УДК 510

**Девришев Н. Э., Хэ Ю., Петросян О. Л.**

# Обнаружение аномалий во временных рядах с помощью методов прогнозирования

**1. Введение.** В настоящее время выявление аномалий применимо к широкому кругу областей [1]. Оно используется банковскими системами безопасности для обнаружения мошеннических действий, в промышленности – для предотвращения неисправностей оборудования из-за отсутствия своевременного ремонта, в системах поиска вторжений. В связи с высокой востребованностью методов выявления аномалий было разработано и протестировано большое количество техник для решения данной задачи [1]. В статье рассматривается метод прогнозирования, который включает в себя алгоритм, с определённой точностью приближающий исходный временной ряд, и модуль, позволяющий классифицировать отклонения от прогноза модели в качестве аномалий.

Применимо к обнаружению аномальных значений во временных рядах метод прогнозирования можно выделить по многим причинам. Во-первых, прогнозирование временных рядов – это отдельная быстроразвивающаяся сфера, соответственно, нам доступны все её инструменты. Во-вторых, метод прогнозирования показывает впечатляющие результаты поиска аномалий как в одномерных, так и в многомерных временных рядах. В-третьих, данная техника прозрачна и легко объяснима.

В настоящей работе продемонстрированы все вышеупомянутые преимущества на наборе данных, предоставленных соревнованием платформы Hexagon-ML [2], используя для прогнозирования ансамблевые (LightGBM, XGBoost) и нейросетевые (FCNN, Bi-GRU, Bi-LSTM) алгоритмы, с последующим выбором наилучшего. В процессе исследований были использованы результаты работ [3–6].

*Девришев Надир Эльнурович* – студент, Санкт-Петербургский государственный университет; e-mail: st077036@student.spbu.ru, тел.: +7(902)182-90-11

*Хэ Юйлун* – студент, Санкт-Петербургский государственный университет; e-mail: heyulong1998@gmail.com, тел.: +7(999)226-63-45

*Петросян Ованес Леонович* – доцент, Санкт-Петербургский государственный университет; e-mail: petrosian.ovanes@yandex.ru, тел.: +7(911)740-80-19

**2. Соревнование.** Метод опробован на наборе данных соревнования «Multi-dataset Time-Series Anomaly Detection Competition, SIGKDD 2021» [2] от популярной платформы Hexagon-ML.

**2.1. Описание данных.** В описании данных рассматриваемого соревнования составители говорят о длительном застое в поиске методов выявления аномалий, а также об однообразии данных, принятых эталонными, к которым исследователи применяют свои методы, что не позволяет отразить всю вариативность задачи. В связи с этим организаторы соревнования *«Multi-dataset Time-Series Anomaly Detection»* предоставляют к изучению 250 одномерных независимых временных рядов, каждый из которых содержит ровно по одному аномальному участку. Предложенный набор отражает результат двадцатилетнего исследования научных статей на тему обнаружения аномалий. Кроме того, такое разнообразие данных принуждает найти единый для всех временных рядов обобщённый алгоритм выявления аномалий.

**2.2. Визуализация данных.** Данные представляют собой 250 одномерных временных рядов, отображённых в 250 файлах формата .txt. В названии каждого файла содержится информация о количестве тренировочных и тестовых данных `<id>_<name>_<split-number>.txt`. Например, название `004_UCR_Anomaly_2500.txt` говорит о том, что в четвёртом по порядку наборе данных 2500 значений представлены для обучения нашей модели, а остальные – для тестирования (рис. 1). Участок с аномальным значением может находиться лишь в тестовой части рассматриваемых данных.

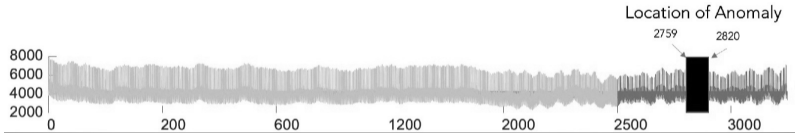


**Рис. 1.** Представление данных с разбиением на тестовую (до 2500) и тренировочную (от 2500) выборки

Каждый временной ряд состоит из повторяющихся видов простых паттернов и одного ярко выраженного аномального участка (рис. 2).

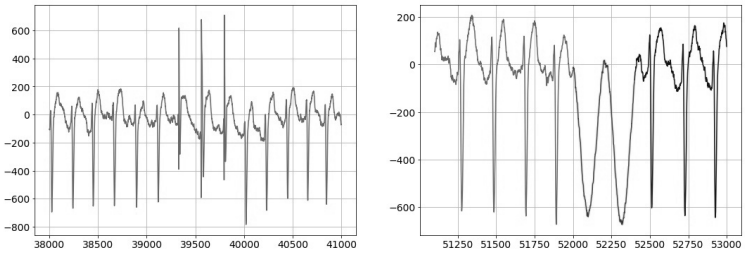


**Рис. 2.** Пример временного ряда и аномального участка

**3. Подход к решению.** На сегодняшний день найдено большое количество техник, с разной степенью точности решающих задачу поиска аномалий в различных её вариациях [1]. Даже для метода прогнозирования не существует единого алгоритма, который бы одинаково хорошо обнаруживал аномалии абсолютно для всех типов временных рядов или, по меньшей мере, для большинства.

Возникновению настоящей работы весьма сильно поспособствовало открытое соревнование по обнаружению аномалий во временных рядах «Power Laws: Detecting Anomalies in Usage» [7] от компании Schneider Electric, предоставившей в свободный доступ не только набор собственных данных, но и алгоритмы финалистов турнира, которые и были взяты нами за основу исследования. В качестве основных алгоритмов прогнозирования временного ряда, использованных призёрами соревнования, можно выделить градиентный бустинг (XGBoost) и простую полносвязную нейронную сеть (Fully Connected Neural Networks, или FCNN). Данные модели с высокой точностью приближали временной ряд, после чего аномальными признавались значения, не входящие в доверительный интервал предсказания.

Качество метода прогнозирования в задаче поиска аномалий определяется преимущественно качеством прогнозирования временного ряда используемой модели. Несмотря на высокую точность приближения временного ряда в наборе данных Scneider Electric, в рассматриваемом соревновании представленные алгоритмы могут не обладать такой же прогнозной способностью. В связи с этим было принято решение заменить алгоритмы финалистов соревнования Schneider Electric на другие предпочтительные для прогнозирования временных рядов алгоритмы, такие как LightGBM, LSTM, Bi-GRU,

и сравнить результаты.

**3.1. Полносвязная нейронная сеть.** Полносвязная нейронная сеть – это сеть, в которой каждый нейрон связан со всеми остальными нейронами, находящимися в соседних слоях. Несмотря на свою простоту, данная архитектура неплохо справляется с предсказанием значений временного ряда. Зачастую, для предотвращения эффекта переобучения используют технологию прореживания.

**3.2. Bi-LSTM.** Двунаправленные сети с долгой краткосрочной памятью (англ. bidirectional long short-term memory) – модификация рекуррентных нейронных сетей, способная учитывать долговременные зависимости. Архитектура показала неплохие результаты в задачах с данными, представленными в виде последовательностей, в частности, в прогнозировании временных рядов. Кроме того, подобные сети улавливают зависимости значений последовательностей как с начала, так и с конца.

**3.3. Bi-GRU.** Управляемые рекуррентные нейроны (англ. bidirectional gated recurrent units) являются упрощённой, но не менее эффективной версией сетей LSTM. Мы так же использовали двунаправленную архитектуру из-за её превосходства над классической в прогнозировании временных рядов.

**3.4. XGBoost.** Градиентный бустинг (англ. extreme gradient boosting) – это техника машинного обучения, строящая модель предсказания в виде ансамбля слабых предсказывающих моделей. Градиентный бустинг обучает множество моделей постепенно, аддитивно и последовательно.

**3.5. LightGBM.** Light Gradient Boosting Machine – более эффективная, экономная и быстрая реализация градиентного бустинга, основанная на ансамбле над решающими деревьями. Данный алгоритм показал впечатляющие результаты на соревновании «The M5 forecasting competition» в 2020-м году.

**3.6. Следующий шаг.** Поиск аномалий не ограничивается одним лишь прогнозированием временного ряда. После обучения алгоритма с хорошей прогнозной способностью необходимо понять, какие именно значения считать аномальными. В задаче с нефиксированным числом аномалий используют построение доверительного интервала прогноза и обозначают аномалиями значения, которые из данного интервала выбиваются. Для правильной работы метода необходимо обеспечить отсутствие в обучающей выборке аномальных значений, чтобы модель не подстраивалась под них. Ввиду спе-

цифики задачи необходимо внести некоторые изменения в вышеописанный метод обозначения аномалий, так как в рассматриваемых нами временных рядах содержится всего одно аномальное значение. На первый взгляд может показаться, что аномалией можно обозначить наиболее отклонившееся от прогноза значение, но практическим путём было выяснено, что данный метод не является действенным, и в качестве ответа выдаются значения, на которых ошиблась рассматриваемая модель. Решением является использование интегрального отклонения, т. е. суммы отклонений на отдельно взятом участке, вычисляемой по формуле

$$R_k = \sum_{i=k-\frac{w}{2}}^{k+\frac{w}{2}} |y_i - \widetilde{y}_i|, \qquad k = \overline{\frac{w}{2}, n - \frac{w}{2}}, \tag{1}$$

где $n$ – длина временного ряда, $w$ – ширина окна, $y_i$ – истинные значения, $\widetilde{y}_i$ – прогнозируемые.

О других интересных методах обнаружения аномалий можно узнать в статьях [6, 8, 9].

**4. Результаты.** Для всех вычислений использовался компьютер с процессором Intel(R) Core(TM) i3-7020U @ 2.30GHz, оперативной памятью 4,00 Гб и операционной системой Windows 10 Home. Реализация описанных алгоритмов проводилась в Jupyter Notebook 6.4.5.

Здесь оцениваются и сравниваются между собой результаты работы пяти алгоритмов, о которых было написано в пункте 3.

**4.1. Точность моделей.** Как уже было заявлено ранее, метод прогнозирования в задаче поиска аномалий сильно зависит от качества прогнозирующей модели, поэтому крайне важно обратить внимание на выбор правильного алгоритма.

В таблице 1 представлено сравнение среднего коэффициента детерминации ($\boldsymbol{R^2}$, R-квадрат) для пяти используемых моделей прогнозирования. Среднее считалось по подвыборке наборов данных.

**Таблица 1.** Качество алгоритмов

| | **Коэффициент детерминации** |
|---|---|
| Neural Networks | 0,78577447 |
| XGBoost | 0,96153277 |
| LightGBM | 0,95830702 |
| Bi-LSTM | 0,85766110 |
| Bi-GRU | 0,86914308 |

**4.2. Поиск аномалий.** После применения прогнозирующей модели для приближения временного ряда следующим важным шагом является детекция аномалий. В таблице 2 представлена точность обнаружения аномалий различными алгоритмами. Для проверки точности поиска аномалий была выбрана подвыборка, так как изначально набор данных содержал большое количество однообразных временных и рядов.

**Таблица 2.** Качество алгоритмов

| | **Процент верно обнаруженных аномалий** |
|---|---|
| Neural Networks | 52,9% |
| XGBoost | 23,5% |
| LightGBM | 47,1% |
| Bi-LSTM | 88,2% |
| Bi-GRU | 58,9% |

**4.3. Выводы.** Полученные результаты показали зависимость между качеством алгоритма прогнозирования и точностью обнаружения аномалий.

Как легко заметить, высокая прогнозируемая способность не гарантирует высокой точности выявления аномальных значений. Наоборот, достаточно хорошие прогнозирующие модели XGBoost и LightGBM обладают плохой способностью правильно обнаруживать аномалии. Это объясняется сложностью и мощностью алгоритмов. Они способны приближать не только данные, встречающиеся в обучающей выборке, но и аномальные значения.

Другой же крайностью являются полносвязные нейронные сети и сети Bi-GRU, которые обладают более слабой прогнозной способностью, из-за чего среди большого количества сильных отклонений истинных значений от прогнозируемых сложно выделить аномальные.

Лучшим выбором для рассматриваемой задачи оказался алгоритм Bi-LSTM, который достаточно хорошо ввиду своей сложности приближает временную последовательность, но при этом не подстраивается под аномальные значения из тестовой выборки (рис. 3).

**5. Заключение.** Метод прогнозирования является очень эффективной техникой обнаружения аномалий. Точность данного метода коррелирует с прогнозной способностью использующейся модели. Но к выбору алгоритма стоит подходить осторожно, выбирая среднее

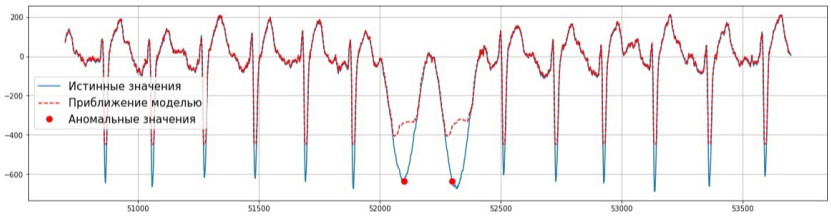


**Рис. 3.** Пример работы алгоритма Bi-LSTM

между сложной и мощной моделью и моделью совсем слабой, обладающей плохой обобщающей способностью.

## Литература


1. Chandola V., Banerjee A., Kumar V. Anomaly detection: A survey // ACM Computing Surveys. 2009. Vol. 41. No 3. P. 1–58.

2. Multi-dataset Time-Series Anomaly Detection Competition, SIGKDD 2021 [Электронный ресурс]: `URL:https://compete.hexagon-ml.com/practice/competition/39/` (дата обращения: 01.03.22).

3. Староверова К. Ю., Буре В. М. Мера различия временных рядов, основанная на их характеристиках // Вестник Санкт-Петербургского университета. Прикладная математика. Информатика. Процессы управления. 2017. Т. 13. № 1. С. 51–60.

4. Zhang Y., Xu F., Zou J., Petrosian O. L., Krinkin K. XAI Evaluation: Evaluating Black-Box Model Explanations for Prediction // II International Conference on Neural Networks and Neurotechnologies (NeuroNT). 2021. P. 13–16.

5. Zhang Y., Ma R., Liu J., Liu X., Petrosian O. L., Krinkin K. Comparison and Explanation of Forecasting Algorithms for Energy Time Series // Mathematics. 2021. Vol. 9. No 21. Art. no 2794.

6. Zou J., Petrosian O., Xu F.Explainable AI: Using Shapley Value to Explain the Anomaly Detection System Based on Machine Learning Approaches // Процессы управления и устойчивость. 2020. Vol. 7. No 1. P. 355–360.

7. Power Laws: Detecting Anomalies in Usage [Электронный ресурс]: URL:https://www.drivendata.org/competitions/52/anomaly-detection-electricity/ (дата обращения: 01.03.22).

8. Zou J., Xu F., Zhang Y., Petrosian O. L., Krinkin K. High-Dimensional Explainable AI for Cancer Detection// International Journal of Artificial Intelligence. 2021. Vol. 19. No 2. P. 195–217.

9. Zou J., Petrosian O. L. Explainable AI: Using shapley value to explain complex anomaly detection ML -based systems // Frontiers in Artificial Intelligence and Applications. 2020. Vol. 332. P. 152–164.