДАННЫХ

Захарова Т.В., студент гр. 09-213, II курс
Казанский (Приволжский) федеральный университет, г. Казань

В мире информационных технологий, где данные играют ключевую роль, обнаружение аномалий становится все более важной задачей. Аномалии, или выбросы, представляют собой данные, которые существенно отличаются от обычного шаблона или поведения. Это может быть признаком неисправности в системе, мошеннической деятельности или других проблемах, требующих внимания. В последние годы Байесовские сети стали одним из мощных инструментов для выявления аномалий в данных [1-5].

Байесовская сеть – это вероятностная модель, представляющая собой граф, в котором узлы представляют случайные переменные, а ребра между узлами представляют вероятностные зависимости между этими переменными. С помощью Байесовских сетей можно моделировать неопределенность и выражать вероятностные зависимости между переменными.

Одним из ключевых преимуществ Байесовских сетей является их способность моделировать сложные вероятностные зависимости в данных. Это делает их эффективным инструментом для обнаружения аномалий, особенно в ситуациях, когда аномалии могут быть следствием сложных и неочевидных взаимосвязей [6, 7].

Существует несколько способов использования Байесовских сетей для обнаружения аномалий:

- Моделирование нормального поведения: Байесовские сети могут быть обучены на наборе данных, чтобы моделировать нормальное поведение системы или процесса. После этого любые отклонения от этого нормального поведения могут быть интерпретированы как аномалии [8, 9].
- Выявление несовпадений в данных: Байесовские сети могут использоваться для сравнения различных характеристик данных и выявления несовпадений или неожиданных закономерностей. Например, если средняя температура в помещении обычно колеблется в определенном диапазоне, а затем внезапно возникают сильные колебания, это может быть признаком аномалии.
- Обнаружение мошеннической деятельности: В финансовой сфере Байесовские сети могут использоваться для выявления мошеннических операций. Они могут анализировать образцы потребления, транзакции или другие

финансовые данные и идентифицировать необычные или подозрительные паттерны, которые могут указывать на мошенничество.

- Анализ сетевой активности: В области кибербезопасности Байесовские сети могут использоваться для анализа сетевой активности и обнаружения аномального поведения, такого как вторжения или атаки на систему.

Байесовские сети представляют собой мощный инструмент для обнаружения аномалий в данных. Их способность моделировать сложные вероятностные зависимости и выявлять необычные паттерны делает их ценным инструментом для различных областей, включая финансы, кибербезопасность, здравоохранение и многое другое. В будущем можно ожидать дальнейшего развития методов анализа данных на основе Байесовских сетей для более точного и эффективного обнаружения аномалий.

Список литературы:

1. 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.
2. Pearl J. Probabilistic Reasoning in Intelligent Systems: Networks of Plausible Inference / J. Pearl. – San Mateo : Morgan Kaufmann, 1988. – 552 p.
3. Koller D. Probabilistic Graphical Models: Principles and Techniques / D. Koller, N. Friedman. – Cambridge : MIT Press, 2009. – 1231 p.
4. Heckerman D. A tutorial on learning with Bayesian networks / D. Heckerman // Learning in Graphical Models. – Dordrecht : Springer, 1998. – P. 301–354. – DOI: 10.1007/978-94-011-5014-9_11.
5. Friedman N. Bayesian network classifiers / N. Friedman, D. Geiger, M. Goldszmidt // Machine Learning. – 1997. – Vol. 29. – P. 131–163. – DOI: 10.1023/A:1007465528199.
6. Cheng J. Comparing Bayesian network classifiers / J. Cheng, R. Greiner // Proceedings of the Fifteenth Conference on Uncertainty in Artificial Intelligence. – San Francisco : Morgan Kaufmann, 1999. – P. 101–108. – URL: https://arxiv.org/abs/1301.6684. (дата обращения: 01.06.2025).
7. Mihaljević B. Bayesian networks for interpretable machine learning and optimization / B. Mihaljević, C. Bielza, P. Larrañaga // Neurocomputing. – 2021. – Vol. 456. – P. 648–665. – DOI: 10.1016/j.neucom.2021.01.138.
8. Pauwels S. An anomaly detection technique for business processes based on extended dynamic Bayesian networks / S. Pauwels, T. Calders // Proceedings of the 34th ACM/SIGAPP Symposium on Applied Computing. – New York : ACM, 2019. – P. 494–501. – DOI: 10.1145/3297280.3297326.

9. Hill D. J. Real-time Bayesian anomaly detection in streaming environmental data / D. J. Hill, B. S. Minsker, E. Amir // Water Resources Research. – 2009. – Vol. 45, № 4. – Article W00D28. – DOI: 10.1029/2008WR006956.