УДК 004.056

В.В. ВОЛОБУЕВ

Научный руководитель – к.т.н., доцент В.С. КИРЕЕВ

Национальный исследовательский ядерный университет «МИФИ», Москва

ВРЕМЕННЫЕ МЕТКИ В ГРАФАХ ЗНАНИЙ ДЛЯ АНАЛИЗА ИНЦИДЕНТОВ

Предложен подход к добавлению временных меток в графы знаний для анализа инцидентов. Разработана схема добавления временных атрибутов и алгоритм фильтрации событий. Практическая ценность работы заключается в создании механизма для обогащения графов знаний временной информацией.

Введение

Современные информационные системы генерируют множество событий, анализ которых требует учета времени их возникновения. Существующие подходы к работе с графами знаний часто не учитывают временные характеристики данных, что затрудняет анализ последовательности событий при расследовании инцидентов [1–3, 5]. Для построения исходного графа знаний из текстовых данных в данной работе используется подход, основанный на нейросетевой модели T5 [4], который был дополнен механизмом временных меток.

Цель работы

Целью работы является разработка подхода к добавлению временных меток в графы знаний для анализа инцидентов.

Объект и предмет исследования

Объектом исследования выступают графы знаний как способ представления информации о событиях. Предметом исследования является механизм присвоения и использования временных меток для анализа временных последовательностей.

Процесс исследования

Для достижения цели решены следующие задачи: изучены основные способы хранения временных данных в графах [6]; разработана схема добавления временных атрибутов к элементам графа; создан алгоритм фильтрации событий по временным интервалам; реализован прототип системы для демонстрации возможностей подхода.

Предложенный подход позволяет добавлять к сущностям и связям графа знаний временные метки, указывающие момент их регистрации. Разработанный алгоритм обеспечивает выборку событий за заданный период времени и построение временных последовательностей. Прототип системы наглядно демонстрирует возможность анализа хронологии событий и выявления связанных инцидентов в пределах заданного временного окна.

Заключение

Практическая ценность работы заключается в создании доступного и эффективного механизма для обогащения графов знаний временной информацией. Разработанный подход может быть успешно использован в системах мониторинга и анализа событий для исследования последовательности действий при расследовании инцидентов. Полученные результаты открывают перспективы для дальнейшего развития методов временного анализа в графах знаний.

Список литературы

1. Калинина А.Ю., Киреев В.С. Визуализация корпуса документов с помощью извлечения сущностей и связей предметной области на основе нейросетевой модели глубокого обучения T5 / А.Ю. Калинина, В.С. Киреев // XXV Международная научно-техническая конференция «Нейроинформатика-2023»: Сборник научных трудов.

2. Гринева Н.В. Применение графов для определения состояний нарушения безопасности активов [Электронный ресурс] / Н.В. Гринева // CyberLeninka. – 2024. – URL: https://cyberleninka.ru/article/n/primenenie-grafov-dlya-opredeleniya-sostoyaniy-narusheniya-bezopasnosti-aktivov (дата обращения: 22.09.2025)

3. Дойникова Е.В. Совершенствование графов атак для мониторинга кибербезопасности: оперирование неточностями, обработка циклов, отображение инцидентов и автоматический выбор защитных мер / Е.В. Дойникова // Программные продукты и системы. – 2018. – Т. 15, № 1. м С. 45–60.

4. Израилов К.Е. Метод обнаружения атак различного генеза на сложные объекты на основе интеллектуальной нечеткой графо-ориентированной модели / К.Е. Израилов // Вопросы кибербезопасности. – 2023. – № 3. – С. 90–100. – DOI: 10.21681/2311-3456-2023-3-90-100.

5. Косимова М.Ш. Приложения теории графов в компьютерной сетевой безопасности [Электронный ресурс] / М. Ш. Косимова // CyberLeninka. – 2024. – URL: https://cyberleninka.ru/article/n/prilozheniya-teorii-grafov-v-kompyuternoy-setevoy-bezopasnosti (дата обращения: 15.10.2025).

6. Манжосов А.В. Метод автоматизированного построения графа знаний связности формальных моделей норм и требований в области информационной безопасности / А. В. Манжосов, И. П. Болодурина // Методы и системы защиты информации. – 2022. – № 2(44). – С. 49–56. – DOI: 10.14529/secur220207.