

Ю.Л. Леохин, Р.С. Зубков

АРХИТЕКТУРЫ СИСТЕМ УПРАВЛЕНИЯ КОРПОРАТИВНЫМИ КОМПЬЮТЕРНЫМИ СЕТЯМИ С ФУНКЦИЕЙ ПРОГНОЗИРОВАНИЯ СОСТОЯНИЙ

В статье проводится анализ архитектур систем управления компьютерными сетями, предлагаются архитектуры систем управления со встроенной функцией прогноза состояний компьютерной сети, описывается состав модулей и алгоритмы функционирования.

Ключевые слова: система управления, компьютерная сеть, прогнозирование, архитектура, фазовые снимки, фазовая траектория

Y.L. Leokhin, R.S. Zubkov

ARCHITECTURE OF CONTROL SYSTEMS OF CORPORATE COMPUTER NETWORKS WITH FUNCTION OF FORECASTING OF CONDITIONS

In article the analysis of architecture of control systems is carried out by computer networks, architecture of control systems with the built-in function of a forecast of conditions of a computer network are offered, the structure of modules and algorithms of functioning is described.

Keywords: control system, computer network, forecasting, architecture, phase pictures, phase trajectory

Интеграция России в мировую экономику и вступление в ВТО заставляют предприятия и целые отрасли нашей страны повышать свою конкурентоспособность. Для этого необходимым условием является модернизация технической и технологической базы, внедрение новых, современных технологий и модернизация ИТ-инфраструктуры. Транспортную основу ИТ-инфраструктуры современного предприятия составляет корпоративная компьютерная сеть (ККС), служащая для обмена информацией между приложениями информационных систем. Качество услуг, предоставляемых ИТ-инфраструктурой, главным образом зависит от эффективности мониторинга и управления процессами передачи данных между приложениями информационной системы предприятия.

Современная корпоративная компьютерная сеть предприятия должна удовлетворять следующим требованиям: масштабируемость, территориальная распределенность и гетерогенность. В этих условиях для эффективного функционирования корпоративной компьютерной сети необходимо внедрение в ИТ-инфраструктуру предприятия интеллектуальной системы управления [7, 8]. Это позволит сбалансировать нагрузку на ИТ-инфраструктуру, поддерживать заданную скорость обмена информацией, предотвращать сбои. Кроме того, может не потребоваться проведение дорогостоящих мероприятий по модернизации корпоративной компьютерной сети предприятия и увеличения штата ИТ-специалистов.

Существуют пять базовых типов архитектур систем управления компьютерными сетями [9, 10, 11]:

1. Одноуровневая архитектура. Все сетевые узлы взаимодействуют друг с другом по единому управляющему протоколу, что позволяет им реализовывать взаимодействие напрямую с интегрирующим менеджером – «на одном языке». Такая архитектура позволяет реализовать только основные функции управления и не предоставляет возможности использования специфических функций управления, присущих различным устройствам. Реализация такой архитектуры в большой корпоративной сети не эффективна из-за большого количества разнородного сетевого оборудования и различных коммуникационных протоколов. Одноуровневая структура представлена на рис. 1.

2. Иерархическая архитектура. Такой тип архитектуры основан на иерархии менеджеров. Каждый сегмент корпоративной сети имеет управляющую станцию для мониторинга состояния сетевых устройств сегмента. С помощью элементарного сетевого менеджера, установленного на управляющей станции администратора, администратор управляет сетевыми устройствами. Эти управляющие станции взаимодействуют с корпоративными управляющими станциями, которые, в свою очередь, взаимодействуют с интегрирующей управляющей станцией. Таким образом, управляющая станция нижнего уровня иерархии может быть как агентом, так и менеджером. Иерархическая архитектура представлена на рис. 2.

3. Ячеистая архитектура. Это сложная архитектура управления корпоративной компьютерной сетью, в которой реализован иерархический подход. Данный тип архитектуры состоит из нескольких менеджеров верхнего уровня, взаимодействующих напрямую друг с дру-

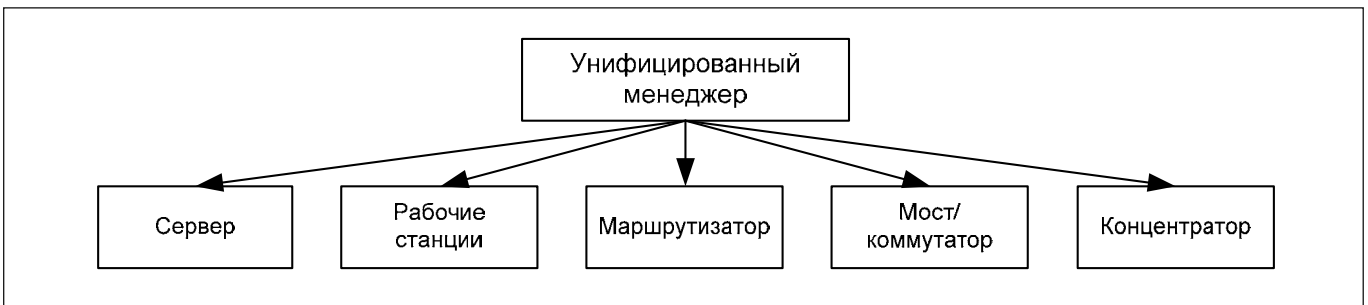


Рис. 1. Одноуровневая архитектура

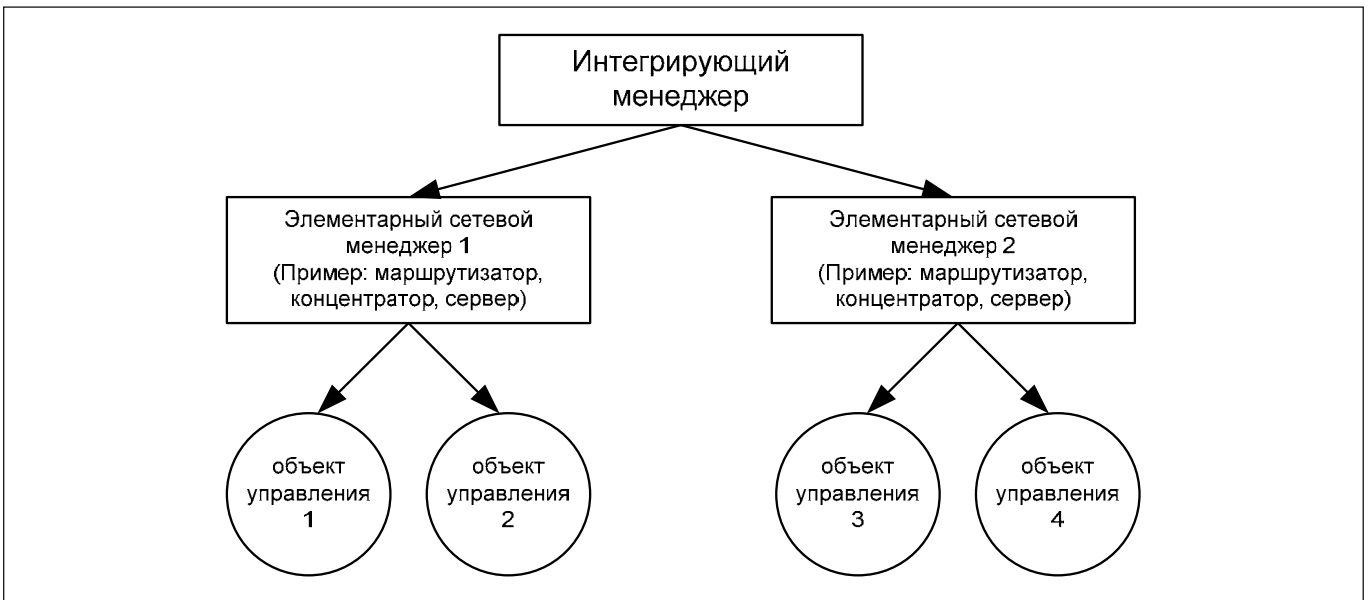


Рис. 2. Иерархическая архитектура

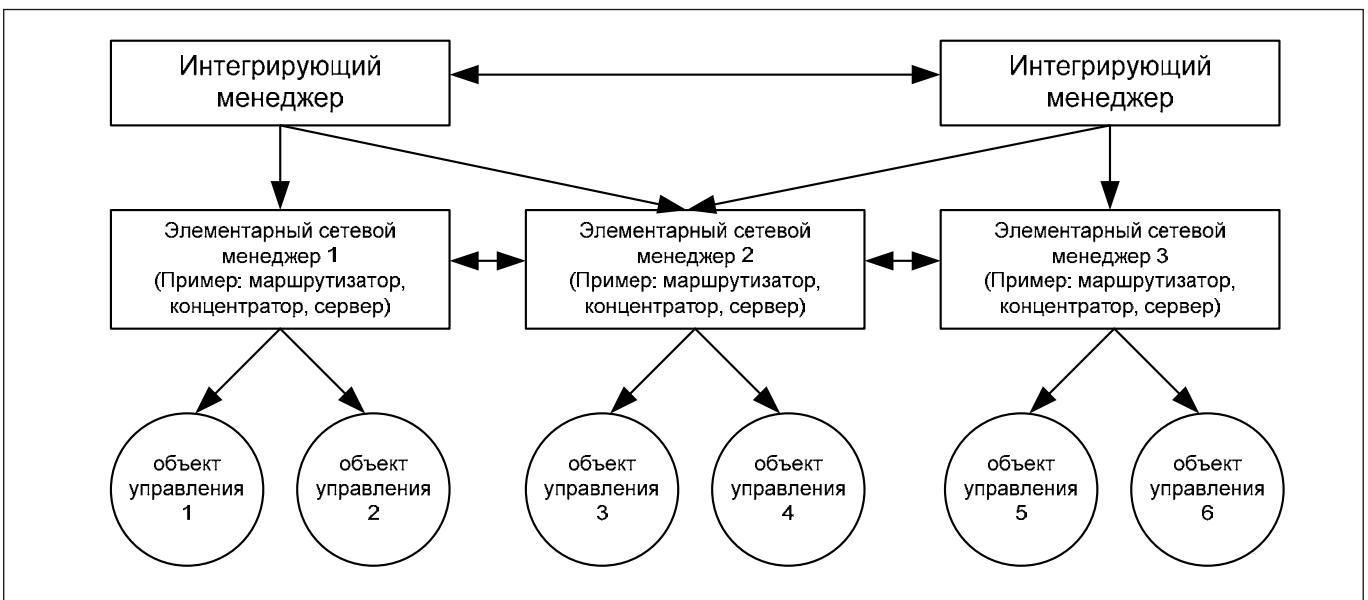


Рис. 3. Ячеистая архитектура

гом и с менеджерами нижнего уровня. Допускается взаимодействие между элементарными менеджерами. Ячеистая архитектура представлена на рис. 3.

4. Платформенная архитектура. Платформенная архитектура базируется на универсальном прикладном программном интерфейсе, определенном и

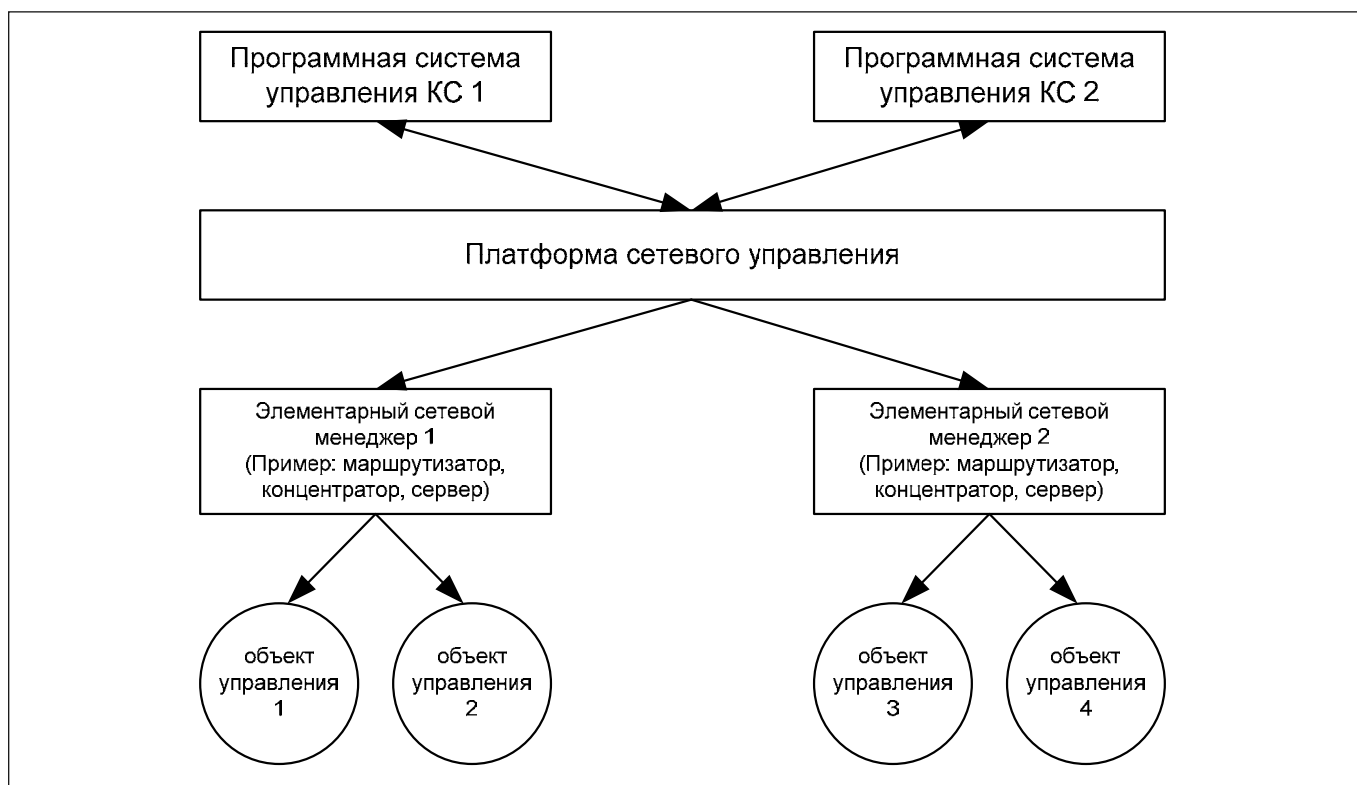


Рис. 4. Платформенная архитектура

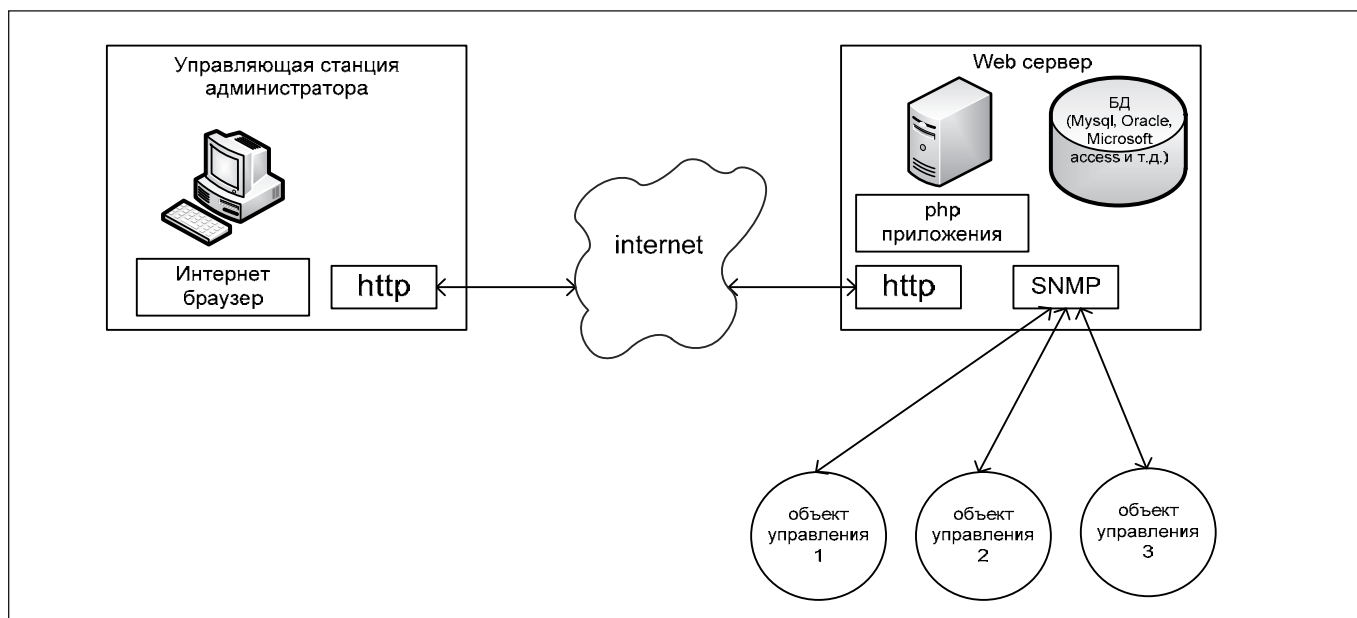


Рис. 5. Архитектура на основе Web-технологий

поддержанным различными производителями. Такая архитектура обеспечивает универсальность, а, следовательно, независимость от производителя и предоставляет набор базовых инструментальных средств для разработки управляющих сетевых приложений. Платформенная архитектура представлена на рис. 4.

5. Распределённая архитектура на основе Web-технологий. Для организации системы управления на основе Web-технологий используется протокол HTTP (HyperText Transfer Protocol – протокол передачи гипертекста). Доступ удаленного пользователя к управляющему приложению осуществляется при помощи веб-браузера и средств аутентификации, что позволяет

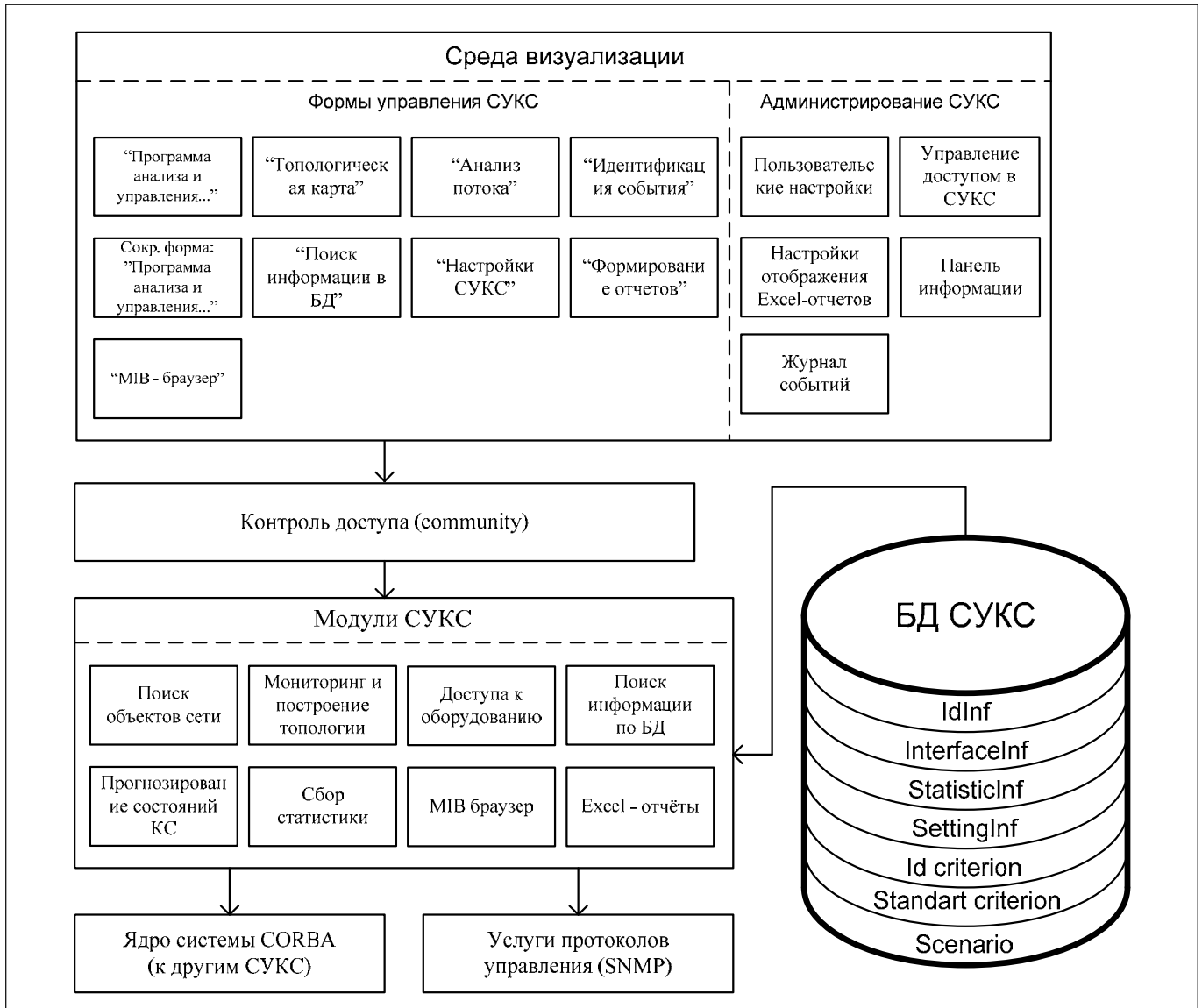


Рис. 6. Обобщенная архитектура SIREN

заменить специальное клиентское ПО, которое обычно используется для управления корпоративными сетями, стандартным клиентским ПО. Управляющее приложение может быть создано при помощи скриптового языка программирования общего назначения php (Hypertext Preprocessor – интерпретатор компилирующего типа) и взаимодействовать с СУБД. Архитектура системы управления представлена на рис. 5.

В настоящее время создано немало программных продуктов для мониторинга и управления компьютерной сети. Результаты проведенного анализа известных систем управления компьютерными сетями (СУКС) [1] позволили обосновать необходимость разработки средств прогнозирования критических событий [2].

Для решения этой задачи предлагается внедрить в СУКС подсистему прогнозирования состояний КС. Это позволит заблаговременно предпринять меры по пред-

отвращению нежелательных событий или минимизировать их влияние на процесс передачи данных.

Предлагаемая архитектура системы управления SIREN (System Independent Regulation of Equipment Network – система автономного управления оборудованием сети) является иерархической распределенной [3]. Обобщенная архитектура разработанной SIREN представлена на рис.6.

В состав системы SIREN входят семь модулей, МIB-браузер, среда визуализации и база данных. Опишем функции основных модулей системы управления.

Модуль доступа к оборудованию

Модуль доступа к оборудованию осуществляет сетевой (низкоуровневый) доступ к объектам сети с целью получить информацию о состоянии объекта. К модулю доступа предъявляются следующие требования:

1. Модуль должен обеспечить доступ к разнообразной информации опрашиваемого объекта.
2. Опрашиваемый объект не должен требовать сложной настройки и установки уникального программного обеспечения.
3. Передача данных должна осуществляться стандартным образом.

В качестве управляющего протокола выбран протокол SNMP как наиболее распространенный и используемый на данный момент.

В основу реализации модуля доступа положена модель администрирования для протокола IP. Простота и мобильность этой модели сделали ее популярной даже вне среды Internet. Она стала наиболее широко применяемой моделью сетевого администрирования. Основными компонентами этой модели являются: SMI (Structure of Management Information – структура управления информацией), MIB и SNMP.

Для получения необходимой информации от сетевого устройства формируется запрос к SNMP-агенту. Модулю доступа передаются необходимые для стандартного SNMP-запроса параметры:

1. IP-адрес (или имя) опрашиваемого объекта. Объект должен поддерживать SNMP.
2. Адрес поддерева базы данных MIB (Object Identifier). В соответствии с требованиями протокола SNMP определяет ветвь информационной управляющей базы MIB. OID может быть представлен в символьном виде с разделителем (точкой): .iso.org.dod.internet.mgmt.mib-2.system.sysName или в числовом с разделителем точкой (используется в проекте): .1.3.6.1.2.1.1.5
3. Пароль доступа к устройству (community) – имя “сообщества”, которому разрешен доступ к данным на опрашиваемом объекте.

Модуль поиска сетевых устройств

Модуль поиска сетевых устройств предназначен для автоматического поиска активных IP-адресов объектов сети. Для определения типа сетевого устройства достаточно прочитать информацию из таблицы MIB. Необходимым условием наличия информации является сетевая активность данного объекта, в противном случае ответ на запрос будет пуст. Процесс определяет потенциально возможные активные IP-адреса и диапазоны сканирования IP-адресов, ориентируясь на таблицы маршрутизации сетевых устройств (.1.3.6.1.2.1.4.21 – ipRouteTable), а также ветвь .1.3.6.1.2.1.2 (информация об интерфейсах) базы данных MIB. Затем выполняются попытки установления сеансов связи. Если СУКС не удастся идентифицировать хотя бы одно сетевое устройство с активной БД, пользователю предлагается ввести IP-адрес одного из центральных устройств самостоятельно.

Модуль сбора статистики

Модуль сбора статистики формирует всю необходимую информацию для занесения в базу данных SI-REN и дальнейшего анализа. Модуль сбора статистики выполняет следующие функции:

1. Формирования данных для SNMP-запроса, включая подготовку и передачу соответствующих данных для SNMP-запроса модулю доступа к оборудованию.
2. Перевод данных в пользовательский формат, включая данные о системном времени, типе портов устройства и т.д.
3. Заполнение БД данными, полученными от сетевых устройств.

Полученные от сетевого устройства данные о типе портов в целочисленном формате преобразуются в логические имена интерфейса. Например: цифре 6 соответствует тип порта Ethernet.

Модуль поиска информации по базе данных

БД системы состоит из 7 таблиц идентификационной, статистической информации и критериев снимков. Для соответствия идентификационной и статистической информации записи маркируются. Данный модуль служит для сортировки информации в базе данных по ключу. Для определения, какой записи соответствует тот или иной идентификатор, можно самостоятельно просмотреть содержимое БД. Также с помощью данного модуля администратор может оперативно найти всю необходимую информацию о сетевом устройстве, заполнив соответствующую форму поиска.

Модуль Excel-отчетов

Модуль Excel-отчетов служит для вывода в удобную для анализа и обработки инструментальную среду необходимой информации. Модуль выполняет следующие функции:

- инициализацию Excel приложения;
- вывод информации и комментариев;
- формирование и вывод графической информации;
- расчет масштаба и значений осей графика;
- расчет параметров осей.

Модуль мониторинга сети

Модуль мониторинга сети выполняет построение топологической карты сети и сообщает администратору сети о перегрузке или отказах сетевого оборудования. К подобным средствам можно отнести следующие приложения: Nagios, Zabbix, Monit, Cacti и другие. Перечисленные системы мониторинга способны отправлять информационные сообщения администратору сети на электронную почту, пейджер или мобильный

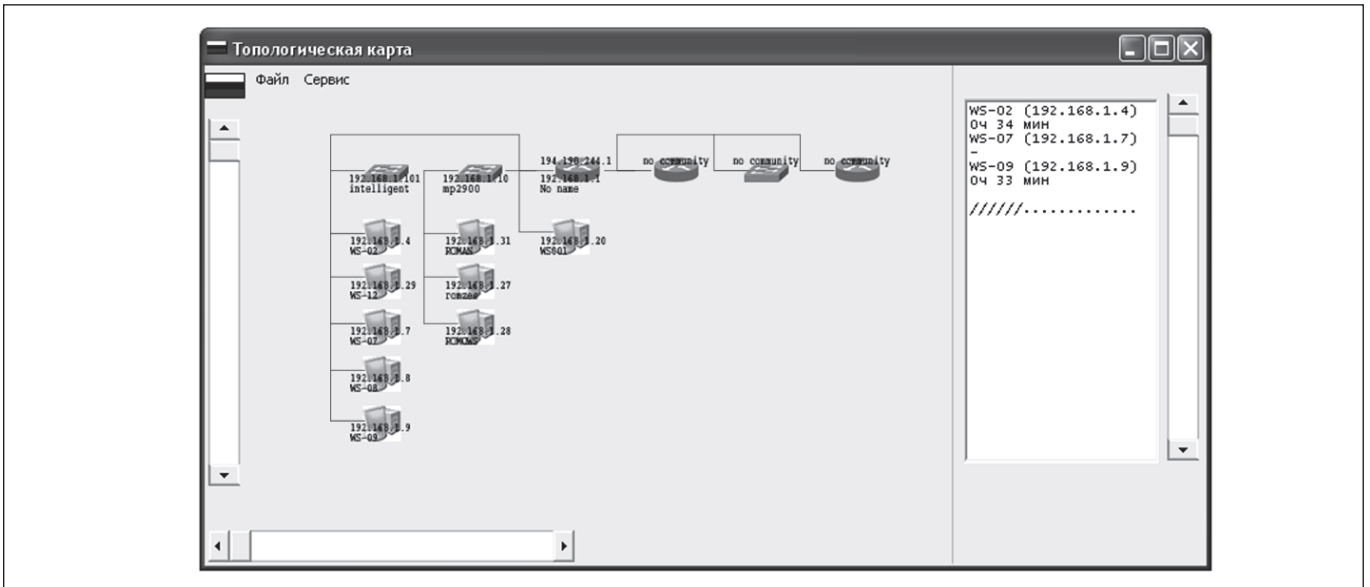


Рис. 7. Пример построенной топологии КС

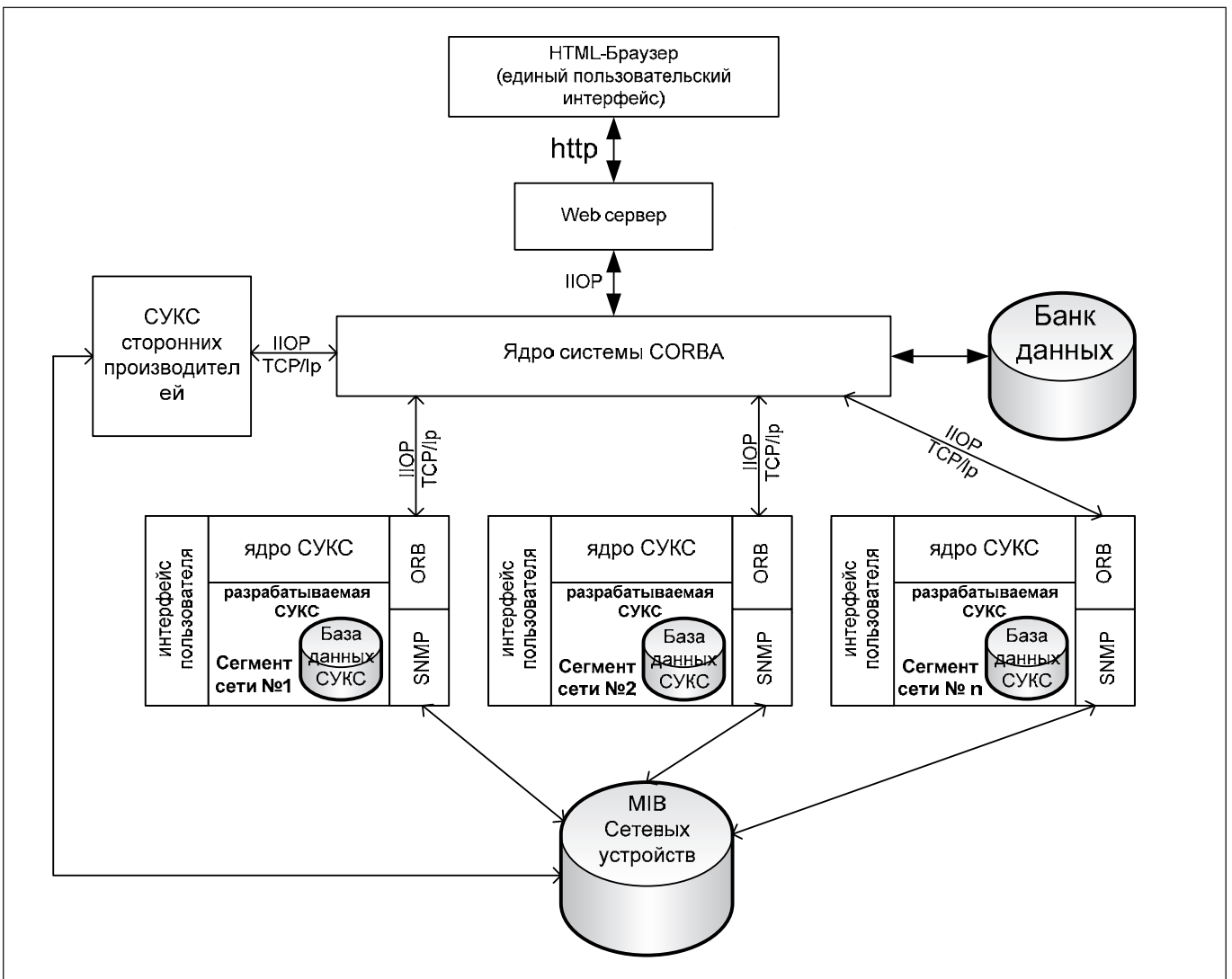


Рис. 8. Архитектура единой системы управления SIREN с использованием технологии CORBA

телефон. В предлагаемой системе управления передача сообщений администратору происходит по электронной почте с помощью почтового приложения MS Outlook.

Алгоритм работы модуля (рис. 7) можно разделить на три этапа:

1. Построение топологии КС осуществляется по алгоритму с помощью сетевой утилиты ring и базы управляющей информации MIB. Для быстрой диагностики порта в MIB используются объекты IfPhysAddress, IfAdminStatus и IfOperStatus. Принцип размещения модулем обозначений на топологической карте КС прост и интуитивно понятен. По горизонтали располагаются передающие сетевые устройства (коммутаторы, маршрутизаторы и т.д.), по вертикали – рабочие станции, подключенные к данному сетевому устройству. Красным цветом отмечены связи неактивных устройств.

2. Наблюдение за компьютерной сетью реализовано при помощи функции SNMP trap и процедуры планового опроса сетевых устройств. Для уменьшения нагрузки на ресурсы сети, несмотря на незначительный объём SNMP-сообщений, не рекомендуется устанавливать высокую частоту опроса для всех сетевых узлов. Максимальный объём SNMP-сообщения равен 484 байтов, что составляет 0.473 килобайта (RFC 1157).

3. Информирование пользователя об отказах обслуживания. Для этих целей в среде визуализации СУКС предусмотрена панель информации.

Реализация SIREN в составе единой унифицированной системы управления на основе технологии CORBA для корпоративной КС

Для применения SIREN в сетях масштаба предприятия предлагается использовать технологию CORBA. Это позволит создать единую среду управления с распределенной архитектурой, способную эффективно функционировать в условиях любой сложной, гетерогенной топологии сети любого масштаба как самостоятельно, так и с использованием других систем управления компьютерной сетью.

Для создания такой единой системы в необходимых сегментах корпоративной сети устанавливается программное обеспечение SIREN, в состав которого интегрирован CORBA-брокер ORB (Object Request Broker – брокер объектных запросов). Библиотека CORBA-брокера (ORB) может использоваться в виде разделяемой библиотеки, а также “собираться” вместе с приложением. Бета-версия брокера находится в свободном доступе в сети Интернет.

Для взаимодействия между брокерами используется протокол ИОР (Internet Inter-ORB Protocol).

Архитектура единой системы представлена на рис. 8.

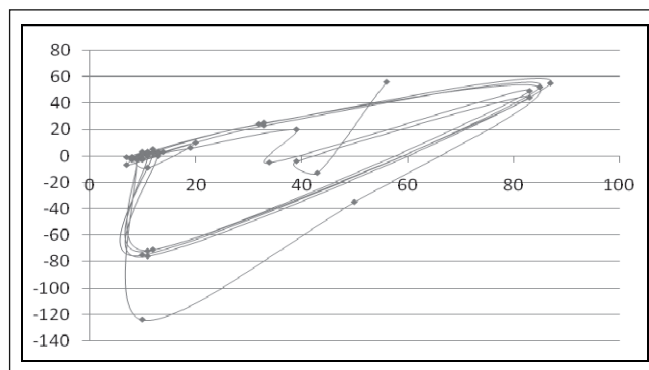


Рис. 9. Фазовый снимок параметра скорости входящего потока в условиях “без нагрузки”

Данный подход обладает рядом преимуществ:

- возможность управления сетью любого масштаба;
- возможность интеграции с другими системами управления компьютерными сетями;
- доступ к зарегистрированным эталонным фазовым снимкам событий системы управления из всех сегментов компьютерной сети с помощью общей БД;
- централизованное управление из единого пользовательского интерфейса;
- в случае сбоя и разрыва связи между корпоративной компьютерной сетью и каким-либо сетевым сегментом, функционирование системы управления в локализованном сегменте продолжится. Сбой будет диагностироваться и предотвращаться как со стороны единой системы управления корпоративной компьютерной сетью, так и со стороны системы управления в локальном сегменте.

Модуль прогнозирования состояний КС

Одной из отличительных особенностей SIREN от других аналогичных программных продуктов является наличие модуля прогнозирования состояний КС.

Для прогнозирования состояний предлагается на основе статистики, предшествующей ранее наблюдавшимся событиям, регистрировать отпечатки фазовых траекторий динамики состояния компьютерной сети. Далее проводится верификация снимков признаков и снимков потока значений факторов. В случае их совпадения идентифицируется событие. Для верификации на уникальность снимков событий и снимков потока значений предлагается использовать подходы биометрической технологии [4, 5, 6].

Под снимком фазовых состояний (фазовый снимок) компьютерной сети понимается одна или несколько фазовых траекторий параметра или параметров КС на одной плоскости за определенный временной интервал. Пример снимка фазового состояния КС по одному из параметров показан на рис. 9.

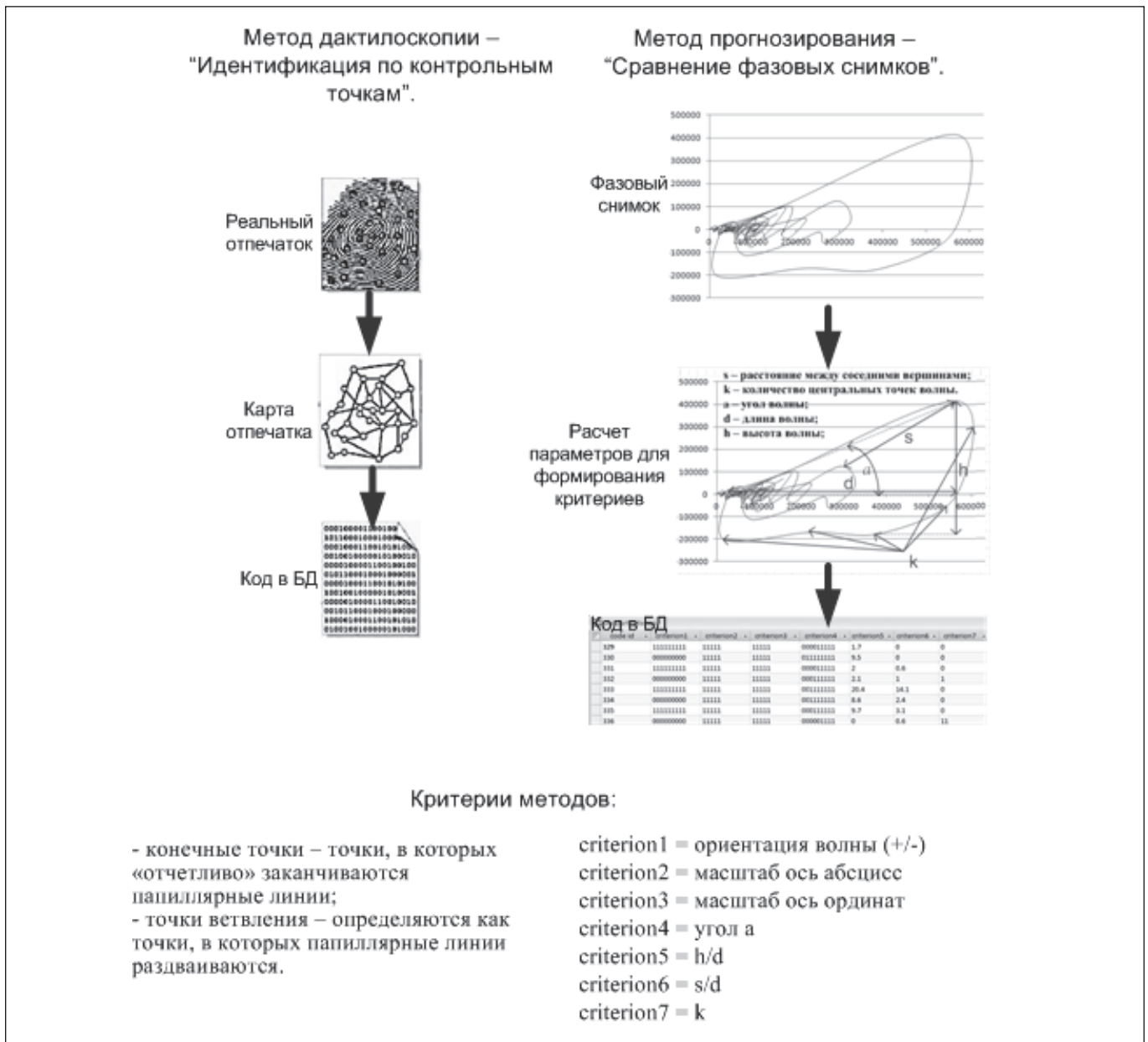


Рис. 10. Сопоставление этапов и критериев метода дактилоскопии и прогнозирования

Для возможности сравнения фазовых снимков состояний КС в режиме реального времени был использован и адаптирован метод дактилоскопии "Идентификация по контрольным точкам". Для адаптации метода дактилоскопии под решение задачи анализа сложной технической системы была выбрана сравниваемая единица – волна фазового снимка, а также найдены сравниваемые критерии (рис. 10):

- ориентация волны на фазовом снимке (+/-);
- масштаб оси абсцисс (рассматривается разряд максимальной точки);
- масштаб оси ординат (рассматривается разряд максимальной точки);
- угол наклона волны (α);

- отношение высоты к длине волны (h/d);
- отношение расстояния между вершинами предыдущей и рассматриваемой волн к длине рассматриваемой волны (s/d);
- количество центральных точек (k).

Следует отметить, что выбранные критерии относительны и не зависят от скалярных величин сравниваемых фазовых снимков. Это позволяет анализировать динамику узоров фазового снимка. Кроме того, в методе прогнозирования использовано 7 критериев, а в методе дактилоскопии – 2 критерия.

Обобщенная схема модуля прогнозирования SIREN с функцией сравнения фазовых снимков представлена на рис. 11.

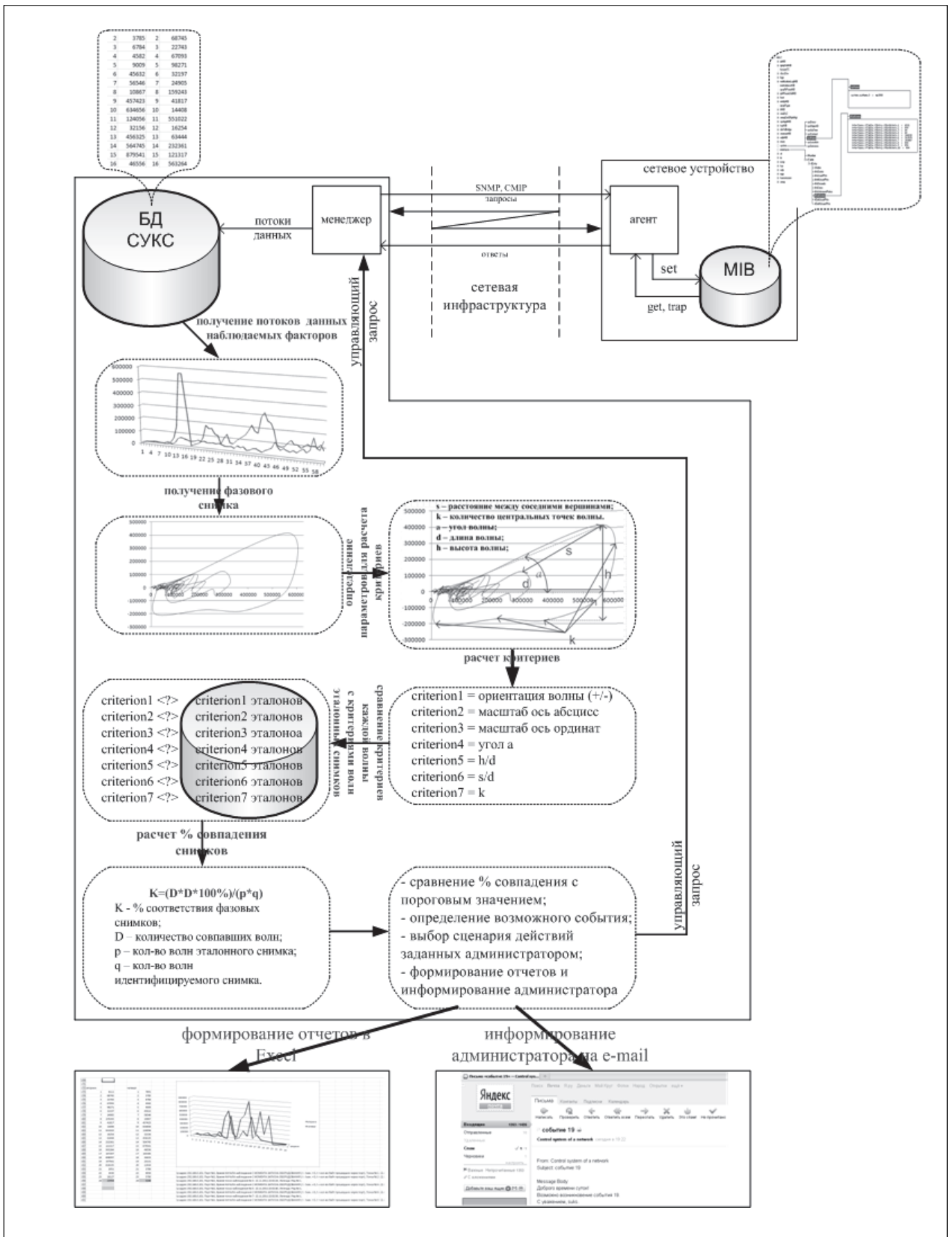


Рис. 11. Обобщенная схема работы модуля прогнозирования разработанной SIREN

Получаемая из БД МІВ сетевых устройств статистическая информация потока данных преобразуется в снимок фазовой траектории, которая состоит из волн. В реальном времени происходит анализ поступившей волны и определяются значения её критериев. Затем в БД эталонных состояний организуется поиск по рассчитанным критериям. В случае достаточного совпадения критериев волны потока с одной из волн эталонного снимка, волны считаются идентичными. Далее анализируется следующая волна потока и/или проводится итоговая оценка соответствия фазовых снимков. Оценка выполняется по формуле, используемой в дактилоскопии [5, 6]:

$$K = (D \times D \times 100\%) / (p \times q),$$

где K – % соответствия фазовых снимков; D – общее количество совпавших волн фазового снимка; p – количество всех волн эталонного снимка; q – количество всех волн идентифицируемого фазового снимка. Экспериментально было выявлено значение оптимального уровня соответствия фазовых снимков (K). Проведено по 30 экспериментов для каждого параметра порога уникальности и собрана следующая статистика:

FAR (False Acceptance Rate) – пропуск события
 FRR (False Rejection Rate) – ложная тревога
 Порог уникальности 20 процентов – FRR=21 FAR=0
 Порог уникальности 30 процентов – FRR=17 FAR=0
 Порог уникальности 40 процентов – FRR=10 FAR=1
 Порог уникальности 50 процентов – FRR=3 FAR=2
 Порог уникальности 60 процентов – **FRR=1 FAR=1**
 Порог уникальности 70 процентов – **FRR=0 FAR=1**
 Порог уникальности 80 процентов – FRR=0 FAR=7
 Порог уникальности 90 процентов – FRR=0 FAR=24

Из данных проведенного эксперимента видно, что наименьший процент ошибок находится в интервале процента уникальности равном 60-70%. В биометрии пороговым значением является 65%.

Необходимо отметить, что при использовании метода сравнения фазовых снимков для прогнозирования состояний компьютерной сети точность прогнозирования увеличивается за счет использования оцифрованных данных без потери качества на сканировании изображения. С другой стороны, точность прогноза уменьшается за счет необходимости затраты времени на реакцию системы. Поэтому возможность предотвращения события в немалой степени зависит от производительности рабочей станции, на которой установлена система, и способности компьютерной сети оперативно передать управляющий запрос.

В случае превышения заданного порога ожидается наступление спрогнозированного состояния. Для предотвращения этого состояния система начинает выполнять

заранее подготовленный администратором сценарий, формировать и отправлять запросы критичным сетевым узлам. Сценарий описывается заранее сетевым администратором для предотвращения наступления конкретного состояния или события на этапах обучения системы.

Пример экранной формы со спрогнозированным состоянием КС представлен на рис. 12.

На 1-ом графике на рис. 12 представлен поток значений наблюдаемого параметра 11 порта устройства с id=3590, на 2-ом графике – фазовый снимок наблюдаемого потока, на 3-ем графике – совпавший эталонный снимок из БД.

Из прогноза состояния – (см. график справа внизу на рис.12) следует, что значения наблюдаемого параметра будут равны 0.

Совпадение фазовых снимков равно 81%.

Спустя 10 временных интервалов, считая от 33, из графика потока (см. 1-ый график сверху на рис.12) стало очевидно, что прогноз подтвердился.

На экранной форме видно, что системе удалось спрогнозировать “2-ую волну” (см. 1-ый график сверху на рис. 12).

Условия, в которых функционирует СУКС, могут различаться по следующим критериям:

- разнотипность сетевых устройств;
- специфика требований, предъявляемых к компьютерной сети со стороны пользователей;
- разнообразие топологии и применяемых стандартов.

Однако независимо от условий работы система управления должна обеспечивать базовые требования, введенные существующими стандартами и рекомендациями в области управления компьютерной сетью.

Согласно рекомендациям концепции TMN [15,16,17] существуют следующие уровни управления:

- бизнесом;
- сервисом;
- сетью;
- элементами сети.

Все составляющие процесса, касающиеся управления компьютерной сетью (пункт 3 и 4), могут быть определены при помощи пяти функциональных компонентов (ITU-T X.700) [12,13,14]:

1. Управление ошибками и неисправностями (Fault management).
2. Контроль производительности (Performance management).
3. Управление конфигурацией (Configuration management).
4. Управление учетом средств пользователей и поставщиков услуг (Accounting management).
5. Управление безопасностью сети (Security management).

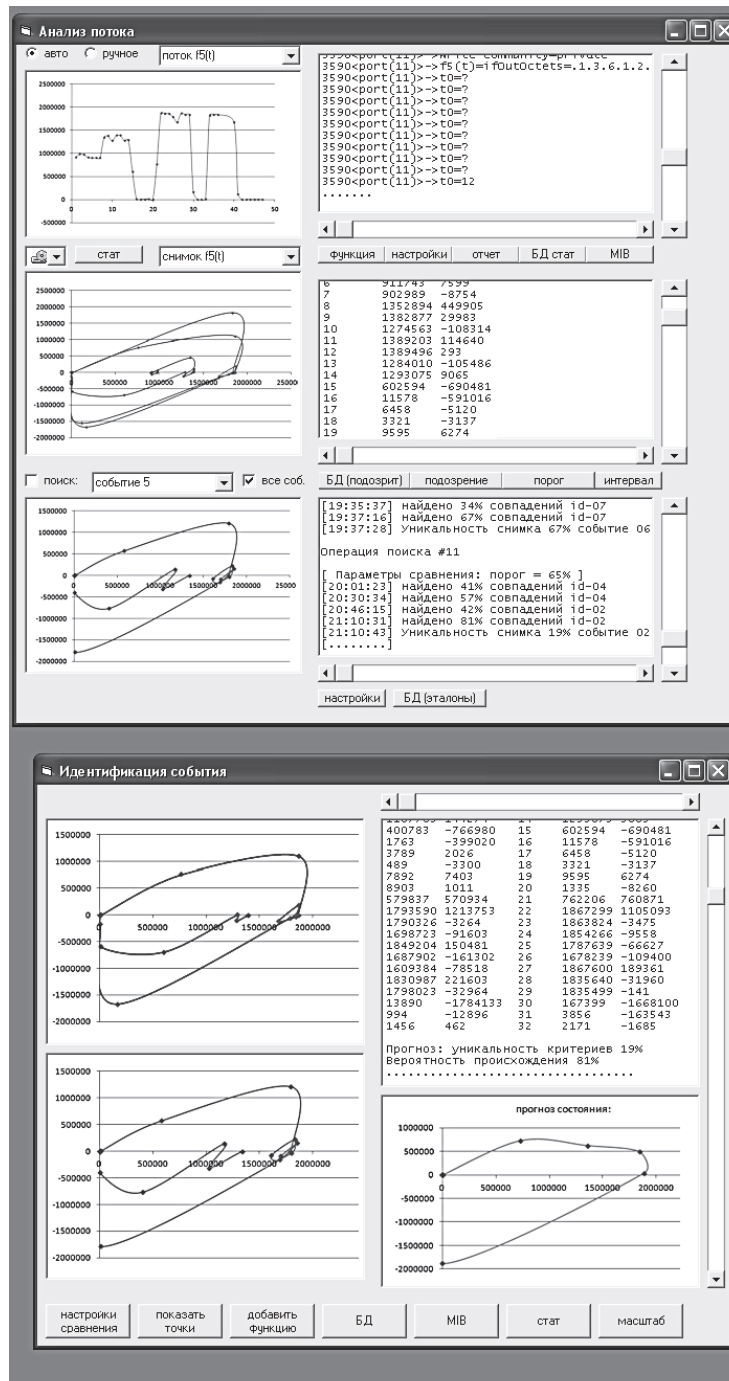


Рис. 12. Экранная форма примера прогноза состояния

Стандарты ISO 7498-4 определяют пять концептуальных задач управления компьютерными сетями, которые совпадают с пятью функциональными компонентами управления компьютерными сетями концепции TMN:

1. Управление неисправностями.
2. Управление эффективностью.
3. Управление конфигурацией.
4. Управление учетом использования ресурсов.

5. Управление защитой данных.

Следует отметить, что SIREN способна формировать прогноз состояний для решения задач управления неисправностями и эффективностью услуг передачи данных. При помощи браузера MIB можно выполнять конфигурацию сетевого оборудования. Также в SIREN реализован мощный набор инструментов для анализа статистической информации и формирования отчетов. Для защиты данных пользователя SIREN способна вы-

являть действия злоумышленника уже на раннем этапе подготовки сетевой атаки (например, по фазовым состояниям параметров индикаторов “прощупывания” КС).

Благодаря перечисленным возможностям обученная SIREN в дальнейшем, без участия администратора компьютерной сети, способна удовлетворять требованиям, обозначенным стандартами ITU-T X.700 и ISO 7498-4.

Выводы

Внедрение разработанной системы управления компьютерной сетью SIREN на ряде предприятий позволило повысить качество функционирования корпоративной компьютерной сети. Одной из важных особенностей разработанного программного обеспечения является способность строить качественный прогноз, предотвращать сбои, поддерживать заданные характеристики передачи данных между сообщениями корпоративной информационной системы предприятия. Предложенный вариант модернизации экономичен и не требует внедрения дорогостоящих программно-аппаратных комплексов.

ЛИТЕРАТУРА

1. Зубков Р.С. Тезисы доклада “Аналитический обзор систем управления корпоративными сетями” 18 февраля 2010 года, МГИЭМ.
2. Зубков Р.С. Тезисы доклада “Методы и технологии повышения QOS в IP-сетях”, 18 февраля 2009 г, МГИЭМ.
3. Леохин Ю.Л. Корпоративные сети. Архитектура, технологии, управление. – М.: Европейский центр по качеству, 2008. С. 97 – 101.
4. Вакуленко А., Юхин А., Биометрические методы идентификации личности: обоснованный выбор и внедрение // ВУТЕ. 2006. №1.
5. Jain A., Bolle R., Pankanti Sh. Biometrics: Personal Identification in Networked Society. – USA, Massachusetts, Kluwer Academic Publishers, 2002. P. 419.
6. O’Gorman L., Sammon M.J., Seul M. Practical Algorithms for Image Analysis: Description, Examples, Programs and Projects. – USA, New York, Cambridge University Press, 2008. P. 355.
7. Иванов И.А., Леохин Ю.Л. Интеллектуальное управление компьютерными сетями // Автоматизация и современные технологии. 2006. № 12. С. 26-31.
8. Назаров А.В., Лоскутов А.И. Нейросетевые алгоритмы прогнозирования и оптимизации систем. – СПб.: Наука и техника, 2003. С. 384.
9. Леохин Ю.Л. Архитектура современных систем управления корпоративными сетями // Качество. Инновации. Образование. 2009. № 2. С. 53-64.
10. Леохин Ю.Л. Корпоративные сети. Архитектура, технологии, управление – М.: Европейский центр по качеству, 2008. С. 109-112, 118 – 127.
11. Леохин Ю.Л. Управление и администрирование в компьютерных сетях: программные системы управления компьютерными сетями. – М.: МГИЭМ, 1998. С. 15-17, 25-29.
12. Замятин В.С., Попов Ф.А. Принципы создания и задачи сетевого/системного управления компьютерными сетями // М-лы Международной научно-методической конференции “Новые информационные технологии в университетском образовании”, Кемерово, 2002 г. С. 1-4.
13. Леохин Ю.Л. Управление параметрами структуры корпоративной сети // Качество. Инновации. Образование. 2009. № 5. С. 47-53.
14. Freeman R.L. Fundamentals of telecommunications. – USA, New Jersey, Wiley, 2005. P. 539-541.
15. Леохин Ю.Л., Бекасов В.Ю. Корпоративные сети: состояние, перспективы и тенденции. – М.: Фонд Качество, 2008. С. 121-124.
16. Clark M.P. Data networks, IP, and the Internet: protocols, design, and operation. – England, West Sussex, Wiley, 2003. – P. 369-403.
17. Hall Jane. Management of telecommunication systems and services: modeling and implementing TMN-based multi-domain management. – Springer, 1996. P. 150-159.

Леохин Юрий Львович,

д-р техн. наук, профессор,

нач. отдела организации научных исследований

МИЭМ НИУ ВШЭ.

e-mail: leo@miem.edu.ru

Зубков Роман Сергеевич,

аспирант МИЭМ НИУ ВШЭ