СОДЕРЖАНИЕ

Изм.

Лист

№ докум.

Подп.

Дата

Лист

1

КП.09.02.03.06ПЗ

Разраб.

Имгрунт Г. И.

Пров.

Попов И. Д.

Н. контр.

Утв.

Проектирование информационной системы интернет-магазина Пояснительная записка

Лит.

Листов

ФСПО ГУАП

[ВВЕДЕНИЕ 2](#_Toc166686651)

[1 Теоретическая часть 3](#_Toc166686652)

[1.1 Описание предметной области 3](#_Toc166686653)

[1.2 Принципы построения компьютерных сетей 3](#_Toc166686654)

[1.3 Постановка задачи 5](#_Toc166686655)

[ЗАКЛЮЧЕНИЕ 6](#_Toc166686656)

[2 Практическая часть 6](#_Toc166686657)

[2.1 Выбор сетевого оборудования и его обоснование 8](#_Toc166686658)

[2.2 Базовая настройка сети 11](#_Toc166686659)

[2.2.1 Настройка статических IP-адресов 11](#_Toc166686660)

[2.2.2 GRE-туннели 12](#_Toc166686661)

[2.2.3 Настройка серверов 14](#_Toc166686662)

[2.3 Настройка маршрутизации 15](#_Toc166686663)

[2.4 Настройка сервисов 18](#_Toc166686664)

[2.4.1 DNS, DHCP, Netwatch, VRRP 18](#_Toc166686665)

[2.4.2 Настройка NAT и HAproxy 22](#_Toc166686666)

[2.5 Тестирование работоспособности сети 23](#_Toc166686667)

[ЗАКЛЮЧЕНИЕ 29](#_Toc166686668)

[СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ 30](#_Toc166686669)

[ПРИЛОЖЕНИЕ А 31](#_Toc166686670)

[ПРИЛОЖЕНИЕ Б 31](#_Toc166686671)

[ПРИЛОЖЕНИЕ В 31](#_Toc166686672)

[ПРИЛОЖЕНИЕ Г 31](#_Toc166686673)

## **ВВЕДЕНИЕ**

Системные и сетевые администраторы играют важную роль в обеспечении надежности и безопасности сети. Системные администраторы отвечают за установку и обновление программного обеспечения, а также за мониторинг и оптимизацию работы серверов. Сетевые администраторы администрируют сетевое оборудование, настраивают маршрутизацию трафика, обеспечивают безопасность интернет-соединения.

Благодаря работе системных и сетевых администраторов интернет-магазин может эффективно функционировать, привлекать больше клиентов и увеличивать прибыль.

Основная цель данного проекта, настройка сетевой и системной инфраструктуры интернет-магазина. По средством выполнения следующих задач:

* Построение схем сети
* Выбор сетевого и системного оборудования
* Выбор и настройка сетевых проколов
* Управления сервисами

Отчет начинается с введения, где кратко изложены основные цели и задачи работы. Далее идет построение схемы сети, где приводится графическое изображение структуры сети и IP-план. Затем идет выбор оборудования, где описывается используемое для сети оборудование и его особенности.

После определения нужного оборудования в отчете указана организация сетевого администрирования, где описывается структура управления и настройки сети. После этого в отчете находится настройка серверов и сервисов.

Отчет завершается списком использованных источников, которые были использованы при работе над курсовым проектом.

## **1 Теоретическая часть**

### **1.1 Описание предметной области**

В интернет-магазине есть главный офис и два филиала. Для функционирования интернет-магазина требуется веб-сервер и база данных, которая будет содержать информацию о товаре, продаваемого в магазине. Серверы расположены в главном офисе, также в главном офисе находиться персональный компьютер администратора для мониторинга и настройки оборудований. Филиалы интернет-магазина представляют собой склад или пункт выдачи, в которых есть сотрудник, который выдает товар курьерам или покупателям. Поэтому все, что нужно в филиалах это компьютер, который должен иметь доступ к главному офису. Запросы с филиалов по-умолчанию пересылаются на внешний маршрутизатор главного офиса.

Для отказоустойчивой работы сети, было принято решение настройки двух внешних маршрутизаторов в главном офисе, которые подключены к разному провайдеру. Это решает проблему отключение устройств со стороны локальной сети и со стороны провайдера. В филиалах один внешний маршрутизатор, но доступно два выхода в глобальную сеть. В филиал не будут обращаться клиенты и там не находится сервер, поэтому поломка не навредит работе магазина. Изменения количества товара можно будет записать на локальном устройстве, и при решении проблем с сетью данные запишутся на сервер.

### **1.2 Принципы построения компьютерных сетей**

В курсовой работе присутствуют провайдерскии сети, которые находятся в автономных системах. Для внешних маршрутизаторов интернет-магазина были выданы статические адреса.

На Рисунке 1 изображена приблизительная схема интернет-магазина, построенная в виртуальной среде GNS3.

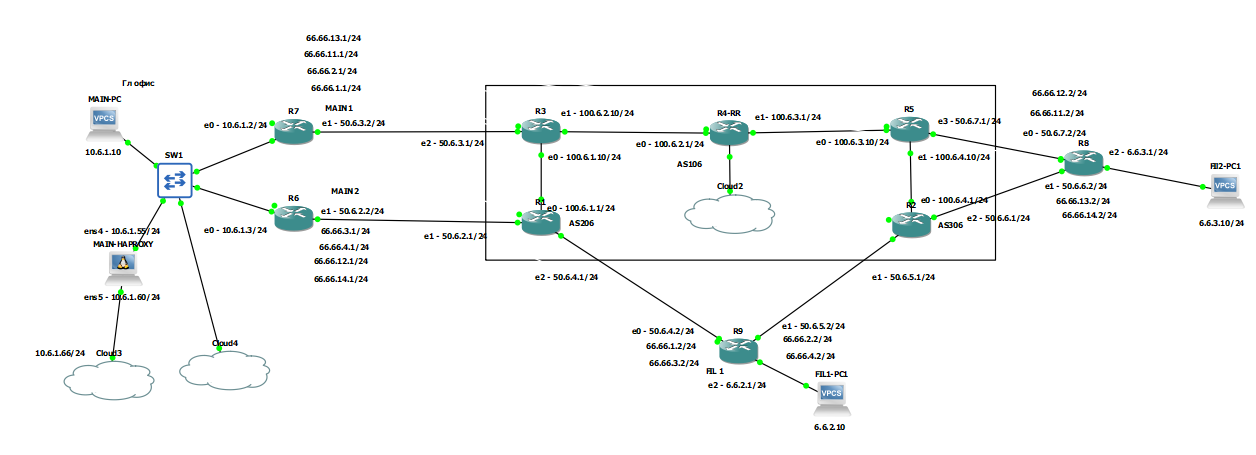


Рисунок 1 – Примерная схема сети

В таблице 1 описаны пользователи сети и их роли.

Таблица 1 - Пользователи



Весь трафик в сети будет проходить через главный офис, поэтому в сети должны быть настроены сетевые туннели и маршруты по-умолчанию.

В филиалах и главном офисе динамически выдаются адреса для устройств.

Для обеспечения отказоустойчивости на филиалах два выхода в интернет и будет настроена система динамического переключения маршрутов для автономной работы сети. В главном офисе будет создан виртуальный канал для автоматического переключения активных маршрутизаторов, и обеспечения отказоустойчивости.

Доступ к базе данных разрешен только для веб сервера и компьютера администратора, для недоступности к информации о закупках и продажах обычных пользователей.

Чтобы веб сервер мог бесперебойно работать в главном офисе будет настроена система перенаправления запросов на два сервера. Поэтому при отключении одного сервера, сайт магазина будет доступен.

Также для доступа локальных устройств в глобальную сеть в главном офисе на внешних маршрутизаторах будет настроена динамическая замена адресов. А для доступности веб серверов из глобальной сети нужно настроить проброс портов.

Для доступности сайтов из глобальной сети будет настроен сервис обработки доменных имен.

### **1.3 Постановка задачи**

Протоколы и сервисы, необходимые для настройки сети интернет-магазина, будут описаны далее.

В первую очередь необходимо установить соединение между маршрутизаторами и всеми сетевыми устройствами с использованием витой пары.

На внешних маршрутизаторах получить IP-адреса от провайдера.

Программная утилита WinBOX позволяет настроить туннелирование между филиалами и центральным офисом с применением протокола GRE для VPN.

Для эффективной маршрутизации между центральным офисом и филиалами предпочтительно использовать динамический протокол маршрутизации OSPF.

Для динамического распределения IP-адресов в локальных сетях рекомендуется использовать DHCP.

Для обеспечения доступности доменных имен из сети часто применяется DNS.

Для замены IP-адресов и преобразования рекомендуется использовать NAT.

Для обеспечения отказоустойчивости веб-серверов будет настроена система HAproxy.

Для ограничения доступа к базе данных рекомендуется использовать брандмауэр (Firewall).

## **ЗАКЛЮЧЕНИЕ**

В результате анализа требований к функционированию интернет-магазина и его филиалов, были выделены ключевые компоненты инфраструктуры: веб-сервер, база данных, компьютеры персонала, внешние маршрутизаторы и локальное хранилище данных. Настройка двух внешних маршрутизаторов в главном офисе и одного в филиалах позволит обеспечить отказоустойчивость сети и минимизировать риски простоя.

Для оптимальной работы интернет-магазина рекомендуется регулярно проводить обслуживание и мониторинг сетевого оборудования, регулярно обновлять программное обеспечение и резервировать данные для предотвращения потери информации. Также важно обеспечить безопасность информации, устанавливая межсетевые экраны и шифрование данных. Обучение персонала об основах работы с сетью и информационной безопасностью также является важным компонентом успешного функционирования интернет-магазина.

## **2 Практическая часть**

В практической части будет произведена настройка сети интернет-магазина и все IP-адреса будут выданы согласно примерной схеме изображенной на Рисунке 1 и IP-плану описанному в таблице 2, 3, 4.

Также для корректной настройки сети необходимо использовать L1, L2, L3 схемы.

Схема сети L1 показана в приложении А.

Схема сети L2 показана в приложении Б.

Схема сети L3 показана в приложении В.

Схема диаграммы маршрутизации показана в приложении Г.

Таблица 2 – IP-план главного офиса



Таблица 3 - IP-план Филиала 1



Таблица 4 – IP-план Филиала 2



### **2.1 Выбор сетевого оборудования и его обоснование**

При принятии решения о выборе сетевого оборудования для проекта следует учитывать цели и требования проекта, совместимость с уже существующей инфраструктурой, надежность, производительность, безопасность и соответствие бюджету. Необходимо выбирать оборудование от проверенных производителей с надежной системой защиты от кибератак. Только учитывая все эти факторы, можно гарантировать выбор оптимального сетевого оборудования, которое будет успешно использоваться в рамках проекта.

В таблице 5 было выбрано оптимальное сетевое оборудование для сети магазина.

Таблица 5 – Сетевое оборудование



Это оборудование подходит для сети интернет-магазина по следующим причинам.

Маршрутизатор MikroTik RB5009UG+S+IN обеспечивает высокую производительность и надежность в работе сети, позволяя эффективно управлять трафиком данных и обеспечивать безопасность сети.

Управляемый коммутатор TP-LINK TL-SG108E позволяет настраивать параметры соединений для оптимизации работы сети, повышая ее производительность и обеспечивая гибкость в управлении.

Витая пара cat 6.a и коннекторы cat 6.a обеспечивают высокоскоростную передачу данных и минимизируют потери сигнала, что важно для работы интернет-магазина, где скорость загрузки страниц и выполнения заказов играет ключевую роль.

В таблице 6 расписаны характеристики для компьютеров в сети. Для системного администратора и сотрудников пунктов выдачи не всегда необходимо обладать высокопроизводительным компьютером. Основная задача таких специалистов заключается в обеспечении стабильной работы информационной системы предприятия и оказании технической поддержки пользователям.

Обычно, для выполнения данных задач не требуется значительных вычислительных мощностей, в отличие, например, от разработчиков программного обеспечения или графических дизайнеров. Более того, в некоторых случаях использование мощных компьютеров может быть излишним, так как такие устройства потребляют больше энергии и имеют более высокую стоимость обслуживания.

Основные требования для компьютеров системных и сетевых администраторов и сотрудников пунктов выдачи обычно сводятся к надежной работе, хорошей стабильности операционной системы, а также возможности запуска офисных приложений. Поэтому, для большинства задач таких специалистов вполне достаточно компьютеров средней мощности и удобства использования.

Таблица 6 – Характеристики персонального компьютера



В Таблице 7 расписаны комплектующие для сервера DELL R550 16SFF.

Таблица 7 – Комплектующие сервера



В таблице 8 высчитаны общее количество затрат на сетевую инфраструктуру.

Таблица 8 – Общие затраты



### **2.2 Базовая настройка сети**

### **2.2.1 Настройка статических IP-адресов**

На всех маршрутизаторах были настроены статические адреса. На рисунке 2 изображена настройка IP-адресов. На рисунке 3 все IP-адреса маршрутизатора R6. На сетевых устройствах R7, R8, R9 все адреса настроены согласна IP-плану в Таблицах 2, 3, 4.

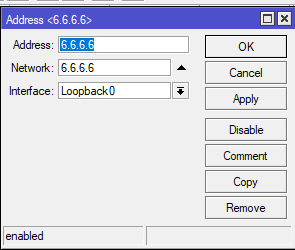


Рисунок 2 – Настройка IP-адреса

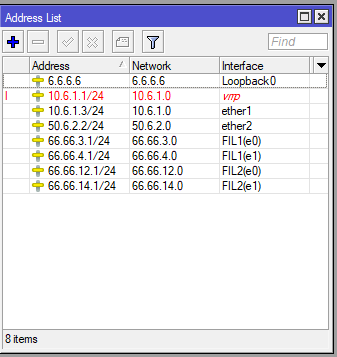


Рисунок 3 - Адреса интерфейсов на R6

### **2.2.2 GRE-туннели**

На рисунке 4 изображен пример настройки GRE-туннеля. Тоннели на всех маршрутизаторах были настроены идентично. Туннели изображены на схеме L3 в приложении В. На рисунке 5, 6, 7, 8 находится список туннелей каждого маршрутизатора в сети.

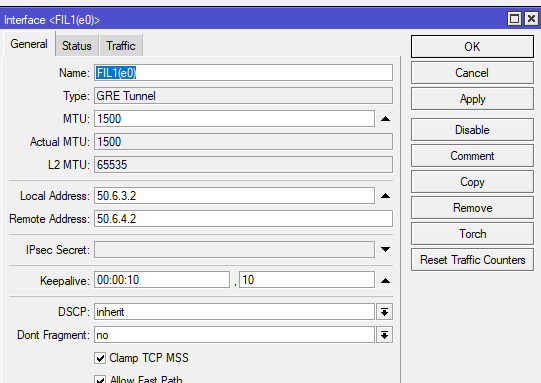


Рисунок 4 – Настройка GRE-туннеля на R7

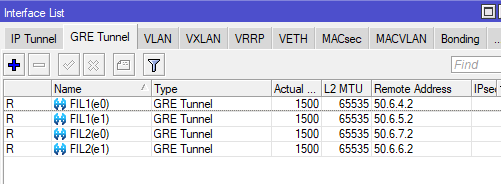


Рисунок 5 – Список туннелей на R6

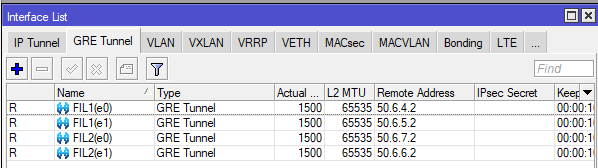


Рисунок 6 – Список туннелей R7

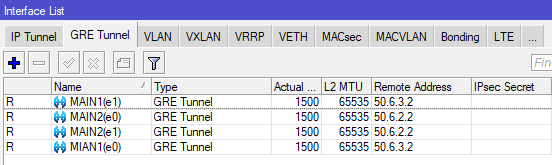


Рисунок 7 – Список туннелей R8

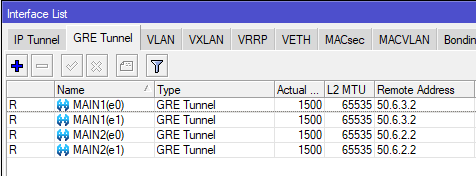


Рисунок 8 – Список туннелей R9

### **2.2.3 Настройка серверов**

Для настройки веб-сервера apache2 и добавления собственной страницы на Red Hat Enterprise Linux (RHEL) были выполнены следующие шаги:

Для установки apache2 была выполнена следующая команда:

sudo yum install httpd

Запуск службы apache2 и добавление её в овтозапуск:

sudo systemctl start httpd

sudo systemctl enable httpd

Создание директории для сайта в каталоге /var/www/html:

sudo mkdir /var/www/html/mywebsite

Создание простой HTML-страницы в файле index.html:

<!DOCTYPE html>

<html>

<head>

<title>Мой сайт</title>

</head>

<body>

<h1>Добро пожаловать на мой сайт!</h1>

</body>

</html>

Установка разрешений на файлы и директории сайта:

sudo chown -R apache:apache /var/www/html/mywebsite

sudo chmod -R 755 /var/www/html/mywebsite

Для настройки конфигурации apache2, был создан новый файл конфигурации в каталоге /etc/httpd/conf.d с названием mywebsite.conf, и добавлен следующий код:

<VirtualHost \*:80>

ServerAdmin webmaster@example.com

DocumentRoot /var/www/html/mywebsite

</VirtualHost>

Перезапуск службы apache2 для приминения изминений:

sudo systemctl restart httpd

Для создания и настройки базы данных были установлены пакеты MariaDB и phpMyAdmin:

sudo apt update

sudo apt install mariadb-server

sudo apt install phpmyadmin

После установки phpMyAdmin был выбран сервер apache2.

Перезапуск apache, чтобы применить изменения:

sudo systemctl restart apache2

Создание нового пользователя и базы данных в MariaDB:

sudo mysql -u root

CREATE DATABASE example\_db;

GRANT ALL ON example\_db.\* TO 'example\_user'@'localhost' IDENTIFIED BY 'password';

GRANT ALL ON example\_db.\* TO 'example\_user'@'%' IDENTIFIED BY 'password';

FLUSH PRIVILEGES;

Exit

Далее был перезапущен apache2:

sudo systemctl restart apache2

### **2.3 Настройка маршрутизации**

На рисунках 9, 10, 11, 12 изображены маршруты между филиалами и главным офисом на маршрутизаторах R6, R7, R8, R9.

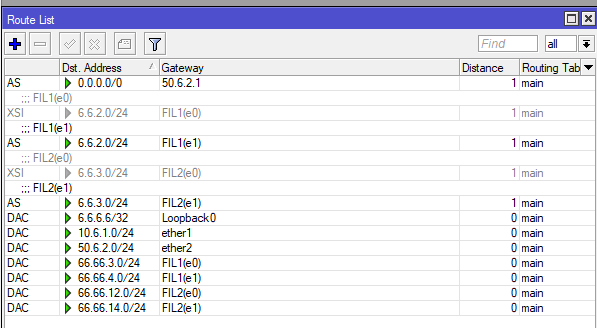


Рисунок 9 – Маршруты на R6

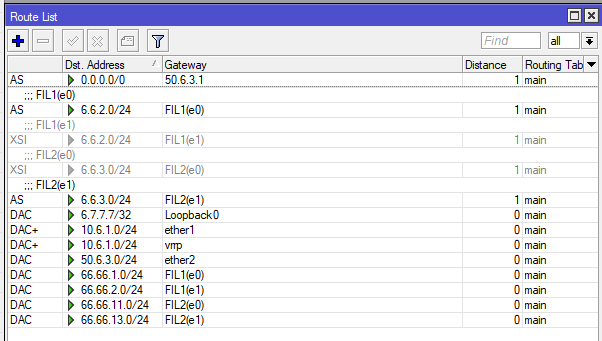


Рисунок 10 – Маршруты на R7

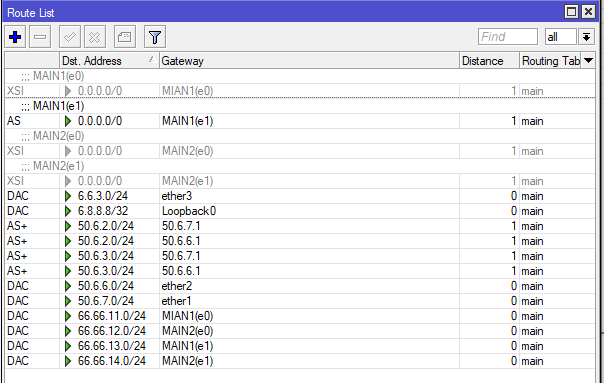


Рисунок 11 – Маршруты на R8

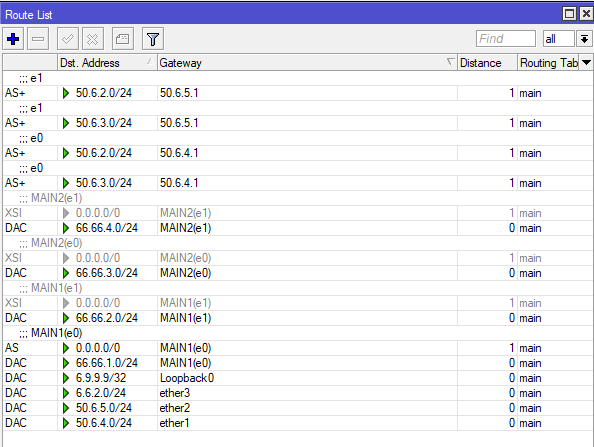


Рисунок 12 – Маршруты на R9

### **2.4 Настройка сервисов**

### **2.4.1 DNS, DHCP, Netwatch, VRRP**

На рисунке 13 указан DNS-сервер для R7. Также идентично были указаны серверы для пересылки записей с доменными именами для R6, R8, R9.

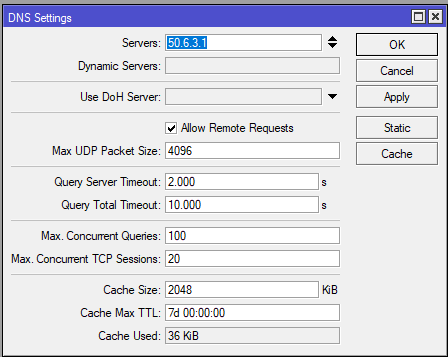


Рисунок 13 – Настройка DNS

В главном офисе и филиалах DHCP были настроены идентично. Пример настройки DHCP на рисунке 14, 15.

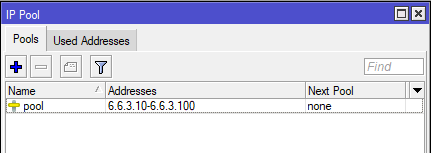


Рисунок 14 – Создание пула адресов для DHCP на R8

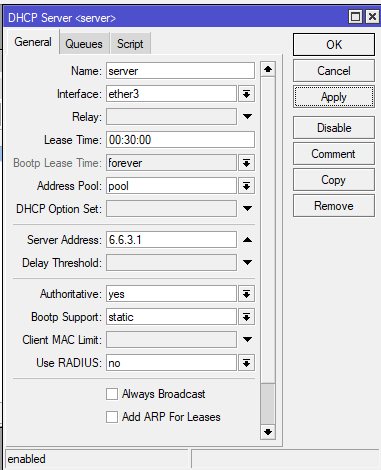


Рисунок 15 – Настройка DHCP-сервера на R8

Netwatch на филиалах был настроен идентично. Настройка Netwatch в главном офисе на маршрутизаторах R6 и R7 схожа. Поэтому на рисунках 16,17 показана настройка Netwatch для R7, а на рисунках 18, 19 для филиала 1.

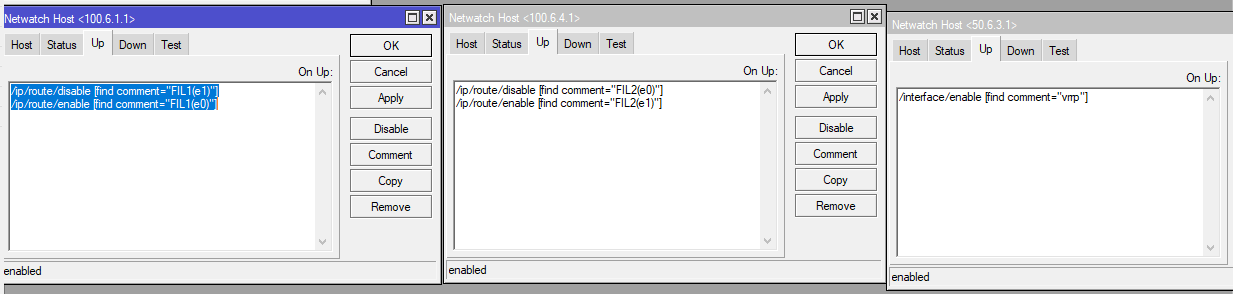


Рисунок 16 – Настройка netwatch с включенными правилами на R7

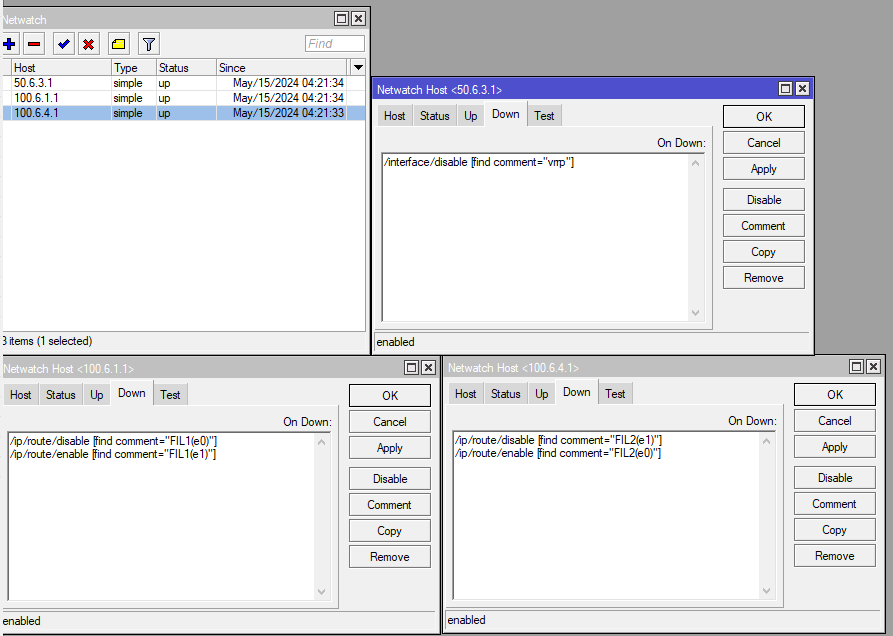


Рисунок 17 - Настройка netwatch с выключенными правилами на R7

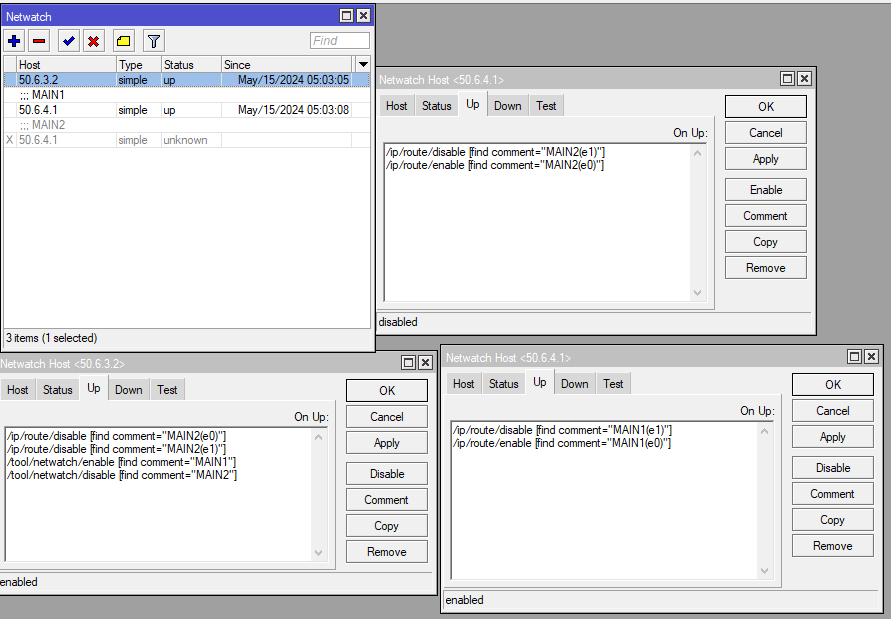


Рисунок 18 - Настройка netwatch с включенными правилами в филиале 1

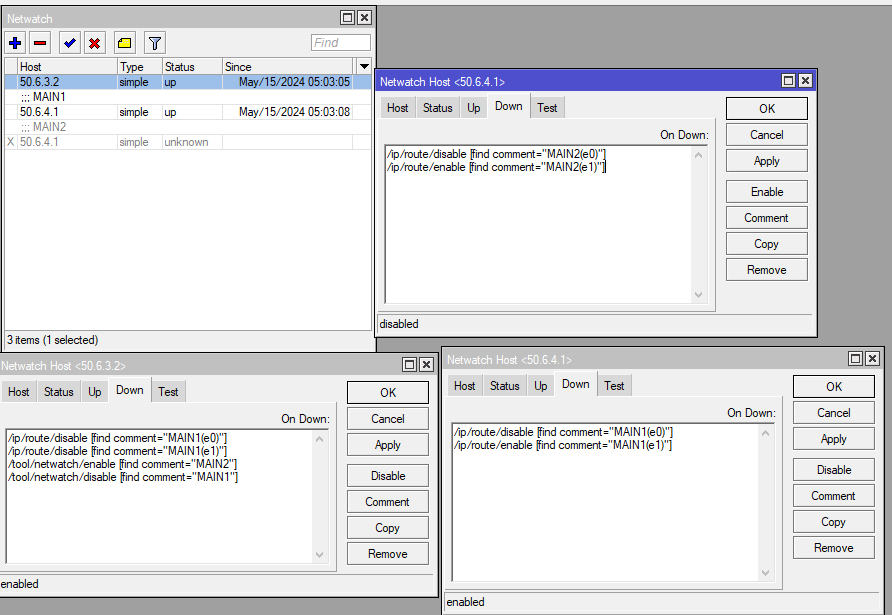


Рисунок 19 - Настройка netwatch с включенными правилами в филиале 1

Настройка VRRP на R7 на рисунке 20, для R6 настройка идентична.

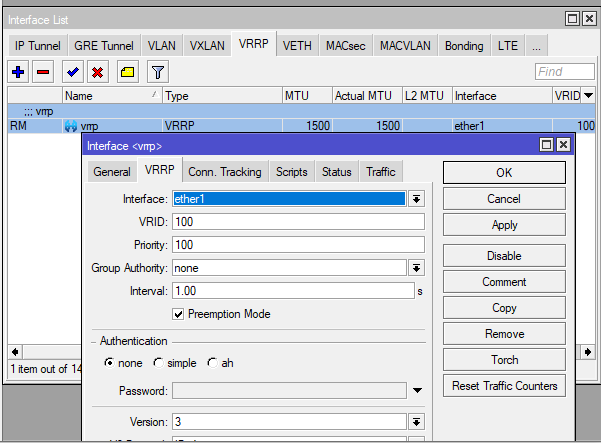


Рисунок 20 – Настройка VRRP на R7

### **2.4.2 Настройка NAT и HAproxy**

На рисунках 21, 22 настройка проброса портов и подмена адресов на R7, на R6 настройка одинакова. На R8, R9 это настраивать не нужно так, как весь трафик идет по-умолчанию через главный офис.

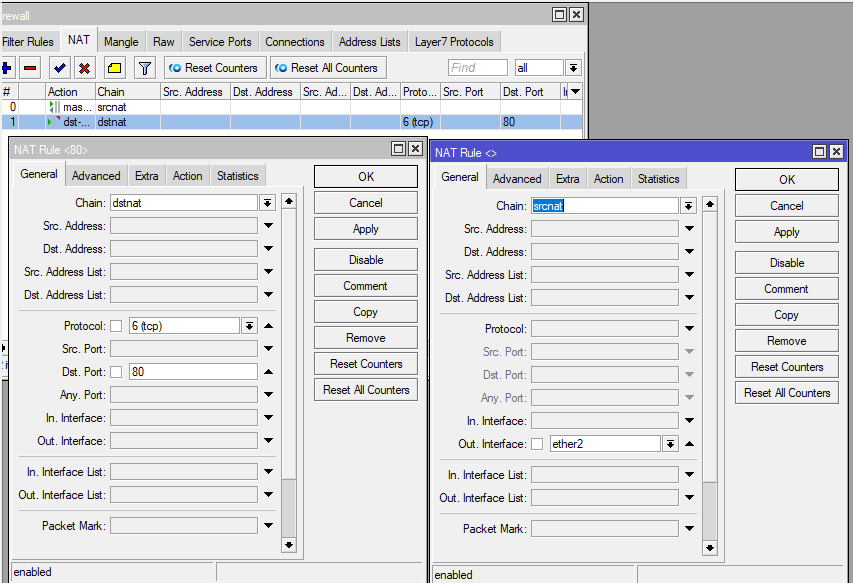


Рисунок 21 – Настройка проброса портов и nat на R7

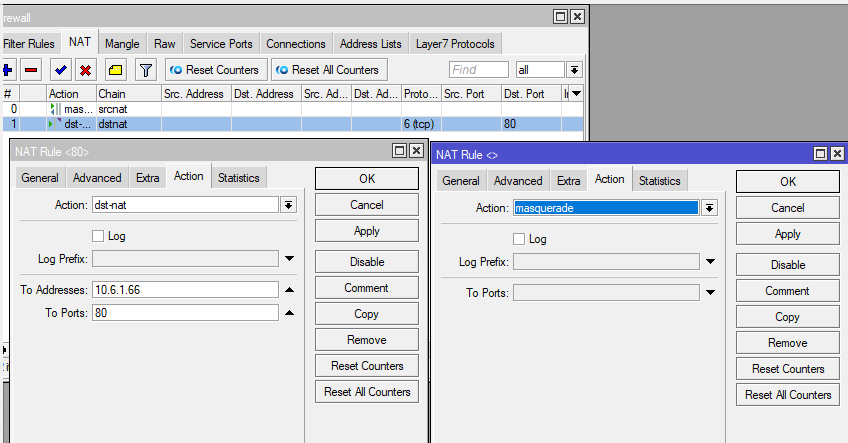


Рисунок 22 - Настройка проброса портов и nat на R7 вкладка action

Далее будет описана настройка HAproxy на операционной системе debian.

Обновление системного репозитория debian:

$ sudo apt update

$ sudo apt upgrade -y

Установка haproxy:

$ sudo apt install haproxy -y

Для управления haproxy с помощью сценария инициализации в файле /etc/default/haproxy была добавлена следющая строка:

ENABLED=1

Для настройки балансировщика конфиг в конфигурационном файле /etc/haproxy/haproxy.cfg был изменен на следующий конфиг:

frontend Local\_Server

bind 10.6.1.55:82

mode http

default\_backend webserver

backend webserver

mode http

balance roundrobin

option forwardfor

http-request set-header X-Forwarded-Port %[dst\_port]

http-request add-header X-Forwarded-Proto https if { ssl\_fc }

option httpchk HEAD / HTTP/1.1rnHost:localhost

server web1 10.6.1.65:80

server web2 10.6.1.66:80

### **2.5 Тестирование работоспособности сети**

На рисунках 23 видно, как маршруты между филиалами проходят через GRE туннели.

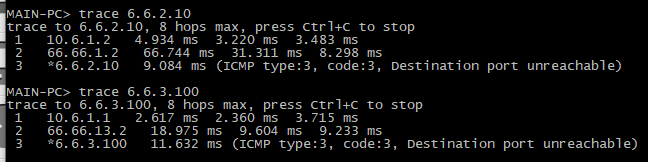


Рисунок 23 – Проверка доступности локальной сети

На рисунке 24 пользователь может обратиться в интернет, тем самым подтверждая работоспособность NAT и DNS.

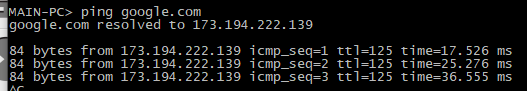


Рисунок 24 – Проверка работоспособности DNS и NAT

Рисунок 25, 26 отображает открытые сайты, которые могут меняться каждый новый запрос с помощью AHproxy.

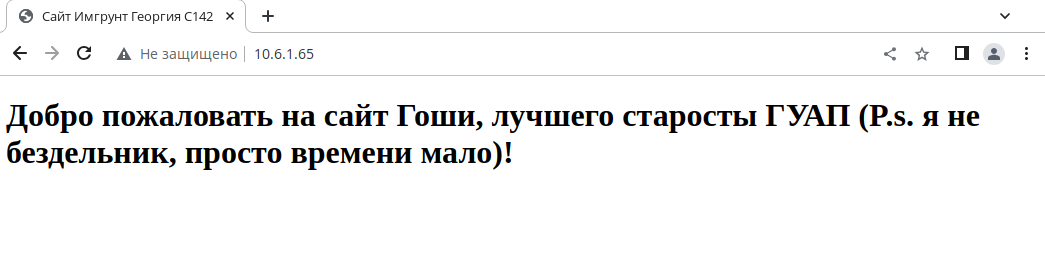


Рисунок 25 – Проверка webserv1

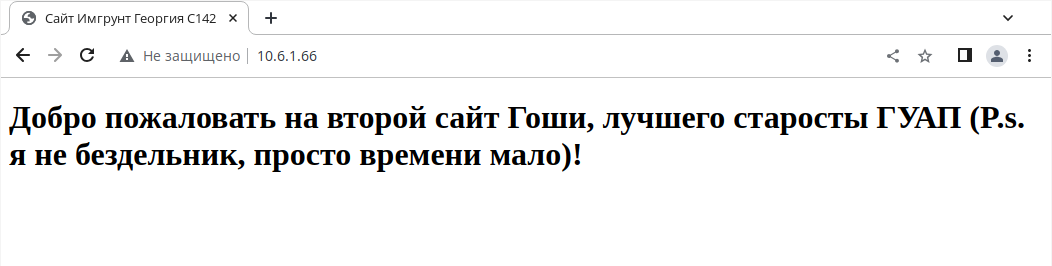


Рисунок 26 - Проверка webserv2

Рисунки 27, 28 демонстрируют работу netwatch, посредством отключения одного из правил, после поломки маршрутизатора R7.

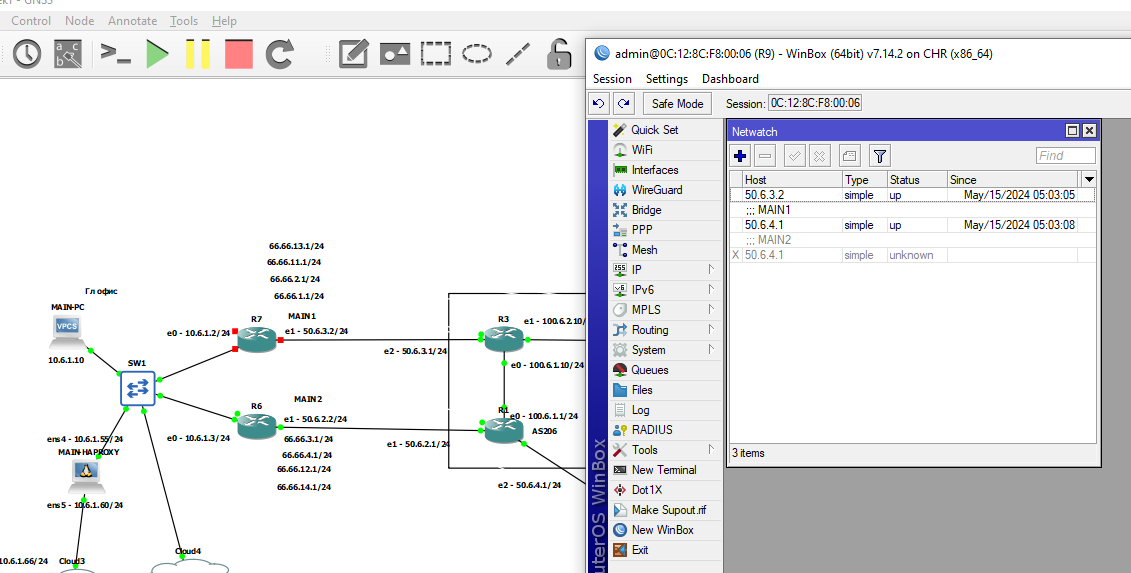


Рисунок 27 – Netwatch

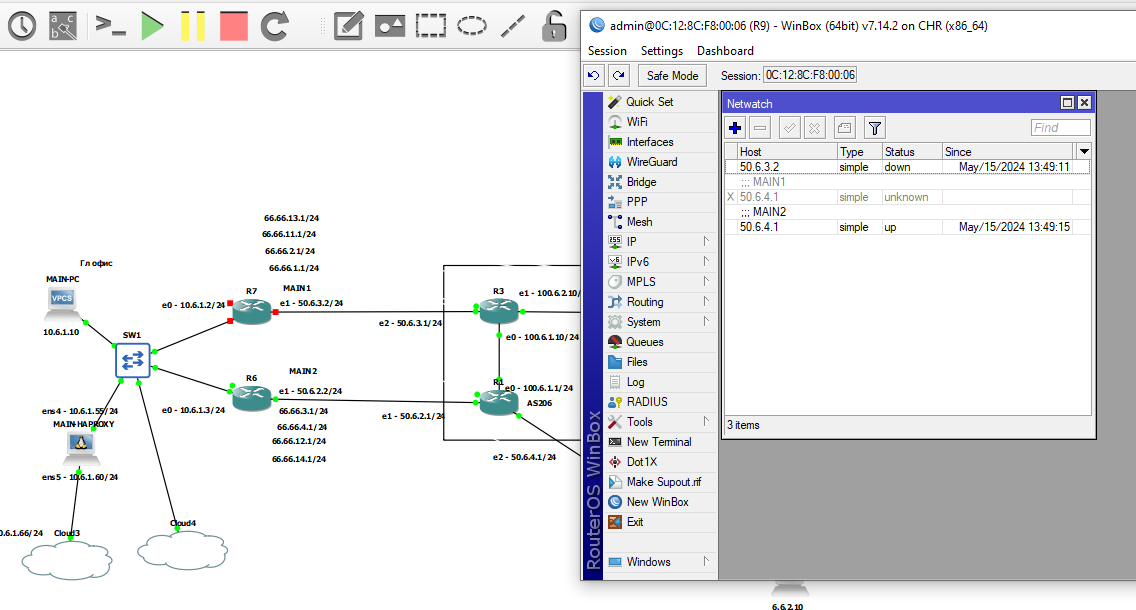


Рисунок 28 – Netwatch отключил другое правило из-за отключения R7

На рисунках 29, 30 показано рабочее состояние vrrp.

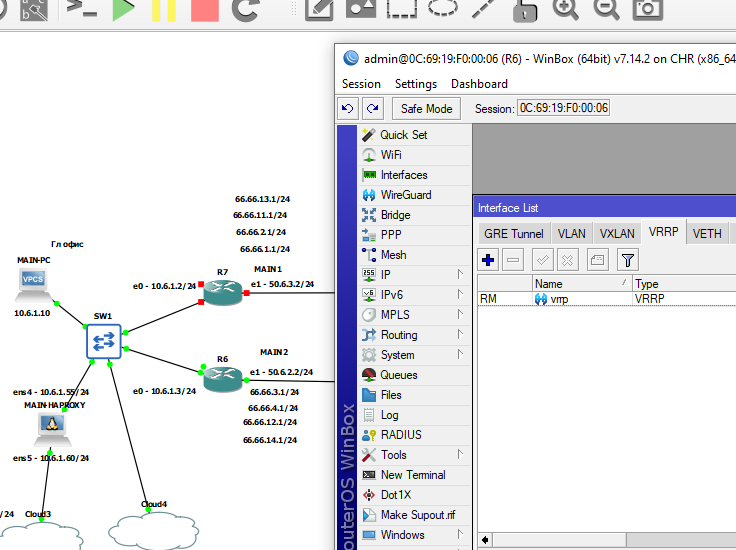


Рисунок 29 – Проверка VRRP, R6 master

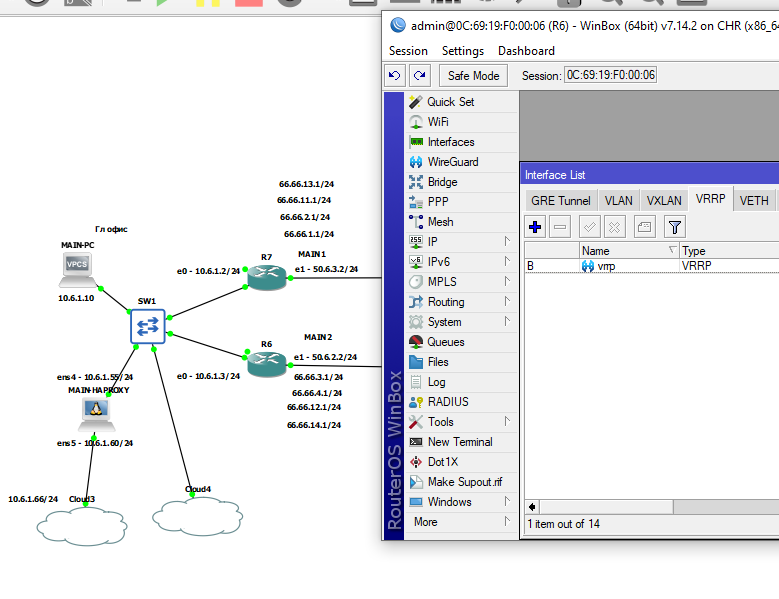


Рисунок 30 - Проверка VRRP, R6 backup

Админ может обратиться к базе данных, по адресу сервера это можно увидеть на рисунках 31, 32.

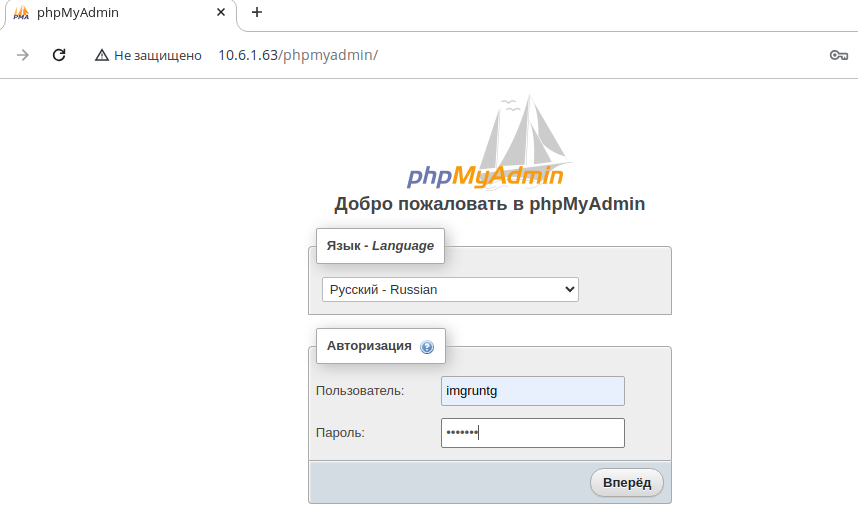


Рисунок 31 – Попытка регистрации на bd

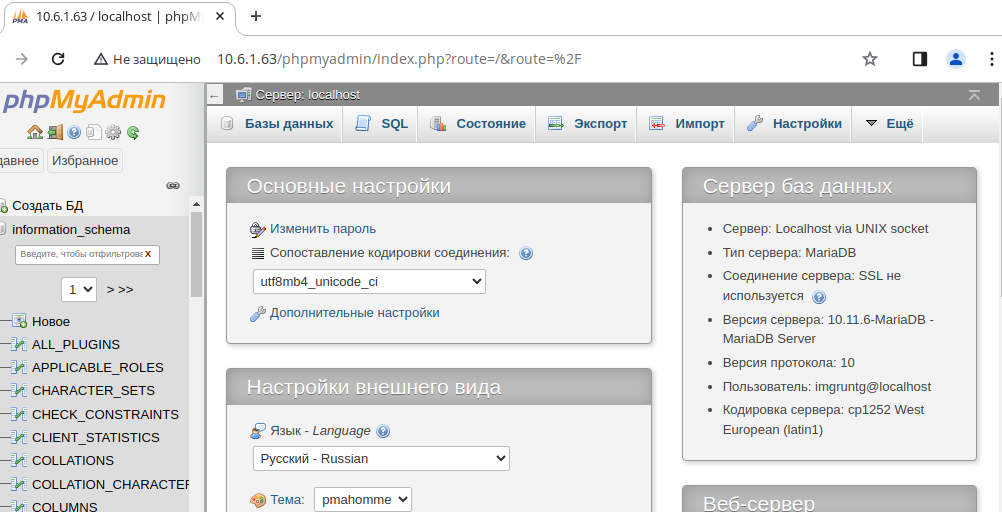


Рисунок 32 – Открытая база данных

## **ЗАКЛЮЧЕНИЕ**

В ходе настройки проекта были успешно развернуты VPN, DNS, DHCP, netwatch, веб сервера и другие компоненты, необходимые для эффективной работы интернет-магазина. Все функциональные требования были выполнены на высоком уровне и обеспечивают стабильную и безопасную работу системы.

Однако, для дополнительного увеличения уровня безопасности интернет-магазина, рекомендуется настроить дополнительные механизмы защиты, такие как межсетевые экраны, системы обнаружения вторжений и аудит безопасности. Эти меры помогут укрепить защиту от различных угроз и повысить общий уровень безопасности веб-сайта.

Таким образом, проект по настройке инфраструктуры интернет-магазина был успешно завершен, а дополнительные меры безопасности помогут обеспечить защиту данных клиентов и непрерывную работу системы.

## **СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ**

1 Информация о настройки маршрутизации OSPF – URL: https://netskillup.ru/cisco/hardware-configuration/ospf-single area?ysclid=lvgkr12g4v133487672 (Дата обращения: 01.05.2024);

2 Настройка BGP – URL: https://help.mikrotik.com/docs/display/ROS/BGP (Дата обращения: 02.05.2024);

3 Сети связи - Гольдштейн Б.С., Соколов Н.А., Яновский Г.Г.;

4 Основы сетевых технологий на базе коммутаторов и маршрутизаторов. – Васин Н.Н.;

5 Информация о NAT – URL: https://help.mikrotik.com/docs/display/ROS/NAT (Дата обращения: 09.05.2024);

6 Резервирование интернет-канала на Mikrotik– URL: https://www.dmosk.ru/miniinstruktions.php?mini=mikrotik-reserv&ysclid=lvesrvxfvh239236844 (Дата обращения: 11.05.2024);

7 База знаний системного администратора – URL: https://sysadminium.ru/mikrotik\_router\_backup\_with\_vrrp/?ysclid=lveu4s6lb0959239560/ (Дата обращения: 11.05.2024);

8 VPN:GRE – URL: https://mikrotik.wiki/wiki/VPN:GRE(Дата обращения: 11.05.2024);

## **ПРИЛОЖЕНИЕ А**

**Схема L1**

## **ПРИЛОЖЕНИЕ Б**

**Схема L2**

## **ПРИЛОЖЕНИЕ В**

**Схема L3**

## **ПРИЛОЖЕНИЕ Г**

**ДИАГРАММА МАРШРУТИЗАЦИИ**