УДК 004.89

ДЕТЕКТИРОВАНИЕ АНОМАЛИЙ В ИИФОРМАЦИОННЫХ СИСТЕМАХ ПО ДАННЫМ МОНИТОРИНГА

Хоанг М. Т. (ИТМО)

Научный руководитель – кандидат технических наук, доцент Зудилова Т. В. (ИТМО)

Введение. Современные информационные системы представляют собой сложные распределенные структуры, обеспечивающие бесперебойную работу различных сервисов и приложений. Однако наличие множества взаимодействующих компонентов повышает вероятность возникновения аномалий, которые могут проявляться в виде сбоев, неожиданных нагрузок, сетевых атак или проблем с производительностью [1].

Для обеспечения надежности и безопасности инфраструктуры необходимо эффективное детектирование аномалий, что может быть достигнуто с помощью машинного обучения. Анализ данных мониторинга позволяет выявлять отклонения от нормы, прогнозировать возможные сбои и предотвращать аварийные ситуации [2]. Работа посвящена исследованию подхода к практическому применению машинного обучения для детектирования аномалий в инфраструктуре.

Основная часть. Для реализации приложения детектирования аномалий необходимо решить ряд ключевых этапов: сбор и предобработка данных мониторинга; выбор и обучение моделей; разработка приложения и его интеграция в реальную инфраструктуру.

Первый этап включает сбор и агрегирование данных, таких как системные логи, метрики производительности и сетевой трафик. На основе собранных данных проводится их предобработка: удаление шумов, нормализация и приведение к единому формату.

После подготовки данных следует этап выбора и обучения моделей машинного обучения, способных эффективно выявлять аномалии. На этом этапе важно учитывать особенности инфраструктуры и характер анализируемых данных, а также проводить тестирование моделей на исторических данных.

Следующий этап — разработка самого приложения. Это включает проектирование архитектуры и рабочих процессов, выбор подходящих технологий и инструментов разработки. Важной частью является создание интуитивно понятного и гибко настраиваемого пользовательского интерфейса, обеспечивающего удобную работу с системой мониторинга.

Заключительный этап — внедрение приложения в реальную инфраструктуру. Это включает развертывание, интеграцию с существующими системами мониторинга, тестирование на реальных данных и оптимизацию работы для повышения точности обнаружения аномалий.

Выводы. В результате исследования разработан метод детектирования аномалий в информационных системах, основанный на анализе данных мониторинга с использованием машинного обучения. Предложенный подход позволяет автоматически выявлять отклонения, что способствует повышению отказоустойчивости системы и снижению затрат на устранение последствий сбоев.

Список использованных источников:

1. Анализ Современных Систем мониторинга, Т.А Гайфулин, Д. С. Костомаров, научная статья, ЭВМ и программная обработка данных // Журнал Известия. ТулГУ. Технические науки, 2013.

2. Stahmann, Philip & Rieger, Bodo. A Benchmark for Real-Time Anomaly Detection Algorithms Applied in Industry. // Machine Learning, Optimization, and Data Science. — 2023. — P.20–34.