Д. т. н. А. В. СКАТКОВ, Д. Ю. ВОРОНИН, Д. Н. ДАНИЛЬЧУК

Украина, Севастопольский национальный технический университет
E-mail: dima@voronins.com

Дата поступления в редакцию
31.10 2007 г.

Оппонент *д. т. н. С. А. НЕСТЕРЕНКО*
(ОНПУ, г. Одесса)

СИСТЕМА ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЙ ПО ВЫБОРУ СТРУКТУРЫ СИСТЕМЫ МОНИТОРИНГА

Рассмотрен структурный синтез систем мониторинга. Описана система поддержки принятия решений по выбору структуры системы мониторинга и дисциплины опроса узлов фрагмента компьютерной сети.

Использование мониторинга оправдано в любой отрасли промышленности или сфере услуг. Системы мониторинга позволяют контролировать любой производственный процесс (например, выпечки хлеба или изготовления телевизоров). Огромное значение мониторинг имеет в областях, связанных с передачей данных в компьютерных системах или сетях.

Система мониторинга компьютерной сети (**КС**) представляет собой программно-аппаратный комплекс, решающий широкий класс задач, направленных на обеспечение работоспособности сети. Основные из них:

— подготовка данных для принятия решений по организации работы сети;
— обеспечение информационной безопасности;
— использование в объектах критического применения;
— обеспечение гарантоспособности сети.

Наиболее известной является задача наблюдения за состоянием компьютерной сети. Она связана со сбором информации и подготовкой данных [1], которые в дальнейшем могут быть использованы для принятия решения об оптимизации работы КС. Если рассмотреть сетевые записи работы сегмента КС, то основное, что выделяется на общем фоне, — это огромный объем передаваемых данных. Эти данные могут передаваться внутри сегмента и за его пределы. В состав этих данных входит как системный трафик (данные, передаваемые для обеспечения корректной работы КС), так и пользовательский (данные, передаваемые непосредственно пользователями). Использование мониторинга позволяет определить характеристики различных видов трафика, оценить нагрузку на различные участки сегмента КС, а также на всю КС в целом.

Используя собранные системой мониторинга данные, можно разработать план действий по повышению эффективности работы КС в случае ее расширения. (Расширение КС подразумевает добавление к сети новых серверов, рабочих станций или сетевых служб.) Однако до реализации расширения КС необходимо определить, каким образом подключить к сети новый элемент, какие связи и маршрутизаторы задействовать, и каким образом повлияет на работу КС добавление нового элемента. С использованием информации, полученной от системы мониторинга, можно принять решение о наиболее эффективной точке и способах подключения нового элемента к сети, а в некоторых случаях — и о реконфигурации существующей КС.

Использование данных мониторинга может помочь более эффективно производить поиск неисправностей в КС. Обнаружение неработающего сетевого оборудования (сетевых плат или маршрутизаторов) не представляет особых проблем. Вместе с тем, сетевое оборудование может работать нестабильно, т. е. время от времени передаются и получаются лишь некоторые данные через КС. Тогда происходит заполнение сети некорректной информацией, что приводит к замедлению работы всей КС. В таких случаях выявить нестабильно работающее сетевое оборудование значительно сложнее. Использование же мониторинга позволяет отследить такую ситуацию по некоторым косвенным признакам, таким как обращение к несуществующим ресурсам или организация ненужного трафика.

Следующая задача системы мониторинга заключается в обеспечении информационной безопасности КС [1]. Мониторинг может быть очень полезен для борьбы с хакерами, а точнее, позволяет обнаружить атаки хакера на сеть. Хотя проникновение хакера в КС может остаться незамеченным, он не может скрыть следов своей деятельности внутри сети. Использование мониторинга позволяет отследить потоки трафика и обнаружить незаконный DHCP-сервер либо имитацию IP-адреса. Имитация IP-адреса может возникнуть не только вследствие атаки хакера, но и в случае нестабильной работы сетевого оборудования.

Несомненно, важной задачей является использование систем мониторинга для наблюдения за объектами критического применения [2]. Использование компьютерных технологий в областях, связанных с повышенными требованиями к надежности и управлению объектами критического применения, напри-

мер в ядерной энергетике, обязывает производить непрерывный контроль не только самого объекта, но и управляющей им системы. Использование мониторинга позволяет своевременно и с достаточной степенью достоверности получать информацию о состоянии объекта, позволяет вовремя отследить аварийные либо предаварийные ситуации и принять меры по их предотвращению.

Наконец, можно сказать о такой задаче как обеспечение гарантоспособности КС [3]. Сама концепция гарантоспособности подразумевает способность КС предоставлять некоторые услуги, которым можно оправданно доверять. Гарантоспособность является комплексным свойством, включающим безотказность, готовность, целостность, конфиденциальность, достоверность. Гарантоспособность имеет некоторые общие свойства с информационной безопасностью, также можно провести аналогию с управлением объектами критического применения, однако отсутствие обеспечения гарантоспособности ведет лишь к материальным потерям и не несет угрозы человеческой жизни или окружающей среде.

Постановка задачи

Пусть задан некоторый фрагмент компьютерной сети. Фрагмент представляет собой совокупность узлов, объединенных между собой при помощи среды коммутации. Каждый узел компьютерной сети состоит из процессорного блока и буферного накопителя. Особенности структуры узлов позволяют подключать либо отключать дополнительные процессоры в процессорном блоке, а также изменять объем буферного накопителя.

Необходимо для данного фрагмента компьютерной сети разработать структуру системы мониторинга и исследовать эффективность ее функционирования.

Необходимо разработать и реализовать указанное средство проектирования структуры системы мониторинга с использованием адаптивных алгоритмов на этапе выбора дисциплины опроса узлов фрагмента КС. Провести исследования с целью выявления параметров, влияющих на эффективность функционирования системы мониторинга, и предложить способы повышения эффективности.

Входными данными являются описание фрагмента компьютерной сети и требования пользователя к системе мониторинга для заданного фрагмента КС.

Выходными данными является полностью сформированная структура системы мониторинга в соответствии с классификацией, представленной в [4]. Классификация основана на таких структурных признаках, как тип системы управления, структура процессорного блока, наличие буферного накопителя, логика функционирования системы мониторинга и других. Таким образом, шифр конкретной реализации системы мониторинга составляется из последовательности групп символов, разделенных между собой косой чертой. Каждая из групп символов соответствует определенному классификационному признаку. Например, для системы мониторинга с централизованной системой управления, производящей мониторинг нескольких узлов на нескольких процессорах, с использованием буферного накопителя и информационных фильтров, инициатором мониторинга является узел сети; производится многофазный мониторинг; система имеет раздельную память и производит наблюдение случайных величин по жестко заданной программе. Шифр системы мониторинга можно записать следующим образом: ccon / mn / mp / be / ni / fe / mph / dif / var / hl (структура представлена на **рис. 1**).

Неоспоримым преимуществом предложенной классификации является то, что она описывает кон-

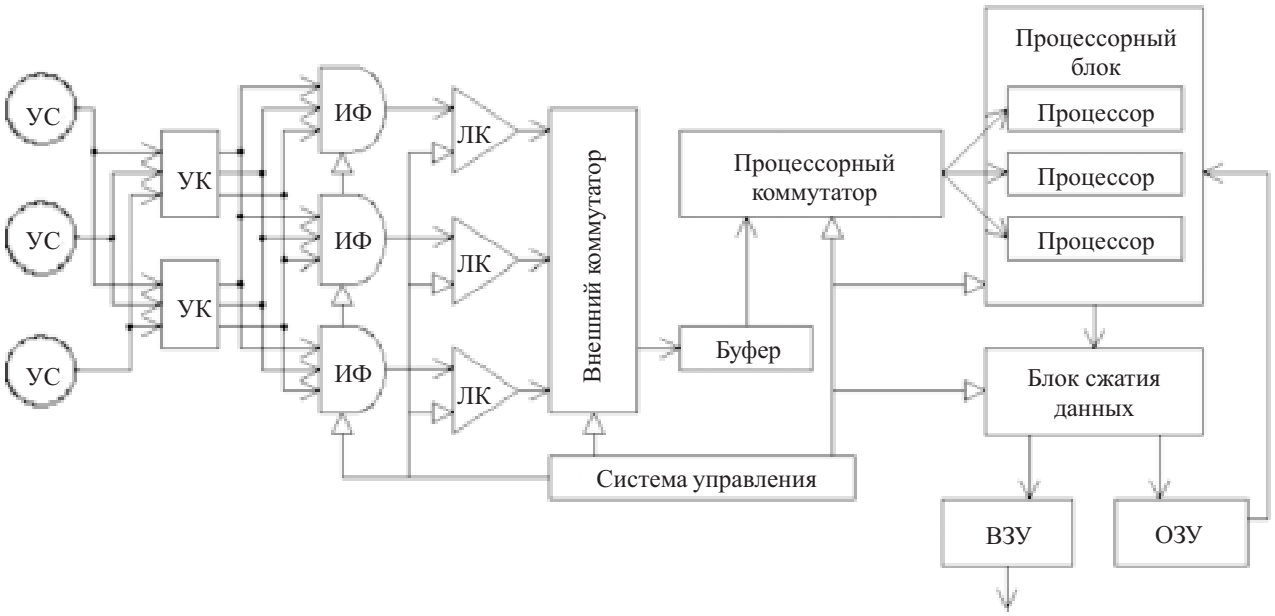

Рис. 1. Структурная схема системы мониторинга ccon / mn / mp / be / ni / fe / mph / dif / var / hl:
УС — узел компьютерной сети; УК — узловой коммутатор; ИФ — информационный фильтр; ЛК — логический ключ; ВЗУ/ОЗУ — внешнее/оперативное запоминающее устройство

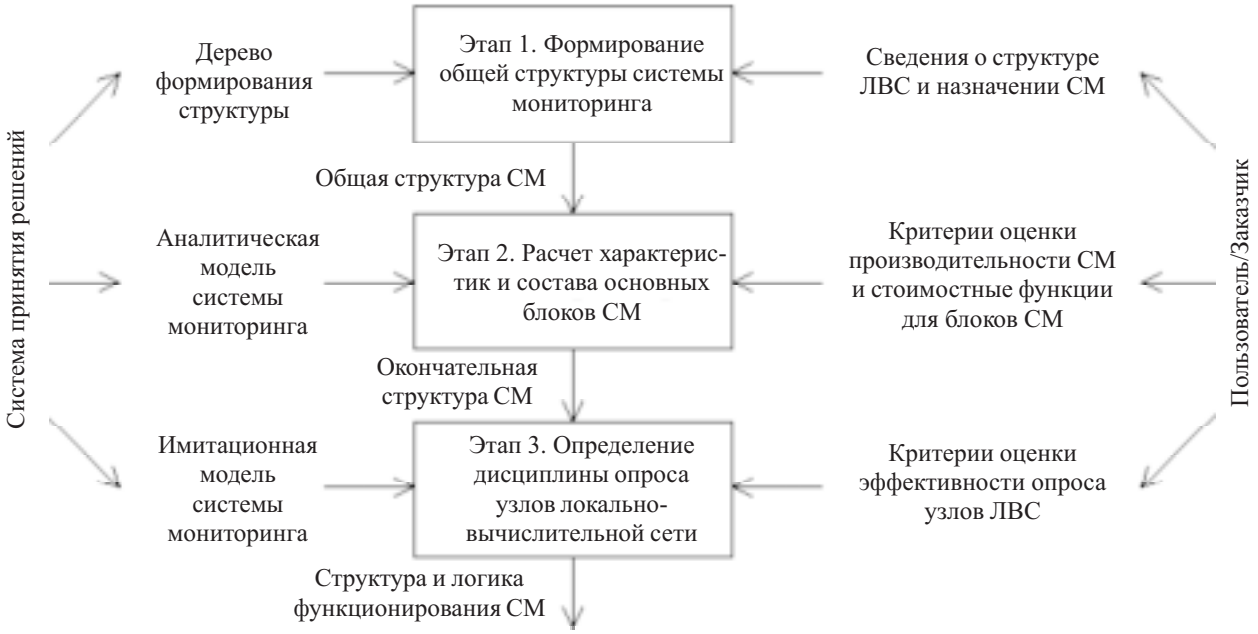

Рис. 2. Этапы формирования структуры системы мониторинга (ЛВС — локальная вычислительная сеть; СМ — система мониторинга)

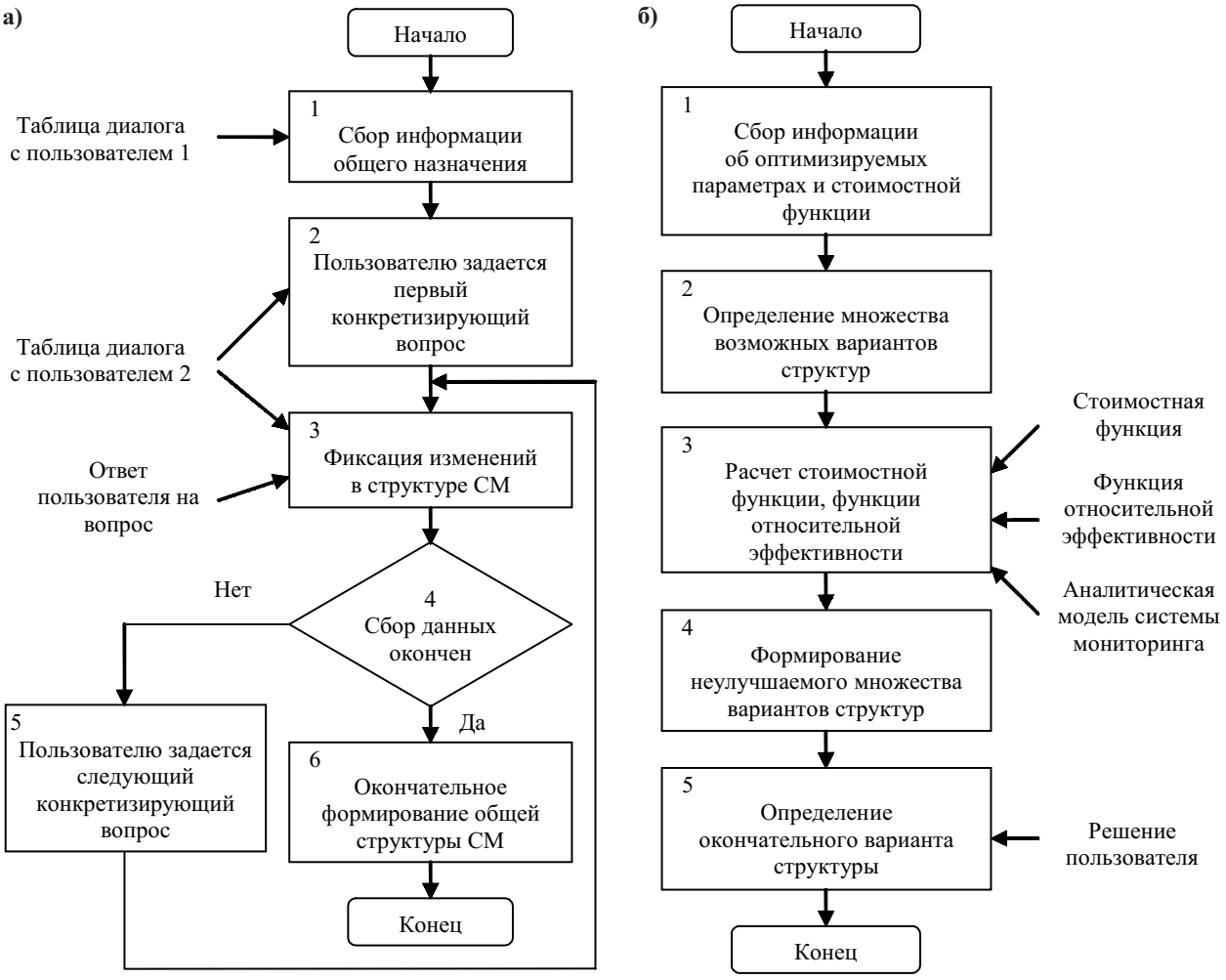

Рис. 3. Граф-схема этапа формирования общей структуры системы мониторинга:
***а* — этап 1; *б* — этап 2**

кретные различия в структуре системы мониторинга вместо использования абстрактных классов систем мониторинга.

Реализация системы поддержки принятия решений по выбору структуры системы мониторинга

Процесс формирования структуры системы мониторинга для некоторого фрагмента КС можно разделить на три этапа: формирование общей структуры мониторинга, расчет количественных характеристик функциональных блоков системы мониторинга и определение дисциплины опроса узлов фрагмента корпоративной вычислительной сети. На **рис. 2** изображены этапы формирования структуры системы мониторинга.

На первом этапе (см. **рис. 3**, *а*) формируется общий вид структуры системы мониторинга. Определяются цели и задачи, возложенные на систему, а также структурные блоки и их состав (например, буферный накопитель, информационные фильтры, запоминающие структуры). Общая структура системы мониторинга формируется в процессе диалога с пользователем.

На втором этапе (см. рис. 3, *б*) определяются параметры составных элементов системы мониторинга — такие как быстродействие и число процессоров в процессорном блоке, емкость буферного накопителя и т. д. Второй этап выполняется с использованием аналитической модели системы мониторинга. Критерии оценки и стоимостные функции задаются пользователем.

На третьем этапе для разработанной структуры системы мониторинга определяется используемая дисциплина опроса узлов сети. В разрабатываемой системе проектирования структуры системы мониторинга используется шесть возможных дисциплин опроса узлов ВС — три базовые дисциплины и три производные от них, носящие адаптивный характер. Производится имитационное моделирование работы системы мониторинга с использованием каждой из дисциплин опроса с последующим сопоставлением и, соответственно, выбором наиболее эффективной. Результатом проведения этого этапа является решение использовать конкретную дисциплину опроса в разрабатываемой системе мониторинга.

Заключение

Предложенная система поддержки принятия решений по выбору структуры системы мониторинга может активно использоваться при «пилотном» проектировании систем мониторинга. Система имеет интуитивно понятный интерфейс и обеспечивает удобную среду для проведения исследований, направленных на повышение эффективности функционирования системы мониторинга для фрагмента компьютерной сети.

Подготовленный пользователь (инженер-системотехник) при выборе параметров процессорного блока и буферного накопителя системы мониторинга может сократить вычислительные затраты как минимум в два раза.

В рамках проведенных исследований были изучены зависимости между задаваемыми пользователем требованиями и структурой системы мониторинга. По результатам проведенных исследований можно сделать следующие выводы.

1. Использование циклической дисциплины опроса на начальном этапе функционирования системы мониторинга позволяет сократить время настройки фрагмента КС как минимум на 50% по сравнению с другими рассмотренными дисциплинами опроса.

2. Использование адаптивных алгоритмов опроса узлов КС позволяет улучшить значение стоимостной функции примерно на 15% по сравнению с использованием базовых дисциплин обслуживания.

Предложенная система также может быть полезна при изучении студентами ряда дисциплин, связанных с компьютерными сетями.

ИСПОЛЬЗОВАННЫЕ ИСТОЧНИКИ

1. Уилсон Э. Мониторинг и анализ сетей. Методы выявления неисправностей. – М.: Лори, 2002.

2. Ястребенецкий М. А., Васильченко В. Н., Виноградская С. В. и др. Безопасность атомных станций: информационные и управляющие системы.— К.: Техніка, 2004.

3. Харченко В. С. Гарантоспособность и гарантоспособные системы: элементы методологии // Радиоэлектронные и компьютерные системы.— 2006.— № 5.— С. 7—19.

4. Скатков А. В., Воронин Д. Ю., Данильчук Д. Н. Структурный анализ систем мониторинга // Восточно-Европейский журнал передовых технологий.— 2007.— № 2.— С. 36—44.

НОВЫЕ КНИГИ

Яценков В. С. Микроконтроллеры Microchip® с аппаратной поддержкой USB.— М.: Горячая линия–Телеком, 2008.

В настоящее время использование шины USB является наиболее популярным методом для подключения периферийных устройств к компьютеру. Микроконтроллеры Microchip серии PIC18F2455/2550/4455/4550 включают в себя не только аппаратную поддержку шины USB, но и других популярных протоколов обмена данными, а также функциональные модули таймеров, АЦП, ЦАП и ШИМ, что позволяет создавать на основе этих микроконтроллеров самые разнообразные оконечные устройства, взаимодействующие с персональным компьютером. В книге приведено полное техническое описание микроконтроллеров Microchip PIC18F2455/2550/4455/4550, рассмотрены примеры практического применения.