МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«КУБАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
(ФГБОУ ВО «КубГУ»)

Физико-технический факультет

Кафедра теоретической физики и компьютерных технологий

К У Р С О В А Я Р А Б О Т А

АНАЛИЗ ТЕХНОЛОГИИ МОНИТОРИНГА СЕТИ В ПАО «РОСТЕЛЕКОМ»

Работу выполнил _____ Тыщенко Валерий Геннадьевич

Курс 3

Направление 09.03.02 Информационные системы и технологии

Научный руководитель
канд. физ.-мат. наук, доцент_____ М. А. Благодырь

Нормоконтролер
инженер_____ Г. Д. Цой

Краснодар 2016

СОДЕРЖАНИЕ

ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

ПАО	Публичное Акционерное Общество
ПО	Программное Обеспечение
SNMP	Simple Network Management Protocol
TCP/IP	Transmission Control Protocol / Internet Protocol
MIB	Management Information Base
УЦН	Устранение Цифрового Неравенства

ВВЕДЕНИЕ

В настоящее время информационная инфраструктура многих предприятий является сложнейшим соединением разномасштабных и разнородных сетей и систем. Для того чтобы обеспечить их слаженную и эффективную работу, необходима управляющая платформа или, как ее называют чаще, система мониторинга. В настоящее время существует порядка двух десятков систем мониторинга сетей и сетевого оборудования. Актуальность и необходимость таких систем переоценить очень сложно. Благодаря мониторингу появляется возможность отслеживать такие показатели серверной инфраструктуры как влажность, температуру, объем свободного дискового пространства на серверах и другие, что позволяет оперативно обнаружить сбой, и оповестить о нём системного администратора, вовремя предупредив опасные последствия.

Система мониторинга сети в ПАО «Ростелеком» является неотъемлемой частью деятельности компании, играющей немаловажную роль в обеспечении высококачественных услуг для своих клиентов и отлаженной работе оборудования.

В качестве объекта исследования данной работы выступает система мониторинга сети в ПАО «Ростелеком»

Целью данной работы является исследование и анализ программного обеспечения мониторинга сети «Zabbix», выявление основных достоинств и недостатков данных систем в компании ПАО «Ростелеком».

Для этого необходимо решить следующие задачи:

- ознакомление с основными теоретическими понятиями систем мониторинга;
- изучение деятельности компании ПАО «Ростелеком»;
- ознакомление с основными задачами и функциями системы мониторинга «Zabbix»;
- анализ готового продукта «Zabbix», используемого в компании ПАО «Ростелеком».

Полученные в данной работе результаты, в первую очередь, направлены на выявление основных недостатков и проблем в программном обеспечении, представляемом компанией «Zabbix SIA» для ПАО «Ростелеком». Устранение найденных недостатков положительно повлияет на производительность труда персонала, позволит существенно экономить время и ресурсы компании.

1 Системы мониторинга сетей и сетевого оборудования

1.1 Основы мониторинга компьютерной сети

Компьютерная сеть — это система программных и аппаратных компонентов, тесно взаимосвязанных друг с другом. Разумеется, компьютерная сеть может состоять и из двух компьютеров, но, как правило, их число в сети существенно больше. При этом компьютерная сеть не является простым объединением компьютеров, а представляет собой достаточно сложную систему. Любая компьютерная сеть характеризуется (Рисунок 1) топологией, протоколами, интерфейсами, сетевыми техническими и программными средствами.

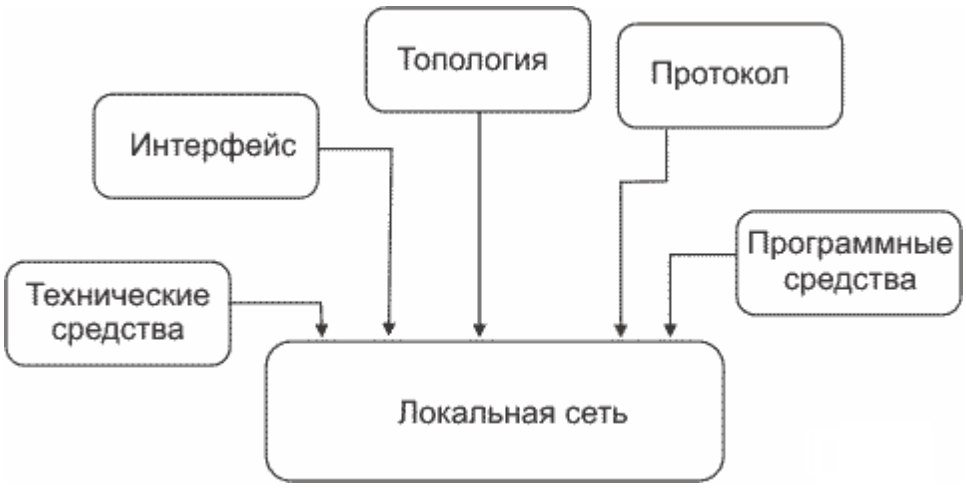

Рисунок 1 - Общая схема компьютерной сети

Все устройства, работающие в сети, протоколы, сама сеть образуют сложнейшую систему, которая требует постоянного мониторинга и контроля в силу важности выполняемых функций. Как хорошо бы не была настроена компьютерная сеть, и насколько бы надежное программное обеспечение не было установлено на серверном оборудовании и компьютерах - полагаться только на

системного администратора в данном вопросе крайне нерационально. Нужны средства контроля состояния сети, которые работают в автоматическом режиме и действуют непрерывно, сообщая своевременно о потенциальных аварийных ситуациях. Термином мониторинг сети называют работу системы, которая выполняет постоянное наблюдение за компьютерной сетью в поисках медленных или неисправных систем, и которая при обнаружении сбоев сообщает о них сетевому администратору с помощью почты, телефона или других средств оповещения. Эти задачи являются подмножеством задач управления сетью. [1]

Система мониторинга сети выполняет наблюдение за сетью в поисках проблем, вызванных перегруженными и/или отказавшими серверами, другими устройствами или сетевыми соединениями. Неудавшиеся запросы (например, в том случае, когда соединение не может быть установлено или, когда сообщение не было доставлено) обычно вызывают реакцию со стороны системы мониторинга. В качестве реакции может быть:

- отправлен сигнал тревоги системному администратору;

- автоматически активирована система защиты от сбоев, которая временно выведет проблемный сервер из эксплуатации, до тех пор, пока проблема не будет решена, и так далее. [2]

Постоянный мониторинг системы дает возможность обнаружения "узких мест" в сети, локализации ошибок и своевременного исправления ситуации.

Мониторинг состояния компьютерной сети, как правило, осуществляется одной или несколькими рабочими станциями или серверами. Существует два вида мониторинга:

- активный мониторинг, предполагающий опрос устройств с определённой периодичностью для определения доступности самих устройств и сервисов, которые они предоставляют, а также проверки состояния устройств в настоящий момент, например, процент загрузки процессора, дисков, температуры и других;

- пассивный мониторинг, предполагающий ожидание от устройств сообщений о событиях, происходящих в системе. Чаще всего такие сообщения присылаются устройствами посредством простого протокола сетевого

управления (SNMP). Это протокол прикладного уровня, который является составной частью протокола TCP/IP и позволяет администраторам руководить производительностью сети, находить и устранять сетевые проблемы.

Обычно на практике в системах мониторинга данные виды комбинируются.

1.2 Методы мониторинга состояния сети

Все множество средств, применяемых для мониторинга локальных сетей, можно разделить на несколько основных классов:

- системы управления сетью. Программные системы, занимающиеся сбором данных о состоянии узлов и коммуникационных устройств сети, данные о трафике, циркулирующем в сети. Эти системы выполняют в автоматическом режиме действия по управлению сетью - такие как включение и отключение портов устройств, изменение параметров мостов адресных таблиц мостов, коммутаторов и маршрутизаторов и т.п;

- средства управления системой. Средства управления системой часто выполняют функции, аналогичные функциям систем управления, но по отношению к другим объектам. В первом случае объектами управления являются 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. Эти системы 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 единственным устройством, и в этом их основное отличие от централизованных систем управления;

- анализаторы протоколов. Представляют собой программные или аппаратно-программные системы, которые ограничиваются, в отличие от систем управления, лишь функциями мониторинга и анализа трафика в сетях;

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

- 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;

- многофункциональные устройства анализа и диагностики. Приборы, совмещающие функции нескольких устройств: анализаторов протоколов, кабельных сканеров и даже ряд возможностей ПО сетевого управления; [6]

Выбор методов мониторинга зависит от целого набора факторов, среди которых возможности программного обеспечения, конфигурации серверов и сети и многие другие. В общем случае можно говорить о таких элементах как:

- проверка физической доступности оборудования;

- проверка работоспособности служб и сервисов, которые в настоящее время работают в сети;

- детальная проверка важных критериев функционирования сети (загрузки, производительности и других);

- проверка специфичных параметров, свойственных для данного конкретного окружения (наличие значений в таблицах базы данных, проверка содержимого лог-файлов).

В любом случае любая проверка начинается с тестирования доступности оборудования, которая может быть нарушена в силу отключения оборудования либо отказе каналов связи. Это предполагает проверку по ICMP-протоколу

(протокол межсетевых управляющих сообщений), когда проверяется не только факт ответа, но и время, за который проходит сигнал, а также количество запросов, которые были потеряны.

Следующим этапом является проверка работоспособности критичных служб. Обычно это означает TCP-подключение к тому порту сервера, где должна быть запущена служба, а также отправка выполнение тестового запроса.

Далее происходит проверка нагрузки, где выясняются также данные о памяти и загруженности процессора, свободном дисковом пространстве, статусах принтеров у сервера печати и другие принципиально важные проверки.

И, наконец, многие окружения требуют еще и специфических проверок, таких как запросы к базе данных, которые контролируют работу какого-либо приложения, проверка файловых отчетов или значений настроек, отслеживание наличия некоторого файла (к примеру, создаваемого при возникающих проблемах в системе). [5]

Системы управления сетью позволяют в автоматическом режиме контролировать сетевой трафик и управлять коммуникационным оборудованием сети. Большинство современных систем управления сетью построены на основе протокола SNMP. [3]

1.3 Использование протокола SNMP для анализа состояния сетей

Протокол SNMP (Simple Network Management Protocol, простой протокол сетевого управления) представляет собой протокол для управления сложными сетями TCP/IP. Он позволяет автоматически собирать информацию об ошибках и отказах устройств. [3]

С помощью SNMP администраторы могут управлять и настраивать компьютеры сети из центрального компьютера, не используя программы управления сетью. Они могут также использовать SNMP для наблюдения за

производительностью сети, определяя сетевые проблемы и отслеживания тех, кто использует сеть, и то, как используется сеть. [7]

Таким образом, благодаря удобству и "практической полезности" данного протокола сетевого управления, в настоящее время он остается самым популярным протокола для сбора данных о работоспособности активного сетевого оборудования и сети. Его используют десятки систем мониторинга по всему миру.

SNMP помогает определить:

- загрузку каналов передачи данных свитчей и маршрутизаторов (номер порта, пропускную способность);

- параметры ИБП (пинг, напряжение, заряд аккумуляторов, состояние и режим работы и так далее);

- параметры RAID-массива или внешнего хранилища данных (вид, состояние работы, загрузку и прочее);

- параметры принтера или МФУ (пинг, количество тонера, сетевое имя), принт-сервера, телефонной станции. [4]

Все устройства, "поддающиеся" управлению, имеют собственный программный комплекс, необходимый для того, чтобы была возможность работы с протоколом SNMP, которое называется агентом. Этот агент является посредником между внутренними структурами объекта, над которым производится управление и менеджером. Менеджер - это программа, которая работает в это же время на рабочей станции сетевого управления. Чаще всего их взаимодействие происходит таким образом, что менеджер инициирует запрос по адресу к агенту, агент занимается его обработкой, сбором данных и далее отправляет эти данные назад. В редких случаях агент и сам без помощи менеджера имеет возможность выступать инициатором обмена данными.

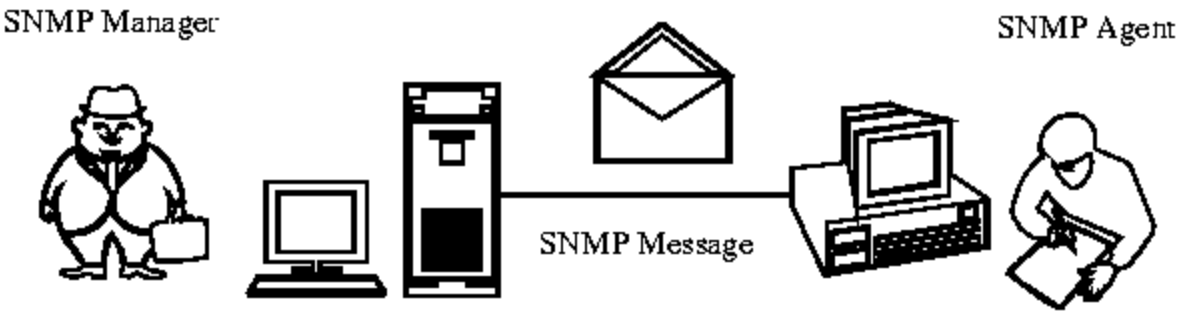

Рисунок 2 - Взаимодействие агента и менеджера

Клиентское программное обеспечение обычно бывает запущено на рабочей станции администратора, а программа-сервер запущена на каждом маршрутизаторе или узле сети, вовлеченные в процесс управления (Рисунок 2).

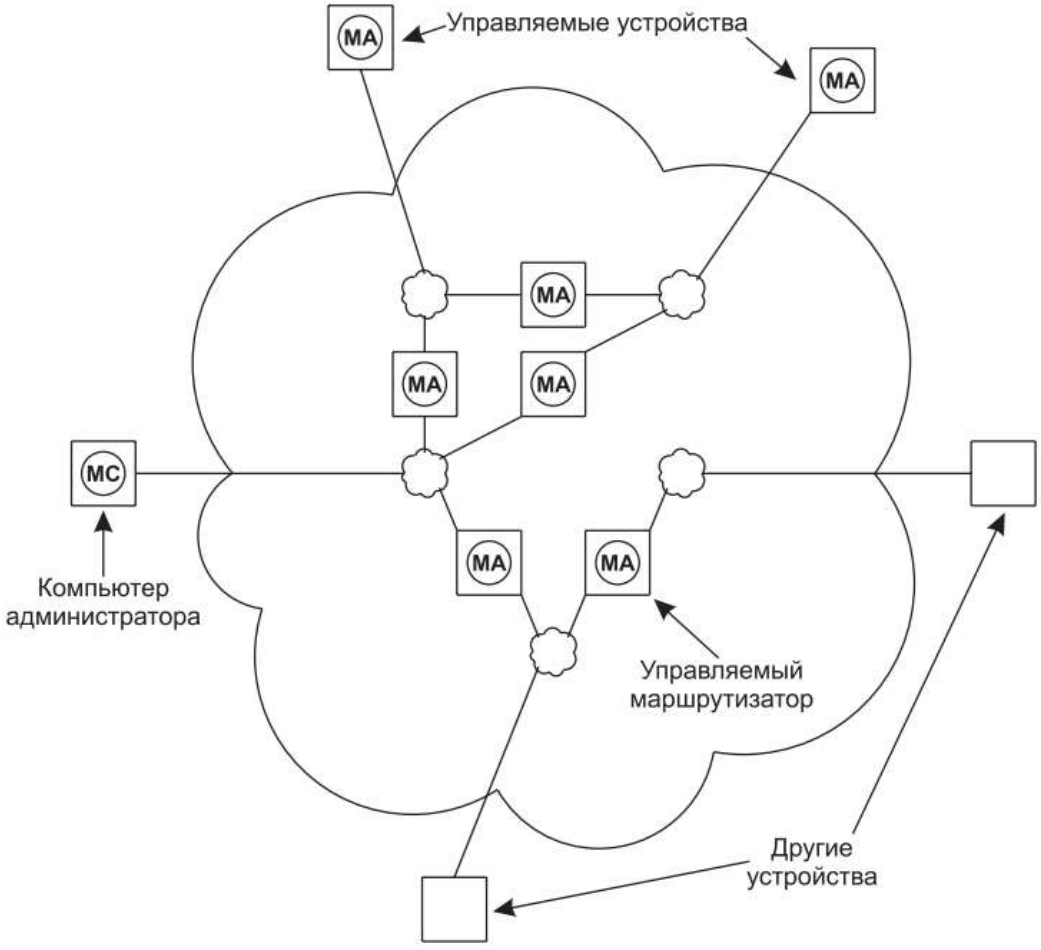

Рисунок 3 - Схема взаимодействия устройств в сети

Чаще всего агент имеет ряд событий, в случае возникновения которых он должен сообщить об этом менеджеру, после чего менеджер должным образом реагирует на оповещение агента. Примерами таких событий могут служить перезагрузка в результате проблем с питанием или же какая-либо другая аварийная ситуация.

Благодаря тому, что производили сетевого оборудования разработали унифицированную модель, которая дает возможность иметь доступ к данным техники, менеджер может заниматься управлением различными видами оборудования. Данная модель представляет собой минимальный объем данных, без которых не удастся контролировать и управлять работой оборудования. К примеру, если говорить о сетевом принтере, то для него этот минимум будет содержать информацию о загрузке процессора, время работы, статус, количество портов и еще несколько важных характеристик.

Таким образом, немаловажным аспектом работы с SNMP является то, что менеджер имеет возможность безо всяких сложностей взаимодействовать с агентами от самых разных производителей. Это достигается посредством делегирования всех трудностей по взаимодействию с оборудованием агенту, который обладает стандартный интерфейс для доступа к характеристикам техники.

Простой протокол сетевого управления также и позволяет определять административные связи в отношения между управляемыми маршрутизаторами, то есть аутентификация администраторов. Кроме того вся необходимая для управления устройством информация находится именно на самом устройстве в так называемой Административной Базе Данных (MIB - Management Information Base). Эта база данныхявляется набором переменных, отражающих состояние объекта, над которым совершается управление. Каждый производитель сетевого оборудования, помимо стандартных переменных, включает в MIB какие-либо параметры, специфичные для данного устройства. Но при этом не нарушается принцип представления и доступа к административной информации. Таким образом, SNMP как непосредственно сетевой протокол предоставляет

исключительно набор команд для работы с переменными MIB. Этот набор включает следующие операции:

Таблица 1 - Операции протокола SNMP

Операция	Описание
get-request	Используется для работы одного или более параметров MIB
get-next-request	Используется для последовательного чтения значений. Обычно используется для чтения значений из таблиц. После запроса первой строки при помощи get-request, get-next-request используют для чтения оставшихся строк в таблице
set-request	Используется для установки значения одной или более переменных MIB
get-response	Возвращает ответ на запрос get-request, get-next-request или set-request
trap	Уведомительное сообщение о событиях типа cold или warm restart или возникновении аварийной ситуации

Схематично работу данных методов можно изобразить так, как показано на рисунке 4.

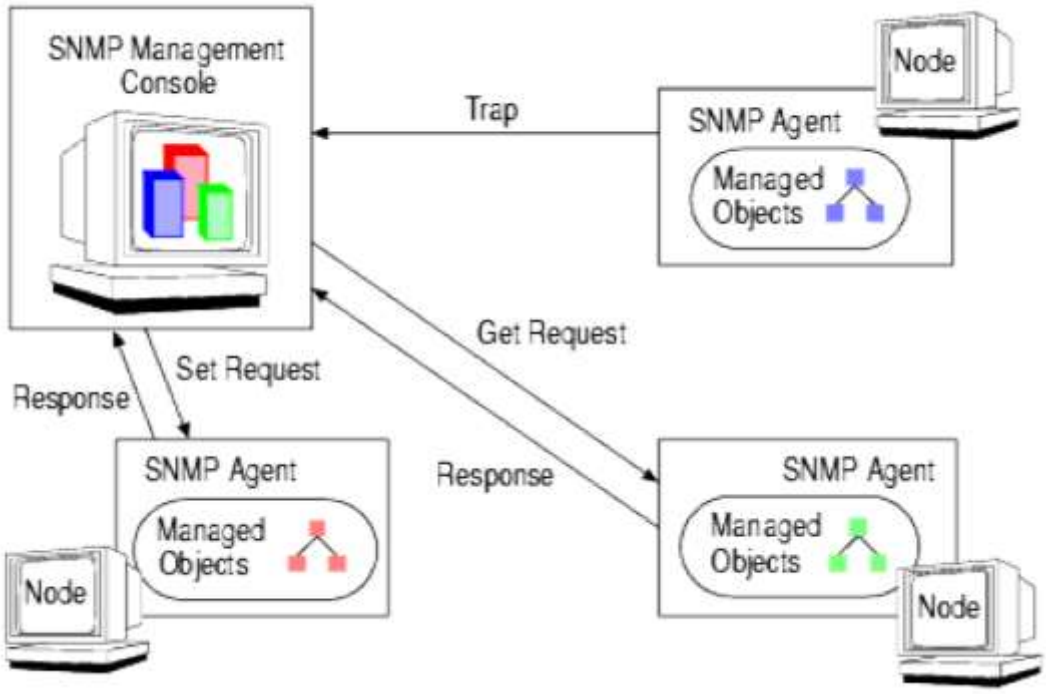

Рисунок 4 - Работа команд протокола SNMP

В итоге удается сохранить простоту протокола, но и сделать его весьма и весьма мощным средством, позволяющим задавать наборы команд управления сетевыми устройствами. Задача обеспечения выполнения команд состоит, таким образом, в регистрации специальных переменных MIB и реакции устройства на их изменения.

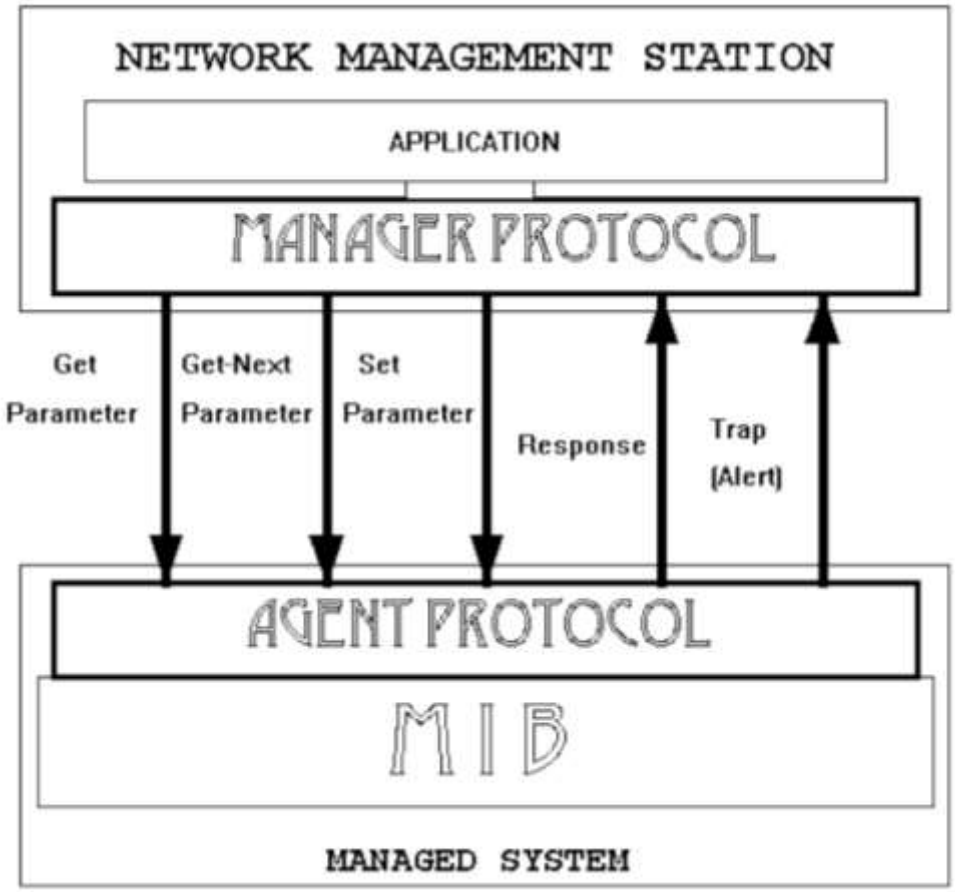

Рисунок 5 – Структура MIB

Каждому элементу соответствует численный и символьный идентификатор. В имя переменной включается полный путь до нее от корневого элемента root.

Также в отличие от других протоколов сетевого управления, SNMP использует в основе своего управления не ряд команд, а альтернативный подход под названием "fetch-store" (принцип выборки-хранения). И это гораздо более рациональный подход, так как при построении протоколов на основе команд возникают большие сложности в их структуре, ведь для каждой операции в протоколе существует отдельная команда, а при появлении новых элементов данных в протокол требуется внести изменения. Главными достоинствами использования принципа "fetch-store" являются простота, гибкость и устойчивость, которая очень высока.

С точки зрения администратора, SNMP по-прежнему остается весьма и весьма закрытым, но эта проблема находит свое решение посредством реализации пользовательского интерфейса к программам поддержки сетевого управления. В настоящее время таких программ великое множество и большинство из них обладают графическим пользовательским интерфейсом, где можно увидеть схемы сетевых соединений и используется принцип "навести и щелкнуть" для взаимодействия с пользователем. [2]

В настоящее время самой новой версией протокола SNMP является SNMPv3, которая создана на основе его предыдущих версий. Она существенно дополняет возможности и структуру прошлых версий. К примеру, для универсальности и гибкости настройки в протокол SNMPv3 включены средства, которые обеспечивают несколько аспектов защиты, и каждый из них имеется возможность сконфигурировать отдельно от остальных (аутентификация сообщений, конфиденциальность, удаленная конфигурация и другие). Подводя итоги вышесказанному, SNMP - это простой протокол, основанный на запросах и откликах, предназначенный для обмена между SNMP менеджером и SNMP агентом. Информационная база данных управления (MIB) определяет переменные, обслуживаемые агентом, которые менеджер может как запросить, так и установить.

2 Системы мониторинга в ПАО «Ростелеком»

2.1 Устранение цифрового неравенства

Развитие информационных технологий становится сегодня важнейшим фактором в жизни общества. Их широкое распространение преобразует общественную жизнь и приводит к революционным сдвигам в экономической, социальной, культурной и других сферах. За последние 5-7 лет к традиционным СМИ и СМК добавились сотовая связь, Интернет, спутниковое и кабельное телевидение, в ближайшем будущем ожидается приход интерактивного цифрового телевидения, что уже сейчас постепенно внедряется в жизнь современного человека.

«Цифровое неравенство» может рассматриваться как социальная проблема, нуждающаяся в решении через расширение возможностей доступа населения к информационно-коммуникационным технологиям (например, создание «центров общественного доступа»), т. е. через включение такого доступа в набор социальных благ, услуг, которые государство обязано предоставить гражданам.

В самом общем представлении термин "цифровое неравенство" описывает ситуацию, которая возникает, когда в обществе существуют социальные группы, которые имеют доступ к современным цифровым технологиям коммуникации (прежде всего, к Интернету), и теми, кто не имеет. Данное определение, связанное с наличием или отсутствием доступа к технологиям, может быть применено как к обществу одной страны (внутреннее цифровое неравенство), так и к нескольким странам или регионам (международное цифровое неравенство).

Федеральная программа "Устранение цифрового неравенства" призвана дать жителям глухих деревень скоростной интернет и связать их, таким образом, с окружающим миром.

С появлением волоконно-оптической линии связи, построенной «Ростелекомом» в рамках проекта УЦН, за счет значительно возросшей пропускной способности канала передачи данных, подключать к интернету даже самые отдаленные поселки стало намного проще, чем раньше.

Целью проектов, разрабатываемых для ПАО «Ростелеком», является создание в рамках муниципальных районов сети доступа (СД), состоящей из одной или нескольких точек доступа WiFi (ТД) для устранения существующего разрыва в качестве предоставления услуг передачи данных для жителей населенных пунктов (с численностью от 250 до 500 жителей, где установлены таксофоны).

С 1 апреля 2014 года ПАО «Ростелеком» назначен единственным оператором универсального обслуживания на всей территории страны.

В рамках программы по устранению цифрового неравенства ПАО «Ростелеком» предстоит обеспечить строительство волоконно-оптических линий связи (ВОЛС) общей протяженностью около 200 тысяч километров. Все точки доступа в Интернет должны быть организованы в более 13,6 тысячи населенных пунктов страны, в которых проживает около 4 миллионов человек.

Строительство ВОЛС будет осуществляться таким образом, чтобы ШПД обязательно появился во всех прилегающих городах, селах и деревнях. В результате миллионы жителей России получат высокоскоростной доступ в информационное общество со всеми его возможностями для общения, обмена информацией, получения госуслуг, образования, онлайн-банкинга и коммерции, в общем всего того, без чего уже невозможно представить жизнь человека в цифровой среде.

Точка доступа представляет собой базовую станцию, которая состоит из Ethernet-коммутатора, Wi-Fi-роутера и антенны, обеспечивающей круговое покрытие. Доступом в Интернет могут воспользоваться владельцы мобильных

телефонов, смартфонов, ноутбуков, планшетов и других устройств, оснащенных модулем Wi-Fi.

Системы мониторинга в «Ростелекоме» позволят выполнять такие функции как:

- сбор всех необходимых данных;
- построение графиков в режиме реального времени;
- веб-мониторинг;
- хранение данных истории;
- сетевое обнаружение;
- настройка системы прав доступа.

С помощью имеющейся системы мониторинга компания ПАО «Ростелеком» сможет надлежащим образом обеспечивать высококачественную связь и доступ в интернет в труднодоступных местах нашей страны.

2.2 Сеть передачи данных

Сеть передачи данных — совокупность трёх и более оконечных устройств (терминалов) связи, объединённых каналами передачи данных и коммутирующими устройствами (узлами сети), обеспечивающими обмен сообщениями между всеми оконечными устройствами.

Существуют следующие виды сетей передачи данных:

- телефонные сети — сети, в которых оконечными устройствами являются простые преобразователи сигнала между электрическим и видимым/слышимым;
- компьютерные сети — сети, конечными устройствами которых являются компьютеры.

По принципу коммутации сети делятся на:

- сети с коммутацией каналов — для передачи между оконечными устройствами выделяется физический или логический канал, по которому возможна непрерывная передача информации. Сетью с коммутацией каналов

является, например, телефонная сеть. В таких сетях возможно использование узлов весьма простой организации, вплоть до ручной коммутации, однако недостатком такой организации является неэффективное использование каналов связи, если поток информации непостоянный и малопредсказуемый;

- сети с коммутацией пакетов — данные между конечными устройствами в такой сети передаются короткими посылками — пакетами, которые коммутируются независимо. По такой схеме построено подавляющее большинство компьютерных сетей. Этот тип организации весьма эффективно использует каналы передачи данных, но требует более сложного оборудования узлов, что и определило использование почти исключительно в компьютерной среде.

ПАО «Ростелеком» обладает собственной мощной магистральной сетью связи, отвечающей всем требованиям современных рыночных условий.

Собственная магистральная цифровая сеть связи протяженностью около 500 тыс. км, построенная на основе ВОЛС с использованием SDH- и DWDM-технологий, а также местные сети, протяженностью свыше 2,6 млн. км, обеспечивают полное покрытие территории Российской Федерации и передачу любого типа информации: голоса, данных, видео.

Характеристики сети:

- состоит из магистральных линий связи, соединенных через транзитные междугородные и международные узлы связи (ТМгУС и ТМнУС) с сетями национальных и зарубежных операторов;

- используются современные SDH- и DWDM-технологии;

- свыше 350 точек доступа в России и за рубежом;

- участие в 17 международных кабельных системах;

- прямые стыки со 190 сетями в 70 странах;

- резервирование сети по географически распределенным маршрутам.

Данные характеристики говорят о том, что ПАО «Ростелеком» имеет широкие возможности благодаря имеющейся системе мониторинга, которая

играет несомненно важнейшую роль в обеспечении высококачественной работы сетей передачи данных.

3 Программное обеспечение компании ПАО «Ростелеком»

3.1 Краткие сведения о компании ПАО «Ростелеком»

ПАО «Ростелеком» – одна из крупнейших в России и Европе телекоммуникационных компаний национального масштаба, присутствующая во всех сегментах рынка услуг связи и охватывающая миллионы домохозяйств в России.

Компания занимает лидирующее положение на российском рынке услуг ШПД и платного телевидения: количество абонентов услуг ШПД превышает 11,9 млн, а платного ТВ «Ростелекома» – более 8,8 млн пользователей, из которых свыше 3,7 миллионов смотрит уникальный федеральный продукт «Интерактивное ТВ».

«Ростелеком» является безусловным лидером рынка телекоммуникационных услуг для российских органов государственной власти и корпоративных пользователей всех уровней.

Компания — признанный технологический лидер в инновационных решениях в области электронного правительства, облачных вычислений, здравоохранения, образования, безопасности, жилищно-коммунальных услуг.

Стабильное финансовое положение Компании подтверждается кредитными рейтингами: агентства Fitch Ratings на уровне “BBB-”, а также агентства Standard&Poor’s на уровне “BB+”.

Основные компоненты стратегии Ростелекома в фиксированном сегменте:

- технологическое преимущество в IP сетях (Строительство оптоволоконных сетей доступа, расширение мощности магистральной и региональных сетей);

- дифференцированные продукты (Приоритет на развитие уникальных контентных продуктов, triple play услуги и другие пакетные предложения, стимулирование развития новых продуктов);

- организационная трансформация (трансформация корпоративной и организационной структуры);

- клиентский сервис на уровне лучших практик (модернизация системы клиентского обслуживания, внедрение единой OSS/BSS платформы);

- повышение эффективности (оптимизация капитальных затрат с фокусом на рентабельность инвестиций, повышение производительности труда).

3.2 Анализ программного обеспечения мониторинга сети «Zabbix»

Zabbix - это инструмент мониторинга и управления сетевым оборудованием, созданный в 2001 году Алексеем Владышевым.

Данная система мониторинга примечательна своими графическими возможностями визуализации анализа данных, а также обеспечением SLA (англ. Service Level Agreement - соглашение об уровне предоставления услуги). ZABBIX поддерживает несколько видов мониторинга. Simple checks может проверять доступность и реакцию стандартных сервисов, таких как SMTP или HTTP без установки какого-либо программного обеспечения на наблюдаемом хосте. ZABBIX agent может быть установлен на UNIX-подобных или Windows хостах для получения данных о нагрузке процессора, использования сети, дисковом пространстве и тд. External check - выполнение внешних программ. ZABBIX также поддерживает мониторинг через SNMP.

Zabbix поддерживает и поллеры, и трапперы. Все отчеты и статистика Zabbix, так же как и параметры настройки, доступны через Веб-интерфейс. Веб-интерфейс обеспечивает доступ к информации о состоянии сети и жизнеспособности серверов из любого места. Правильно настроенный, Zabbix

может сыграть важную роль в мониторинге ИТ инфраструктуры. Это верно и для маленьких организаций с несколькими серверами и для больших организаций со множеством серверов.

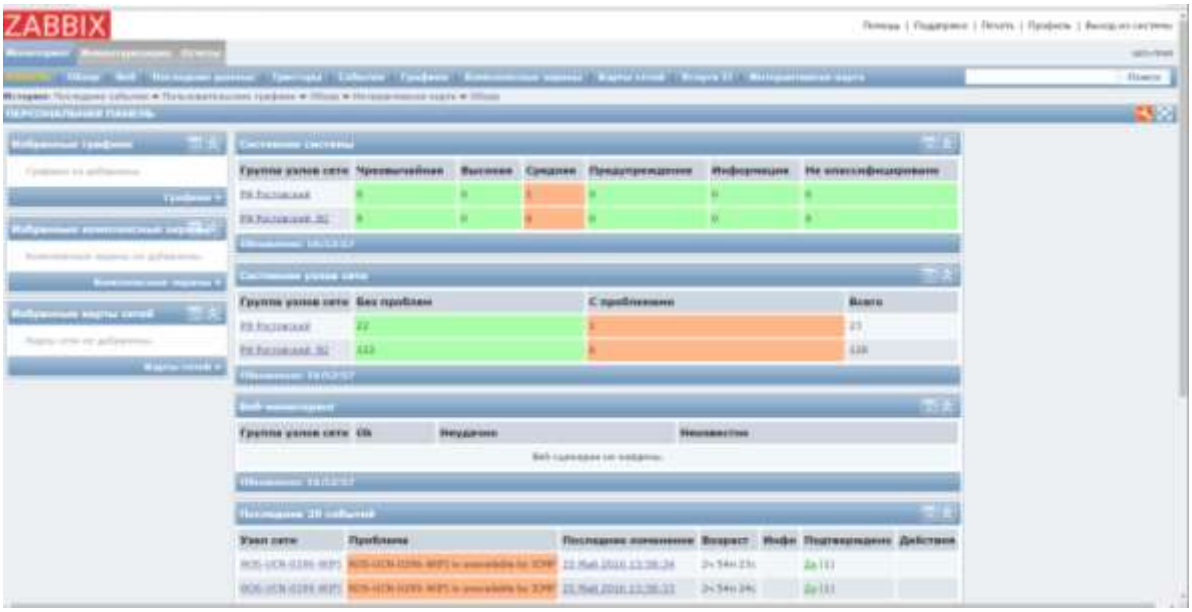

Рисунок 6 – Персональная панель ПО мониторинга «Zabbix»

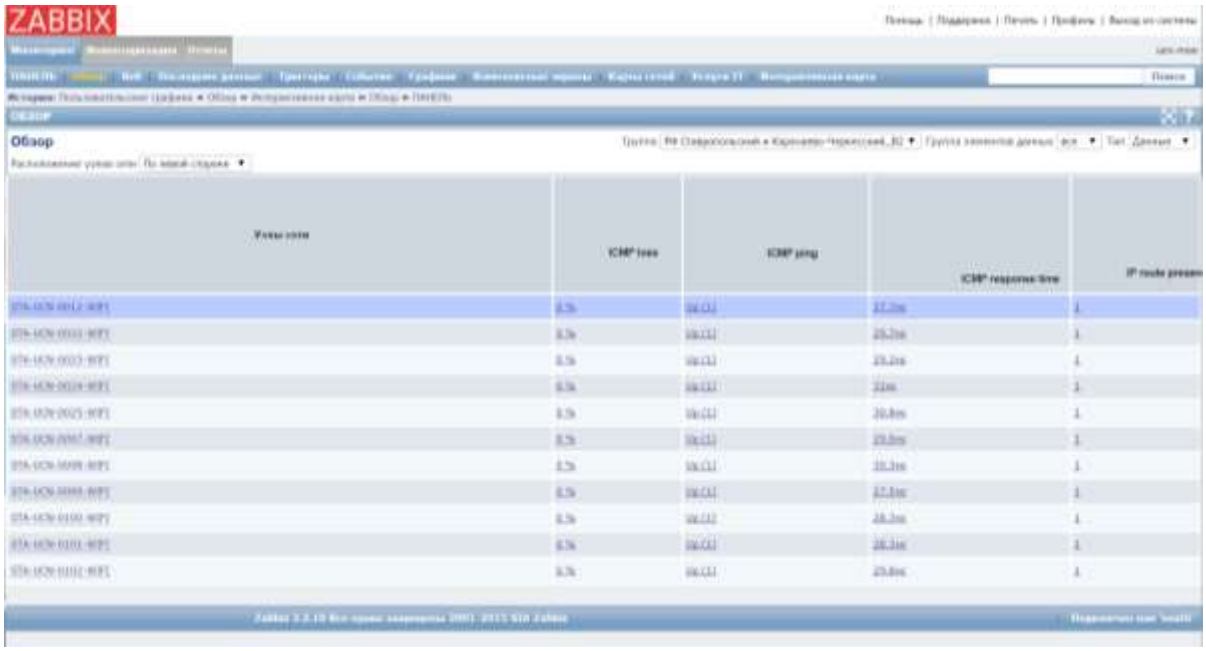

Рисунок 7 – Обзор расположения узлов сетей

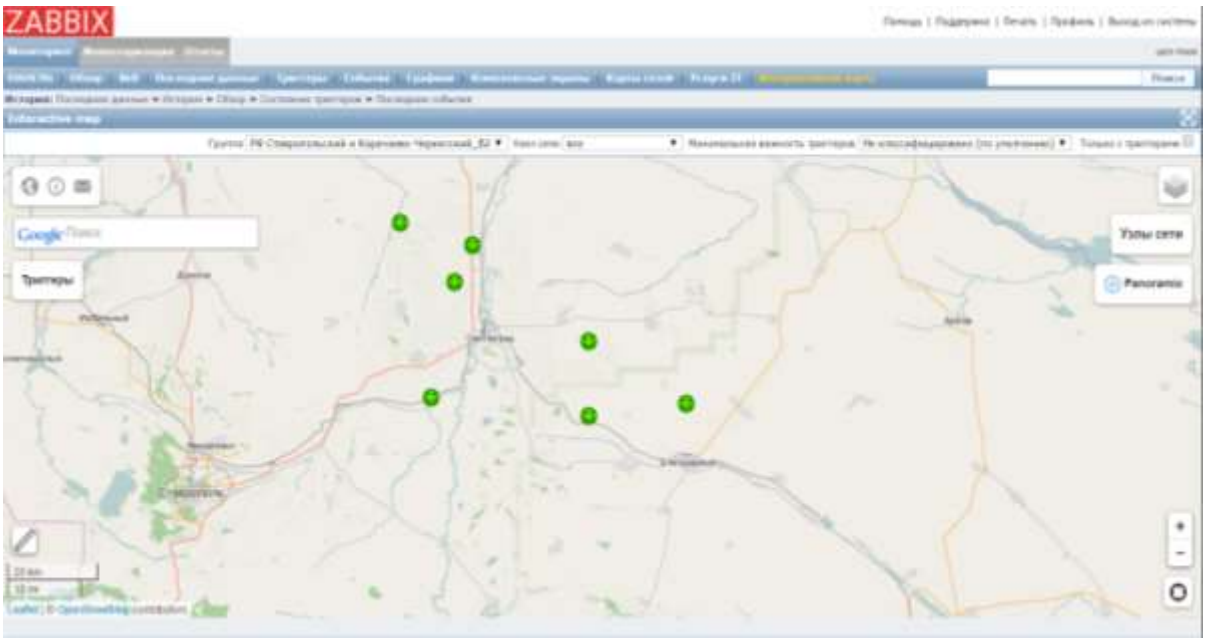

Рисунок 8 – Интерактивная карта

Система мониторинга «Zabbix» позволяет выполнение целого ряда задач:

- мониторинг сети;
- группировка устройств;
- автоматическое обнаружения;
- гибкое конфигурирование;
- визуализация данных и доступ через web-интерфейс;
- события и реакция на них в виде оповещений и выполнения команд;
- возможность расширения существующей функциональности через плагины;
- хранения конфигурации и истории мониторинга в БД;
- создание карт сети и управление доступом.

Так же основными преимуществами данной сети мониторинга являются:

- вся конфигурация хранится в базе, управляется через web-интерфейс;
- единая точка доступа для пользователей;
- разграничение доступа к данным и конфигурации;
- минимальный интервал между замерами — 1 секунда;

- с серверов собираются не результаты проверок (сломалось или нет),а количественные характеристики работы, которые анализируются на стороне сервера;
- время хранения данных ограничено лишь дисковым пространством;
- развитые возможности анализа собранных данных.

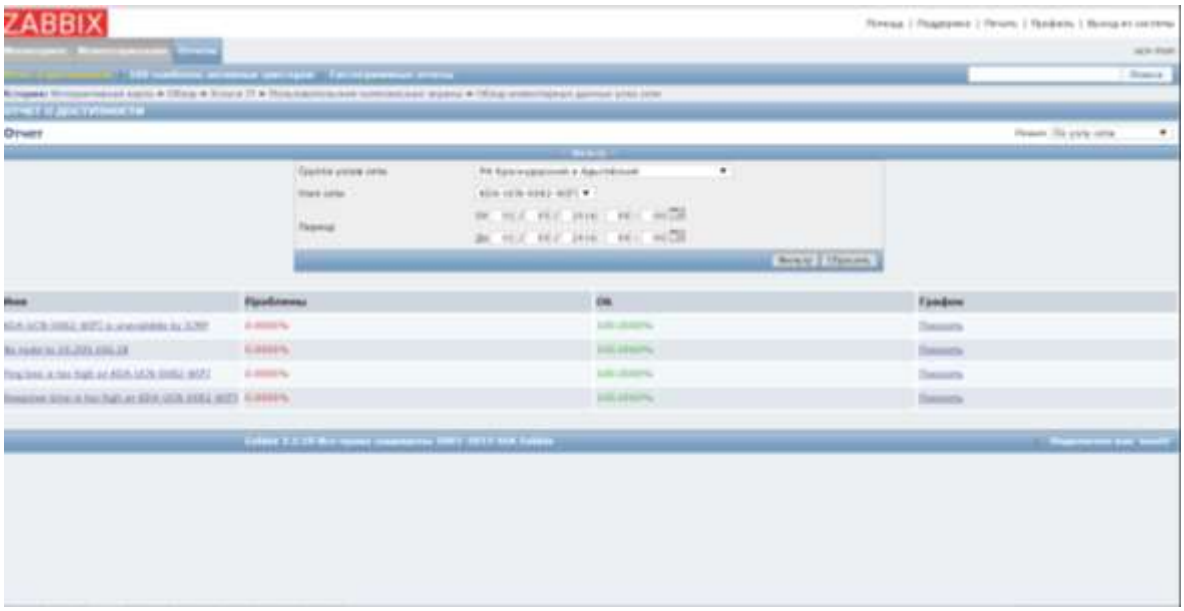

Рисунок 9 – Панель последних данных

Однако, в ходе проведения анализа мной был обнаружен ряд недостатков данного ПО мониторинга сети:

- самым глобальным недостатком данного ПО мониторинга является хранение истории всех элементов данных в СУБД. Если пользователя не интересует история изменения элементов данных, а лишь события (доступность/недоступность устройства, состояние сетевых интерфейсов), он будет вынужден хранить историю элементов данных хотя бы одни сутки. При больших инсталляциях это создает большую нагрузку на СУБД;
- отсутствуют встроенные средства резервирования. Пользователь не имеет возможности резервировать необходимые элементы без использования сторонних средств;

- возникают сложности с отображением событий в панели мониторинга (с включенным по группам фильтром), если устройство принадлежит нескольким группам (Рисунок 13);

- использование большого количества внешних проверок (с помощью скриптов) тормозит работу системы мониторинга в целом (возможно появление или увеличение очереди элементов, ожидающих обновления) (Рисунок 10, 11, 12);

- присутствует относительная сложность создания элементов данных и шаблонов без базовых знаний SNMP, IPMI и регулярных выражений;

- встроенные средства отрисовки карт сетей имеют относительно плохое качество исполнения (Рисунок 8, альтернативный вариант Рисунок 14);

- не обеспечивается отказоустойчивость. ПО не сохраняет свою работоспособность после отказа одного или нескольких его компонентов.

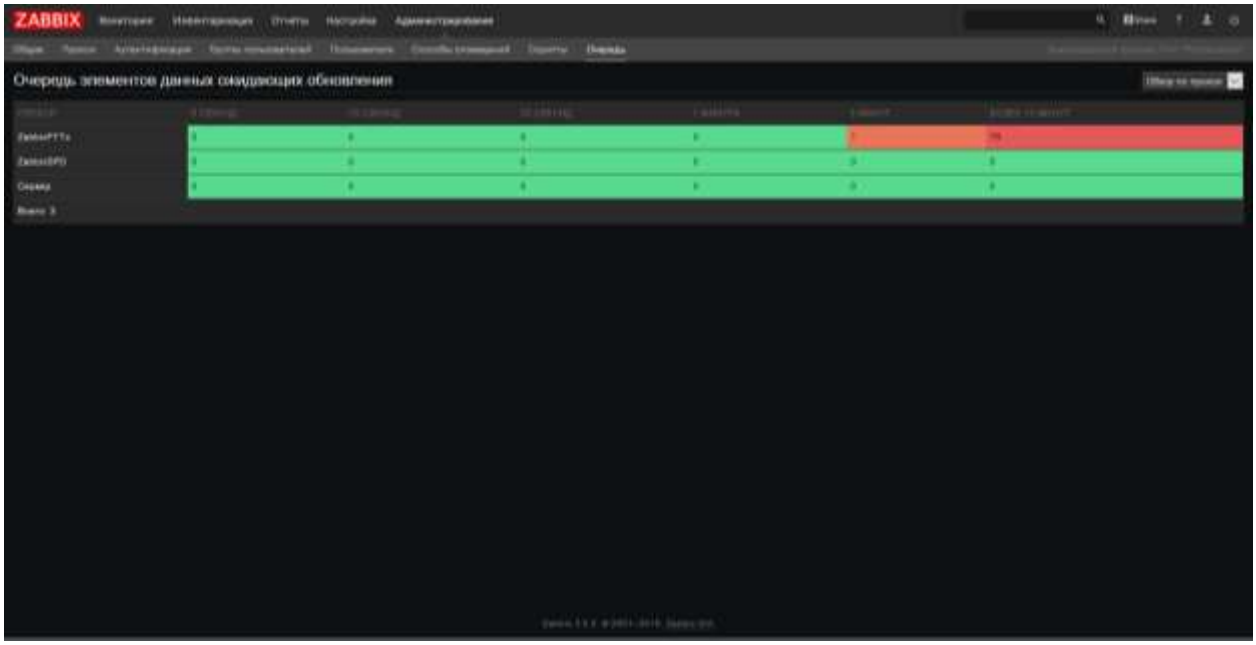

Рисунок 10 – Очередь элементов, ожидающих обновления

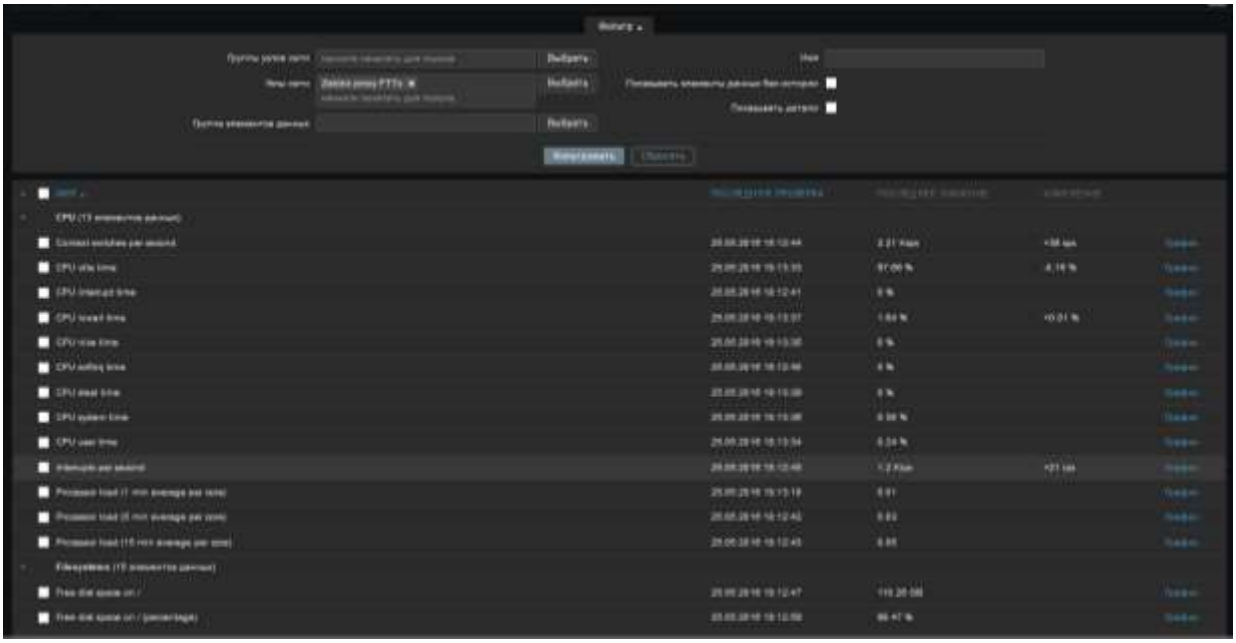

Рисунок 11 – Большое количество внешних проверок. Часть 1

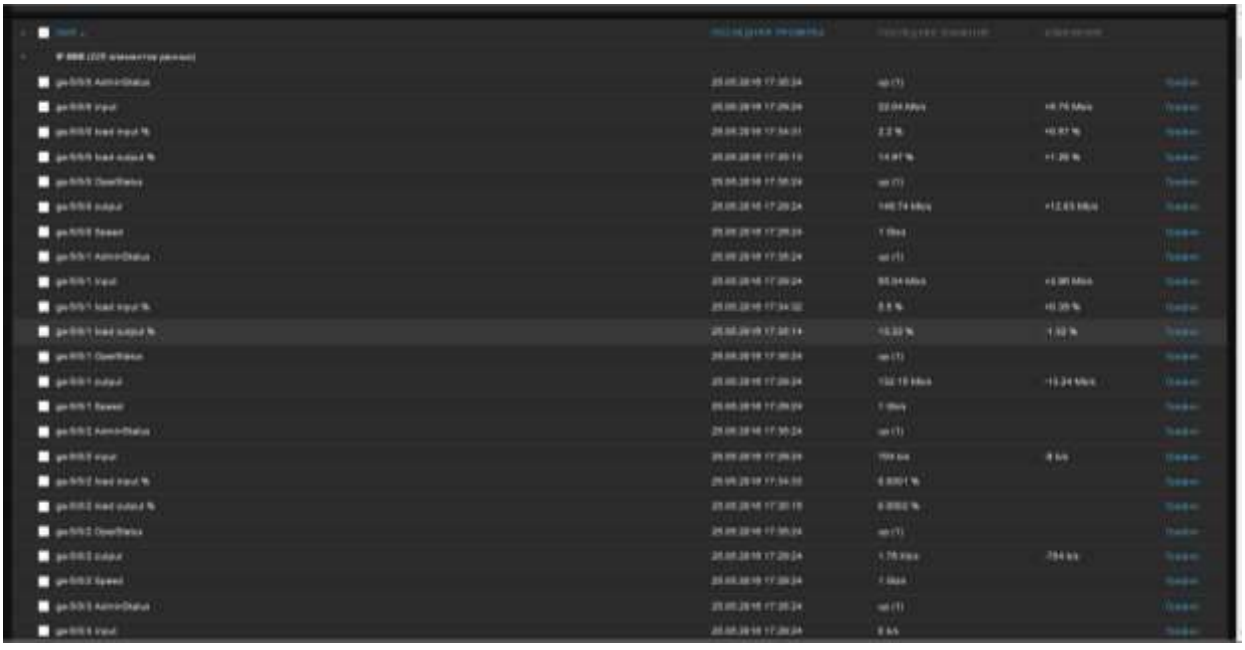

Рисунок 12 - Большое количество внешних проверок. Часть 2

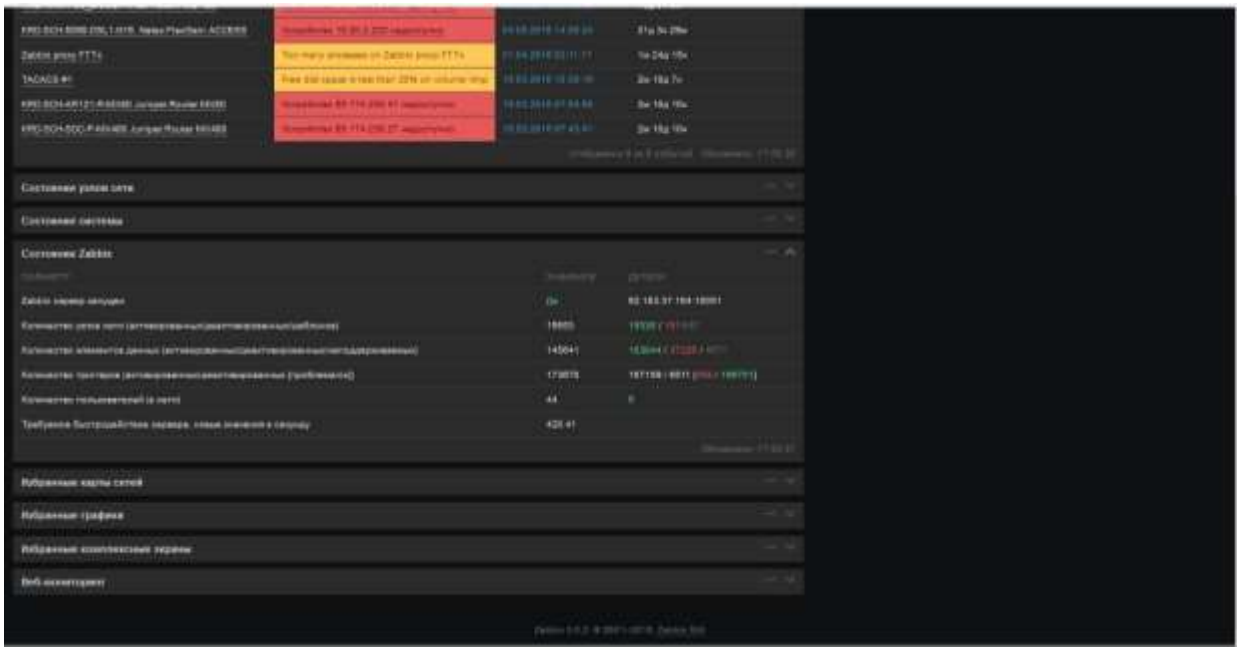

Рисунок 13 – Панель мониторинга, отображение событий

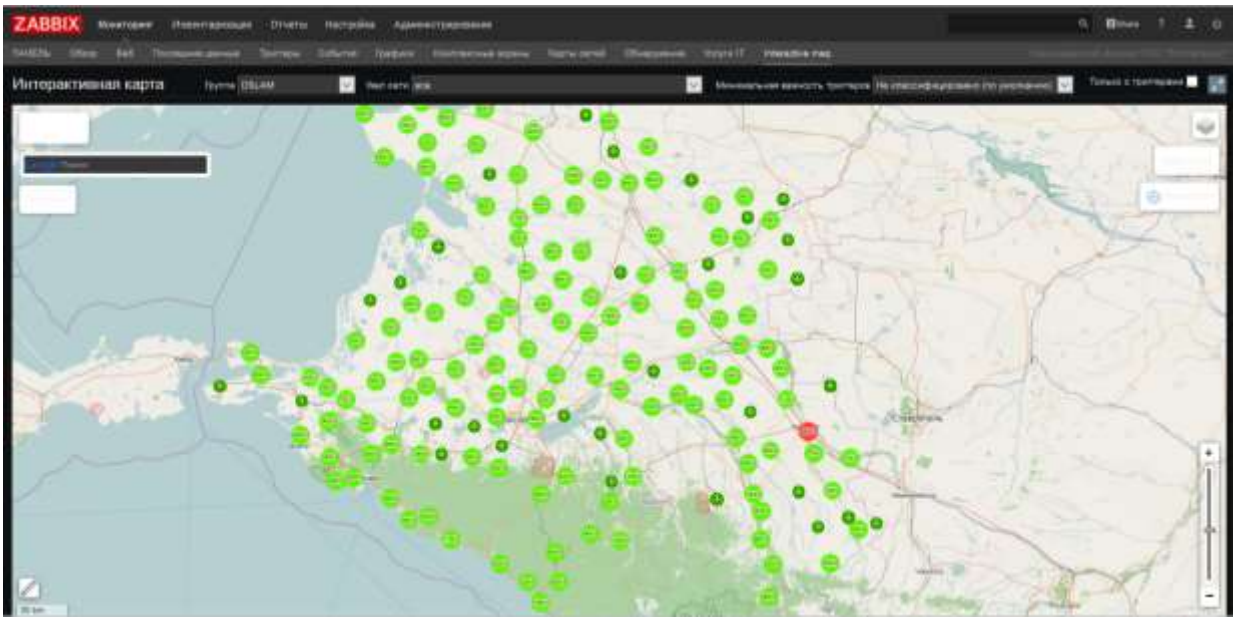

Рисунок 14 – Альтернативный вариант интерактивной карты с использованием плагина «plug-in Interactive map»

ЗАКЛЮЧЕНИЕ

Результаты данной курсовой работы заключаются в следующем:

1 Произведено исследование всех основных понятий и положений, связанных с системой мониторинга сети. Изучены основные методы состояния мониторинга сети такие как: системы управления сетью, средства управления системой, анализаторы протоколов, экспертные системы и др. Рассмотрены способы использования протокола SMNP для анализа состояния сетей.

2 Изучены основные примеры использования системы мониторинга сети компанией ПАО «Ростелеком», такие как: устранение цифрового неравенства и сеть передачи данных.

3 Изучена основная деятельность компании ПАО «Ростелеком», а также рассмотрены основные компоненты стратегии компании. Произведен анализ работы программного обеспечения системы мониторинга сети, используемого ПАО «Ростелеком», в ходе которого были сделаны следующие выводы:

- программное обеспечение «Zabbix» является отличным программным продуктом компании «Zabbix SIA» и успешно выполняет требуемые от нее функции, такие как:

1) мониторинг сети;
2) группировка устройств;
3) автоматическое обнаружения;
4) гибкое конфигурирование;
5) визуализация данных и доступ через web-интерфейс;
6) события и реакция на них в виде оповещений и выполнения команд;
7) возможность расширения существующей функциональности через плагины;
8) создание карт сети и управление доступом.

Однако, данное программное обеспечение имеет ряд недостатков и проблем, влияющих на производительность труда работников компании:

1) отсутствие встроенных средств резервирования;

2) возникновение сложностей с отображением событий в панели мониторинга (с включенным по группам фильтром), если устройство принадлежит нескольким группам;

3) использование большого количества внешних проверок (с помощью скриптов) тормозит работу системы мониторинга в целом;

4) присутствует относительная сложность создания элементов данных и шаблонов без базовых знаний SNMP, IPMI и регулярных выражений;

5) встроенные средства отрисовки карт сетей имеют относительно плохое качество исполнения (Рисунок 8, альтернативный вариант Рисунок 14);

6) не обеспечивается отказоустойчивость. ПО не сохраняет свою работоспособность после отказа одного или нескольких его компонентов.

Полученные в данной курсовой работе результаты прежде всего связаны с выявлением недостатков данного программного обеспечения, непосредственно влияющих на эффективность работы системы и обеспечивавших ее рабочее состояние сотрудников, и, следовательно, на деятельность самой компании. Их будущее устранение повлечет за собой увеличение производительности труда работников, а значит и выгоды получаемой от использования программы.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1 ГОСТ Р 53728-2009 Качество услуги "Передача данных" - М.: Изд-во Стандартинформ, 2011. - 21с.

2 Уилсон, Э. - Мониторинг и анализ сетей. Методы выявления неисправностей: практическое пособие. - М.: Лори-2005. -364с.

3 Олифер, В. Г., Олифер, Н. А. - Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. 4-е изд. — СПб.: Питер, 2010. — 944с.

4 Родичев, Ю.А. Компьютерные сети: архитектура, технологии, защита: учебное пособие для вузов. – Самара: Универсгрупп, 2012. – 468с.

5 Дуглас Э. Камер - Сети TCP/IP. Принципы протоколы и структура: научно-популярное издание. -М: Вильямс - 2013. -848с.

6 Комер, Д. TCP/IP крупным планом. Практическое пособие.- Спб:БХВ-Петербург-2009. -672с.

7 Масич Г.Ф. Сети передачи данных. – М: Пермский НИПУ – 2014. – 192с.