УДК 004.89

СРАВНЕНИЕ ПОДХОДОВ МАШИННОГО ОБУЧЕНИЯ И ГЛУБОКОГО ОБУЧЕНИЯ В ОБНАРУЖЕНИИ АНОМАЛИЙ В ТЕЛЕКОММУНИКАЦИОННЫХ ДАННЫХ

Федорова В.Л., студент гр. ИУ12-41М, III курс
Московский государственный технический университет имени Н. Э. Баумана,
г. Москва

Обнаружение аномалий в телекоммуникационных данных играет важную роль в обеспечении качества обслуживания и безопасности сетей связи. В данной статье мы сравним подходы машинного обучения и глубокого обучения в контексте обнаружения аномалий в телекоммуникационных данных, проанализируем их преимущества и недостатки, а также рассмотрим сферы их применения [1].

Подходы машинного обучения:

- *Методы машинного обучения* включают в себя такие алгоритмы, как метод ближайших соседей, методы кластеризации, наивный байесовский классификатор, метод опорных векторов и случайный лес.
- *Преимущества:* Эти методы могут быть эффективны в обнаружении простых аномалий и обработке небольших объемов данных. Они обладают хорошей интерпретируемостью результатов и требуют относительно небольшого объема вычислительных ресурсов.
- *Недостатки: Методы машинного обучения могут иметь ограниченную способность выявления сложных аномалий и требуют тщательного инженерного проектирования признаков [2].*

Подходы глубокого обучения:

- *Глубокое обучение* включает в себя нейронные сети с многими слоями, такие как сверточные нейронные сети (CNN), рекуррентные нейронные сети (RNN) и глубокие автоэнкодеры.
- *Преимущества:* Глубокое обучение обладает способностью автоматического извлечения признаков из данных, что делает его эффективным для обнаружения сложных и нелинейных аномалий. Оно также может обрабатывать большие объемы данных и обучаться на них без необходимости ручного определения признаков.
- *Недостатки: Глубокое обучение требует большого количества размеченных данных для обучения, а также вычислительных ресурсов для обучения и инференса [3].*

Сравнение:

- *Прецизия:* Глубокое обучение обычно обеспечивает более высокую точность в обнаружении сложных аномалий, в то время как методы машинного обучения могут быть более подходящими для простых задач.
- *Объем данных:* Глубокое обучение лучше подходит для обработки больших объемов данных, в то время как методы машинного обучения могут быть эффективны при ограниченном количестве данных.
- *Интерпретируемость:* Методы машинного обучения часто обладают более простой интерпретацией результатов, в то время как глубокое обучение может быть менее интерпретируемым из-за сложности моделей и процесса обучения [4].

Применение:

- *Методы машинного обучения* могут быть эффективны в обнаружении аномалий в телекоммуникационных данных, таких как обнаружение необычных паттернов звонков или трафика.
- *Глубокое обучение* может быть особенно полезным для обнаружения сложных аномалий, таких как атаки в сетях связи или необычные модели потребления услуг.

Оба подхода, машинное обучение и глубокое обучение, имеют свои преимущества и недостатки в обнаружении аномалий в телекоммуникационных данных. Выбор подхода зависит от конкретной задачи, объема данных и требований к точности и интерпретируемости результатов [5].

Список литературы:

1. Lakhina, A. Diagnosing network-wide traffic anomalies / A. Lakhina, M. Crovella, C. Diot // Proceedings of the ACM SIGCOMM Conference. – New York : ACM, 2004. – P. 219–230. – DOI 10.1145/1015467.1015492.
2. Thottan, M. Anomaly detection in IP networks / M. Thottan, C. Ji // IEEE Transactions on Signal Processing. – 2003. – Vol. 51, № 8. – P. 2191–2204. – DOI 10.1109/TSP.2003.814797.
3. Barford, P. A signal analysis of network traffic anomalies / P. Barford, J. Kline, D. Plonka, A. Ron // Proceedings of the ACM SIGCOMM Internet Measurement Workshop. – Marseille : ACM, 2002. – P. 71–82. – DOI 10.1145/637201.637210.
4. Brutlag, J. D. Aberrant behavior detection in time series for network monitoring / J. D. Brutlag // Proceedings of the 14th Systems Administration Conference. – New Orleans : USENIX Association, 2000. – P. 139–146.

5. Fontugne, R. MAWILab: combining diverse anomaly detectors for automated anomaly labeling and performance benchmarking / R. Fontugne, P. Borgnat, P. Abry, K. Fukuda // Proceedings of the 6th International Conference on Emerging Networking Experiments and Technologies. – New York : ACM, 2010. – Article 8. – DOI 10.1145/1921168.1921179.