АО «Иридиум»

РУКОВОДСТВО АДМИНИСТРАТОРА

Автоматизированное рабочее место абонента
электронной почты DEEPMAIL
(Серверная часть «DEEPMAIL модуль взаимодействия»)

RU.УГСФ.00003-01 90 01

Листов 105

2025

АННОТАЦИЯ

Настоящий документ содержит руководство администратора по установке и настройке программного обеспечения на почтовом сервере «DEEPMAIL SERVER» (Серверной части «DEEPMAIL модуль взаимодействия») (далее – «Сервер») автоматизированного рабочего места абонента электронной почты «DeepMail» (далее – «АРМ «DeepMail»»), работающей под управлением операционных систем Альт, Astra Linux, Debian, Ubuntu и РЕДОС.

В руководстве администратора приведены:

- порядок установки и настройки Сервера;
- порядок создания почтовых доменов;
- порядок добавления контроллера почтового домена;
- порядок настройки синхронизации почтовых доменов;
- порядок настройки DNS почтового домена;
- порядок управления пользователями почтового домена;
- порядок создания, редактирования и удаления групп пользователей;
- порядок управления общими почтовыми ящиками;
- порядок управления лицензиями;
- порядок настройки объявлений;
- порядок настройки мастера миграции.

Описание порядка работы с клиентской части под управлением ОС Linux, Windows и Android приведено в:

- RU.УГСФ.00003-01 34 01 Руководство пользователя. Автоматизированное рабочее место абонента электронной почты «DeepMail» (Клиентская часть для работы под управлением операционной системы Linux);
- RU.УГСФ.00003-01 34 02 Руководство пользователя. Автоматизированное рабочее место абонента электронной почты «DeepMail» (Клиентская часть для работы под управлением операционной системы Windows);
- RU.УГСФ.00003-01 34 03 Руководство пользователя. Автоматизированное рабочее место абонента электронной почты «DeepMail» (Клиентская часть для работы под управлением операционной системы Android).

СОДЕРЖАНИЕ

1 ОБЩИЕ СВЕДЕНИЯ

Сервер предназначен для комплексного управления электронной почтой, календарями и адресными книгами пользователей.

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

Сервер обеспечивает:

- 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;
- возможность работы под управлением российских сертифицированных ОС, таких как: Альт и Astra Linux, Ред ОС;
- возможность работы на российских системах виртуализации (ПК «Звезда», ПК «Иридиум»);
- защита от спама и вирусов;
- возможность миграции почтовых баз и учетных записей пользователей с любого почтового сервера, в том числе с Microsoft Exchange Server;
- протоколирование событий;
- возможность работы со сторонними пользователями (в базовой функциональности для обмена почтовыми сообщениями, а также для работы с календарями и адресными книгами);
- взаимодействие с различными исполнениями клиентской части АРМ «DeepMail» с реализованной системой защиты информации безопасности в соответствии с требованиями ГОСТ;
- работу бот-платформы для интеграции с корпоративными ресурсами;

автоматизацию обработки стандартизованных запросов в электронной почте и встроенном мессенджере.

1.1 Условия, необходимые для функционирования изделия

1.1.1 Требования к техническим средствам

Требования к техническим средствам представлены в таблице 1.

Таблица 1 – 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	

1.1.2 Требования к программным средствам

Сервер функционирует в операционных системах: 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.

Для комплексного отслеживания работы всех сервисов и метрик Сервера АРМ «DeepMail» рекомендуется использовать систему мониторинга Zabbix. В рамках этой интеграции применяется готовый, предварительно настроенный шаблон Zabbix, который включает все необходимые параметры контроля. Подключение между сервером Zabbix и узлами АРМ «DeepMail» осуществляется через агента zabbix-agent2, обеспечивающего безопасный сбор данных и двустороннюю синхронизацию. Это решение позволяет централизованно анализировать производительность, оперативно выявлять сбои и сокращает время на развертывание системы мониторинга.

1.1.3 Обеспечение мониторинга

Для комплексного отслеживания работы всех сервисов и метрик Сервера АРМ «DeepMail» рекомендуется использовать систему мониторинга Zabbix. В рамках этой интеграции применяется готовый, предварительно настроенный шаблон Zabbix, который включает все необходимые параметры контроля. Подключение между сервером Zabbix и узлами АРМ «DeepMail» осуществляется через агента zabbix-agent2, обеспечивающего

безопасный сбор данных и двустороннюю синхронизацию. Это решение позволяет централизованно анализировать производительность, оперативно выявлять сбои и сокращает время на развертывание системы мониторинга.

В поставляемом с дистрибутивом шаблоне Zabbix для DeepMail реализовано обеспечение базового мониторинга работы всех основных сервисов почтовой платформы DeepMail, развернутой в Docker контейнерах. Каждый сервис отслеживается на предмет доступности критичных сервисов DeepMail, потреблению системных ресурсов сервисами, состоянию сетевого обмена, проблемам (Drop/Error), а в случае SMTP – размеру очереди писем.

В сводной таблице 2 приведены данные по основным сервисам и метрикам, которые настроены в шаблоне *zabbix_deepmail-2.0-4.yaml* для мониторинга.

Таблица 2 – Параметры *zabbix_deepmail-2.0-4.yaml*

Сервис	Статус контейнера	CPU	RAM	Входящий трафик	Исходящий трафик	Drop/Error Network	Особые показатели
admin	+	+	+	+	+	+	
antispam	+	+	+	+	+	+	
auth	+	+	+	+	+	+	
fetchmail	+	+	+	+	+	+	
front	+	+	+	+	+	+	
imap	+	+	+	+	+	+	
ldap	+	+	+	+	+	+	
oletools	+	+	+	+	+	+	
resolver	+	+	+	+	+	+	
smtp	+	+	+	+	+	+	Почтовая очередь
webdav	+	+	+	+	+	+	
webmail	+	+	+	+	+	+	

Примечание:

- статус контейнера – это Alive/dead (up/down) каждого сервиса через Docker API;
- CPU – это потребление CPU контейнера;
- RAM – это потребление памяти контейнера;
- входящий/исходящий трафик – это объём входящих/исходящих байтов по сети;

- Drop/Error Network – это отслеживание ошибок и потерь пакетов в сетевом стеке каждого контейнера;

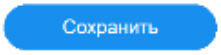
- почтовая очередь – это отслеживание размера активной очереди писем.

1.1.4 Обеспечение интеграции антивируса KSMG с DeepMail

1.1.4.1 Подготовка и резервное копирование

Настройка производится только после установки и предварительной настройки DeepMail и KSMG. Перед началом настройки интеграции создайте снапшоты всех виртуальных машин/контейнеров DeepMail и KSMG перед внесением изменений.

1.1.4.2 Настройка в веб-интерфейсе

В главном меню перейдите в раздел «Панель управления» → «Профили». Откройте профиль SMTP для редактирования, нажав кнопку  напротив профиля SMTP, далее в поле «Ретрансляционные сети» укажите IP адрес KSMG (например, *192.168.92.157/32*, далее данный адрес используется как пример), в поле «Узел ретрансляции» укажите: *192.168.92.157*. Сохраните изменения нажав кнопку 

, находящуюся ниже редактируемых полей.

Выполните реконфигурацию SMTP-сервиса, для этого необходимо перейти в главном меню в раздел «Панель управления» → «Реконфигурация». Для сервиса SMTP необходимо нажать «Реконфигурировать».

Добавьте релейный домен, перейдя в главном меню в раздел «SMTP транспорт» → «Релейные домены». Далее требуется нажать 

.

В открывшемся окне укажите:

- в поле «Имя релейного домена» – *exemple.ru*;

- в поле «Удаленный хост» – *192.168.92.157*.

1.1.4.3 Настройка на нодах DeepMail

На всех нодах отредактируйте файл конфигурации */mnt/deepmail/core/deepmail.env*, выполнив команду:

sudo nano /mnt/deepmail/core/deepmail.env

и добавив в файл следующие строки:

RELAYHOST=192.168.92.157:25

RELAYNETS=192.168.92.157/32

После внесения данных правок, выйдете из режима редактирования с сохранением, далее перезапустите сервисы на всех нодах выполнив следующие команды:

deepmail stop

deepmail start

1.1.4.4 Отключение антиспама

В веб-интерфейсе перейдите в главном меню в раздел «Панель управления» → «Профили». Для каждого профиля (IMAP и SMTP) снимите галочку Антиспам активен (milter).

Выполните реконфигурацию сервисов перейдя в главном меню в раздел «Панель управления» → «Реконфигурация». Для сервисов SMTP и IMAP необходимо нажать «Реконфигурировать».

1.1.4.5 Отключение встроенного антивируса

На всех нодах отредактируйте файл конфигурации /mnt/deepmail/core/deepmail.env выполнив команду:

sudo nano /mnt/deepmail/core/deepmail.env

и отредактировав параметр антивируса:

ANTIVIRUS=none

Далее требуется перезапустить сервисы, выполнив команды:

deepmail stop

deepmail start

1.1.4.6 Настройка KSMG

Настройте KSMG для приема и отправки писем:

- укажите IP-адрес DeepMail сервера в качестве исходящего узла;
- настройте политики сканирования (антивирус, антиспам).

Проверьте связь между KSMG и DeepMail с помощью команды:

telnet 192.168.92.157 25

1.1.4.7 Проверка работы

Отправьте тестовое письмо через DeepMail.

Убедитесь, что:

- письмо проходит через KSMG (проверьте логи KSMG);
- встроенный антиспам/антивирус DeepMail не блокирует письма.

Проверьте обработку угроз:

- отправьте письмо с тестовым вирусом (например, EICAR);
- убедитесь, что KSMG блокирует его.

1.1.4.8 Важные замечания

Для поддержания стабильной работы Сервера важно выполнять следующие действия:

- после изменений всегда выполняйте реконфигурацию сервисов через веб-интерфейс;
- мониторьте логи DeepMail (*/var/log/deepmail/*) и KSMG при возникновении ошибок;
- регулярно обновляйте базы сигнатур KSMG.

Если настройки применены корректно, весь почтовый трафик будет обрабатываться антивирусом KSMG.

2 УСТАНОВКА И НАСТРОЙКА СЕРВЕРА

2.1 Подготовка к установке

2.1.1 Особенности разворачивания Сервера в ОС Astra Linux

Перед установкой Сервера в ОС Astra Linux необходимо выполнить следующие действия:

1) Повысить права до суперпользователя (root), выполнив команду:

   sudo su

2) Отключить мандатный контроль, выполнив команды:

   selinux status

   selinux disable

После перезагрузки он опять будет включен.

3) Выполнить минорное и мажорное обновление, используя команды:

   sudo apt update

   sudo apt list --upgradable

   sudo apt full-upgrade (*full* обязательно).

4) Во время обновления, запущенного на шаге 3 соглашаться со всем.

5) Перезагрузить ВМ.

6) С правами root DeepMail выполнить:

   stop

   start

7) Проверить профили на наличие галочки HAProxy.

8) Если что-то менялось выполнить реконфигурацию.

9) Выполнить шаг 6.

2.1.2 Распаковка архива

- скачать архив «*deepmail-server-*<номер версии>*tar.gz*» на управляющий сервер (Ansible control node);
- открыть терминал;
- распаковать архив, выполнив в терминале команду:

  tar -xvf deepmail-server-2.0….tar.gz -d /your_folder

2.1.3 Настройка портов

Для полнофункциональной работы Сервера необходимо открыть и не блокировать следующие порты и сети:

1) внешние:
   - 25 – smtp (tcp);
   - 587 – smtp;
   - 465 – smtp ssl;
   - 143 – imap;
   - 993 – imap ssl;
   - 443 – https;
   - 389 – ldap;
   - 636 – ldaps;
   - 110 – POP3;
   - 995 – POP3S.
2) внутренние:
   - 8001;
   - 8002;
   - 8003;
   - 8004;
   - 2525 – smtp;
   - 11332 – antispam.
3) NFS:
   - 111;
   - 2049;
   - 635;
   - 4045;
   - 4046;
   - 4049.
4) Docker:
   - 192.168.203.0/24;
   - 172.21.0.1/24.

2.2 Настройка inventory – файла и детализация его параметров

Файл *inventory-example.yml* определяет топологию инфраструктуры и параметры компонентов.

В таблице 3 приведено описание параметров *inventory-example.yml* файла, а также рекомендации по их редактированию.

Таблица 3 – Параметры файла *inventory-example.yml*

Параметр	Значение по умолчанию	Описание/рекомендация
ansible_ssh_common_args	*'-o StrictHostKeyChecking=no'*	Параметр *ansible_ssh_common_args* необходимо оставить без изменений
install_packages	*false*	Параметр *install_packages* позволяет включать/отключать (*true/false*) предустановку пакетов
antispam_enabled	*true*	Параметр позволяет включить использование антиспама
antivirus_enabled	*false*	Параметр позволяет включить использование антивируса
override_compose	*true*	Параметр позволяет включить возможность обновления *docker-compose.yml*
override_certs	*false*	Параметр позволяет включить возможность обновления *ssl* сертификатов
default_domain	*“deepmail.loc”*	Параметр позволяет добавить домен по умолчанию
default_hostname	*“mail.deepmail.loc”*	Параметр позволяет добавить имя хоста
psql_pass	*'password'*	Параметр задает пароль для пользователя БД.

Параметр	Значение по умолчанию	Описание/рекомендация
reconfig_pg	*false*	Параметр определяет, нужно ли менять конфигурацию PostgreSQL.
haproxy_use	*false*	Параметр позволяет включить возможность использовать *haproxy*
haproxy_address	*“0.0.0.0”*	Параметр позволяет добавить адрес *haproxy*
keepalived_use	*false*	Параметр определяет будет ли использоваться отказоустойчивый *haproxy* (для *haproxy* будет необходимо 2 хоста)
pgcluster_use	*false*	Параметр определяет будет ли использоваться отказоустойчивый кластер БД (*postgresql, etcd, patroni_haproxy_keepalived* – минимум 3 хоста)
pgcluster_virtual_ip	*0.0.0.0*	В данном параметре указывается виртуальный IP, при использовании кластера БД.
Пути к файлам на нодах		
core_storage_path	*"/mnt/deepmail/core"*	Путь до папки *core* на хосте core
webdav_storage_path	*"/mnt/deepmail/dav"*	Путь до папки *dav* на хосте *core* и *webdav*
mail_storage_path	*"/mnt/deepmail/mail"*	Путь до папки *mail* на хосте core
smtp_storage_path	*"/var/deepmail/smtp"*	Путь до папки *smtp* на хосте core
archive_storage_path	*"/mnt/deepmail/archive"*	Путь до папки *archive* на хосте *core*

Параметр	Значение по умолчанию	Описание/рекомендация
Пути к файлам на NFS хранилище		
nfs_core_storage_path	*"/mnt/deepmail/core"*	Путь до *core* (конфигурационные файлы) хранилища на хосте *NFS*
nfs_webdav_storage_path	*"/mnt/deepmail/dav"*	Путь до *dav* (календари, адресные книги, списки задач) хранилища на хосте *NFS*
nfs_mail_storage_path	*"/mnt/deepmail/mail"*	Путь до *mail* (почта) хранилища на хосте *NFS*
nfs_archive_storage_path	*"/mnt/deepmail/archive"*	Путь до папки *archive* на хосте *core*
Пути к конфигурационным файлам сервисов (рекомендуется не менять)		
auth_conf_path	*"/etc/deepmail/auth-service"*	Путь к конфигурационным файлам сервиса авторизации. Рекомендуется не менять
webdav_conf_path	*"/etc/deepmail/webdav-service"*	Путь к конфигурационным файлам календарей и адресных книг. Рекомендуется не менять
imap_conf_path	*"/etc/deepmail/imap-service"*	Путь к конфигурационным файлам сервиса входящих сообщений. Рекомендуется не менять
smtp_conf_path	*"/etc/deepmail/smtp-service"*	Путь к конфигурационным файлам сервиса исходящих сообщений. Рекомендуется не менять
Три хоста хранилища: почта, коллекция и конфигурационные файлы		
storage_core: *hosts:* *0.0.0.0:* *ansible_user: root*	Указывается пользователь для подключения по ssh, его пароль и пароль для повышения привилегий	Можно устанавливать на одну виртуальную машину

Параметр	Значение по умолчанию	Описание/рекомендация
ansible_ssh_pass: 'password' *ansible_become_pass: 'password'* *storage_mail:* *hosts:* *0.0.0.0:* *ansible_user: root* *ansible_ssh_pass: 'password'* *ansible_become_pass: 'password'* *storage_dav:* *hosts:* *0.0.0.0:* *ansible_user: root* *ansible_ssh_pass: 'password'* *ansible_become_pass: 'password'*		
Настройка хоста сервера haproxy		
haproxy: *hosts:* *0.0.0.0:* *ansible_user: root* *ansible_ssh_pass: 'password'* *ansible_become_pass: 'password'*	В параметрах указывается пользователь для подключения по ssh, его пароль и пароль для повышения привилегий.	Закомментированные параметры символом «#» необходимо раскомментировать для конфигурации при использовании 2 хостов (для отказоустойчивости с помощью keepalived), в обратном случае оставить без изменений.

Параметр	Значение по умолчанию	Описание/рекомендация
keepalived_master: false *keepalived_interface: enp3s0* # *0.0.0.0:* # *ansible_user: root* # *ansible_ssh_pass: 'password'* # *ansible_become_pass: 'password'* # *keepalived_master: false* # *keepalived_interface: enp3s0* # *хост сервера postgresql* *postgresql:* *hosts:* *0.0.0.0:* *ansible_user: root* *ansible_ssh_pass: 'password'* *ansible_become_pass: 'password'*		Если keepalived не используем, то в параметре *keepalived_master* оставляем *false*. При использовании keepalived, на основную ноду haproxy ставим *true*, на остальных *false*. Как указывалось, ранее, если для повышения отказоустойчивости не используется keepalived, дальнейшие закомментированные символом «#» строки остаются неизменными. При использовании keepalived, указываем название сетевого интерфейса, который использует хост, а символы «#» необходимо удалить. Для подключения указывается пользователь для подключения по ssh, его пароль и пароль для повышения привилегий. Параметр *etcd_nodename* не менять. Закомментированные параметры символом «#»

Параметр	Значение по умолчанию	Описание/рекомендация
etcd_nodename: datanode1 *pg_interface: enp3s0* *# 0.0.0.0:* *# ansible_user: root* *# ansible_ssh_pass: 'password'* *# ansible_become_pass: 'password'* *# etcd_nodename: datanode2 # не менять* *# pg_interface: enp3s0* *# 0.0.0.0:* *# ansible_user: root* *# ansible_ssh_pass: 'password'* *# ansible_become_pass: 'password'* *# etcd_nodename: datanode3 # не менять* *# pg_interface: enp3s0*		необходимо раскомментировать при использовании отказоустойчивого кластера БД. (etcd, postgresql, patroni_haproxy, keepalived - минимум 3 хоста для кластера). Если кластер БД не используется, далее в настройках параметров ничего не меняется. При использовании кластера БД, необходимо указать название сетевого интерфейса, который использует хост
Хосты для сервисов core, auth, webdav		
core: *hosts:* *0.0.0.0:* *ansible_user: root*	Указывается пользователь для подключения по ssh, его пароль и пароль для повышения привилегий	Параметры конфигурации используются в закомментированном виде при нескольких однотипных хостах

Параметр	Значение по умолчанию	Описание/рекомендация
ansible_ssh_pass: 'password' *ansible_become_pass: 'password'* *nodename: "node1"* # *0.0.0.0:* # *ansible_user: root* # *ansible_ssh_pass: 'password'* # *ansible_become_pass: 'password'* # *nodename: "node2"* *auth:* *hosts:* *0.0.0.0:* *ansible_user: root* *ansible_ssh_pass: 'password'* *ansible_become_pass: 'password'* # *0.0.0.0:* # *ansible_user: root* # *ansible_ssh_pass: 'password'* # *ansible_become_pass: 'password'*		Параметр nodename не менять. Параметр nodename не менять

Параметр	Значение по умолчанию	Описание/рекомендация
webdav: *hosts:* *0.0.0.0:* *ansible_user: root* *ansible_ssh_pass: 'password'* *ansible_become_pass: 'password'* # *0.0.0.0:* # *ansible_user: root* # *ansible_ssh_pass: 'password'* # *ansible_become_pass: 'password'*		

Важно! Остальные строки файла редактировать запрещено.

Необходимо сохранить изменения перед закрытием файла.

2.3 Запуск установки

Минимальная конфигурация инфраструктуры для установки состоит из двух виртуальных машин. На одной размещаются сервисы Core, WebDAV, auth, на второй база данных PostgreSQL, NFS и HAProxy (установка обязательна).

2.3.1 Развертывание хранилища (storage.yaml)

Цель:

- создание NFS для хранения данных;
- настройка прав доступа.

Необходимо выполнить команду в терминале:

ansible-playbook -i /path/to/inventory-example.yml /path/to/playbooks/storage.yml

2.3.2 Установка основных компонентов (install.yml)

Цель:

- развертывание Docker-контейнеров;
- настройка сетевых интерфейсов.

Необходимо выполнить команду в терминале:

ansible-playbook -i /path/to/inventory-example.yml /path/to/playbooks/install.yml

2.4 Установка и настройка PostgreSQL

Цель:

- создание базы данных для хранения данных;
- настройка прав доступа.

Для автоматизированной установки БД в терминале необходимо выполнить команду:

ansible-playbook -i /path/to/inventory-example.yml /path/to/playbooks/pg.yml

После выполнения команды будет установлена БД с конфигурацией, настройка которой описана в подразделе 2.2.

2.5 Установка и конфигурирование HAProxy

Цель:

- обеспечение высокой доступности и балансировки нагрузки для TCP- и HTTP-приложений;
- настройка правил маршрутизации запросов.

Для установки HAProxy необходимо выполнить команду:

ansible-playbook -i /path/to/inventory-example.yml /path/to/playbooks /haproxy.yml

После выполнения команды будет установлена HAProxy с конфигурацией, настройка которой описана в подразделе 2.2.

2.6 Веб-клиент: полная настройка

2.6.1 Вход в веб-клиент

Для входа в веб-клиент необходимо перейти по адресу HAProxy: *https://10.10.10.10*, (*10.10.10.10* – IP адрес HAProxy).

2.6.2 Подключение БД

Выполнить подключение к созданной БД, указав следующие параметры:

- в поле «Хост» указать IP сервера PostgreSQL;
- в поле «Порт» указать «*5432*»;
- в поле «Имя пользователя» указать имя пользователя базы данных DeepMail;
- в поле «Пароль» указать пароль пользователя от базы данных DeepMail;
- в поле «Тип аутентификации» выбрать *trust*.

3 АДМИНИСТРИРОВАНИЕ ПОЧТОВОГО СЕРВЕРА

3.1 Вход в интерфейс администратора

Для доступа к интерфейсу администратора необходимо:

- открыть веб-браузер и перейти по ссылке в формате «*https://<IP>*», где <IP> – это IP-адрес или имя почтового домена;
- в появившемся окне авторизации необходимо указать адрес электронной почты: *admin@<domain>* (*<domain>* – имя домена, указанного при установке); и пароль администратора: *PASSWORD*, и затем нажать кнопку «Войти» (рисунок 1).

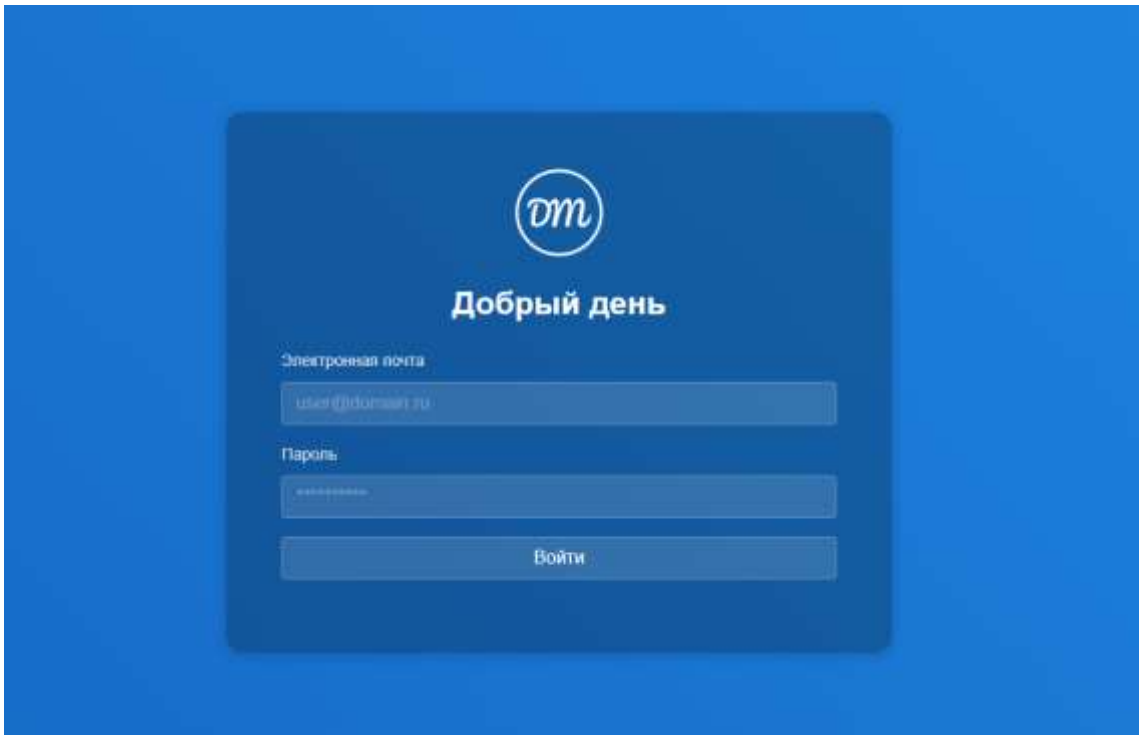


Рисунок 1 – Окно авторизации в веб-интерфейс администарота

При успешной авторизации будет открыто окно настроек веб-клиента почтового сервера.

Для настройки профилей необходимо:

1) перейти в панель управления;

2) перейти во вкладку «Профили» (см. 3.2.2);

3) открыть форму настройки профиля IMAP, нажав кнопку  :

- заполнить имя хоста;
- активировать чекбокс при использовании HAProxy;
- ввести IP адрес HAProxy;

- активировать остальные необходимые чекбоксы;
- ввести максимум пользовательских IP подключений;
- ввести интервал уведомления об отсутствии активности IMAP;
- ввести адрес антиспама при использовании – IP адрес Core;

4) настроить параметры smtp профиля аналогично с настройкой IMAP:

- первые четыре пункта аналогичны настройке IMAP;
- настроить реле;
- настроить параметры антиспама аналогично IMAP;

5) настроить параметры WebDAV профиля: указать имя хоста, указать связи с HAProxy, указать максимальный размер файла;

6) в левой панели перейти на вкладку «Система»;

7) перейти по стрелке рядом с кнопкой «Добавить сервис»;

8) добавить сервисы WebDAV и Auth. При необходимости можно добавить требующееся количество сервисов WebDAV и Auth. Сервис Core создается автоматически;

9) реконфигурировать все сервисы, дождаться пока они станут «*healthy*».

При первом входе в настройки АРМ «DeepMail» с учетной записью администратора должно появиться окно с номером лицензии (рисунок 2).

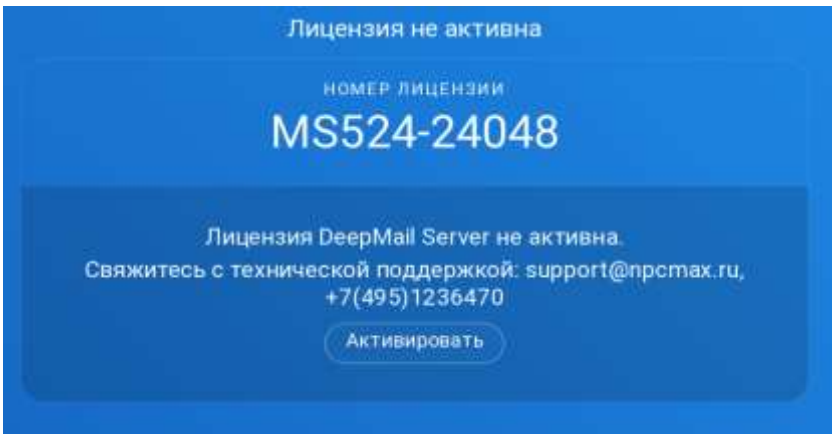


Рисунок 2 – Окно с деталями лицензии

Для активации лицензии необходимо запросить лицензионный ключ активации у разработчика. Лицензионный ключ генерируется по номеру лицензии (см. рисунок 2). Для ввода полученного лицензионного ключа необходимо нажать кнопку Активировать, и ввести лицензионный ключ в соответствующее поле (рисунок 3). Нажать кнопку Активировать.

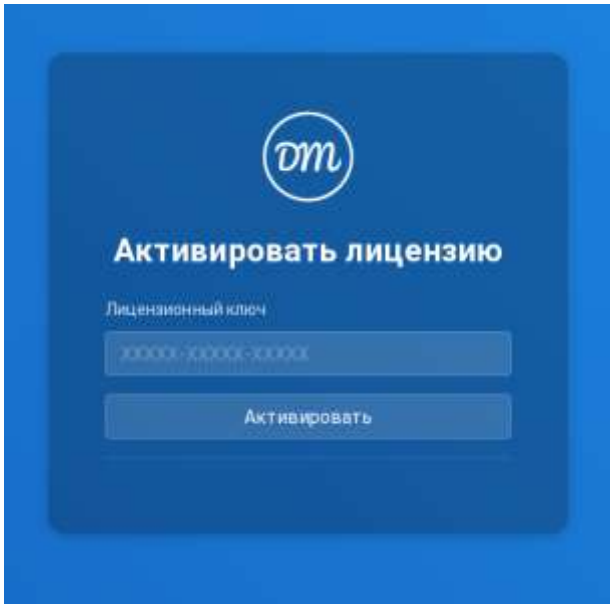


Рисунок 3 – Окно ввода лицензионного ключа

В случае успешной активации в окне авторизации должна появиться надпись «Лицензия активирована» (рисунок 4).

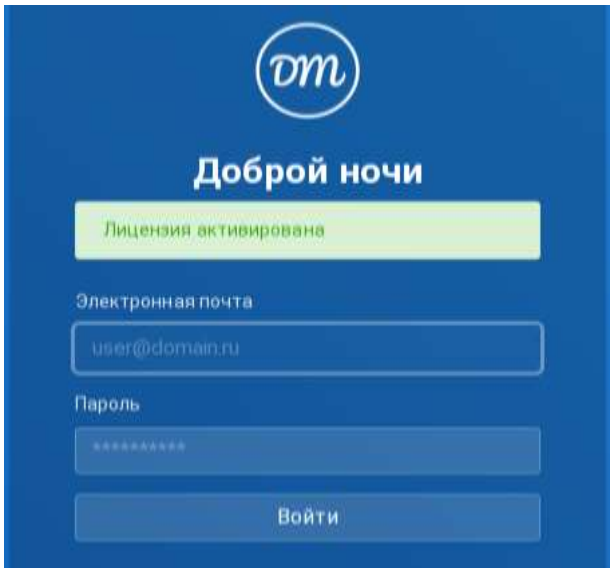


Рисунок 4 – Сообщение об активации лицензии

После аутентификации откроется веб-клиент с раскрытым интерфейсом почтового ящика или интерфейсом администратора Сервера. В случае необходимости перехода к интерфейсу администратора из интерфейса почтового ящика необходимо нажать кнопку 

(рисунок 5).

Рисунок 5 – Кнопка DeepMail перехода в интерфейс администратора

После этого откроется интерфейс администратора Сервера (рисунок 6).

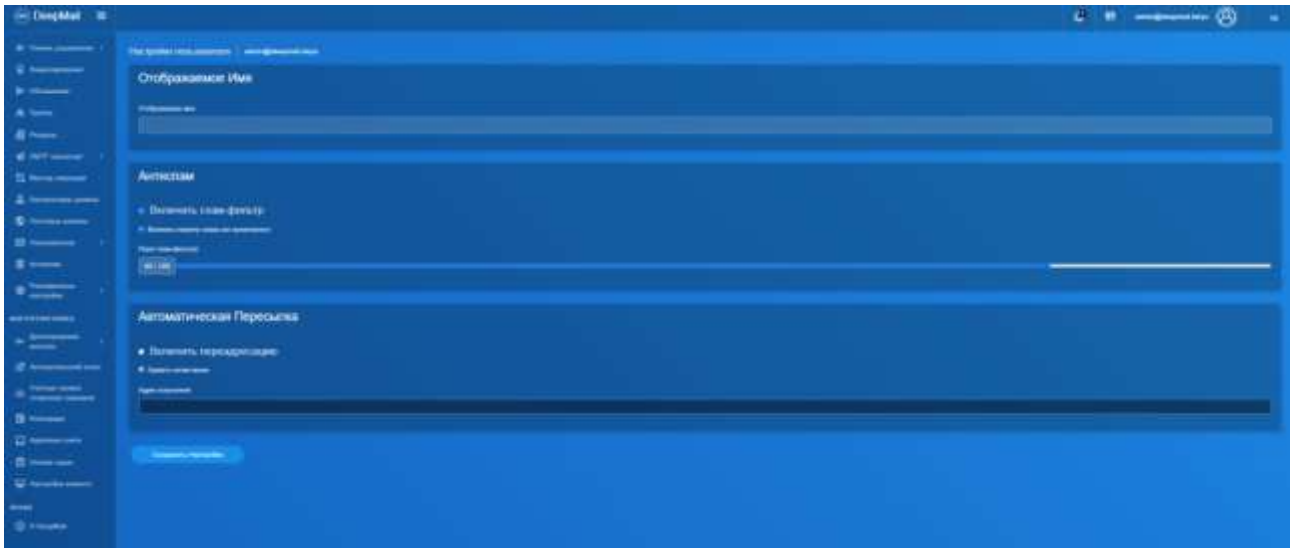


Рисунок 6 – Интерфейс администратора. Окно «Настройки пользователя»

В окне «Настройки пользователя» задаются следующие параметры:

- отображаемое имя пользователя;
- параметры работы антиспама (в блоке «Антиспам»);
- адреса для пересылки почты (в блоке «Автоматическая пересылка»).

В левой части окна расположено меню, которое содержит основные инструменты настроек и администрирования Сервера (рисунок 7).

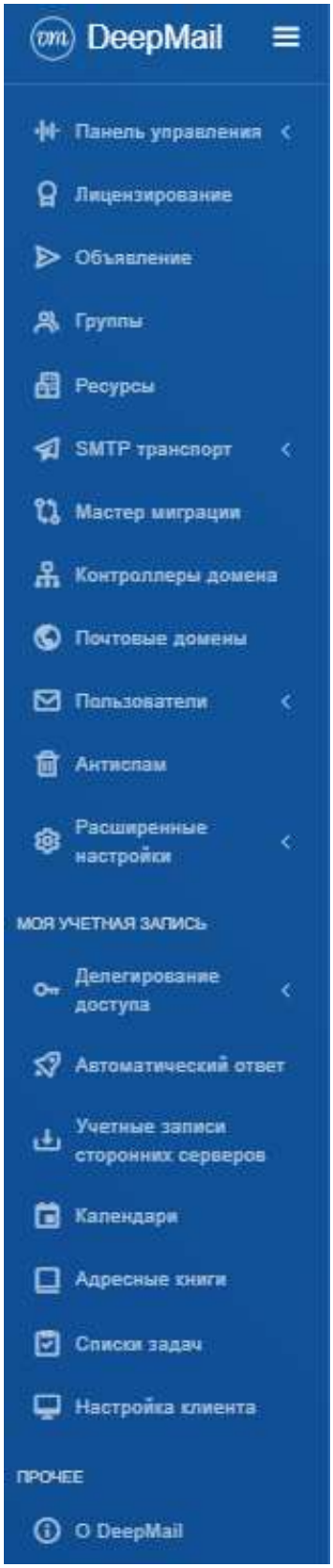


Рисунок 7 – Меню инструментов настроек и администрирования

Чтобы свернуть меню необходимо нажать кнопку  . (см. рисунок 7). Компактное представление меню инструментов настроек и администрирования представлено на рисунке 8.

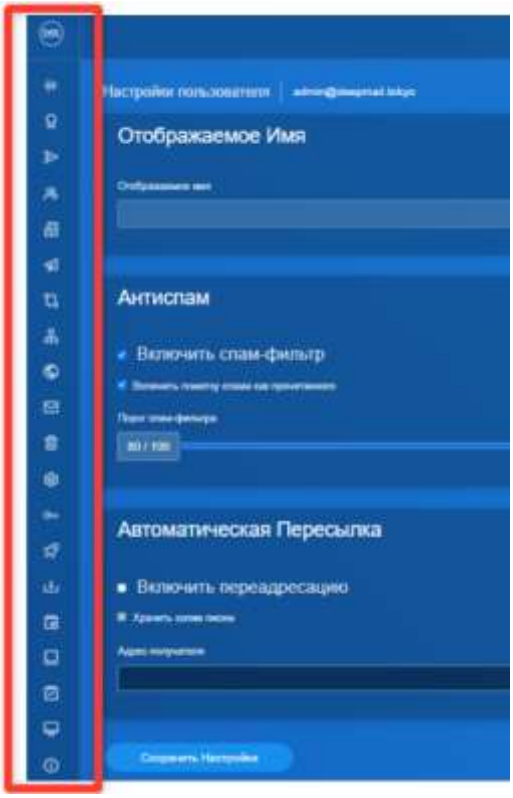


Рисунок 8 – Компактное представление меню инструментов настроек и администрирования

Предпросмотр меню инструментов доступен при наведении на него курсора, меню будет отображено в темном виде (рисунок 9).

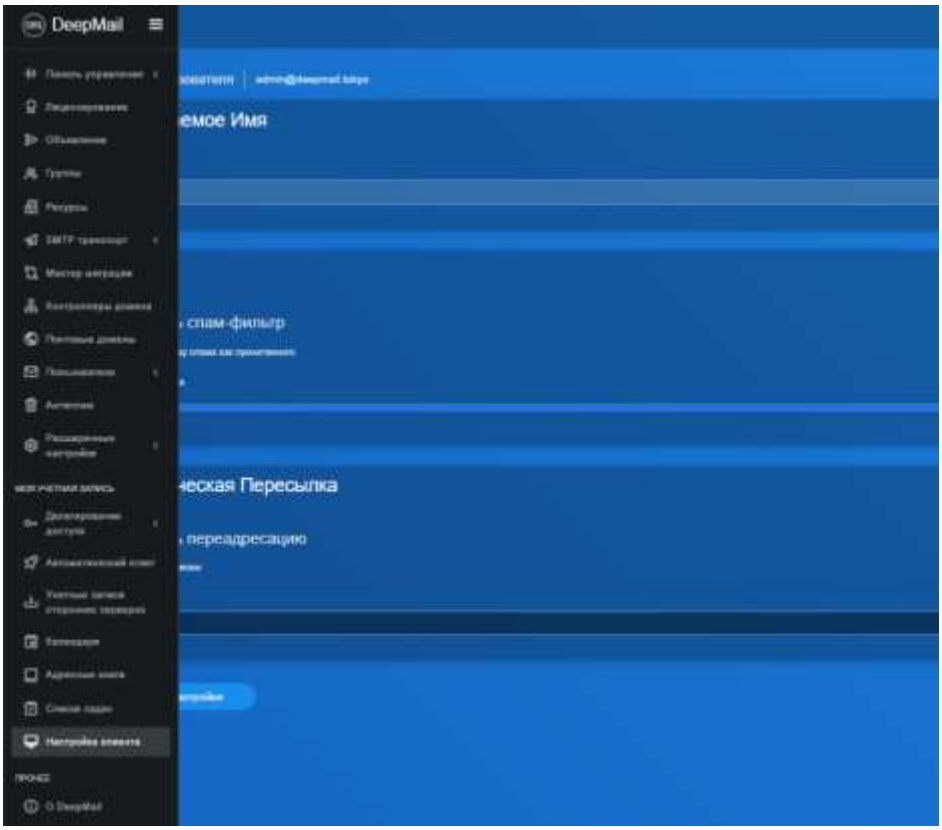


Рисунок 9 – Развернутое меню настроек и администрирования

Чтобы вернуть меню инструментов в исходное состояние необходимо нажать кнопку  (см. рисунок 9).

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

Рисунок 10 – Меню переключения языка интерфейса

3.2 Инструмент «Панель управления»

Инструмент администрирования «Панель управления» состоит из нескольких инструментов:

- Система;
- Профили;
- Реконфигурация (рисунок 11).

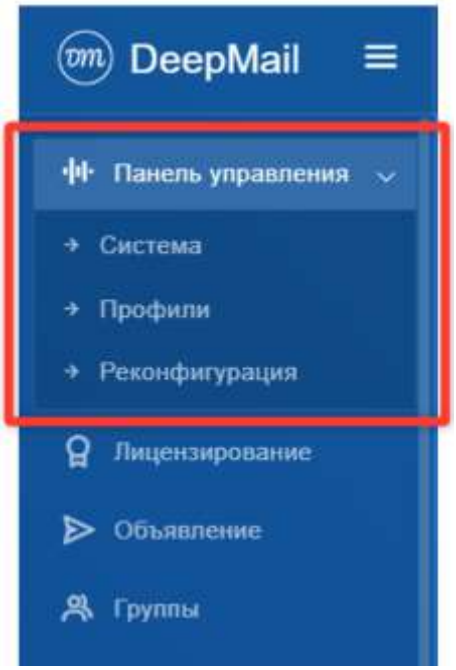


Рисунок 11 – Состав инструмента администрирования «Панель управления»

3.2.1 «Система»

Инструмент «Система» предназначен для мониторинга ресурсов почтового узла АРМ «DeepMail». Для перехода в окно информации о ресурсах необходимо в меню «Панель управления» интерфейса администратора выбрать «Система» (рисунок 12).

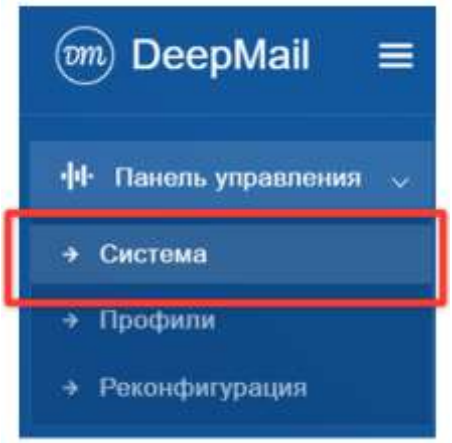


Рисунок 12 – Выбор инструмента «Система»

В результате выбора откроется окно с информацией о статусе работы нод почтового узла, о распределении использованной физической памяти для каждой ноды, объемом используемых ресурсов (ЦП и ОЗУ) микросервисами для каждой ноды (рисунок 13).

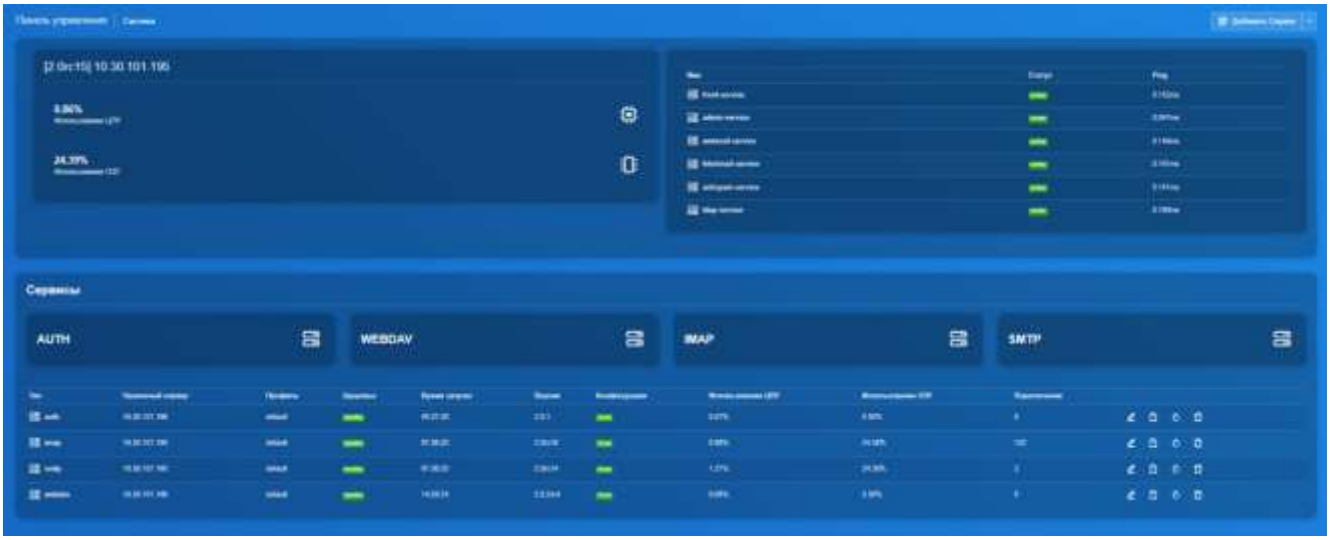


Рисунок 13 – Окно «Панель управления»

В окне «Сервисы» содержится основная информация о работе микросервисов почты, а также кнопки управления этими микросервисами (рисунок 14).

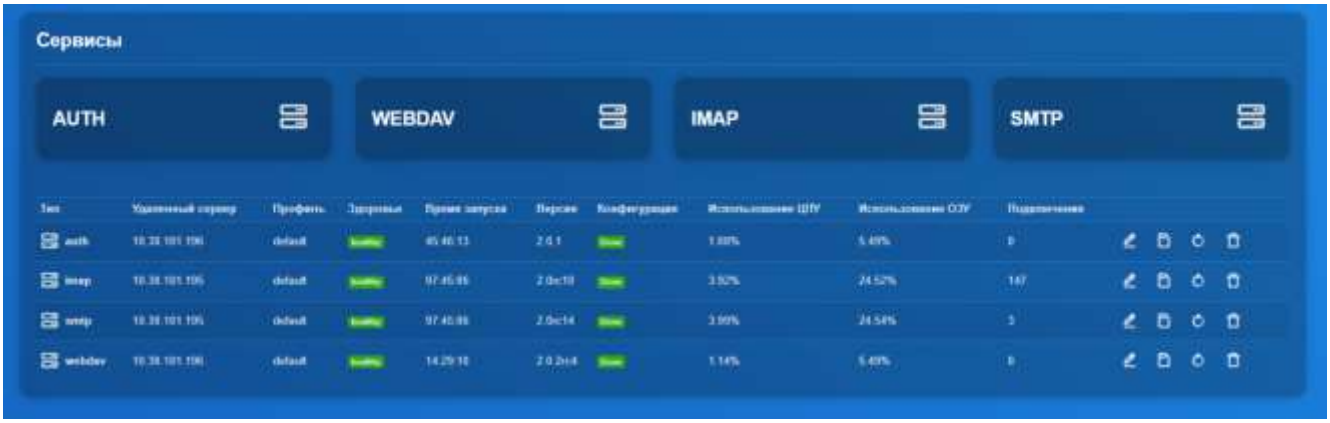


Рисунок 14 – Панель всех сервисов ноды

В информации отображены следующие показатели и функциональные элементы:

- загрузка процессора (в %);
- использование ОЗУ;
- количество активных сервисов;
- кнопка  предназначена для перезапуска микросервисов;
- кнопка  предназначена для удаления микросервисов;
- кнопка  предназначена для реконфигурации микросервисов;
- кнопка  предназначена для редактирования микросервисов.

В случае изменения профиля, привязанного к сервисам, сервис необходимо реконфигурировать. Сервисы, находящиеся в процессе ожидания запуска реконфигурации, отмечены статусом «Wait» (рисунок 15).

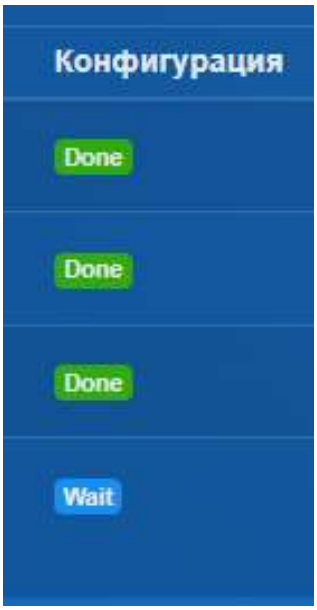


Рисунок 15 – Конфигурация

Возможные статусы сервисов:

- «Done» –изменения приняты;
- «Wait»– конфигурация была изменена, но еще не принята сервисом;
- «Error» –ошибка при попытке реконфигурации.

Для редактирования параметров сервиса необходимо нажать кнопку  . В результате откроется форма редактирования, позволяющая изменить IP адрес и профиль сервиса (рисунок 16).

Рисунок 16 – Форма редактирования параметров сервиса

Перезапуск необходимо подтвердить, нажав кнопку «Подтвердить» (рисунок 17).

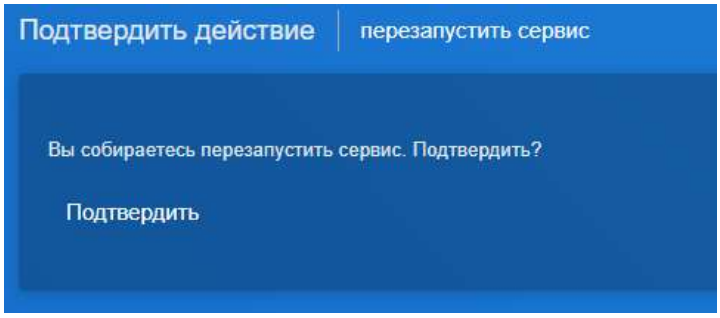


Рисунок 17 – Подтверждение перезапуска

3.2.2 «Профили»

Для просмотра профилей сервисов Сервера необходимо в меню «Панель управления» интерфейса администратора выбрать «Профили» (рисунок 18).

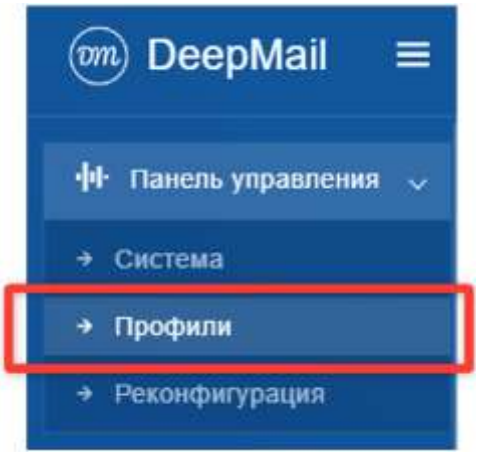


Рисунок 18 – Инструмент «Профили»

Откроется окно администрирования профилей (рисунок 19).

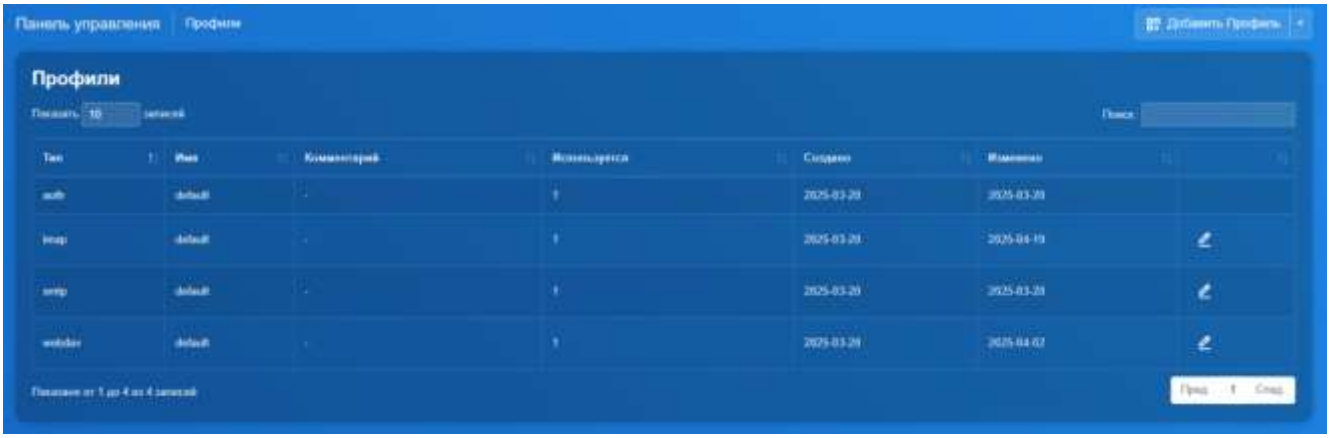


Рисунок 19 – Окно инструмента «Профили»

В окне «Профили настроек» приведены детали настроек, которые уникальны для каждого типа сервиса. Профиль привязывается к сервису или сервисам конкретного типа (например, IMAP-профиль привязывается к сервису IMAP). В колонке «Используется» приведено число сервисов, к которым привязан данный профиль.

Для настройки корзин первого и второго (скрытая корзина) уровней, куда попадают письма из обычной корзины после ее очистки, требуется напротив профиля IMAP (см. рисунок 18) нажать кнопку  и в открывшемся окне настроить параметры автоочистки корзин (рисунок 20).

Рисунок 20 – Настройка параметров автоочистки

Корзина первого уровня находится в папке */var/deepmail/mail/exemple@exemple.ru/Trash*, корзина второго уровня находится в папке */var/deepmail/mail/exemple@exemple.ru/Recoverable*.

В папке */var/deepmail/mail/exemple@exemple.ru/Recoverable/Deleted Items* находятся удаленные письма из корзины первого уровня.

Для настройки ретрансляционных сетей, требуется напротив профиля SMTP (см. рисунок 18) нажать кнопку  и в открывшемся окне настроить параметры «Ретрансляционных сетей» профиля SMTP (рисунок 21).

Рисунок 21 – Настройка «Ретрансляционных сетей»

В поле «Ретрансляционные сети» необходимо указать необходимые сети *<IP-адрес>/32*, через запятую.

Важно! IP-адреса указываются через запятую без пробелов.

Далее необходимо выполнить реконфигурацию сервиса, нажав на кнопку  напротив сервиса SMTP в меню «Панель управления» → «Система». Затем требуется открыть файл *mnt/deepmail/core/deepmail.env* и в конце файла добавить строку:

RELAYNETS=<IP-адрес>/32

После настройки ретрансляционных сетей необходимо на обеих нодах произвести перезапуск DeepMail выполнив следующие команды:

deepmail stop

deepmail start

3.2.3 «Реконфигурация»

Для просмотра сервисов Сервера, требующих реконфигурации, необходимо в меню «Панель управления» интерфейса администратора выбрать «Реконфигурация» (рисунок 22).

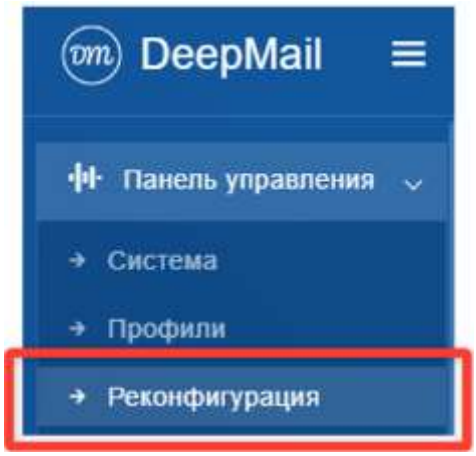


Рисунок 22 – Инструмент «Реконфигурация»

Откроется окно реконфигурации сервисов (рисунок 23).

Рисунок 23 – Окно реконфигурации сервисов

В данном окне приведена информация о сервисах, требующих реконфигурации после изменения профиля и сервисах, чья реконфигурация была завершена с ошибкой. Отсутствие данных в окне означает, что все сервисы находятся в актуальном состоянии.

3.3 Инструмент «Лицензирование»

Для просмотра информации о лицензировании (количестве пользователей и сроке действия лицензий) необходимо в меню интерфейса администратора выбрать инструмент «Лицензирование» (рисунок 24).

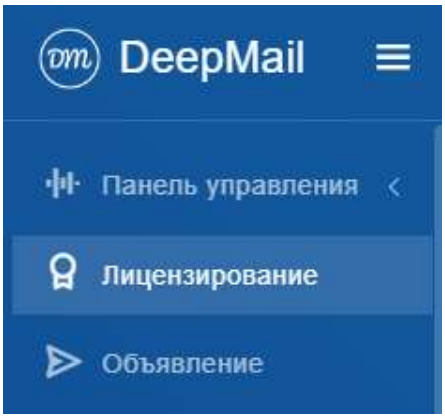


Рисунок 24 – Инструмент «Лицензирование»

В результате выбора на экране появится окно с детальной информацией о лицензировании (рисунок 25).

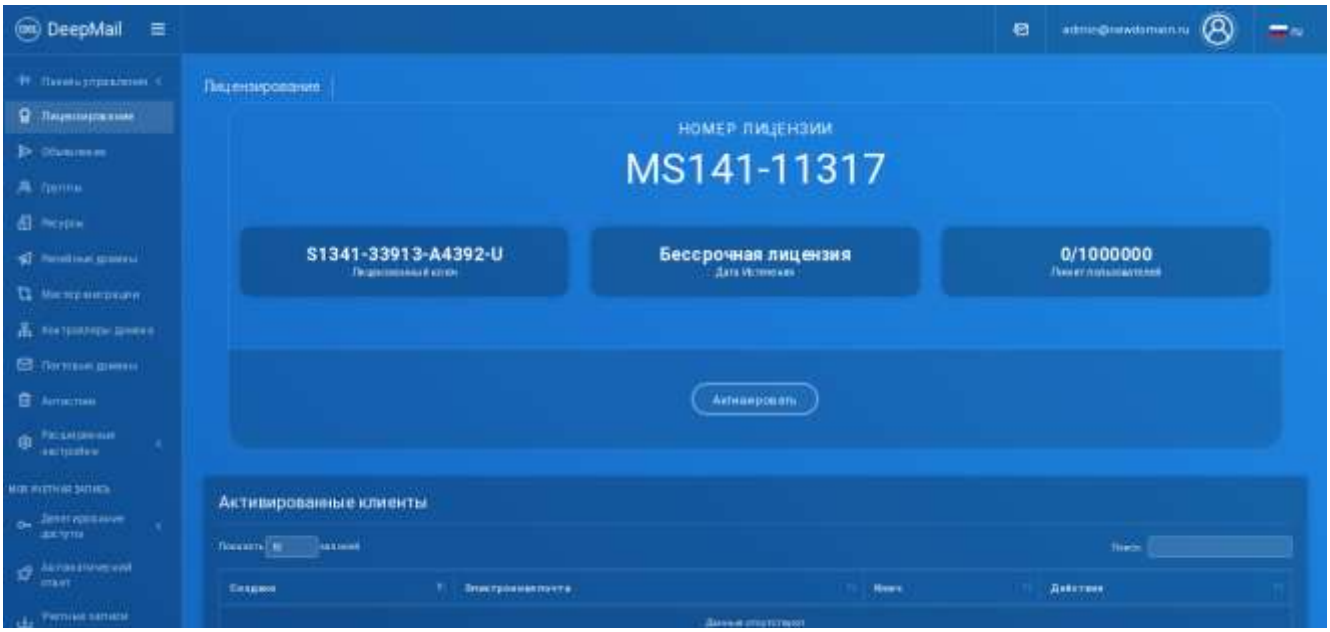


Рисунок 25 – Окно «Лицензирование»

3.3.1 Активация лицензии

Для активации новой лицензии в окне «Лицензирование» (см. рисунок 25) необходимо нажать кнопку Активировать, ввести лицензионный ключ, полученный вместе с дистрибутивом или напрямую от разработчика, и нажать кнопку Активировать. В случае успешной активации лицензии на экране появится окно с информацией о пройденной активации (см. рисунок 4).

Примечание. Для получения лицензионного ключа в случае его отсутствия необходимо обратиться в СТП разработчика.

3.3.2 Панель «Активированные клиенты»

Панель «Активированные клиенты» окна «Лицензирование» содержит следующую информацию о клиентах с активной лицензией:

- «Создано» – дата получения лицензии клиентом;
- «Электронная почта» – электронная почта клиента;
- «Ключ» – номер лицензионного ключа клиента;
- «Действия» – действия, разрешенные администратору применительно к данным клиента (например, удаление).

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

3.4 Инструмент «Объявление»

Инструмент «Объявление» предназначен для создания и отправки публичных объявлений пользователям. Получателями публичного объявления являются все учетные записи домена.

Для перехода к инструменту необходимо в меню интерфейса администратора выбрать «Объявление» (рисунок 26).

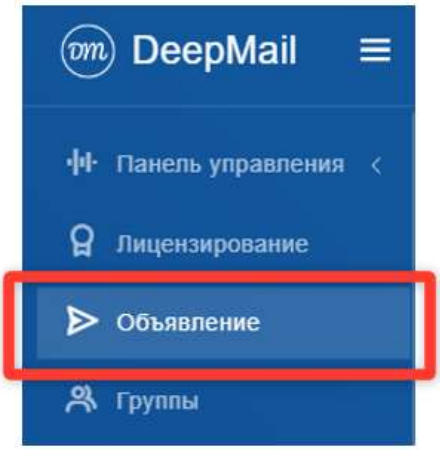


Рисунок 26 – Инструмент «Объявление»

Откроется окно для создания и отправки публичных объявлений (рисунок 27).

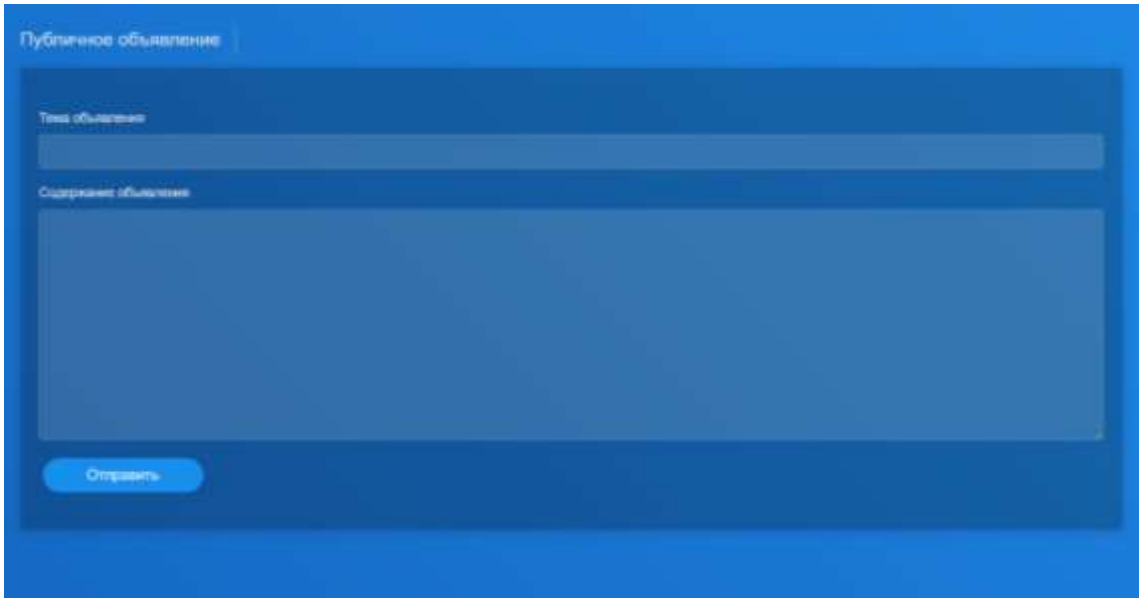
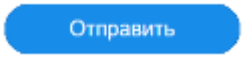
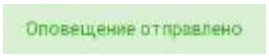


Рисунок 27 – Окно «Публичное объявление»

Для создания публичного объявления необходимо указать тему объявления, добавить содержание в соответствующие поля и нажать кнопку 

. В случае успешной рассылки объявления в окне появится сообщение 

.

3.5 Инструмент «Группы»

Для перехода к инструменту «Группы» необходимо в меню интерфейса администратора выбрать «Группы» (рисунок 28).

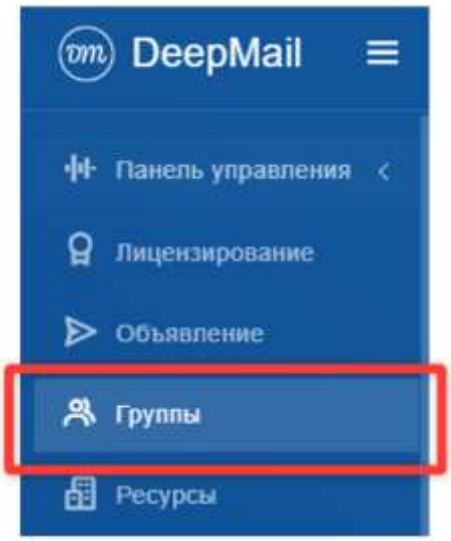


Рисунок 28 – Инструмент «Группы»

В результате выбора на экране появится окно «Группы», содержащее список групп пользователей всех почтовых доменов (рисунок 29).

Рисунок 29 – Окно «Группы»

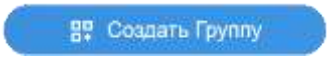
Инструмент «Группы» позволяет создавать, редактировать, удалять пользовательские группы, добавлять в группы и удалять из групп пользователей, а также назначать им различные права.

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».

Права реализованы в виде доступа к соответствующим окнам интерфейса.

3.5.1 Создание группы пользователей

Для создания новой группы необходимо нажать кнопку 

. В результате в окне появится форма создания группы (рисунок 30).

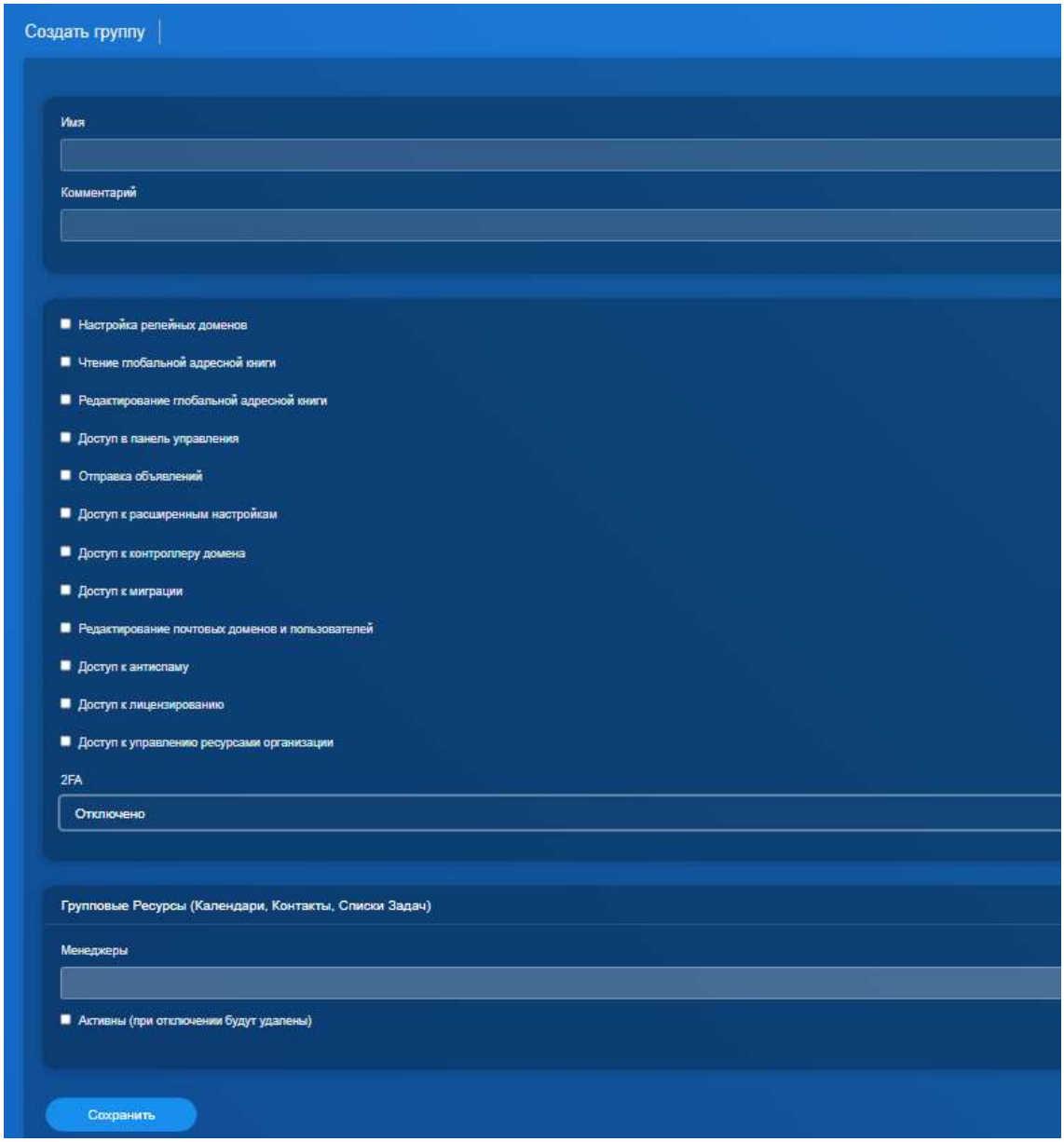


Рисунок 30 – Форма «Создать группу»

В форме «Создать группу» необходимо указать название группы, комментарий, назначить права участникам группы, отметив соответствующие чек-боксы, и нажать кнопку Сохранить (см. рисунок 30).

3.5.2 Настройка двухфакторной аутентификации

Сервер Deepmail поддерживает двухфакторную аутентификацию (2FA) в качестве дополнительной меры безопасности, которая используется вместе с основным методом входа по логину и паролю.

Основой для работы двухфакторной аутентификации служит механизм TOTP (Time-based One-Time Password Algorithm). Данный механизм предполагает использование стороннего приложения-аутентификатора, такого как Google Authenticator, Yandex Ключ и другие. Процесс настройки и использования выглядит следующим образом.

Для активации 2FA пользователю необходимо включить соответствующую настройку в административной панели. При следующей попытке входа в системе будет сгенерирован QR-код, содержащий уникальный 32-битный ключ (seed). Этот QR-код необходимо отсканировать в приложении-аутентификаторе. Важно отметить, что система предоставляет QR-код для настройки только один раз при первом подключении. Если вход выполняется через толстый клиент, то клиентское приложение запрашивает у сервера специальный URI через API, который выполняет ту же роль, что и QR-код.

После того как приложение-аутентификатор считало ключ, оно начинает генерировать одноразовые коды, основанные на этом ключе и текущем времени. Полученный код пользователь вводит на сервере для завершения регистрации. Сервер проверяет код, и при успешной валидации пользователю выдается специальный токен.

С этого момента для входа в систему пользователь вводит не только логин и пароль, но и одноразовый код из приложения. После успешной аутентификации клиент использует для последующих запросов полученный токен, который заменяет пароль. Это позволяет не запрашивать код 2FA при каждом обращении к системе.

Администратору предоставляются инструменты для централизованного управления этой функцией. Вы можете принудительно включать или отключать обязательное использование двухфакторной аутентификации для целых групп пользователей. Если для группы включена 2FA, ее участники не смогут войти в систему, используя только логин и пароль, — от них всегда будет требоваться токен. В случае необходимости администратор может сбросить уникальный ключ (seed) для любого пользователя, что приведет к необходимости повторной настройки приложения-аутентификатора с новым QR-кодом.

Включение и отключение настройки двухфакторная аутентификации доступно на уровне групповых настроек. Для включения пользователям 2FA необходимо перейти в настройки группы (см. рисунок 30)., и отредактировать ее настройки.

В пункте включения/отключения 2FA выбрать доступный механизм – TOTP (см. Рисунок 31). Для всех пользователей группы будет включен механизм 2FA.

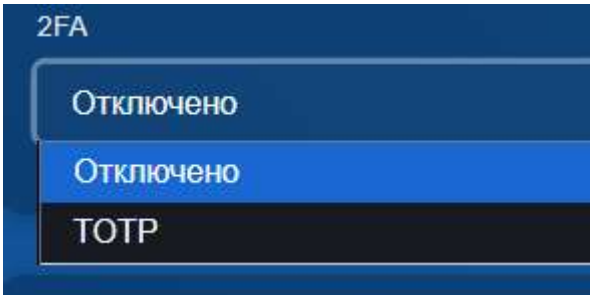


Рисунок 31 – Включение/отключение 2FA

После включения механизма 2FA, при ближайшей аутентификации пользователю из данной группы, будет предложено ввести код из приложения аутентификатора (см. Рисунок 32).

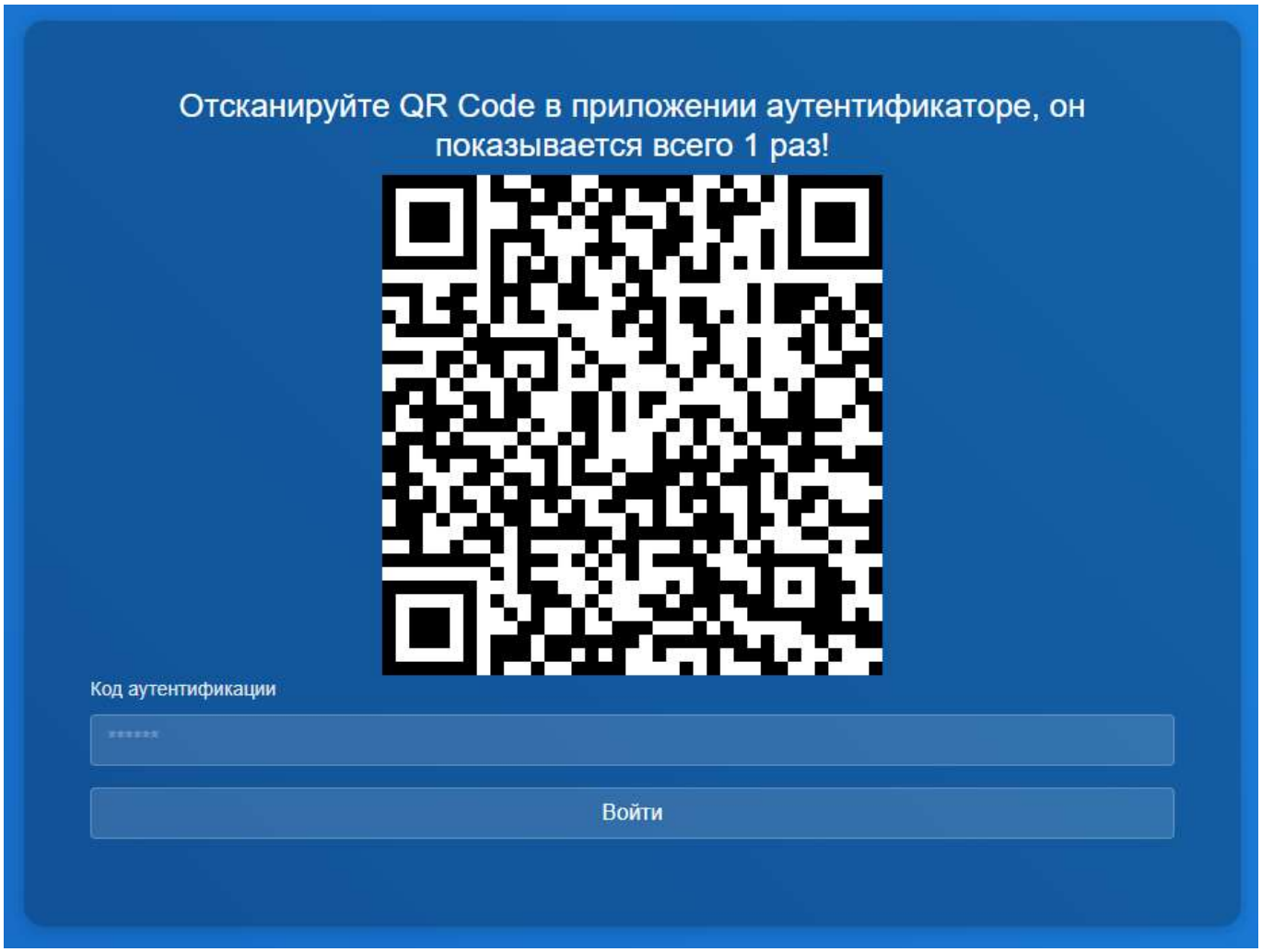


Рисунок 32 – Код из приложения аутентификатора

Важно, QR код показывается всего один раз! если его не сохранить и выйти с страницы, заново настроить возможно только с ролью администратора, сбросив 2FA в настройках конкретного пользователя и домена, нажав кнопку «Сбросить 2FA» (см. Рисунок 33).

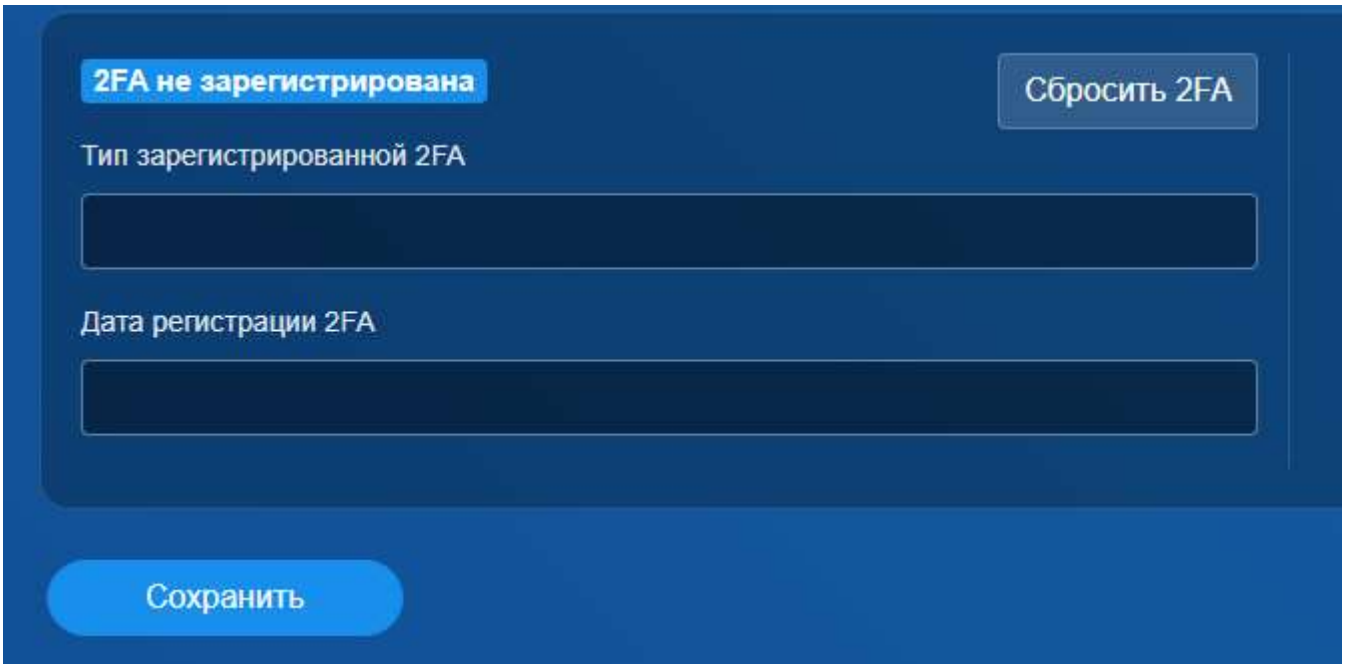


Рисунок 33 – Сброс 2FA

После успешного входа в настройках конкретного пользователя будет отображаться, что 2FA успешно зарегистрирована с фиксацией даты регистрации 2FA (см. Рисунок 34).

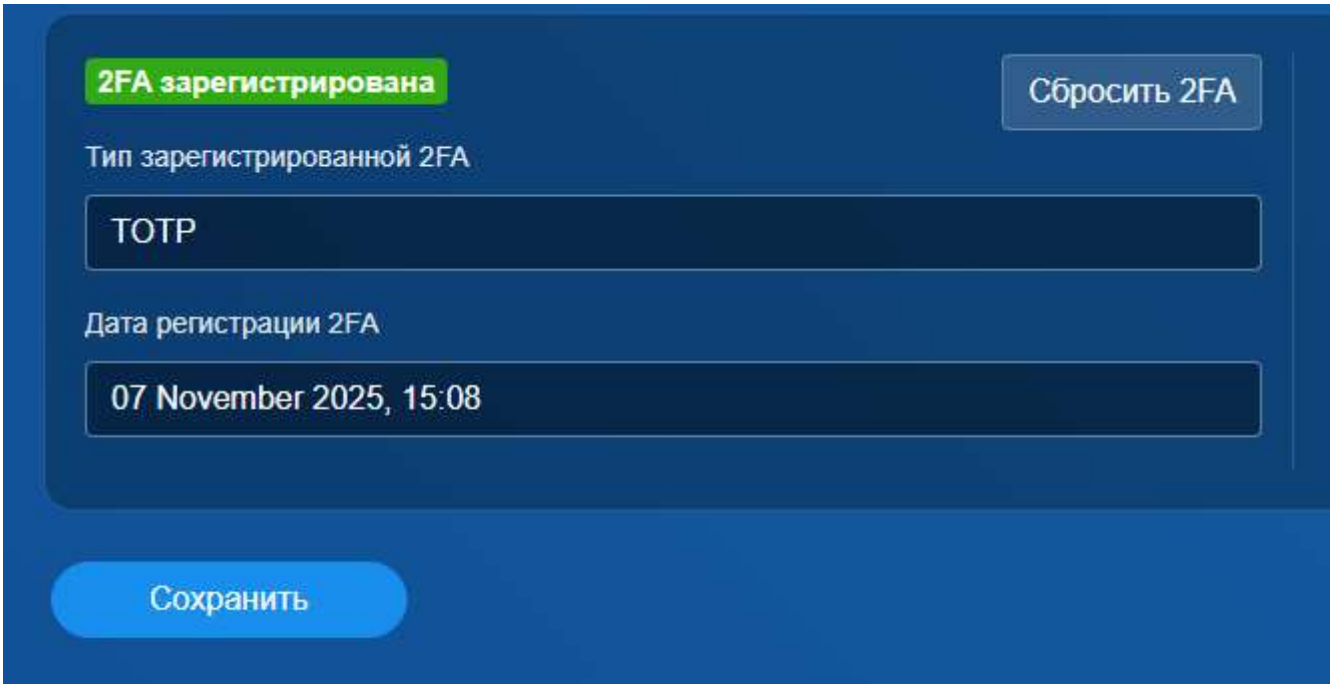


Рисунок 34 – 2FA зарегистрирована

3.5.3 Действия, выполняемые с группами

Для просмотра информации о группе необходимо в окне «Группы» нажать кнопку (см. рисунок 29). В результате откроется окно «Информация о группе» (рисунок 35).

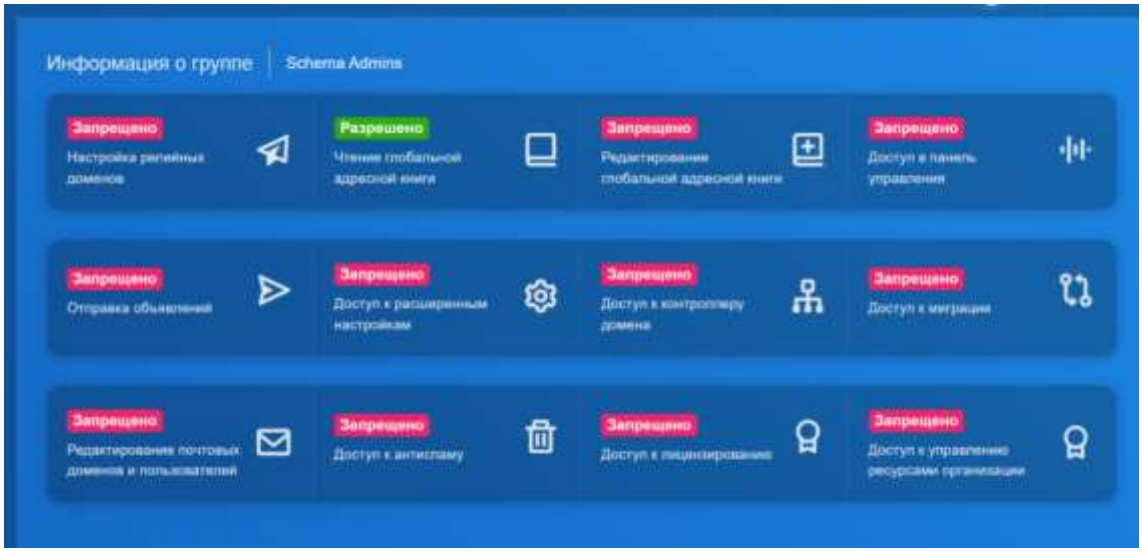


Рисунок 35 – Окно с информацией о группе

Для просмотра пользователей группы необходимо в окне «Группы» нажать кнопку  (см. рисунок 29). В результате откроется окно «Список пользователей в группе» (рисунок 36).

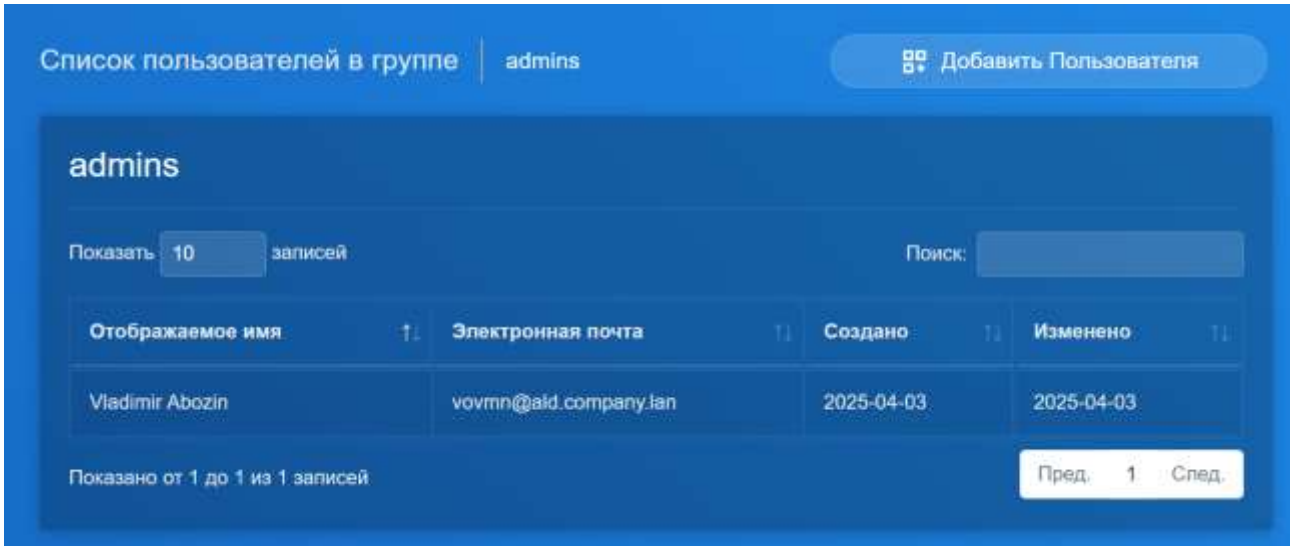


Рисунок 36 – Окно «Список пользователей в группе»

Для добавления пользователя в группу необходимо нажать кнопку 

.

В появившейся форме «Добавить пользователя к группе» выбрать добавляемого пользователя из выпадающего списка (или начать вводить его адрес в поле «Электронная почта»), и нажать кнопку «Отправить» (рисунок 37).

Рисунок 37 – Форма «Добавить пользователя к группе»

Кнопка  в окне «Группы» (см. рисунок 29) предназначена для редактирования выбранной группы, например позволяет переназначить права группе и открывает форму настройки группы, аналогичную форме создания (см. рисунок 30).

Для удаления группы необходимо в окне «Группы» (см. рисунок 29) нажать кнопку  , расположенную в строке группы, и подтвердить удаление в окне «Подтвердить действия».

3.6 Инструмент «Ресурсы»

Система позволяет централизованно управлять ресурсами организации (помещения, транспорт, оборудование) посредством автоматизации процесса бронирования.

Для управления ресурсами организации предназначен инструмент «Ресурсы». Чтобы перейти к нему в меню интерфейса администратора необходимо выбрать «Ресурсы» (рисунок 38).

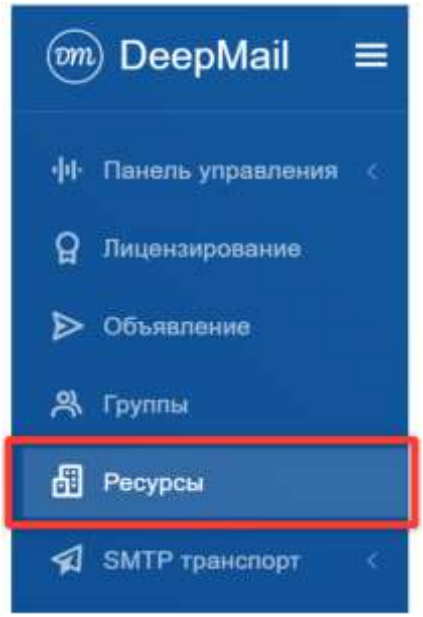


Рисунок 38 – Инструмент «Ресурсы»

Откроется окно «Список ресурсов» (рисунок 39).

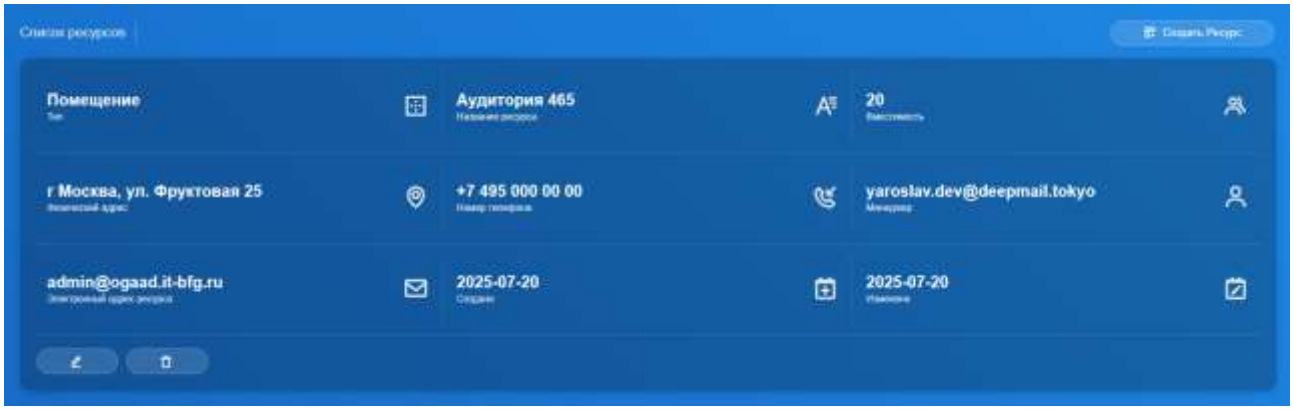


Рисунок 39 – Окно «Список ресурсов»

3.6.1 Создание нового ресурса

При добавлении нового ресурса в систему предусмотрена обязательная классификация ресурса по типу: транспорт (например, служебные автомобили) или помещение (например, переговорные комнаты). Ресурсу присваивается уникальное название, которое будет отображаться у всех пользователей системы, и электронная почта – идентификатор ресурса.

Для бронирования ресурса под определенное событие необходимо в карточке события указать электронный адрес ресурса в качестве участника. В случае если ресурс доступен для брони, организатор получит подтверждение об успешном бронировании. В случае если ресурс не доступен, организатор получит уведомление об отказе в бронировании.

Каждому ресурсу назначается менеджер – пользователь, который получает в своем Клиенте доступ к календарю ресурса (отображается вместе с личными календарями). Менеджер может просматривать все события ресурса и управлять его занятостью, а также, при необходимости, делегировать права управления календарем ресурса другим пользователям. Таким образом, система обеспечивает автоматический контроль занятости ресурсов.

Для создания нового ресурса необходимо в окне «Список ресурсов» нажать кнопку 

(см. рисунок 39).

В появившейся форме «Создать ресурс» в списке «Тип» необходимо выбрать тип создаваемого ресурса: «Транспорт» или «Помещение», указать наименование ресурса, менеджера, указать адрес электронной почты ресурса и нажать кнопку «Сохранить» (рисунок 40).

Рисунок 40 – Форма «Создать ресурс»

В окне появится системное сообщение «Ресурс создан», а созданный ресурс отобразится в списке ресурсов.

3.6.2 Редактирование ресурса

Для редактирования ресурса необходимо нажать кнопку  (см. рисунок 39), и внести изменения в появившуюся форму «Изменить ресурс» (рисунок 41).

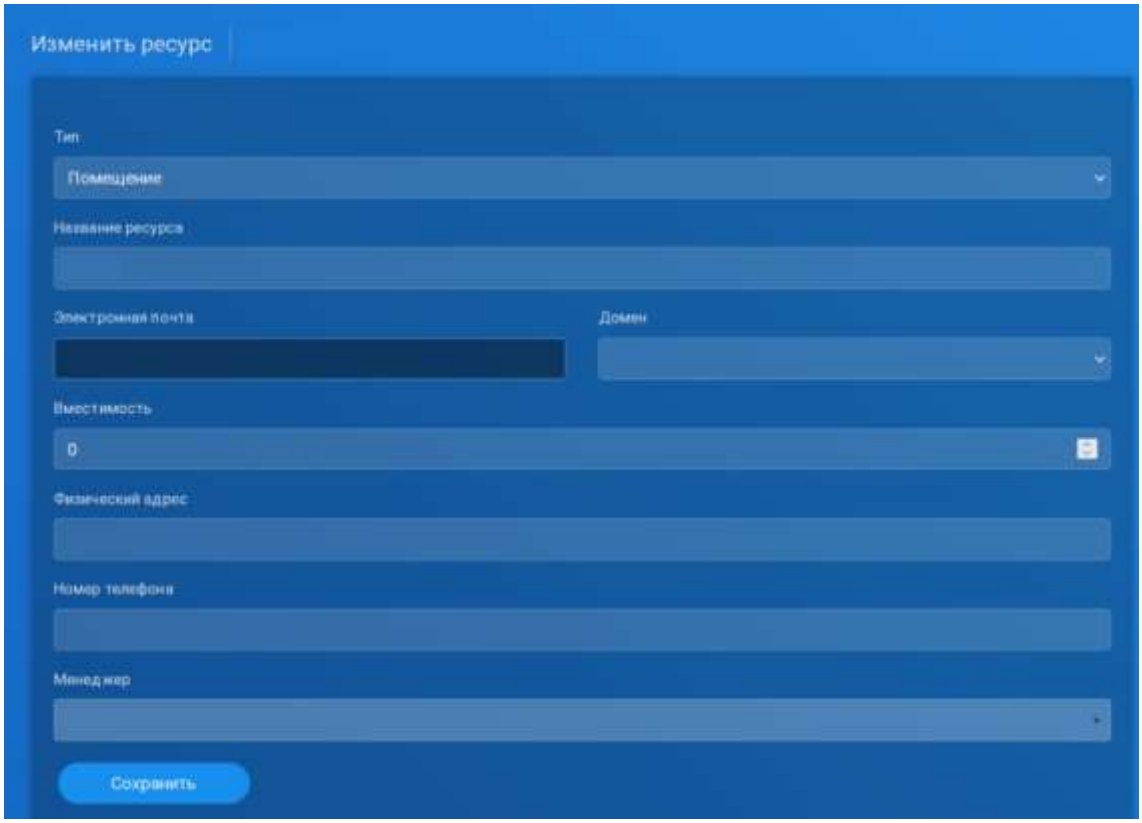


Рисунок 41 – Форма «Изменить ресурс»

3.6.3 Удаление ресурса

Для удаления ресурса необходимо нажать кнопку  (см. рисунок 39), и подтвердить удаление в открывшемся окне «Подтвердить действие».

3.7 Инструмент «SMTP транспорт»

Меню «SMTP транспорт» интерфейса администратора содержит два инструмента: «Релейные домены» и «Транспортные правила» (рисунок 42).

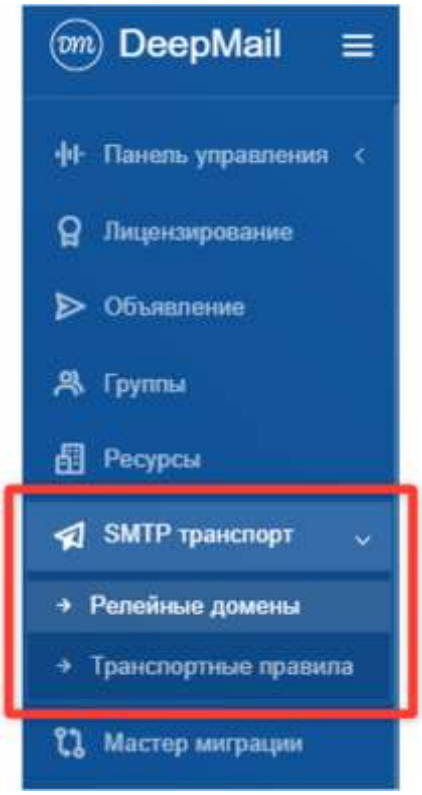


Рисунок 42 – Инструмент «Релейные домены»

Почтовый сервер АРМ «DeepMail» может отправлять электронные сообщения не напрямую, а через сервер – посредник.

Для настройки пересылки почты через сервер – посредник необходимо перейти к инструменту «Релейные домены», выбрав его в меню интерфейса администратора (рисунок 43).

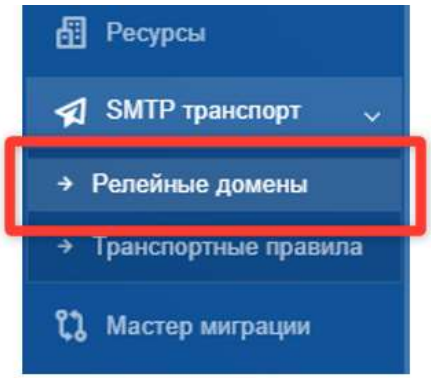


Рисунок 43 – Выбор инструмента «Релейные домены»

Окно «Список релейных доменов» содержит список настроенных релейных доменов (рисунок 44).

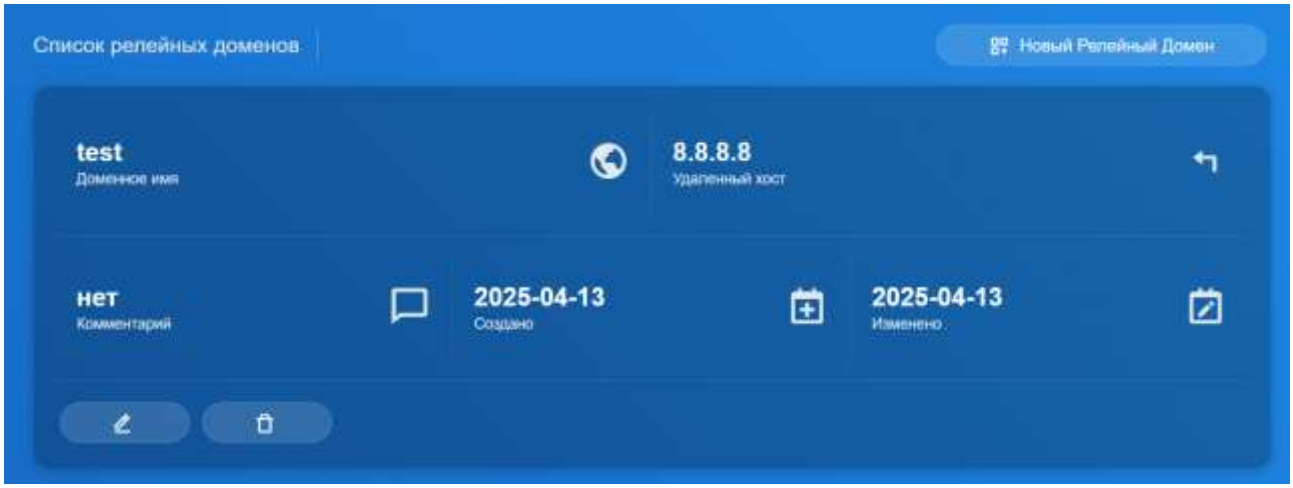


Рисунок 44 – Окно «Список релейных доменов»

3.7.1 Создание нового релейного домена

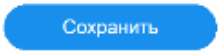
Для создания нового релейного домена необходимо в окне «Релейные домены» нажать кнопку 

(см. рисунок 44).

В появившейся форме создания релейного домена указать:

- «Имя релейного домена» – доменное имя исходного сервера, которое хотим использовать для релейного домена;
- «Удаленный хост» – IP-адрес HAProxy удаленного хоста (реле) (рисунок 45).

Рисунок 45 – Форма «Новый релейный домен»

Для завершения создания и сохранения параметров необходимо нажать кнопку 

(см. рисунок 45).

Для того чтобы почта переправлялась через созданный сервер, необходимо в разделе бокового меню перейти в «Панель управления» → «Профили» (см. рисунок 18) и напротив профиля SMTP нажать  .

В открывшемся меню в параметре «Ретрансляционные сети» должно быть заполнены значения *10.10.10.0/24, 192.168.1.3/32*, в параметре «Узел ретрансляции» должно быть заполнено значение *10.10.10.100*.

В случае, если используется антиспам RSPAMD, дополнительно необходимо скорректировать в файле *deepmail.env* параметры RELAYHOST и RELAYNETS, если антиспам RSPAMD не используется, эта настройка не требуется.

Например:

RELAYNETS=10.10.10.7/32,10.10.10.8/32

RELAYHOST=10.10.10.9:25

10.10.10.7 и *10.10.10.8* – IP адреса или подсети нод кластера пограничных серверов

10.10.10.9 – IP адрес точки входа на кластер пограничных серверов

IP адрес сети должен указываться с маской */32*.

Для вступления настроек в силу необходимо в терминале выполнить команду *deepmail reload* на каждой запущенной ноде.

Примечание. Если в качестве релейного сервера используется сервер «DeepMail», то необходимо изменить конфигурацию на нем.

3.7.2 Редактирование релейного домена

Для редактирования релейного домена необходимо в окне со списком релейных доменов нажать кнопку  (см. рисунок 44). После этого откроется форма «Изменить релейный домен» (рисунок 46).

Рисунок 46 – Форма «Изменить релейный домен»

Внесите изменения в поля появившейся формы, и нажмите кнопку «Сохранить» (см. рисунок 46).

3.7.3 Удаление релейного домена

Для удаления релейного домена необходимо в окне со списком релейных доменов нажать кнопку  (см. рисунок 44) и подтвердить удаление в открывшейся форме «Подтвердить действие».

3.7.4 «Транспортные правила»

Инструмент «Транспортные правила» (правила потока обработки почты) позволяет обрабатывать проходящие через организацию сообщения по заданным правилам.

Чтобы настроить транспортные правила необходимо в меню «SMTP транспорт» интерфейса администратора выбрать «Транспортные правила» (рисунок 47).

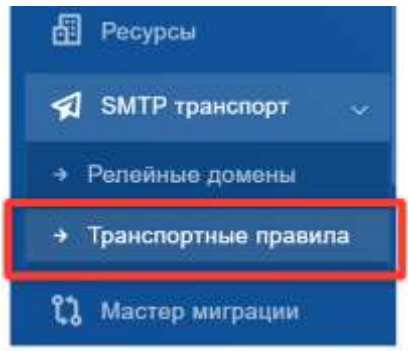


Рисунок 47 – Выбор инструмента «Транспортные правила»

Откроется окно «Транспортные правила», которое содержит список настроенных правил (рисунок 48).

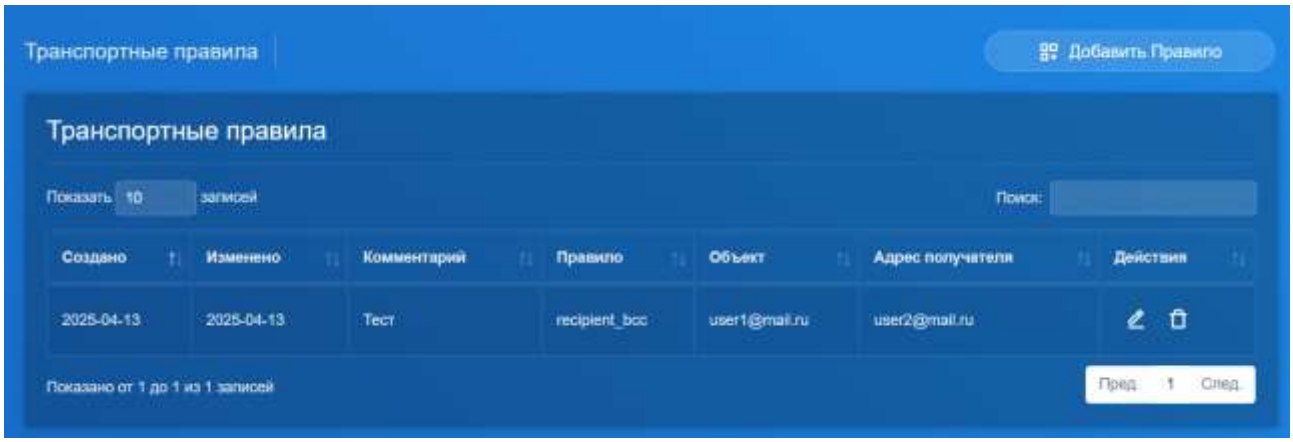


Рисунок 48 – Окно «Транспортные правила»

В АРМ «DeepMail» реализованы следующие типы правил:

- «Recipient BCC» – если пользователь получает сообщение, то оно копируется на адрес получателя.
- «Sender BCC» – если пользователь отправляет письмо, то оно копируется на адрес получателя.
- «Always BCC» – если пользователь отправляет или получает письмо, то оно копируется на адрес получателя (рисунок 49).

Рисунок 49 – Окно «Настройка транспортных правил»

Важно! Не пересылается, а именно копируется в исходном состоянии.

Для ограничения отправителя в правах по доменам и отправителям необходимо (далее описывается создание правила, для ограничения пользователю отправки писем в рамках домашнего/ локального домена) выполнить следующие действия:

Необходимо изменить конфигурационный файл всех нод */mnt/deepmail/core/nodes/node{N}/docker- compose.yml*.

В нем необходимо заменить строчку, отмеченную на рисунке 50.

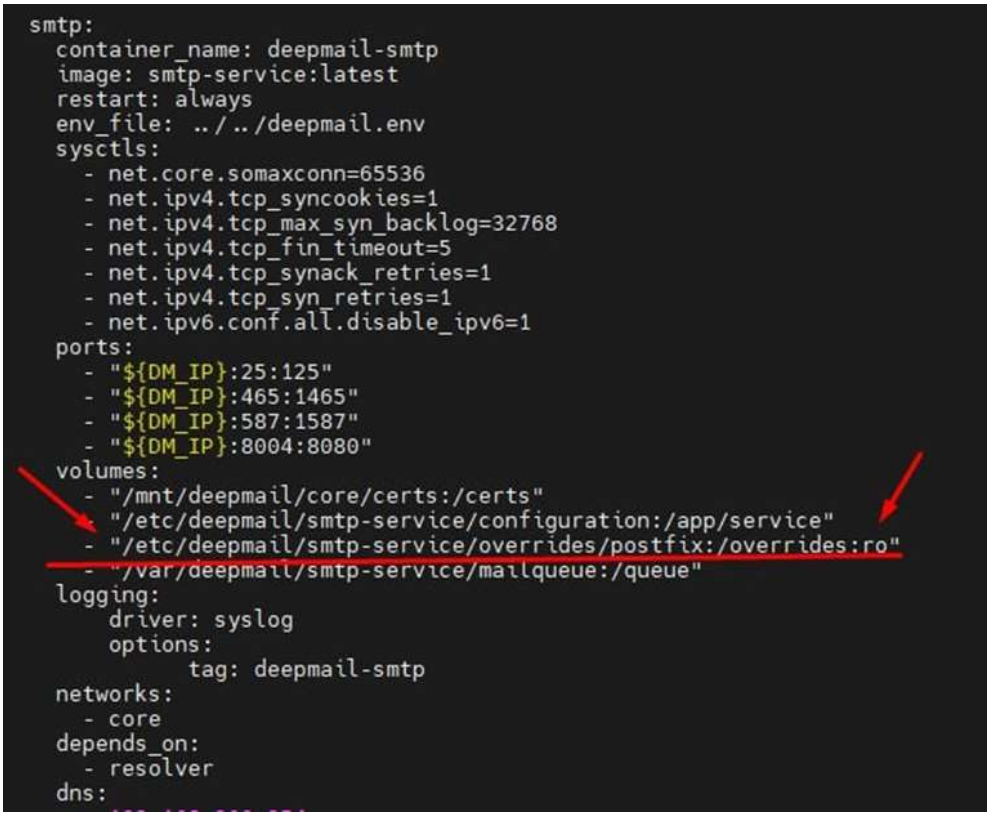


Рисунок 50 – Строчка для замены в конфигурационном файле

Указанную строку необходимо изменить на следующее значение:

/mnt/deepmail/core/overrides/postfix:/overrides

В результате правила, которые требуется настроить «подтягивались» сразу всеми нодами из общего хранилища. Удаление значения «*:ro*» в конце строки необходимо, чтобы отменить режим «read-only».

Далее необходимо перейти в директорию */mnt/deepmail/core/overrides/postfix* и создать файл *postfix.cf*.

В файл необходимо добавить содержимое:

smtpd_recipient_restrictions = check_recipient_access lmdb:/overrides/recipient_restrictions_domain, socketmap:unix:/tmp/smtp-proxy.socket:aviable, check_sender_access lmdb:/overrides/reject_senders, check_policy_service unix:/tmp/smtp-proxy.socket

Далее необходимо создать *recipient_restrictions* и указать:

exemple.domen OK

Далее необходимо создать *reject_senders* и указать пользователей, которым будет запрещено отправлять письма за пределы домена:

user1@exemple.domen REJECT

После этого требуется выполнить команды:

docker exec -it deepmail-smtp postmap /overrides/recipient_restrictions

docker exec -it deepmail-smtp postmap /overrides/reject_senders

Данные команды выполняют для проверки того, что необходимые файлы (*recipient_restrictions.lmdb, reject_senders.lmdb*) созданы в папке */mnt/deepmail/core/overrides/postfix*, и в содержимом папки присутствуют файлы:

- *postfix.cf*;
- *recipient_restrictions*;
- *recipient_restrictions.lmdb*;
- *reject_senders*;
- *reject_senders.lmdb*.

После проверки поочередно на всех нодах необходимо выполнить команды:

deepmail stop

deepmail start

В результате пользователи, занесенные в файл *reject_senders* могут отправлять письма только на домены, которые указаны в файле *recipient_restrictions*. Все остальные пользователи могу отправлять письма без ограничений.

Если необходимо отредактировать список доменов или пользователей необходимо редактировать файлы *ecipient_restrictions* и *reject_senders*, после чего еще раз выполнить команды:

docker exec -it deepmail-smtp postmap /overrides/recipient_restrictions

docker exec -it deepmail-smtp postmap /overrides/reject_senders

И команды:

deepmail stop

deepmail start

3.8 Инструмент «Мастер миграции»

Настройка миграции осуществляется при помощи инструмента «Мастер миграции».

Для перехода к инструменту необходимо в меню интерфейса администратора выбрать «Мастер миграции» (рисунок 51).

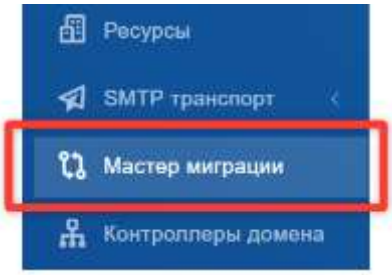


Рисунок 51 – Инструмент «Мастер миграции»

Окно «Мастер миграции» содержит список сторонних доменов, подключенных к серверу АРМ «DeepMail» (рисунок 52).

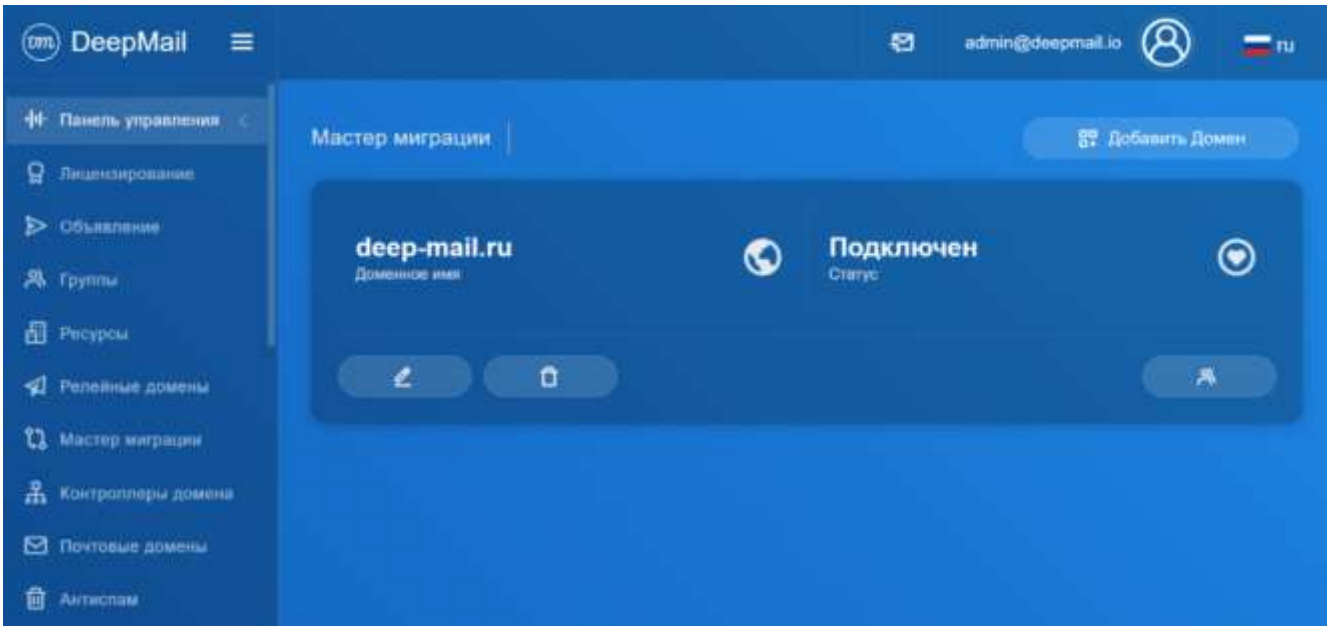


Рисунок 52 – Окно «Мастер миграции» со списком подключенных доменов

Для изменения настроек миграции необходимо на панели домена нажать кнопку  (см. рисунок 52). В результате в окне появится форма «Изменить домен для миграции» с настройками миграции, доступными для редактирования.

Для просмотра списка пользователей, чьи аккаунты требуется перенести в новый домен, необходимо нажать кнопку  (см. рисунок 52). В результате на экране отобразится форма «Список пользователей для миграции» (рисунок 53).

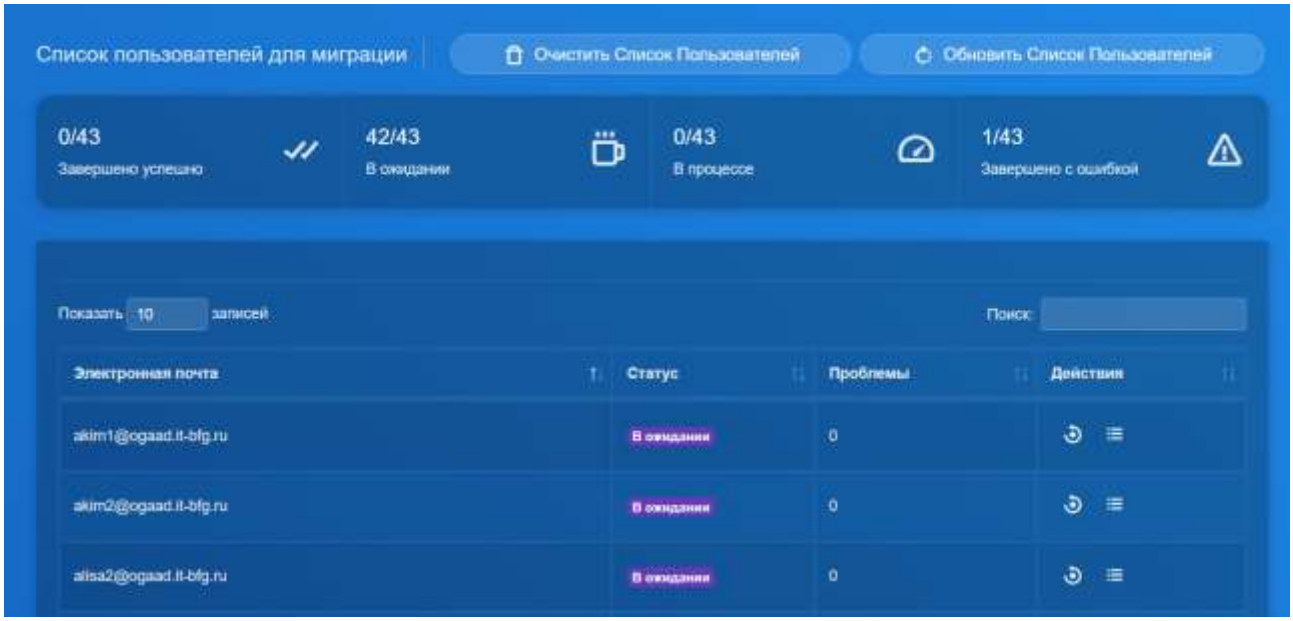


Рисунок 53 – Список для миграции

В верхней части формы содержится статистика миграции пользователей домена. Существуют следующие статусы миграции:

- «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 данных возникла ошибка, содержание которой можно увидеть в файле лога «migration_user_data.log».

Кнопка , расположенная в строке пользователя, предназначена для перезапуска миграции.

Кнопка предназначена для просмотра логов миграции пользовательских данных.

В случае большого количества записей поле «Поиск:» позволяет быстро найти информацию пользователя в таблице (рисунок 54).

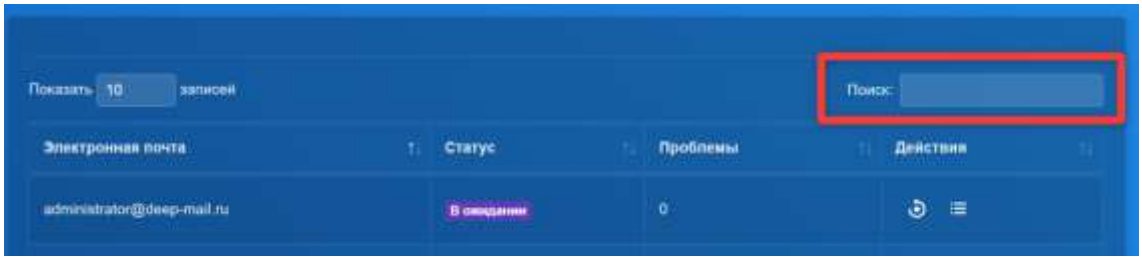


Рисунок 54 – Поле «Поиск:»

Обновить информацию о статусе миграции можно с помощью кнопки 

, расположенной над списком пользователей (см. рисунок 53).

Удалить пользователей из списка можно с помощью кнопки 

(см. рисунок 53).

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

Для добавления домена, с которого требуется перенести данные, необходимо в окне мастера миграции нажать кнопку 

(см. рисунок 52) и затем подтвердить готовность нажав «Продолжить» (рисунок 55).

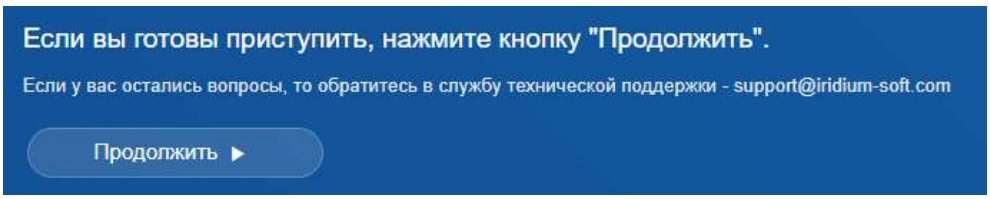


Рисунок 55 – Начало настройки миграции. Кнопка «Продолжить»

В окне появится форма настройки миграции на первом шаге «Базовые настройки» (рисунок 56).

Рисунок 56 – Настройка миграции. Шаг «Базовые настройки»

Настройка миграции состоит из следующих шагов:

- базовые настройки;
- настройка подключения к серверу по IMAP;

- подключение к серверу по IMAP;
- итоговая информация.

На шаге «Базовые настройки» необходимо выбрать почтовый домен (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 копировать новые непрочитанные входящие письма с предыдущего сервера на новый.

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 57).

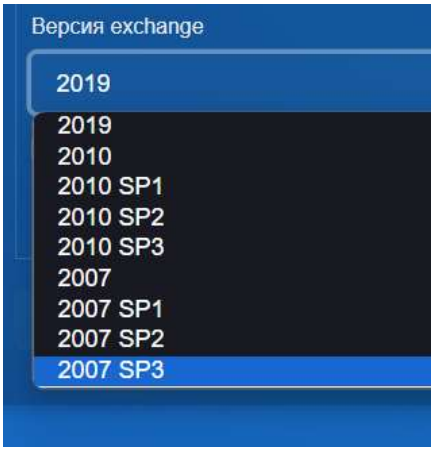


Рисунок 57 – Выбор версии сервера MS Exchange

Для миграции данных с сервера Microsoft Exchange на нем необходимо включить возможность работы по IMAP протоколу (см. инструкцию https://learn.microsoft.com/ru-ru/exchange/clients/pop3-and-imap4/configure-imap4?view=exchserver-2019).

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

Для перехода к следующему шагу нажмите кнопку «Далее» (см. рисунок 56).

На шаге «IMAP» необходимо указать IP-адрес удаленного IMAP-сервера и порт подключения (рисунок 58).

Рисунок 58 – Настройка миграции. Шаг «IMAP»

При необходимости можно воспользоваться опцией «Использовать SSL».

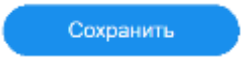
Удаленный хост также может быть размещен по адресу IPv4.

На шаге «Проверка подключения» будет отображен статус подключения по протоколу IMAP (рисунок 59).

Рисунок 59 – Проверка подключения к IMAP-серверу

На шаге «Итоговая информация» будет отображена информация с числом пользователей для миграции (рисунок 60).

Рисунок 60 – Настройка миграции. Шаг «Итоговая информация»

Для сохранения настроек нажмите кнопку  (см. рисунок 60).

3.8.2 Удаление настроек миграции для домена

Чтобы удалить настройки миграции для выбранного домена необходимо в окне мастера миграции нажать кнопку  (см. рисунок 52), и в открывшейся форме «Подтвердить действие» подтвердить удаление.

3.9 Инструмент «Контроллеры домена»

Для перехода к подключению контроллеров домена необходимо в меню интерфейса администратора выбрать «Контроллеры домена» (рисунок 61).

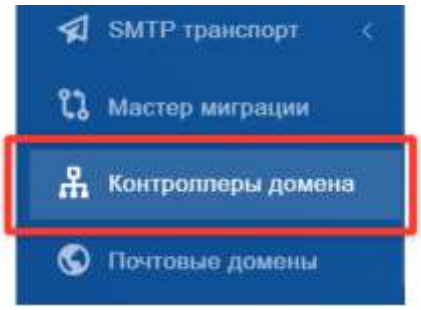


Рисунок 61 – Инструмент «Контроллеры домена»

В окне «Контроллеры домена» отображается перечень подключенных контроллеров домена (рисунок 62).

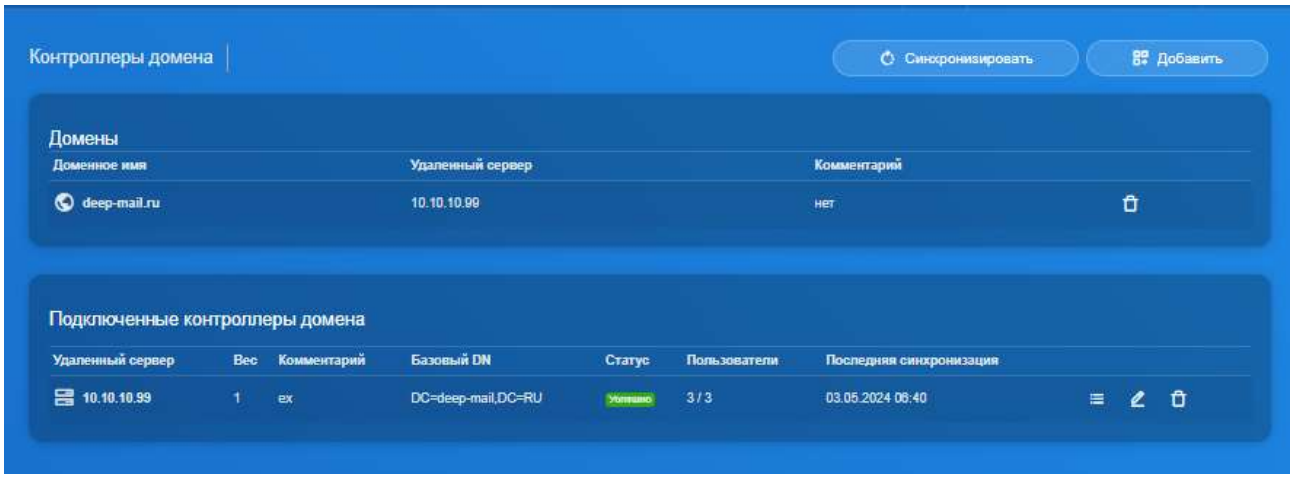


Рисунок 62 – Окно «Контроллеры домена»

Доступно подключение для следующих контроллеров домена: Samba DC, MS AD, ALD Pro, OpenLDAP.

Для просмотра списка логов подключенных контроллеров необходимо в окне контроллеров домена нажать кнопку  (см. рисунок 62).

3.9.1 Добавление контроллера домена

Для добавления контроллера домена необходимо нажать кнопку 

, расположенную в правом верхнем углу окна «Контроллеры домена» (см. рисунок 62). В результате на экране появится форма «Добавить контроллер домена», в которой необходимо указать параметры контроллера (рисунок 63).

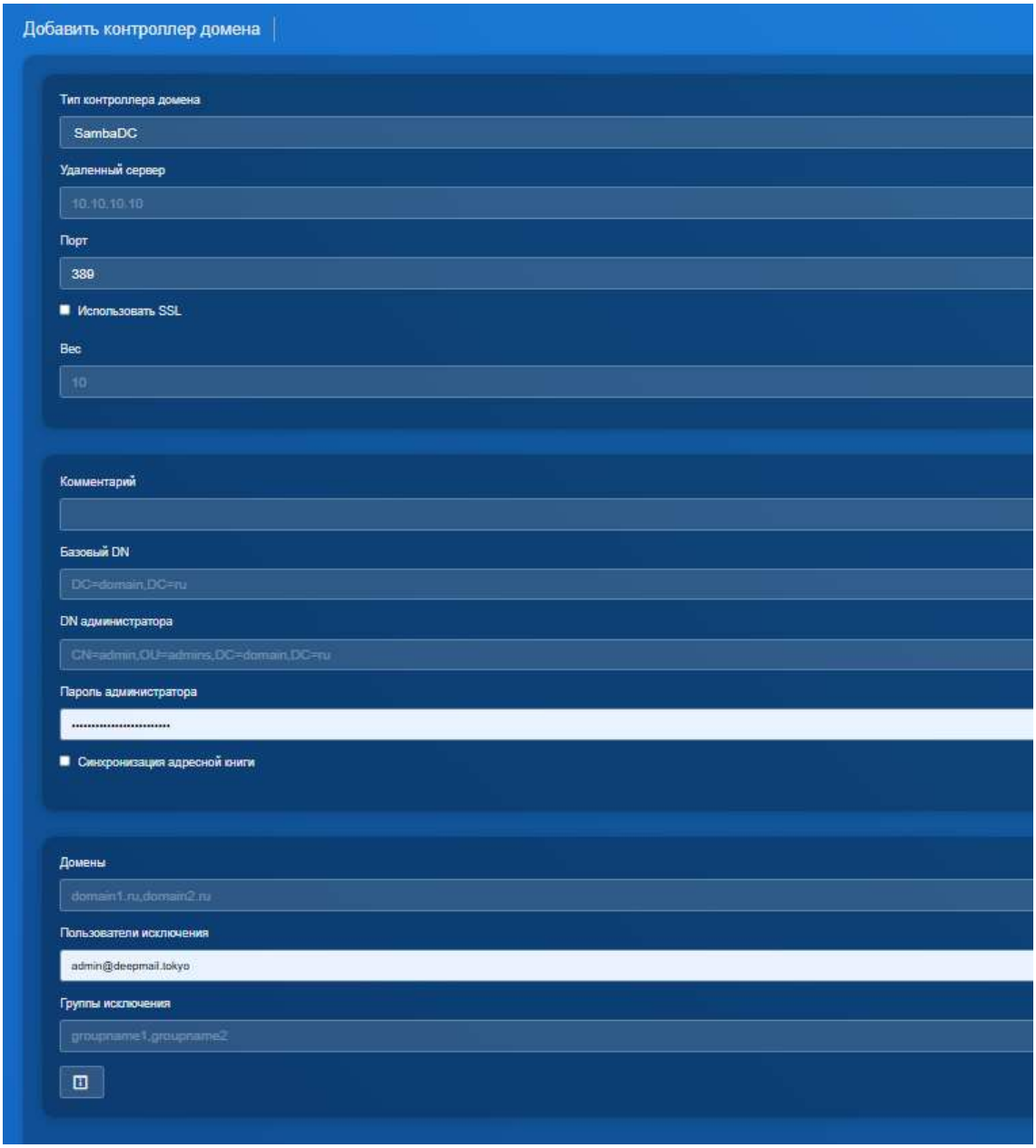


Рисунок 63 – Настройка подключения контроллера домена

Выберите тип подключаемого контроллера домена (рисунок 64).

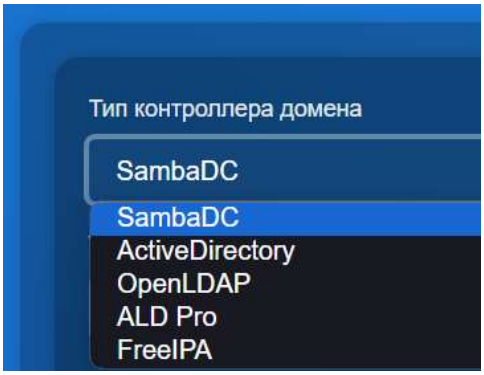


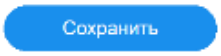
Рисунок 64 – Выбор типа контроллера домена

Указать следующие параметры контроллера:

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

Примечание. Пользователи из групп-исключений будут добавлены как пользователи без группы.

При заполнении данных важно правильно указать вес. Вес определяет приоритет контроллера домена. В случае невозможности подключится к основному контроллеру домена система будет обращаться к контроллеру домена с наименьшим весом и далее до установления подключения.

Для сохранения настроек необходимо нажать кнопку 

.

3.9.2 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, необходимо нажать кнопку 

, при этом информация о подключенных доменах отобразится в секции «Домены» окна «Контроллеры домена», а информация о подключенных контроллерах домена в секции «Подключенные контроллеры домена» (рисунок 65).

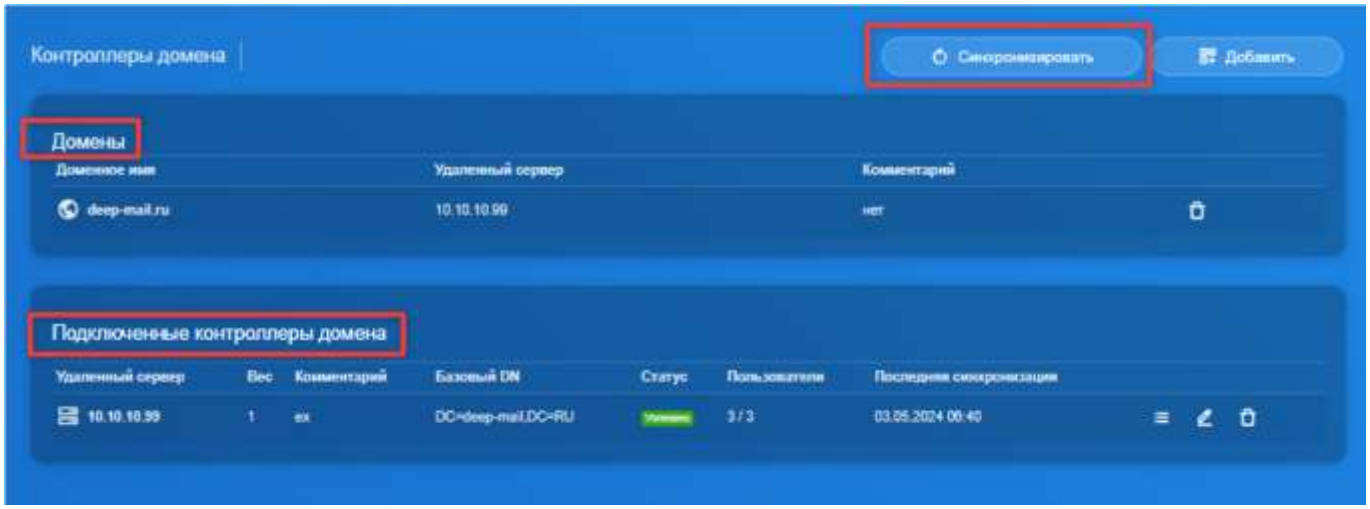


Рисунок 65 – Кнопка «Синхронизировать» и секции информации

В начале подключения контроллер домена имеет статус «В очереди», затем статус меняется на «Подключение» или «Синхронизация». Если авторизация пройдена, подключение выполнено, то статус становится «Успешно» (см. рисунок 65). В случае неудачного подключения статус контроллера – «Ошибка».

При подключении к контроллеру домена передаются имена пользователей, информация о их принадлежности к пользовательским группам, а также почтовые ящики пользователей. Почтовые ящики пользователей должны автоматически появиться в подключенном домене. Описание работы с почтовыми доменами приведено в «Инструмент «Почтовые домены»».

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

Для изменения настроек подключения необходимо нажать кнопку , и внести изменения в появившуюся форму.

3.9.3 Удаление контроллера домена

Для удаления контроллера домена необходимо нажать кнопку , и подтвердить удаление в открывшейся форме «Подтвердить действие».

3.10 Инструмент «Почтовые домены»

Настройка почтовых доменов производится в окне «Список доменов», для перехода к которому, необходимо в меню интерфейса администратора выбрать «Почтовые домены» (рисунок 66).

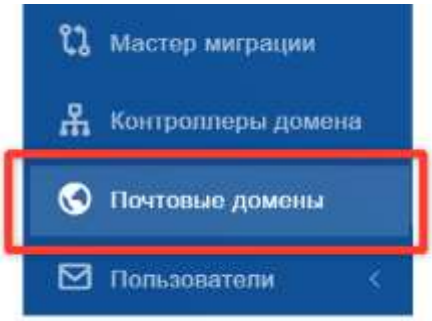


Рисунок 66 – Инструмент «Почтовые домены»

Окно «Список доменов» содержит список почтовых доменов, обслуживаемых сервером (рисунок 67).

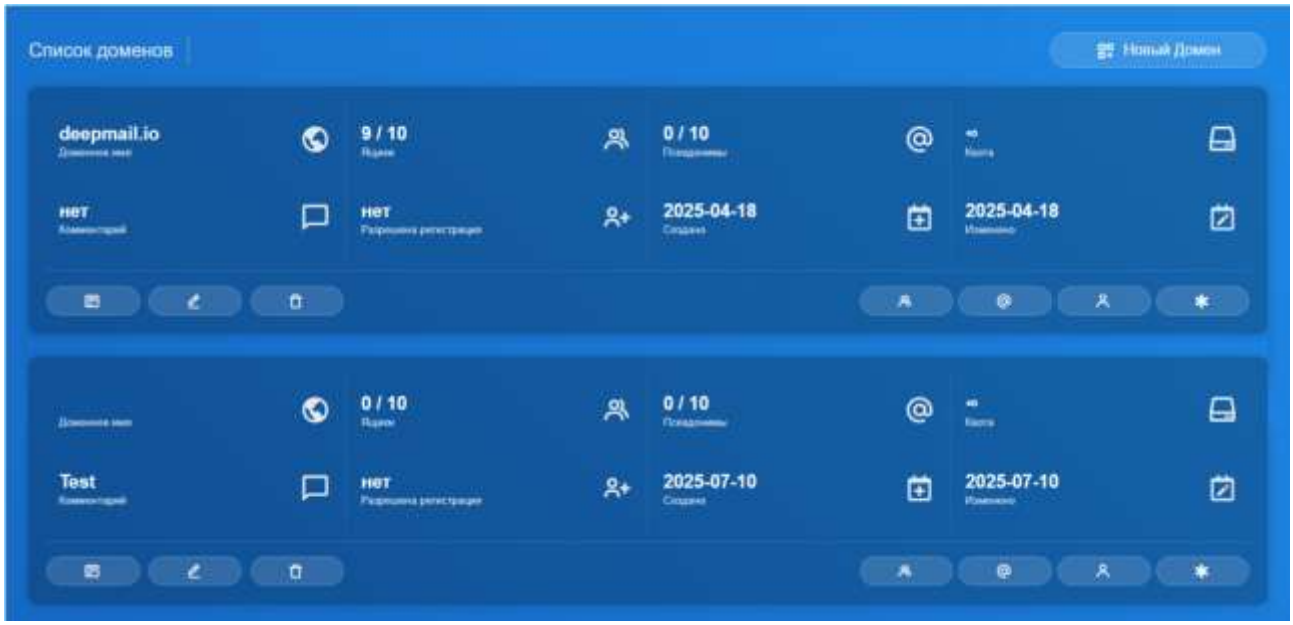
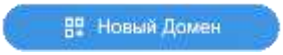


Рисунок 67 – Окно «Список доменов»

3.10.1 Действия с почтовыми доменами

3.10.1.1 Добавление нового почтового домена

Для добавления нового почтового домена необходимо в окне «Список доменов» нажать кнопку 

(см. рисунок 67). После этого будет выполнен переход к форме добавления нового почтового домена «Новый домен» (рисунок 68).

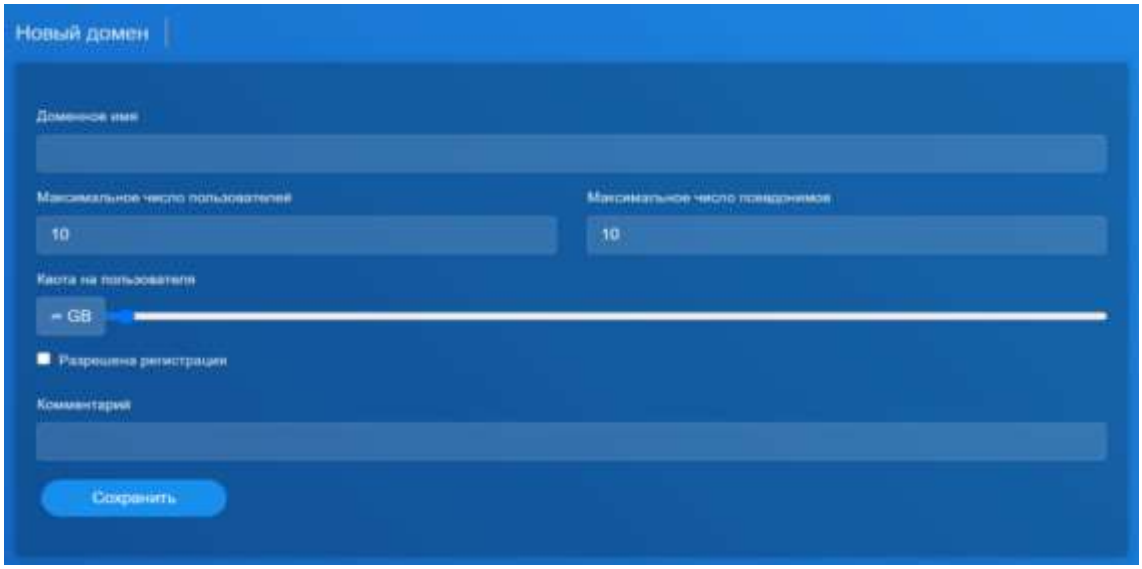
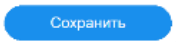


Рисунок 68 – Окно «Новый домен»

В открывшейся форме необходимо указать основные параметры нового почтового домена, такие как:

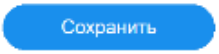
- «Доменное имя»;
- «Максимальное число пользователей»;
- «Максимальное число псевдонимов;
- выделить допустимую долю памяти на каждого пользователя в графе «Квота на пользователя»;
- определить опцию «Разрешена регистрация».

Для сохранения параметров необходимо нажать кнопку 

. В результате в окне появится сообщение 

, а новый домен отобразится в списке почтовых доменов.

3.10.1.2 Изменение почтового домена

Для изменения параметров созданных почтовых доменов необходимо в окне «Список доменов» нажать кнопку  (см. рисунок 67). После этого будет выполнен переход к форме к форме редактирования параметров домена «Изменить домен» в которой можно внести изменения в параметры домена и нажать кнопку 

(рисунок 69).

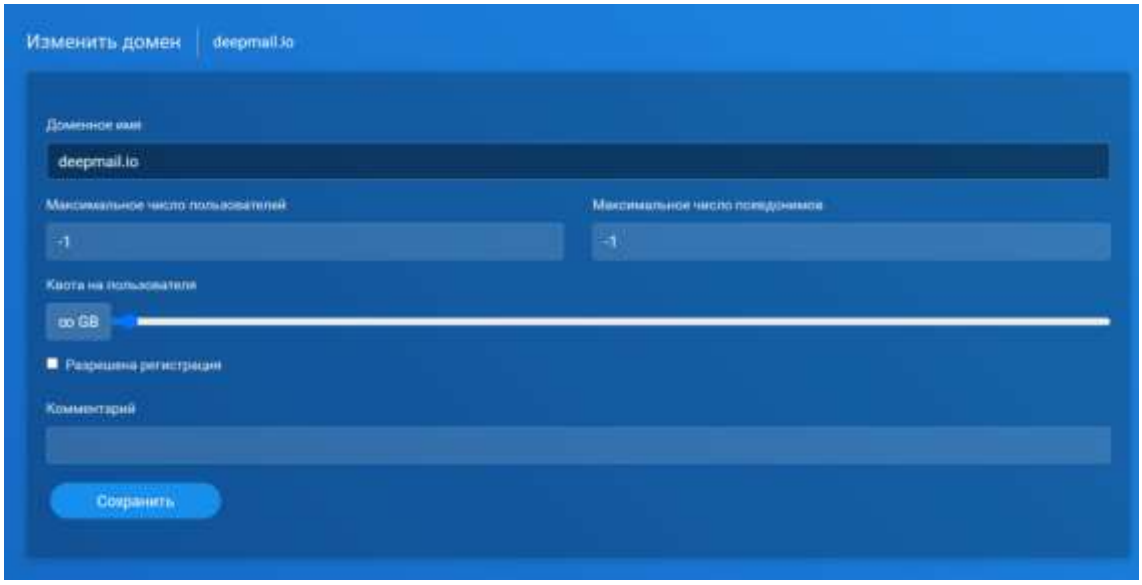


Рисунок 69 – Форма «Изменить домен»

В результате в окне появится сообщение  , а внесенные изменения отобразятся на панели почтового домена.

3.10.1.3 Удаление почтового домена

Для удаления почтового домена необходимо нажать кнопку  , расположенную на панели выбранного домена (рисунок 70).

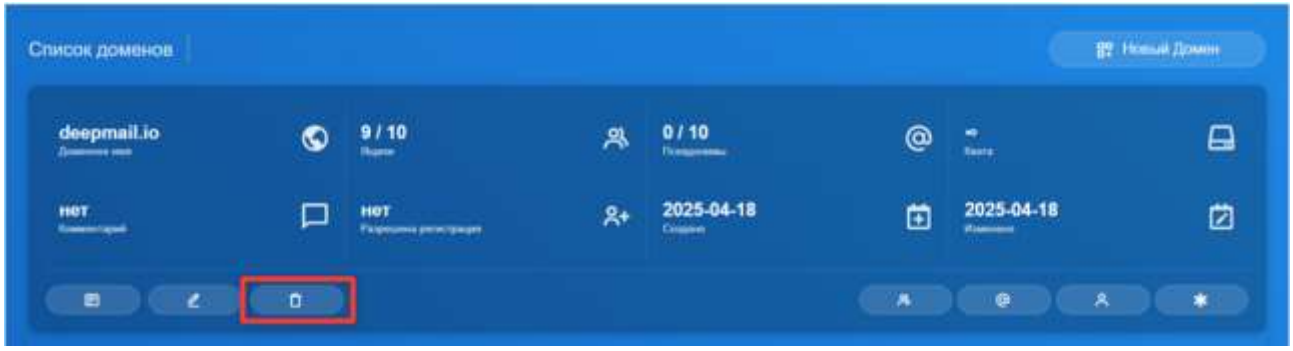


Рисунок 70 – Кнопка «Удалить»

Подтвердите удаление в открывшейся форме «Подтвердить действие».

3.10.2 Управление пользователями домена

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

Для вызова формы управления пользователями домена необходимо нажать кнопку  (рисунок 71).

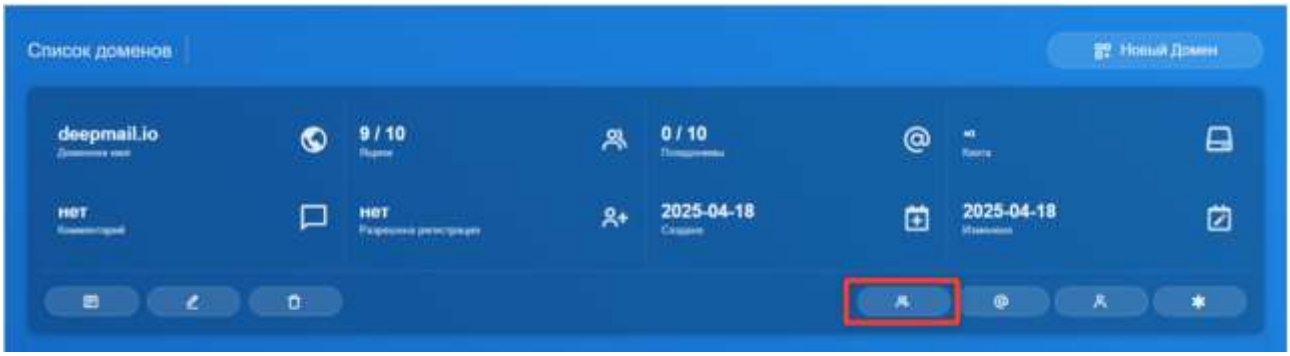


Рисунок 71 – Кнопка «Пользователи»

Откроется окно «Список пользователей» с поименным списком пользователей выбранного домена, отображенным в табличном виде (рисунок 72).

Рисунок 72 – Окно «Список пользователей»

В таблице представлена информация по всем пользователям домена, включая размер почтовых ящиков и размер занятой ими памяти.

3.10.2.1 Создание нового пользователя почтового домена

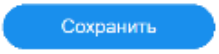
Для создания нового пользователя домена в окне «Список пользователей» необходимо нажать кнопку  (см. рисунок 72). На экране появится форма «Новый пользователь» (рисунок 73).

Рисунок 73 – Форма «Новый пользователь»

В форме необходимо указать электронный адрес нового пользователя, пароль и при необходимости добавить группу или группы пользователей.

Далее необходимо выбрать протокол доступа пользователя к почте (POP3, SMTP или IMAP), назначить квоту памяти на почтовый ящик (рисунок 74).

Рисунок 74 – Настройка квоты памяти и почтовых протоколов для пользователя

Для сохранения нажмите кнопку 

.

3.10.2.2 Редактирование и настройка параметров почтового ящика пользователя

Для изменения настроек учетной записи пользователя необходимо нажать кнопку  (см. рисунок 72), и внести изменения в параметры пользователя в форме «Изменить пользователя» (рисунок 75).

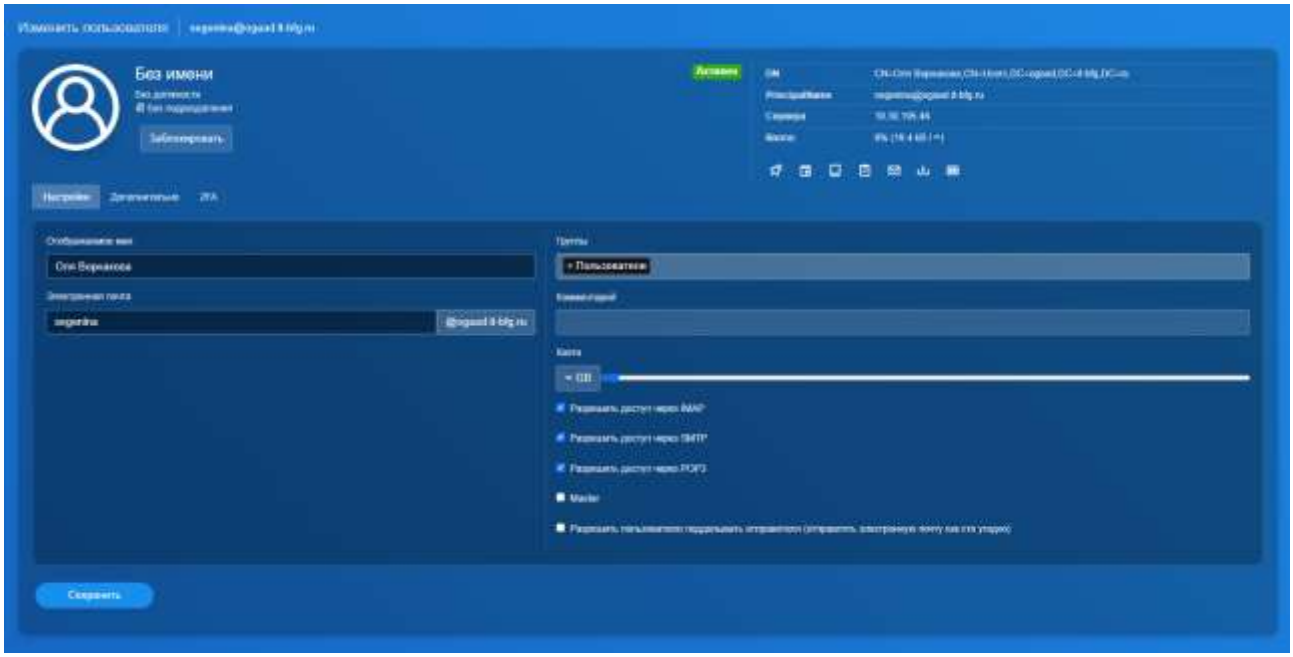


Рисунок 75 – Форма «Изменить пользователя»

Для настройки параметров спам фильтра или переадресации сообщений необходимо перейти на вкладку «Дополнительно» (рисунок 76).

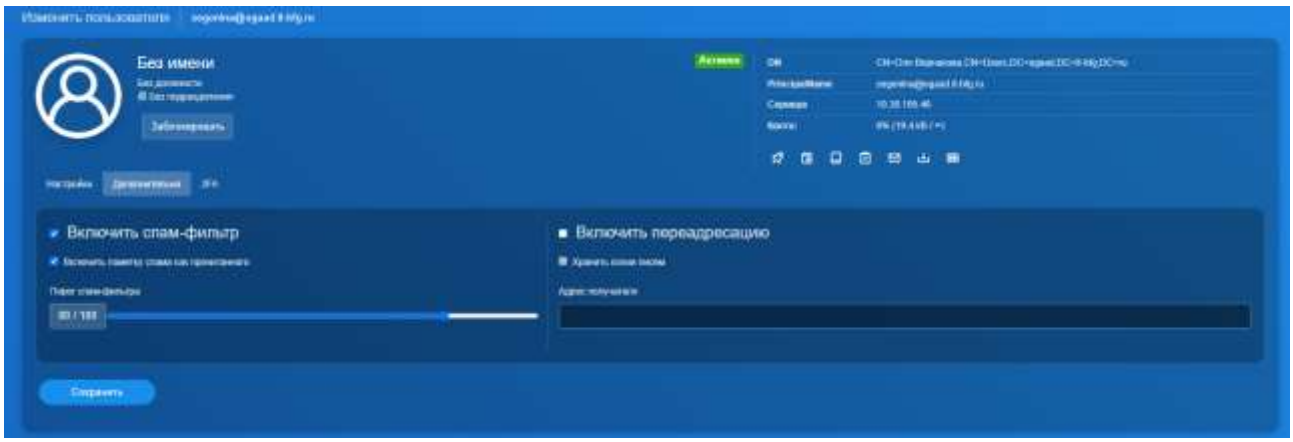


Рисунок 76 – Дополнительные настройки пользователя

Данные подключения и адрес сервера пользователей, подключенных через LDAP, отображаются в правой части окна (рисунок 77).

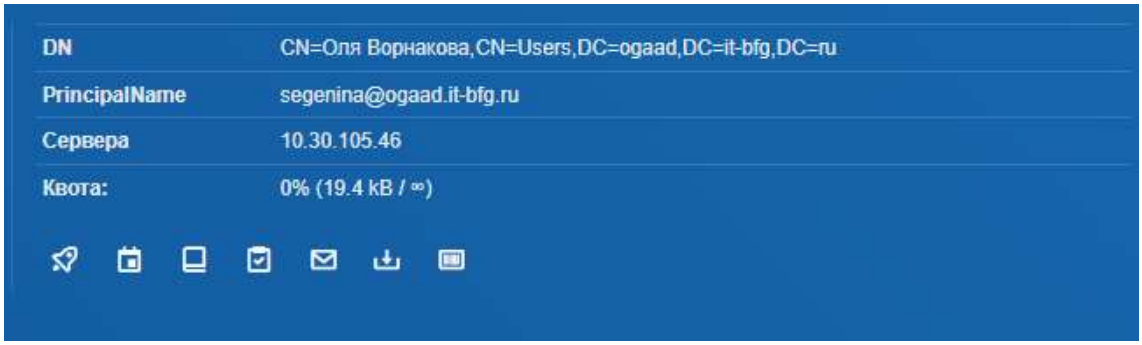


Рисунок 77 – Данные пользователя, подключенного через LDAP

Внесите изменения и нажмите кнопку Сохранить (см. рисунок 76).

3.10.2.3 Блокировка пользователя

Заблокированные пользователи не могут отправлять и получать почту.

Для блокировки пользователя необходимо нажать кнопку Заблокировать, расположенную рядом с аватаром пользователя (см. рисунок 76), при этом статус пользователя изменится на Заблокирован.

Для разблокировки пользователя необходимо нажать кнопку Разблокировать (будет размещена там же, что и кнопка блокировки), в результате чего статус пользователя изменится на Активен.

3.10.2.4 Удаление пользователя

Для удаления пользователя необходимо нажать кнопку, расположенную на панели пользователя (см. рисунок 72), и подтвердить удаление в открывшейся форме «Подтвердить действие».

3.10.3 Псевдонимы почтового домена

3.10.3.1 Создание псевдонима почтового домена

Сервер позволяет добавлять дополнительные почтовые адреса (псевдонимы) пользователю или нескольким пользователям, при этом сообщения, приходящие на адрес псевдонима, будут автоматически отсылаться на все аккаунты, к которым он привязан.

Для добавления дополнительного адреса необходимо в окне «Список доменов» на панели выбранного домена нажать кнопку @ (рисунок 78).

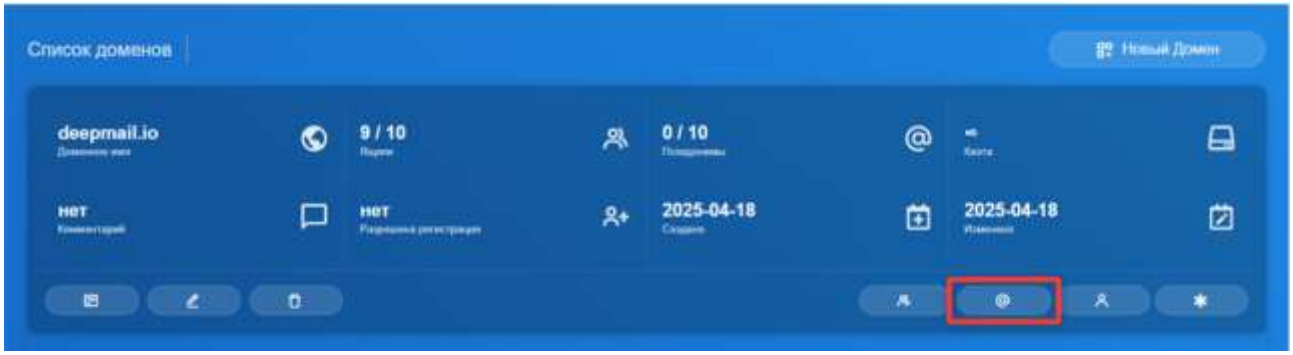


Рисунок 78 – Кнопка для перехода к созданию псевдонимов

На экране появится окно «Список псевдонимов» (рисунок 79).

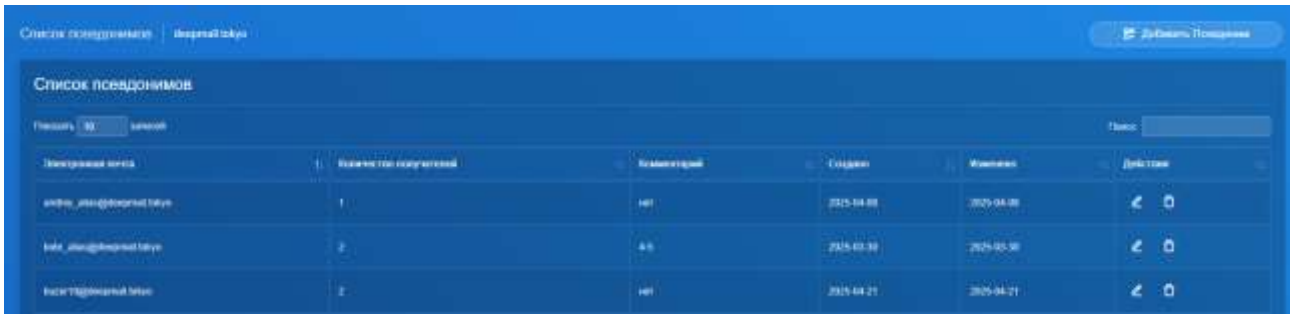


Рисунок 79 – Окно «Список псевдонимов» пользователей домена

Нажмите кнопку 

для открытия формы создания нового псевдонима (рисунок 80).

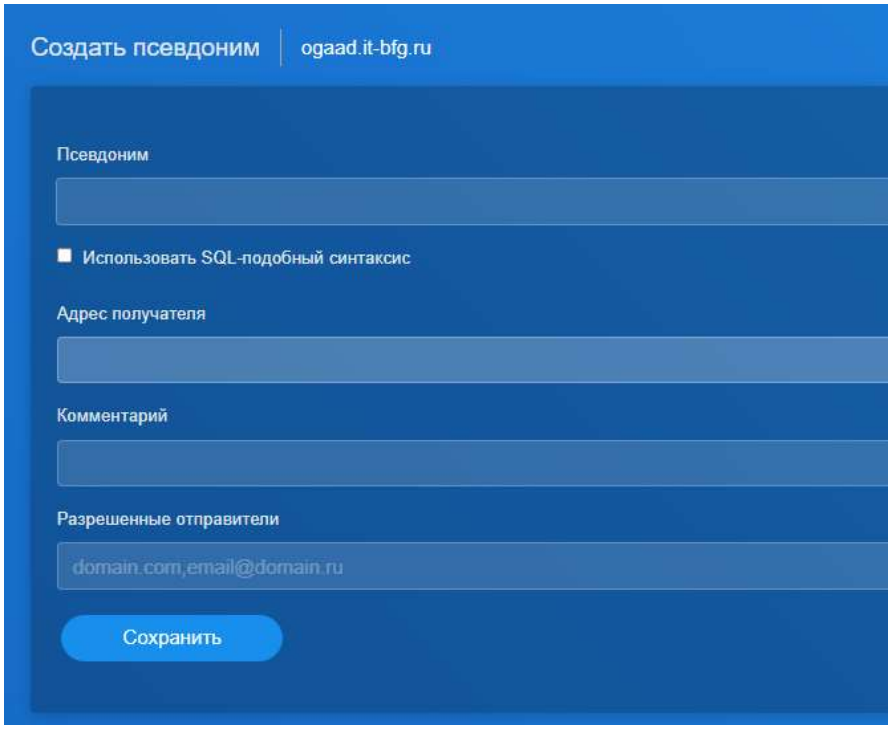
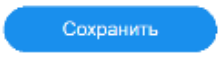


Рисунок 80 – Форма «Создать псевдоним»

В появившейся форме необходимо заполнить параметры: «Псевдоним» (электронный адрес псевдонима), «Адрес получателя» (существующий почтовый адрес или адрес домена), «Комментарий» (заполнять необязательно) и «Разрешенные отправители» (можно указать как целый домен, так и отдельный электронный адрес, никто кроме указанных в этом поле отправителей не сможет отправить письмо на этот псевдоним).

Нажать кнопку 

. Созданный псевдоним должен отобразиться в списке псевдонимов домена.

3.10.3.2 Удаление псевдонима почтового домена

Для удаления псевдонима необходимо нажать кнопку  , расположенную в строке этого псевдонима (см. рисунок 79), и подтвердить удаление в открывшейся форме «Подтвердить действие».

3.10.4 Менеджеры почтового домена

Для управления менеджерами почтового домена необходимо в окне «Список доменов» на панели выбранного домена нажать кнопку  (рисунок 81).

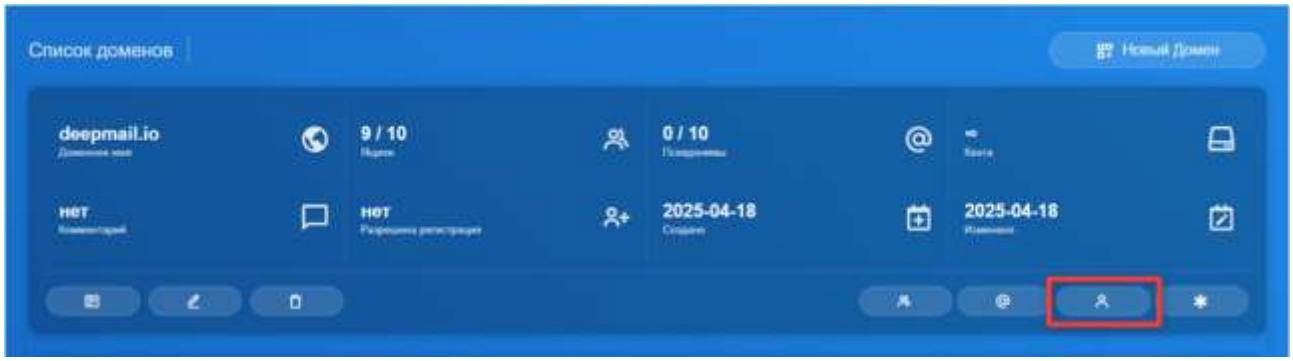


Рисунок 81 – Кнопка перехода к списку менеджеров домена на панели почтового домена

На экране появится окно «Список менеджеров» (рисунок 82).

Рисунок 82 – Окно со списком менеджеров почтового домена

3.10.4.1 Добавление менеджера почтового домена

Для добавления менеджера почтового домена необходимо в окне «Список менеджеров» нажать кнопку 

(см. рисунок 82).

На экране появится окно с формой «Добавить менеджера» (рисунок 83),

Рисунок 83 – Форма «Добавить менеджера»

Выбрать пользователя из выпадающего списка и нажмите кнопку Отправить.

В результате выбранный пользователь появится в списке менеджеров.

3.10.4.2 Удаление менеджера почтового домена

Для удаления менеджера необходимо в окне «Список менеджеров» нажать кнопку , расположенную в строке выбранного менеджера (см. рисунок 82), и подтвердить удаление в открывшейся форме «Подтвердить действие».

3.10.5 Альтернативный почтовый домен

Сервер позволяет настраивать альтернативные имена почтового домена, при этом почта доходит до пользователей как по основному имени домена, так и по всем альтернативным именам.

Для просмотра списка альтернативных имен почтового домена необходимо в окне «Список доменов» нажать кнопку *, расположенную на панели выбранного почтового домена (рисунок 84).

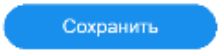
Рисунок 84 – Кнопка для перехода к списку альтернативных имен почтового домена

На экране появится окно «Список альтернативных доменов» (рисунок 85).

Рисунок 85 – Окно «Список альтернативных доменов»

3.10.5.1 Создание альтернативного почтового домена

Для создания альтернативного имени почтового домена необходимо перейти к форме «Создать альтернативный домен», нажав кнопку 

(см. рисунок 85). В открывшейся форме указать имя домена и нажать «Сохранить» 

(рисунок 86).

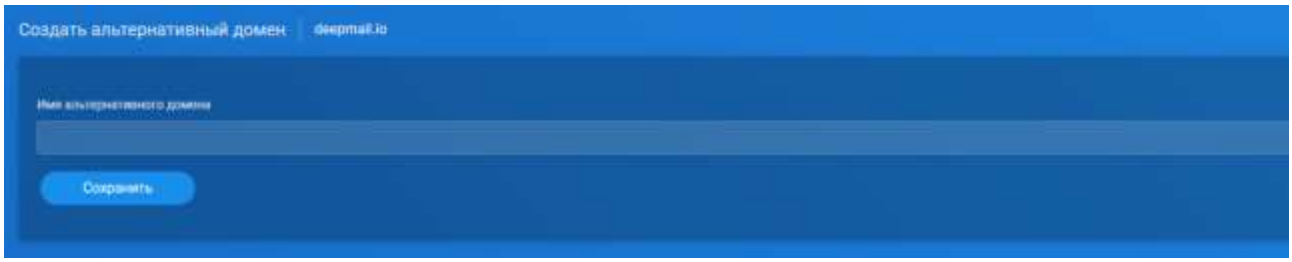


Рисунок 86 – Форма «Создать альтернативный домен»

В окне появится сообщение 

, а домен появится в списке альтернативных доменов (см. рисунок 85).

3.10.5.2 Удаление альтернативного почтового домена

Для удаления альтернативного почтового домена необходимо в окне «Список альтернативных доменов» нажать кнопку 
, расположенную на панели этого альтернативного домена (см. рисунок 85), и подтвердить удаление в открывшейся форме «Подтвердить действие».

3.10.6 Настройка DNS почтового домена

Для просмотра DNS записей домена необходимо в окне «Список доменов» на панели выбранного домена нажать кнопку  (рисунок 87).

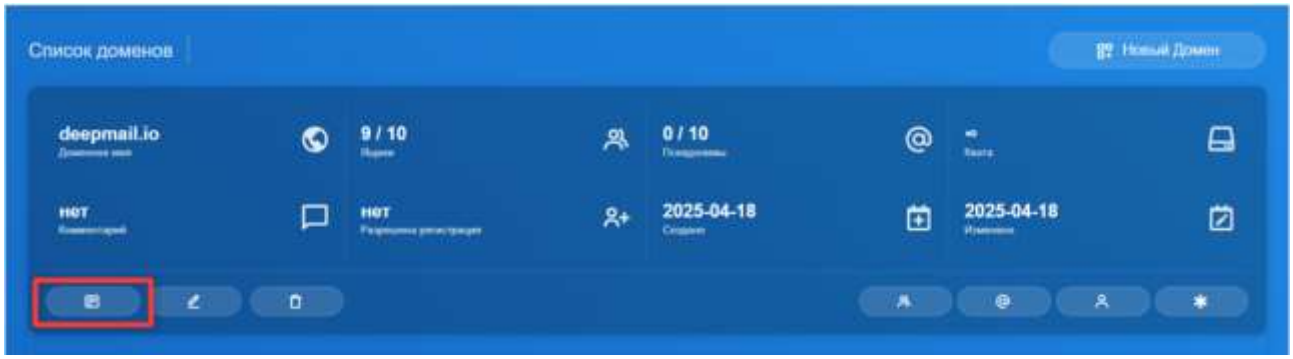


Рисунок 87 – Кнопка перехода к просмотру DNS записей домена

В результате откроется форма «Подробности домена» (рисунок 88).

Рисунок 88 – Окно «Подробности домена»

В окне «Подробности домена» приведена следующая информация:

- «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 сообщений, гарантирующей их подлинность;
- «DNS DMARC запись», которая определяет политику сервера получателя в отношении сообщений, отправленных с домена, но не прошедших аутентификацию;
- «Записи автоматической настройки DNS-клиента» почтового клиента.

Форма содержит кнопку 

(см. рисунок 88), 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.

Данные для настройки рекомендуется брать из таблицы 4.

SPF (Sender Policy Framework) представляет собой текстовую запись в TXT-записи DNS домена. Запись содержит информацию о списке серверов, которые имеют право отправлять сообщения от имени этого домена и механизм обработки сообщений, отправленных с 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 регламентирует серверу, что делать с сообщением, если записи DKIM и SPF окажутся некорректны. Корректные DKIM и SPF подтверждают, что сообщение отправлено от имени домена, указанного в поле «От:» в письме. Таким образом, DMARC наряду с SPF и DKIM отвечает за аутентификацию почты.

Если сгенерированных ключей домена нет, то форма «Подробности домена» будет иметь вид представленный на рисунке 89.

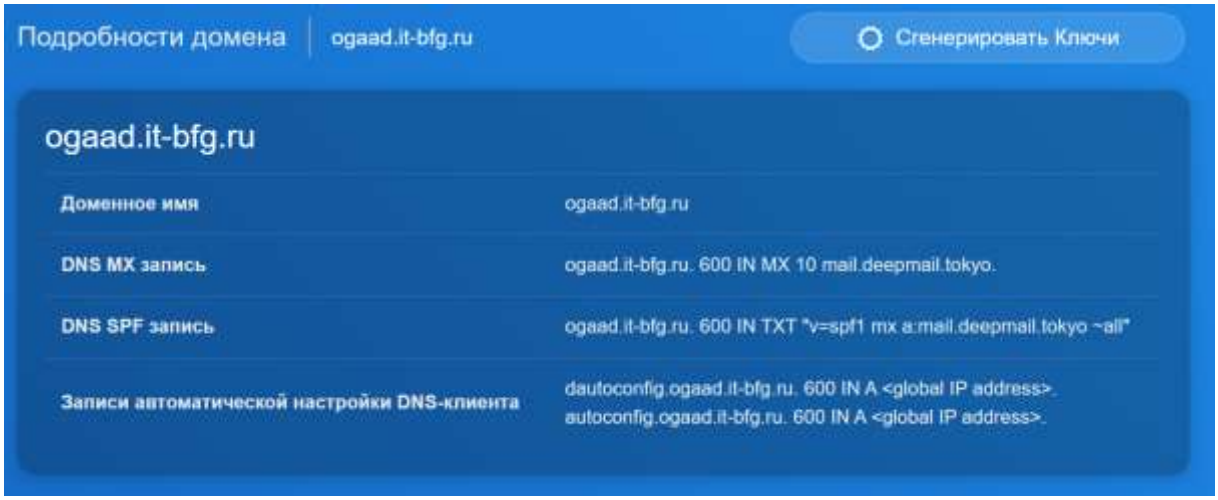


Рисунок 89 – Кнопка «Сгенерировать ключи»

Для генерации ключей необходимо в форме с подробной информацией о домене нажать кнопку Сгенерировать Ключи (см. рисунок 89), и подтвердить действие в следующем окне (рисунок 90).

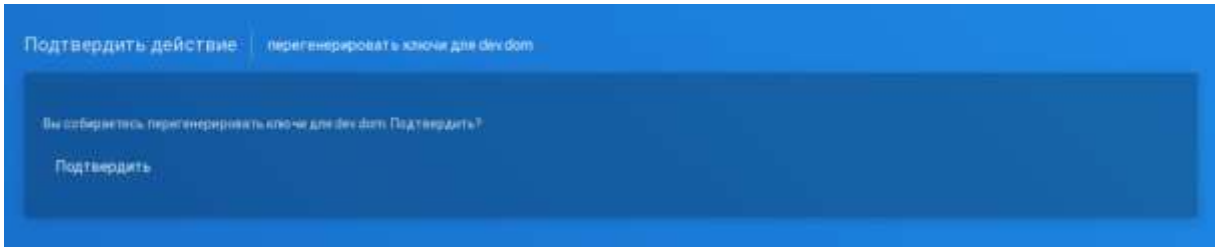


Рисунок 90 – Кнопка «Подтвердить»

После генерации ключа его текст копируется из появившегося после генерации раздела «ПУБЛИЧНЫЙ КЛЮЧ DKIM» и вставляется в «DNS DKIM запись», кнопка Сгенерировать Ключи заменяется кнопкой Перегенерировать Ключи (рисунок 91).

Рисунок 91 – Автоматическое добавление DKIM ключа в запись

В таблице 4 приведены необходимые DNS-записи с общепринятыми обозначениями:

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

Таблица 4 – Типы DNS записей

Тип	Имя	Значение	Дополнительная 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	-

3.10.7 Управление общими почтовыми ящиками

Почта, приходящая в почтовый ящик, может быть доступна сразу нескольким пользователям. Эти пользователи могут использовать адрес данного почтового ящика для отправки своих сообщений. Такие почтовые ящики называются общими. Управление общими почтовыми ящиками производится в рамках одного почтового домена.

3.10.7.1 Создание общего почтового ящика

Для создания общего почтового ящика необходимо перейти в окно «Список доменов» (Инструмент «Почтовые домены»), выбрать почтовый домен в котором будет создан новый общий почтовый ящик, и нажать кнопку  (см. пункт 3.10.2).

В открывшемся окне «Список пользователей» необходимо нажать кнопку 

(рисунок 92).

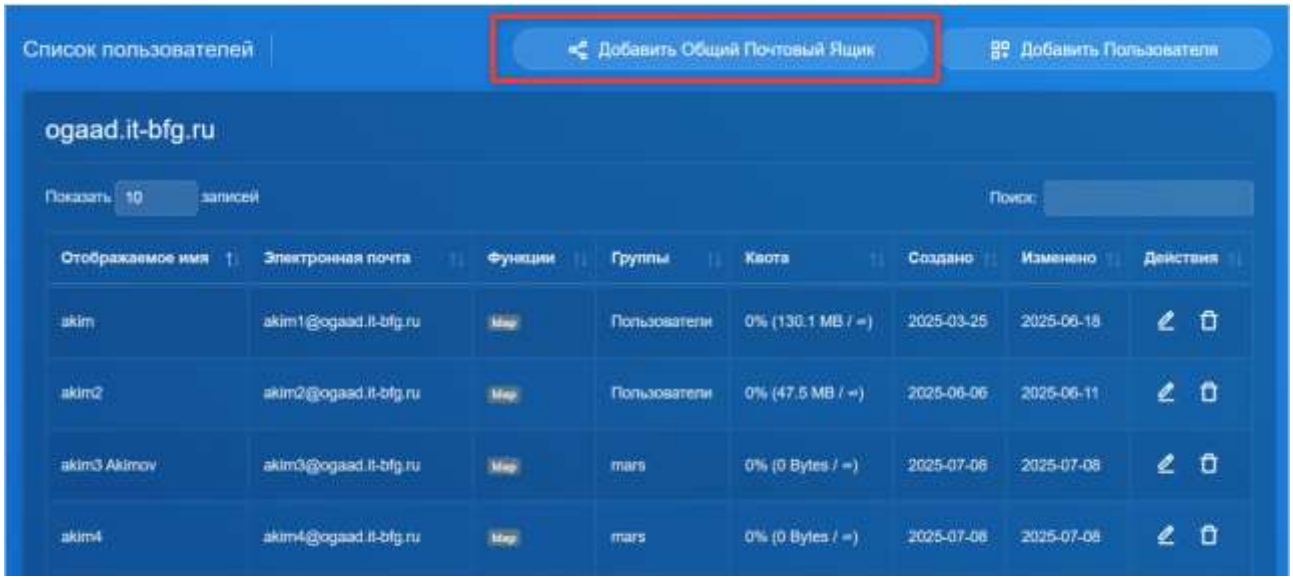


Рисунок 92 – Окно «Список пользователей»

На экране появится форма «Новый общий почтовый ящик» (рисунок 93).

Рисунок 93 – Окно создания нового общего почтового ящика

В форме «Новый общий почтовый ящик» необходимо заполнить следующие данные:

- в поле «Отображаемое имя» указать отображаемое имя общего почтового ящика;
- в поле «Электронная почта» указать адрес общего почтового ящика;
- в поле «Группы указать группу или группы, которые будут иметь доступ к данному почтовому ящику;
- в поле «Пользователи, имеющие доступ» указать отдельный список пользователей (при наличии), у которых будет доступ к ящику;

– выставить квоту памяти ящика в области «Квота».

Для сохранения указанных данных необходимо нажать кнопку Сохранить (см. рисунок 93).

В списке пользователей в столбце «Функции» добавленный почтовый ящик отмечен как «Общий почтовый ящик» (рисунок 94).

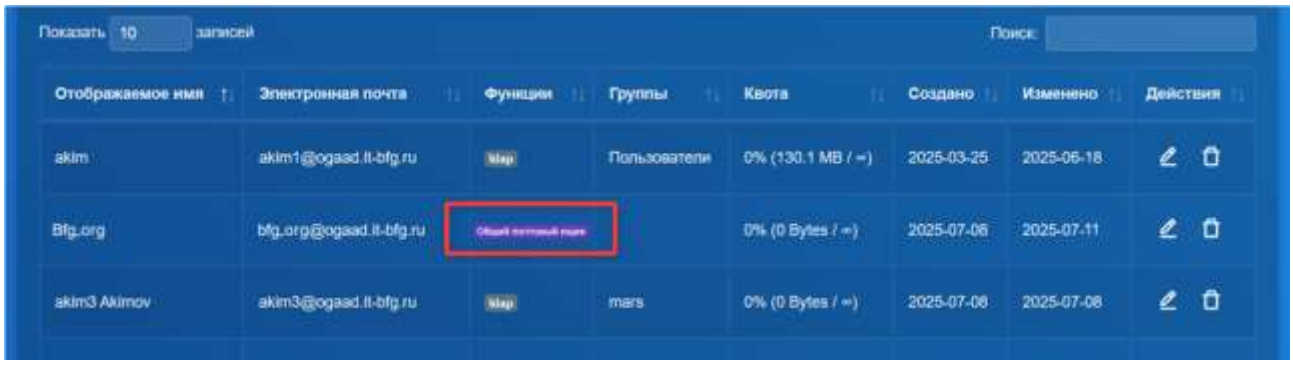


Рисунок 94 – Общий почтовый ящик в списке пользователей

3.10.7.2 Редактирование общего почтового ящика

Для перехода к форме редактирования общего почтового ящика необходимо нажать кнопку , расположенную в списке пользователей, в строке общего почтового ящика, столбец «Действия» (см. рисунок 94).

Настройке доступны все параметры почтового ящика за исключением адреса электронной почты. Для сохранения внесенных изменений необходимо нажать кнопку Сохранить.

3.10.7.3 Удаление общего почтового ящика

Для удаления общего почтового ящика необходимо нажать кнопку , расположенную в списке пользователей, в строке общего почтового ящика, столбец «Действия» (см. рисунок 94) и подтвердить удаление в открывшейся форме «Подтвердить действие».

3.11 Инструмент «Пользователи»

Для управления параметрами пользователей применяется инструмент администрирования «Пользователи», который состоит из инструментов:

– «WebDav ACL», предназначенный для делегирования прав на календари, папки задач и адресные книги;

– «Список переадресаций», предназначенный для настройки переадресации писем с почтовых ящиков (рисунок 95).

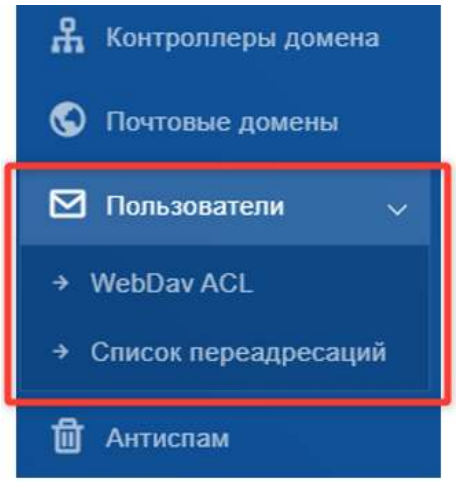


Рисунок 95 – Инструмент «Пользователи»

3.11.1 Пользователи| WebDav ACL

ACL (Access Control List) – механизм для гибкой маршрутизации трафика на основе условий. В контексте WebDAV ACL определяет правила, по которым запросы с данными календарей и контактов направляются к WebDAV-серверу

Для управления делегированием прав необходимо в меню интерфейса администратора выбрать «Пользователи» → «WebDav ACL» (см. рисунок 95).

На экране отобразится окно «Пользователи| WebDav ACL», в котором приведена информация о настроенных правах делегирования для конкретных пользователей (рисунок 96).

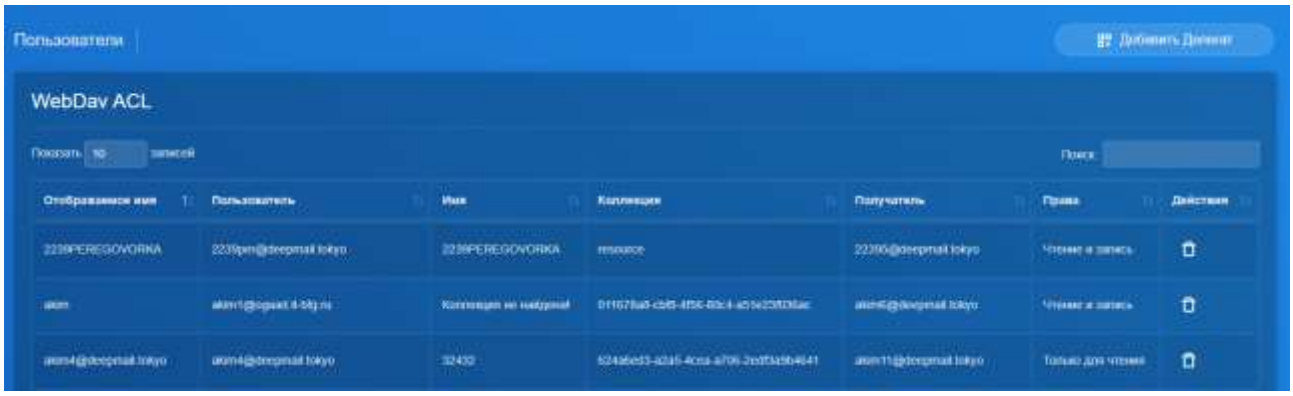
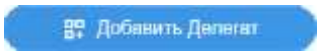


Рисунок 96 – Окно «WebDav ACL»

Делегирование осуществляется в рамках одного домена.

Чтобы делегировать права необходимо в окне «Пользователи| WebDav ACL» нажать кнопку 

(см. рисунок 96), после чего откроется окно настройки делегирования «Добавить делегат» (рисунок 97).

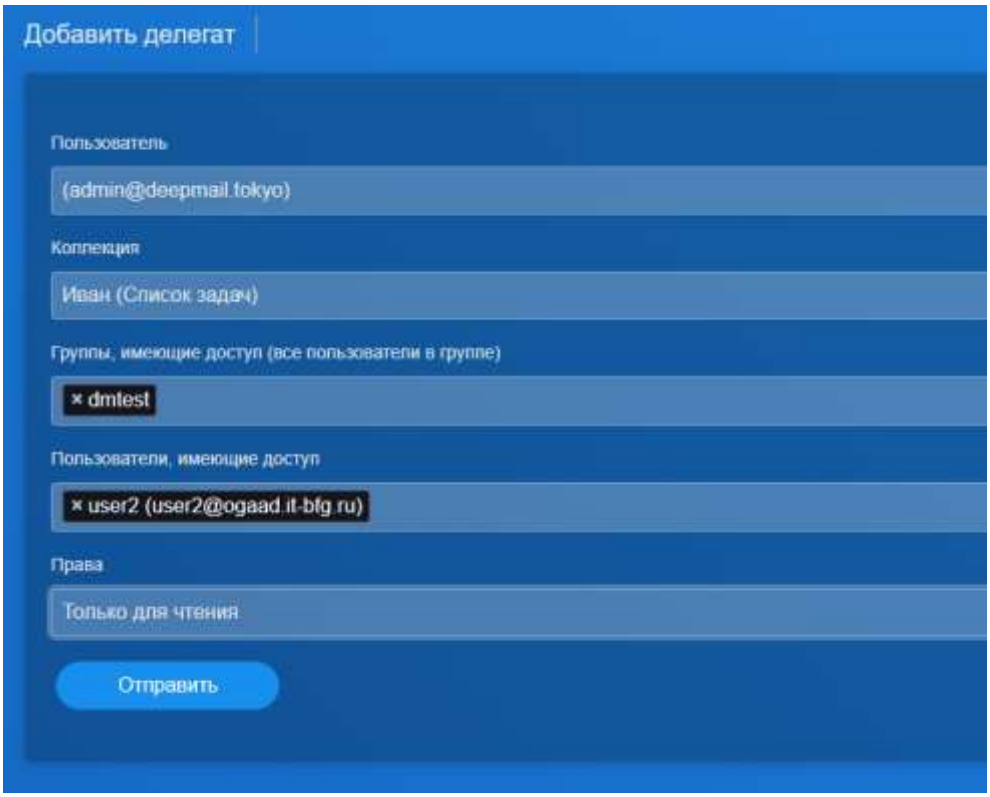


Рисунок 97 – Настройка делегирования

В открывшемся окне необходимо заполнить поля:

- «Пользователь» – электронный адрес пользователя, который делегирует права;
- «Коллекция» – выбрать из выпадающего списка доступные объекты (папки) для делегирования прав на них;
- «Группы, имеющие доступ (все пользователи в группе)» – группа (или несколько групп) пользователей, которой будет предоставлен доступ к выбранной коллекции;
- «Пользователи, имеющие доступ» – пользователь (или несколько пользователей), которому будет предоставлен доступ к выбранной коллекции;
- «Права» – тип прав, которые получат выбранные группы или пользователи (могут быть «Только для чтения», «Чтение и запись»).

Пользователи могут самостоятельно давать права на собственные календари и папки задач и контактов выполняя настройки делегирования через десктопную (установленную непосредственно на ПК) версию Клиента (описание действий приведено в руководстве пользователя на Клиент).

3.11.2 Список переадресаций

Для настройки переадресаций необходимо в меню интерфейса администратора выбрать «Пользователи» → «Список переадресаций» (рисунок 98).

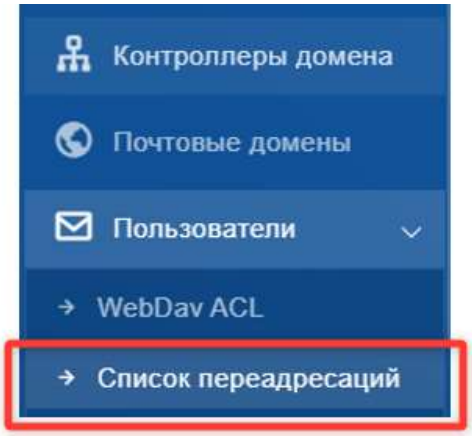


Рисунок 98 – Инструмент «Список переадресаций»

Для настройки переадресации необходимо в окне со списком переадресаций нажать кнопку 

, после чего откроется окно «Добавить переадресацию» для настройки переадресаций (рисунок 99).

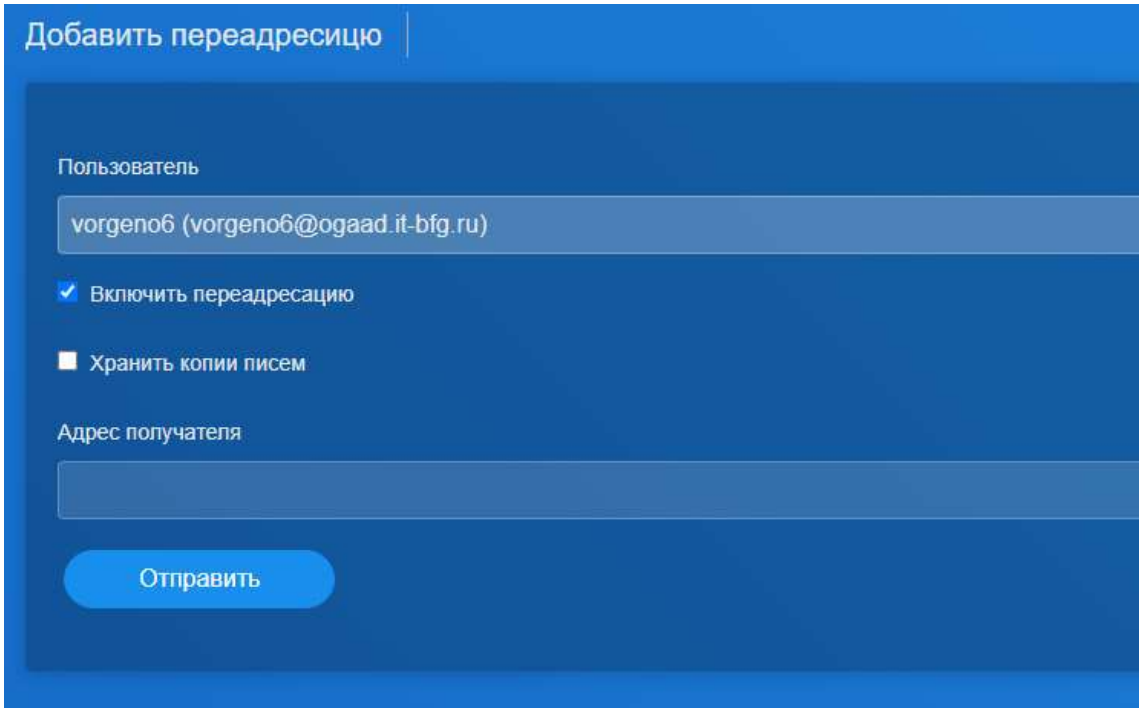


Рисунок 99 – Настройка переадресаций

В данном окне необходимо заполнить поля:

- «Пользователь» – электронный адрес пользователя чья корреспонденция будет переадресовываться;

– «Адрес получателя» – электронный адрес пользователя, на который будут переадресовываться письма.

Для включения переадресации необходимо отметить параметр «Включить переадресацию».

При необходимости сохранения копий писем в почтовом ящике первоначального получателя необходимо отметить параметр «Хранить копии писем».

Для завершения настройки переадресации нажмите кнопку 

(см. рисунок 99).

3.12 Инструмент «Антиспам»

Для перехода к инструменту работы со спам-фильтром необходимо в меню интерфейса администратора выбрать «Антиспам» (рисунок 100).

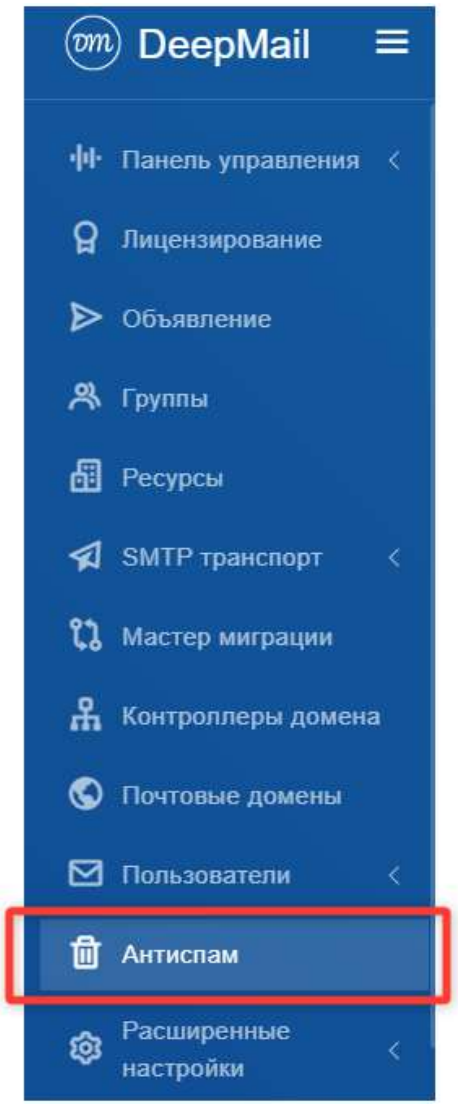


Рисунок 100 – Инструмент «Антиспам»

В результате появится окно системы фильтрации спама RSPAMD, содержащее статистические данные и информацию о параметрах спам-фильтрации (рисунок 101).

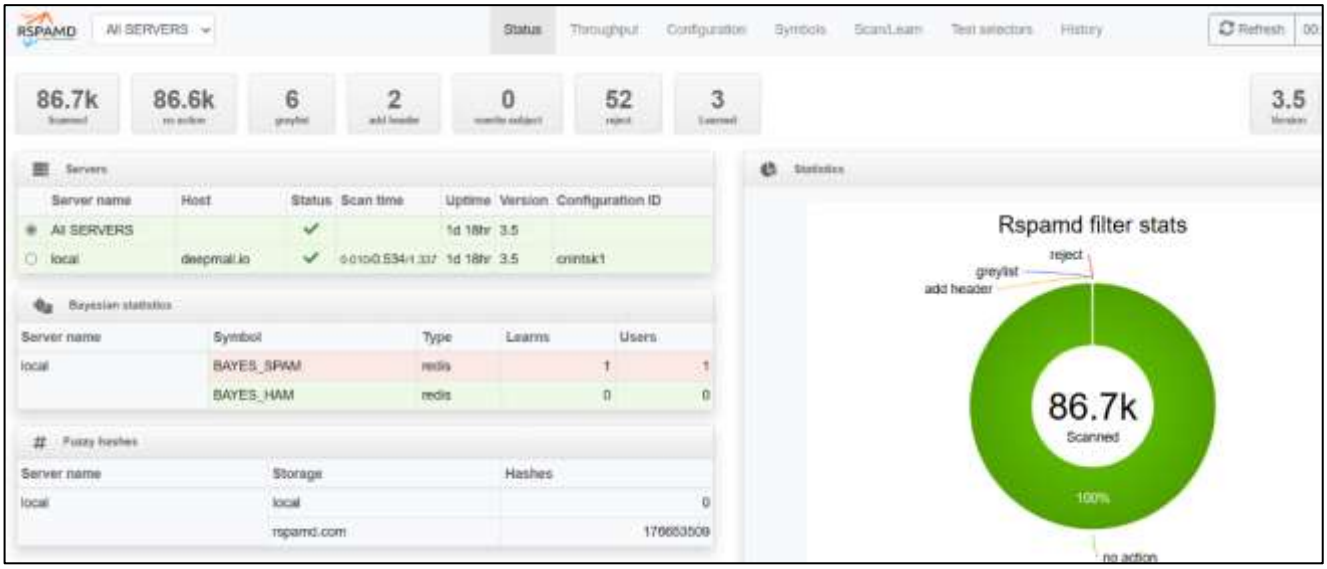


Рисунок 101 – Окно системы RSPAMD

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

На вкладке «History» отображается история обработки сообщений (рисунок 102).

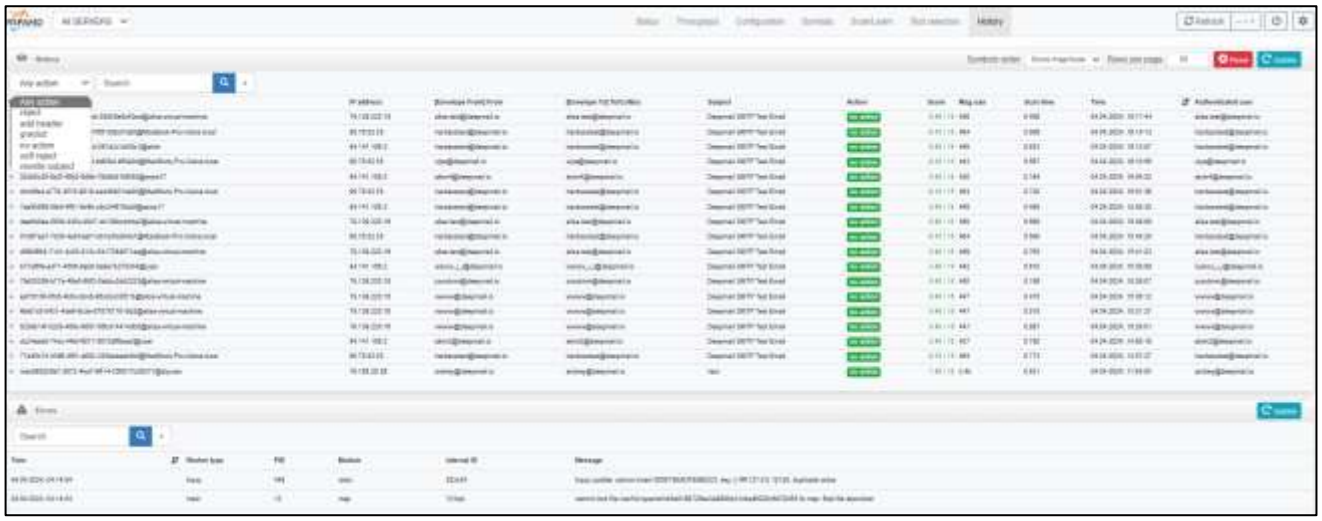


Рисунок 102 – Окно системы RSPAMD, вкладка «History»

3.13 Инструмент «Расширенные настройки»

Инструмент администрирования «Расширенные настройки» содержит два инструмента: «Настройки SSL/TSL» и «Настройки конфигурации» (рисунок 103).

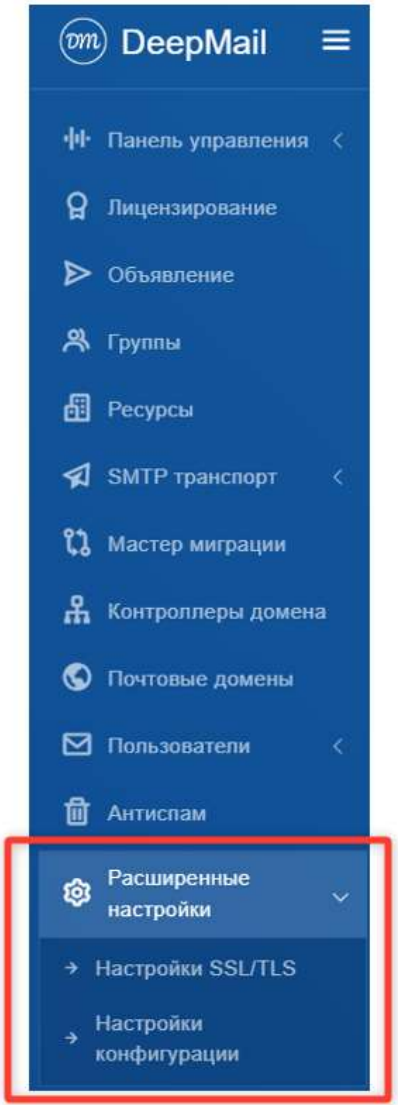


Рисунок 103 – «Расширенный настройки»

3.13.1 «Настройки SSL/TLS»

Для перехода к настройкам SSL/TLS необходимо в меню «Расширенные настройки» интерфейса администратора выбрать «Настройки SSL/TLS» (рисунок 104).

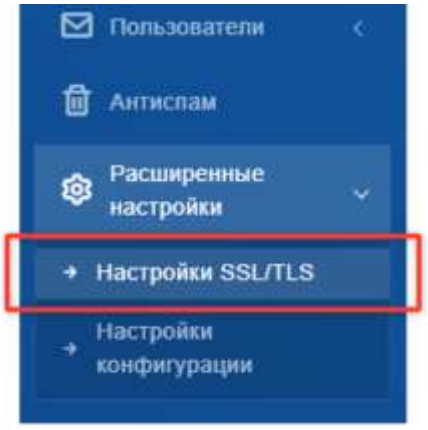


Рисунок 104 – «Настройки SSL/TLS»

На экране отобразится окно «Настройки SSL/TLS» (рисунок 105).

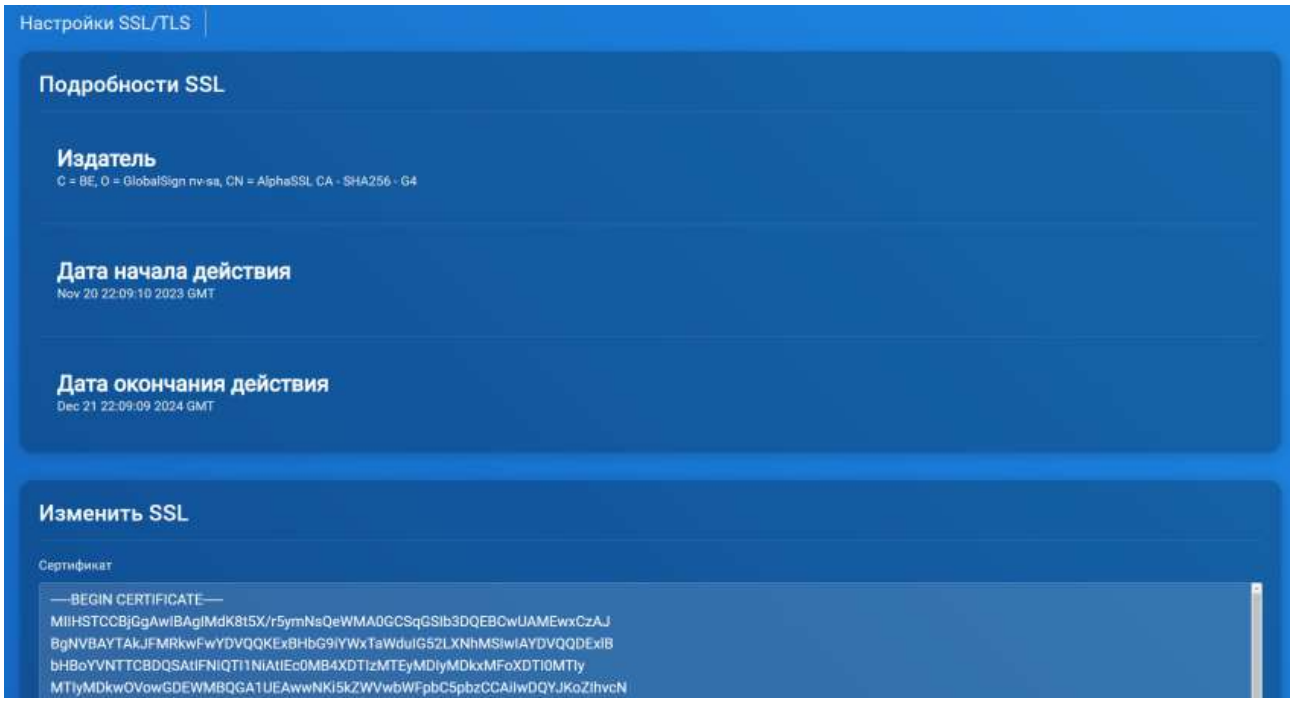


Рисунок 105 – Окно инструмента «Настройки SSL/TLS»

Для того, чтобы установить или сменить сертификаты, необходимо иметь:

- доменный сертификат (выдается на имя сервера или почтового домена, например mail.example.com. Это основной SSL-сертификат);

- промежуточные сертификаты (CA Bundle, Intermediate CA, связывают ваш сертификат с корневым сертификатом Центра сертификации. Почтовые клиенты должны доверять всей цепочке до корневого сертификата, иначе будет ошибка доверия);

- корневой сертификат (как правило, устанавливается только в хранилища доверенных корней на клиентских устройствах, но иногда для совместимости добавляют в цепочку);

- приватный ключ, необходимо использовать только тот приватный ключ, который сгенерировали при создании CSR (запроса на сертификат). Ключ не должен быть зашифрован паролем (почтовый сервер не запросит пароль автоматически). Приватный ключ должен оставаться строго на сервере, не передавать его никому, не показывать публично.

Убедитесь, что имеете все необходимые сертификаты. Если у вас имеются несколько пар сертификатов и ключей, необходимо их объединить в один файл в порядке: сертификат → цепочка → корень; ключ отдельно.

Каждый сертификат должен заканчиваться на строке:

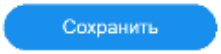
-----END CERTIFICATE-----

, а ключ:

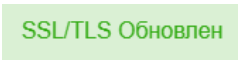
-----END PRIVATE KEY-----

Важно! Проверьте, чтобы между блоками не было «слипшихся» строк: при необходимости разделите их одной пустой строкой или новой строкой (5 дефисов в начале и конце блоков).

В открывшемся окне «Настройки SSL/TLS» (см. рисунок 105) требуется заполнить (заменить в случае смены) два поля – «Сертификат» и «Ключ».

В поле «Сертификат» необходимо вставить всю цепочку сертификатов. Затем в поле «Ключ» вставить ваш приватный ключ, после чего нажать на кнопку 

.

При успешном добавлении сертификата появится оповещение 

.

Важно! Перед заменой сертификатов убедитесь, что у вас сохранены старые сертификаты, если нет – сделайте их копию. Копии понадобятся в том случае, если вы неправильно добавите новые сертификаты.

Далее необходимо заменить сертификаты на HAProxy. Необходимо подключиться к хосту, где установлена HAProxy и перейти в папку с сертификатами, которая указана в конфигурационном файле */etc/haproxy/haproxy.cfg* (обычно */deepmail/ssl/*).

В директории должны находиться два файла – *cert.pem* (файл с цепочкой сертификатов) и *cert.pem.key* (файл с ключом).

Важно! Перед обновлением необходимо сделать копии данных файлов, на случай быстрого возврата к старым сертификатам.

Откройте файл *cert.pem* для редактирования, удалите его содержимое и вставьте туда новую цепочку сертификатов. Сохраните изменения и закройте файл.

Откройте файл *cert.pem.key* для редактирования, удалите его содержимое и вставьте туда новый ключ. Сохраните изменения и закройте файл.

Выполните команду:

systemctl restart haproxy.service

Затем убедитесь, что сервис находится в статусе *active*, выполнив команду:

systemctl status haproxy.service

На этом добавление/ обновление сертификатов будет завершено. Проверить, что сертификаты обновились можно, зайдя в веб-интерфейс и нажав на элемент в виде замка в начале строки адреса (элемент может отличаться и зависит от вашего браузера) (рисунок 106).

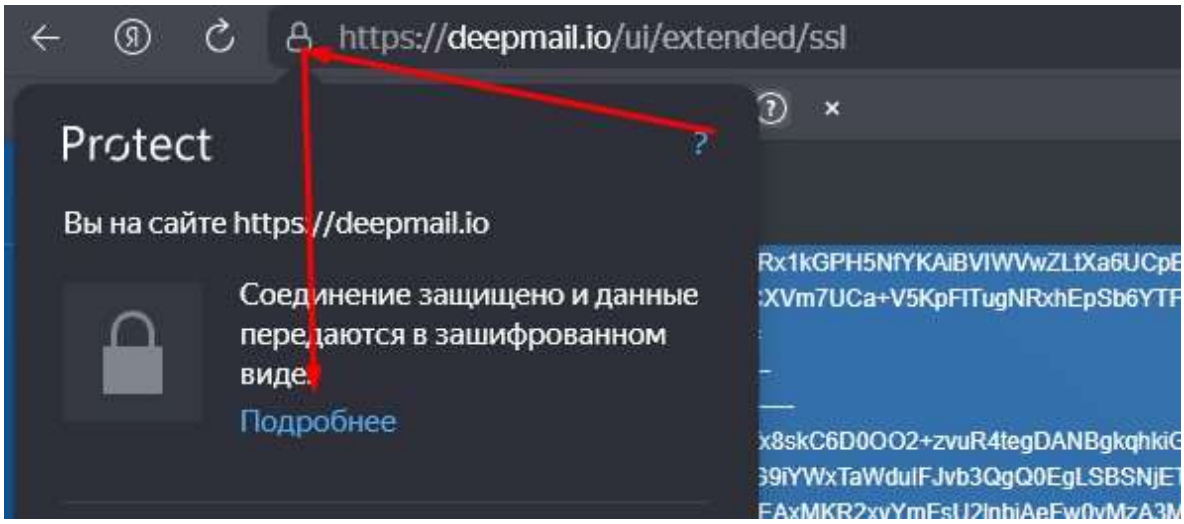


Рисунок 106 – Проверка обновления сертификатов

3.13.2 «Настройка конфигурации»

Для перехода к настройкам конфигурации необходимо в меню «Расширенные настройки» интерфейса администратора выбрать инструмент «Настройки конфигурации» (рисунок 107).

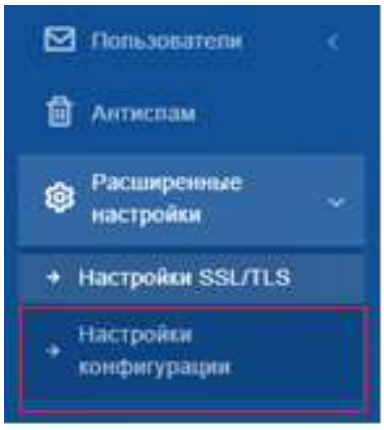


Рисунок 107 – Инструмент «Настройки конфигурации»

После этого на экране отобразится окно «Настройка конфигурации| Настройка почты». Для перехода к настройкам уведомления об окончании квот необходимо в данном окне нажать кнопку «Уведомление Об Окончании Квоты» (рисунок 108).

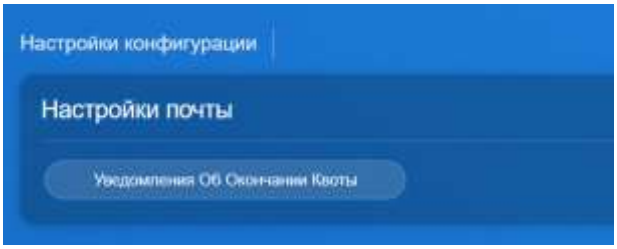


Рисунок 108 – Окно «Настройка конфигурации| Настройка почты», кнопка «Уведомление Об Окончании Квоты»

В появившейся форме «Настройка конфигурации| Уведомления об окончании квоты» укажите необходимые параметры и нажмите кнопку Сохранить.

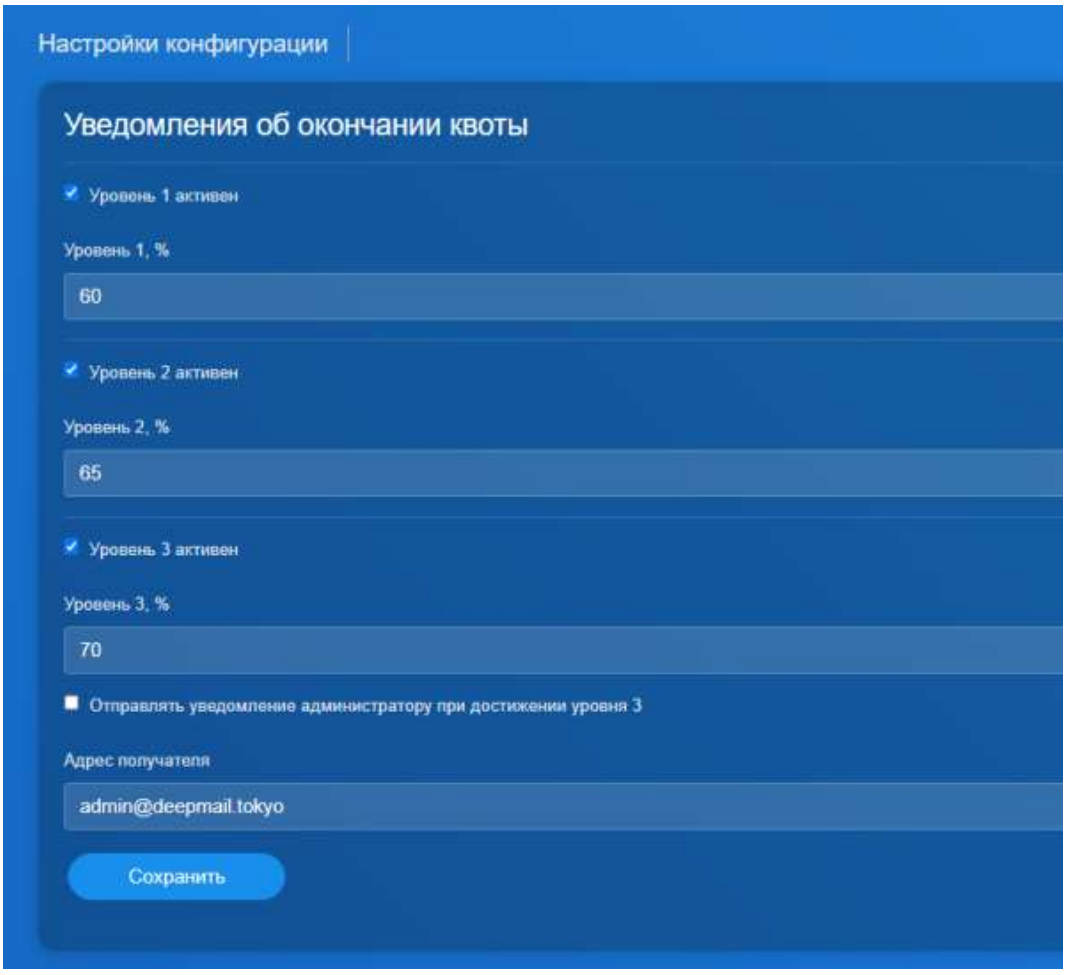


Рисунок 109 – Настройка параметров уведомлений об окончании квоты

3.14 Раздел «Моя учетная запись»

В данном разделе размещены обычные инструменты веб-клиента DeepMail, которые доступны как администратору, так и обычным пользователям для выполнения в веб-клиенте персональных настроек своего почтового аккаунта (рисунок 110).

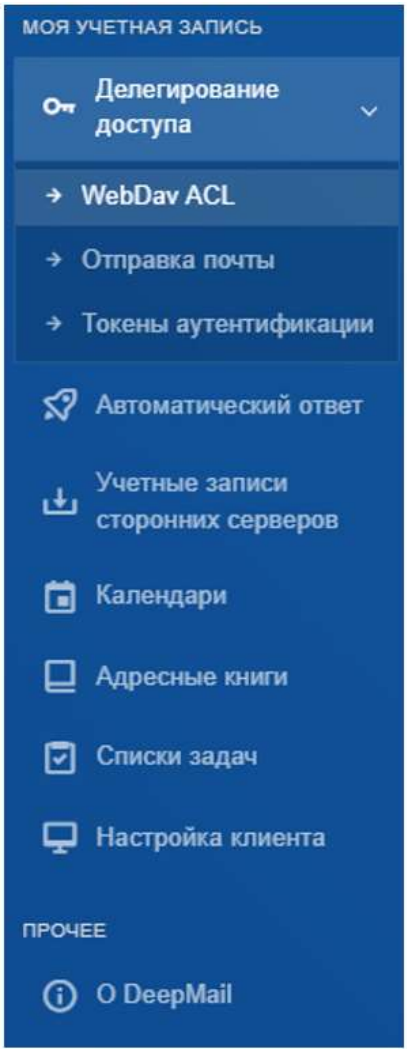


Рисунок 110 – Раздел «Моя учетная запись»

3.14.1 Инструмент «Делегирование доступа»

Инструмент «Делегирование доступа» содержит инструменты «WebDav ACL», «Отправка почты» и «Токены аутентификации» (рисунок 111).

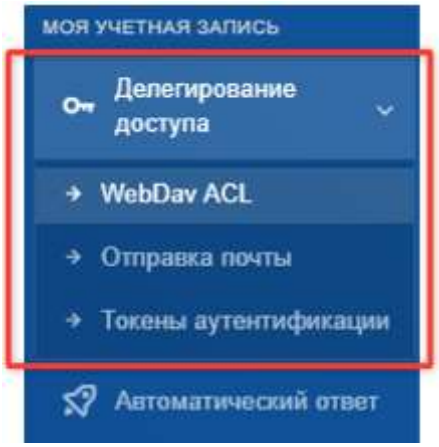


Рисунок 111 – Инструмент «Делегирование доступа»

3.14.1.1 «WebDav ACL»

Для перехода к настройке делегирования доступа к собственным календарям, адресным книгам и папкам задач необходимо в разделе «Моя учетная запись» выбрать «Делегирование доступа» → «WebDav ACL» (см. рисунок 111).

На экране отобразится окно «Пользователи| WebDav ACL» со списком делегатов, если права уже назначались (рисунок 112).

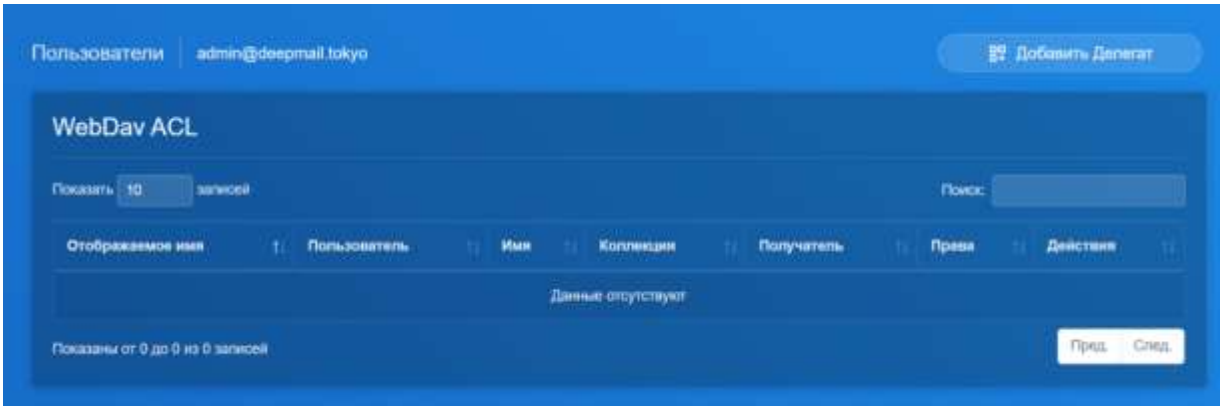


Рисунок 112 – Окно параметров «WebDav ACL»

Дальнейшие действия аналогичны действиям администратора при работе с инструментом администрирования «Пользователи| WebDav ACL» (см. 3.11.1).

3.14.1.2 «Отправка почты»

Для делегирования прав на отправку почтовых сообщений пользователя «от вашего имени» и/ или «с полной подменой отправителя» необходимо в разделе «Моя учетная запись» выбрать «Делегирование доступа» → «Отправка почты» (см. рисунок 111).

В появившемся окне «Отправка почты» в соответствующем поле (или в обоих полях) укажите адрес электронной почты пользователя, которому делегируются права, и нажмите кнопку Сохранить (рисунок 113).

Рисунок 113 – Окно «Отправка почты»

3.14.1.3 «Токены аутентификации»

Делегирование прав доступа на полное управление данными учетной записи одного пользователя другому осуществляется посредством выдачи токенов (ключей доступа).

Для создания такого ключа необходимо в разделе «Моя учетная запись» выбрать «Делегирование доступа» → «Токены аутентификации» (см. рисунок 111).

На экране отобразится окно «Токены аутентификации» со списком предоставленных ключей, если они уже назначались (рисунок 114).

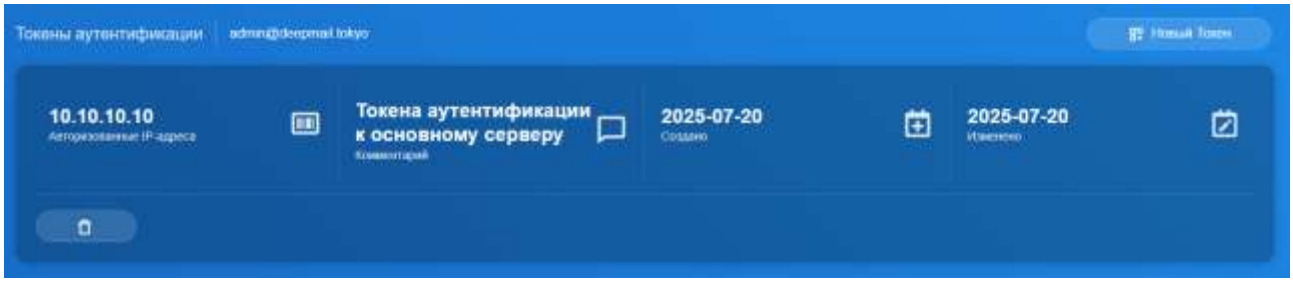


Рисунок 114 – Окно «Токены аутентификации»

Чтобы создать токен необходимо нажать кнопу «Новый Токен», расположенную в правом верхнем углу окна «Токены аутентификации» (см. рисунок 114). Созданный токен передается пользователю, который авторизуясь в Клиент или веб-клиент с данным токеном в качестве пароля и адресом электронной почты пользователя-владельца учетной записи, получает полный доступ к данным этой учетной записи.

При удалении токена доступ к подключенным учетным записям блокируется.

3.14.2 Инструмент «Автоматический ответ»

Инструмент «Автоматический ответ» позволяет создавать, включать и выключать автоответчик.

Для создания автоответчика необходимо в разделе «Моя учетная запись» выбрать инструмент «Автоматический ответ» (рисунок 115).

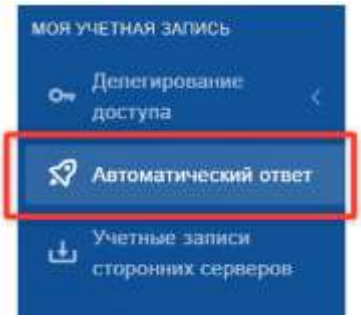


Рисунок 115 – «Автоматический ответ»

В появившемся окне «Автоматический ответ» указать следующие параметры:

- заголовок автоответа;
- сообщение автоответа;
- начало отпуска;
- конец отпуска (рисунок 116).

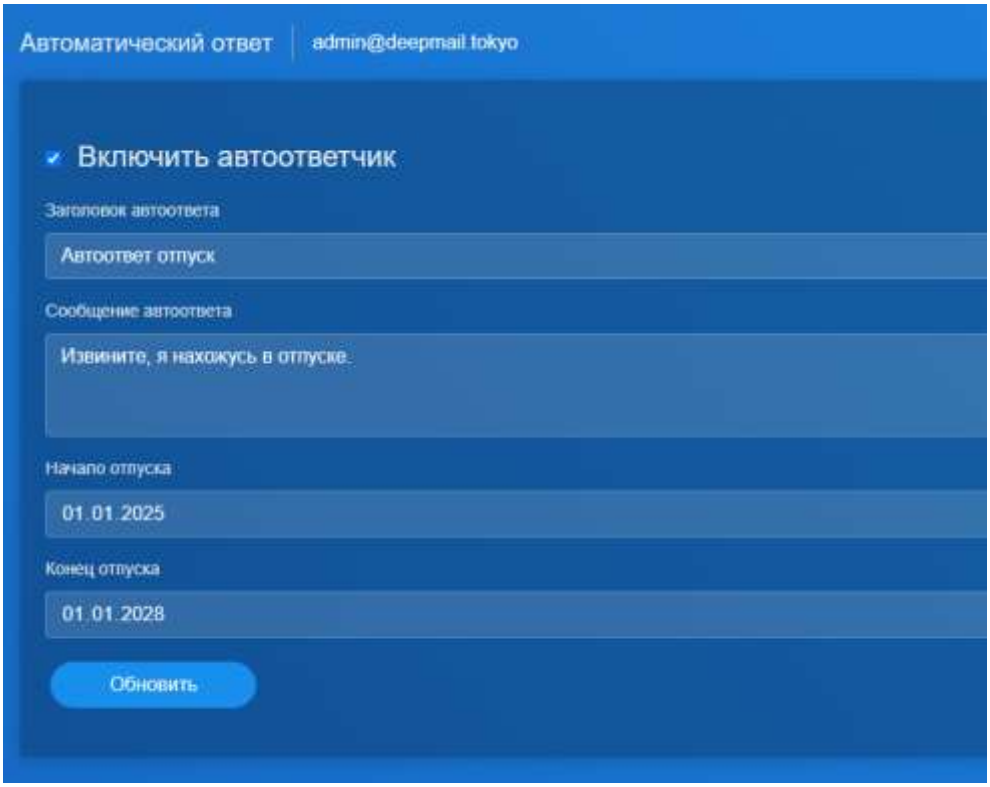


Рисунок 116 – Окно инструмента «Автоматический ответ»

Примечание: автоответ приходит один раз в день на одного пользователя.

3.14.3 Инструмент «Учетные записи сторонних серверов»

Для управления учетными записями сторонних серверов необходимо перейти к инструменту «Учетные записи сторонних серверов», выбрав его в разделе «Моя учетная запись» (см. рисунок 110).

Чтобы добавить детали подключения к стороннему серверу необходимо нажать кнопку «Добавить Учетную Запись» и в появившейся форме указать следующие данные:

- «Протокол» – протокол передачи электронных сообщений (по умолчанию IMAP);
- «Имя хоста или IP» – имя или IP-адрес почтового сервера, с которого будет забираться почта;
- «Порт TCP»;
- «Включить TLS» – протокол, обеспечивающий безопасную передачу данных;

– «Имя пользователя»;

– «Пароль»;

– при необходимости выбрать включение «Хранить письма локально»;

– при необходимости выбрать включение «Сканировать письма локально»;

– папка для получения на сервер (по умолчанию «Входящие») (рисунок 117).

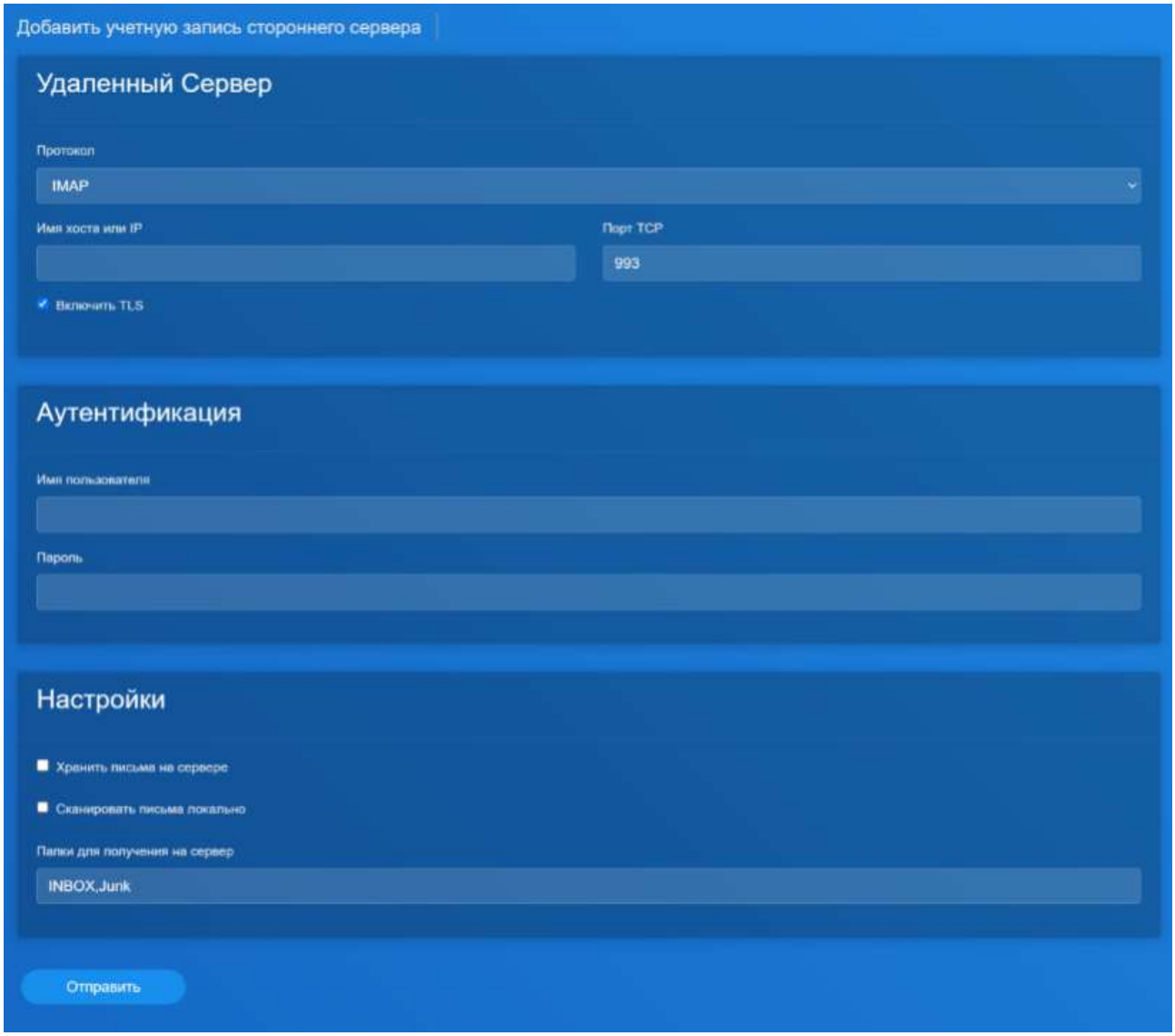


Рисунок 117 – Окно добавления параметров стороннего сервера

Для завершения нажмите кнопку 

.

3.14.4 Инструмент «Календари»

Для управления параметрами календарей пользователя необходимо перейти к инструменту «Календари», выбрав его в разделе «Моя учетная запись» (см. рисунок 110).

В окне «Календари» отображены все календари учетной записи, в том числе и календарь ресурса, если пользователь является его менеджером (см. 3.6).

Инструмент «Календари» позволяет создавать и удалять существующие календари пользователя через веб-интерфейс Клиента (рисунок 118).

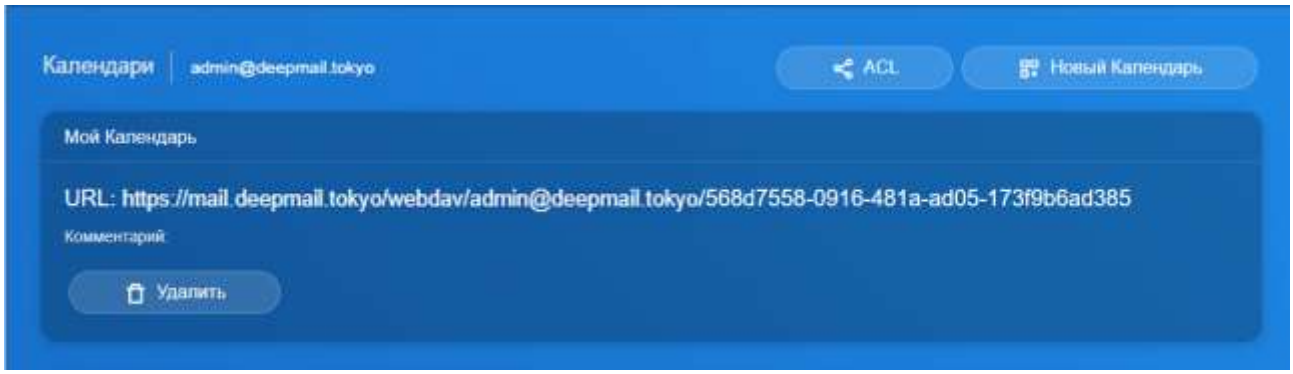


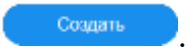
Рисунок 118 – Окно инструмента «Календари»

Для создания календаря необходимо в окне инструмента «Календари» нажать кнопку 

(см. рисунок 118).

Откроется форма «Создать календарь», в которой необходимо ввести имя календаря и, если нужно, добавить комментарий (рисунок 119).

Рисунок 119 – Окно «Создать календарь»

Для завершения создания календаря нажмите на кнопку 

.

При нажатии в окне инструмента «Календари» на кнопку 

(см. рисунок 118) будет выполнен переход к окну «Пользователи| WebDav ACL» для делегирования прав доступа (см. 3.14.1.1).

3.14.5 Инструмент «Адресные книги»

Для управления данными адресных книг пользователя необходимо перейти к инструменту «Адресные книги», выбрав его в разделе «Моя учетная запись» (см. рисунок 110).

Инструмент «Адресные книги» позволяет создавать и удалять существующие адресные книги пользователя через веб-интерфейс Клиента.

В окне инструмента «Адресные книги» отображены все книги контактов учетной записи (рисунок 120).

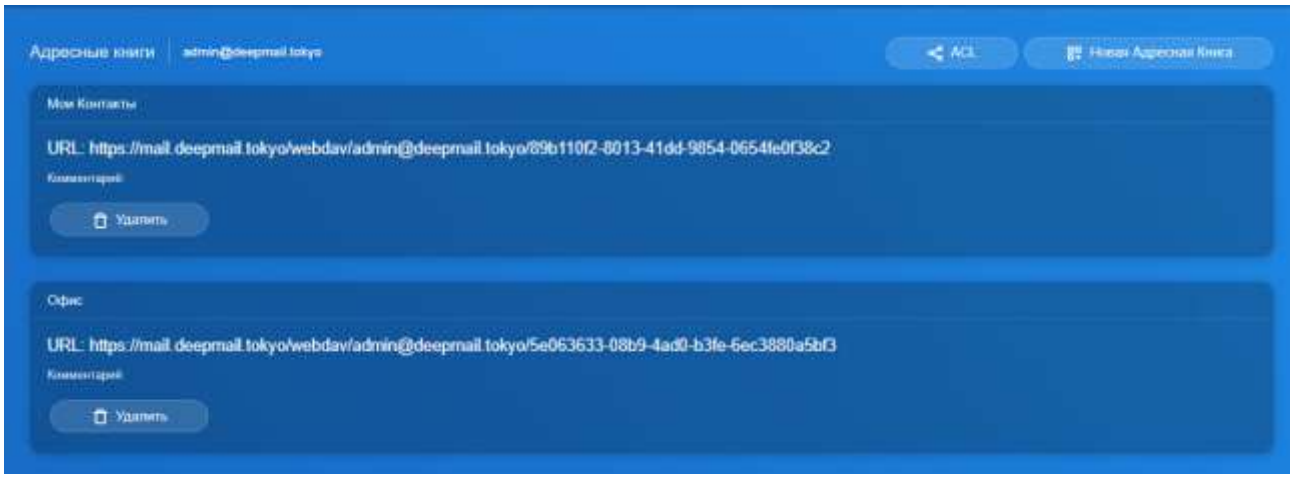


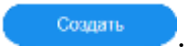
Рисунок 120 – Окно инструмента «Адресные книги»

Для создания адресной книги необходимо в окне инструмента «Адресные книги» нажать кнопку 

(см. рисунок 120).

Откроется форма «Создать адресную книгу», в которой необходимо ввести имя адресной книги и, если нужно, добавить комментарий (рисунок 121).

Рисунок 121 – Окно «Создать адресную книгу»

Для завершения создания адресной книги нажмите на кнопку 

.

Чтобы удалить адресную книгу необходимо в окне инструмента «Адресные книги» нажать кнопку 

, размещенную на панели выбранной адресной книги (см. рисунок 120).

При нажатии в окне инструмента «Адресные книги» на кнопку 

(см. рисунок 120) будет выполнен переход к окну «Пользователи| WebDav ACL» для делегирования прав доступа (см. 3.14.1.1).

3.14.6 Инструмент «Списки задач»

Для управления задачами пользователя необходимо перейти к инструменту «Списки задач», выбрав его в разделе «Моя учетная запись» (см. рисунок 110).

Инструмент «Списки задач» позволяет создавать и удалять папки задач пользователя через веб-интерфейс Клиента.

В окне инструмента «Списки задач» отображены все существующие папки задач учетной записи (рисунок 122).

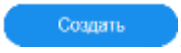
Рисунок 122 – Инструмент «Списки задач»

Чтобы создать папку задач необходимо в окне инструмента «Списки задач» нажать кнопку 

(см. рисунок 122).

Откроется форма «Создать список задач» в которой необходимо ввести имя папки задач и, при необходимости, оставить комментарий (рисунок 123).

Рисунок 123 – Форма «Создать список задач»

Для завершения создания папки задач нажмите на кнопку 

.

Чтобы удалить папку задач необходимо в окне инструмента «Адресные книги» нажать кнопку Удалить, размещенную на панели выбранной папки (см. рисунок 122).

При нажатии в окне инструмента «Списки задач» на кнопку ACL (см. см. рисунок 122) будет выполнен переход к окну «Пользователи| WebDav ACL» для делегирования прав доступа (см. 3.14.1.1).

3.14.7 Инструмент «Настройка клиента»

Для выполнения настроек синхронизации десктопного (установленного непосредственного на ПК) Клиента с Сервером пользователю может понадобиться некоторая информация. Необходимые данные содержатся в инструменте «Настройка клиента». Чтобы перейти в инструмент «Настройка клиента», выберете его в разделе «Моя учетная запись» (см. рисунок 110). После этого на экране отобразится окно «Настройка клиента| Настройте свой почтовый клиент» (рисунок 124).

Рисунок 124 – Инструмент «Настройка клиента»

ПЕРЕЧЕНЬ ТЕРМИНОВ

Определения терминов, применяемых в настоящем документе, приведены в таблице 5.

Таблица 5 – 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

Термин	Определение
Иконка	Графическое изображение элемента пользовательского интерфейса (меню, кнопки, значка, списка и т.д.)
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)

Термин	Определение
Сообщения	Сообщения, передаваемые по электронной почте на базе ПО DeepMail
Спам	Массовая рассылка корреспонденции рекламного характера (нежелательных сообщений) лицам, не выразившим желания ее получить
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

ПЕРЕЧЕНЬ ПРИНЯТЫХ СОКРАЩЕНИЙ

БД – база данных;

АРМ – автоматизированное рабочее место;

ЛВС – локальная вычислительная сеть;

ОЗУ – оперативное запоминающее устройство, или оперативная память;

ОС – операционная система;

ПК – персональный компьютер;

ПО – программное обеспечение;

ПЭВМ – персональная электронная вычислительная машина;

СТП – служба технической поддержки;

УЗ – учетная запись;

ЦП – центральный процессор.