Акционерное общество «Иридиум»
(АО «Иридиум»)

РУКОВОДСТВО АДМИНИСТРАТОРА
ПО УСТАНОВКЕ И НАСТРОЙКЕ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ НА ПОЧТОВОМ СЕРВЕРЕ «DEEPMAIL SERVER» (СЕРВЕРНАЯ ЧАСТЬ «DEEPMAIL МОДУЛЬ ВЗАИМОДЕЙСТВИЯ»)

RU.УГСФ.00003-01 90 01

Листов: 120

Москва, 2024 г.

АННОТАЦИЯ

Настоящий документ содержит руководство администратора автоматизированного рабочего места абонента почтового сервера DeepMail Server (далее – Сервер), а именно его компонента – серверное части для работы под управлением операционных систем Альт, Astra Linux, Debian, Ubuntu и РЕДОС.

В документе изложена последовательность действий системного администратора, необходимых для установки и настройки Сервера. Описание использования основных функций Сервера и подробное структурированное описание экранных форм веб-интерфейса администратора и описание работы с ними.

СОДЕРЖАНИЕ

1. ТЕРМИНЫ ОПРЕДЕЛЕНИЯ, СОКРАЩЕНИЯ И ОБОЗНАЧЕНИЯ

1.1 Термины и определения

Термины, используемы далее по тексту, их определения показаны в таблице 1.

Таблица 1 – Термины и определения

Термин	Определение
RSS-канал	RSS (англ. Really Simple Syndication) процедура, позволяющая при помощи программ-агрегаторов, получать и обновлять интересующую пользователя информацию с интернет ресурсов на его АРМ
SIP-телефония	Голосовая связь через интернет на основе протокола SIP (англ. Session Initiation Protocol – протокол установления сеанса), позволяющая устройствам абонентов «понимать» друг друга и правильно передавать данные, чередуя запросы и ответы. Помимо SIP-телефонии используется термин IP-телефония или VoIP-телефония. Зачастую они применяются, как синонимы
Автоматизированное рабочее место (АРМ)	Рабочее место специалиста, оснащенное персональным компьютером, программным обеспечением и совокупностью информационных ресурсов индивидуального или коллективного пользования, которые позволяют ему вести обработку данных с целью получения информации, обеспечивающей поддержку принимаемых им решений при выполнении профессиональных функций
Веб-канал	Механизм предоставления интернет содержимого в форматах на основе XML, без визуального сопровождения и с учетом индивидуальных предпочтений пользователя
Дистрибутив	Форма распространения программного обеспечения, обычно содержащая программу-установщик (для выбора режимов и параметров установки) и набор файлов, содержащих отдельные части программного средства
Домен (или доменное имя)	Уникальное имя, служащее для идентификации области расположения ресурса (веб – сайта) в сети Интернет
Иконка	Графическое изображение элемента пользовательского интерфейса (меню, кнопки, значка, списка и т.д.)

Термин	Определение
Кластер	Группа компьютеров, серверов или процессоров, объединённых высокоскоростными каналами связи, представляющая с точки зрения пользователя единый аппаратный ресурс
Клиент (Клиентская часть программного обеспечения - электронной почты «DEEPMAIL»)	Программный компонент, позволяющий в удобной пользователю форме осуществлять управление данными почтового сервиса: принимать и отправлять письма, сортировать входящие и исходящие сообщения, настраивать уведомления, формировать календарь событий и др.
Локальные папки	Хранилище информации на ПК
Моментальный снимок (или снапшот)	Резервная копия файлов или каталогов на определенный момент времени; каждый моментальный снимок содержит файлы или каталоги, которые можно восстановить при необходимости
Нода	Сервер, соединённый с другими серверами в некое сообщество, называемое «кластером»
Онлайн, офлайн	Статусы состояния подключения к сети интернет. «Онлайн» – подключение есть, «офлайн» – подключение отсутствует
Политика	Набор правил, которые сообщают, как создавать моментальные снимки/управлять ими; Политики регулируют такие функции, как сжатие, хранение моментальных снимков и планирование автоматического создания моментальных снимков
Пользователь	Субъект, обладающий правами использования и использующий ПО для решения своих задач
Пользовательский интерфейс	UI (англ. user interface – интерфейс пользователя) совокупность средств и методов, обеспечивающая передачу информации, между пользователем и программно-аппаратным обеспечением, в удобной для пользователя форме
Репозиторий	Место хранения, в котором сохраняются моментальные снимки (снапшоты)
Сообщения	Сообщения, передаваемые по электронной почте на базе ПО DeepMail
Спам	Массовая рассылка корреспонденции рекламного характера (нежелательных сообщений) лицам, не выразившим желания ее получить

Термин	Определение
Токен	Устройство, предназначенное для генерации электронных ключей, позволяющих пользователю произвести авторизацию в системе
Учетная запись	Совокупность данных о пользователе, хранящаяся в системе и необходимая для его распознавания (идентификации) и подтверждения подлинности его данных (аутентификации) при входе в систему

2. ОБЩИЕ СВЕДЕНИЯ

Почтовый сервер DeepMail Server (далее – Сервер) предназначен для комплексного управления электронной почтой, календарями и адресными книгами в т.ч. в рамках государственных корпораций, а также бизнес-структур и учреждений.

В процессе эксплуатации обеспечивается бесперебойное функционирование сервера при одновременной работе до миллиона пользователей DeepMail.

Микросервисная архитектура гарантирует:

- высокую отказоустойчивость;
- быстрое самовосстановление и масштабируемость в период колебания нагрузок;
- поддержку контроллеров домена SambaDC, ALD Pro, MS AD, FreeIPA;
- возможность развертывания в кластере;
- возможность использования учетных записей сторонних серверов;
- возможность настройки релейных доменов.
- Обеспечивается поддержка:
- российских сертифицированных ОС, таких как «Альт», «Astra Linux», «Ред ОС»;
- работы на российских системах виртуализации (ПК «Звезда», ПК «Иридиум», ПАК «Горизонт-ВС»);
- персональных автоответчиков;
- встроенной защиты от спама и вирусов;
- лёгкой миграции почтовых баз и учетных записей пользователей с любого почтового сервера, в том числе с Microsoft Exchange Server;
- протоколирования событий;
- сторонних пользователей (в базовой функциональности для обмена почтовыми сообщениями, а также для работы с календарями и адресными книгами);
- взаимодействия с кроссплатформенным Клиентом DeepMail (добавляется расширенная функциональность с обеспечением высокого уровня информационной безопасности, криптозащиты в соответствии с ГОСТ);
- современной бот-платформы для интеграции с корпоративными ресурсами;

- автоматизации обработки стандартизованных запросов в электронной почте и встроенном мессенджере.

3. СИСТЕМНЫЕ ТРЕБОВАНИЯ

3.1 Требования к техническим средствам

Требования к техническим средствам представлены в таблице 2.

Таблица 2 – Требования к техническим средствам (для 1000 пользователей)

Параметр	Минимальные требования	Рекомендуемые требования
Количество ядер процессора	4	8
Объем ОЗУ, Гбайт	8	16
Объем HDD, Гбайт	100 + квота пользователя ×1000	

3.2 Требования к программным средствам

Сервер функционирует на ОС: Альт, Astra Linux, Debian, Ubuntu и RedOS.

ПО, в котором размещаются контейнеры Docker Engine.

Надстройка над докером, позволяющая запускать множество контейнеров одновременно и маршрутизировать потоки данных между ними docker-compose v2.

4. АДМИНИСТРИРОВАНИЕ ПОЧТОВОГО СЕРВЕРА

4.1 Вход в Web-интерфейс администратора

Для доступа в web-интерфейс необходимо открыть web-браузер и перейти по ссылке в формате «https://<IP>», где <IP> – это IP-адрес почтового домена. После перехода по ссылке вы попадете в окно авторизации (рисунок 1). Для первичного входа в систему необходимо использовать данные по умолчанию:

- логин: admin@<domain> (<domain> – имя домена, указанного при установке);
- пароль: PASSWORD.

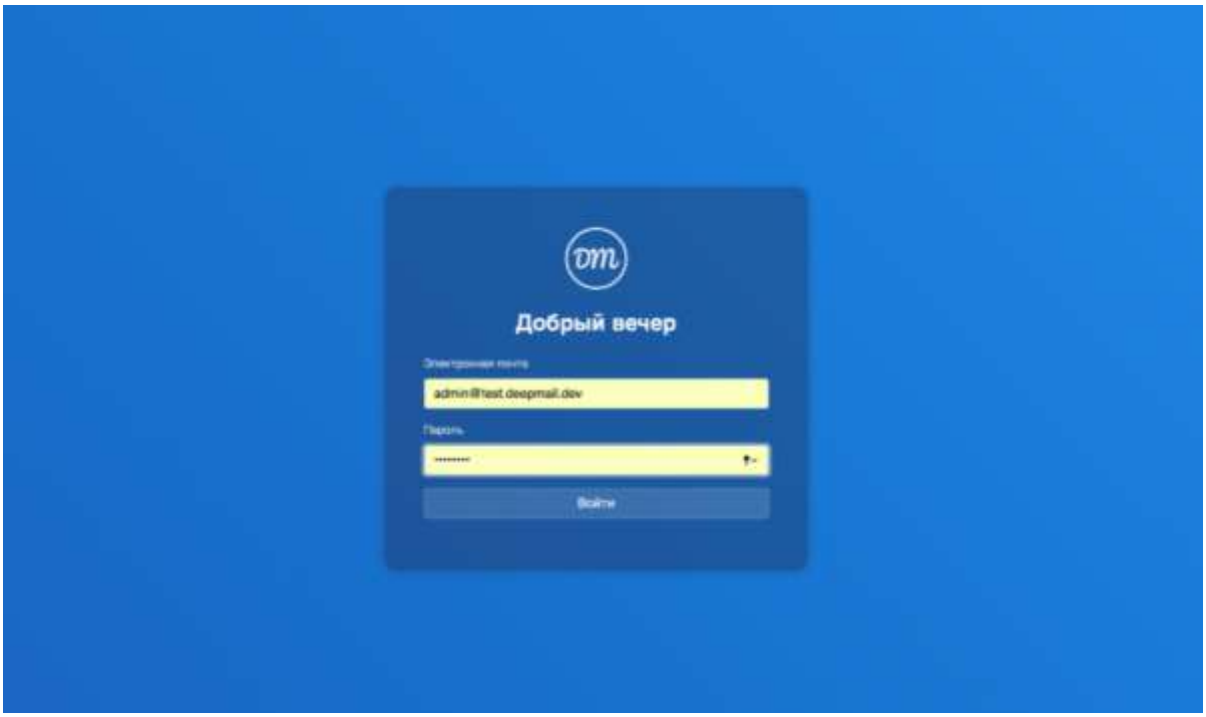


Рисунок 1 – Окно авторизации пользователя в web-интерфейсе

Введите логин и пароль по умолчанию для авторизации и нажмите кнопку 

.

При успешной авторизации будет открыта страница web-версии почтового клиента. Оформление страницы можно изменить, при помощи кнопок  и  расположенных в левом нижнем углу страницы. Для перехода в интерфейс администратора необходимо нажать на кнопку 

выделенную на рисунке 2).

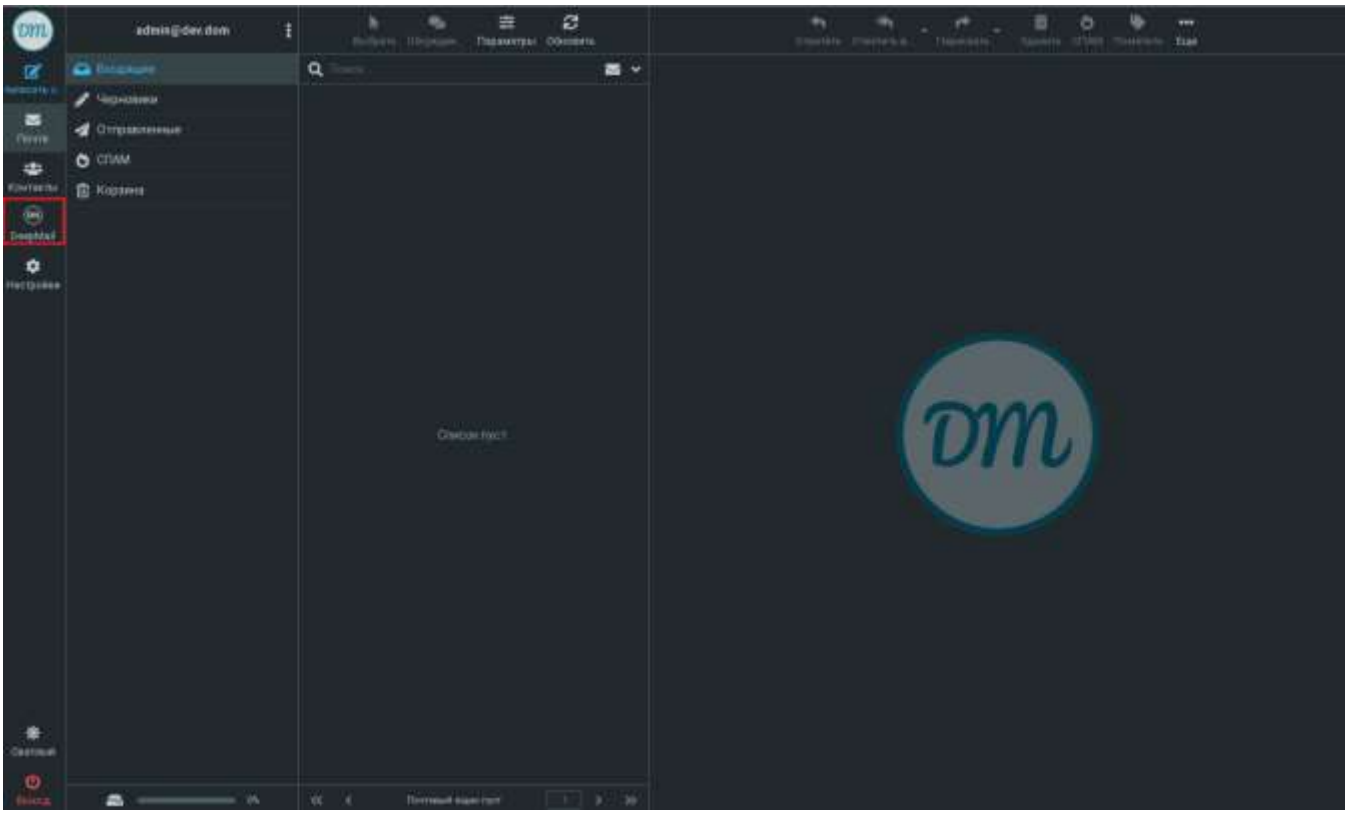


Рисунок 2 – Кнопка DeepMail перехода в интерфейс администратора

При первом входе в настройки DeepMail под учетной записью администратора должно появиться окно с номером лицензии, аналогичное показанному на рисунке 3.

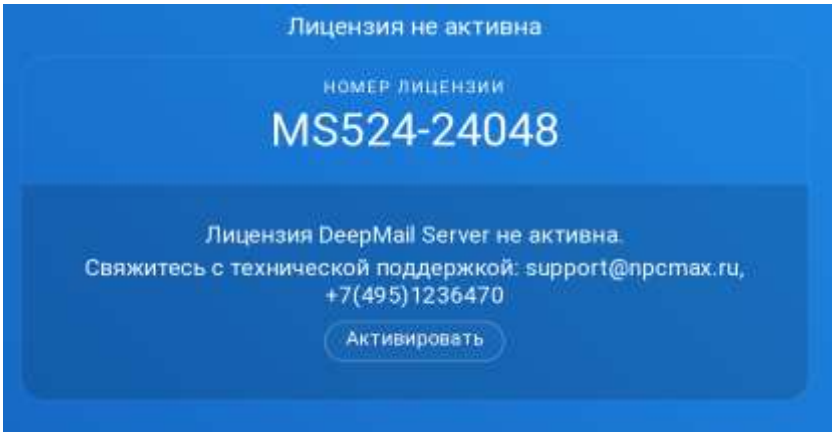


Рисунок 3 – Окно активации лицензии

Для активации лицензии администратор должен запросить лицензионный ключ активации у разработчика. Лицензионный ключ генерируется по номеру лицензии (см. рисунок 3). Для ввода полученного лицензионного ключа необходимо нажать

кнопку 

, в появившемся окне активации (рисунок 4) полученный от разработчика лицензионный ключ и нажать кнопку «Активировать».

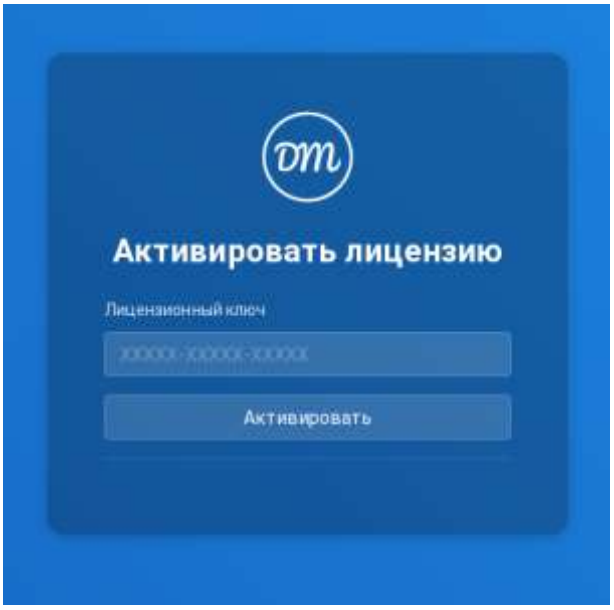


Рисунок 4 – Окно ввода лицензионного ключа

В случае успешной активации в окне авторизации должна появиться надпись «Лицензия активирована» (рисунок 5).

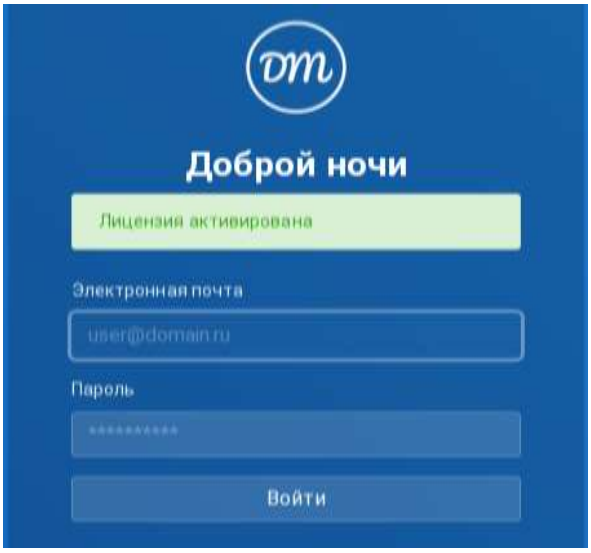


Рисунок 5 – Сообщение об активации лицензии

После ввода логина и пароля администратора будет запущен веб-интерфейс почтового ящика. Для перехода в интерфейс администратора (рисунок 6) необходимо нажать на кнопку 

(см. рисунок 2).

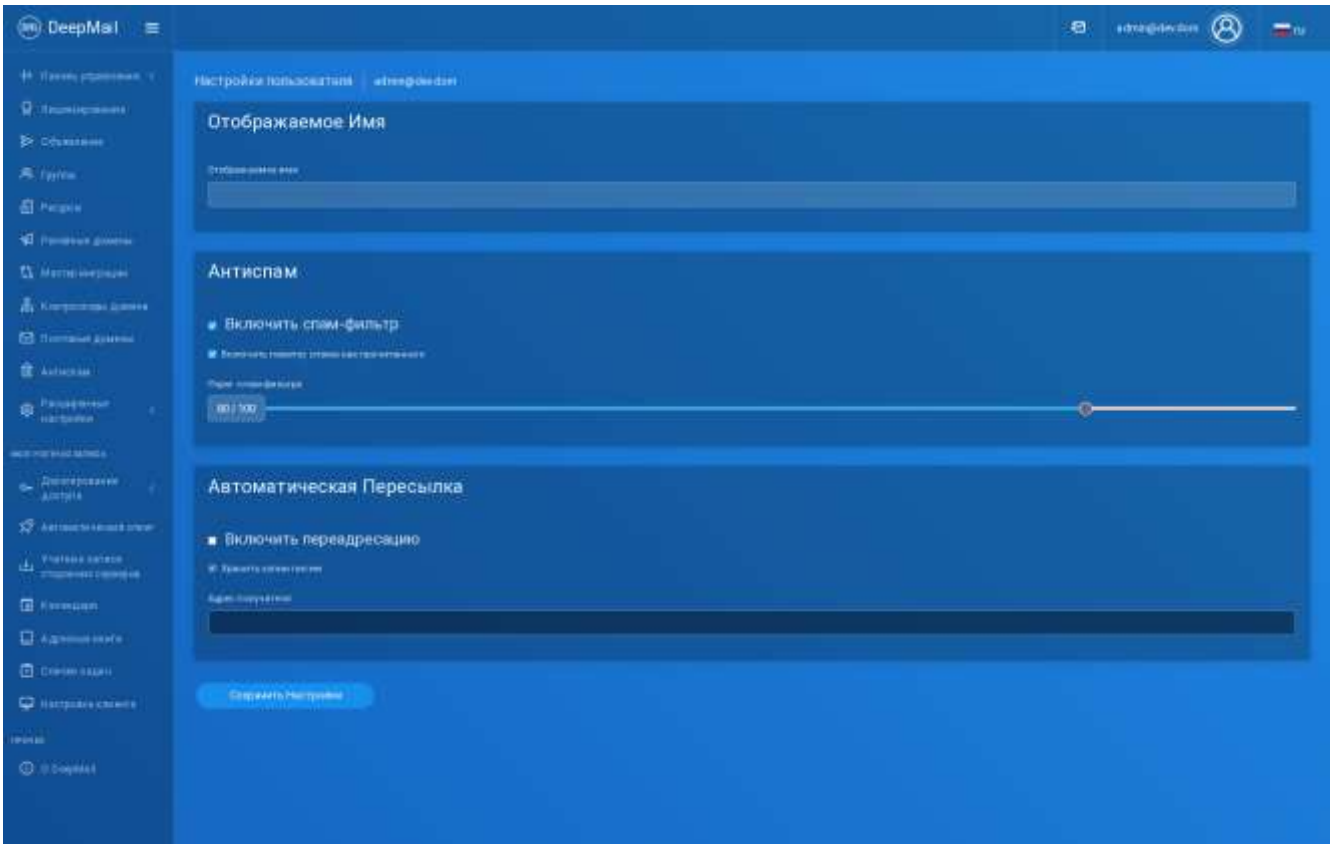


Рисунок 6 –Интерфейс администратора открытой вкладкой «Настройки пользователя»

На открывшейся вкладке «Настройки пользователя» администратор может настроить следующие параметры:

- «Отображаемое имя пользователя»;
- параметры работы антиспама в блоке «Антиспам»;
- параметры работы переадресации в блоке «Автоматическая пересылка» с указанием адреса для пересылки почты.

В левой части экрана интерфейса администратора расположено вертикальное меню, которое содержит в себе основные пункты меню настроек и администрирования Сервера (рисунок 7).

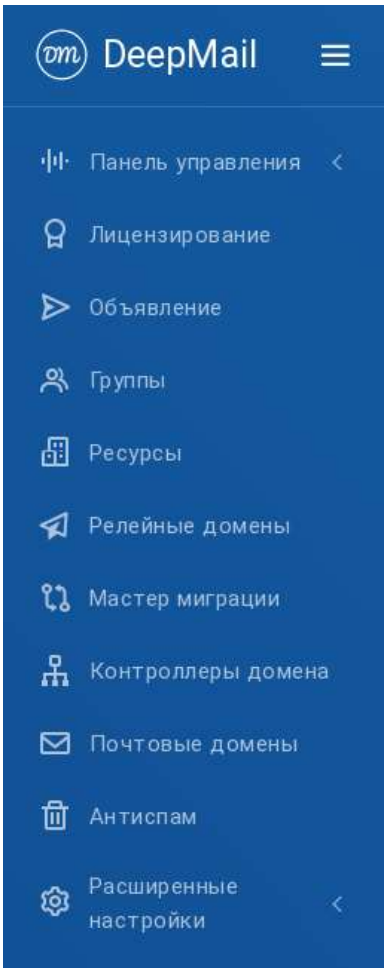


Рисунок 7 – Меню настроек и администрирования

Вертикальное меню, которое по умолчанию зафиксировано на странице, можно минимизировать нажав на кнопку  (рисунок 8).

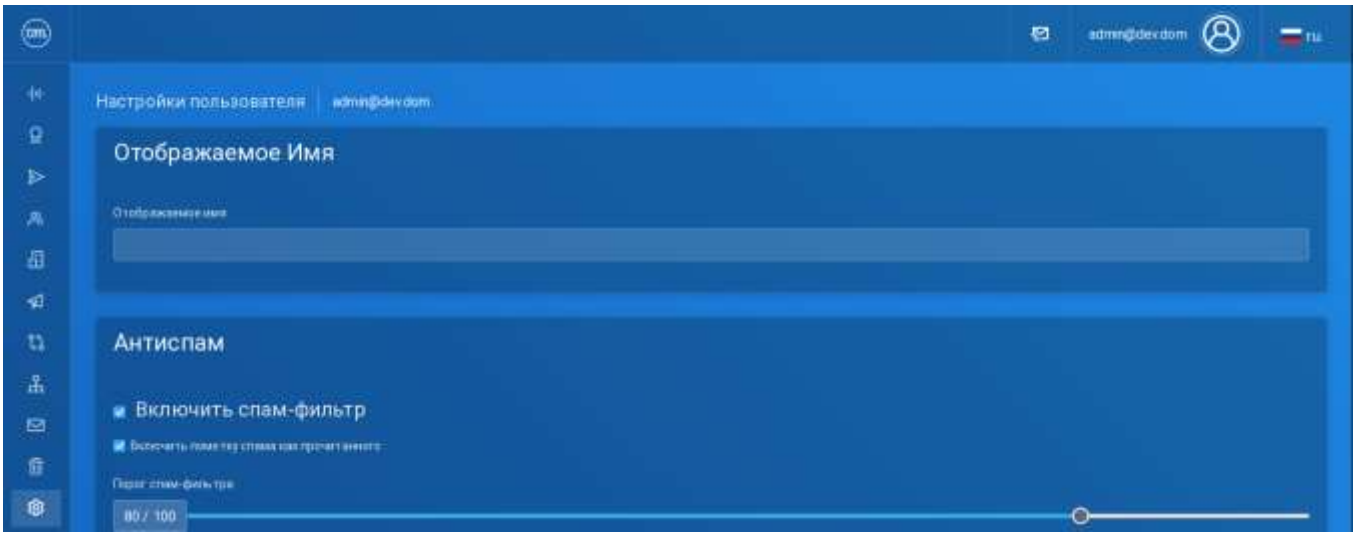


Рисунок 8 – Свернутое меню настроек и администрирования

При наведении курсора на свернутое меню настроек оно автоматически раскроется (рисунок 9). Для возврата к фиксированному меню настроек, необходимо повторно нажать на кнопку  .

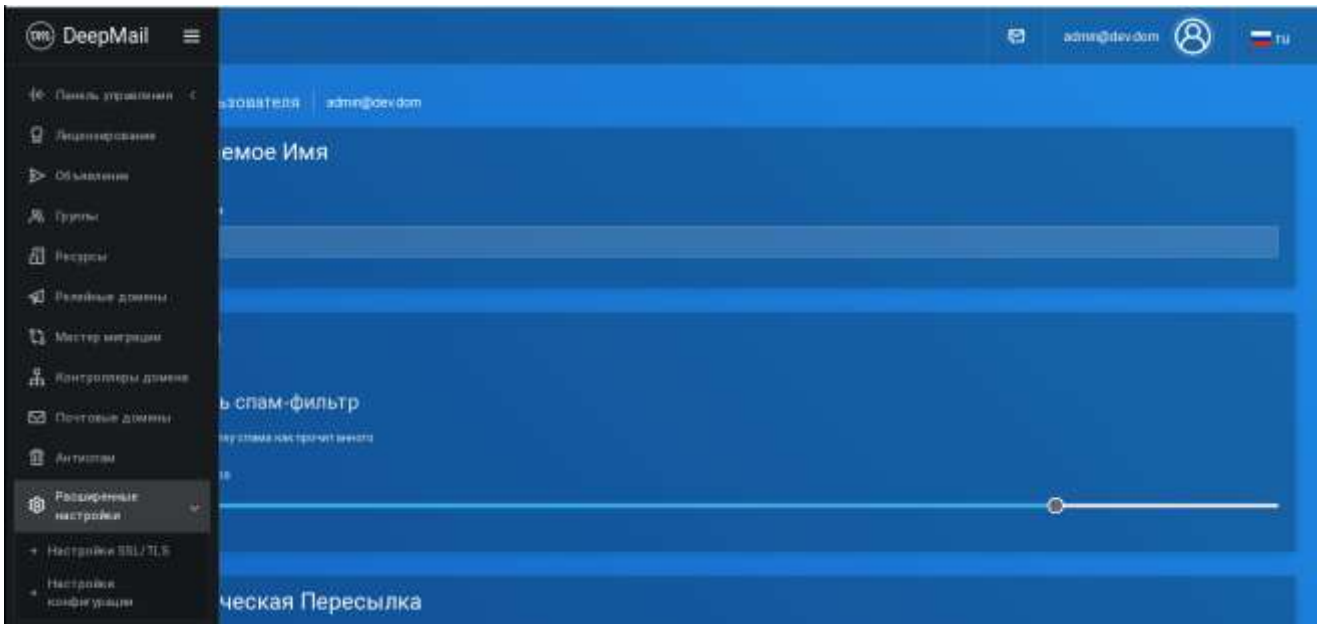


Рисунок 9 – Развернутое меню настроек и администрирования

В левом верхнем углу интерфейса администратора находится меню переключения языка интерфейса (рисунок 10).

Рисунок 10 – Меню переключения языка интерфейса

Для возврата к web-версии почтового клиента необходимо нажать на кнопку  .

4.2 Пункт вертикального меню «Панель управления»

После прохождения процедуры авторизации администратору будет доступен пункт меню «Панель управления», в которой можно просмотреть информацию о всех сервисах сервера (статус нод, статус сервисов ноды, нагрузка на ЦПУ, нагрузка на

ОЗУ, логи, состояние памяти хранилища). «Панель управления» содержит 2 подпункта «Система» и «Статистика» (рисунок 11).

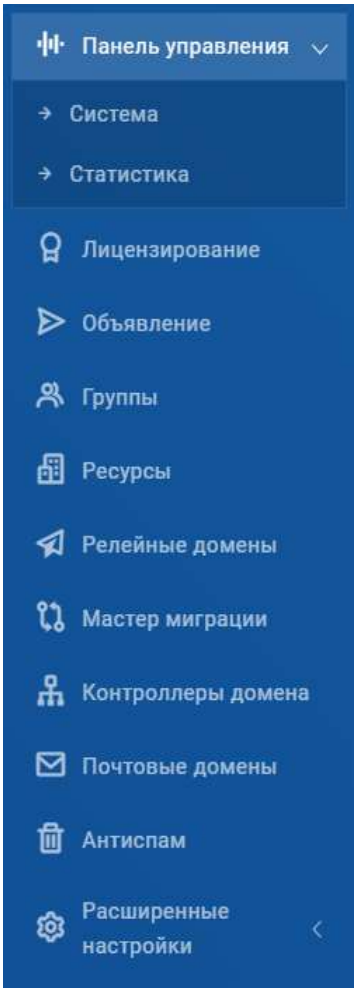


Рисунок 11 – Пункт меню «Панель управления»

4.2.1 Подпункт вертикального меню «Система»

Статистику работы почтового сервера в панели управления администратора можно

Подпункт вертикального меню «Система» (рисунок 13) предназначен для мониторинга ресурсов почтового узла DeepMail. Для перехода необходимо выбрать подпункт «Система» пункт вертикального меню «Панель управления» (рисунок 12).

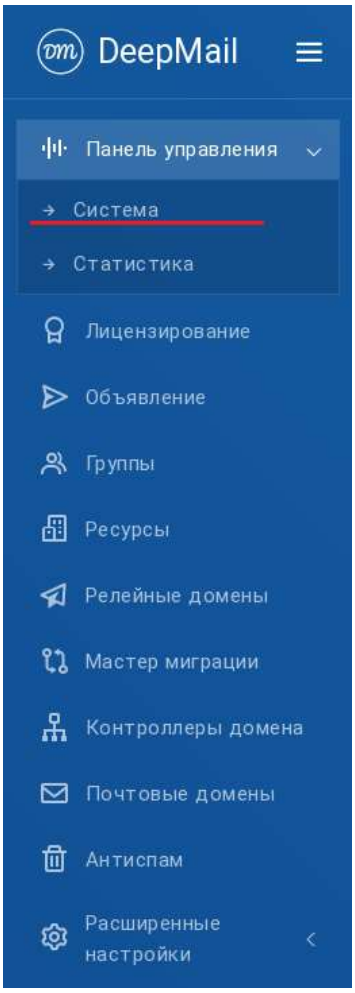


Рисунок 12 – Подпункт вертикального меню «Система»

После выбора подпункта «Система» будет открыта вкладка «Панель управления», которая отображает информацию о статусе работы нод почтового узла, распределение использованной физической памяти для каждой ноды, объем используемых ресурсов (ЦП и ОЗУ) микросервисами для каждой ноды и журналы работ (логи) для каждого микросервиса (рисунок 13).

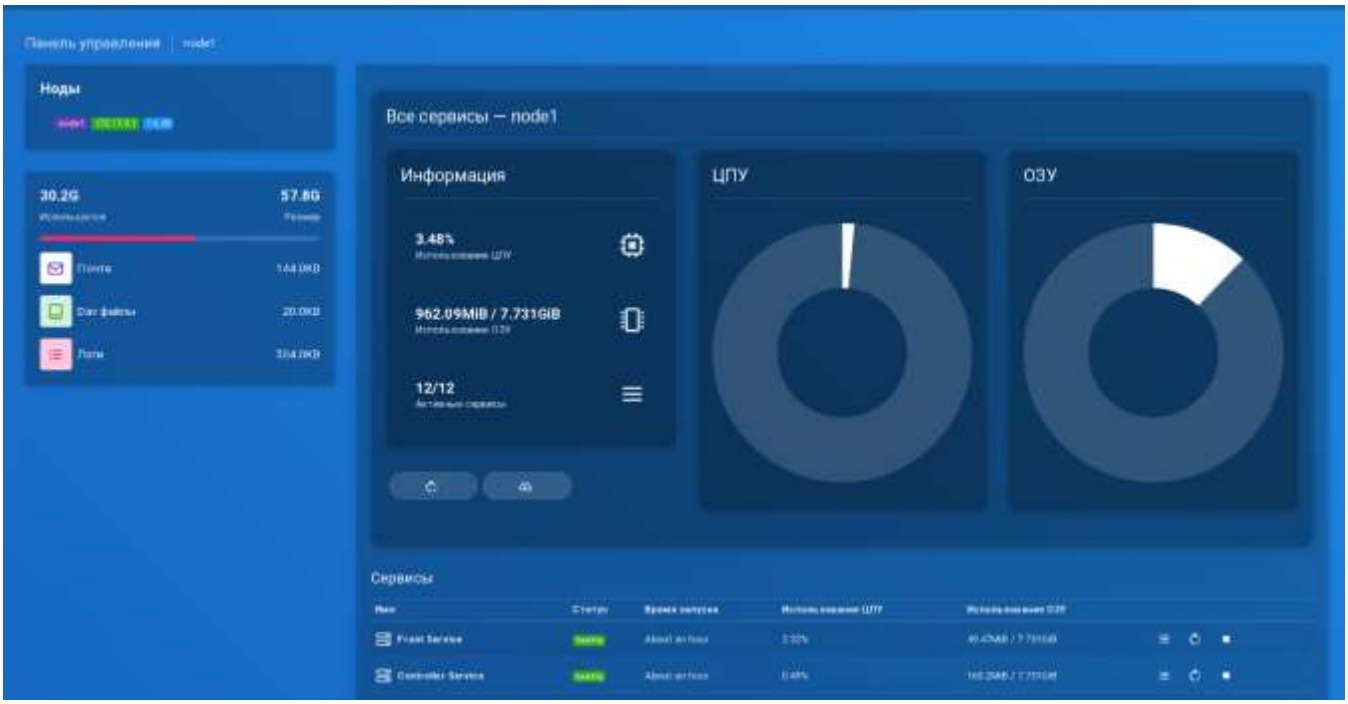


Рисунок 13 – Вид вкладки «Панель управления»

В панели нод (рисунок 14) показан список всех нод кластера. По каждой ноде выводится её IP-адрес и номер версии почтового узла DeepMail.

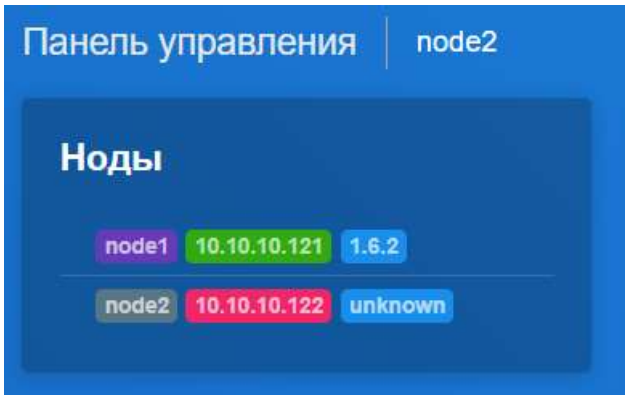


Рисунок 14 – Панель выбора нод сервера

Для того, чтобы выбрать интересующую ноду администратор должен нажать левой клавишей мыши по интересующей ноде, после чего информация о ресурсах и работе микросервисов выбранной ноды отобразится в других панелях.

Распределение физической памяти NFS-хранилища отображается в отдельной панели (рисунок 15).

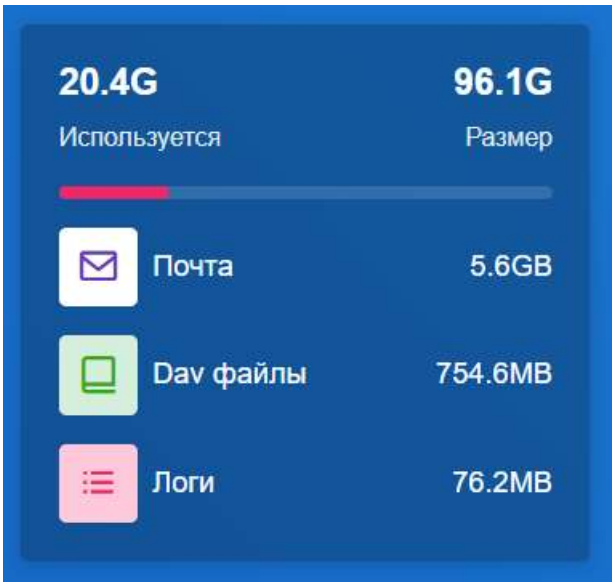


Рисунок 15 – Панель NFS-хранилища

В панели отображается количество располагаемой и использованной физической памяти, распределение занятой памяти между почтовыми сообщениями («Почта»), Dav-файлами (календари, контакты и др.) и логами.

Основная информация о работе микросервисов почты, а также кнопки управления этими микросервисами, отображается на панели «Все сервисы» (рисунок 16).

Рисунок 16 – Панель всех сервисов ноды

Вкладка отображает использование аппаратных ресурсов микросервисами выбранной ноды:

- загрузка процессора (в %);
- использование ОЗУ;
- количество активных сервисов.

Для перезагрузки ноды администратор должен нажать кнопку  , для выгрузки логов работы ноды администратор должен нажать кнопку  .

Таблица «Сервисы» (рисунок 17) отображает подробную информацию о работе микросервисов ноды, а также кнопки управления и просмотра логов работы микросервиса.

Рисунок 17 – Список микросервисов ноды

Администратор может перезапустить работу микросервиса кнопкой  или  остановить кнопкой. Логи работы микросервиса можно посмотреть, нажав кнопку  .

4.2.2 Подпункт вертикального меню «Статистика»

Статистику работы почтового сервера в панели управления администратора можно посмотреть, выбрав подпункт вертикального меню «Статистика» (рисунок 18).

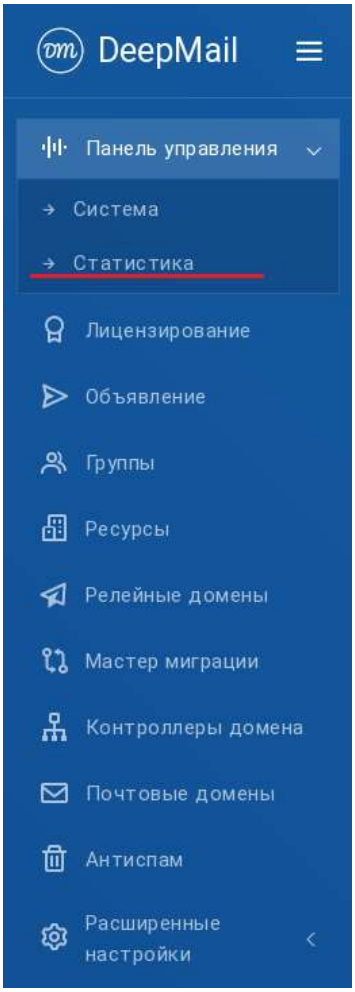


Рисунок 18 – Подпункт вертикального меню «Статистика»

На экране откроется вкладка «Статистика», на которой отображен календарь с возможностью выбора даты. Статистику можно посмотреть в разрезе каждого узла, поэтому в окошке выбора даты отобразятся все доступные узлы (рисунок 19).

Рисунок 19 – Вкладка «Статистика»

После выбора даты и узла отобразится общая статистика (рисунок 20).

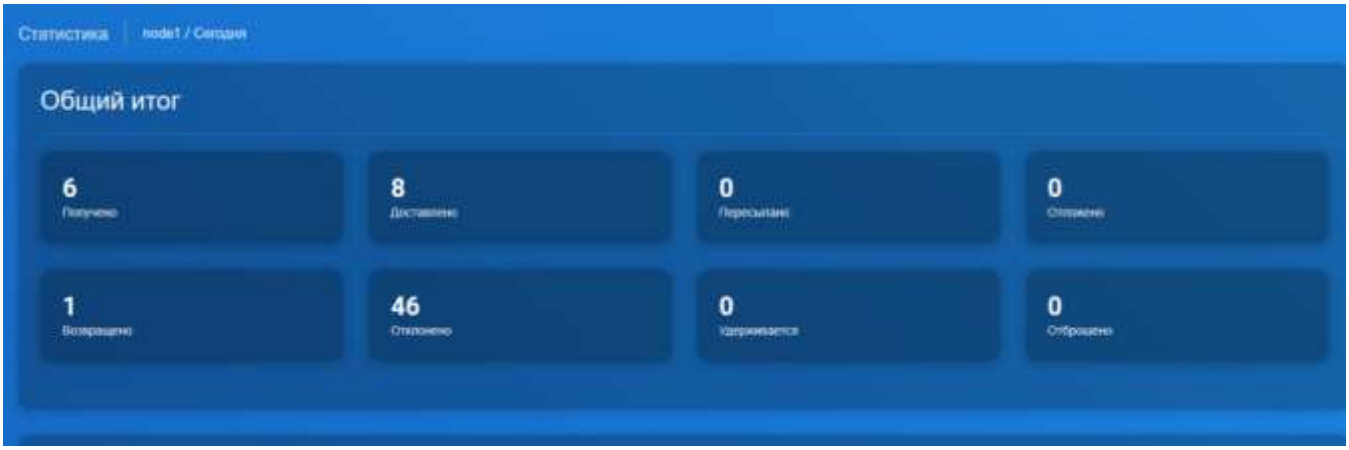


Рисунок 20 – Статистика для выбранного узла и даты

На панели «Сводка почасового трафика» представлена почасовая статистика и сводка по доменам (рисунок 21).

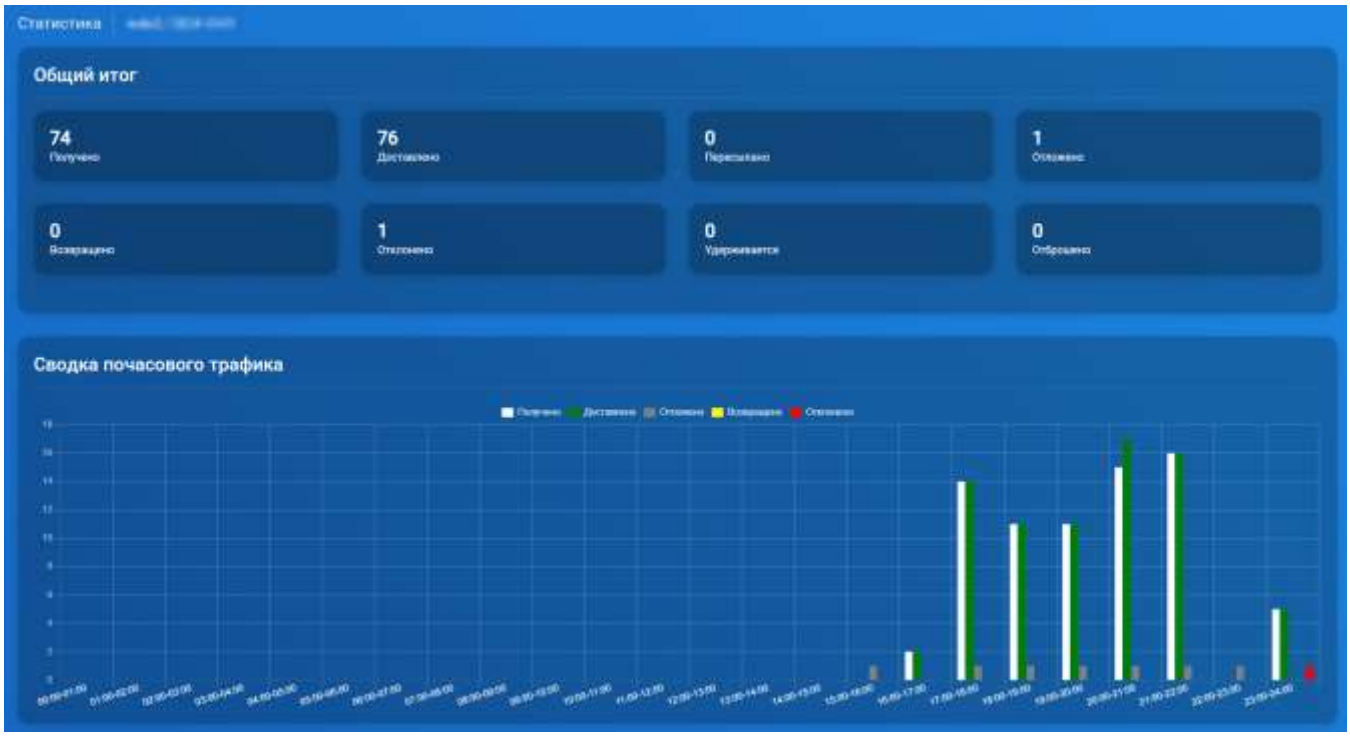


Рисунок 21 – Сводка почасового трафика для доменов

4.3 Пункт вертикального меню «Лицензирование»

Подробная информация о лицензии (количество пользователей и срок действия) представлена во вкладке «Лицензирование» (рисунок 22) для перехода на которую, необходимо выбрать пункт вертикального меню «Лицензирование» (рисунок 23).

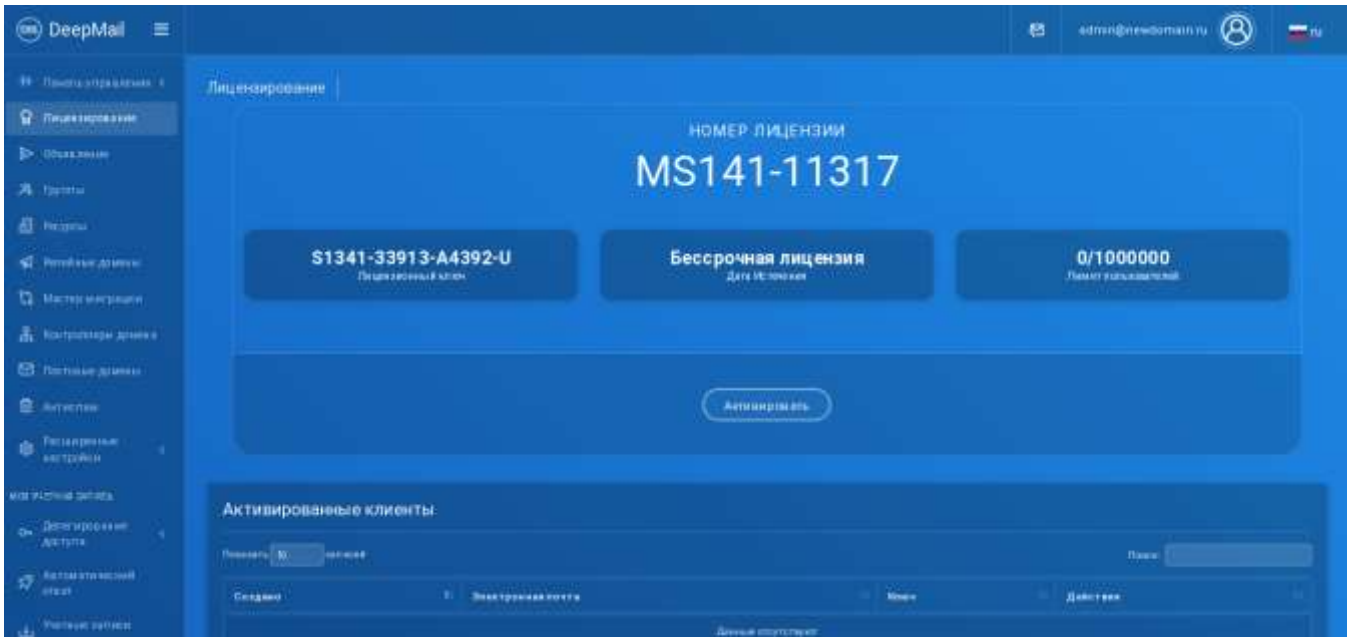


Рисунок 22 – Вкладка «Лицензирование»

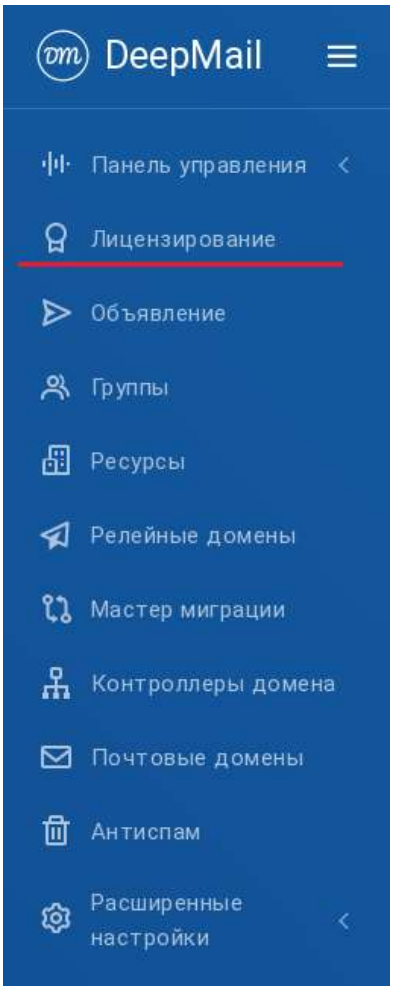


Рисунок 23 – Пункт вертикального меню «Лицензирование»

4.3.1 Активация лицензии

Для активации новой лицензии администратору необходимо на вкладке «Лицензирование» нажать на кнопку Активировать. В открывшемся окне (см. рисунок 4) необходимо ввести лицензионный ключ, полученный вместе с дистрибутивом, либо запросить лицензионный ключ у разработчика. Лицензионный ключ генерируется по номеру лицензии (см. рисунок 3). После ввода полученного лицензионного ключа в поле «Лицензионный ключ» необходимо нажать кнопку Активировать.

4.3.2 Панель «Активированные клиенты»

На панели «Активированные клиенты», в виде таблицы отображены клиенты, которые получили от сервера лицензию. Таблица состоит из следующих столбцов:

- «Создано» – дата получения лицензии конкретным клиентом;
- «Электронная почта» – электронная почта конкретного клиента;
- «Ключ» – номер лицензионного ключа, полученный конкретным клиентом;
- «Действия» – действия, которые администратор может сделать с конкретным клиентом (в данном случае удаление).

Для удаления активированного клиента из списка, администратору необходимо нажать на кнопку , расположенную в столбце «Действия» и подтвердить удаление в следующем окне «Подтвердить действия».

4.4 Пункт вертикального меню «Объявление»

Для перехода во вкладку «Публичное объявление» (рисунок 25), администратор должен выбрать пункт «Объявление» вертикального меню (рисунок 24).

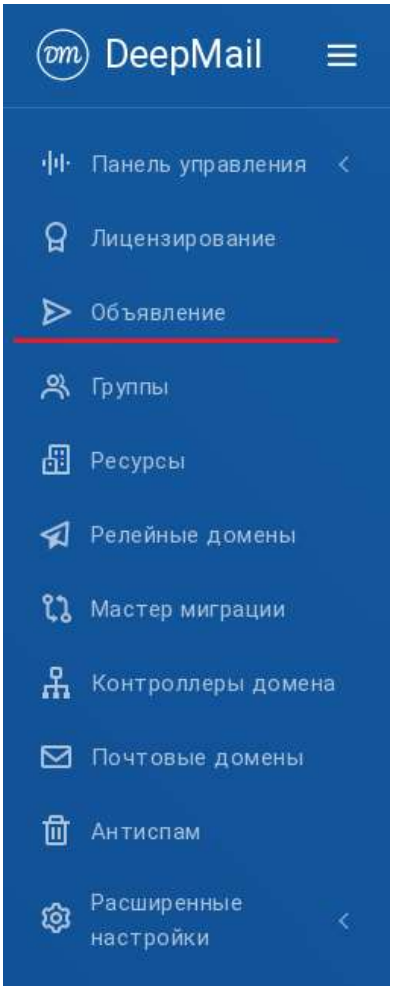


Рисунок 24 – Пункт вертикального меню «Объявление»

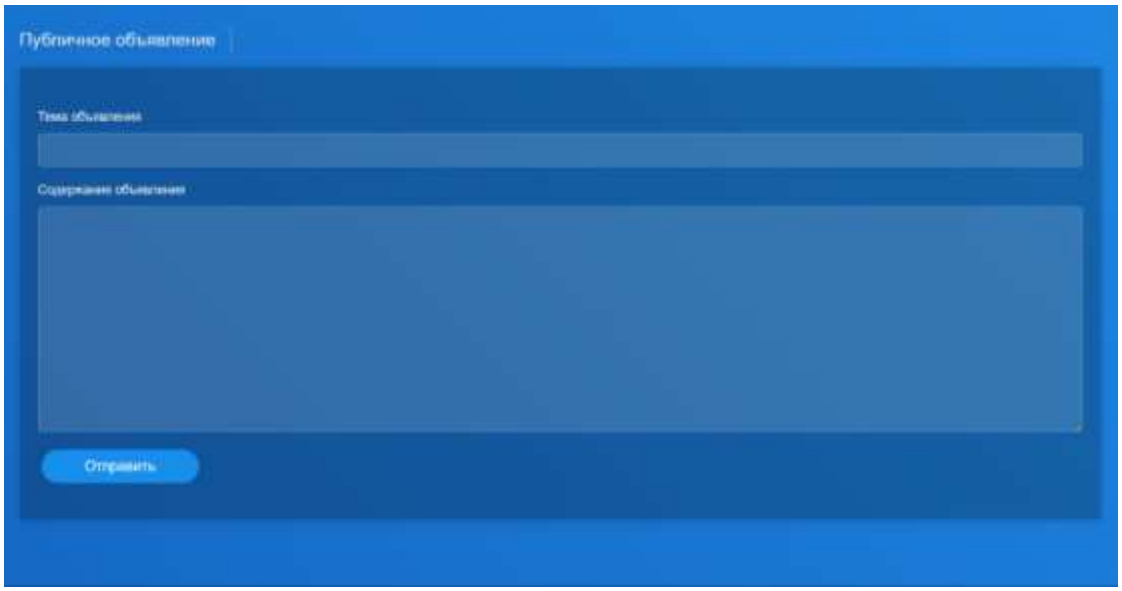


Рисунок 25 – Вкладка «Публичное объявление»

После ввода названия темы в поле «Тема объявления» и содержания в поле «Содержание объявления» объявления администратор должен нажать кнопку Отправить. При успешной отправке появится сообщение Оповещение отправлено.

4.5 Пункт вертикального меню «Группы»

Управление группами происходит через вкладку «Группы», вызываемую пунктом вертикального меню «Группы» (рисунок 26).

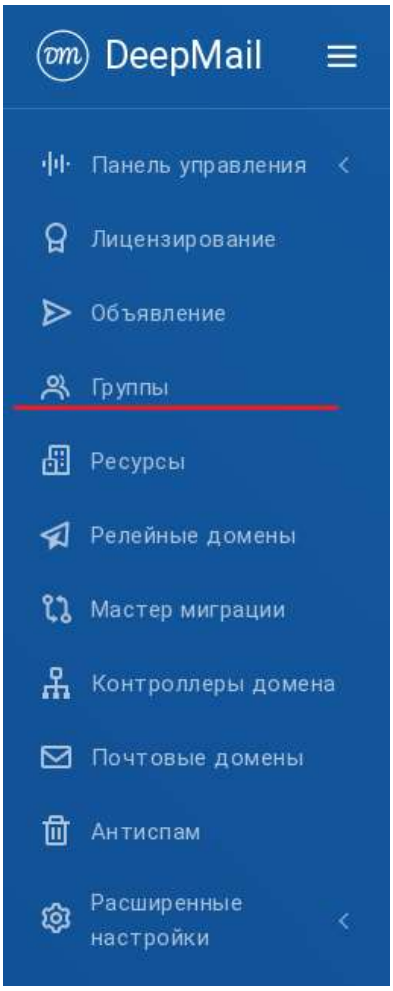


Рисунок 26 – Пункт вертикального меню «Группы»

При открытии отобразится вкладка «Группы», на которой будет отображен список групп пользователей всех почтовых доменов (рисунок 27).

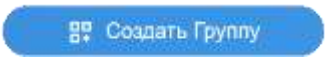
Рисунок 27 – Вкладка «Группы»

Во вкладке «Группы» администратор может создавать, редактировать и удалять различные группы пользователей, добавлять и удалять в них пользователей, а также наделять их правами. Администратор может предоставлять пользователям групп следующие права:

- «Настройка релейных доменов»;
- «Чтение глобальной адресной книги»;
- «Редактирование глобальной адресной книги»;
- «Доступ в панель управления»;
- «Отправка объявлений»;
- «Доступ к расширенным настройкам»;
- «Доступ к контроллеру домена»;
- «Доступ к миграции»;
- «Редактирование почтовых доменов и пользователей»;
- «Доступ к антиспаму»;
- «Доступ к лицензированию»;
- «Доступ к управлению ресурсами организации».

Доступ к правам реализуется в виде доступа пользователей к соответствующим вкладкам.

4.5.1 Создание группы пользователей

Для создания новой группы администратор должен нажать кнопку 

, после чего откроется форма создания группы, показанная на рисунке 28.

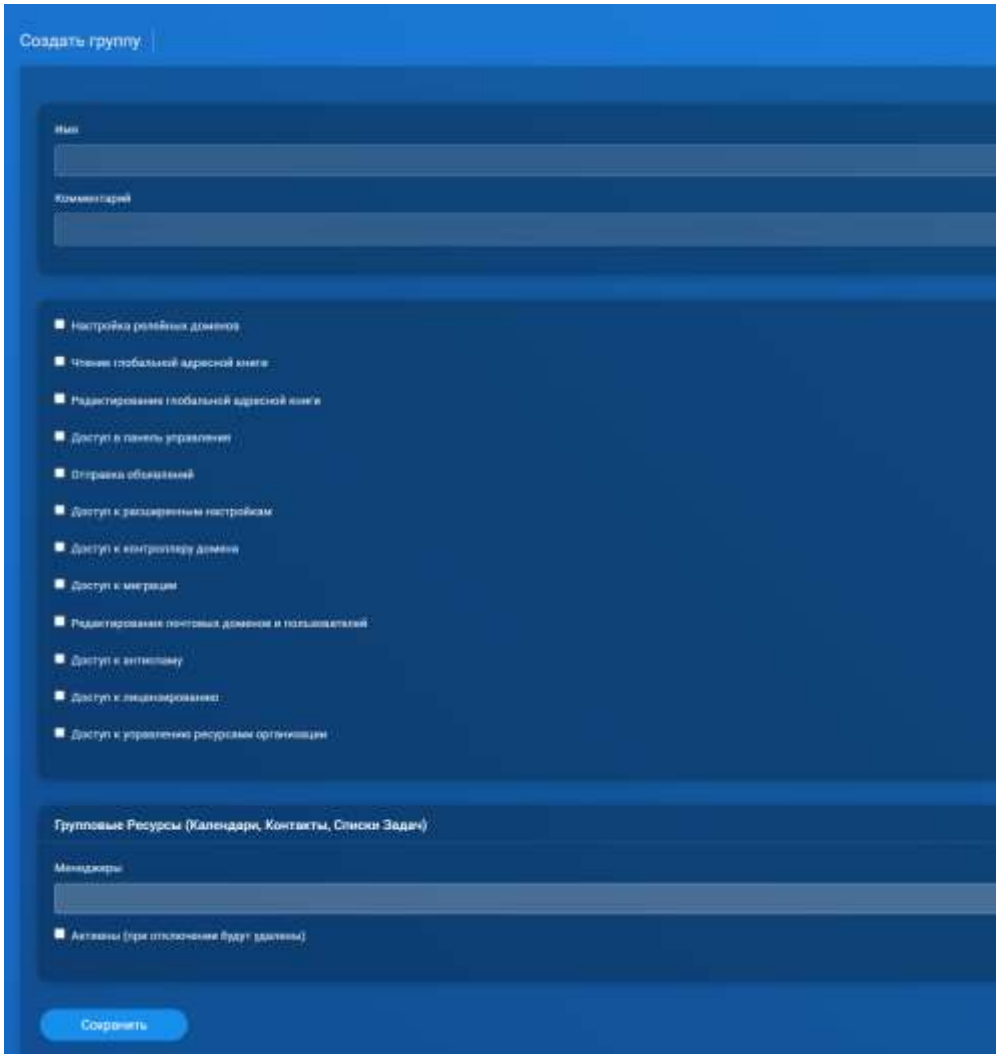
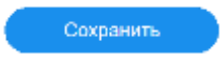


Рисунок 28 – Форма «Создать группу»

В форме «Создать группу» администратор должен ввести название группы, комментарий и назначить права участникам группы отметкой соответствующих чекбоксов. Для создания группы администратор должен нажать кнопку 

.

4.5.2 Редактирование группы

Для просмотра подробной информации о группе администратор должен нажать кнопку  . Подробная информация о группе представлена во вкладке «Информация о группе», показанной на рисунок 29.

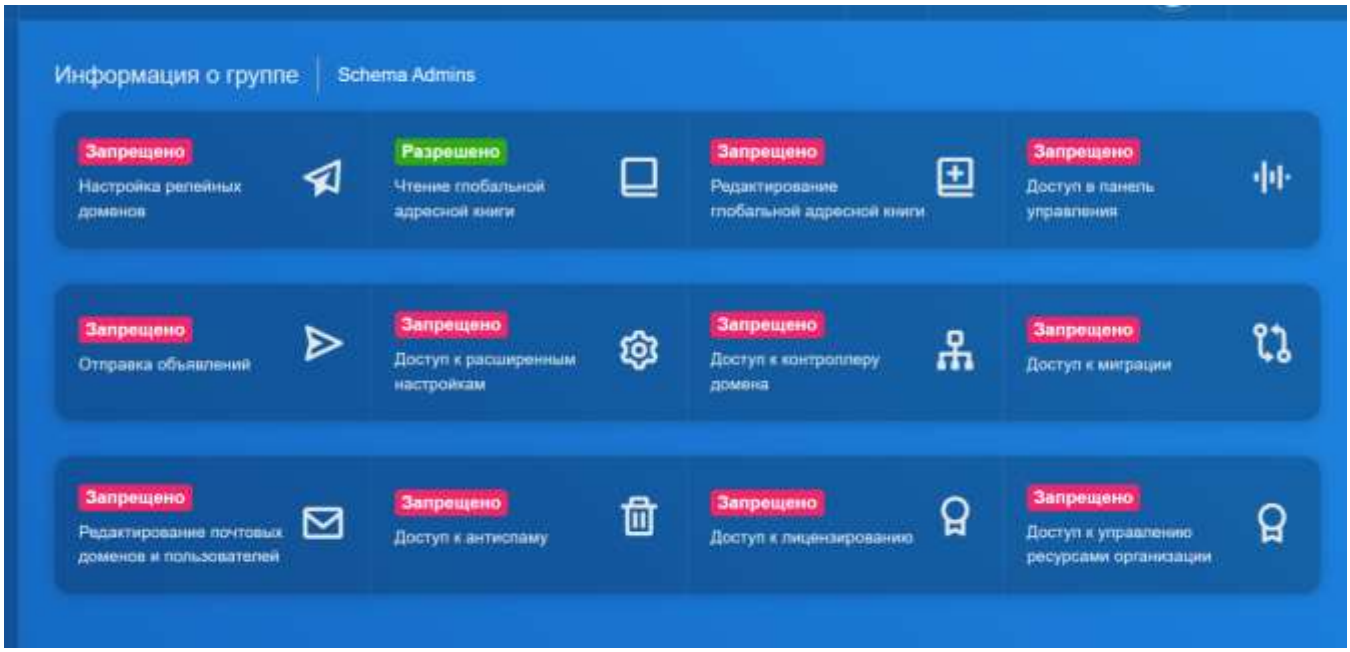


Рисунок 29 – Вкладка с подробной информацией о группе

Для просмотра и добавления пользователей в группу администратор должен найти панель этой группы (вкладка «Группы») и нажать кнопку  , открывающую форму «Список пользователей в группе», показанную на рисунке 30.

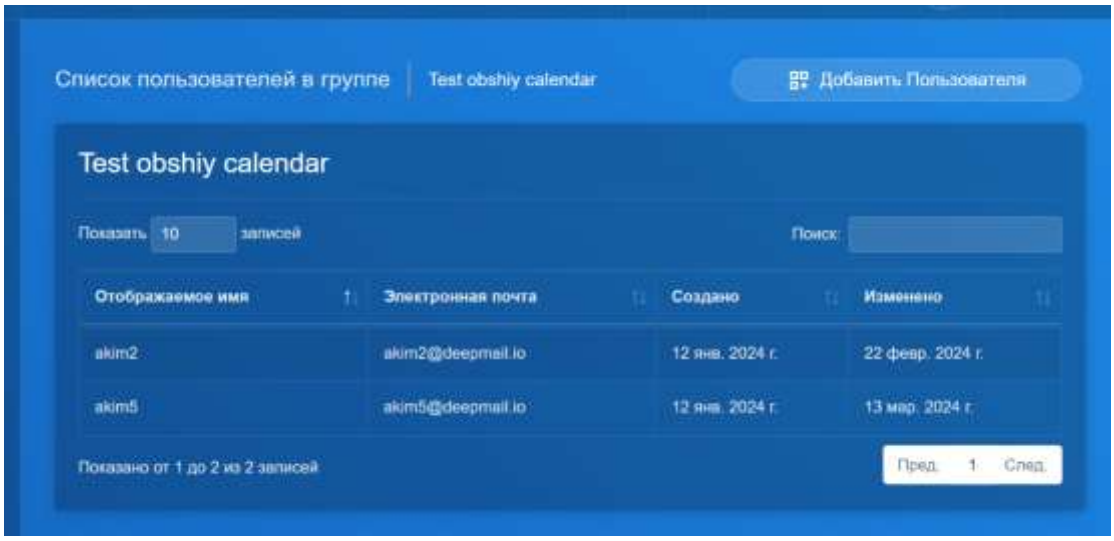


Рисунок 30 – Форма «Список пользователей в группе»

Для добавления пользователя в группу администратор должен нажать кнопку 

, открывающую форму «Добавить пользователя к группе» показанную на рисунке 29).

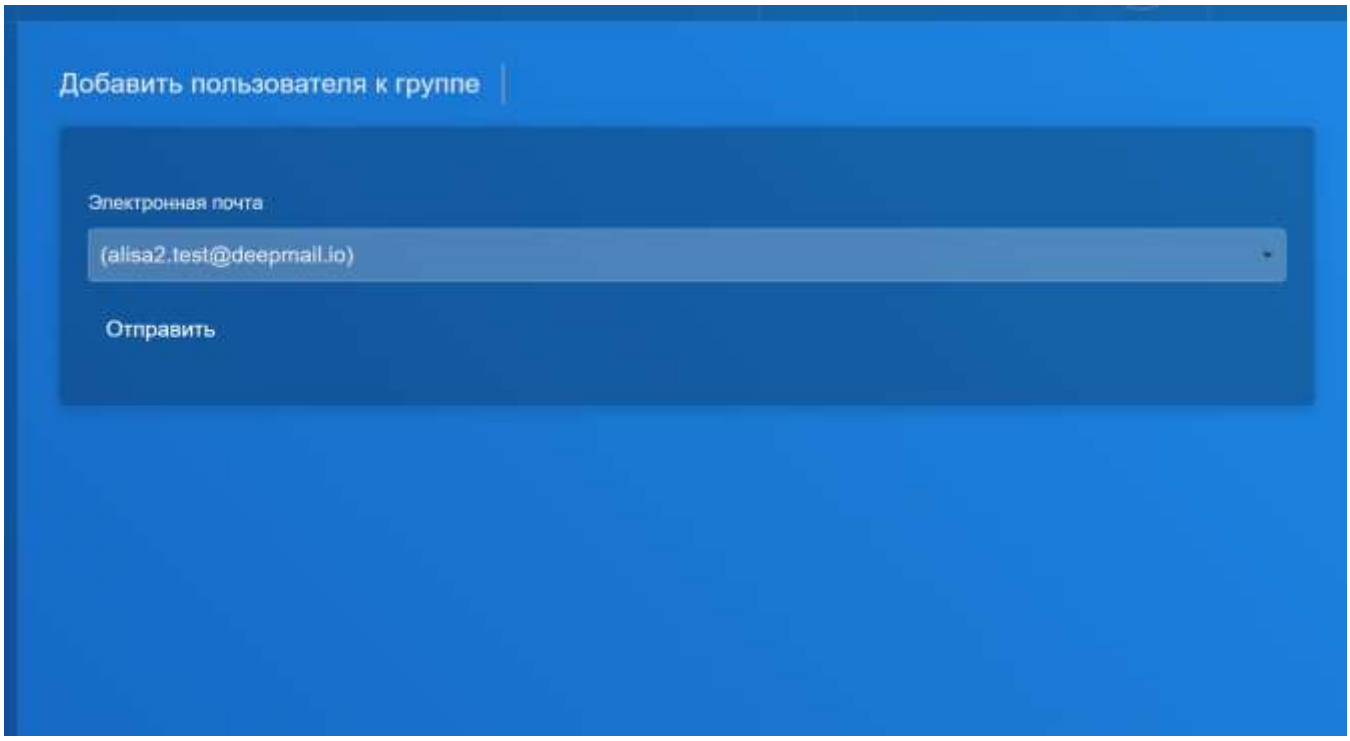


Рисунок 31 – Форма «Добавить пользователя к группе»

Администратор должен выбрать добавляемого пользователя из выпадающего списка (или начать вводить его адрес в поле) и нажать кнопку «Отправить».

Кнопка  позволяет переназначить права группе и открывает панель настройки прав группы, показанную ранее на рисунке 28.

4.5.3 Удаление группы

Для удаления группы администратор должен нажать кнопку  в строке группы и подтвердить удаление в следующем окне «Подтвердить действия».

4.6 Пункт вертикального меню «Ресурсы»

Управление ресурсами организации осуществляется во вкладке «Список ресурсов» (рисунок 33), для открытия которой необходимо выбрать пункт вертикального меню «Ресурсы» (рисунок 32).

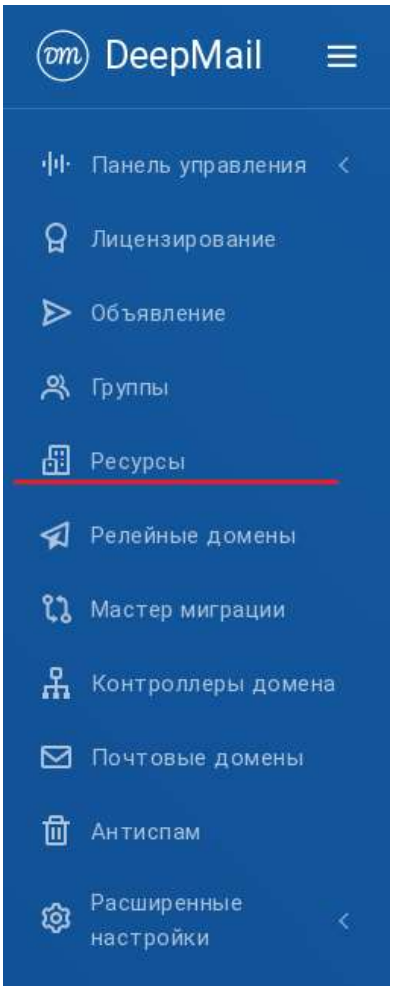


Рисунок 32 – Пункт вертикального меню «Ресурсы»

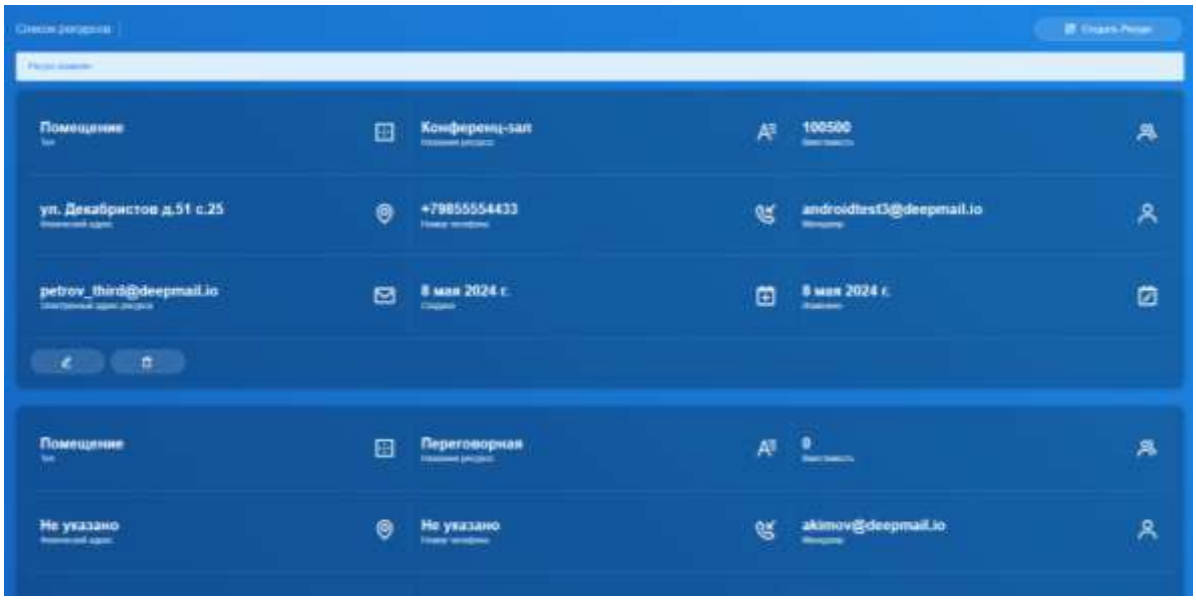


Рисунок 33 – Вкладка «Список ресурсов»

4.6.1 Создание нового ресурса

Для создания ресурса администратор должен нажать кнопку 

, после чего откроется форма «Создать ресурс», показанная на рисунке 34. При создании ресурса, есть возможность выбрать его тип «Транспорт» или «Помещение» из выпадающего меню в поле «Тип».

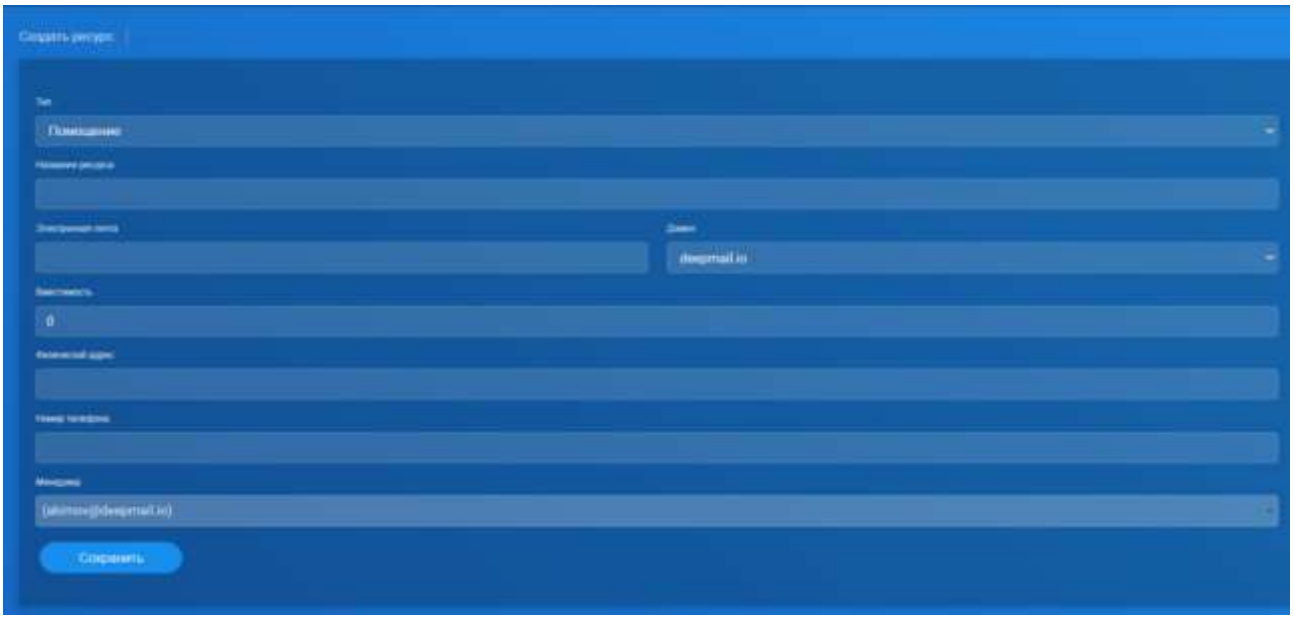
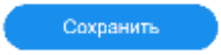


Рисунок 34 – Форма «Создать ресурс»

После заполнения всех полей администратор долен нажать кнопку 

. Созданный ресурс отобразится в списке ресурсов (рисунок 35), а также появится системное сообщение 

.

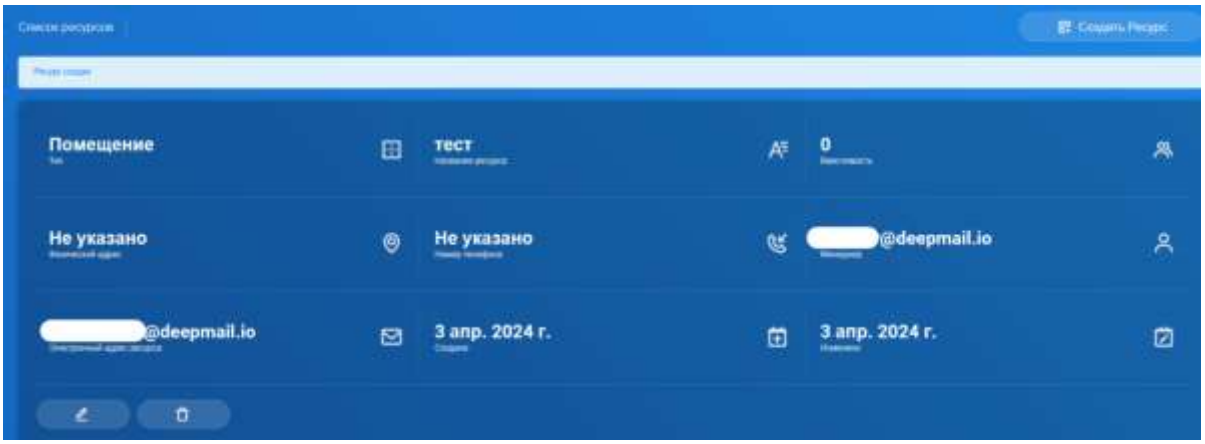


Рисунок 35 – Отображение ресурса на вкладке «Список ресурсов»

4.6.2 Редактирование ресурса

Для редактирования ресурса администратор должен нажать кнопку  , после чего откроется форма «Изменить ресурс» (рисунок 36), в которой можно изменить все данные, кроме поля «Электронная почта».

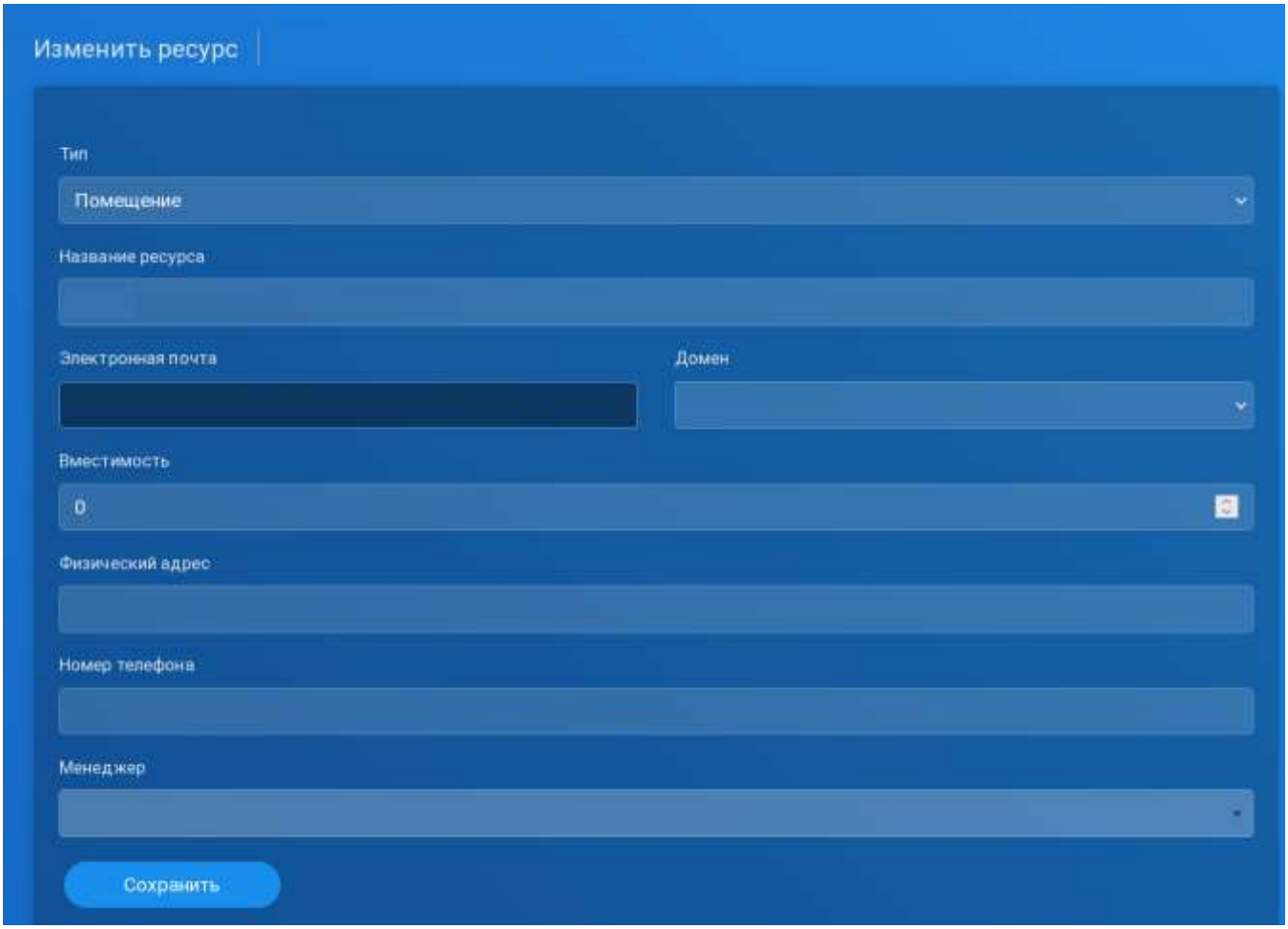


Рисунок 36 – Форма «Изменить ресурс»

4.6.3 Удаление ресурса

Для удаления ресурса администратор должен нажать кнопку  и подтвердить удаление в открывшейся форме «Подтвердить действие».

4.7 Пункт вертикального меню «Релейные домены»

Почтовый сервер DeepMail может отправлять все исходящие письма не напрямую, а через другой почтовый сервер. Настройка пересылки почты сервера (настройки релейного домена) описана ниже.

Для настройки пересылки почты через другой сервер администратор должен открыть пункт вертикального меню «Релейные домены» (рисунок 37).

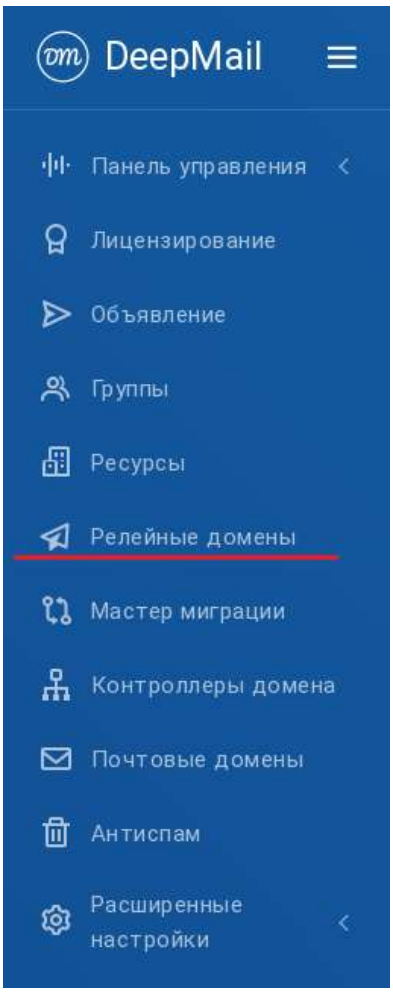


Рисунок 37 – Выбор вкладки «Релейные домены»

В открывшейся вкладке «Список релейных доменов» (рисунок 38) будет (при наличии) отображен список созданных релейных доменов.

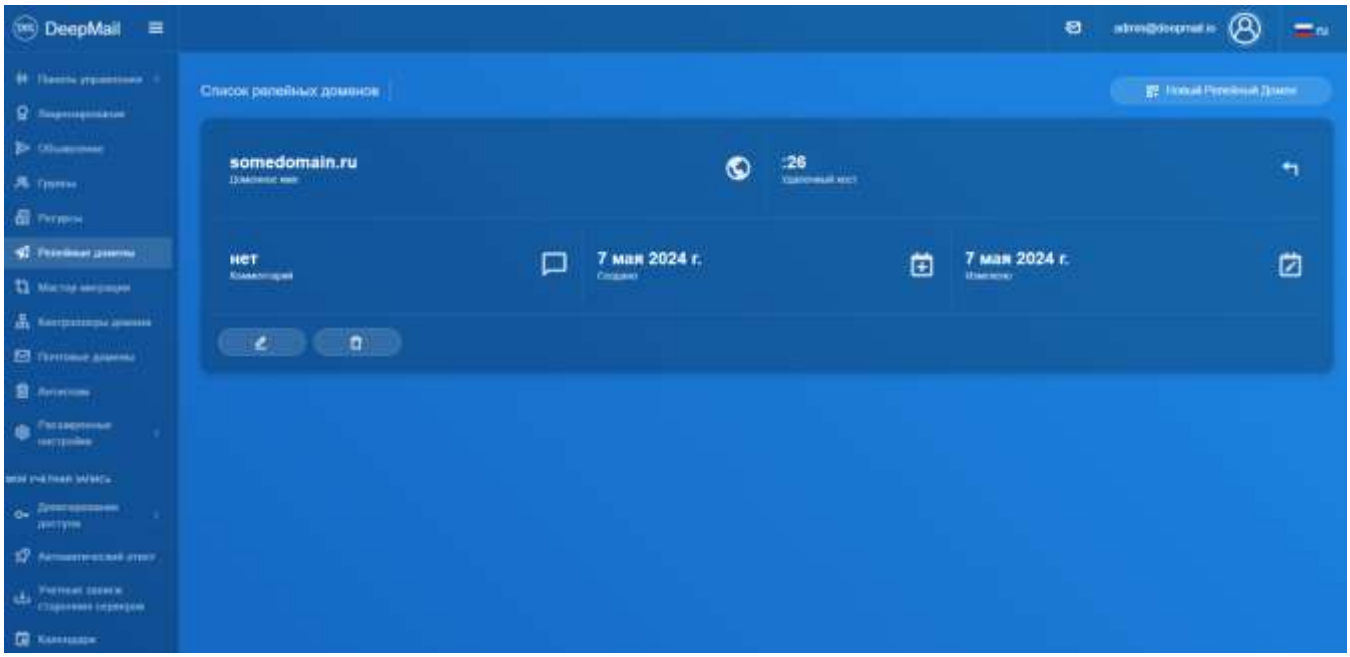


Рисунок 38 – Вкладка «Список релейных доменов»

4.7.1 Создание релейного домена

Рассмотрим пример переадресации почты с сервера, состоящего из нескольких нод с сервером балансировки, через релейный домен с единичной нодой.

Для этого необходимо на каждой ноде открыть для редактирования файл «/deepmail/deepmail.env» и ввести следующие строки:

RELAYHOST=<IP-адрес сервера-реле>:<smtp-порт>

RELAYNETS=< IP-адрес сервера-реле>/32

Сохранить изменения, выполнить перезагрузку сервера командой *«deepmail reload».*

Далее необходимо открыть для редактирования файл «/deepmail/deepmail.env» на релейном домене и ввести строки (необходимо указать IP-адреса всех нод через запятую) *RELAYNETS=<IP-адрес ноды 1>/32, <IP-адрес ноды 2>/32,*

Сохранить изменения, выполнить перезагрузку сервера командой *«deepmail reload».*

Далее необходимо зайти в веб-клиент сервера-реле под учетной записью администратора, выбрать пункт вертикального меню «Релейные домены», добавить

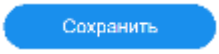
релейный домен через кнопку 

, после чего откроется форма создания нового релейного домена, показанная на рисунке 39.

Рисунок 39 – Форма «Новый релейный домен»

Во вкладке «Новый релейный домен» необходимо указать:

- «Имя релейного домена» – доменное имя исходного сервера;
- «Удаленный хост» – IP-адрес HAProxy исходного сервера;

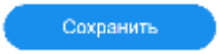
После ввода необходимых параметров необходим нажать кнопку 

.

4.7.2 Редактирование релейного домена

Для редактирования релейного домена администратор должен нажать кнопку 
, после чего откроется форма «Изменить релейный домен» (рисунок 40).

Рисунок 40 – Форма «Изменить релейный домен»

После ввода необходимых параметров необходим нажать кнопку 

.

4.7.3 Удаление релейного домена

Для удаления релейного домена администратор должен нажать кнопку  и подтвердить удаление в открывшейся форме «Подтвердить действие».

4.8 Пункт вертикального меню «Мастер миграции»

Настройка миграции со сторонних серверов происходит во вкладке «Мастер миграции», выбор которой показан на рисунке 41.

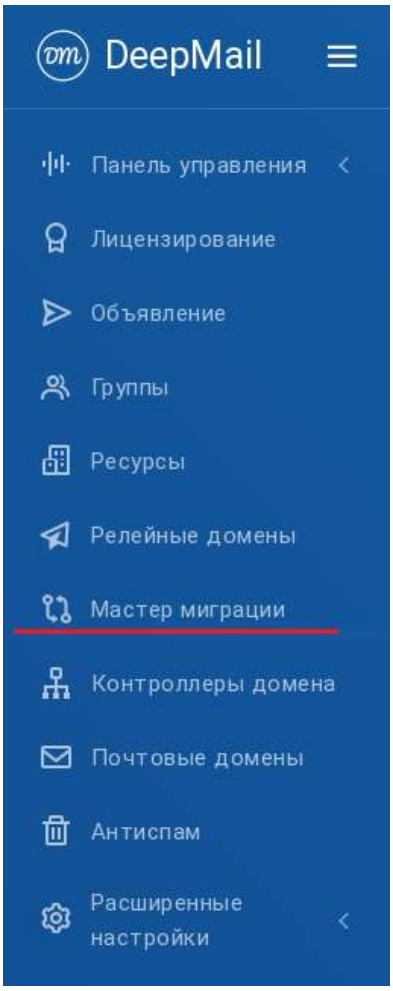


Рисунок 41 – Пункт вертикального меню «Мастер миграции»

В открывшейся вкладке «Мастер миграции» отображается список подключенных к серверу DeepMail сторонних доменов (рисунок 42).

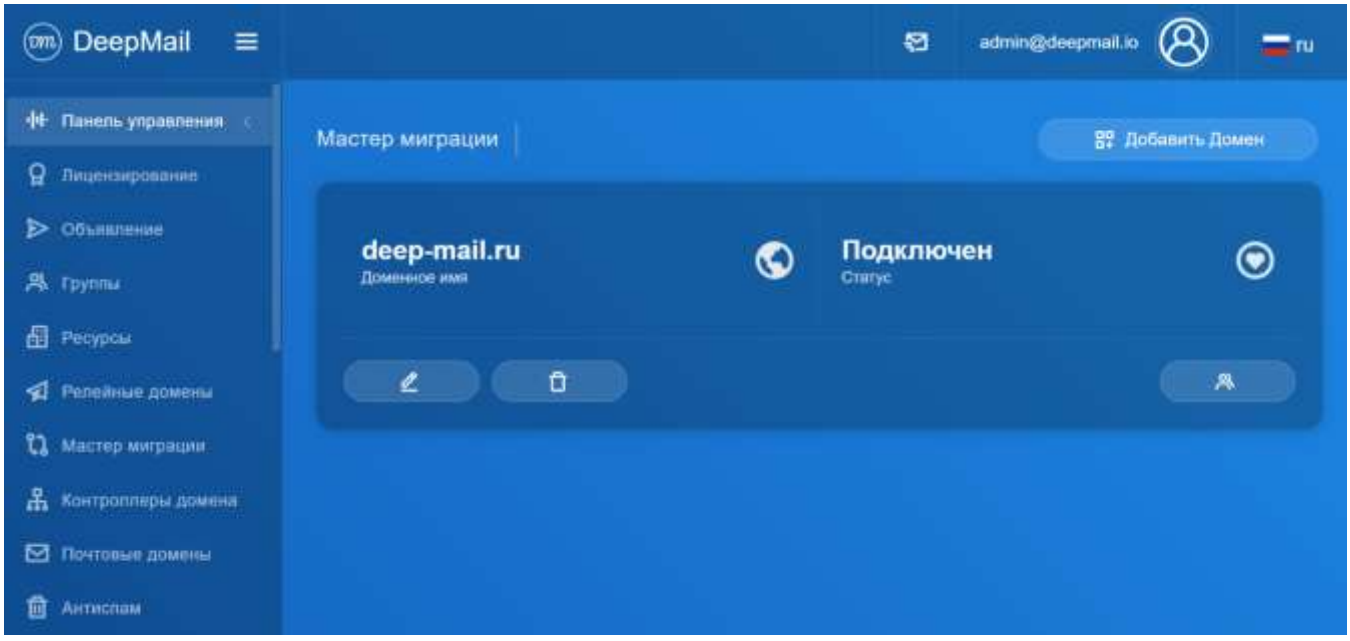


Рисунок 42 – Вкладка «Мастер миграции» со списком подключенных доменов

Для изменения настроек миграции администратор должен нажать кнопку  на панели конкретного домена, в результате чего откроется форма «Изменить домен для миграции». Для просмотра списка пользователей, аккаунты которых мигрируют с предыдущего домена, администратор должен нажать кнопку  , после чего откроется вкладка «Список пользователей для миграции» (рисунок 43).

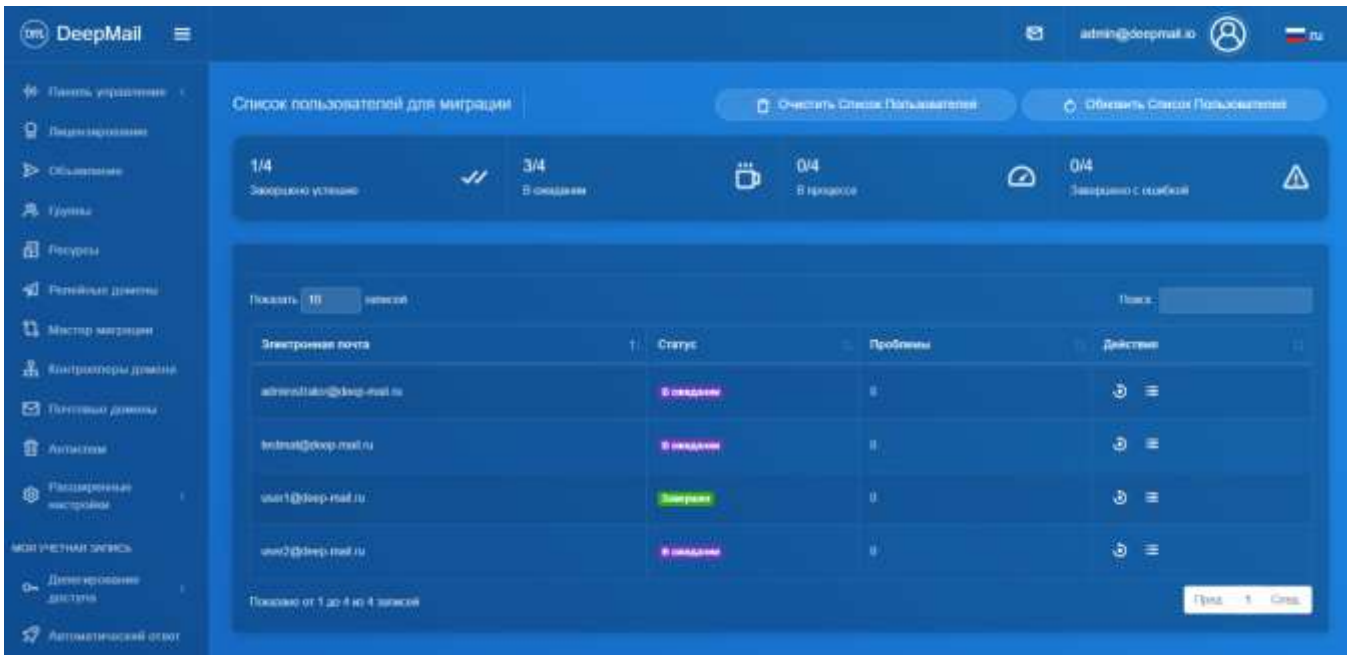


Рисунок 43 – Пользователи домена для миграции

В верхней части формы находится статистика по миграции для пользователей домена. Миграция аккаунтов пользователей может иметь следующие статусы:

- «В ожидании» – сервер ожидает первой авторизации пользователя, чтобы получить его пароль для авторизации на предыдущем сервере;
- «В процессе» – процесс передачи файлов пользователя с предыдущего сервера еще не завершен.
- «Завершено успешно» – миграция завершена;
- «Завершено с ошибкой» – во время миграции пользователя возникла ошибка, содержание которой можно увидеть в файле лога MigrationMaster.log, архив с которыми необходимо предварительно скачать в панели управления.

В списке пользователей для миграции домена (рисунок 44) в строке каждого пользователя находится кнопка перезапуска миграции и кнопка просмотра логов миграции пользователя.

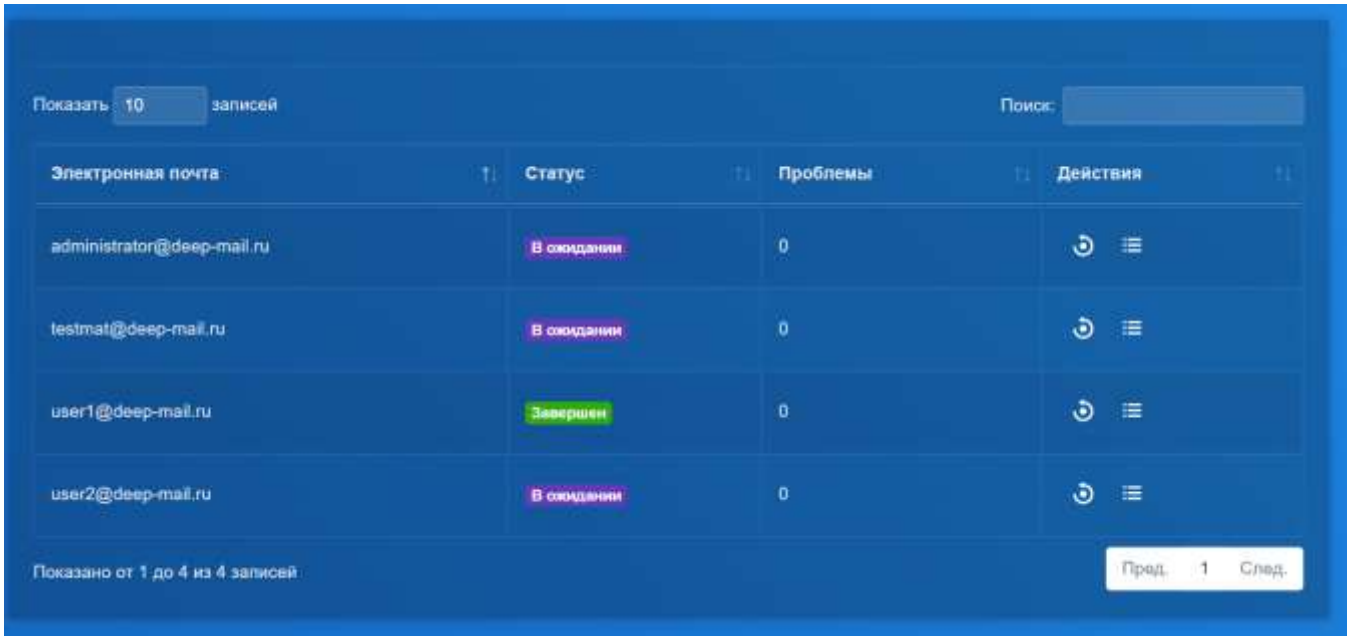


Рисунок 44 – Список пользователей домена для миграции

При значительном количестве пользователей администратор может воспользоваться полем поискового запроса над таблицей. Обновить информацию о статусе миграции всех пользователей домена администратор может с помощью кнопки Обновить Список Пользователей над списком пользователей. Кнопка Очистить Список Пользователей удаляет всех пользователей из списка.

4.8.1 Создание настроек миграции и подключение к IMAP-серверу стороннего домена

Для добавления домена, с которого будет осуществлена миграция, администратор должен нажать кнопку Добавить Домен, после чего откроется форма настройки миграции, показанная на рисунке 45.

Если сервером, с которого будет осуществляться миграция, является Microsoft Exchange, то включите на нем возможность работы по IMAP

(https://learn.microsoft.com/ru-ru/exchange/clients/pop3-and-imap4/configure-imap4?view=exchserver-2019).

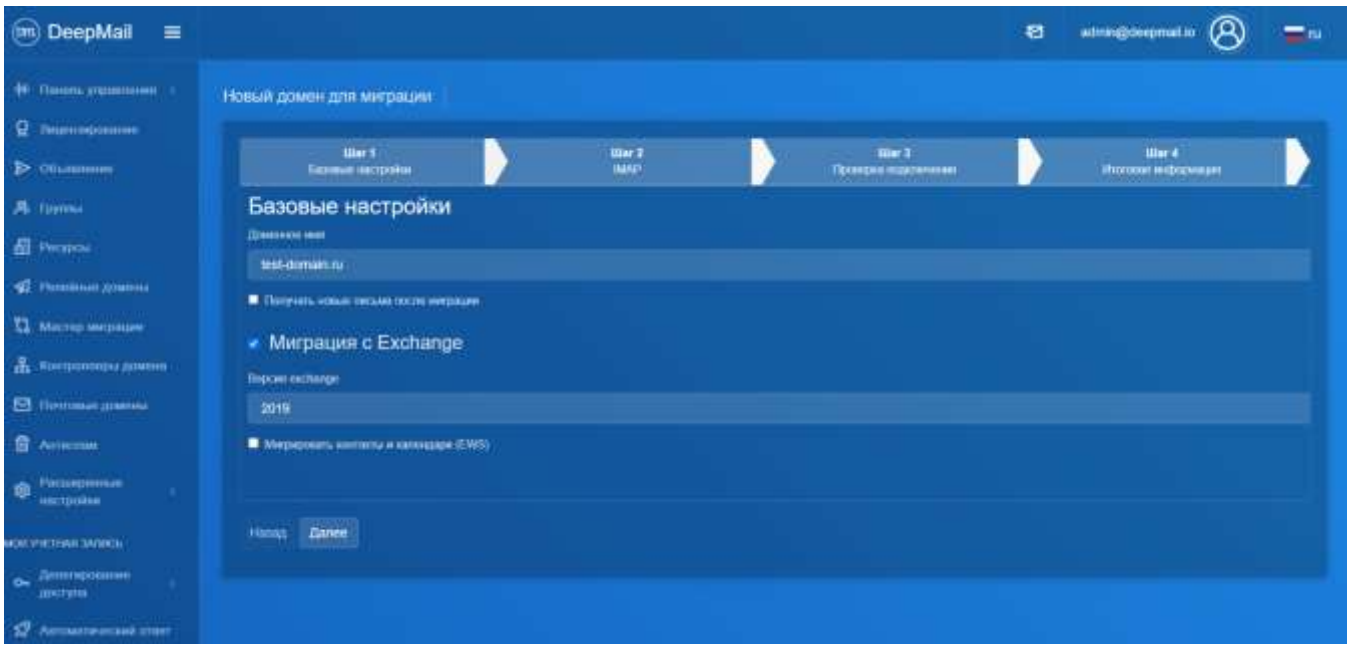


Рисунок 45 – Настройка миграции. Шаг «Базовые настройки»

Настройка миграции состоит из четырех шагов:

- базовые настройки;
- настройка и подключение к серверу по IMAP;
- подключение к серверу по IMAP;
- итоговая информация.

На шаге «Базовые настройки» администратор должен выбрать почтовый (домен из списка уже подключенных), с которого будет происходить миграция.

При включении опции «Получать письма после миграции» после окончания миграции почтового аккаунта пользователя, будет создан объект «fetchmail», который будет забирать входящие письма с предыдущего сервера.

При включении опции «Миграция с Exchange» будет учитываться, что миграция почты по IMAP-протоколу будет производится с Exchange Server, а также будет доступен выбор версии Exchange Server, с которого производится миграция. (рисунок 46).

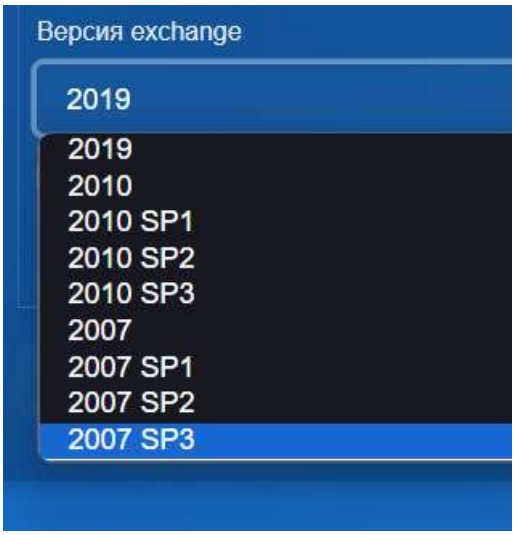


Рисунок 46 – Выбор версии сервера MS Exchange

При включении опции «Мигрировать контакты и календари (EWS)» перед началом миграции почты будет выполнена миграция контактов, календарей и их содержимого.

На следующем шаге «IMAP» (рисунок 47) администратору необходимо указать IP-адрес удаленного IMAP-сервера и порт подключения. При необходимости можно воспользоваться опцией «Использовать SSL».

Рисунок 47 – Настройка миграции. Шаг «IMAP»

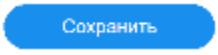
Удаленный хост также может быть размещен по адресу IPv4 или IPv6 (адрес IPv6 должен быть заключен в квадратные скобки: [2001:D88: :]).

На следующем шаге «Проверка подключения» отобразится статус подключения по протоколу IMAP (рисунок 48).

Рисунок 48 – Проверка подключения к IMAP-серверу

На финальном шаге «Итоговая информация» отобразится информация с числом пользователей для миграции (рисунок 49).

Рисунок 49 – Шаг «Итоговая информация»

Кнопка  сохраняет изменения настроек.

4.8.2 Удаление настроек миграции для домена

Удаление настроек миграции для домена происходит после нажатия на кнопку  и подтвердить удаление в открывшейся форме «Подтвердить действие».

4.9 Пункт вертикального меню «Контроллеры домена»

Подключение контроллеров домена осуществляется через пункт вертикального меню «Контроллеры домена» (рисунок 50).

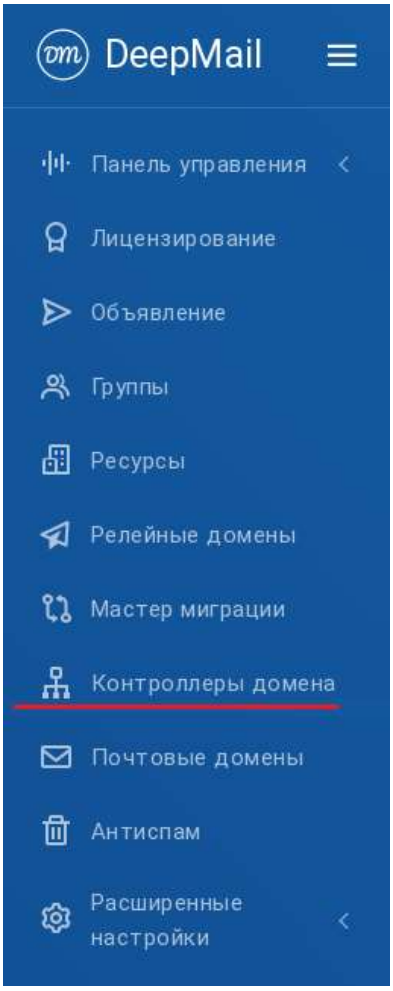


Рисунок 50 – Пункт вертикального меню «Контроллеры домена»

В открывшейся вкладке «Контроллеры домена» доступно подключение следующих контроллеров домена: Samba DC, MS AD, ALD Pro, OpenLDAP. Выбрав необходимый пункт меню, отобразится список подключенных контроллеров домена (рисунок 51).

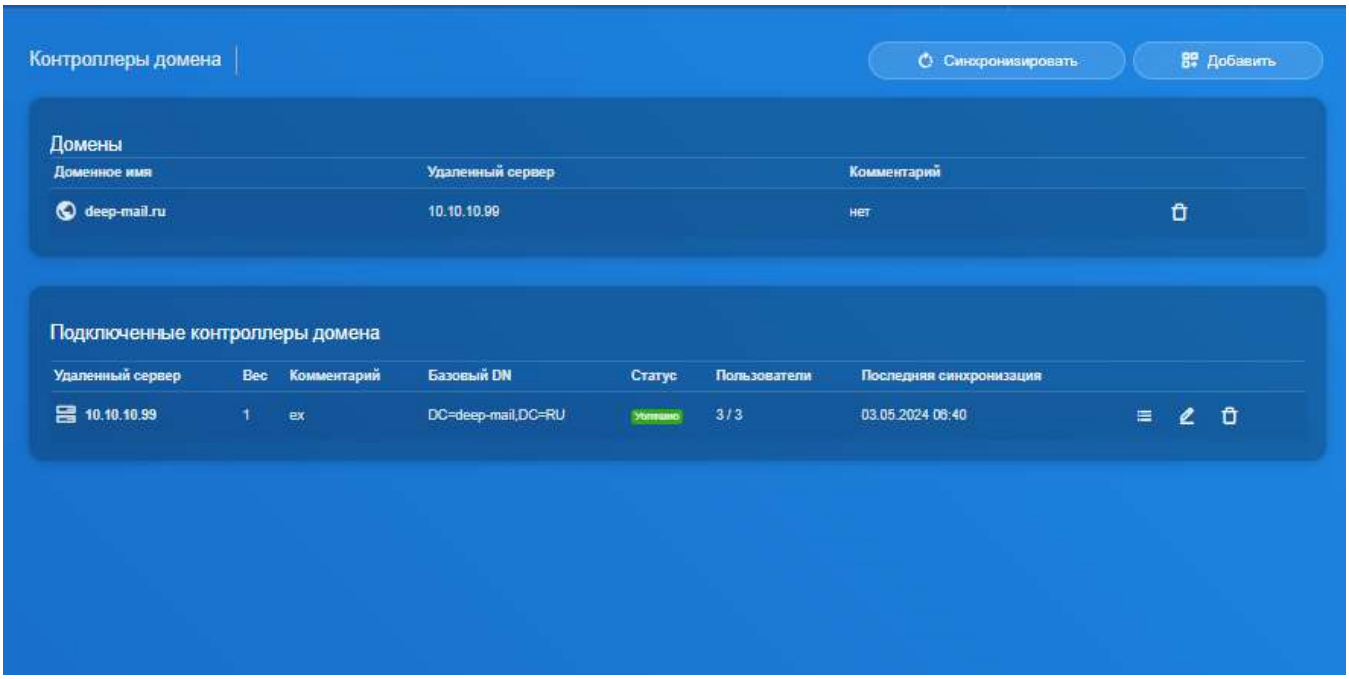


Рисунок 51 – Вкладка «Контроллеры домена»

4.9.1 Добавление контроллера домена

Для добавления контроллера домена необходимо нажать кнопку 

в правом верхнем углу, после чего откроется форма «Добавить контроллер домена» (рисунок 52).

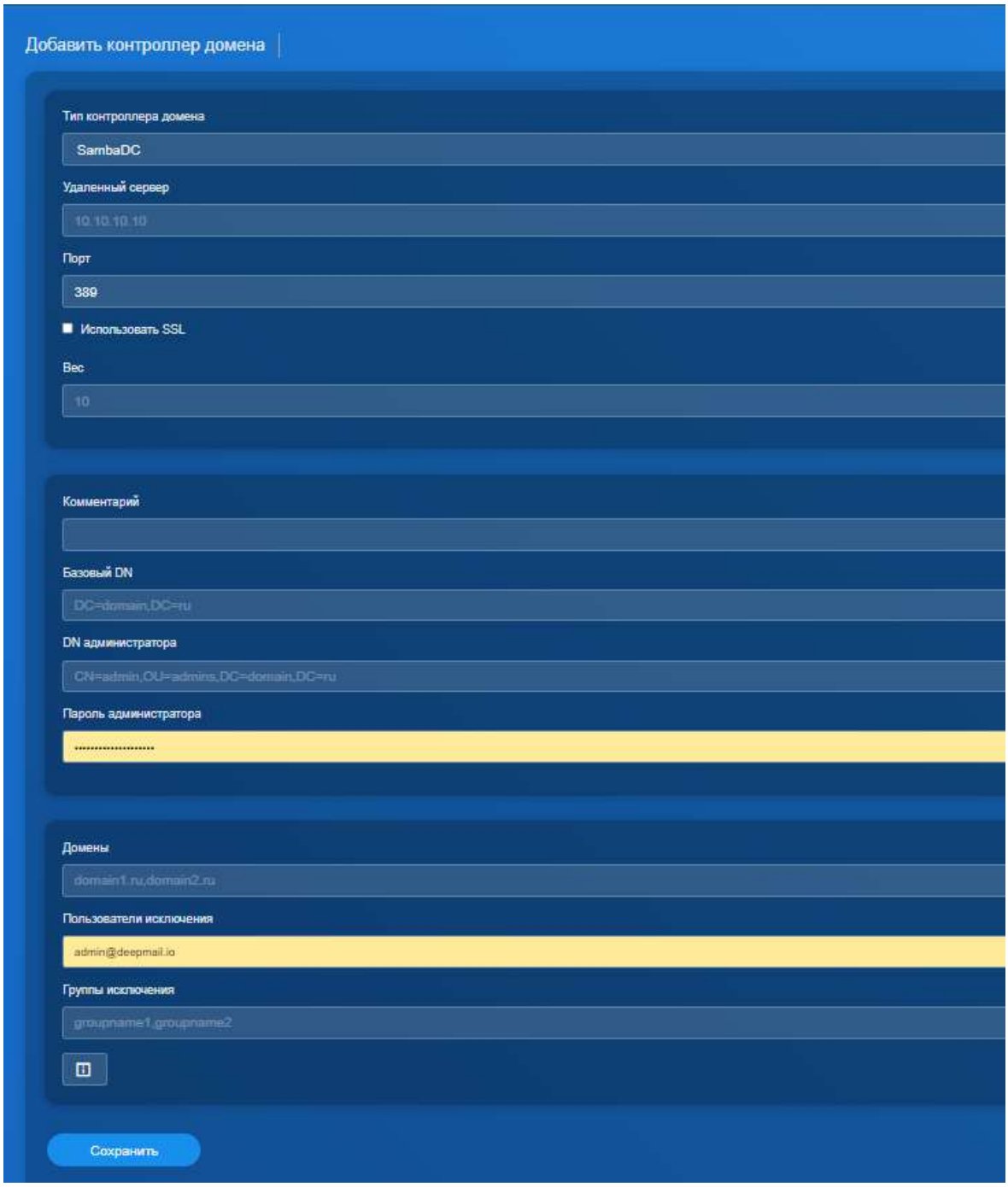


Рисунок 52 – Настройка подключения контроллера домена

Далее администратор должен выбрать тип подключаемого контроллера домена из предложенных (рисунок 53).

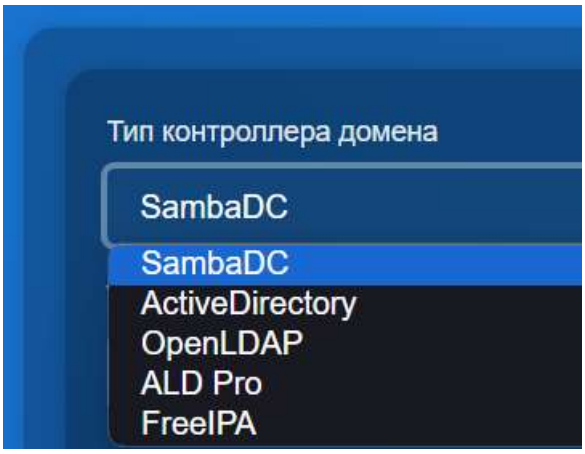


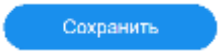
Рисунок 53 – Выбор типа контроллера домена

После выбора типа контроллера домена необходимо заполнить параметры контроллера домена:

- IP-адрес контроллера домена в поле «Удаленный сервер»;
- порт подключения в поле «Порт»;
- ввести необходимые поля LDIF для базового доменного имени (Базовый DN) и администратора (DN администратора);
- ввести пароль администратора удаленного домена;
- ввести поддомены в поле «Домены»;
- ввести группы-исключения и пользователей –исключения в поле «Группы исключения».

Примечание. Пользователи из групп-исключений все равно будут добавлены, но как пользователи без группы.

При заполнении данных важно правильно указать вес. Вес указывает приоритет контроллера домена. Система будет обращаться сначала к контролеру домена с наименьшим весом, в случае невозможности подключится к основному контроллеру домена, система обратится к следующему контроллеру домена с наименьшим весом и так далее.

После настроек подключения необходимо нажать кнопку 

.

4.9.2 Синхронизация контроллеров домена

Как правило синхронизация данных с контроллером домена происходит по расписанию со значительными интервалами. Для того, чтобы оперативно получить актуальные данные с подключенных доменов администратор должен нажать кнопку 

(рисунок 54).

Подключенные домены должны отображаться в панели «Домены», а подключенные контроллеры доменов в панели «Подключенные контроллеры домена» (рисунок 54).

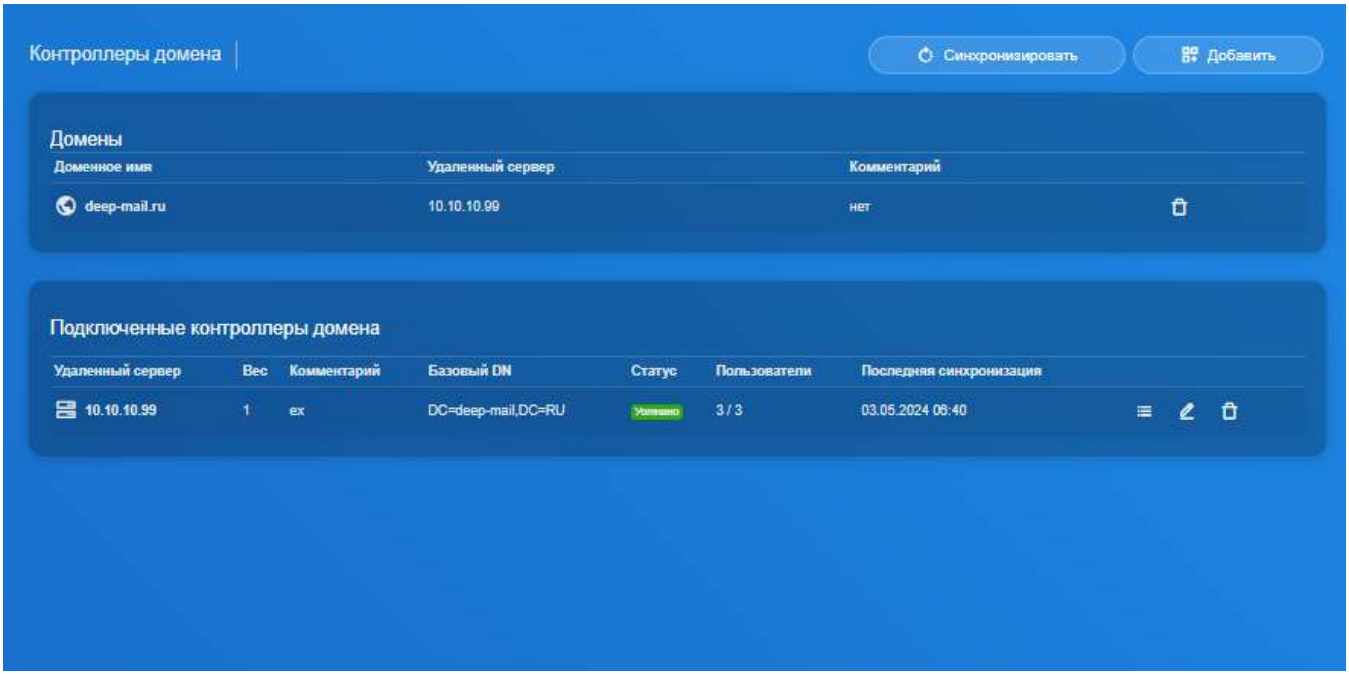


Рисунок 54 – Отображение подключенных доменов

При подключении контроллера домена он должен иметь статус «В очереди», затем статус изменится на «Подключение» или «Синхронизация». Если авторизация пройдена, подключение выполнено, домен получит статус «Успешно». В случае если подключение выполнить не удалось домен получит статус «Ошибка».

При подключении к контроллеру домена передаются имена пользователей, их принадлежность к группам и почтовые ящики. Почтовые ящики пользователей должны автоматически появиться во вкладке «Почтовые домены», работа с которой представлена далее в пункте 4.10.

Подробную информацию о процессе подключении домена и о передаче данных можно посмотреть, нажав кнопку просмотра логов .

Для изменения настроек подключения администратор может нажать кнопку .

4.9.3 Удаление контроллера домена

Удаление контроллера домена происходит после нажатия на кнопку и подтвердить удаление в открывшейся форме «Подтвердить действие».

4.10 Пункт вертикального меню «Почтовые домены»

Настройка почтовых доменов происходит во вкладке «Список доменов», вызов которой происходит из вертикального меню «Почтовые домены» (рисунок 55).

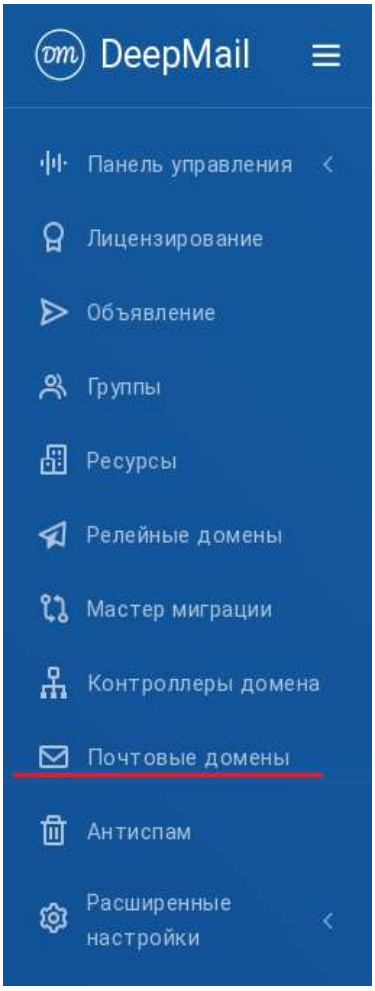


Рисунок 55 – Пункт вертикального меню «Почтовые домены»

На открывшейся вкладке отобразится список почтовых доменов, обслуживаемых сервером (рисунок 56).

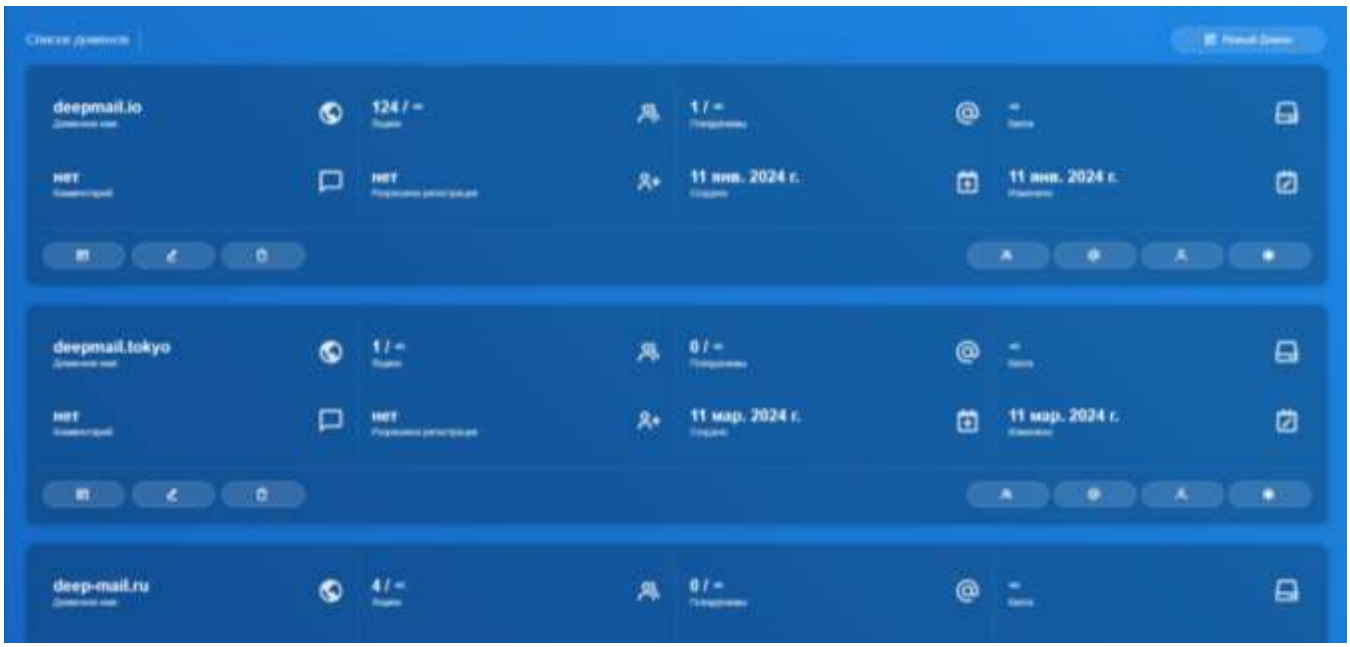
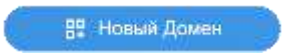


Рисунок 56 – Вкладка «Список доменов»

После установки должен отображаться почтовый домен с доменным именем, введенным при установке – корневой почтовый домен.

4.10.1 Почтовые домены

4.10.1.1 Добавление нового почтового домена

Для добавления нового почтового домена администратору необходимо нажать кнопку 

, открывающую форму «Новый домен», показанную на рисунке 57.

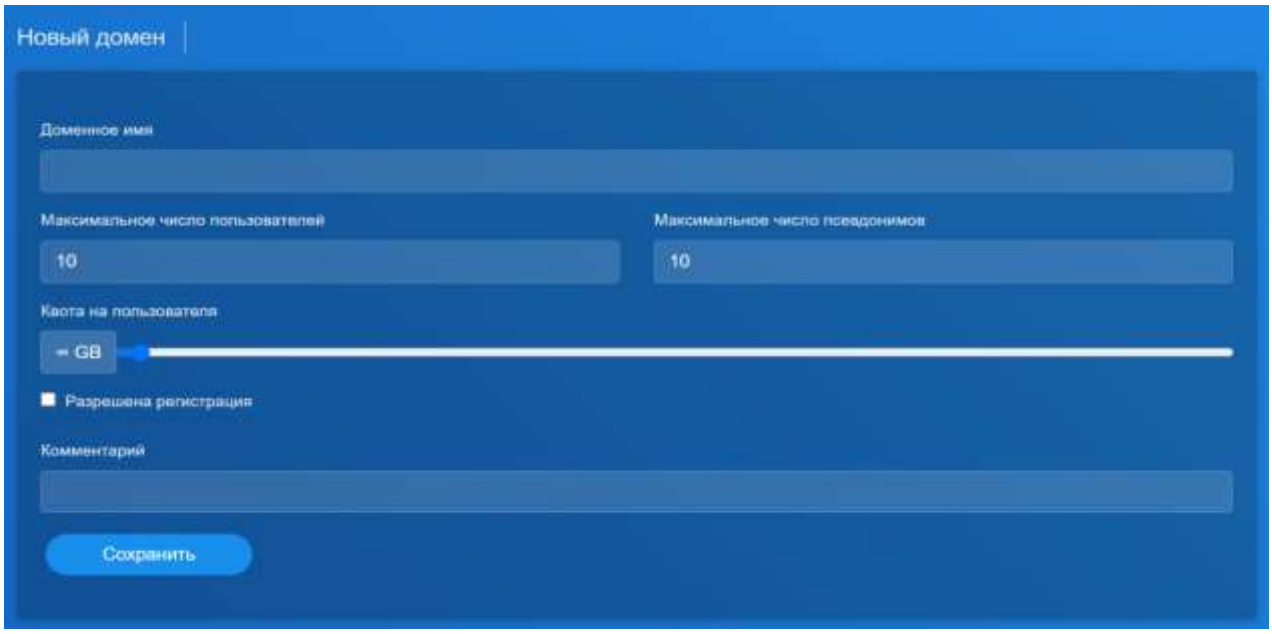


Рисунок 57 – Вкладка «Новый домен»

В открывшейся форме «Новый домен» администратор должен ввести основные параметры нового почтового домена, такие как «Доменное имя», «Максимальное число пользователей», «Максимальное число псевдонимов», а также выделить Квоту памяти на каждого пользователя в графе «Квота на пользователя» и определить опцию «Разрешена регистрация». Заполнив основные параметры необходимо нажать кнопку Сохранить. После этого появится сообщение Домен сохранен deepmail.to, а новый домен отобразится в списке почтовых доменов.

4.10.1.2 Изменение почтового домена.

Кнопка на панели выбранного почтового домена открывает форму «Изменить домен» (рисунок 58). Для внесения изменений администратор должен нажать кнопку Сохранить. После этого появится сообщение Домен сохранен deepmail.to, а внесенные изменения отобразятся на панели почтового домена.

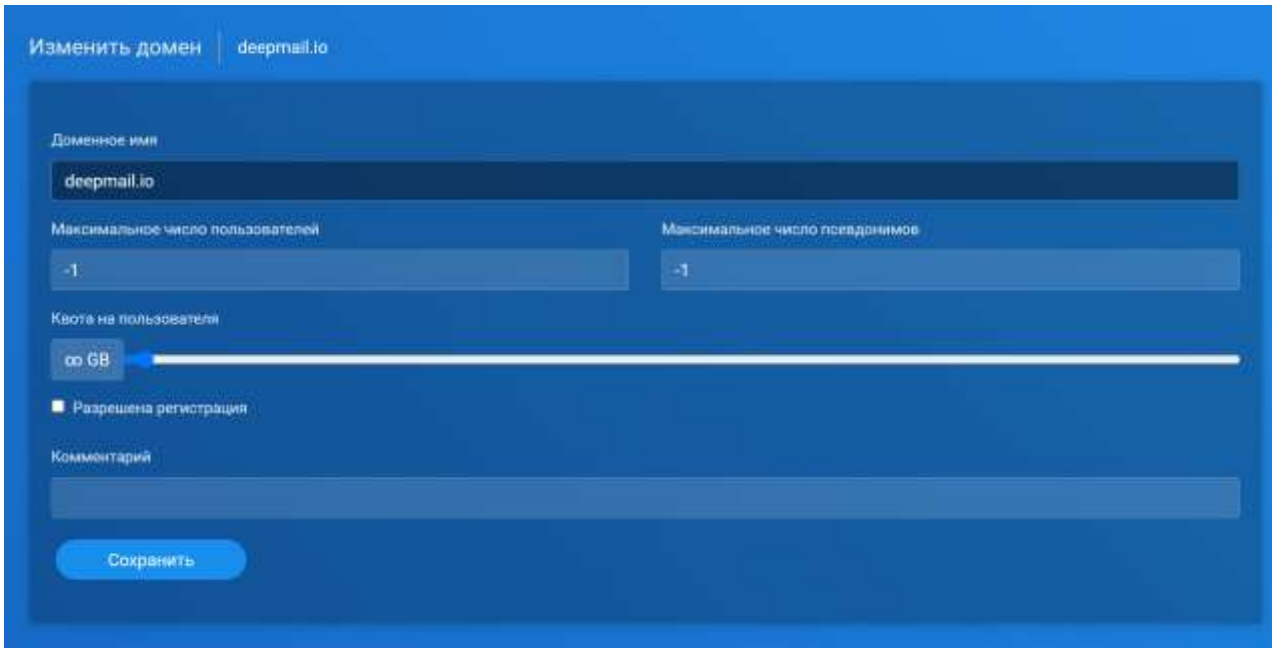


Рисунок 58 – Форма «Изменить домен»

4.10.1.3 Удаление почтового домена

Для удаления почтового домена администратор должен нажать кнопку  в панели этого домена (рисунок 59) и подтвердить удаление в открывшейся форме «Подтвердить действие».

Рисунок 59 – Кнопка «Удалить» на панели домена

4.10.2 Управление пользователями домена

Управление пользователями осуществляется в пределах одного почтового домена. Администратор может добавлять, удалять и блокировать пользователей, назначать размер их почтовых ящиков, добавлять их в группы и удалять из групп.

Для вызова формы управления пользователями домена администратор должен кнопку  на панели домена (рисунок 60).

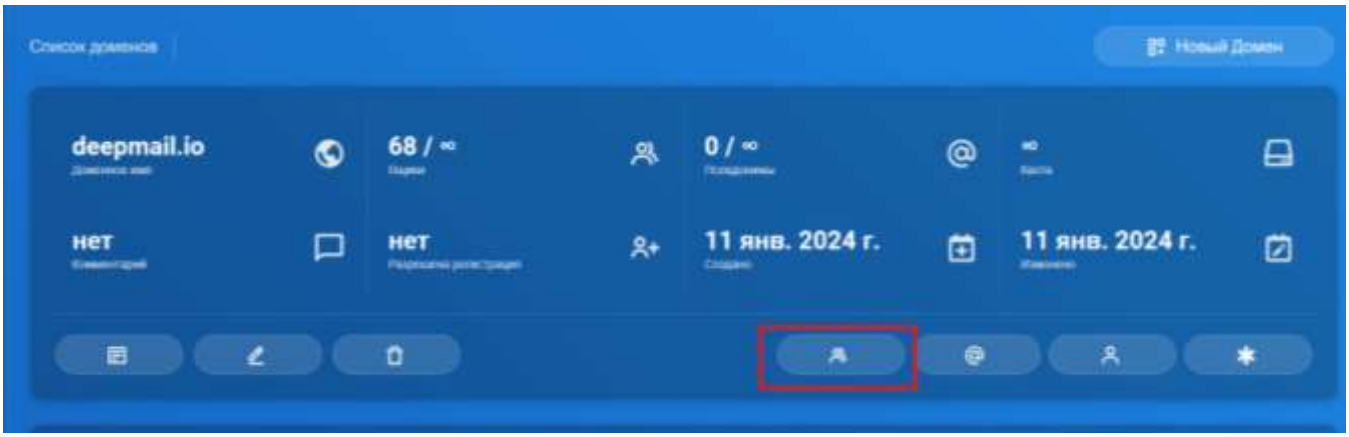


Рисунок 60 – Кнопка «Пользователи»

Открывшийся список пользователей домена показан на рисунке 61.

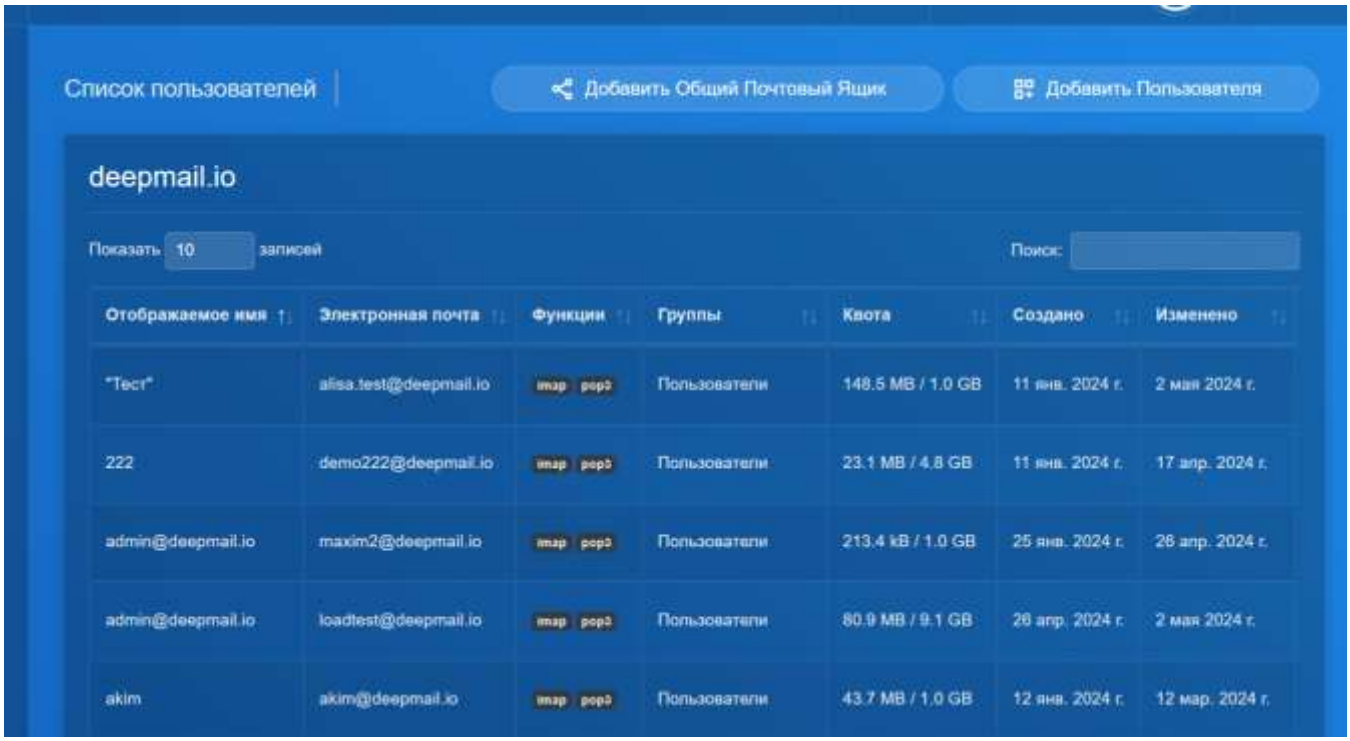


Рисунок 61 – Вкладка «Список пользователей»

В таблице представлена информация по всем пользователям домена, в том числе размер почтовых ящиков и размер занятой памяти в них.

4.10.2.1 Создание нового пользователя почтового домена

Для создания нового пользователя почтового домена администратор должен нажать кнопку 

, после чего откроется форма добавления нового пользователя (рисунок 62).

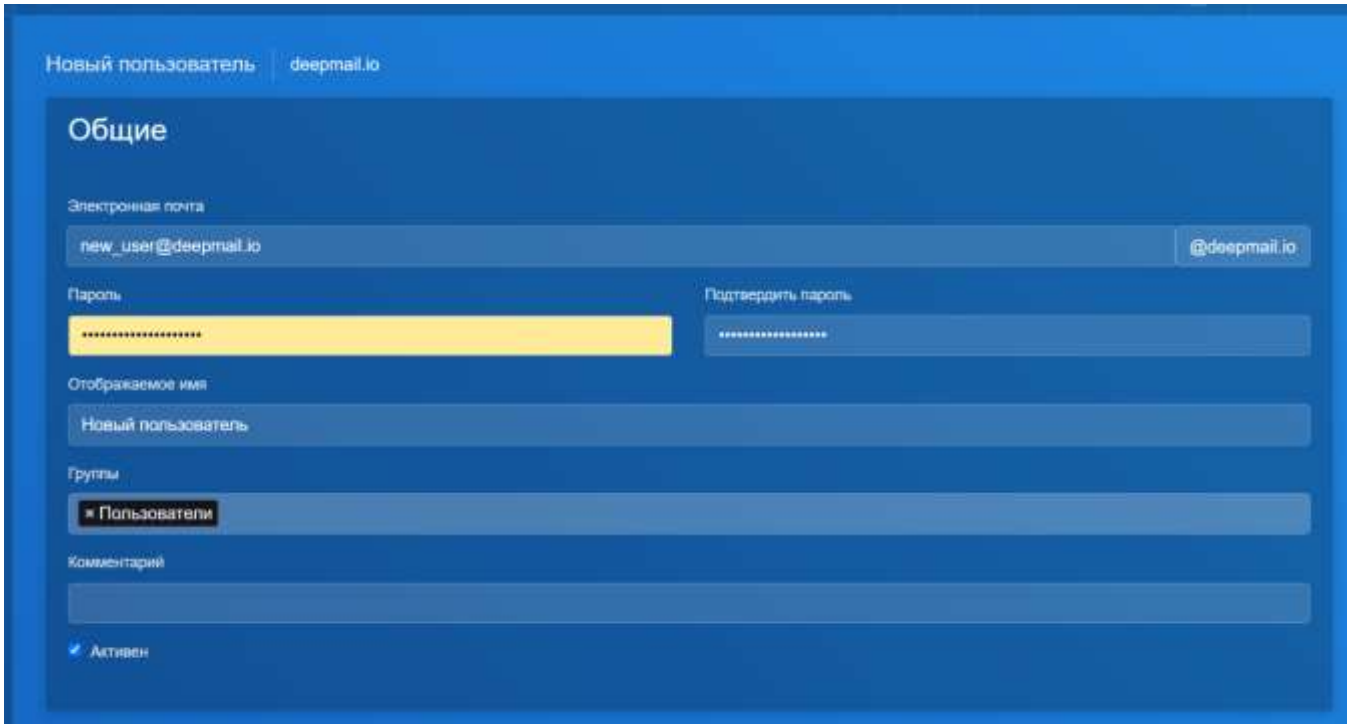
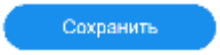


Рис. 62 – Форма «Новый пользователь»

В ней администратор должен ввести имя почтового ящика нового пользователя, пароль и, при необходимости, добавить группу или группы.

Далее администратор должен выбрать допускаемые протокол доступа пользователя к почте (POP3 или IMAP) и назначить квоту памяти на почтовый ящик (рисунок 63) и нажать кнопку 

.

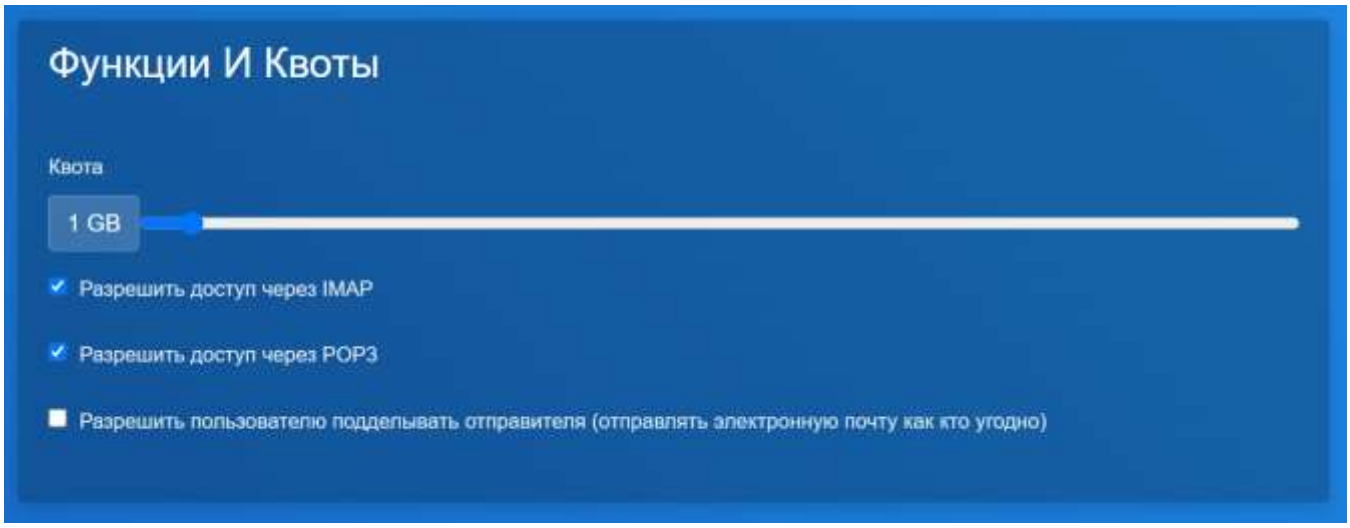


Рисунок 63 – Настройка квоты памяти и почтовых протоколов для пользователя

4.10.2.2 Редактирование пользователя

Для изменения настроек учетной записи пользователя почтового домена администратор должен нажать кнопку  в таблице пользователей. При этом откроется форма «Изменить пользователя» (рисунок 64). Администратор может менять те же параметры, что и при создании пользователя, кроме электронного адреса почты.

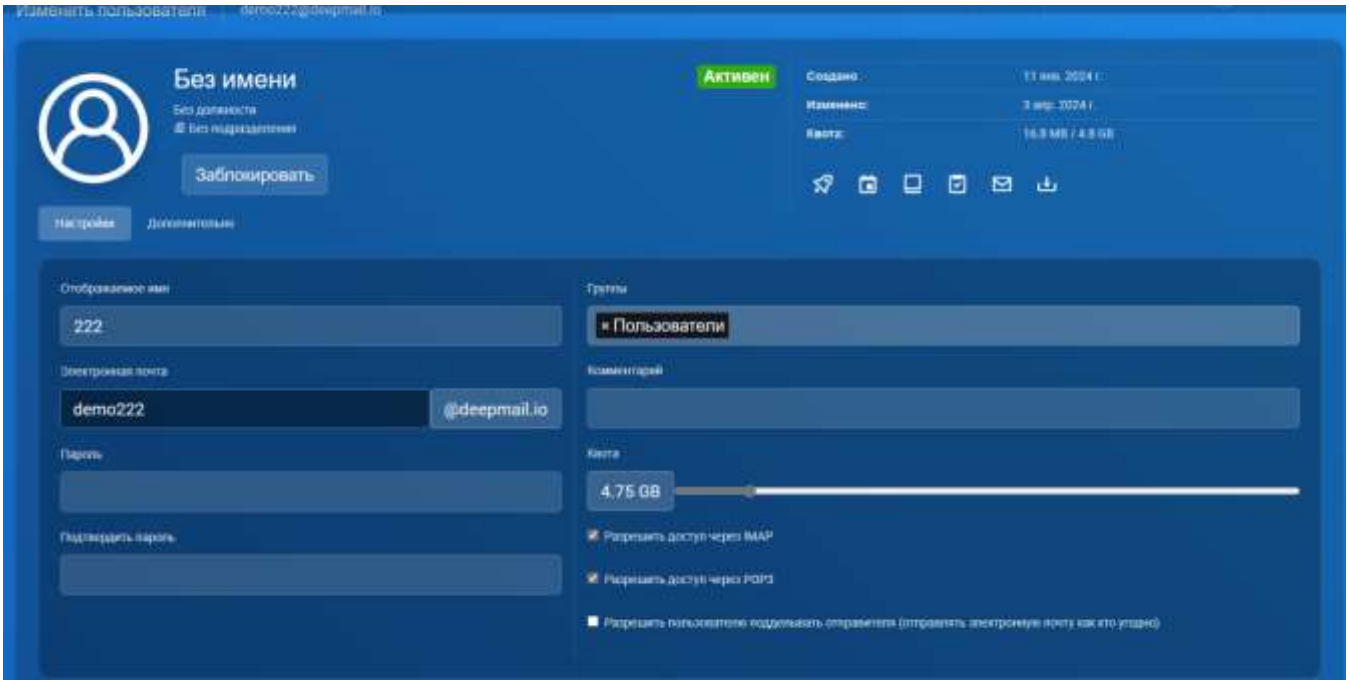


Рисунок 64 – Форма «Изменить пользователя»

На вкладке «Дополнительно» (рисунок 65) настраивается спам фильтр и переадресация писем.

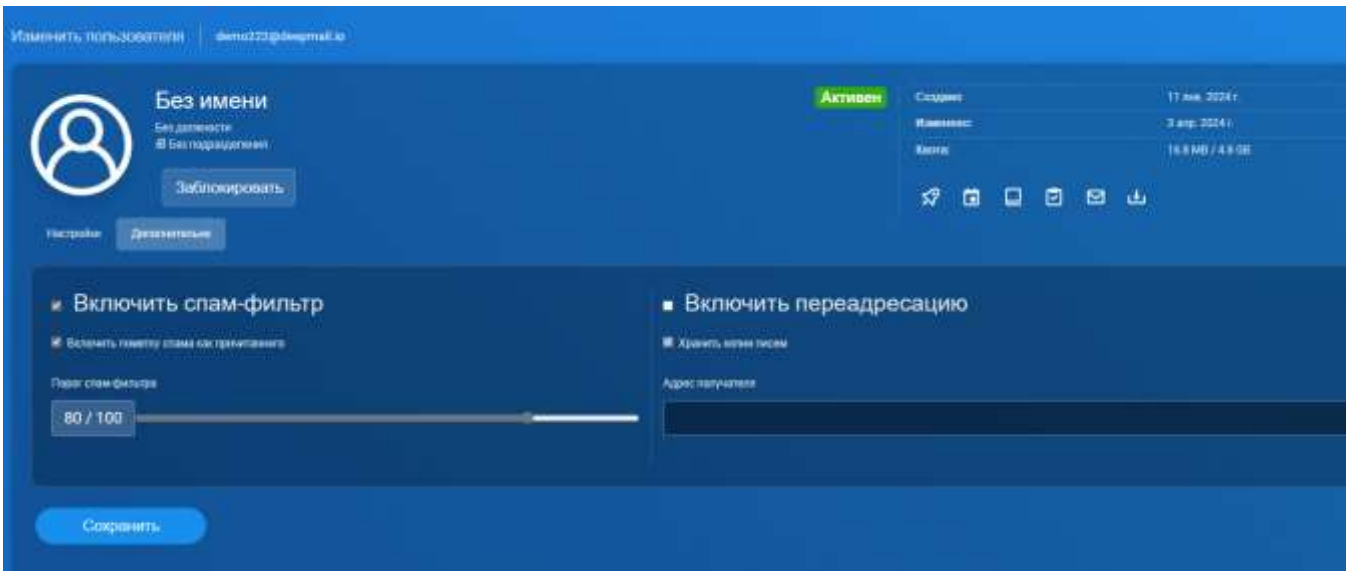


Рисунок 65 – Вкладка дополнительных настроек пользователя

Для пользователей, подключенных через LDAP, при их редактировании, с правой стороны будут отображаться данные этого подключения и адрес сервера (рисунок 66).

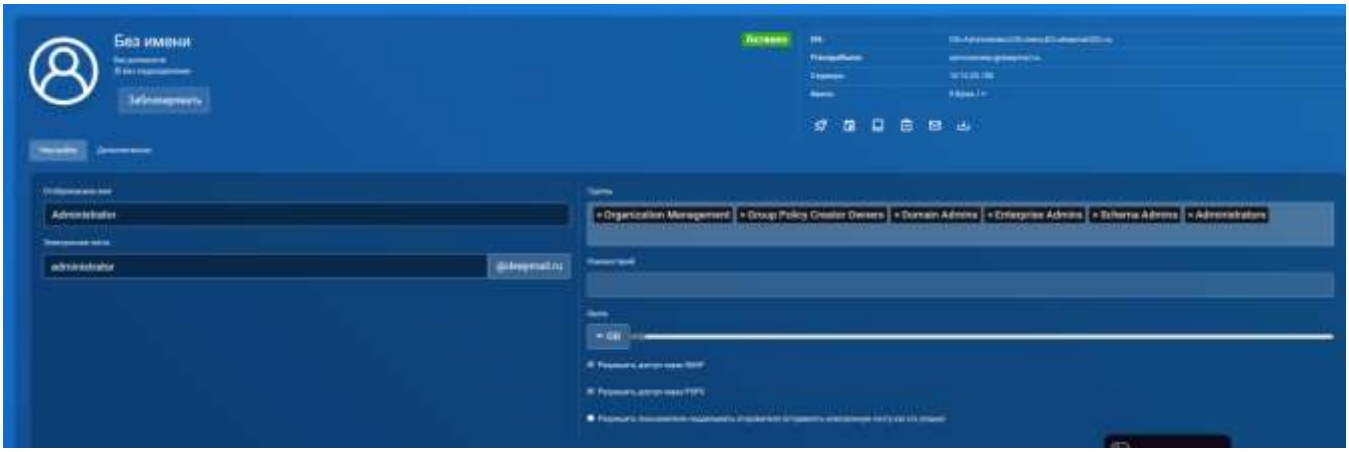
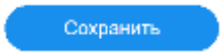


Рисунок 66 – Данные пользователя, подключенного через LDAP

После завершения редактирования параметров администратор должен нажать кнопку 

.

4.10.2.3 Блокировка пользователя

Заблокированные администратором пользователи не могут отправлять и получать почту.

Для блокировки пользователя администратор должен нажать кнопку 

рядом с  пользователя (см. рисунок 66). Заблокированный пользователь получит статус 

в списке пользователей.

Для разблокировки пользователя должен нажать кнопку 

, после чего статус пользователя 

в форме редактирования пользователя должен сменится на 

.

4.10.2.4 Удаление пользователя

Для удаления группы администратор должен нажать кнопку  на вкладке удаление и подтвердить удаление в открывшейся форме «Подтвердить действие».

4.10.3 Псевдонимы почтового домена

4.10.3.1 Создание псевдонима почтового домена

Администратор может назначить пользователю дополнительный почтовый ящик или почтовый ящик для нескольких пользователей, при этом письма, приходящие на адрес псевдонима, будут автоматически отсылаться на все аккаунты, к которым он привязан.

Для перехода на вкладку «Список псевдонимов» (рисунок 67) администратор должен нажать кнопку 

.

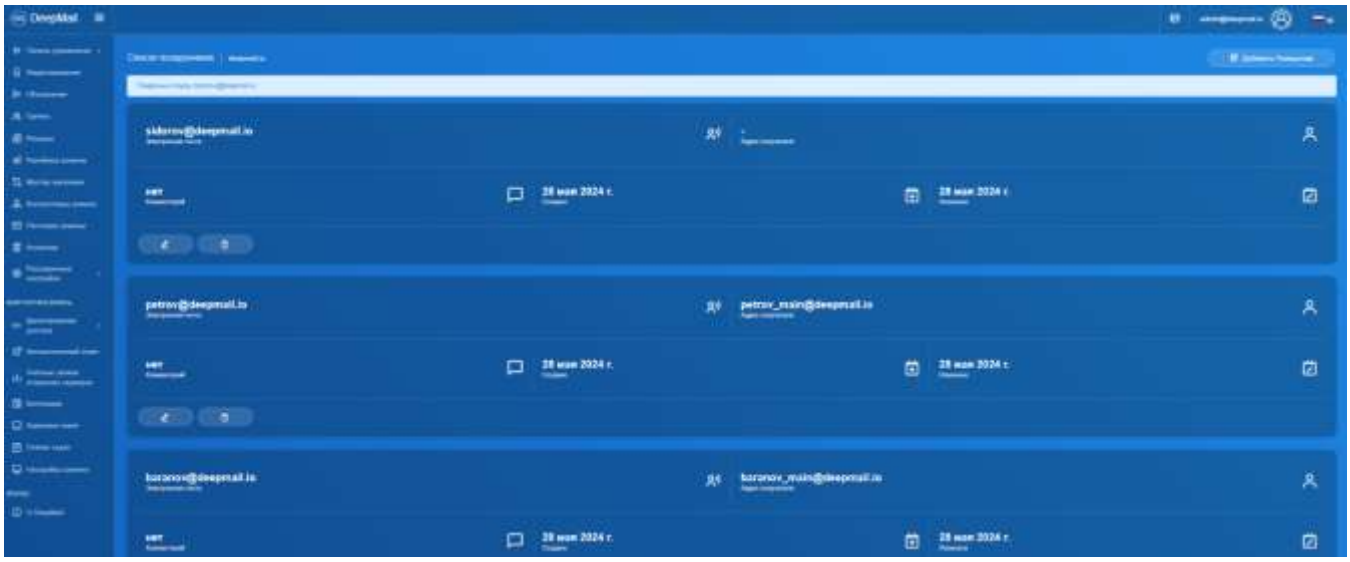


Рисунок 67 – Вкладка «Список псевдонимов» пользователей домена

Для создания нового псевдонима администратор должен нажать кнопку 

, которая откроет форму «Создать псевдоним», показанную на рисунке 68.

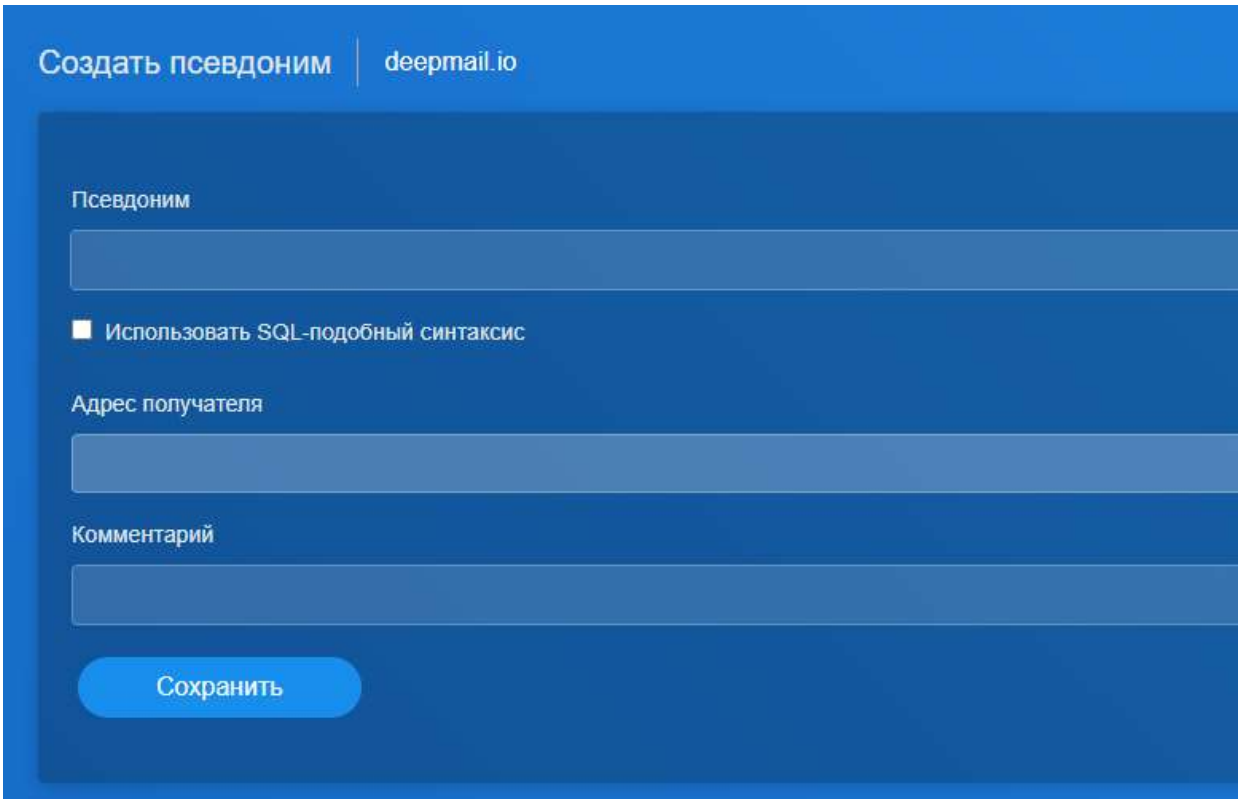


Рисунок 68 – Форма «Создать псевдоним»

Администратор должен заполнить данными поля «Псевдоним», «Адрес получателя» (в этом поле необходимо указать существующий почтовый адрес или

адреса домена) и «Комментарий» (при необходимости). После ввода всех данных администратор должен нажать кнопку Сохранить. Созданный псевдоним должен отобразиться в панели псевдонимов домена.

4.10.3.2 Удаление псевдонима почтового домена

Для удаления администратор должен нажать кнопку в панели этого псевдонима и подтвердить удаление в открывшейся форме «Подтвердить действие».

4.10.4 Менеджеры почтового домена

Для управления менеджерами почтового домена администратор должен нажать кнопку в панели этого почтового домена (рисунок 69), после чего откроется вкладка «Список менеджеров» (рисунок 70).

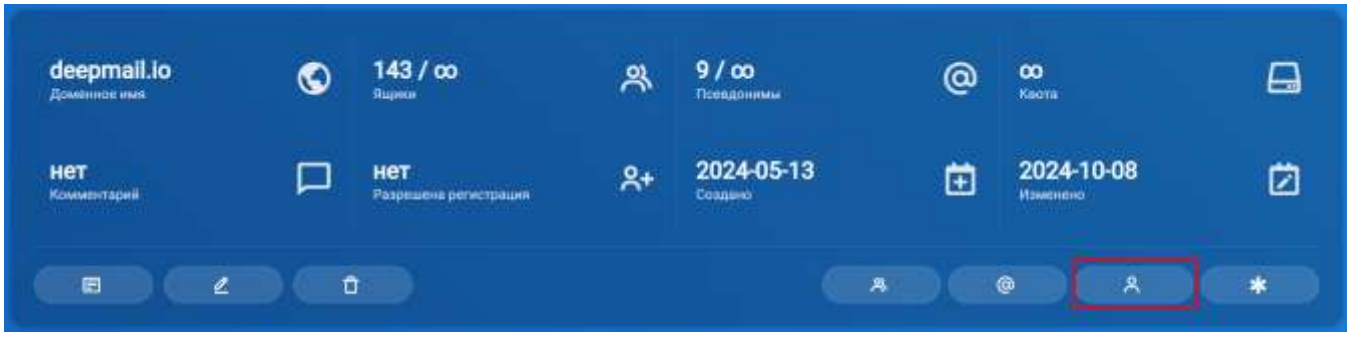


Рисунок 69 – Кнопка на панели почтового домена

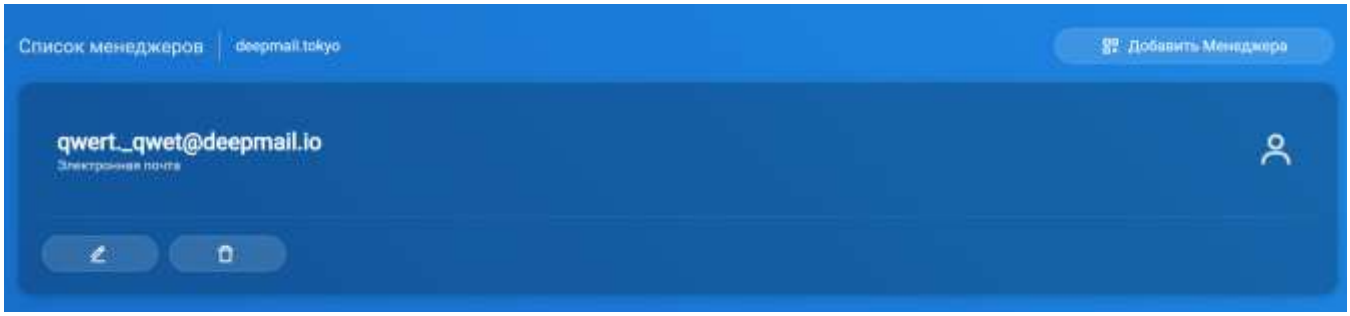


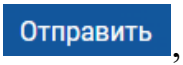
Рисунок 70 – Вкладка «Список менеджеров»

4.10.4.1 Добавление менеджера почтового домена

Для добавления менеджера почтового домена должен нажать кнопку 

, которая откроет форму «Добавить менеджера», показанную на рисунке 68.

Рисунок 71 – Форма «Добавить менеджера»

После выбора менеджера из выпадающего списка, необходимо нажать на кнопку 

, после чего пользователь отобразится на вкладке «Список менеджеров».

4.10.4.2 Удаление менеджера почтового домена

Для удаления администратор должен нажать кнопку  в панели этого менеджера и подтвердить удаление в открывшейся форме «Подтвердить действие».

4.10.5 Альтернативный почтовый домен

Администратор может задавать альтернативные имена почтового домена, при этом почта должна доходить до пользователей как по основному имени домена, так и по всем альтернативным именам. Для просмотра списка альтернативных имен администратор должен перейти в меню «Почтовые домены» нажать кнопку  на панели почтового домена (рисунок 72), после чего откроется вкладка «Список альтернативных доменов».

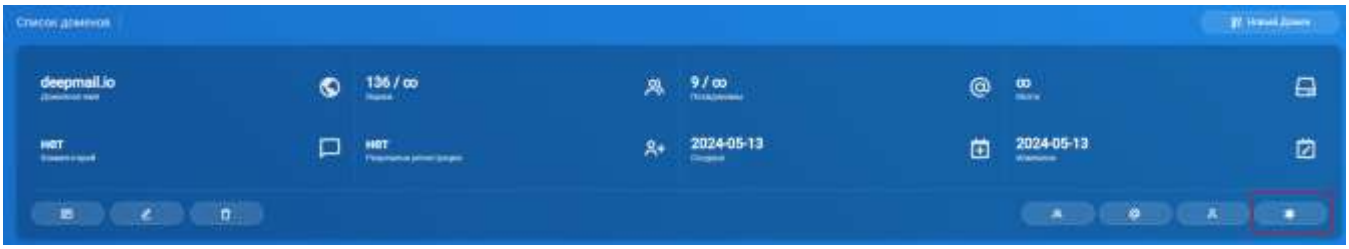


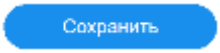
Рисунок 72 – Кнопка «Альтернативные домены»

4.10.5.1 Создание альтернативного почтового домена

Для создания альтернативного имени почтового домена администратору необходимо нажать кнопку 

, после чего откроется форма «Создать альтернативный домен» (рисунок 73).

Рисунок 73 – Форма «Создать альтернативный домен»

Далее администратору необходимо заполнить поле «Имя альтернативного домена» и нажать на кнопку 

. Появится сообщение 

, а добавленный альтернативный домен отобразится на вкладке «Альтернативные домены» (рисунок 74).

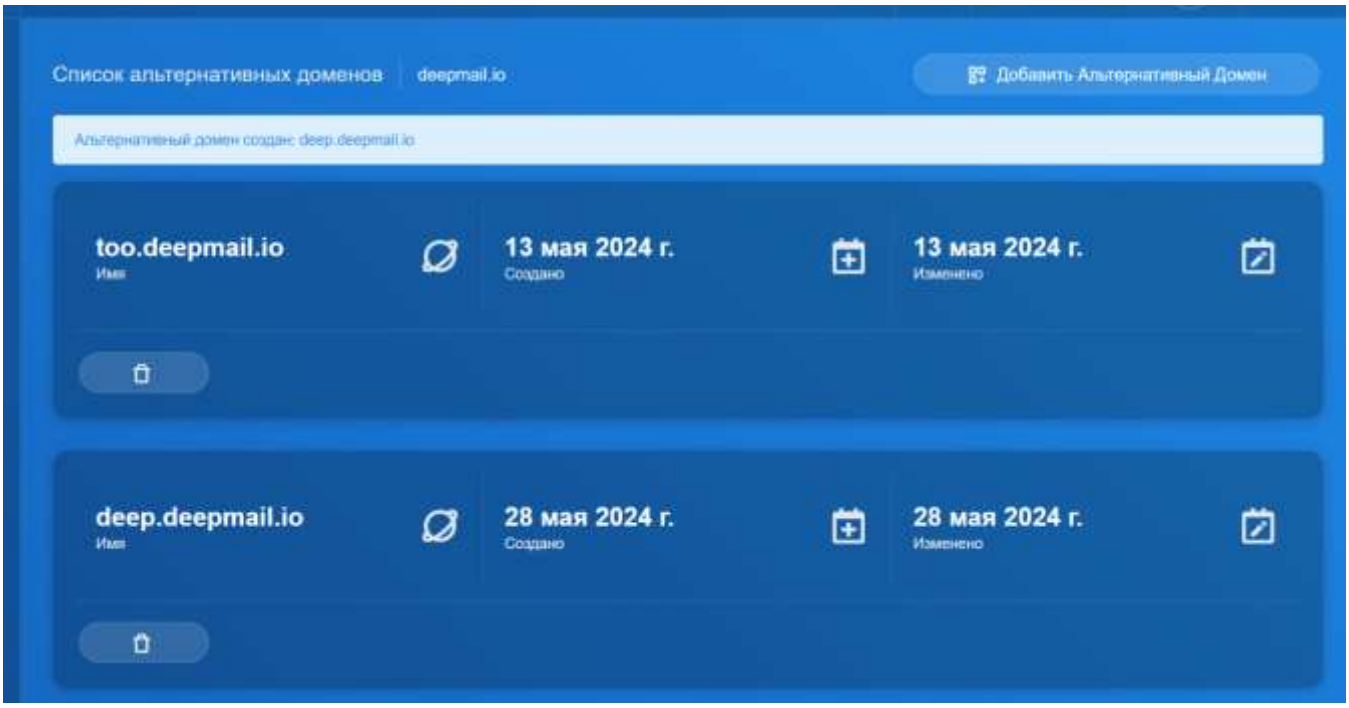


Рисунок 74 – Форма «Список альтернативных доменов»

4.10.5.2 Удаление альтернативного почтового домена

Для удаления почтового домена администратор должен нажать кнопку  в панели этого альтернативного домена и подтвердить удаление в открывшейся форме «Подтвердить действие».

4.10.6 Настройка DNS почтового домена

Для просмотра DNS записей домена администратор должен нажать кнопку  , в результате чего откроется форма «Подробности домена» (рисунок 75).

Рисунок 75 – Вкладка «Подробности домена»

Во вкладке «Подробности домена» представлены:

- «Доменное имя» с указанием почтового домена;
- «DNS MX запись» с указанием почтового сервера, и его веса (приоритета);
- «DNS SPF-запись» с указанием имени доверенного почтового сервера, рассылающего почту домена;
- «Публичный ключ DKIM» и «DNS DKIM запись» для создания цифровой подписи писем, гарантирующей их подлинность;
- «DNS DMARC запись», которая определяет политику сервера получателя в отношении писем, отправленных с домена, но не прошедших аутентификацию;
- «Записи автоматической настройки DNS-клиента» почтового клиента.

Форма содержит кнопку 

, создающую новую пару ключей DKIM.

При настройке DNS почтового домена необходимо настроить DNS SPF запись, сгенерировать ключи DKIM и настроить запись DNS DKIM и DNS DMRAC.

SPF (Sender Policy Framework) представляет из себя текстовую запись в TXT-записи DNS домена. Запись содержит информацию о списке серверов, которые имеют право отправлять письма от имени этого домена и механизм обработки писем, отправленных от других серверов.

DomainKeys Identified Mail метод E-mail аутентификации. Технология DomainKeys Identified Mail (DKIM) объединяет несколько существующих методов антифишинга и антиспама с целью повышения качества классификации и идентификации легитимной электронной почты. Вместо традиционного IP-адреса, для определения отправителя сообщения DKIM добавляет в него цифровую подпись, связанную с именем домена организации. Подпись автоматически проверяется на стороне получателя, после чего, для определения репутации отправителя, применяются «белые списки» и «чёрные списки».

В технологии DomainKeys для аутентификации отправителей используются доменные имена. DomainKeys использует существующую систему доменных имен (DNS) для передачи открытых ключей шифрования.

DMARC – протокол, который указывает серверу, что делать с письмом, если записи DKIM и SPF окажутся некорректны. Корректные DKIM и SPF подтверждают, что письмо отправлено от имени домена, указанного в поле «От:» в письме. Таким образом, DMARC наряду с SPF и DKIM отвечает за аутентификацию почты.

Для генерации ключей нужно выбрать вкладку «Почтовые домены» и нажать кнопку  у настраиваемого домена. После открытия формы (рисунок 76) с подробной информацией о домене нужно нажать кнопку 

, и подтвердить действие в следующем окне (рисунок 77), чтобы получить ключи DKIM.

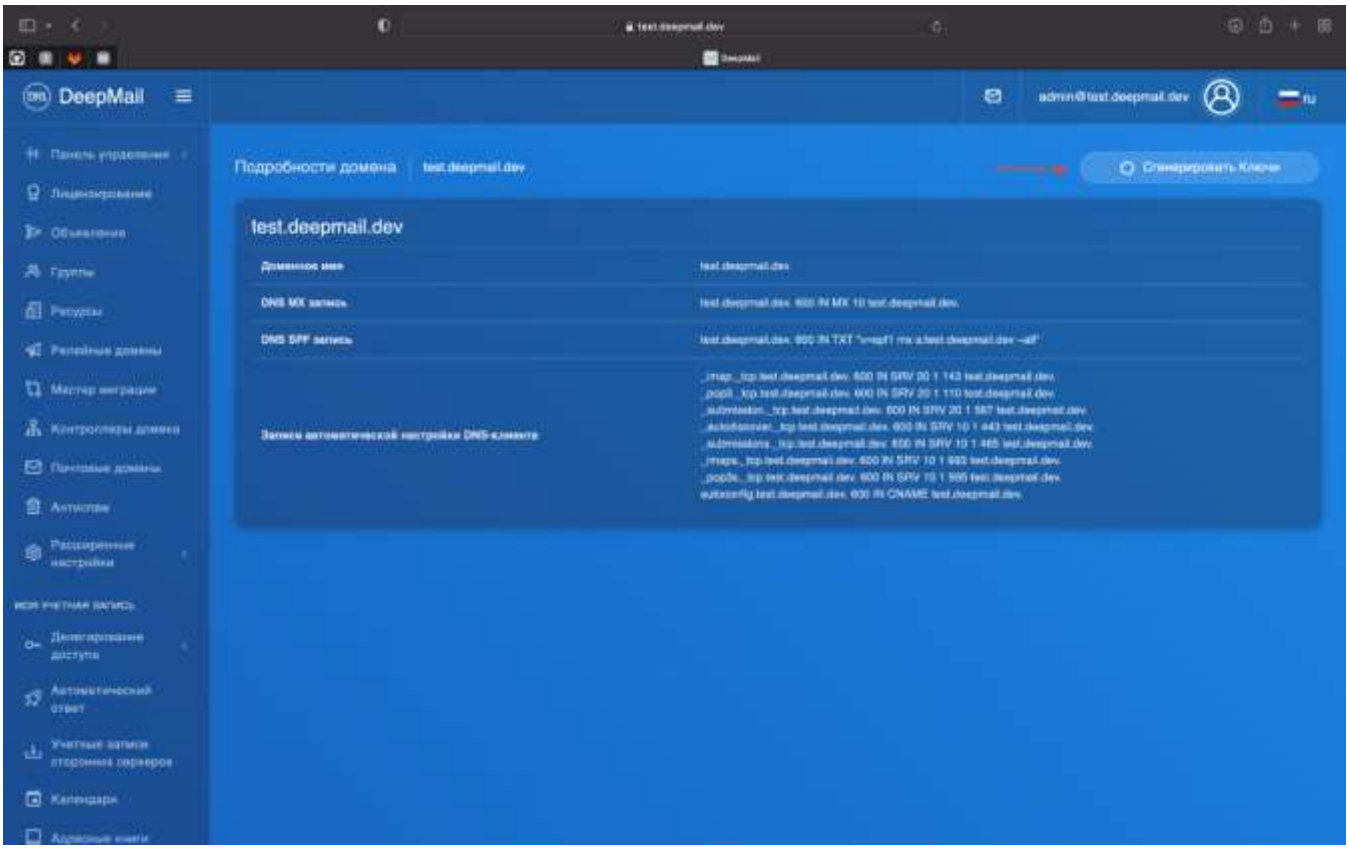


Рисунок 76 – Вкладка «Подробности домена». Кнопка «Сгенерировать ключи»

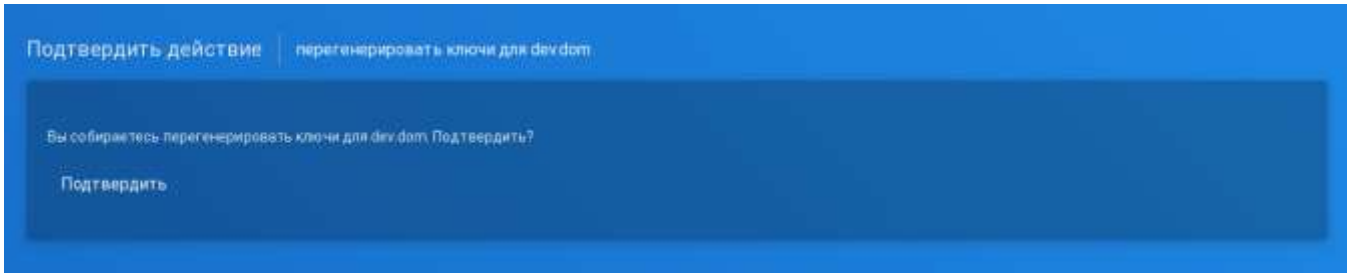


Рисунок 77 – Вкладка «Подтвердить действие»

После генерации ключа, его текст копируется из появившегося после генерации раздела «ПУБЛИЧНЫЙ КЛЮЧ DKIM» и вставляется в «DNS DKIM запись» (рисунок 78).

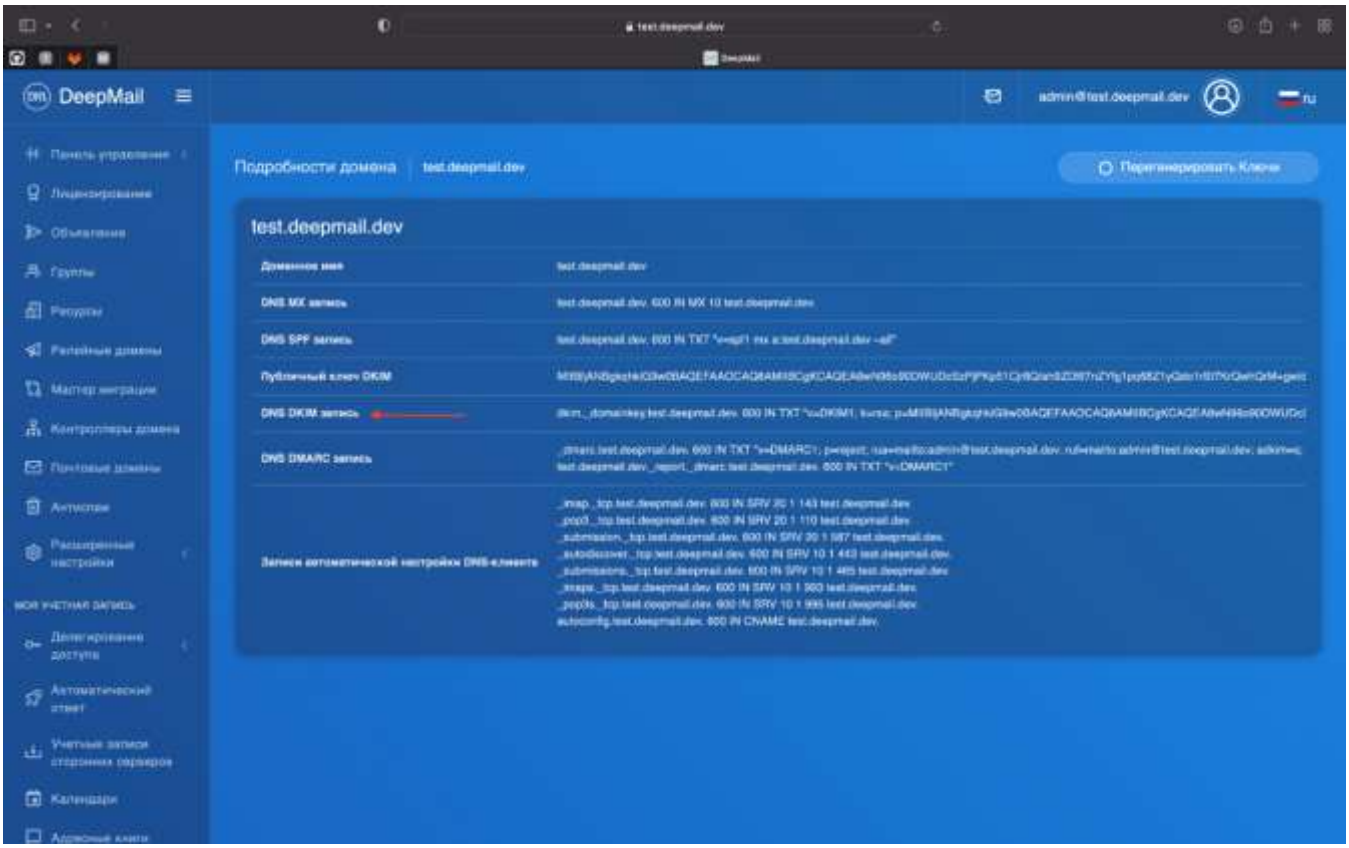


Рисунок 78 – Автоматическое добавление DKIM ключа в запись

Также можно сразу скопировать DNS DMARC и DNS SPF записи (рисунок 79).

Рисунок 79 – DNS DMARC и DNS SPF записи

В таблице 3, приведены необходимые DNS-записи с общепринятыми обозначениями:

- «Yourdomain» – имя почтового домена;
- «xxx.xxx.xxx.xxx» – IP-адрес;
- «DIM_KEY» – ваш DKIM key.

Таблица 3 – Типы DNS записей

Тип	Имя	Значение	Доп. информация
MX	yourdomain.ru.	mail.yourdomain.ru.	priority = 10
A	mail.yourdomain.ru.	xxx.xxx.xxx.xxx	
A	dautoconfig.yourdomain.ru.	xxx.xxx.xxx.xxx	
TXT	yourdomain.ru.	v=spf1 mx a:yourdomain.ru ip4:xxx.xxx.xxx.xxx ~all	
TXT	dkim._domainkey.yourdomain.ru.	v=DKIM1; k=rsa; p=DKIM_KEY	
TXT	yourdomain.ru._report._dmarc.yourdomain.ru.	v=DMARC1	
TXT	_dmarc.yourdomain.ru.	v=DMARC1; p=reject; rua=mailto:admin@yourdomain.ru; ruf=mailto:admin@yourdomain.ru; adkim=s; aspf=s	

4.10.7 Управление общими почтовыми ящиками

Почта, приходящая в почтовый ящик, может быть доступна сразу нескольким пользователям. Эти пользователи также могут отправлять письма от адреса этого ящика. Управление общими почтовыми ящиками производится в рамках одного почтового домена.

4.10.7.1 Создание общего почтового ящика

Для создания общего почтового ящика администратор должен открыть вкладку «Список доменов», выбрать почтовый домен, в котором будет создан новый общий

почтовый ящик и нажать кнопку  (рисунок 80). Откроется вкладка «Список пользователей» (рисунок 81)

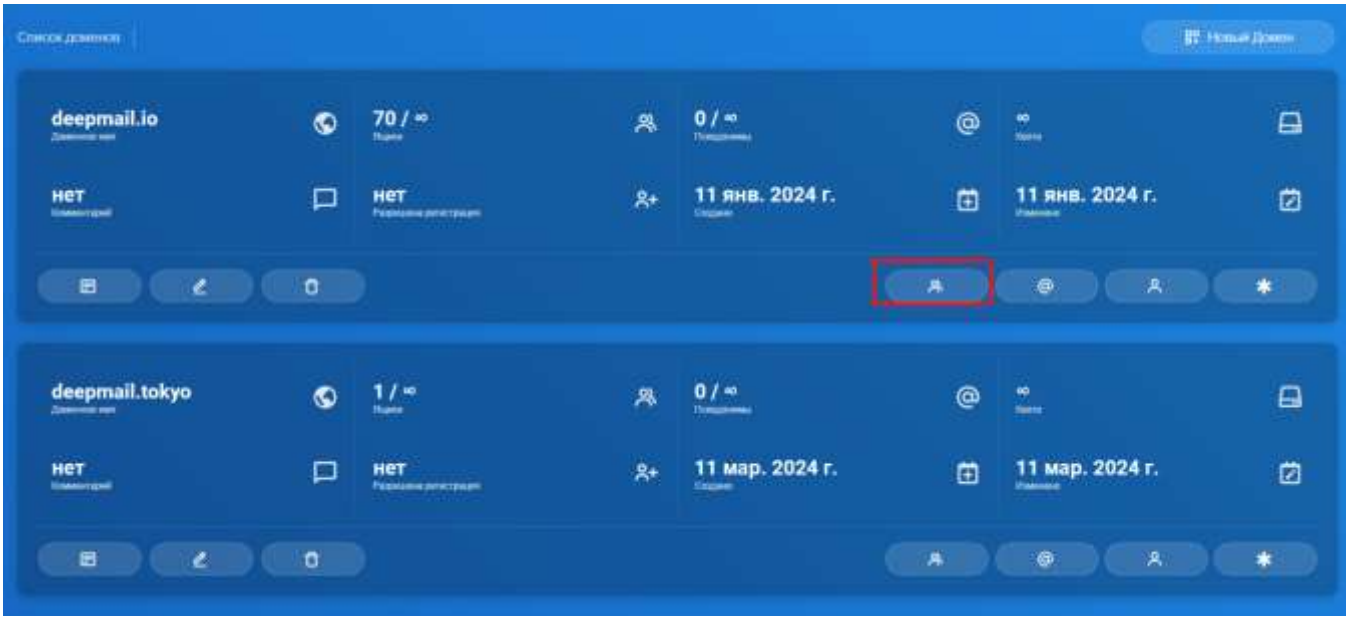


Рисунок 80 – Кнопка «Пользователи» во вкладке «Список доменов»

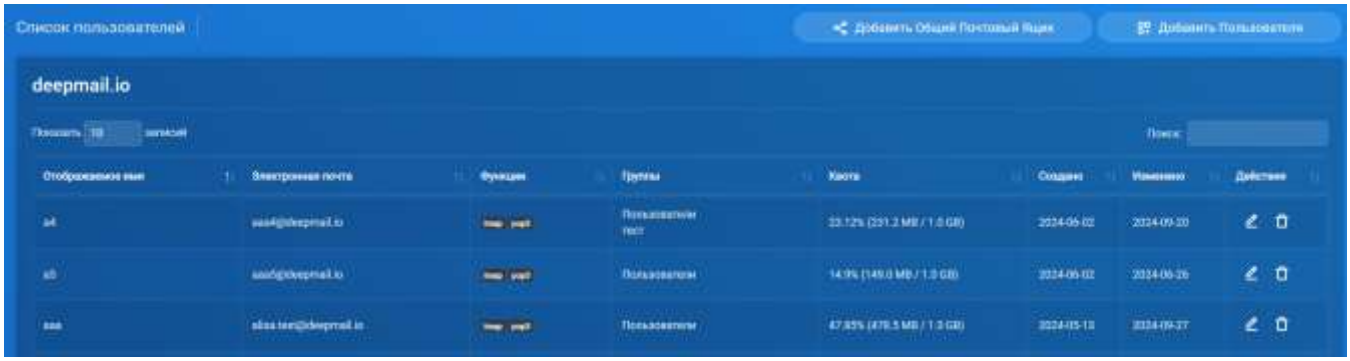


Рисунок 81 –Вкладка «Список пользователей»

Далее администратор должен нажать кнопку 

.

Создание общего почтового ящика происходит в открывшейся форме «Новый общий почтовый ящик» (рисунок 82), администратору надо заполнить следующие данные:

- отображаемое имя общего почтового ящика в поле «Отображаемое имя»;
- непосредственно адрес общего почтового ящика в поле «Электронная почта»;

- группу или группы, имеющие доступ в поле «Группы, имеющие доступ (все пользователи в группе)»;
- отдельный список пользователей (при наличии), у которых будет доступ к ящику в поле «Пользователи, имеющие доступ»;
- выставить квоту памяти ящика в области «Квота».

Рисунок 82 – Вкладка создания нового общего почтового ящика

После заполнения всех данных администратор должен нажать кнопку Сохранить.

Общие почтовые ящики отмечаются в списке пользователей статусом Общий почтовый ящик в столбце «Функции».

4.10.7.2 Редактирование общего почтового ящика

Редактирование почтового ящика происходит с помощью кнопки и вызывает форму, аналогичную показанной ранее на рисунке 82. Администратор может перенастроить значение всех параметров в форме, кроме «Электронная почта». Для подтверждения сделанных изменений администратор должен нажать кнопку Сохранить.

4.10.7.3 Удаление общего почтового ящика

Для удаления общего почтового ящика администратор должен нажать кнопку  и подтвердить удаление общего почтового ящика в открывшейся форме «Подтвердить действие».

4.11 Пункт вертикального меню «Антиспам»

Для перехода на вкладку «RSPAMD» (рисунок 84), которая отвечает за управление антиспамом, необходимо выбрать пункт «Антиспам» вертикального меню, выбор которого показан на рисунке 83.

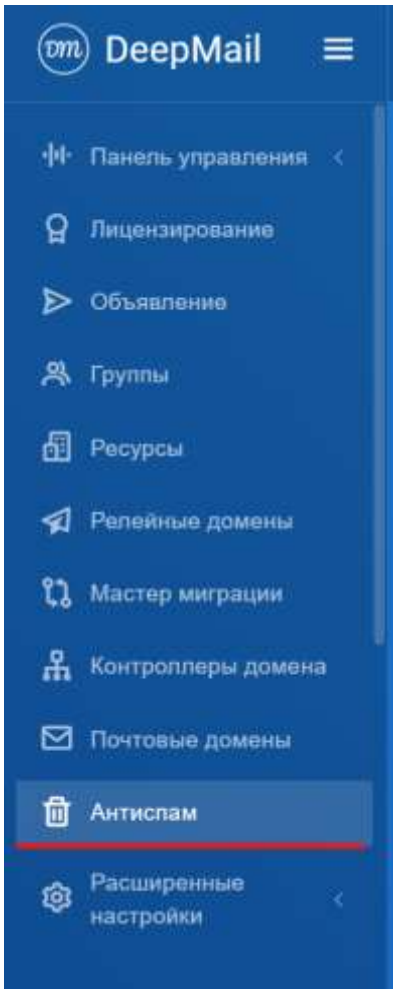


Рисунок 83 – Пункт вертикального меню «Антиспам»

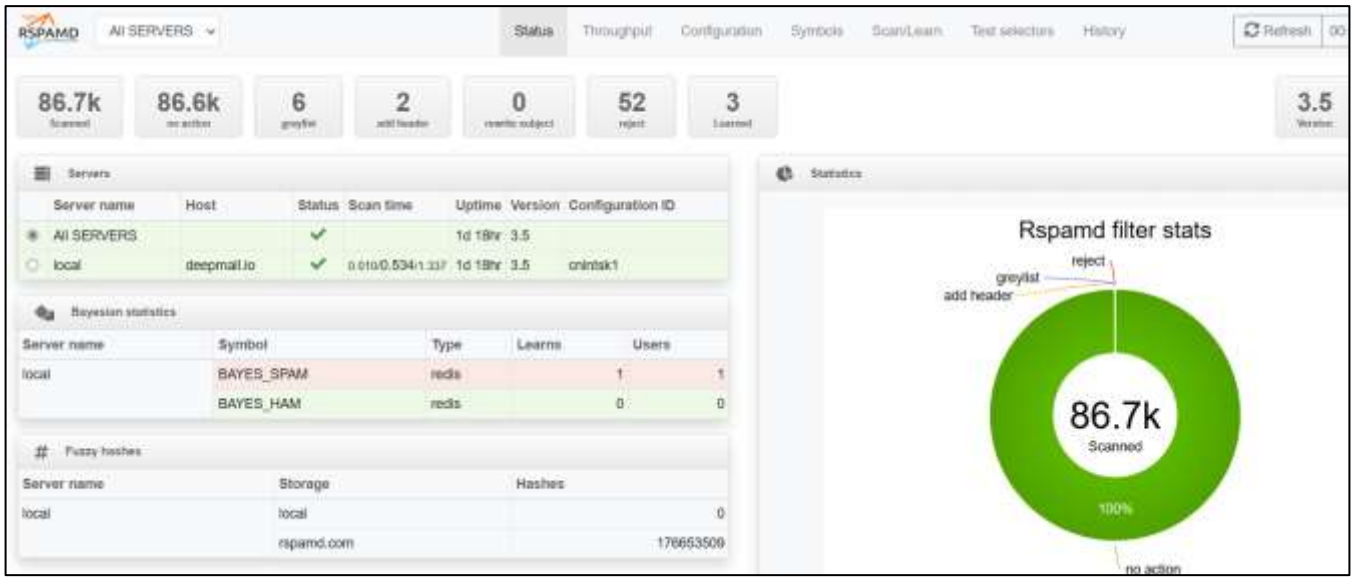


Рисунок 84 – Вкладка «Антиспам»

«RSPAMD» может работать как в автономном режиме, так и в режиме «онлайн». При работе системы в режиме онлайн – сигнатуры загружаются с интернета. При работе системы в автономном режиме – сигнатуры не обновляются, и система просто занимается анализом самих писем.

На вкладке «History» (рисунок 85) отображается история обработки писем.

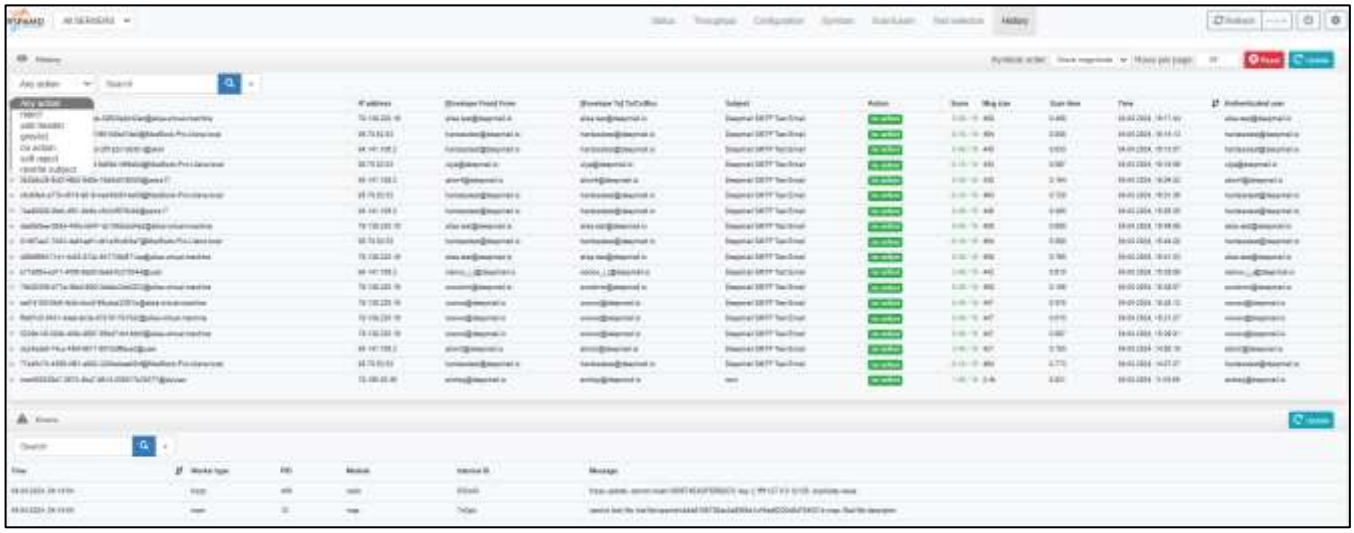


Рисунок 85 – Вкладка «History»

4.12 Пункт вертикального меню «Расширенные настройки»

Пункт вертикального меню «Расширенные настройки» содержит 2 подпункта «Настройки SSL/TSL» и «Настройки конфигурации» (рисунок 86).

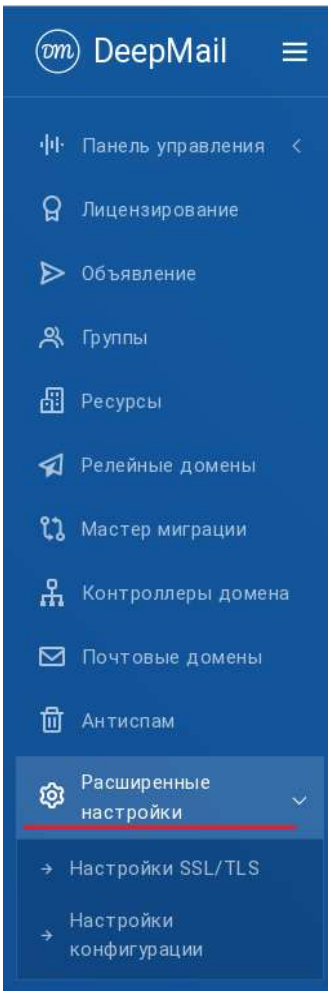


Рисунок 86 – Пункт вертикального меню «Расширенный настройки»

4.1 Подпункт вертикального меню «Настройки SSL/TSL»

Для перехода к настройкам SSL/TSL администратору необходимо выбрать подпункт «Настройки SSL/TSL» пункта вертикального меню «Панель управления» (рисунок 87), после чего откроется вкладка «Настройки SSL/TSL» (рисунок 88)

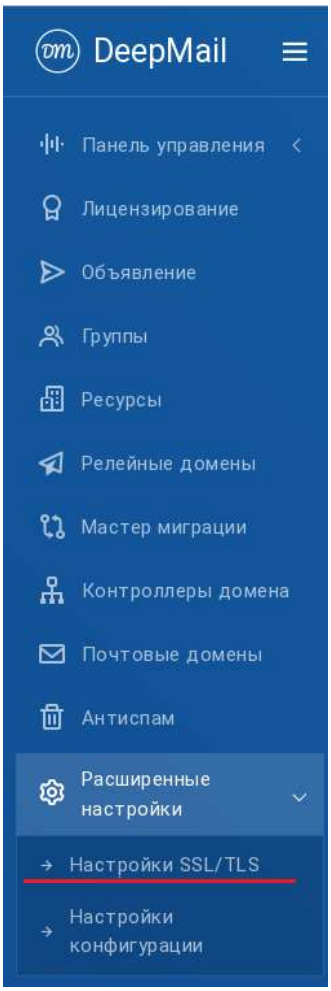


Рисунок 87 – Подпункт вертикального меню «Настройки SSL/TLS»

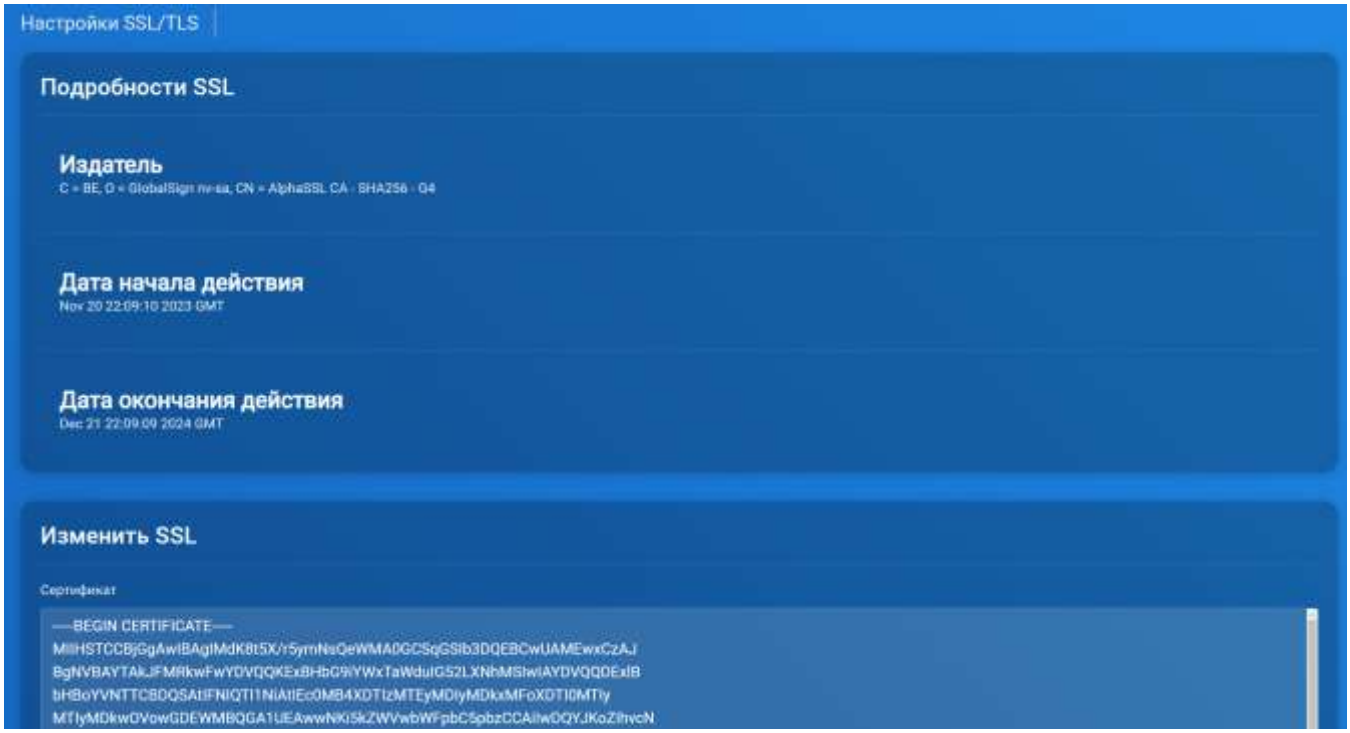
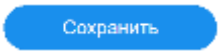


Рисунок 88 – Вкладка «Настройки SSL/TLS»

После установки будет установлен самоподписанный сертификат SSL, который необходимо заменить. Для замены сертификата и ключа нужно указать сертификат и ключ (в формате PEM) в соответствующих полях для ввода на панели «Изменить SSL» и нажать кнопку 

.

5. УСТАНОВКА И НАСТРОЙКА СЕРВЕРА

5.1 Развертывание узла Сервера

Развертывание узла Сервера на единичной виртуальной машине состоит из следующих этапов:

- установка окружения;
- распаковка архива;
- запуск установщика;
- выбор пути до хранилища;
- ввод имени базового почтового домена;
- ввод IP-адреса, который должен слушать сервер;
- выбор сертификата протокола TLS;
- выбор антивируса (или его отключение);
- ввод IP-адреса DNS сервера;
- настройка подключения к СУБД.

5.1.1 Установка окружения Сервера

Для работы Сервера необходим пакет Docker. Команды для установки Docker и Docker compose v2, в зависимости от используемой ОС, представлены в таблице 4.

Таблица 4 – Команды для установки Docker и Docker compose

Устанавливаемое ПО	ОС	Команда
Docker	ALT Linux	*«sudo apt-get install docker-engine»* (для старых репозиториев: *«sudo apt-get install docker-ce»*)
	Astra Linux, Ubuntu, Debian	*«sudo apt install docker.io»*
Docker compose	ALT Linux	*sudo apt-get install docker-compose*
	Astra Linux, Ubuntu, Debian	*sudo apt install docker-compose*

5.1.2 Распаковка архива с дистрибутивом Сервера

Дистрибутив Сервера поставляется в виде архива (*.tar.gz). Для распаковки архива необходимо набрать команду:

«*sudo tar -xvzf deepmail-server-*.tar.gz*».

После распаковки архива будет создана директория deepmail-server-<номер версии> (рисунок 89), в которой будет находится исполнительный файл установщика deepmail-installer.

Рисунок 89 – Содержимое разархивированной папки

5.1.3 Запуск установки Сервера

Для запуска установки Сервера необходимо перейти в разархивированную папку и запустить установщик выполнив команду «*sudo ./deepmail-installer*».

Для отключения установки антиспама необходимо дополнительно указать ключи *«–whithout_antispam*» или «–w*as*». Вид запущенного установщика показан на рисунке 90.

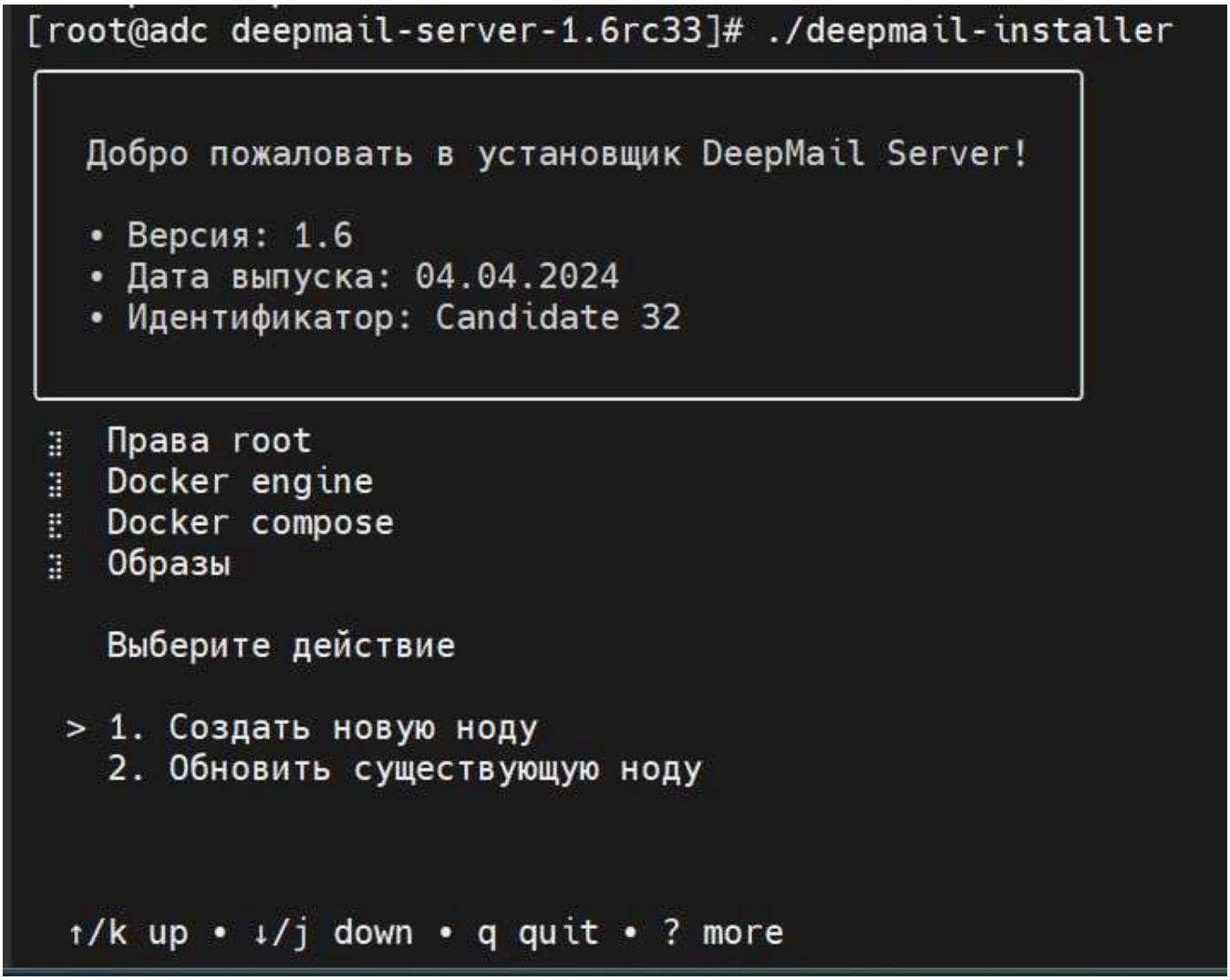


Рисунок 90 – Окно установщика Сервера

Для перемещения по пунктам установщика использовать клавиши «j» и «k», для редактирования параметра надо начать ввод нового значения (клавиша «←» (Backspace) для возврата к исходному значению), для подтверждения «Enter», для выхода «q».

Выбрать «Создать новую ноду». Далее необходимо выбрать путь до хранилища (рисунок 91).

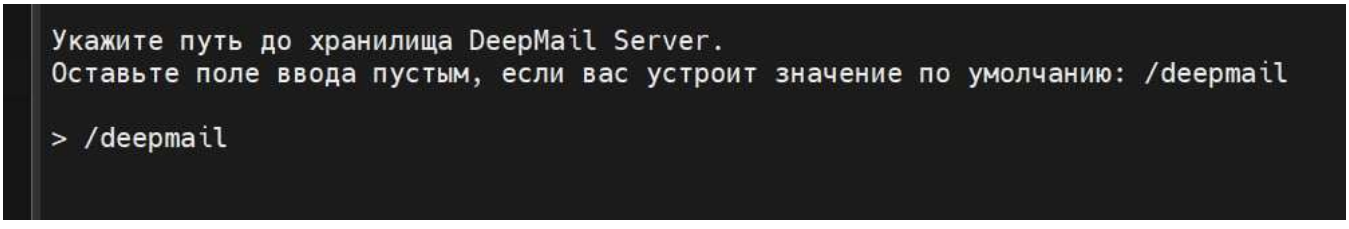


Рисунок 91 – Выбор места хранилища

Далее необходимо выбрать имя базового почтового домена. В данном домене будет находиться postmaster. (рисунок 92)

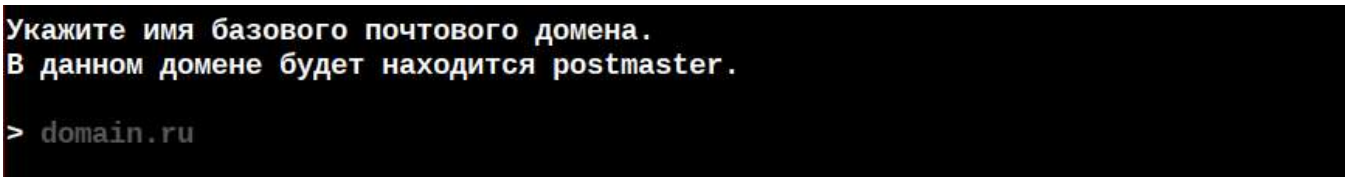


Рисунок 92 – Выбор почтового домена

Далее выбрать IP-адрес, который должен прослушивать DeepMail (рисунок 93):

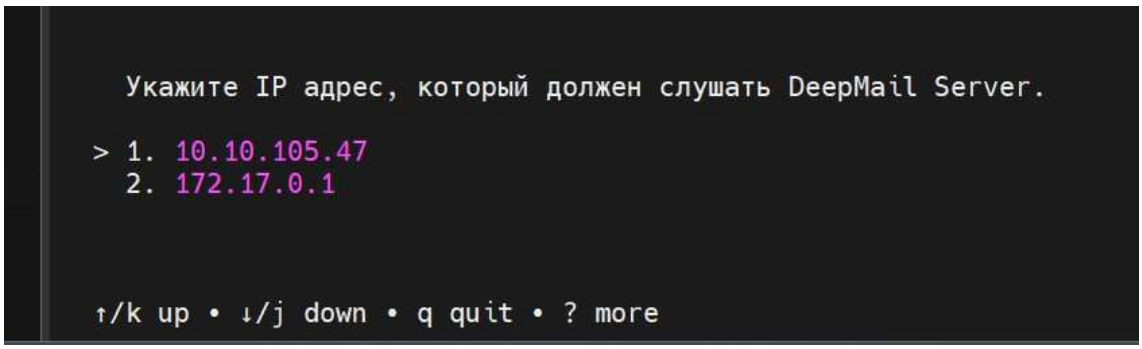


Рисунок 93 – Выбор IP-адреса

Выбрать вариант протокола защиты транспортного уровня TLS:

- «Cert» – собственный (самоподписанный) сертификат (необходимо заменить после установки);
- «letsencrypt» – автогенерируемый сертификат «Let’s encrypt» (только при настроенном внешнем DNS).

Выбрать вариант антивируса:

- «Clamav»;
- «Без антивируса» (none написано в дистрибутиве).

Выбрать IP-адрес DNS-сервера (при его наличии) или оставить поле пустым, если планируется использовать встроенный DNS-resolver (рисунок 94).

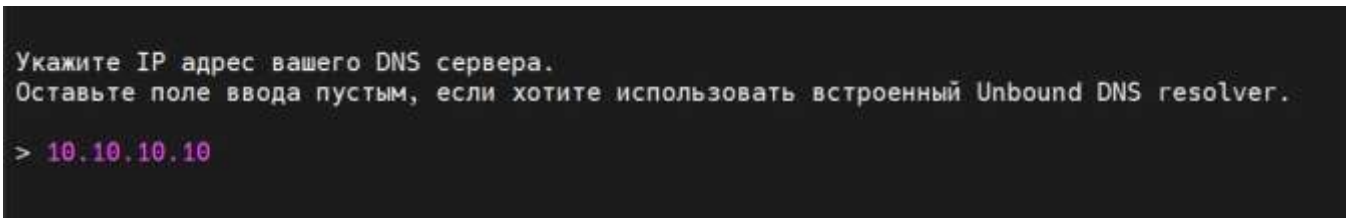


Рисунок 94 – Настройка DNS-сервера

Выбрать тип СУБД (SQLite, PostgreSQL или MySQL) (рисунок 95).

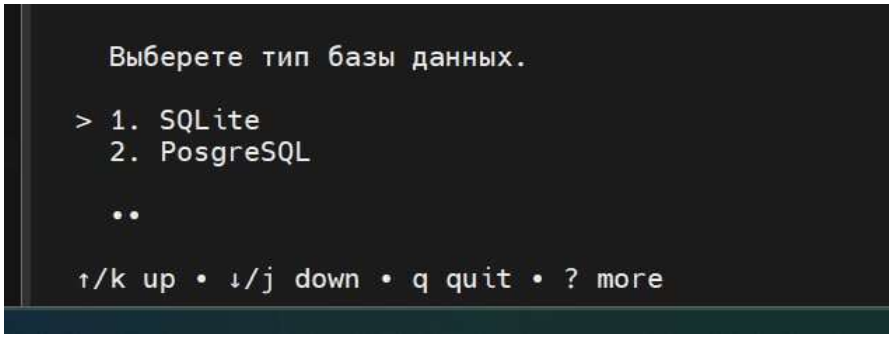


Рисунок 95 – Выбор типа СУБД

Выбор типа СУБД PostgreSQL требует дополнительного ввода IP-адреса удаленного сервера базы данных, имя пользователя и пароля базы данных (рисунок 96).

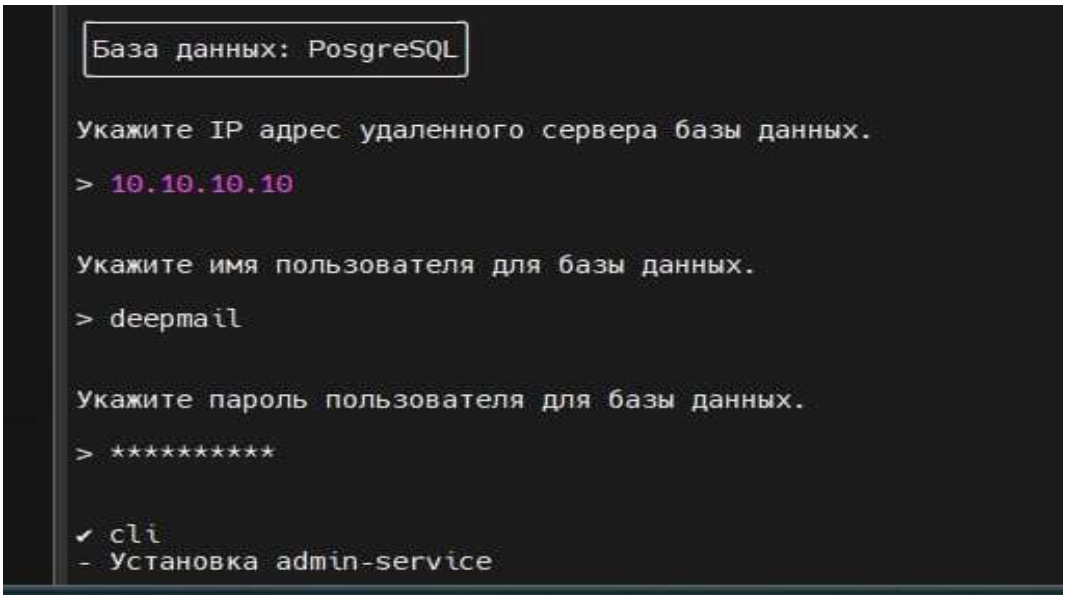


Рисунок 96 – Ввод данных для подключения к СУБД

5.2 Развертывание кластера Сервера

Развертывание кластера адресов DeepMail подразумевает развертывание Сервера на нескольких нодах (виртуальных машинах), создание хранилища и настройка балансировки нагрузки HAProxy.

Почтовый кластер Сервера показан на рисунке 97.

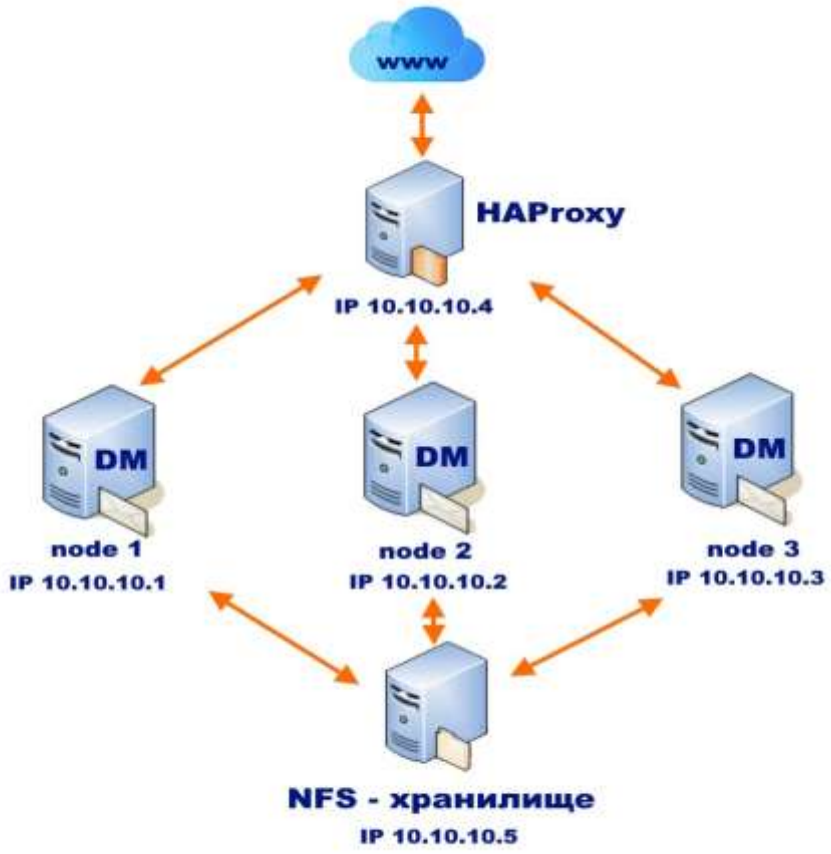


Рисунок 97 – Схема почтового кластера Сервера

Далее в описании установки и настройки кластера в качестве примера будут использоваться IP-адреса, указанные на рисунке 97.

Для настройки единичного Сервера необходимо выполнить только пункт 5.1 настоящего документа.

5.2.1 Создание NFS-хранилища

5.2.1.1 Разворачивание NFS-сервера

Для скачивания и установки пакета NFS-сервера необходимо ввести команды, указанные в таблице 5.

Таблица 5 – Команды для установки и настройки NFS-сервера

Устанавливаемое ПО	ОС	Команда
NFS-сервер	Alt Linux	*«sudo apt-get install nfs-server»* *«sudo systemctl start nfs»*
	Astra Linux, Debian, Ubuntu	*«sudo apt install nfs-kernel-server»*

После чего нужно создать директорию для будущего NFS-хранилища Сервера с помощью команды *«sudo mkdir /mnt/deepmail».*

Затем необходимо на нужном количестве нод создать директорию «/deepmail», желательно до установки дистрибутива Сервера.

Далее нужно отредактировать файл «/etc/exports» на NFS-хранилище добавив в него строку:

«/mnt/deepmail 10.10.10.1(rw,sync,no_subtree,no_subtree_check,no_root_squash) 10.10.10.2(rw,sync,no_subtree,no_subtree_check,no_root_squash) 10.10.10.3(rw,sync,no_subtree,no_subtree_check,no_root_squash)».

Введенная строка показана на рисунке 98.

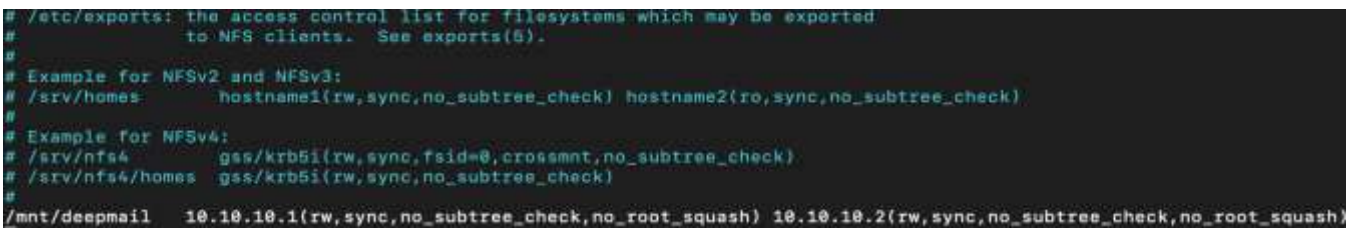


Рисунок 98 – Редактирование файла «/etc/exports»

Для экспорта каталогов без перезагрузки машины надо ввести команду *«sudo exportfs -rav»* (таким образом разрешаем/экспортируем папку «mnt/deepmail» с NFS-сервера на IP-адрес нод).

5.2.1.2 Подключение NFS-хранилища

Для подключения NFS-хранилища на каждой ноде необходимо выполнить его монтирование при помощи команды *«mount 10.10.10.5:/mnt/deepmail/ /deepmail».*

После монитрования NFS-хранилища, на каждой ноде нужно добавить строку «*10.10.10.5:/mnt/deepmail/ /deepmail nfs defaults 0 0*» в файл «/etc/fstab», где «*10.10.10.5»* – IP-адрес созданного ранее NFS-хранилища (рисунок 99).

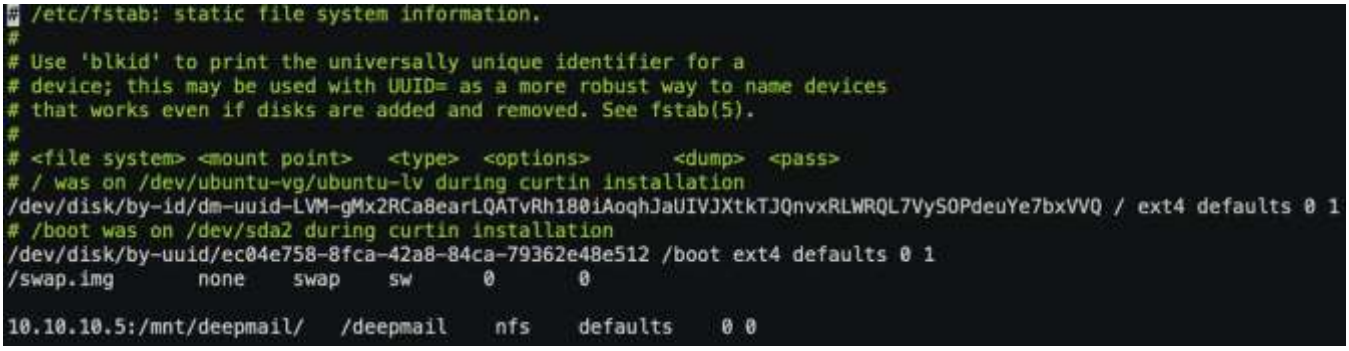


Рисунок 99 – Редактиование системного файла «fstab» ноды

5.2.2 Разворачивание дистрибутива Сервера на нодах

Далее необходимо установить окружение Сервера на каждой ноде.

5.2.2.1 Установка окружения

Для работы Сервера необходимы пакеты «docker» и «docker compose». Команды для их установки, в зависимости от ОС, приведены в таблице 6.

Таблица 6 – Команды для установки «docker» и «docker compose»

Устанавливаемое ПО	ОС	Команда
docker	ALT Linux	*«sudo apt-get install docker-engine»* (для старых репозиториев: *«sudo apt-get install docker-ce»*)

Устанавливаемое ПО	ОС	Команда
	Astra Linux, Ubuntu, Debian	*«sudo apt install docker.io»*
docker compose	ALT Linux	*«sudo apt-get install docker-compose»*
	Astra Linux, Ubuntu, Debian	*«sudo apt install docker-compose»*

5.2.2.2 Установка нод Сервера

Для установки первой ноды необходимо выполнить распаковку дистрибутива Сервера командой *«sudo tar -xvzf deepmail-server-*.tar.gz».*

В распакованной папке будет файл «deepmail-installer», который необходимо запустить командой *«sudo ./deepmail-installer».*

Установщик можно запустить с параметром «--*without*_antispam» или «-*was»*, при указании данного параметра антиспам сервис будет отключен.

После запуска установщика необходимо указать первичную информацию:

- Путь до NFS-хранилища (оставить по умолчанию «/deepmail»);
- Базовый домен (рисунок 100);

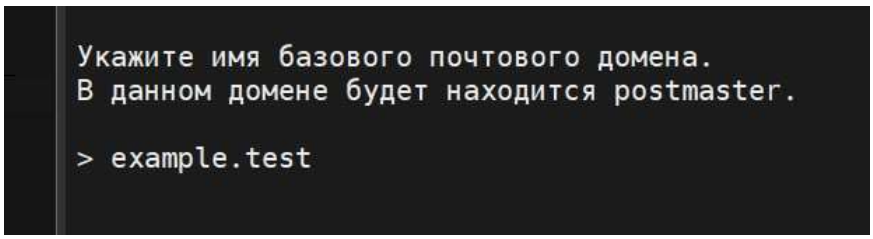


Рисунок 100 – Ввод имени почтового домена

- IP-адрес на рисунке 101, выбирается IP-адрес текущей ноды;

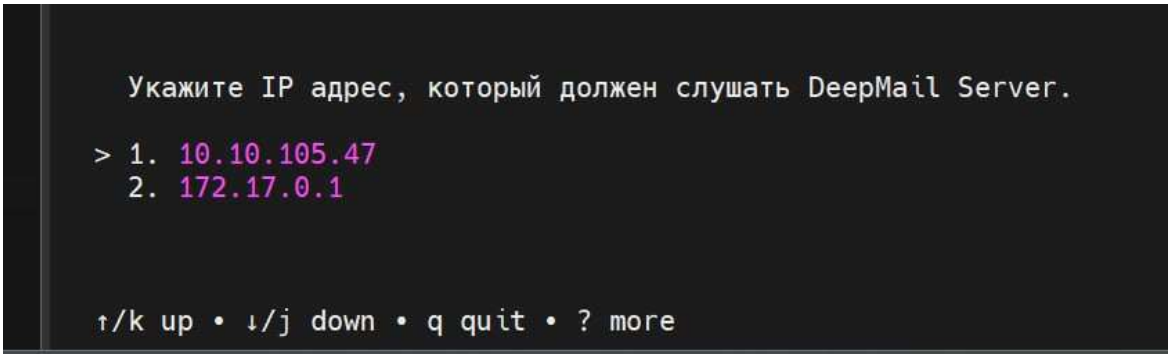


Рисунок 101 – Выбор IP-адреса

- Вариант TLS (рисунок 102):
  a) cert – собственный SSL сертификат;
  b) letsencrypt – автогенерируемый сертификат Let's encrypt (только при настроенном внешнем DNS).

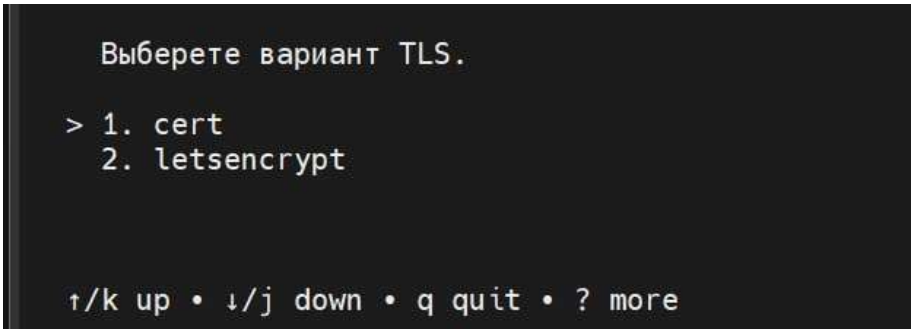


Рисунок 102 – Выбор варианта TLS

- Выбрать вариант антивируса:
  c) Clamav;
  d) Без антивируса.
- IP-адрес DNS-сервера (рисунок 103);

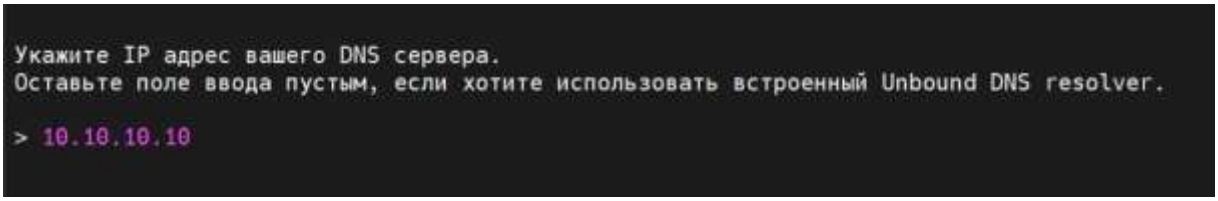


Рисунок 103 – Ввод IP-адреса DNS-сервера

- Выбор типа базы данных (рисунок 104).

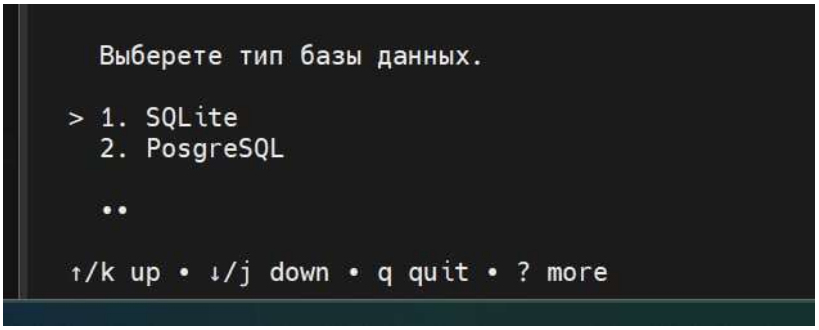


Рисунок 104 – Выбор типа БД

При выборе базы данных PostgreSQL необходимо указать IP-адрес SQL-сервера, имя пользователя и пароль для базы данных (рисунок 105).

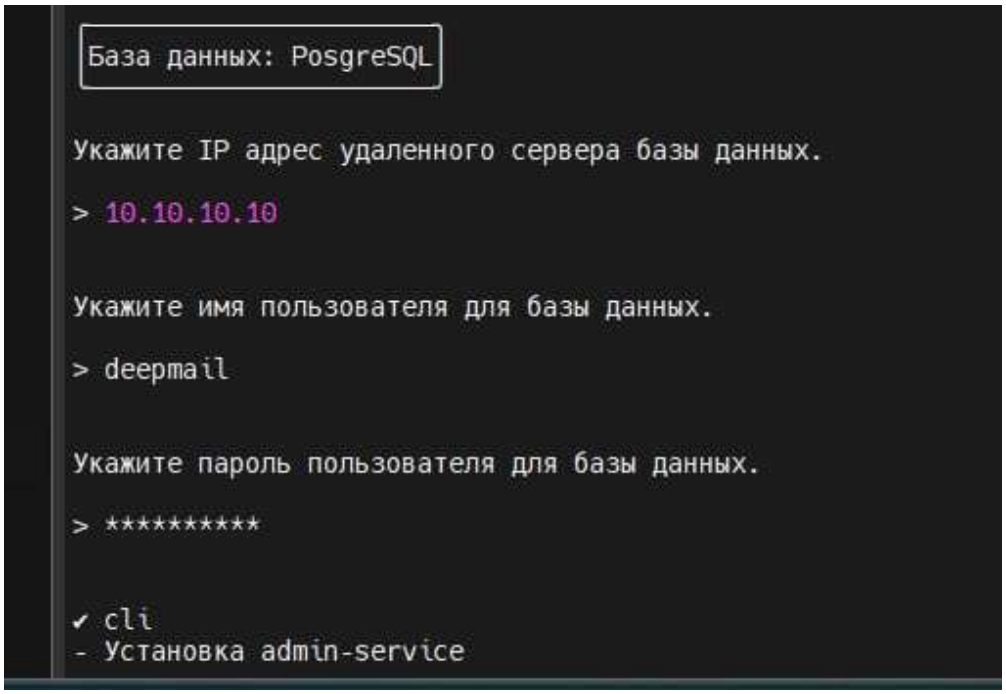


Рисунок 105 – Настойки для подключения к СУБД

После ввода всех данных должен запуститься процесс установки сервера. Установка выполняется пошагово.

5.2.2.3 Установка следующих нод

Установку следующих нод необходимо производить аналогично пункту 5.2.2.2.

После запуска установщика необходимо указать путь до NFS-хранилища и IP-адрес текущего хоста (рисунок 106), после чего запустится процесс установки.

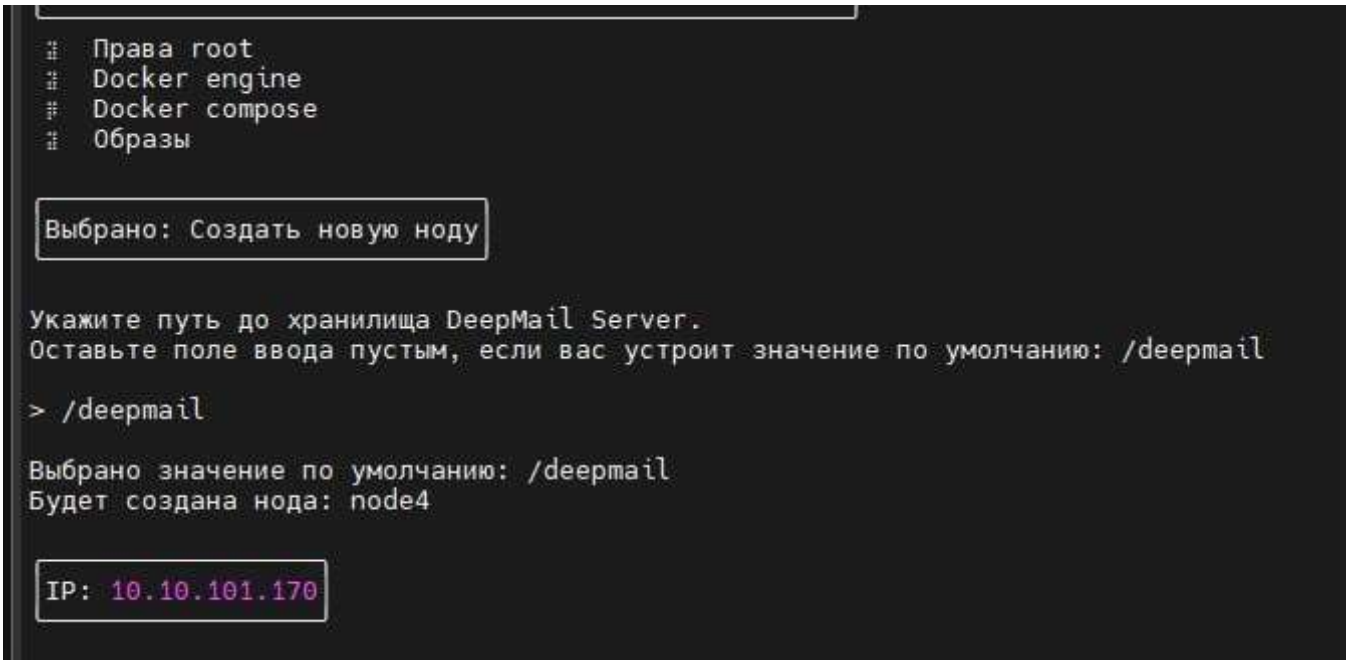


Рисунок 106 – Установка последующих нод

Данные действия требуется провести на необходимом количестве нод.

5.2.3 Развертывание сервера-балансировки HAproxy

Далее приведен пример настройки сервера-балансировки HAProxy для Сервера, используемого в кластере.

5.2.3.1 Установка пакета сервера-балансировки HAProxy

Для установки пакета «haproxy» в зависимости от ОС необходимо воспользоваться одной из команд таблицы 7.

Таблица 7 – Команды для установки пакета «haproxy» для разных ОС

Устанавливаемое ПО	ОС	Команда
haproxy	Alt Linux	*«sudo apt-get install haproxy»*

Устанавливаемое ПО	ОС	Команда
	Astra Linux, Debian, Ubuntu	*«sudo apt install haproxy»*

5.2.3.2 Настройка сервера-балансировки HAProxy

После установки сервера-балансировки HAProxy необходимо заполнить файл конфигурации «/etc/haproxy/haproxy.cfg».

Прописать IP-адреса всех нод и доменное имя в строке «*option smtpchk HELO deepmail.io*», где вместо «*deepmail.io*» ваше доменное имя, введенное ранее при установке).

Пример конфигурации на сервере-балансировки HAProxy:

```
defaults
        mode                    http
        log                     global
        option                  redispatch
        retries                 3
        timeout http-request    10s
        timeout queue           1m
        timeout connect         10s
        timeout client          1m
        timeout server          1m
        timeout http-keep-alive 10s
        timeout check           10s
        maxconn                 3000

frontend http_deepmail_front
        mode http
        bind 10.10.10.4:443 ssl crt /deepmail/ssl
        use_backend webdav_deepmail_backend if { path /webdav } || { path_beg /webdav/ }
```

```
    default_backend ui_deepmail_backend

backend ui_deepmail_backend
    stats uri /haproxy
    stats enable
    stick-table type ip size 1m expire 1h
    stick on src
    server node1 10.10.10.1:443 check send-proxy ssl verify none weight 10
    server node2 10.10.10.2:443 check send-proxy ssl verify none weight 5
    server node3 10.10.10.3:443 check send-proxy ssl verify none weight 3

backend webdav_deepmail_backend
    stats enable
    balance roundrobin
    stick-table type ip size 1m expire 1h
    stick on src
    server node1 10.10.10.1:443 check send-proxy ssl verify none
    server node2 10.10.10.2:443 check send-proxy ssl verify none
    server node3 10.10.10.3:443 check send-proxy ssl verify none

frontend imaps_deepmail_front
    mode tcp
    bind 10.10.10.4:993 ssl crt /deepmail/ssl
    default_backend imaps_deepmail_backend

backend imaps_deepmail_backend
    mode tcp
    balance source
    stick store-request src
    stick-table type ip size 200k expire 30m
```

```
        server node1 10.10.10.1:993 check send-proxy ssl verify none
        server node2 10.10.10.2:993 check send-proxy ssl verify none
        server node3 10.10.10.3:993 check send-proxy ssl verify none

frontend smtp_deepmail_front
        mode tcp
        bind 10.10.10.4:25
        default_backend smtp_deepmail_backend

backend smtp_deepmail_backend
        mode tcp
        server node1 10.10.10.1:25 check send-proxy
        server node2 10.10.10.2:25 check send-proxy
        server node3 10.10.10.3:25 check send-proxy
frontend smtps_deepmail_front
        mode tcp
        bind 10.10.10.4:465 ssl crt /deepmail/ssl
        default_backend smtps_deepmail_backend

backend smtps_deepmail_backend
        mode tcp
        balance roundrobin
        option smtpchk HELO deepmail.io
        server node1 10.10.10.1:465 check send-proxy ssl verify none
        server node2 10.10.10.2:465 check send-proxy ssl verify none
        server node3 10.10.10.3:465 check send-proxy ssl verify none
```

В примере указана конфигурация, которая соответствует схеме почтового кластера Сервера (см. рисунок 97):

- *10.10.10.1* – IP-адрес первой ноды;
- *10.10.10.2* – IP-адрес второй ноды;

- *10.10.10.3* – IP-адрес третьей ноды;
- *10.10.10.4* – IP-адрес HAProxy.

После заполнения файла конфигурации «/etc/haproxy/haproxy.cfg» нужно проверить его на ошибки, при помощи команды *«/usr/sbin/haproxy -c -f /etc/haproxy/haproxy.cfg».*

Если ошибок не обнаружено, то нужно перезапустить сервер-балансировки HAProxy при помощи команды *«systemctl restart haproxy».*

Если ошибки обнаружены, необходимо создать папку «/deepmail/ssl» и скопировать в нее файлы ключа «key.pem» и сертификата «cert.pem» из папки «/deepmail/certs» любой ноды. Далее необходимо переименовать скопированные файлы:

- файл сертификата «cert.pem» в «cert.crt»;
- файл ключа в «key.pem» в «cert.crt.key».

После этого повторить команду *«/usr/sbin/haproxy -c -f /etc/haproxy/haproxy.cfg».*

И перезапустить сервер-балансировки HAProxy выполнив команду *«systemctl restart haproxy».*

Проконтролировать подключение нод к кластеру Сервера можно в веб-интерфейсе администратора, подпункте «Система» вертикального меню «Панель управления», работа с которой представлена далее в пункте 4.2.1.

5.3 Обновление узла Сервера

При установке Сервера в кластере необходимо обновить каждую ноду отдельно.

Распаковать архив, как при установке, командой «*sudo tar -xvzf deepmail-server-*.tar.gz*» (рисунок 107).

```
root@stenddm:/home/testdm# tar -xvzf deepmail-server-*.tar.gz
tar: Ignoring unknown extended header keyword 'LIBARCHIVE.xattr.com.apple.quarantine'
./deepmail-server-1.6/
tar: Ignoring unknown extended header keyword 'LIBARCHIVE.xattr.com.apple.quarantine'
./deepmail-server-1.6/cmd/
tar: Ignoring unknown extended header keyword 'LIBARCHIVE.xattr.com.apple.quarantine'
./deepmail-server-1.6/.HELO
tar: Ignoring unknown extended header keyword 'LIBARCHIVE.xattr.com.apple.quarantine'
./deepmail-server-1.6/cvd/
tar: Ignoring unknown extended header keyword 'LIBARCHIVE.xattr.com.apple.quarantine'
./deepmail-server-1.6/images/
tar: Ignoring unknown extended header keyword 'LIBARCHIVE.xattr.com.apple.quarantine'
./deepmail-server-1.6/deepmail-installer
tar: Ignoring unknown extended header keyword 'LIBARCHIVE.xattr.com.apple.quarantine'
./deepmail-server-1.6/.VERSION
./deepmail-server-1.6/images/admin-service.tar.gz
./deepmail-server-1.6/images/imap-service.tar.gz
./deepmail-server-1.6/images/fetchmail-service.tar.gz
./deepmail-server-1.6/images/webdav-service.tar.gz
./deepmail-server-1.6/images/broker-service.tar.gz
./deepmail-server-1.6/images/webmail-service.tar.gz
./deepmail-server-1.6/images/nginx-service.tar.gz
./deepmail-server-1.6/images/oletools-service.tar.gz
./deepmail-server-1.6/images/smtp-service.tar.gz
tar: Ignoring unknown extended header keyword 'LIBARCHIVE.xattr.com.apple.quarantine'
./deepmail-server-1.6/images/redis.tar.gz
./deepmail-server-1.6/images/antispam-service.tar.gz
./deepmail-server-1.6/images/clamav-service.tar.gz
./deepmail-server-1.6/images/ldap-service.tar.gz
./deepmail-server-1.6/images/resolver-service.tar.gz
tar: Ignoring unknown extended header keyword 'LIBARCHIVE.xattr.com.apple.quarantine'
./deepmail-server-1.6/cvd/daily.cvd
tar: Ignoring unknown extended header keyword 'LIBARCHIVE.xattr.com.apple.quarantine'
./deepmail-server-1.6/cvd/main.cvd
tar: Ignoring unknown extended header keyword 'LIBARCHIVE.xattr.com.apple.quarantine'
./deepmail-server-1.6/cmd/deepmail
root@stenddm:/home/testdm#
```

Рисунок 107 – Распаковка архива с установщиком

Установщик можно запустить с параметром «*--without_antispam*» или «*-was*», при указании данного параметра антиспам сервис будет отключен.

Для обновления нужно запустить установщик командой «*sudo ./deepmail-installer --update*» (с параметром «*--update*» или «*-u*», но это необязательно). Ответ системы на команду обновления показан на рисунке 108.

Рисунок 108 – Ответ системы на команду обновления ноды Сервера

5.3.1 Настройка работы с пограничными серверами

Для настройки пограничного сервера необходимо в файл «deepmail.env» добавить строчку, где будут указаны IP-адреса или подсети кластера DeepMail. Чтобы указать конкретный IP-адрес, а не подсеть, необходимо указать адрес с маской /32.

RELAYNETS=10.10.10.10/32,10.10.102.0/24

После внесенных правок необходимо выполнить команду *«deepmail reload»* на каждой запущенной ноде для вступления настроек в силу.

Далее в интерфейсе администратора нужно перейти в меню «Релейные домены» (рисунок 109) и добавить релейные домены для локальных доменов, что обслуживаются основным кластером DeepMail, нажатием кнопки «Новый Релейный Домен» на вкладке «Список релейных доменов».

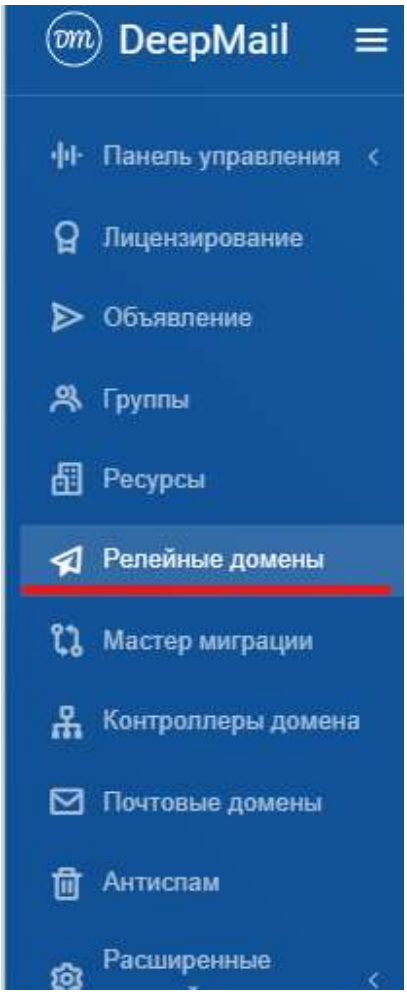


Рисунок 109 – Пункт вертикального меню «Релейные домены»

В открывшейся форме «Новый релейный домен» (рисунок 110) указать доменное имя почтового сервера и удаленный хост (IP-адрес точки входа на основной кластер DeepMail).

Рисунок 110 – Форма «Новый релейный домен»

Поле «Удаленный хост» заполняется следующим образом:

- пустое – хост будет найден по MX записи домена (smtp:domain);
- port – хост будет найден по MX записи домена, будет использоваться заданный порт (smtp:domain:port);
- target – хост будет найден по A/AAA записи (smtp:[target]);
- target:port – хост будет найден по A/AAA записи, будет использоваться заданный порт (smtp:[target]:port);
- mx:target – хост будет найден по MX записи (smtp:target);
- mx:target:port – хост будет найден по MX записи, будет использоваться заданный порт (smtp:target:port).

5.4 Настройка основного пограничного сервера DeepMail

Для отправки почты через созданные пограничные сервера в файле «deepmail.env» необходимо указать параметры «*RELAYHOST*» и «*RELAYNETS*». В нижеуказанном примере «*10.10.10.9*» – IP-адрес точки входа на кластер пограничных серверов, «*10.10.10.7*» и «*10.10.10.8*» – IP-адреса или подсети нод кластера пограничных серверов. Чтобы указать конкретный IP-адрес, а не подсеть, необходимо указать адрес с маской /32, например:

RELAYNETS=10.10.10.7/32,10.10.10.8/32

RELAYHOST=10.10.10.9:25

После внесенных правок необходимо выполнить команду *«deepmail reload»* на каждой запущенной ноде для вступления настроек в силу.

Схема настройки пограничного сервера показана на рисунке 111.

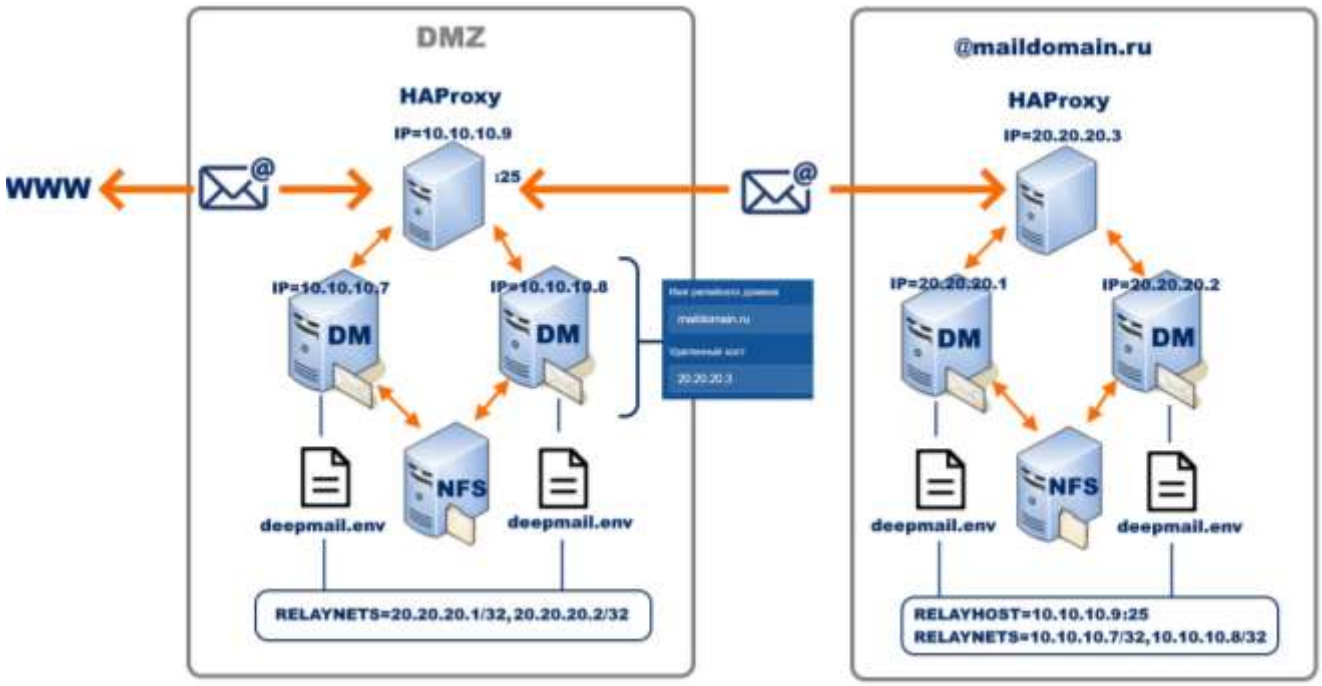


Рисунок 111 – Схема настройки пограничного кластера

5.5 Управление резервным копированием

5.5.1 Создание репозитория резервного копирования

Репозиторий резервного копирования должен создаваться на машине, хранящей резервные копии.

Для создания репозитория резервного копирования администратору необходимо выполнить следующие действия:

- положить бинарный файл в «/usr/bin» выполнив команду «*ls /usr/bin/ | grep deep deepbackup*» (рисунок 112);

```
root@repa:~# ls /usr/bin/ | grep deep
deepbackup
root@repa:~#
```

Рисунок 112 – Создание бинарного файла

- проверить, наличие прав доступа на выполнение выполнив команду «*ls -l /usr/bin/deepbackup*» (рисунок 113). При отсутствии прав доступа назначить их выполнив команду «*chmod a+x /usr/bin/deepbackup*»;

```
root@repa:~# ls -l /usr/bin/deepbackup
-rwxr-xr-x 1 root root 48510262 Apr  2 07:18 /usr/bin/deepbackup
```

Рисунок 113 – Проверка наличия прав на выполнение

- создать каталог для хранения резервных копий в корневом каталоге выполнив команду «*mkdir backups*» (рисунок 114);

```
root@repa:~# mkdir backups
root@repa:~#
```

Рисунок 114 – Создание каталога для хранения резервных копий

- создать репозиторий для хранения резервных копий выполнив команду «*deepbackup repository create filesystem --path /root/backups*». После выполнения команды, система предложит ввести пароль. Он используется для шифрования данных (рисунок 115);

```
root@repa:~# deepbackup repository create filesystem --path=/root
/backups
Enter password to create new repository:
Re-enter password for verification:
Инициализация репозитория с помощью:
  хэш блока:          BLAKE2B-256-128
  шифрование:          AES256-GCM-HMAC-SHA256
  разделитель:            DYNAMIC-4M-BUZHASH
```

Рисунок 115 – Создание пароля репозитория для резервных копий

- после создания репозитория для резервных копий, необходимо подключится к нему, выполнив команду «*deepbackup repository connect filesystem --path=/root/backups*» и ввести созданный ранее пароль (рисунок 116).

```
root@repa:~# deepbackup repository connect filesystem --path=/roo
t/backups
Enter password to open repository:

Подключено к репозиторию
```

Рисунок 116 – Подключение к репозиторию для резервных копий

5.5.2 Настройка сервера-репозитория для резервных копий

После старта и настройки репозитория для резервных копий, администратору необходимо настроить список пользователей, у которых будет доступ к серверу репозитория. Для добавления пользователя, который будет подключаться к серверу репозитория необходимо выполнить команду «*deepbackup server user add <имя пользователя>@<hostname>*» (рисунок 117).

```
root@repa:~# deepbackup server user add root@mail
Введите новый пароль для пользователя root@mail:
Повторно введите новый пароль для проверки:

        Обновленные учетные данные пользователя вступят в силу че
рез 5-10 минут или после перезапуска сервера.
        Чтобы обновить учетные данные на работающем сервере, испо
льзуйте команду "deepbackup server refresh".
```

Рисунок 117 – Добавление пользователя репозитория

Также администратору доступны команды:

- «*deepbackup server user list*» – позволяет вывести список пользователей;
- «*deepbackup server user set*» – позволяет сменить пароль пользователя;
- «*deepbackup server user delete*» – позволяет удалить пользователя.

После создания пользователя необходимо создать сертификаты, для этого необходимо запустить сервер-репозиторий вручную выполнив несколько команд:

«*deepbackup server start* \

--tls-generate-cert \

--tls-cert-file /root/my.cert \

--tls-key-file /root/my.key \

--address 0.0.0.0:51515 \

--server-control-username control \

--server-control-password <ПАРОЛЬ>»

Данную процедуру необходимо выполнить один раз.

При использовании собственных сертификатов в выполнении данной команды нет необходимости.

В результате выполнения команды будут сгенерированы файлы сертификата TLS и ключа, которые будут сохранены в каталогах «~/my.cert» и «~/my.key» соответственно, а также будет сгенерирован отпечаток сертификата SHA256 (рисунок 118), который будет использован позже.

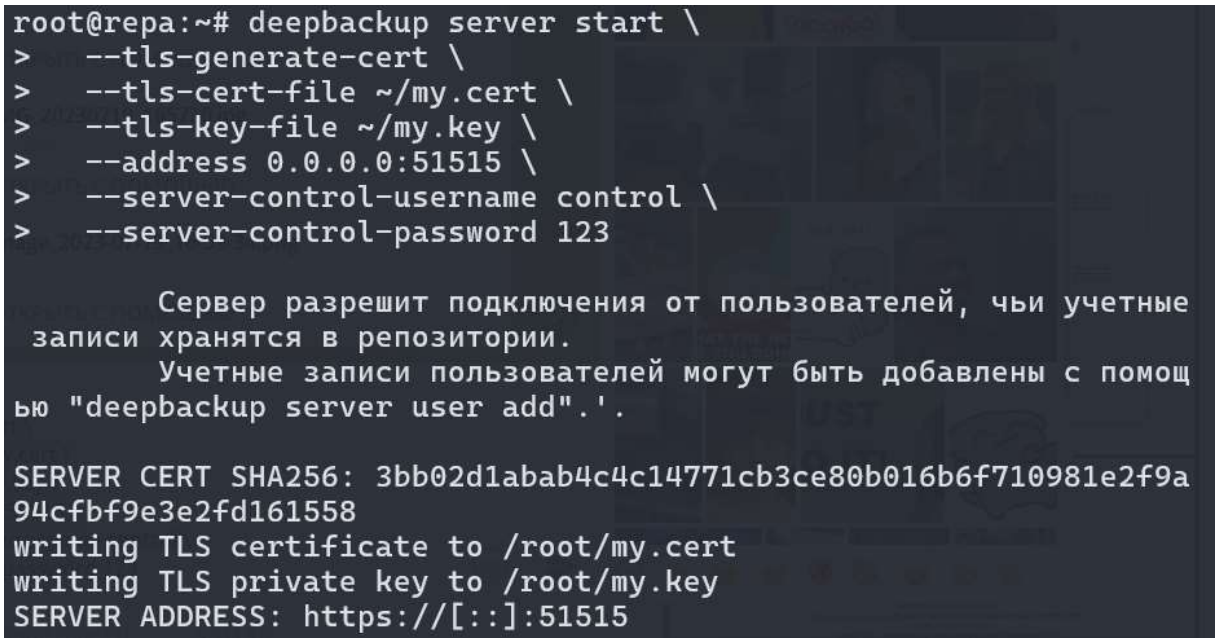


Рисунок 118 – Создание сертификатов и ключа отпечатка

После создания сертификатов необходимо запустить сервер как службу, для этого в каталоге «/lib/systemd/system/» необходимо создать файл «deepbackup.service», выполнив команду «*sudo touch /lib/systemd/system/deepbackup.service*».

В созданный файл «deepbackup.service» необходимо записать следующее содержимое:

[Unit]

Description=DeepBackup Server

After=syslog.target

After=network.target

[Service]

Type=simple

User=root

Group=root

ExecStart=/usr/bin/deepbackup server start --tls-cert-file /root/my.cert --tls-key-file /root/my.key --address 0.0.0.0:51515 --server-control-username control --server-control-password <ПАРОЛЬ>

#Restart=always

RestartSec=5

[Install]

WantedBy=multi-user.target

EditorConfig

После чего запустить службу командой «*systemctl daemon-reload systemctl start deepbackup.service*» (рисунок 119).

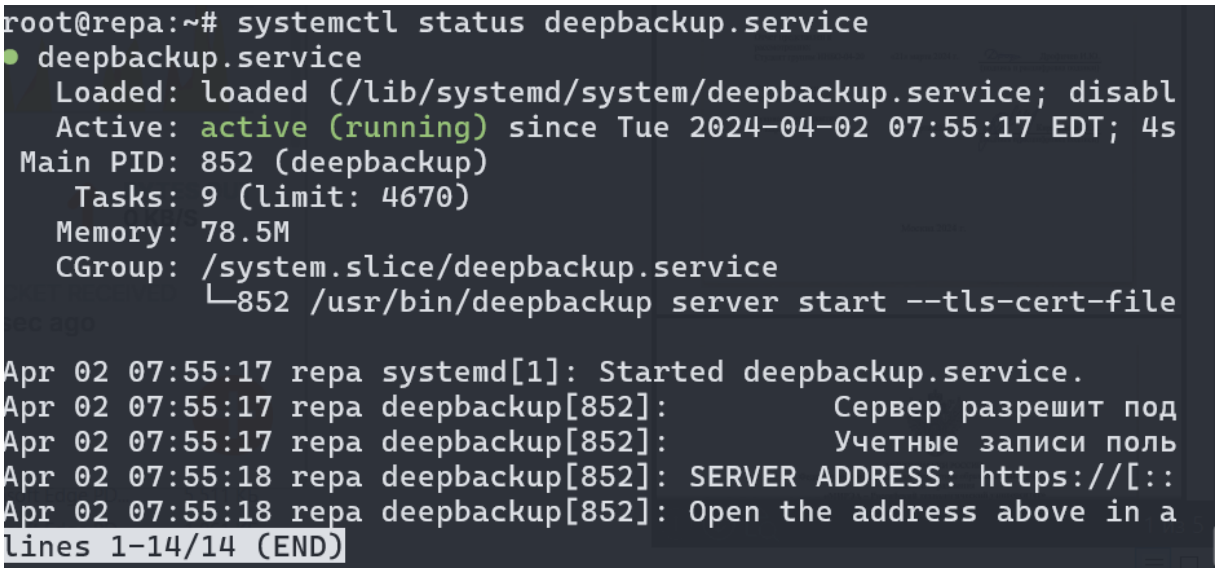


Рисунок 119 – Ответ системы на команду запуска службы «deepbackup.service»

Чтобы узнать ключ, который понадобится для подключения к серверу репозитория, администратору необходимо выполнить команду «*openssl x509 -in ~/my.cert -noout -fingerprint -sha256 | sed 's/://g'*».

5.5.3 Подключение к серверу репозитория и настройка политик

Для подключения к серверу репозитория на почтовом сервере необходимо выполнить следующие действия:

- убедиться, что администратор имеет права на исполнение в каталоге «/usr/bin» (при необходимости выдать права). Убедиться, что в каталоге «/usr/bin» распложен исполняемый файл «deepbackup»;
- выполнить подключение к серверу репозитория через UI, либо через команду «deepbackup ui». При подключении через UI, утилита проверяет наличие директории «/deepmail». Если её не удастся найти, то будет предложен ввод пути вручную. Если путь найден, то в соответствующей вкладке меню необходимо ввести данные настроенного сервера репозитория (рисунок 120).

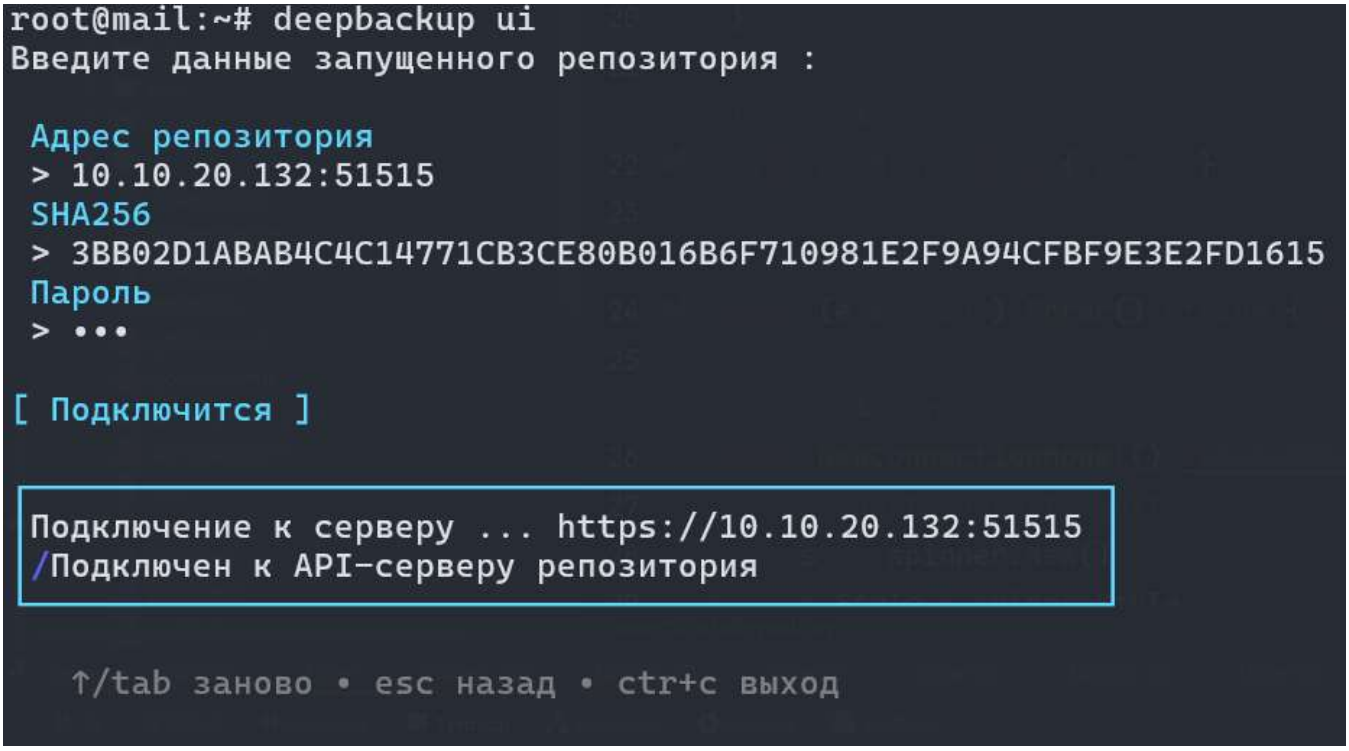


Рисунок 120 – Ввод данных для связи с удаленным ренпозиторием

В каталоге «/deepmail/» будет создан подкаталог «.deepbackupconfig», в котором будут созданы конфигурационные файлы со сведениями для подключения к репозиторию (рисунок 121).

```
root@mail:~# ls -a /deepmail/
.  ..  .deepbackupconfig
root@mail:~# ls -a /deepmail/.deepbackupconfig/
.  ..  repository.config  repository.config.deepbackup-password
root@mail:~#
```

Рисунок 121 – Созданные файлы конфигурации в директории «/deepmail/»

При повторном открытии UI, при наличии файла с данными для подключения поля будут заполнены известными сведениями (рисунок 122).

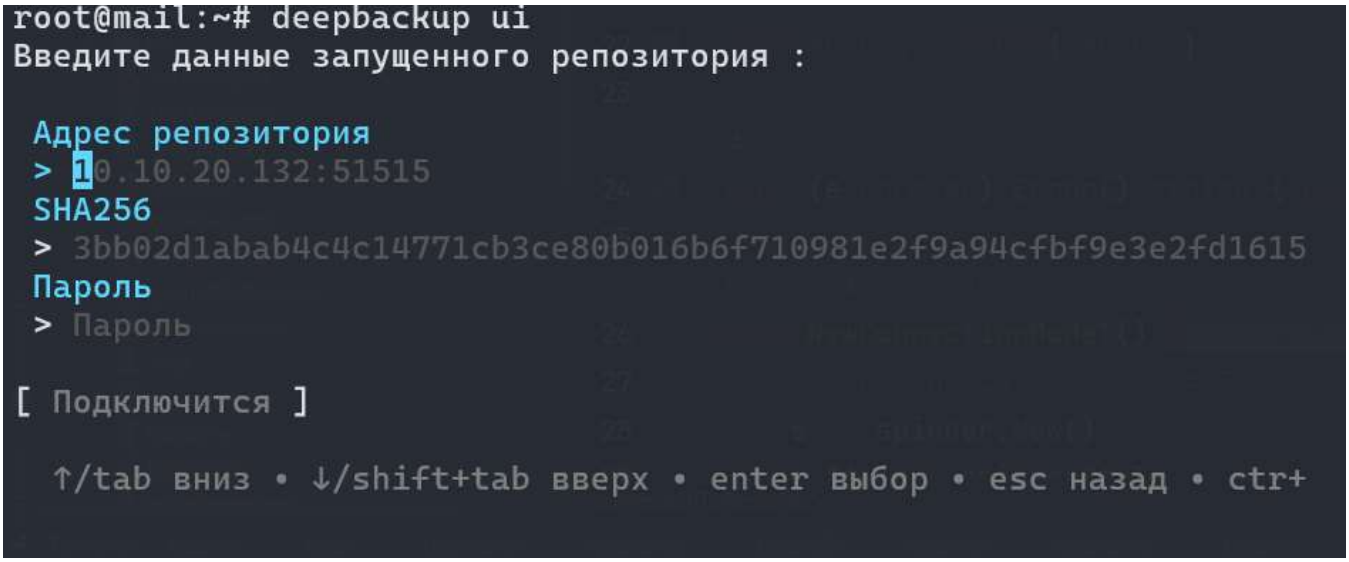


Рисунок 122 – Повторный запуск deepbackup UI, поля заполнены

Для подключения к серверу репозитория через консоль необходимо выполнить команду «*deepbackup repository connect server --url=https://10.10.20.132:51515 --server-cert-fingerprint <ключ> --config-file /deepmail/.deepbackupconfig/repository.config*».

После флага «*--server-cert-fingerprint*» необходимо указать отпечаток сертификата SHA256, полученный при настройке сервера репозитория.

После настройки подключения, перед созданием резервных копий, необходимо настроить правила, которые будут определять: правила игнорирования определенных файлов (директорий), а также количество хранимых резервных копий.

Чтобы добавить игнорирование определенных файлов или директорий при резервном копировании (только после подключения репозитория) необходимо

выполнить команду «*deepbackup policy set --add-ignore=dovecot* /deepmail --config-file /<ПУТЬ К ДИРЕКТОРИИ /deepmail>/.deepbackupconfig/repository.config*».

В результате выполнения вышеуказанной команды, будут проигнорированы все файлы и папки начинающиеся на «dovecot» (рисунок 123).

```
root@mail:~# deepbackup policy set --add-ignore=dovecot* /deepmai
l --config-file /deepmail/.deepbackupconfig/repository.config
Настройка политики для root@mail:/deepmail
 - добавление "dovecot*" в "ignore rules"
root@mail:~#
```

Рисунок 123 – Ответ системы на игнорирование копирования папок

Ключ «*--add ignore*» задает правила игнорирования.

В качестве примера, настроим игнорирование папки «DeepDav.cache». Для этого необходимо выполнить команду «*deepbackup policy set --add-ignore=**/.DeepDav.cache/** /deepmail --config-file /<ПУТЬ К ДИРЕКТОРИИ /deepmail>*/.deepbackupconfig/repository.config».

По умолчанию в системе хранится до 10 резервных копий каждой категории (недавние снимки, ежедневные и так далее). То есть при создании подряд больше 10 резервных копии, самые старые будут удаляться, чтобы увеличить это значение необходимо установить правило определяющее количество хранимых резервных копий.

Для указания количества хранимых копий необходимо выполнить команду «*deepbackup policy set --keep-latest=500 /deepmail --config-file / <ПУТЬ К ДИРЕКТОРИИ /deepmail>/.deepbackupconfig/repository.config*».

В результате выполнения команды (рисунок 124) количество хранимых резервных копий увеличено до 500.

```
root@mail:~# deepbackup policy set --keep-latest=500 /deepmail --
config-file /deepmail/.deepbackupconfig/repository.config
Настройка политики для root@mail:/deepmail
 - установка "number of latest backups to keep" в значение 500.
root@mail:~#
```

Рисунок 124 – Ответ системы на изменение числа хранимых копий

Вместо флагов «*--keep-latest*» возможно указание флага:

- «*--keep-annual=500*» – количество самых последних ежегодных резервных копий;
- «*--keep-monthly=500*» – количество самых последних ежемесячных резервных копий;
- «*--keep-weekly=500*» – количество самых последних недельных резервных копий;
- «*--keep-daily=500*» – количество самых последних ежедневных резервных копий;
- «*--keep-hourly=500*» – количество самых последних почасовых резервных копий.

5.5.4 Запуск системы резервного копирования DeepBackup

Запуск системы резервного копирования DeepBackup происходит командой «*deepbackup ui*», после чего появится интерфейс пользователя, показанный на рисунке 125.

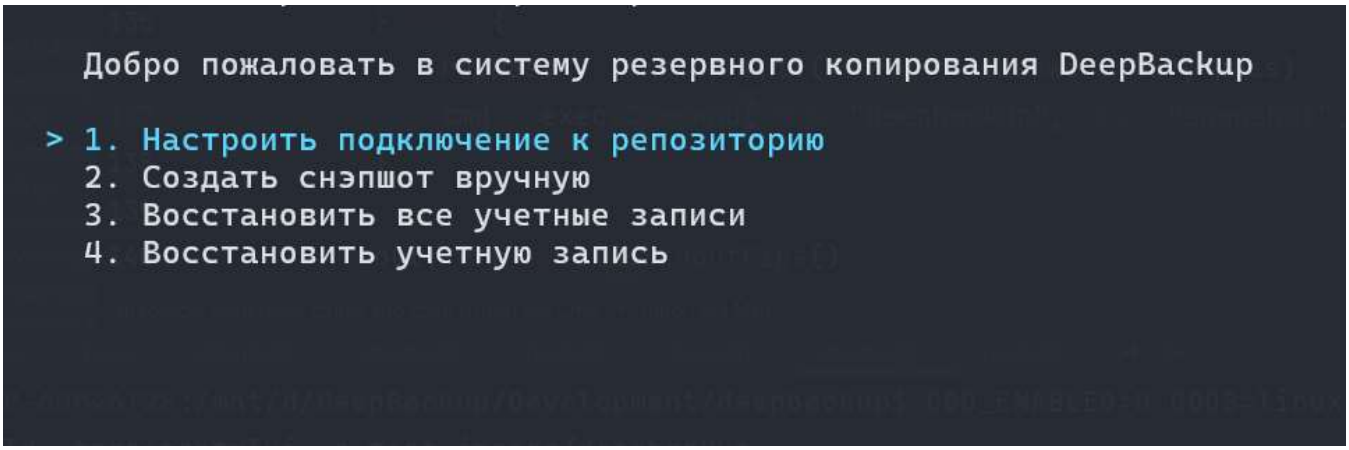


Рисунок 125 – Интерфейс системы резервного копирования DeepBackup

Для подключения к репозиторию администратору необходимо выбрать пункт «Настроить подключение к репозиторию» и ввести IP-адрес репозитория, а также ввести отпечаток сертификата SHA256, полученный при настройке сервера репозитория и пароль (рисунок 126).

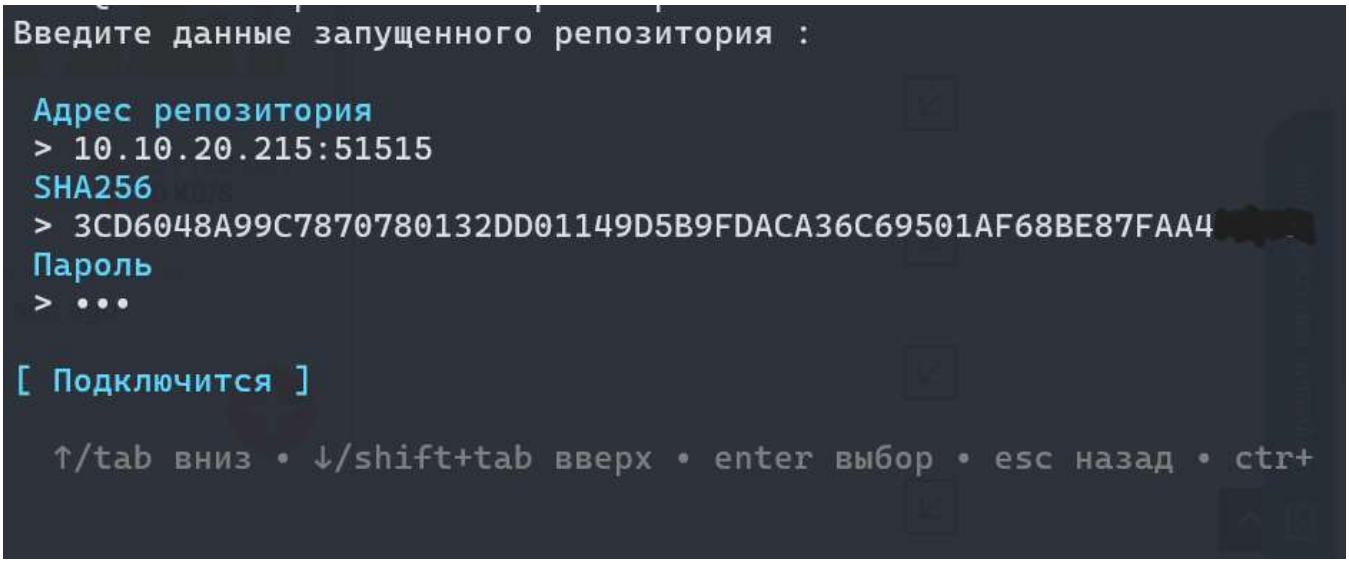


Рисунок 126 – Ввод настроек при первом подключении к репозитрию

В случае успешного подключения появится соответствующая надпись (рисунок 127).

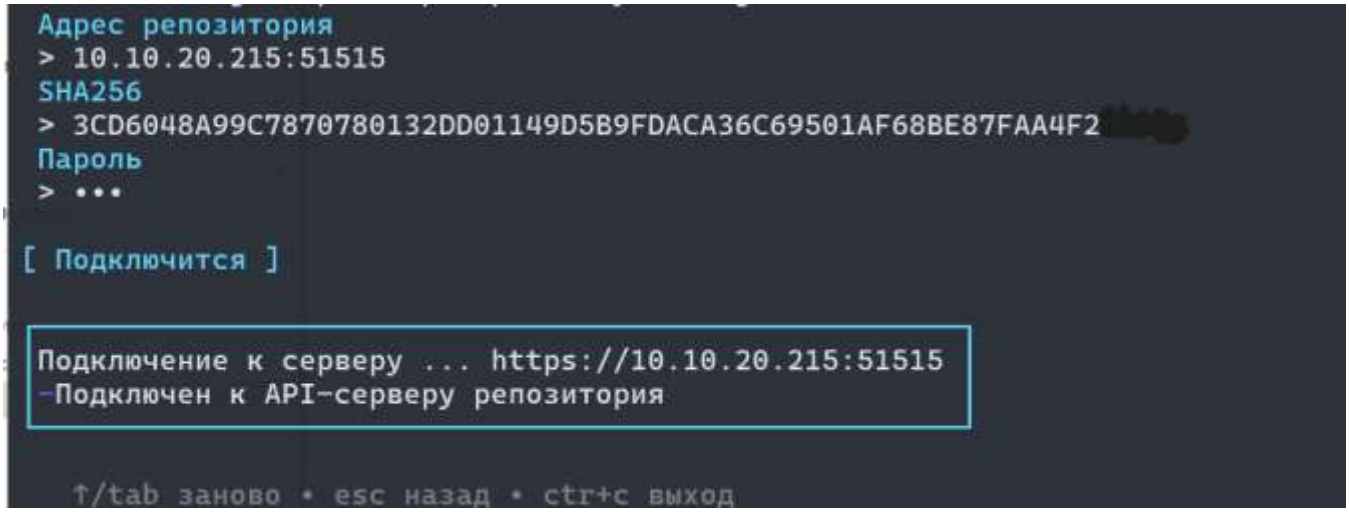


Рисунок 127 – Успешное подключение к серверу репозитория

5.5.1 Создание резервной копии

Для создания резервной копии почты достаточно перейти в соответствующий пункт меню, ввести пароль от репозитория и нажать клавишу «Enter» (рисунок 128).

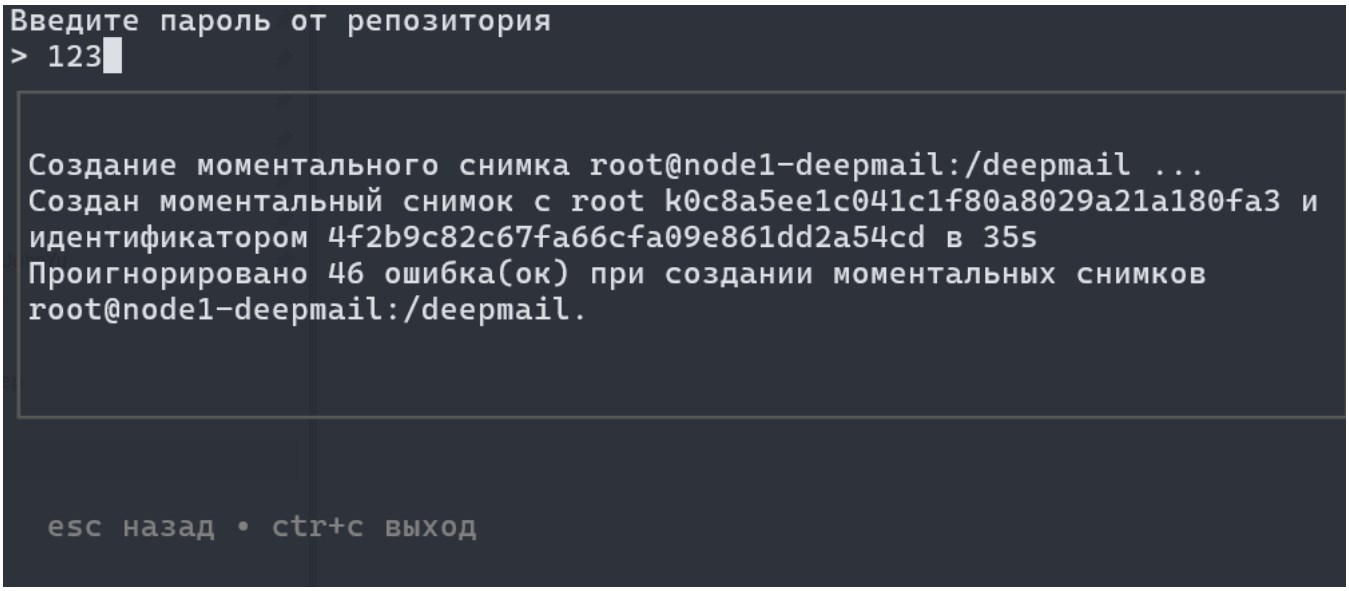


Рисунок 128 – Ответ системы на создание моментального снимка

5.5.2 Восстановление учетных записей

Для восстановления учетной записи администратору необходимо выбрать соответствующий пункт меню (см. рисунок 125), выбрать необходимую резервную копию (рисунок 129) и нажать клавишу «Enter». После этого указать опцию восстановления (почту или коллекцию) и нажать на кнопку «Восстановить» (рисунок 130).

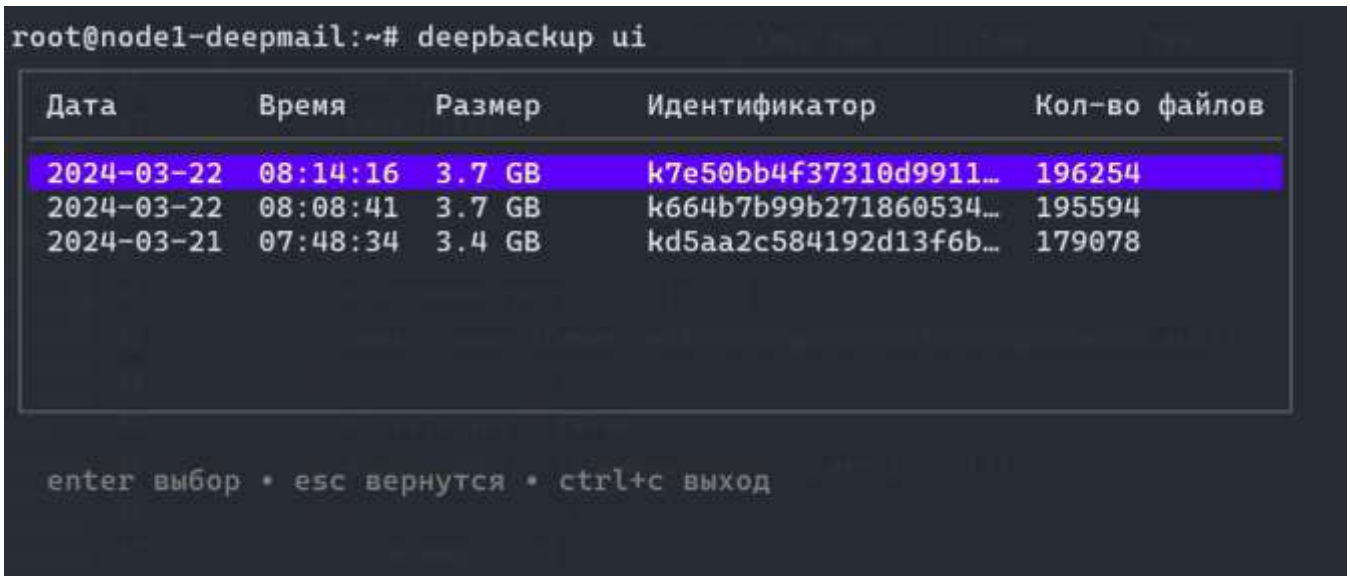


Рисунок 129 – Выбор снимка учетной записи

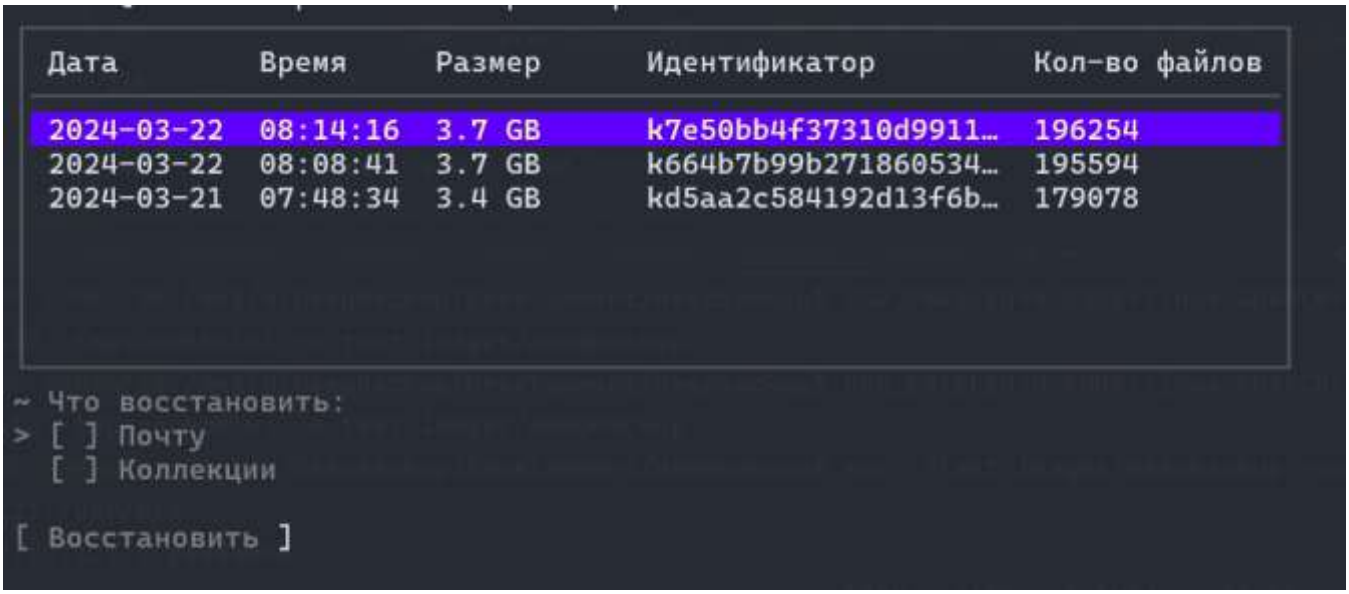


Рисунок 130 – Выбор параметров восстановления (почта или коллекции)

Далее необходимо выбрать аккаунт для восстановления, и отметить, какие данные требуется восстановить (рисунок 131).

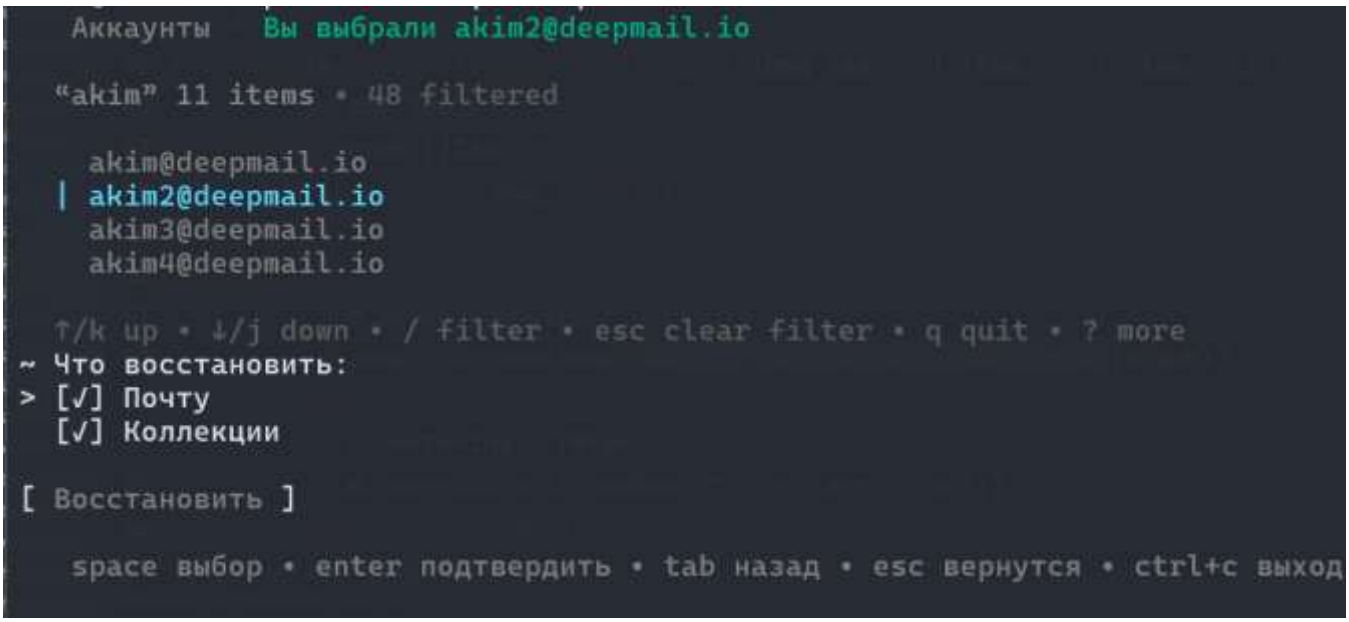


Рисунок 131 – Выбор аккаунта для восстановления

5.5.3 Запуск сервера-репозитория в качестве сервиса

Для запуска сервера репозитория в качестве сервиса администратору необходимо создать файл «/lib/systemd/system/deepbackup.service» с содержимым:

[Unit]

Description=DeepBackup Server

After=syslog.target

After=network.target

[Service]

Type=simple

User=root

Group=root

ExecStart=/usr/bin/deepbackup server start --tls-cert-file /root/my.cert --tls-key-file /root/my.key --address 0.0.0.0:51515 --server-control-username control --server-control-password 123

#Restart=always

RestartSec=5

[Install]

WantedBy=multi-user.target

Запустить перезагрузку служб командой «*systemctl daemon-reload*»

Запустить сервис репозитория на сервере командой «*systemctl start deepbackup.service*» (рисунок 132).

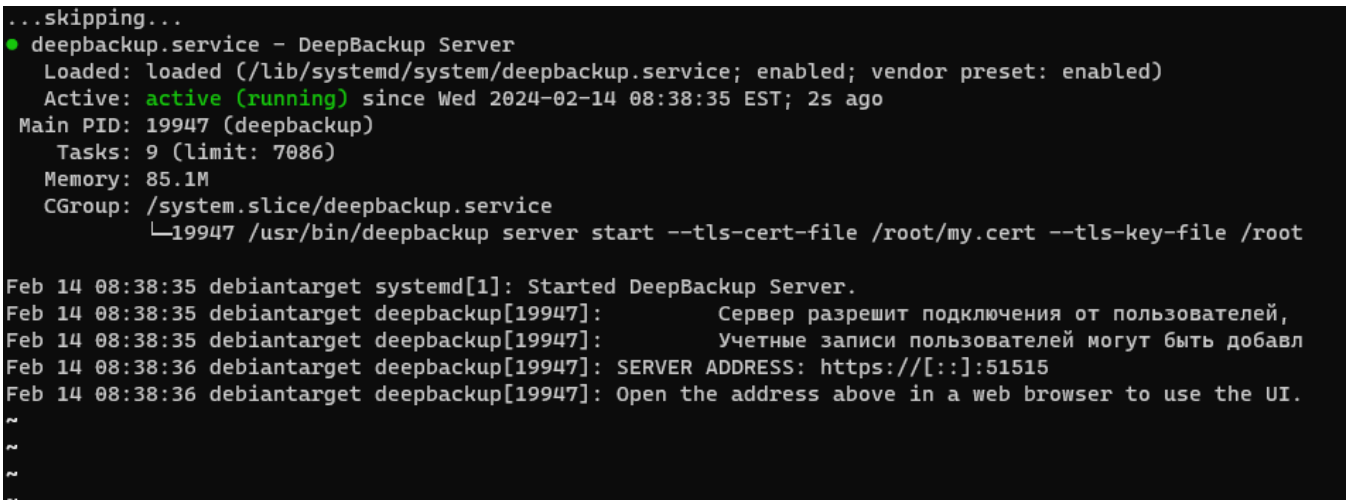


Рисунок 132 – Ответ системы на запуск сервиса репозитория

5.5.4 Файлы конфигурации

Файлы конфигурации на стороне клиента хранятся в директории «/deepmail/.deepbackupconfig» (рисунок 133).

```
root@node1-deepmail:~# ls /deepmail/.deepbackupconfig/
repository.config  repository.config.deepbackup-password
```

Рисунок 133 – Файлы конфигурации репозитория

Пароль репозитория хранится в зашифрованном виде (рисунок 134)

```
root@repa:~# cat /root/.config/deepbackup/repository.config.deepb
ackup-password
MTIzroot@repa:~#
```

Рисунок 134 – Файл пароля

Содержимое конфигурационного файла на стороне клиента сервера-репозитория показано на рисунке 135.

```
root@mail:~# cat /deepmail/.deepbackupconfig/repository.config
{
  "apiServer": {
    "url": "https://10.10.20.132:51515",
    "serverCertFingerprint": "3bb02d1abab4c4c14771cb3ce80b016b6f7
10981e2f9a94cfbf9e3e2fd161558"
  },
  "caching": {},
  "hostname": "mail",
  "username": "root",
  "description": "API Server: https://10.10.20.132:51515",
  "enableActions": false,
  "formatBlobCacheDuration": 900000000000
}root@mail:~#
```

Рисунок 135 – Содержимое конфигупационного файла репозитория (на стороне клиента)

Содержимое конфигурационного файла на стороне сервера-репозитория показано на рисунке 136.

```
root@repa:~# cat /root/.config/deepbackup/repository.config
{
  "storage": {
    "type": "filesystem",
    "config": {
      "path": "/root/backups",
      "fileMode": 384,
      "dirMode": 448,
      "dirShards": null
    }
  },
  "caching": {
    "cacheDirectory": "../../.cache/deepbackup/29ca5f8589ca2d45",
    "maxCacheSize": 5242880000,
    "maxMetadataCacheSize": 5242880000,
    "maxListCacheDuration": 30
  },
  "hostname": "repa",
  "username": "root",
  "description": "Repository in Filesystem: /root/backups",
  "enableActions": false,
  "formatBlobCacheDuration": 900000000000
}root@repa:~#
```

Рисунок 136 – Содержимое конфигурационного файла на сервере-репозитории

5.5.5 Создание снапшота

Первое что надо сделать для создания снапшота – это создать репозиторий, где будут хранится снапшоты, и подключиться к нему. После создания репозитория и подключения к нему можно создавать снапшоты.

Администратор должен выполнить команду «*deepbackup snapshot create <директория с файлами>*»

После создания снапшота печатается идентификатор корня моментального снимка, который начинается с «k…» *«uploaded snapshot 9a622e33ab134ef440f76ed755f79c2f (root kfe997567fb1cf8a13341e4ca11652f70) in 1m42.044883302s».*

Все снапшоты в deepbackup – инкрементные. Это значит, что какие-либо данные загружаются единожды, а после перезагружаются только фалы, которые изменились.

Множество повторяющихся файлов хранятся в единственном экземпляре за счет встроенной дедупликации.

Deepbackup создает снапшот из файлов или директорий, которые вам требуются, после шифрует снапшот прежде, чем он покинет компьютер, а после загружает зашифрованные снапшоты на требуемое хранилище в подключенный репозиторий.

Посмотреть историю снапшотов можно с помощью команды *«deepbackup snapshot list».*

Пример истории снапшотов показан на рисунке 137.

```
 deepbackup snapshot list $HOME/Projects/github.com/deepbackup/deepbackup
username:путь
  2024-03-22 20:15:51 PDT kb9a8420bf6b8ea280d6637ad1adbd4c5 61.4 MB drwxr-xr-x f
  + 1 identical snapshots until 2024-03-22 20:15:57 PDT
  2024-03-22 20:21:39 PDT kbb7dd85a55ca79f282b59b57e5f9c479 61.4 MB drwxr-xr-x f
```

Рисунок 137 – Пример истории снапшотов

Чтобы сравнить два снапшота администратору необходимо выполнить команду «*deepbackup diff <id1> <id2>*».

Чтобы посмотреть содержимое снапшота администратору необходимо выполнить команду «*deepbackup ls -l <id>*».

Для каждого файла и директории в директории хранится имя, размер, атрибуты и идентификатор объекта.

Для изучения свойств объекта администратору необходимо выполнить команду «*deepbackup show -j <id_объекта>»*. Параметр «-j» указывает на то, что вывод данных будет в формате JSON. Таким образом команда: «*deepbackup content show -j kb9a8420bf6b8ea280d6637ad1adbd4c5*» вернет свойства объекта (рисунок 138).

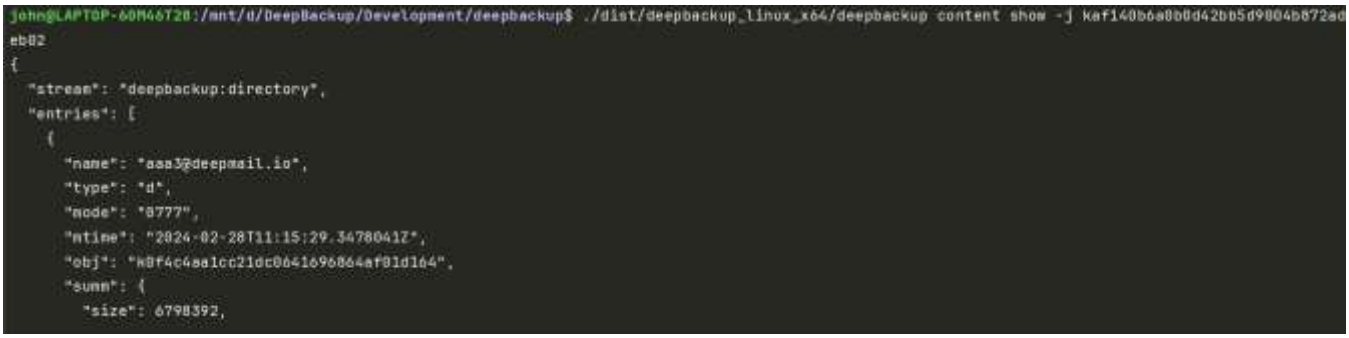


Рисунок 138 – Отображение свойств объекта в формате JSON

5.5.6 Восстановление снапшота

Существует два пути восстановления снапшота:

- через монтирование;
- с помощью команды «*deepbackup restore*».

Для монтирования снапшота администратору необходимо выполнить следующие действия:

- создать папку для монтирования выполнив команду «*mkdir /tmp/mnt*»;
- выполнить монтирование файла снимка выполнив команду «*deepbackup mount <имя файла снэпшота> /tmp/mnt*».

Для восстановления снапшота с помощью команды «*deepbackup restore*» администратору необходимо выполнить команду «*deepbackup snapshot restore <sources>*».

Восстановление выполняется из снапшота: восстановление (возможно, поверхностное) указанного файла или каталога из снапшота в целевой путь. По умолчанию целевой путь будет создан командой восстановления, если он не существует (рисунок 139).

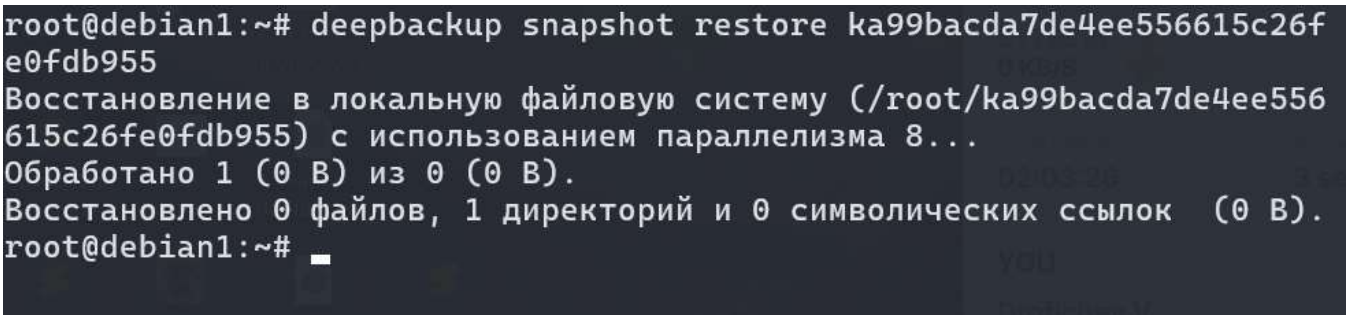


Рисунок 139 – Ответ системы на команду восстановления снимка

Также можно восстанавливать отдельную директорию или отдельный файл, для этого после идентификатора резервной копии необходимо указать путь. Пример *«deepbackup snapshot restore <id>/path»*.

У команды «*deepbackup restore*» есть флаги, корректирующие поведение при восстановлении, когда конечный элемент уже существует:

- «*-no-overwrite-files*» – не переписывать файлы;
- «*-no-overwrite-directories*» – не переписывать директории;
- «*-no-overwrite-symlinks*» – не переписывать символические ссылки.

5.6 Управление почтовой очередью

Для управления почтовой очередью администратор должен зайти в контейнер сервиса SMTP, используя команду «*sudo docker exec -it deepmail-smtp bash*».

Для наблюдения очереди администратору необходимо выполнить команду *«postsuper -r ALL»* (рисунок 140).

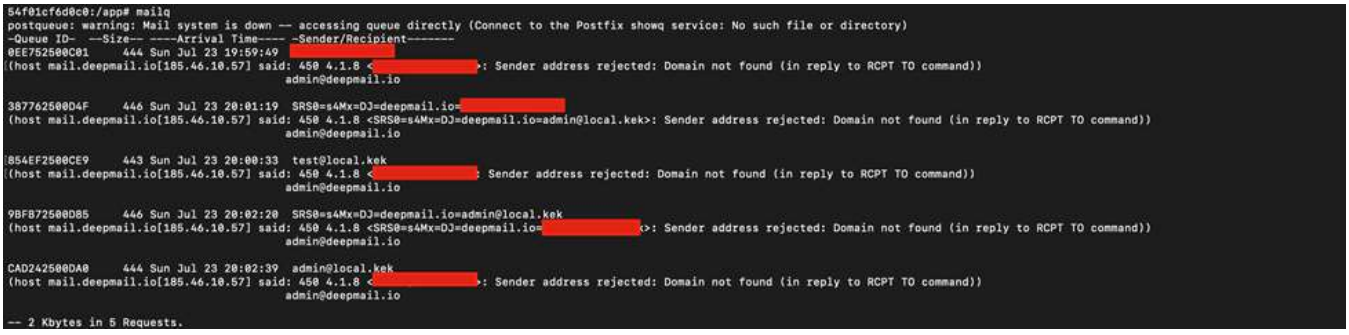


Рисунок 140 – Просмотр почтовой очереди

Для удаления письма из очереди администратору необходимо выполнить команду *«postsuper -d <ID письма>»* (рисунок 141).

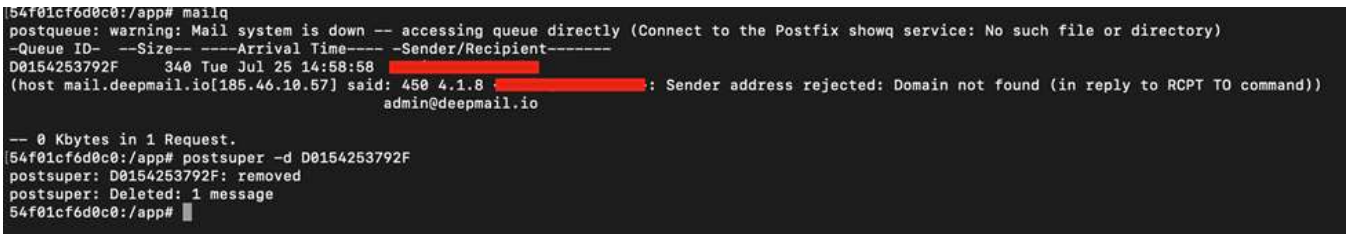


Рисунок 141 – Ответ системы на команду удаления письма из очереди

Для удаления всех писем из очереди администратор должен набрать команду *«postsuper -d ALL»*.

5.7 Подключение внешней базы данных

ВНИМАНИЕ! Если вы собираетесь переносить базу данных, прочитайте данную статью до конца перед началом работ.

Для подключения внешней базы данных необходимо указать данные для подключения в конфигурационном файле «deepmail.env», который находится в корне хранилища DeepMail, необходимо заполнить следующие переменные для подключения:

- DB_FLAVOR – тип базы данных;
- DB_HOST – ip адрес базы данных;
- DB_USER – пользователь для входа;
- DB_PW – пароль для входа;
- DB_NAME – имя базы данных;
- DEEPMAILWEB_DB_FLAVOR – тип базы данных для веб-клиента;
- DEEPMAILWEB_DB_HOST – ip адрес базы данных для веб-клиента;
- DEEPMAILWEB_DB_USER – пользователь для входа для веб-клиента;
- DEEPMAILWEB_DB_PW – пароль для входа для веб-клиента;
- DEEPMAILWEB_DB_NAME – имя базы данных для веб-клиента.

Пример задания переменных для СУБД **PostgreSQL**:

DB_FLAVOR=postgresql
DB_HOST=10.10.10.10
DB_USER=deepmail
DB_PW=deepmail
DB_NAME=deepmail

DEEPMAILWEB_DB_FLAVOR=postgresql
DEEPMAILWEB_DB_HOST=10.10.10.10
DEEPMAILWEB_DB_USER=deepmail

DEEPMAILWEB_DB_PW=deepmail

DEEPMAILWEB_DB_NAME=deepmailweb

Порт подключения по умолчанию – «*5432*». Для указания нестандартного порта подключения нужно указать его в переменной «DB_HOST/ DEEPMAILWEB_DB_HOST», например, *DB_HOST=10.10.10.10:1234*.

Пример задания переменных для СУБД **MySQL**:

DB_FLAVOR=mysql

DB_HOST=10.10.10.10

DB_USER=deepmail

DB_PW=deepmail

DB_NAME=deepmail

DEEPMAILWEB_DB_FLAVOR=mysql

DEEPMAILWEB_DB_HOST=10.10.10.10

DEEPMAILWEB_DB_USER=deepmail

DEEPMAILWEB_DB_PW=deepmail

DEEPMAILWEB_DB_NAME=deepmailweb

Порт подключения по умолчанию – «*5432*». Для указания нестандартного порта подключения нужно указать его в переменной «DB_HOST/ DEEPMAILWEB_DB_HOST», например, *DB_HOST=10.10.10.10:1234*,

Для вступления изменений в силу необходимо выполнить команду «*deepmail relaod*», после чего почтовые сервисы должны обновиться (рисунок 142).

Рисунок 142 – Обновление сервисов

Если необходимо перенести данные из старой базы данных в новую, то перед изменениями в файле конфигурации «deepmail.env» нужно выполнить команду «*deepmail export*» (рисунок 143).

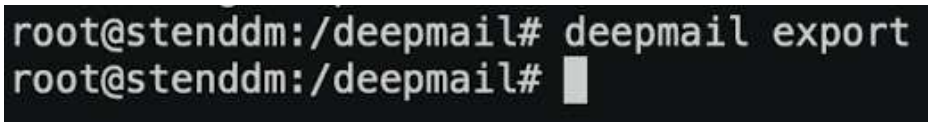


Рисунок 143 – Команда для экспортирования базы данных

После подключения внешней базы данных нужно проверить экспортированные данные командой «*deepmail import -validate*» (рисунок 144).

Рисунок 144 – Ответ системы на экспортированные данные

Если ошибок не обнаружено, то можно производить импорт командой «*deepmail import*» (рисунок 145).

Рисунок 145 – Ответ системы на импортирование базы данных