

РОСЖЕЛДОР
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ОБРАЗОВАНИЯ

СИБИРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ПУТЕЙ СООБЩЕНИЯ (СГУПС)

К защите:

Заведующий кафедрой

Информационные технологии
транспорта

наименование кафедры

Д-р техн. наук, профессор

В.И. Хабаров

инициалы, фамилия

Подпись

дата

**ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА
(БАКАЛАВРСКАЯ РАБОТА)**

Тема: Моделирование процесса предоставления услуги доступа к сети
Интернет на железнодорожных станциях. Автоматизация контроля за состоянием
услуги доступа к Интернет

БР.БИСТ.11.2018

шифр документа

Выполнил

В.А. Коренкова

подпись

инициалы, фамилия

дата

Руководитель

Канд. техн. наук, доцент

А.О. Коломеец

инициалы, фамилия

подпись

дата

Консультанты по разделам

1 Описание предметной области

Руководитель центра оперативно-
технологической связи

Е.Г. Каверин

подпись

2 Моделирование процесса
предоставления доступа к сети
Интернет

Начальник отдела эксплуатации СПД и
телекоммуникационного оборудования

А.С. Васильев

подпись

Нормоконтролер работы

Доцент кафедры ИТТ, канд. техн. наук

Е.В. Редьков

подпись

2018 г.
СИБИРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Факультет: Бизнес-информатики

Кафедра: Информационные технологии транспорта

Направление: Информационные системы и технологии

Профиль: Информационные системы и технологии на транспорте

УТВЕРЖДАЮ: зав. кафедрой д-р техн. наук, профессор

В.И. Хабаров

«____» _____ 2018 г.

ЗАДАНИЕ

на выполнение выпускной квалификационной работы

студенту

Коренковой Веронике Александровне

(Фамилия, Имя, Отчество)

1. Т е м а «Моделирование процесса предоставления услуги доступа к сети Интернет на железнодорожных станциях. Автоматизация контроля за состоянием услуги доступа к Интернет»

утверждена приказом № 511/с от «22» мая 2018 г.

2. Задание выдано «7» мая 2018 г.

2. Срок сдачи законченной работы на кафедру «11» июня 2018 г.

3. Исходные данные: устав предприятия, должностные инструкции, нормативно-распорядительная документация, официальный сайт компании

5.Содержание расчетно-пояснительной записки

Наименования разделов и вопросов	Примерно е количество страниц	График (сроки) выполнения
Введение	2	07.05.2018
Описание предметной области	16	10.05.2018
Моделирование процесса предоставления доступа к сети Интернет	13	15.05.2018.
Разработка системы контроля доступа сети Интернет	18	30.05.2018
Технико–экономическое обоснование разработки и внедрения системы контроля доступа к сети Интернет	10	01.06.2018
Заключение	1	09.06.2018

6.Содержание и объемы графической части

Наименование графического документа (чертежа, схемы, графика)	Количество листов формата А1	График (сроки) выполнения
Презентация в формате PowerPoint	19	10.06.2018

7. Консультанты по разделам

Наименование Раздела	Фамилия, И. О. консультанта	Подпись консультанта, дата выдачи задания
Описание предметной области	Е.Г. Каверин	
Моделирование процесса предоставления доступа к сети Интернет	А.С. Васильев	

Руководитель канд. техн. наук,
доцент кафедры ИТТ

_____ А.О. Коломеец
подпись

Задание к исполнению принял
студент гр. БИСТ-411_____

_____ В.А. Коренкова
подпись

-

УДК 004.725, 004.418

АННОТАЦИЯ

В работе представлено 69 страниц, 60 рисунков, 4 таблицы, 12 формул, 15 источников, 1 приложение.

ИНЖЕНЕР-ЭЛЕКТРОНИК, СЕТЬ, КОНТРОЛЬ ЗА СОСТОЯНИЕМ УСЛУГИ ДОСТУПА К ИНТЕРНЕТ.

В процессе выполнения выпускной квалификационной работе была рассмотрена предметная область и проведен анализ бизнес-процессов инженера-электроника. В результате выполнения выпускной квалификационной работы был проанализирован процесс предоставления услуги доступа к Интернет работникам железнодорожной станции и разработано программное обеспечение для контроля за состоянием услуги доступа к Интернет.

UDC 004.725, 004.418

ANNOTATION

In work 69 pages, 60 drawings, 4 tables, 12 formulas, 15 sources, 1 application are submitted.

ELECTRONIC ENGINEER, NETWORK, CONTROL OVER THE STATE OF THE INTERNET ACCESS SERVICE.

In the course of performance to final qualification work the subject domain has been considered and the analysis of business processes of the electronics engineer is carried out. As a result of performance of final qualification work process of providing service of access to the Internet to employees of the railway station has been analysed and the software is developed for control of a condition of service of access to the Internet.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ.....	8
1 Описание предметной области	10
1.1 Введение в предметную область	10
1.2 Моделирование бизнес–процессов	11
1.3 Деятельность Новосибирского регионального центра связи	16
1.4 Обзор существующего программного обеспечения для мониторинга сети	18
1.5 Выводы по первому разделу	25
2 Моделирование процесса предоставления доступа к сети Интернет	26
2.1 Понятие прокси-сервера и его назначение	26
2.2 Автоматизированная система обработки заявок	28
2.3 Организация доступа пользователей к информационным системам общего пользования (сети Интернет)	36
2.4 Выводы по второму разделу	38
3 Разработка системы контроля доступа к сети Интернет	39
3.1 Описание протокола управления сетью SNMP	39
3.2 Разработка программного обеспечения	42
3.3 Тестирование программного обеспечения на реальных устройствах	43
3.4 Результаты эксплуатации системы контроля доступа к сети Интернет	49
3.5 Инструкция пользователя информационной системы SNMP – контроль	51
3.6 Выводы по третьему разделу	56
4 Технико–экономическое обоснование разработки и внедрения	

системы контроля доступа к сети Интернет	57
4.1 Определение трудоемкости, длительности разработки и размеров заработной платы	57
4.2 Определение себестоимости работ по разработки и внедрению программного обеспечения	59
4.3 Расчет стоимости дополнительного программного обеспечения и инфраструктуры для внедрения программного обеспечения	62
4.4 Расчет общей стоимости проекта	62
4.5 Оценка экономической эффективности проекта	63
4.6 Выводы по четвертому разделу	66
ЗАКЛЮЧЕНИЕ	67
СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ	68
ПРИЛОЖЕНИЕ А - Акт внедрения результатов работы	70

СПИСОК СОКРАЩЕНИЙ

ОАО «РЖД» - открытое акционерное общество «Российские железные дороги»;

ЦСС – центральная станция связи;

РЦС – региональный центр связи;

ARIS – architecture of integrated information systems;

Pandora FMS - pandora flexible monitoring system;

IP – internet protocol;

АСОЗ – автоматизированная система обработки заявок;

NETCONF — network configuration protocol;

SSH – secure shell;

SOAP – simple object access protocol;

TLS – transport layer security;

BEEP – blocks extensible exchange protocol;

RPC – remote procedure call;

ПО – программное обеспечение;

ЕК АСУ ЕСПП – автоматизированная система управления единой службой поддержки пользователей;

ЕК АСУ ТР – единая корпоративная система управления трудовыми ресурсами;

ГК – главный каталог;

DNS – domain name system;

AD – active directory;

ПЭВМ - персональная электронно-вычислительная машина;

ИС – информационная система;

SNMP – simple network management protocol;

БД – база данных.

ВВЕДЕНИЕ

В соответствии с распоряжением правительства Российской Федерации от 28.07.2017 № 1632-р Об утверждении программы «Цифровая экономика Российской Федерации» утверждены несколько направлений развития нашей страны. Одним из базовых направлений развития цифровой экономики в России на период до 2014 года является развитие информационной инфраструктуры и информационная безопасность. К этому вектору развития подключилась одна из самых больших транспортных компаний страны – ОАО «Российские железные дороги» [1]. В рамках этого направления юридически обосновано использование виртуальных организаций, которые могут состоять из нескольких компаний-партнеров. Они могут объединить свои информационные ресурсы и капиталы для осуществления процесса производства оказываемых услуг и/или производства продукта. Отказоустойчивое функционирование виртуальных предприятий возможно при условии развитых коммуникаций и корпоративных информационных систем. Цифровая экономика способствует экономическому росту предприятия. Она затрагивает такие вопросы, как мониторинг в режиме реального времени, возможность удаленной работы, анализ больших массивов данных, сокращение производственных потерь. К информационным технологиям сейчас предъявляют повышенные требования. Технические решения должны быть гибкими и масштабируемыми. В своей работе автоматизированные системы должны дополняться алгоритмами обработки больших массивов данных, аналитикой и искусственным интеллектом. Организации, владеющие серверами и другими сетевыми устройствами, стремятся к их бесперебойной и производительной работе. В виду удаленного расположения указанных устройств, возникают сложности при их технической поддержке. В первую очередь это обусловлено удаленным расположением этих устройств друг от

друга и от центра мониторинга. Кроме сбора информации системы мониторинга и администрирования позволяют напрямую обращаться к оборудованию и конфигурировать его параметры. Для расширения сети нужно знать в каком состоянии сейчас сеть, а также необходимы данные о состоянии сети ранее. Сетевой мониторинг начинается с проверки основных показателей уровня ядра сети. Проводят проверки и сообщают администратору сети, значения, полученные от устройства, к примеру значения пропускной способности канала, время откликов коммутаторов и других сетевых устройств. Приложения, которые зависят от производительности сети, к примеру IP-телефонии, «видео по требованию», значительно повышают интерес к мониторингу. На ОАО «РЖД» очень распространена IP-телефония, с ее помощью сотрудники могут решать вопросы в оперативном порядке, а также по IP-телефонии проводятся селекторные совещания. С помощью анализа аварийных сообщений, которое выдается администратору можно спрогнозировать последующее поведение сети, а также найти неисправные оборудования и заменить их. Работа с оборудованием напрямую и невозможность спрогнозировать поведение сети определяет актуальность необходимости внедрения системы «SNMP - контроль».

Целью выпускной квалификационной работы является анализ бизнес-процессов по организации услуги доступа к сети Интернет и разработка программного обеспечения для контроля доступа.

Для достижения поставленной цели необходимо решить следующие задачи:

- проанализировать обязанности инженера–электроника;
- ознакомиться с автоматизированной системой обработки заявок и рассмотреть ее основные функции;
- провести анализ протоколов мониторинга и управления сетью;
- разработать программное обеспечение контроля доступа к сети Интернет.

1 Описание предметной области

1.1 Введение в предметную область

Проектируемая информационная система является система мониторинга оборудования на станциях Новосибирского региона.

Малые станции региона находятся далеко от более крупных станций, система мониторинга позволяет увидеть состояние оборудования. Так же разрабатываемая система может дополнить систему, которая служит для оформления заявок на предоставления доступа к сети Интернет. Можно отслеживать состояния устройств, принадлежащих пользователю, предоставляемому доступ к сети.

Центральная станция связи – филиал открытого акционерного общества «Российские железные дороги» является обособленным подразделением ОАО «РЖД» [2]. Центральная станция связи предлагает широкий спектр услуг по услуге связи, которая обеспечивает необходимыми телекоммуникационными ресурсами и услугами связи. С помощью предлагаемых услуг ЦСС и его филиалы организуют работу по обеспечению безопасности движения поездов.

Если рассматривать сеть, построенную на некотором участке пути, к примеру, взять два населенных пункта причем один из которых это малая станция.

Физически к оборудованию которое находится на малой станции добраться не всегда легко, на это могут влиять как погодные условия, так и наличие свободной бригады.

Бесспорно, некоторые вопросы не могут решиться на расстоянии, очень важно присутствие специалиста на месте аварии. Чтобы снизить количество возникающих аварий, а также снизить расходы за счет выездов бригады на место аварии и повысить скорость устранения аварий, было разработано специальное программное обеспечение по администрированию и мониторингу состояния сети.

1.2 Моделирование бизнес–процессов

Каждый работник на предприятии при поступлении на работу должен изучить документы такие как трудового договора, правила охраны труда и техники безопасности, а также обязанности в соответствии со своей должностной инструкцией. В должностной инструкции указываются права, должностные обязанности и прописывается ответственность работника.

Разрабатываемую систему может использовать персонал организации, которому по должностной инструкции необходимо следить за состоянием устройств для устранения и своевременное обслуживания оборудования.

При разработке информационной системы, для наглядности разрабатывают диаграммы, в которых обозначают процессы, которые выполняет заказчик (пользователь). Некоторые из этих процессов нужно автоматизировать.

Для описания бизнес-процессов можно взять инженера – электроника, который соответствует требованиям использования системы.

На рисунке 1.1 представлена диаграмма вариантов использования (Use Case) обязанностей инженера–электроника одного из контролирующего лица за состоянием оборудования, которая основана на должностной инструкции [3].



Рисунок 1.1 – Диаграмма Use Case инженера–электроника

На рисунке 1.2 представлена диаграмма вариантов использования процесса учета технического состояния оборудования.

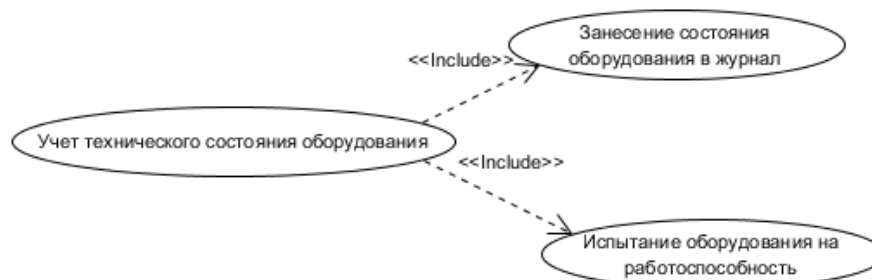


Рисунок 1.2 – Диаграмма учета технического состояния

Процесс испытания оборудования на работоспособность можно представить в виде диаграммы последовательности, которая изображена на рисунке 1.3.



Рисунок 1.3 – Диаграмма последовательности процесса испытания оборудования на работоспособность

Процесс занесения состояния оборудования в журнал можно представить в виде диаграммы последовательности, которая изображена на рисунке 1.4.

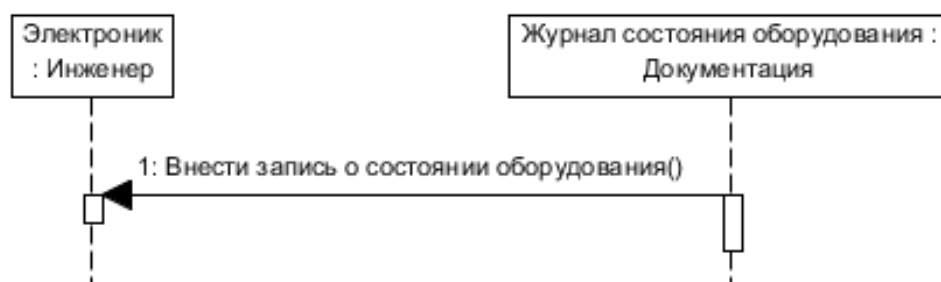


Рисунок 1.4 – Диаграмма процесса внесение состояния оборудования в журнал

Описанный процесс так же можно представить в диаграмме состояний представленной на рисунке 1.5.

Учет технического состояния оборудования связан с процессом выполнения ремонтных работ. Суть данного процесса в том, чтобы отслеживать состояния оборудования путем испытаний. Полученный результат инженер–электроник анализирует на выявления брака и записывает данный результат в журнал учета состояния. Если по результатам испытания в оборудовании обнаружен брак, то оформляем лист на ремонт оборудования.

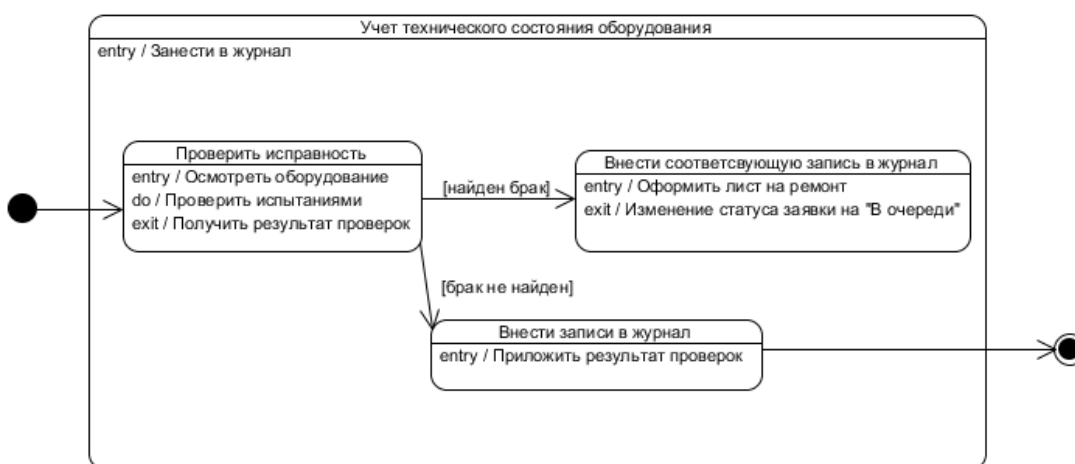


Рисунок 1.5 – Диаграмма состояния учета технического состояния оборудования

На рисунке 1.6 представлена диаграмма вариантов использования процесса «Анализ и учет обслуживаемого оборудования».



Рисунок 1.6 – Диаграмма анализа и учета обслуживаемого оборудования

Каждый процесс, представленный в диаграмме на рисунке 1.6 можно описать с помощью диаграмм последовательности, которые представлены на рисунках 1.7-1.8.



Рисунок 1.7 – Диаграмма последовательности изучения режимов и условий эксплуатации

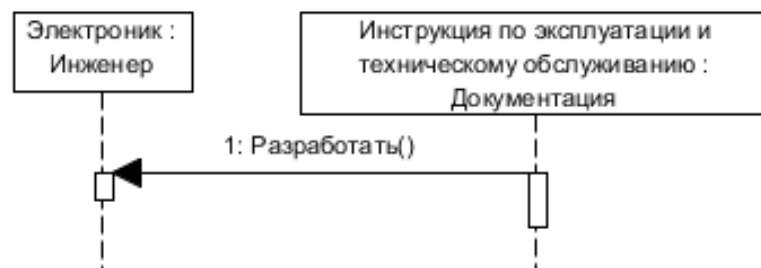


Рисунок 1.8 – Диаграмма последовательности разработки документов по эксплуатации и техническому обслуживанию

На рисунке 1.9 представлена диаграмма вариантов использования процесса выполнения ремонтных работ.



Рисунок 1.9 – Диаграмма процесса выполнения ремонтных работ

На рисунке 1.10 представлена диаграмма последовательности процесса «Изучить лист о ремонте оборудования».

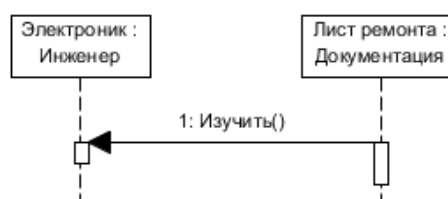


Рисунок 1.10 – Диаграмма процесса изучения листа о ремонте

На рисунке 1.11 представлена диаграмма вариантов использования процесса «Производить наладку».

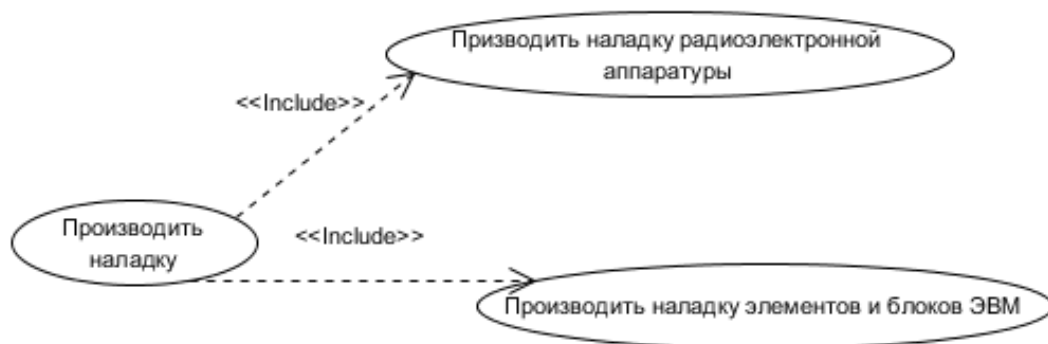


Рисунок 1.11 – Диаграмма процесса производства наладки

На рисунке 1.12 представлена диаграмма последовательности наладки радиоэлектронной аппаратуры.



Рисунок 1.12 – Диаграмма процесса наладки радиоэлектронной аппаратуры

На рисунке 1.13 представлена диаграмма последовательности процесса наладки элементов и блоков ЭВМ.

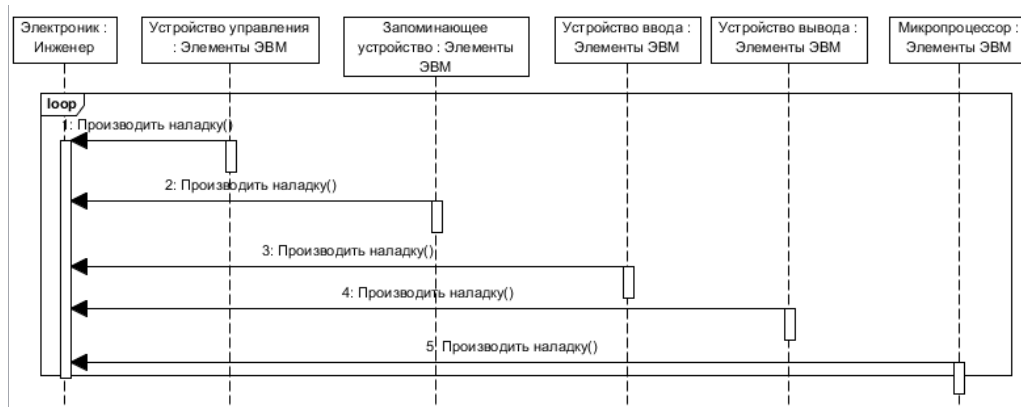


Рисунок 1.13 – Диаграмма процесса наладки элементов и блоков

1.3 Деятельность Новосибирского регионального центра связи

Новосибирский региональный центр связи обслуживает устройства связи и радиосвязи в границах Новосибирского отделения дороги 1048 км пути. На рисунке 1.14 представлена схема расположения предприятий, обслуживающихся в Новосибирском региональном центре связи.



Рисунок 1.14 – Схема расположения предприятий, обсуживающих
Новосибирским региональным центром связи

Основная деятельность центра связи направлена на предоставление оперативно-технологической связи и радиосвязи для подразделений ОАО «РЖД», а также предоставление услуг связи в соответствии с лицензиями для сторонних организаций и пользователей. Для дальнейшего рассмотрения предметной области необходимо изучить организационную структуру предприятия. На рисунке 1.15 представлена организационная структура Новосибирского регионального центра связи, выполненная в нотации ARIS.

Центр состоит из 6 производственных участков и объединяющих 28 ремонтно-восстановительных бригад:

- производственный участок по обслуживанию устройств связи и радиосвязи Татарская – Кургат;
- производственный участок по обслуживанию устройств связи и радиосвязи Кокошино – Новосибирск;

- производственный участок по обслуживанию устройств связи и радиосвязи Новосибирский узел;
- производственный участок по обслуживанию устройств связи и радиосвязи Инская – Промышленная;
- производственный участок по обслуживанию устройств связи и радиосвязи Болотная – Черепаново;
- производственный участок мониторинга и диагностики сети связи (ЦТО) [4].

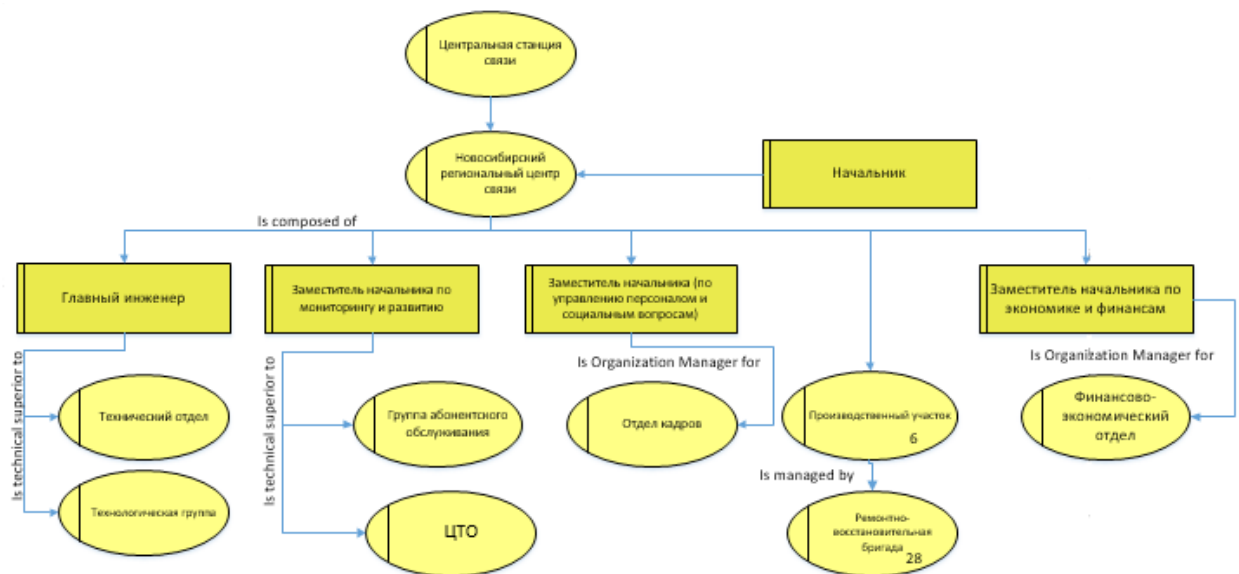


Рисунок 1.15 – Организационная структура Новосибирского РЦС в нотации ARIS

Основными задачами Новосибирского регионального центра связи являются:

- обеспечить услугами технологической связи все подразделения ОАО «РЖД», которые находятся на границах обслуживания РЦС. Технологическая связь позволяет поддерживать организацию перевозочного процесса. Так же позволяет управлять структурными подразделениями, персоналом организации и финансовыми ресурсами, где приоритетом является обеспечение безопасности движения поездов;
- оказание услуг связи на возмездной основе в рамках, выданных ОАО «РЖД» лицензий на оказание услуг связи;

- осуществление иных видов деятельности, предусмотренных законодательными и иными нормативными актами Российской Федерации, и внутренними документами ОАО «РЖД» и Центральной станции связи [4].

1.4 Обзор существующего программного обеспечения для мониторинга сети

В настоящее время существуют разнообразные программы по администрированию и мониторингу сети. Все они разные и каждая программа предназначена для определённых целей. В работе проанализированы 3 программы их преимущества и недостатки, для того чтобы сделать вывод, учесть преимущества и недостатки других программ для дальнейшей разработки.

10-Strike LANState – программа для администрирования и мониторинга серверов, компьютеров и других сетевых устройств [5]. Стоимость программы различается в зависимости от версии и количества хостов. Со стоимостью можно ознакомиться в таблице 1.1.

Таблица 1.1 – Информация о стоимости лицензии

Тип лицензии	Стоимость, руб.
Лицензия для мониторинга 100 хостов	7990
Лицензия для мониторинга 200 хостов	9990
Лицензия для мониторинга 500 хостов	14990
Лицензия для мониторинга 1000 хостов	19990
Лицензия на организацию (количество хостов неограниченно; до 20 рабочих мест с программой)	49990
Лицензия на организацию с филиалами (количество хостов неограниченно; до 50 рабочих мест с программой)	99990

Стоимость лицензии указано на момент 29.01.2018 года.

Интерфейс программы представлен на рисунке 1.16. Данную программу можно скачать с официального сайта и воспользоваться, если нужно 30-дневной пробной версией.

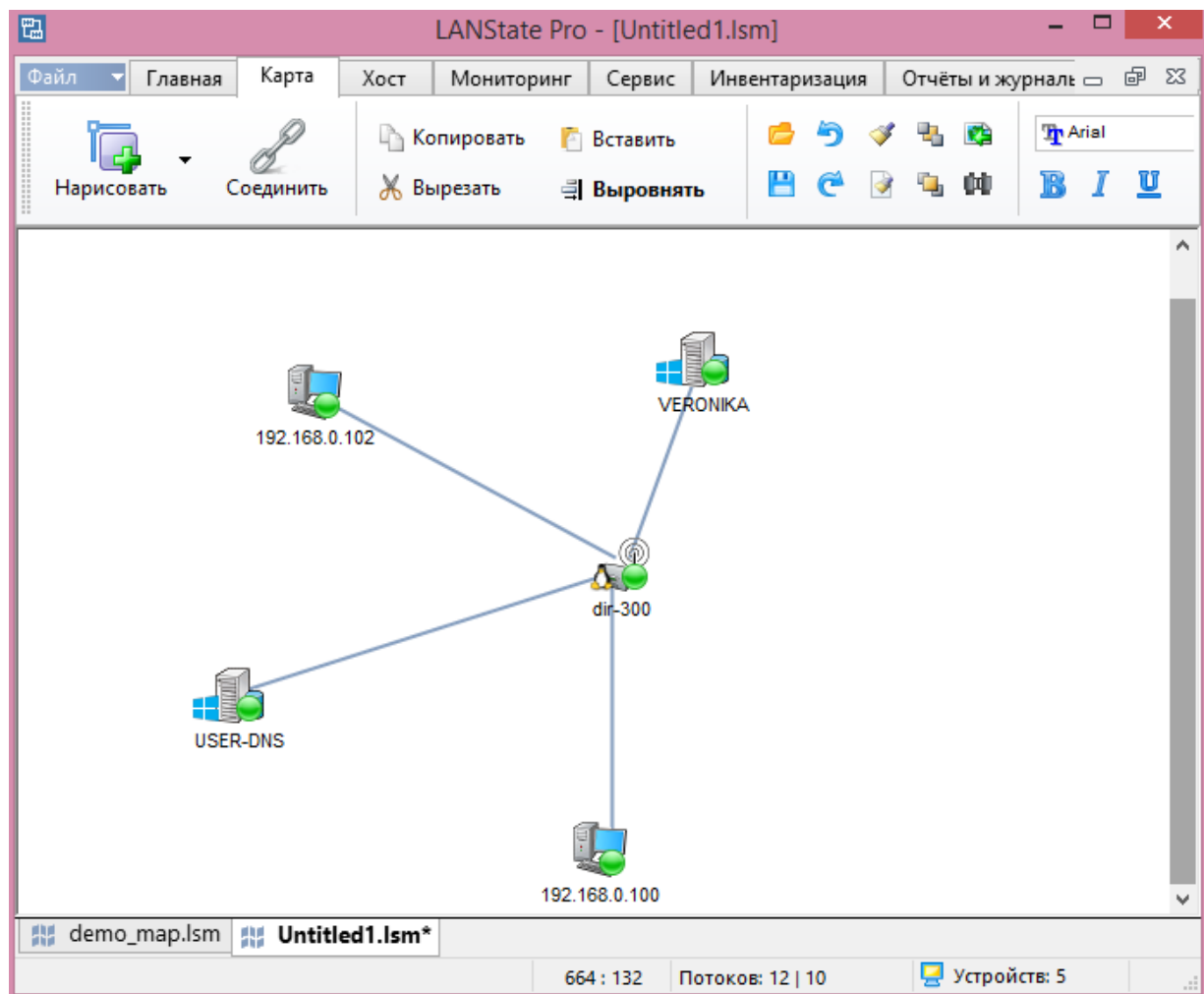


Рисунок 1.16 – Интерфейс программы LANState

При запуске программы можно выбрать режим работы с сетевыми устройствами, построить сеть автоматически на основе имеющихся устройств или нарисовать свою сеть.

Программа позволяет выгрузить статистику как общую, так и конкретного устройства, на рисунке 1.17 представлена статистика домашнего компьютера, находящегося в сети.

Система автоматически опрашивает устройства, и запоминает время его отклика. На рисунке 1.18 можно увидеть проверку, которую сделала программа к выбранному устройству.

Параметр	Значение
Адрес хоста	192.168.0.103
IP-адрес	192.168.0.103
DNS-имя	Veronika.fl.zsttk.ru
MAC-адрес	14-2D-27-05-29-B1
Производитель Ethernet-адаптера	[Hon Hai Precision Ind. Co.,Ltd.]
Пользователь	MSSQLSERVER01; MSSQLSERVER02; MSSQLSERVER03; MSSQLSERVER04; MSSQLSERVER05; MSSQLSERVER06; MSSQLSERVER07; MSSQLSERVER08; MSSQLSERVER09; MSSQLSERVER10; MSSQLSERVER11; MSSQLSERVER12; MSSQLSERVER13; MSSQLSERVER14; MSSQLSERVER15; MSSQLSERVER16; MSSQLSERVER17; MSSQLSERVER18; MSSQLSERVER19; MSSQLSERVER20; verunchik175@outlook.com
Домен	WORKGROUP
Сервер	VERONIKA
Тип ОС	Windows 6.3 Server running the master browser service
Дата/время	13.02.2018 20:46:41
Время работы	5 ч., 45 мин., 31 сек.
Диски	<не удалось определить>

Рисунок 1.17 – Общая информация о устройстве

[illegible]

Рисунок 1.18 – Окно настройки мониторинга

В результате использования этой программы выявлены следующие преимущества и недостатки.

Преимущества программы:

- программа автоматически строит сеть, определяет устройства и получает от него информацию;
- строить сеть можно самостоятельно;
- звуковое оповещение при не ответе устройства, SMS, E-mail;

- выгрузка статистики;
- не требует установки дополнительного ПО на сервера и другие сетевые устройства.

Недостатки программы:

- нельзя пользоваться функциями программы такими как «Учет трафика, мониторинг контроля канала связи», по нажатию предлагается купить специализированную для этого программу;
- долгий поиск разнообразных настроек;
- нет защиты паролем на вход.

Pandora FMS (Pandora Flexible Monitoring System) – система позволяющая осуществлять мониторинг сети, и визуально отображать состояние системы. Стоимость самой версии на 1000 хостов составляет – 187 613 тыс. рублей (на 11.01.2018), стоимость расширенной версии на любое количество хостов составляет 268 019 тыс. рублей (на 11.01.2018). На рисунке 1.19 – 1.20 можно увидеть интерфейс программы [6].

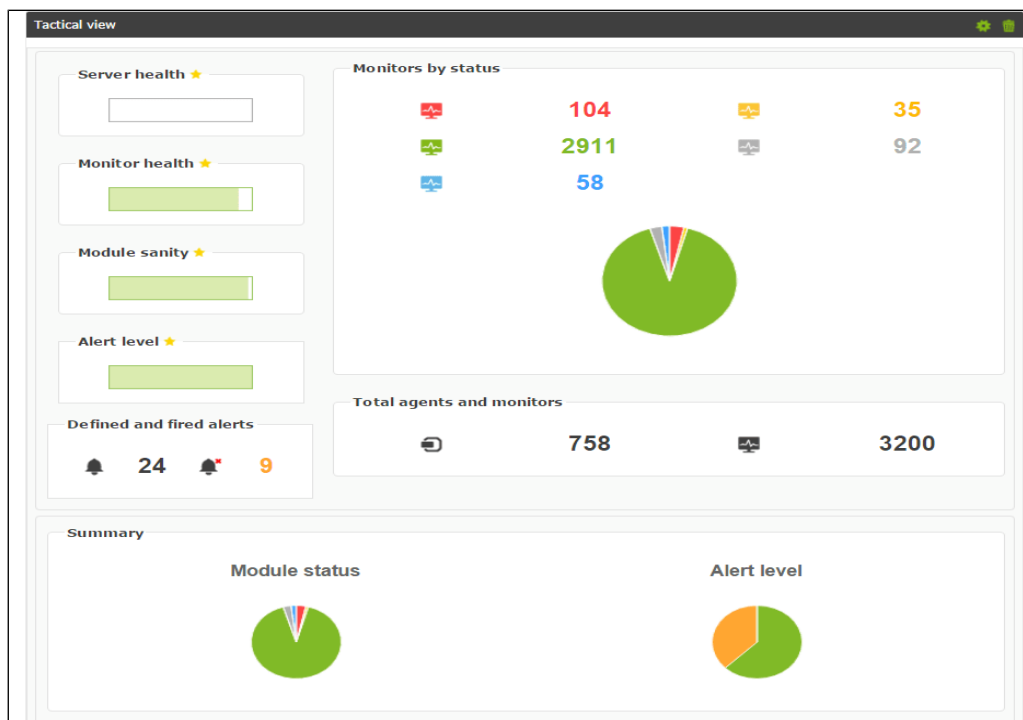


Рисунок 1.19 – Представление результатов работы программы

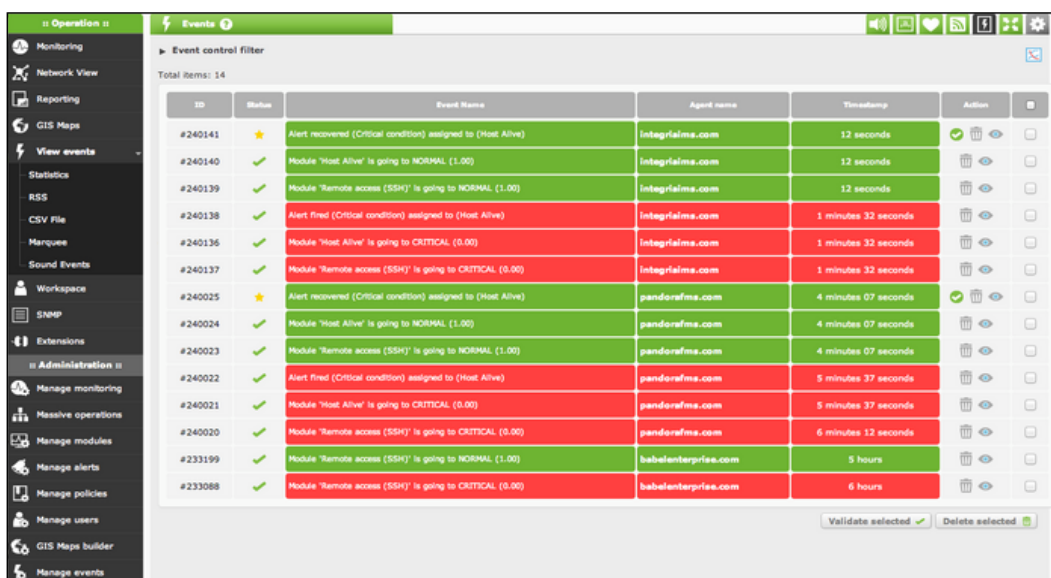


Рисунок 1.20 – Окно с сигналами об ошибках

Данная программа предлагает большой список функций. Были изучены некоторые из них и составлены следующие преимущества и недостатки.

Преимущества программы:

- оповещение пользователя об инцидентах;
- доступ каждого пользователя или групп пользователей на вход и работу;
- составление отчетности;
- автоматически определяют топологию сети;
- хранение данных длительное время для дальнейшей отчетности.

Недостатки программы:

- высокая стоимость;
- нельзя контролировать трафик;
- для небольшого предприятия, которому нужно контролировать сеть, эта система слишком многофункциональна.

Zenoss Core – бесплатное, но позволяющее избавиться от серьезных проблем на предприятии система, позволяет контролировать находящиеся в сети устройства и их конфигурацию [7].

На рисунке 1.21 можно увидеть интерфейс программы.

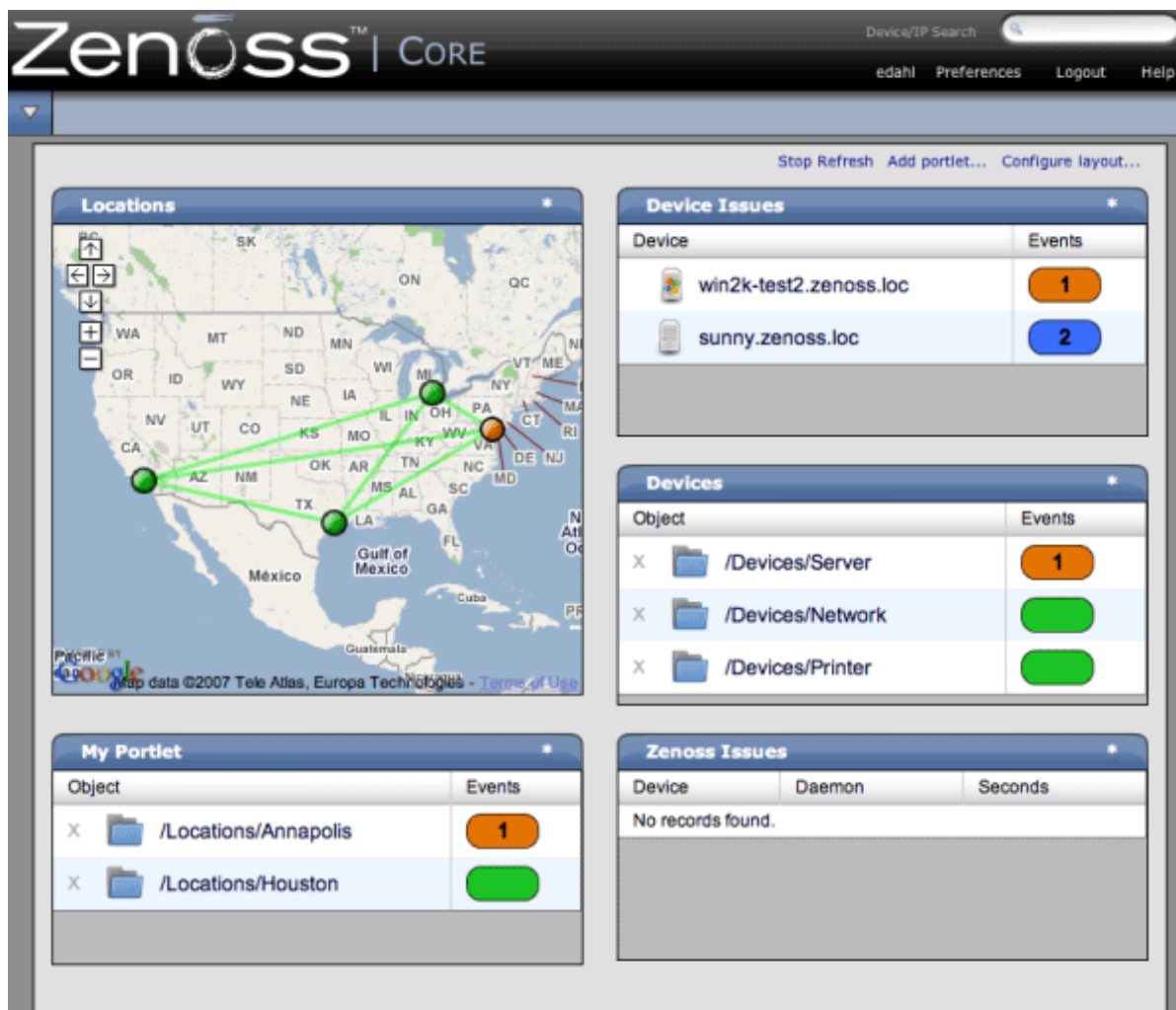


Рисунок 1.21– Интерфейс программы Zenoss core

Преимущества программы:

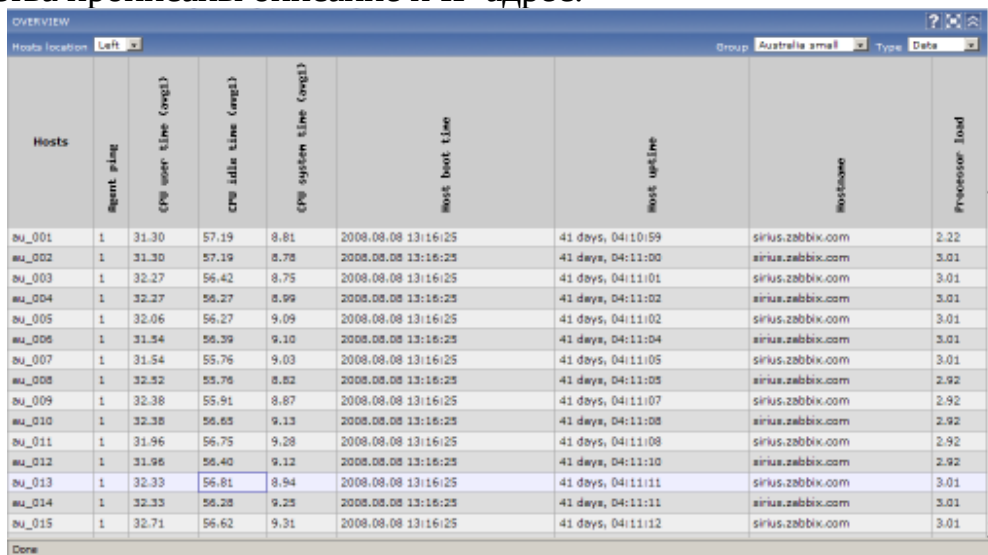
- удобный интерфейс;
- оповещение пользователей об инцидентах связанных с отключением портов, не ответа оборудования;
- бесплатное программное обеспечение;
- возможность расширения функциональности за счет других плагинов;
- доступна функция авто обнаружения активных системах в сети.

Недостатки программы:

- недостаточная защищенность данных;
- программа не полностью является бесплатной, для лучшей производительности и защищенности нужно покупать дополнения.

Zabbix – система мониторинга предназначена для контроля за состоянием сетевого оборудования.

Zabbix состоит из сервера, базы данных, веб-интерфейса и агента. Zabbix-агент устанавливается на устройствах и предоставляет данные серверу. На рисунке 1.22 представлены узлы сети (хост) для каждого устройства прописаны описание и IP-адрес.



Hosts	Agent ping	CPU user time (%)	CPU idle time (%)	CPU system time (%)	Host boot time	Host uptime	Hostname	Processor load
bu_001	1	31.30	57.19	8.81	2008.08.08 13:16:25	41 days, 04:10:59	sirius.zabbix.com	2.22
bu_002	1	31.30	57.19	8.78	2008.08.08 13:16:25	41 days, 04:11:00	sirius.zabbix.com	3.01
bu_003	1	32.27	56.42	8.75	2008.08.08 13:16:25	41 days, 04:11:01	sirius.zabbix.com	3.01
bu_004	1	32.27	56.27	8.99	2008.08.08 13:16:25	41 days, 04:11:02	sirius.zabbix.com	3.01
bu_005	1	32.06	56.27	9.09	2008.08.08 13:16:25	41 days, 04:11:02	sirius.zabbix.com	3.01
bu_006	1	31.54	56.39	9.10	2008.08.08 13:16:25	41 days, 04:11:04	sirius.zabbix.com	3.01
bu_007	1	31.54	55.76	9.03	2008.08.08 13:16:25	41 days, 04:11:05	sirius.zabbix.com	3.01
bu_008	1	32.52	55.76	8.82	2008.08.08 13:16:25	41 days, 04:11:05	sirius.zabbix.com	2.92
bu_009	1	32.38	55.91	8.87	2008.08.08 13:16:25	41 days, 04:11:07	sirius.zabbix.com	2.92
bu_010	1	32.38	56.65	9.13	2008.08.08 13:16:25	41 days, 04:11:08	sirius.zabbix.com	2.92
bu_011	1	31.96	56.75	9.28	2008.08.08 13:16:25	41 days, 04:11:08	sirius.zabbix.com	2.92
bu_012	1	31.96	56.40	9.12	2008.08.08 13:16:25	41 days, 04:11:10	sirius.zabbix.com	2.92
bu_013	1	32.33	56.81	8.94	2008.08.08 13:16:25	41 days, 04:11:11	sirius.zabbix.com	3.01
bu_014	1	32.33	56.28	9.25	2008.08.08 13:16:25	41 days, 04:11:11	sirius.zabbix.com	3.01
bu_015	1	32.71	56.62	9.31	2008.08.08 13:16:25	41 days, 04:11:12	sirius.zabbix.com	3.01

Рисунок 1.22 – Окно с описанием устройств

В Zabbix существует возможность создавать условия-триггеры, которые срабатывают при неполадках или авариях. При срабатывании включается звуковое оповещение. При отсутствии администратора на месте система имеет возможность отправлять уведомления на почту или sms или самостоятельно решить возникшую проблему с помощью заранее действий которые запускаются при срабатывании определенного триггера.

Преимущества программы:

- возможность использования внешних скриптов для получения данных от устройств;
- позволяет исправить критическую ситуацию с помощью заранее определенных действий;
- оповещение администратора даже при отсутствии его на рабочем месте;
- составление отчетности и построение диаграмм.

Недостатки программы:

- не существует стандартного способа защитить взаимодействие между агентами и их сервером.

1.5 Выводы по первому разделу

На основании рассмотренного материала в разделе были сделаны следующие выводы:

- на инженера–электроника возложено множество обязанностей, каждая из которых была рассмотрена и изучена. Все выполняющиеся функции работника занимают много времени, особенно те, которые связаны с ремонтом оборудования или устранения критических ситуаций. Автоматизация данных процессов позволит работникам оперативно реагировать на критические ситуации связанные с отключением оборудования, перезагрузки или влияние параметров оборудования на его состояние;
- центральная станция связи, являющаяся филиалом ОАО «РЖД», как и многие большие компании использует программы по мониторингу и администрированию сети. Автоматизация контроля доступа к сети интернет, а также мониторинг пользователей сети позволяет избавиться от огромных затрат организации на наладку и обеспечение бесперебойной работы;
- на сегодняшний день представлено множество программ и встроенных в них функций, но не каждая подойдет к конкретной организации. Покупка лицензии программы сильно сказывается на бюджете предприятия, поэтому внедрение программы контроля предназначенной для конкретных целей организации сказывается благоприятно на бюджете организации.

2 Моделирование процесса предоставления доступа к сети Интернет

2.1 Понятие прокси-сервера и его назначение

Большая организация всегда будет беспокоиться вопросами безопасности данных и работоспособности своих технических средств. Ограничение доступа к сети Интернет всем сотрудникам организации является не очень мудрым решением так же, как и доступ к сети Интернет всем сотрудникам. Прокси-сервер является не только дополнительным источником защиты данных организации, а также ускоряет работу, а именно, когда пользователь отправляет запрос в Интернет, запрос идет на прокси-сервер, после чего он отправляет запрос уже от своего имени [8]. Наглядно этот процесс можно увидеть на рисунке 2.1.



Рисунок 2.1 – Запрос через прокси-сервер

Как правило, организации, прокси-сервер нужен для некоторых из ниже перечисленных целей:

- обеспечить доступ к сети Интернет с компьютеров локальной сети;
- экономить внешний трафик клиента или внутренний трафик компании;
- ускорить доступ к ресурсу (кэш данных) – если доступ к определенному ресурсу происходит часто, на прокси-сервере создается копия этого ресурса и при следующем обращении прокси-сервер запускает копию, тем самым снижая нагрузку на канал и ускоряя получение информации с ресурса;
- ограничить доступ – прокси-сервер можно настроить таким образом, что компьютеры локальной сети могут выходить в Интернет не на все ресурсы, а только на те, которые компания допускает (например, корпоративный сайт, почта).

Если смотреть с технической точки зрения, после настройки прокси-сервера нужно настроить клиентские компьютеры.

При обращении к ресурсу клиентский компьютер должен обращаться по IP-адресу и нужному порту прокси-сервера, а не к IP-адресу сервера (ресурса).

Если клиентский компьютер настроен, то при обращении к ресурсу, компьютер открывает соединение с прокси-сервером отправляет ему запрос на ресурс.

В свою очередь, прокси-сервер делает проверку на правильность запроса и разрешение доступу к этому ресурсу клиентскому компьютеру.

Получив все необходимые данные, если клиентский компьютер имеет доступ к указанному им ресурсу, то прокси-сервер делает запрос этому ресурсу и передает информацию пользователю, в противном случае пользователю передается информация об ошибке.

2.2 Автоматизированная система обработки заявок

На сегодняшний день, в каждой большой организации есть отдел, который отвечает за бесперебойную работу сети, а также люди, которые занимаются предоставлением доступа к Интернет. Чаще всего, организация экономит на персонале, занимающимся этой работой, и вся обязанность ложится на одном или несколько человек. Организация, имеющая множество отделов и подразделений должны заботиться о безопасности данных и экономии своих ресурсов. Бумажная система крайне неудобно, учитывая масштабы некоторых предприятий, к примеру, ОАО «РЖД».

Прокси-сервер и администратор находятся на станции Новосибирск-Главный, при бумажной системе, чтобы пользователь со станции Барабинск получил доступ к информационным ресурсам он должен выполнить ряд действий со своей заявкой, после прохождения всех этапов, описанных ниже, заявка доходит до Информационно-вычислительного центра, где осуществляется одобрение или отказ. Этот долгий процесс отнимает рабочее время у пользователя, которому действительно нужен доступ к ресурсу, так и у всех руководителей, встречающихся на этапах согласования и подписания заявления. Внедрение данной системы исключает потерю заявок, контроль окончания сроков предоставления доступа к информационным ресурсам. Для устранения таких проблем и была внедрена «Автоматизированная система обработки заявок на предоставление доступа к информационным ресурсам» [9].

Система предоставляет следующую функциональность:

- создание заявки на предоставление доступа к информационным ресурсам;
- просмотр заявки на предоставление доступа к информационным ресурсам;
- просмотр и печать формы заявки на предоставление доступа к информационным ресурсам;
- редактирование заявки на предоставление доступа к информационным ресурсам;
- согласование заявки на предоставление доступа к информационным ресурсам;
- утверждение заявки на предоставление доступа к

информационным ресурсам;

- отклонение заявки на предоставление доступа к информационным ресурсам;
- визирование заявки на доступ к информационным ресурсам;
- отзыв заявки на предоставление доступа к информационным ресурсам;
- удаление заявки на предоставление доступа к информационным ресурсам;
- инициирование закрытия доступа по заявке на предоставление доступа к информационным ресурсам;
- поиск заявок на предоставление доступа к информационным ресурсам;
- формирование отчетов по заявкам на предоставление доступа к информационным ресурсам;
- корректировка персональных данных;
- назначение заместителей и визирующих лиц [9].

Данная система состоит из следующих подсистем:

- подсистема хранения и обработки заявок, которая обеспечивает маршрутизацию заявок и функции их автоматической обработки, а также предоставляет средства автоматической нумерации заявок, формирования отчета и выполнения поиска;
- подсистема пользовательского интерфейса, которая предоставляет пользователю интерфейс и обеспечивает работу пользователю в Системе;
- подсистема архивного хранения заявок на предоставления доступа к Системе, процессы согласования которых завершены;
- подсистема аналитической отчетности для формирования различных отчетов по реализованным в Системе процессам предоставления доступа к информационным системам ОАО «РЖД» за произвольный период времени;
- подсистема двухсторонней интеграции с ЕК АСУ ЕСПП для первоначальной загрузки данных в системный справочник информационных систем и их последующей актуализации, а также передачи данных об утвержденных заявках в ЕК АСУ ЕСПП;
- подсистема односторонней интеграции с ЕК АСУ ТР для первоначальной загрузки данных в справочник

пользователей Системы и их последующей актуализации;

- подсистема односторонней интеграции с системой управления доступом к ИС – КУБ для передачи данных об утвержденных заявках.

Система взаимодействует со следующими инфраструктурными системами ОАО «РЖД»:

- единая служба глобального каталога и служба разрешения имен (ГК и DNS) для обеспечения авторизации пользователей в Системе на основе учетных записей ГК и DNS;

- автоматизированная система управления трудовыми ресурсами (ЕК АСУ ТР) для первичного заполнения и поддержания в актуальном состоянии системного справочника пользователей ИС. Обновление данных происходит автоматически раз в сутки (регламент);

- автоматизированная система управления единой службой поддержки пользователей (АСУ ЕСПП) для передачи из АС ОЗ в АСУ ЕСПП данных об утвержденных заявках [9];

- почтовая система (ЭПС РЖД) для отправки почтовых уведомлений, сформированных в Системе.

Функционал системы представлен в виде диаграммы прикладной системы, выполненной в нотации ARIS на рисунке 2.2.

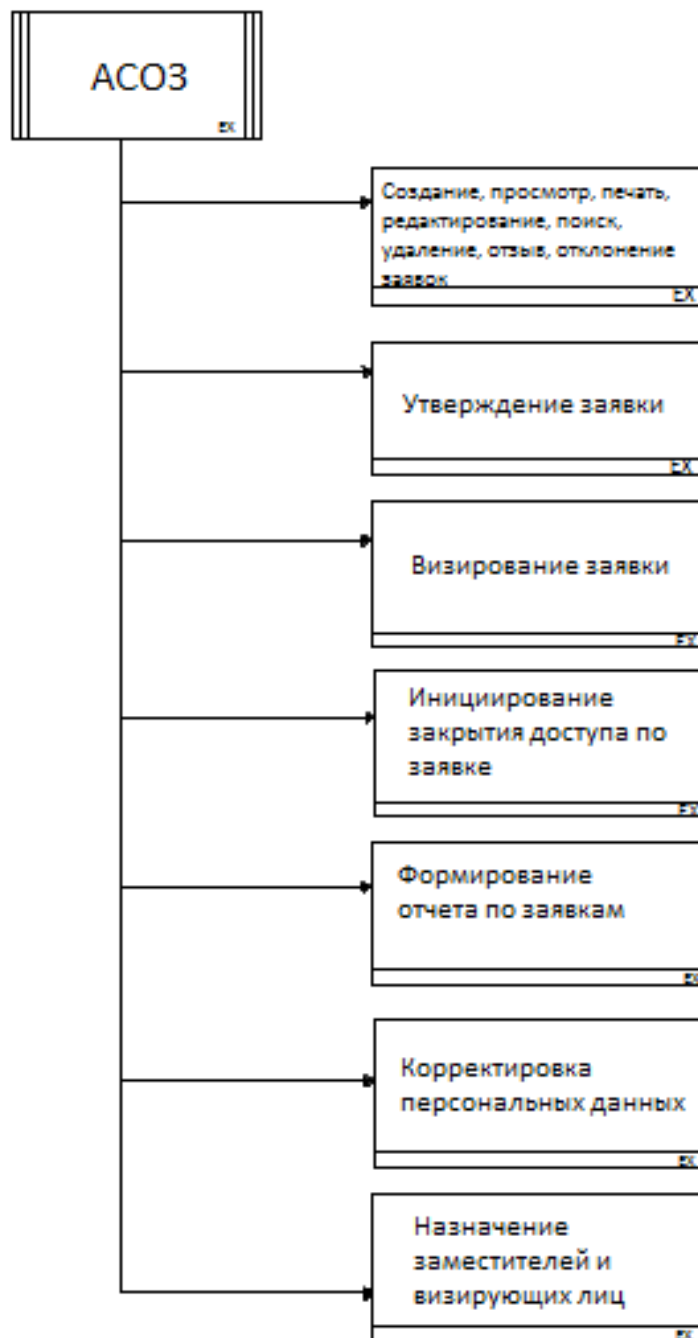


Рисунок 2.2 – Функциональные возможности АСОЗ

Роль пользователя в системе зависит от его должности и от исполняемых обязанностей. Права, которыми может пользоваться в системе пользователь, к примеру просмотр, поиск или работа с заявками определяется на основании какой роль у пользователя.

Далее приведено описание каждой из ролей системы.

Пользователь – эта роль присваивается абсолютно всем автоматически. Роль используется для обработки заявок, а самой главной

задачей является создание заявок. Весь функционал данной роли представлен на рисунке 2.3.

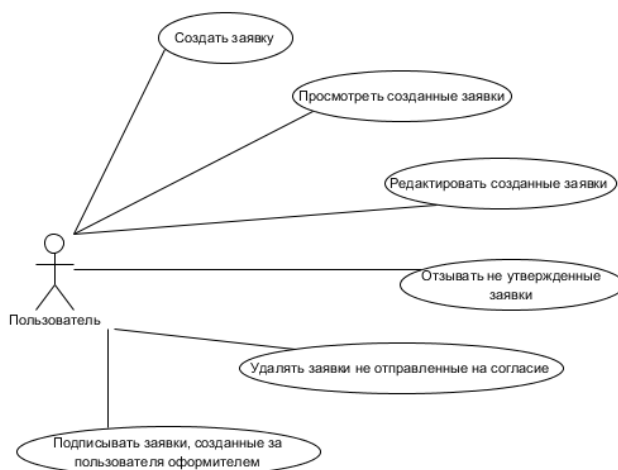


Рисунок 2.3 – Основные задачи пользователя

На рисунке 2.4 наглядно представлена страница создания заявки.

Рисунок 2.4 – Страница создания заявки

При первом запуске система распознавание подключившегося пользователя, для получения данных о его роли в системе [9].

Если данные учетной записи, под которой выполнено подключение, существуют в AD и системе АСОЗ, система распознает пользователя по учетной записи [9]. Смотреть на рисунке 2.5.

Личные данные пользователя

Пользователь распознан по учетной записи, заходит первый раз, данные для ознакомления. Изменение данных возможно на странице персональных настроек.

Филиал: Калининградская ЖД

Подразделение: Подразделение_тест\Отдел пользователя

Пользователь ИР: Пользователь И. И. (10101)

Фамилия: Пользователь

Имя: Иван

Отчество: Иванович

Должность: Агент (СФТО) | категории

Табельный номер: 10101

Электронный адрес: izotov.a@digdes.com

Внутренний телефон:

Номер комнаты:

Сохранить

Рисунок 2.5 – Страница с личными данными пользователя

Если данные учетной записи, под которой выполнено подключение, отсутствуют в AD, система производит поиск по табельному номеру и адресу электронной почты. Смотреть рисунок 2.6.

Табельный номер: 1235677

Подразделение:

Пользователь ИР:

Найти

Выбрать

Отмена

Рисунок 2.6 – Окно поиска по табельному номеру

Если распознавание по учетной записи и табельному номеру не дало результатов, пользователю предлагается самостоятельно выбрать данные из справочника сотрудников.

Такое распознавание происходит при первом входе любого пользователя вне зависимости от роли. Существующие роли в системе:

- утверждающий/согласующий – согласует/утверждает заявки на предоставление доступа к информационным ресурсам. Данную роль назначает Администратор. В качестве роли согласующего лица могут быть - руководитель подразделения, распорядитель ИС, администратор ИС, администратор безопасности, утверждающее лицо. Функции данной роли представлен на рисунке 2.7;

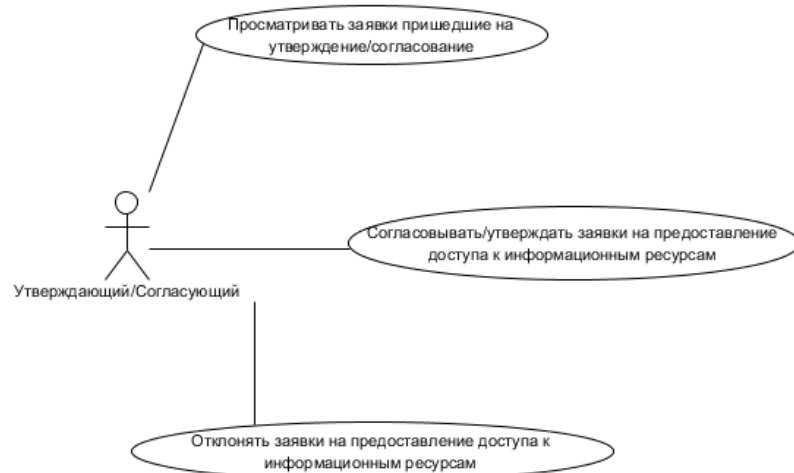


Рисунок 2.7 – Основные задачи утверждающего/согласующего
 - ответственный оформитель – оформляет заявки за других пользователей. Существуют разные виды ответственных оформителей, их функции представлены на рисунках 2.8-2.10;

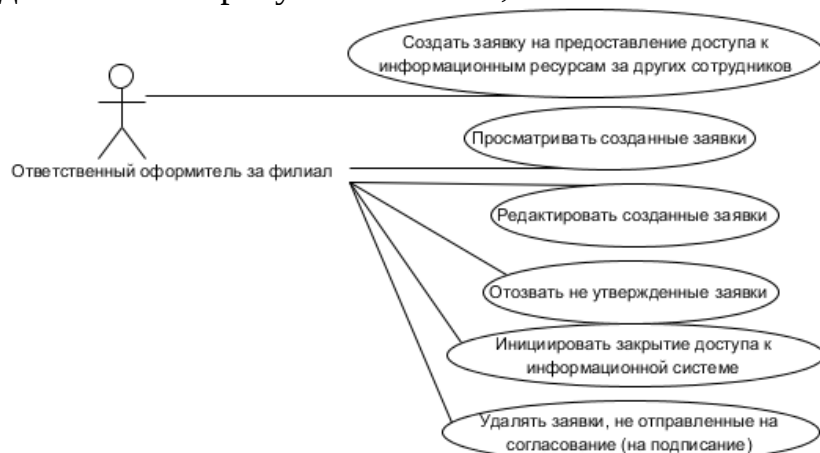


Рисунок 2.8 – Основные задачи ответственного оформителя за филиал

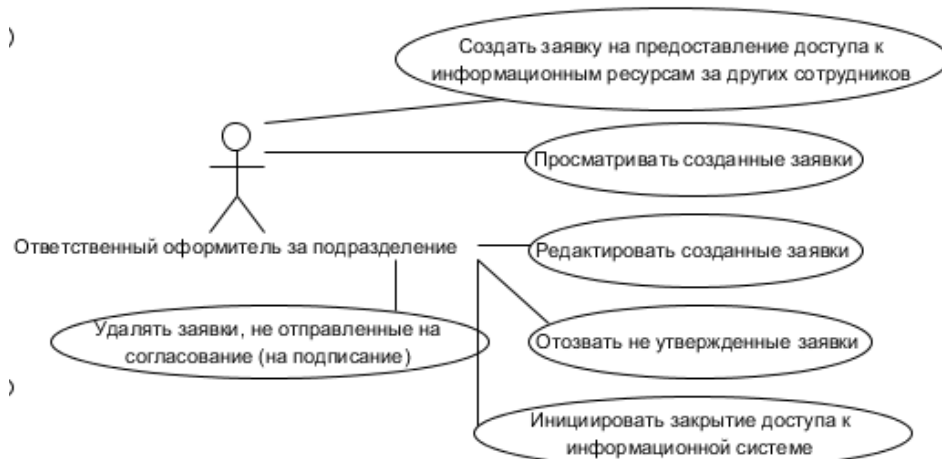


Рисунок 2.9 – Основные задачи ответственного оформителя за подразделение



Рисунок 2.10 – Основные задачи ответственного оформителя за подразделение и подчиненные организационные единицы

- контролер – данная роль используется с целью контроля подачи и рассмотрения заявок пользователями. Рассмотренные функции контролера представлены на рисунке 2.11;

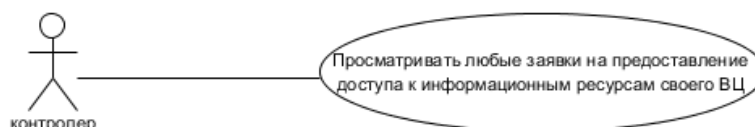


Рисунок 2.11 – Основная функция роли контролера

- визирующий за «ФИО» - назначается пользователю, если он является заместителем сотрудника, указанного в названии роли и ответственного за утверждение/согласование заявок. Визирование не подразумевает права подписи, то есть полномасштабного замещения отсутствующего сотрудника. Данная роль назначается Администратором системы или руководителем подразделения [9]. Основные функции представлены на рисунке 2.12;

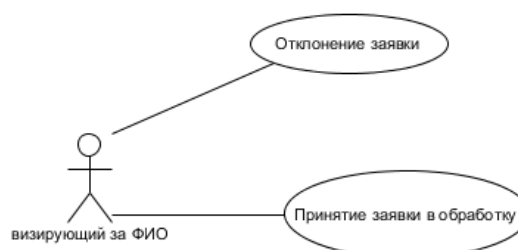


Рисунок 2.12 – Основные функции визирующего за «ФИО»

- утверждающий/согласующий за «ФИО» - назначается пользователю, если он является заместителем сотрудника, указанного в

названии роли и ответственного за утверждение/согласование заявок. Данная роль подразумевает полное замещение, включая непосредственно согласование и утверждение заявок, а также право подписи [9]. Данная роль назначается Администратором системы или самим сотрудником, назначающим себе заместителя с правом подписи. Основные функции данной роли представлены на рисунке 2.13;

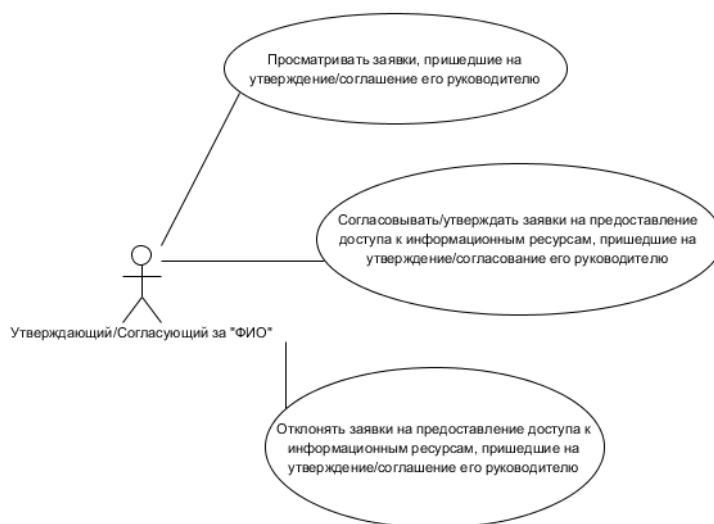


Рисунок 2.13 – Основные функции утверждающего/согласующего за «ФИО»

2.3 Организация доступа пользователей к информационным системам общего пользования (сети Интернет)

Предоставление пользователям доступа к информационным ресурсам осуществляется на основании их заявок, которые оформляются с использованием автоматизированных систем обработки заявок на доступ к информационным ресурсам. Решение о предоставлении доступа внутренним пользователям в зоне ответственности информационно-вычислительного центра к информационным системам общего пользования в связи с производственной необходимостью принимается на основании заявки, которая составляется пользователем или ответственным за оформление заявок [9]. В дальнейшем пользователь может наблюдать за состоянием заявки, где указывается на каком этапе она находится. При входе в систему формируется список заявок, доступных для обработки, представлено на

рисунке 2.14. Доступность заявок зависит от исполняемой роли.

Получено 59 заявок										Заявок на странице: 10
	№	Дата создания	Автор	Состояние	Пользователь ИР	ИС-ИР	Тип заявки	Доступ до	Дата поступления на согласование	Печатная форма
<input type="checkbox"/>	4090/2010	22.04.2010	Соколова Н.А.	На согласовании Администратор системы А., 11111 Диспетчер маневровый железнодорожной ста, Подразделение администратора системы	Соколова Н.А.	АСУ ТЕСТ	Подключение	22.04.2012	22.04.2010	
<input type="checkbox"/>	4485/2011	14.02.2011	Шевченко А. Ю.	Отозвана	Шевченко А. Ю.	Система информационного сервиса "ЭФФЕКТ"01. Суточный отчет 58 листов	Подключение	14.02.2012		
<input type="checkbox"/>	4513/2010	27.04.2010	Соколова Н.А.	На согласовании Администратор системы А., 11111 Диспетчер маневровый железнодорожной ста, Подразделение администратора системы	Соколова Н.А.	АСУ ТЕСТ	Подключение	27.04.2012	27.04.2010	
<input type="checkbox"/>	4519/2010	27.04.2010	Соколова Н.А.	На согласовании Администратор системы А., 11111 Диспетчер маневровый железнодорожной ста, Подразделение администратора системы	Соколова Н.А.	АСУ ТЕСТ	Подключение	27.04.2012	27.04.2010	

Рисунок 2.14 – Список заявок

В информационно-вычислительном центре заявки рассматриваются, подписываются администратором безопасности и начальником отдела безопасности информационных ресурсов, подписываются руководителем подразделения - распорядителя информационной системы (раздела информационной системы) заявки с прилагаемыми материалами направляются на согласование в соответствующий региональный центр безопасности, а затем на утверждение в службу корпоративной информатизации железной дороги. Утвержденные заявки служба корпоративной информатизации железной дороги направляет в соответствующий информационно-вычислительный центр для исполнения.

Подключение к информационным системам общего пользования внутренних пользователей осуществляется работниками информационно-вычислительного центра, которые устанавливают на ПЭВМ пользователя «агента безопасности», а также производят необходимую настройку программного обеспечения в соответствии с политикой и стандартами информационной безопасности ОАО «РЖД». Доступ к информационным системам общего пользования осуществляется только при наличии на ПЭВМ пользователя корпоративного антивирусного программного обеспечения в активном состоянии с регулярным обновлением антивирусных баз данных [9]. Срок действия использования информационных ресурсов 2 года со дня исполнения заявки. По окончании срока действия заявки пользователь будет отключен от информационной системы (информационных ресурсов) которой

был предоставлен доступ. При увольнении или перевода работника, пользователя отключают от предоставленных ресурсов.

Продление права доступа пользователя осуществляется на основании своевременно оформленной и согласованной заявки [9]. Установка Системы на рабочих станциях пользователей не требуется. Вход пользователей в систему осуществляется через Internet Explorer путем ввода в адресной строке адреса веб-приложения Системы. При входе осуществляется авторизация пользователя в Системе на основе его учетной записи в ГК и DNS ОАО «РЖД».

2.4 Выводы по второму разделу

В данном разделе было рассмотрено моделирование предоставления доступа к Интернет. Данное изучение позволило сделать ряд выводов:

- использование прокси – сервера должно иметь обязательный характер для больших организаций. Контролировать всех пользователей в локальной сети в таких организациях очень сложно, особенно если контроль нацелен с целью экономии трафика компании и предотвращения хищения данных организации из внешней среды;
- автоматизированная система была введена в эксплуатацию с 2011 года на ОАО «РЖД». Были выявлены преимущества данной системы, такие как удобство использования, централизованная организация управления и сокращение сроков отказа или одобрения заявки;
- при отправке пользователем заявки на предоставление доступа, руководитель подразделения, в котором работает пользователь всегда будет уведомлен кто и для каких целей будет использовать ресурсы. Также все последующие роли принимают непосредственное участие на одобрение или отказ заявки, что позволяет контролировать решение предыдущего согласующего/утверждающего лица.

3 Разработка системы контроля доступа сети Интернет

3.1 Описание протокола управления сетью SNMP

Сеть в организации может постоянно расти и объединяться, вопросы управления такими сетями становятся очень важными. Управление сетью строится между станцией управления сетью называемой менеджером и элементами сети. Элементом сети может служить любое устройство которое использует протокол TCP/IP. Примерами таких устройств может служить, коммутатор, маршрутизатор, принтер и другие устройства.

Протокол SNMP используется для управления сетевыми устройствами. С помощью протокола часто решаются такие задачи как опрос оборудования в сети и управление оборудованием. Первая задача реализуется с помощью таких запросов как GET и GETNEXT. Вторая задача выполняется при помощи запроса SET, который позволяет изменять состояния оборудования, к примеру, отключить интерфейс на оборудовании [10].

SNMP есть в трех версиях SNMPv1, SNMPv2 и SNMPv3. Первая версия протокола является самой небезопасной, сообщения протокола подвержены модификации, подмене и прослушиванию. Он базируется на аутентификации на основе единой текстовой строки, которая передается в теле сообщения и является своеобразным паролем. Первая версия является часто используемой, так как она является самой простой.

Вторая версия протокола SNMP была несколько раз модифицирована, по итогу вернулись к модели безопасности на основе сообществ. В результате повысилось быстродействие протокола и безопасность.

Третья версия протокола стала поддерживать аутентификацию на основе имени пользователя, а также шифрование трафика.

Суть работы протокола в том, что на управляемой системе есть запущенная программа (агент) которая передает менеджеру информацию об устройстве, как правило, этот обмен данными односторонний. В SNMP

взаимодействие устроено по принципу запрос – ответ. Сам по себе агент инициировать сообщения не может кроме случая, когда устройство предупреждает администратора о критических ситуациях, к примеру переход оборудования с бесперебойного питания на питание от батарей. Сообщение, которое отправляет устройство называется trap.

Так как адреса объектов устройства представлены в числовом виде, для упрощения работы с ними и указания какие параметры можно контролировать через SNMP используется информационная база управления MIB. Объекты в MIB имеют иерархическую структуру которая представлена в виде дерева. В базе управляющей информации содержится десять корневых узлов каждый из которых содержит в себе разное число объектов. Каждый объект в дереве MIB имеет числовой идентификатор называемым OID и уникальную константу Object Name, которая представлена для всего MIB и соответствующую определенному OID.

Для примера, адрес объекта содержащий наименование система 1.3.6.1.2.1.1.5, а его имя будет sysName.

SNMP использует транспортный протокол UDP, протокол является наименее требовательным и позволяет быстро получать информацию от устройств.

При отправке запросов менеджер чтобы распознавать ответы, полученные от устройства помечает их, к примеру, при отправке нескольким устройствам запроса он прикрепляет для каждого уникальный ID, для того чтобы понять от какого устройства при ответе получены данные.

При отправке ответа, устройство добавляет в свой ответ тот ID который получил от менеджера не модифицируя его.

Среди преимуществ данного протокола можно выделить:

- открытость стандарта;
- удобство использования;
- простота (кроме SNMPv3);

- низкая стоимость реализации.

Среди недостатков можно выделить:

- работа через ненадежный протокол UDP;
- неприспособленность при работе с большими данными в крупных сетях;
- отсутствие взаимной аутентификации между менеджером и агентом.

Наряду с этим протоколом были разработки и других, схожих с SNMP протоколом. Одним из таких протоколов можно выделить NETCONF. Отличительной чертой от протокола SNMP является использование в качестве транспорта четыре протокола: SSH, SOAP, TLS, BEEP.

В протоколе NETCONF определены базовые операций, такие как get, get-config, edit-config, copy-config, delete-config, lock, unlock, close-session, kill-session.

Все эти операции оборачиваются в RPC запросы, которые в свою очередь представляются в XML. Протокол на уровне с SNMP имеет ряд преимуществ:

- использование более надежных протоколов в отличие от UDP который используется в SNMP;
- возможность открытия нескольких сессий;
- производить конфигурацию путем отправки нескольких параметров одним запросом;
- делать откат конфигураций;
- получать результаты в виде RPC – reply.

Пример запроса, который заключается в том, чтобы спросить часть текущей конфигурации представлен на рисунке 3.1.

На представленной xml - разметке значение message-id=100 указывается как при запросе, так и сохраняется при ответе на этот запрос. Нужно это для того чтобы отличать ответы, полученные на разные запросы.

```

    <rpc message - id=«100»
    xmlns=«urn:ietf:params:xml:ns:netconfbase:1.0»>
    <get-config>
    <source>
    <running/>
    </source>
    <filter type= «subtree»>
    <configuration>
    <protocols/>
    </configuration>
    </filter>
    </get-config>
    </rpc>

```

Рисунок 3.1 – Xml разметка запроса

Данный протокол отлично работает для оборудования линейки Juniper. С оборудованием компании Cisco, протокол NETCONF работает, но с ним возникают сложности такие как:

- запросы обрабатываются долго, они очень сильно нагружают CPU;
- вывод в виде XML происходит некорректно, пропадают описания некоторых параметров;
- на некоторые часть команд, ответ не совсем совпадает с запросом (к примеру, при запросе вывода состояния vlan ответ может выдать конфигурации всех портов и vlan).

Протокол SNMPv2 выбрал для мониторинга устройств в разрабатываемой системе, так как этот протокол является часто используемым в управлении сетью, а главное поддерживается в полной мере тестируемыми устройствами. Все его преимущества позволяют сделать вывод что данный протокол позволяет в полной мере контролировать сеть и благодаря этому избегать критических ситуаций.

3.2 Разработка программного обеспечения

В качестве среды разработки была выбрана Microsoft Visual Studio

2012, а в качестве языка программирования язык C#. Эти средства были выбраны, так как во время обучения были получены навыки работы в них [11].

В качестве системы управления базами данным используется Microsoft SQL Server 2016 [12].

При разработке информационной системы была подключена и использована библиотека SnmpSharpNet. Эта библиотека свободно распространяется и может использоваться бесплатно для коммерческих целей.

Данную библиотеку разработала компания Milan Sinadinovic, офис находится в США.

Скачивания данной библиотеку на данный момент составляет больше 1 млн.

Библиотека SnmpSharpNet распространяется по лицензии GNU GPL. Цель GNU GPL — предоставить пользователю права копировать, модифицировать и распространять (в том числе на коммерческой основе) программы, а также гарантировать, что и пользователи всех производных программ получают вышеперечисленные права [13].

3.3 Тестирование программного обеспечения на реальных устройствах

Тестирование программного обеспечение проходило на двух видов устройств: домашние ноутбуки и маршрутизатор cisco.

Организация, занимающаяся мониторингом сети или подключением устройств к сети Интернет чаще всего использует устройства компании Cisco.

Маршрутизатор, используемый для тестирования является Cisco 871 – K9. Данный маршрутизатор поддерживает SNMP, что позволяет программному обеспечению контролировать это устройство [14]. Внешний вид тестируемого маршрутизатора представлен на рисунке 3.2.



Рисунок 3.2 – Внешний вид устройства

Со стороны панели управления устройство представлено на рисунке 3.3.



Рисунок 3.3 – Панель управления устройства

Для осуществления первоначальной настройки требуется подключаться через консольный порт, кабель представляет собой с одной стороны RJ-45 с другой RS-232, данный кабель представлен на рисунке 3.4.



Рисунок 3.4 – Консольный кабель

При настройке на ноутбуке в котором отсутствует COM порт, был использован кабель-адаптер AM - COM DB9M(RS232), представленный на рисунке 3.5.



Рисунок 3.5 – Кабель для подключения к ноутбуку

Вся схема подключения выглядит так, как представлено на рисунке 3.6.

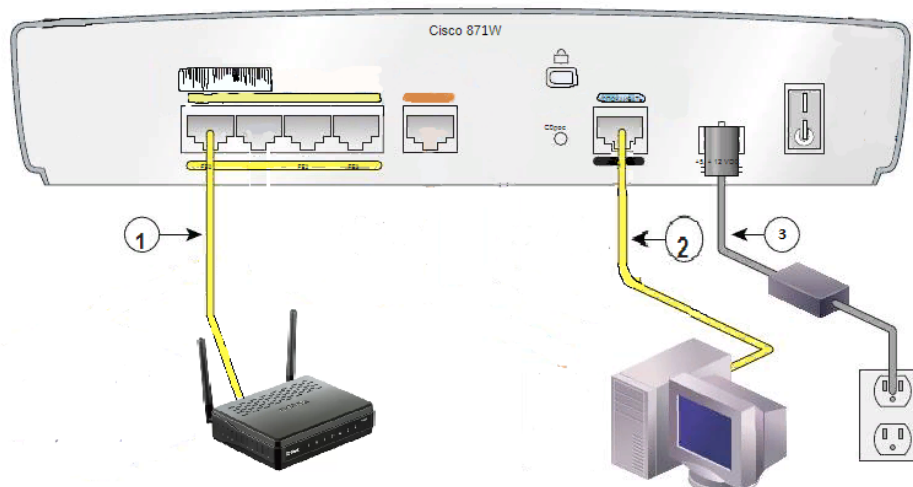


Рисунок 3.6 – Схема подключения к ноутбуку

На рисунке 3.6 представлено:

- под 1 номером – подключение к роутеру;
- под 2 номером – подключение через консольный провод к ноутбуку или компьютеру;
- под 3 номером – шнур электропитания.

Для работы с оборудованием и для его мониторинга рассмотрим технические характеристики Cisco 871 – К9 представлены в таблице 3.1

Таблица 3.1 – Технические характеристики

Характеристика	Описание
Тип устройства	маршрутизатор (router)
Базовая скорость передачи данных	10/100 Мбит/сек
Межсетевой экран (Firewall)	есть
Объем оперативной памяти	128 Мб
Объем флэш-памяти	52 Мб
Поддержка IEEE 802.1q (VLAN)	есть
Количество портов	4
WAN-порт	Ethernet 10/100 Мбит/сек
Поддержка SNMP	есть
Поддержка Telnet	есть
Web-интерфейс	есть

Настройка оборудования Cisco проводилась с помощью программного обеспечения PuTTY. Данная программа позволяет удаленно управлять устройством. При первоначальной настройке оборудования следуют определить какой COM порт назначен этому оборудованию. Это можно посмотреть в диспетчере устройств. После чего при запуске PuTTY выбрать тип соединения Serial и прописать COM порт, указанный в диспетчере устройств. Окно конфигурации представлено на рисунке 3.7.

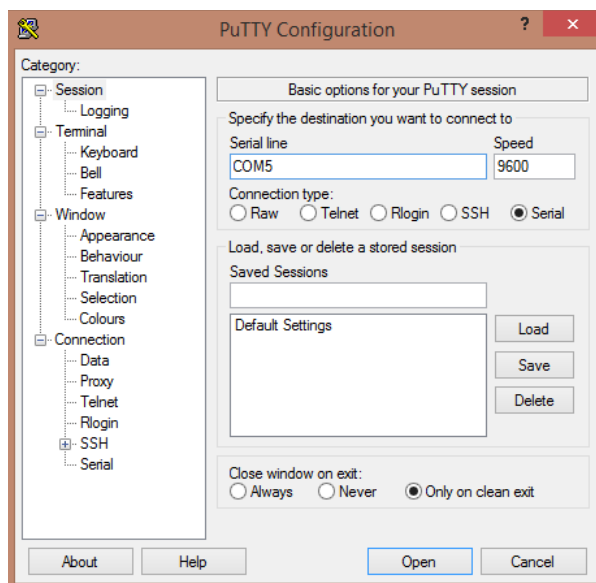


Рисунок 3.7 – Окно конфигурации

На рисунках 3.8 – 3.10 представлена подробная настройка оборудования для последующей работы с ним.

```

--- System Configuration Dialog ---

Would you like to enter the initial configuration dialog? [yes/no]:
% Please answer 'yes' or 'no'.
Would you like to enter the initial configuration dialog? [yes/no]: yes

At any point you may enter a question mark '?' for help.
Use ctrl-c to abort configuration dialog at any prompt.
Default settings are in square brackets '[]'.

Basic management setup configures only enough connectivity
for management of the system, extended setup will ask you
to configure each interface on the system

Would you like to enter basic management setup? [yes/no]: yes
Configuring global parameters:

Enter host name [Router]: test

```

Рисунок 3.8 – Настройка имени хоста

```
Configure SNMP Network Management? [yes]: yes
Community string [public]: all
```

Рисунок 3.9 – Настройка SNMP

```
test(config)#snmp-server location Novosibirsk
test(config)#snmp-server contact veronika@ya.ru
test(config)#exit
```

Рисунок 3.10 – Настройка параметров

Для выбора нужной команды следует войти в привилегированный режим командой enable после чего поставить знак вопроса, и в дальнейшем программа выведет список команд с описанием [13]. Команды, предусмотренные для использования в данном оборудовании представлены на рисунках 3.11-3.12.

```
test#?
Exec commands:
  access-enable      Create a temporary Access-List entry
  access-profile     Apply user-profile to interface
  access-template    Create a temporary Access-List entry
  archive            manage archive files
  auto              Exec level Automation
  beep              Blocks Extensible Exchange Protocol commands
  cd                Change current directory
  clear             Reset functions
  clock             Manage the system clock
  cns               CNS agents
  configure         Enter configuration mode
  connect           Open a terminal connection
  copy              Copy from one file to another
  crypto            Encryption related commands.
  debug             Debugging functions (see also 'undebug')
  delete            Delete a file
  dir               List files on a filesystem
  disable           Turn off privileged commands
  disconnect        Disconnect an existing network connection
  dot11             IEEE 802.11 commands
  dot1x             IEEE 802.1X Exec Commands
  emm               Run a configured Menu System
  enable            Turn on privileged commands
  eou               EAPoUDP
  erase             Erase a filesystem
  event             Event related commands
  exit              Exit from the EXEC
  format            Format a filesystem
  fsck              Fsck a filesystem
  help              Description of the interactive help system
  if-mgr            IF-MGR operations
  isdn              Run an ISDN EXEC command on an ISDN interface
  lock              Lock the terminal
  login             Log in as a particular user
  logout            Exit from the EXEC
  mkdir             Create new directory
  monitor           Monitoring different system events
  more              Display the contents of a file
  mrinfo            Request neighbor and version information from a multicast
```

Рисунок 3.11 – Список существующих команд часть 1

name-connection	Name an existing network connection
no	Disable debugging functions
partition	Partition disk
ping	Send echo messages
ppp	Start IETF Point-to-Point Protocol (PPP)
pwd	Display current working directory
radius	radius exec commands
release	Release a resource
reload	Halt and perform a cold restart
rename	Rename a file
renew	Renew a resource
restart	Restart Connection
resume	Resume an active network connection
rmdir	Remove existing directory
rsh	Execute a remote command
send	Send a message to other tty lines
set	Set system parameter (not config)
setup	Run the SETUP command facility
show	Show running system information
slip	Start Serial-line IP (SLIP)
spec-file	format spec file commands
ssh	Open a secure shell client connection
start-chat	Start a chat-script on a line
systat	Display information about terminal lines
tcquit	Quit Tool Command Language shell
tcldsafe	Tool Command Language shell SAFE mode
tcldsh	Tool Command Language shell
telnet	Open a telnet connection
terminal	Set terminal line parameters
test	Test subsystems, memory, and interfaces
traceroute	Trace route to destination
trm	Trend Registration Module
tunnel	Open a tunnel connection
undebug	Disable debugging functions (see also 'debug')
upgrade	Upgrade commands
verify	Verify a file
vlan	Configure VLAN parameters
vtp	Configure global VTP state
webvpn	WebVPN exec command
where	List active connections
write	Write running configuration to memory, network, or terminal
xconnect	Xconnect EXEC commands

Рисунок 3.12 – Список существующих команд часть 2

После настройки маршрутизатора следует проверить соединение с ним. Для этого в командной строке cmd введена команда ping и IP-адрес устройства, выполнение данной команды представлено на рисунке 3.13.

```

C:\Windows\system32>ping 192.168.0.11

Обмен пакетами с 192.168.0.11 по 32 байтами данных:
Ответ от 192.168.0.11: число байт=32 время=8мс TTL=255
Ответ от 192.168.0.11: число байт=32 время=2мс TTL=255
Ответ от 192.168.0.11: число байт=32 время=20мс TTL=255
Ответ от 192.168.0.11: число байт=32 время=2мс TTL=255

Статистика Ping для 192.168.0.11:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    (0% потерь)
Приблизительное время приема-передачи в мс:
    Минимальное = 2мсек, Максимальное = 20 мсек, Среднее = 8 мсек

```

Рисунок 1.13 – Выполнение команды ping с устройством

Результаты выполнения команды показывают, что узел доступен и

соединение работает.

3.4 Результаты эксплуатации системы контроля доступа к сети Интернет

Для решения поставленной задачи, которая заключается в разработке программного обеспечения для контроля доступа к сети Интернет, при разработке системы была создана база данных, которая сохраняет в себе информацию об оборудовании за которым ведется контроль, сделанные проверки на выявления ошибок и сами ошибки.

Данная система может предназначаться для мониторинга сети, составления выводов и принятия решений по результатам своевременной проверки устройств. При запуске системы происходит опрос устройств, занесенный в БД.

В целях безопасности разработанная информационная система лишена возможности изменять данные об устройстве в БД. Для изменения информации об устройстве, руководитель подразделения должен обратиться к администратору баз данных.

В БД существуют следующие таблицы:

Таблица User1 – предназначена для хранения пользователей системы. В данную таблицу входят такие атрибуты:

- login – хранит в себе логин пользователя и использует тип данных char хранит не более 15 символов;
- password – хранит пароли пользователей и использует тип данных char и хранит не более 15 символов.

Таблица Obogud – данная таблица предназначена для занесения нового оборудования в БД. Таблица имеет следующие атрибуты:

- Ip – сетевой адрес устройства по которому происходит подключение. Тип данных используемый для данного атрибута является char(15);

- Hardware – данный атрибут содержит в себе информацию об устройстве, его модели и определяется типом данных char ограниченного в 100 символов;
- SysNam – хранит в себе системное имя опрашиваемого устройства и определяется типом char ограниченного в 30 символов;
- Contact – хранит в себе информацию о владельце или способ связи с ним и определяется типом данных char в 50 символов;
- Locat – содержит в себе информацию по расположению устройства и определяется типом данных char(50);
- Uptime – содержит в себе информации о времени с последней загрузки системы и использует тип данных char(30);
- Cpu – данный атрибут содержит в себе информацию о нагрузки CPU и использует тип данных char(10);
- PrinB – атрибут предназначен для хранения информации о количестве принятых байт и использует типа данных char в ограничении 100 символов;
- OtpvB - атрибут предназначен для хранения информации о количестве отправленных байт и использует типа данных char в ограничении 100 символов.

Таблица proverka – предназначена для хранения проведенных проверок с устройствами. Данная таблица содержит в себе следующие атрибуты:

- dat – атрибут хранит дату проверки и определяется типом данных datetime;
- ip - сетевой адрес устройства по которому происходит подключение. Тип данных используемый для данного атрибута является char(15);
- locat - содержит в себе информацию по расположению устройства и определяется типом данных char(50);
- PrinB – атрибут предназначен для хранения информации о количестве принятых байт и использует типа данных char в ограничении 100 символов;

- OtpB - атрибут предназначен для хранения информации о количестве отправленных байт и использует типа данных char в ограничении 100 символов;

- User11 – хранит в себе пользователя, находящегося в системе во время проверок устройства. Использует тип данных char(15).

Таблица osh – предназначена для хранения ошибок, найденных в процессе проверки. Таблица содержит в себе следующие атрибуты:

- dat – атрибут хранит дату нахождения ошибки и определяется типом данных datetime;

- ip – сетевой адрес устройства в котором обнаружены неполадки. Использует тип данных char(15);

- Hardware – атрибут содержит в себе данные об устройстве и определяется типом данных char(100);

- Oshibka – атрибут содержит в себе описание найденной ошибки устройства и использует тип данных char в ограничении 100 символов.

3.5 Инструкция пользователя информационной системы SNMP-контроль

При входе в систему «SNMP - контроль» требуется ввести логин и пароль, который есть у каждого инженера – электроника занимающегося контролем оборудования и составления отчетности о состоянии оборудования.

При вводе неправильного логина или пароля появляется окно с соответствующим сообщением.

Диалоговое окно входа в систему представлено на рисунке 3.14.

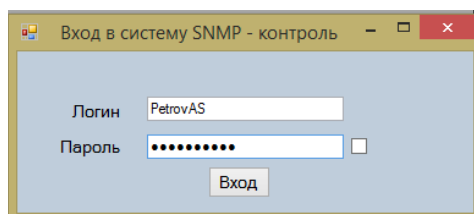


Рисунок 3.14 – Вход в систему

По нажатию элемента управления checkbox – отобразится пароль. Данное действие представлено на рисунке 3.15.

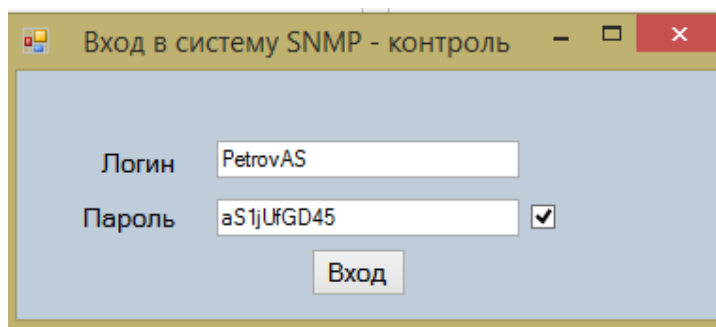


Рисунок 3.15 – Просмотр введенного пароля

По проверке своих данных, пользователь нажимает кнопку «Вход» и в случае если данный пользователь существует в системе и данные введены правильные, откроется главное окно системы, представленное на рисунке 3.16.

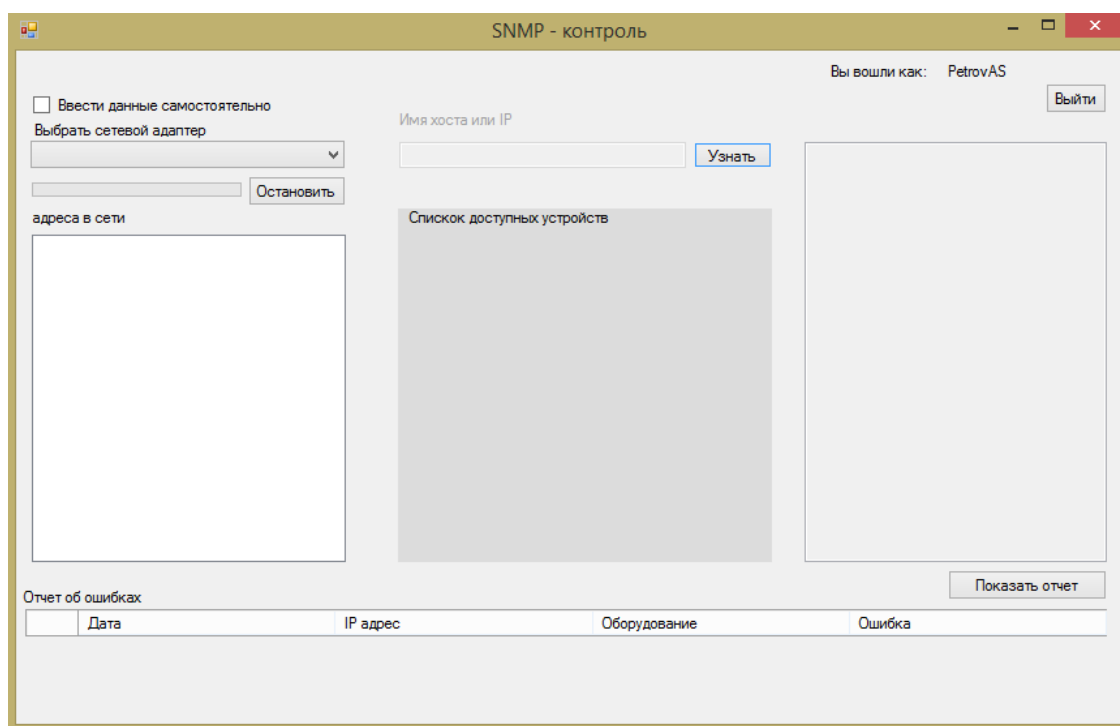


Рисунок 3.16 – Главное окно системы

Так как система запускается первый раз и в базе данных не хранится информации об оборудовании, в главном окне ничего не появляться.

Чтобы добавить оборудование в систему контроля, можно воспользоваться несколькими способами. Первый способ — это поиск устройств с помощью доступных адаптеров. Для поиска следует раскрыть список доступных адаптеров и выбрать нужный, результат этого действия представлен на рисунке 3.17.

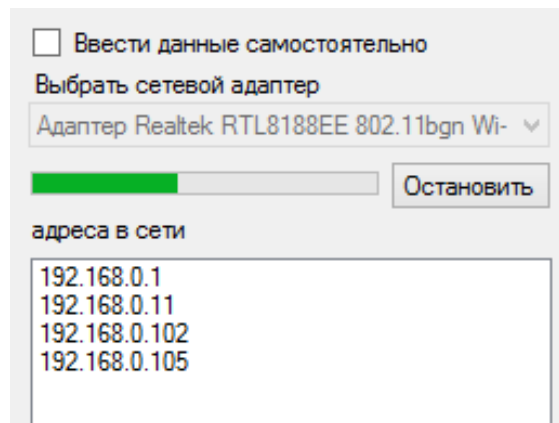


Рисунок 3.17 – Поиск доступных устройств

Для получения информации от устройства следует выбрать его из списка и нажать на кнопку «Узнать». Если устройство поддерживает протокол SNMP и данный протокол включен на этом устройстве, оборудование добавляется в список устройств и подлежит дальнейшему опросу. Успешный процесс добавления устройства представлен на рисунке 3.18.

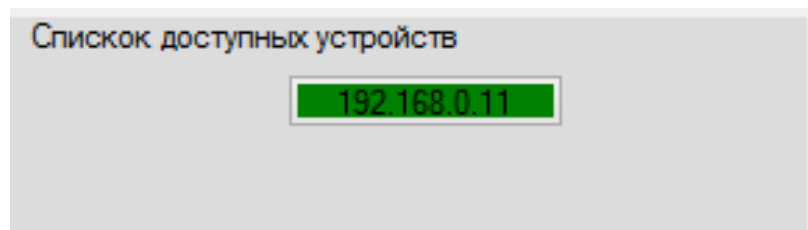


Рисунок 3.18 – Добавление устройства для мониторинга

Помимо описанного способа есть возможность в ручную задавать IP адрес или имя хоста. Для того чтобы писать адрес вручную нужно поставить галочку «Ввести данные самостоятельно», пример данного действия представлен на рисунке 3.19.

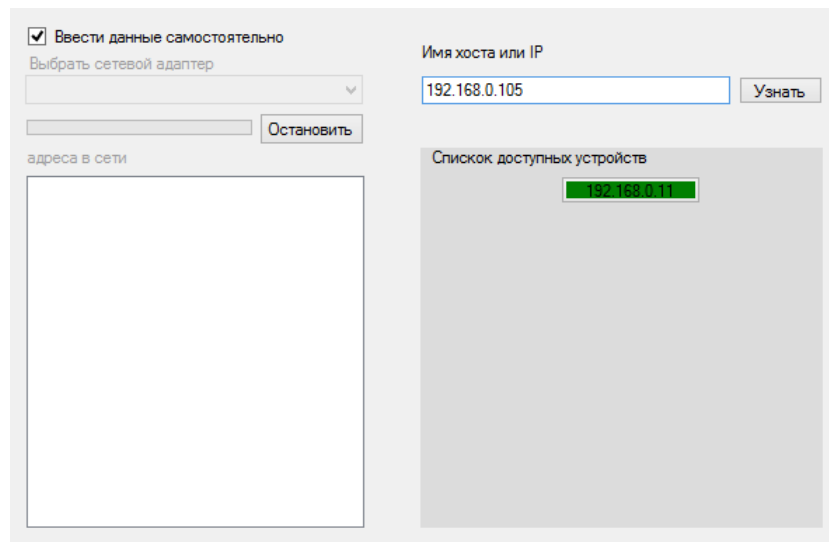


Рисунок 3.19 – Ввод IP адреса вручную

При добавлении устройства в систему, в боковой панели отображаются опрашиваемые значения. Вывод опрашиваемых значений представлен на рисунке 3.20.

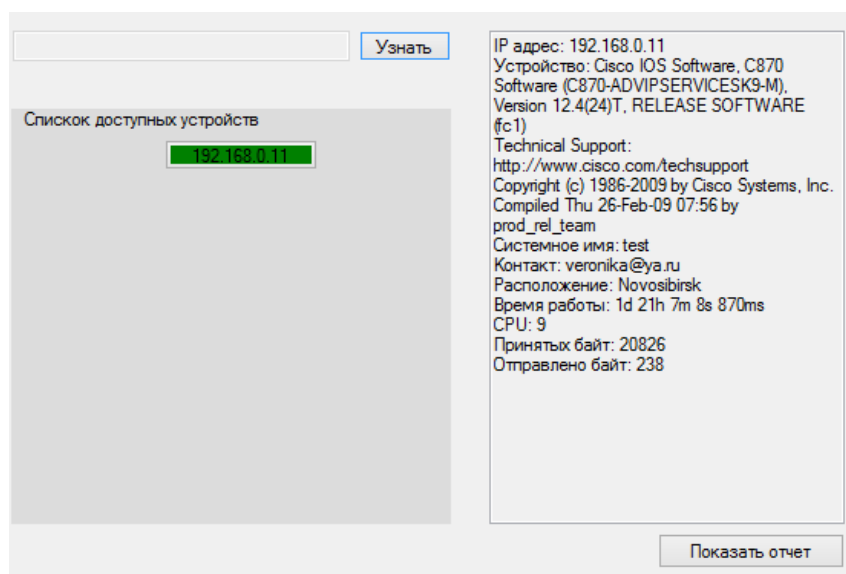


Рисунок 3.20 – Вывод информации об устройстве

Система опрашивает устройства каждую минуту. При опросе устройств, берутся во внимания такие параметры как время с последней загрузки системы и CPU.

Для тестирования было поставлено пороговое значение загрузки CPU в размере 10%, система выдает звуковой сигнал, изменяет состояния на красный свет и в графе «Отчет об ошибках» выводятся соответствующая информация, представленная на рисунке 3.21.

Отчет об ошибках		Поиск устройств		
	Дата	IP адрес	Оборудование	Ошибка
▶	11.06.2018 21:13:02	192.168.0.11	Cisco IOS Software, C870 Softwar...	Следует обратить внимание на трафик! Устройство сильно нагружено.

Рисунок 3.21 – Отчет об ошибках

Еще одна из возможностей это выгрузка отчета в Excel. Данный представляются в таблицу после чего можно осуществить выгрузку данных. Выгрузка из БД данных о проверке представлено на рисунке 3.22.

Выгрузка отчета о проверках									
Файл									
В целях экономии времени введите дату начала и дату окончания формирования отчета									
	27.05.2018 00:00	-	28.05.2018 00:00	OK					
	Дата	Ip-адрес	Расположение	Время работы	CPU	Принято байт	Отправлено байт	Контроль	
▶	27.05.2018 ...	192.168.0.11	Novosibirsk ...	0d 0h 56m 58s 9...	0	401	268	PetrovAS	
	27.05.2018 ...	192.168.0.11	Novosibirsk ...	0d 0h 57m 31s 5...	9	403	270	PetrovAS	
	27.05.2018 ...	192.168.0.11	Novosibirsk ...	0d 0h 57m 41s 9...	0	404	271	PetrovAS	
	27.05.2018 ...	192.168.0.11	Novosibirsk ...	0d 0h 56m 58s 9...	0	401	268	PetrovAS	
	27.05.2018 ...	192.168.0.11	Novosibirsk ...	0d 0h 57m 31s 5...	9	403	270	PetrovAS	
	27.05.2018 ...	192.168.0.11	Novosibirsk ...	0d 0h 57m 41s 9...	0	404	271	PetrovAS	

Рисунок 3.22 – Выгрузка результатов проверок из БД

Для того чтобы сохранить результат следует нажать на «Файл» и выбрать «Сохранить». На рисунке 3.23 представлено диалоговое окно выбора места сохранения и название файла.

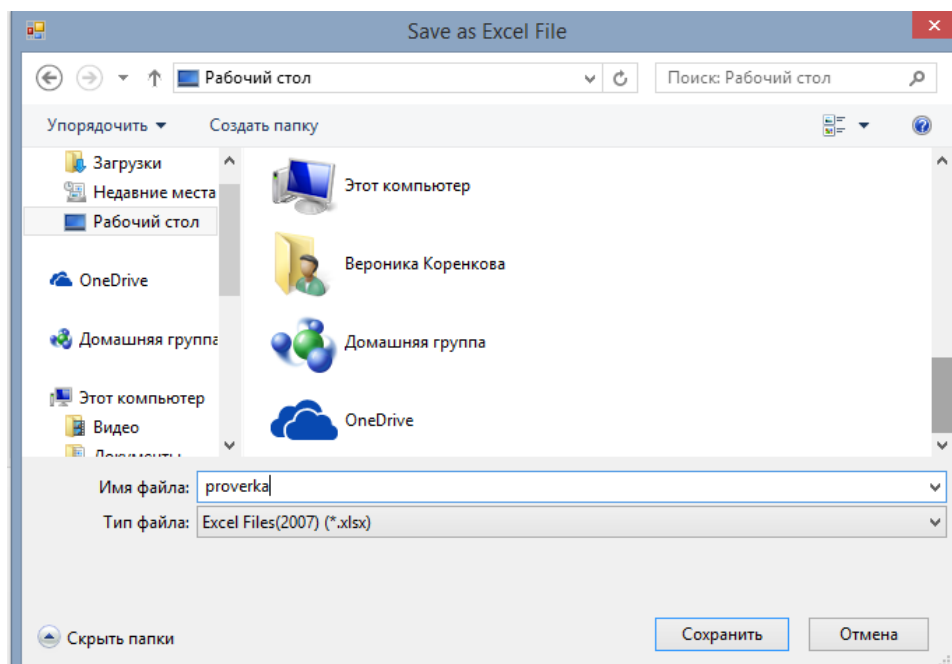


Рисунок 3.23 – Выбор места сохранения

Результат сохранения в Excel файл представлен на рисунок 3.24.

Дата	IP адрес	Расположение	Время работы	CPU	Принято байт	Отправлено байт	Контроллер
27.05.2018	192.168.0.11	Novosibirsk	0d 0h 56m 58s 90ms	0	401	268	PetrovAS
27.05.2018	192.168.0.11	Novosibirsk	0d 0h 57m 31s 590ms	9	403	270	PetrovAS
27.05.2018	192.168.0.11	Novosibirsk	0d 0h 57m 41s 960ms	0	404	271	PetrovAS
27.05.2018	192.168.0.11	Novosibirsk	0d 0h 56m 58s 90ms	0	401	268	PetrovAS
27.05.2018	192.168.0.11	Novosibirsk	0d 0h 57m 31s 590ms	9	403	270	PetrovAS
27.05.2018	192.168.0.11	Novosibirsk	0d 0h 57m 41s 960ms	0	404	271	PetrovAS

Рисунок 3.24 – Результаты сохранения в файл

3.6 Выводы по третьему разделу

На основании рассмотренных протоколов управления сетью, анализа преимуществ и недостатков протоколов, сделал выбор в пользу протокола SNMP. Имеющееся оборудование, предназначенное для тестирования поддерживается данным протоколом что позволяет осуществлять контроль за оборудованием.

В данном разделе была рассмотрена библиотека SnmpSharpNet которая была подключена в проект для работы с протоколом SNMP. Данная библиотека позволяет передать oid-ы оборудованию и получить ответ от оборудования по каждому параметру.

При разработке ПО была создана БД которая хранит в себе информацию об оборудовании, произведенных системой проверок и изменения состояния оборудования в критическую сторону. Данная разработанная система позволяет оперативно отслеживать состояние и передавать ее пользователю, что позволяет снизить риск выхода оборудования из строя. Система может наполниться такими функциями как автоматическое построение схемы сети.

4 Техничко–экономическое обоснование разработки и внедрения системы контроля доступа к сети Интернет

4.1 Определение трудоемкости, длительности разработки и размеров заработной платы

Разрабатываемая система «SNMP – контроль» предназначена для мониторинга устройств в сети, с целью получения данных как о состоянии оборудования в целом, так и для контроля доступа к Интернет. Программное обеспечение позволяет сократить время и трудоёмкость процесса путем построения иерархии критериев с последующей оценкой возможных альтернатив по каждому из выбранных критериев.

Найденные в результате работы программного обеспечения решения будут математически обоснованными, что может гарантировать получение наиболее оптимального результата.

Целью разработки программного обеспечения является контроль доступа к сети Интернет, сокращение рабочего времени на проверки работоспособности оборудования и снижение затрат компании на выезд бригады или одного электромеханика к месту расположения оборудования, и как следствие рост прибыли предприятия.

Основная задача программного обеспечения – обеспечить работнику актуальную информацию о состоянии оборудования с целью своевременного устранения неполадок.

Расчет экономической эффективности разработки и внедрения программного обеспечения проводится на предварительном этапе, до начала работ по анализу предметной области, проектированию и разработки программного обеспечения. Следовательно, приведённый расчет является примерным и отображает потенциальный экономический эффект внедрения программного обеспечения [15].

Экономия обеспечивается за счет снижения затрат рабочего времени на проверку всех оборудования в сети, а также снижения затрат на выезд работнику к месту расположения оборудования и составление отчетных

форм. Проект разработки и внедрения программного обеспечения состоит из следующих этапов:

- определение и анализ требований к проектированной системе, в этот этап входит под этап согласования и утверждения технического задания;
- проектирование основных составляющих программного обеспечения: база данных, интерфейса, бизнес-логики;
- выбор платформы и реализация программного обеспечения;
- внедрение и адаптация программного обеспечения в подразделения ОАО «РЖД».

Наиболее сложный и трудоемкий этап – это внедрение и адаптация программного обеспечения. Он в свою очередь состоит из этапов: доработка типового программного обеспечения, поставляемого разработчиком, в соответствии со спецификой деятельности каждого подразделения предприятия; тестирование программного обеспечения; обучение пользователей [15].

В таблице 4.1 представлен расчет трудоемкости, длительности разработки по этапам и размер заработной платы специалистов, участвующих в реализации проекте.

Таблица 4.1 - Определение трудоемкости, длительности разработки и размеров зарплаты

Наименование этапа	Исполнители	Часовая ставка, рублей	Время работы, часов	Фонд заработной платы, рублей
1. Определение и анализ требований к проектированной системе	Руководитель проекта	350	104	36400
	Инженер – электроник	105	72	7560
	Программист	300	168	50400

Окончание таблицы 4.1

Наименование этапа	Исполнители	Часовая ставка, рублей	Время работы, часов	Фонд заработной платы
--------------------	-------------	------------------------	---------------------	-----------------------

				платы, рублей
2. Проектирование основных составляющих программного обеспечения	Архитектор информационных систем	270	220	59400
	Программист	300	240	72000
3. Выбор платформы и реализация программного обеспечения	Архитектор информационных систем	270	220	59400
	Архитектор баз данных	260	280	72800
	Дизайнер	280	320	89600
	Программист	300	400	120000
4. Внедрение и адаптация программного обеспечения	Руководитель проекта	350	80	28000
	Программист	300	60	18000
	Технолог-тестировщик	280	160	44800
	Инженер - электроник	105	160	16800
ИТОГО:			2484	675 160

4.2 Определение себестоимости работ по разработки и внедрению программного обеспечения

В себестоимость работ по разработки и внедрению программного обеспечения включаются следующие затраты:

- заработная плата;
- социальные отчисления на заработную плату;
- производственные расходы;
- накладные расходы;
- налог на добавленную стоимость.

Размер заработной платы в соответствии с таблицей 4.1 определен и составляет 675160 руб.

Социальные отчисления на медицинское и пенсионное страхование составляет 30,2 % от заработной платы. Таким образом, социальные отчисления рассчитываются по формуле 4.1.

$$C_{отч} = \frac{C_{зп} * C_{пр}}{100} = \frac{(675160,00 * 30,2)}{100} = 203898,32 \text{ рублей,} \quad (4.1)$$

где $C_{отч}$ – размер социальных отчислений, руб.;

$C_{зп}$ – размер заработной платы, руб.;

$C_{пр}$ – количество процентов на социальные отчисления, %.

Все этапы реализации проекта необходимо выполнять с использованием компьютерного оборудования. Для реализации проекта в общей сложности необходимо 2 484 часов машинного времени. Потребляемая электрическая мощность одного машинного места составляет 0,4 кВт. Стоимость электроэнергии составляет 2,49 руб. за 1 кВт. Таким образом, стоимость электроэнергии на реализацию проекта рассчитывается как на формуле 4.2.

$$C_{э} = C_{ч} * C_{эл} * C_{м} = 2484 * 2,49 * 0,4 = 2474,06 \text{ рублей,} \quad (4.2)$$

где $C_{э}$ – стоимость электроэнергии на реализацию проекта, руб.;

$C_{ч}$ – общее количество часов машинного времени, ч.;

$C_{эл}$ – стоимость электроэнергии, руб.;

$C_{м}$ – потребляемая электрическая мощность одного машинного места, кВт.

На первом и четвертом этапе реализации проекта необходима поддержка оперативной мобильной связи и услуг курьерской почты. Для этих целей проектом запланированы траты в размере 1540 руб. на услуги связи и 1600,00 руб. на услуги курьерской почты. Таким образом, прочие прямые расходы, связанные с реализацией проекта рассчитывается по формуле 4.3.

$$C_{пр} = C_{ср} * C_{св} * C_{п} = 2474,06 + 1540,00 + 1600,00 = 5614,00 \text{ рублей,} \quad (4.3)$$

где $C_{пр}$ – размер прочих расходов, руб.;

$C_{ср}$ – стоимость электроэнергии на реализацию проекта рассчитанной по формуле 4.2, руб.;

$C_{св}$ – траты на услуги связи, руб.;

$C_{п}$ – траты на курьера, руб.

При реализации проекта выделяют накладные расходы в размере 10 % от стоимости реализации проекта без НДС. Они составляют 1091911,60 руб.

Кроме этого, при реализации проекта выделяют рентабельность в размере 7 % от прямых затрат. Рентабельность связана с дополнительными затратами на выплату отпускных пособий специалистам за время их работы над проектом. В таблице 4.2 представлен общий расчет себестоимости разработки и внедрения программного обеспечения.

Таблица 4.2 – Расчет себестоимости разработки и внедрения программного обеспечения

Статья затрат	Сумма затрат, рублей	Удельный вес, %
1. Заработная плата	675160,00	52,40
2. Начисления на заработную плату (30,2 %)	203898,32	15,83
3. Производственные расходы (5 %)	33758,00	2,62
4. Прочие прямые расходы	5614,00	0,44
5. Итого прямых затрат	918430,00	-
6. Накладные расходы (10 % ст. 8)	109191,16	8,47
7. Рентабельность (7 % ст. 5)	64290,12	4,99
8. Стоимость реализации проекта без НДС	1091911,60	-
9. НДС (18 %)	196544,09	15,25
10. Общая стоимость реализации	1288455,69	100,00

4.3 Расчет стоимости дополнительного программного обеспечения и инфраструктуры для внедрения программного обеспечения

Программное обеспечение функционирует на базе сервера под управлением операционной системой Microsoft Windows Server. В качестве системы управления базами данных используется Microsoft SQL Server.

Кроме дополнительного программного обеспечения необходимо подключение компьютеров к локальной сети. В настоящее время ОАО «РЖД» имеет все вышеописанные программные и технические составляющие для реализации проекта. Поэтому дополнительные затраты составляют 0 руб. Общая стоимость реализации проекта равна сумме стоимости внедрения программного обеспечения и единовременных затрат в сфере его использования. Единовременные затраты в сфере использования в данном случае складываются из стоимости приобретения программного обеспечения и её транспортировки [15]. При реализации данного проекта программное обеспечение, техническая, пользовательская и другая документация будут передаваться в электронном виде. Поэтому транспортные расходы составляют 0 руб.

4.4 Расчет общей стоимости проекта

Общая стоимость проекта состоит из трех компонент и вычисляется по формуле (4.1).

$$C_{\text{общ}} = C_{\text{рв}} + C_{\text{доп}} + C_{\text{тр}}, \quad (4.4)$$

где $C_{\text{общ}}$ – общая стоимость проекта, руб.;

$C_{\text{рв}}$ – стоимость разработки и внедрения программного обеспечения, руб.;

$C_{\text{доп}}$ – затраты на дополнительное программное обеспечения и развитие информационной инфраструктуры, руб.;

$C_{\text{тр}}$ – транспортные расходы, руб.

В итоге общая стоимость проекта рассчитывается по формуле 4.5.

$$1288455,69 + 0 + 0 = 1288455,69 \text{ рублей}, \quad (4.5)$$

4.5 Оценка экономической эффективности проекта

Выполнить оценку экономической эффективности внедрения программного обеспечения заранее достаточно сложно, так как эффект от внедрения информационной системы будет ощущаться для всего предприятия в целом. Проведем оценку экономической эффективности с использованием двух временных критериев: время, затраченное на проверку оборудования и время, затраченное на анализ и составление отчетных форм о состоянии оборудования в журнал. Результаты контроля необходимо заносить в журналы ежедневно. На это тратится в среднем 15 % рабочего времени при средней заработной плате инженера - электроника в размере 25000 рублей. Следовательно, затраты в денежной форме на регистрацию результатов контроля ежемесячно составляют по формуле 4.6.

$$C_3 = \frac{C_{сзп} * C_{пр}}{100} = \frac{25000 * 15}{100} = 3750 \text{ рублей,} \quad (4.6)$$

где C_3 – ежемесячные затраты на результаты контроля в бумажной форме, руб.;

$C_{сзп}$ – средняя заработная плата инженера-электроника, руб.;

$C_{пр}$ – процент затрат времени на внесения записи в журнал, %.

Использование программного обеспечения позволяет сократить этот показатель до 5 %.

Следовательно, затраты в денежной форме на регистрацию результатов контроля ежемесячно будут составлять по формуле 4.7.

$$C_{зп} = \frac{C_{сзп} * C_{пи}}{100} = \frac{25000 * 5}{100} = 1250 \text{ рублей,} \quad (4.7)$$

где $C_{зп}$ – затраты на регистрацию результатов контроля с помощью ПО, руб.;

$C_{сзп}$ – средняя заработная плата инженера-электроника, руб.;

$C_{\text{пи}}$ – процент затрат времени на внесения записи в журнал с помощью программного обеспечения, %.

Составление и анализ результатов контроля оборудования проводит инженер - электроник. В среднем эта процедура занимает более 10 % рабочего времени при средней заработной плате инженера -электроника в размере 25000 рублей. Следовательно, затраты в денежной форме на проведение анализа и составление отчетных форм составляют по формуле 4.8.

$$C_{\text{па}} = \frac{C_{\text{сзп}} * C_{\text{ар}}}{100} = \frac{25000 * 10}{100} = 2500 \text{ рублей}, \quad (4.8)$$

где $C_{\text{па}}$ – затраты на проведение анализа и составление отчетных форм, руб.;

$C_{\text{сзп}}$ – средняя заработная плата инженера-электроника, руб.;

$C_{\text{ар}}$ – процент затрат времени на составление и анализ результатов контроля, %.

Использование программного обеспечения позволяет сократить этот показатель до 0 %. Так как анализ и составление отчетных форм будут проводить программно. Следовательно, затраты в денежной форме на проведение анализа и составление отчетных форм будут составлять 0 руб. Новосибирский региональный центр связи имеет 28 ремонтно-восстановительных бригад. Вычислим затраты по первому критерию. В целом по компании ежемесячно они составляют по формуле 4.9.

$$C_{\text{пк}} = C_{\text{бр}} * C_{\text{кр}} = 28 * 3750 = 105000 \text{ рублей}, \quad (4.9)$$

где $C_{\text{пк}}$ – затраты по первому критерию, руб.;

$C_{\text{бр}}$ – количество бригад в Новосибирском РЦС;

$C_{кр}$ – затраты в денежной форме на регистрацию результатов контроля ежемесячно определяющееся по формуле 4.6.

Соответственно затраты на проведение анализа и составление отчетных форм инженерами в целом по ремонтно–восстановительным бригадам ежемесячно составляют по формуле 4.10.

$$C_{паб} = C_{бр} * C_{от} = 28 * 2500 = 70000 \text{ рублей,} \quad (4.10)$$

где $C_{паб}$ – затраты на анализ и составление отчетных форм в ремонтно-восстановительных бригадах, руб.;

$C_{бр}$ – количество бригад в Новосибирском РЦС;

$C_{от}$ – затраты в денежной форме на проведение анализа и составление отчетных форм, определяющееся по формуле 4.8.

Учитывая положительный эффект при внедрении программного обеспечения, связанный с сокращением времени на регистрацию результатов и составление отчетов вычислим ежемесячную экономию денежных средств представленной в формуле 4.11.

$$C_{эк} = (C_{пк} + C_{паб}) - (C_{бр} * C_{зе} + C_{бр} * C_{ад}) \quad (4.11)$$

где $C_{пк}$ - затраты по первому критерию, руб.;

$C_{паб}$ - затраты на анализ и составление отчетных форм в ремонтно-восстановительных бригадах, руб.;

$C_{бр}$ – количество бригад в Новосибирском РЦС;

$C_{зе}$ – затраты в денежной форме на регистрацию результатов контроля ежемесячно определяющиеся по формуле 4.7;

$C_{ад}$ – затраты в денежной форме на проведение анализа и составление отчетных форм с помощью программного обеспечения.

Расчет представлен в формуле 4.12.

$$C_{эк} = (105000 + 70000) - (28 \cdot 1250 + 28 \cdot 0) = 140000 \text{ рублей} , \quad (4.12)$$

По полученным результатам строится график окупаемости от внедрения программного обеспечения представленный на рисунке 4.1.

По графику видно, что уже на 12-й месяц после реализации проекта появляется положительный экономический эффект.

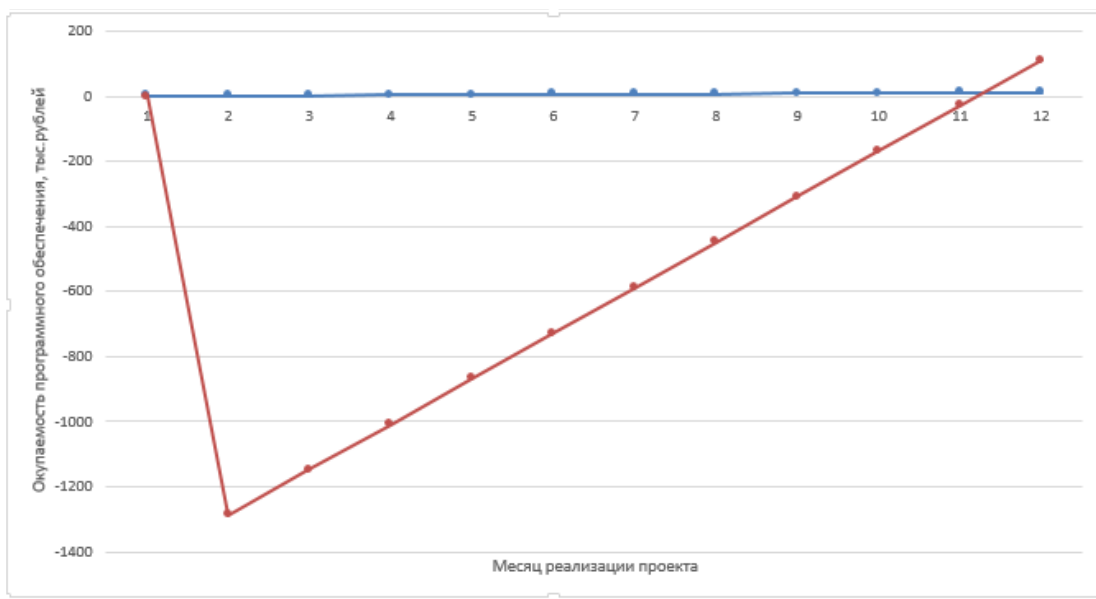


Рисунок 4.1 – График окупаемости внедрения программного обеспечения

4.6 Выводы по четвертому разделу

В данном разделе был проведен расчет технико-экономического обоснования внедрения системы контроля доступа к сети Интернет.

Результат показал, что внедрение системы контроля доступа позволит компании экономить на таких критериях как: время, затраченное на проверку оборудования и время, затраченное на анализ и составление отчетных форм о состоянии оборудования в журнал.

Экономический эффект появится на двенадцатый месяц использования данного программного обеспечения.

ЗАКЛЮЧЕНИЕ

В результате выполнения выпускной квалификационной работы проанализирована структура организации и бизнес-процессы инженера-электроника в Новосибирском региональном центре связи с целью разработки программного обеспечения автоматизации процессов по работе с оборудованием.

В рамках выполнения выпускной квалификационной работы проведен анализ АСОЗ для обеспечения доступа к ресурсам пользователей железнодорожных станций к сети Интернет. Рассмотрены функциональные возможности системы и бизнес-процессы пользователей.

Проведен анализ протоколов управления сетью. На основе анализа сделан выбор протокола для использования его при разработке программного обеспечения.

Заключающей задачей выполнения дипломной работы является разработка системы контроля доступа к сети Интернет. Система обеспечивает непрерывный контроль за устройствами сети, оперативно оповещает пользователя о неполадках на оборудовании и готовит отчетность о состоянии оборудования за конкретный период. Весь функционал системы позволяет быстро реагировать на инциденты для устранения проблем без допущения распространения аварий до конечного пользователя.

По результатам выполнения выпускной квалификационной работы составлен акт внедрения результатов в Центре оперативно-технологической связи, представленный в приложении А.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

- 1 Об утверждении программы «Цифровая экономика Российской Федерации» [Текст]: распоряжение правительства РФ от 28.07.2017 N 1632-р.
- 2 Центральная станция связи: [Электронный ресурс]. URL: http://css-rzd.ru/pls/portal30/lais_css.dyn_index.show (дата обращения 15.04.2018)
- 3 Охрана труда и промышленная безопасность: [Электронный ресурс]. URL: <http://prom-nadzor.ru/content/dolzhnostnaya-instrukciya-inzhenera-elektronika> (дата обращения 19.04.2018)
- 4 Об утверждении Типового положения о дорожной дирекции связи железных дорог - филиалов ОАО "РЖД" [Текст]: распоряжение от 3 апреля 2006 года N 576р //ОАО «РЖД». -2006.
- 5 Сетевые программы для системных администраторов: [Электронный ресурс]. URL: <https://www.10-strike.ru/> (дата обращения 15.04.2018)
- 6 Pandora Fms Enterprise: [Электронный ресурс]. URL: <https://pandorafms.com/> (дата обращения 19.04.2018)
- 7 Zenoss Own IT: [Электронный ресурс]. URL: <https://www.zenoss.com/> (дата обращения 19.04.2018).
- 8 Фленов М.Е. Linux глазами хакера [Текст] / М.Е. Фленов. – 4-е изд., перераб. и доп. – СПб.: БВХ-Петербург, 2016. – 432 с.
- 9 Руководство пользователя: [Электронный ресурс]. URL: http://portal-asoz.rzd.ru/asoz/help/asoz_help.html (дата обращения 20.04.2018)
- 10 Бирюков А.А. Информационная безопасность: защита и нападение [Текст] / А.А. Бирюков. – Москва: ДМК Пресс, 2013. - 474 с.
- 11 Троелсен Э. Язык программирования C# 6.0 и платформа .NET 4.6 [Текст] / Э.Троелсен, Ф. Джепикс; пер. с англ. Ю. Артеменко. – 7-е изд. – Москва: Вильямс, 2016. – 1440 с.
- 12 Рафалович В. Data mining или интеллектуальный анализ данных для занятых. Практический курс [Текст] / В. Рафалович. – Москва: СмартБук, 2014. – 96 с.

13 Олифер В., Олифер Н. Компьютерные сети. Принципы, технологии, протоколы [Текст] / В. Олифер, Н. Олифер. – 5 изд. – СПб.: Питер, 2016. – 992 с.

14 Cisco [Электронный ресурс]. URL: <https://www.cisco.com/> (дата обращения 14.05.2018)

15 Миньков С.Л. Техничко-экономическое обоснование выполнения проекта: методическое пособие [Текст] / С.Л. Миньков. – Томск: ТУСУР, 2014. – 30 с.

Приложение А

Акт внедрения результатов работы

Утверждаю

Руководитель Центра оперативно-технологической связи



Е.Г. Каверин

2018 г.

АКТ

внедрения результатов выпускной квалификационной работы

Коренковой Вероники Александровны

Настоящий акт составлен о том, что результаты выпускной квалификационной работы «Моделирование процесса предоставления услуги доступа к сети Интернет на железнодорожных станциях. Автоматизация контроля за состоянием услуги доступа к Интернет» внедрены в технологических процесс Центра оперативно-технологической связи – РЦС - 2. Достигнутые в рамках работы результаты позволили повысить качества оказываемых услуг, сократить время на реагирование по заявкам абонентов и пользователей и увеличить производительность труда технологов. По результатам обсуждения принято решение о целесообразности дальнейшего совершенствования, разработанного в рамках выпускной квалификационной работы программного обеспечения.