УДК 004.056.5

Разработка метода мониторинга и обнаружения аномалий в динамических системах IoT-устройств

Хахилев Н.И. (ИТМО)
Научный руководитель – кандидат технических наук, доцент Коржук В.М. (ИТМО)

Введение. Динамические системы IoT-устройств представляют собой сложную сеть взаимосвязанных датчиков и устройств, генерирующих огромные объемы данных в режиме реального времени. Установление связи между характеристиками IoT-устройств, структурой сети и паттернами нормального и аномального поведения имеет большое практическое значение, поскольку это позволяет разрабатывать эффективные методы мониторинга и раннего обнаружения проблем. Для обеспечения надежной работы таких систем требуется решение специальных задач по анализу больших объемов разнородных данных и выявлению отклонений от нормального функционирования. Изучение динамики IoT-систем наиболее актуально в связи с их стремительным развитием и возросшими требованиями к их надежности и безопасности для пользователей и окружающей среды [1].

Основная часть. С помощью разработанного метода решаются следующие два типа задач:

1) Задачи о мониторинге нормального функционирования IoT-устройств и выявлении отклонений от заданных параметров работы [1].
2) Задачи об обнаружении аномалий и потенциальных угроз безопасности в динамических системах IoT. При нормальной работе IoT-устройства генерируют данные с определенными статистическими характеристиками, отклонение от которых может сигнализировать о проблемах. Аномалии в работе IoT-систем могут быть вызваны как внутренними факторами, так и внешними воздействиями. Существует множество примеров в различных областях применения IoT, когда несвоевременное обнаружение аномалий приводило к серьезным сбоям в работе систем и нарушению их нормального функционирования. Задачи второго типа можно разделить на две категории по характеру возникновения аномалий [2]:

1) Аномалии, причины которых могут быть нестационарные процессы, не связанные с работой самих IoT-устройств, примером могут служить резкие изменения в окружающей среде или сбои в каналах передачи данных [3].
2) Аномалии, возникновение которых может быть обусловлено целенаправленными действиями злоумышленников, например, попытками взлома устройств или DDoS-атаками [3].

Выводы. Проведен анализ методов мониторинга и обнаружения аномалий в динамических системах IoT-устройств и разработана методика их применения и оценки эффективности.

Список использованных источников:

1) Технотон Инжиниринг. Разработка смарт датчиков, IoT датчиков // Технотон Инжиниринг. – 2025. – URL: https://ru.rd-technoton.com/tehnologiya-smart-datchikov-pri-razrabotke-iot-ustrojstv.html (дата обращения: 25.02.2025).

2) IoT Устройства: определение, применение, преимущества и будущее технологий // SofIoT. – 2024. – URL: https://sofiot.ru/blog/poleznye-materialy-iot/iot-ustroystva-opredelenie-primenenie-preimushchestva-i-budushchee-tekhnologiy/ (дата обращения: 25.02.2025).

3) Создание IoT-приложений с помощью tinyML // Control Engineering Россия. – 2025. – URL: https://controleng.ru/innovatsii/cifrovye-dvojniki/tinyml/ (дата обращения: 25.02.2025).

Автор_____Хахилев Н.И.

Научный руководитель_____Коржук В.М.