**Кучер Алексей Викторович. Интеллектуальная система поддержки принятия решения на основе нечеткой логики для диагностики состояния сети передачи данных : диссертация ... кандидата технических наук : 05.13.01 Краснодар, 2007 221 с., Библиогр.: с. 192-202 РГБ ОД, 61:07-5/4571**

**61:07-5/4571**

**ГОУ ВПО «Кубанский государственный технологический университет»**

**На правах рукописи**

**КУЧЕР Алексей Викторович**

**ИНТЕЛЛЕКТУАЛЬНАЯ СИСТЕМА ПОДДЕРЖКИ ПРИНЯТИЯ**

**РЕШЕНИЯ НА ОСНОВЕ НЕЧЕТКОЙ ЛОГИКИ ДЛЯ ДИАГНОСТИКИ СО**

**СТОЯНИЯ СЕТИ ПЕРЕДАЧИ ДАННЫХ**

**Специальность 05.13.01 - «Системный анализ, управление и обработка**

**информации (информационные и технические системы)**

**Диссертация на соискание ученой степени**

**кандидата технических наук**

**Научный руководитель: к.т.н., профессор А.П.Частиков**

**Краснодар - 2007**

**СОДЕРЖАНИЕ**

**ВВЕДЕНИЕ 5**

**1 Обзор существующих решений и сущность проблемы мони-торинга и диагностики сетей передачи данных регионально¬го оператора связи 14**

**1.1 Анализ существующих систем управления сетями и место в**

**них задач мониторинга и диагностики сетевых процессов \_ 14**

**1.2 Анализ основных видов деятельности администратора сети**

**передачи данных и экспертная оценка критического множе¬ства задач по управлению сетевыми ресурсами 21**

**1.3 Анализ существующих методов мониторинга и диагностики**

**сетевых аномалий 26**

**1.3.1 Сигнатурный анализ 28**

**1.3.2 Статистические методы 31**

**1.3.3 Интеллектуальные системы 40**

**1.4 Анализ существующих методов и приемов поддержки при¬**

**нятия решений для задач мониторинга и диагностики со¬стояния сети передачи данных 43**

**1.4.1 Обобщенная схема принятия решения 44**

**1.4.2 Типы управленческих решений и формы их поддержки 47**

**1.4.3 Требования к СППР должностных лиц предприятия связи**

**по управлению сетью передачи данных 52**

**1.5 Характеристики и сравнительный анализ СППР, основан-ных на знаниях 54**

**1.5.1 Структура СППР, основанных на знаниях 54**

**1-.5.2 Классификация функциональных применений СППР,**

**основанных на знаниях, в исследуемой предметной об¬ласти 57**

**1.5.3 Организация знаний в базе знаний интеллектуальной**

**системы 58**

**1.6 Цели и задачи исследования 63**

**1.7 Выводы 65**

**2 Теоретические основы и математическое обеспечение интел-лектуальной СППР для диагностики состояния сети переда¬чи данных 67**

**2.1 Математическая модель сигнатурного анализатора сетевого**

**трафика 67**

**2.2 Математическая модель статистического анализатора сете¬вого трафика 72**

**2.3 Математическая модель нечеткой интеллектуальной систе¬мы для диагностики состояния сети передачи данных 82**

**2.3.1 Определение состава и характеристики входных и выход¬ных переменных нечеткой интеллектуальной системы 84**

**2.3.2 Математическая модель нечеткой базы знаний 88**

**2.3.3 Модели функций принадлежности лингвистических пере¬менных 92**

**2.3.4 Математическая модель системы нечеткого логического**

**вывода и дефаззификация выходного показателя 94**

**2.3.5 Задача оптимизации нечеткой базы знаний и методы её**

**решения 100**

**2.4 Выводы 103**

**3 Структура, состав, алгоритмическая и программная реали¬зация интеллектуальной СППР для диагностики состояния**

**сети передачи данных 106**

**3.1 Общие принципы построения и структурная схема интел¬**

**лектуальной СППР для диагностики состояния сети переда¬чи данных 106**

**3.2 Операционная схема методики разработки интеллектуаль¬**

**ной СППР для диагностики состояния сети передачи дан¬ных 113**

**3.3 Выбор инструментальных средств разработки интеллекту¬**

**альной СППР для диагностики состояния сети передачи данных 118**

**\* 3.4 Алгоритмическая реализация интеллектуальной СППР для**

**диагностики состояния сети передачи данных 124**

**3.4.1 Структура входных данных для мониторинга состояния**

**сети передачи данных 125**

**3.4.2 Алгоритм мониторинга состояния сети передачи данных \_ 130**

**3.4.3 Алгоритмическая реализация статистического анализатора 131**

**3.4.4 Алгоритмическая реализация сигнатурного анализатора 134**

**3.5 Разработка нечеткой интеллектуальной системы 138**

**3.5.1 Структурная схема нечеткой интеллектуальной системы \_ 138**

**3.5.2 Процедура разработки нечеткой интеллектуальной систе¬мы 145**

**• 3.6 Особенности программной реализации СППР 146**

**3.7 Выводы 151**

**4 Экспериментальные исследования работоспособности и эф-фективности интеллектуальной СППР для диагностики со-стояния сети передачи данных 153**

**4.1 Методика тестирования и оценки эффективности про¬граммных средств интеллектуальной СППР 153**

**4.2 Результаты тестирования программных средств системы 169**

**4.3 Оценка работоспособности и эффективности программных**

**средств системы 170**

**4.4 Оценка экономической эффективности внедрения интел¬лектуальной СППР 174**

**4.5 Настройка нечеткой базы знаний интеллектуальной систе¬мы 176**

**4.6 Выводы 185**

**ЗАКЛЮЧЕНИЕ 188**

**СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ 192**

**ПРИЛОЖЕНИЯ 1. ФРАГМЕНТЫ КОДА ПРОГРАММЫ, РЕА¬ЛИЗУЮЩИЕ АЛГОРИТМ МОНИТОРИНГА СОСТОЯНИЯ СЕТИ ПЕРЕДАЧИ ДАННЫХ 203**

**ПРИЛОЖЕНИЕ 2. СВИДЕТЕЛЬСТВО ОБ ОФИЦИАЛЬНОЙ РЕГИСТРАЦИИ ПРОГРАММЫ ДЛЯ ЭВМ 216**

**ПРИЛОЖЕНИЕ 3. АКТ О ПРОВЕДЕНИИ КОМПЛЕКСНЫХ ИСПЫТАНИЙ ПРОГРАММНОГО ПРОДУКТА «Интеллекту¬альная СППР для диагностики состояния СПД» 218**

**♦ ПРИЛОЖЕНИЕ 4. АКТ О ВНЕДРЕНИИ РЕЗУЛЬТАТОВ ДИС¬СЕРТАЦИОННОЙ РАБОТЫ В УЧЕБНЫЙ ПРОЦЕСС КУБГТУ 220**

ЗАКЛЮЧЕНИЕ

Основным научным результатом диссертационной работы является тео­ретическое обоснование, исследование методов построения и разработка ин­теллектуальной системы поддержки принятия решения на основе нечеткой ло­гики для мониторинга, анализа и диагностики состояния программно­аппаратного комплекса мультисервисной сети передачи данных регионального оператора связи.

Основные теоретические и практические результаты работы заключаются в следующем.

1. Исследованы современные системы управления компьютерными сетя­ми и место в них задач мониторинга, анализа и диагностики сетевых процессов. Проведен анализ существующих методов и приемов поддержки принятия ре­шений для задач управления СПД регионального оператора связи. Результатом данного исследования является вывод о необходимости создания человеко- машинной системы поддержки принятия решений, обеспечивающей информа­ционную, вычислительную и интеллектуальную поддержку профессиональной деятельности должностных лиц.
2. Исследованы современные методы диагностики сетевых аномалий (сигнатурный анализ, статистические методы, использование интеллектуаль­ных (экспертных) систем, нейросетей и генетических алгоритмов), выявлены их достоинства и недостатки. Сделан вывод о необходимости использования ком­плексного подхода к решению задач анализа и диагностики состояния элемен­тов сети передачи данных.
3. Проведен анализ основных видов деятельности администраторов СПД регионального оператора связи по управлению программно-аппаратным ком­плексом и сетевыми службами в виде множества задач. Проведено ранжирова­ние задач по степени их важности. Методами математической статистики про­ведено исследование наличия корреляционных связей между группами задач.

Определены критические задачи, которые оказались связанные с обнаружением и устранением аномалий в работе программного обеспечения, оборудования и сетевых служб.

1. Проведен сравнительный анализ моделей СППР, основанных на знани­ях. Сделан вывод о целесообразности из всех видов моделей выбрать нечеткую интеллектуальную систему, как наиболее подходящую в качестве советующей системы для решения нештатных нечетких задач, возникающих в процессе экс­плуатации СПД.
2. Разработана математическая модель сигнатурного анализатора анома­лий сетевого трафика. Проведена оценка вычислительной сложности сигнатур­ного метода и доказана возможность его использования в составе СППР для диагностики состояния СПД.
3. Разработана математическая модель статистического анализатора сете­вого трафика на основе метода подбора параметров весовых функций для вы­числения текущих статистических характеристик потока пакетов. Проведено обоснование выбора вида весовой функции и исследована её взаимосвязь с длиной выборки, достаточной для получения усредненных характеристик пото­ка пакетов СПД.
4. Разработана методика определения текущих статистических характери­стик потока сетевых пакетов: выборочное среднее £, выборочная дисперсия *d2* и статистика/2. Определены критерии аномального поведения сетевого трафи­ка.
5. Проведено обоснование выбора нечеткой модели представления знаний об источниках сетевых аномалий и нечеткой интеллектуальной (экспертной) системы, способной обрабатывать нечеткую информацию о нештатных ситуа­циях в рамках нечетких алгоритмов функционирования СПД. Определен состав и дана характеристика входных и выходных лингвистических переменных и их термов для построения нечеткой базы знаний с MISO-структурой.
6. Разработана математическая модель нечеткой базы знаний отдельного уровня модели сети как системы логических высказываний, связывающей зна­чения входных переменных с одним из возможных состояний уровня СПД. По­строена система логических уравнений, позволяющая вычислять значения функций принадлежности различных решений при фиксированных значениях выходных переменных.
7. Разработана математическая модель системы нечеткого логического вывода, основанная на использовании композиционного правила вывода Л.Заде. Обосновано использование нечеткого логического вывода Мамдани при нечетком значении входных переменных и метода дефаззификации (по методу «центра тяжести») выходного показателя.
8. Сформулирована задача оптимизации нечеткой базы знаний иссле­дуемой предметной области и показаны пути её решения на основе структур­ной и параметрической идентификации.
9. Разработан метод диагностики состояния СПД, основанный на детек­тировании и идентификации аномалий на всех уровнях сети. Экспертным пу­тем определены источники сетевых аномалий на каждом уровне сети.
10. Разработана структура интеллектуальной СППР для диагностики со­стояния СПД, реализующая проведение сигнатурного и статистического анали­за сетевого трафика и работу нечеткой интеллектуальной системы в случае по­явления нештатной сетевой ситуации.
11. Проведен анализ и обоснован выбор объектно-ориентированного язы­ка Java в качестве основного средства программирования СППР, позволяющего объединить разнородные элементы СППР между собой. Проанализированы со­временные средства разработки нечетких систем и сделан выбор в пользу паке­та Fuzzy Logic Toolbox вычислительной среды MatLab, который позволяет осуществить эффективную разработку нечеткой интеллектуальной системы для диагностики состояния СПД.
12. Определены показатели эффективности функционирования разрабо­танной СППР. Проведен эксперимент по проверке работоспособности и эффек­тивности разработанной СППР. Полученные оценки позволяют утверждать, что разработанная система обладает надежным программным обеспечением, хоро­шими возможностями по обнаружению и идентификации сетевых аномалий, может выявлять и идентифицировать их на всех уровнях сети за приемлемое время.
13. Проведена экономическая оценка эффективности внедрения разрабо­танной СППР по следующим показателям: стоимость разработки, стоимость эксплуатации и экономическая выгода от внедрения системы. Расчеты показа­ли, что расходы на создание и поддержку системы окупаются за первый год её эксплуатации. Внедрение системы позволит сохранить региональному операто­ру связи только на одном узле или сегменте СПД более 2 млн. 800 тыс. руб. в год.
14. Проведена настройка нечеткой базы знаний интеллектуальной систе­мы средствами Optimization Toolbox системы Matlab, построены таблицы весо­вых коэффициентов правил нечеткой базы знаний на двух обучающих выбор­ках и графики функций принадлежности нечетких термов входных и выходных переменных. Тестирование нечеткой системы Мамдани, после настройки, сви­детельствует о том, что база знаний хорошо описывает взаимосвязь признаков источников сетевых аномалий, соответствующего уровня модели сети, с вы­ходным показателем степени возможности состояния соответствующего уровня модели СПД.

По теме диссертации опубликовано 16 печатных работ. Из них 10 статей (в том числе 3 в изданиях, рекомендованных ВАК) и 6 тезисов докладов на Всероссийских конференциях. На программные продукты, используемые в СППР, получено свидетельство об официальной регистрации программ для ЭВМ в Федеральной службе по интеллектуальной собственности, патентам и товарным знакам.