УДК 004.056.3

# Метод поиска первопричин инцидента в распределённых системах

**Заглубоцкий А.В.**
**Научный руководитель - кандидат технических наук, доцент Гусарова Н.Ф.**
Университет ИТМО
avzaglubotskii@itmo.ru

## Введение

Одной из частых задач, которая возникает в работе DevOps-инженеров, является поиск первопричин инцидентов. Ввиду роста масштаба и сложности современных распределенных систем, традиционные методы анализа, которые используют только логи, метрики и трассировки, становятся всё менее эффективными. Кроме того, существующие подходы к поиску первопричин часто основаны на предобученных моделях, использующих заранее подготовленные датасеты с типовыми сценариями инцидентов [1]. Однако, такой подход не является эффективным, так как при обучении редко охватываются все возможные варианты поведения системы, а также могут ошибочно интерпретировать нормальные процессы как аномальные.

## Основная часть

В рамках данной работы предлагается метод, который основан на применении Code Property Graph (CPG) - структуры данных, объединяющая три представления о коде: дерево абстрактного синтаксиса (AST), граф потока управления (CFG) и граф зависимости программы (PDG) [2]. Данная структура позволяет анализировать не только синтаксическую структуру, но и как элементы кода связаны между собой, что способствует более глубокому пониманию логики работы кода.

Дополнительно данный граф обогащается телеметрией, включающая сведения из логов, метрик и трассировок выполнения. Используя данную интеграцию, можно связать события, которые происходили во время работы системы, с конкретными частями исходного кода.

## Выводы

Разработан метод, обеспечивающий более глубокое понимание работы системы за счет объединения структурного представления программы с реальными данными о её выполнении. Такой подход позволяет видеть, как код функционирует в реальных условиях, что существенно повышает скорость и точность анализа инцидентов.

## Литература

1. Wang, P., Zhang, X., Cao, Z. Anomaly detection for microservice system via augmented multimodal data and hybrid graph representations // Information Fusion. — 2025. — Vol. 118. — Article 103017.
2. Lekssays, A., Mouhcine, H., Tran, K., Yu, T., Khalil, I. LLMxCPG: Context-Aware Vulnerability Detection Through Code Property Graph-Guided Large Language Models // USENIX Security Symposium, 2025.