УДК 004.652.4

05.00.00 Технические науки

**ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ВЫЧИСЛИТЕЛЬНОЙ СЕТИ С ИСПОЛЬЗОВАНИЕМ ИНТЕЛЛЕКТУАЛЬНЫХ СИСТЕМ**

Кучер Виктор Алексеевич
к.т.н

Магомадов Алексей Сайпудинович
д.т.н.

Чигликова Надежда Дмитриевна
к.т.н.

Дьяченко Роман Александрович
д.т.н.
*Кубанский государственный технологический университет, Краснодар, Россия*

Статья посвящена созданию интеллектуальной системы управления надёжностью работы сложной вычислительной сети. Это обусловлено тем, что современное телекоммуникационное оборудование генерирует всевозрастающее количество статистической информации. В целях информационной безопасности предлагается использовать в управлении сетями экспертную систему

Ключевые слова: ВЫЧИСЛИТЕЛЬНЫЕ СЕТИ, ИНТЕЛЛЕКТУАЛЬНАЯ СИСТЕМА УПРАВЛЕНИЯ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

UDC 004.652.4

Technical sciences

**PROVIDING INFORMATION SECURITY OF DATA-PROCESSING NETWORK WITH USE OF INTELLIGENT SYSTEM**

Kucher Viktor Alekseevich
Cand.Tech.Sci.

Magomadov Aleksey Saipudinovich
Dr.Sci.Tech.

Chiglikova Nadezhda Dmitrievna
Cand.Tech.Sci.

Dyachenko Roman Aleksandrovich
Dr.Sci.Tech.
*Kuban State Technological University, Krasnodar, Russia*

The article is devoted to creation of intelligent management system of complex data-processing network. This is caused by the fact that modern telecommunication hardware generates growing amount of statistic information. Expert system is offered to be used in management of networks for the purpose of information security

Keywords: DATA-PROCESSING NETWORKS, INTELLIGENT MANAGEMENT SYSTEM, INFORMATION SECURITY

Дальнейшее развитие современных сложных объектов управления, большой объем поступающей информации, трудоемкость решаемых задач, малое время для принятия решений приводят в отдельных случаях к несоответствию возможностей человека требованиям эффективно управлять объектом. Выход из данного положения заключается в создании интеллектуальной системы управления для помощи в оперативном управлении автоматическими системами, контроля правильности их работы и прогнозировании развития ситуации на объекте.

Существующая система управления (СУ) может быть представлена следующим образом (рис. 1) [1]:

$$Y = F(X, E, U),$$

где Y - множество состояний объекта управления (ОУ), E - множество состояний среды, в которой находится объект управления, U - множество управляемых параметров объекта.

Указанная СУ не всегда позволяет осуществить робастное управление сложными объектами. Для решения этой задачи были созданы интеллектуальные системы управления. Основное отличие интеллектуальных систем – наличие механизма системной обработки знаний. Главная архитектурная особенность, которая отличает интеллектуальные СУ от традиционных, - это механизм получения, хранения и обработки знаний для реализации соответствующих функций.

Известны роль и место интеллектуальной СУ при управлении таким сложным объектом как вычислительная сеть (ВС). Современная ВС состоит из коммутаторов, маршрутизаторов, межсетевых экранов, систем обнаружения вторжений и другого оборудования. Для управления этим оборудованием, предотвращения возможных сбоев и отказов необходима система управления ВС. Причем данная система должна быть не только автоматизированной, но и обладать интеллектуальными возможностями.


Рисунок 1. Традиционная система управления

Отметим что, современное телекоммуникационное оборудование генерирует множество статистической информации о своем состоянии. При этом администратор сети, даже очень опытный, не в силах отслеживать состояние всех устройств в ВС. Именно поэтому большая часть работы по сбору и анализу технологической информации о функционировании сети должна проводиться системой управления, а администратору должна выводиться только обработанная информация. В настоящее время существует несколько современных информационных технологий, позволяющих создавать интеллектуальные СУ: экспертные системы, искусственные нейронные сети, нечеткая логика, генетические алгоритмы и др.

На рис. 2 представлен один из возможных вариантов структуры

интеллектуальной системы управления ВС на базе экспертной системы (ЭС). Объекты 1, 2, … , N - это управляемые объекты сети: концентраторы, коммутаторы, маршрутизаторы, межсетевые экраны, системы обнаружения вторжений и другое программно-аппаратное сетевое оборудование.

Для управления соответствующим телекоммуникационным оборудованием используется специальное программное обеспечение - агент[2]. Они предназначены для сбора информации о состоянии контролируемых устройств и передача управляющих команд и откликов на них. Процедура диагностирования технологического состояния сетевого оборудования представляет собой определенную последовательность проверок реакции ОУ на управляющие и возмущающие воздействия. Эффективность процедур диагностирования определяется оптимальностью выбранной последовательности проверок, которую назовем стратегией поиска диагноза в множестве всех возможных причин отказов оборудования [1].

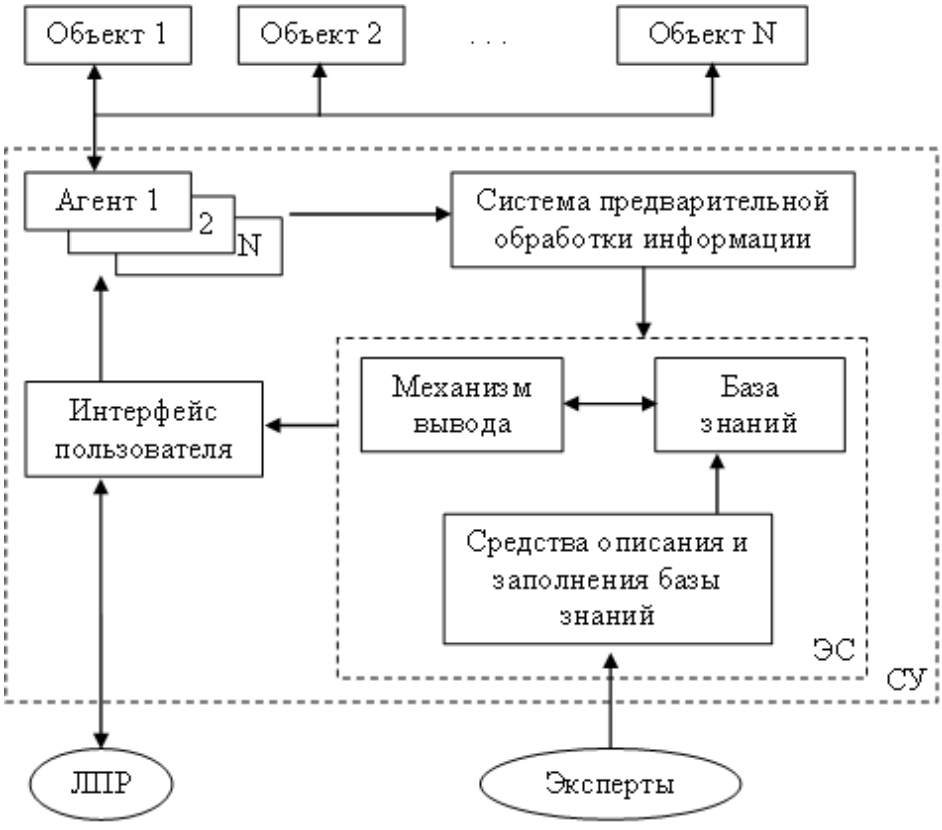


Рисунок 2. Система управления сетью с использованием ЭС

Предварительная обработка информации предназначена для сбора и обработки информации от агентов. Так как различное оборудование может передавать информацию о своем состоянии в отличном друг от друга формате, то предварительная обработка нужна для приведения полученных данных к унифицированному виду, понятному для обработки ЭС.

ЭС осуществляет анализ полученных данных и выдачу соответствующих объяснений или рекомендаций администратору сети или лицу, принимающему решения (ЛПР), например, по управлению конфигурацией оборудования, о причинах аномальной работы сети, о возможных последствиях, к которым может привести сложившаяся ситуация в ВС и др.

База знаний играет важнейшую роль в работе ЭС. Во многом насколько полно будут представлены в ней знания эксперта, зависит то, как будет ЭС анализировать полученные данные и выдавать соответствующие рекомендации.

Система правил представляет экспертные знания в следующем виде [1,3]:

$$\forall i, \forall j, \forall m_i : X_i = x_i \Rightarrow Pb(D_j \mid \overline{X}) = Pb_s(D_j \mid x_{im_i}),$$

где $\overline{X}$ – ряд признаков, по конкретным значениям которых принимается суждение о субъективной вероятности события из заранее определенного ряда событий $D_j$; $x_{im_i}$ – конкретное значение $X_i$ из множества $\{x_{im_i}\}$; $Pb_s$ - субъективная вероятность наступления события из множества возможных значений $\{Pb_s\}$.

Одной из удобных и привычных форм представления знаний импликативного вида для эксперта является – лингвистическая. Признаки $X_i$ и вероятности $Pb$ представлены лингвистическими переменными, определяемыми кортежами [1]:

$$\langle X_i, T_i, V_i, G_i, M_i \rangle, \langle Pb, P, U, S, Q \rangle,$$

где $X_i$ , $Pb$ – наименование соответствующих лингвистических переменных; $T_i$, $P$ – терм-множества переменных $X_i$ и $Pb$ соответственно, т.е. множество их лингвистических значений, представляющих собой наименования нечетких переменных $A_{if_i}$ $(f_i = \overline{1, p_i})$ и $B_l$ $(l = \overline{1, m})$ со значениями из универсальных множеств $V_i$ и $U$; $G_i$ и $S$ – синтаксические правила, порождающие названия $A_{if_i}$ и $B_l$ значений переменных $X_i$ и $Pb$; $M_i$ и $Q$ – семантические правила, позволяющие превращать каждое новое значение лингвистической переменной в нечеткую переменную.

Администратор осуществляет взаимодействие с СУ с помощью интерфейса пользователя.

**Литература**

1. Алиев Р.А., Абдикеев Н.М., Шахназаров М.М. Производственные системы с искусственным интеллектом. М., 1990, с. 202-222.

2. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы. СПб., 2002, с. 583-630.

3. Девятков В.В. Системы искусственного интеллекта: Учеб. пособие для высших учебных заведений. М., 2001, с. 242-289.

**References**

1. Aliev R.A., Abdikeev N.M., Shahnazarov M.M. Proizvodstvennye sistemy s iskusstvennym intellektom. M., 1990, s. 202-222.

2. Olifer V.G., Olifer N.A. Komp'juternye seti. Principy, tehnologii, protokoly. SPb., 2002, s. 583-630.

3. Devjatkov V.V. Sistemy iskusstvennogo intellekta: Ucheb. posobie dlja vysshih uchebnyh zavedenij. M., 2001, s. 242-289.