Федеральное агентство железнодорожного транспорта
Омский государственный университет путей сообщения

Кафедра «Автоматика и системы управления»

К ЗАЩИТЕ ДОПУСТИТЬ
Заведующий кафедрой АиСУ

_____ С.Н. Чижма
(подпись)

«_____» _____ 2009 г.

СИСТЕМА МОНИТОРИНГА СЕТЕВОГО ОБОРУДОВАНИЯ РЦС-3

Пояснительная записка к дипломному проекту

ИНМВ.128267.000 ПЗ

СОГЛАСОВАНО

Консультант по экономике –
доцент кафедры ЭЖТ и УК

А.Н. Шендалев

_____
(подпись)

«_____» _____ 2009 г.

Студент гр. 24 з

С.И. Экштаин

_____
(подпись)

«_____» _____ 2009 г.

Консультант по безопасности
и экологичности –
преподаватель кафедры БЖ и Э

А.А. Кообар

_____
(подпись)

«_____» _____ 2009 г.

Руководитель –
преподаватель
кафедры АиСУ

А.С. Окишев

_____
(подпись)

«_____» _____ 2009 г.

Омск 2009

ОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ПУТЕЙ СООБЩЕНИЯ

Факультет ИАТИТ Кафедра АиСУ

Специальность 230201 – Информационные системы и технологии

УТВЕРЖДАЮ:

Зав. кафедрой

/ С.Н. Чижма /

« » 2009г.

З А Д А Н И Е

на дипломный проект студента

Экштаин Сергея Ивановича

1 Тема проекта: Система мониторинга сетевого оборудования РЦС-3

утверждена приказом по университету от «29» апреля 2009 г. № 267/С

2 Срок сдачи студентом законченного проекта «9» июня 2009 г.

3 Исходные данные к проекту:

– количество АРМов – 60 ед.;

– Server AOS – 1 ед.;

– коммутатор Cisco Catalyst 2950 – 6 ед.;

– коммутатор Cisco Catalyst 2940 – 1 ед.;

– маршрутизатор Cisco 7200 – 1 ед.;

– маршрутизатор Cisco 3900 – 1 ед.;

– коммутатор 3COM OfficeConnect – 1 ед.;

– модем HDSL ADC PairGane 2Mb/s – 4 ед.;

– модем ADSL Zyxel 782E – 1 ед.;

– Open Source ПО Cacti и RRDTool;

– ПО MySQL, PHP, Apach, Net-SNMP;

– ПО Windows XP, Windows Server 2003.

4 Содержание расчетно-пояснительной записки (перечень подлежащих разработке вопросов):

4.1. Обзор систем мониторинга и используемых сетевых технологий

4.1.1. Классификация средств мониторинга и анализа

4.1.2 Анализаторы протоколов

4.1.3 Сетевые анализаторы

4.1.4 Кабельные сканеры и тестеры

4.1.5 Многофункциональные портативные приборы мониторинга

4.1.6. Системы мониторинга IP сетей

4.1.7. Принцип работы систем мониторинга IP сетей

4.1.8. Протокол SNMP

4.1.9. Структура и типы блоков управляющей информации (MIB)

4.2. Выбор ПО

4.2.1. Сравнение Open Source систем мониторинга

4.2.2. Система мониторинга Cacti

4.2.3. RRD (Round Robin Database). Промышленный стандарт

5.1 Проблемы перегруженности СПД 1 лист

5.2 Алгоритм работы системы 1 лист

5.3 Отображение собранной информации 1 лист

5.4 Карта сети 1 лист

5.5 Временные интервалы отображения графиков 1 лист

5.6 Система оповещения о событиях 1 лист

5.7 Система голосового оповещения и система ведения логов событий 1 лист

5.8 Зависимость эффективности работы предприятия от времени реагирования на событие 1 лист

6 Консультанты по проекту (с указанием относящихся к ним разделов проекта)

Раздел	Консультант	Подпись, дата

		задание выдал	задание принял
Нормоконтроль	Александров А.В.		
Экономика	Шендалев А.Н.		
Охрана труда	Кообар А.А.		

Руководитель проекта _____ / Окишев А.С. /_____

КАЛЕНДАРНЫЙ ПЛАН

№ п-п	Наименование разделов дипломного проекта	Срок выполнения	Примечание
1	Анализ проблемы, выбор темы диплома составление плана пояснительной записки, уточнение плана работы	26.03.2009	
2	Окончательный сбор материала по теме диплома, написание теоретической части (1 главы)	16.04.2009	
3	Первый вариант пояснительной записки, составление плана доклада и списка графического материала	14.05.2009	
4	Готовый дипломный проект, графический материал, доклад к защите дипломного проекта	04.06.2009	

7 Дата выдачи задания «16 » марта 2009 г.

Руководитель _____

(подпись)

Задание принял к исполнению _____

(подпись)

Реферат

УДК 004.7

Пояснительная записка к дипломному проекту содержит 107 страниц, 47 рисунков, 23 таблицы, 15 использованных источников, 4 приложения, 8

листов графического материала.

Корпоративная сеть, коммутатор, сервер, загрузка сети, сетевое оборудование, пропускная способность, система мониторинга сетевого оборудования, анализ, системы управления, SNMP, MIB, агент, IP сети, маршрутизатор, программное обеспечение, Open Source, Cacti, RRDTool, интерфейс, Web серевер Apache, СУБД MySQL, PHP, Perl, Cisco, NetSNMP, алгоритм, устройства, установка, консоль, график.

Целью дипломного проекта является разработка системы мониторинга сетевого оборудования РЦС-3, для наблюдения за сетью предприятия и оперативного выявления и устранения возникающих проблем для бесперебойной работы оборудования в режиме online.

В ходе дипломного проектирования разработана система мониторинга для сетевого оборудования, установленного на предприятии РЦС-3. Система мониторинга построена на базе программного обеспечения Cacti и RRDTool. Данное программное обеспечения является Open Source ПО, т.е. программное обеспечение с открытым исходным кодом.

При проектировании системы мониторинга была учтена структура сети предприятия, объекты мониторинга, а также задачи, возложенные на систему мониторинга.

Результатом дипломного проектирования является законченная система мониторинга, построенная на базе бесплатно распространяемого ПО, но в тоже время не уступающая, а в некоторых случаях и превосходящая свои платные аналоги по функционалу и масштабируемости.

Пояснительная записка к дипломному проекту выполнена в текстовом редакторе Microsoft Word 2007, графическая часть выполнена в пакете Microsoft Visio 2003, презентация дипломного проекта выполнена с использованием Microsoft PowerPoint 2007.

Содержание

В конверте на обороте обложки:
диск CD-R. 1_Экштаин_С.И_24з_Диплом.doc.
2_Презентация.ppt.

На отдельных листах:

Введение

Для управления корпоративными сетями передачи данных чрезвычайно важна возможность получения достоверной информации о структуре потоков данных, о природе этих потоков, о приложениях, генерирующих эти потоки и потребляющих дефицитные сетевые ресурсы. Предотвращение утечек этих ресурсов из-за наличия в сети компьютеров с аномальным поведением, в том числе зараженных или взломанных, использованием в сети изощренных файлообменных приложений является актуальной задачей.

Важнейшей задачей для оперативного управления сетью и перспективного планирования ее развития, является задача учета потребления ресурсов сети на значительных временных интервалах (часы, сутки, недели, месяцы) различными группами пользователей – определенных либо статически, либо динамически (участники видеоконференции из разных организаций, участники традиционных конференций и/или собраний). Другая важная задача, обычно упускаемая из вида при построении систем сетевого мониторинга, связана с оперативным отслеживанием состояния сети и ее компонентов с целью обнаружения аномального поведения, которое может быть следствием атак на сеть или нарушениями порядка использования сетевых ресурсов абонентами. Принимая во внимание

высокую ценность сетевых ресурсов (в первую очередь – пропускной способности внешних каналов), следует, прежде всего, обеспечить возможность оперативного и ретроспективного анализа нерегулярностей и аномалий. Таким образом, система мониторинга должна также рассматриваться, как важная компонента системы обеспечения безопасности корпоративной сети.

Корпоративная сеть предприятия РЦС-3 практически полностью построена на сетевом оборудовании фирмы Cisco. Для связи предприятия с сетью интранет ОАО РЖД имеется выделенный канал пропускной способностью 2 Мбит\сек. В РЦС-3 имеются АРМы, работающие в online режиме с серверами, расположенными в Москве, а в связи с тем что пропускная способность канала очень маленькая, то при возникновении ситуации, когда еще какой-либо компьютер в сети генерирует много трафика, направленного во внешнюю сеть, АРМы, работающие в режиме online, не могут связаться с центральным сервером в Москве. Такая ситуация вызывает множество проблем, препятствующих стабильной работе предприятия в оперативном режиме.

Целью дипломного проекта является разработка системы мониторинга сетевого оборудования, для наблюдения за сетью предприятия и оперативного выявления и устранения возникающих проблем для бесперебойной работы оборудования в режиме online.

1 Обзор систем мониторинга и используемых сетевых технологий

1.1 Классификация средств мониторинга и анализа

Все многообразие средств, применяемых для мониторинга и анализа вычислительных сетей, можно разделить на несколько крупных классов.

Системы управления сетью (Network Management Systems) – централизованные программные системы, которые собирают данные о

состоянии узлов и коммуникационных устройств сети, а также данные о трафике, циркулирующем в сети. Эти системы не только осуществляют мониторинг и анализ сети, но и выполняют в автоматическом или полуавтоматическом режиме действия по управлению сетью: включение и отключение портов устройств, изменение параметров мостов адресных таблиц мостов, коммутаторов и маршрутизаторов и т.п. Примерами систем управления могут служить популярные системы HPOpen View, Sun Net Manager, IBM Net View.

Средства управления системой (System Management) часто выполняют функции, аналогичные функциям систем управления, но по отношению к другим объектам. В первом случае объектом управления является программное и аппаратное обеспечение компьютеров сети, а во втором – коммуникационное оборудование. Вместе с тем, некоторые функции этих двух видов систем управления могут дублироваться, например, средства управления системой могут выполнять простейший анализ сетевого трафика. Встроенные системы диагностики и управления (Embeddedsystems) выполняются в виде программно-аппаратных модулей, устанавливаемых в коммуникационное оборудование, а также в виде программных модулей, встроенных в операционные системы. Они выполняют функции диагностики и управления только одним устройством, и в этом их основное отличие от централизованных систем управления. Примером средств этого класса может служить модуль управления концентратором Distrebuted 5000, реализующий функции автосегментации портов при обнаружении неисправностей, приписывания портов внутренним сегментам концентратора и некоторые другие. Как правило, встроенные модули управления «по совместительству» играют роль SNMP-агентов, поставляющих данные о состоянии устройства для систем управления.

Анализаторы протоколов (Protocolanalyzers) представляют собой программные или аппаратно-программные системы, которые

ограничиваются, в отличие от систем управления, лишь функциями мониторинга и анализа трафика в сетях. Хороший анализатор протоколов может захватывать и декодировать пакеты большого количества протоколов, применяемых в сетях – обычно несколько десятков. Анализаторы протоколов позволяют установить некоторые логические условия для захвата отдельных пакетов и выполняют полное декодирование захваченных пакетов, то есть показывают в удобной для специалиста форме вложенность пакетов протоколов разных уровней друг в друга с расшифровкой содержания отдельных полей каждого пакета.

Оборудование для диагностики и сертификации кабельных систем – это оборудование можно поделить на четыре основные группы: сетевые мониторы, приборы для сертификации кабельных систем, кабельные сканеры и тестеры (мультиметры).

Сетевые мониторы (называемые также сетевыми анализаторами) предназначены для тестирования кабелей различных категорий. Следует различать сетевые мониторы и анализаторы протоколов. Сетевые мониторы собирают данные только о статистических показателях трафика – средней интенсивности общего трафика сети, средней интенсивности потока пакетов с определенным типом ошибки и т.п.

Назначение устройств для сертификации кабельных систем непосредственно следует из их названия. Сертификация выполняется в соответствии с требованиями одного из международных стандартов на кабельные системы.

Кабельные сканеры используются для диагностики медных кабельных систем. Тестеры предназначены для проверки кабелей на отсутствие физического разрыва.

Экспертные системы. Этот вид систем аккумулирует человеческие знания о выявлении причин аномальной работы сетей и возможных способах приведения сети в работоспособное состояние. Экспертные системы часто

реализуются в виде отдельных подсистем различных средств мониторинга и анализа сетей: систем управления сетями, анализаторов протоколов, сетевых анализаторов. Простейшим вариантом экспертной системы является контекстно-зависимая help-система. Более сложные экспертные системы представляют собой так называемые базы знаний, обладающие элементами искусственного интеллекта. Примером такой системы является экспертная система, встроенная в систему управления Spectrum компании Cabletron.

Многофункциональные устройства анализа и диагностики. В последние годы в связи с повсеместным распространением локальных сетей возникла необходимость разработки недорогих портативных приборов, совмещающих функции нескольких устройств: анализаторов протоколов, кабельных сканеров – и некоторые возможности ПО сетевого управления.

1.1.1 Системы управления

В соответствии с рекомендациями ISO можно выделить следующие функции средств управления сетью.

Управление конфигурацией сети и именованием – состоит в конфигурировании компонентов сети, включая их местоположение, сетевые адреса и идентификаторы, управление параметрами сетевых операционных систем, поддержание схемы сети; также эти функции используются для именования объектов.

Анализ производительности – помогает на основе накопленной статистической информации оценивать время ответа системы и величину трафика, а также планировать развитие сети.

Управление безопасностью – включает в себя контроль доступа и сохранение целостности данных. В функции входит процедура аутентификации, проверки привилегий, поддержка ключей шифрования, управления полномочиями. К этой же группе можно отнести важные механизмы управления паролями, внешним доступом, соединения с другими сетями.

Учет работы сети – включает регистрацию и управление используемыми ресурсами и устройствами. Эта функция оперирует такими понятиями как время использования и плата за ресурсы.

Из приведенного списка видно, что системы управления выполняют не только функции мониторинга и анализа работы сети, необходимые для получения исходных данных для настройки сети, но и включают функции активного воздействия на сеть – управления конфигурацией и безопасностью, которые нужны для отработки выработанного плана настройки и оптимизации сети. Сам этап создания плана настройки сети обычно остается за пределами функций системы управления, хотя некоторые системы управления имеют в своем составе экспертные подсистемы, помогающие администратору или интегратору определить необходимые меры по настройке сети.

Средства управления сетью (Network Management) не следует путать со средствами управления компьютерами и их операционными системами (System Management).

Средства управления системой обычно выполняют следующие функции:

– учет используемых аппаратных и программных средств. Система автоматически собирает информацию об обследованных компьютерах и создает записи в базе данных об аппаратных и программных ресурсах. После этого администратор может быстро выяснить, чем он располагает и где это находится. Например, узнать о том, на каких компьютерах нужно обновить драйверы принтеров, какие ПК обладают достаточным количеством памяти и дискового пространства и т. п.;

– распределение и установка программного обеспечения. После завершения обследования администратор может создать пакеты рассылки программного обеспечения – очень эффективный способ для уменьшения стоимости такой процедуры. Система может также позволять

централизованно устанавливать и администрировать приложения, которые запускаются с файловых серверов, а также дать возможность конечным пользователям запускать такие приложения с любой рабочей станции сети;

– удаленный анализ производительности и возникающих проблем. Администратор может удаленно управлять мышью, клавиатурой и видеть экран любого ПК, работающего в сети под управлением той или иной сетевой операционной системы. База данных системы управления обычно хранит детальную информацию о конфигурации всех компьютеров в сети для того, чтобы можно было выполнять удаленный анализ возникающих проблем.

Примерами средств управления системой являются такие продукты, как System Management Server компании Microsoft или LAN Desk Manager фирмы Intel, а типичными представителями средств управления сетями являются системы HPOpen View, Sun Net Manager и IBM Net View.

Создание систем управления сетями немыслимо без ориентации на определенные стандарты, так как управляющее программное обеспечение и сетевое оборудование, а, значит, и агентов для него, разрабатывают сотни компаний. Поскольку корпоративная сеть наверняка неоднородна, управляющие инструменты не могут отражать специфики одной системы или сети.

Наиболее распространенным протоколом управления сетями является протокол SNMP (Simple Network Management Protocol), его поддерживают сотни производителей. Главные достоинства протокола SNMP – простота, доступность, независимость от производителей. В значительной степени именно популярность SNMP задержала принятие CMIP, варианта управляющего протокола по версии OSI. Протокол SNMP разработан для управления маршрутизаторами в сети Internet и является частью стека TCP/IP.

SNMP – это протокол, используемый для получения от сетевых устройств информации об их статусе, производительности и характеристиках, которые хранятся в специальной базе данных сетевых устройств, называемой MIB (Management Information Base). Существуют стандарты, определяющие структуру MIB, в том числе набор типов ее переменных (объектов в терминологии ISO), их имена и допустимые операции этими переменными (например, читать). В MIB, наряду с другой информацией, могут храниться сетевой и/или MAC-адреса устройств, значения счетчиков обработанных пакетов и ошибок, номера, приоритеты и информация о состоянии портов. Древовидная структура MIB содержит обязательные (стандартные) поддеревья, а также в ней могут находиться частные (private) поддеревья, позволяющие изготовителю интеллектуальных устройств реализовать какие-либо специфические функции на основе его специфических переменных.

Агент в протоколе SNMP – это обрабатывающий элемент, который обеспечивает менеджерам, размещенным на управляющих станциях сети, доступ к значениям переменных MIB, и тем самым дает им возможность реализовывать функции по управлению и наблюдению за устройством. Типичная структура системы управления изображена на рисунке 1.1.

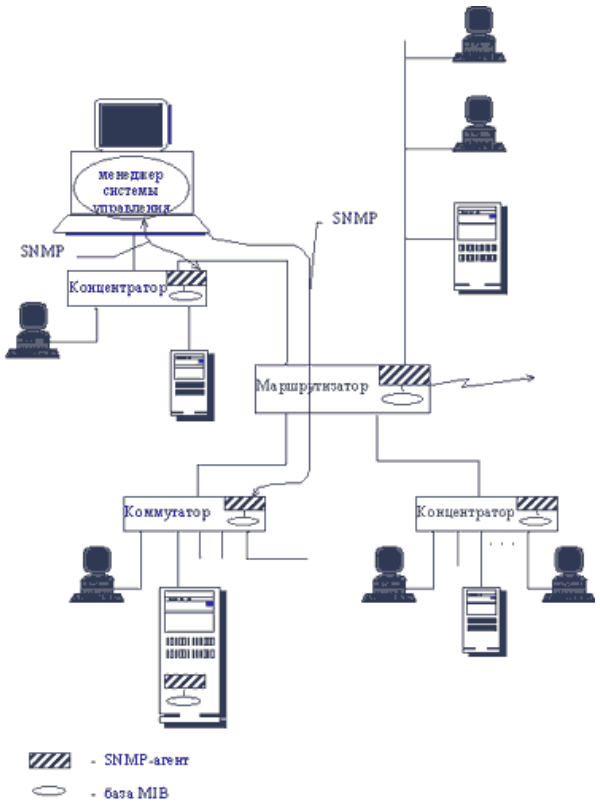


Рисунок 1.1 – Типичная структура системы управления сетью

Основные операции по управлению вынесены в управляющую станцию. При этом устройство работает с минимальными издержками на поддержание управляющего протокола. Оно использует почти всю свою вычислительную мощность для выполнения своих основных функций маршрутизатора, моста или концентратора, а агент занимается сбором статистики и значений переменных состояния устройства и передачей их менеджеру системы управления. SNMP – это протокол типа «запрос-ответ», то есть на каждый запрос, поступивший от менеджера, агент должен передать ответ. Особенностью протокола является его чрезвычайная простота – он включает в себя всего несколько команд.

Команда Get-request используется менеджером для получения от агента значения какого-либо объекта по его имени.

Команда GetNext-request используется менеджером для извлечения значения следующего объекта (без указания его имени) при последовательном просмотре таблицы объектов.

С помощью команды Get-response агент SNMP передает менеджеру ответ на одну из команд Get-request или GetNext-request.

Команда Set используется менеджером для установления значения какого-либо объекта либо условия, при выполнении которого агент SNMP должен послать менеджеру соответствующее сообщение. Может быть определена реакция на такие события как инициализация агента, рестарт агента, обрыв связи, восстановление связи, неверная аутентификация и потеря ближайшего маршрутизатора. Если происходит любое из этих событий, то агент инициализирует прерывание.

Команда Trap используется агентом для сообщения менеджеру о возникновении особой ситуации.

Версия SNMPv.2 добавляет к этому набору команду GetBulk, которая позволяет менеджеру получить несколько значений переменных за один запрос.

1.1.2 Встроенные средства мониторинга и анализа сетей

1.1.2.1 Агенты SNMP

Сегодня существует несколько стандартов на базы данных управляющей информации. Основными являются стандарты MIB-I и MIB-II, а также версия базы данных для удаленного управления RMONMIB. Кроме этого, существуют стандарты для специальных MIB устройств конкретного типа (например, MIB для концентраторов или MIB для модемов), а также частные MIB конкретных фирм-производителей оборудования.

Первоначальная спецификация MIB-I определяла только операции чтения значений переменных. Операции изменения или установки значений объекта являются частью спецификаций MIB-II.

Версия MIB-I (RFC 1156) определяет до 114 объектов, которые подразделяются на 8 групп:

– System – общие данные об устройстве (например, идентификатор поставщика, время последней инициализации системы);

– Interfaces – описываются параметры сетевых интерфейсов устройства (например, их количество, типы, скорости обмена, максимальный размер пакета);

– AddressTranslationTable – описывается соответствие между сетевыми и физическими адресами (например, по протоколу ARP);

– InternetProtocol –данные, относящиеся к протоколу IP (адреса IP-шлюзов, хостов, статистика об IP-пакетах);

– ICMP – данные, относящиеся к протоколу обмена управляющими сообщениями ICMP;

– TCP – данные, относящиеся к протоколу TCP (например, о TCP-соединениях);

– UDP – данные, относящиеся к протоколу UDP (число переданных, принятых и ошибочных UPD-дейтаграмм);

– EGP – данные, относящиеся к протоколу обмена маршрутной информацией ExteriorGatewayProtocol, используемому в сети Internet (число принятых с ошибками и без ошибок сообщений).

Из этого перечня групп переменных видно, что стандарт MIB-I разрабатывался с жесткой ориентацией на управление маршрутизаторами, поддерживающими протоколы стека TCP/IP. В версии MIB-II (RFC 1213), принятой в 1992 году, был существенно (до 185) расширен набор стандартных объектов, а число групп увеличилось до 10.

1.1.2.2 Агенты RMON

Новейшим добавлением к функциональным возможностям SNMP является спецификация RMON, которая обеспечивает удаленное взаимодействие с базой MIB. До появления RMON протокол SNMP не мог использоваться удаленным образом, он допускал только локальное управление устройствами. База RMON MIB обладает улучшенным набором

свойств для удаленного управления, так как содержит агрегированную информацию об устройстве, что не требует передачи по сети больших объемов информации. Объекты RMONMIB включают дополнительные счетчики ошибок в пакетах, более гибкие средства анализа графических трендов и статистики, более мощные средства фильтрации для захвата и анализа отдельных пакетов, а также более сложные условия установления сигналов предупреждения. Агенты RMONMIB более интеллектуальны по сравнению с агентами MIB-I или MIB-II и выполняют значительную часть работы по обработке информации об устройстве, которую раньше выполняли менеджеры. Эти агенты могут располагаться внутри различных коммуникационных устройств, а также быть выполнены в виде отдельных программных модулей, работающих на универсальных ПК и ноутбуках (примером может служить LANalyzerNovell).

Объекту RMON присвоен номер 16 в наборе объектов MIB, а сам объект RMON объединяет 10 групп следующих объектов:

– Statistics – текущие накопленные статистические данные о характеристиках пакетов, количестве коллизий и т.п.;

– History – статистические данные, сохраненные через определенные промежутки времени для последующего анализа тенденций их изменений;

– Alarms – пороговые значения статистических показателей, при превышении которых агент RMON посылает сообщение менеджеру;

– Host – данных о хостах сети, в том числе и об их MAC-адресах;

– HostTopN – таблица наиболее загруженных хостов сети;

– TrafficMatrix – статистика об интенсивности трафика между каждой парой хостов сети, упорядоченная в виде матрицы;

– Filter – условия фильтрации пакетов;

– PacketCapture – условия захвата пакетов;

– Event – условия регистрации и генерации событий.

Данные группы пронумерованы в указанном порядке, поэтому, например, группа Hosts имеет числовое имя 1.3.6.1.2.1.16.4.

Всего стандарт RMONMIB определяет около 200 объектов в 10 группах, зафиксированных в двух документах – RFC 1271 для сетей Ethernet и RFC 1513 для сетей Token Ring.

Отличительной чертой стандарта RMONMIB является его независимость от протокола сетевого уровня (в отличие от стандартов MIB-I и MIB-II, ориентированных на протоколы TCP/IP). Поэтому его удобно использовать в гетерогенных средах, использующих различные протоколы сетевого уровня.

1.1.3 Анализаторы протоколов

В ходе проектирования новой или модернизации старой сети часто возникает необходимость в количественном измерении некоторых характеристик сети таких, например, как интенсивности потоков данных по сетевым линиям связи, задержки, возникающие на различных этапах обработки пакетов, времена реакции на запросы того или иного вида, частота возникновения определенных событий и других характеристик.

Для этих целей могут быть использованы разные средства и прежде всего – средства мониторинга в системах управления сетью. Некоторые измерения на сети могут быть выполнены и встроенными в операционную систему программными измерителями, примером тому служит компонента ОС WindowsNT Performance Monitor. Даже кабельные тестеры в их современном исполнении способны вести захват пакетов и анализ их содержимого.

Но наиболее совершенным средством исследования сети является анализатор протоколов. Процесс анализа протоколов включает захват циркулирующих в сети пакетов, реализующих тот или иной сетевой протокол, и изучение содержимого этих пакетов. Основываясь на результатах анализа, можно осуществлять обоснованное и взвешенное

изменение каких-либо компонент сети, оптимизацию ее производительности, поиск и устранение неполадок. Очевидно, что для того, чтобы можно было сделать какие-либо выводы о влиянии некоторого изменения на сеть, необходимо выполнить анализ протоколов и до, и после внесения изменения.

Анализатор протоколов представляет собой либо самостоятельное специализированное устройство, либо персональный компьютер, обычно переносной, класса Notebook, оснащенный специальной сетевой картой и соответствующим программным обеспечением. Применяемые сетевая карта и программное обеспечение должны соответствовать топологии сети (кольцо, шина, звезда). Анализатор подключается к сети точно также, как и обычный узел. Отличие состоит в том, что анализатор может принимать все пакеты данных, передаваемые по сети, в то время как обычная станция - только адресованные ей. Программное обеспечение анализатора состоит из ядра, поддерживающего работу сетевого адаптера и декодирующего получаемые данные, и дополнительного программного кода, зависящего от типа топологии исследуемой сети. Кроме того, поставляется ряд процедур декодирования, ориентированных на определенный протокол, например, IPX. В состав некоторых анализаторов может входить также экспертная система, которая может выдавать пользователю рекомендации о том, какие эксперименты следует проводить в данной ситуации, что могут означать те или иные результаты измерений, как устранить некоторые виды неисправности сети.

Некоторые анализаторы протоколов позволяют автоматизировать просмотр информации, находящейся в буфере, и находить в ней данные по заданным критериям. В то время, как фильтры проверяют входной поток на предмет соответствия условиям фильтрации, функции поиска применяются к уже накопленным в буфере данным.

1.1.4 Оборудование для диагностики и сертификации кабельных систем

К оборудованию данного класса относятся сетевые анализаторы, приборы для сертификации кабелей, кабельные сканеры и тестеры. Прежде, чем перейти к более подробному рассмотрению этих устройств, приведем некоторые необходимые сведения об основных электромагнитных характеристиках кабельных систем.

Основными электрическими характеристиками, влияющими на работу кабеля, являются: затухание, импеданс (волновое сопротивление), перекрестные наводки двух витых пар и уровень внешнего электромагнитного излучения.

Перекрестные наводки между витыми парами или Near End Crosstalk (NEXT) – представляют собой результат интерференции электромагнитных сигналов, возникающих в двух витых парах. Один из кабелей витой пары является передающим, а второй – приемным. При прохождении сигнала по одному из кабелей, например передающему, в приемном кабеле возникают перекрестные наводки. Величина NEXT зависит от частоты передаваемого сигнала – чем выше величина NEXT, тем лучше (для категории 5 NEXT должен быть не менее 27 Дб при частоте 100 Мгц, для кабеля категории 3 на частоте 10 МГц NEXT должен быть не менее 26 Дб).

Затухание (Attenuation) – представляет собой потерю амплитуды электрического сигнала при его распространении по кабелю. Затухание имеет два основных источника: электрические характеристики кабеля и поверхностный эффект. Последний объясняет зависимость затухания от частоты. Затухание измеряется в децибелах на метр. Для кабеля категории 5 при частоте 100 Мгц затухание не должно превышать 23,6 Дб на 100 м, а для кабеля категории 3, применяемого по стандарту IEEE 802.3 10BASE-T, допустимая величина затухания на сегменте длиной 100 м не должна превышать 11,5 Дб при частоте переменного тока 10 МГц.

Импеданс (волновое сопротивление) – это полное (активное и реактивное) сопротивление в электрической цепи. Импеданс измеряется в

омах и является относительно постоянной величиной для кабельных систем. Для неэкранированной витой пары наиболее часто используемые значения импеданса – 100 и 120 Ом. Характерные значения импеданса для сетей стандарта Ethernet на коаксиальном кабеле составляют 50 Ом, а для сетей стандарта Arcnet – 93 Ом. Резкие изменения импеданса по длине кабеля могут вызвать процессы внутреннего отражения, приводящие к возникновению стоячих волн. Рабочая станция, подключенная к кабелю вблизи узла стоячей волны, не сможет получать адресованные ей сообщения.

Активное сопротивление – это сопротивление постоянному току в электрической цепи. В отличие от импеданса активное сопротивление не зависит от частоты и возрастает с увеличением длины кабеля. Для неэкранированной витой пары категории 5 активное сопротивление не должно превышать 9,4 Ом на 100 м.

Емкость – это свойство металлических проводников накапливать энергию. Два электрических проводника в кабеле, разделенные диэлектриком, представляют собой конденсатор, способный накапливать заряд. Емкость является нежелательной величиной, поэтому ее следует делать как можно меньше. Высокое значение емкости в кабеле приводит к искажению сигнала и ограничивает полосу пропускания линии. Для кабельных систем категории 5 значение емкости не должно превышать 5,6 нФ на 100 м.

Уровень внешнего электромагнитного излучения, или электрический шум – это нежелательное переменное напряжение в проводнике. Электрический шум бывает двух типов: фоновый и импульсный. Электрический шум можно также разделить на низко-, средне- и высокочастотный. Источниками фонового электрического шума являются в диапазоне до 150 КГц линии электропередачи, телефоны и лампы дневного света; в диапазоне от 150 КГц до 20 Мгц компьютеры, принтеры, ксероксы; в диапазоне от 20 Мгц до 1 ГГц – телевизионные и радиопередатчики,

микроволновые печи. Основными источниками импульсного электрического шума являются моторы, переключатели и сварочные агрегаты. Электрический шум измеряется в мВ. Кабельные системы на витой паре не сильно подвержены влиянию электрического шума (в отличие от влияния NEXT).

1.1.5 Сетевые анализаторы

Сетевые анализаторы представляют собой эталонные измерительные инструменты для диагностики и сертификации кабелей и кабельных систем. В качестве примера можно привести сетевые анализаторы компании Hewlett Packard – HP 4195A и HP 8510C.

Сетевые анализаторы содержат высокоточный частотный генератор и узкополосный приемник. Передавая сигналы различных частот в передающую пару и измеряя сигнал в приемной паре, можно измерить затухание и NEXT. Сетевые анализаторы – это прецизионные крупногабаритные и дорогие (стоимостью более $20000) приборы, предназначенные для использования в лабораторных условиях специально обученным техническим персоналом.

1.1.6 Кабельные сканеры

Данные приборы позволяют определить длину кабеля, NEXT, затухание, импеданс, схему разводки, уровень электрических шумов и провести оценку полученных результатов. Существует достаточно много устройств данного класса, например, сканеры компаний Microtest Inc., Fluke Corp., Datacom Technologies Inc., Scope Communication Inc. В отличие от сетевых анализаторов сканеры могут быть использованы не только специально обученным техническим персоналом, но даже администраторами-новичками.

Для определения местоположения неисправности кабельной системы (обрыва, короткого замыкания, неправильно установленного разъема и т.д.) используется метод «кабельного радара», или Time DomainReflectometry

(TDR). Суть этого метода состоит в том, что сканер излучает в кабель короткий электрический импульс и измеряет время задержки до прихода отраженного сигнала. По полярности отраженного импульса определяется характер повреждения кабеля (короткое замыкание или обрыв). В правильно установленном и подключенном кабеле отраженный импульс совсем отсутствует.

Точность измерения расстояния зависит от того, насколько точно известна скорость распространения электромагнитных волн в кабеле. В различных кабелях она будет разной. Скорость распространения электромагнитных волн в кабеле (NVP – Nominal Velocityof Propagation) обычно задается в процентах к скорости света в вакууме. Современные сканеры содержат в себе электронную таблицу данных о NVP для всех основных типов кабелей и позволяют пользователю устанавливать эти параметры самостоятельно после предварительной калибровки.

Наиболее известными производителями компактных (их размеры обычно не превышают размеры видеокассеты стандарта VHS) кабельных сканеров являются компании Microtest Inc., Wave Tek Corp., Scope CommunicationInc.

1.1.7 Тестеры

Тестеры кабельных систем – наиболее простые и дешевые приборы для диагностики кабеля. Они позволяют определить непрерывность кабеля, однако, в отличие от кабельных сканеров, не дают ответа на вопрос о том, в каком месте произошел сбой.

1.1.8 Многофункциональные портативные приборы мониторинга

В последнее время начали выпускаться многофункциональные портативные приборы, которые объединяют в себе возможности кабельных сканеров, анализаторов протоколов и даже некоторые функции систем управления, сохраняя в то же время такое важное свойство, как портативность. Многофункциональные приборы мониторинга имеют

специализированный физический интерфейс, позволяющий выявлять проблемы и тестировать кабели на физическом уровне, который дополняется микропроцессором с программным обеспечением для выполнения высокоуровневых функций.

Рассмотрим типичный набор функций и свойств такого прибора, который оказывается очень полезным для диагностики причин разнообразных неполадок в сети, происходящих на всех уровнях стека протоколов, от физического до прикладного.

Прибор обычно предоставляет пользователю удобный и интуитивно понятный интерфейс, основанный на системе меню. Графический интерфейс пользователя реализован на многострочном жидкокристаллическом дисплее и индикаторах состояния на светодиодах, извещающих пользователя о наиболее общих проблемах наблюдаемых сетей. Имеется обширный файл подсказок оператору с уровневым доступом в соответствии с контекстом. Информация о состоянии сети представляется таким образом, что пользователи любой квалификации могут ее быстро понять.

Многофункциональные приборы сочетают наиболее часто используемые на практике функции кабельных сканеров с рядом новых возможностей тестирования.

Функция сканирования кабеля позволяет измерять длину кабеля, расстояние до самого серьезного дефекта и распределение импеданса по длине кабеля. При проверке неэкранированной витой пары могут быть выявлены следующие ошибки: расщепленная пара, обрывы, короткое замыкание и другие виды нарушения соединения.

Для сетей Ethernet на коаксиальном кабеле эти проверки могут быть осуществлены на работающей сети.

Функция определения распределения кабельных жил – осуществляет проверку правильности подсоединения жил, наличие промежуточных

разрывов и перемычек на витых парах. На дисплей выводится перечень связанных между собой контактных групп.

Функция определения карты кабелей – используется для составления карты основных кабелей и кабелей, ответвляющихся от центрального помещения.

В зависимости от конфигурации возможно определить длину, импеданс, схему подключения жил, затухание и параметр NEXT на частоте до 100 МГц. Автоматическая проверка выполняется для:

– коаксиальных кабелей;

– экранированной витой пары с импедансом 150 Ом;

– неэкранированной витой пары с сопротивлением 100 Ом.

Целостность цепи при проверке постоянным током используется при проверке коаксиальных кабелей для верификации правильности используемых терминаторов и их установки.

Определение номинальной скорости распространения – функция вычисляет номинальную скорость распространения (Nominal Velocity of Propagation, NVP) по кабелю известной длины и дополнительно сохраняет полученные результаты в файле для определяемого пользователем типа кабеля (User Defined cable type) или стандартного кабеля.

Комплексная автоматическая проверка пары «сетевой адаптер-концентратор» – этот комплексный тест позволяет последовательно подключить прибор между конечным узлом сети и концентратором. Тест дает возможность автоматически определить местонахождение источника неисправности – кабель, концентратор, сетевой адаптер или программное обеспечение станции.

Автоматическая проверка сетевых адаптеров – проверяет правильность функционирования вновь установленных или «подозрительных» сетевых адаптеров. Для сетей Ethernet по итогам проверки сообщаются: MAC-адрес, уровень напряжения сигналов (а также

присутствие и полярность импульсов Link Test для 10BASE-T). Если сигнал не обнаружен на сетевом адаптере, то тест автоматически сканирует соединительный разъем и кабель для их диагностики.

Функции сбора статистики позволяют в реальном масштабе времени проследить за изменением наиболее важных параметров, характеризующих «здоровье» сегментов сети. Статистика обычно собирается с разной степенью детализации по разным группам.

Сетевая статистика отображает наиболее важные статистические показатели – коэффициент использования сегмента (utilization), уровень коллизий, уровень ошибок и уровень широковещательного трафика. Превышение этими показателями определенных порогов в первую очередь говорят о проблемах в том сегменте сети, к которому подключен многофункциональный прибор.

Статистика ошибочных кадров – функция позволяет отслеживать все типы ошибочных кадров для определенной технологии. Например, для технологии Ethernet характерны следующие типы ошибочных кадров.

Укороченные кадры (Short frames). Это кадры, имеющие длину, меньше допустимой, то есть меньше 64 байт. Иногда этот тип кадров дифференцируют на два класса – просто короткие кадры (short), у которых имеется корректная контрольная сумма, и «коротышки» (runts), не имеющие корректной контрольной суммы. Наиболее вероятными причинами появления укороченных кадров являются неисправные сетевые адаптеры и их драйверы.

Удлиненные кадры (Jabbers). Это кадры, имеющие длину, превышающую допустимое значение в 1518 байт с хорошей или плохой контрольной суммой. Удлиненные кадры являются следствием затянувшейся передачи, которая появляется из-за неисправностей сетевых адаптеров.

Кадры нормальных размеров, но с плохой контрольной суммой (Bad FCS) и кадры с ошибками выравнивания по границе байта. Кадры с неверной

контрольной суммой являются следствием множества причин – плохих адаптеров, помех на кабелях, плохих контактов, некорректно работающих портов повторителей, мостов, коммутаторов и маршрутизаторов. Ошибка выравнивания всегда сопровождается ошибкой по контрольной сумме, поэтому некоторые средства анализа трафика не делают между ними различий. Ошибка выравнивания может быть следствием прекращения передачи кадра при распознавании коллизии передающим адаптером.

Кадры-призраки (ghosts) являются результатом электромагнитных наводок на кабеле. Они воспринимаются сетевыми адаптерами как кадры, не имеющие нормального признака начала кадра – 10101011. Кадры-призраки имеют длину более 72 байт, в противном случае они классифицируются как удаленные коллизии. Количество обнаруженных кадров-призраков в большой степени зависит от точки подключения сетевого анализатора. Причинами их возникновения являются петли заземления и другие проблемы с кабельной системой. Знание процентного распределения общего количества ошибочных кадров по их типам может многое подсказать администратору о возможных причинах неполадок в сети. Даже небольшой процент ошибочных кадров может привести к значительному снижению полезной пропускной способности сети, если протоколы, восстанавливающие искаженные кадры, работают с большими тайм-аутами ожидания квитанций. Считается, что в нормально работающей сети процент ошибочных кадров не должен превышать 0,01 %, то есть не более 1 ошибочного кадра из 10 000.

В некоторых многофункциональных приборах отсутствует возможность декодирования захваченных пакетов, как в анализаторах протоколов, а вместо этого собирается статистика о наиболее важных пакетах, свидетельствующих о наличии проблем в сетях. Например, при анализе протоколов стека TCP/IP собирается статистика по пакетам протокола ICMP, с помощью которого маршрутизаторы сообщают конечным

узлам о возникновении разного рода ошибок. Для ручной проверки достижимости узлов сети в приборы включается поддержка утилиты IP Ping, а также аналогичных по назначению утилит NetWare Ping и NetBIOS Ping.

1.2 Мониторинг IP сетей

Основной момент безопасности – это построение системы наблюдения за пользованием сети интернет.

Под мониторингом IP сетей будем рассматривать программно-аппаратный комплекс, позволяющий вести наблюдения за формированием распределения трафика IP и позволяющий получать широкий спектр отчетности по данному вопросу.

«Сердцем» сети интернет является маршрутизатор. Технологию построения системы мониторинга будем рассматривать на примере широко используемого оборудования фирмы Cisco. Данные для анализа может предоставить именно это устройство, поскольку маршрутизация (перенаправление) всех IP (Internet Protocol) пакетов конкретной сети производится им.

В принципе, для этих целей можно использовать несколько IP протоколов. Рассмотрим, как построить систему с использованием Telnet и, специально предложенный для этих целей фирмой Cisco, Netflow.

Прежде всего, маршрутизатор позволяет получить информацию в виде коллекции строк, содержащих разноплановую информацию, в частности IP адреса источника и получателя, количество пакетов и их суммарную величину в байтах, в случае Telnet. В случае Netflow добавляется IP интерфейса, тип пакета (цифра, телефония, телевидение и т.п.) и в дальнейшем эта спецификация может расширяться (конкретная структура зависит от версии протокола).

Для средней сети, не говоря уже о большой, количество подобных записей может достигать миллионов строк за сутки. Так если вести запись в файл, то за сутки его размер может достичь 100 Мбайт и более. В

стандартной технологии «Log» файлов обработать подобные объемы не представляется возможным, невзирая на использование развернутой системы фильтров.

Важным моментом для подобных систем является правильный выбор методики и критериев агрегирования исходной информации. Т.е. получаемые за один сеанс от маршрутизатора строки помещаются в таблицу исходной информации, предварительно синтаксически разобранными (разделив строку на ее составляющие фразы и поместив их в отдельные поля). Это необходимо по соображениям скорости и надежности первичных процессов. Далее осуществляется свертка исходной информации по заданным критериям: время первичного интегрирования, входящие и исходящие сети, тип трафика и т.д. – первичная информация. В дальнейшем, развернутому анализу подлежит именно она.

При использовании протокола Telnet, появляется необходимость использовать дополнительную базу данных содержащую сценарии взаимодействия с маршрутизатором, т.е. эмулировать диалог работы в режиме терминала. Поскольку в сценарии могут содержаться логин администратора и его пароль, такую базу данных лучше хранить отдельно от основной. Не исключено использование для этих целей настольных баз данных (MS Access, Paradox, Fox Pro и т.д.), так как объемы хранимой информации небольшие. В таком случае базу данных необходимо разместить на сервере, где располагается основной счетчик, обеспечив доступ на уровне файловой системы только административных служб. Поскольку Telnet полностью открытая сессия, желательно как можно «ближе» разместить маршрутизатор и компьютер, где установлено приложение.

На рисунке 1.2 представлена блок-схема системы IP мониторинга с использованием Telnet.

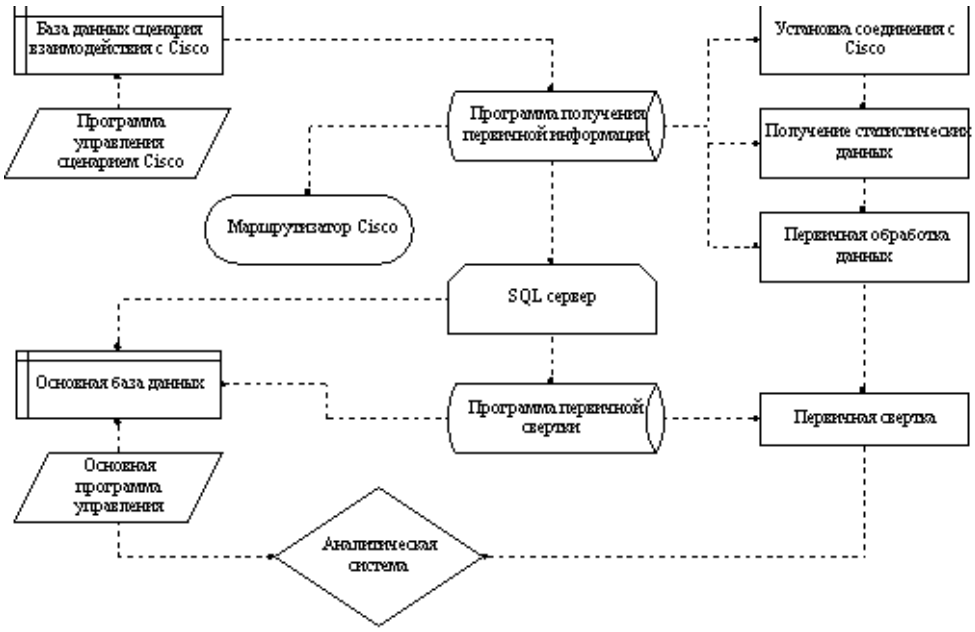


Рисунок 1.2 – Блок-схема системы IP мониторинга с использованием Telnet

Программа получения первичной информации (в случае Windows NT Server это должен быть сервис), используя базу данных сценария взаимодействия с маршрутизатором, устанавливает с последним сессию, выполняет, если необходимо соответствующие настройки, и получает первичную информацию в виде коллекции строк.

Далее, происходит синтаксический разбор информации, и в виде записей она помещается в базу данных статистических показателей. Сразу же запускается команда очистки счетчиков Cisco. Если в какой либо момент происходит ошибка, то SQL сервер откатывает транзакцию, и очистки счетчика маршрутизатора не происходит.

IP адреса более удобно хранить в виде 4-х полей по байту. Такой способ позволяет использовать активно понятие маски и избежать излишних процедур преобразования. После помещения первичной информации в базу, запускается программа первичной агрегации, которая анализирует и обрабатывает агрегаты, которыми могут быть сети, группы сетей и отдельные компьютеры. Такие программы создаются средствами SQL сервера и стартуют либо из программы получения первичной информации, либо средствами СУБД.

На каждом шаге выполнения опроса необходимо проверять безошибочность выполнения каждой операции. И в случае какого-либо сбоя всегда вернуться на предыдущий шаг, поместив в Log соответствующую запись. Для повышения надежности можно размещать программу первичной обработки на том же компьютере, где установлен сервер баз данных.

Необходимой утилитой является программа управления сценарием Cisco, которая, в сущности, является эмулятором макросов для сессии Telnet и позволяет построить правильный диалог с маршрутизатором.

Частота опроса маршрутизатора зависит от многих факторов, прежде всего от самого маршрутизатора, от величины сети и т.п., при этом может колебаться от единиц до десятков минут.

В отличие от использования Telnet, при использовании протокола Netflow (предложенного Cisco) нет необходимости в создании сессии специализированного программного обеспечения и маршрутизатора, поскольку в его основе лежит UDP. Сущность заключается в следующем: маршрутизатор на определенный порт компьютера постоянно высылает данные, при этом не используется верификация (подтверждение) их получения.

Маршрутизатор посылает на выделенный порт специализированного компьютера исходные данные. Сервисный компьютер «слушает» порт и, как только приходит информация, фиксирует данные, обрабатывает их, производя синтаксический разбор, и помещает в базу данных. Запуск программы свертки первичной информации в этом случае осуществляется только SQL сервером. Причем здесь также необходимо оптимизировать объемы хранимой информации и времена ее обработки.

На рисунке 1.3 представлена блок-схема системы IP мониторинга с использованием Netflow.

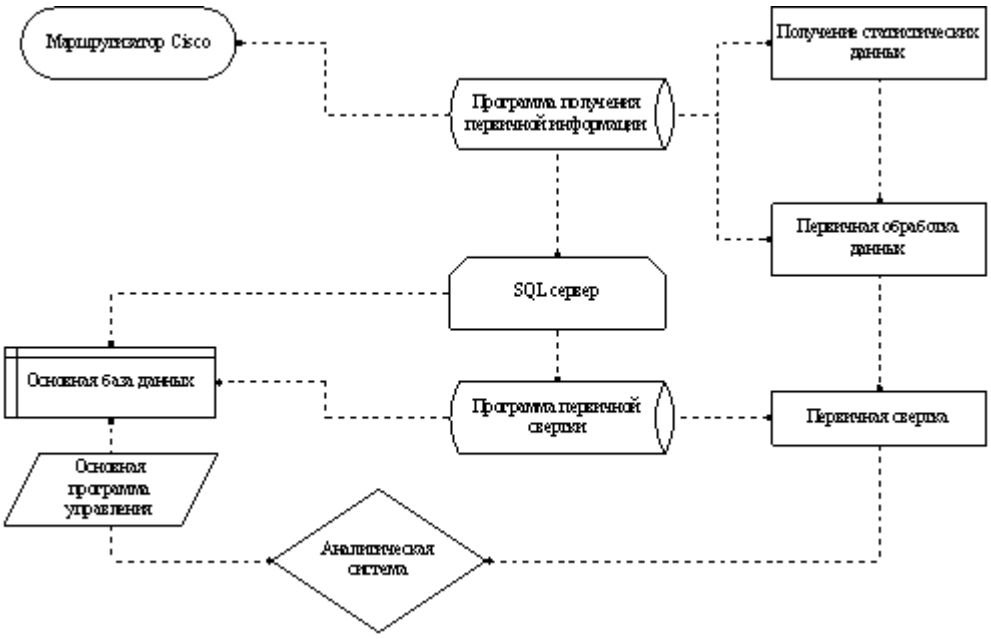


Рисунок 1.3 – Блок-схема системы IP мониторинга с использованием Netflow

К сожалению, в случае возникновения аварийных ситуаций происходит потеря статистических данных. Однако, используя систему записи ошибок в log файл можно рассчитывать коэффициент просчетов, который в дальнейшем использовать для коррекции данных.

В отличие от использования Telnet, при использовании Netflow невозможно вести проверку соединения с Cisco. Поэтому возникает необходимость во внешних средствах проверки сетевых соединений (например, с использованием Ping) или в случае активной сети по времени последнего обсчета.

Общим в обоих случаях является аналитическая система, которая позволяет построить различные расчетные схемы, ввести различные критерии анализа формирования IP трафика, контролировать входящий и исходящий трафик любой сети вплоть до отдельного хоста и т.д. На практике хорошие результаты показало использование OLAP технологий как основы аналитической системы. Для управления структурой данных аналитической системы необходима соответствующая утилита.

Приведем основные отличия использования протоколов Telnet и Netflow:

– отсутствие создания сессии при использовании Netflow устраняет необходимость создания специальных программных структур управляемых сценарием. Фактически, в случае наличия нескольких маршрутизаторов обрабатываемый трафик определяется только теми, для которых определены команды подсчета и поставки информации. С другой стороны, этот фактор в свою очередь обязывает создавать специализированные средства мониторинга целостности сети (например, ping);

– Netflow возвращает более расширенные сведения, интерфейс, тип пакетов и т.д. Это позволит мониторить различные составляющие IP: компьютерные сети, телефонию, телевидение и т.д. – на различных интерфейсах;

– при использовании Netflow значительно снижается коэффициент технологических ошибок, поскольку при использовании Telnet возникают просчеты за счет разности времен получения статистики и обнуления счетчиков;

– в случае Netflow существует потребность в спецификации формата данных в зависимости от используемого BIOS маршрутизатора. Т.е. в зависимости от используемой версии Netflow требуется и соответствующий обработчик. Функцию обработчик можно вынести во внешние структуры (например, dll);

– в случае Netflow требуется более качественная сеть, нежели в случае использования Telnet. В случае нарушения сетевых соединений система никаким образом на это не среагирует, если не предусмотрены специальные средства.

Использование системы мониторинга IP сетей не заканчивается только наблюдениями за использованием интернет. На ее основе можно строить развернутые учетно-расчетные системы для клиентов провайдеров сети интернет. Можно оценивать входящий и исходящий трафик, разделяя его по государственному принципу. В случае Netflow можно строить

расчетные системы по различным спектрам перспективных услуг – IP телефонии, IP телевидения и т.д., что позволит строить достаточно гибкие финансовые схемы оплаты интернет услуг. На основе предлагаемой системы возможно построение систем блокирования и предупреждения. Однако сама по себе система мониторинга IP сетей не является самодостаточной для обеспечения полной безопасности. Она является составной частью общей информационной системы безопасности предприятия. И только разумное сочетание методик и средств позволит системному администратору спать спокойно.

1.3 Протокол SNMP

Протокол SNMP работает на базе транспортных возможностей UDP (возможны реализации и на основе TCP) и предназначен для использования сетевыми управляющими станциями. Он позволяет управляющим станциям собирать информацию о положении в сети интернет. Протокол определяет формат данных, а их обработка и интерпретация остаются на усмотрение управляющих станций или менеджера сети. SNMP-сообщения не имеют фиксированного формата и фиксированных полей. При своей работе SNMP использует управляющую базу данных (MIB – Management Information Base, RFC 1213, RFC 1212).

Алгоритмы управления в интернет обычно описывают в нотации ASN.1 (Abstract Syntax Notation). Все объекты в интернет разделены на 10 групп и описаны в MIB: система, интерфейсы, обмены, трансляция адресов, IP, ICMP, TCP, UDP, EGP, SNMP. В группу «система» входит название и версия оборудования, операционной системы, сетевого программного обеспечения и прочее. В группу «интерфейсы» входит число поддерживаемых интерфейсов, тип интерфейса, работающего под IP (Ethernet, LAPB etc.), размер дейтограмм, скорость обмена, адрес интерфейса. IP-группа включает в себя время жизни дейтограмм, информация о фрагментации, маски субсетей и т.д. В TCP-группу входит алгоритм

повторной пересылки, максимальное число повторных пересылок и прочее. Ниже приведена таблица команд (PDU – Protocol Data Unit) SNMP:

Таблица 1.1 – Команды SNMP

Команда SNMP	Тип PDU	Назначение
GET-request	0	Получить значение указанной переменной или информацию о состоянии сетевого элемента
GET_next_request	1	Получить значение переменной, не зная точного ее имени (следующий логический идентификатор на дереве MIB)
SET-request	2	Присвоить переменной соответствующее значение. Используется для описания действия, которое должно быть выполнено
GET response	3	Отклик на GET-request, GET_next_request и SET-request. Содержит также информацию о состоянии (коды ошибок и другие данные)
TRAP	4	Отклик сетевого объекта на событие или на изменение состояния
GetBulkRequest	5	Запрос пересылки больших объемов данных, например, таблиц
InformRequest	6	Менеджер обращает внимание партнера на определенную информацию в MIB
SNMPv3-Trap	7	Отклик на событие (расширение по отношению v1 и v2)
Report	8	Отчет (функция пока не задана)

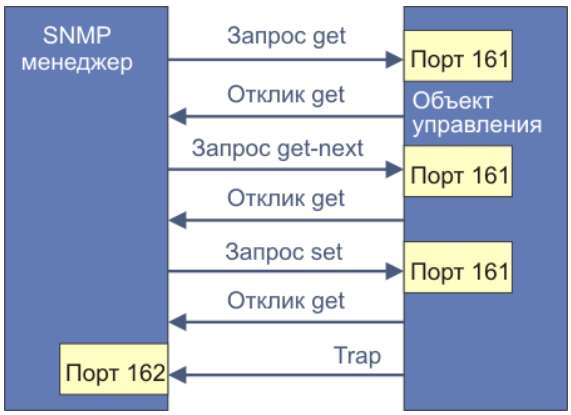


Рисунок 1.4 – Схема запросов/откликов SNMP

Формат SNMP-сообщений, вкладываемых в UDP-дейтограммы, имеет вид, показанный на рисунке 1.5.

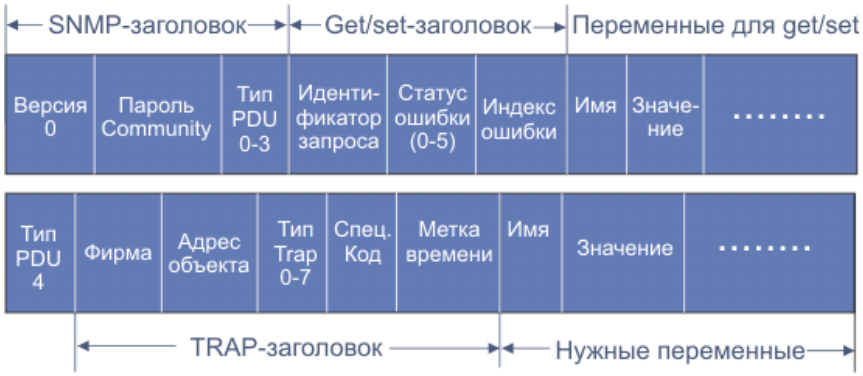


Рисунок 1.5 – Формат SNMP-сообщений, вкладываемых в UDP-дейтограммы

Поле версия содержит значение, равное номеру версии SNMP минус один. Поле пароль (community – определяет группу доступа) содержит последовательность символов, которая является пропуском при взаимодействии менеджера и объекта управления. Обычно это поле содержит 6-байтовую строку public, что означает общедоступность. Для запросов GET, GET-next и SET значение идентификатора запроса устанавливается менеджером и возвращается объектом управления в отклике GET, что позволяет связывать в пары запросы и отклики. Поле фирма (enterprise) = sysobjectid объекта. Поле статус ошибки характеризуется целым числом, присланным объектом управления (таблица 1.3).

Таблица 1.2 – Номера и назначения используемых портов

Назначение	Порт	Пояснение

SNMP	161/TCP	Simple Network Management Protocol
SNMP	162/TCP	Trap
SMUX	199/TCP	SNMP Unix Multiplexer
SMUX	199/UDP	SNMP Unix Multiplexer
synoptics-relay	391/TCP	SynOptics SNMP Relay Port
synoptics-relay	391/UDP	SynOptics SNMP Relay Port
Agentx	705/TCP	AgentX
snmp-tcp-port	1993/TCP	cisco SNMP TCP port
snmp-tcp-port	1993/UDP	cisco SNMP TCP port

Таблица 1.3 – Коды ошибок

Статус ошибки	Имя ошибки	Описание
0	Noerror	Все в порядке
1	Toobig	Объект не может уложить отклик в одно сообщение
2	Nosuchname	В операции указана неизвестная переменная
3	badvalue	В команде set использована недопустимая величина или неправильный синтаксис
4	Readonly	Менеджер попытался изменить константу
5	Generr	Прочие ошибки

Если произошла ошибка, поле индекс ошибки (error index) характеризует, к какой из переменных это относится. error index является указателем переменной и устанавливается объектом управления не равным нулю для ошибок badvalue, readonly и nosuchname. Для оператора TRAP (тип PDU=4) формат сообщения меняется. Таблица типов TRAP представлена ниже.

Таблица 1.4 – Коды TRAP

Тип TRAP	Имя TRAP	Описание

0	Coldstart	Установка начального состояния объекта
1	Warmstart	Восстановление начального состояния объекта
2	Linkdown	Интерфейс выключился. Первая переменная в сообщении идентифицирует интерфейс
3	Linkup	Интерфейс включился. Первая переменная в сообщении идентифицирует интерфейс
4	Authenticationfailure	От менеджера получено snmp-сообщение с неверным паролем (community)
5	EGPneighborloss	R$GP-партнер отключился. Первая переменная в сообщении определяет IP-адрес партнера

Для тип TRAP 0-4 поле специальный код должно быть равно нулю. Поле временная метка содержит число сотых долей секунды (число тиков) с момента инициализации объекта управления. Так, прерывание coldstart выдается объектом через 200 мс после инициализации.

В последнее время широкое распространение получила идеология распределенного протокольного интерфейса DPI (Distributed Protocol Interface). Для транспортировки snmp-запросов может использоваться не только UDP-, но и TCP-протокол. Это дает возможность применять SNMP–протокол не только в локальных сетях. Форматы SNMP-DPI-запросов (версия 2.0) описаны в документе RFC 1592. Пример заголовка snmp-запроса приведен на рисунке 1.6 (изображенные поля образуют единый массив).

Рисунок 1.6 – Формат заголовка SNMP-запроса

Поле Флаг=0x30 является признаком ASN.1-заголовка. Коды Ln – представляют собой длины полей, начинающиеся с байта, который следует за кодом длины, вплоть до конца сообщения-запроса (n – номер поля длины), если не оговорено другое. Так L1 – длина пакета-запроса, начиная с T1 и до конца пакета, а L3 – длина поля пароля. Субполя Tn – поля типа следующего за ними субполя запроса. Так T1=2 означает, что поле характеризуется целым числом, а T2=4 указывает на то, что далее следует пароль (поле community, в приведенном примере = public). Цифры под рисунками означают типовые значения субполей. Код 0xA – является признаком GET-запроса, за ним следует поле кода PDU. Блок субполей идентификатора запроса служит для тех же целей, что и другие идентификаторы – для определения пары запрос-отклик. Собственно идентификатор запроса может занимать один или два байта, что определяется значением L. CO – статус ошибки (CO=0 – ошибки нет); TM – тип MIB-переменной (в приведенном примере = 0x2B); ИО – индекс ошибки. Цифровой код MIB-переменной отображается последовательностью цифровых субполей, характеризующих переменную, например: переменная 1.3.6.1.2.1.5 (в символьном выражении iso.org.dod.internet.mgmt.mib.icmp) характеризуется последовательностью кодов 0x2B 0x06 0x01 0x02 0x01 0x05 0x00.

Начиная с января 1998 года, выпущен набор документов, посвященных SNMPv3. В этой версии существенно расширена функциональность, разработана система безопасности. В данной версии реализована модель, базирующаяся на процессоре SNMP (SNMP Engine) и содержащая несколько подсистем (диспетчер, система обработки сообщений, безопасности и управления доступом, рисунок 1.7). Перечисленные подсистемы служат основой функционирования генератора и обработчика команд, отправителя и обработчика уведомлений и прокси-сервера (Proxy Forwarder), работающих на прикладном уровне. Процессор SNMP

идентифицируется с помощью snmpEngineID. Обеспечение безопасности модели работы SNMP упрощается обычно тем, что обмен запросами-откликами осуществляется в локальной сети, а источники запросов-откликов легко идентифицируются.

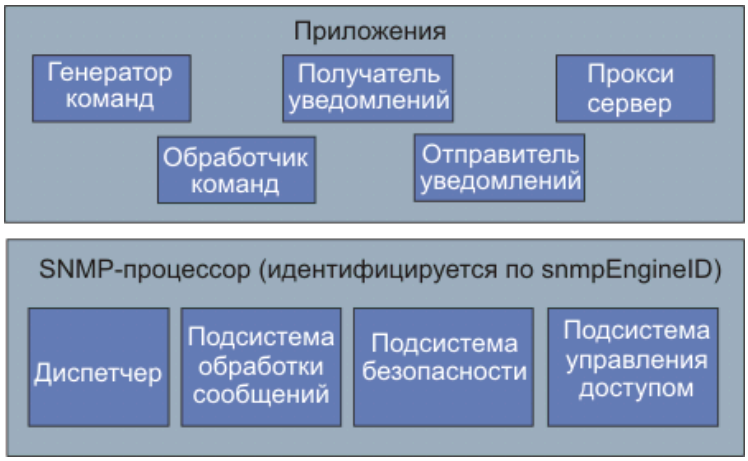


Рисунок 1.7 – Архитектура сущности SNMP (SNMP-entity)

Компоненты процессора SNMP перечислены в таблице 1.5 (RFC 2571 и RFC 2573).

Таблица 1.5 – Компоненты процессора SNMP

Название компонента	Функция компонента
Диспетчер	Позволяет одновременную поддержку нескольких версий SNMP-сообщений в процессоре SNMP. Этот компонент ответственен за прием протокольных блоков данных (PDU), за передачу PDU подсистеме обработки сообщений, за передачу и прием сетевых SNMP-сообщений
Подсистема обработки сообщений	Ответственна за подготовку сообщений для отправки и за извлечение данных из входных сообщений
Подсистема безопасности	Предоставляет услуги, обеспечивающие безопасность: аутентификацию и защищенность сообщений от перехвата и искажения. Допускается реализация нескольких моджелей

	безопасности
Подсистема управления доступом	Предоставляет ряд услуг авторизации, которые могут использоваться приложениями для проверки прав доступа
Генератор команд	Инициирует SNMP-запросы Get, GetNext, GetBulk или Set, предназначенные для локальной системы, которые могут использоваться приложениями для проверки прав доступа
Обработчик команд	Воспринимает SNMP-запросы Get, GetNext, GetBulk или Set, предназначенные для локальной системы, это индицируется тем, что contextEngeneID в полученном запросе равно соответствующему значению в процессоре SNMP. Приложение обработчика команд выполняет соответствующие протокольные операции, генерирует сообщения отклика и посылает их отправителю запроса
Отправитель уведомлений	Мониторит систему на предмет выявления определенных событий или условий и генерирует сообщения Trap или Inform. Источник уведомлений должен иметь механизм определения адресата таких сообщений, а также параметров безопасности
Получатель уведомлений	Прослушивает сообщения уведомления и формирует сообщения-отклики, когда приходит сообщение с PDU Inform
Прокси-сервер	Переадресует SNMP-сообщения. Реализация этого модуля является опционной

На рисунке 1.8 показан формат сообщений SNMPv3, реализующий модель безопасности UBM (User-Based Security Model).

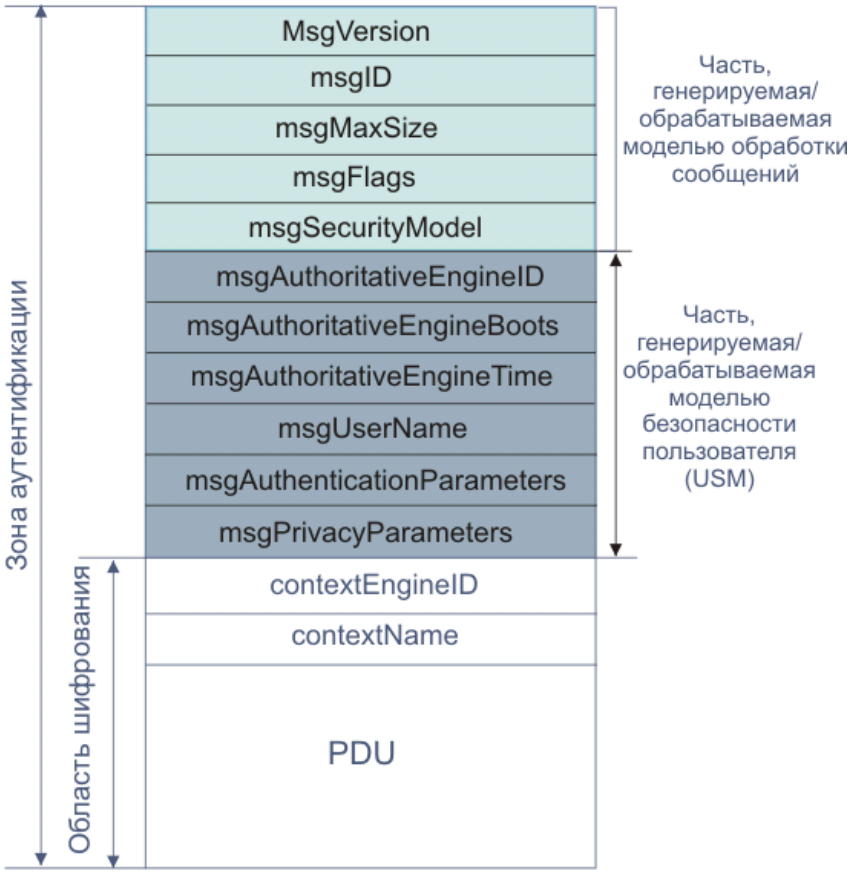


Рисунок 1.8 – Формат сообщений SNMPv3 с UBM

Модель безопасности USM (User-Based Security Model) использует концепцию авторизованного сервера (authoritative Engine). При любой передаче сообщения одна или две сущности, передатчик или приемник, рассматриваются в качестве авторизованного SNMP-сервера.

Своевременность сообщения определяется с учетом показания часов авторизованного сервера. Когда авторизованный сервер посылает сообщение (Trap, Response, Report), оно содержит текущее показание часов, так что неавторизованный получатель может синхронизовать свои часы. Когда неавторизованный сервер посылает сообщение (Get, GetNext, GetBulk, Set, Inform), он помещает туда текущую оценку показания часов места назначения, позволяя получателю оценить своевременность прихода сообщения.

Процесс локализации ключа, описанный ниже, устанавливает единственного принципала, который может владеть ключом. Ключи могут

храниться только в авторизованном сервере, исключая хранение нескольких копий ключа в разных местах.

Когда исходящее сообщение передается процессором сообщений в USM, USM заполняет поля параметров безопасности в заголовке сообщения.

Механизм аутентификации в SNMPv3 предполагает, что полученное сообщение действительно послано принципалом, идентификатор которого содержится в заголовке сообщения, и он не был модифицирован по дороге. Для реализации аутентификации каждый из принципалов, участвующих в обмене, должен иметь секретный ключ аутентификации, общий для всех участников (определяется на фазе конфигурации системы). В посылаемое сообщение отправитель должен включить код, который является функцией содержимого сообщения и секретного ключа. Одним из принципов USM является проверка своевременности сообщения (смотри выше), что делает маловероятной атаку с использованием копий сообщения.

Система конфигурирования агентов позволяет обеспечить разные уровни доступа к MIB для различных SNMP-менеджеров. Это делается путем ограничения доступа некоторым агентам к определенным частям MIB, а также с помощью ограничения перечня допустимых операций для заданной части MIB. Такая схема управления доступом называется VACM (View-Based Access Control Model). В процессе управления доступом анализируется контекст (vacm Context Table), а также специализированные таблицы vacm Security To Group Table, vacm Tree Family Table и vacm Access Table.

SNMP-протокол служит примером системы управления, где для достижения нужного результата выдается не команда, а осуществляется обмен информацией, решение же принимается «на месте» в соответствии с полученными данными. Внедрены подсистемы аутентификации, информационной безопасности и управления доступом.

Таблица 1.6 – RFC-документы по протоколу SNMP

Название	Дата	Наименование документа

STD-15	май 1990 г	Simple Network Management Protocol (RFC 1157)
STD-16	май 1990 г	Structure and Identification of Management Information for TCP/IP-based Internets (RFC 1155)
SNMPv2		
RFC 1902	январь 1996 г	Structure of Management Information for Version 2 of the Simple Network Management Protocol (SNMPv2)
RFC 1903	январь 1996 г	Textual Conventions for Version 2 of the Simple Network Management Protocol (SNMPv2)
RFC 1904	январь 1996 г	Conformance Statements for Version 2 of the Simple Network Management Protocol (SNMPv2)
RFC 1905	январь 1996 г	Protocol Operations for Version 2 of the Simple Network Management Protocol (SNMPv2)
RFC 1906	январь 1996 г	Transport Mappings for Version 2 of the Simple Network Management Protocol (SNMPv2)
RFC 1907	январь 1996 г	Management Information Base for Version 2 of the Simple Network Management Protocol (SNMPv2)
RFC 1908	январь 1996 г	Coexistence between Version 1 and Version 2 of the Internet-standard Network Management Framework
SNMPv3		
RFC 2570	апрель 1999 г	Introduction to Version 3 of the Internet-standard Network Management Framework

Окончание таблицы 1.6

Название	Дата	Наименование документа
RFC2571	апрель 1999 г	An Architecture for Describing SNMP Management Frameworks
RFC2572	апрель 1999 г	Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)

RFC2573	апрель 1999 г	SNMP Applications
RFC2574	апрель 1999 г	The User-Based Security Model for Version 3 of the Simple Network Management Protocol (SNMPv3). Безопасность уровня сообщений (MD5 и SHA + DES CBC)
RFC2575	апрель 1999 г	View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)

1.4 Структура и типы блоков управляющей информации (MIB)

Вся управляющая информация для контроля ЭВМ и маршрутизаторами интернет концентрируется в базе данных MIB (Management Information Base, RFC 1213 или STD0017). Именно эти данные используются протоколом SNMP. Система SNMP состоит из трех частей: менеджера SNMP, агента SNMP и базы данных MIB. Агент SNMP должен находиться резидентно в памяти объекта управления. SNMP-менеджер может быть частью системы управления сетью NMS (Network Management System), что реализуется, например, в маршрутизаторах компании Cisco (CiscoWorks).

MIB определяет, например, что IP программное обеспечение должно хранить число всех октетов, которые приняты любым из сетевых интерфейсов, управляющие программы могут только читать эту информацию.

Согласно нормативам MIB управляющая информация делится на восемь категорий.

Таблица 1.7 – MIB-категории

MIB-категория	Описание	Код
system	Операционная система ЭВМ или маршрутизатора	1
Interfaces	Сетевой интерфейс	2
addr.trans	Преобразование адреса (напр., с помощью ARP)	3

IP	Программная поддержка протоколов интернет	4
ICMP	Программное обеспечение ICMP-протокола	5
TCP	Программное обеспечение TCP-протокола	6
UDP	Программное обеспечение UDP-протокола	7
EGP	Программное обеспечение EGP-протокола	8
SNMP	Программное обеспечение SNMP-протокола	11

Таблица 1.8 – Системные переменные MIB

Системная переменная	Описание	Код
Sysdescr	Текстовое описание объекта	1
Sysobjectid	Идентификатор производителя в рамках дерева 1.3.6.1.4.1	2
Sysuptime	Время с момента последней загрузки системы (timeticks)	3
Syscontact	Имя системного менеджера и способы связи с ним	4
Sysname	Полное имя домена	5
Syslocation	Физическое местоположение системы	6
Sysservice	Величина, которая характеризует услуги, предоставляемые узлом (сумма номеров уровней модели OSI)	7

Каждый протокол (например, IP) имеет свою таблицу преобразования адресов. Для IP это ipnettomediatable. Способ пропечатать эту таблицу с помощью программы SNMPI описан ниже.

MIB II содержит управляемые объекты, принадлежащие к группе snmp. SNMP-группа предоставляет информацию о SNMP-объектах, информационных потоках, о статистике ошибок (таблица 1.9).

Таблица 1.9 – Статистика ошибок SNMP

Название объекта	Описание	Код
snmpInPkts	Число пакетов, полученных от слоя, расположенного ниже SNMP	1
snmpOutPkts	Число пакетов доставленных от SNMP к нижележащему слою	2
snmpInBadVersions	Индицирует число PDU, полученных с ошибкой в поле версия	3
snmpInBadCommunityNames	Индицирует число PDU, полученных с нечитаемым или нелегальным именем community	4
snmpInBadCommunityUses	Полное число SNMP-пакетов, полученных с нечитаемым или нелегальным значение операции для данного имени community	5
snmpInAsnParsErrs	Указывает полное число ошибок ASN.1 или BER, которые не могут быть обработаны во входных SNMP-сообщениях	6
snmpInTooBigs	Указывает число полученных PDU со слишком большим значением поля статус ошибки	8
snmpInNoSuchNames	Указывает число PDU, полученных с индикацией ошибки в поле nosuchname	9
snmpInBadValues	Указывает число PDU, полученных с индикацией ошибки в поле badvalue	10

Окончание таблицы 1.9

Название объекта	Описание	Код
snmpInReadOnlys	Указывает число PDU, полученных с индикацией ошибки в поле readonly	11
snmpNnGenErrs	Указывает число PDU, полученных с generr полем	12

snmpInTotalReqVar	Указывает число объектов MIB, которые были восстановлены	13
snmpInTotalSetVars	Указывает число объектов MIB, которые были изменены	14
snmpInGetRequests	Указывает число соответствующих PDU, которые были получены	15
snmpInGetNexts	Указывает полное число PDU с запросами GetNext	16
snmpInSetRequests	Указывает полное число PDU, полученных с запросами SET	17
snmpInGetResponses	Указывает полное число PDU, полученных с откликами на запросы	18
snmpInTraps	Указывает полное число, полученных и успешно обработаных TRAP	19
snmpOutTooBig	Указывает число посланных PDU с полем toobig	20
snmpOutNoSuchName	Указывает число посланных PDU с полем nosuchname	21
snmpOutBadValues	Указывает число посланных PDU с полем badvalue	22
snmpOutGenErrs	Указывает число посланных PDU с полем genErrs	24
snmpOutGetRequests	Указывает число посланных PDU Get-Request	25
snmpOutGetNexts	Указывает число посланных PDU Get-NEXT	26
snmpOutSetRequests	Указывает число посланных PDU SET	27
snmpOutGetResponses	Указывает число посланных PDU откликов	28
snmpOutTraps	Указывает число посланных PDU TRAPs	29
snmpEnableAuthTraps	Говорит о том, разрешены или нет ловушки (TRAPS)	30

В интернет MIB каждый объект должен иметь имя (object identifier), синтаксис и метод кодировки.

Стандарт ASN.1 определяет форму представления информации и имен. Имена переменных MIB соответствуют в свою очередь стандартам ISO и CCITT. Структура имен носит иерархический характер, отображенный на рисунке 1.9.

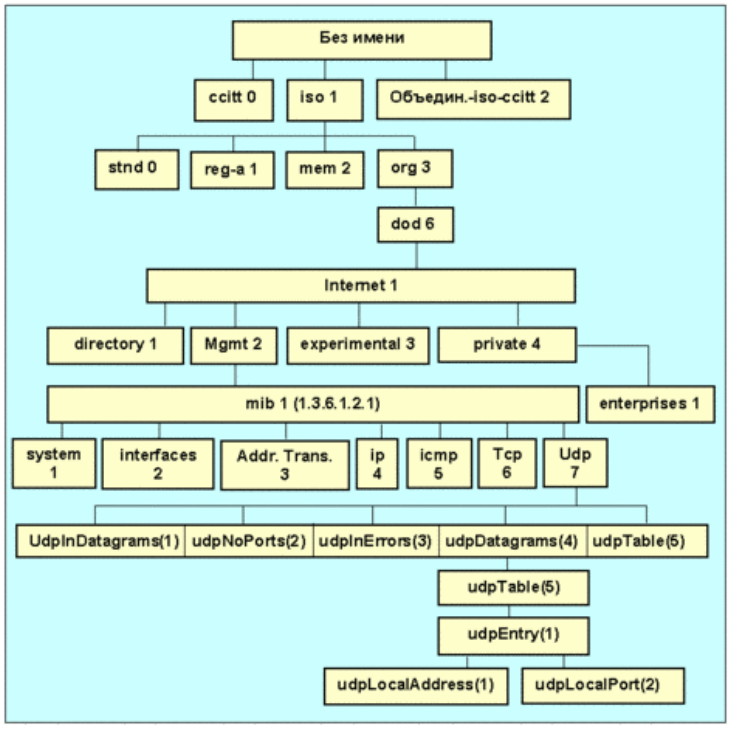


Рисунок 1.9 – Структура идентификаторов переменных в MIB

Помимо стандартного набора переменных и таблиц MIB возможно использование индивидуальных расширений этой базы данных. Это можно продемонстрировать на примере MIB маршрутизаторов Cisco (рисунок 1.10).

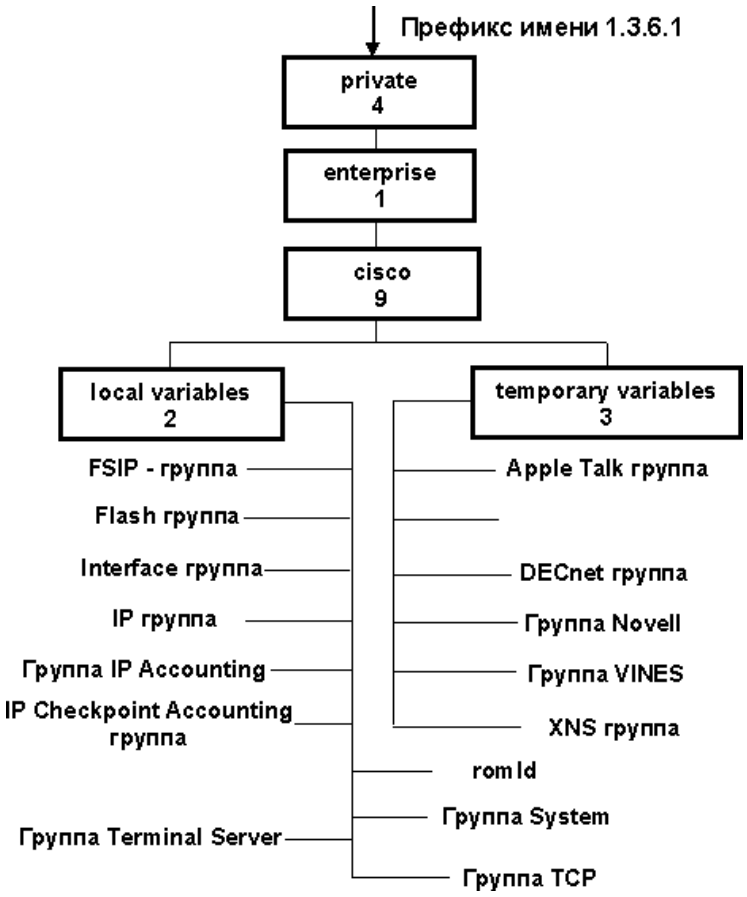


Рисунок 1.10 – Расширение базы данных MIB маршрутизаторов Cisco

Маршрутизаторы Cisco поддерживают две базы данных: active accounting и checkpoint accounting. В первую заносятся текущие результаты измерения входящего и исходящего трафика. Эти результаты копируются в базу данных checkpoint accounting и, если там уже имеются предыдущие данные, они объединяются. Для очистки базы данных checkpointed database выдается команда clear IP accounting, а для базы checkpoint – clear IP accounting checkpoint (для использования этих команд необходимы системные привилегии). Объем памяти, выделяемой для этих баз данных задается командой IP accounting-threshold <значение>, по умолчанию максимальное число записей в базе данных равно 512.

Синтаксис каждого объекта описывается в рамках ASN.1 и показывает побитовое представление объекта. Кодирование объекта характеризует то, как тип объекта отображается через его синтаксис и передается по телекоммуникационным каналам. Кодирование производится в

соответствии с базовыми правилами кодирования asn.1. Все описания объектов базируются на типовых шаблонах и кодах asn.1 (RFC 1213).

Формат шаблона показан ниже:

– object (Объект) – имя типа объекта с соответствующим ему идентификатором объекта (object identifier);

– syntax (Синтаксис) – asn.1 описание синтаксиса типа объекта;

– definition (Определение) – текстовое описание типа объекта;

– access (доступ) – опции доступа;

– status (состояние) – статус типа объекта.

Маршруты также являются объектами MIB. Согласно требованиям к MIB, каждому маршруту в этой базе соответствует запись, схема которой приведена ниже на рисунке 1.11.

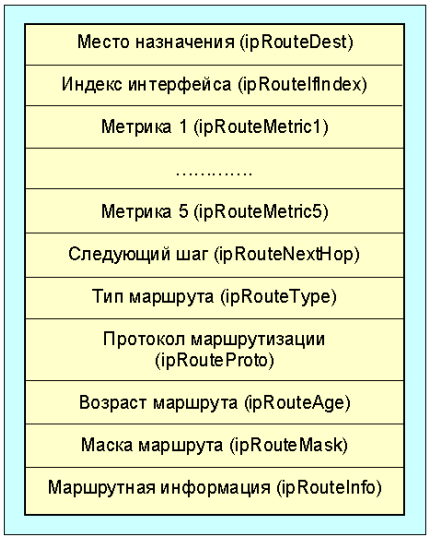


Рисунок 1.11 – Формат записи маршрутной таблицы в MIB

Поле место назначения представляет собой IP-адрес конечной точки маршрута. Поле индекс интерфейса определяет локальный интерфейс (физический порт), через который можно осуществить следующий шаг по маршруту. Следующие пять полей (метрика от 1 до 5) характеризуют оценку маршрута. В простейшем случае, например для протокола RIP, достаточно было бы одного поля. Но для протокола OSPF необходимо 5 полей, разные TOS (Type Of Service). Поле следующий шаг представляет собой IP-адрес следующего маршрутизатора. Поле тип маршрута имеет значение 4 для

опосредованного достижения места назначения; 3 – для прямого достижения цели маршрута; 2 – для нереализуемого маршрута и 1 – для случаев отличных от вышеперечисленных.

Поле протокол маршрутизации содержит код протокола. Для RIP этот код равен 8, для OSPF – 13, для BGP – 14, для IGMP – 4, для прочих протоколов 1. Поле возраст маршрута описывает время в секундах, прошедшее с момента последней коррекции маршрута. Следующее поле – маска маршрута используется для выполнения логической побитовой операции. И над адресом в IP-дейтограммы перед сравнением результата с кодом, хранящимся в первом поле записи (место назначения). Последнее поле маршрутная информация содержит код, зависящий от протокола маршрутизации и обеспечивающий ссылки на соответствующую информацию в базе MIB.

2 Выбор программного обеспечения

2.1 Сравнение Open Source систем мониторинга

Свободно распространяемая система Cacti была создана специально для решения задач мониторинга сетевого оборудования и компьютеров, подключенных к сети. Она предоставляет пользователю удобный веб-интерфейс к утилите RRDTool, предназначенной для работы с круговыми базами данных (Round Robin Database), которые используются для хранения информации об изменении одной или нескольких величин за определенный промежуток времени.

Интерфейс отображения статистики, собранной с сетевых устройств, представлен в виде дерева, структура которого задается самим пользователем. Как правило, графики группируют по определенным критериям, причем один и тот же график может присутствовать в разных ветвях дерева (например, трафик через сетевой интерфейс сервера – в той, которая посвящена общей картине интернет-трафика компании, и в ветви с параметрами данного устройства). Есть вариант просмотра заранее составленного набора графиков, и есть режим предпросмотра. Каждый из графиков можно рассмотреть отдельно, при этом он будет представлен за

последние день, неделю, месяц и год. Возможно самому выбрать временной промежуток, за который будет сгенерирован график, причем сделать это можно, как указав календарные параметры, так и просто выделив мышкой определенный участок на нем.

Nagios – это приложение, предназначенное для выполнения мониторинга систем и сетей. Оно следит за назначенными приложениями и службами и генерирует оповещения в зависимости от поведения наблюдаемых служб. До какого-то времени проект был известен как NetSaint. В настоящий момент, хотя сайт NetSaint работает, дальнейшая разработка проекта продолжается под именем Nagios.

Nagios позволяет отследить разнообразные отказы сетевых сервисов, будь то отсутствие активности SMTP- или POP-сервера, отказы веб-сервера или неполадки на какой-либо из рабочих станций в сети. С помощью механизмов удаленного запуска тестовых процедур можно контролировать свободное место и другие критичные для работоспособности параметры вычислительных ресурсов. Возможности этой системы расширяемы и достаточно масштабируемы. Ее можно применять как для мониторинга одного сервера, выпускающего сеть небольшой организации, состоящую всего из трех компьютеров, в интернет, так и для контроля нескольких десятков компьютеров, выполняющих различные задачи. Для этого изначально в системе введены уровни абстрагирования от отдельных вычислительных ресурсов и пользователей. Это позволяет с помощью минимального количества изменений в конфигурации изменять получателей определенных типов сообщений о недоступности сервисов, что весьма удобно при постоянной ротации административного персонала системы и при учете изменений продолжительности рабочего дня отдельных администраторов.

OpenNMS – система мониторинга сетевой инфраструктуры уровня предприятия, распространяемая по модели свободного программного

обеспечения (Open Source). Кроме обычной для Open Source-проектов поддержки сообществом пользователей, производитель предоставляет многоуровневое коммерческое сопровождение продукта: от внедрения до обеспечения технической поддержки 24x7 и обучения персонала. Данная система реализована на Java, поэтому появляется такое положительное качество, как кроссплатформенность.

Теоретически OpenNMS может запуститься на любой платформе, поддерживающей Java SDK 1.4 и выше. Также к положительным качествам можно отнести модульность системы и возможность развертывания частей системы на раздельных серверах (СУБД, демоны сбора статистики и веб-интерфейс могут быть разнесены).

Система OpenNMS отвечает за мониторинг функционирующих в сетевой инфраструктуре сервисов, таких как Web, DNS, DHCP, сервисы СУБД (Oracle, MSSQL, PostgreSQL и др.), информация о состоянии сетевых устройств также доступна. В системе упрощены способы добавления новых сетевых устройств для мониторинга, и общий принцип работы основан на автоматическом обнаружении (discovery) сетевых устройств. Обнаружение состоит из двух частей – определение интерфейсов (IP-адресов) и определение функционирующих на этих интерфейсах сервисов. Определение интерфейсов осуществляется на основе протокола ICMP (Ping), а определение сервисов с помощью сборщиков (collectors).

Основной единицей мониторинга системы является интерфейс (interface), который уникально определяется на основе IP-адреса. Сервисы (services) привязаны к интерфейсам, а интерфейсы, расположенные на одном устройстве, группируются в узел (node).

Следующая таблица позволяет оценить возможности различных систем для мониторинга/управления сетью.

Таблица 2.1 – Сравнение систем мониторинга

Функции	Cacti	Nagios	OpenNMS

Диаграммы	Да	Да	Да
Отчеты SLA	Нет	Через плагин	Да
Логическое группирование	Нет	Да	Нет
Trending (тенденции)	Да	Да	Да
Trend Prediction (прогнозирование тенденции)	Неизвестно	Нет	Неизвестно

Окончание таблицы 2.1

Функции	Cacti	Nagios	OpenNMS
Автоматический Discovery	Через плагин	Через плагин	Да
Агент	Нет	Да	Да
SNMP	Да	Через плагин	Да
Syslog	Нет	Через плагин	
Внешние скрипты	Да	Да	Да
Плагины	Да	Да	Да
Уровень создания плагинов	Средний	Легкий	Неизвестно
Триггеры / Тревоги	Да	Да	Да
Доступ через Web	Полный доступ	Просмотр, Отчеты, Управление	Полный доступ

Распределенный мониторинг	Неизвестно	Да	Да
Инвентаризация	Нет	Через плагин	Да
Метод хранения данных	RRDtool, MySQL, PostgreSQL	Плоская база данных, SQL	RRDtool, PostgreSQL
Лицензия	GNU GPL	GNU GPL	GNU GPL
Карты	Через плагин (Weathermap)	Динамические и настраиваемые	Да
Управление доступом	Неизвестно	Да	Неизвестно
События	Неизвестно	Да	Да
Язык	PHP (requirement)	C	Java

2.2 Система мониторинга Cacti

Любая система, предназначенная для решения серьезных задач, требует обязательного наблюдения за ее работой, анализа эффективности и тщательного разбора полетов в случае успеха либо неудачи внедрения того или иного новшества, изменения конфигурации. Это возможно лишь в том случае, когда у вас есть подробная информация о том, «как это было раньше» и «как это есть сейчас», то есть о состоянии системы в различные моменты времени. Свободно распространяемая система Cacti была создана специально для решения подобных задач.

Система обслуживает ряд устройств, к которым есть доступ по сети. С устройством ассоциированы хранилища данных. Хранилище создается на основе шаблона данных, который задает соответствие входных величин (полученных из SNMP-запросов или из скриптов) полям в базе данных и устанавливает дополнительные параметры хранения этих величин.

2.3 RRD (Round Robin Database). Промышленный стандарт логирования и отображения графиков

RRDtool – набор утилит для работы с RRD (Round-robin Database, Кольцевая база данных). Созданы Тоби Отикером (Tobi Oetiker) для хранения и обработки динамических (изменяющихся во времени) последовательностей данных, таких как сетевой трафик, пропускная способность сети, температура, загрузка ЦПУ. Вся информация хранится в кольцевой базе данных, ячейки которой задействуются циклически, в связи с чем размер БД остается постоянным. Заложенные алгоритмы усредняют результат, таким образом, можно охватить больший промежуток времени при малых размерах баз. Хотя именно поэтому RRDTool нельзя использовать там, где нужны точные результаты, например в биллинговой системе. Кроме того, за большую гибкость в работе приходится платить отсутствием единого конфигурационного файла и некоторой сложностью в настройках, но эту проблему стараются решить за счет использования различного рода дополнений. RRDtools, помимо прочего, включают в себя возможность графического отображения хранимой информации. Данный набор утилит распространяется под лицензией GNU GPL.

Объем хранимых данных не увеличивается со временем (ячейки хранения используются циклически). Использование различных функций консолидации данных позволяет охватывать большие интервалы времени без чрезмерного увеличения объема БД за счет снижения разрешающей способности.

2.4 Web серевер Apache

Apache HTTP-сервер – свободно распространяемый веб-сервер. С апреля 1996 и до настоящего времени является самым популярным HTTP-сервером в интернете. По статистике Netcraft, в августе 2007 года он работал на 51 % всех веб-серверов, в марте 2009 года – на 49 %.

Основными достоинствами Apache считаются надежность и гибкость конфигурации. Он позволяет подключать внешние модули для предоставления данных, использовать СУБД для аутентификации

пользователей, модифицировать сообщения об ошибках и т. д. Поддерживает IPv6. Недостатком наиболее часто называется отсутствие удобного стандартного интерфейса для администратора.

Сервер был написан в начале 1995 года и считается, что его имя восходит к шуточному названию «a patchy» (англ. «заплаточный»), так как он устранял ошибки популярного тогда сервера Всемирной паутины NCSA HTTPd 1.3. В дальнейшем, с версии 2.x сервер был переписан заново и теперь не содержит кода NCSA, но имя осталось.

Сервер Apache поддерживает одновременную работу и, следовательно, может обслуживать большое количество клиентов. Количество клиентов, которое может одновременно обслуживаться, ограничивается лишь используемыми аппаратными средствами и операционной системой. Сервер может быть легко сконфигурирован с помощью редактирования текстовых файлов или, используя один из многочисленных инструментов с графическим интерфейсом. В соответствии со своей модульной архитектурой, множество возможностей, которые необходимы для работы некоторых приложений, могут быть реализованы в виде дополнительных модулей Apache. Для поддержки такой возможности для разработчиков модулей реализован хорошо документированный API. Модульность и существование множества бесплатных модулей позволяет легко создать мощный веб-сервер без изменения его исходного кода. Используя на сервере множество доступных скриптовых языков, можно легко создать любое веб-приложение. Для использования любого скриптового языка необходим только соответствующий подключаемый модуль. Диаграмма на рисунке 2.1 показывает HTTP сервер Apache в своем окружении.

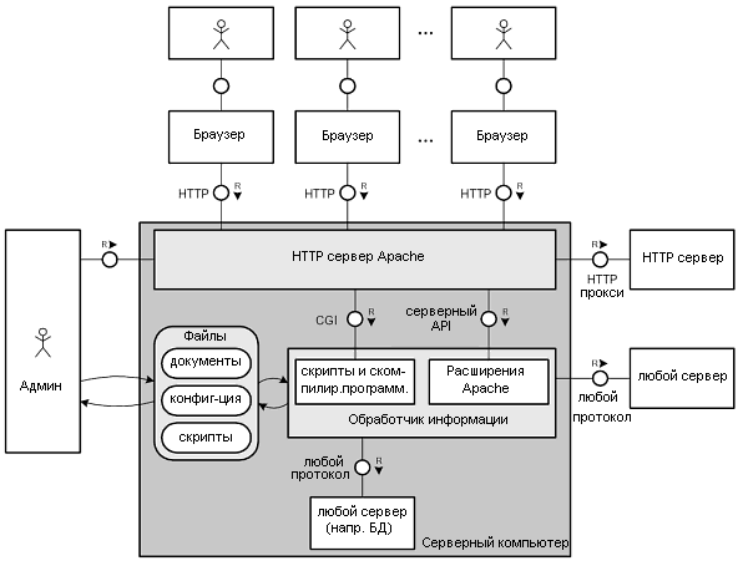


Рисунок 2.1 – Принцип работы веб сервера Apache

2.5 СУБД MySQL

MySql – это быстрая, надежная, открыто распространяемая СУБД. MySql, как и многие другие СУБД, функционирует по модели «клиент/сервер». Под этим подразумевается сетевая архитектура, в которой компьютеры играют роли клиентов либо серверов. На рисунке 2.2 изображена схема передачи информации между компьютером клиента и жестким диском сервера.

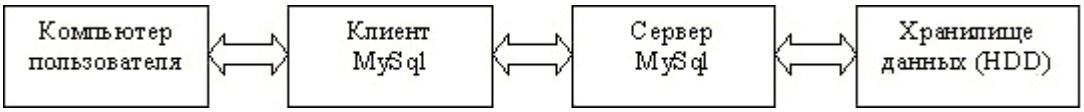


Рисунок 2.2 – Схема передачи данных в архитектуре "клиент/сервер"

СУБД управляет одной или несколькими базами данных. База данных представляет собой совокупность информации, организованной в виде множеств. Каждое множество содержит записи унифицированного вида. Сами записи состоят из полей. Обычно множества называют таблицами, а записи – строками таблиц.

Такова логическая модель данных. На жестком диске вся база данных может находиться в одном файле. В MySql для каждой базы данных создается отдельный каталог, а каждой таблице соответствуют три файла. В

других СУБД могут использоваться иные принципы физического хранения данных.

Строки таблиц могут быть связаны друг с другом одним из трех способов. Простейшее отношение – «один к одному». В этом случае строка первой таблицы соответствует одной единственной строке второй таблицы. На диаграммах такое отношение выражается записью 1:1.

Отношение «один ко многим» означает ситуацию, когда строка одной таблицы соответствует нескольким строкам другой таблицы. Это наиболее распространенный тип отношений. На диаграммах он выражается записью 1:N. Наконец, при отношении «многие ко многим» строки первой таблицы могут быть связаны с произвольным числом строк во второй таблице. Такое отношение записывается как N:M.

Клиентская программа MySql представляет собой утилиту командной строки. Эта программа подключается к серверу по сети. Команды, выполняемые сервером, обычно связаны с чтением и записью данных на жестком диске. Клиентские программы могут работать не только в режиме командной строки. Есть и графические клиенты, например MySql GUI, PhpMyAdmin и др.

MySql взаимодействует с базой данных на языке, называемом SQL (Structured Query Language – язык структурированных запросов). SQL предназначен для манипуляции данными, которые хранятся в Системах управления реляционными базами данных (RDBMS). SQL имеет команды, с помощью которых данные можно извлекать, сортировать, обновлять, удалять и добавлять. Стандарты языка SQL определяет ANSI (American National Standards Institute). В настоящее время действует стандарт, принятый в 2003 году (SQL-3).

SQL можно использовать с такими RDBMS как MySql, mSQL, PostgresSQL, Oracle, Microsoft SQL Server, Access, Sybase, Ingres. Эти системы RDBMS поддерживают все важные и общепринятые операторы

SQL, однако каждая из них имеет множество своих собственных патентованных операторов и расширений.

SQL является общим языком запросов для нескольких баз данных различных типов.

2.6 Система разработки сценариев PHP

В области программирования для Сети, PHP – один из популярнейших скриптовых языков (наряду с JSP, Perl и языками, используемыми в ASP.NET) благодаря своей простоте, скорости выполнения, богатой функциональности и распространению исходных кодов на основе лицензии PHP. PHP отличается наличием ядра и подключаемых модулей, «расширений»: для работы с базами данных, сокетами, динамической графикой, криптографическими библиотеками, документами формата PDF и т. п. Любой желающий может разработать свое собственное расширение и подключить его. Существуют сотни расширений, однако в стандартную поставку входит лишь несколько десятков хорошо зарекомендовавших себя. Интерпретатор PHP подключается к веб-серверу либо через модуль, созданный специально для этого сервера (например, для Apache или IIS), либо в качестве CGI-приложения.

Кроме этого, он может использоваться для решения административных задач в операционных системах UNIX, GNU/Linux, Microsoft Windows, Mac OS X и AmigaOS. Однако в таком качестве он не получил распространение, отдавая пальму первенства Perl, Python и VBScript.

В настоящее время PHP используется сотнями тысяч разработчиков. Порядка 20 миллионов сайтов сообщают о работе с PHP, что составляет более пятой доли доменов интернета.

Синтаксис PHP подобен синтаксису языка Си. Некоторые элементы, такие как ассоциативные массивы и цикл foreach, заимствованы из Perl.

Для работы программы не требуется описывать какие-либо переменные, используемые модули, и т.п. Любая программа может начинаться непосредственно с оператора PHP.

Простейшая программа Hello world на PHP выглядит следующим образом:

```
<?php
  echo 'Hello, world!';
?>
```

PHP исполняет код, находящийся внутри ограничителей, таких как <?php ?>. Все, что находится вне ограничителей, выводится без изменений. В основном, это используется для вставки PHP-кода в HTML-документ, например так:

```
<html>
 <head>
  <title>Тестируем PHP</title>
 </head>
 <body>
  <?php echo 'Hello, world!'; ?>
 </body>
</html>
```

Помимо ограничителей <?php ?>, допускается использование дополнительных вариантов, таких как <? ?> и <script language="php"> </script>. Кроме того, до версии 6.0 допускается использование ограничителей языка программирования ASP <% %> (конструкции <? ?> и <% %> могут быть выключены в конфигурационном файле php.ini).

Имена переменных начинаются с символа $, тип переменной объявлять не нужно. В отличие от имен функций и классов, имена переменных чувствительны к регистру. Переменные обрабатываются в

строках, заключенных в двойные кавычки, и heredoc-строках (строках, созданных при помощи оператора).

PHP рассматривает переход на новую строку как пробел, так же как HTML и другие языки со свободным форматом. Инструкции разделяются с помощью точки с запятой (;), за исключением некоторых случаев.

PHP поддерживает три типа комментариев: в стиле языка Си (ограниченные /* */), C++ (начинающиеся с // и идущие до конца строки) и оболочки UNIX (с # до конца строки).

PHP является языком программирования с динамической типизацией, не требующим указания типа при объявлении переменных, равно как и самого объявления переменных. Преобразования между скалярными типами зачастую осуществляется неявно без дополнительных усилий (впрочем PHP предоставляет широкие возможности и для явного преобразования типов).

К скалярным типам данных относятся:

– целый тип (integer);

– вещественный тип данных (float, double);

– логический тип (boolean);

– строковый тип (string);

– и специальный тип NULL.

К нескалярным типам относится:

– «ресурс» (resource);

– массив (array);

– и объект (object).

Диапазон целых чисел (integer) в PHP зависит от платформы (обычно это диапазон 32-битных знаковых целых чисел, то есть от −2 147 483 648 до 2 147 483 647). Числа можно задавать в десятичной, восьмеричной и шестнадцатеричной системах счисления. Диапазон вещественных чисел (double) также зависит от платформы.

PHP предоставляет разработчикам логический тип (boolean), способный принимать только два значения TRUE («истина») и FALSE («ложь»). При преобразовании в логический тип число 0, пустая строка, ноль в пустой строке «0», NULL и пустой массив считаются FALSE. Все остальные значения автоматически преобразуются в TRUE.

Специальный тип NULL предназначен для переменных без определенного значения. Единственным значением данного типа является константа NULL. Тип NULL принимают неинициализированные переменные, переменные инициализированные константой NULL, а также переменные, удаленные при помощи конструкции unset().

Ссылки на внешние ресурсы имеют тип «ресурс» (resource). Переменные данного типа, как правило, представляют собой дескриптор, позволяющий управлять внешними объектами, такими как файлы, динамические изображения, результирующие таблицы базы данных и т. п.

Массивы (array) поддерживают числовые и строковые ключи и являются гетерогенными. Массивы могут содержать значения любых типов, включая другие массивы. Порядок элементов и их ключей сохраняется.

2.7. Язык программирования Perl

Perl – интерпретируемый язык, приспособленный для обработки произвольных текстовых файлов, извлечения из них необходимой информациии и выдачи сообщений. Он также удобен для написания различных системных программ. Этот язык прост в использовании, эффективен, но про него трудно сказать, что он элегантен и компактен.

Perl был создан в 1986 году как инструмент для администрирования и конфигурирования системных ресурсов сети, состоящей из Unix-компьютеров. Он сочетает в себе лучшие черты C, shell, sed и awk, поэтому для тех, кто знаком с ними, изучение Perl-a не представляет особого труда. Синтаксис выражений Perl-a близок к синтаксису C. В отличие от большинства утилит ОС UNIX Perl не ставит

ограничений на объем обрабатываемых данных и если хватает ресурсов, то весь файл обрабатывается как одна строка. Рекурсия может быть произвольной глубины. Хотя Perl приспособлен для сканирования текстовых файлов, он может обрабатывать так же двоичные данные и создавать .dbm файлы, подобные ассоциативным массивам. Perl позволяет использовать регулярные выражения, создавать объекты, вставлять в программу на C или C++ куски кода на Perl-е, а также позволяет осуществлять доступ к базам данных.

Язык Perl был создан для повышения эффективности обработки текстовых документов. Он ориентирован на обработку строк. В настоящее время язык получил большое распространение как инструмент создания исполняемых модулей WWW-сервера. Существующие пакеты расширения обеспечивают доступ к SQL-серверам непосредственно из Perl-программы. Это позволяет использовать его для решения всех задач, возникающих при обеспечении WWW-доступа к базам данных. Perl эффективен также при обработке произвольных структур данных: существующих отчетов, списков, карточек в электронном виде.

Хотя CGI-приложения можно писать практически на любом языке, Perl и CGI-программирование стали синонимами для многих программистов. Как сказал Хасан Шрейдер (Hassan Shroeder), первый вебмастер Sun, «Perl – это артерия интернета». Perl – самый широко используемый язык для CGI-программирования, и для этого есть много веских причин:

– Perl легко выучить: его синтаксис напоминает другие языки (например C), потому что он «многое прощает», при ошибке выдается подробное сообщение, помогающее быстро локализовать проблему;

– Perl способствует быстрой разработке, так как это интерпретируемый язык, исходный код не надо компилировать перед запуском;

– Perl доступен на многих платформах с минимальными изменениями;

– Perl содержит очень мощные функции для обработки строк со встроенной в язык поддержкой поиска и замены по регулярным выражениям;

– Perl обрабатывает двоичные данные так же легко, как и текст;

– Perl не требует четкого разделения на типы: числа, строки и логические выражения являются обычными скалярами;

– Perl взаимодействует с внешними приложениями очень просто и обеспечивает собственные функции для работы с файловыми системами.

Для Perl есть много свободно доступных модулей от CPAN, начиная с модулей для создания динамической графики до интерфейсов с интернет-серверами и системами управления базами данных.

Perl действительно очень быстрый: считывая исходный файл, он тут же компилирует его в низкоуровневый код, который потом исполняет. Обычно компиляция и исполнение в Perl не воспринимаются как отдельные шаги, поскольку выполняются вместе: Perl запускается, читает исходный файл, компилирует его, запускает и затем завершает работу. Этот процесс повторяется каждый раз, когда запускается сценарий Perl, в том числе CGI-сценарии. Поскольку Perl так эффективен, этот процесс происходит достаточно быстро, чтобы обрабатывать все запросы не на самых загруженных серверах. Однако следует обратить внимание, что в системах Windows это гораздо менее эффективно из-за необходимости создания новых процессов.

3 Разработка системы мониторинга

3.1 Структура вычислительной сети РЦС-3

Сеть передачи данных РЦС-3 имеет структуру, представленную в Приложении Б. В состав сети входит оборудование:

– коммутатор Cisco Catalyst 2950 – 6 ед.;

– коммутатор Cisco Catalyst 2940 – 1 ед.;

– маршрутизатор Cisco 7200 – 1 ед.;

– маршрутизатор Cisco 3800 – 1 ед.;

– коммутатор 3COM OfficeConnect – 1 ед.;

– модем HDSL ADC PairGane 2Mb/s – 4 ед.;

– модем ADSL Zyxel 782E – 1 ед .

Маршрутизаторы серии 7200 обеспечивают высокую надежность, отказоустойчивость, поддержку широкого спектра сред передачи данных. Данный маршрутизатор в сети РЦС используется для выхода во внешнюю

сеть интранет ОАО РЖД. Маршрутизатор серии 3800 выполняет роль резервного маршрутизатора на случай отказа основного, также оба маршрутизатора агрегируют внутренний трафик сети и распределяют нагрузку на внешний канал. Сеть СПД разделена на несколько зон VLAN для агрегации трафика отделов. Для присоединения отдаленных отделов к сети предприятия используются высокоскоростные модемы. В сети предприятия функционируют АРМы ЕСМА, требующие работы в оперативном режиме, поэтому сохранение пропускной способности внешних каналов является главной задачей сети и обслуживающего персонала.

3.2 Принцип работы системы мониторинга Cacti

Свободно распространяемая система Cacti предоставляет пользователю удобный веб-интерфейс к утилите RRDTool, предназначенной для работы с круговыми базами данных (Round Robin Database), которые используются для хранения информации об изменении одной или нескольких величин за определенный промежуток времени. Интерфейс отображения статистики, собранной с сетевых устройств, представлен в виде дерева, структура которого задается самим пользователем. Как правило, графики группируют по определенным критериям, причем один и тот же график может присутствовать в разных ветвях дерева.

Для работы системы необходимо следующее программное обеспечение: Apache, PHP, NetSNMP, RRDTool, Perl, MySQL. Рассмотрим, для чего предназначено данное программное обеспечение в рамках функционирования системы мониторинга.

Веб-сервер Apache необходим для запуска веб-интерфеиса системы мониторинга и отправки запросов на обработку данных. PHP необходима для функционирования веб-интерфейса, так как веб-интерфейс полностью написан на языке программирования PHP, также PHP используется как обработчик скриптов для опроса оборудования. NetSNMP используется для опроса сетевого оборудования по протоколу SNMP, также можно

использовать для этой цели стандартную службу SNMP, входящую в состав Windows, но стандартная служба не работает с SNMP 3 версии. RRDtool – набор утилит для работы с RRD (Round-robin Database, кольцевая база данных). Предназначен для хранения и обработки динамических (изменяющихся во времени) последовательностей данных, таких как сетевой трафик, пропускная способность сети, температура, загрузка ЦПУ. Все данные хранятся в кольцевой базе, размер которой остается неизменным. Perl используется как обработчик скриптов для опроса оборудования, написанных на языке Perl. MySQL необходим для создания и функционирования базы данных веб-оболочки системы мониторинга.

Прежде чем настраивать Cacti, следует понять логику ее работы. Система обслуживает ряд устройств (Devices – в терминологии Cacti). Каждое устройство – это хост, к которому есть доступ по сети, то есть оно характеризуется IP-адресом или DNS-именем. С устройством ассоциированы хранилища данных (Data Sources). Каждое такое хранилище обслуживает один график (Graph), причем на этом графике может рисоваться несколько переменных – хранилище для них всех будет одно. Хранилище создается на основе шаблона данных (Data Template), который задает соответствие входных величин (полученных из SNMP-запросов или из скриптов) полям в базе данных и устанавливает дополнительные параметры хранения этих величин. Сами же входные величины получаются из методов сбора данных (Data Input Methods) или запросов (Data Queries). Первые предназначены для величин, количество которых заранее известно (например, количество процессов – это всегда одно целое число), а вторые – наоборот (например, статистика с сетевых интерфейсов, число которых может быть различным). График генерируется из круговой базы данных (хранилища) каждый раз заново, когда загружается страничка. Алгоритм и параметры его создания задаются шаблоном графика (Graph Template). Шаблоны хостов (Host Templates) упрощают работу с однотипными устройствами и позволяют

привязать определенные шаблоны графиков и запросы к данному типу хоста. Например, для маршрутизаторов Cisco – один набор графиков, а для UNIX-серверов – другой.

Все данные с устройств система получает по протоколу SNMP, с помощью обращения к программе NetSNMP и передачи ей входных параметров. Система для опроса оборудования использует скрипты, написанные на языке Perl и PHP. Для построения графиков используются xml шаблоны.

Алгоритм работы системы представлен в приложениях В и Г.

3.3 Настройка сетевого оборудования

Мониторинг сети осуществляется по протоколу SNMP, следовательно, все оборудование, за которым необходимо наблюдать, должно поддерживать данный протокол. Сетевое оборудование предприятия РЦС-3 в основном представлено оборудованием фирмы Cisco, за исключением нескольких единиц оборудования другого производителя. Высокоскоростные модемы настраиваются с помощью веб-интерфейса путем проставления галочек в соответствующих пунктах. Далее будет описано, как настроить маршрутизаторы и коммутаторы Cisco, их настройка не сильно отличается в зависимости от модели устройства, поэтому будет представлен общий алгоритм действий для всех устройств.

Для того чтобы настроить сетевое оборудование фирмы Cisco необходимо выполнить ряд следующих команд:

Router#configure terminal

Router(config)#snmp-server community cacti RO – где «public» значение «только чтение» community

Router(config)#exit

Router#

Router#write memory

Building configuration...

[OK]

Далее следует убедиться в том, что настройки SNMP Community Strings присутствуют в конфигурационном файле:

Router#show running-config

....

....

snmp-server community cacti RO

....

....

После приведенных выше действий оборудование готово к опросу по протоколу SNMP. После того как данная настройка будет произведена на всех маршрутизаторах и коммутаторах сети, можно также настроить то, кому будут предназначаться «ловушки», отправляемые устройствами, для этого в настройках SNMP на маршрутизаторах и коммутаторах необходимо прописать ip-адрес компьютера, которому предназначаются «ловушки», в данном случае это компьютер, на котором функционирует система мониторинга.

Сеть ОАО РЖД является закрытой сетью, т.е. не имеет прямого выхода в сеть интернет, поэтому в данной ситуации возможно использование 2 версии протокола SNMP не поддерживающего шифрование трафика. Безопасность данной версии протокола определяется только строкой community.

3.4 Установка и первоначальная настройка компонентов системы

3.4.1 Установка и конфигурирование PHP

Есть два основных способа установки PHP под Windows: вручную, либо инсталлятором InstallShield. Далее будет описан способ установки с помощью InstallShield. Windows PHP-инсталятор, доступный на страницы downloads по адресу http://www.php.net/, устанавливает CGI-версию PHP и, для IIS, PWS и Xitami.

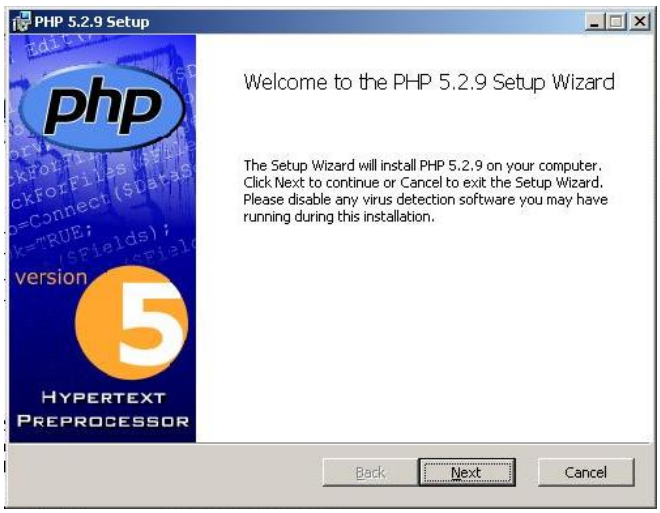


Рисунок 3.1 – Инсталлятор PHP

Далее указываем директорию, в которую будет производиться установка.

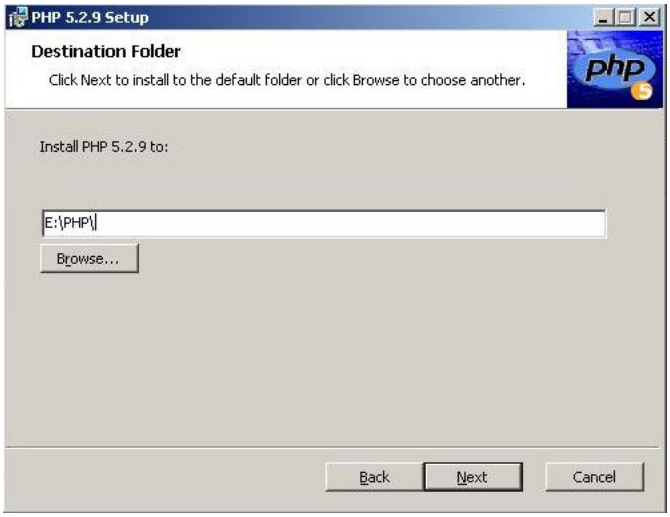


Рисунок 3.2 – Директория установки

Затем необходимо включить поддержку веб-сервера, на котором будет работать PHP, и указать директорию, куда установлен веб-сервер.

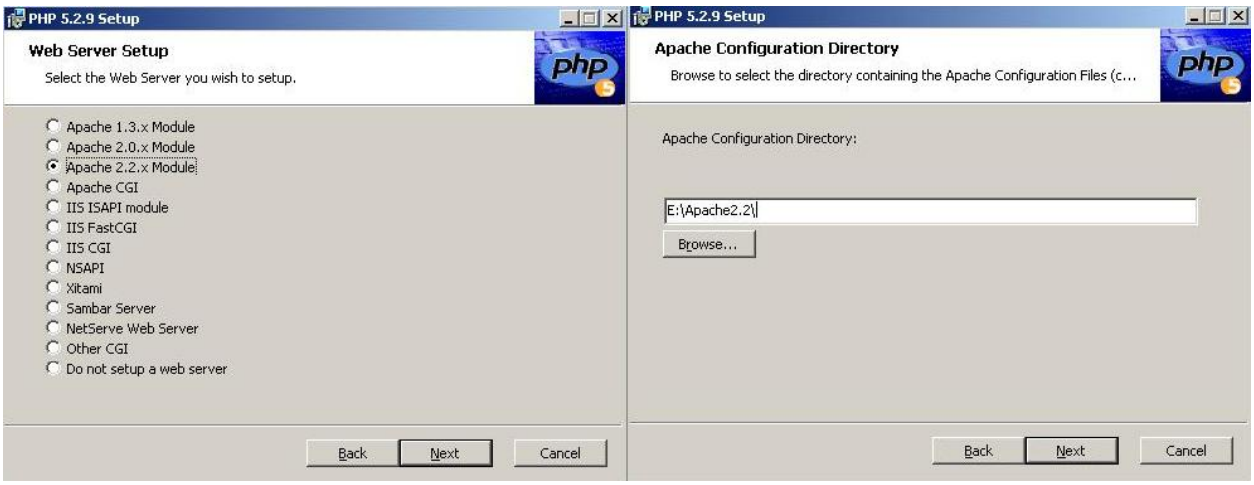


Рисунок 3.3 – Установка поддержки веб-сервера Apache

Далее необходимо добавить к переменной окружения Windows PATH следующий путь: e:\php. Доступ к Windows path можно получить через Control Panel по пути: System | Advanced | Environment Variables | System Variables.

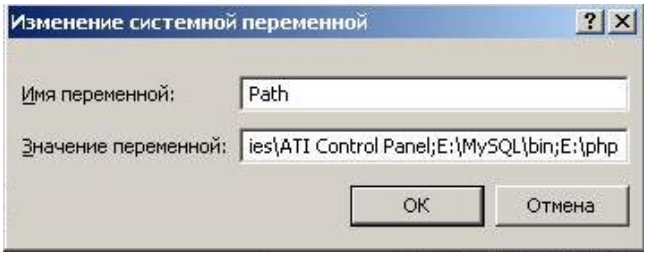


Рисунок 3.4 – Добавление переменной окружения

Создаем переменные окружения PHPRC со значением: e:\php и переменную окружения MIBDIRS со значением e:\php\extras\mibs.

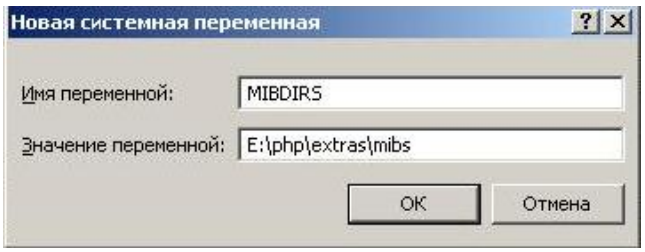


Рисунок 3.5 – Создание переменной окружения

Переименовываем файл e:\php\php.ini.dist в php.ini. В этом файле необходимо раскоментировать следующие строки:

extension_dir = c:phpext

extension=php_mysql.dll

extension=php_snmp.dll

extension=php_sockets.dll

cgi.force_redirect = 0

Также необходимо дать пользователю, из-под которого будет выполняться назначенное задание, права на изменение файла .index, расположенного по пути, заданному в переменной Windows MIBDIRS.

3.4.2 Установка и конфигурирование веб-сервера Apache

До начала установки необходимо удостовериться, что на сервере остановлены любые IIS сервера. Для установки веб-сервера запускаем InstallShield, далее следуем инструкциям по установке. После удачной установки открываем конфигурационный файл httpd.conf, который находится в директории E:\Apache2.2\conf\ httpd.conf, и вносим изменения в этот файл.

При использовании Apache 2.x и PHP 5 нужно добавить следующие линии:

LoadModule php5_module e:phpphp5apache2.dll

AddType application/x-httpd-php .php

DirectoryIndex index.html index.htm index.php

Затем необходимо проверить работоспособность веб-сервера и возможность его работы с PHP. Для этого переходим в веб-браузере на страницу http://localhost/test/test.php, и если на странице отображается информация об установленном PHP, то веб-сервер работает корректно и PHP установлен правильно.

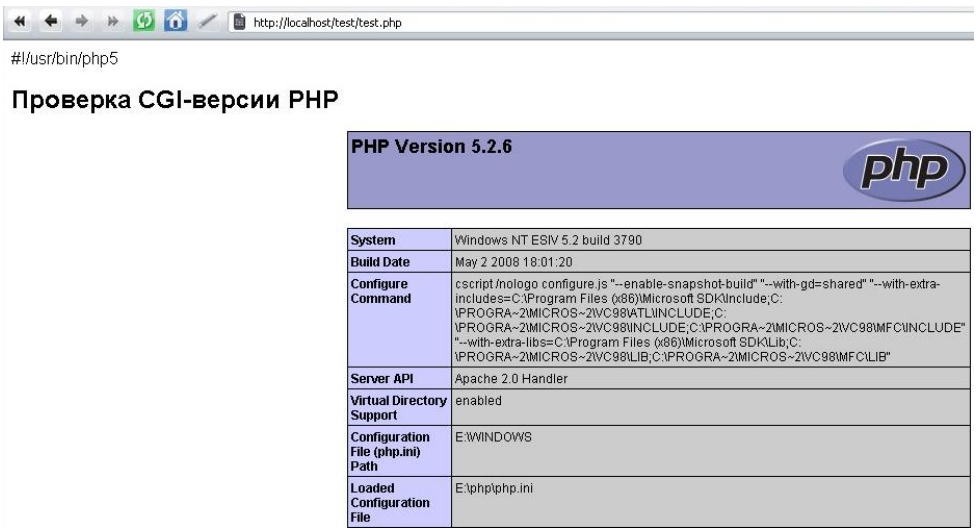


Рисунок 3.6 – Проверка работоспособности веб-сервера

После установки необходимо дать пользователю, из-под которого будет выполняться назначенное задание, права для изменение файлов, находящихся в директории веб-сервера.

3.4.3 Установка RRDTool

Для установки RRDTool распаковываем RRDTool.zip файл с веб-сайта Cacti в c:\cacti\RRDTool.exe.

Настройка базы данных RRDTool не требуется, так как система мониторинга Cacti предназначена для работы с этой базой, то все параметры, необходимые для записи данных в базу, уже присутствуют в настройках системы мониторинга.

3.4.4 Установка и конфигурирование MySQL

Для установки MySQL запускаем InstallShield, далее следуем инструкциям по установке.

После установки будет предложено сконфигурировать MySQL. Далее будет продемонстрированы основные этапы конфигурирования MySQL.

Рисунок 3.7 – Приглашение сконфигурировать MySQL server

Так как в данной базе данных транзакции будут осуществляться только внутри базы, необходимо выбрать соответствующий пункт.

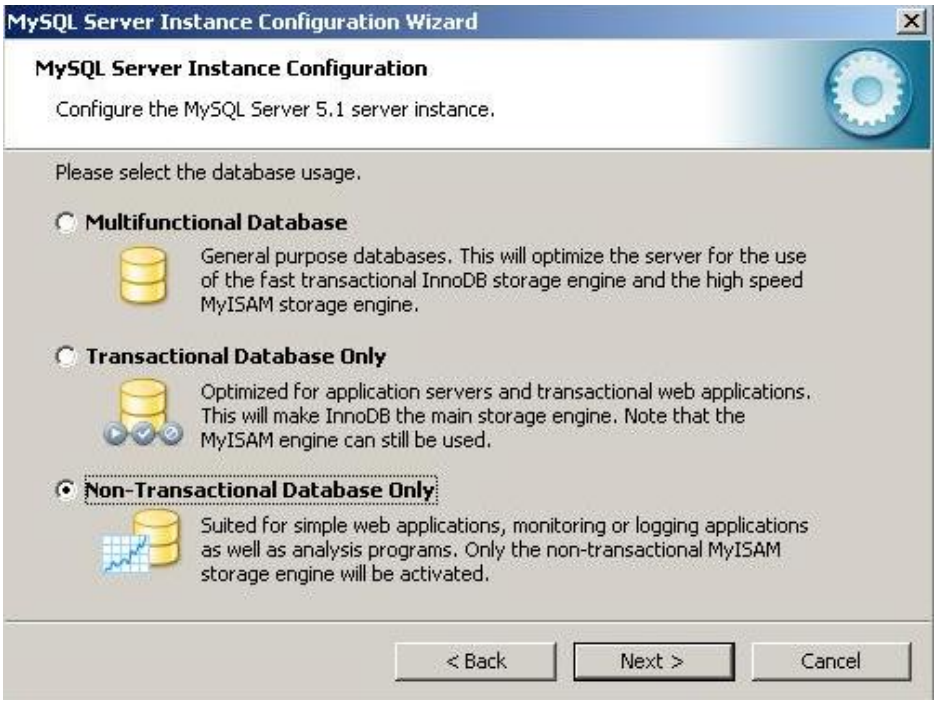


Рисунок 3.8 – Выбор метода транзакций

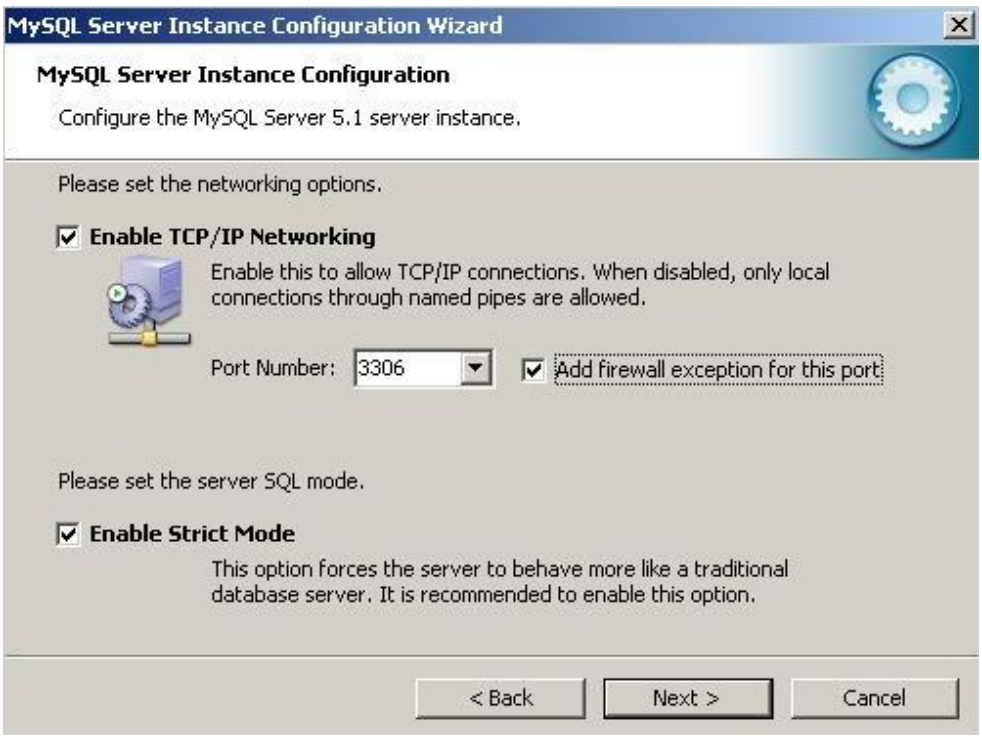


Рисунок 3.9 – Установка опций сети

Далее необходимо создать базу данных для системы мониторинга и пользователя.

Устанавливаем пароль для пользователя root следующей командой:

shell> cd mysqlbin shell> mysqladmin –user=root password somepassword shell> mysqladmin –user=root –password reload.

Создаем базу данных MySQL:

shell> mysqladmin –user=root –password create cacti.

Импортируем дефолтную базу данных Cacti:

shell> mysql –user=root –password cacti < e:apache2/htdocs/cacti/cacti.sql.

Создаем MySQL пользователя для Cacti:

shell> mysql –user=root –password mysql mysql> GRANT ALL ON cacti.* TO cactiuser@localhost IDENTIFIED BY ’somepassword’; mysql> flush privileges;.

Также будет необходимо изменить аккаунт cactiuser со старым паролем.

shell> UPDATE mysql.user SET Password = OLD_PASSWORD('cactipwd') WHERE Host = 'localhost' AND User = 'cactiuser'; mysql> FLUSH PRIVILEGES;.

Для более удобного администрирования базы данных необходимо установить PhpMyAdmin. Его установка производится путем распаковывания архива с программой в корневую директорию веб-сервера. После этого администрирование базы данных можно будет производить через веб-браузер.

3.4.5 Установка Net-SNMP

Для установки Net-SNMP запускаем InstallShield, далее следуем инструкциям по установке.

Рисунок 3.10 – Установка Net-SNMP

Для полноценной работы программы в среде Windows необходимо включить поддержку расширений Windows.

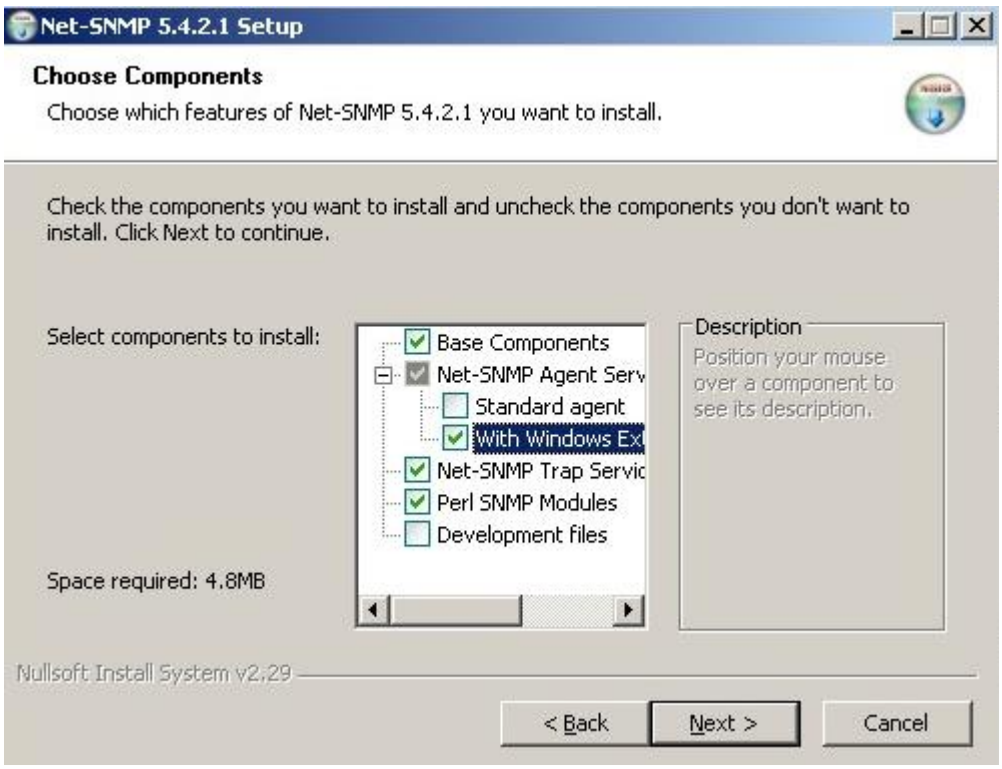


Рисунок 3.11 – Включение поддержки расширений Windows

3.4.6 Конфигурирование Cacti

Перед тем как начать конфигурирование Cacti, необходимо отредактировать файл E:/Apache2.2/htdocs/cacti/include/config.php и указать пользователя MySQL, его пароль, имя БД, и порт БД для конфигурации Cacti.

$database_default = “cacti”;

$database_hostname = “localhost”;

$database_username = “cactiuser”;

$database_password = “cacti”;

$database_port = “3306″;

Далее переходим в веб-браузере по адресу http://localhost/cacti/index.php.

Авторизуемся, используя логин и пароль admin/admin. Будет необходимо сменить пароль сразу после авторизации.

После этого открывается главная консоль системы мониторинга. Главная консоль предоставляет доступ ко всем настройкам системы. Из главной консоли можно создать новый график, добавить новое устройство,

изменить способ отображения графиков в дереве графиков. Также есть возможность настроить отображение графиков: цвет графиков, подписи графиков, размер. Из главной консоли можно добавлять новых пользователей, добавлять плагины, настраивать плагины. Предоставляется возможность импортировать и экспортировать шаблоны графиков, а также настраивать шаблоны, с помощью которых строятся графики.

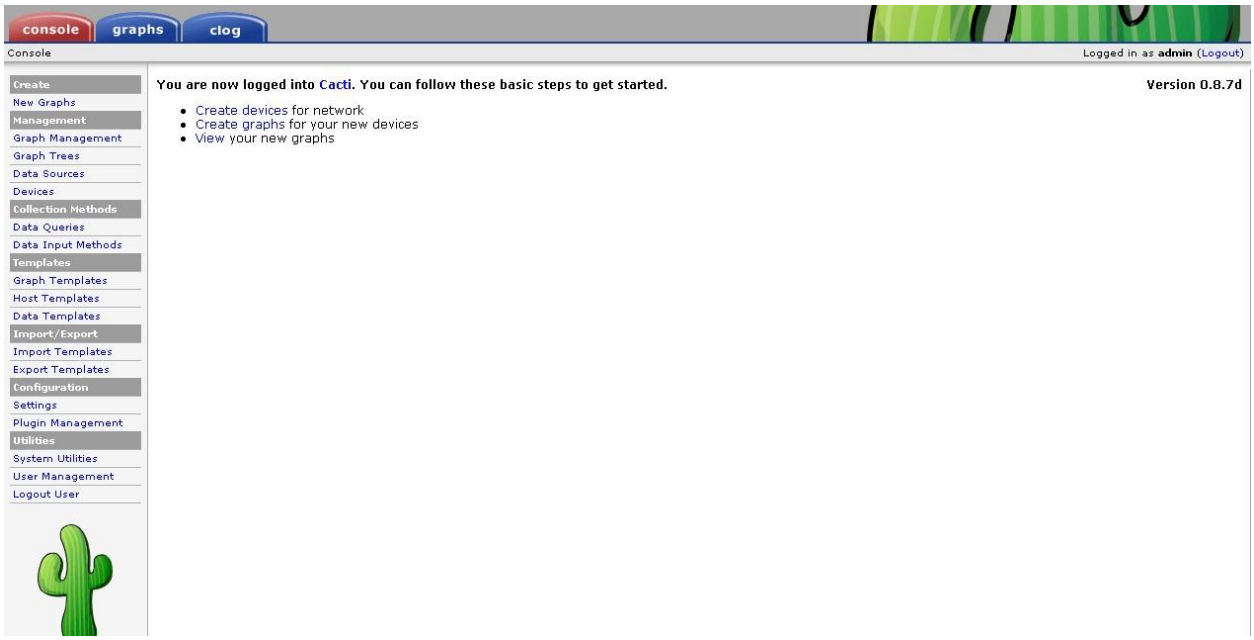


Рисунок 3.12 – Главная консоль Cacti

Из консоли Cacti переходим в раздел Settings->Paths и проверяем либо изменяем пути к правильному расположению файлов. Если вы планируете использовать Cactid, то очень важно, чтобы все пути вместо прямых слэшей включали только обратные слэши.

Рисунок 3.13 – Раздел Settings

Входим в систему под пользовательским аккаунтом, из-под которого будет запускаться задача по расписанию, и проверяем, что цикл опроса Cacti работает. Сделать это можно, выполнив следующую команду:

php c:/cacti_web_root/cacti/poller.php.

Вывод должен выглядеть следующим образом:

E:>php c:inetpubwwwrootcactipoller.php OK u:0.00 s:0.06 r:1.32 OK u:0.00 s:0.06 r:1.32 OK u:0.00 s:0.16 r:2.59 OK u:0.00 s:0.17 r:2.62 10/28/2005 04:57:12 PM - SYSTEM STATS: Time:4.7272 Method:cmd.php Processes:1 Threads:N/A Hosts:1 HostsPerProcess:2 DataSources:4 RRDsProcessed:2.

После разового запуска должен создаться файл cacti.log в директории /cacti/log/ и rrd файлы в каталоге /cacti/rra/.

Далее необходимо настроить расписание задачи, войдя в систему как администратор. Эта задача должна запускать poller.php каждые 5 минут.

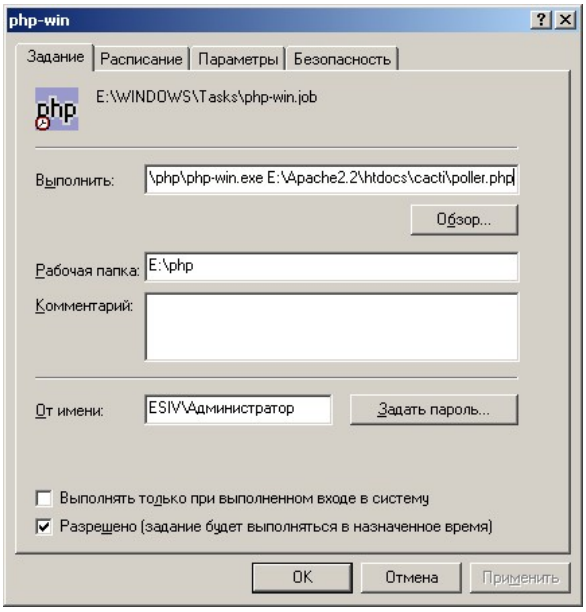


Рисунок 3.14 – Расписание задач для запуска poller.php

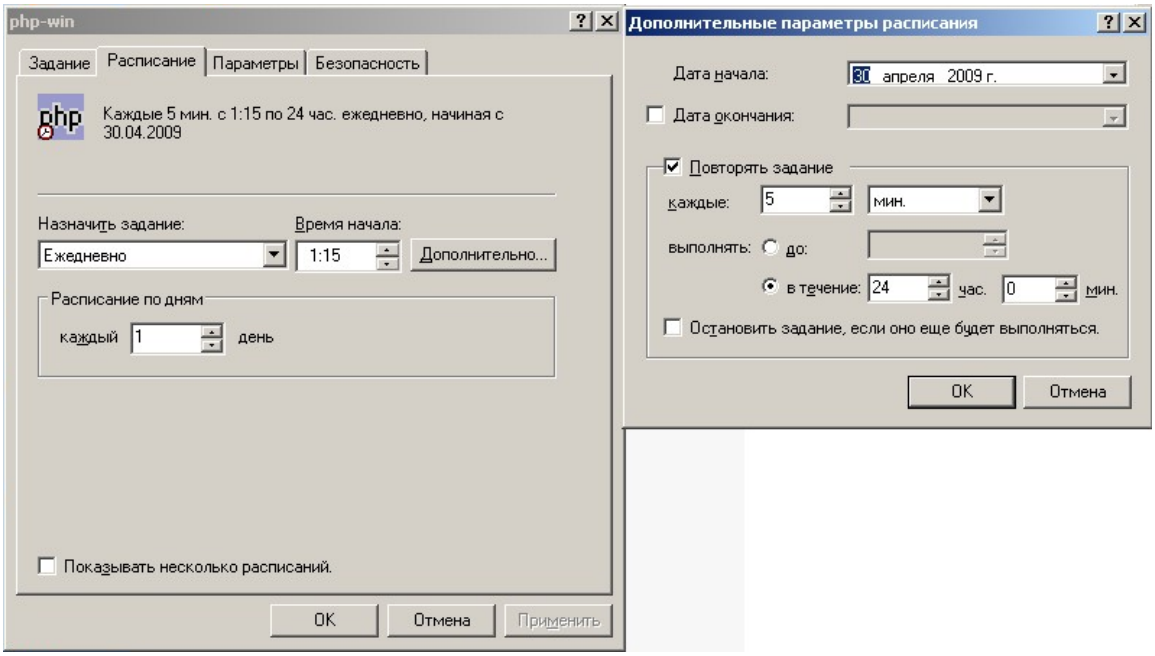


Рисунок 3.15 – Установка времени выполнения задачи

3.5 Возможности системы мониторинга Cacti

Система мониторинга Cacti является широко масштабируемой системой. Данная система может обслуживать большое количество устройств, но чем больше обслуживаемых устройств, тем более быстродействующий нужен компьютер, на котором функционирует сама система. Задача системы мониторинга – следить за оборудованием и в случае

проблем с ним оповещать об этом администратора сети, все эти задачи без затруднений выполняет система Cacti.

Пользовательский интерфейс представлен в виде вкладок, которые отображают различные параметры системы, главная вкладка «console» обеспечивает доступ к административному меню, позволяющему производить полную настройку системы, остальные вкладки предоставляют доступ к графикам и установленным плагинам.

Рисунок 3.16 – Вкладка «Console»

График генерируется из круговой базы данных (хранилища) каждый раз заново, когда загружается страничка. Алгоритм и параметры его создания задаются шаблоном графика (Graph Template). Шаблоны хостов (Host

Templates) упрощают работу с однотипными устройствами и позволяют привязать определенные шаблоны графиков и запросы к данному типу хоста.

Cacti позволяет завести несколько пользователей и разграничить их права как на просмотр статистики, так и на управление системой. Логика разделения доступа позволяет для каждого пользователя установить общую политику («Запретить» или «Разрешить»), а затем сделать из нее исключения.

Графики можно создать, выбрав пункт меню «New Graphs», затем следует выбрать устройство, для которого будет создан график, и какой именно график будет создан.

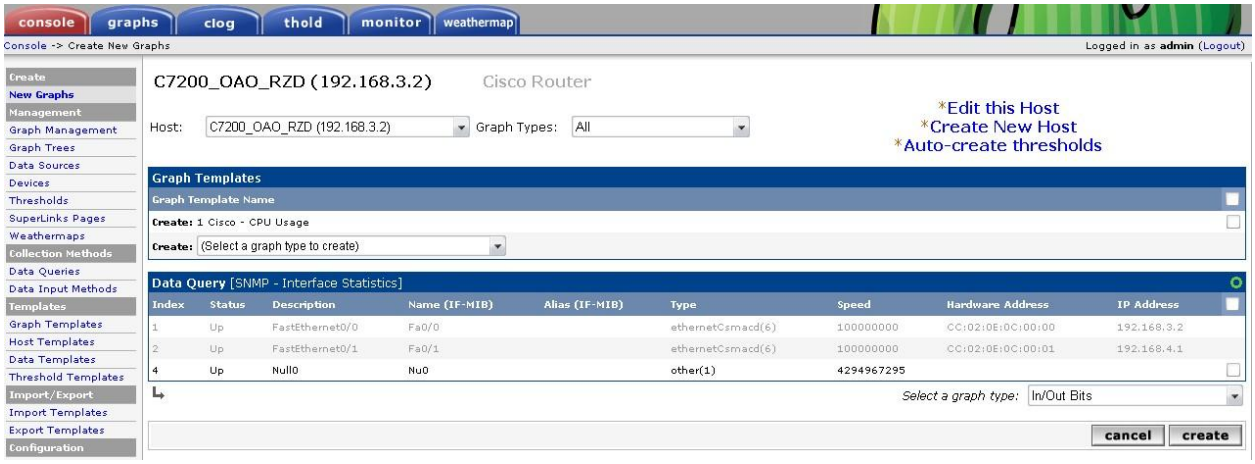


Рисунок 3.17 – Вкладка «New Graphs»

Пункт меню «Graph Management» позволяет просмотреть, какие графики созданы и их характеристики, также выбрав определенный график, есть возможность его настроить и посмотреть отладочную информацию, если график строится неправильно или не строится совсем. Также можно настроить все параметры графика: цвет, размер, название осей и другие.

Рисунок 3.18 – Пункт меню «Graph Management»

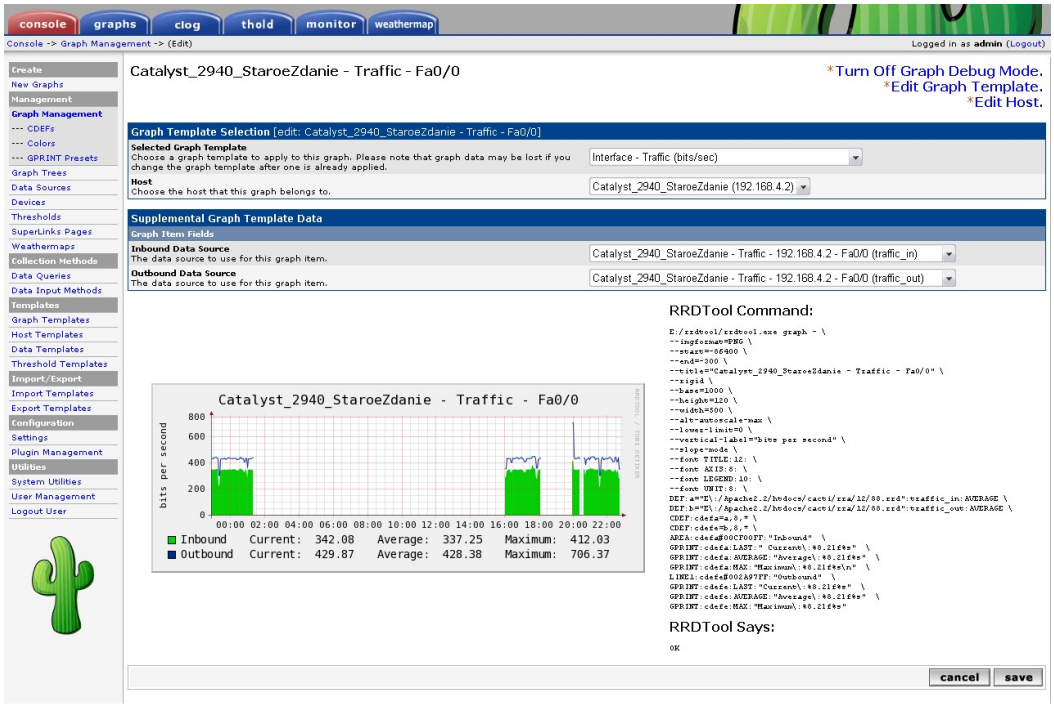


Рисунок 3.19 – Просмотр отладочной информации

Пункт мню «Graph Trees» позволяет настроить отображение дерева графиков, набор графиков, то, в какой последовательности будут

отображаться графики. Также можно группировать графики по определенным критериям.

Рисунок 3.20 – Пункт меню «Graph Trees»

Вкладка «Graphs» позволяет просмотреть графики, полученные при помощи опроса устройств. Интерфейс отображения статистики, собранной с сетевых устройств, представлен в виде дерева, структура которого задается самим пользователем. Как правило, графики группируют по определенным критериям, причем один и тот же график может присутствовать в разных ветвях дерева (например, трафик через сетевой интерфейс сервера – в той, которая посвящена общей картине интернет-трафика компании, и в ветви с параметрами данного устройства). Есть вариант просмотра заранее составленного набора графиков, и есть режим предпросмотра. Каждый из графиков можно рассмотреть отдельно, при этом он будет представлен за последние день, неделю, месяц и год. Возможно самому выбрать временной промежуток, за который будет сгенерирован график, причем сделать это можно, как указав календарные параметры, так и просто выделив мышкой определенный участок на нем. Минимальный интервал отображения информации на графике составляет 5 минут, но с помощью установки

дополнительного плагина можно просматривать графики в реальном времени с интервалом опроса устройств от 5 секунд до 1 минуты, для этого необходимо выбрать соответствующую иконку, расположенную около графика, и щелкнуть по ней, откроется новое окно с графиком и выбором интервала отображения.

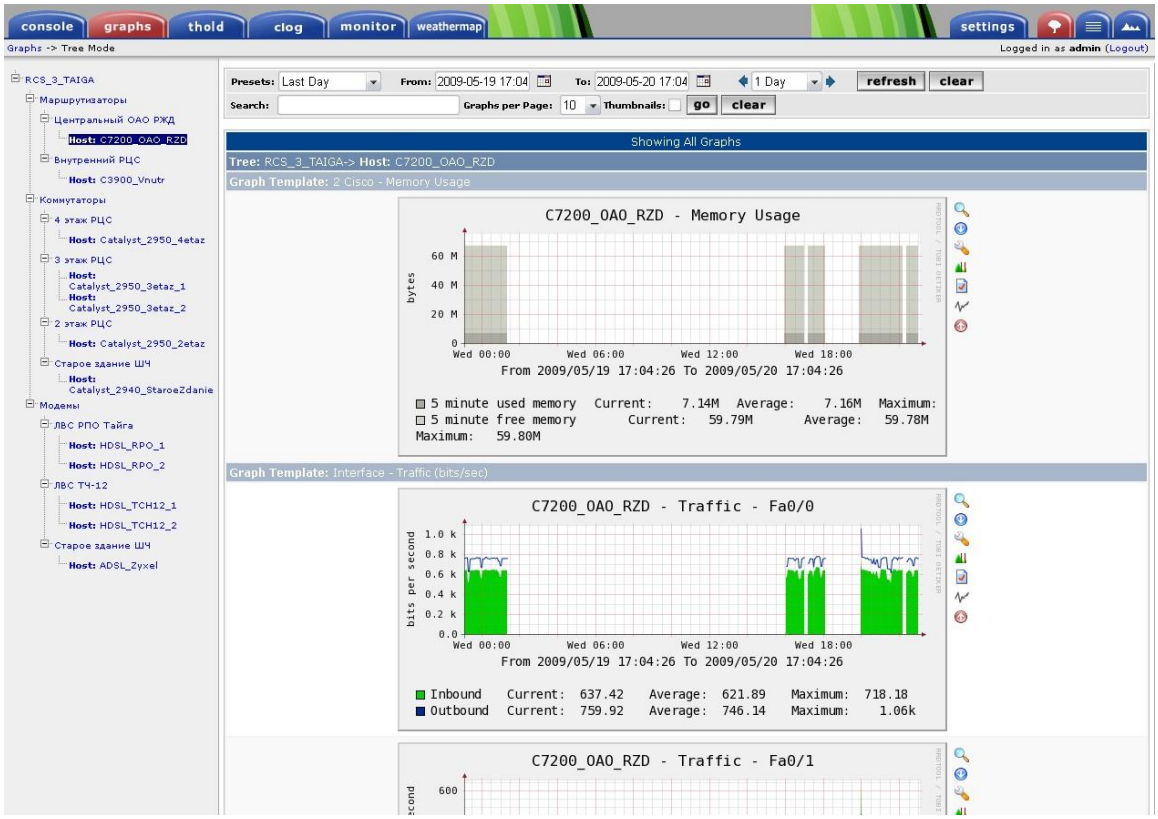


Рисунок 3.21 – Вкладка «Graphs»

Рисунок 3.22 – Временные интервалы одного графика

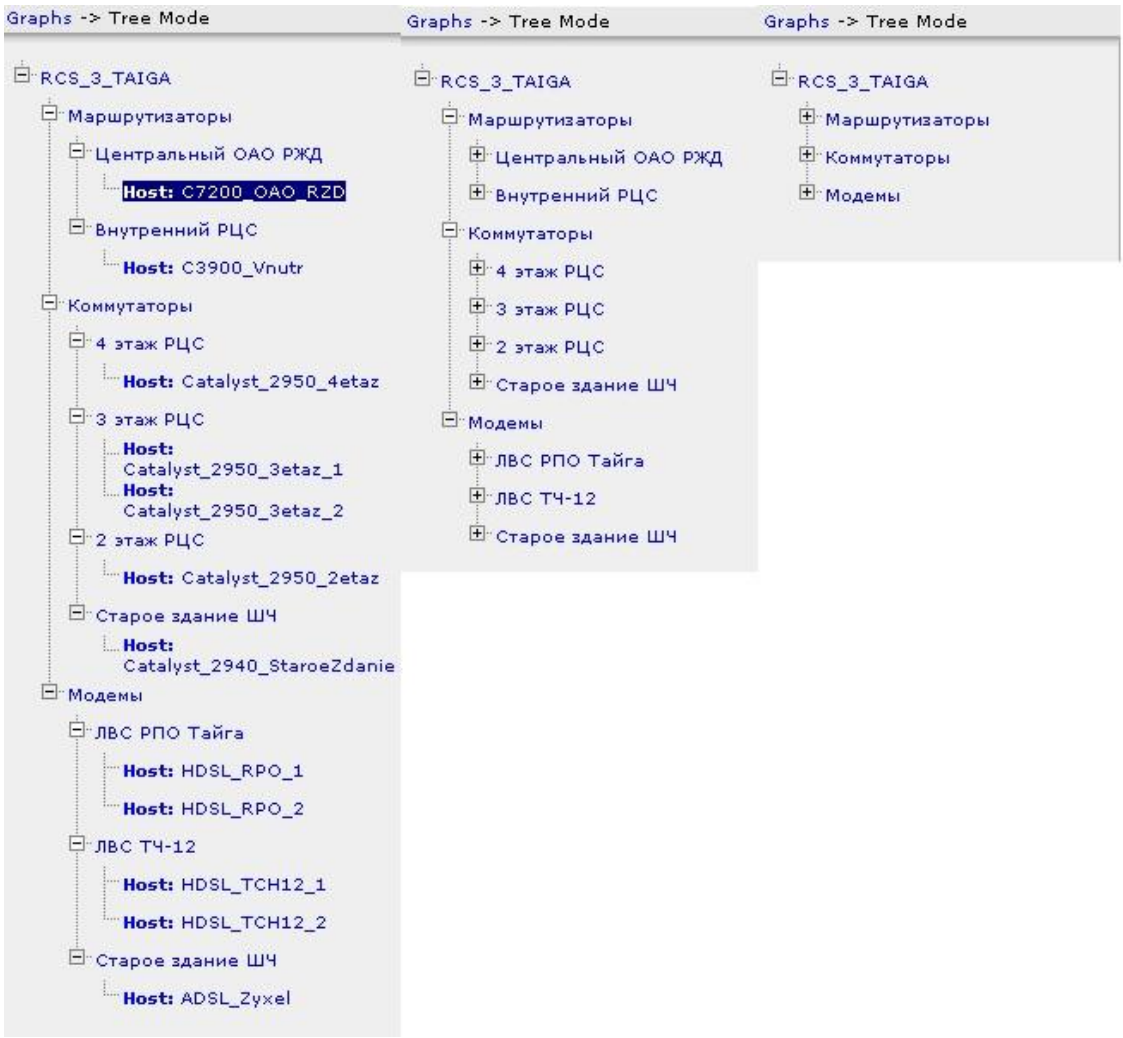


Рисунок 3.23 – Дерево устройств

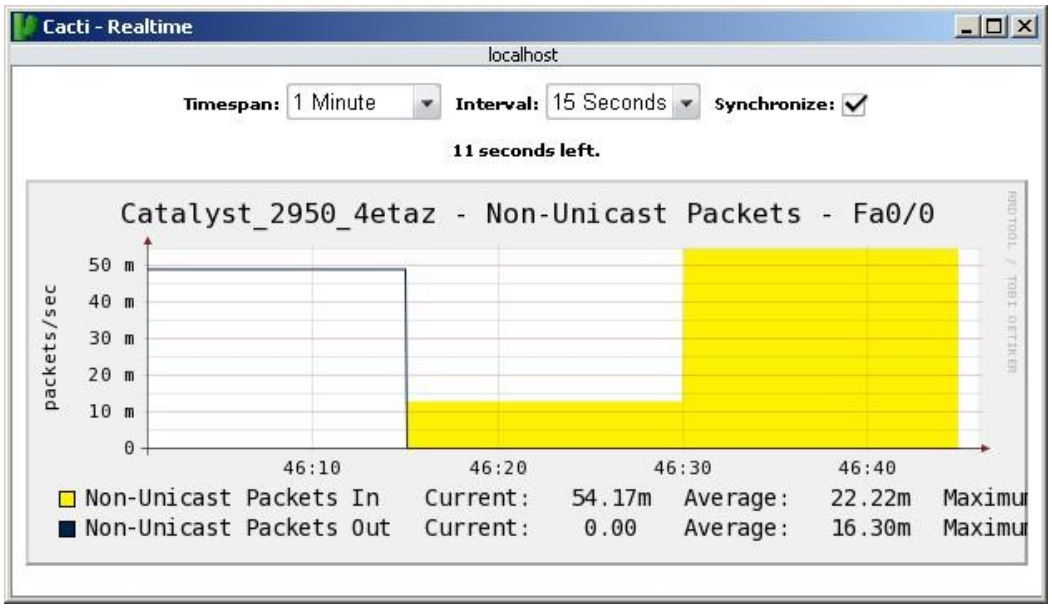


Рисунок 3.24 – Отображение графика в реальном времени

Также во вкладке «Graphs» можно посмотреть отладочную информацию по каждому графику. Графики можно передвигать вверх по странице с помощью иконок, расположенных возле графиков. Есть возможность сортировать графики по дате, по времени, показывать графики только с определенным интервалом, это можно сделать с помощью фильтра, расположенного вверху страницы. С помощью настроек можно полностью изменить вид страницы отображения графиков: в несколько рядов, сразу все и другое.

Возможности системы не ограничиваются только построением графиком и вариациями с их отображением. С помощью плагинов можно расширить возможности программы до невообразимых пределов, а если не найдется нужного плагина, его можно написать своими силами, что не составит большого труда для администратора, знающего язык программирования PHP.

3.6 Установка, настройка и функционал плагинов

Далее следует установит и настроить плагины. Для системы Cacti написано множество плагинов, все плагины написаны на языке

программирования PHP. Каждый плагин обладает определенным функционалом, и у администратора есть возможность выбирать те плагины, которые необходимы на данном этапе развития администрируемой сети.

Если необходим плагин специфического функционала, его можно написать на языке PHP и присоединить к системе мониторинга. Для сети РЦС-3 достаточно плагинов, которые уже существуют, и нет необходимости создавать новые плагины, так как задачи, решаемые системой мониторинга в данной сети, являются тривиальными.

Перед началом установки плагинов необходимо установить поддержку плагинов, для этого скачиваем с сайта производителя файлы, называемые архитектура плагина, и заменяем файлы в корневой папке Cacti на скачанные файлы. После этого можно приступать к установке плагинов.

Для того чтобы установить плагин, необходимо скопировать папку с файлами плагина в папку, которая находится по адресу E:\Apache2.2\htdocs\cacti\plugins\. Далее необходимо внести небольшие изменения в конфигурационные файлы плагина, а именно: прописать имя пользователя и пароль, которые используются для доступа к базе данных. После этого в главный конфигурационный файл системы (global.php) необходимо добавить следующие строки:

```
$plugins = array();
$plugins[] = 'название плагина';
```

Затем переходим в веб-интерфейс системы и открываем пункт меню Plugin Management, в данной вкладке представлены установленные плагины и есть возможность их активировать или приостановить их работу.

Рисунок 3.25 – Пункт меню Plugin Management

3.6.1 Плагин Clog

Данный плагин позволяет просматривать логи, которые ведет программа. При каждом событии система записывает его в лог файл, то, что будет записываться в лог файл, настраивается с помощью пункта меню «Settings»: полное логирование, логирование критических событий и другое.

В данной вкладке можно применять различные фильтры для поиска нужной информации. Все события помечены определенными цветами, для того чтобы легче было их интерпретировать: красный цвет обозначает критическое событие, зеленый – успешное выполнение, серый – незначимое событие.

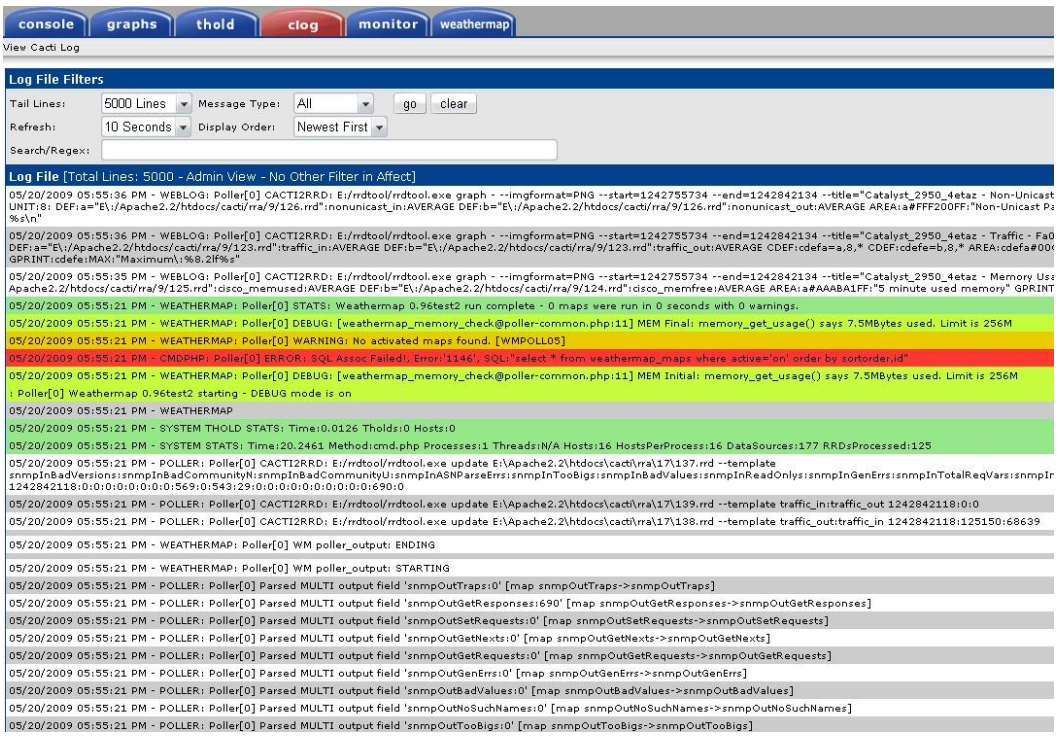


Рисунок 3.26 – Вкладка «Clog»

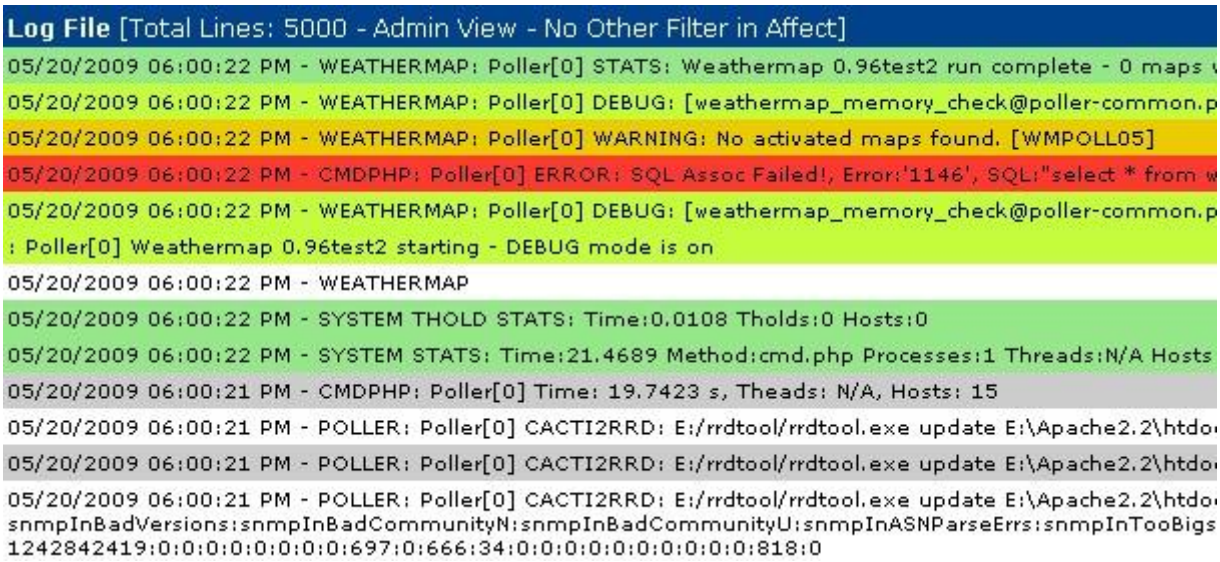


Рисунок 3.27 – Выделение цветами событий

3.6.2 Плагин Thresthold

Плагин Thresthold представляет собой надстройку для отправки оповещений о каких-либо событиях на электронный почтовый ящик. В данном плагине можно произвести настройку событий, при возникновении которых на электронную почту администратора будет отправлено уведомление. Например, настройка параметра максимальной загрузки

интерфейса на определенном порту маршрутизатора выставлена на значение 2Мбит\сек, если возникнет превышение лимита, то заранее определенное письмо будет немедленно отправлено администратору. Также можно наблюдать за настроенными событиями непосредственно с веб-интерфейса, для этого необходимо открыть вкладку плагина.

Рисунок 3.28 – Вкладка «thold»

На данном рисунке видно, что один из модемов находится в нерабочем состоянии, об этом событии администратору сети было отправлено сообщение.

Настройка данного плагина можно произвести из главного меню, выбрав пункт Thresholds. Затем выбираем добавление новой задачи, затем устройство, с которым будем работать и параметр, который необходимо отслеживать. После этого необходимо выставить максимальное и минимальное значение отслеживаемых параметров и адрес электронного почтового ящика, на который будет отправлено сообщение при превышении параметров.

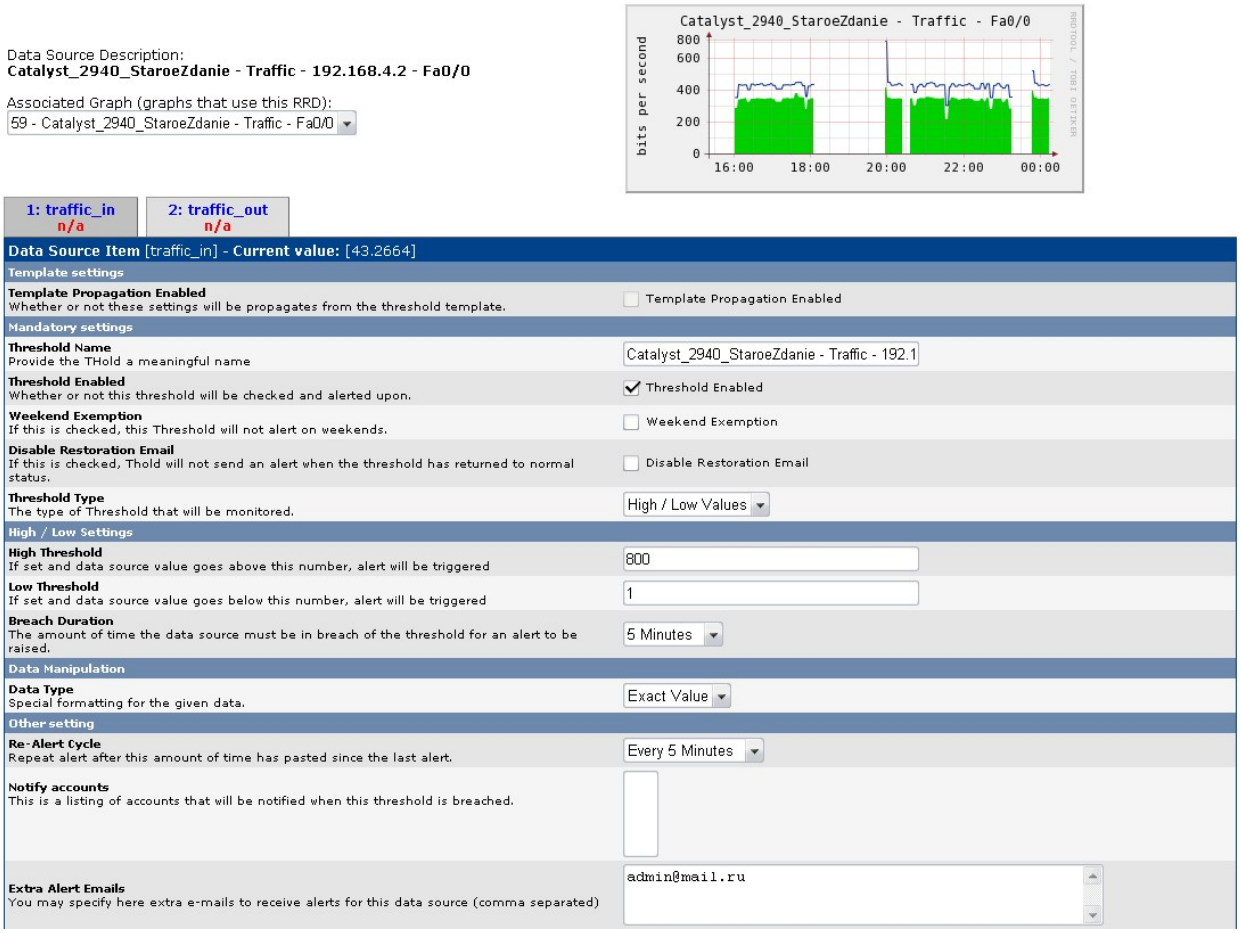


Рисунок 3.29 – Настройка параметров оповещения

Настройка того, какое сообщение отправляется в случае превышения максимального значения параметра, производится из меню управления выбором пункта «Settings», а затем выбором вкладки «Alerting/Thold». В этой вкладке можно настроить события, при которых отправится сообщение: warning, error, critical или debug. Также здесь можно настроить текст сообщения и много других параметров, относящихся к данному плагину. Для сети РЦС необходимо настроить оповещение о превышении трафика на интерфейсах маршрутизаторов и о доступности сетевых устройств. Также можно подключить к системе мониторинга все компьютеры предприятия и следить за тем, сколько трафика генерирует каждый компьютер в отдельности, и если будет превышение трафика, отправлять сообщения администратору.

3.6.3 Плагин monitor

Данный плагин позволяет следить за доступностью устройств, и отображать их доступность в графическом виде: с помощью иконок различного цвета. Также этот плагин при переходе на соответствующую вкладку может выдавать голосовое оповещение, если какое-либо из устройств недоступно. Настройка плагина производится из главного меню с помощью пункта «Settings», затем необходимо выбрать «Misc». В данном разделе можно настроить звуковой файл для оповещения, вид отображения устройств на вкладке плагина и интервал опроса устройств.

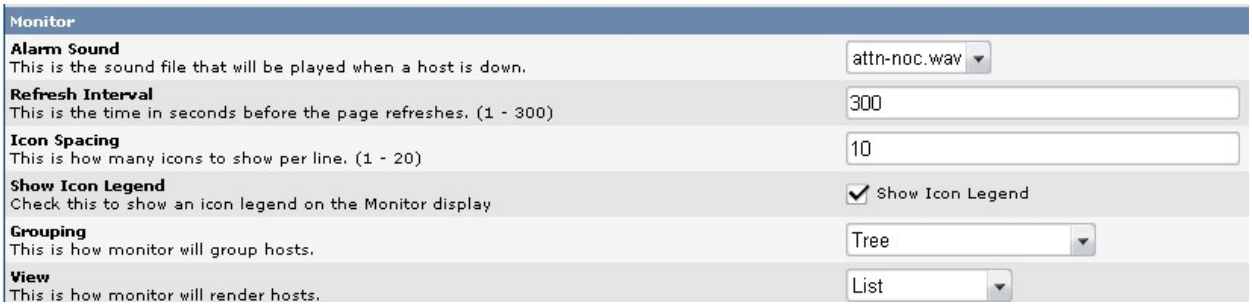


Рисунок 3.30 – Настройка плагина «monitor»

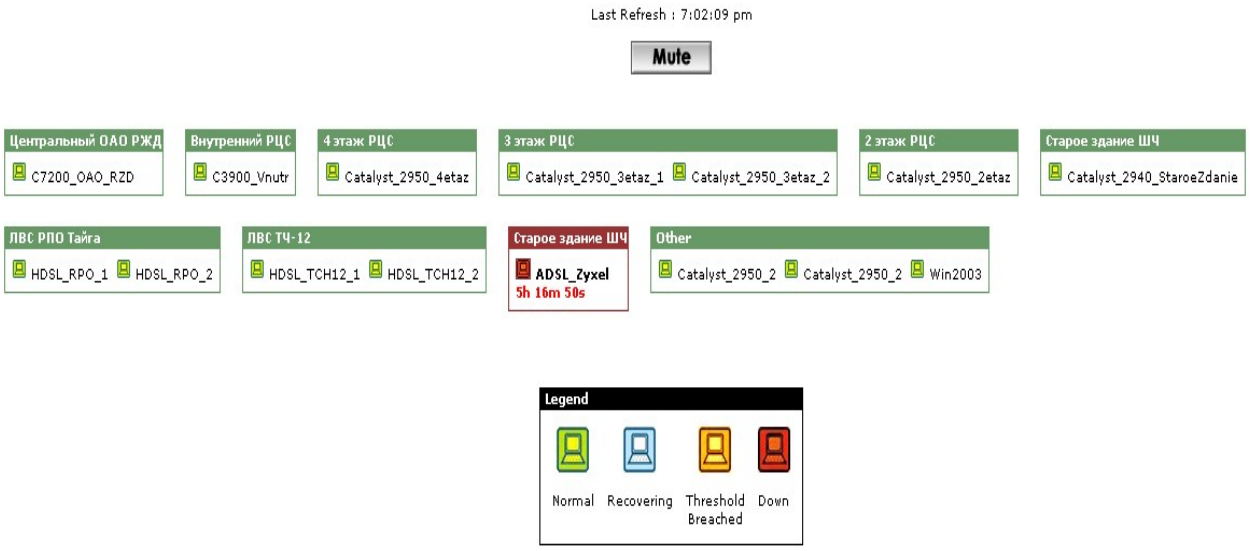


Рисунок 3.31 – Вкладка плагина «monitor»

На вкладке плагина также можно посмотреть время простоя устройства в нерабочем состоянии. Если навести курсор на иконку устройства, то появится всплывающее окошко с параметрами устройства, кликнув на иконку устройства, можно просмотреть графики, принадлежащие

данному устройству. Все устройства сгруппированы по их физическому месторасположению для облегчения восприятия информации.

3.6.4 Плагин Weathermaps

Данный плагин позволяет создавать карту сети и линии связи между сетевыми устройствами. На карту сети наносятся все сетевые устройства и линии связи между ними. Для создания карты сети используется Weathermap Editor, в нем можно выбрать иконки устройств и то, какие параметры будут отображать линии связи. Линии связи можно настроить на отображение многих параметров, например, на отображение загрузки каналов связи или отображение количества ошибок в канале.

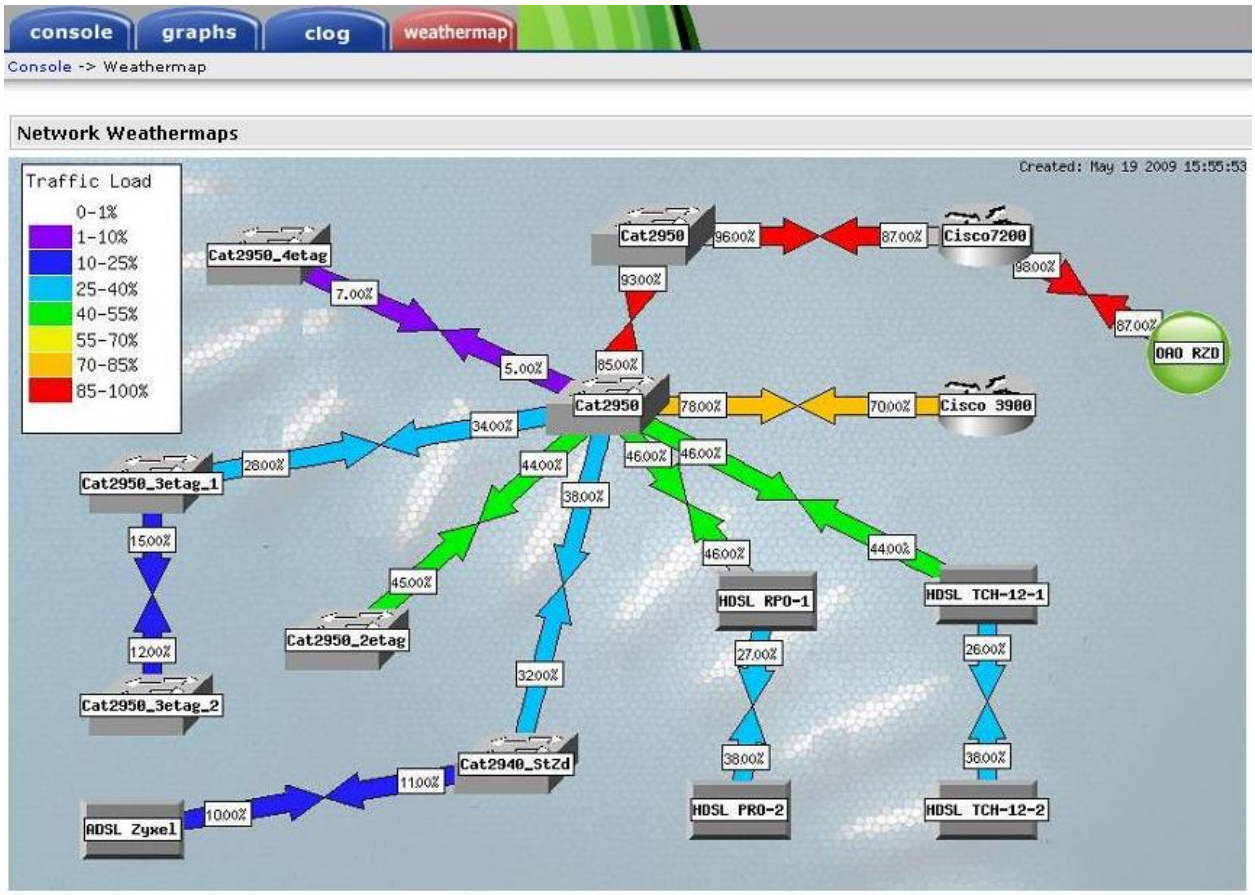


Рисунок 3.32 – Вкладка плагина Weathermap

На рисунке изображена сеть РЦС, линии между сетевыми устройствами отображают каналы связи. Цвет линии обозначает загруженность канала связи: красный цвет обозначает максимальную загрузку, фиолетовый минимальную. Как видно из рисунка, максимальная

загрузка сети наблюдается на маршрутизаторе, так как там канал пропускной способностью 2Мбит\сек. Моделирование сети производилось с помощью эмулятора сетевого оборудования, но была как можно реалистичнее воспроизведена ситуация, которая существует на предприятии. Данные для обрисовки сети берутся из круговых баз данных RRD, как и данные для построения графиков.

3.7 Разработка скриптов на языке xml для опроса оборудования по SNMP

Одной из основных задач системы мониторинга на предприятии РЦС-3, является отслеживание загрузки интерфейса на маршрутизаторе, который осуществляет передачу данных в сеть ОАО РЖД. Для осуществления передачи данных в сеть ОАО РЖД используется маршрутизатор Cisco 7200, для данного маршрутизатора отсутствуют скрипты опроса загрузки интерфейса.

Так как вышеупомянутые скрипты отсутствуют, их необходимо написать. Для написания скриптов можно использовать различные языки программирования: Perl, PHP. Для написания данного скрипта будет использован язык xml. Скрипт, который будет разработан, необходим для опроса оборудования и получения информации от него. Принцип работы скрипта следующий: при срабатывании поллера вызывается данный скрипт, который передает определенные OID программе NetSnmp, та в свою очередь опрашивает устройство и получает от него данные, полученные данные передаются обратно скрипту, а затем на обработку системе мониторинга. В результате всех действий в базу данных запишется результат опроса устройства, а при запросе пользователя сформируется необходимый график.

Далее будет представлен разработанный скрипт и прокомментированы основные строки.

Скрипт для отслеживания загрузки интерфейса:

<interface>

<name>Interfaces</name> // название скрипта

<description>Querie for a list of monitorable interfaces</description>

<oid_index>.1.3.6.1.2.1.2.2.1.1</oid_index> // запрос индекса интерфейса

<oid_num_indexes>.1.3.6.1.2.1.2.1.0</oid_num_indexes> // запрос номера интерфейса

<index_order>ifDescr:ifName:ifHwAddr:ifIndex</index_order> // имена переменных принятых в MIB для опроса интерфейсов

<index_order_type>numeric</index_order_type>

<index_title_format>|chosen_order_field|</index_title_format>

<fields>

<ifIndex>

<name>Index</name>

<method>walk</method>

<source>value</source>

<direction>input</direction>

<oid>.1.3.6.1.2.1.2.2.1.1</oid>

</ifIndex>

<ifOperStatus>

<name>Status</name>

<method>walk</method>

<source>value</source>

<direction>input</direction>

<oid>.1.3.6.1.2.1.2.2.1.8</oid> // запрос статуса

</ifOperStatus>

<ifDescr>

<name>Description</name>

<method>walk</method>

<source>value</source>

<direction>input</direction>
<oid>.1.3.6.1.2.1.2.2.1.2</oid> // запрос описания интерфейса
</ifDescr>
<ifName>
<name>Name (IF-MIB)</name>
<method>walk</method>
<source>value</source>
<direction>input</direction>
<oid>.1.3.6.1.2.1.31.1.1.1.1</oid> // запрос имени интерфейса
</ifName>
<ifAlias>
<name>Alias (IF-MIB)</name>
<method>walk</method>
<source>value</source>
<direction>input</direction>
<oid>.1.3.6.1.2.1.31.1.1.1.18</oid> // запрос алиаса
</ifAlias>
<ifType>
<name>Type</name>
<method>walk</method>
<source>value</source>
<direction>input</direction>
<oid>.1.3.6.1.2.1.2.2.1.3</oid> // запрос метки
</ifType>
<ifSpeed>
<name>Speed</name>
<method>walk</method>

<source>value</source>

<direction>input</direction>

<oid>.1.3.6.1.2.1.2.2.1.5</oid> // запрос скорости на которой работает интерфейс

</ifSpeed>

<ifInOctets>

<name>Bytes In</name>

<method>walk</method>

<source>value</source>

<direction>output</direction>

<oid>.1.3.6.1.2.1.2.2.1.10</oid> // запрос количества принятых байт

</ifInOctets>

<ifOutOctets>

<name>Bytes Out</name>

<method>walk</method>

<source>value</source>

<direction>output</direction>

<oid>.1.3.6.1.2.1.2.2.1.16</oid> // запрос количества переданных байт

</ifOutOctets>

<ifIP>

<name>IP Address</name>

<method>walk</method>

<source>OID/REGEXP:.*\.([0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3})$</source>

<direction>input</direction>

<oid>.1.3.6.1.2.1.4.20.1.2</oid> // запрос на получение ip адреса устройства

</ifIP>
</fields>
</interface>.

После написания скрипт необходимо импортировать в программу, для этого файл скрипта копируется в папку по адресу E:\Apache2.2\htdocs\cacti\scripts\. Затем заходим в веб-интерфейс Cacti, в главной консоли управления выбираем пункт «Import Templates», затем нажимаем кнопку «Обзор» и в открывшемся окне выбираем файл скрипта. После этого скрипт готов к работе и Cacti «знает», как обрабатывать его.

Для того чтобы данный скрипт можно было применять к маршрутизатору cisco 7200, необходимо ассоциировать скрипт с устройством. Для того чтобы ассоциировать скрипт с устройством необходимо в главной консоли выбрать пункт «Host Templates», затем выбрать интересующее нас устройство и в выпадающем меню выбрать необходимый скрипт. Теперь можно добавить график к устройству. Для добавления графика к устройству в главной консоли выбираем «New Graphs», затем устройство и добавляем необходимый график. После добавления графика к устройству этот график следует добавить в дерево графиков. Когда все пункты будут выполнены и пройдет 2 цикла поллера, можно увидеть вновь построенный график. График, построенный с помощью разработанного скрипта, представлен на рисунке 3.33.

После того как график начнет отображать загрузку интерфейса, необходимо настроить плагин «Thresholds», для того чтобы при превышении определенного лимита загрузки интерфейса, администратору сети отправлялось электронное сообщение. Также можно подключить к системе мониторинга все компьютеры сети и отслеживать загрузку интерфейсов на них, тогда не составит труда выяснить кто генерировал большое количество трафика и было ли это санкционировано и необходимо для работы. Таким

образом можно контролировать количество служебного трафика и трафика, генерируемого просто так, и вовремя реагировать на это.

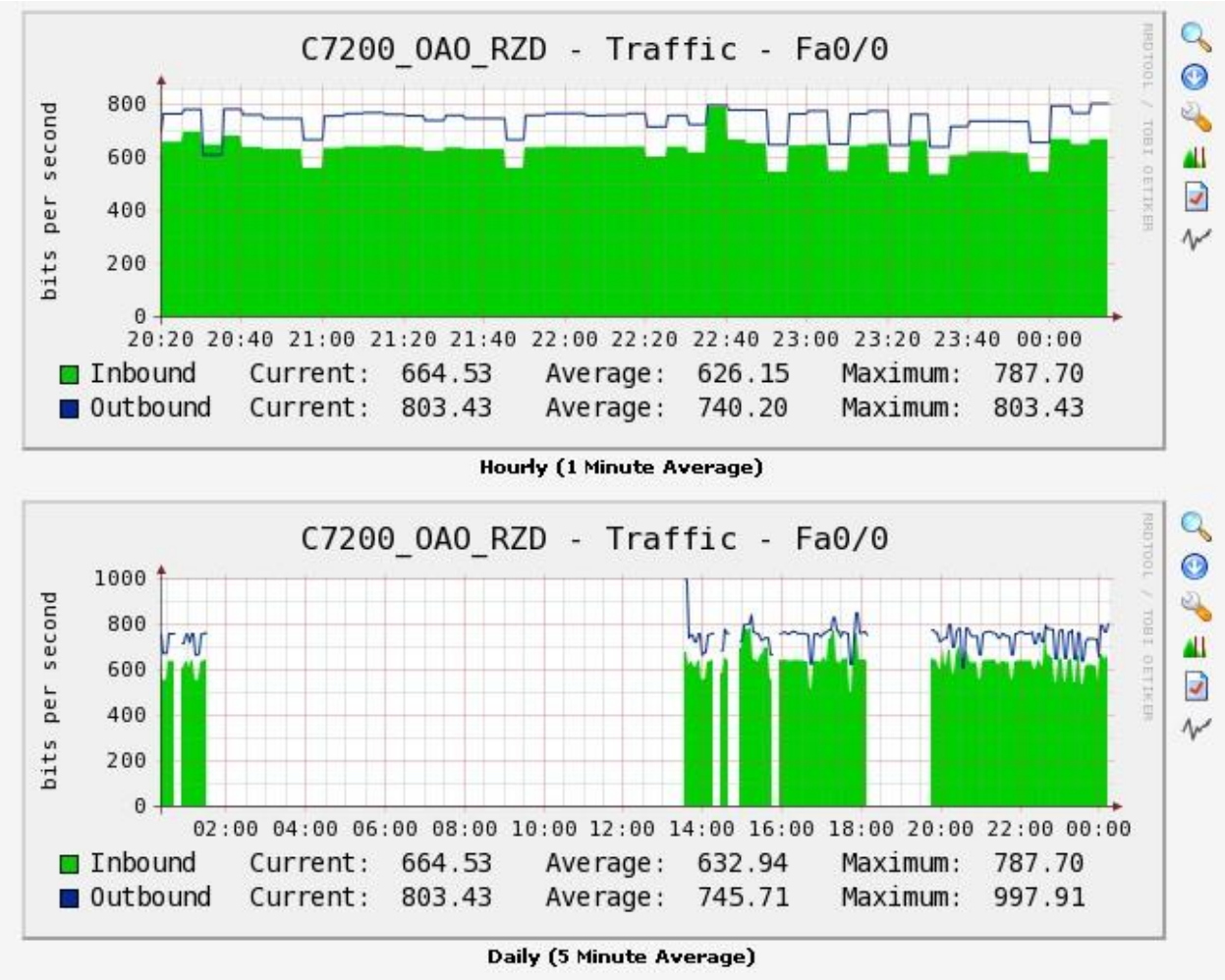


Рисунок 3.33 – График загрузки интерфейса маршрутизатора

4 Оценка затрат на создание системы мониторинга сетевого оборудования РЦС-3

4.1 Основные составляющие стоимости программного средства

Расчетной базой стоимости (цены) проектирования или создания программного средства (ПС) является определение себестоимости.

Под ПС следует понимать программу или совокупность программ на носителе данных, снабженную программной документацией (эксплуатационной и для сопровождения), разработанную в соответствии с принятыми регламентирующими документами и прошедшую необходимые испытания.

Себестоимость – это денежное выражение затрат предприятия на создание и реализацию продукции. Себестоимость связана с такими показателями как прибыль и рентабельность, поэтому имеет важное значение для экономики предприятия.

Структура и размер затрат, входящих в себестоимость программного продукта, определяются условиями его создания.

Наиболее сложным при определении стоимости программного продукта является установление временных затрат на его разработку. Для определения затрат времени на разработку ПС, установления численности специалистов, выполняющих эту работу, а также для определения трудоемкости разработки до начала работ используют укрупненные нормы времени (УНВ), в основу разработки которых положены фотохронометрические наблюдения, данные оперативного учета и отчетности, результаты анализа организации труда ряда конкретных проектов и мероприятия по его совершенствованию.

УНВ на разработку ПС охватывают работы на всех стадиях разработки:

– техническое задание (ТЗ);

– эскизный проект (ЭП);

– технический проект (ТП);

– рабочий проект (РП);

– внедрение (ВН).

Некоторые стадии разработки ПС могут отсутствовать (например, стадия ЭП) или объединяться друг с другом (например, стадии ТП и РП). Конкретный состав стадий разработки определенного ПС устанавливается в ТЗ на разработку этого ПС.

УНВ рассчитаны с учетом следующих факторов, влияющих на трудоемкость разработки ПС:

– объем;

– сложность;

– степень новизны;

– условия и средства разработки ПС (тип ЭВМ и операционной системы, языки и системы программирования, используемые СУБД и технологические средства, в том числе CASE-средства);

– степень использования в разработке стандартных модулей и типовых программ.

4.2 Расчет трудоемкости разработки программного средства

В соответствии с исходными данными (пункт а) по каталогу функций ПС определяем объем каждой из функций разрабатываемой системы мониторинга сетевого оборудования. Объемы функций в условно-машинных командах (УМК) представлены в таблице 4.1.

Таблица 4.1 – Объемы функций разрабатываемого ПС

Наименование (содержание) функции	Номер функции	Объем функции, УМК
Управление работой компонентов ПС	101	3560
Ввод данных в интерактивном режиме	103	1680
Вывод данных в табличной форме на экран и на печать	104	3740
Обработка ошибочных ситуаций	105	5790
Система настройки ПС на условия применения	106	3270
Обработка записей базы данных	205	2750
Общий объем (сумма объемов функций)		20790

Согласно формуле (4.1) определяем общий объем разрабатываемого ПС как сумму объемов частей, реализующих отдельные функции:

$$V_O = \sum_{i=1}^{n} V_i \,, \tag{4.1}$$

где V_i – объем i-й функции ПС;

n – общее число функций ПС.

$$V_O = V_1 + V_2 + ... + V_{10} = 20790 \ .$$

Сложность ПС учитывается по одиннадцати основным и пяти дополнительным характеристикам, отражающим наличие в ПС элементов повышенной сложности (интеллектуальный интерфейс, машинная графика и др.).

Сначала определим группу сложности ПС. Особенностями разрабатываемой системы является наличие машинной графики, которая позволяет создавать графические описания измерений проводимых данной системой. Также система создает файлы и сортирует их. По наличию этих характеристик согласно таблице 5 методических указаний [11] определяем, что ПС относится к 2-ой (средней) группе сложности.

Кроме того, разрабатываемая программа предназначена для моделирования процессов. Таким образом, она обладает тремя основными характеристиками, отражающими наличие элементов повышенной сложности.

К дополнительным характеристикам повышения сложности программы относятся:

– наличие экранных подсказок и меню функций (K_1 = 0,06);

– возможность связи с другими ПС (K_4 = 0,08).

С учетом перечисленных дополнительных характеристик определяем коэффициент сложности ПС:

$$K_{сл} = 1 + \sum_{i=1}^{n} K_i \ , \qquad (4.2)$$

где K_i, – коэффициент, учитывающий уровень повышения сложности по i-й дополнительной характеристике ПС;

n – количество дополнительно учитываемых характеристик ПС.

$$K_{сл} = 1 + \sum_{i=1}^{4} K_i = 1 + 0{,}06 + 0{,}08 = 1{,}14.$$

Базовая трудоемкость разработки ПС определяется по таблице 4 методических указаний в зависимости от группы сложности ПС и от объема ПС. Для 2-ой группы сложности и объема ПС V_o = 20790 УМК определяем два ближайших значения базовой трудоемкости:

– для V_{01} = 20000 УМК $T_{б1}$ = 2858 чел.-дней (норма № 15);

– для V_{02} = 22000 УМК $T_{б2}$ = 2957 чел.-дней (норма № 16).

Методом линейной интерполяции определяем:

$$T_б = T_{б1} + \frac{(T_{б1} - T_{б2}) \cdot (V_o - V_{o1})}{V_{o2} - V_{o1}}, \qquad (4.3)$$

$$T_б = 2858 + \frac{(2957 - 2858) \cdot (20790 - 20000)}{22000 - 20000} \approx 2898 \text{чел.} - \text{дней}$$

Трудоемкость разработки ПС с учетом конкретных условий и используемых средств определяется по формуле:

$$T_{у.р.} = T_б \cdot K_{у.р.}, \qquad (4.4)$$

где $K_{у.р.}$ – поправочный коэффициент, учитывающий конкретные условия и средства разработки ПС.

Коэффициент $K_{у.р.}$ определяем по таблице 8 методических указаний. Программа разрабатывается на языке сценариев PHP и системой программирования на основе СУБД типа SQLServer и ЭВМ типа IBM PC с

операционной системой Windows XP с использования локальных или глобальных сетей. Для этих условий разработки $K_{у.р.} = 0{,}19$.

Рассчитываем по формуле (4.4) скорректированное значение трудоемкости разработки ПС с учетом конкретных условий и средств разработки:

$$T_{у.р.} = 2898 \cdot 0{,}19 \approx 551 \text{ чел.-дней.}$$

Приближенная общая трудоемкость разработки ПС рассчитывается по формуле:

$$T_о = T_{у.р.} \cdot K_{сл}, \quad (4.5)$$

$$T_о = 551 \cdot 1{,}28 \approx 706 \text{ чел.-дней.}$$

Определим трудоемкость каждой стадии разработки ПС. Создание системы мониторинга сетевого оборудования предусматривает проведение трех стадий разработки, содержание которых описано в таблице 4.2.

Таблица 4.2 – Стадии разработки ПС системы мониторинга сетевого оборудования

Стадия разработки	Содержание работ
ТЗ (анализ)	Определение целей разработки системы. Изучение информации о структуре и составе сети.
ТРП (проектирование и реализация)	Изучение технологий и протоколов сетевого мониторинга. Разработка необходимых компонентов приложения.
ВН (внедрение)	Проверка на соответствие ТЗ. Внедрение системы.

Так как ПС разрабатывается без применения CASE-технологии, то трудоемкость каждой отдельной стадии разработки T_i (кроме стадии РП), определяется по формуле:

$$T_i = L_i \cdot K_н \cdot T_o \,, \qquad (4.6)$$

где L_i – удельный вес трудоемкости i-й стадии разработки;

$K_н$ – поправочный коэффициент, учитывающий степень новизны ПС.

Трудоемкость стадии РП:

$$T_{РП} = L_{РП} \cdot K_н \cdot K_т \cdot T_o \,, \qquad (4.7)$$

где $K_т$ – поправочный коэффициент, учитывающий степень использования в разработке типовых (стандартных) программ и ПС.

ТП и РП объединяются в стадию «Технорабочий проект» (ТРП), поэтому трудоемкость стадии ТРП определяется суммированием 85 процентов от трудоемкости стадии ТП и 100 процентов трудоемкости стадии РП.

Значение поправочного коэффициента $K_н$, учитывающего степень новизны ПС и оцениваемого экспертно, определяется по таблице 1 методических указаний. Система мониторинга разрабатывается на основе известных программ (Cacti, RRDTool и др.), предназначена для использования на известном типе ЭВМ (IBM PC) и в распространенной операционной системе Windows XP. Поэтому в соответствии с таблицей 1, ПС имеет степень новизны «В», а значение коэффициента новизны составляет $K_н$ = 0,7.

Значение удельного веса трудоемкости i-й стадии разработки L_i зависит от степени новизны разрабатываемого ПС и определяется по таблице 2 методических указаний. Коэффициенты удельных весов стадий разработки программы, имеющей степень новизны «В» и разрабатываемой без применения CASE-технологии, приведены в таблице 4.3.

Так как стадия ЭП не предусмотрена в ТЗ, то удельный вес трудоемкости стадии ТП определяется по формуле:

$$L_{ТП} = L_{ЭП} + L_{ТП}. \qquad (4.8)$$

$$L_{ТП} = 0{,}19 + 0{,}28 = 0{,}47.$$

Таблица 4.3 – Значения коэффициентов удельного веса трудоемкости стадий разработки

Код степени новизны	Значение коэффициентов L_i без применения CASE-технологии			
В	L_1 (ТЗ)	L_2 (ТП)	L_3 (РП)	L_4 (ВН)
	0,08	0,47	0,34	0,11

Значение поправочного коэффициента K_m, учитывающего степень использования в разработке типовых (стандартных) программ и оцениваемого экспертно, определяется по таблице 3 методических указаний.

Для разработки системы мониторинга используются стандартные компоненты среды разработки PHP, которые относятся к типовым программным средствам. Их доля составляет около 60% разработки, поэтому коэффициент $K_m = 0{,}6$.

После определения всех поправочных коэффициентов вычисляем по формулам (4.6) и (4.7) трудоемкость каждой стадии разработки, чел. – дней:

$$T_{ТЗ} = 0{,}08 \cdot 0{,}7 \cdot 706 = 40;$$

$$T_{ТП} = 0{,}47 \cdot 0{,}7 \cdot 706 = 233;$$

$$T_{РП} = 0{,}34 \cdot 0{,}7 \cdot 0{,}6 \cdot 706 = 101;$$

$$\text{Т}_{\text{ТРП}} = 0{,}85 \cdot \ 233 + 1 \cdot \ 101 = 300;$$

$$T_{ВН} = 0{,}11 \cdot 0{,}7 \cdot 706 = 55.$$

Общая трудоемкость разработки ПС определяется по формуле, чел.-дней:

$$T_{общ} = \sum_{i=1}^{n} T_i \,, \qquad (4.9)$$

где T_i – трудоемкость i-й стадии разработки ПС, чел.-дней;

n – количество стадий разработки ПС.

$$T_{общ} = 40 + 300 + 55 \approx 395 \text{ чел.-дней.}$$

Необходимый срок реализации ПС можно определить по формуле:

$$t = \sum_{i=1}^{n} \frac{t_i}{N_i \Phi}, \tag{4.10}$$

где t – время, необходимое для разработки ПС, лет;

n – число стадий разработки ПС;

t_i – трудоемкость i-й стадии разработки ПС, чел.-дней;

N_i – количество разработчиков, принимающих участие в разработке ПС на i-й стадии, чел.;

Φ – фонд рабочего времени одного разработчика, дней в год.

Если сроки разработки ПС заданы, то их соблюдения добиваются путем подбора нужного количества разработчиков на каждой стадии разработки ПС. В нашем случае конкретный срок сдачи проекта не задан, поэтому будем считать, что на всех стадиях достаточно одного разработчика, т.е. N_i = 1. Количество стадий разработки n = 3, а годовой фонд рабочего времени по пятидневной рабочей неделе с учетом праздников и выходных составляет 250 дней. Необходимые сроки реализации стадий приведены в таблице 4.4.

Таблица 4.4 – Расчет времени разработки ПС

Стадия	Трудоемкость, чел.-дней	Количество работников	Годовой фонд, дни	Время разработки ПС на стадии, лет
ТЗ	40	1	250	0,16
ТРП	300	1	250	1,2
ВП	55	1	250	0,22
Итого время разработки ПС				1,58

Для того чтобы рассчитать затраты машинного времени T_i, (т.е. количество часов работы ЭВМ) при разработке ПС, необходимо определить эти затраты на каждой стадии разработки ПС в процентном отношении от

трудоемкости соответствующей стадии (выраженной в чел.-днях) с помощью коэффициентов $К_{м.в.}$ по формуле:

$$t_{м.в.i} = K_{м.в.} T_i \, , \qquad (4.11)$$

где $t_{м.в.i}$ – количество часов работы ЭВМ на i-й стадии разработки ПС;

$К_{м.в.}$ – коэффициент перевода T_i в $t_{м.в.i}$, пропорциональный удельному весу длительности работы ЭВМ в общей трудоемкости i-й стадии разработки ПС.

Результаты расчета машинного времени приведены в таблице 4.5.

Таблица 4.5 – Затраты машинного времени

Характер разработки ПС	Код стадии	Удельный вес работы ЭВМ в трудоемкости стадии, %	Значение коэффициента $К_{м.в.}$	Затраты машинного времени $t_{м.в.i}$, ч
Без применения CASE-технологии	ТЗ	20	1,6	64
	ТРП	60	4,8	1440
	ВН	80	6,4	352
Итого затраты машинного времени				1856

4.5 Расчет затрат на разработку программного средства

При расчете заработной платы необходимо ориентироваться на принятые в данной отрасли и на предприятии порядок оплаты труда, разрядность работы исполнителей, затраты времени на условия и разработку ПС, предусмотренные виды надбавки и доплаты.

В общем случае основная заработная плата исполнителей определяется по формуле, р.:

$$ФЗП_{осн} = Ч_{яв} \cdot О \cdot Т_{общ} \cdot К_{н.д.}, \quad (4.12)$$

где $Ч_{яв}$ – явочная численность работников, чел.;

$О$ – оклад (месячная тарифная ставка), р.;

$Т_{общ}$ – общая трудоемкость разработки ПС, чел.-дней;

$К_{н.д.}$ – коэффициент, учитывающий надбавку и доплату.

Электроник 1 категории на железной дороге имеет 11-ый тарифно-квалификационный разряд, месячная тарифная ставка по которому составляет 12741,5 р. Размер премии составляет 10% от оклада. Районный коэффициент для кемеровской области равен 30%. Фонд основной заработной платы рассчитывается как сумма перечисленных составляющих:

$$ФЗП_{окл} = 1 \cdot 12741{,}5 \cdot \frac{395 \cdot 12}{250} = 241578{,}84 \text{р.};$$

$$ФЗП_{пр} = ФЗП_{окл} \cdot 0{,}1 = 24157{,}88 \text{ р.};$$

$$ФЗП_{р.к.} = (ФЗП_{окл} + ФЗП_{пр}) \cdot 0{,}30 = 79721{,}02 \text{ р.};$$

$$ФЗП_{осн.} = ФЗП_{окл} + ФЗП_{пр} + ФЗП_{р.к.};$$

$$ФЗП_{осн.} = 241578{,}84 + 24157{,}88 + 79721{,}02 = 345457{,}74 \text{ р.}$$

Дополнительная заработная плата устанавливается в процентах от основной и может быть принята в размере 10%.

$$ФЗП_{доп} = 345457{,}74 \cdot 0{,}10 = 34545{,}77 \text{ р.}$$

Общий фонд заработной платы:

$$ФЗП_{общ} = 345457{,}74 + 34545{,}77 = 380003{,}51 \text{ р.}$$

Итоги расчета фонда заработной платы сведены в таблицу 4.6.

Таблица 4.6 – Расчет фонда заработной платы (в рублях)

Разряд	Трудоемкость, чел.-дней	Оклад	Надбавка и доплата		Дополнительная заработная плата	Месячный фонд заработной платы	Фонд заработной платы на весь объем работ
			премия	по районному коэфф.			
11	395	12741,5	1274,15	3822,45	1783,81	19622,26	380003,51

Отчисления по единому социальному налогу рассчитываются в процентном отношении от общего фонда заработной платы (основного и дополнительного). Для условий разработки на железной дороге ставка принимается в размере 26,7 %. Таким образом:

$$C_{ECH} = 380003{,}51 \cdot 0{,}267 = 101460{,}94 \text{ р.}$$

Размер амортизационных отчислений зависит от принятого на предприятии метода расчета. В ОАО РЖД принят линейный метод начисления амортизации, при котором амортизационные отчисления определяются по формуле, р.:

$$C_a = K \cdot H_a \frac{T_{общ}}{T_г} \cdot 10^{-2}, \quad (4.13)$$

где K – первоначальная или восстановительная стоимость ЭВМ, р.;

H_a – норма амортизационных отчислений, %;

$T_г$ – календарный годовой фонд времени, дни.

Норма амортизационных отчислений при применении линейного метода определяется по формуле:

$$H_a = \frac{1}{n} \cdot 100\%, \quad (4.14)$$

где n – срок полезного использования ЭВМ, лет (n = 5).

$$H_a = \frac{1}{5} \cdot 100\% = 20\%.$$

Возьмем первоначальную стоимость ЭВМ K = 14000 р. Время работы оборудования за время выполнения проекта $T_г$ = 250 дней, $T_{общ}$ = 395 дней. Тогда общий размер амортизационных отчислений составит:

$$C_a = 14000 \cdot 20 \cdot \frac{395}{250} \cdot 10^{-2} = 4424 \text{ р.}$$

Расходы на электрическую энергию рассчитываются по формуле, р.:

$$C_Э = Ц_Э Э_Э, \quad (4.15)$$

где $Ц_Э$ – тариф на электрическую энергию, р./кВт·ч.;

$Э_Э$ – расчетное потребление количества электрической энергии, кВт·ч,

$$Э_Э = П_у P_у T_у, \quad (4.16)$$

где $П_у$ – количество оборудования данного вида;

$P_у$ – установленная мощность оборудования, кВт;

$T_у$ – фонд работы оборудования, ч.

При расчете потребления электроэнергии учитываем, что в среднем потребляется мощность $P_у$ = 330 Вт (ЖК монитор – 30 Вт, системный блок – 300 Вт). Фонд работы оборудования $T_у$ = 3891 ч. (таблица 4.5). В Кемеровской области установлен тариф на электрическую энергию для организаций $Ц_Э$ = 1, 6623 р./кВт·ч. Тогда расходы на электроэнергию составят:

$$Э_Э = 1 \cdot 0{,}33 \cdot 3891 = 1284{,}03 \text{ кВт·ч;}$$

$$C_Э = 1{,}6623 \cdot 1284{,}03 = 3548{,}08 \text{ р.}$$

Накладные расходы – это затраты на содержание аппарата управления, обслуживание работников и организацию работ, в данном случае составляют 12,36% от суммы всех затрат при разработке ПС.

$$C_Н = (C_{ЕСН} + C_Э + C_{АМ} + ФЗП_{общ}) \cdot 0{,}1236.$$

$$C_Н = (101460{,}94 + 3548{,}08 + 4424 + 380003{,}51) \cdot 0{,}1236 = 60494{,}36 \text{ р.}$$

Себестоимость разработки ПС определяется как сумма рассчитанных выше статей (основная и дополнительная заработная плата, отчисления по единому социальному налогу, амортизационные отчисления, затраты на электроэнергию, накладные расходы).

Результаты расчета себестоимости представлены в таблице 4.7.

Таблица 4.7 – Структура затрат на разработку ПС

Наименование статьи затрат	Сумма, р.	Удельный вес, %
Основная заработная плата	345457,74	62,82
Дополнительная заработная плата	34545,77	6,28
Отчисления по социальному налогу	101460,94	18,45
Амортизационные отчисления	4424	0,80
Электроэнергия	3548,08	0,65
Накладные расходы	60494,36	11,00
Себестоимость	549930,89	100,00

4.6 Определение цены программного средства

Уровень цены ПС зависит от издержек производства предприятия (себестоимости) и нормативной прибыли. Кроме того, необходимо учесть налог на добавленную стоимость. Таким образом, цена ПС определяется по формуле:

$$Ц = С + П + НДС \ , \qquad (4.17)$$

где $С$ – себестоимость ПС, р.;

$П$ – сумма плановых накоплений, р.;

$НДС$ – налог на добавленную стоимость, р.

Сумма плановых накоплений $П$ устанавливается для каждого конкретного предприятия отдельно. Для ОАО РЖД эта величина составляет 6% от полной себестоимости при разработке ПС.

В соответствие с действующим законодательством налог на добавленную стоимость составляет 18% от цены ПС.

По формуле (4.17) цена ПС составит:

$$Ц = 549930{,}89 + 32995{,}85 + (549930{,}89 + 32995{,}85) \cdot 0{,}18 = 687853{,}55 \text{ р.}$$

Таким образом, цена системы мониторинга сетевого оборудования РЦС-3, составляет 687785,55 р.

5 Обеспечение требований безопасности труда при организации рабочих мест

5.1 Характеристика возможных опасных и вредных производственных факторов на рабочем месте

Факторы производственной среды оказывают существенное влияние на функциональное состояние и работоспособность оператора ЭВМ. По характеру негативного воздействия все производственные факторы можно условно разделить на две группы: опасные и вредные. Воздействие опасного производственного фактора приводит к травме или к другому резкому ухудшению здоровья. Вредные факторы воздействуют на оператора ЭВМ в течение всего трудового стажа и постепенно приводят к заболеваниям или снижению работоспособности.

Классификация опасных и вредных производственных факторов приведена в ГОСТ 12.0.003-74* (переиздан с дополнениями в 1999 г.). Опасные и вредные производственные факторы подразделяются по природе действия на четыре группы:

– физические;

– химические;

– биологические;

– психофизические.

Первые три группы включают воздействия, оказываемые производственной техникой и рабочей средой. Психофизиологические факторы характеризуют изменения состояния человека под влиянием тяжести и напряженности труда. Включение их в систему факторов производственной опасности обусловлено тем, что чрезмерные трудовые нагрузки в итоге могут также привести к заболеваниям.

Как правило, существенно влияние на работоспособность оператора ЭВМ оказывают физические и психофизические производственные факторы, а воздействие химических и биологических факторов незначительно. Поэтому в дальнейшем основное внимание будет уделено описанию физических и психофизических производственных факторов и мероприятиям по устранению или снижению их воздействия.

Согласно ГОСТ 12.0.003-74*, существует 20 видов опасных и вредных физических производственных факторов. Как правило, на оператора ЭВМ в определенных условиях могут воздействовать следующие физические факторы:

– повышенный уровень шума на рабочем месте;

– повышенная или пониженная влажность воздуха;

– повышенное напряжение в электрической цепи;

– повышенный уровень электромагнитных излучений;

– отсутствие или недостаток естественного света;

– недостаточная освещенность рабочей зоны;

– повышенная яркость света;

– пониженная контрастность;

– повышенная пульсация светового потока;

– повышенная или пониженная подвижность воздуха;

– повышенный уровень ионизирующих излучений в рабочей зоне;

– повышенный уровень статического электричества;

– повышенная напряженность электрического поля;

– повышенная напряженность магнитного поля;

– прямая и отраженная блесткость.

Опасные и вредные психофизиологические производственные факторы по характеру действия делятся на:

– физические перегрузки (статические и динамические);

– нервно-психические перегрузки (умственное напряжение и перенапряжение, монотонность труда, эмоциональные перегрузки, утомление, эмоциональный стресс, эмоциональная перегрузка).

Один и тот же опасный или вредный производственный фактор по природе своего действия может относиться одновременно к различным группам.

На рабочем месте существует опасность воздействия опасных и вредных производственных факторов, для того чтобы свести к минимуму воздействие этих факторов необходимо точное выполнение требований охраны труда.

5.2 Анализ наличия опасных зон и эффективности действия технических средств, обеспечивающих безопасность обслуживания оборудования

Электрические установки, к которым относится практически все оборудование ЭВМ, представляют для человека большую потенциальную опасность, так как в процессе эксплуатации или проведении профилактических работ человек может коснуться частей, находящихся под напряжением. Специфическая опасность электроустановок: токоведущие проводники, корпуса стоек ЭВМ и прочего оборудования, оказавшегося под напряжением в результате повреждения (пробоя) изоляции, не подают каких-либо сигналов, которые предупреждают человека об опасности. Реакция человека на электрический ток возникает лишь при протекании последнего через тело человека. Исключительно важное значение для предотвращения

электротравмотизма имеет правильная организация обслуживания действующих электроустановок ВЦ, проведения ремонтных, монтажных и профилактических работ. При этом под правильной организацией понимается строгое выполнение ряда организационных и технических мероприятий и средств, установленных действующими «Правилами технической эксплуатации электроустановок потребителей и правила техники безопасности при эксплуатации электроустановок потребителей» (ПТЭ и ПТБ потребителей) и «Правила установки электроустановок» (ПУЭ) В зависимости от категории помещения необходимо принять определенные меры, обеспечивающие достаточную электробезопасность при эксплуатации и ремонте электрооборудования. Так, в помещениях с повышенной опасностью электроинструменты, переносные светильники должны быть выполнены с двойной изоляцией или напряжение питания их не должно превышать 42 В. В ВЦ к таким помещениям могут быть отнесены помещения машинного зала, помещения для размещения сервисной и периферийной аппаратуры. В особо опасных же помещениях напряжение питания переносных светильников не должно превышать 12 В, а работа с напряжением не выше 42 В разрешается только с применением СИЗ (диэлектрических перчаток, ковриков и т.п.). Работы без снятия напряжения на токоведущих частях и вблизи них, работы проводимые непосредственно на этих частях или при приближении к ним на расстояние менее установленного ПЭУ. К этим работам можно отнести работы по наладке отдельных узлов, блоков. При выполнении такого рода работ в электроустановках до 1000 В необходимо применение определенных технических и организационных мер, таких как: ограждения расположенные вблизи рабочего места и других токоведущих частей, к которым возможно случайное прикосновение; работа в диэлектрических перчатках или стоя на диэлектрическом коврике; применение инструмента с изолирующими рукоятками, при отсутствии такого инструмента следует пользоваться

диэлектрическими перчатками. Работы этого вида должны выполнятся не менее чем двумя работниками.

В ВЦ разрядные токи статического электричества чаще всего возникают при прикосновении к любому из элементов ЭВМ. Такие разряды опасности для человека не представляют, но кроме неприятных ощущений они могут привести к выходу из строя ЭВМ. Для снижения величины возникающих зарядов статического электричества в ВЦ покрытие технологических полов следует выполнять из однослойного поливинилхлоридного антистатического линолеума. Другим методом защиты является нейтрализация заряда статического электричества ионизированным газом. В промышленности широко применяются радиоактивные нитрализаторы. К общим мерам защиты от статического электричества в ВЦ можно отнести общие и местное увлажнение воздуха.

При обслуживании оборудования необходимо применять технические средства, обеспечивающие безопасность обслуживания оборудования, а также выполнять все требования ПЭ и ПТБ.

5.3 Характеристика производственного процесса на рабочем месте

Рациональный режим труда и отдыха предусматривает соблюдение определенной длительности непрерывной работы на ПК и перерывов, регламентированных с учетом продолжительности рабочей смены, вида и категории трудовой деятельности.

Выделяют 3 вида работ, выполняемых на ПК: группа А – работа по считыванию информации с экрана с предварительным запросом, группа Б – работа по вводу информации, группа В – творческая работа в режиме диалога с ПК.

Категории тяжести и напряженности работы на ПК (I, II, III) определяются уровнем нагрузки за рабочую смену: для группы А – по суммарному числу считываемых знаков, для группы Б – по суммарному

числу считываемых или вводимых знаков, для группы В – по суммарному времени непосредственной работы на ПК.

Таблица 5.1 – Категории работ

Категория работы (по тяжести и напряженности)	Уровень нагрузки за рабочую смену при видах работы на ПК		
	Группа А кол-во знаков	Группа Б кол-во знаков	Группа В,час
I	до 20000	до 15000	до 2,0
II	до 40000	до 30000	до 4,0
III	до 60000	до 40000	до 6,0

Количество и длительность регламентированных перерывов, их распределение в течение рабочей смены устанавливается в зависимости от категории тяжести и напряженности работы на ПК и продолжительности рабочей смены.

При 8-часовой рабочей смене и работе с ПК регламентированные перерывы следует устанавливать:

– для 1 категории работ через 2 часа от начала смены и через 2 часа после обеденного перерыва продолжительностью 15 минут каждый;

– для II категории работ через 2 часа от начала рабочей смены и через 1,5-2,0 часа после обеденного перерыва продолжительностью 15 минут каждый или продолжительностью 10 минут через каждый час работы;

– для III категории работ через 1,5-2,0 часа от начала рабочей смены и через 1,5-2,0 часа после обеденного перерыва продолжительностью 20 минут каждый или продолжительностью 15 минут через каждый час работы.

При 12-часовой рабочей смене регламентированные перерывы должны устанавливаться в первые 8 часов работы аналогично перерывам при 8-часовой рабочей смене, а в течение последних 4 часов работы, независимо от категории и вида работ, каждый час продолжительностью 15 минут.

Продолжительность непрерывной работы на ПК без регламентированного перерыва не должна превышать 2 часов. При работе на ПК в ночную смену (с 22 до 6 часов) продолжительность регламентированных перерывов увеличивается на 60 минут, независимо от категории и вида трудовой деятельности. Эффективными являются нерегламентированные перерывы (микропаузы) длительностью от 1 до 3 минут. Число и распределение микропауз в течение рабочей смены устанавливается индивидуально. Регламентированные перерывы и микропаузы целесообразно использовать для выполнения комплекса упражнений и гимнастики для глаз, пальцев рук, массажа и акупрессуры. Выбор комплексов упражнений осуществляется пользователем индивидуально в зависимости от ощущений усталости. Комплексы упражнений целесообразно менять через 2-3 недели.

Для уменьшения неблагоприятного влияния монотонии рекомендуется, при возможности, чередовать виды выполняемой работы. Регламентированные перерывы желательно проводить вне рабочего места. Пользователям ПК, выполняющим работу с высоким уровнем напряженности, показана психологическая разгрузка во время регламентированных перерывов и в конце рабочего дня в специально оборудованных помещениях (комната психологической разгрузки).

С целью предупреждения нарушения здоровья все пользователи ПК проходят обязательные предварительные медицинские осмотры при поступлении на работу, а также периодические медицинские осмотры согласно действующему приказу МЗ России «О порядке проведения предварительных и периодических осмотров работников и медицинских регламентах допуска к профессии» от 14.03.1996 № 90 (ред. от 06.02.2001).

Периодические медицинские осмотры для работающих на ПК проводятся 1 раз в год в лечебно-профилактических учреждениях, с обязательным участием терапевта, невропатолога и окулиста, а также

проведением общего анализа крови и ЭКГ и 1 раз в 3 года – в центрах профилактики.

Не допускаются к работе на ПК женщины со времени установления беременности и в период кормления грудью. Близорукость, дальнозоркость и другие нарушения рефракции должны быть полностью корригированы очками. Для работы должны использоваться очки, подобранные с учетом рабочего расстояния от глаз до экрана дисплея. При более серьезных нарушениях состояния зрения вопрос о возможности работы на ПК решается врачом-офтальмологом.

Досуг рекомендуется использовать для пассивного и активного отдыха (занятия на тренажерах, плавание, езда на велосипеде, бег, игра в теннис, футбол, лыжи, аэробика, прогулки по парку, лесу, экскурсии, прослушивание музыки и т.п.).

Дважды в год (весной и поздней осенью) рекомендуется проводить курс витаминотерапии (поливитамины) в течение месяца. Следует отказаться от вредных привычек. Категорически должно быть запрещено курение на рабочих местах и в помещениях с ПК.

5.4 Эргономический анализ организации рабочего места оператора ЭВМ

К рабочему месту относится часть пространства, в котором человек преимущественно осуществляет трудовую деятельность и проводит большую часть рабочего времени. Рабочее место влияет непосредственно на безопасность труда и сохранение здоровья, повышает культуру и эффективность труда.

Согласно ГОСТ 12.2.032-78 конструкция рабочего места и взаимное расположение всех его элементов должно соответствовать антропометрическим, физическим и психологическим требованиям. Большое значение имеет также характер работы. В частности, при организации

рабочего места оператора ЭВМ должны быть соблюдены следующие требования эргономики:

– оптимальное размещение оборудования, входящего в состав рабочего места;

– достаточное рабочее пространство, позволяющее осуществлять все необходимые движения и перемещения;

– достаточная зона обзора;

– оптимальное взаимное расположение рабочих мест.

Основным рабочим положением является положение сидя, при котором утомление оператора минимально. Таким образом, выполняемая работа по степени тяжести является легкой (категория 1а), так как производится сидя и сопровождается незначительным физическим напряжением. Рабочее место для выполнения работ в положении сидя организуется в соответствии с ГОСТ 12.2.032-78. Требования к организации рабочего места оператора ЭВМ изложены в СанПиН 2.2.2/2.4.1340-03.

Элементами рабочего места оператора являются:

– рабочий стол;

– кресло;

– подставка для ног;

– устройства ввода-вывода (дисплей, клавиатура, мышь);

– основное оборудование (системный блок);

– дополнительное оборудование (принтер);

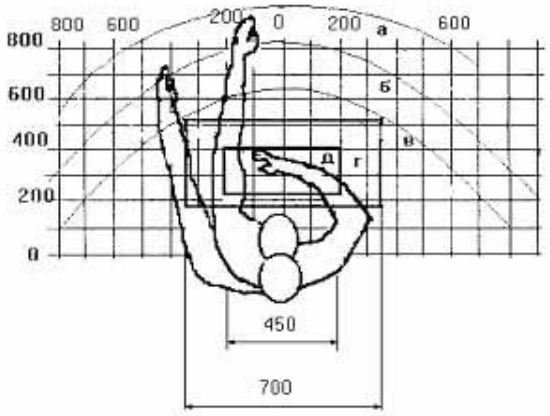
– рабочая документация.

Рациональная планировка рабочего места предусматривает четкий порядок размещения средств труда и документации. То, что требуется для выполнения работ чаще, расположено в зоне легкой досягаемости рабочего пространства.

Моторное поле – это пространство рабочего места, в котором могут осуществляться двигательные действия человека.

Максимальная зона досягаемости рук – это часть моторного поля рабочего места, ограниченная дугами, описываемыми максимально вытянутыми руками при движении их в плечевом суставе.

Оптимальная зона – это часть моторного поля рабочего места, ограниченного дугами, описываемыми предплечьями при движении в локтевых суставах с опорой в точке локтя и с относительно неподвижным плечом (рисунок 5.1).



а – зона максимальной досягаемости, б – зона досягаемости пальцев при вытянутой руке, в – зона легкой досягаемости ладони, г – оптимальное пространство для грубой ручной работы, д – оптимальное пространство для тонкой ручной работы.

Рисунок 5.1 – Зоны досягаемости рук в горизонтальной плоскости

Рассмотрим оптимальное размещение предметов труда на рабочем месте оператора ЭВМ в пределах зон досягаемости рук:

– дисплей размещается в центре зоны б на расстоянии от 600 до 700 мм от глаз пользователя;

– клавиатура – в зоне д, манипулятор мышь – в зоне г (справа);

– системный блок – в зоне б (слева);

– принтер – в зоне а (справа);

– рабочая документация размещается на свободной поверхности стола и выдвижных ящиках в пределах зоны б.

Конструкция рабочего стола обеспечивает возможность размещения на рабочей поверхности необходимого комплекта оборудования и документов с учетом характера выполняемой работы. Высота рабочей поверхности нерегулируемого по высоте стола составляет 725 мм. Размеры рабочей поверхности стола: глубина – 650 мм, ширина – 1250 мм. Рабочий стол имеет пространство для ног высотой – 675 мм, шириной – 600 мм, глубиной на уровне колен – 450 мм и на уровне вытянутых ног – 650 мм. Поверхность стола обладает свойствами, исключающими появление бликов в поле зрения программиста. В правой части стола расположены три выдвижных ящика для хранения документации, канцелярских принадлежностей и личных вещей.

Кресло обеспечивает поддержание физиологически рациональной рабочей позы оператора в процессе трудовой деятельности, создает условия для изменения позы с целью снижения статического напряжения мышц шейно-плечевой области и спины, а так же для исключения нарушения циркуляции крови в нижних конечностях. Поверхность сидения имеет ширину и глубину 400 мм. Высота опорной поверхности спинки составляет 300 мм, ширина – 400 мм.

Кресло оснащено подъемно-поворотным механизмом, позволяющим регулировать высоту и углы наклона сиденья и спинки, а также расстояние спинки от переднего края сиденья, при этом регулировка каждого параметра является независимой, легко осуществляемой и имеет надежную фиксацию. Обеспечивается регулирование высоты сидения в пределах от 400 до 550 мм и угла наклона вперед до 15 градусов, назад до 5 градусов. Спинка имеет слегка вогнутую поверхность и небольшой наклон назад, который регулируется в вертикальной плоскости пределах 30 градусов.

Сиденье и спинка кресла имеют полумягкую поверхность, с нескользящим, слабо электризующимся и воздухопроницаемым покрытием, обеспечивающим легкую очистку от загрязнений.

Рабочее место оператора ЭВМ оборудуется подставкой для ног, имеющей ширину 300 мм, глубину 400 мм, регулировку по высоте в пределах до 150 мм и по углу наклона опорной поверхности подставки до 20 градусов. Подставка имеет рифленую поверхность и бортик высотой 10 мм по переднему краю.

При расположении устройств ввода-вывода и другого оборудования следует учитывать не только зоны досягаемости рук, но и размеры информационного поля оператора. Информационное поле – это пространство, в котором расположены информационные сигналы (дисплеи, индикаторы и т.д.). Наилучший объем видения находится внутри конуса, получаемого при отклонении на 15 градусов в любом направлении от оптимальной линии взгляда, которая смещена на 15 градусов относительно горизонтальной линии взгляда. Максимальный объем видения по вертикали ограничен 90 градусами вверх и 70 градусами вниз, по горизонтали – 120 градусами влево и вправо от оптимальной линии взгляда.

В соответствии с этими требованиями дисплей устанавливается немного ниже уровня глаз оператора на расстоянии от 600 до 700 мм. Наклон поверхности экрана составляет 15 градусов относительно вертикали. Размер диагонали экрана составляет 17 дюймов. Это позволяет поместить дисплей внутри наилучшего объема видения без увеличения расстояния до экрана. Остальное оборудование размещается так, чтобы информационные индикаторы находились в пределах максимального объема видения оператора.

Клавиатура и мышь могут свободно перемещаться по поверхности стола и располагаются на расстоянии от 100 до 300 мм от переднего края, обращенного к работающему.

Аварийные органы управления располагаются в пределах зоны досягаемости моторного поля и максимального объема видения, при этом

предусматриваются специальные средства опознания и предотвращения их случайного включения или выключения.

Также существуют требования эргономики к взаимному расположению рабочих мест, согласно которым расстояние между рабочими столами с видеомониторами (в направлении тыла поверхности одного видеомонитора и экрана другого видеомонитора) выбрано равным 2,5 м, а расстояние между боковыми поверхностями видеомониторов – 1,5 м. Раздельное размещение мониторов позволяет убрать из информационного поля оператора постороннюю информацию. При выполнении работы, требующей значительного умственного напряжения или высокой концентрации внимания, рабочие места могут быть изолированы друг от друга перегородками высотой от 1,5 до 2,0 м.

5.5 Обеспечение оптимальных санитарно-гигиенических условий туда в помещениях для ЭВМ

5.5.1 Требования к помещениям для работы с ЭВМ

Помещения для эксплуатации ЭВМ должны иметь естественное и искусственное освещение. Естественное и искусственное освещение должно соответствовать требованиям действующей нормативной документации. Окна в помещениях, где эксплуатируется вычислительная техника, преимущественно должны быть ориентированы на север и северо-восток.

Оконные проемы должны быть оборудованы регулируемыми устройствами: жалюзи, занавеси, внешние козырьки и др.

Площадь на одно рабочее место пользователей ЭВМ с дисплеем на базе электроннолучевой трубки (ЭЛТ) должна составлять не менее 6 м^2, с дисплеем на базе плоских дискретных экранов (жидкокристаллические, плазменные) – 4,5 м^2.

При использовании ЭВМ с дисплеем на базе ЭЛТ (без вспомогательных устройств – принтер, сканер и др.), отвечающих требованиям международных стандартов безопасности компьютеров, с

продолжительностью работы менее четырех часов в день допускается минимальная площадь 4,5 $м^2$ на одно рабочее место пользователя.

Для внутренней отделки интерьера помещений, где расположены ЭВМ, должны использоваться диффузно-отражающие материалы со следующими коэффициентами отражения: для потолка – от 0,7 до 0,8; для стен – от 0,5 до 0,6; для пола – от 0,3 до 0,5.

Помещения, где размещаются рабочие места с ЭВМ, должны быть оборудованы защитным заземлением (занулением) в соответствии с техническими требованиями по эксплуатации.

Не следует размещать рабочие места с ЭВМ вблизи силовых кабелей и вводов, высоковольтных трансформаторов, технологического оборудования, создающего помехи в работе ЭВМ.

5.5.2 Требования к микроклимату, содержанию в воздухе аэроионов и вредных химических веществ

В производственных помещениях, в которых работа с использованием ЭВМ является основной (диспетчерские, операторские, расчетные, кабины и посты управления, залы вычислительной техники и др.) и связана с нервно-эмоциональным напряжением, должны обеспечиваться оптимальные параметры микроклимата для категории работ 1а и 1б в соответствии с действующими санитарно-эпидемиологическими нормативами микроклимата производственных помещений СанПиН 2.2.2/2.4.1340-03.

В помещениях, оборудованных ЭВМ, проводится ежедневная влажная уборка и систематическое проветривание после каждого часа работы на ЭВМ.

Уровни положительных и отрицательных аэроионов в воздухе помещений, где расположены ЭВМ, должны соответствовать действующим санитарно-эпидемиологическим нормативам (таблица 5.2).

Таблица 5.2 – Уровни ионизации воздуха помещений

Уровни	Число ионов в 1 $см^3$ воздуха

	n +	n –
Минимально необходимые	400	600
Оптимальные	от 1500 до 3000	от 30000 до 50000
Максимально допустимые	50000	50000

Содержание вредных химических веществ в производственных помещениях, в которых работа с использованием ЭВМ является основной (диспетчерские, операторские, расчетные, кабины и посты управления, залы вычислительной техники и др.), не должно превышать предельно допустимых концентраций загрязняющих веществ в атмосферном воздухе населенных мест в соответствии с действующими гигиеническими нормативами.

5.5.3 Требования к уровням шума и вибрации

В производственных помещениях при выполнении основных или вспомогательных работ с использованием ЭВМ уровни шума на рабочих местах не должны превышать 50 дБА.

При выполнении работ с использованием ЭВМ в производственных помещениях уровень вибрации не должен превышать допустимых значений вибрации для рабочих мест (категория 3, тип «В») в соответствии с действующими санитарно-эпидемиологическими нормативами (таблица 5.3).

Шумящее оборудование (печатающие устройства, серверы и т.п.), уровни шума которого превышают нормативные, должно размещаться вне помещений с ЭВМ.

Таблица 5.3 – Санитарные нормы вибрации категории 3, технологического типа «В»

Среднегеометри-ческие частоты полос, Гц	Допустимые значения по осям X0, Y0, Z0							
	Виброускорения				Виброскорости			
	$м/с^2$		дБ		$м/с \cdot 10^{-2}$		дБ	
	1/3 окт.	1/1 окт.	1/3 окт.	1/1 окт.	1/3 окт.	1/1 окт.	1/3 окт.	1/1 окт.
1,6	0,0125		32		0,1300		88	
2,0	0,0112	0,200	31	36	0,0890	0,180	85	91
2,5	0,0100		30		0,0630		82	
3,15	0,0090		29		0,0445		79	
4,0	0,0080	0,014	28	33	0,0320	0,063	76	82
5,0	0,0080		28		0,0250		74	
6,3	0,0080		28		0,0200		72	
8,0	0,0080	0,014	28	33	0,0160	0,032	70	76
10,0	0,0100		30		0,0160		70	
12,5	0,0125		32		0,0160		70	
16,0	0,0160	0,028	34	39	0,0160	0,028	70	75
20,0	0,0196		36		0,0160		70	
25,0	0,0250		38		0,0160		70	
31,5	0,0315	0,056	40	45	0,0160	0,028	70	75
40,0	0,0400		42		0,0160		70	
50,0	0,0500		44		0,0160		70	
63,0	0,0630	0,112	46	51	0,0160	0,028	70	75
80,0	0,0800		48		0,0160		70	
Корректированные и эквивалентные корректированн	1,6000	0,014		33		0,028		75

ые значения и их уровни								

5.5.4 Требования к освещению

Рабочие столы следует размещать таким образом, чтобы видеодисплейные терминалы были ориентированы боковой стороной к световым проемам, чтобы естественный свет падал преимущественно слева.

Искусственное освещение в помещениях для эксплуатации ЭВМ должно осуществляться системой общего равномерного освещения. В производственных и административно-общественных помещениях, в случаях преимущественной работы с документами, следует применять системы комбинированного освещения (к общему освещению дополнительно устанавливаются светильники местного освещения, предназначенные для освещения зоны расположения документов).

Освещенность на поверхности стола в зоне размещения рабочего документа должна быть от 300 до 500 лк. Освещение не должно создавать бликов на поверхности экрана. Освещенность поверхности экрана не должна быть более 300 лк.

Следует ограничивать прямую блесткость от источников освещения, при этом яркость светящихся поверхностей (окна, светильники и др.), находящихся в поле зрения, должна быть не более 200 кд/м^2.

Следует ограничивать отраженную блесткость на рабочих поверхностях (экран, стол, клавиатура и др.) за счет правильного выбора типов светильников и расположения рабочих мест по отношению к источникам естественного и искусственного освещения, при этом яркость бликов на экране ЭВМ не должна превышать 40 кд/м^2 и яркость потолка не должна превышать 200 кд/м^2.

Показатель ослепленности для источников общего искусственного освещения в производственных помещениях должен быть не более 20.

Показатель дискомфорта в административно-общественных помещениях не более 40.

Яркость светильников общего освещения в зоне углов излучения от 50 до 90 градусов с вертикалью в продольной и поперечной плоскостях должна составлять не более 200 кд/м^2, защитный угол светильников должен быть не менее 40 градусов.

Светильники местного освещения должны иметь не просвечивающий отражатель с защитным углом не менее 40 градусов.

Следует ограничивать неравномерность распределения яркости в поле зрения пользователя ЭВМ, при этом соотношение яркости между рабочими поверхностями не должно превышать 5:1, а между рабочими поверхностями и поверхностями стен и оборудования – 10:1.

В качестве источников света при искусственном освещении следует применять преимущественно люминесцентные лампы типа ЛБ и компактные люминесцентные лампы (КЛЛ). При устройстве отраженного освещения в производственных и административно-общественных помещениях допускается применение металлогалогенных ламп. В светильниках местного освещения допускается применение ламп накаливания, в том числе галогенных.

Для освещения помещений с ЭВМ следует применять светильники с зеркальными параболическими решетками, укомплектованными электронными пуско-регулирующими аппаратами (ЭПРА). Допускается использование многоламповых светильников с электромагнитными пуско-регулирующими аппаратами (ЭПРА), состоящими из равного числа опережающих и отстающих ветвей.

Применение светильников без рассеивателей и экранирующих решеток не допускается.

При отсутствии светильников с ЭПРА лампы многоламповых светильников или рядом расположенные светильники общего освещения следует включать на разные фазы трехфазной сети.

Общее освещение при использовании люминесцентных светильников следует выполнять в виде сплошных или прерывистых линий светильников, расположенных сбоку от рабочих мест, параллельно линии зрения пользователя при рядном расположении видеодисплейных терминалов. При периметральном расположении компьютеров линии светильников должны располагаться локализовано над рабочим столом ближе к его переднему краю, обращенному к оператору.

Коэффициент запаса для осветительных установок общего освещения должен приниматься равным 1,4.

Коэффициент пульсации не должен превышать 5%.

Для обеспечения нормируемых значений освещенности в помещениях для использования ЭВМ следует проводить чистку стекол оконных рам и светильников не реже двух раз в год и проводить своевременную замену перегоревших ламп.

5.5.5 Требования к уровням электромагнитных полей

Временные допустимые уровни (ВДУ) ЭМП, создаваемых ЭВМ на рабочих местах пользователей представлены в таблице 5.4.

Таблица 5.4 – Временные допустимые уровни ЭМП, создаваемых ЭВМ

Наименование параметров		ВДУ
Напряженность электрического поля, В/м	в диапазоне частот от 5 Гц до 2 кГц	25
	в диапазоне частот от 2 кГц до 400 кГц	2,5
Плотность магнитного потока, нТл	в диапазоне частот от 5 Гц до2 кГц	250
	в диапазоне частот	25

	от 2 кГц до 400 кГц	
Напряженность электростатического поля, кВ/м		15

5.5.6 Требования к визуальным параметрам дисплеев

Предельно допустимые значения визуальных параметров дисплеев, контролируемые на рабочих местах, представлены в таблице 5.5.

Для дисплеев на ЭЛТ частота обновления изображения должна быть не менее 75 Гц при всех режимах разрешения экрана, гарантируемых нормативной документацией на конкретный тип дисплея, и не менее 60 Гц для дисплеев на плоских дискретных экранах (жидкокристаллических или плазменных).

Таблица 5.5 – Предельно допустимые значения визуальных параметров дисплеев

Параметры	Допустимые значения
Яркость белого поля, кд/м^2, не менее	35
Неравномерность яркости рабочего поля, %, не более	± 20
Контрастность (для монохромного режима), не менее	3:1
Временная нестабильность изображения	Не должна фиксироваться
Пространственная нестабильность изображения (дрожание), мм, не более	$2 \cdot 10^{-4} \cdot L$, где L – проектное расстояние наблюдения

Охрана труда представляет собой систему законодательных, социально-экономических, организационных, технических, санитарно-гигиенических и лечебно-профилактических мероприятий и средств, обеспе-

чивающих безопасность, сохранение здоровья и работоспособность человека в процессе труда.

Охрана труда исследует трудовой процесс с позиций обеспечения его безопасности для жизни и здоровья трудящихся.

В соответствии с трудовым законодательством на всех предприятиях, в учреждениях и организациях должны быть созданы здоровые и безопасные условия труда. Обеспечение таких условий возлагается на администрацию, которая обязана внедрять современные средства техники безопасности, предупреждающие производственный травматизм, и создавать санитарно-гигиенические условия, предотвращающие возникновение профессиональных заболеваний.

Заключение

В результате работы, выполненной в рамках данного дипломного проекта, была разработана система мониторинга сетевого оборудования для предприятия РЦС-3. Разработанная система базируется на свободно распространяемом программном обеспечении, что является выгодным для предприятия с экономической точки зрения.

Разработанная система мониторинга может работать с оборудованием различных типов и различных производителей. Вся информация, собранная с различных точек контроля консолидируется в одном месте и предоставляется администратору в графическом виде (графики), отображение собранной информации в виде графиков упрощает и ускоряет анализ состояния сети и сетевого оборудования. Так же система обладает функцией удалённого оповещения администратора сети об изменении состояния контролируемого оборудования и каналов связи, путем отправки сообщения на электронный почтовый ящик.

Данная система мониторинга адаптирована для решения специфических задач на конкретном предприятии, а именно, отслеживание загрузки низкоскоростных каналов связи и предоставлении информации о том, что послужило причиной загрузки сети. Так как предприятие РЦС-3 осуществляет работу в оперативном режиме, то доступность внешних сетевых ресурсов является критически важным фактором для работы предприятия.

Представленная система мониторинга является легко масштабируемой, т.е. при перестроении сети или необходимости добавления задач мониторинга, система может быть легко модернизирована с помощью разработки новых или установки существующих плагинов. Система поддерживает практически все сетевые устройства и списки опрашиваемых параметров, но если необходимо опрашивать устройство по специфическому параметру, то можно написать скрипт для опроса устройства, что не является трудоёмким процессом.

Произведен расчет стоимости разработки программного средства для мониторинга сетевого оборудования РЦС-3. Себестоимость программного обеспечения составила около 550000 рублей с учетом всех надбавок и коэффициентов.

В заключение рассмотрены вопросы обеспечения безопасности работ по обслуживанию ЭВМ. Описаны основные вредные и опасные производственные факторы, которые могут влиять на операторов ЭВМ. Выполнен эргономический анализ рабочего места оператора. Выбраны технические средства и организационные мероприятия, обеспечивающие безопасность обслуживания ЭВМ. Приведены основные санитарно-гигиенические требования, предъявляемые к помещениям с ЭВМ.

Библиографический список

1 Configuring SNMP Support [Электронный ресурс] / Компания «Cisco Systems, Inc.» – Электрон. текстовые дан. (243990 байт) – М.: Компания «Cisco Systems, Inc.», 1992-2009. – Режим доступа: http://www.cisco.com/en/US/docs/ios/12_2/configfun/configuration/guide/fcf014.html

2 OpenNet: Полезные SNMP MIB object (OID) для Cisco [Электронный ресурс] / Maxim Chirkov – Электрон. текстовые дан. (98326 байт) – М.: Maxim Chirkov, 2005-2009. – Режим доступа: http://www.opennet.ru/openforum/vsluhforumID3/37680.html

3 Cacti: The Complete RRDTool-based Graphing Solution [Электронный ресурс] / Компания «The Cacti Group» – Электрон. текстовые дан. (123561 байт) – М.: Компания «The Cacti Group», 2004-2009. – Режим доступа: http://www.cacti.net/index.php

4 SNMP Object Navigator [Электронный ресурс] / Компания «Cisco Systems, Inc.» – Электрон. текстовые дан. (64572 байт) – М.: Компания «Cisco

Systems, Inc.», 1992-2008. – Режим доступа: http://tools.cisco.com/Support/SNMP/do/BrowseOID.do

5 Cacti Users [Электронный ресурс] / «Cactiusers.org» – Электрон. текстовые дан. (52935 байт) – М.: «Cactiusers.org», 2003-2009. – Режим доступа: http://cactiusers.org/index.php

6 Системы мониторинга и управления [Электронный ресурс] / Компания «Управление и мониторинг сетевой инфраструктуры» – Электрон. текстовые дан. (187590 байт) – М.: Компания «Управление и мониторинг сетевой инфраструктуры», 2005-2009. – Режим доступа: http://mmtools.ru/wp/?page_id=13

7 Основы PHP [Электронный ресурс] / А. Муругов. – Электрон. текстовые дан. (280240 байт) – М.: PHP.SU, 2007-2009. – Режим доступа: http://www.php.su.html

8 Ульман, Л. Основы программирования на PHP: Пер. с англ. – М.: ДМК Пресс, 2001. 288 с.

9 Курило, В.А. Выполнение раздела «Безопасность и экологичность» в дипломных проектах: методические указания для студентов электромеханических и теплоэнергетических специальностей / В.А. Курило, Л.Я. Уфимцева, Б.В. Мусаткина, О.В. Игнатов. Омск: Омский гос. ун-т путей сообщения, 2004. 35 с.

10 СанПин 2.2.2/2.4.1340 – 03. Гигиенические требования к персональным электронно-вычислительным машинам и организация работы.

11 Панычев, А.Ю. Расчет стоимости программного средства: методические указания для дипломного проектирования / А.Ю. Панычев. Омск: Омский гос. ун-т путей сообщения, 2003. 25 с.

12 СТП ОмГУПС – 1.2 – 2005. Общие требования и правила оформления текстовых документов.

13 Олифер, В.Г. Компьютерные сети. Принципы, технологии, протоколы: учебник для вузов / В.Г. Олифер, Н.А. Олифер. СПб.: Питер,

2006. 958 с.

14 Хилл, Б. Полный справочник по Cisco/ Б. Хилл. СПб.: Вильямс, 2004. 772 с.

15 Семенов, Ю.А Протоколы и ресурсы Интернет / Ю.А. Семенов М.: Радио и связь 2004. 464 с.

Приложение А

(обязательное)

Графический материал

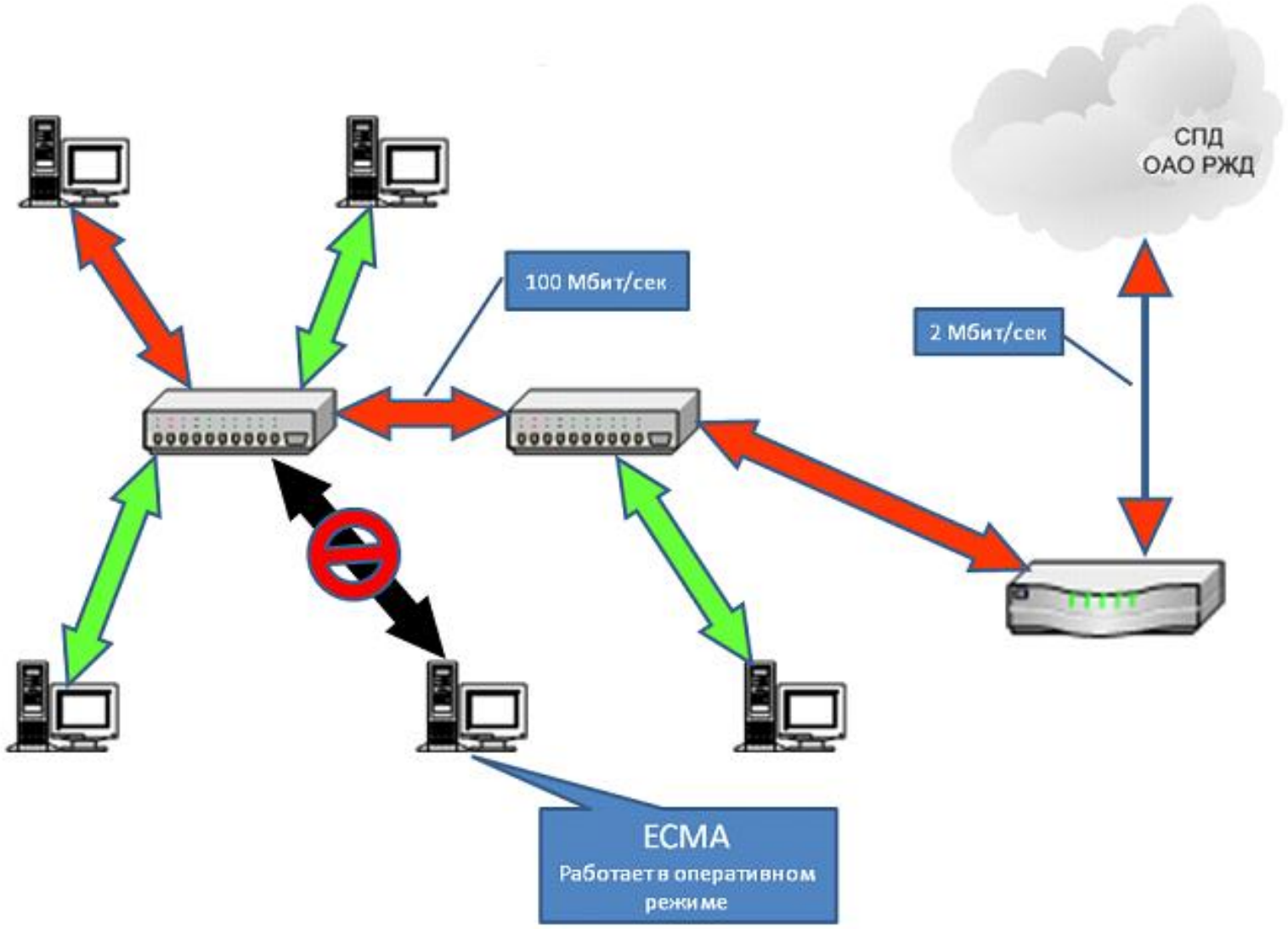


Рисунок А.1 – Проблемы перегруженности СПД

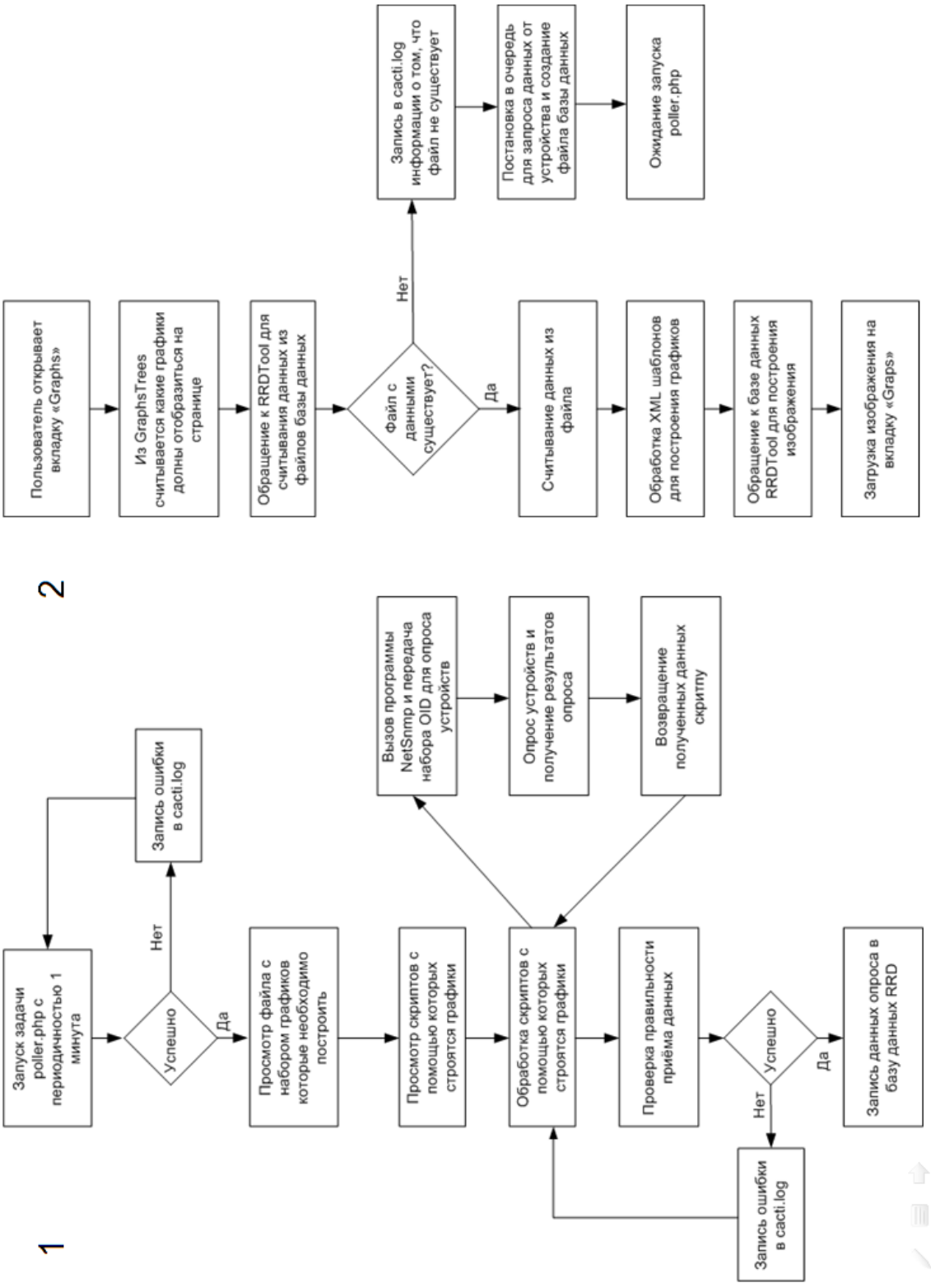


Рисунок А.2 – Алгоритм работы программы

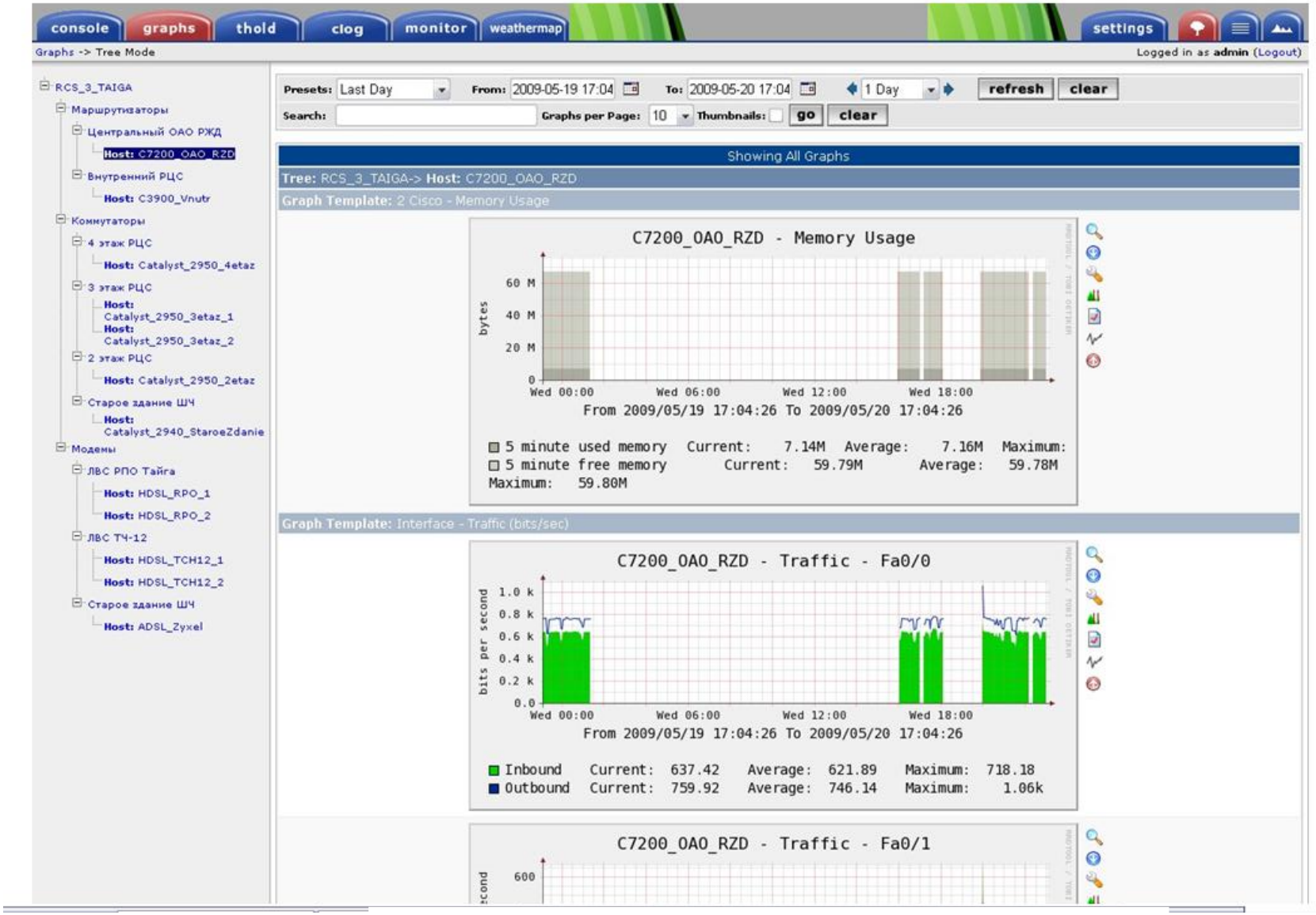


Рисунок А.3 – Отображение собранной информации

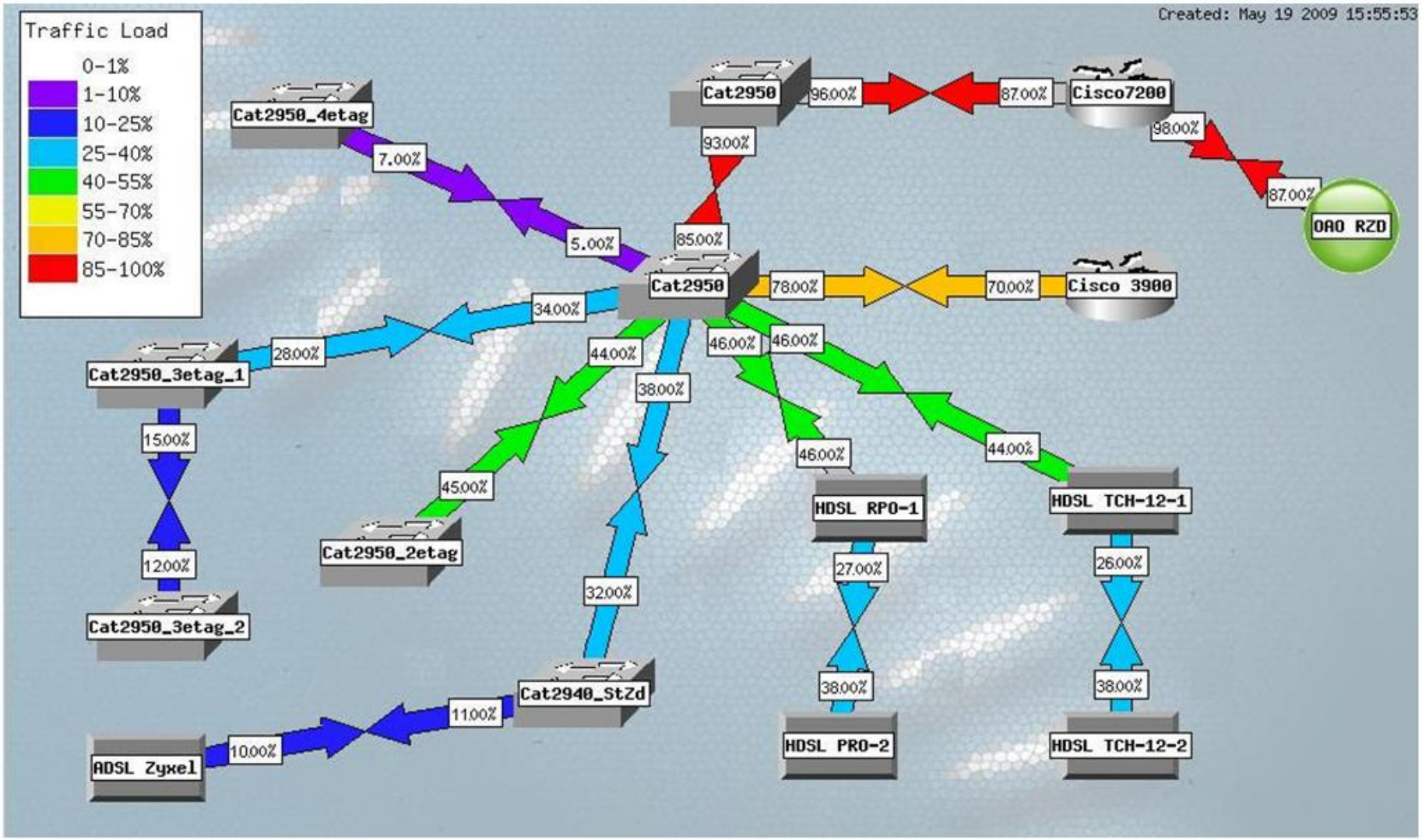
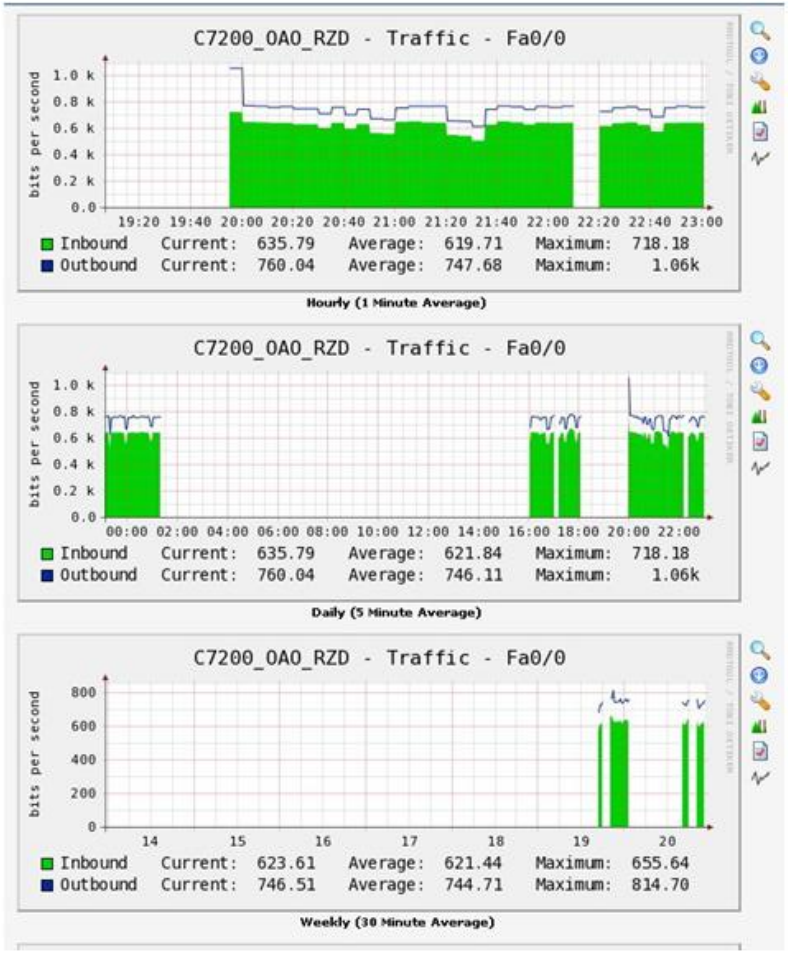


Рисунок А.4 – Карта сети



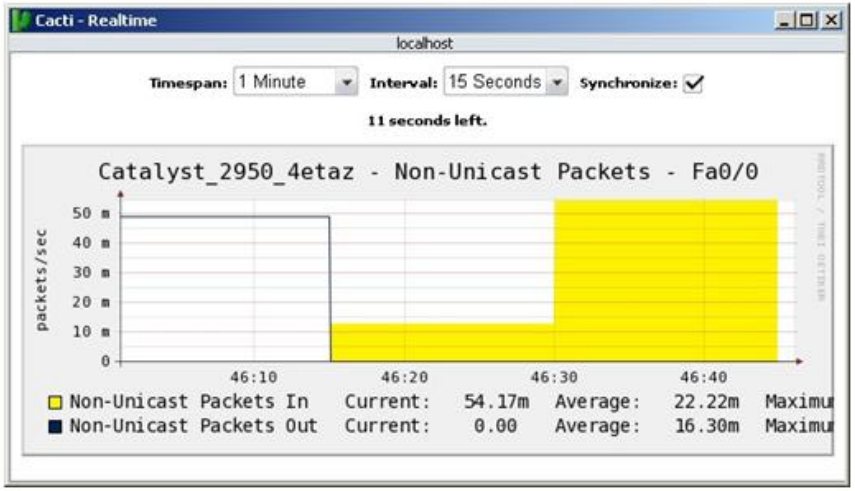


Рисунок А.5 – Временные интервалы отображения графиков

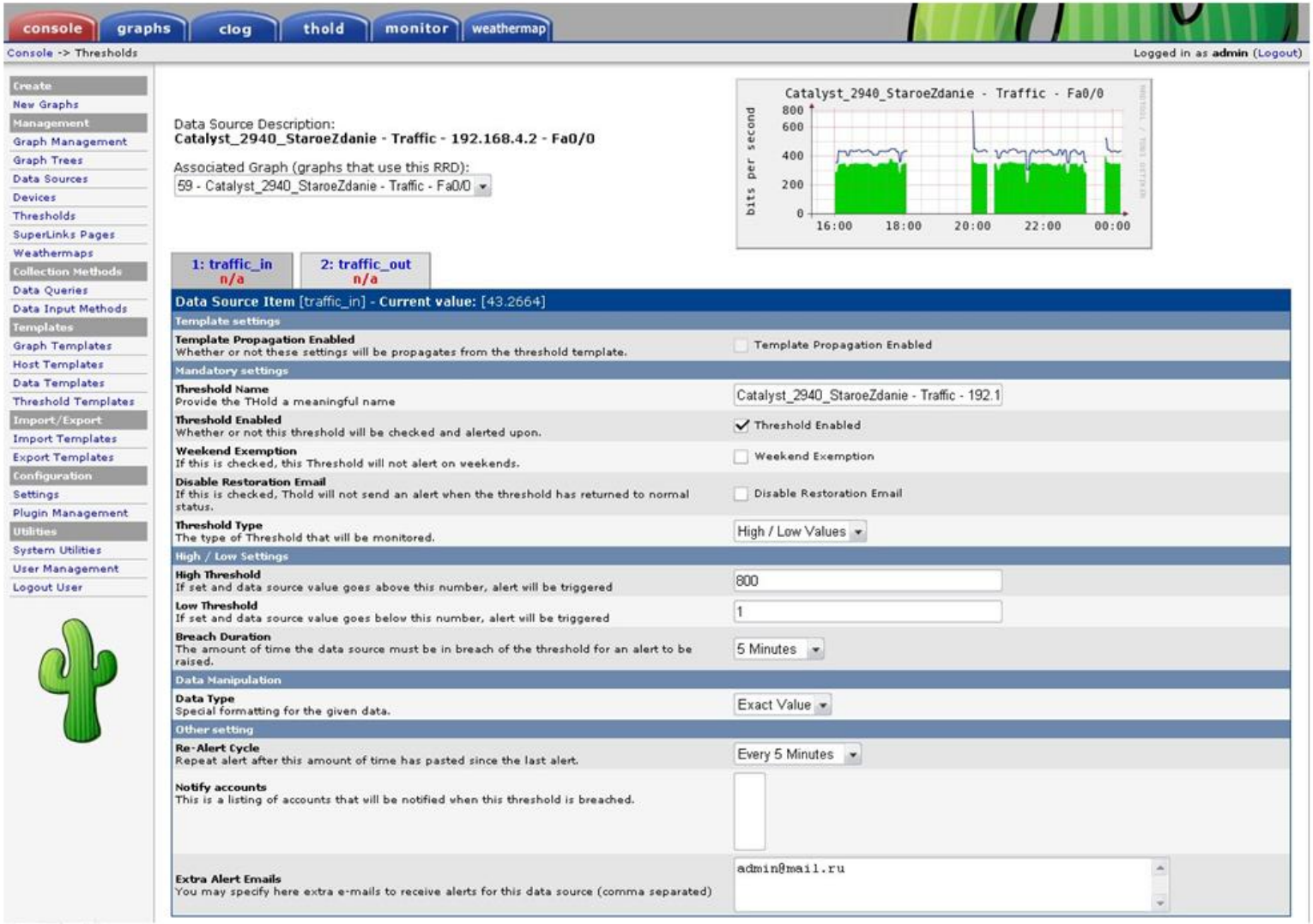


Рисунок А.6 – Система оповещения о событиях

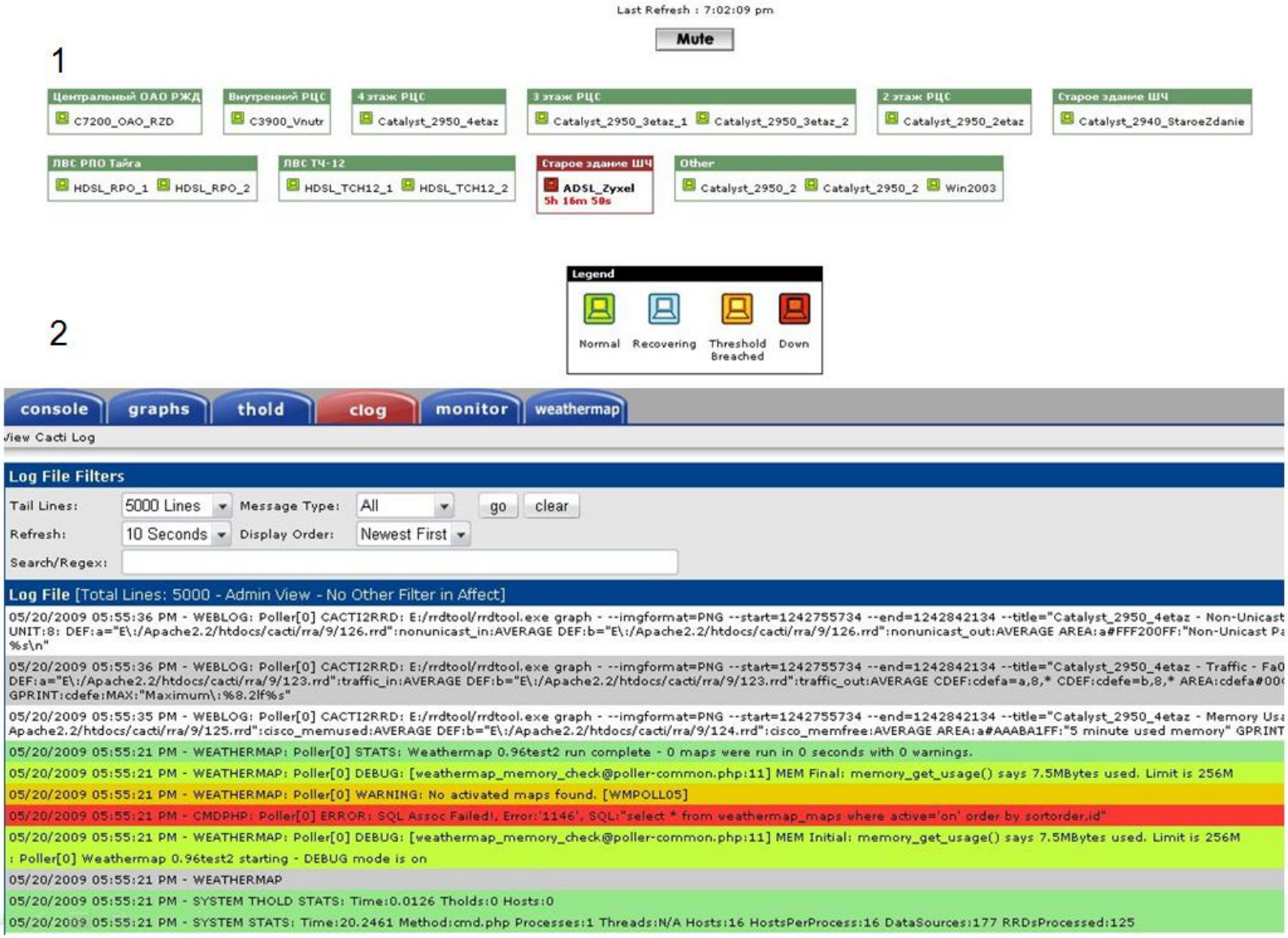


Рисунок А.7 – Система оповещения и система ведения логов событий

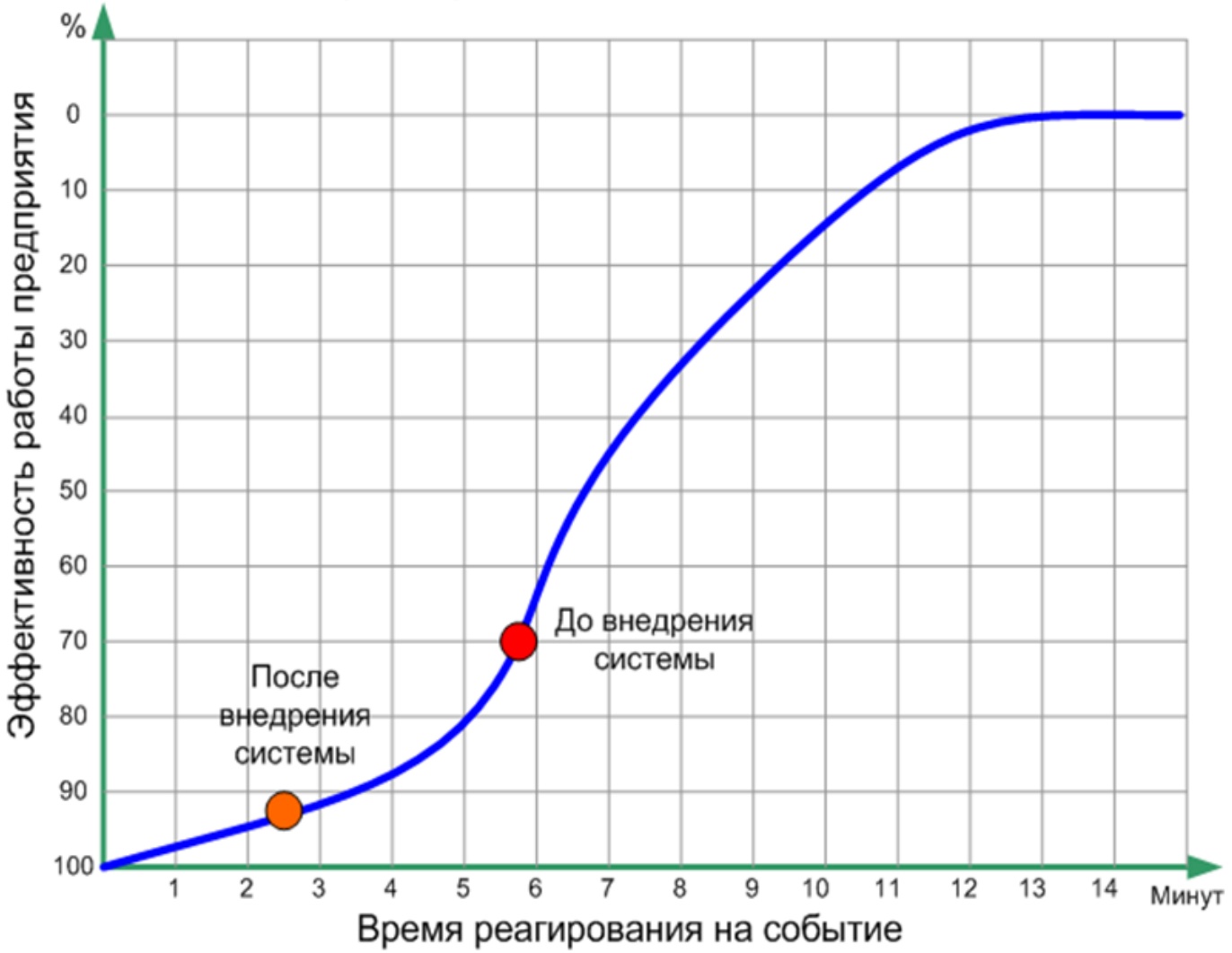


Рисунок А.8 – Зависимость эффективности работы предприятия от времени реагирования на событие

Приложение Б

Приложение В

(обязательное)

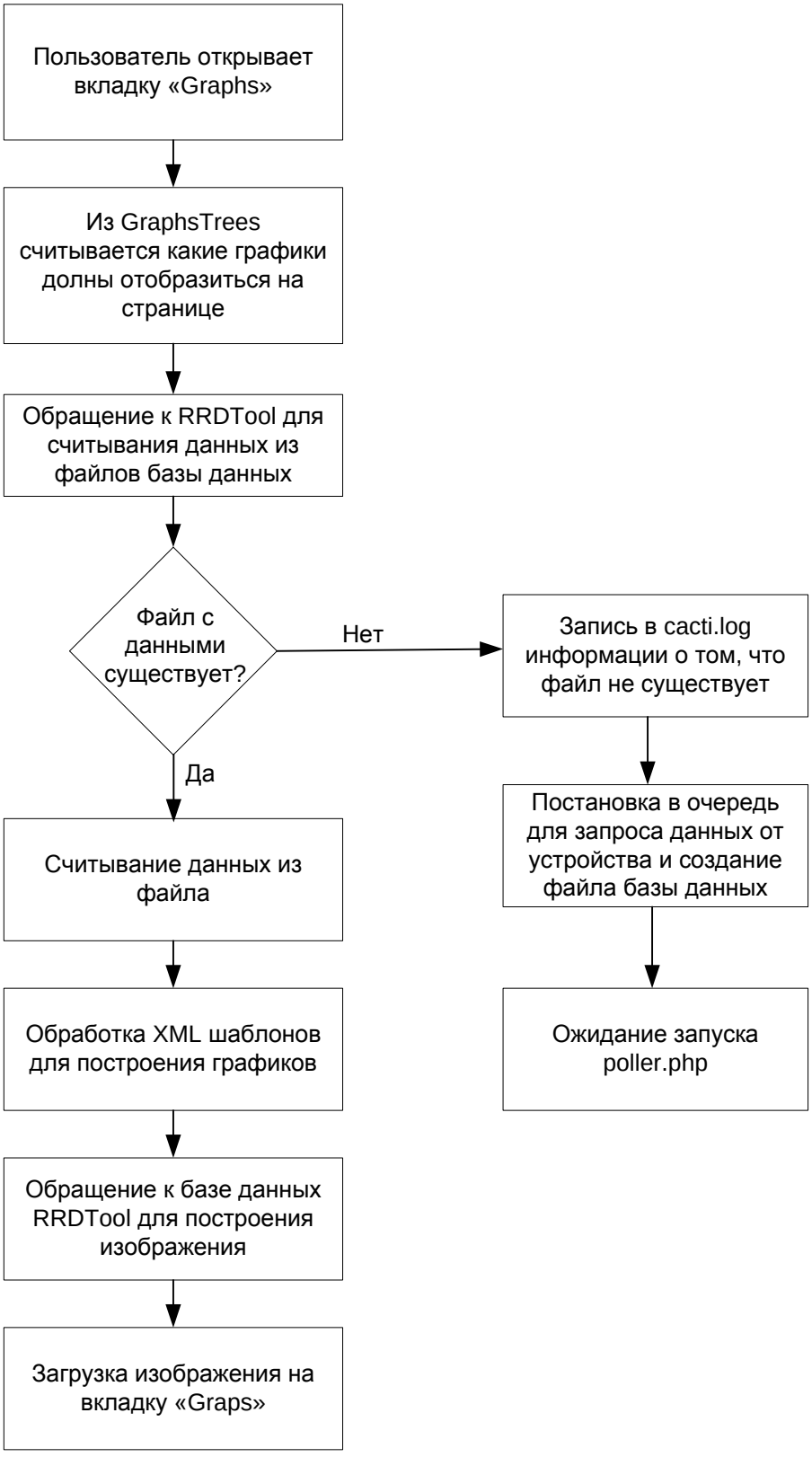


Рисунок В.1 – Графическая схема алгоритма работы программы

Приложение Г

(обязательное)

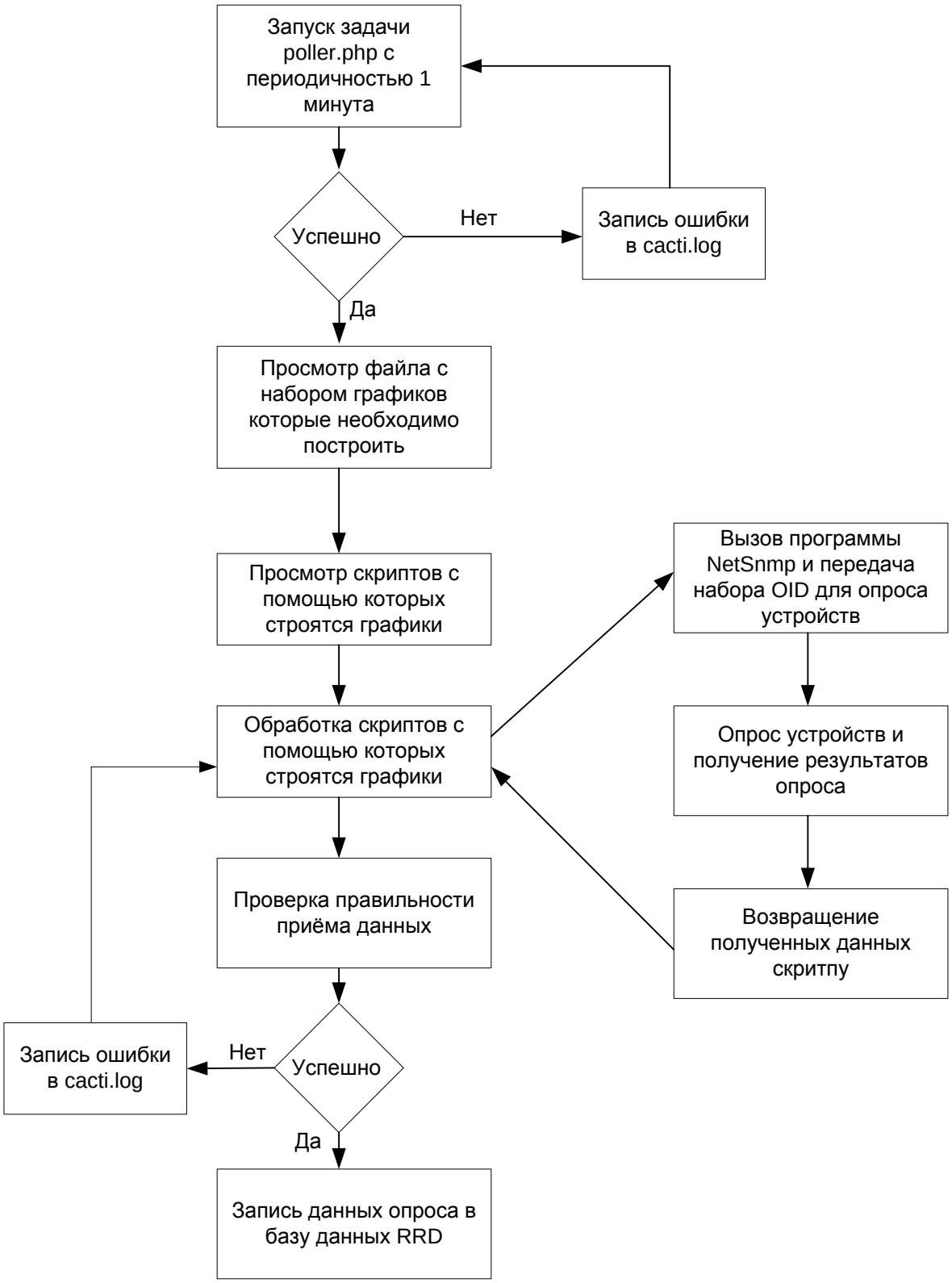


Рисунок Г.1 – Графическая схема алгоритма работы программы