УДК 002:34+004.056.5

05.00.00 Технические науки

МОДЕЛЬ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРОЦЕССОВ УПРАВЛЕНИЯ ВЫЧИСЛИТЕЛЬНЫМИ СЕТЯМИ

Кучер Виктор Алексеевич
к.т.н.

Атрощенко Валерий Александрович
к.т.н.

Видовский Леонид Адольфович
д.т.н.

Трофимов Виктор Маратович
д.ф.-м.н.
Кубанский государственный технологический университет, Краснодар, Россия

С целью повышения безопасности передачи информации предложен один из возможных подходов к моделированию процессов управления вычислительными сетями с элементами интеллектуальной поддержки принятия решений. Отталкиваясь от графовой модели сети, узлами которой являются сетевые устройства (с программными агентами управления), а дугами – логические каналы информационного взаимодействия между оборудованием ВС, выстраивается технология безадресного зондирования, обеспечивающая полноту контроля состояния всего оборудования сети. Для классификации состояния ВС предложен способ вычисления значений функции надежности. Выработка сигнала несоответствия инициирует выполнение цикла управления, в результате которого осуществляется корректировка состояния сетевого оборудования. К существующему инструментарию сетевого управления предлагается добавить экспертную систему, состоящую из базы знаний, механизма вывода и средств описания и заполнения базы знаний

Ключевые слова: ВЫЧИСЛИТЕЛЬНАЯ СЕТЬ, БЕЗАДРЕСНОЕ ЗОНДИРОВАНИЕ, ФУНКЦИЯ НАДЁЖНОСТИ, ЭКСПЕРТНАЯ СИСТЕМА, НЕЧЁТКАЯ ЛОГИКА, АГЕНТЫ ИНФОРМАЦИИ

UDC 002:34+004.056.5

Technical sciences

MODEL OF INFORMATION SECURITY FOR CONTROL PROCESSES OF COMPUTER NETWORKS

Kucher Victor Alekseevich
Cand.Tech.Sci.

Atroshchenko Valeriy Aleksandrovich
Dr.Sci.Tech.

Vidovskiy Leonid Adolfovich
Dr.Sci.Tech.

Trofimov Viktor Maratovich
Dr.Sci.Tech.
Kuban State Technological University, Krasnodar, Russia

In order to improve the security of information transfer we have offered one of the possible approaches to modeling process control computer networks with elements of intelligent decision support. We proceed from the graph model of network nodes which are network devices with software control agents, and arcs are logical channels of information exchange between the equipment computer systems. We built an addressless sensing technology which ensures the completeness of monitoring of all network equipment. To classify the computer networks state we provided a method for calculating the values of reliability. Development of signal mismatch triggers the control cycle as a result of which the adjustment of the state of network equipment. For existing tools we proposed adding network control expert system consists of a knowledge base, inference mechanism and means of description and fill in the knowledge base

Keywords: COMPUTER NETWORK, UNADDRESSED SENSING, RELIABILITY FUNCTION, EXPERT SYSTEMS, FUZZY LOGIC, INFORMATION AGENTS

1. Введение

Известно [1, 2], что любая сложная вычислительная сеть требует дополнительных специальных средств управления помимо тех, которые встроены в сетевые операционные системы. Это связано с большим

количеством сетевого оборудования, которое влияет на работоспособность сети в целом. Поддержка распределенной вычислительной сети (ВС) возможна только при использовании централизованной системы управления, которая в автоматическом режиме собирает статистику о работоспособности элементов сети и предоставляет эту информацию администратору ВС для принятия решений.

В настоящее время ни один проект ВС не обходится без моделирования будущей сети. Целью настоящей статьи является разработка одного из возможных подходов к моделированию процессов управления ВС с элементами интеллектуальной поддержки принятия решений.

Структура системы управления ВС (фрагмент сети показан на рисунке 1) может быть представлена в виде графовой модели, узлами которой являются сетевые устройства (с программными агентами управления), а дугами – логические каналы информационного взаимодействия между оборудованием ВС [1-4].

Рассматриваемая как объект контроля система, представляет собой совокупность n составляющих ее элементов, соединенных между собой функциональными связями. Каждое сетевое устройство может находиться в двух устойчивых состояниях: исправном и отказа. Вероятность исправного состояния обозначим p_i, а вероятность отказа – q_i ($q_i = 1 - p_i$). Будем считать, что отказы отдельных устройств между собой независимы.

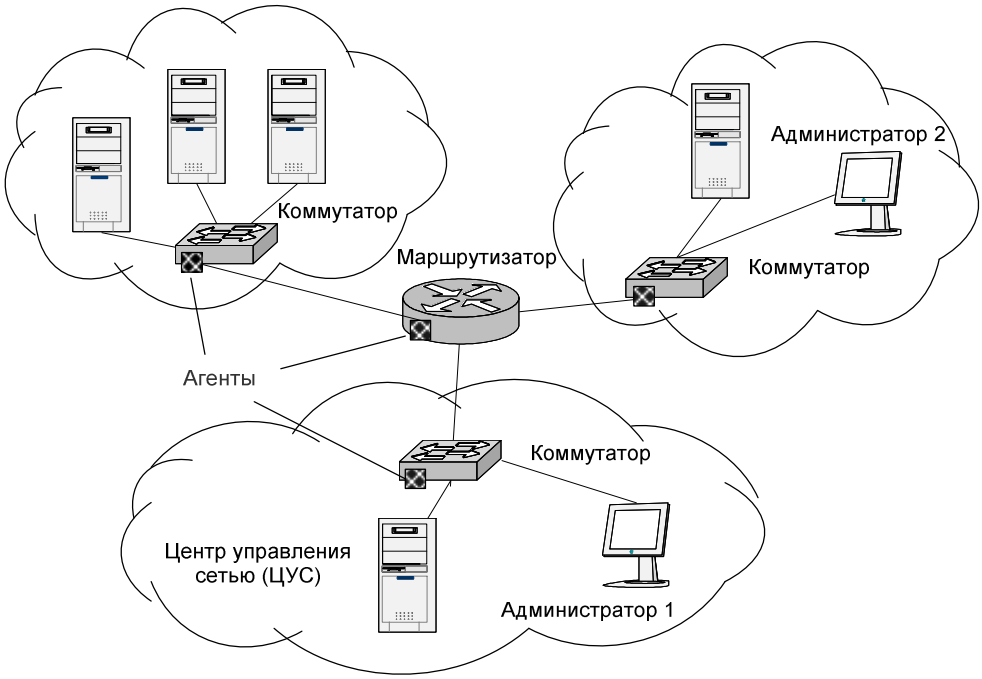

Рисунок 1 – Фрагмент ВС с устройствами управления

Контроль состояния вычислительной сети заключается в последовательном применении специальных тестов, каждый из которых проверяет отдельные функции сетевых устройств.

Процессы управления оборудованием сети могут быть представлены в виде замкнутого технологического цикла, состоящего из отдельных связанных по целям и результатам фаз (рисунок 2) [5]. Первые четыре фазы определяют цикл контроля, а остальные – цикл управления.

Цикл контроля объединяет фазы формирования первичной информации о состоянии сетевого устройства, передачи этой информации в центр управления сетью (ЦУС), обобщения и обработки информации о состоянии устройства и принятия соответствующего решения в условиях неполноты и неопределенности данных.

Контроль состояния сети преследует следующие цели:

- проверить работоспособность всего оборудования сети;

- отыскать неисправное сетевое оборудование.

В первом случае достаточно применить тест, проверяющий всю сеть (назовем его «глобальный зондовый тест»). Во втором случае процедура контроля включает множество тестов. Исход теста T_i назовем успешным, если в проверяемом в нем подмножестве сетевых устройств G_i не обнаружено неисправных компонентов (агентов), обеспечивающих формирование сообщений с заранее определенной структурой и их выдачу в адрес ЦУС.

Задача заключается в построении такой процедуры (выборе совокупности и очередности тестов $\{T\}$) контроля системы $P_в(\Delta R, \Delta t, \{T\})$, чтобы выполнялись следующие условия:

$$P_в(\Delta R, \Delta t, \{T\}) \geq \overline{P_в};$$
$$C_K \rightarrow \min_{\forall K},$$

где $P_в(\Delta R, \Delta t, \{T\})$ – вероятность того, что существенные отклонения показателей надёжности ΔR не останутся не выявленными при использовании совокупности тестов $\{T\}$ в течение заданного интервала времени Δt; $\overline{P_в}$ – предельное значение вероятности; C_K – расходы на организацию контроля.

Рассмотрим технологию зондового контроля [5]. Сущность контроля состояния сетевого оборудования с использованием глобального зондового теста заключается в образовании замкнутых маршрутов, покрывающих все вершины графа и обязательно проходящих через вершину, являющуюся генератором зондов. Под зондовым тестом понимается короткое сообщение, передающееся по сети через определенные интервалы времени по замкнутому маршруту, который заканчивается в узле генераторе тестов.

Реализация безадресного зондирования обеспечивает полноту контроля состояния всего оборудования сети. Такая технология контроля позволяет узлам, через которые проходят тест-зонды, отслеживать

состояние той части сети, информация о которой записана в проходящих зондах.

Наиболее сложной фазой цикла контроля является фаза идентификации состояния оборудования ВС. Результатом идентификации является определение необходимости корректировки процессов функционирования оборудования на основе данных о текущих значениях показателей функционирования сети. Необходимость корректировки определяется выработкой сигнала несоответствия. Таким образом, ЦУС и агенты оборудования ВС работают постоянно, а информация состояния передается через кванты времени или при изменении состояния до пределов допустимого. Основным моментом в цикле контроля является анализ поведения критерия функционирования сети, назовем его функцией надежности $R = F(K)$, где K - вектор показателей надежности оборудования сети. Состояние сети $s \in S$ классифицируется по областям значений, которые принимает функция R. Для классификации состояния ВС необходимо уметь вычислять значение функции надежности R.

Пусть работоспособность сети характеризуется значениями показателей $K_1, K_2, ..., K_n$. Тогда сигнал $q(R)$, характеризующий несоответствие состояния сети требуемому, определяется следующими условиями:

1) $q(R) = 0$, если значения $K_1(t), K_2(t), ..., K_n(t)$ в моменты $t = 1,2,...$ контроля состояния сети соответствуют заданным требованиям;

2) $q(R) = 1$ - в противном случае.

Функцию надежности R необходимо искать в виде [4]

$R = F(\{K_i\}, \{K_{iH}\}), i \in \overline{1,n}$,

где K_{iH} - множество показателей работоспособности сети, заданных нормативными требованиями;

K_i - параметр состояния i-го сетевого устройства.

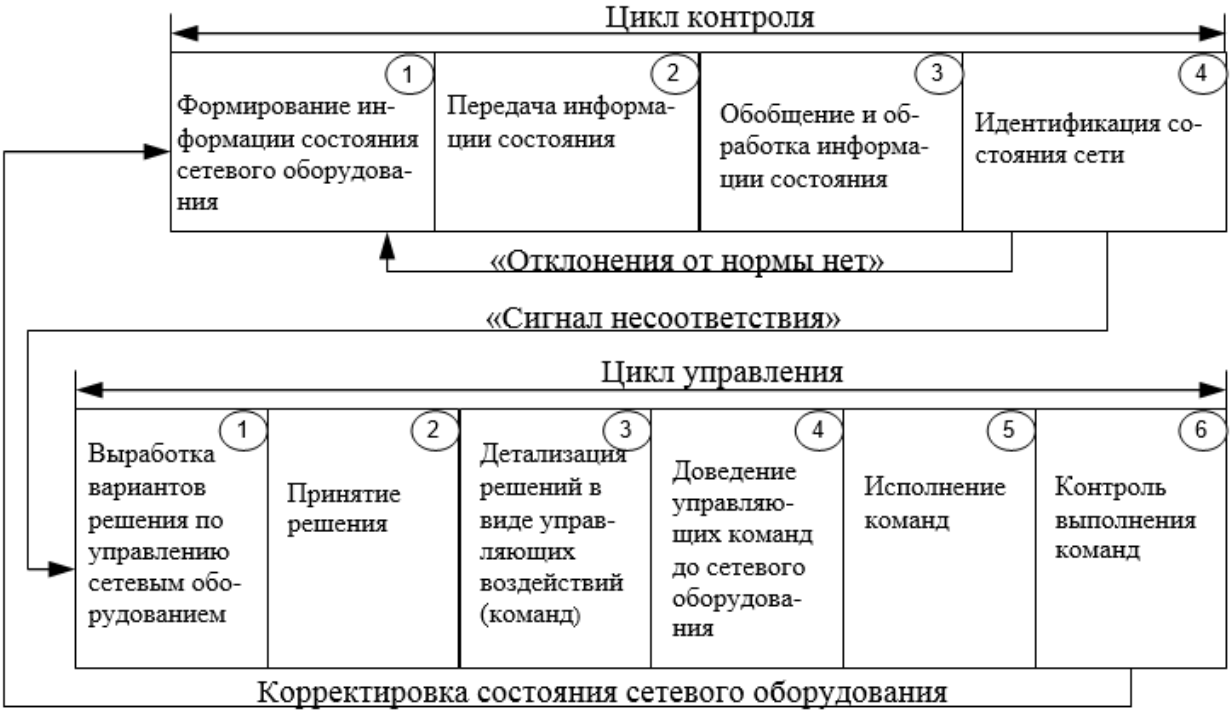

Рисунок 2 – Процессы управления оборудованием ВС

Сформулируем предпосылки и допущения, принимаемые при определении значений сигнала несоответствия $q(R)$ [5]:

1. Примем, что требуемое значение параметров состояния оборудования ВС задаются интервально $K_{i_1} \le K_{i_{доп}} \le K_{i_2}$, $i \in \overline{1,n}$. При попадании значения параметра K_i в диапазон $\lfloor K_{i_1}, K_{i_2} \rfloor$ требования по обеспечению надежности функционирования ВС выполняются полностью и $R = 1$. Диапазон $\lfloor K_{i_1}, K_{i_2} \rfloor$, $i \in \overline{1,n}$ будем называть требуемым.

2. Наряду с требуемым рассматривается также диапазон $\lfloor (1-\Delta_{i_1})K_{i_1}, (1-\Delta_{i_2})K_{i_2} \rfloor$. При нахождении параметра состояния K_i в допустимом диапазоне считается, что уровень надежности снизился, но не на столько, чтобы вырабатывался сигнал тревоги и $q(R) = 0$. Значение $q(R) = 1$ вырабатывается только при выходе K_i за пределы допустимого диапазона. С помощью величины Δ_{i_1} и Δ_{i_2} можно регулировать скорость

реакции ЦУС на изменения в обстановке. Чем точнее сведения о поведении параметров состояния, тем меньше должны быть величины Δ_{i_1} и Δ_{i_2}. Выбор величин Δ_{i_1} и Δ_{i_2} осуществляется администратором ЦУС.

Схема формирования сигнала несоответствия представлена на рисунке 3. Выделяются три нечеткие зоны: «норма», «критическое состояние», «отказ». Сигнал $q(R)$ формируется из двух составляющих, характеризующих попадание K_i в требуемый (q_0) и допустимый (q_1) диапазоны. Значение сигнала несоответствия q формируется по следующему правилу: $q = q_0 \cdot q_1$.

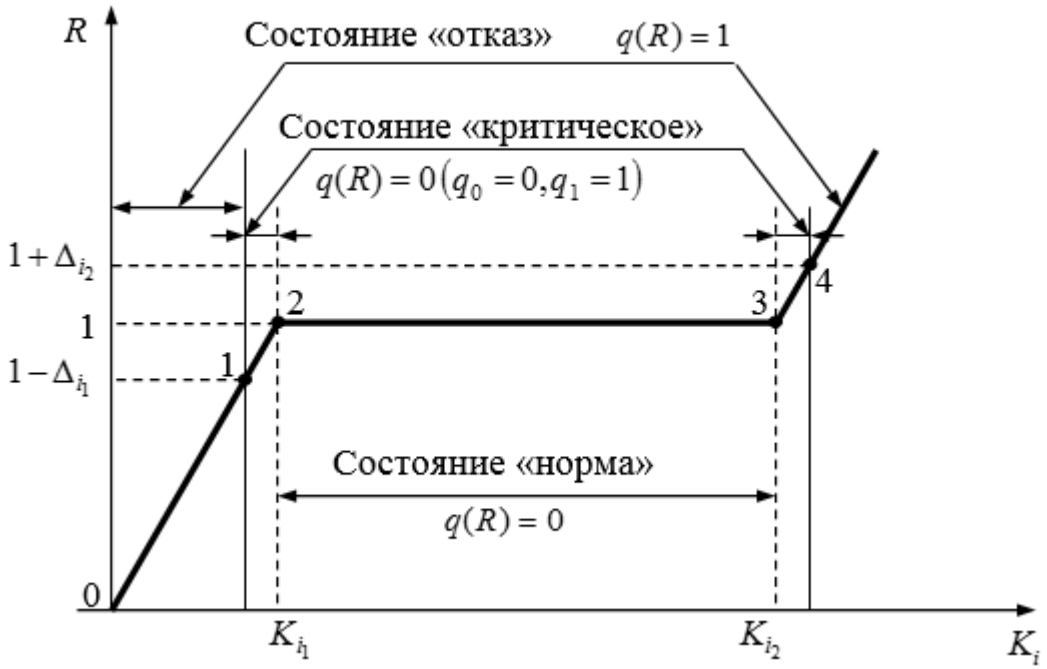

Рисунок 3 – Схема формирования сигнала несоответствия

Выработка сигнала несоответствия инициирует выполнение цикла управления, в результате которого осуществляется корректировка состояния сетевого оборудования.

На рисунке 4 представлена структура центра управления сетью. На каждом сетевом устройстве размещается агент – программное обеспечение, которое позволяет управлять соответствующим телекоммуникационным

оборудованием. Агенты предназначены для сбора информации о состоянии оборудования ВС и передачи управляющих команд на него [1,3]. Компонент предварительной обработки данных предназначен для сбора и обработки информации от агентов. Это нужно для приведения полученных данных к унифицированному виду, понятному для обработки в ЦУС.

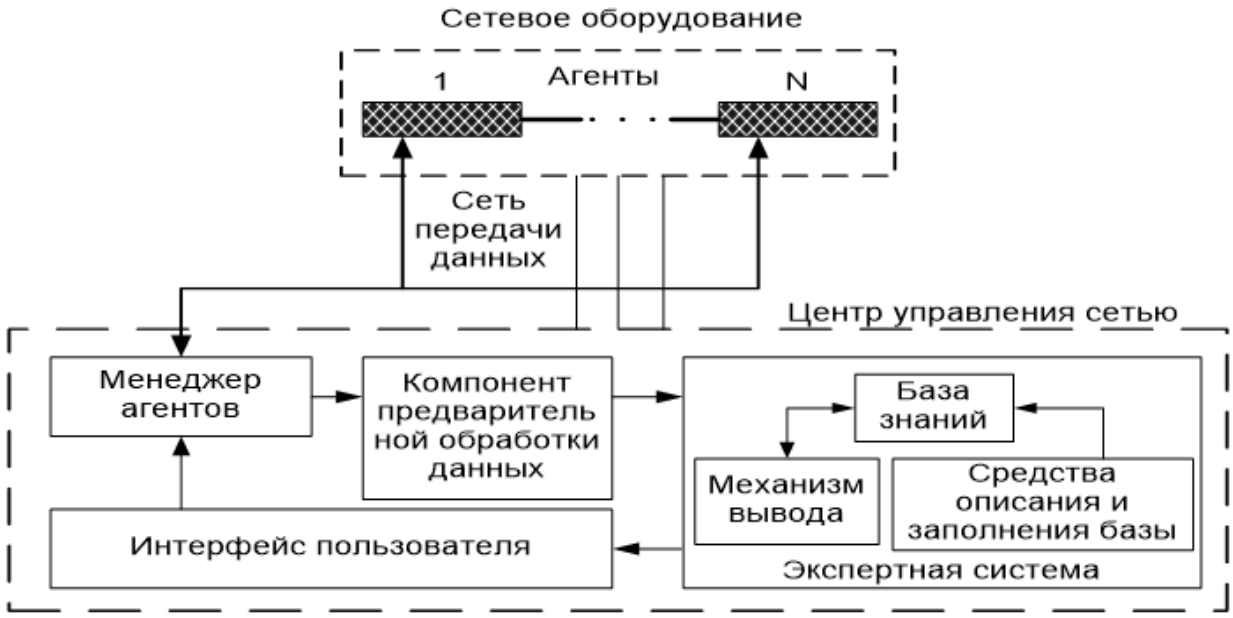

Рисунок 4 – Структура центра управления сетью

Существующий инструментарий сетевого управления намного выигрывает, если к нему добавить экспертную систему (ЭС). ЭС состоит из базы знаний, механизма вывода и средств описания и заполнения базы знаний. ЭС анализирует статистику и осуществляет выдачу соответствующих рекомендаций администратору (менеджеру агентов) ВС по управлению конфигурацией оборудования, о неисправностях, сбоях и других причинах аномальной работы сети, о возможных последствиях для принятия управленческих решений.

Заключение

Разработана модель управления вычислительными сетями, в которой ЦУС и агенты оборудования ВС работают постоянно, а

информация состояния передается через кванты времени или при изменении состояния до пределов допустимого. Основным моментом в цикле контроля является анализ поведения критерия функционирования сети, или функции надежности, определённым образом заданной. Состояние сети классифицируется по областям значений, которые принимает эта функция. Добавление экспертной системы существенно улучшит качество анализа процессов в вычислительной сети.

Литература

1. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы. СПб., 2002, с. 583-630.
2. Информационная безопасность. Обзор рисков. Телеком - *LETA Group*, 2012 - *http://www.leta.ru/netcat_files/File/riski_telecom.pdf*
3. *Гук М.* Аппаратные средства локальных сетей. Энциклопедия. СПб., 2002, с. 457-469.
4. Брайдо В.Л. Вычислительные системы, сети и телекоммуникации. СПб., 2002, с. 625-644.
5. Ухлинов Л.М. Управление безопасностью информации в автоматизированных системах. М., 1996, с. 29-39.

References

1. Olifer V.G., Olifer N.A. Komp'juternye seti. Principy, tehnologii, protokoly. SPb., 2002, s. 583-630.
2. Informacionnaja bezopasnost'. Obzor riskov. Telekom - LETA Group, 2012 - http://www.leta.ru/netcat_files/File/riski_telecom.pdf
3. Guk M. Apparatnye sredstva lokal'nyh setej. Jenciklopedija. SPb., 2002, s. 457-469.
4. Brajdo V.L. Vychislitel'nye sistemy, seti i telekommunikacii. SPb., 2002, s. 625-644.
5. Uhlinov L.M. Upravlenie bezopasnost'ju informacii v avtomatizirovannyh sistemah. M., 1996, s. 29-39.