**Бекенева Яна Андреевна Формализация процессов обработки и интеллектуального анализа информации от разнородных источников в системах распределенного мониторинга**

ОГЛАВЛЕНИЕ ДИССЕРТАЦИИ

кандидат наук Бекенева Яна Андреевна

Введение

ГЛАВА 1. ОБЗОР СРЕДСТВ ОБРАБОТКИ И АНАЛИЗА ДАННЫХ В СИСТЕМАХ МОНИТОРИНГА

1.1 Постановка задачи

1.2 Формальное описание событий и их последовательностей на основе информации от систем мониторинга

1.3 Преобразование данных от разнородных источников

1.3.1. Алгоритмы корреляции событий

1.3.2. Задача устранения неопределенностей в данных

1.4 Выявление аномалий в процессах

1.5 Подходы к прогнозированию аномалий в процессах

1.6 Обзор алгоритмов классификации

1.7 Методики для выявления и прогнозирования отклонений

1.8 Выводы

2 ГЛАВА 2 ФОРМАЛИЗАЦИЯ ОБРАБОТКИ РАЗНОРОДНЫХ ДАННЫХ В СИСТЕМАХ РАСПРЕДЕЛЕННОГО МОНИТОРИНГА

2.1 Формальная модель последовательностей событий в системах распределенного мониторинга

2.1.1. Представление процесса в системах распределенного мониторинга

2.1.2. Задача выявления отклонений в событиях

2.1.3. Выявление типовых шаблонов для предсказания аномалий

2.2 Метод формирования последовательностей событий на основе данных от разнородных источников

2.2.1. Общие преобразования данных

2.2.2. Объединение записей, описывающих одно и то же событие

2.2.1.1 Неопределенность, связанная с идентификацией объекта наблюдения при одном событии

2.2.1.2 Неопределенность, связанная с идентификацией объекта наблюдения при нескольких одновременных событиях

2.3 Выводы

3 ГЛАВА 3 МЕТОДИКА АНАЛИЗА ПОСЛЕДОВТЕЛЬНОСТИ СОБЫТИЙ

3.1 Методика решения задач интеллектуального анализа событий

3.2 Анализ отдельно взятых событий

3.2.1 Группировка записей по составу атрибутов

3.2.2 Выбор модели классификации для каждой группы

3.2.3 Обучение моделей классификации

3.2.4 Применение обученных моделей к новым данным

3.3 Анализ последовательностей событий

3.3.1 Задача поиска частых наборов элементов

3.3.1.1 Разделение последовательности событий на транзакции

3.3.1.2 Идентификация транзакции

3.3.1.3 Идентификация элемента в транзакции

3.3.1.4 Определение порядка элементов в транзакции

3.3.1.5 Применение алгоритмов частых наборов

3.3.1.6 Выявление отклонений в ходе исполняемого процесса

3.4 Выявление отклонений в последовательности событий методами интеллектуального анализа процессов

3.4.1 Подготовка данных для применения методов интеллектуального анализа процессов

3.4.2 Применение методов интеллектуального анализа процессов

3.5 Выводы

4 ГЛАВА 4 ЭКСПЕРИМЕНТАЛЬНАЯ ПРОВЕРКА ПОЛУЧЕННЫХ РЕЗУЛЬТАТОВ

4.1 Анализ перемещений грузовых транспортных средств на распределенной территории предприятия

4.1.1 Общие преобразования данных

4.1.2 Интеграция записей об одном событии

4.1.3 Выявление отклонений среди отдельно взятых событий

4.1.3.1 Группировка данных по составу атрибутов

4.1.3.2 Классификация событий

4.1.4 Построение ассоциативных правил для последовательностей событий121

4.1.5 Построение модели бизнес процесса

4.2 Анализ перемещений сотрудников на территории офисного здания

4.2.1 Общие преобразования данных

4.2.2 Интеграция данных об одном событии

4.2.3 Выявление отклонений с помощью кластеризации событий

4.2.4 Построение ассоциативных правил для последовательностей событий128

4.2.5 Построение модели бизнес процесса

4.3 Анализ движения трафика в компьютерной сети организации

4.3.1 Общие преобразования данных

4.3.2 Интеграция данных об одном событии

4.3.3 Классификация событий

4.3.4 Построение ассоциативных правил

4.3.5 Построение моделей бизнес процессов

4.4 Выводы по главе

Заключение

Список сокращений и условных обозначений

Список литературы и электронных ресурсов

Приложение А

Приложение Б