АО «Иридиум»

РУКОВОДСТВО АДМИНИСТРАТОРА

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

RU.УГСФ.00003-01 90 01

Листов 198

2026

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 РЕД ОС.

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;
- поддержка почтовых доменов в режиме мультитенантности;
- возможность работы под управлением российских сертифицированных ОС, таких как: Astra Linux Special Edition 1.6, и выше релизы «Орел», «Воронеж», «Смоленск»; «Альт Рабочая станция» версии 9, 10; «Альт СП Рабочая станция»; AltLinux 10.* и выше, Debian 11 и выше; Ubuntu 22.04 и выше; РЕД ОС версии 7.3 и выше, ROSA Linux;
- функционирование программного обеспечения почтового сервиса на АРМ, работающих под управлением операционных систем следующих версий: Windows 10 Home / Pro (32 / 64-разрядная), Windows 11 Home / Pro (32 / 64-разрядная), Linux/Unix
- поддержка доступа через стандартные IMAP/SMTP-клиенты: Outlook – 2021, 2019, 2016, 2013, 2010 и 2007, а также Office 365 для ПК. Для обеспечения корректной работы необходимо использовать официальную надстройку (плагин) к MS Outlook для обеспечения двусторонней синхронизации с DeepMail сервером календарей, задач и контактов по протоколам CalDAV / CardDAV;
- возможность работы на российских системах виртуализации (ПК «Звезда», ПК «Иридиум»);
- защита от спама и вирусов с помощью интеграции с сертифицированными средствами;
- возможность миграции почтовых баз и учетных записей пользователей с любого почтового сервера, в том числе с Microsoft Exchange Server;

- протоколирование событий, в том числе с возможностью экспорта по протоколу syslog;
- поддержка общих почтовых ящиков (shared mailboxes);
- поддержка общих иерархических папок (shared folders / public folders) для групп пользователей;
- поддержка общих календарей;
- поддержка синхронизации контактов и адресных книг по протоколу CardDAV (RFC 6352), включая глобальные адресные книги;
- квотирование размера почтовых ящиков на уровне пользователя, группы и домена без перезапуска сервиса;
- поддержка настраиваемых серверных правил обработки почты (server-side rules);
- 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;
- возможность интеграции с KSMG;
- возможность интеграции с DLP-системой Solar Dozor для контроля почтового трафика;
- возможность интеграции с решением Check Point SandBlast для анализа подозрительных вложений;
- поддержка SMTP (RFC 5321), IMAP4 (RFC 3501) с расширениями IDLE и SORT, SMTPS/STARTTLS, IMAPS с использованием TLS 1.2 и выше;
- поддержка механизмов SPF (RFC 7208), DKIM (RFC 6376), DMARC (RFC 7489);
- возможность интеграции с Microsoft Active Directory по протоколу LDAP;
- автоматизация обработки стандартизованных запросов в электронной почте и встроенном мессенджере;
- обеспечение целевого значения RTO (Recovery Time Objective) при отказе одного ЦОД – не более 5 минут. Целевое значение RPO (Recovery Point Objective) – 0 (отсутствие потери данных).

1.1 Условия, необходимые для функционирования изделия

1.1.1 Требования к техническим средствам

Минимальная конфигурация инфраструктуры для установки серверной части должна состоять из двух ВМ. На одной ВМ размещаются сервисы Core, WebDAV, auth – почтовая нода; на второй – база данных PostgreSQL, NFS и HAProxy (установка обязательна).

Требования к ресурсам в том числе зависят от нагрузки на почтовую систему – количества пользователей, которые будут ее использовать.

Требования к техническим параметрам оборудования необходимым для размещения серверной части на ВМ (для расчетного количества пользователей в 1000 человек) представлены в таблице 1.

Таблица 1 – Требования к техническим средствам (для 1000 пользователей)

Параметр	Минимальные требования на 2 ВМ	Рекомендуемые требования на 2 ВМ
Количество ядер процессора	4+4	8+8
Объем ОЗУ, ГБ	8+8	16+16
Объем HDD, ГБ	100+100 + квота пользователя ×1000	

Для каждой последующей 1000-1500 человек необходимо добавление еще одной ВМ почтовой ноды с соответствующим увеличением ресурсов технических средств.

1.1.2 Требования к программным средствам

Сервер функционирует в ОС следующих вариантов: Astra Linux Special Edition 1.7 версии «Орел», «Воронеж», «Смоленск»; «Альт Рабочая станция» версии 9, 10; «Альт СП Рабочая станция»; Debian не ниже версии 12; Ubuntu; РЕД ОС версии 8 и выше, ROSA Linux.

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.

2 УСТАНОВКА И НАСТРОЙКА СЕРВЕРА

2.1 Общие сведения об архитектуре

Сервер DeepMail разработан по принципу разделения ответственности между управляющим сервером и почтовыми нодами. Такой подход позволяет гибко масштабировать систему: при росте нагрузки можно добавлять дополнительные почтовые ноды, сохраняя единое хранилище и общую базу данных.

В зависимости от требований к отказоустойчивости и доступности, система может быть развёрнута в двух типовых конфигурациях:

- минимальная конфигурация (2 ВМ) – подходит для небольших организаций или тестовых сред. Состоит из одной управляющей машины (DM1ha) и одной почтовой ноды (DM2node). При выходе из строя почтовой ноды сервис становится недоступным до её восстановления;
- конфигурация с отказоустойчивостью (3 ВМ) – включает управляющий сервер (DM1ha) и две почтовые ноды (DM2node и DM3node). HAProxy балансирует нагрузку между нодами, а выход одной из них не приводит к остановке обслуживания пользователей.

2.1.1 Роли и сервисы управляющего сервера (DM1ha)

На виртуальную машину управляющего сервера возлагаются все «центральные» функции, которые не требуют высокой вычислительной мощности в момент обработки почты, но критически важны для целостности данных:

- Ansible – используется однократно при установке и обновлении системы. Позволяет автоматизировать настройку всех серверов по заданному сценарию;
- NFS (Network File System) – центральное сетевое хранилище. Вся почта, календари, адресные книги и конфигурации физически лежат на DM1ha, а почтовые ноды подключаются к этим каталогам через сеть. Это обеспечивает единое состояние данных для всех нод;
- PostgreSQL – основная реляционная база данных. Здесь хранятся метаданные: пользователи, домены, профили, правила фильтрации, настройки и т.д.;
- Redis – кластер из трёх экземпляров, работающих на одной ВМ (для простоты). Используется для кэширования сессий, организации очередей сообщений и быстрого обмена данными между сервисами.
- HAProxy – балансировщик нагрузки. Он распределяет входящие почтовые (SMTP, IMAP) и веб-запросы (HTTP/HTTPS) между почтовыми нодами. В конфигурации с двумя нодами обеспечивает отказоустойчивость, а в минимальной – просто проксирует трафик на одну ноду.

2.1.2 Почтовая нода (DM2node, DM3node)

Каждая почтовая нода запускает контейнерный набор сервисов, которые непосредственно взаимодействуют с пользователями:

- Auth – проверяет учётные данные при подключении по SMTP, IMAP, WebDAV;
- WebDAV – предоставляет доступ к календарям, адресным книгам и задачам по протоколам CalDAV/CardDAV;
- Core – центральный координатор внутренних процессов;
- Front – обрабатывает веб-запросы к пользовательскому интерфейсу (почта, файловый менеджер);
- Admin – веб-интерфейс для администратора;
- Webmail – непосредственно веб-клиент для работы с почтой;
- IMAP – сервер входящей почты;
- SMTP – сервер исходящей почты;
- SFTP (опционально) – доступ к файловому хранилищу;
- антиспам / антивирус (опционально) – фильтрация сообщений с помощью Rspamd и ClamAV;
- Migration (опционально) – сервис миграции из Exchange или других систем;
- LDAP (опционально) – синхронизация пользователей со службой каталогов.

Все эти сервисы запущены в контейнерах Docker, что обеспечивает изоляцию и простоту обновления.

2.2 Подготовка к установке

2.2.1 Требования к операционной системе

В данном руководстве дальнейшая установка приведена для ОС Astra Linux.

Важное замечание по безопасности: уровень защищенности операционной системы должен быть переведён в «Базовый» перед началом установки. На «Усиленном» или «Максимальном» уровне мандатный контроль может блокировать работу Docker и NFS. После завершения установки DeepMail уровень можно вернуть к исходному.

2.2.2 Предварительные шаги

Перед запуском установки убедитесь в выполнении следующих условий:

- все серверы (DM1ha, DM2node, DM3node) установлены, имеют статические IP-адреса и сетевое взаимодействие между собой;
- на каждом сервере настроены правильные DNS-имена (или доступ по IP). Рекомендуется прописать имена в */etc/hosts*;
- с управляющего сервера DM1ha организован SSH-доступ на каждую почтовую ноду по паролю. Ansible будет использовать этот доступ для настройки. При необходимости можно настроить ключи, но в документации предполагается доступ по паролю;
- дистрибутив *deepmail-server-<версия>.tar.gz* скачан и размещён на DM1ha, например, в домашнем каталоге.

2.2.3 Подготовка управляющего сервера DM1ha

На DM1ha нужно установить два пакета, которые будут использоваться только на этапе установки:

sudo apt update

sudo apt install -y ansible sshpass

ansible – система автоматизации, которая выполнит все плейбуки.

sshpass – утилита, позволяющая *ansible* передавать пароль по *SSH* без интерактивного ввода (на основе данных из *inventory.yml*).

2.2.4 Подготовка почтовых нод

На каждой почтовой ноде (DM2node и, при трёхсерверной конфигурации, DM3node) нужно подготовить систему для установки пакетов из репозиториев Astra Linux.

Откройте файл /*etc/apt/sources.list* и выполните команду:

sudo nano /etc/apt/sources.list

Раскомментируйте строки, содержащие *repository-extended* и *repository-main* (удалите символ # в начале). Остальные строки (*devel, cdrom*) можно оставить закомментированными.

Сохраните изменения и выполните обновление списка пакетов, а также установите NFS-клиент:

sudo apt update

sudo apt install -y nfs-common

NFS-клиент необходим, чтобы почтовая нода могла монтировать удалённые хранилища (*core, mail, dav, archive*), которые находятся на управляющем сервере.

2.3 Настройка управляющего сервера (DM1ha)

2.3.1 Распаковка дистрибутива

На DM1ha распакуйте архив и перейдите в каталог с плейбуками:

tar -xvf deepmail-server-<версия>.tar.gz

cd deepmail-server-4.0/*

2.3.2 Редактирование файла инвентаризации (inventory)

Файл *inventory-example.yml* содержит описание всех серверов в инфраструктуре. Скопируйте его и отредактируйте:

cp inventory-example.yml inventory.yml

sudo nano inventory.yml

Этот файл – сердце конфигурации. В нём нужно указать:

- пароли для базы данных (*psql_pass*) и Redis (*redis_password*). Не используйте специальные символы (например, !@#$), чтобы избежать проблем с обработкой в *ansible*;
- IP-адреса всех хостов. Для каждого хоста (*storage, redis, haproxy, postgresql, core, auth, webdav*) нужно задать параметры подключения: *ansible_user, ansible_ssh_pass* (пароль *root*) и *ansible_become_pass* (пароль для повышения привилегий).

Особенности для разных конфигураций:

- для двух ВМ (DM1ha + DM2node) все секции, кроме *core, auth, webdav*, должны ссылаться на IP-адрес DM1ha. В секциях *core, auth, webdav* укажите один IP – адрес DM2node;
- для трёх ВМ (DM1ha + DM2node + DM3node) в секциях *core, auth, webdav* перечислите оба IP-адреса почтовых нод. Это позволит ansible развернуть сервисы на обоих узлах и настроить HAProxy для балансировки между ними.

Остальные строки файла менять не требуется, если вы не используете отказоустойчивый кластер БД или HAProxy с keepalived (эти функции выходят за рамки базовой установки).

Пример конфигурационного inventory – файла с выделением изменяемых параметров ниже для 2х ВМ (файл необходимо отредактировать в части параметров, выделенных черным жирным шрифтом):

all:

vars:

ОСНОВНАЯ КОНФИГУРАЦИЯ

install_packages: true # нужно ли предустанавливать пакеты

***psql_pass:** 'указываете ваш пароль' # пароль для пользователя БД (ВАЖНО: без спецсимволов)*

***redis_password:** "указываете ваш пароль" # пароль для redis*

ДОПОЛНИТЕЛЬНАЯ КОНФИГУРАЦИЯ (ДЛЯ ОПЫТНЫХ ПОЛЬЗОВАТЕЛЕЙ DEEPMAIL)

ansible_ssh_common_args: '-o StrictHostKeyChecking=no' # для ssh

 # keepalived

haproxy_address: "0.0.0.0" # адрес для keepalived

keepalived_use: false # будет ли использоваться отказоустойчивый haproxy (для haproxy будет необходимо 2 хоста)

 # postgresql

pgcluster_use: false # будет ли использоваться отказоустойчивый кластер БД (postgresql+etcd+patroni_haproxy_keepalived) (минимум 3 хоста)

pgcluster_virtual_ip: 0.0.0.0 # виртуальный ip, при использовании кластера БД

 # redis

redis_pool_size: 10000 # Максимальное количество соединений

redis_idle_conns: 10 # Минимальное количество неактивных соединений

redis_dial_timeout: 3 # Таймаут установки соединения

redis_read_timeout: 3 # Таймаут чтения

redis_write_timeout: 3 # Таймаут записи

 # 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

archive_storage_path: "/mnt/deepmail/archive" # путь до папки mail на хосте core

smtp_storage_path: "/var/deepmail/smtp" # путь до папки smtp на хосте core

 # 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 mail (почта) хранилища на хосте NFS

 # пути к конфигурационным файлам сервисов (рекомендуется не менять)

auth_conf_path: "/etc/deepmail/auth-service"

webdav_conf_path: "/etc/deepmail/webdav-service"

imap_conf_path: "/etc/deepmail/imap-service"

smtp_conf_path: "/etc/deepmail/smtp-service"

 # подсети, которые будут использовать сервисы для своей работы

auth_subnet: "192.168.201.0/24"

webdav_subnet: "192.168.202.0/24"

core_subnet: "192.168.203.0/24"

noinet_subnet: "192.168.204.0/24"

ХОСТЫ

storage_core: # Указывается IP-адрес управляющего сервера
hosts:
***x.x.x.x**:*
*ansible_user: **root***
*ansible_ssh_pass: **'ваш пароль от учетной записи root'***
*ansible_become_pass: **'ваш пароль от учетной записи root'***
storage_mail: # Указывается IP-адрес управляющего сервера
hosts:
***x.x.x.x**:*
*ansible_user: **root***
*ansible_ssh_pass: **'ваш пароль от учетной записи root'***
*ansible_become_pass: **'ваш пароль от учетной записи root'***
storage_dav: # Указывается IP-адрес управляющего сервера
hosts:
***x.x.x.x**:*
*ansible_user: **root***
*ansible_ssh_pass: **'ваш пароль от учетной записи root'***
*ansible_become_pass: **'ваш пароль от учетной записи root'***
storage_archive: # Указывается IP-адрес управляющего сервера
hosts:
***x.x.x.x**:*
*ansible_user: **root***
*ansible_ssh_pass: **'ваш пароль от учетной записи root'***
*ansible_become_pass: **'ваш пароль от учетной записи root'***
 # три хоста кластера redis (Можно ставить на 1 ВМ).
 # указывается IP, пользователь для подключения по ssh, его пароль и пароль для повышения привилегий
redis-1: # Указывается IP-адрес управляющего сервера
hosts:
***x.x.x.x**:*
*ansible_user: **root***
*ansible_ssh_pass: **'ваш пароль от учетной записи root'***
*ansible_become_pass: **'ваш пароль от учетной записи root'***

redis-2: # Указывается IP-адрес управляющего сервера
hosts:
***x.x.x.x**:*
*ansible_user: **root***
*ansible_ssh_pass: **'ваш пароль от учетной записи root'***
*ansible_become_pass: **'ваш пароль от учетной записи root'***

redis-3: # Указывается IP-адрес управляющего сервера
hosts:
***x.x.x.x**:*
*ansible_user: **root***
*ansible_ssh_pass: **'ваш пароль от учетной записи root'***
*ansible_become_pass: **'ваш пароль от учетной записи root'***
 # хост сервера haproxy. в закомментированном конфигурация при использовании 2 хостов (для отказоустойчивости с помощью keepalived)

 # указывается IP, пользователь для подключения по ssh, его пароль и пароль для повышения привилегий

haproxy: # Указывается IP-адрес управляющего сервера

hosts:

***x.x.x.x**:*

*ansible_user: **root***

*ansible_ssh_pass: **'ваш пароль от учетной записи root'***

*ansible_become_pass: **'ваш пароль от учетной записи root'***

keepalived_master: false # если keepalived не используем, оставляем false. при использовании keepalived, на основную ноду haproxy ставим true, на остальных false.

keepalived_interface: enp3s0 # если keepalived не используем, ничего не менять. при использовании keepalived, указываем название сетевого интерфейса, который использует хост.

 # 0.0.0.0:

 # ansible_user: root

 # ansible_ssh_pass: 'your_password'

 # ansible_become_pass: 'your_password'

 # keepalived_master: false

 # keepalived_interface: enp3s0

 # хост сервера postgresql

 # указывается IP, пользователь для подключения по ssh, его пароль и пароль для повышения привилегий.

 # в закомментированном виде конфигурация при использовании отказоустойчивого кластера БД. (etcd+postgresql+patroni_haproxy+keepalived) (минимум 3 хоста для кластера)

postgresql: # Указывается IP-адрес управляющего сервера

hosts:

***x.x.x.x**:*

*ansible_user: **root***

*ansible_ssh_pass: **'ваш пароль от учетной записи root'***

*ansible_become_pass: **'ваш пароль от учетной записи root'***

etcd_nodename: datanode1 # не менять

pg_interface: enp3s0 # если кластер БД не используем, ничего не менять. при использовании кластера БД, указываем название сетевого интерфейса, который использует хост.

 # 10.20.201.47:

 # ansible_user: root

 # ansible_ssh_pass: 'your_password'

 # ansible_become_pass: 'your_password'

 # etcd_nodename: datanode2 # не менять

 # pg_interface: enp3s0

 # 10.20.201.47:

 # ansible_user: root

 # ansible_ssh_pass: 'your_password'

 # ansible_become_pass: 'your_password'

 # etcd_nodename: datanode3 # не менять

 # pg_interface: enp3s0

 # хосты для сервисов core, auth, webdav. в закомментированом виде пример при нескольких хостах

```
# указывается IP
core: #Указывается IP-адрес почтовой ноды
  hosts:
    x.x.x.x:
#     0.0.0.0:
auth: #Указывается IP-адрес почтовой ноды
  hosts:
    x.x.x.x:
#     0.0.0.0:
webdav: #Указывается IP-адрес почтовой ноды
  hosts:
    x.x.x.x:
#     0.0.0.0:
```

Пример конфигурационного inventory – файла с выделением изменяемых параметров ниже для 3х ВМ (файл необходимо отредактировать в части параметров, выделенных черным жирным шрифтом):

```
all:
  vars:
### ОСНОВНАЯ КОНФИГУРАЦИЯ ###
      install_packages: true # нужно ли предустанавливать пакеты
      psql_pass: 'указываете ваш пароль' # пароль для пользователя БД (ВАЖНО: без спецсимволов)
      redis_password: "указываете ваш пароль" # пароль для redis
    ### ДОПОЛНИТЕЛЬНАЯ КОНФИГУРАЦИЯ (ДЛЯ ОПЫТНЫХ ПОЛЬЗОВАТЕЛЕЙ DEEPMAIL) ###
      ansible_ssh_common_args: '-o StrictHostKeyChecking=no' # для ssh
      # keepalived
      haproxy_address: "0.0.0.0" # адрес для keepalived
      keepalived_use: false # будет ли использоваться отказоустойчивый haproxy (для haproxy будет необходимо 2 хоста)
      # postgresql
      pgcluster_use: false # будет ли использоваться отказоустойчивый кластер БД (postgresql+etcd+patroni_haproxy_keepalived) (минимум 3 хоста)
      pgcluster_virtual_ip: 0.0.0.0 # виртуальный ip, при использовании кластера БД
      # redis
      redis_pool_size: 10000 # Максимальное количество соединений
      redis_idle_conns: 10 # Минимальное количество неактивных соединений
      redis_dial_timeout: 3 # Таймаут установки соединения
      redis_read_timeout: 3 # Таймаут чтения
      redis_write_timeout: 3 # Таймаут записи
      # 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
      archive_storage_path: "/mnt/deepmail/archive" # путь до папки mail на хосте core
```

smtp_storage_path: "/var/deepmail/smtp" # путь до папки smtp на хосте core
 # 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 mail (почта) хранилища на хосте NFS
 # пути к конфигурационным файлам сервисов (рекомендуется не менять)
auth_conf_path: "/etc/deepmail/auth-service"
webdav_conf_path: "/etc/deepmail/webdav-service"
imap_conf_path: "/etc/deepmail/imap-service"
smtp_conf_path: "/etc/deepmail/smtp-service"
 # подсети, которые будут использовать сервисы для своей работы
auth_subnet: "192.168.201.0/24"
webdav_subnet: "192.168.202.0/24"
core_subnet: "192.168.203.0/24"
noinet_subnet: "192.168.204.0/24"
ХОСТЫ
storage_core: # Указывается IP-адрес управляющего сервера
hosts:
***x.x.x.x**:*
*ansible_user: **root***
*ansible_ssh_pass: **'ваш пароль от учетной записи root'***
*ansible_become_pass: **'ваш пароль от учетной записи root'***
storage_mail: # Указывается IP-адрес управляющего сервера
hosts:
***x.x.x.x**:*
*ansible_user: **root***
*ansible_ssh_pass: **'ваш пароль от учетной записи root'***
*ansible_become_pass: **'ваш пароль от учетной записи root'***
storage_dav: # Указывается IP-адрес управляющего сервера
hosts:
***x.x.x.x**:*
*ansible_user: **root***
*ansible_ssh_pass: **'ваш пароль от учетной записи root'***
*ansible_become_pass: **'ваш пароль от учетной записи root'***
storage_archive: # Указывается IP-адрес управляющего сервера
hosts:
***x.x.x.x**:*
*ansible_user: **root***
*ansible_ssh_pass: **'ваш пароль от учетной записи root'***
*ansible_become_pass: **'ваш пароль от учетной записи root'***
 # три хоста кластера redis (Можно ставить на 1 ВМ).
 # указывается IP, пользователь для подключения по ssh, его пароль и пароль для повышения привилегий
redis-1: # Указывается IP-адрес управляющего сервера

```
    hosts:
      x.x.x.x:
        ansible_user: root
        ansible_ssh_pass: 'ваш пароль от учетной записи root'
        ansible_become_pass: 'ваш пароль от учетной записи root'
  redis-2: # Указывается IP-адрес управляющего сервера
    hosts:
      x.x.x.x:
        ansible_user: root
        ansible_ssh_pass: 'ваш пароль от учетной записи root'
        ansible_become_pass: 'ваш пароль от учетной записи root'
  redis-3: # Указывается IP-адрес управляющего сервера
    hosts:
      x.x.x.x:
        ansible_user: root
        ansible_ssh_pass: 'ваш пароль от учетной записи root'
        ansible_become_pass: 'ваш пароль от учетной записи root'
  # хост сервера haproxy. в закомментированном конфигурация при использовании 2 хостов (для отказоустойчивости с помощью keepalived)
  # указывается IP, пользователь для подключения по ssh, его пароль и пароль для повышения привилегий
  haproxy: # Указывается IP-адрес управляющего сервера
    hosts:
      x.x.x.x:
        ansible_user: root
        ansible_ssh_pass: 'ваш пароль от учетной записи root'
        ansible_become_pass: 'ваш пароль от учетной записи root'
         keepalived_master: false # если keepalived не используем, оставляем false. при использовании keepalived, на основную ноду haproxy ставим true, на остальных false.
         keepalived_interface: enp3s0 # если keepalived не используем, ничего не менять. при использовании keepalived, указываем название сетевого интерфейса, который использует хост.
  #    0.0.0.0:
  #      ansible_user: root
  #      ansible_ssh_pass: 'your_password'
  #      ansible_become_pass: 'your_password'
  #      keepalived_master: false
  #      keepalived_interface: enp3s0
  # хост сервера postgresql
  # указывается IP, пользователь для подключения по ssh, его пароль и пароль для повышения привилегий.
  # в закомментированном виде конфигурация при использовании отказоустойчивого кластера БД. (etcd+postgresql+patroni_haproxy+keepalived) (минимум 3 хоста для кластера)
  postgresql: # Указывается IP-адрес управляющего сервера
    hosts:
      x.x.x.x:
        ansible_user: root
        ansible_ssh_pass: 'ваш пароль от учетной записи root'
```

*ansible_become_pass: **'ваш пароль от учетной записи root'***
etcd_nodename: datanode1 # не менять
pg_interface: enp3s0 # если кластер БД не используем, ничего не менять. при использовании кластера БД, указываем название сетевого интерфейса, который использует хост.
 # 10.20.201.47:
 # ansible_user: root
 # ansible_ssh_pass: 'your_password'
 # ansible_become_pass: 'your_password'
 # etcd_nodename: datanode2 # не менять
 # pg_interface: enp3s0
 # 10.20.201.47:
 # ansible_user: root
 # ansible_ssh_pass: 'your_password'
 # ansible_become_pass: 'your_password'
 # etcd_nodename: datanode3 # не менять
 # pg_interface: enp3s0
 # хосты для сервисов core, auth, webdav. в закомментированом виде пример при нескольких хостах
 # указывается IP
core: #Указывается IP-адрес почтовой ноды
hosts:
x.x.x.x**: **IP-** **почтовой ноды DM2node
x.x.x.x**: **IP-** **почтовой ноды DM3node
auth: #Указывается IP-адрес почтовой ноды
hosts:
x.x.x.x**: **IP-** **почтовой ноды DM2node
x.x.x.x**: **IP-** **почтовой ноды DM3node
webdav: #Указывается IP-адрес почтовой ноды
hosts:
x.x.x.x**: **IP-** **почтовой ноды DM2node
x.x.x.x**: **IP-** **почтовой ноды DM3node
После внесения изменений сохраните файл.

2.3.3 Последовательный запуск плейбуков *ansible*

Выполните четыре команды в строго указанном порядке. Каждая команда настраивает определённую часть инфраструктуры.

ansible-playbook -i inventory.yml playbooks/storage.yaml

storage.yaml – создаёт на DM1ha NFS-экспорты для папок *core, mail, dav, archive*, а также настраивает права доступа. Почтовые ноды получат возможность монтировать эти каталоги.

ansible-playbook -i inventory.yml playbooks/redis.yml

redis.yml – устанавливает Docker (пакет docker.io) на DM1ha, загружает официальный образ Redis и запускает три контейнера redis-1, redis-2, redis-3. Кластер из трёх экземпляров на одном хосте – стандартная конфигурация для отказоустойчивости внутри одного узла.

ansible-playbook -i inventory.yml playbooks/haproxy.yml

haproxy.yml – устанавливает HAProxy на DM1ha и настраивает его для балансировки трафика между почтовыми нодами (в зависимости от того, сколько нод перечислено в core/auth/webdav). HAProxy будет слушать порты 25 (SMTP), 143 (IMAP), 993 (IMAPS), 443 (HTTPS) и другие, и направлять их на соответствующие сервисы.

ansible-playbook -i inventory.yml playbooks/pg.yml

pg.yml – устанавливает PostgreSQL на DM1ha, создаёт базу данных deepmail, пользователя deepmail и задаёт пароль из psql_pass. Также конфигурирует права доступа и выполняет необходимую инициализацию.

Каждый плейбук выводит на экран ход выполнения. Дождитесь сообщения об успешном завершении (PLAY RECAP ... ok=...). В случае ошибки проверьте правильность IP-адресов и паролей в *inventory.yml*.

2.4 Настройка почтовых нод

2.4.1 Установка DEB-пакета

На каждой почтовой ноде (DM2node и DM3node) необходимо установить пакет DeepMail. Скопируйте DEB-файл из распакованного дистрибутива на целевую ноду (например, через scp или winscp) и выполните:

sudo dpkg -i deepmail-server-<версия>.deb

Установка займёт 1–2 минуты. Во время неё выполняются пост-установочные скрипты, которые подготавливают необходимые каталоги и зависимости.

2.4.2 Инициализация DeepMail

Инициализация выполняется только на первой почтовой ноде (DM2node). На DM3node этот шаг не требуется.

sudo deepmail init

После успешного завершения вы увидите сообщение:

DeepMail initializer is ready; visit http://<IP_DM2node>:8080 to continue setup

Это означает, что на порту 8080 запущен временный веб-конфигуратор. Следующие шаги выполняются через браузер.

2.5 Установка и конфигурирование HAProxy

Откройте браузер на любом компьютере, имеющем сетевой доступ к DM2node, и перейдите по адресу *http://<IP_DM2node>:8080*. Вы увидите пошаговый мастер.

Шаг 1. Параметры системы

Поле System IP должно заполниться автоматически (рисунок 1). Укажите имя вашего будущего почтового домена, например, *company.ru*. Это имя будет использоваться для создания адресов электронной почты.

Шаг 2. Подключение к PostgreSQL

Введите IP-адрес управляющего сервера DM1ha (рисунок 1). Порт *5432* и имя пользователя *deepmail* оставьте по умолчанию. В поле пароль введите тот пароль, который вы задали в *psql_pass* в файле инвентаризации.

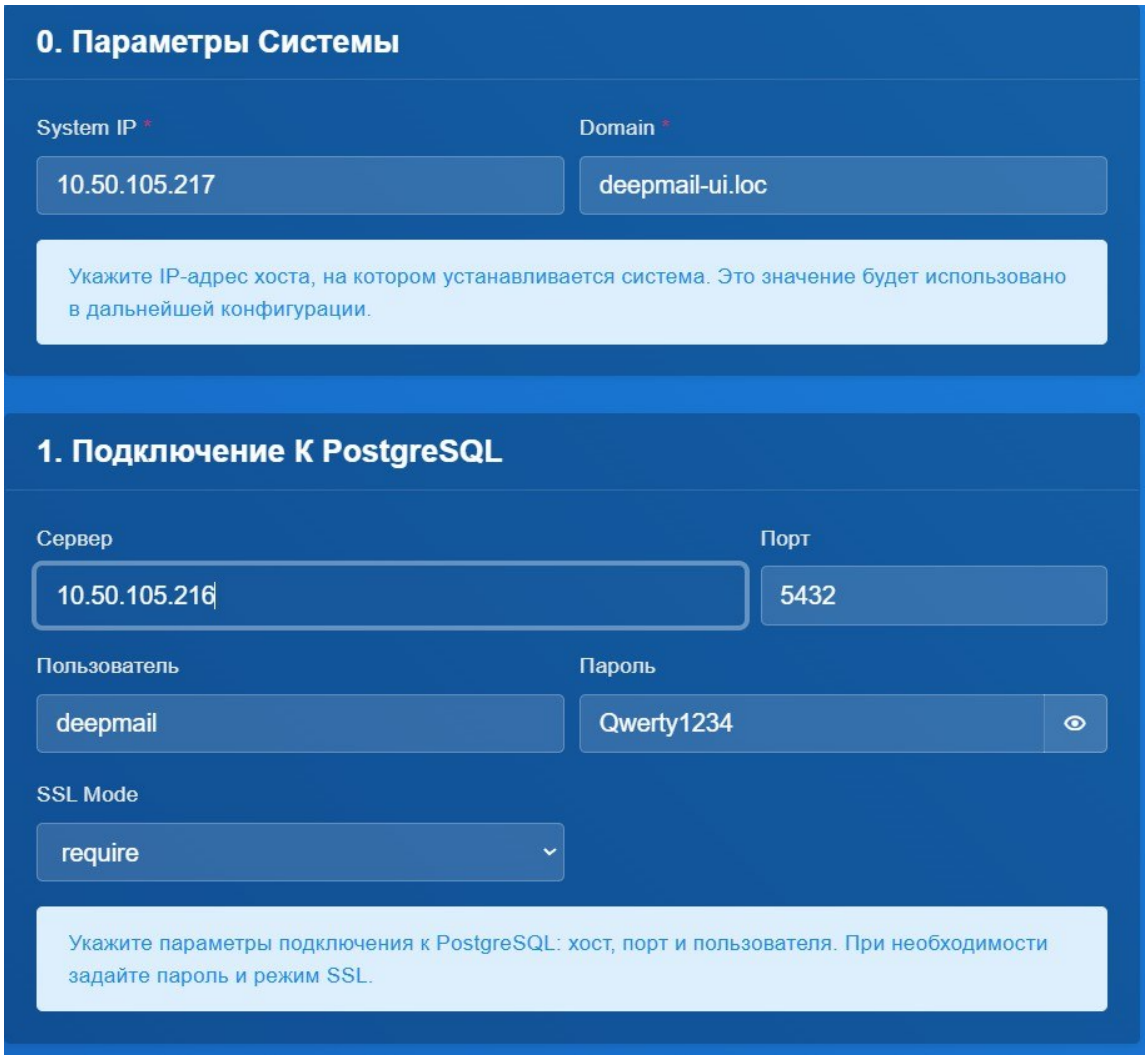


Рисунок 1 – Настройка параметров системы

Шаг 3. Подключение хранилищ

Активируйте чекбокс «Единый host для всех хранилищ» и введите IP-адрес DM1ha (рисунок 2). Система автоматически подставит пути к папкам *core, mail, dav, archive*. Эти каталоги будут примонтированы по NFS и использоваться для хранения всех данных. Данные хранятся в зашифрованном виде.

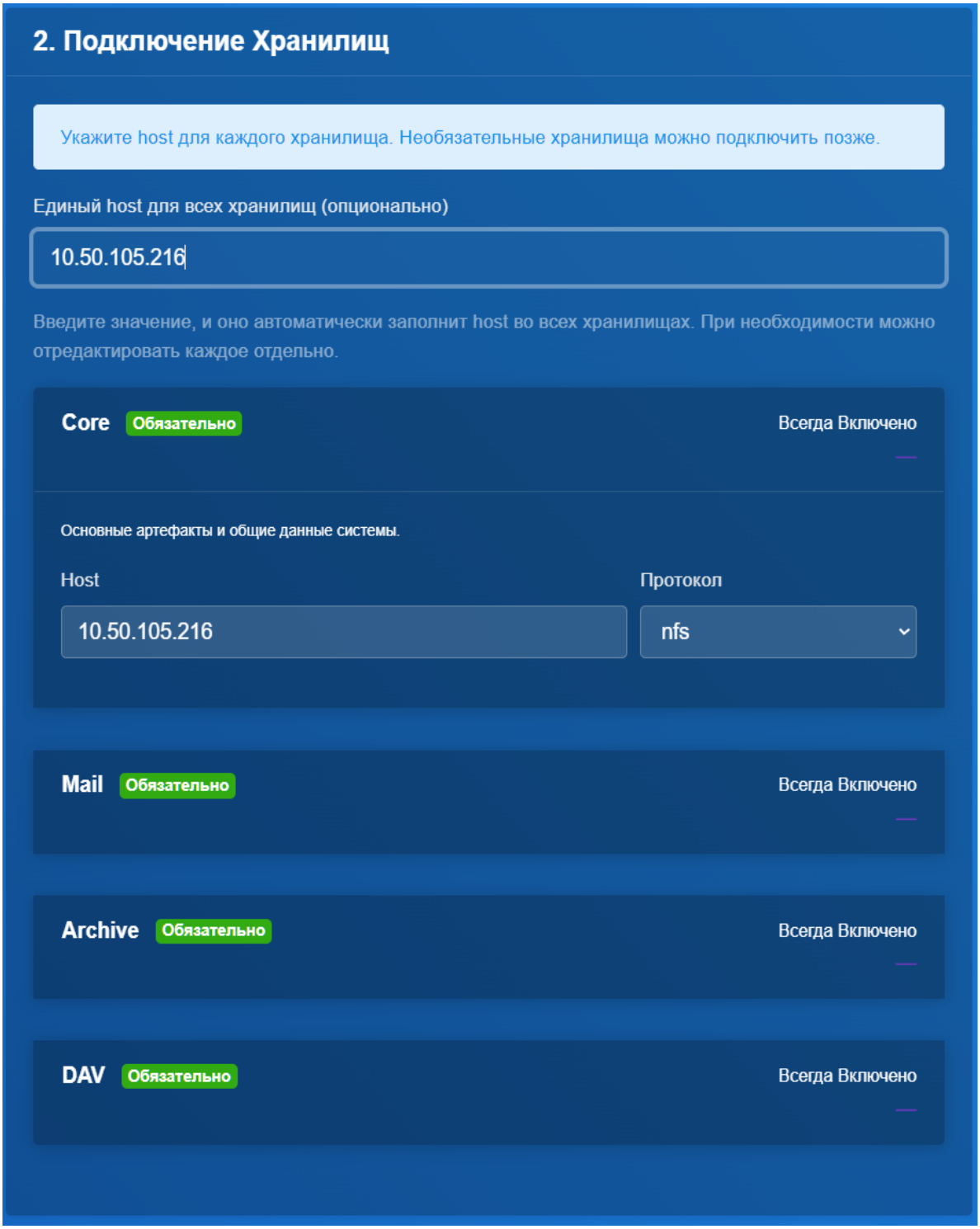


Рисунок 2 – Подключение хранилищ

Шаг 4. Подключение к кластеру Redis

Также укажите единый *host – IP DM1ha* (рисунок 3). В поле пароль введите пароль из *redis_password*. Три контейнера Redis, запущенные на DM1ha, будут доступны по этому адресу.

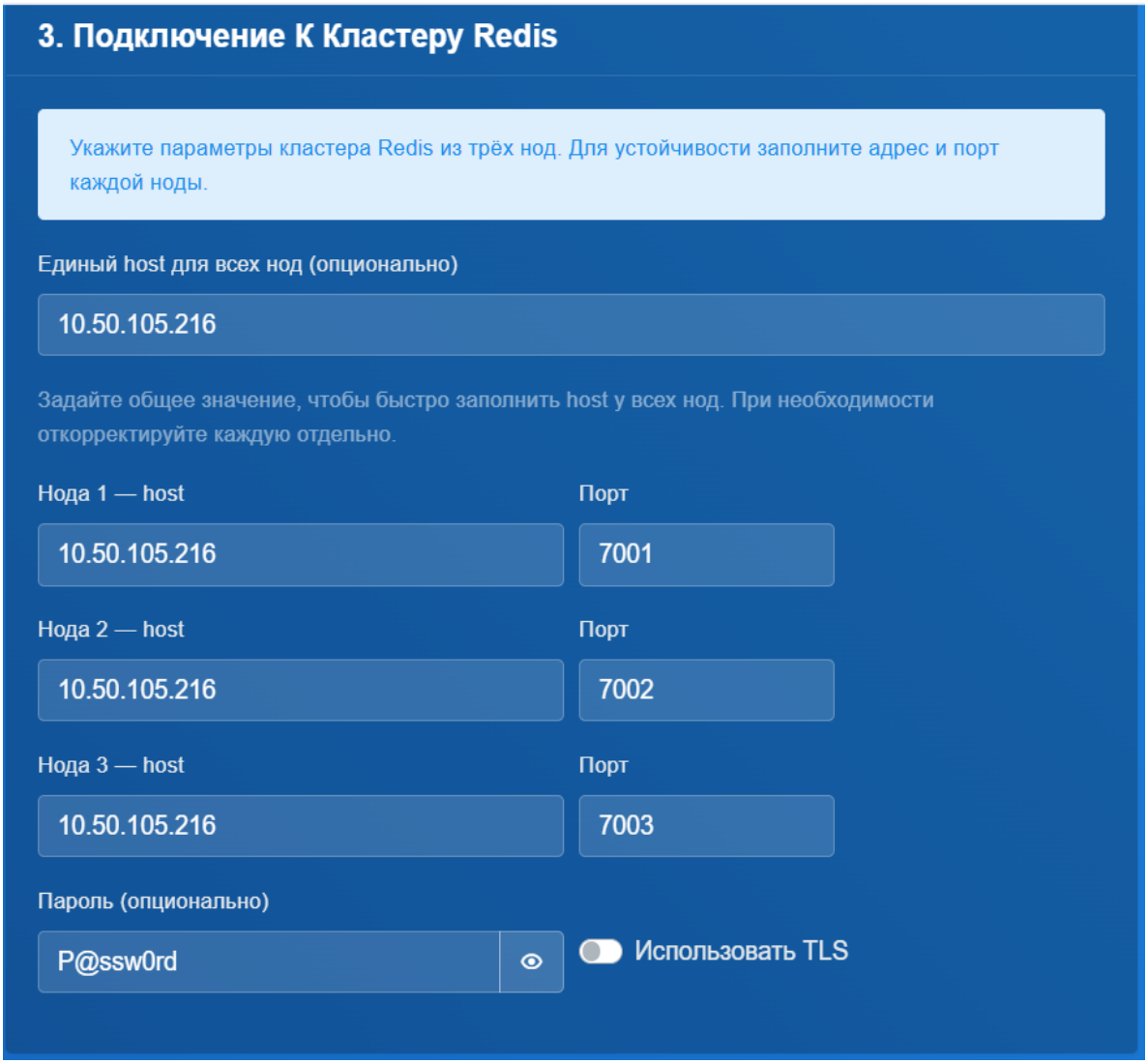


Рисунок 3 – Подключение к кластеру Redis

Шаг 5. Стеки и сервисы

На этой странице перечислены все возможные сервисы DeepMail (рисунок 4). Некоторые флажки уже установлены (*core, webmail, imap, smtp*). Обязательно вручную установите флажки для сервисов Auth и WebDAV – они обеспечивают аутентификацию и работу календарей/контактов.

Дополнительные сервисы включаются по вашему усмотрению:

- Migration – если вы планируете переносить почту с Exchange или IMAP-сервера;
- LDAP – для синхронизации пользователей из Active Directory, FreeIPA, ALD Pro или Samba DC;

- Antivirus и antispam – для фильтрации сообщений (используются ClamAV и Rspamd);

- SFTP – для доступа к файловому хранилищу по протоколу SFTP.

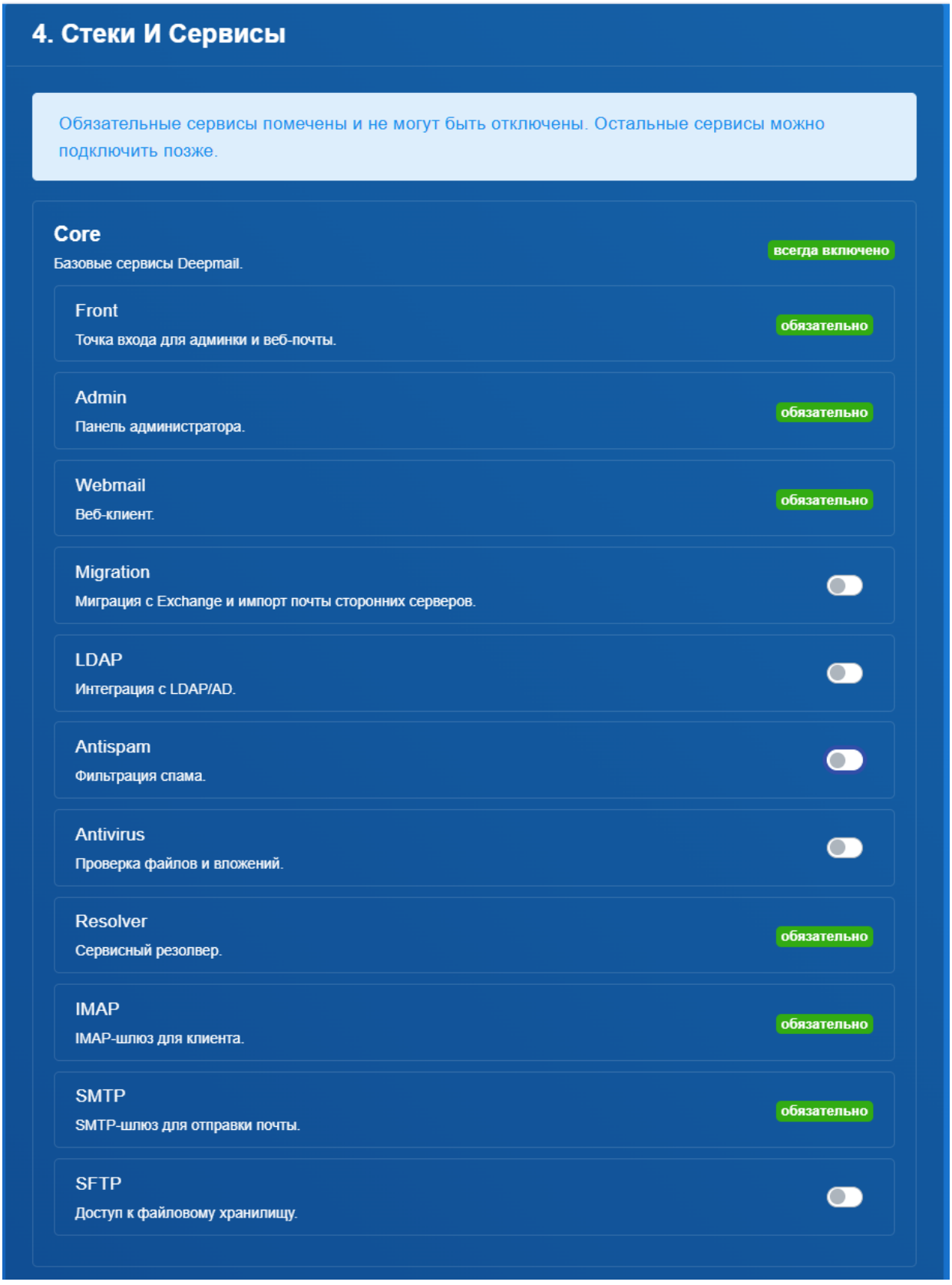


Рисунок 4 – Настройка стеков и сервисов

Шаг 6. Настройка профилей

В поле «Общий hostname» укажите полное доменное имя, которое пользователи будут вводить в настройках почтовых клиентов (например, mail.company.ru).

В поле «Общий real ip» введите IP-адрес управляющего сервера DM1ha (рисунок 5). Этот адрес будет использоваться HAProxy для приёма входящих соединений.

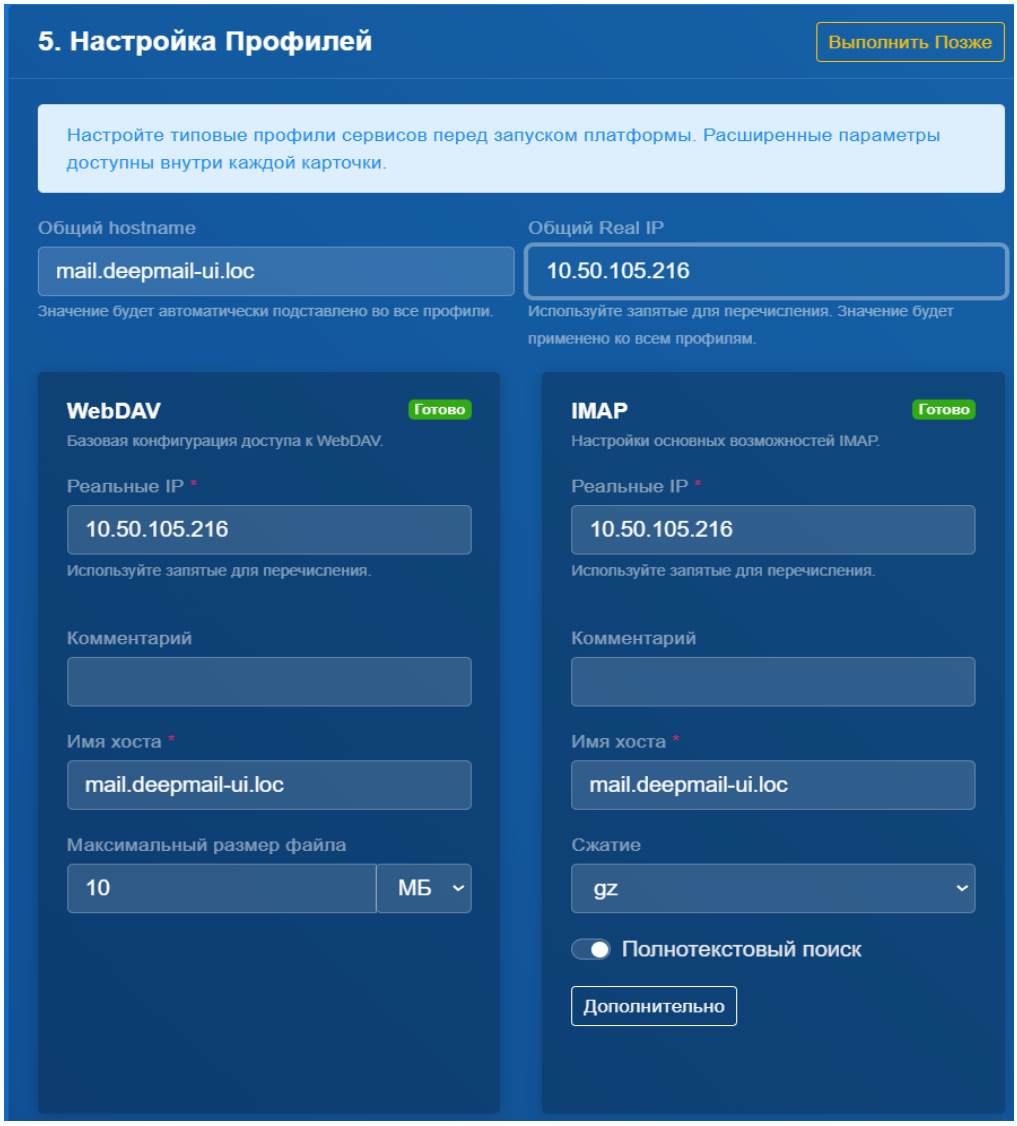


Рисунок 5 – Настройка профилей

Шаг 7. Валидация

Нажмите кнопку «Проверить». Система последовательно протестирует: доступность PostgreSQL, Redis, подключение хранилищ, возможность запуска выбранных сервисов. Дождитесь, когда все пункты перейдут в статус *Success* (зелёные галочки - рисунок 6). Если какой-то шаг завершился ошибкой – вернитесь к предыдущим настройкам и исправьте параметры.

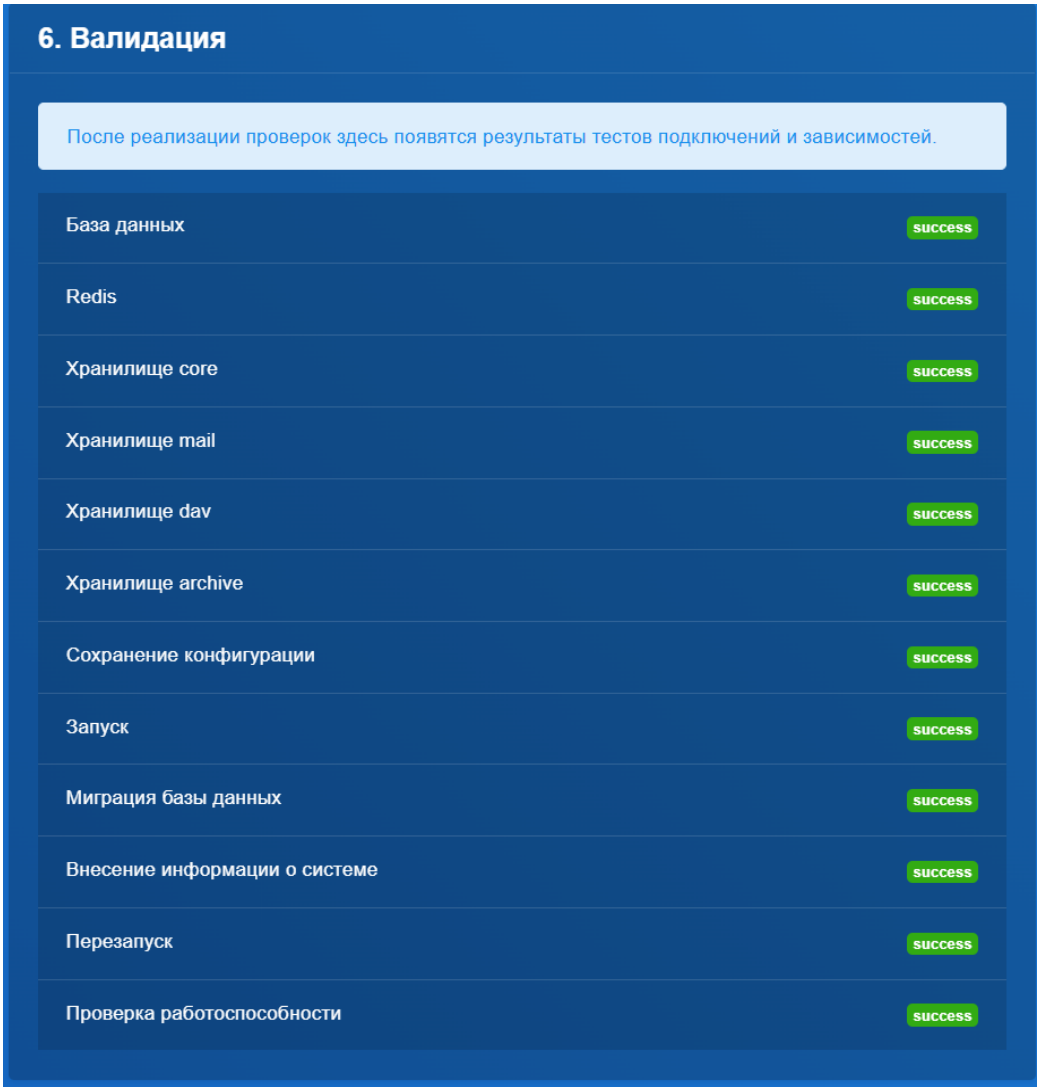


Рисунок 6 – Валидация

Шаг 8. Завершение

Нажмите «Завершить» (рисунок 7). После этого система применит конфигурацию, перезапустит все контейнеры и выведет адрес для входа в панель администратора – обычно *https://<IP_DM1ha>/ui*. Теперь можно переходить к первому входу.

Рисунок 7 – Завершение настройки

2.6 Добавление второй почтовый ноды (только для конфигураций из трех ВМ)

Если вы разворачиваете систему на трёх серверах, после завершения первоначальной установки на DM2node необходимо добавить вторую ноду – DM3node – через веб-интерфейс администратора.

Для входа в панель администратора откройте браузер по адресу *https://<IP_DM1ha>/ui*. Авторизуйтесь с логином *admin@<ваш_домен>* и паролем по умолчанию *PASSWORD* (заглавными буквами). При первом входе система потребует активации лицензии – сообщите номер лицензии в техническую поддержку для получения лицензионного ключа.

В левом меню выберите «Панель управления» → «Система». На открывшейся странице нажмите кнопку «Добавить».

Заполнените параметры новой ноды, в параметрах системы укажите System IP – адрес управляющего сервера DM1ha.

Для подключения хранилищ (для каждого типа CORE, MAIL, DAV, ARCHIVE) выберите соответствующее хранилище, везде указав IP DM1ha.

Активируйте как минимум *core, webmail, imap, smtp, webdav, auth*. Остальные – по необходимости.

Нажмите «Проверить» и дождитесь успешной валидации.

После валидации нажмите «Назад к обзору». Теперь в списке узлов будут отображаться две почтовые ноды: DM2node и DM3node. HAProxy автоматически начнёт распределять нагрузку между ними, а если одна из нод перестанет отвечать – трафик будет перенаправлен на живую.

2.7 Проверка работоспособности

После установки рекомендуется выполнить простые проверки:

- откройте веб-интерфейс администратора, убедитесь, что все сервисы в разделе «Панель управления» → «Система» имеют статус HEALTHY;
- создайте тестовый почтовый домен и пользователя;
- отправьте и получите тестовое письмо между двумя пользователями.

При использовании двух почтовых нод проверьте, что при отключении одной из них (например, выключении ВМ) входящая почта продолжает обрабатываться оставшейся нодой (не более чем через 1-2 минуты после таймаута HAProxy).

2.8 Дальнейшие шаги

Установка завершена. Теперь вы можете приступить к администрированию системы:

- создавать почтовые домены и пользователей;
- подключать контроллеры домена для синхронизации учётных записей;
- настраивать маршрутизацию почты и правила фильтрации;
- организовывать резервное копирование;
- настраивать мониторинг через Zabbix (установка и конфигурирование системы мониторинга см. в **Ошибка! Источник ссылки не найден.**).

Все последующие главы настоящего руководства построены в предположении, что базовая установка уже выполнена и вы имеете доступ к панели администратора.

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 8).

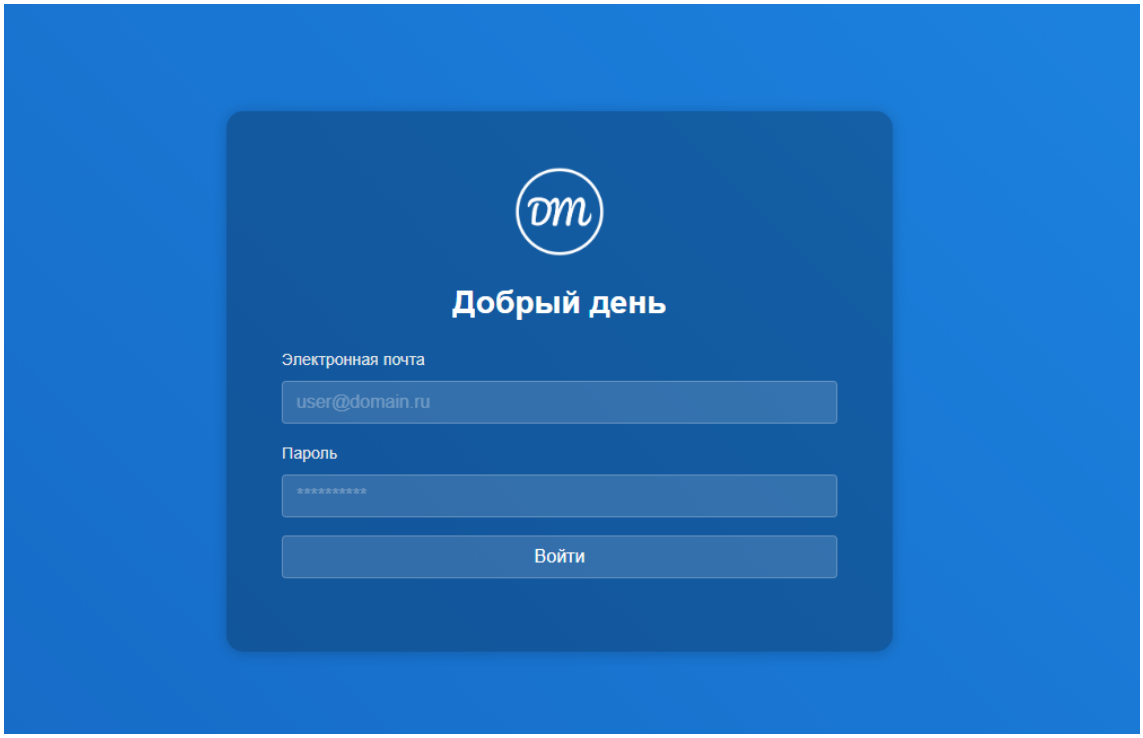


Рисунок 8 – Окно авторизации в веб-интерфейс администратора

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. рисунок 36);

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 9).

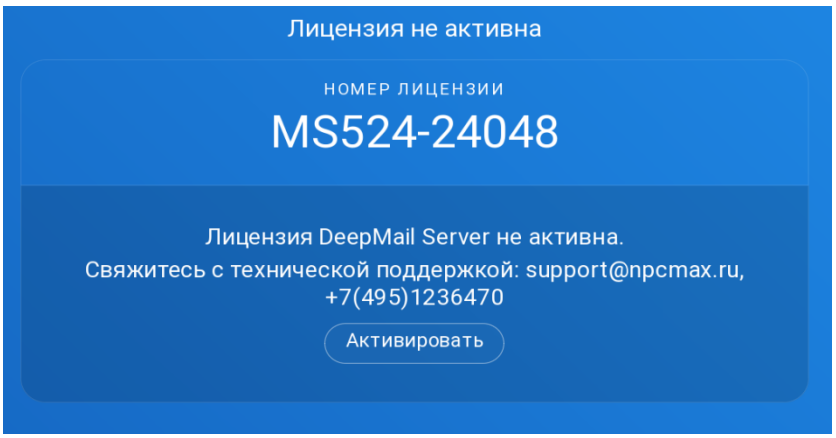


Рисунок 9 – Окно с деталями лицензии

Для активации лицензии необходимо запросить лицензионный ключ активации у разработчика. Лицензионный ключ генерируется по номеру лицензии (см. рисунок 9). Для ввода полученного лицензионного ключа необходимо нажать кнопку Активировать, и ввести лицензионный ключ в соответствующее поле (рисунок 10). Нажать кнопку Активировать.

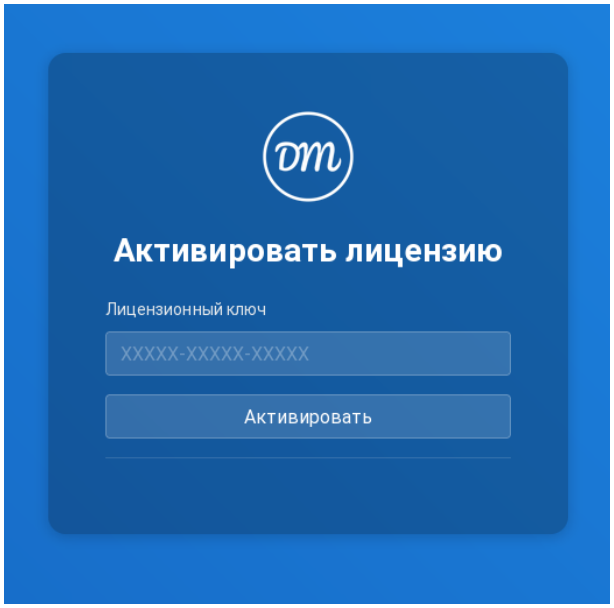


Рисунок 10 – Окно ввода лицензионного ключа

В случае успешной активации в окне авторизации должна появиться надпись «Лицензия активирована» (рисунок 11).

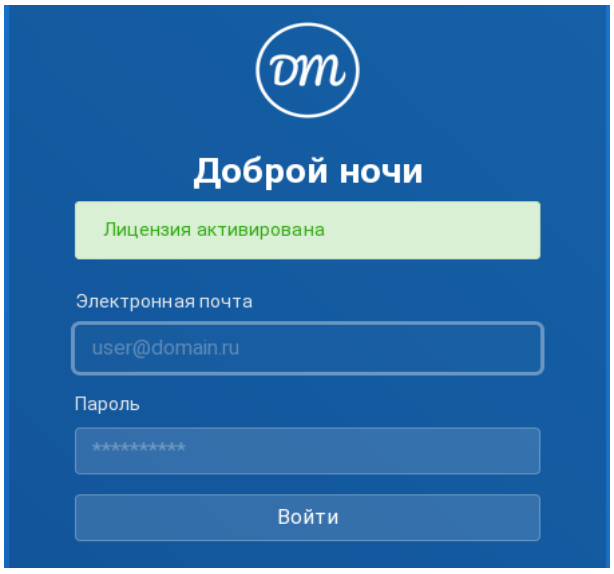


Рисунок 11 – Сообщение об активации лицензии

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 12).

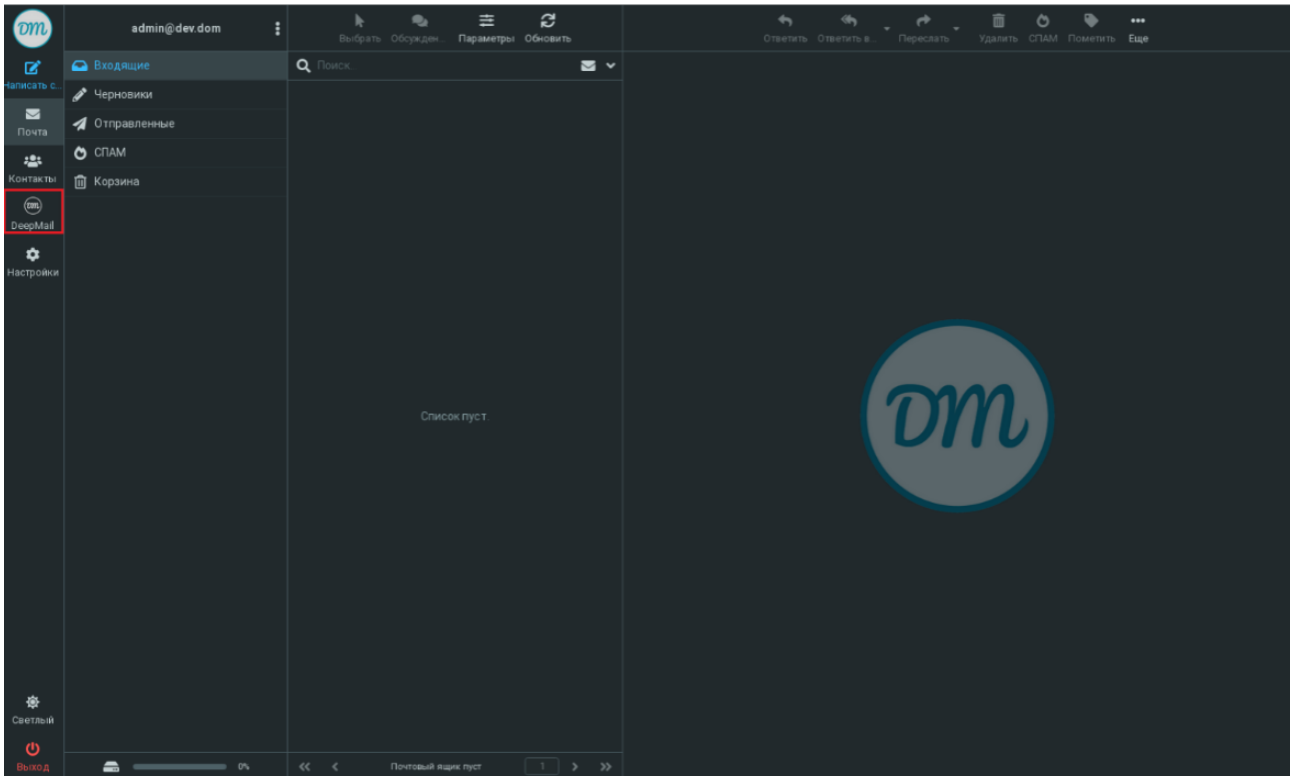


Рисунок 12 – Кнопка DeepMail перехода в интерфейс администратора

После этого откроется интерфейс администратора Сервера (рисунок 13).

Рисунок 13 – 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 14).

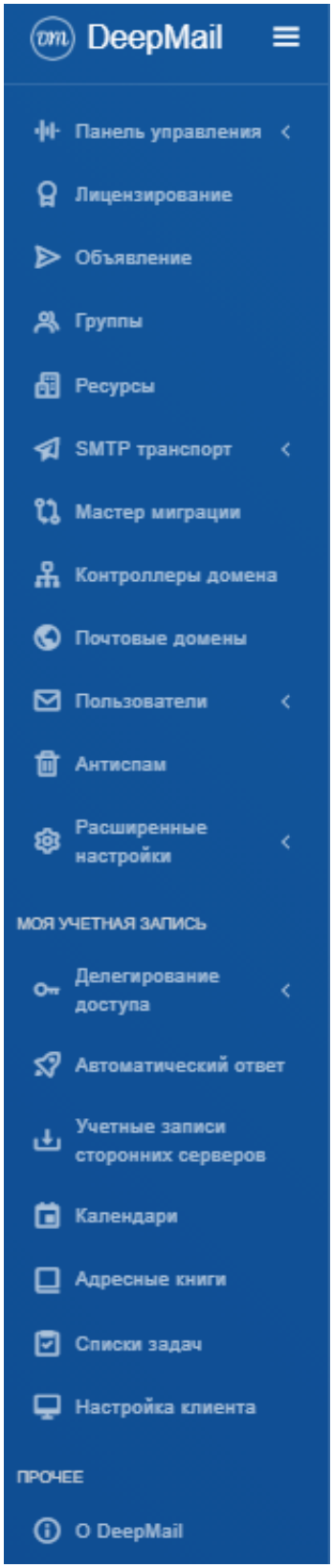


Рисунок 14 – Меню инструментов настроек и администрирования

Чтобы свернуть меню необходимо нажать кнопку  . (см. рисунок 14). Компактное представление меню инструментов настроек и администрирования представлено на рисунке 15.

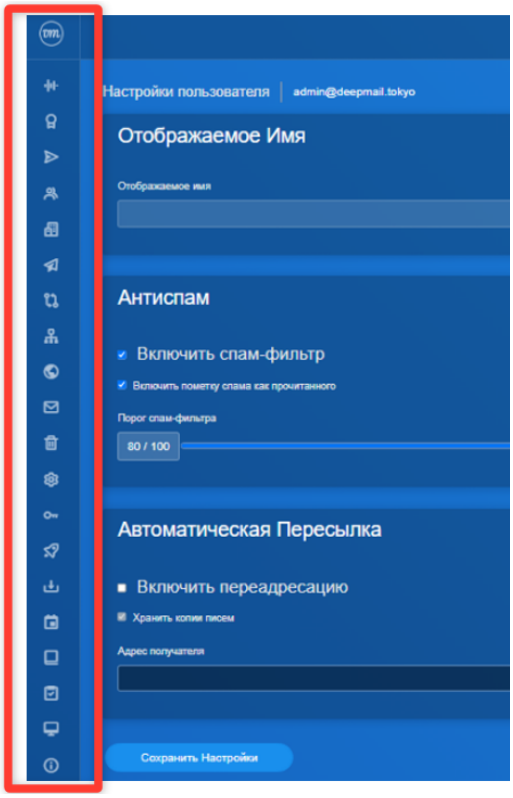


Рисунок 15 – Компактное представление меню инструментов настроек и администрирования

Предпросмотр меню инструментов доступен при наведении на него курсора, меню будет отображено в темном виде (рисунок 16).

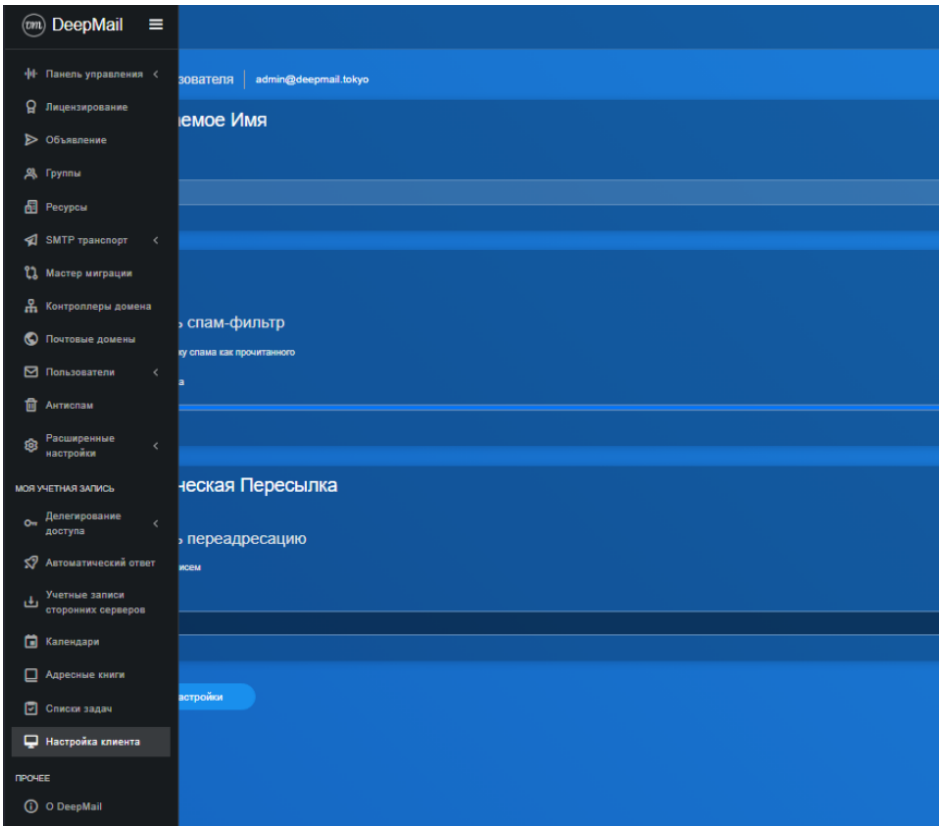


Рисунок 16 – Развернутое меню настроек и администрирования

Чтобы вернуть меню инструментов в исходное состояние необходимо нажать кнопку  (см. рисунок 16).

В верхней панели веб-интерфейса DeepMail расположены элементы для навигации между основными разделами и управления учётной записью. Слева находятся иконки, позволяющие переключаться между веб-клиентом электронной почты (иконка конверта) и файловым менеджером (иконка папки). В правой части панели отображается имя текущего пользователя; при нажатии на него раскрывается меню, где можно перейти в настройки учётной записи, изменить пароль или выйти из системы (рисунок 17).

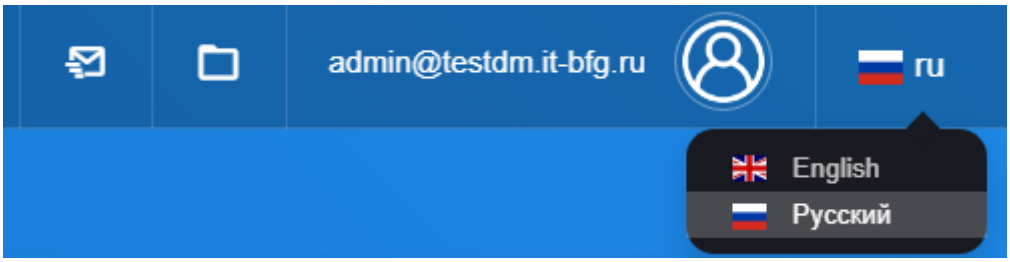


Рисунок 17 – Меню переключения языка интерфейса

В разделе настроек пользователь может, в частности, выбрать язык интерфейса из доступных вариантов (например, русский или английский). После сохранения настроек весь интерфейс почтового клиента и файлового менеджера отобразится на выбранном языке. Смена пароля также выполняется в этом меню: достаточно указать текущий и новый пароли, после чего учётные данные обновляются.

Порядок работы с веб-клиентом пользователя описан в руководстве пользователя Веб-клиента «DeepMail». Для работы с файловым менеджером, необходимо нажать на иконку «Папки», после чего откроется окно аутентификации (рисунок 18), в котором необходимо ввести свой логин и пароль.

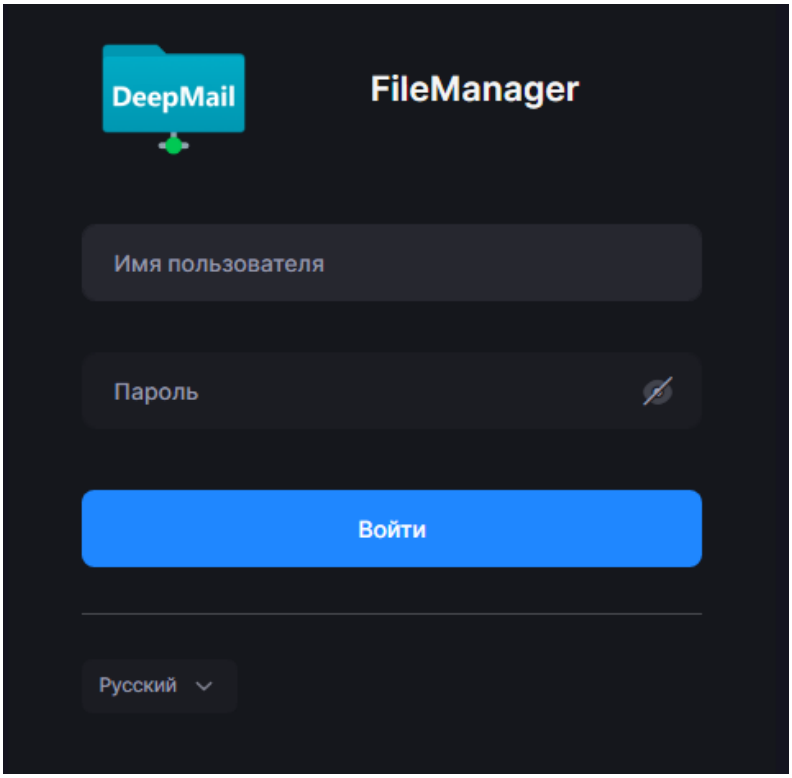


Рисунок 18 – Файловый менеджер аутентификация

Интерфейс файлового менеджера DeepMail (рисунок 19) предоставляет пользователю все необходимые инструменты для работы с личным хранилищем файлов. При переходе в раздел «Файлы» открывается главный экран, где отображается содержимое текущей директории. В верхней части находится строка поиска, позволяющая быстро найти нужный файл по имени. Список файлов представлен в виде таблицы с указанием имени, размера и даты последнего изменения. С помощью кнопок «Новая папка» и «Загрузить файлы» пользователь может создавать папки и добавлять новые файлы, перетаскивая их мышью или выбирая через диалог выбора.

Для каждого файла доступна функция настройки общего доступа. При её вызове открывается форма, в которой можно задать параметры публичной ссылки. В этой форме указывается путь к файлу, который нельзя изменить, и выбирается область доступа: только чтение, запись или чтение и запись. Администратор или владелец файла может защитить доступ паролем, установить срок действия ссылки, ограничить максимальное количество переходов по ней, а также указать разрешённые IP-адреса или подсети в формате CIDR. Дополнительно предусмотрено поле для описания, чтобы пояснить назначение ссылки. Все эти настройки сохраняются по нажатию кнопки «Сохранить», расположенной в нижней части формы.

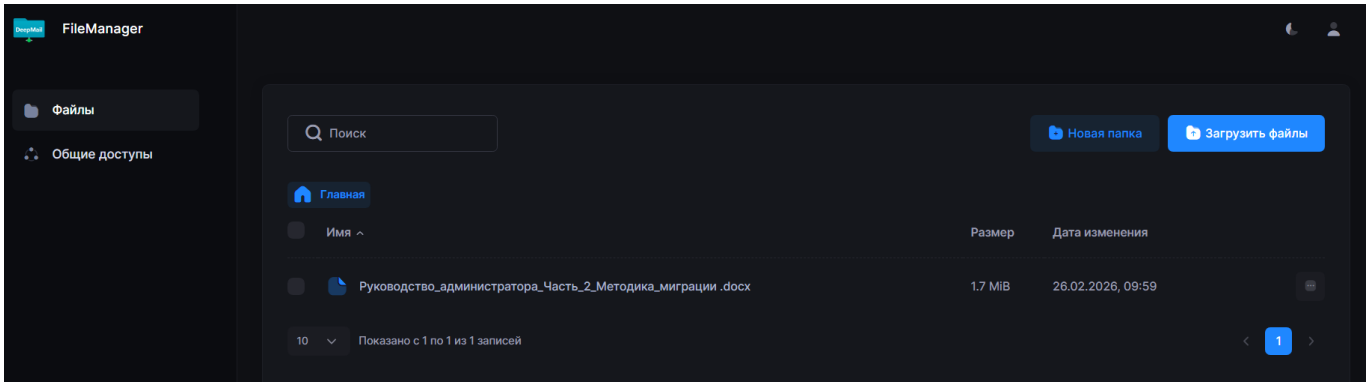


Рисунок 19 – Файловый интерфейс

В правом верхнем углу интерфейса отображается имя текущего пользователя. При нажатии на него раскрывается меню, где можно изменить тему оформления (светлая, тёмная или автоматическая), перейти в настройки профиля, сменить пароль или выйти из системы. Смена пароля выполняется через отдельную форму, где требуется ввести текущий и новый пароли. Выбор темы оформления влияет на внешний вид как файлового менеджера, так и веб-клиента электронной почты, обеспечивая комфортную работу в различных условиях освещения.

3.2 Инструмент «Панель управления»

Инструмент администрирования «Панель управления» состоит из нескольких инструментов:

- Система;
- Репозиторий;
- Хранилища;
- Базы данных;
- Профили;
- Почтовая очередь (рисунок 20).

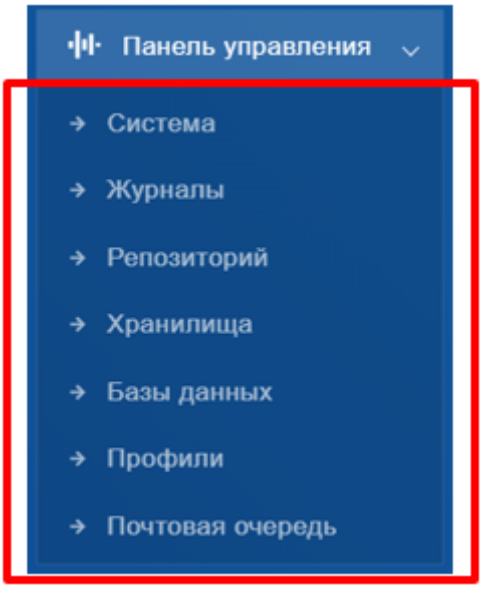


Рисунок 20 – Состав инструмента администрирования «Панель управления»

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 21).

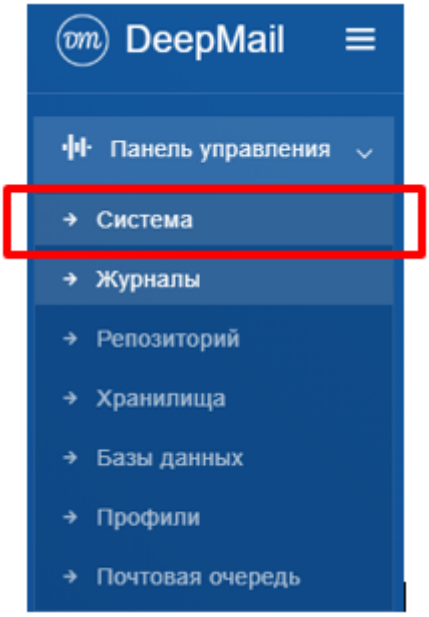


Рисунок 21 – Выбор инструмента «Система»

В результате выбора откроется окно с информацией о удаленных серверах (рисунок 22) Интерфейс представляет собой раздел управления инфраструктурой в панели администратора системы. Он обеспечивает визуальный обзор ландшафта хостов, позволяя контролировать ключевые метрики производительности каждого узла DeepMail, такие как

загрузка процессора и использование оперативной памяти. На экране отображается сводка по удалённому серверу с индикацией его общего состояния, что помогает оперативно выявлять потенциально перегруженные или проблемные хосты до возникновения критических ситуаций. Дополнительно представлена информация о количестве запущенных сервисов и списке подключенных хранилищ данных. Интерфейс включает элементы навигации для перехода к детальному мониторингу и управлению, а также предоставляет возможность удаления хоста из системы.

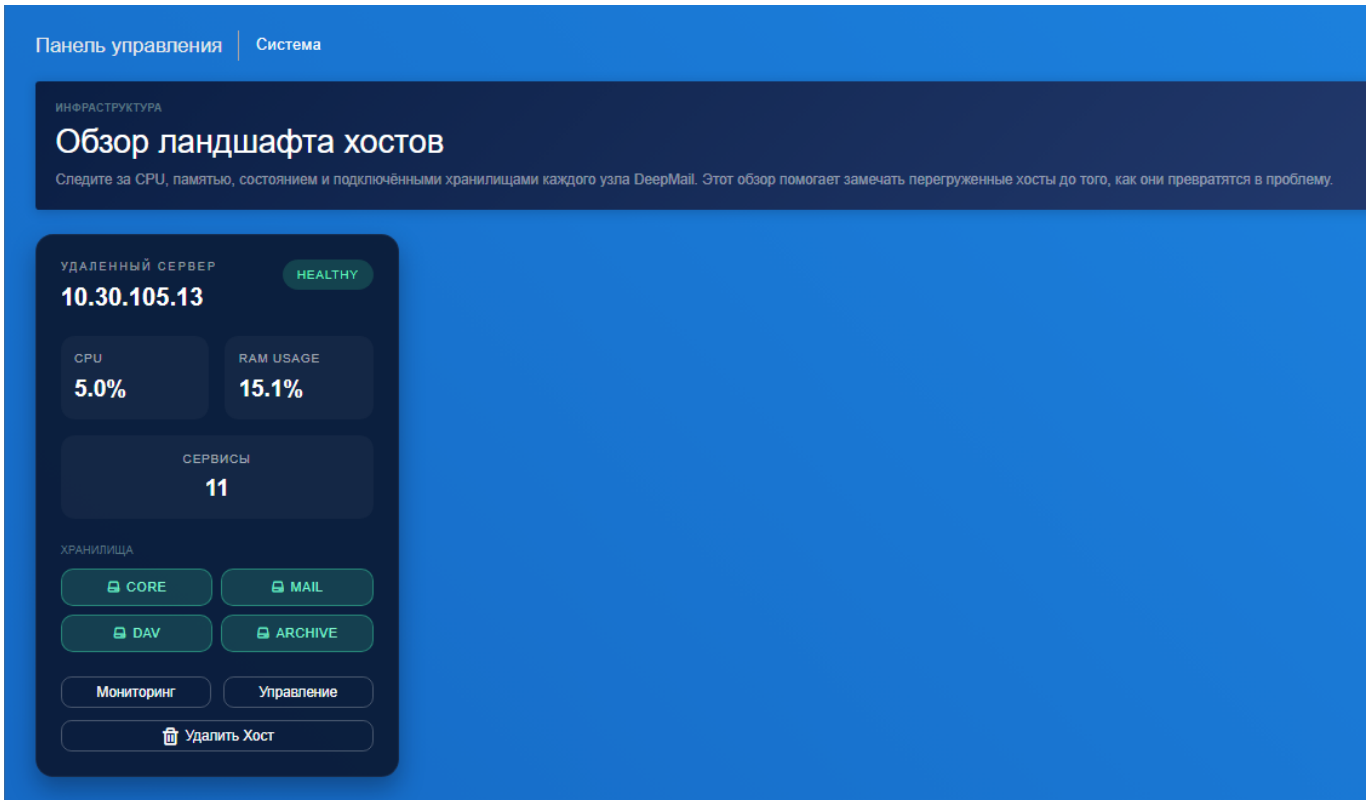
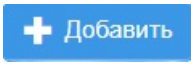


Рисунок 22 – Окно «Панель управления»

При нажатии на панели управления в правом левом углу кнопки 

откроется конфигуратор узла DeepMail (рисунок 23). Данное окно представляет собой интерфейс начальной настройки нового узла DeepMail в панели управления. Оно служит конфигуратором, позволяющим задать основные параметры для развёртывания сервера.

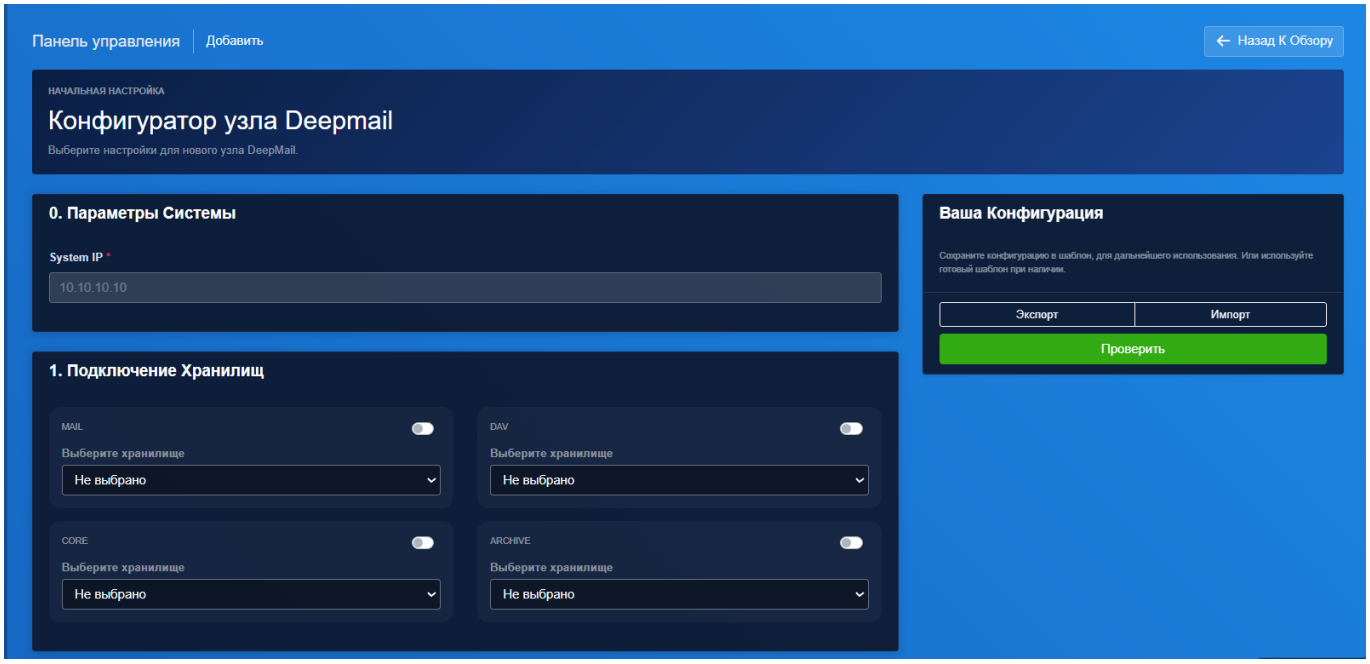


Рисунок 23 – Окно конфигуратор узла DeepMail

В верхней части окна расположен блок для указания системного IP-адреса узла. Ниже находится секция для работы с конфигурациями: пользователь может сохранить текущие настройки в качестве шаблона для последующего использования или загрузить уже существующий шаблон, используя кнопки экспорта и импорта. Здесь же доступна кнопка проверки корректности введённых параметров.

Основную часть интерфейса занимают разделы настройки «Подключения хранилищ», «Стеков и сервисов» и «Валидации.

Первая часть интерфейса настройки подключения хранилищ, в котором для каждого типа данных – почты (MAIL), данных CalDAV/CardDAV (DAV), системных файлов (CORE) и архива (ARCHIVE) – предоставлены выпадающие списки для выбора соответствующего дискового хранилища. Это позволяет гибко распределить ресурсы под различные задачи сервера.

Вторая часть интерфейса «Стеки и сервисы» (рисунок 24) предназначена для настройки распределения профилей между основными сервисными стеками системы. Здесь администратор может назначить конкретные профили конфигурации для таких критически важных компонентов, как SMTP, веб-интерфейсы (core, webmail, admin), службы каталогов (ldap), фильтрации (antispam, antivirus) и доступа к данным (webdav). Рядом с некоторыми сервисами отображаются индикаторы состояния, например, "Следует за отказом", указывающие на режим обеспечения отказоустойчивости. Этот этап позволяет тонко настроить роли и поведение каждого сервиса в новой ноде.

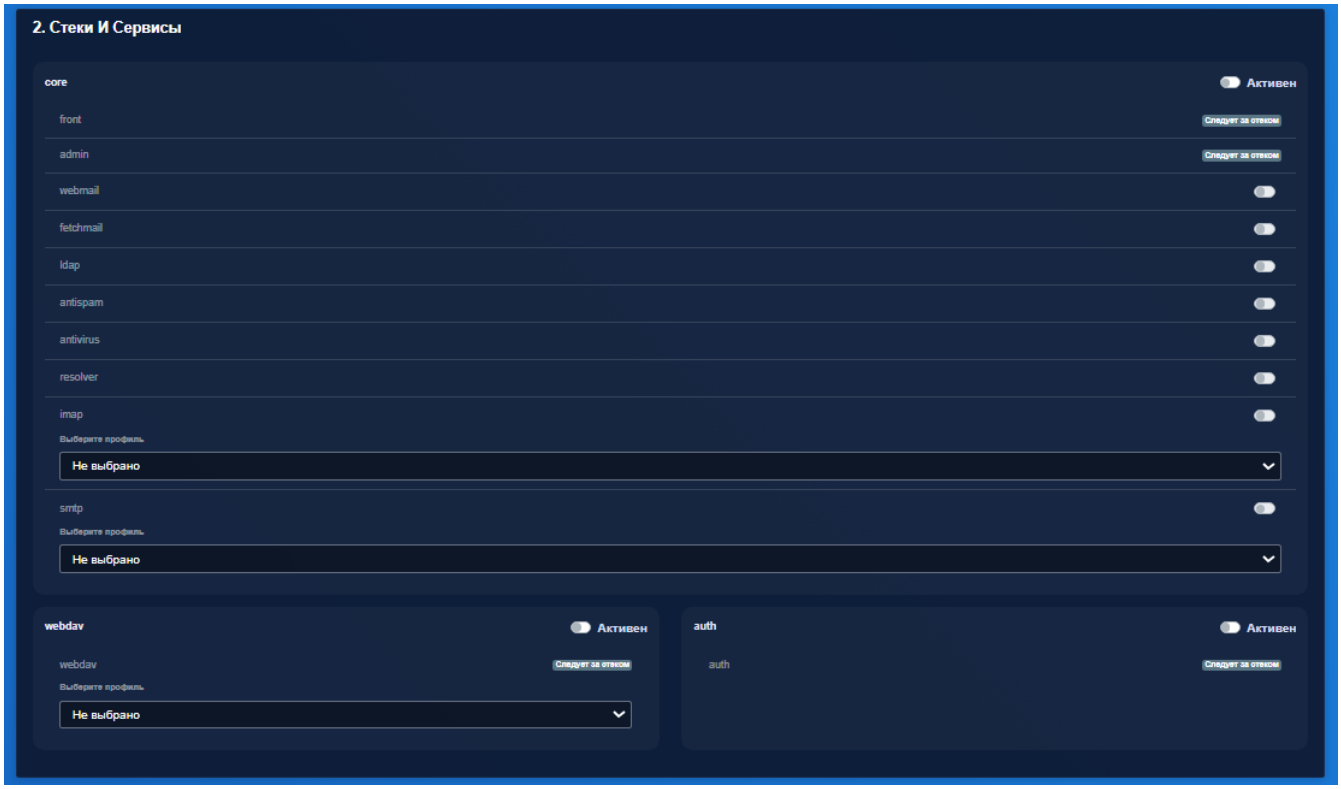


Рисунок 24 – Окно Стеки и сервисы

Вторая часть интерфейса «Валидация» (рисунок 25) представляет собой пошаговый процесс настройки автоматической проверки и запуска системы. Он последовательно проверяет корректность всех предварительных настроек: доступность и подготовку базы данных, Redis, всех подключенных хранилищ (core, mail, dav, archive), сохранение итоговой конфигурации и, наконец, запуск и проверку работоспособности всех сервисов. Каждый этап помечен индикатором [awaiting], что позволяет администратору в реальном времени наблюдать за ходом развёртывания и валидации нового узла перед вводом его в эксплуатацию.

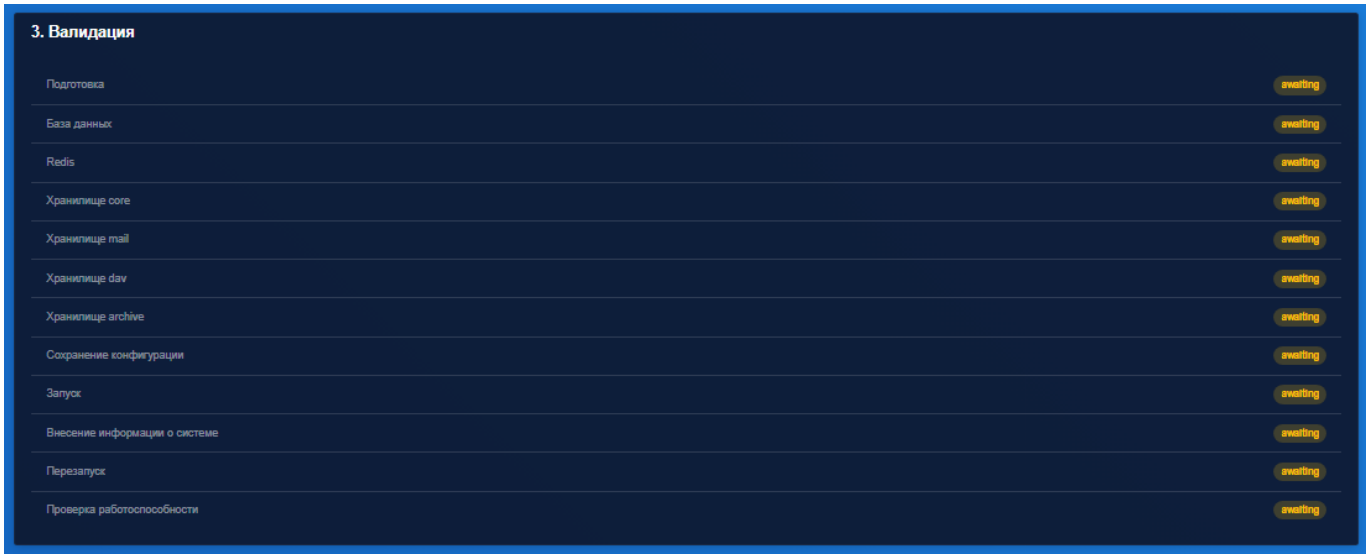


Рисунок 25 – Окно Валидация

Окно обеспечивает пошаговый подход к конфигурации узла, объединяя все ключевые настройки в одном месте для удобства администратора.

Интерфейс «Удаленный сервер» (рисунок 26) представляет собой компактную информационную панель состояния удалённого сервера.

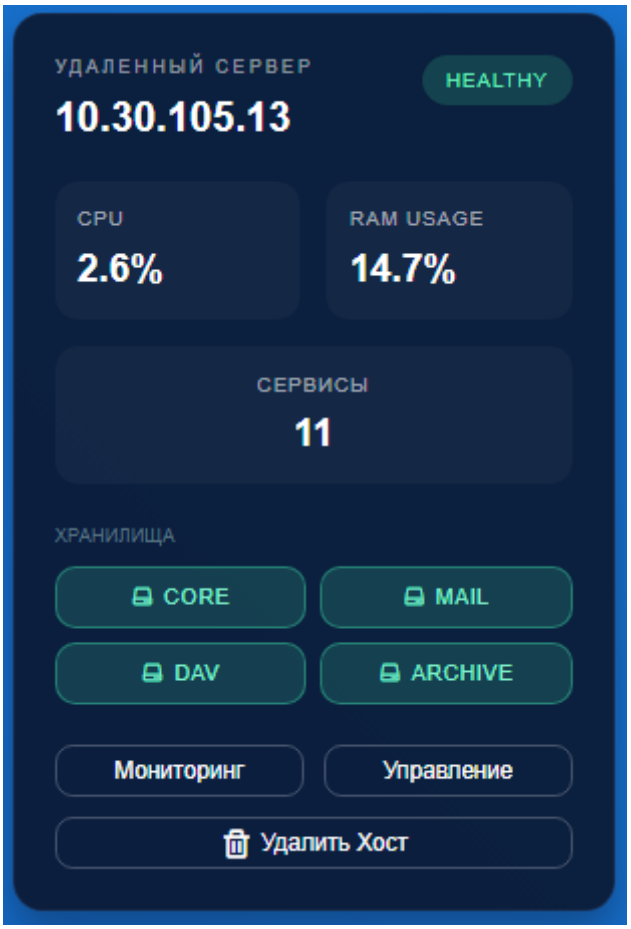


Рисунок 26 – Окно «Удаленный сервер»

В центре внимания – ключевые показатели работоспособности и нагрузки узла DeepMail: статус «HEALTHY» (исправен), IP-адрес (фигурирует в качестве примера), текущая загрузка процессора и оперативной памяти, а также количество активных сервисов.

Ниже перечислены подключённые к ноде хранилища данных (CORE, MAIL, DAV, ARCHIVE).

Интерфейс завершается блоками действий для перехода к расширенному мониторингу, управлению сервером и его удалению из системы. Это позволяет администратору быстро оценить состояние хоста и выполнить необходимые операции.

При нажатии на кнопку 

откроется окно с метриками по мониторингу системы. Окно представляет собой панель комплексного мониторинга

инфраструктуры, предназначенную для отслеживания состояния сетевых компонентов и использования ключевых ресурсов системы (рисунок 27).

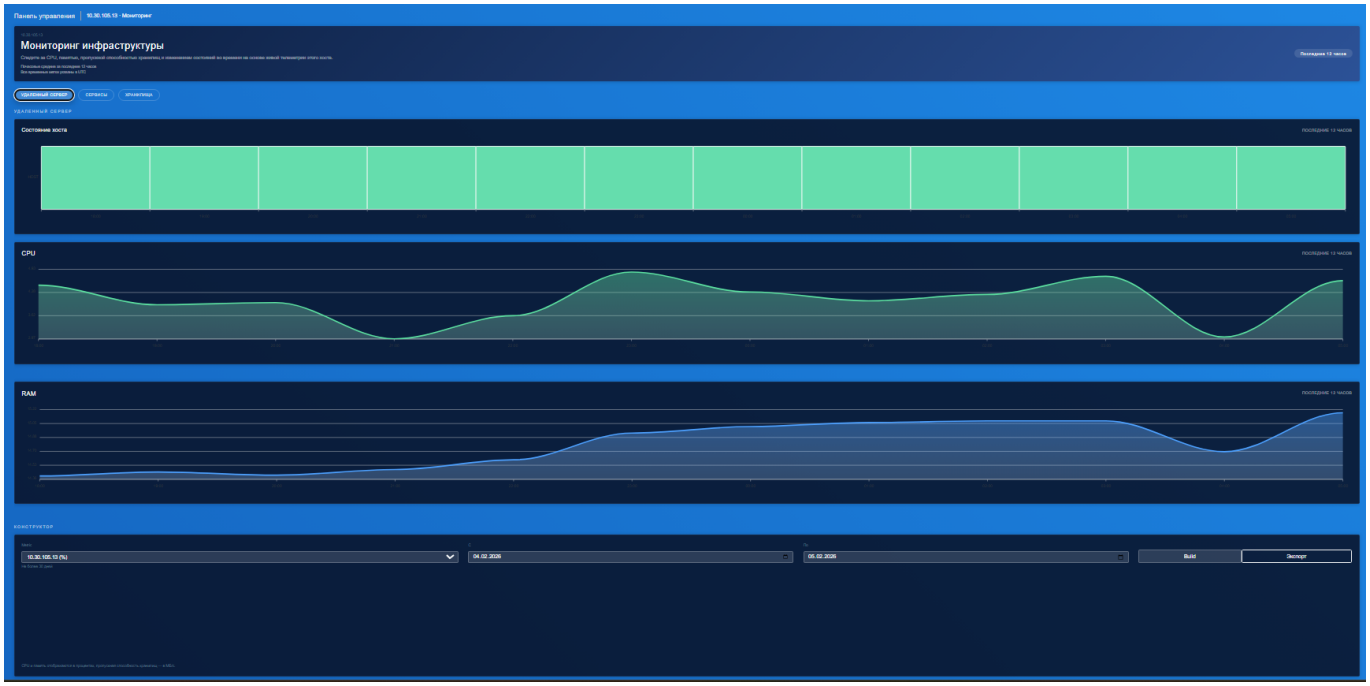


Рисунок 27 – Окно Мониторинг инфраструктуры/ Удаленный сервер

Данный интерфейс представляет собой комплексную панель мониторинга инфраструктуры, сфокусированную на отслеживании производительности конкретного удалённого сервера.

Интерфейс разделён на логические блоки, обеспечивающие многоуровневый анализ состояния системы. В верхней части представлена сводная информация о хосте: выбран мониторинг «Удаленного сервера» (см. рисунок 27), также можно мониторить «Сервисы» (см. рисунок 28) и «Хранилища» (см. рисунок 29). Это позволяет мгновенно оценить общую работоспособность узла.

Центральное место занимают динамические графики загрузки ключевых ресурсов – процессора (CPU) и оперативной памяти (RAM). Графики отображают изменения метрик за выбранный период (по умолчанию «последние 12 часов»), что помогает выявлять тренды и аномалии в потреблении ресурсов. Все данные представлены в процентах использования, а временные метки стандартизированы в формате UTC для единообразия.

Для глубокого анализа доступен детализированный просмотр каждого показателя. Например, при выборе памяти (RAM) открывается специализированный вид с конструктором графиков, где можно настроить отображение данных за период до 30 дней, сравнить разные временные отрезки и экспортировать информацию для внешнего анализа.

Интерфейс снабжён подсказками, поясняющими единицы измерения (проценты для CPU и RAM, МБ/с для пропускной способности хранилища).

Таким образом, панель сочетает оперативный обзор «живого» состояния хоста с мощными инструментами ретроспективного анализа, предоставляя администратору полный контроль над производительностью инфраструктуры.

Интерфейс мониторинга сервисов (рисунок 28) представляет собой панель мониторинга состояния сервисов удалённого сервера, объединяющую информацию о работоспособности отдельных служб и потреблении ими системных ресурсов.

Рисунок 28 – Окно Мониторинг/ Сервисы

Экран разделён на две синхронизированные по времени области. В левой части отображаются графики загрузки центрального процессора (CPU) и оперативной памяти (RAM) за последние 12 часов, показывающие общее потребление ресурсов сервером в динамике.

Правый блок посвящён непосредственно состоянию сервисов (например, каталоги, заявки, такси). Для каждого сервиса представлена цветовая временная шкала, визуализирующая историю его работоспособности за тот же 12-часовой период. Это позволяет моментально соотнести всплески или падения потребления ресурсов (слева) с изменениями статусов конкретных служб (справа).

Для глубокого анализа доступен детализированный просмотр каждого показателя. Например, при выборе памяти (RAM) открывается специализированный вид с

конструктором графиков, где можно настроить отображение данных за период до 30 дней, сравнить разные временные отрезки и экспортировать информацию для внешнего анализа. Интерфейс снабжён подсказками, поясняющими единицы измерения (проценты для CPU и RAM, МБ/с для пропускной способности хранилища).

Таким образом, интерфейс обеспечивает комплексный анализ, где администратор может одновременно наблюдать как общую нагрузку на систему, так и детальную картину доступности каждого сервиса, выявляя прямые зависимости между ними (см. рисунок 28).

Интерфейс мониторинга хранилища (рисунок 29) представляет собой панель мониторинга хранилищ, обеспечивающую комплексный контроль над состоянием, производительностью и использованием дискового пространства на сервере.

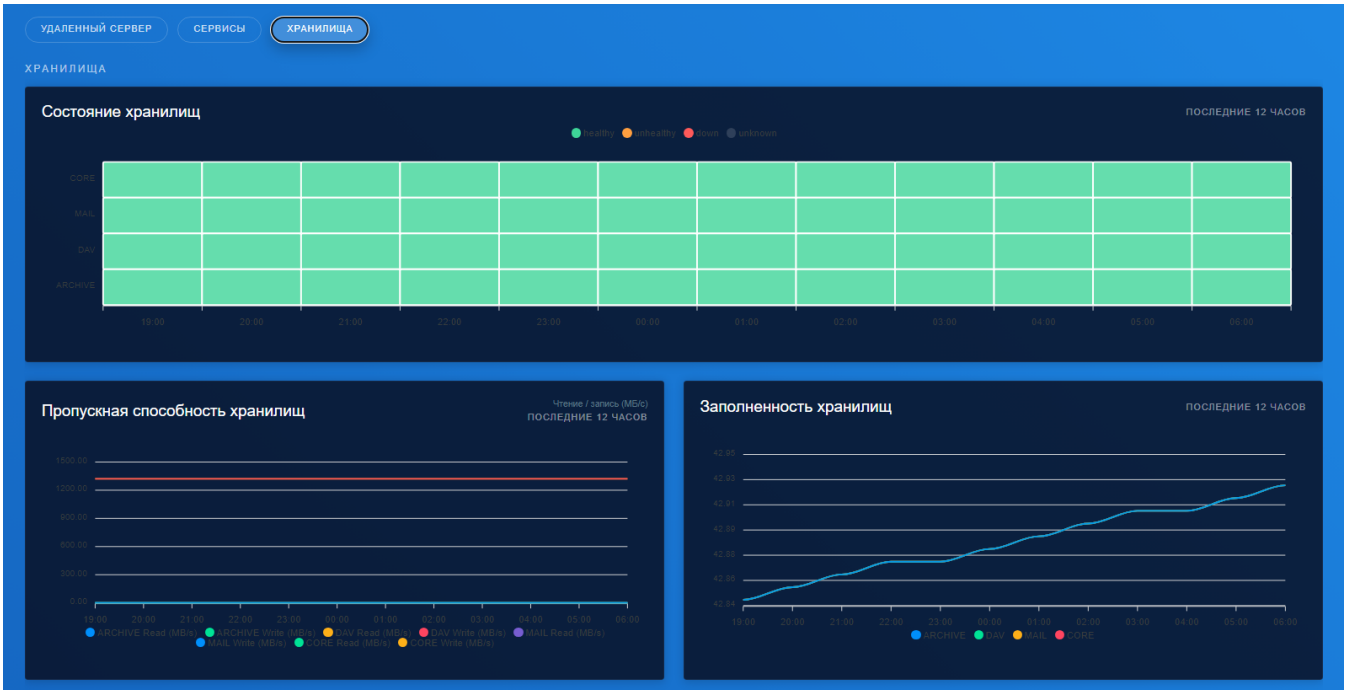


Рисунок 29 – Окно Мониторинг/ Хранилища

Экран визуально разделён на три ключевые секции, каждая из которых отображает данные за единый 12-часовой период, что позволяет проводить корреляционный анализ событий во времени.

В верхней части интерфейса представлен график состояния хранилищ, который с помощью цветовых индикаторов (например, Healthy, Unhealthy) отображает историю их работоспособности. Это позволяет мгновенно определить периоды возникновения проблем с доступностью дисковых массивов.

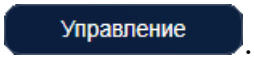
Центральная секция посвящена мониторингу пропускной способности. На детализированном графике показана динамика операций чтения и записи (в МБ/с) для

каждого типа хранилища (например, ARCHIVE, MAIL). Это даёт чёткое понимание нагрузки на подсистему ввода-вывода и помогает выявлять аномальную активность.

Нижний блок отображает заполненность хранилищ в процентах. График демонстрирует, как изменялся объём занятого пространства на каждом из основных томов (CORE, MAIL, ARCHIVE) с течением времени, что критически важно для планирования ресурсов и предотвращения исчерпания дискового пространства.

Для глубокого анализа доступен детализированный просмотр каждого показателя. Например, при выборе памяти (RAM) открывается специализированный вид с конструктором графиков, где можно настроить отображение данных за период до 30 дней, сравнить разные временные отрезки и экспортировать информацию для внешнего анализа. Интерфейс снабжён подсказками, поясняющими единицы измерения (проценты для CPU и RAM, МБ/с для пропускной способности хранилища).

Таким образом, интерфейс объединяет три аспекта мониторинга – доступность, производительность и емкость – предоставляя администратору целостную и наглядную картину здоровья дисковой подсистемы (см. рисунок 29).

Для управления мониторингом в окне «Удаленный сервер (см. рисунок 26) необходимо нажать кнопку 

.

Панель управления мониторингом представляет собой централизованный интерфейс управления и мониторинга конкретного хоста DeepMail, объединяющий ключевые показатели его работоспособности и производительности в реальном времени (рисунок 30).

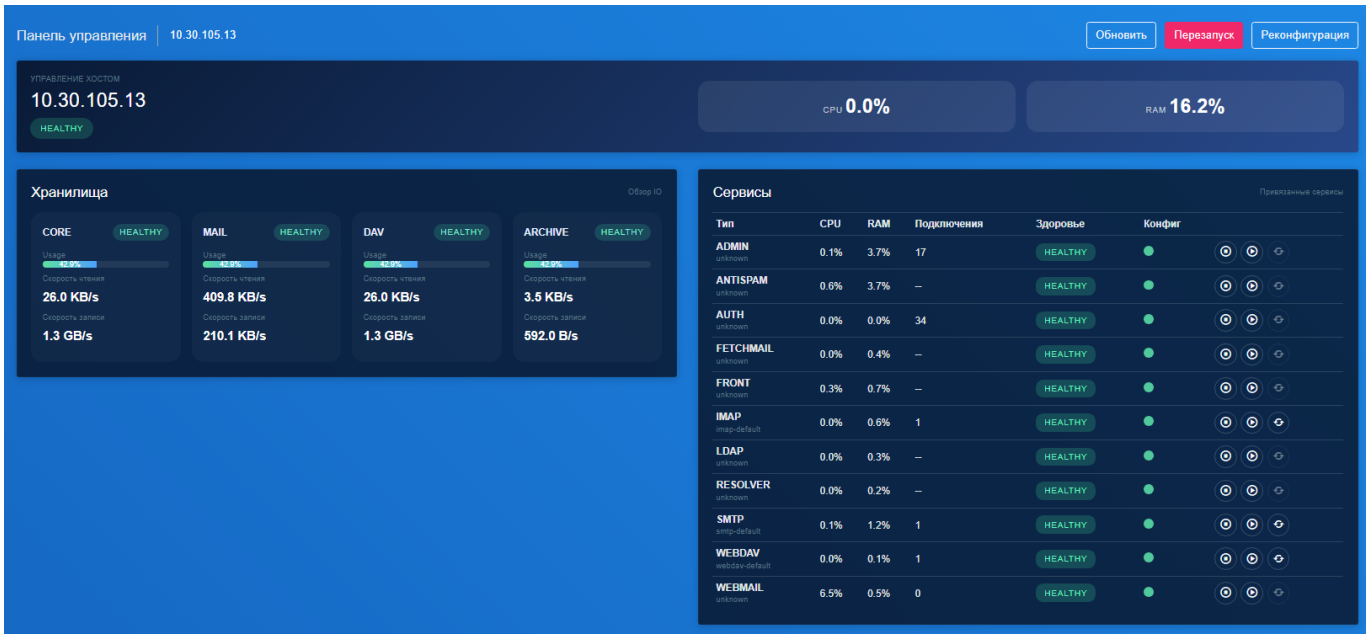


Рисунок 30 – Окно управления мониторингом

В верхней части отображается общий статус хоста (HEALTHY) с текущей загрузкой процессора, а также идентификатор системы. Следом идёт блок контроля хранилищ, где для каждого тома (CORE, MAIL, DAV, ARCHIVE) указано состояние доступности. Здесь же представлены агрегированные метрики скорости чтения и записи данных, что позволяет мгновенно оценить нагрузку на дисковую подсистему.

Основную часть интерфейса занимает детализированная таблица состояния сервисов. Для каждого сервиса (ADMIN, SMTP, IMAP и т.д.) приведены точные значения потребления ресурсов CPU и оперативной памяти в процентах, количество активных сетевых подключений и индикатор здоровья. Это даёт администратору полную картину распределения ресурсов между компонентами системы и помогает быстро выявить проблемные службы.

Таким образом, панель обеспечивает комплексный оперативный обзор, сочетая сводные данные о здоровье узла с детальной аналитикой по каждому сервису, что является основой для эффективного управления инфраструктурой.

3.2.2 Журналы

Раздел «Журналы» в панели управления DeepMail предоставляет администратору два основных режима: просмотр логов в реальном времени (и архивных) и выгрузку отобранных записей во внешний файл. Оба режима интегрированы в единый интерфейс, что позволяет оперативно анализировать события системы и сохранять их для последующего аудита или передачи в системы класса SIEM.

Основное окно разделено на три функциональные области. В левой части находится список «Источники», где перечислены все узлы инфраструктуры: удалённые серверы с их IP-адресами (например, 10.30.101.195), а также служебные источники global (системные события) и migration (логи миграции). Рядом с каждым источником указано количество записей (12/20 – 12 новых, 20 всего). Администратор может выбрать конкретный хост, чтобы сузить выборку, либо оставить значение «Все хосты» для просмотра событий со всех узлов (рисунок 31).

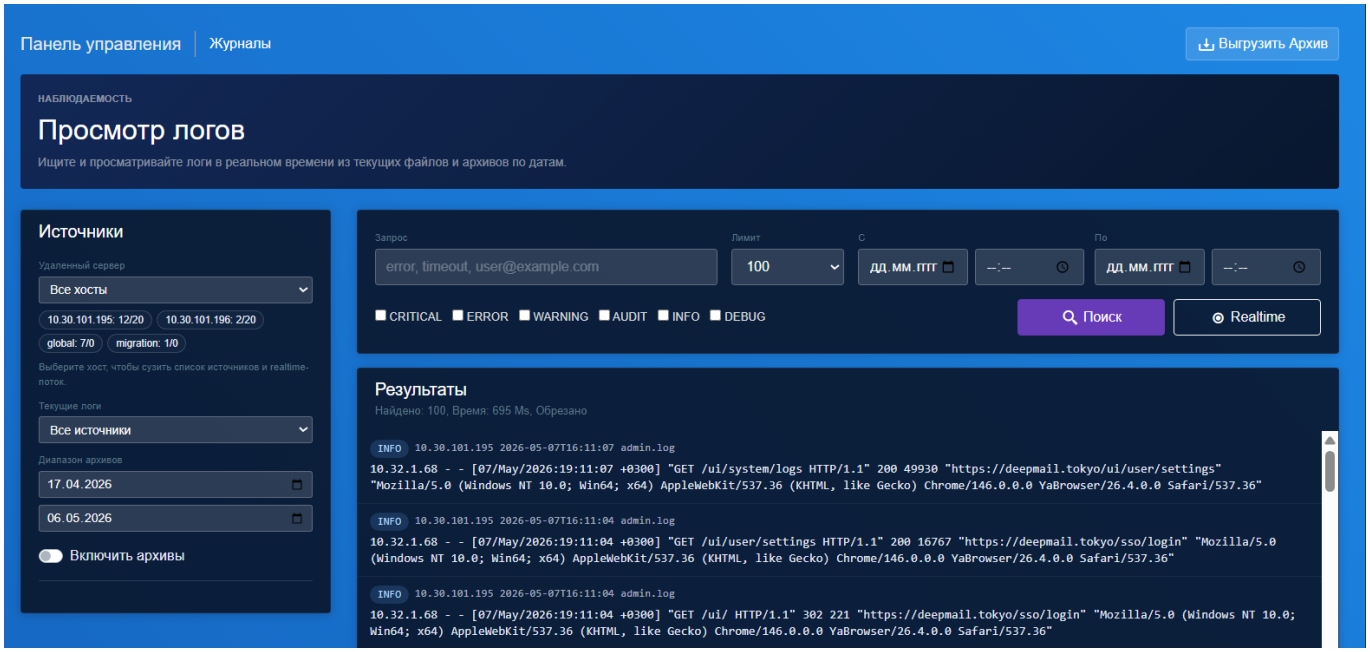


Рисунок 31 – Окно Журналы/ Просмотр логов

Центральная панель содержит элементы управления временным диапазоном. Переключатель «Текущие логи» позволяет наблюдать поток событий в реальном времени без ограничений по дате. Если необходимо обратиться к сохраненным журналам, используется опция «Диапазон архивов» – активируются поля выбора начальной и конечной даты (формат ДД.ММ.ГГГГ). Чекбокс «Включить архивы» объединяет оба режима, выполняя поиск одновременно по текущим файлам и архивным записям за указанный интервал.

Правая область выводит результаты поиска. В заголовке таблицы отображаются служебные сведения: общее количество найденных строк, время выполнения запроса (в миллисекундах) и примечание об обрезании длинных строк. Каждая запись представлена структурированной строкой: уровень важности (INFO, WARNING, ERROR), IP-адрес узла или имя файла журнала (например, admin.log), временная метка в формате ISO, а затем детальное сообщение – дата и время в локальном формате, IP-адрес клиента, метод HTTP, URL, код ответа, реферер и строка агента. Такое представление позволяет быстро идентифицировать источник события и его контекст.

При необходимости сохранить логи для внешнего анализа администратор открывает окно «Настройки выгрузки» (рисунок 32) нажав кнопку Выгрузить Архив (см. рисунок 31).

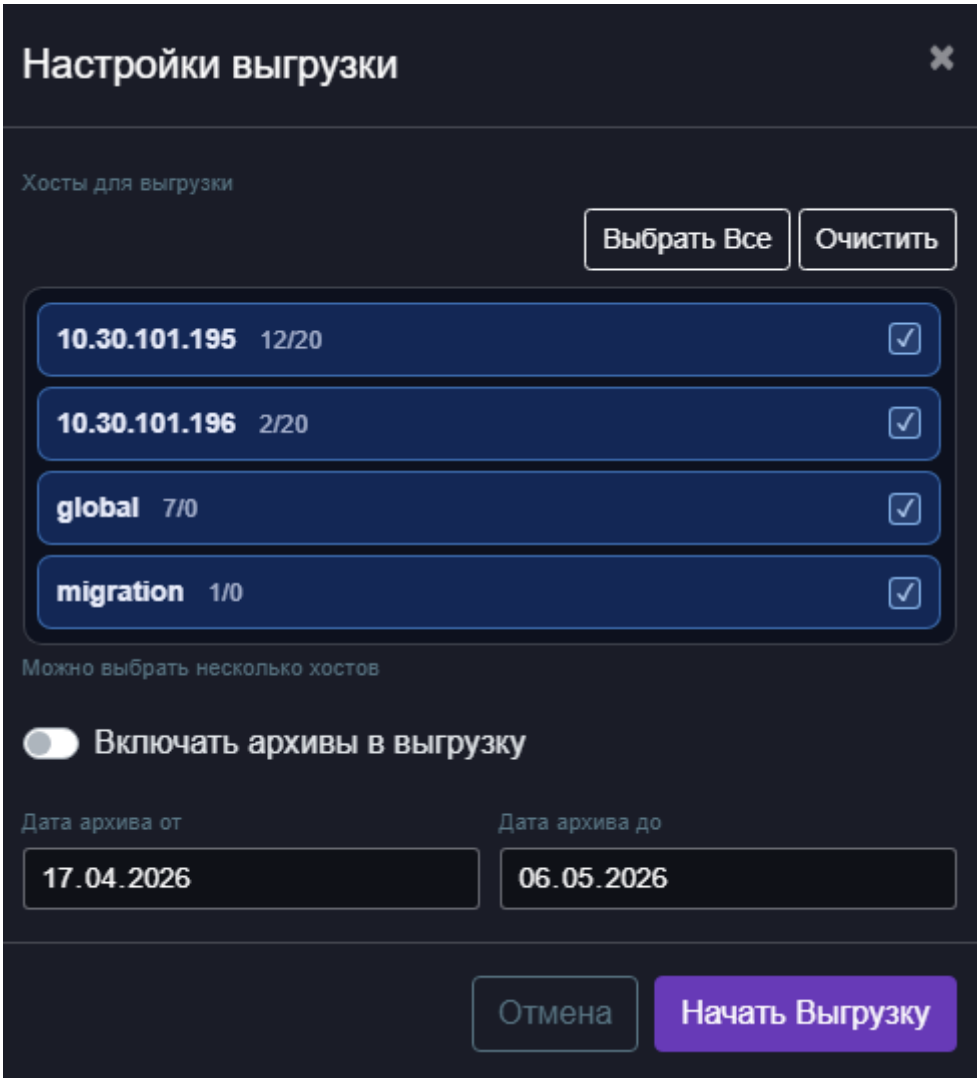


Рисунок 32 – Окно настройки выгрузки журналов

В этом окне представлены все доступные источники – те же хосты и служебные объекты, что и на главном экране. Для каждого источника указано количество записей (например, 10.30.101.195: 12/20). Можно выбрать несколько хостов одновременно, используя чекбоксы, или воспользоваться кнопками «Выбрать Все» и «Очистить». Также доступен флажок «Включать архивы в выгрузку» – если он установлен, в выгрузку попадут и архивные записи за указанный период, и текущие логи. Далее задаются дата архива от и дата архива до – этим ограничивается временной интервал выгружаемых событий. После настройки параметров нажатие кнопки «Начать Выгрузку» инициирует создание файла. Система соберёт все записи, соответствующие выбранным хостам и диапазону дат, и предложит скачать полученный архив в удобном для дальнейшего использования формате (обычно текстовый файл или архив с логами). Эта функция особенно полезна для предоставления журналов службе технической поддержки, для интеграции с внешними анализаторами или для выполнения требований по хранению логов.

3.2.3 Репозиторий

Интерфейс управления репозиториями представляет собой панель управления внутренним репозиторием образов контейнеров для системы DeepMail (рисунок 33).

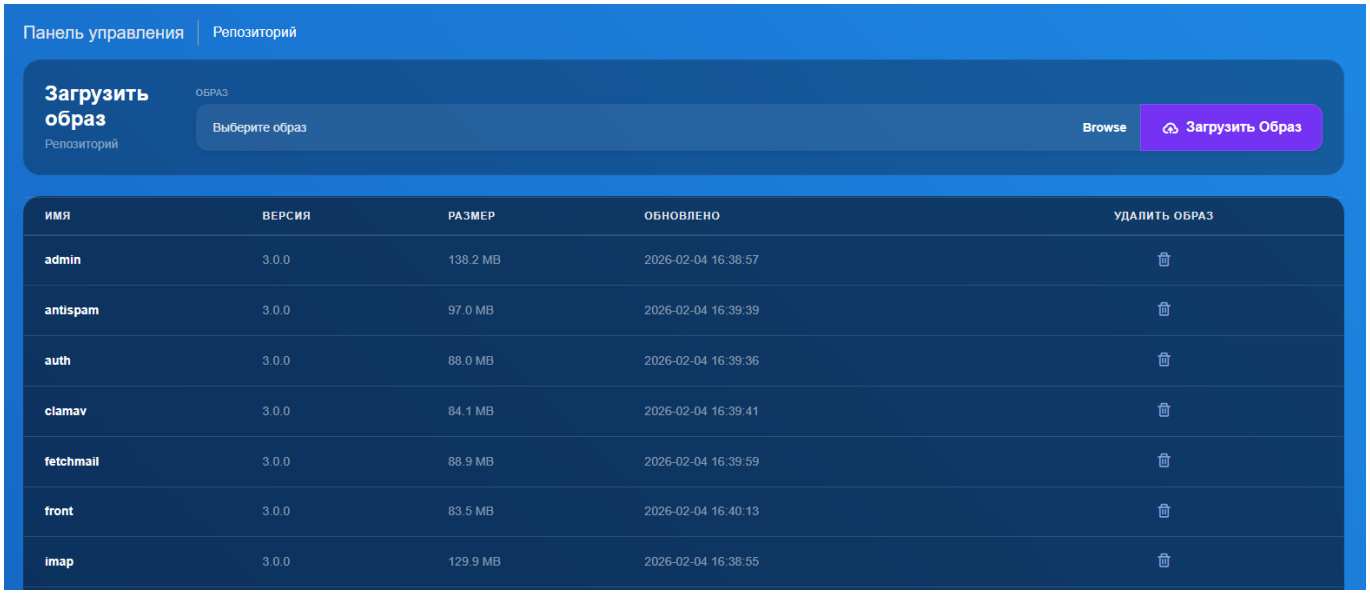


Рисунок 33 – Окно управления репозиториями

Основное назначение панели – централизованное хранилище и управление дистрибутивами всех сервисных компонентов (admin, antispam, auth и т.д.). Интерфейс разделён на две ключевые функциональные зоны.

В верхней части расположен инструмент для загрузки новых образов в репозиторий. Администратор может выбрать готовый образ через поле «Выберите образ» или загрузить его напрямую с локального компьютера, используя кнопку «Browse» и подтвердив действие кнопкой «Загрузить Образ».

Нижнюю часть занимает таблица уже загруженных образов. Для каждого образа указаны его имя, версия, размер, дата последнего обновления и предусмотрена кнопка для удаления. Это позволяет администратору легко отслеживать актуальные версии компонентов, управлять дисковым пространством и поддерживать порядок в библиотеке образов.

Таким образом, панель обеспечивает полный цикл управления программными компонентами кластера DeepMail: от добавления новых дистрибутивов до контроля версий и очистки устаревших образов.

3.2.4 Хранилища

Интерфейс управления хранилищами (рисунок 34) представляет собой панель управления подключенными хранилищами в системе DeepMail, обеспечивающую централизованный контроль над дисковыми ресурсами.

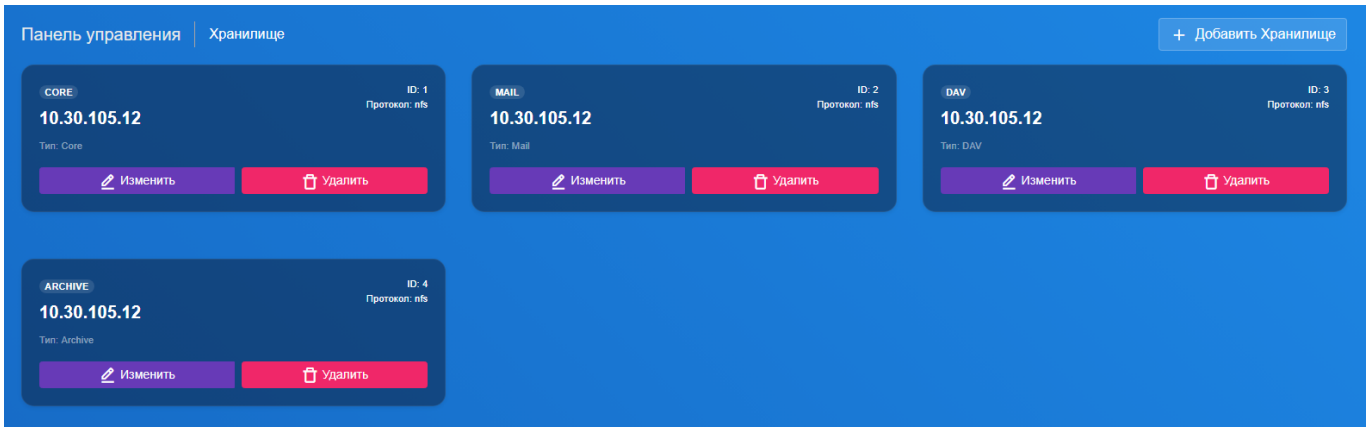


Рисунок 34 – Окно управления хранилищами

Окно сгруппировано по типам хранилищ: CORE (системные данные), MAIL (почтовые ящики), DAV (календари и контакты) и ARCHIVE (архивы). Для каждого типа отображается хост, к которому оно привязано, и его назначение.

Под каждым типом хранилища списком выводятся конкретные точки подключения (ID) с указанием используемого сетевого протокола (например, NFS). Напротив, каждого элемента доступны кнопки «Изменить» и «Удалить», позволяющие перенастроить или отключить конкретное хранилище.

В правом верхнем углу находится кнопка «Добавить хранилище» позволяющая добавить новое хранилище.

Таким образом, интерфейс предоставляет администратору наглядную иерархию всех дисковых ресурсов системы с возможностью детального управления каждым подключением.

3.2.5 Базы данных

Интерфейс управления базами данных представляет собой панель управления системными базами данных и кластерными сервисами в DeepMail (рисунок 35).

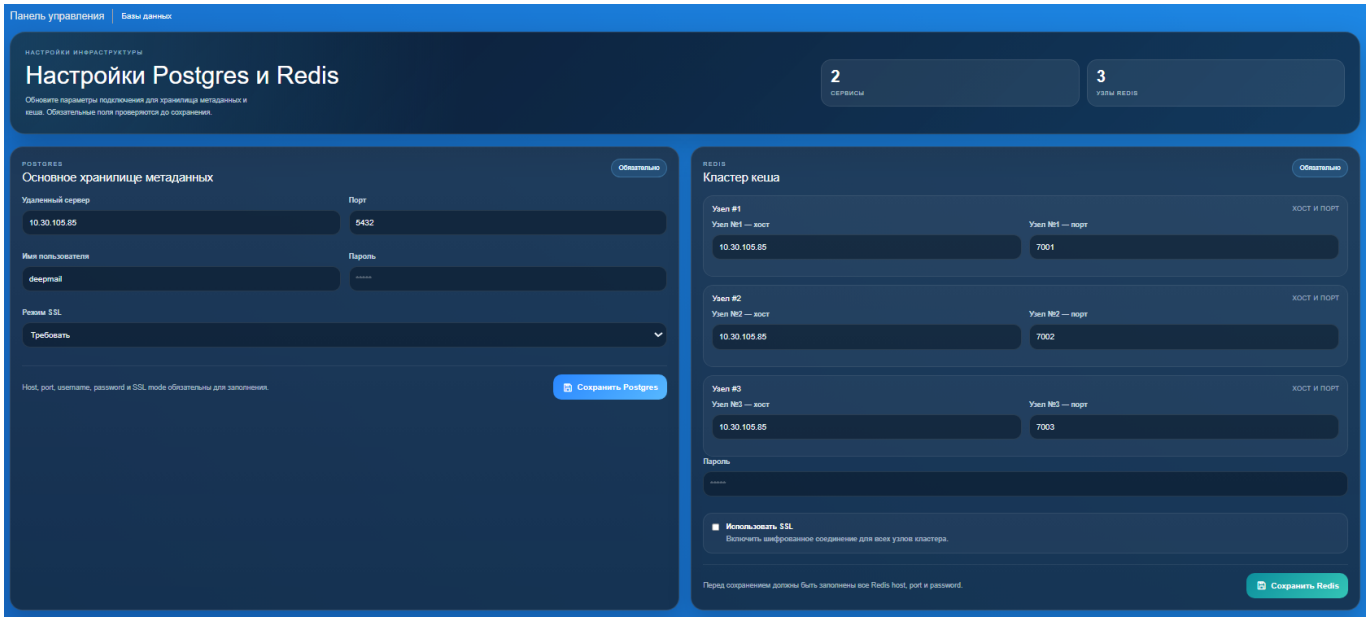


Рисунок 35 – Окно управления базами данных

Он разделён на две основные логические секции, каждая из которых отвечает за настройку критически важного компонента инфраструктуры.

В верхней части расположена конфигурация PostgreSQL (РЕЖИМ POSTGRES), который выступает в роли основного реляционного хранилища для метаданных системы. Здесь администратор может задать параметры подключения к удалённому серверу: IP-адрес, порт, учётные данные пользователя и настроить политику использования шифрования SSL для защиты передаваемых данных. Кнопка «Сохранить Postgres» позволяет применить изменения.

Нижняя секция посвящена настройке кластера Redis (КЛАСТЕР), используемого для кэширования и организации очередей сообщений. Интерфейс позволяет сконфигурировать несколько узлов кластера (в примере – три узла), указав для каждого хост и порт. Также здесь задаётся общий пароль для доступа и опция использования SSL, что обеспечивает безопасность взаимодействия между компонентами системы.

Таким образом, интерфейс предоставляет администратору централизованный и наглядный инструмент для управления всей backend-инфраструктурой хранения данных, объединяя настройки основного хранилища и распределённого кэша в одном месте.

3.2.6 Профили

Интерфейс управления профилями представляет собой панель управления профилями конфигурации в системе DeepMail, предназначенную для централизованного создания, редактирования и распределения настроек между сервисами (рисунок 36).

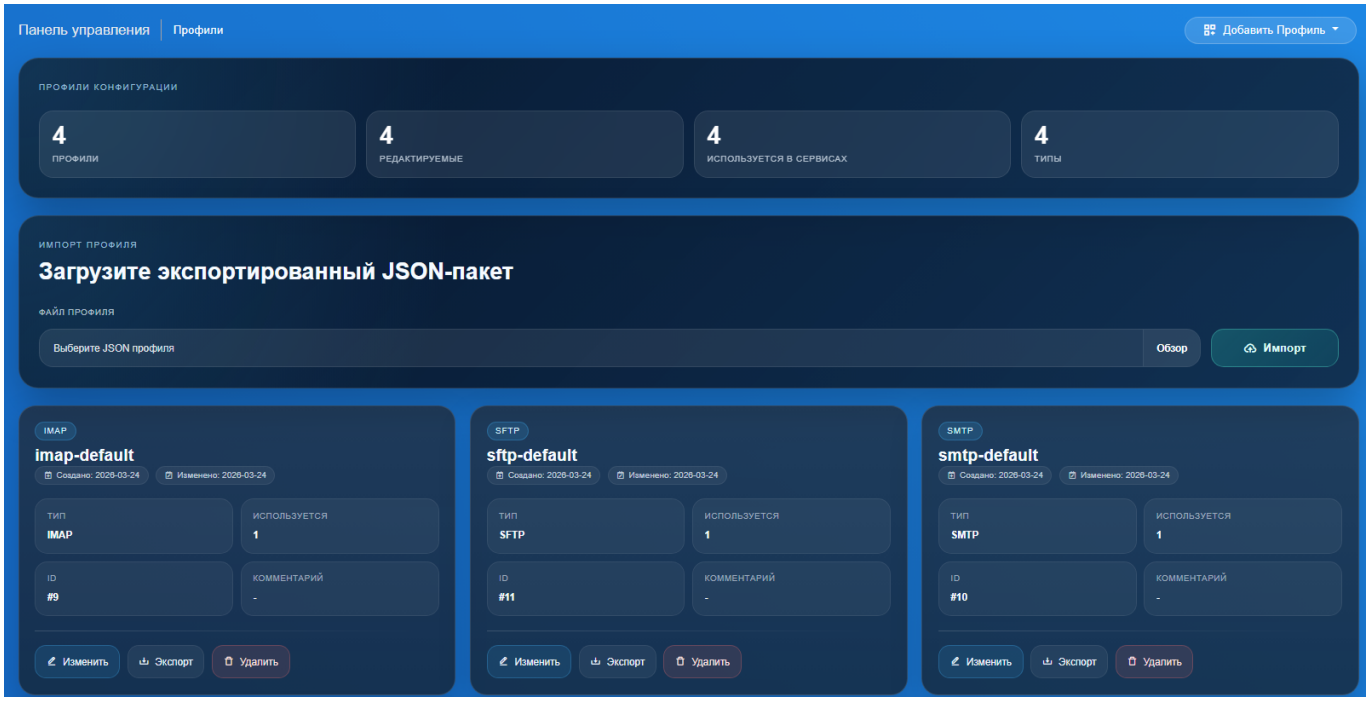


Рисунок 36 – Окно управления профилями

Панель разделена на две ключевые функциональные зоны. В верхней части отображается список существующих профилей (например, профиль IMAP). Для каждого профиля указана служебная информация: дата создания, последнего обновления и возможность добавить комментарий. Рядом с каждым профилем доступны кнопки для его изменения, экспорта в файл и удаления, что обеспечивает полный цикл управления конфигурациями. Изменение конфигураций выполняется без остановки сервиса.

Нижняя секция посвящена импорту профилей. Она позволяет загрузить ранее экспортированный JSON-файл с настройками, используя кнопку "Обзор", и затем применить их, нажав "Импорт". Это удобно для тиражирования одинаковых настроек на разных узлах, восстановления конфигураций или их передачи.

Для добавления нового профиля необходимо в правом верхнем углу окна нажать кнопку «Добавить профиль» и выбрать соответствующий профиль IMAP, WebDav или SMTP, после чего заполнить поля и нажать кнопку «Сохранить».

Таким образом, интерфейс объединяет инструменты для ручного управления профилями и механизмы для их массового импорта/экспорта, предоставляя администратору гибкий и эффективный способ работы с конфигурациями сервисов.

Для коррекции или удаления существующих профилей необходимо на соответствующем профили нажать кнопку «Изменить» или «Удалить» соответственно.

В DeepMail реализована двухуровневая система хранения удалённых писем, обеспечивающая дополнительную защиту от окончательной потери данных. Первый уровень — это стандартная корзина, доступная пользователям через почтовые клиенты и веб-интерфейс. Физически она располагается в подкаталоге */Trash* почтового ящика пользователя. Когда пользователь очищает эту корзину, письма не удаляются безвозвратно, а перемещаются во второй, скрытый уровень — папку */Recoverable*, которая находится в структуре того же ящика. Доступ к этому уровню возможен только на уровне файловой системы сервера и требует привилегий администратора.

Для настройки корзин первого и второго (скрытая корзина) уровней, куда попадают письма из обычной корзины после ее очистки, требуется на поле профиля IMAP (см. рисунок 36) нажать кнопку «Изменить» и в открывшемся окне настроить параметры автоочистки корзин (рисунок 37).

Рисунок 37 – Настройка параметров автоочистки

Параметры автоматической очистки обоих уровней задаются в IMAP-профиле через веб-интерфейс панели управления. Администратор может установить срок хранения писем в каждом из уровней, по истечении которого они будут окончательно удалены с сервера. Настройки применяются централизованно для всех пользователей, использующих данный профиль.

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.

Если возникает необходимость восстановить письма из скрытой корзины, администратору необходимо выполнить следующие действия на сервере, где размещён почтовый ящик пользователя:

- вначале необходимо получить права привилегированного пользователя (*root*) и перейти в корневой каталог, где хранятся все почтовые ящики (по

умолчанию */mnt/deepmail/mail/*). Затем следует войти в каталог конкретного пользователя, например */test2@dmtestbfg.ru/.*

Внутри каталога пользователя расположена структура папок. Для доступа к письмам, ожидающим окончательного удаления, нужно перейти по пути */Recoverable/Deleted Items/cur/.* В этом каталоге находятся файлы, соответствующие каждому удалённому письму. Просмотреть их список можно стандартной командой *ls -la*.

Для восстановления письма или всех писем необходимо скопировать соответствующие файлы обратно в корзину первого уровня, то есть в каталог */Trash/cur/ (*полный путь и команда *cp -v * /mnt/deepmail/mail/пользователь@домен.ru/.Trash/cur/).* Копирование может быть выполнено как для всех файлов сразу, так и выборочно для конкретного сообщения. После завершения копирования критически важно восстановить корректные права доступа: владельцем всех скопированных файлов должен быть пользователь *mail,* а группой — *man*. Это достигается выполнением команды *chown* для каталога */Trash/cur/* или отдельных файлов.

В качестве проверки рекомендуется вывести список первых нескольких файлов в корзине первого уровня и убедиться, что права доступа установлены как 600, а владелец и группа соответствуют ожидаемым (*mail* и *man*). После этого письма становятся доступны пользователю в его стандартной корзине, и он может переместить их в любые другие папки (например, «Входящие» или «Отправленные») средствами своего почтового клиента.

Таким образом, двухуровневая корзина предоставляет администратору инструмент для надёжного восстановления данных при сохранении полного контроля над правами доступа и сроками хранения информации.

Для настройки ретрансляционных сетей, требуется на поле профиля SMTP (см. рисунок 36) нажать кнопку «Изменить» и в открывшемся окне настроить параметры «Ретрансляционных сетей» профиля SMTP (рисунок 38).

Рисунок 38 – Настройка «Ретрансляционных сетей»

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

Важно! IP-адреса указываются через запятую без пробелов.

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.

3.2.7 Почтовая очередь

Интерфейс управления почтовой очередью (рисунок 39) представляет собой панель мониторинга и управления очередью исходящей почты на указанном SMTP-сервисе.

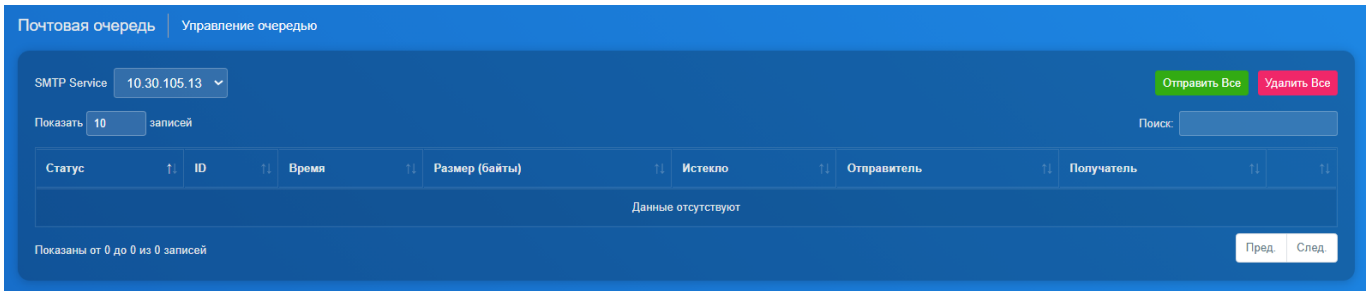


Рисунок 39 – Панель управления почтовой очередью

Основную часть окна занимает таблица, отображающая текущие письма, ожидающие отправки. Для каждого элемента очереди планируется показывать его уникальный идентификатор, время постановки, размер, статус (например, истекло ли время ожидания), адрес отправителя и получателя. В текущий момент очередь пуста, о чём сообщает запись «Данные отсутствуют».

Над таблицей расположены элементы управления для настройки отображения (количество записей на странице) и навигации между страницами. Под таблицей размещены кнопки для массовых операций: принудительная отправка всех писем в очереди и полная очистка очереди.

Таким образом, панель предоставляет администратору инструмент для визуального контроля почтового потока, ручного управления проблемными сообщениями и оперативного вмешательства в случае сбоев в работе SMTP-сервиса.

3.3 Инструмент «Лицензирование»

Для просмотра информации о лицензировании (количестве пользователей и сроке действия лицензий) необходимо в меню интерфейса администратора выбрать инструмент «Лицензирование» (рисунок 40).

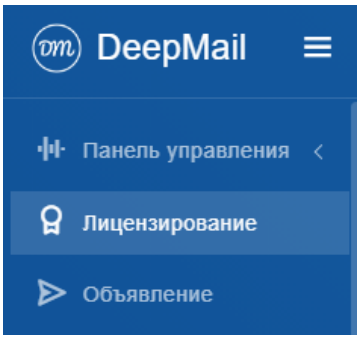


Рисунок 40 – Инструмент «Лицензирование»

В результате выбора на экране появится окно с детальной информацией о лицензировании (рисунок 41).

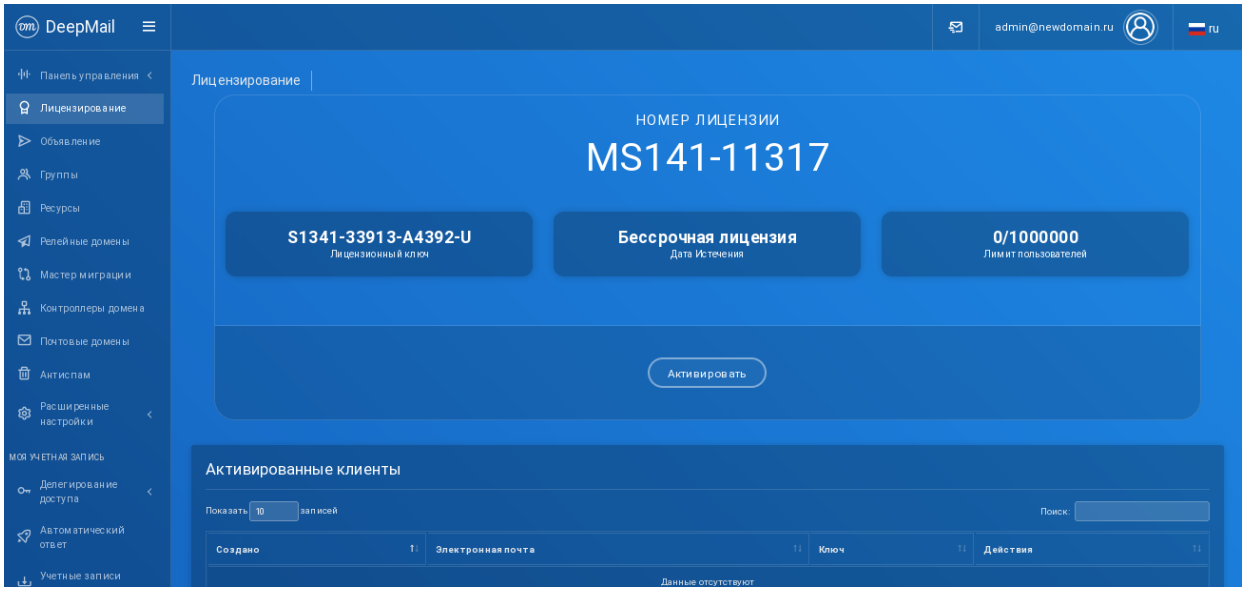


Рисунок 41 – Окно «Лицензирование»

3.3.1 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 42).

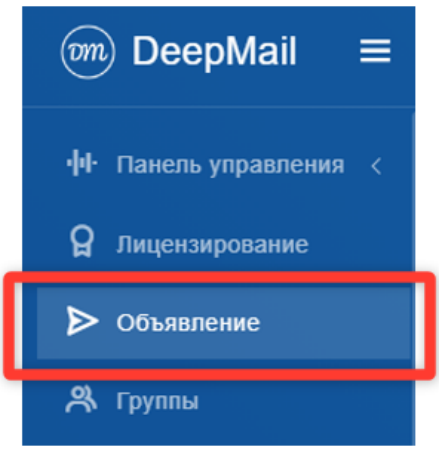


Рисунок 42 – Инструмент «Объявление»

Откроется окно для создания и отправки публичных объявлений (рисунок 43).

Рисунок 43 – Окно «Публичное объявление»

Для создания публичного объявления необходимо указать тему объявления, добавить содержание в соответствующие поля и нажать кнопку Отправить. В случае успешной рассылки объявления в окне появится сообщение Оповещение отправлено.

3.5 Инструмент «Группы»

Для перехода к инструменту «Группы» необходимо в меню интерфейса администратора выбрать «Группы» (рисунок 44).

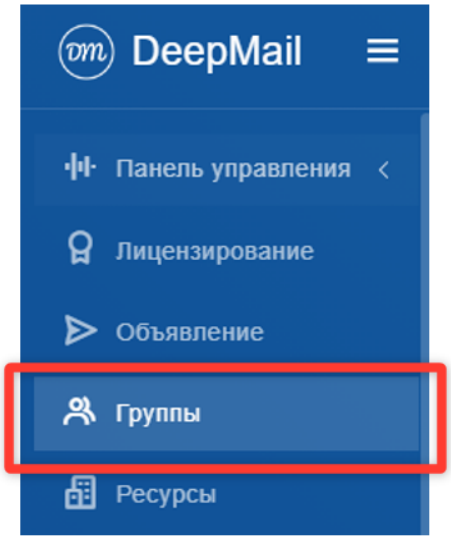


Рисунок 44 – Инструмент «Группы»

В результате выбора на экране появится окно «Группы», содержащее список групп пользователей всех почтовых доменов (рисунок 45).

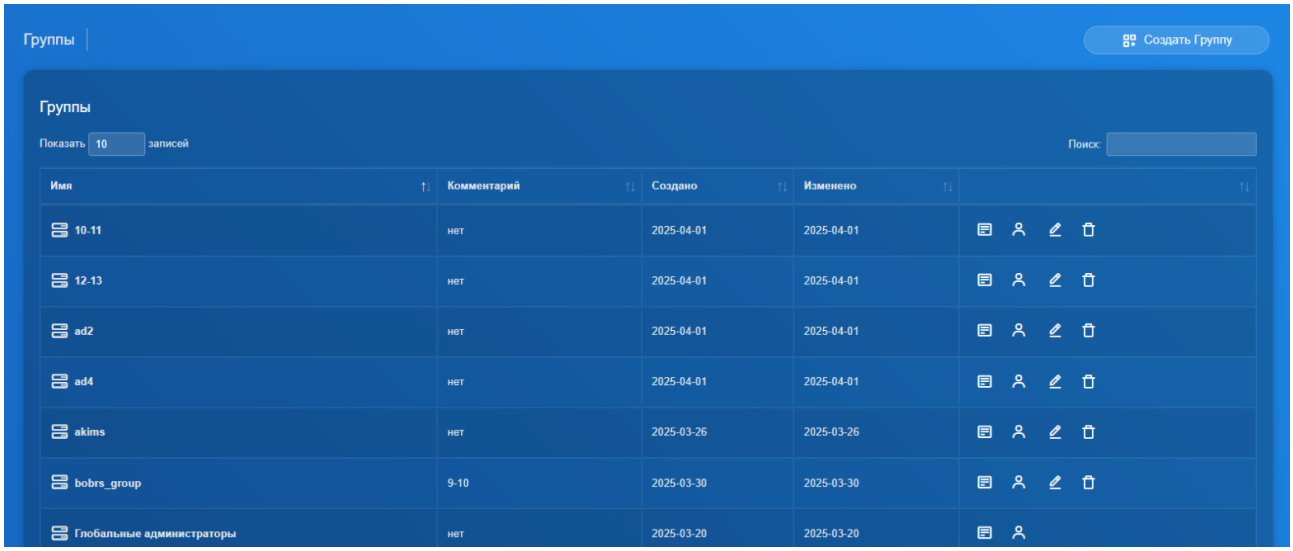


Рисунок 45 – Окно «Группы»

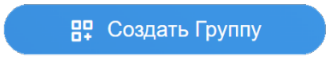
Инструмент «Группы» позволяет создавать, редактировать, удалять пользовательские группы, добавлять в группы и удалять из групп пользователей, а также назначать им различные права.

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 46).

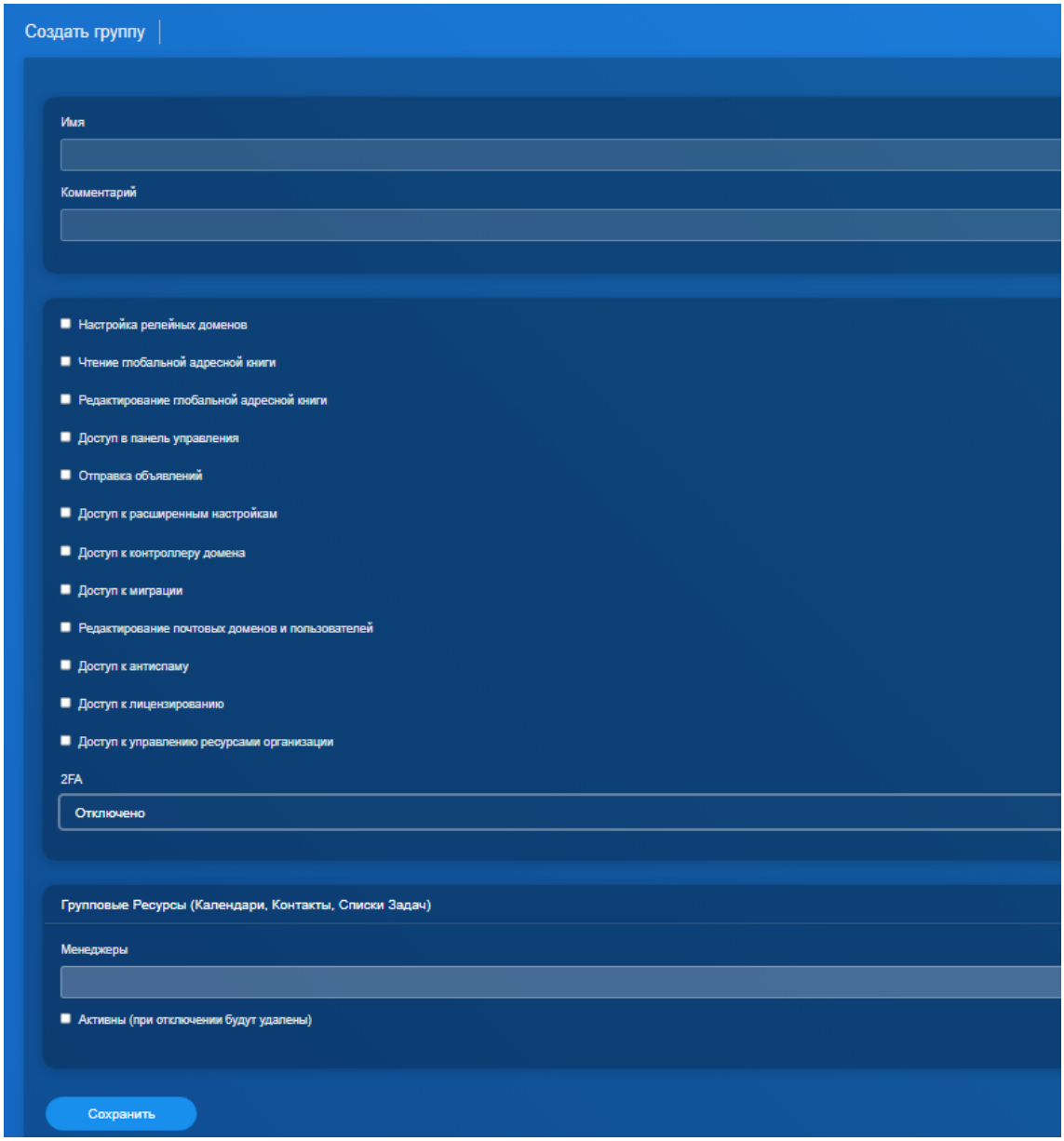


Рисунок 46 – Форма «Создать группу»

В форме «Создать группу» необходимо указать название группы, комментарий, назначить права участникам группы, отметив соответствующие чек-боксы, и нажать кнопку Сохранить (см. рисунок 46).

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.

Чтобы активировать 2FA администратору необходимо включить для пользователя соответствующую настройку в административной панели. При следующей попытке входа через клиентское приложение в системе будет сгенерирован и выведен на экран QR-код, содержащий уникальный 32-битный ключ (seed). Этот QR-код пользователю 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 считает ключ, оно начинает генерировать одноразовые коды, основанные на этом ключе и текущем времени. Полученный код пользователь вводит в окне запроса 2FA в клиентском приложении для завершения регистрации. Сервер проверяет код, и при успешной валидации пользователю выдается специальный токен (ключ подключения).

С этого момента при каждом входе в систему пользователь вводит не только логин и пароль, но и одноразовый код из приложения-аутентификатора. 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 функцией 2FA. 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 одноразовый код. 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 2FA доступно на уровне групповых настроек. Для включения 2FA группе пользователей необходимо перейти в настройки группы (см. рисунок 46) и отредактировать ее настройки.

В пункте включения/ отключения 2FA выбрать доступный механизм – TOTP (см. рисунок 47). Для всех пользователей группы будет включен механизм 2FA.

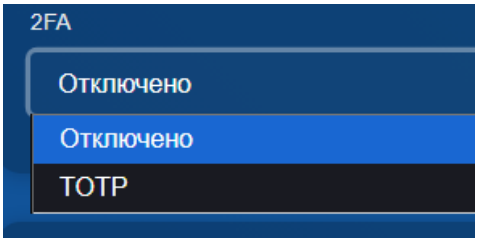


Рисунок 47 – Включение/отключение 2FA

После включения механизма 2FA, при ближайшей аутентификации пользователю из данной группы, будет выведен на экран одноразовый QR-код и предложено ввести код из приложения-аутентификатора (см. рисунок 48).

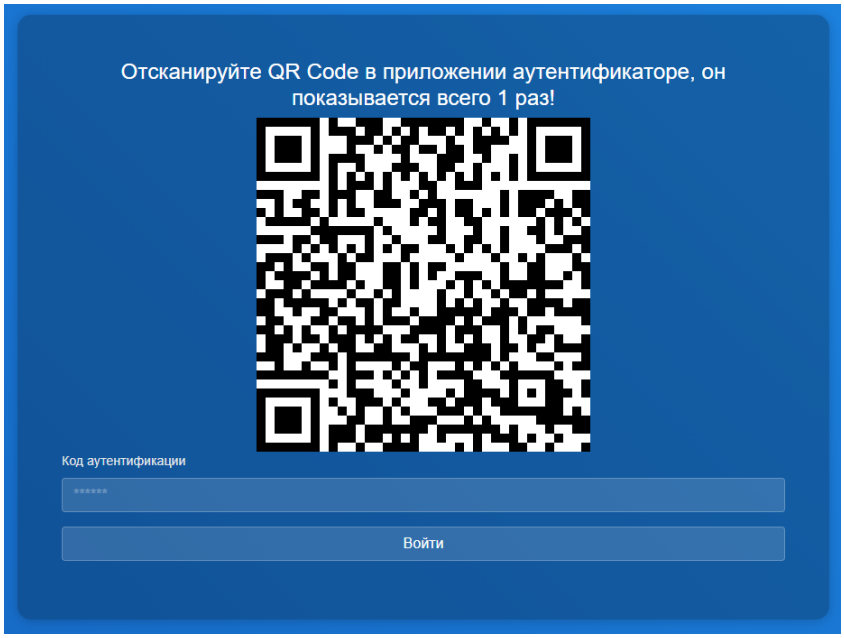


Рисунок 48 – Окно ввода кода из приложения-аутентификатора

Важно! QR-код показывается всего один раз! Если пользователь его не сохранит и закроет окно, администратору необходимо выполнить сброс 2FA в настройках конкретного пользователя и домена, нажав кнопку «Сбросить 2FA» (см. рисунок 49).

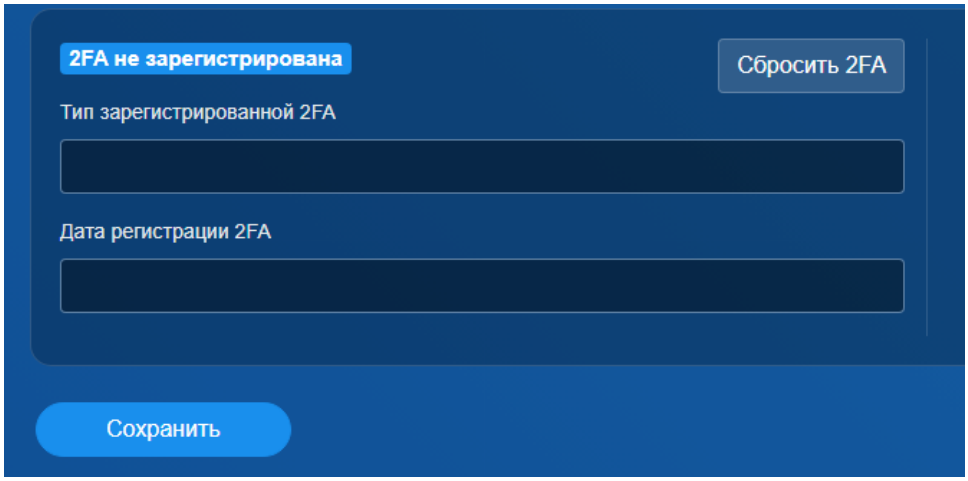


Рисунок 49 – Сброс 2FA

После успешного входа в настройках конкретного пользователя будет отображаться, что 2FA успешно зарегистрирована с фиксацией даты регистрации 2FA (см. рисунок 50).

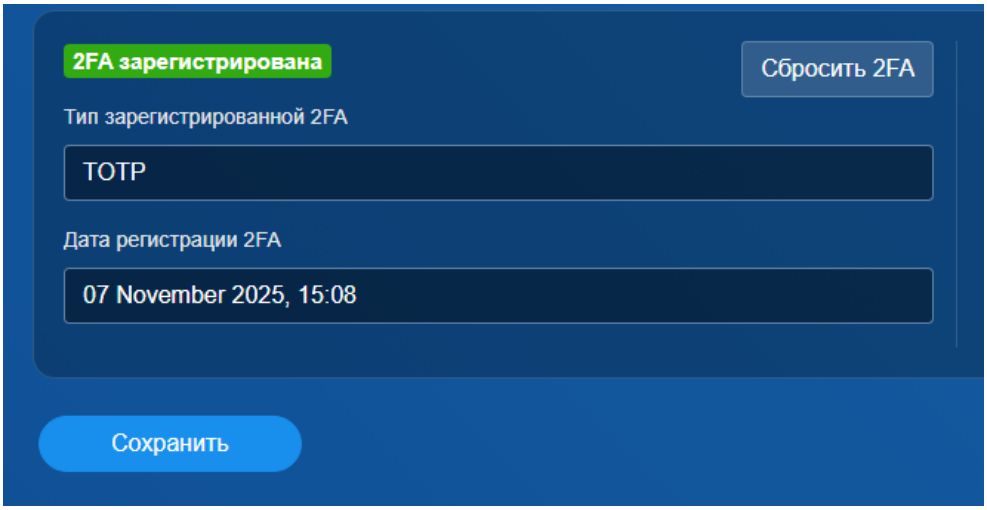


Рисунок 50 – 2FA зарегистрирована

3.5.3 Действия, выполняемые с группами

Для просмотра информации о группе необходимо в окне «Группы» нажать кнопку (см. рисунок 45). В результате откроется окно «Информация о группе» (рисунок 51).

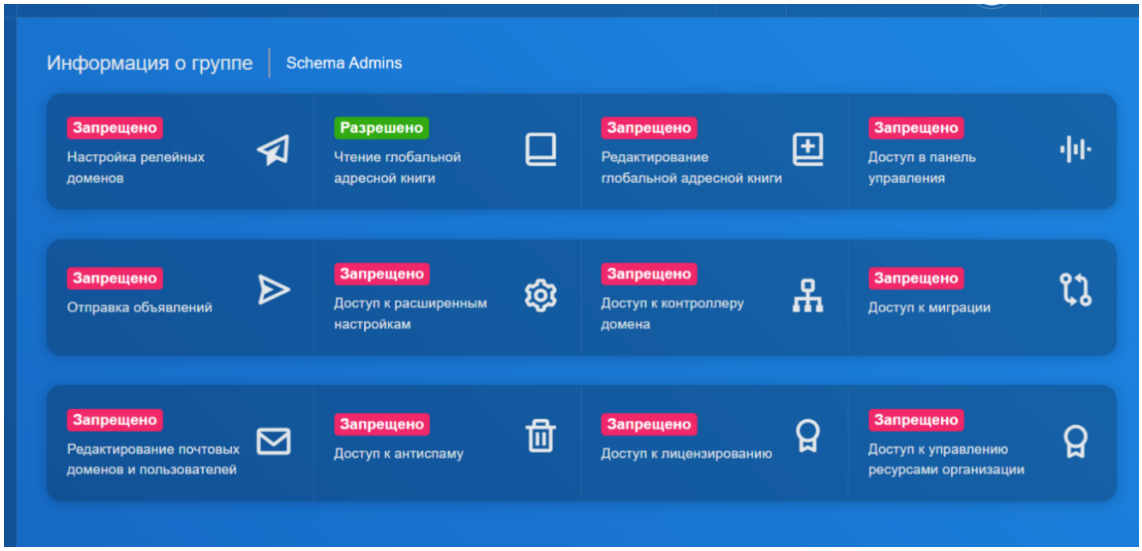


Рисунок 51 – Окно с информацией о группе

Для просмотра пользователей группы необходимо в окне «Группы» нажать кнопку  (см. рисунок 45). В результате откроется окно «Список пользователей в группе» (рисунок 52).

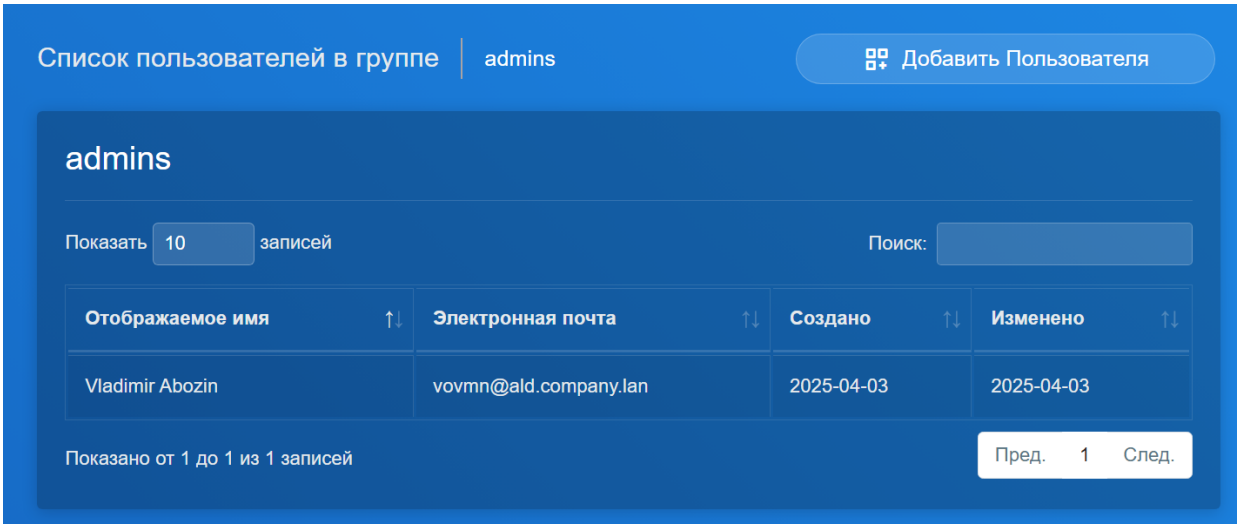
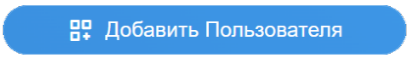


Рисунок 52 – Окно «Список пользователей в группе»

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 53).

Рисунок 53 – Форма «Добавить пользователя к группе»

Кнопка  в окне «Группы» (см. рисунок 45) предназначена для редактирования выбранной группы, например позволяет переназначить права группе и открывает форму настройки группы, аналогичную форме создания (см. рисунок 46).

Для удаления группы необходимо в окне «Группы» (см. рисунок 45) 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 54).

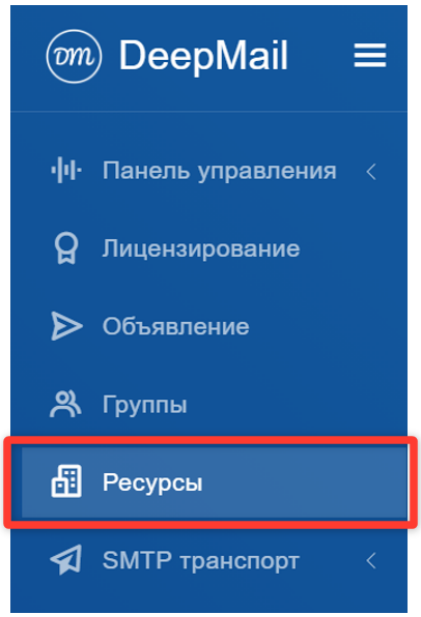


Рисунок 54 – Инструмент «Ресурсы»

Откроется окно «Список ресурсов» (рисунок 55).

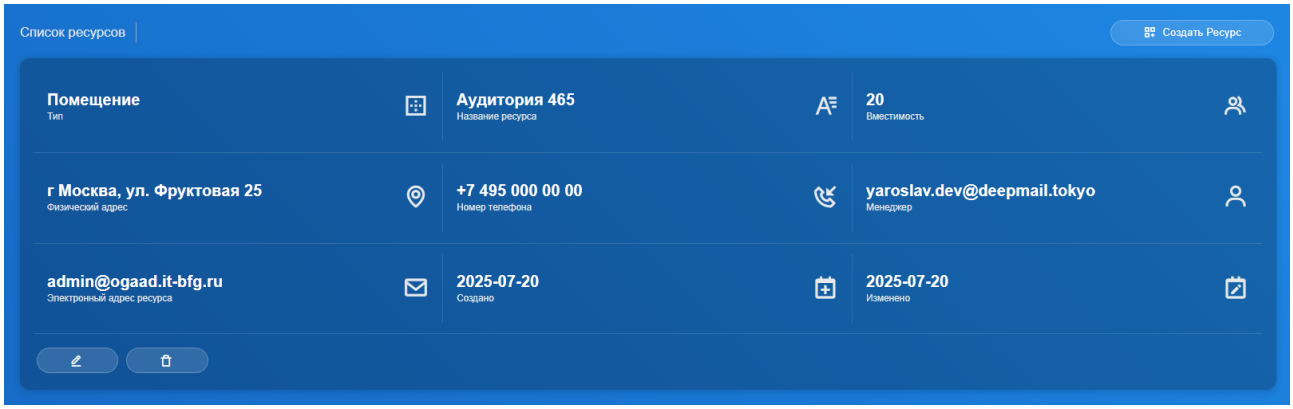


Рисунок 55 – Окно «Список ресурсов»

3.3.1 Активация лицензии

Для активации новой лицензии в окне «Лицензирование» (см. рисунок 41) необходимо нажать кнопку Активировать, ввести лицензионный ключ, полученный вместе с

дистрибутивом или напрямую от разработчика, и нажать кнопку 

. В случае успешной активации лицензии на экране появится окно с информацией о пройденной активации (см. рисунок 11).

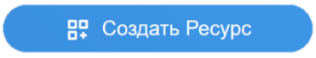
Примечание. Для получения лицензионного ключа в случае его отсутствия необходимо обратиться в СТП разработчика.

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 55).

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 56).

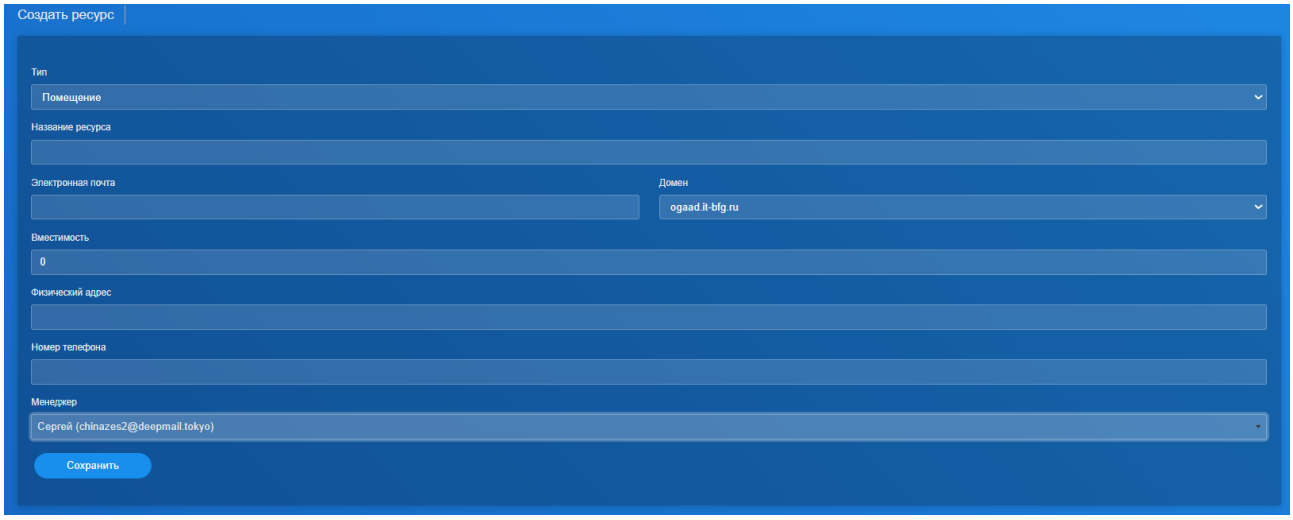


Рисунок 56 – Форма «Создать ресурс»

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 55), и внести изменения в появившуюся форму «Изменить ресурс» (рисунок 57).

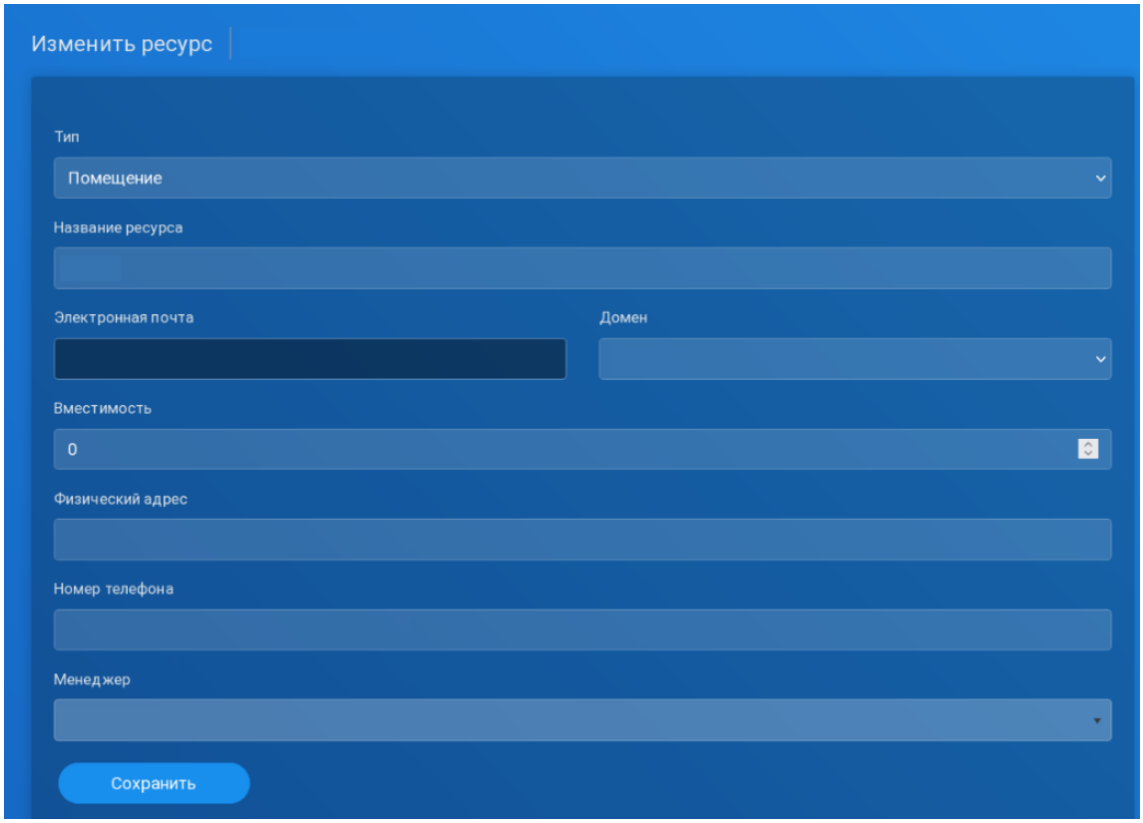


Рисунок 57 – Форма «Изменить ресурс»

3.6.3 Удаление ресурса

Для удаления ресурса необходимо нажать кнопку  (см. рисунок 55), и подтвердить удаление в открывшемся окне «Подтвердить действие».

3.7 Инструмент «SMTP транспорт»

Меню «SMTP транспорт» интерфейса администратора содержит два инструмента: «Релейные домены» (или «Реле»), «Транспортные правила», «Правила доступа по IP» и «Ограничение внешней отправки по IP»(рисунок 58).

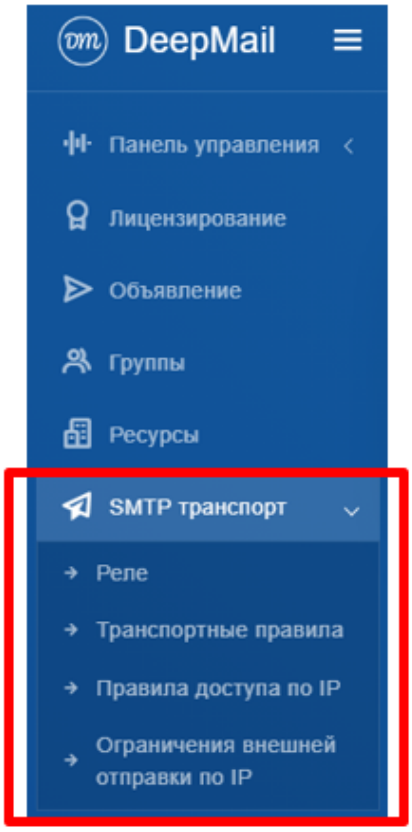


Рисунок 58 – Инструмент «Релейные домены»

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» (или «Реле»), выбрав его в меню интерфейса администратора (рисунок 59).

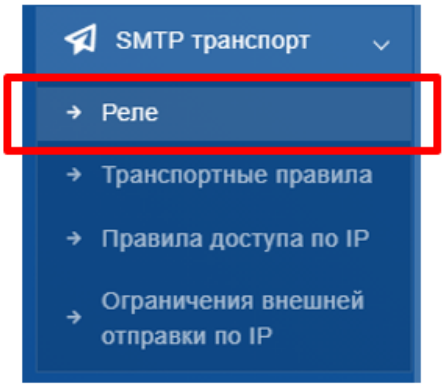


Рисунок 59 – Выбор инструмента «Релейные домены»

Окно «Список релейных доменов» содержит список настроенных релейных доменов (рисунок 60).

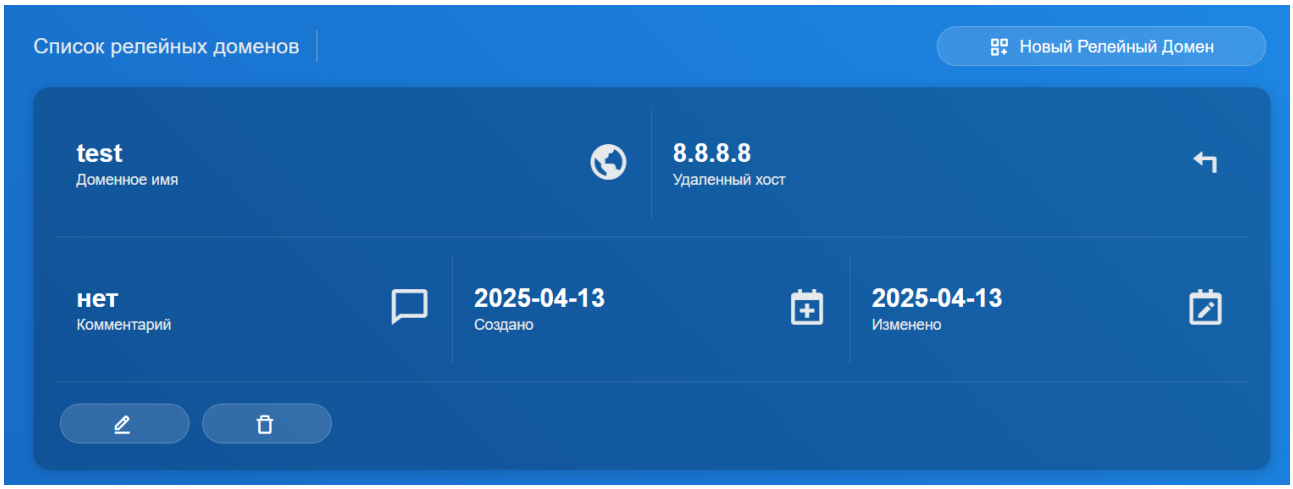
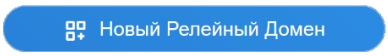


Рисунок 60 – Окно «Список релейных доменов»

3.7.1 Создание нового релейного домена

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

(см. рисунок 60).

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 61).

Рисунок 61 – Форма «Новый релейный домен»

Для завершения создания и сохранения параметров необходимо нажать кнопку Сохранить (см. рисунок 61).

Для того чтобы почта пересылалась через созданный сервер, необходимо в разделе бокового меню перейти в «Панель управления» → «Профили» (см. рисунок 36) 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 60). После этого откроется форма «Изменить релейный домен» (рисунок 62).

Рисунок 62 – Форма «Изменить релейный домен»

Внесите изменения в поля появившейся формы, и нажмите кнопку «Сохранить» (см. рисунок 62).

3.7.3 Удаление релейного домена

Для удаления релейного домена необходимо в окне со списком релейных доменов нажать кнопку  (см. рисунок 60) 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 63).

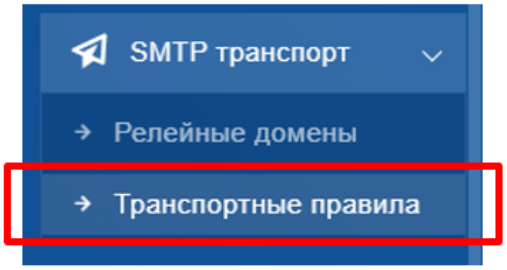


Рисунок 63 – Выбор инструмента «Транспортные правила»

Откроется окно «Транспортные правила», которое содержит список настроенных правил (рисунок 64).

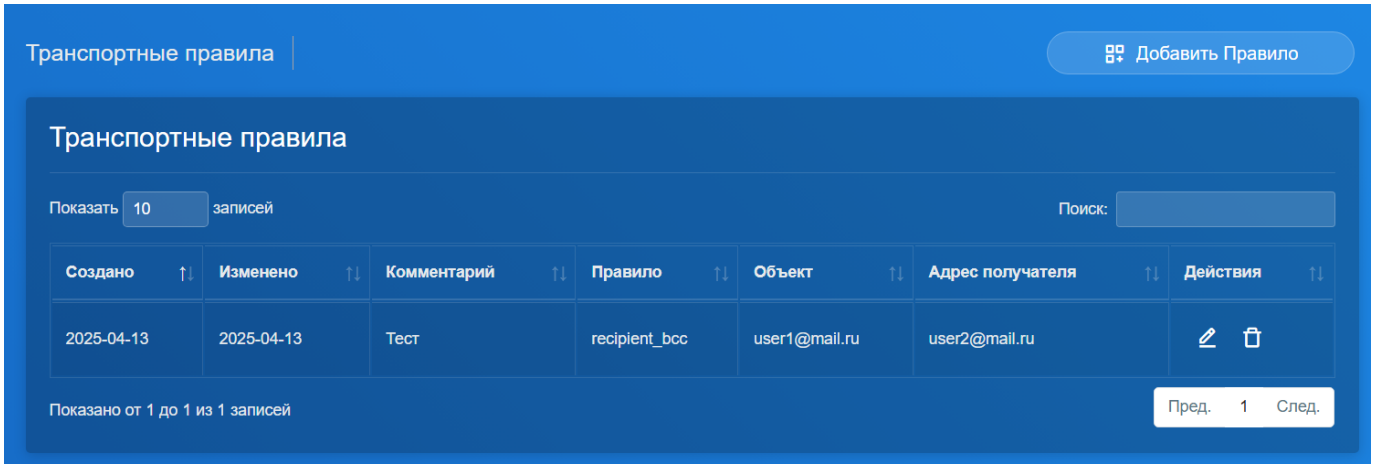


Рисунок 64 – Окно «Транспортные правила»

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 65).

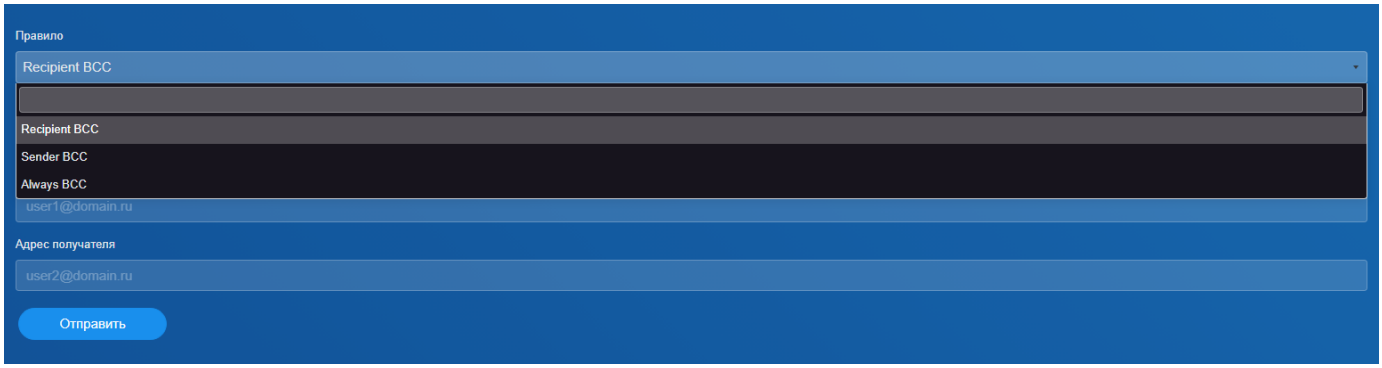


Рисунок 65 – Окно «Настройка транспортных правил»

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

Для создания правила обработки почтовых сообщений сразу для всех пользователей отдельного домена необходимо при создании правила в поле «Объект» указать этот домен в формате «@<доменное имя>» (например «@domain.ru»).

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 66.

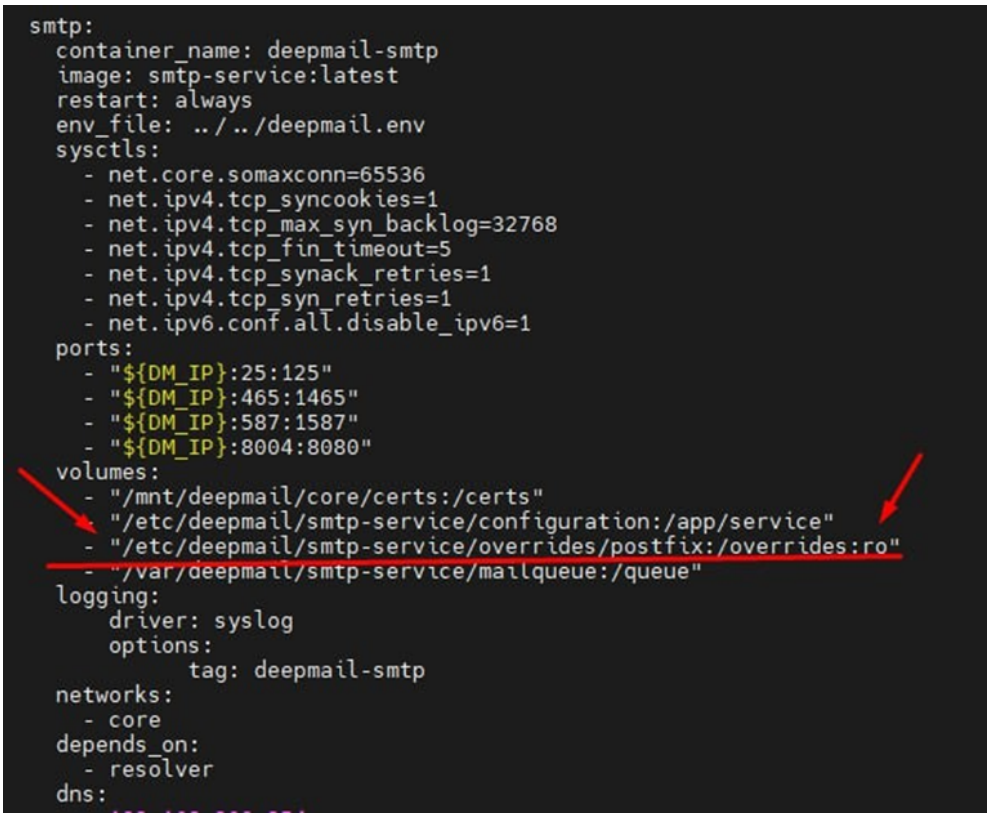


Рисунок 66 – Строчка для замены в конфигурационном файле

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

3.7.5 «Правила доступа по IP»

В разделе «Правила доступа по IP» администратору предоставляется инструмент для тонкой настройки обработки входящих почтовых соединений в зависимости от IP-адреса отправителя. Здесь можно задать, как сервер будет реагировать на почту, поступающую с определённых адресов, и таким образом реализовать гибкую политику безопасности, фильтрации или перенаправления трафика (рисунок 67).

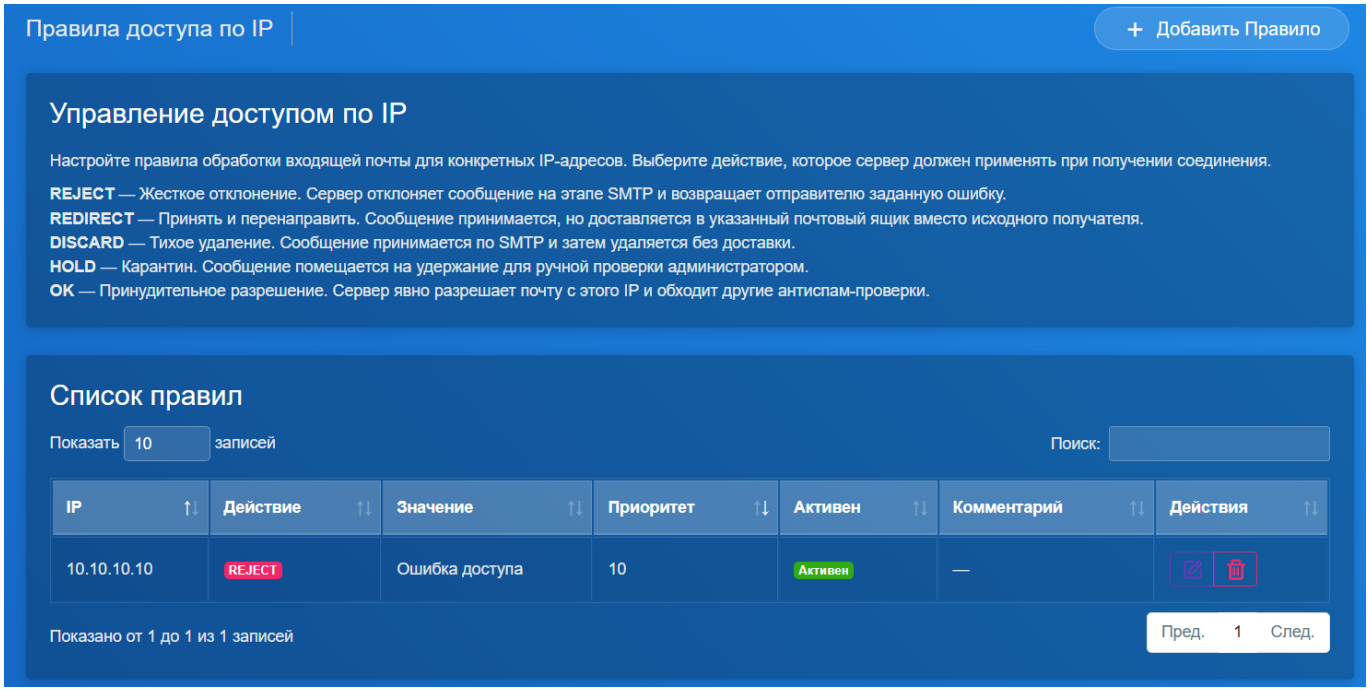


Рисунок 67 – Окно «Управление доступом по IP»

Интерфейс позволяет создавать правила, каждое из которых связывает IP-адрес (или подсеть) с одним из предопределённых действий. Доступны следующие варианты действий:

- REJECT (жесткое отклонение) — сервер сразу отказывает в приёме сообщения на этапе SMTP-рукопожатия и возвращает отправителю заданную ошибку. Используется для блокировки нежелательных источников;

- REDIRECT (перенаправление) — письмо принимается, но вместо исходного получателя доставляется в указанный почтовый ящик. Полезно для централизованного сбора почты с определённых адресов;

- DISCARD (тихое удаление) — сообщение принимается по протоколу SMTP, но затем бесследно удаляется без уведомления отправителя. Применяется для «чёрных дыр» без возврата ошибки;

- HOLD (карантин) — письмо помещается на удержание, после чего администратор может вручную проверить его и принять решение о доставке или удалении;

- OK (принудительное разрешение) — сервер явно разрешает почту с этого IP, обходя любые антиспам-антивирусные проверки. Используется для доверенных источников, чтобы гарантировать доставку.

Для каждого правила можно указать приоритет — чем меньше число, тем выше приоритет. Это позволяет строить цепочки правил: сначала обрабатываются более приоритетные, затем — остальные. Также правило можно временно отключить, сняв флаг «Активен», не удаляя его из списка.

В таблице правил отображаются созданные записи: IP-адрес (или подсеть), выбранное действие, значение (например, текст ошибки для REJECT или целевой адрес для REDIRECT), приоритет, статус активности, комментарий. Для каждого правила доступны действия редактирования (иконка «Продолжить»).

Управление доступом по IP позволяет администратору гибко реагировать на угрозы, доверять определённым отправителям, автоматически перенаправлять почту с критических систем или помещать подозрительный трафик в карантин для последующего анализа. Все изменения применяются к SMTP-сервису в реальном времени.

3.7.6 «Ограничение внешней отправки по IP»

Раздел «Ограничения внешней отправки по IP» предназначен для управления исходящим почтовым трафиком на уровне отдельных IP-адресов. Администратор может задать перечень IP-адресов, с которых разрешена отправка только локальным получателям (внутри почтовой системы), а отправка на внешние домены (за пределы организации) будет запрещена. Это полезно для ограничения сетевых устройств, которые не должны отправлять письма за пределы организации, или для предотвращения возможных компрометаций (рисунок 68).

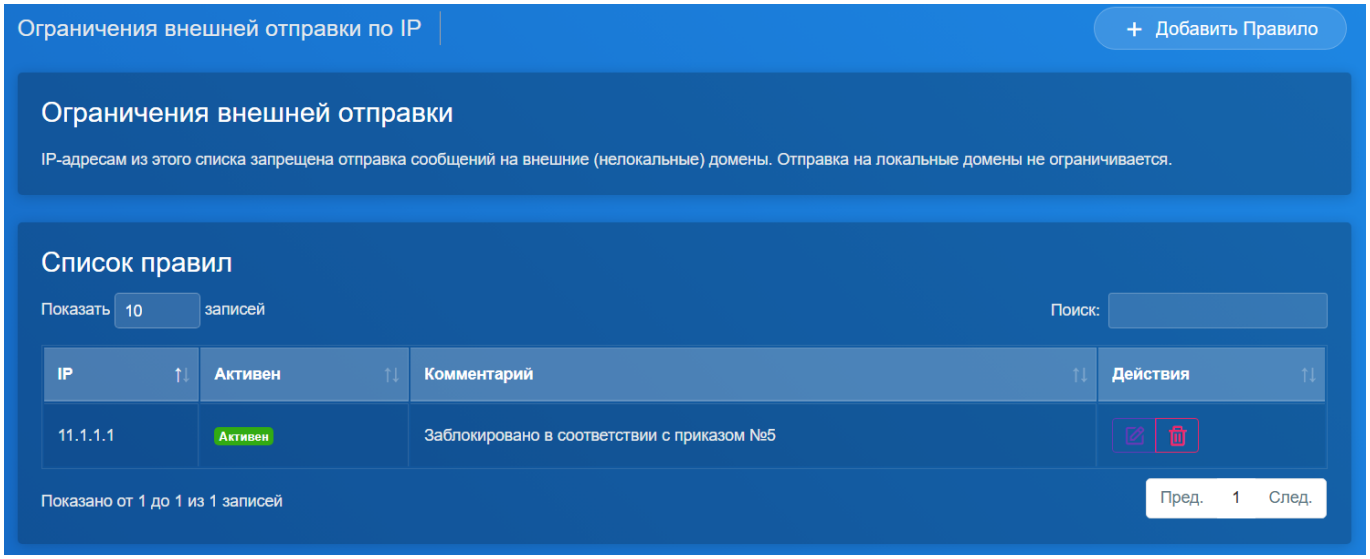


Рисунок 68 – Окно «Ограничение внешней отправки по IP»

Принцип работы следующий: если отправитель (IP-адрес, с которого установлено SMTP-соединение) попадает в список, то при попытке отправить письмо на адрес, не принадлежащий ни одному из обслуживаемых доменов DeepMail, сервер возвращает ошибку. Отправка на локальные адреса (почтовые ящики внутри системы) продолжает работать без ограничений.

В интерфейсе администратора представлена таблица, содержащая IP-адреса (можно указывать как одиночные адреса, так и подсети), статус активности (Активен/Неактивен) и комментарий. Для каждого IP предусмотрены действия по редактированию и удалению. Новые записи добавляются через соответствующую кнопку над таблицей.

При создании правила необходимо указать IP-адрес (или подсеть) и при желании добавить комментарий, поясняющий причину блокировки. Правило можно временно отключить, не удаляя, с помощью переключателя «Активен». Поиск по списку позволяет быстро находить нужные записи.

Таким образом, администратор может гибко управлять правами на внешнюю отправку, усиливая безопасность почтовой инфраструктуры.

3.8 Инструмент «Мастер миграции»

Настройка миграции доменных данных (необходима, например, при переходе с другой почтовой системы) осуществляется при помощи инструмента «Мастер миграции».

Для перехода к инструменту необходимо в меню интерфейса администратора выбрать «Мастер миграции» (рисунок 69).

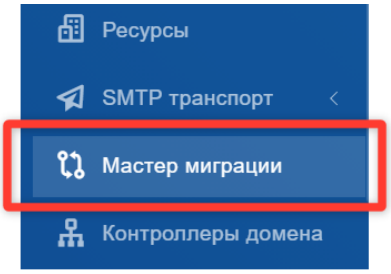


Рисунок 69 – Инструмент «Мастер миграции»

Окно «Мастер миграции» в панели управления DeepMail представляет собой инструмент для переноса почтовых данных пользователей с внешних систем на сервер DeepMail. Интерфейс предлагает выбор между двумя режимами миграции в зависимости от типа исходной почтовой инфраструктуры.

Режим EWS ориентирован на работу с Microsoft Exchange и использует протокол Exchange Web Services, обеспечивая предварительную проверку подключения, автоматическое обнаружение настроек и перенос не только писем, но также календарей, контактов и задач. Этот режим максимально автоматизирован и подходит для современных развёртываний Exchange.

Режим IMAP является классическим и предназначен для миграции с любых почтовых серверов, поддерживающих протокол IMAP. Он включает проверку соединения и настройку параметров подключения, что делает его универсальным решением для переноса данных с устаревших систем или сторонних почтовых платформ.

Администратор выбирает подходящий режим на стартовом экране, после чего открывается соответствующий мастер, ведущий пошагово через процесс настройки, проверки и выполнения миграции. Такой подход позволяет гибко адаптироваться к различным источникам данных и минимизировать ручное вмешательство при переносе пользователей. (рисунок 70).

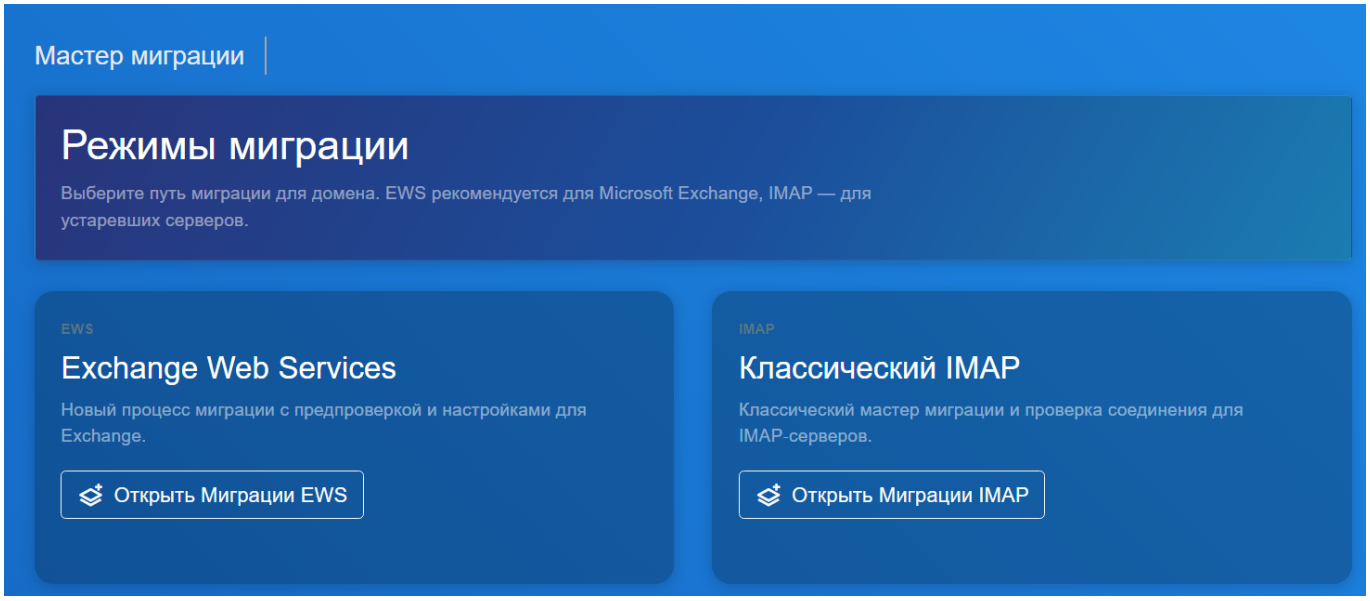


Рисунок 70 – Окно «Мастер миграции»

3.8.1 Инструмент мастер миграции Exchange Web Services

Окно мастера миграции в режиме EWS представляет собой панель управления профилями переноса данных для почтовых доменов. В центральной части отображается список созданных профилей, где для каждого указано имя домена, адрес Exchange-сервера (хост), а также доступны действия для управления профилем: изменение параметров, удаление или переход к списку пользователей для настройки миграции. Дополнительно предусмотрена кнопка добавления нового домена, позволяющая расширить список профилей для последующего переноса почтовых ящиков. Интерфейс позволяет администратору централизованно управлять всеми настройками миграции, выполнять предварительную проверку подключения и контролировать процесс переноса данных (см. рисунок 71).

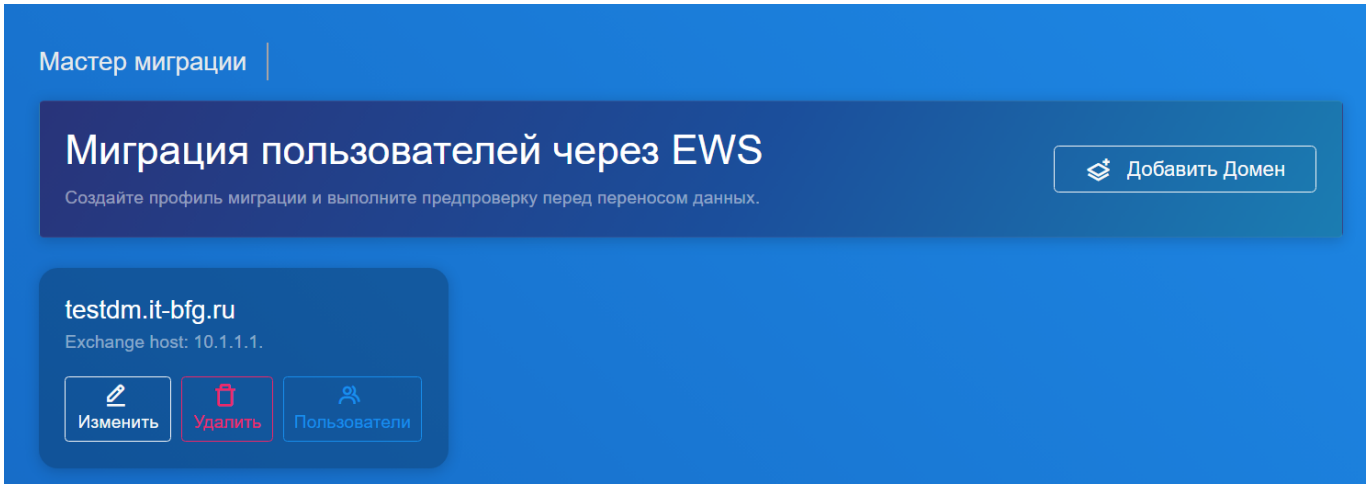


Рисунок 71 – Окно «Мастер миграции» EWS

3.8.1.1 Создание настроек миграции и подключение к EWS-серверу

Для добавления домена, с которого требуется перенести данные, необходимо в окне мастера миграции нажать кнопку «Добавить домен» (см. рисунок 71), после чего откроется окно создания профиля миграции (см. рисунок 72).

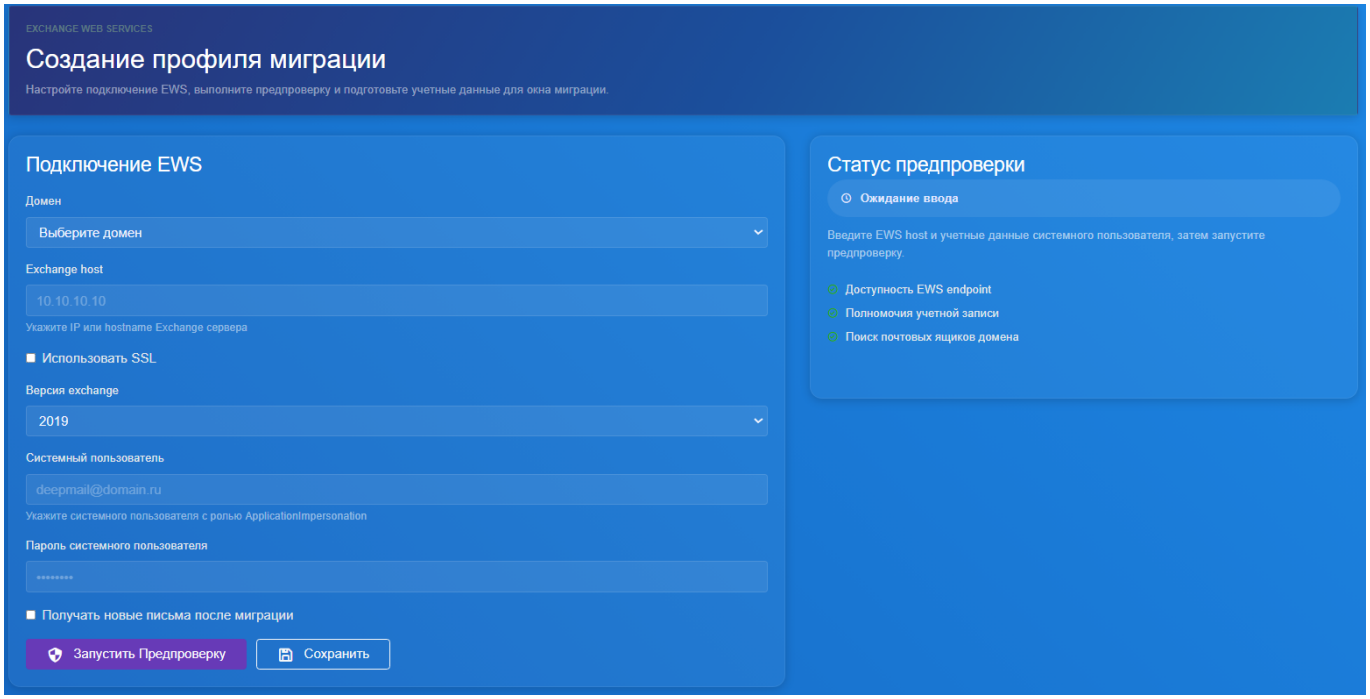


Рисунок 72 – Окно «Создание профиля миграции» EWS

Форма создания профиля миграции через протокол EWS (Exchange Web Services) представляет собой детализированный интерфейс, в котором администратору необходимо последовательно задать параметры подключения к исходному серверу Microsoft Exchange, а затем инициировать предварительную проверку, гарантирующую корректность всех настроек перед запуском переноса данных (нажать на кнопку «Запустить Предпроверку» после заполнения всех полей).

В верхней части окна расположен блок «Подключение EWS», объединяющий все параметры связи с Exchange-сервером. Поле «Домен» представляет собой выпадающий список, в котором выбирается целевой почтовый домен DeepMail, для которого будут переноситься почтовые ящики. Это связывает создаваемый профиль миграции с конкретным доменом назначения, определяя, в какую структуру будут импортированы почтовые данные.

Далее указывается Exchange host — IP-адрес или полное доменное имя сервера Exchange. Это обязательный параметр, по которому мастер миграции будет устанавливать соединение. Рядом расположен флажок «Использовать SSL»: его активация включает шифрование трафика между DeepMail и Exchange по протоколу HTTPS, что рекомендуется для безопасной передачи учётных данных и содержимого почтовых ящиков.

Ниже находится выпадающий список «Версия exchange», где администратор может выбрать версию Exchange, используемую в организации. Выбор версии (например, 2019) влияет на способ формирования EWS-запросов и обеспечивает совместимость с различными выпусками сервера. Если версия не указана явно, система может попытаться определить её автоматически, но явный выбор повышает надёжность.

Ключевым элементом настройки является блок «Системный пользователь». Для миграции требуется учётная запись, обладающая правами ApplicationImpersonation, что позволяет серверу DeepMail действовать от имени любого пользователя в целевом домене. В поле «Системный пользователь» вводится адрес электронной почты этой учётной записи (например, migration@domain.ru), а в поле «Пароль системного пользователя» – его пароль. Без корректных учётных данных мастер не сможет получить доступ к почтовым ящикам пользователей.

Чекбокс «Получить новые письма после миграции» управляет поведением системы в отношении сообщений, которые могут поступить на Exchange в процессе переноса. Если флажок установлен, после завершения миграции будет выполнен повторный проход для подхвата писем, пришедших за время работы мастера. Это помогает минимизировать потерю данных при организации непрерывной работы почты.

Под полями ввода расположены две кнопки: «Запустить Предпроверку» и «Сохранить». Предпроверка должна быть выполнена первой: она проверяет доступность EWS-сервиса, корректность учётных данных и возможность обнаружения почтовых ящиков указанного домена. Только после успешного завершения предпроверки имеет смысл сохранять профиль и переходить к управлению списком пользователей.

Справа или снизу от блока подключения находится панель «Статус предпроверки», где динамически отображается ход выполнения проверок. В исходном состоянии каждый пункт помечен как «Ожидание ввода». После нажатия кнопки «Запустить Предпроверку» система последовательно выполняет три основных теста:

- Доступность EWS endpoint – проверка, отвечает ли указанный Exchange host на запросы по протоколу EWS;

- Полномочия учетной записи – подтверждение того, что введённые логин и пароль корректны, а учётная запись имеет необходимые права ApplicationImpersonation;

- Поиск почтовых ящиков домена – попытка получить список почтовых ящиков в указанном домене, что служит финальным подтверждением готовности к миграции.

Каждый этап может завершиться успехом (зелёная отметка) или ошибкой (красный крест). Только после прохождения всех трёх этапов администратор получает уверенность, что профиль настроен верно, и может сохранить его, а затем перейти к выбору пользователей для миграции.

Таким образом, интерфейс мастера миграции через EWS реализует продуманную пошаговую логику: от выбора домена и сервера через настройку прав доступа к автоматизированной проверке подключения. Это позволяет администратору контролировать каждый этап настройки и избежать ошибок, которые могли бы привести к сбоям при массовом переносе почтовых данных.

3.8.1.2 Запуск миграции EWS-сервера

Чтобы запустить миграцию для выбранного домена необходимо в окне мастера миграции нажать кнопку «Пользователи» (см. рисунок 71), и в открывшейся форме сделать необходимые настройки (см. рисунок 73).

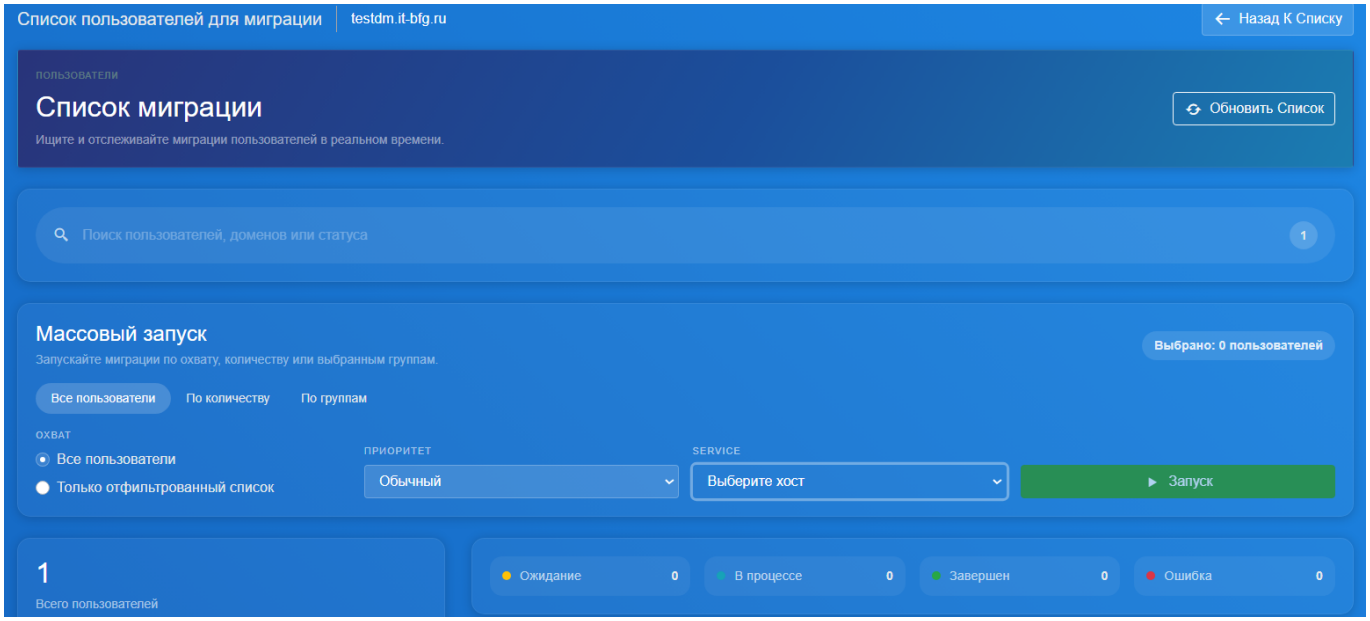


Рисунок 73 – Окно «Запуск миграции» EWS

Интерфейс «Список пользователей для миграции» открывается после того, как администратор создал профиль миграции для домена, и предназначен для управления переносом почтовых ящиков с Exchange-сервера на DeepMail. В верхней части экрана всегда

отображается имя домена, к которому относится текущая миграция, чтобы администратор чётко понимал, с какими учётными записями работает.

В центральной области находится панель управления списком, включающая кнопку «Обновить Список», с помощью которой можно в любой момент подгрузить актуальные данные из Exchange – например, если на исходном сервере появились новые почтовые ящики или изменились статусы уже существующих. Рядом расположена поисковая строка, позволяющая динамически фильтровать пользователей по имени, адресу электронной почты или текущему статусу миграции; это особенно полезно при работе с большим количеством ящиков.

Ключевым элементом интерфейса является блок массового запуска, где администратор задаёт параметры для переноса данных. Вначале выбирается охват: можно запустить миграцию для всех пользователей домена, которые ещё не были перенесены или находятся в состоянии ожидания, либо только для тех ящиков, которые отображаются после применения поискового фильтра – это удобно, когда требуется перенести конкретную группу адресатов. Далее устанавливается приоритет выполнения (например, «Обычный» или «Высокий»), который влияет на порядок обработки очереди: ящики с более высоким приоритетом будут мигрировать раньше. Также необходимо указать узел (хост) DeepMail, на котором будет выполняться перенос, – в распределённой среде администратор может направить нагрузку на определённый сервер, выбрав его из выпадающего списка. Завершается настройка нажатием кнопки «Запуск», после чего система начинает перенос данных, а статусы пользователей в списке начинают обновляться.

Справа от блока управления отображается общее количество пользователей домена и четыре цветных индикатора с подписями «Ожидание», «В процессе», «Завершен» и «Ошибка»». Каждый индикатор показывает число ящиков в соответствующем состоянии, а щелчок по нему фильтрует список, оставляя только тех пользователей, чей статус совпадает с выбранным. Таблица пользователей, расположенная ниже, содержит для каждого ящика адрес электронной почты, текущий статус миграции и доступные действия (запустить миграцию для одного пользователя, посмотреть детали ошибки, отменить операцию).

Работа с интерфейсом строится по простой последовательности. После создания профиля миграции система автоматически извлекает из Exchange список почтовых ящиков домена; администратору достаточно убедиться, что все нужные ящики присутствуют, при необходимости обновив список кнопкой «Обновить Список». Если требуется перенести не всех сразу, применяется поиск или фильтр по статусу, а в блоке массового запуска

выбирается охват «Только отфильтрованный список». Затем задаётся приоритет и хост, после чего нажатием «Запуск» отправляется задача. Статусы ящиков последовательно переходят из «Ожидание» в «В процессе», а затем в «Завершен» или «Ошибка». В случае ошибки администратор может просмотреть детали (например, неверные учётные данные, недоступность EWS, превышение квоты) и принять меры. Если перенос завершился с ошибкой или на Exchange были внесены изменения, миграцию можно запустить повторно для тех же ящиков; система обновит данные, не дублируя уже перенесённые письма, благодаря поддержке инкрементального переноса.

Таким образом, интерфейс предоставляет все необходимые инструменты для централизованного и гибкого управления процессом миграции. Массовый запуск с настройкой охвата и приоритета позволяет эффективно планировать нагрузку, а наглядные индикаторы статусов дают возможность контролировать ход переноса в реальном времени, сокращая время перехода на DeepMail и снижая риск ошибок.

3.8.1.3 Удаление настроек миграции и подключение к EWS-серверу

Чтобы удалить настройки миграции для выбранного домена необходимо в окне мастера миграции нажать кнопку «Удалить» (см. рисунок 71), и в открывшейся форме «Подтвердить действие» подтвердить удаление.

Важно! Не выполняйте удаление настроек мастера миграции, до момента, когда будет закончена миграция всех данных выбранного домена и будет осуществлено отключение от старой почтовой системы. При миграции к мигрированным учетным записям применяются специальные настройки, в случае удаления настроек мастера миграции, такие настройки необходимо будет выполнять в ручном режиме для каждой учетной записи, либо проводить повторную миграцию пользователей.

3.8.2 Инструмент мастер миграции классический IMAP

Окно «Мастер миграции» содержит список сторонних доменов, подключенных к серверу АРМ «DeepMail» (рисунок 74).

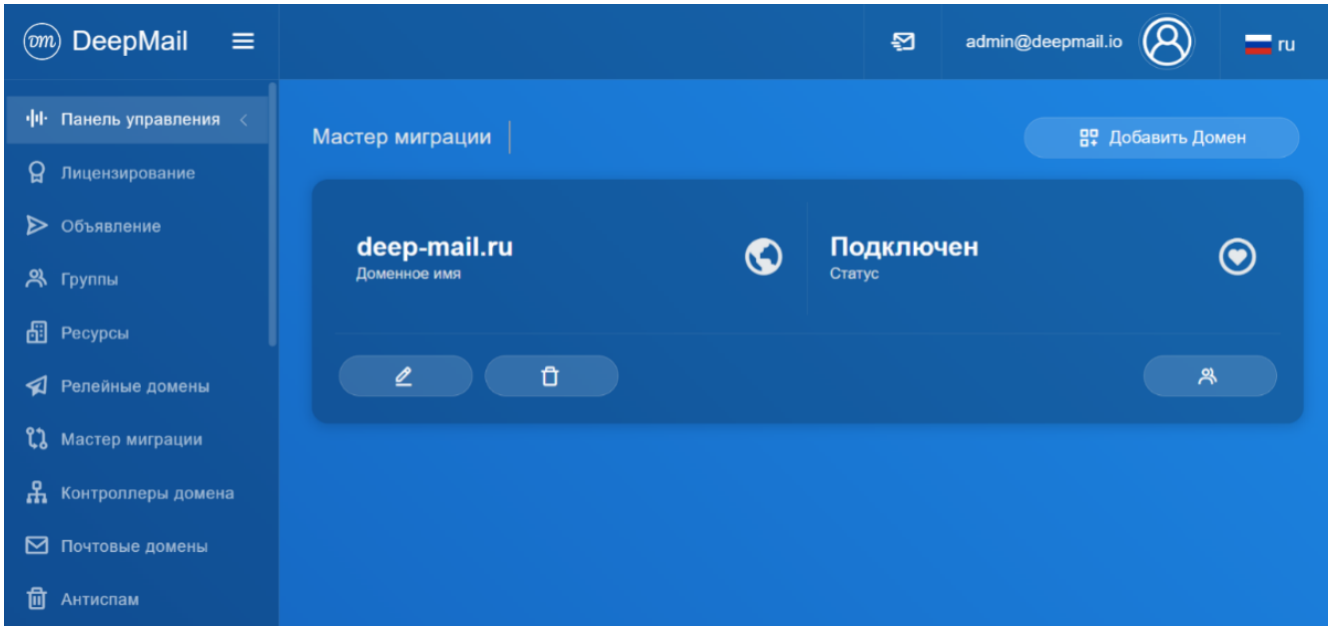


Рисунок 74 – Окно «Мастер миграции» IMAP

Для изменения настроек миграции необходимо на панели домена нажать кнопку  (см. рисунок 74). 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 74). В результате на экране отобразится форма «Список пользователей для миграции» (рисунок 75).

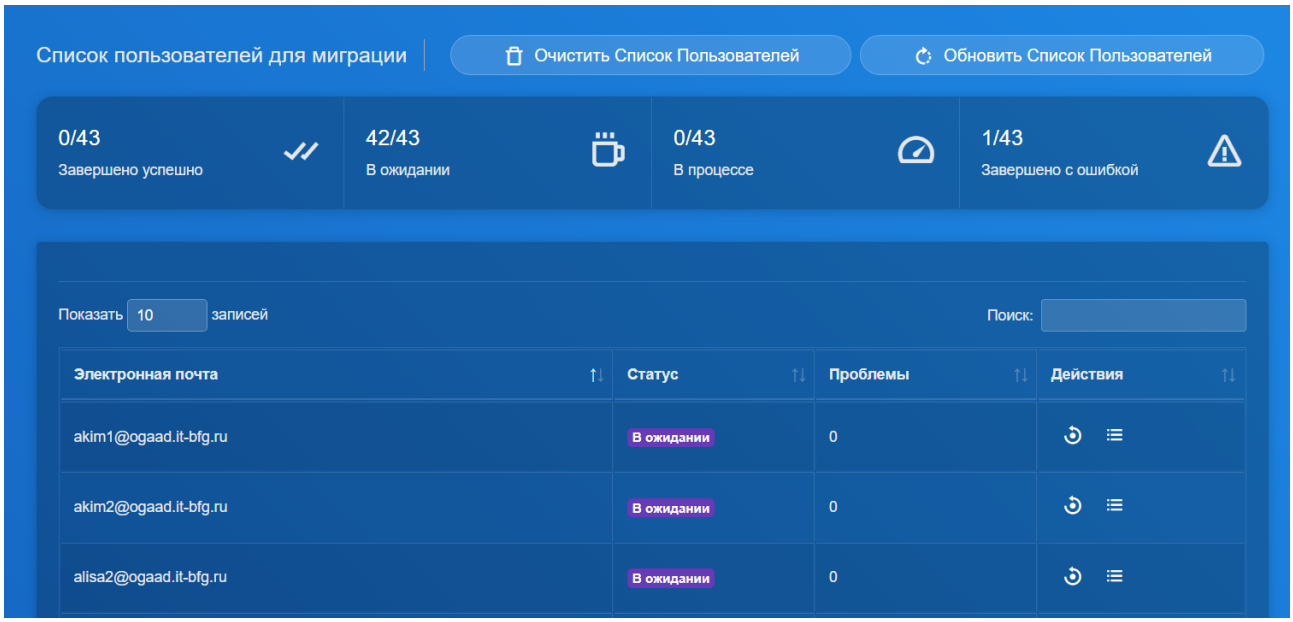


Рисунок 75 – Список для миграции

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 76).

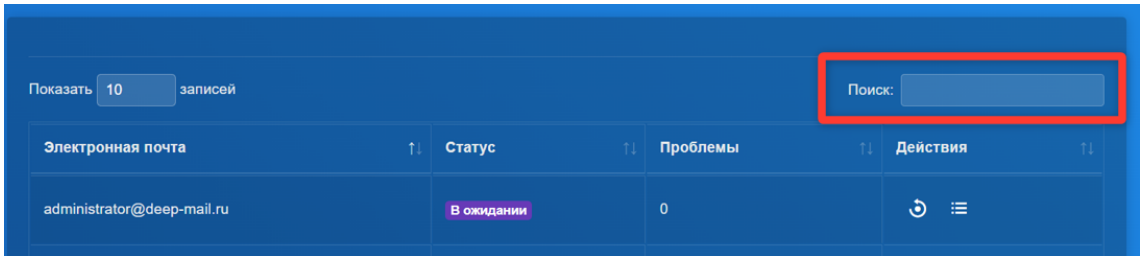


Рисунок 76 – Поле «Поиск:»

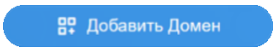
Обновить информацию о статусе миграции можно с помощью кнопки 

, расположенной над списком пользователей (см. рисунок 75).

Удалить пользователей из списка можно с помощью кнопки 

(см. рисунок 75).

3.8.2.1 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 70) и затем подтвердить готовность нажав «Продолжить» (рисунок 77).

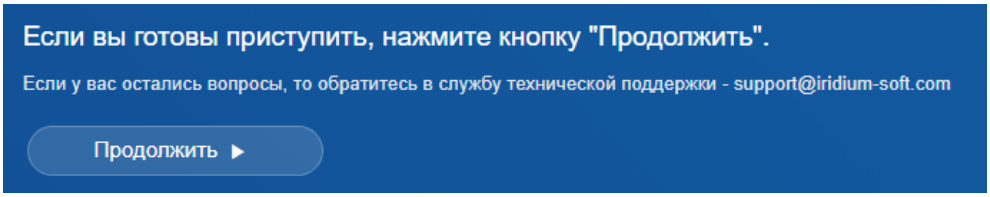


Рисунок 77 – Начало настройки миграции. Кнопка «Продолжить»

В окне появится форма настройки миграции на первом шаге «Базовые настройки» (рисунок 78).

Рисунок 78 – 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 79).

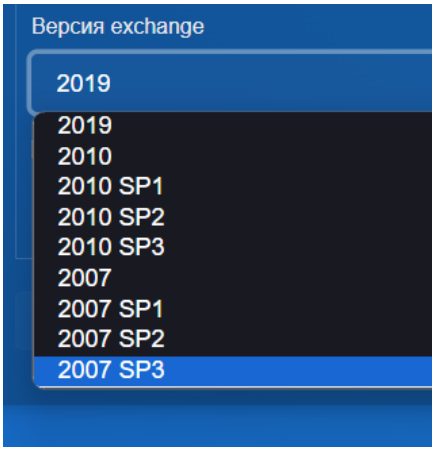


Рисунок 79 – Выбор версии сервера MS Exchange

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 78).

На шаге «IMAP» необходимо указать IP-адрес удаленного IMAP-сервера и порт подключения (рисунок 80).

Рисунок 80 – 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 81).

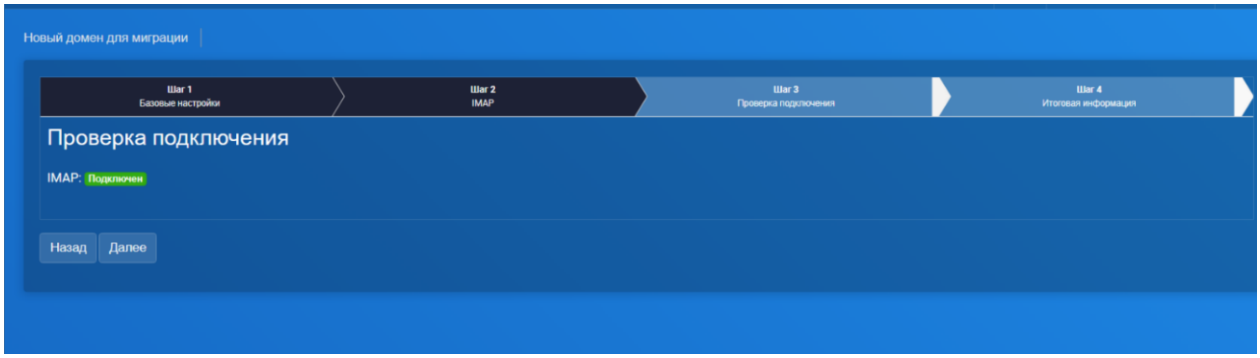
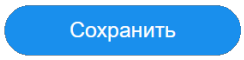


Рисунок 81 – Проверка подключения к IMAP-серверу

На шаге «Итоговая информация» будет отображена информация с числом пользователей для миграции (рисунок 82).

Рисунок 82 – Настройка миграции. Шаг «Итоговая информация»

Для сохранения настроек нажмите кнопку 

(см. рисунок 82).

3.8.2.2 Удаление настроек миграции для домена

Чтобы удалить настройки миграции для выбранного домена необходимо в окне мастера миграции нажать кнопку  (см. рисунок 74), и в открывшейся форме «Подтвердить действие» подтвердить удаление.

Важно! Не выполняйте удаление настроек мастера миграции, до момента, когда будет закончена миграция всех данных выбранного домена и будет осуществлено отключение от старой почтовой системы. При миграции к мигрированным учетным записям применяются специальные настройки, в случае удаления настроек мастера миграции, такие настройки необходимо будет выполнять в ручном режиме для каждой учетной записи, либо проводить повторную миграцию пользователей.

3.8.3 Импорт данных из файлов PST и других форматов

DeepMail поддерживает импорт почтовых данных из локальных файлов, созданных различными почтовыми клиентами. Наиболее востребованным является импорт из файлов PST (Personal Storage Table) – основного формата хранения данных Microsoft Outlook. Также доступен импорт из файлов EML, MSG, MBOX, DBX, VCF, ICS, CSV, WAB и архивов почтовых клиентов The Bat!, Windows Mail.

3.8.3.1 Общие сведения о формате PST

Файл PST (.pst) – это файл данных Outlook, в котором могут храниться:

- письма (включая папки «Входящие», «Отправленные», «Черновики», произвольные папки и архивы);
- события календаря, включая повторяющиеся;
- задачи;
- контакты и группы рассылки.

DeepMail импортирует все перечисленные объекты. Кроме того, при выборе сценария «импорт учётной записи полностью» система переносит также настройки профиля Outlook (правила обработки писем, подписи).

Не импортируются:

- заметки (Notes / IPF.Note, кроме служебных IPF.Note.OutlookHomepage и IPF.StickyNote, которые пропускаются);
- журналы (IPF.Journal);
- служебные элементы Outlook (IPF.Configuration, IPM.DistList, шаблоны папок, «Быстрые контакты» из Skype/Teams).

Такие элементы игнорируются без выдачи сообщений об ошибке – это штатное поведение.

3.8.3.2 Подготовка к импорту PST

Перед началом импорта необходимо выполнить следующие действия:

1. Закрыть Microsoft Outlook полностью, включая фоновые процессы. Если Outlook держит PST открытым, DeepMail не сможет прочитать файл. Для проверки откройте Диспетчер задач и завершите процесс OUTLOOK.EXE, если он присутствует.
2. Найти файл PST. Типичные расположения:

a. LocalAppData\Microsoft\Outlook\ (современные версии Outlook);
b. UserProfile\Documents\Outlook Files\ (Outlook 2010 и новее);
c. AppData\Microsoft\Outlook\ (старые версии). Файл часто называется archive.pst, <email>.pst или outlook.pst.

3. Освободить достаточно места на диске. Импорт создаёт базу данных DeepMail в каталоге AppData\DeepMail\. Размер базы после импорта примерно соответствует размеру исходного PST.
4. При первом импорте желательно использовать чистую учётную запись DeepMail. Это упростит возможный откат в случае ошибок.
5. Убедиться, что квота почтового ящика достаточна для хранения импортируемых данных. По умолчанию для пользователей установлена квота 1 ГБ – при необходимости увеличьте её в настройках пользователя.

3.8.3.3 Пошаговая инструкция импорта PST

В веб-интерфейсе DeepMail перейдите в раздел «Файл» → «Импорт» (или аналогичный пункт, доступный пользователю).

Выберите тип импорта «Импорт из файлов хранилищ Outlook» (ImportingFromPst).

На странице выбора файла нажмите «Обзор» и укажите путь к .pst-файлу.

Если файл принадлежит учётной записи Outlook, система спросит: «Выбранный файл принадлежит учётной записи Outlook. Импортировать учётную запись полностью, включая настройки?». Выберите «Да», если требуется перенести также правила и подписи. Выберите «Нет», если нужно импортировать только данные (письма, календарь, контакты, задачи).

На следующем экране будет показано дерево папок внутри PST с возможностью выборочного импорта. По умолчанию отмечены все папки. Снимите флажки с тех, которые не нужно переносить.

Выберите место назначения для импорта:

— «Импорт данных в корневые папки» – данные будут помещены в соответствующие системные папки выбранной учётной записи (Входящие, Отправленные, Календарь и т.д.) либо в локальные папки.

— «Импорт данных в отдельную папку» – этот вариант предназначен только для почтовых папок; календари и контакты при его выборе не импортируются.

Нажмите «Импортировать». В процессе импорта отображается прогресс в формате: *«Импорт папки '{имя}', обработано элементов: N/M»*.

3.8.3.4 Ограничения при импорте PST

Размер письма. В системе DeepMail действует ограничение на максимальный размер импортируемого письма. Элементы, превышающие заданный порог, автоматически исключаются из процесса. Для успешного импорта таких сообщений необходимо увеличить соответствующее ограничение в настройках сервера.

Имена папок. Имена импортируемых папок не должны содержать символы . (точка) и / (слеш). Папки с такими символами не будут импортированы.

Размер PST. Ограничений со стороны DeepMail нет. Проверена работа с файлами объёмом до 11 ГБ. PST в формате Unicode (современный Outlook) может достигать 50 ГБ, старый формат ANSI ограничен 2 ГБ – оба типа читаются.

Версия Outlook. Поддерживаются PST, созданные Outlook 97 и новее. Файлы .ost (кэш Exchange) не поддерживаются – перед импортом их необходимо экспортировать в .pst штатными средствами Outlook.

Зашифрованные PST. DeepMail не поддерживает импорт PST, защищённых паролем. Перед импортом снимите пароль в Outlook: «Файл → Настройки учётной записи → Файлы данных → Параметры → Изменить пароль» – введите старый пароль, а новый оставьте пустым.

Повреждённые PST. Если файл повреждён, DeepMail выдаст сообщение: «Выбранный файл испорчен или не является файлом Outlook PST». Восстановите файл с помощью утилиты Microsoft SCANPST.EXE (Inbox Repair Tool, входит в состав Office).

Архивы (.zip, .rar, .7z). Прямой импорт из архива невозможен. Необходимо распаковать архив в обычную папку, при необходимости снять пароль, и указать распакованный .pst в мастере импорта. После успешного импорта распакованный файл можно удалить.

3.8.3.5 Особенности работы с открытым PST, правами доступа и кодировкой

PST, занятый другим процессом. Если Outlook (включая фоновый процесс) держит PST открытым, DeepMail покажет сообщение: «Выбранный файл открыт в другой программе (вероятнее всего в Microsoft Outlook). Попробовать произвести импорт еще раз?» Закройте Outlook полностью и нажмите «Да».

Недостаточно прав. Если PST находится в папке, к которой у пользователя нет доступа, появится ошибка: «У Вас недостаточно прав на открытие файла. Пожалуйста, обратитесь к системному администратору». Переместите PST в каталог Documents или другую папку с доступом на чтение/запись.

Кодировка. PST открывается в кодировке системной локали Windows. При импорте файла, созданного на системе с другой кодовой страницей (например, английская Windows → русская), возможны проблемы с отображением символов в темах писем со старой кодировкой (cp1251 ↔ cp1252). В этом случае рекомендуется предварительно открыть PST в Outlook на той же локали, где он был создан.

3.8.3.6 Производительность и прерывание импорта

Двойной проход. Сначала DeepMail подсчитывает общее количество элементов для отображения прогресс-бара («Подготовка элементов для импорта»), затем выполняет собственно импорт. Для больших PST эта подготовка может занимать несколько минут.

Ориентировочная скорость. Примерно 1000 писем в минуту на SSD-диске. PST объёмом 11 ГБ может импортироваться от 1,5 до 3 часов.

Потребление памяти. DeepMail читает PST потоком и записывает в базу данных пакетами, поэтому память не накапливается. Пиковое потребление 1–2 ГБ при импорте писем с тяжёлыми вложениями считается нормальным.

Прерывание импорта. Можно нажать кнопку «Отмена» в мастере. Уже записанные в базу данные останутся. Возобновить импорт с того же места невозможно – при повторном запуске могут появиться дубликаты (см. раздел о дубликатах).

3.8.3.7 Работа с дубликатами

DeepMail автоматически удаляет дубликаты только в одном случае: при импорте в POP3-аккаунт, если письма в PST сохранили идентификатор POP-сервера. Тогда повторный импорт того же PST не создаст дубликатов, и последующая синхронизация с сервером также их не скачает заново.

Во всех остальных сценариях:

— импорт в IMAP, Exchange или локальные папки – дубликаты не отсеиваются;

— импорт в POP3, но PST из IMAP-аккаунта – дубликаты не отсеиваются;

— повторный запуск импорта того же файла – все письма дублируются.

Рекомендация: если необходимо доимпортировать только часть данных после частичного импорта, удалите из DeepMail уже импортированные папки (или целиком учётную запись) и запустите импорт заново. Это проще, чем вручную удалять дубликаты.

3.8.3.8 Размещение импортированных данных

Импортированные данные сохраняются в соответствующих папках DeepMail представленных ниже.

Таблица 2 – Размещение импортированных данных

Исходная папка в PST	Место назначения в DeepMail
Inbox (Входящие)	Папка «Входящие» целевого аккаунта (или «Локальные папки»)
Sent Items (Отправленные)	Папка «Отправленные»
Deleted Items (Удалённые)	Папка «Корзина»
Drafts (Черновики)	Папка «Черновики»
Outbox (Исходящие)	Папка «Исходящие»
Calendar (Календарь)	«Календарь по умолчанию»

Исходная папка в PST	Место назначения в DeepMail
Contacts (Контакты)	«Контакты по умолчанию»
Tasks (Задачи)	«Задачи по умолчанию»
Произвольные почтовые папки	Создаются с теми же именами внутри папки «Входящие»
Archive и пользовательские архивные папки	Создаются с теми же именами

Не размещаются (игнорируются): заметки, журналы, sticky notes, служебные элементы.

3.8.3.9 Типичные ошибки и их устранение

«Файл занят другим процессом» – закройте Outlook (включая фоновые процессы). Если ошибка повторяется, перезагрузите Windows (иногда PST остаётся заблокированным после краха Outlook).

«Файл не существует» / «Файл пустой» – PST имеет нулевой размер или был удалён. Проверьте путь и выберите файл заново.

«Выбранный файл испорчен или не является файлом Outlook PST» – файл повреждён или не является PST. Запустите SCANPST.EXE (входит в состав Office) для восстановления.

«У Вас недостаточно прав на открытие файла» – переместите PST в каталог с полными правами доступа (например, UserProfile\Documents).

«Не удаётся прочитать профили Outlook» – возникает при импорте всего профиля. DeepMail не может прочитать ветку реестра HKCU\Software\Microsoft\Office\...\Outlook\Profiles (обычно из-за групповых политик). Решение: импортировать каждый PST отдельно (без выбора импорта учётной записи полностью).

Импорт завершён «с ошибками. Пропущено элементов: N» – некоторые отдельные элементы не удалось импортировать (например, из-за внутреннего

исключения). Основной массив данных перенесён. Для выяснения деталей включите расширенное логирование (параметр LogImport=true) и изучите файл App Tracing.log.

Импорт зависает – если прогресс не двигается более 15 минут, проверьте Диспетчер задач: процесс DM.exe потребляет CPU? Если да – импорт идёт, просто обрабатывается большая папка (более 10 000 писем с вложениями). Если CPU = 0% и память не растёт – импорт залип. Принудительно закройте DeepMail, удалите недоимпортированные данные и запустите импорт заново.

3.8.3.10 Импорт больших PST по частям

Рекомендуется импортировать очень большие PST (более 10 ГБ) по частям, чтобы снизить риск сбоя и упростить контроль:

1. На этапе выбора папок снимите все флажки, оставив только одну-две крупные папки.
2. Запустите импорт.
3. После его завершения повторите импорт, выбрав следующие папки (уже импортированные не отмечайте).

Этот метод безопасен для всех типов аккаунтов, кроме POP3 (там лучше импортировать всё за один раз – см. раздел о дубликатах). Преимущества: меньший шанс наткнуться на сбойный элемент в середине процесса и возможность прервать импорт в удобное время.

3.8.3.11 Проверка после импорта

После завершения импорта рекомендуется:

1. Сравнить количество писем в DeepMail с исходным PST (хотя бы в нескольких папках).
2. Открыть несколько писем разных типов (простой текст, HTML, с вложениями, с приглашениями на встречи) и убедиться в их корректном отображении.
3. Проверить случайные события календаря и контакты (если они импортировались).
4. Если были созданы новые папки, убедиться, что они имеют правильные имена.
5. После успешной проверки исходный PST можно удалить или переместить в долгосрочный архив.

3.8.3.12 Импорт других форматов

DeepMail также поддерживает импорт данных из следующих форматов (каждый формат доступен как отдельный пункт в мастере импорта):

— .eml – отдельные письма в формате MIME (любые почтовые клиенты).

— .msg – одиночные письма, сохранённые из Outlook.

— .mbox – почтовые ящики Thunderbird, Apple Mail и других клиентов.

— .dbx – почтовые папки Outlook Express.

— The Bat! – почтовые сообщения и контакты из клиента The Bat!.

— Windows Mail / Windows Live Mail – данные из встроенного почтового клиента Windows.

— .vcf – контакты в формате vCard.

— .ics – события календаря в формате iCalendar.

— .csv – таблицы контактов (например, экспорт из Excel или других систем).

— .wab – старая адресная книга Windows (Windows Address Book).

3.8.3.13 Краткая памятка администратору (для ответов пользователям)

При возникновении у пользователей вопросов по импорту данных из PST, руководствуйтесь следующими краткими рекомендациями.

Таблица 3 – Размещение импортированных данных

Задача	Рекомендация
Перенос почты из Outlook	Файл → Импорт → «Импорт из файлов хранилищ Outlook» → выбрать .pst.
Импорт архива .pst.zip	Распаковать архив, затем импортировать PST.
Импорт PST из OneDrive	Сначала скачать файл локально (облачный файл может быть нестабилен).
Импорт .ost	В Outlook экспортировать в .pst, затем импорт.

Задача	Рекомендация
Импорт PST с паролем	В Outlook снять пароль, затем импорт.
Импорт большого PST (более 10 ГБ)	Разбить на части (импорт по папкам), запустить в нерабочее время.
Перенос только календаря	В мастере выбрать только календарные папки.
Поиск причины ошибки	Включить LogImport=true, повторить импорт, изучить App Tracing.log.

3.9 Инструмент «Контроллеры домена»

Для перехода к подключению контроллеров домена необходимо в меню интерфейса администратора выбрать «Контроллеры домена» (рисунок 83).

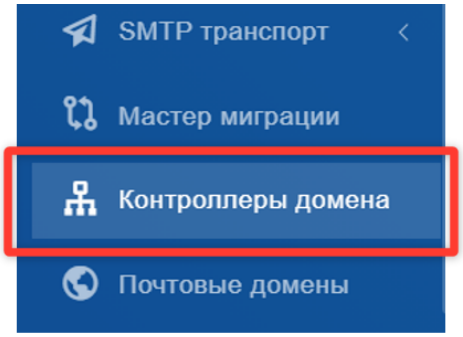


Рисунок 83 – Инструмент «Контроллеры домена»

В окне «Контроллеры домена» отображается перечень обслуживаемых доменов и подключенных контроллеров домена, в верхней области отображены общие количественные показатели (рисунок 84).

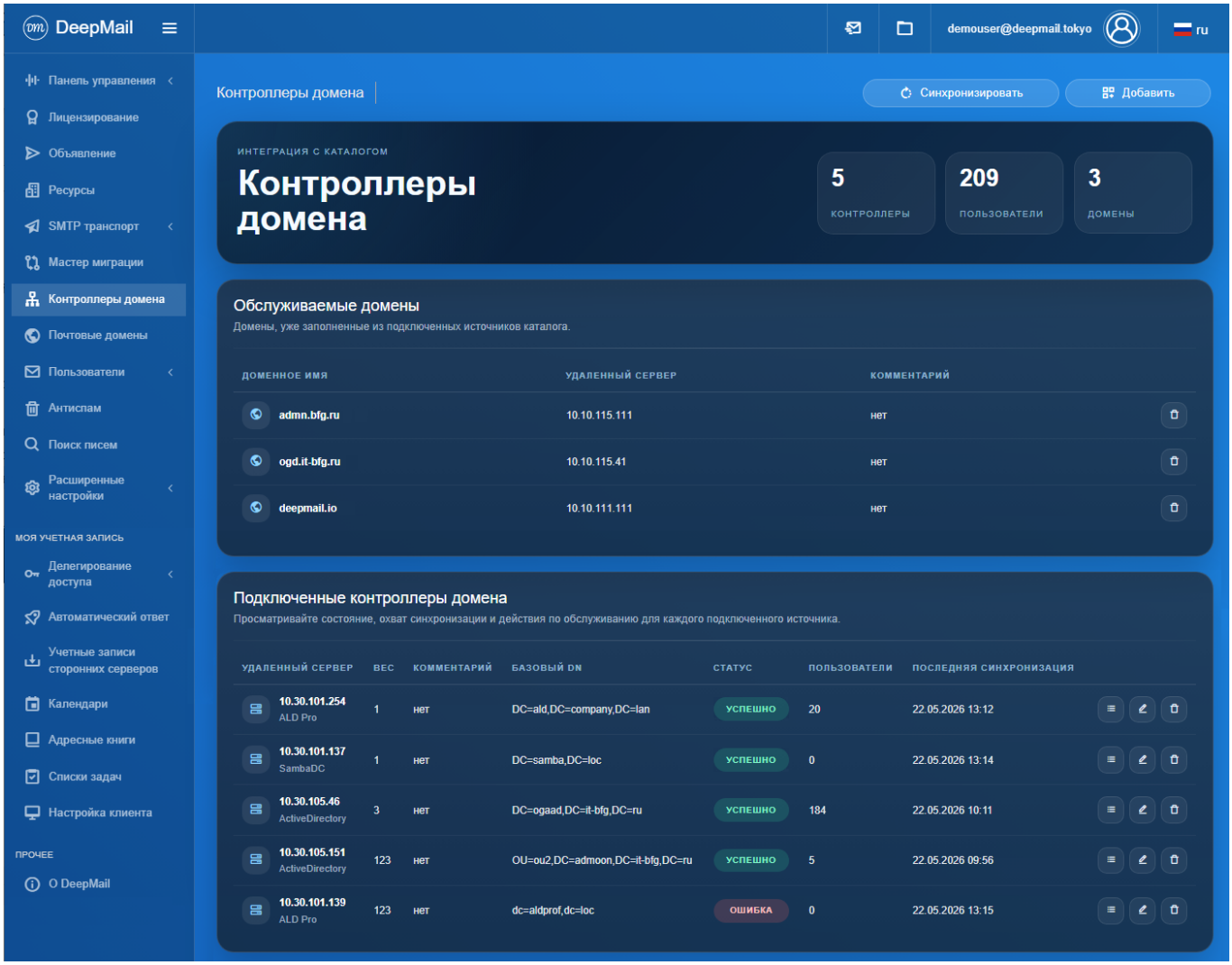


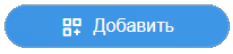
Рисунок 84 – Окно «Контроллеры домена»

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

В системе доступно подключение неограниченного количества контроллеров, таким образом обеспечивая наличие резервных контроллеров домена с различными IP-адресами. Контроллеры добавляются с разным приоритетом (параметр «Вес»), если один «умирает», система обращается к другому контроллеру (подробнее см. в пункте 3.9.1).

Для просмотра списка логов подключенных контроллеров необходимо в окне контроллеров домена нажать кнопку  (см. рисунок 84).

3.9.1 Подключение контроллера домена

Для подключения контроллера домена необходимо нажать кнопку  , расположенную в правом верхнем углу окна «Контроллеры домена» (см. рисунок 84). В

результате на экране появится форма «Добавить контроллер домена», в которой необходимо указать параметры контроллера (рисунок 85, рисунок 86, рисунок 87).

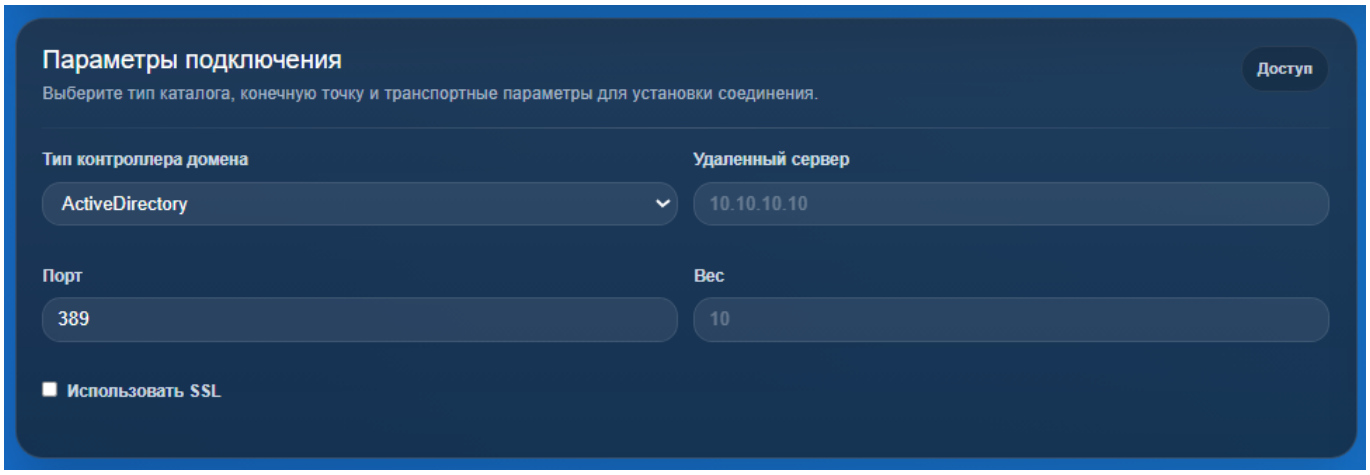


Рисунок 85 – Настройка параметров подключения контроллера домена

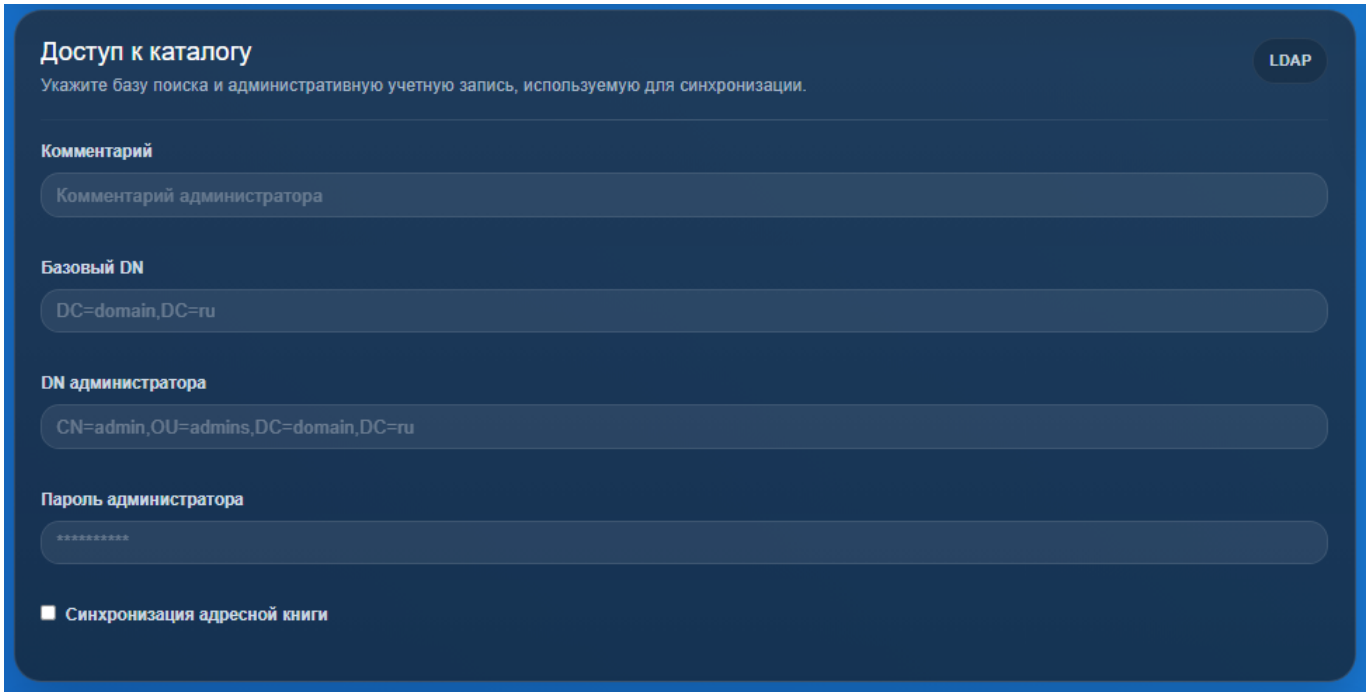


Рисунок 86 – Настройка параметров доступа к каталогу домена

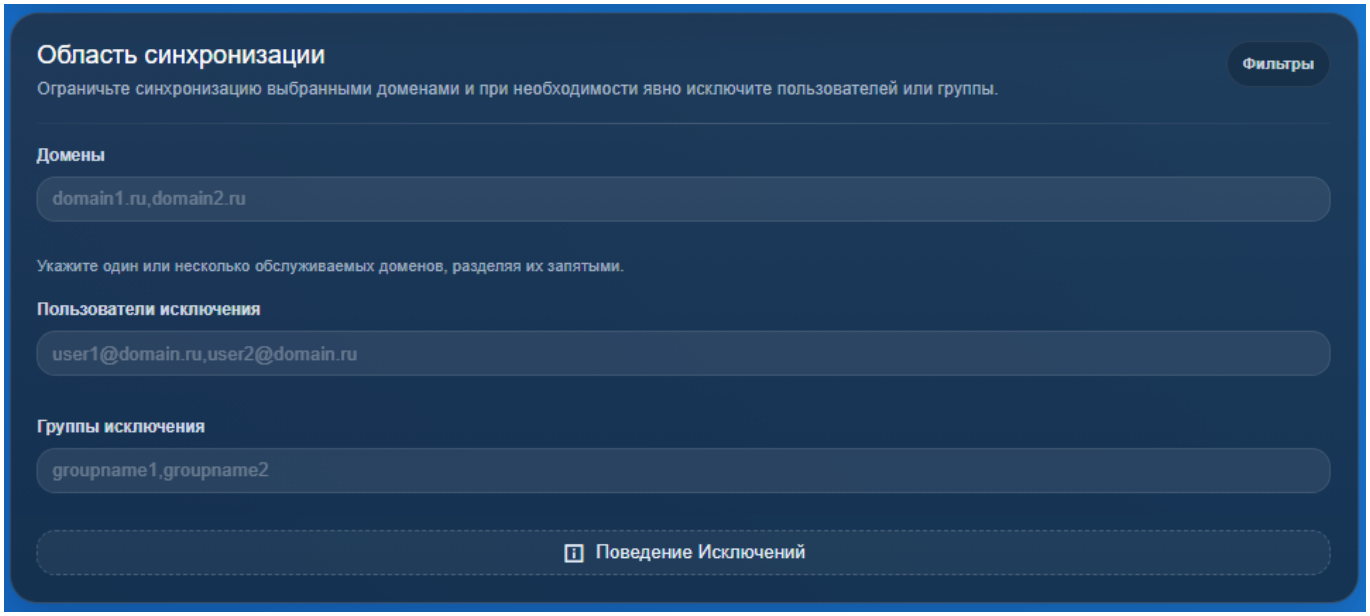


Рисунок 87 – Настройка параметров области синхронизации домена

Выберите тип подключаемого контроллера домена (рисунок 88).

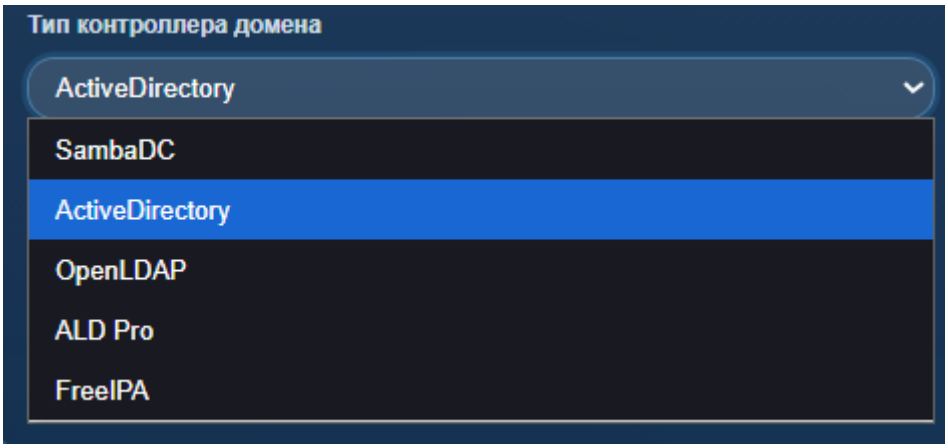


Рисунок 88 – Выбор типа контроллера домена

Далее укажите следующие параметры контроллера:

- в поле «Удаленный сервер» указать IP-адрес контроллера домена;
- в поле «Порт» указать порт подключения;
- в поле «Вес» – числовое значение приоритета;
- указать необходимые параметры 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 параметр «Вес». Это числовое значение, которое 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.

Заметки администратора размещены в форме для информации (рисунок 89).

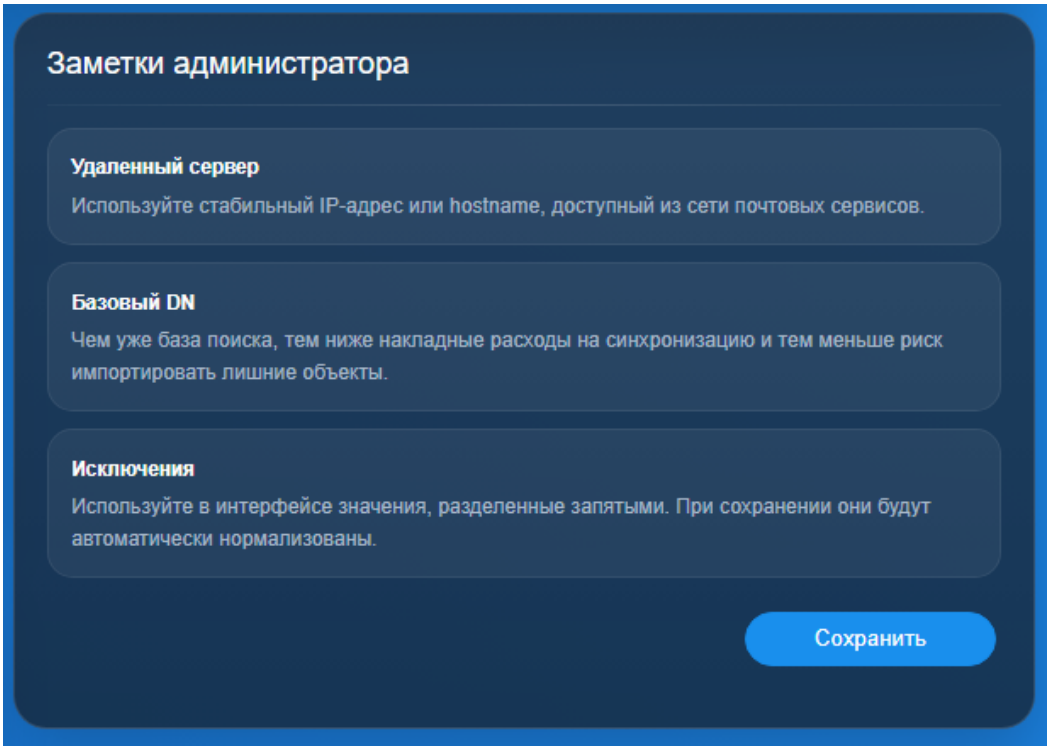


Рисунок 89 – Область заметок администратора

Для сохранения настроек необходимо нажать кнопку Сохранить (см. рисунок 89).

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 Синхронизировать, 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 90).

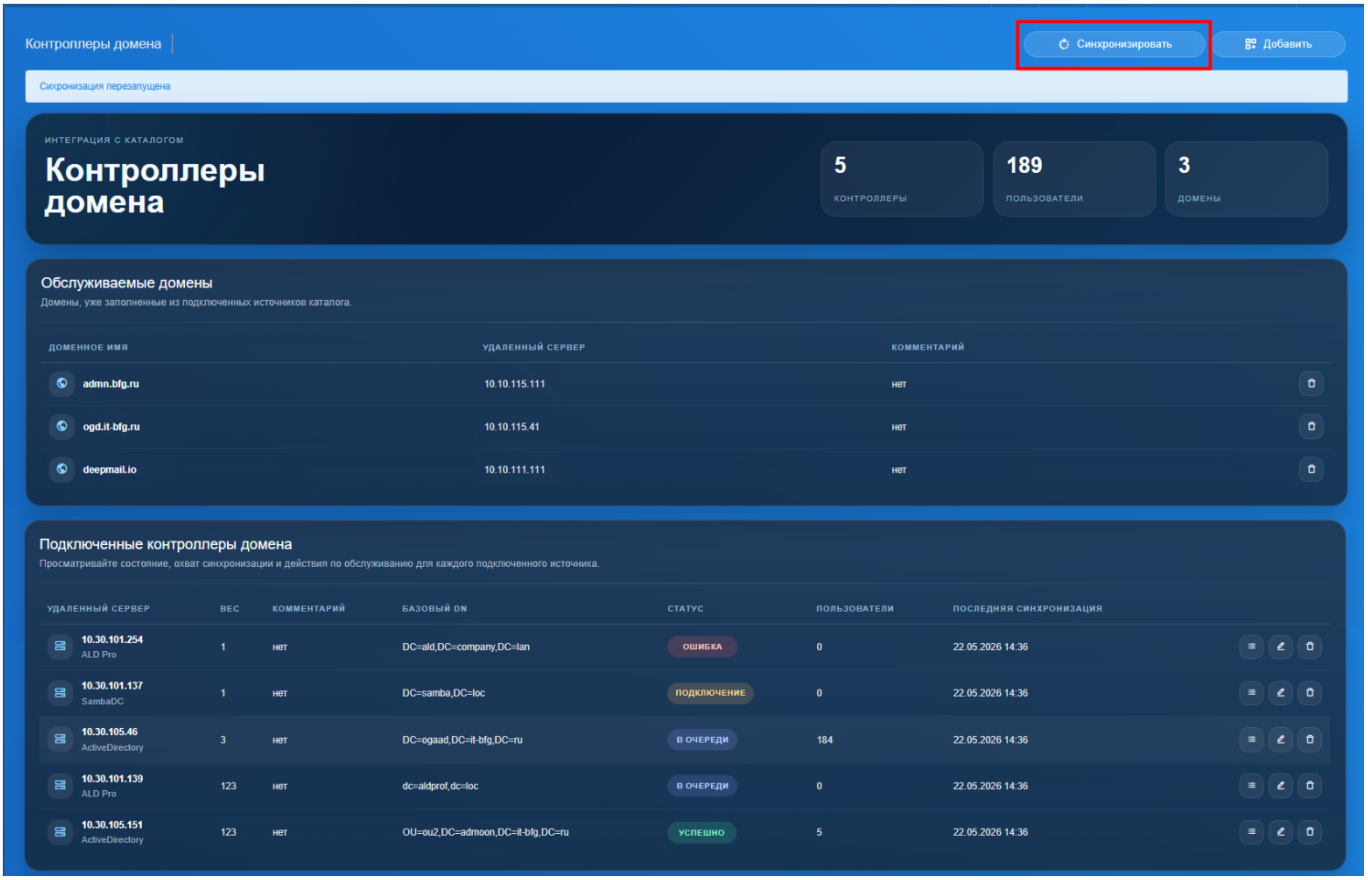


Рисунок 90 – Кнопка «Синхронизировать» и секции информации

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 90). 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  (см. рисунок 90).

Для изменения настроек подключения необходимо нажать кнопку  (см. рисунок 90), и внести изменения в появившуюся форму.

3.9.3 Удаление контроллера домена

Для удаления контроллера домена необходимо нажать кнопку  (см. рисунок 90), 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 91).

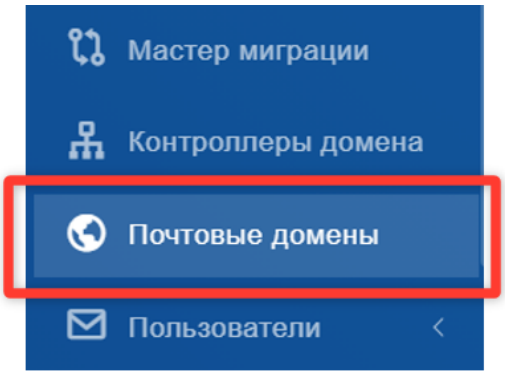


Рисунок 91 – Инструмент «Почтовые домены»

Окно «Список доменов» содержит список почтовых доменов, обслуживаемых сервером (рисунок 92).

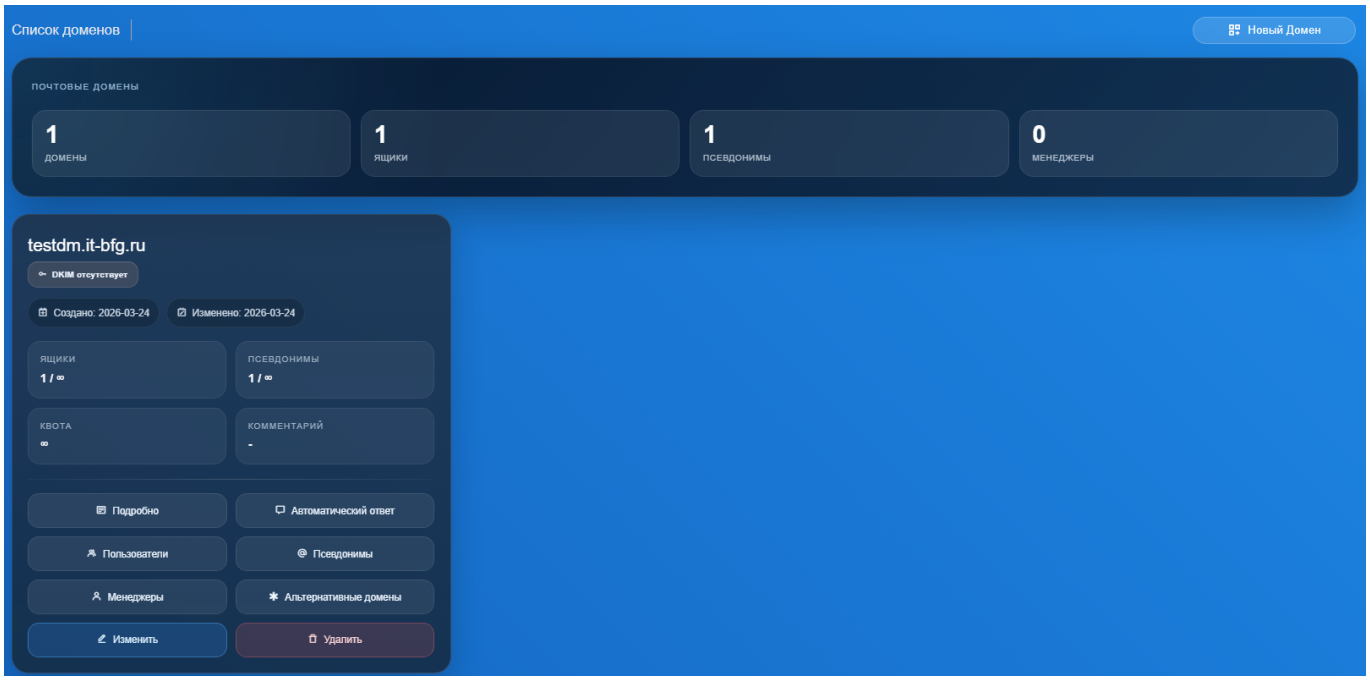


Рисунок 92 – Окно «Список доменов»

Интерфейс «Список доменов» представляет собой централизованную панель управления всеми почтовыми доменами, обслуживаемыми сервером DeepMail. На стартовом экране администратор видит обобщённую статистику по всем доменам: общее количество доменов, общее число почтовых ящиков, псевдонимов и назначенных менеджеров. Эти цифровые индикаторы позволяют быстро оценить масштаб инфраструктуры.

Для каждого домена в интерфейсе выделен отдельный блок, в котором сгруппированы все сведения и инструменты управления. В левой части блока отображается имя домена и его статус: при отсутствии подключённого DKIM-ключа система выводит соответствующую метку «ДКМ отсутствует», сигнализируя о необходимости настройки подписи. Рядом указаны даты создания и последнего изменения домена — это помогает отслеживать жизненный цикл конфигурации.

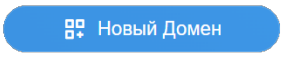
Центральная часть блока содержит карточку с текущими значениями лимитов и потребления ресурсов. Для каждого домена отображается количество занятых почтовых ящиков относительно максимально разрешённого (например, 1 из бесконечности), число созданных псевдонимов и установленная квота на дисковое пространство (здесь обозначена как ∞, что означает отсутствие ограничения). Поле «Комментарий» позволяет администратору оставлять произвольные заметки, связанные с доменом, что удобно при ведении учёта.

В правой части блока расположены кнопки быстрого перехода к основным операциям управления доменом. С помощью пункта «Подробно» можно открыть расширенную карточку домена, содержащую полный набор настроек. «Автоматический ответ» ведёт к конфигурации автоответчика, который может быть включён для всех ящиков домена. Кнопка «Пользователи» открывает список учётных записей, созданных в домене, позволяя управлять ящиками, а «Посредники» и «Менеджеры» дают доступ к настройке делегирования прав управления. Раздел «Альтернативные домены» служит для добавления псевдонимов домена — дополнительных имён, на которые также будет приниматься почта. Завершают блок кнопки «Изменить» для редактирования основных параметров домена (например, квот, профилей SMTP/IMAP) и «Удалить» для его полного удаления из системы.

Таким образом, интерфейс «Список доменов» объединяет в себе сводную статистику по всей почтовой системе и детальные инструменты управления каждым доменом, позволяя администратору быстро переходить к настройке пользователей, псевдонимов, прав доступа и ключевых почтовых функций, не теряя из виду общую картину инфраструктуры.

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 92). После этого будет выполнен переход к форме добавления нового почтового домена «Новый домен» с основными настройками, настройками сетевых параметров и протоколов (рисунок 93, рисунок 94, рисунок 95, рисунок 96).

Панель управления доменом в DeepMail объединяет несколько вкладок, позволяющих администратору гибко настраивать параметры почтового домена, управлять сетевыми интерфейсами, протоколами, правами отправки и вести служебные заметки. Каждая вкладка отвечает за определённый аспект конфигурации, а их совокупность обеспечивает полный контроль над поведением домена.

В основных настройках (рисунок 93) задаются базовые характеристики домена.

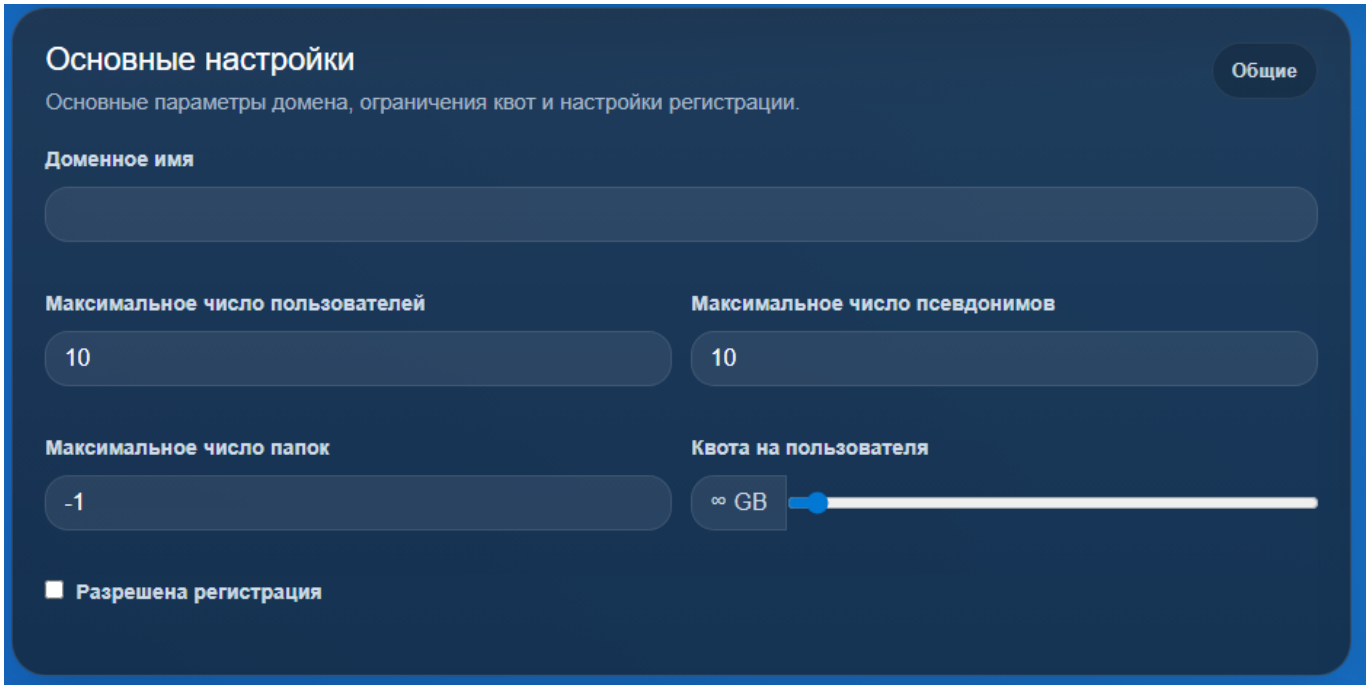


Рисунок 93 – Окно «Новый домен» основные настройки

Поле «Доменное имя» содержит имя почтового домена, которое будет использоваться для формирования адресов электронной почты. Здесь же определяются ограничения на количество создаваемых почтовых ящиков – «Максимальное число пользователей» позволяет установить жёсткий лимит, предотвращающий неконтролируемое создание учётных записей. Аналогично, «Максимальное число псевдонимов» ограничивает

количество одновременно активных псевдонимов для одного почтового ящика. Поле «Максимальное число папок» задаёт квоту на количество папок, а «Квота на пользователя» задает ограничение на дисковое пространство, доступное всем ящикам домена – значение «∞» означает отсутствие ограничений. Флажок «Разрешена регистрация» управляет возможностью самостоятельного создания новых почтовых ящиков пользователями через веб-интерфейс или другие механизмы самозаписи.

Раздел сетевых настроек (рисунок 94) определяет, под какими именами и с каких сетей доступен домен.

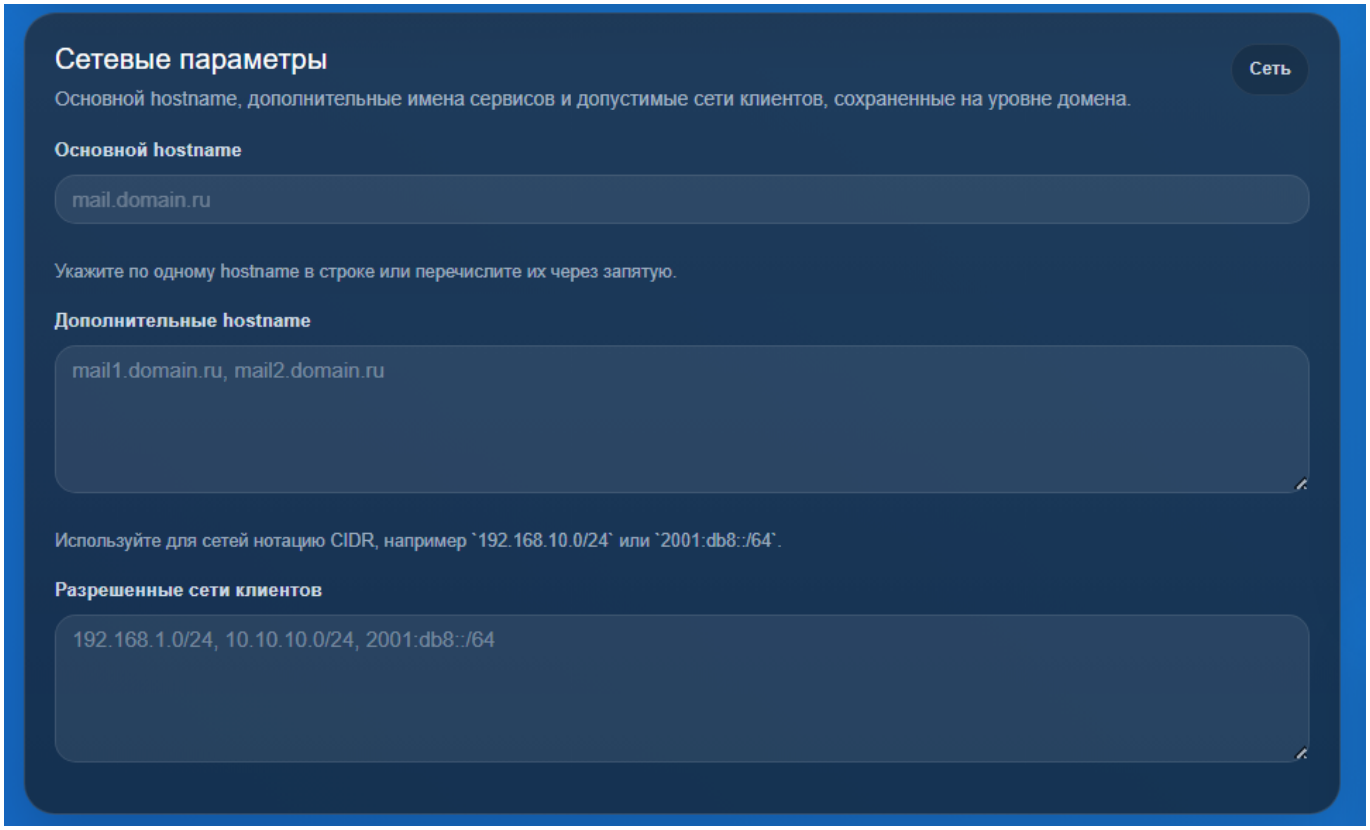


Рисунок 94 – Окно «Новый домен» сетевые параметры

«Основной hostname» – это главное доменное имя почтового сервера, которое будет использоваться в MX-записях, при формировании ссылок в веб-интерфейсе и в качестве имени сервера для почтовых клиентов. «Дополнительные hostname» позволяют привязать к домену альтернативные имена, например, для различных поддоменов или исторических имён сервера. Эти имена могут перечисляться через запятую. «Разрешенные сети клиентов» служат для ограничения доступа к почтовым сервисам домена: здесь указываются диапазоны IP-адресов (в нотации CIDR), с которых разрешены подключения. Если поле заполнено, то все попытки доступа с адресов вне указанных сетей будут отклонены, что повышает безопасность.

Во вкладке «Поддерживаемые протоколы» (рисунок 95) настраивается набор протоколов, доступных для домена, а также правила авторизации для отправки почты. Для каждого протокола можно включить или отключить его поддержку:

- IMAP – доступ к почтовым ящикам через IMAP-клиенты;
- POP3 – поддержка устаревших почтовых клиентов, использующих POP3;
- SMTP – возможность отправки и приёма почты по протоколу SMTP;
- WebDAV – поддержка CalDAV и CardDAV для синхронизации календарей и контактов.

Блок «Кому разрешено отправлять» задатт политику исходящей почты. Пользователи домена могут отправлять письма всем (без ограничений), только внутри своего домена (только адресатам того же домена) или только внутри локальной почтовой системы (включая другие домены на том же сервере, но не на внешние адреса). Флажок «Требовать SMTP-аутентификацию» определяет, обязаны ли пользователи проходить аутентификацию перед отправкой писем через SMTP – отключение этого требования может использоваться для внутренних доверенных сетей. Опция «GSSAPI» включает поддержку аутентификации Kerberos (GSSAPI) для почтовых клиентов, что позволяет использовать единый вход в доменной среде.

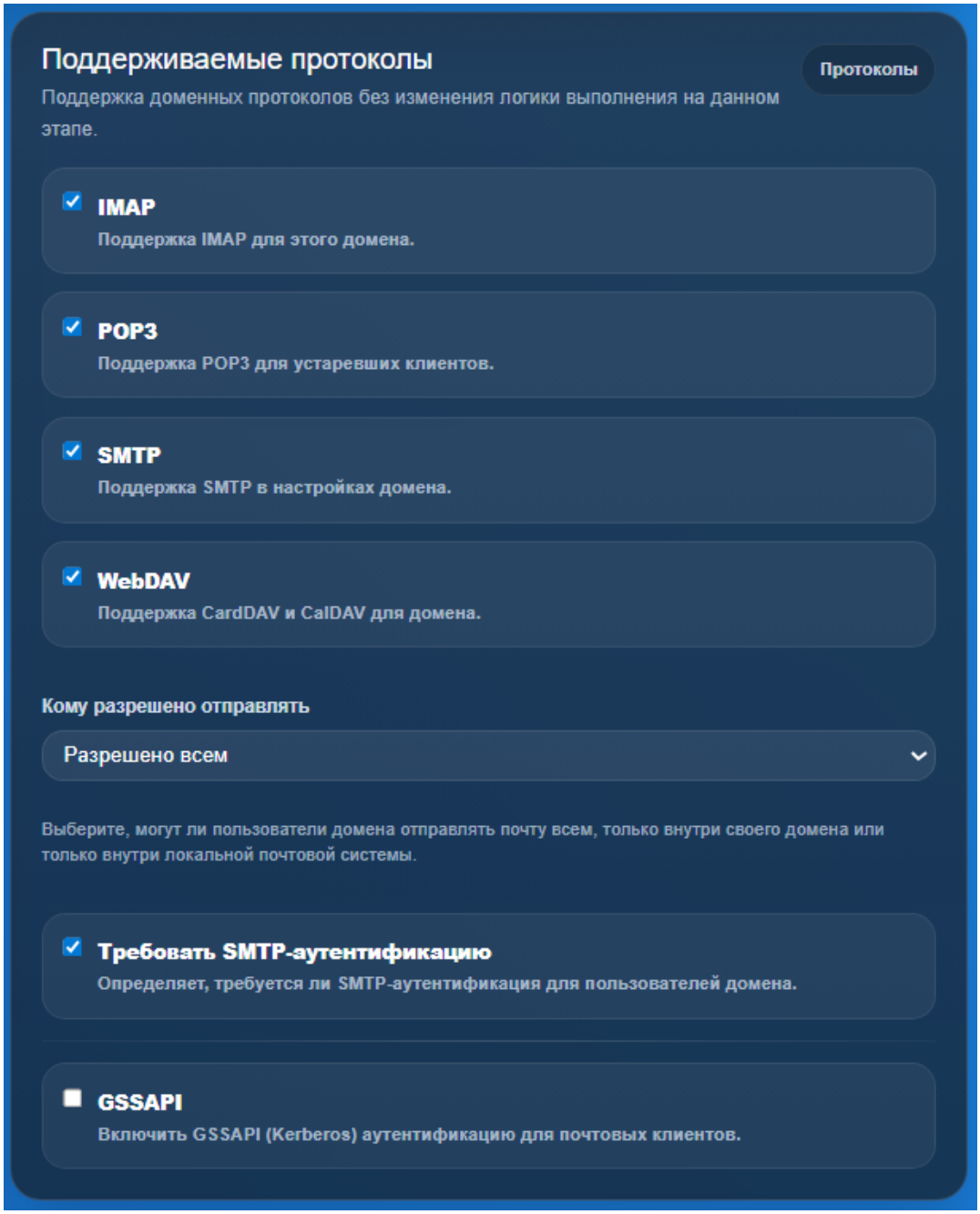


Рисунок 95 – Окно «Новый домен» поддерживаемые протоколы

Раздел «Заметки администратора» (рисунок 96) предоставляет администратору возможность оставлять произвольные текстовые комментарии, связанные с доменом.

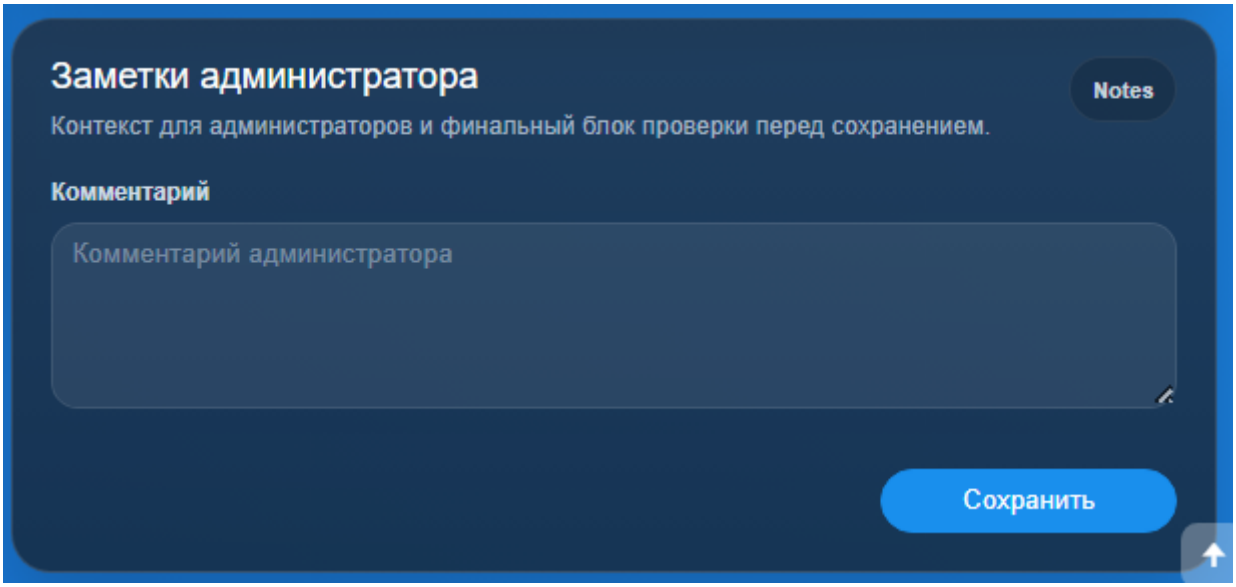


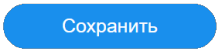
Рисунок 96 – Окно «Новый домен» заметки администратора

Поле «Комментарий» может содержать служебные пометки, или любую другую полезную информацию. Сохранённые заметки хранятся вместе с конфигурацией домена и могут быть просмотрены другими администраторами, что облегчает совместную работу и документирование.

Все изменения в настройках домена применяются после нажатия кнопки «Сохранить» в соответствующей вкладке. Система автоматически выполняет реконфигурацию затронутых сервисов (SMTP, IMAP и т.д.) без необходимости ручного перезапуска. Такая детализированная настройка позволяет администратору гибко адаптировать поведение каждого домена под требования организации, будь то строгие сетевые ограничения, поддержка устаревших протоколов или интеграция с внешней аутентификацией.

3.10.1.2 Изменение почтового домена

Для изменения параметров созданных почтовых доменов необходимо в окне «Список доменов» нажать кнопку 

(см. рисунок 92). После этого будет выполнен переход к форме, идентичной параметрам создания нового домена, редактирования параметров домена «Изменить домен» в которой можно внести изменения в параметры домена и нажать кнопку 

(рисунок 97).

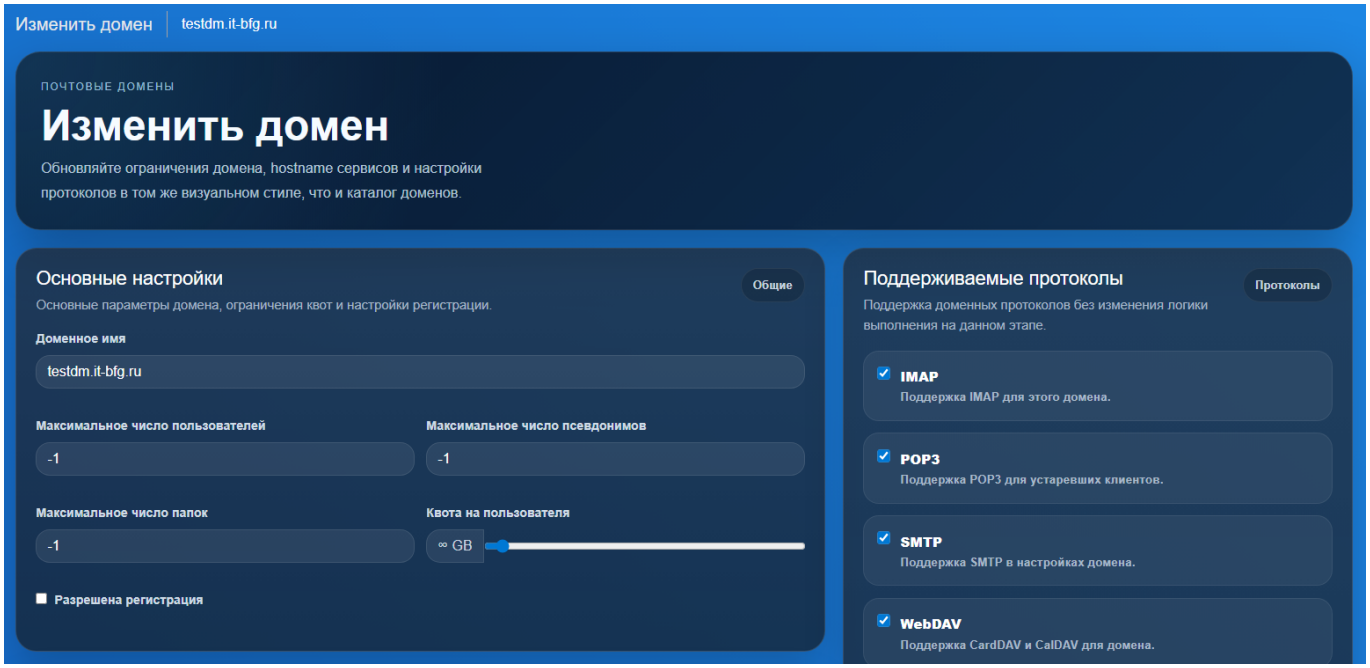


Рисунок 97 – Форма «Изменить домен»

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

3.10.1.3 Настройка автоматического ответа для почтового домена

Для настройки автоматического ответа для выбранного почтового домена необходимо в окне «Список доменов» нажать кнопку Автоматический ответ (см. рисунок 92), относящуюся к почтовому домену, на котором необходимо настроить автоматический ответ. После этого будет выполнен переход к форме редактирования параметров автоматического ответа, в которой необходимо внести заголовок и текст автоответа, а также дату начала и окончания работы автоответчика, после внесения всей информации нажать кнопку Обновить (рисунок 98).

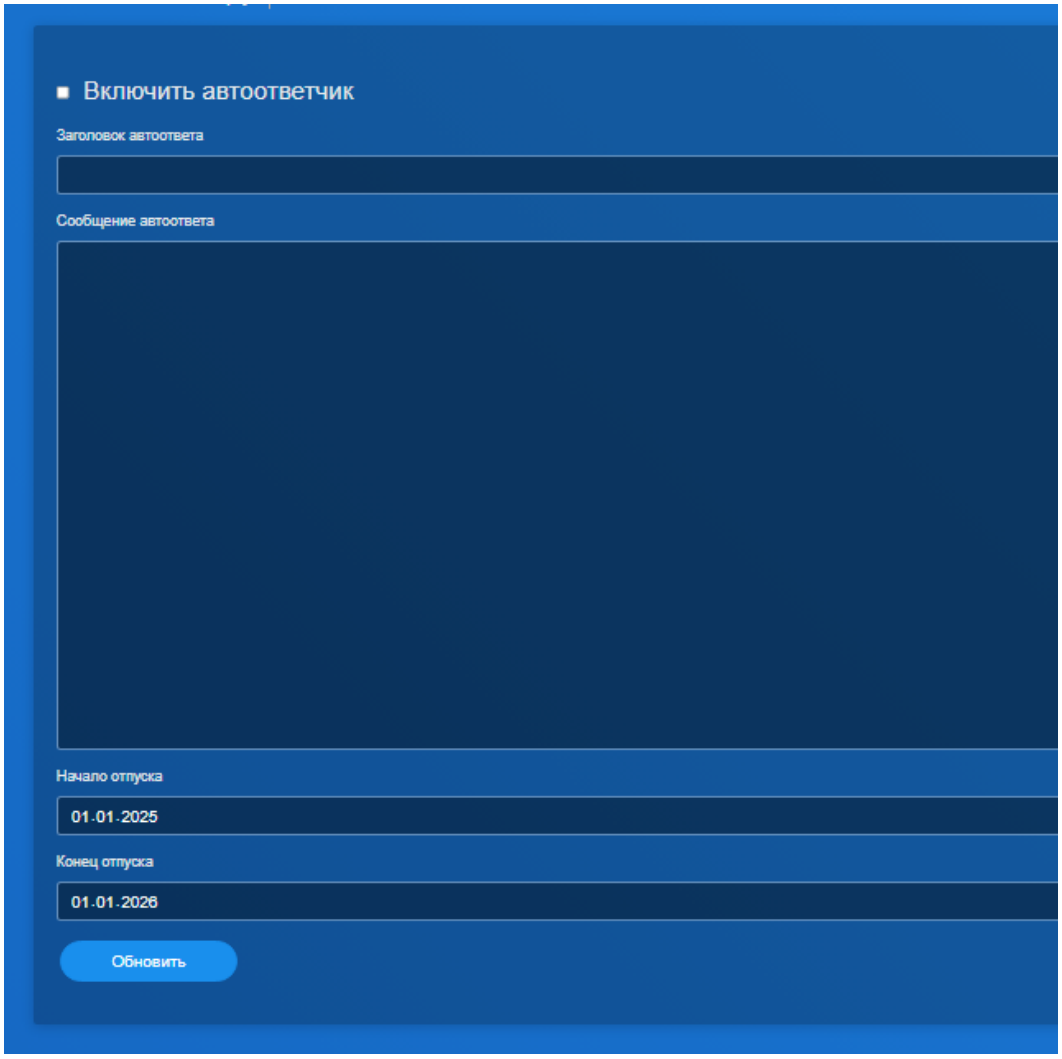


Рисунок 98 – Форма «Включить автоответчик для почтового домена»

При данной настройке, возможность настройки личного автоответчика для конкретного почтового ящика блокируется (рисунок 99).

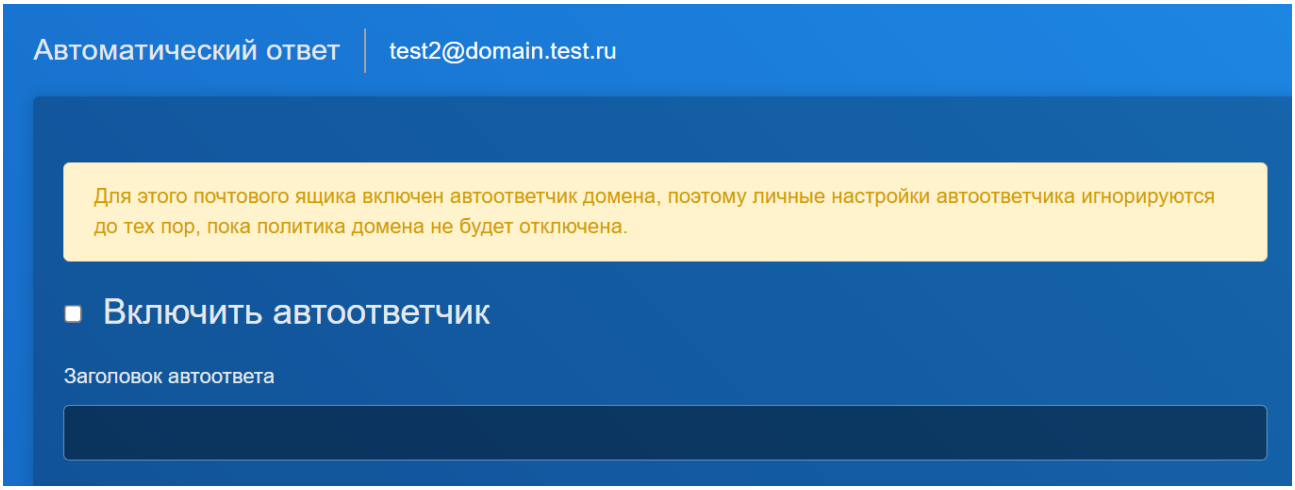


Рисунок 99 – Форма «Блокирование настройки личного автоответчика»

3.10.1.4 Удаление почтового домена

Для удаления почтового домена необходимо нажать кнопку Удалить, расположенную на панели выбранного домена (рисунок 100).

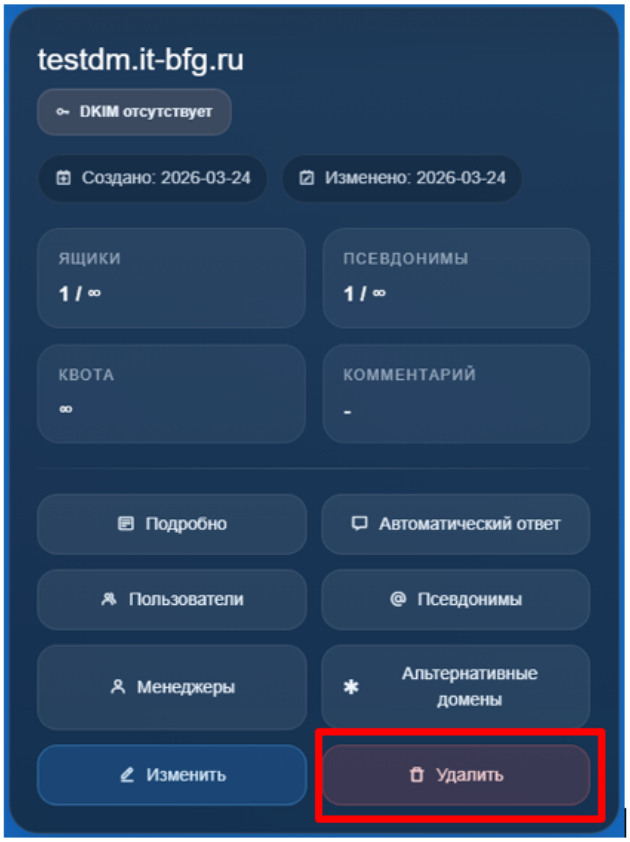


Рисунок 100 – Кнопка «Удалить»

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 Пользователи (рисунок 101).

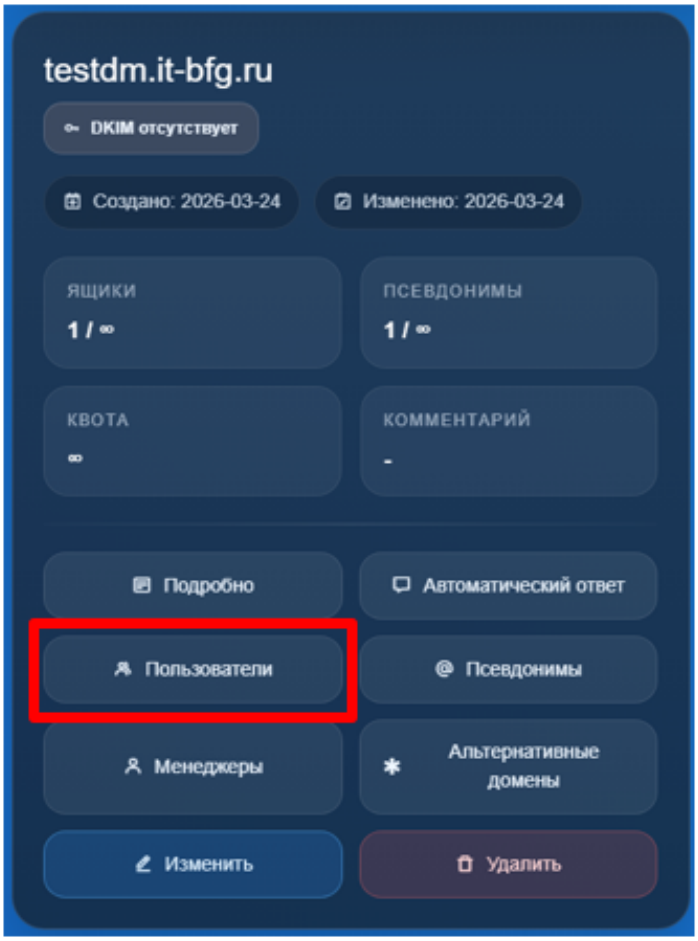


Рисунок 101 – Кнопка «Пользователи»

Откроется окно «Список пользователей» с поименным списком пользователей выбранного домена, отображенным в табличном виде (рисунок 102).

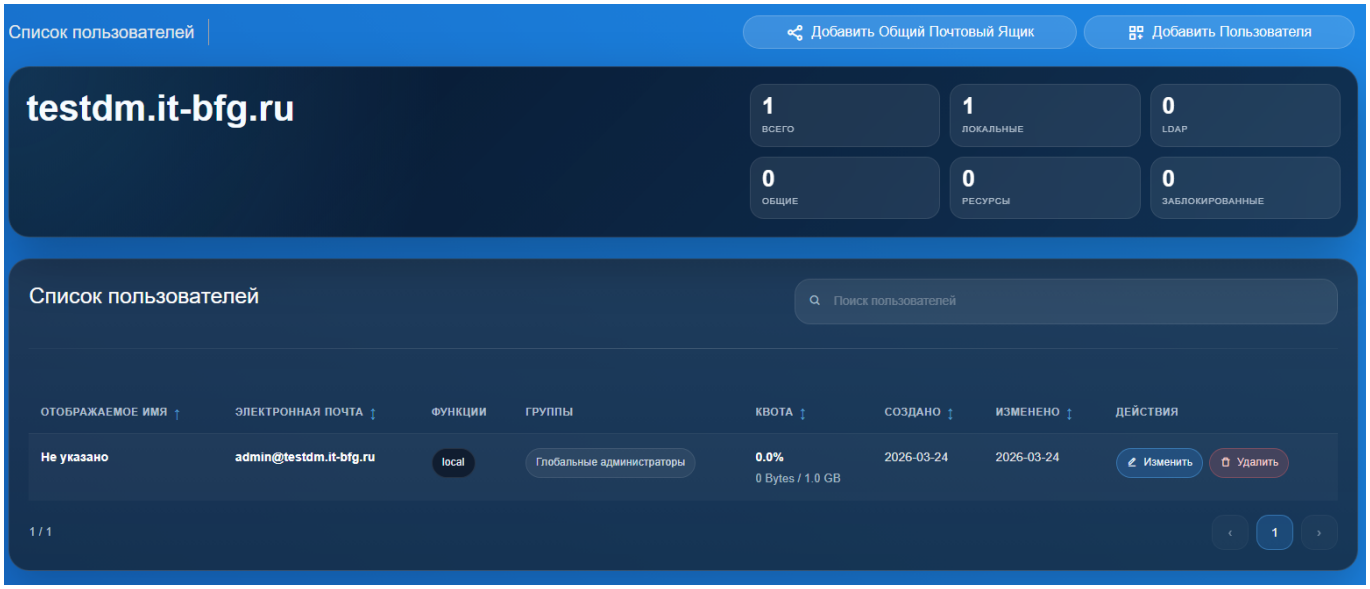
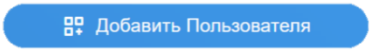


Рисунок 102 – Окно «Список пользователей»

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 102). На экране появится форма «Новый пользователь» (рисунок 103).

Рисунок 103 – Форма «Новый пользователь»

Форма редактирования почтового ящика в панели администратора DeepMail объединяет несколько тематических разделов, позволяющих настроить учетную запись пользователя с высокой степенью детализации.

В верхней части расположен блок «Основные настройки» (рисунок 104), где задается локальная часть адреса электронной почты (поле «Электронная почта» с уже выбранным доменом), пароль с обязательным подтверждением, отображаемое имя, которое будут видеть получатели, а также членство в группах каталога.

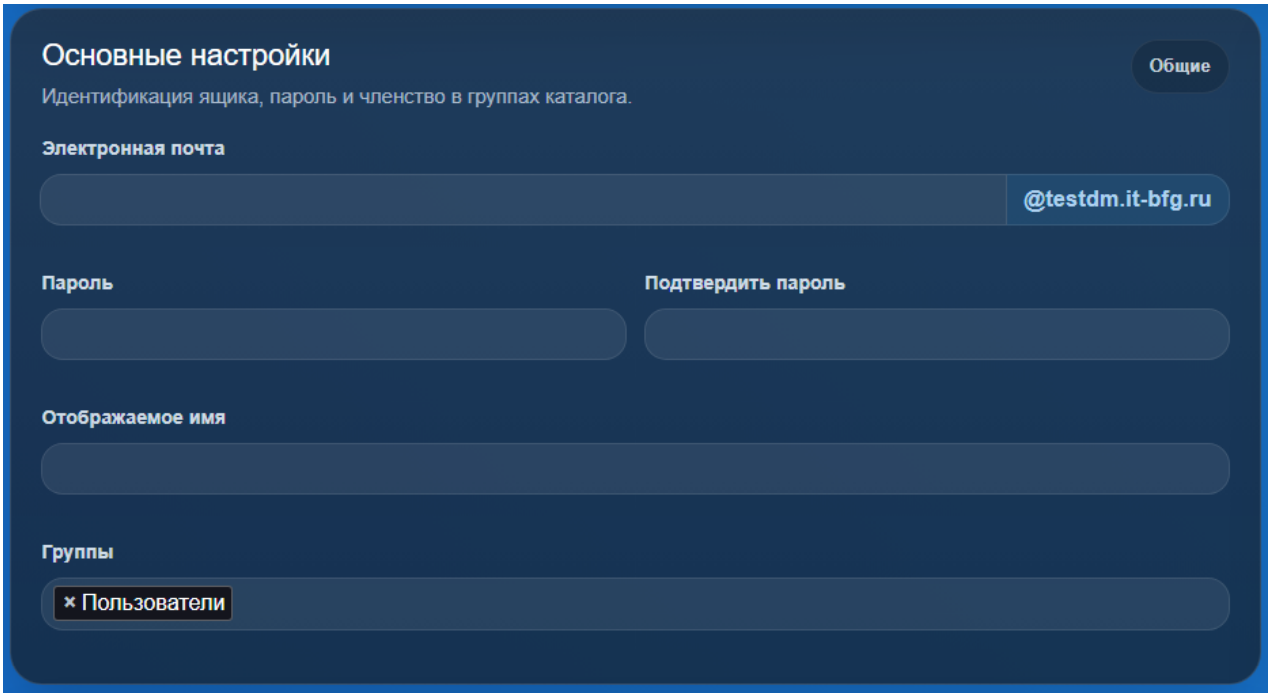


Рисунок 104 – Форма «Новый пользователь» Основные настройки

Список групп представлен в виде переключаемых элементов, что позволяет легко включать ящик в одну или несколько групп, например, «Пользователи», «Бизнес-партнёры», «Аналитика» и другие.

Следующий раздел – «Квоты и лимиты» – дает возможность ограничить ресурсы, потребляемые почтовым ящиком. Здесь можно установить максимальный размер почтового хранилища (квоту), указав значение в гигабайтах, и ограничить количество создаваемых папок (значение -1 означает отсутствие ограничений) (рисунок 105).

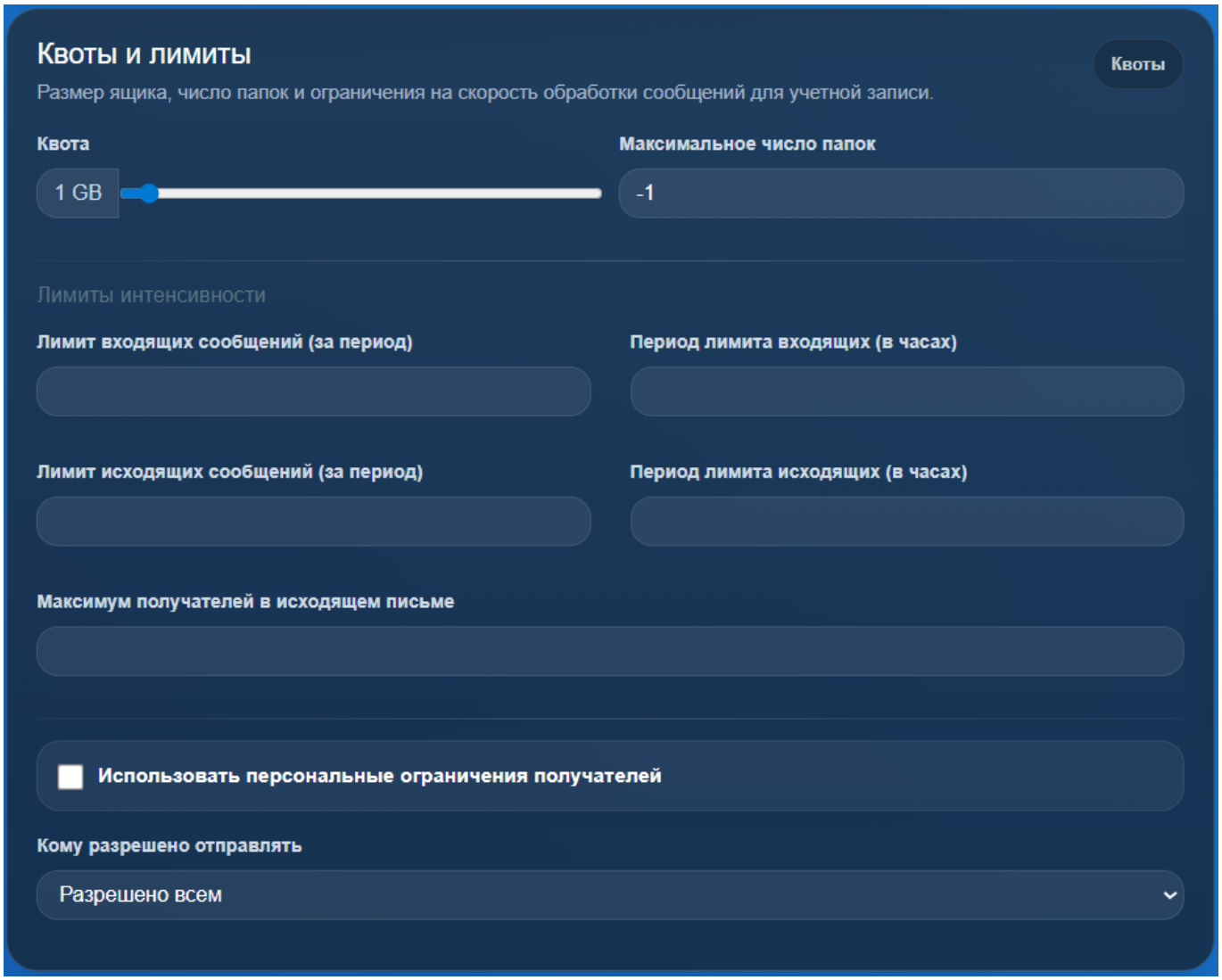


Рисунок 105 – Форма «Новый пользователь» Квоты и лимиты

В подразделе «Лимиты интенсивности» настраиваются пороговые значения для защиты от злоупотреблений: администратор может задать максимальное число входящих и исходящих сообщений за определённый период (в часах), а также ограничить количество получателей в одном исходящем письме. Флажок «Использовать персональные ограничения получателей» позволяет активировать индивидуальные правила для данного ящика, а поле «Кому разрешено отправлять» уточняет допустимый круг адресатов (например, «Разрешено

всем», «Только внутри домена»). Опция «Разрешить пользователю подделывать отправителя» управляет возможностью менять адрес в поле «От» при отправке писем.

В «Автоматическая блокировка сеанса при бездействии» настраивается время неактивности пользователя в системе в случае превышении которого, сессия автоматически блокируется. В случае настроенной автоматической блокировки сеанса пользователем локально, серверная настройка не используется.

В блоке «Шаблоны и доступ» администратор может применить предварительно созданный шаблон, который задаёт типовой набор прав (рисунок 106).

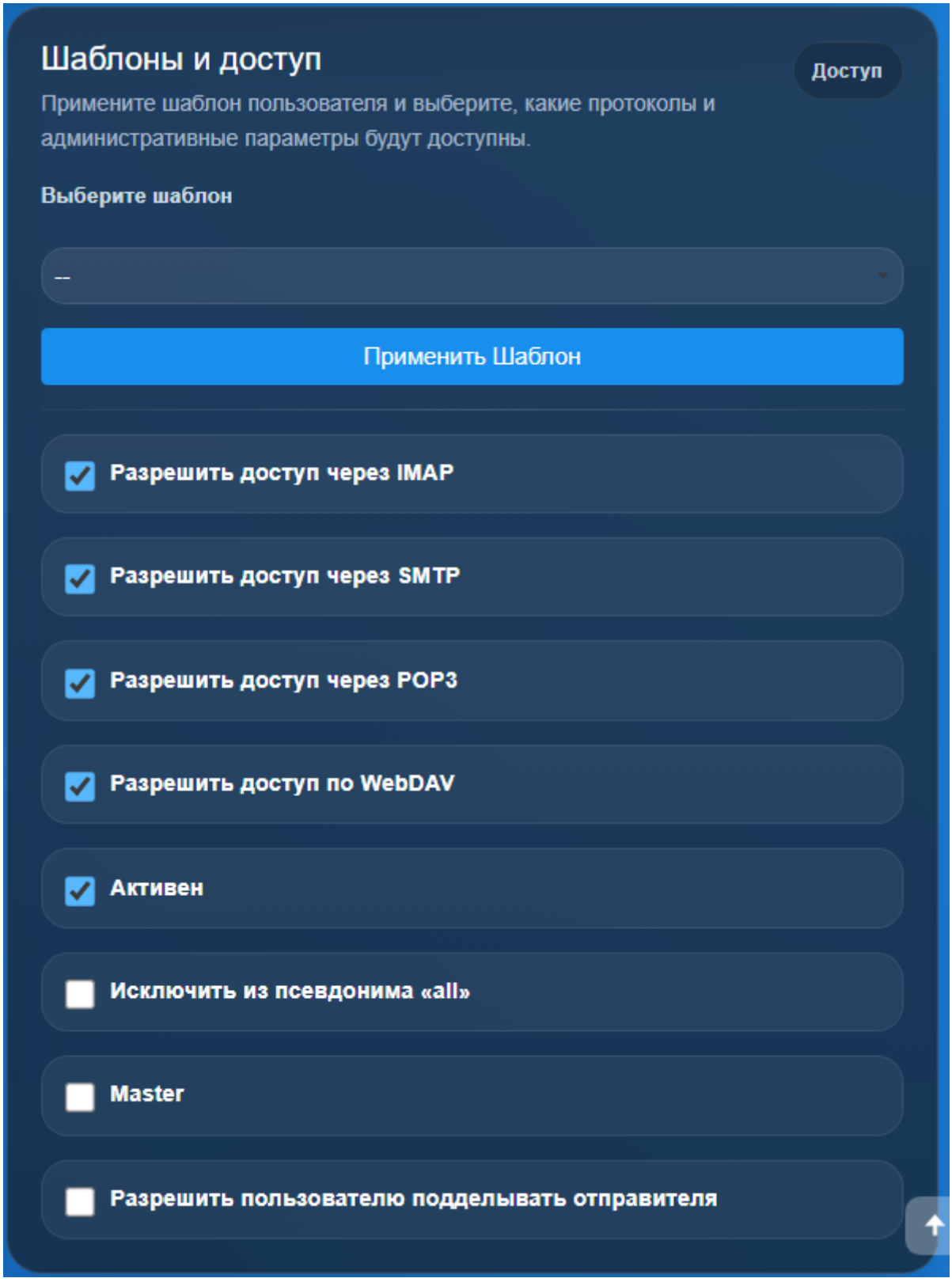


Рисунок 106 – Форма «Новый пользователь» Шаблоны и доступы

Отдельно настраивается доступ по протоколам: IMAP, SMTP, POP3 и WebDAV. Флажок «Активен» определяет, может ли пользователь входить в систему – снятие отметки блокирует ящик. Опция «Исключить из псевдонима all» исключает данный ящик из общего списка рассылки, охватывающего всех пользователей домена. Флаг «Master» предоставляет

учётной записи права суперпользователя, что обычно используется для служебных ящиков. Здесь же дублируется опция разрешения подделки отправителя для удобства.

Завершает форму раздел «Notes» (Заметки), предназначенный для административных комментариев (рисунок 107).

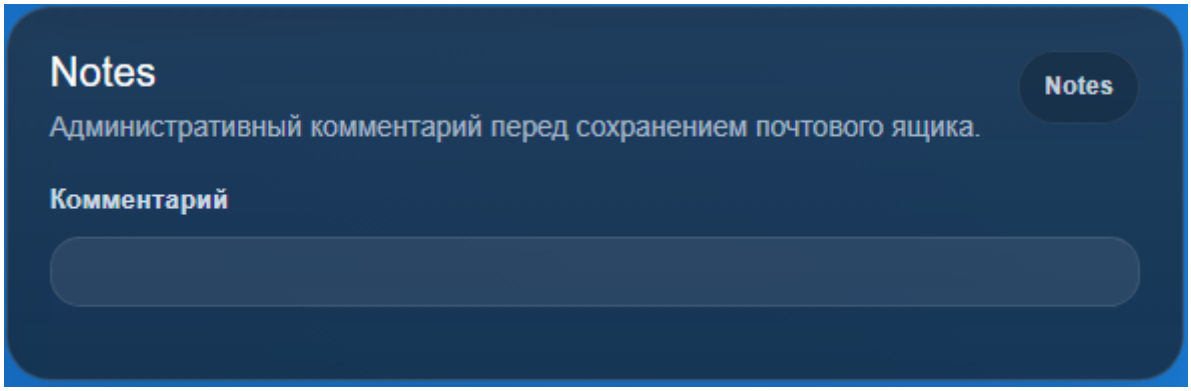
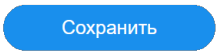


Рисунок 107 – Форма «Новый пользователь» Заметки

В текстовое поле можно внести любую служебную информацию, связанную с почтовым ящиком — например, дату создания, ответственного сотрудника или особые условия использования. Все внесённые изменения сохраняются после нажатия кнопки «Сохранить», расположенной в конце страницы. Система применяет настройки без необходимости перезагрузки сервисов, что обеспечивает оперативность администрирования.

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 102), и внести изменения в параметры (страница аналогична «созданию нового пользователя») пользователя в форме «Изменить пользователя» (рисунок 108).

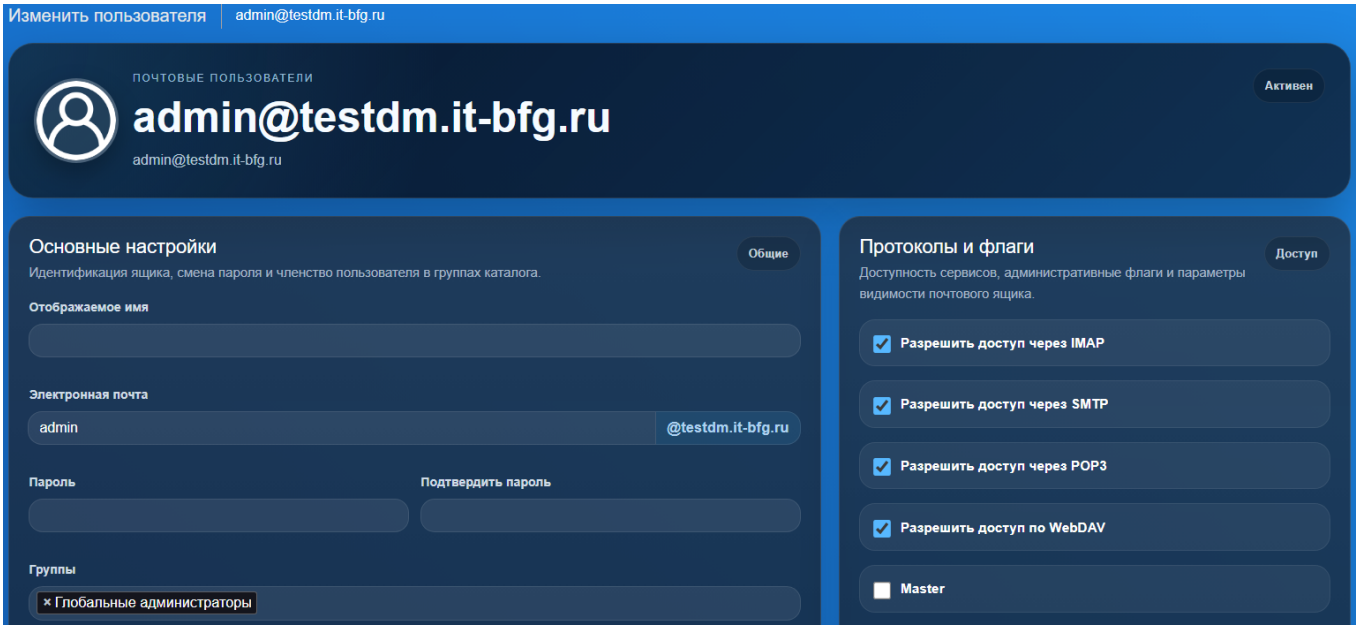


Рисунок 108 – Форма «Изменить пользователя»

При редактировании пользователя, добавляются дополнительные разделы, для просмотра состояния учетной записи (рисунок 109) и настройки двухфакторной аутентификации (2FA) (рисунок 110).

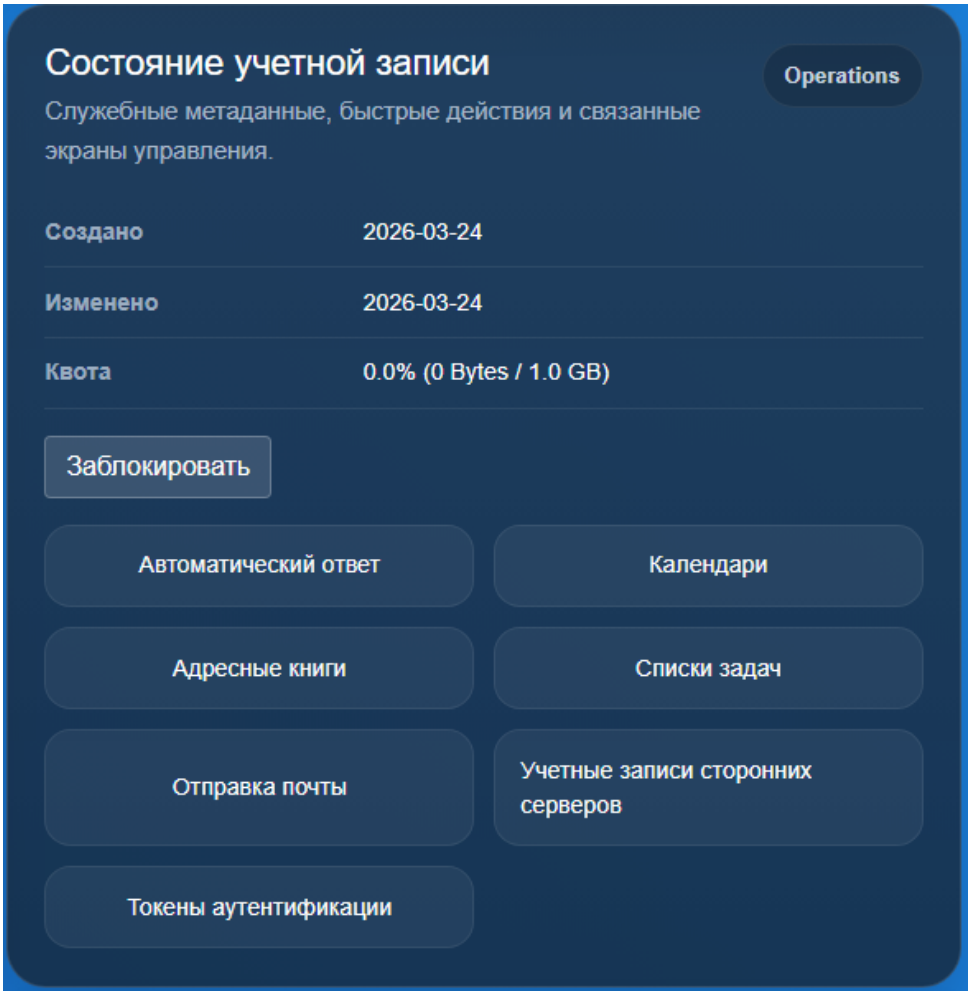


Рисунок 109 – Состояние учетной записи

В интерфейсе редактирования учётной записи пользователя раздел «Состояние учетной записи» предоставляет администратору сводную информацию о текущем статусе почтового ящика и инструменты для оперативного управления доступом к отдельным функциям.

В верхней части этого блока отображаются служебные метаданные: дата создания ящика и дата последнего изменения его параметров. Ниже приводится индикатор использования квоты, где наглядно показано, какой объём дискового пространства уже занят письмами, а какой остаётся доступным. Значение выводится в процентах, а также в байтах и гигабайтах, что позволяет быстро оценить, не приближается ли ящик к установленному лимиту.

Кнопка «Заблокировать», который дает возможность администратору временно приостановить доступ данного пользователя.

Также данный раздел позволяет управлять конкретным сервисам для данного пользователя - Автоматический ответ, Календарь, Адресные книги, Списки задач, Отправка почты, Учетные записи сторонних серверов, Токены аутентификации.

В форме редактирования учетной записи пользователя блок «Двухфакторная аутентификация» (рисунок 110) предназначен для мониторинга и административного управления дополнительным уровнем защиты почтового ящика.

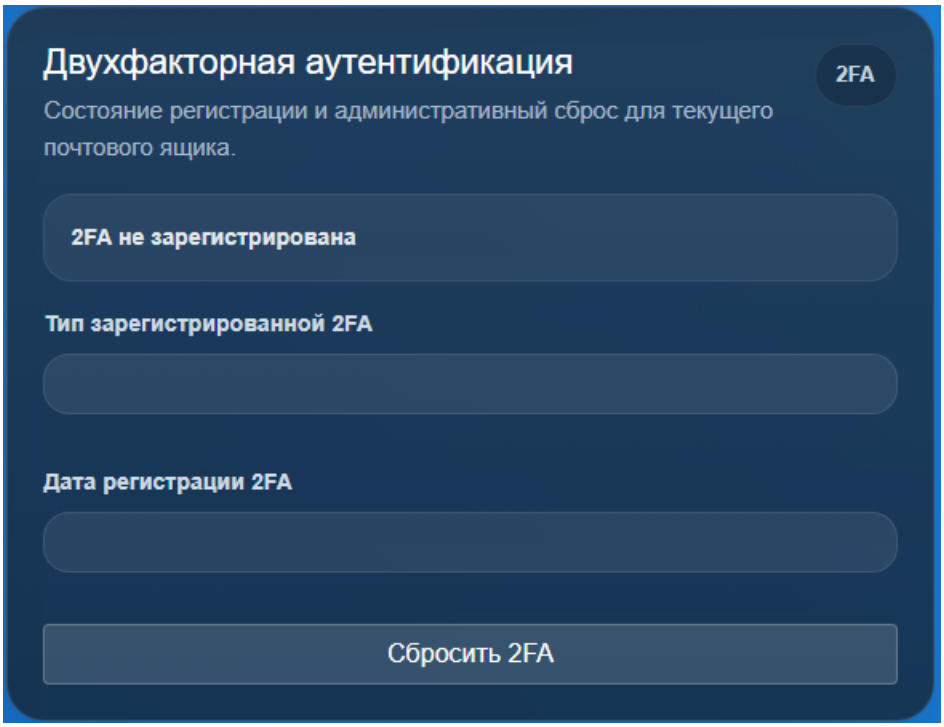
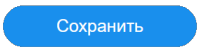


Рисунок 110 – Данные пользователя, подключенного через LDAP

Здесь администратор видит текущее состояние 2FA: сообщение «2FA не зарегистрирована» указывает на то, что пользователь ещё не настроил одноразовые коды, либо настройка была сброшена. Когда двухфакторная аутентификация активна, в полях «Тип зарегистрированной 2FA» (например, TOTP) и «Дата регистрации 2FA» отображается соответствующая информация.

Кнопка «Сбросить 2FA» позволяет администратору принудительно перезагрузить двухфакторную аутентификацию для данного почтового ящика. Это необходимо, если пользователь потерял доступ к приложению-аутентификатору, сменил устройство или забыл резервные коды. После сброса пользователь при следующем входе сможет заново настроить 2FA по стандартной процедуре (сканирование QR-кода). Такой механизм даёт администратору централизованный контроль над доступом, позволяя быстро восстанавливать учётные записи без потери данных, сохраняя при этом общую политику безопасности.

Включатель «Статус присутствия» устанавливает возможность пользователя включать и отключать в своем интерфейсе отображение статуса своего присутствия в сети. При включенном «Статус присутствия» в настройках пользователя на сервере в пользовательском веб-интерфейсе становится доступна настройка «Отображать статус присутствия в сети» с вариантами: «Для всех пользователей», «Только для своих контактов».

Внесите изменения и нажмите кнопку 

.

3.10.2.3 Настройка параметров автоответчика пользователя

Для настройки параметров автоответчика конкретного почтового ящика, требуется в разделе настройки пользователя (см. рисунок 109) нажать на кнопку 

, после чего откроется окно настройки автоответа для данного почтового ящика (рисунок 111).

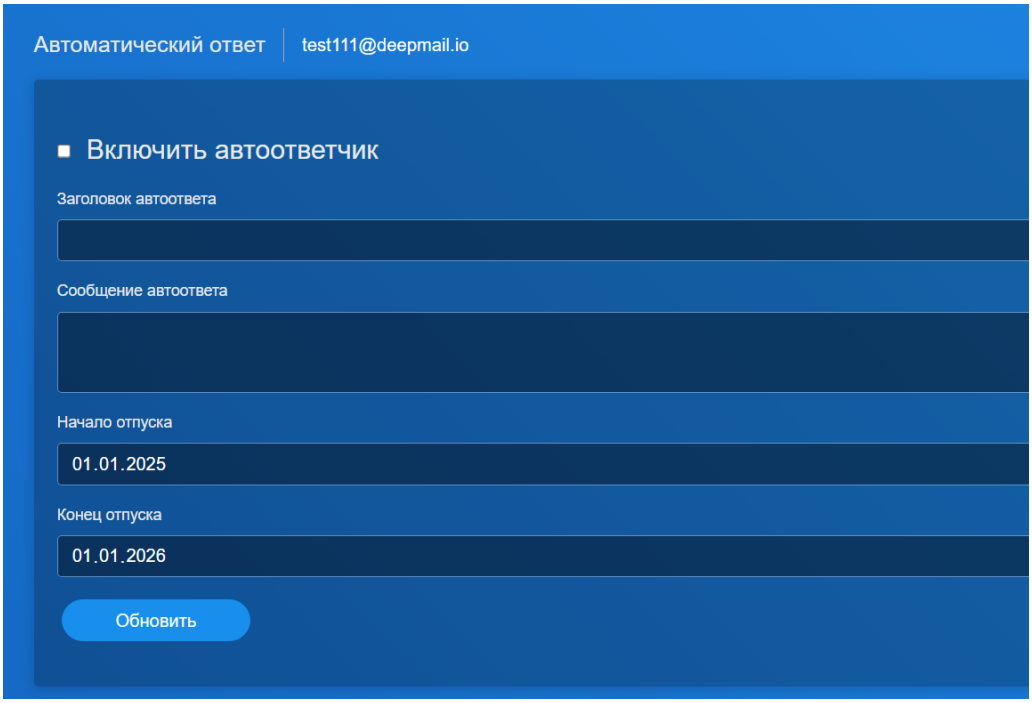
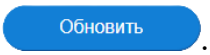


Рисунок 111 – Настройка автоответа пользователя

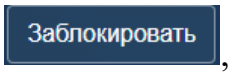
Для настройки автоответа требуется обязательно поставить «галочку» напротив надписи: «Включить автоответчик» и заполнить «Заголовок автоответа», «Сообщение автоответа» и даты начала и окончания работы автоответчика (например, на период отпуска).

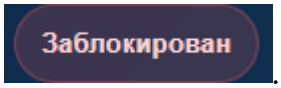
После внесения всей информации необходимо нажать кнопку 

.

3.10.2.4 Блокировка пользователя

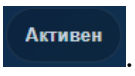
Заблокированные пользователи не могут отправлять и получать почту.

Для блокировки пользователя необходимо нажать кнопку 

, расположенную в разделе «Состояние учетной записи» (см. рисунок 109), при этом статус пользователя изменится на 

.

Для разблокировки пользователя необходимо нажать кнопку 

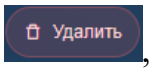
(будет размещена там же, что и кнопка блокировки), в результате чего статус пользователя изменится на 

.

Включатель «Заблокировать автоматически в случае неуспешной авторизации» предназначен для настройки автоматической блокировки пользователя на указанный отрезок времени в случае превышения им установленного количества неудачных попыток авторизации. При включении «Заблокировать автоматически в случае неуспешной

авторизации» на странице параметров пользователя появятся поля «Количество неудачных попыток авторизации» и «Период блокировки», в которых необходимо указать соответствующие значения.

3.10.2.5 Удаление пользователя

Для удаления пользователя необходимо нажать кнопку 

, расположенную на панели пользователя (см. рисунок 102), 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 112).

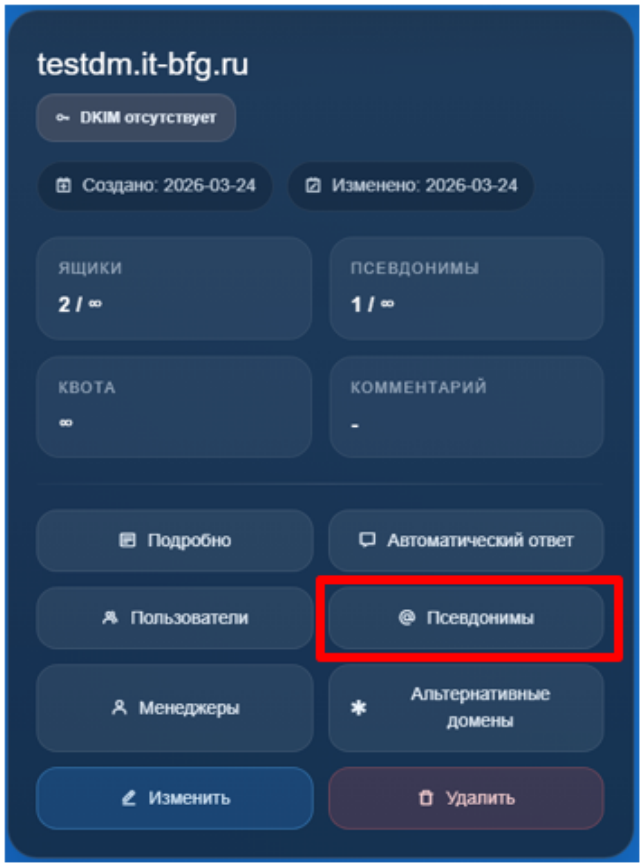
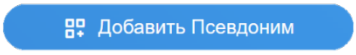


Рисунок 112 – Кнопка для перехода к созданию псевдонимов

На экране появится окно «Список псевдонимов» (рисунок 113).

Рисунок 113 – Окно «Список псевдонимов» пользователей домена

Нажмите кнопку  для открытия формы создания нового псевдонима (рисунок 114).

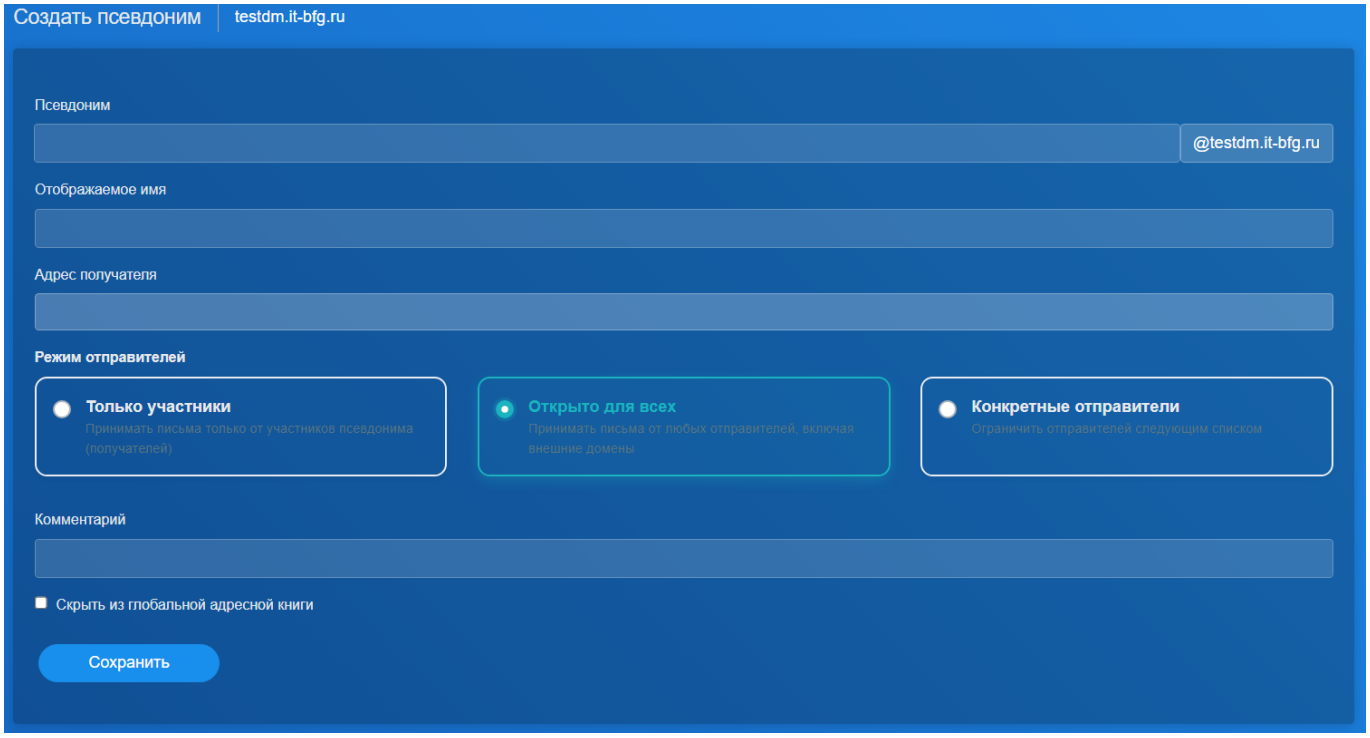
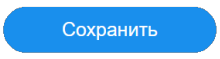


Рисунок 114 – Форма «Создать псевдоним»

В появившейся форме необходимо заполнить параметры: «Псевдоним» (электронный адрес псевдонима), «Отображаемое имя», «Адрес получателя» (существующий почтовый адрес или адрес домена), «Комментарий» (заполнять необязательно) и «Режим отправителей» (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 113), 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 115).

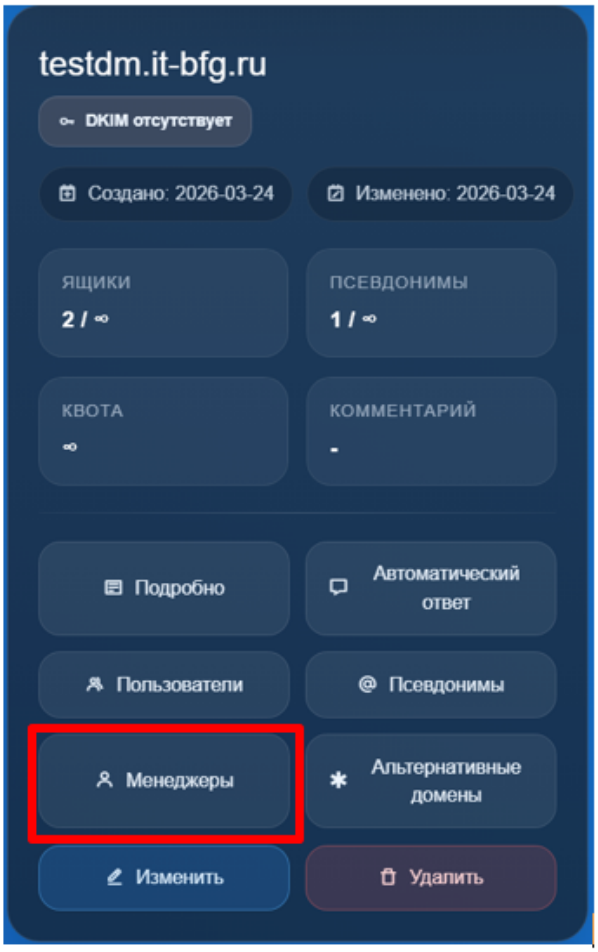


Рисунок 115 – Кнопка перехода к списку менеджеров домена на панели почтового домена

На экране появится окно «Список менеджеров» (рисунок 116).

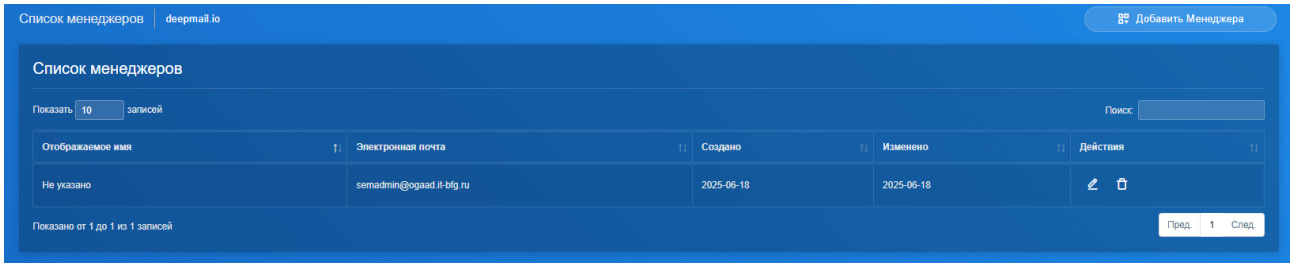


Рисунок 116 – Окно со списком менеджеров почтового домена

3.10.4.1 Добавление менеджера почтового домена

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

(см. рисунок 116).

На экране появится окно с формой «Добавить менеджера» (рисунок 117),

Рисунок 117 – Форма «Добавить менеджера»

Выбрать пользователя из выпадающего списка и нажмите кнопку 

.

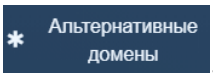
В результате выбранный пользователь появится в списке менеджеров.

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 116), 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 118).

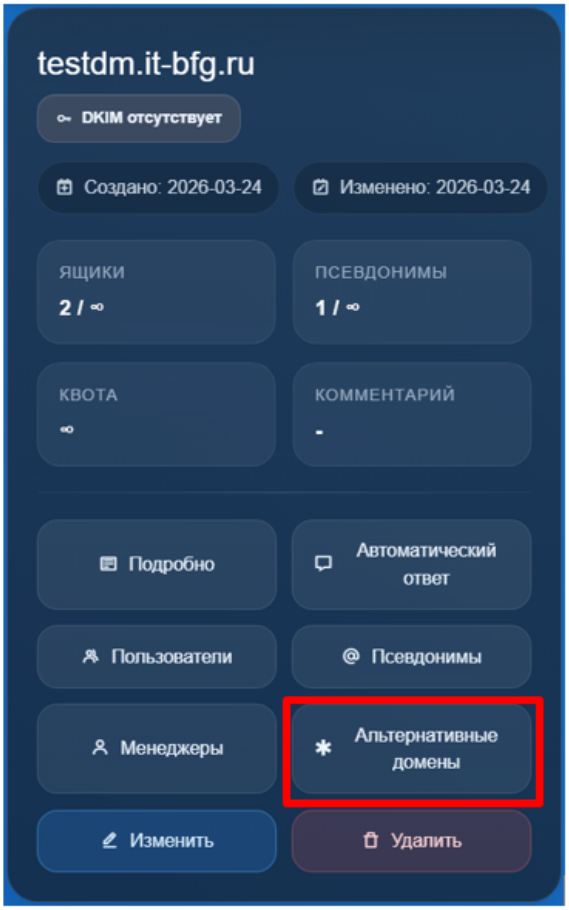


Рисунок 118 – Кнопка для перехода к списку альтернативных имен почтового домена

На экране появится окно «Список альтернативных доменов» (рисунок 119).

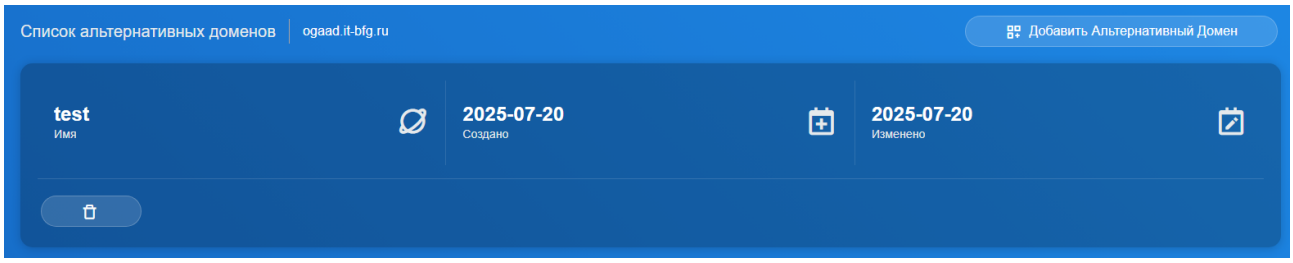
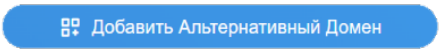
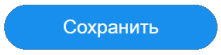


Рисунок 119 – Окно «Список альтернативных доменов»

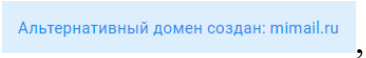
3.10.5.1 Создание альтернативного почтового домена

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

(см. рисунок 119). В открывшейся форме указать имя домена и нажать «Сохранить» 

(рисунок 120).

Рисунок 120 – Форма «Создать альтернативный домен»

В окне появится сообщение 

, а домен появится в списке альтернативных доменов (см. рисунок 119).

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 119), 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 121).

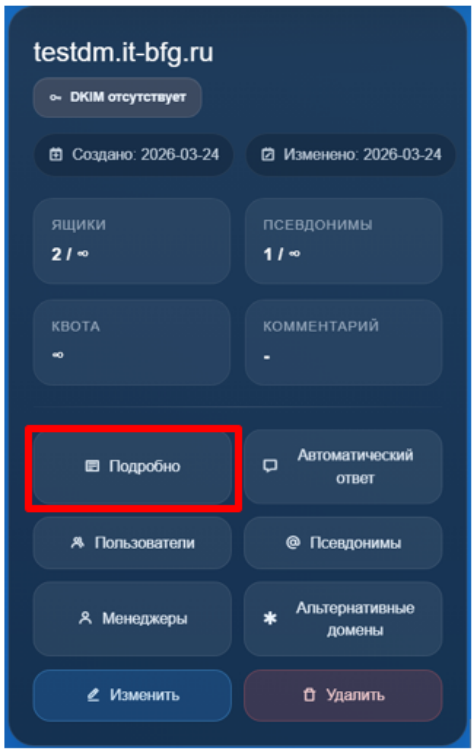


Рисунок 121 – Кнопка перехода к просмотру DNS записей домена

В результате откроется форма «Подробности домена» (рисунок 122).

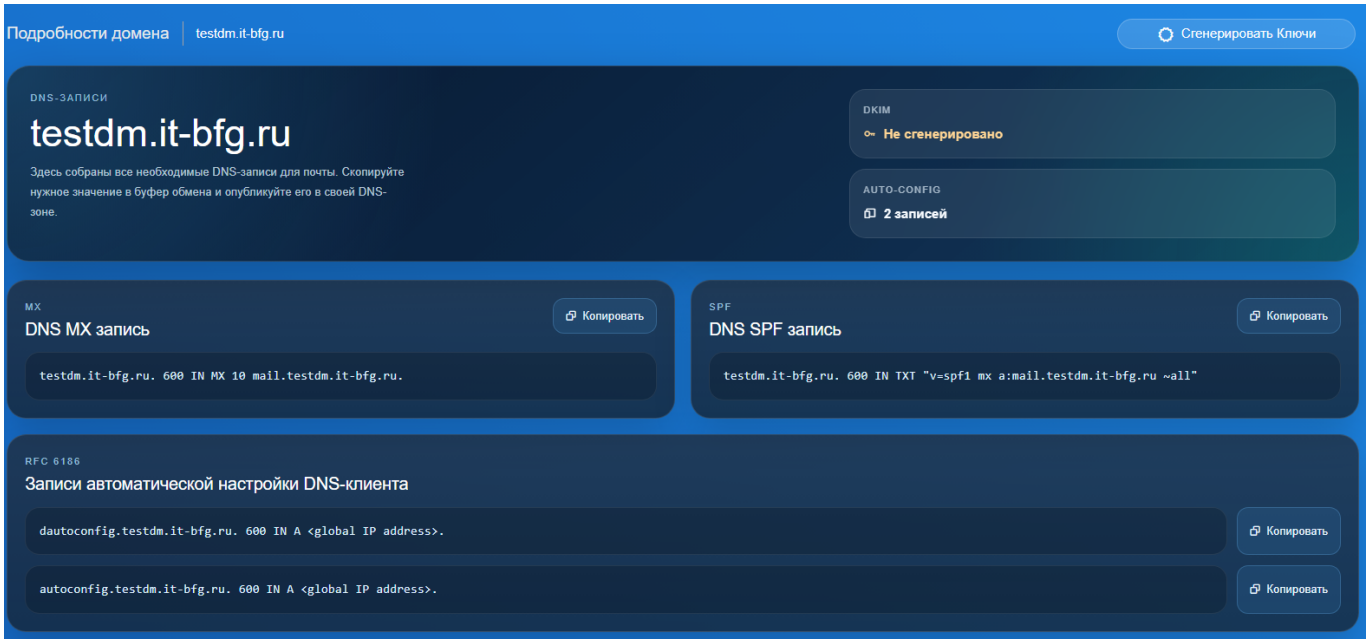


Рисунок 122 – Окно «Подробности домена»

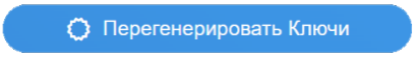
В окне «Подробности домена» приведена следующая информация:

- «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 122), 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 123.

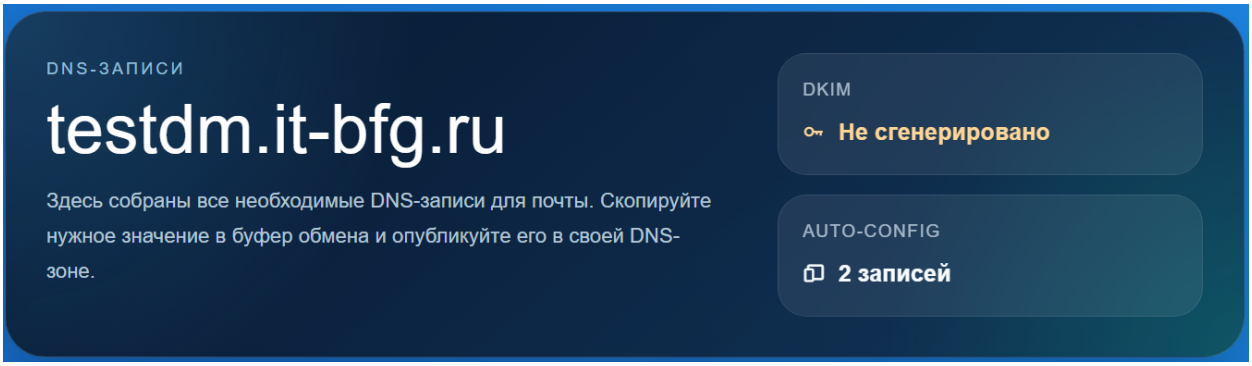
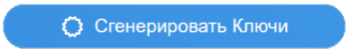


Рисунок 123 – Кнопка «Сгенерировать ключи»

Для генерации ключей необходимо в форме с подробной информацией о домене нажать кнопку 

(см. рисунок 123), и подтвердить действие в следующем окне (рисунок 124).

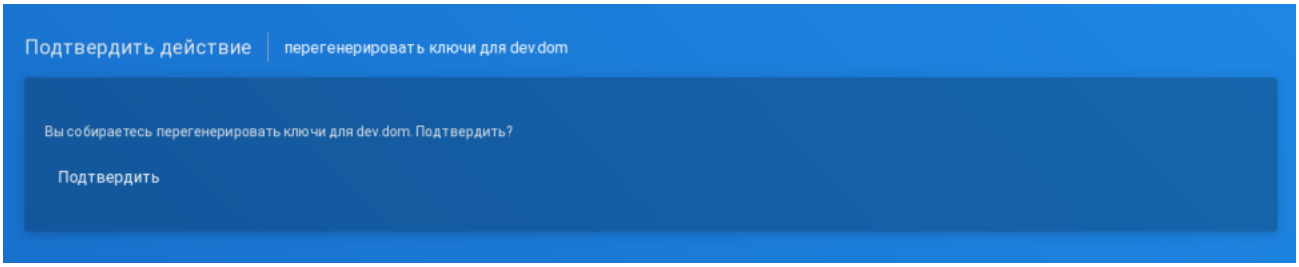
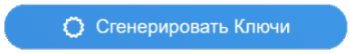
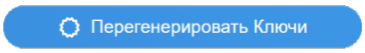


Рисунок 124 – Кнопка «Подтвердить»

После генерации ключа его текст копируется из появившегося после генерации раздела «ПУБЛИЧНЫЙ КЛЮЧ DKIM» и вставляется в «DNS DKIM запись», кнопка 

заменяется кнопкой 

(рисунок 125).

Рисунок 125 – 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	-

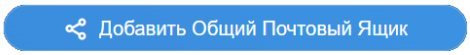
3.10.7 Управление общими почтовыми ящиками

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 пользователей» (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 126).

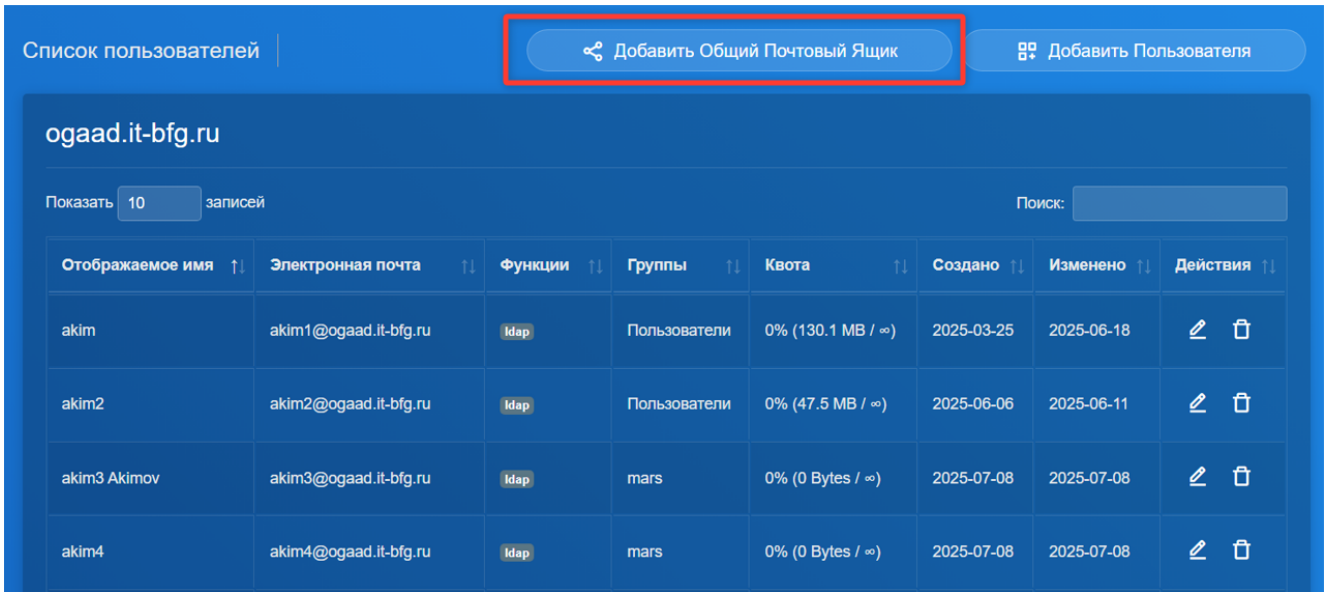


Рисунок 126 – Окно «Список пользователей»

На экране появится форма «Новый общий почтовый ящик» (рисунок 127).

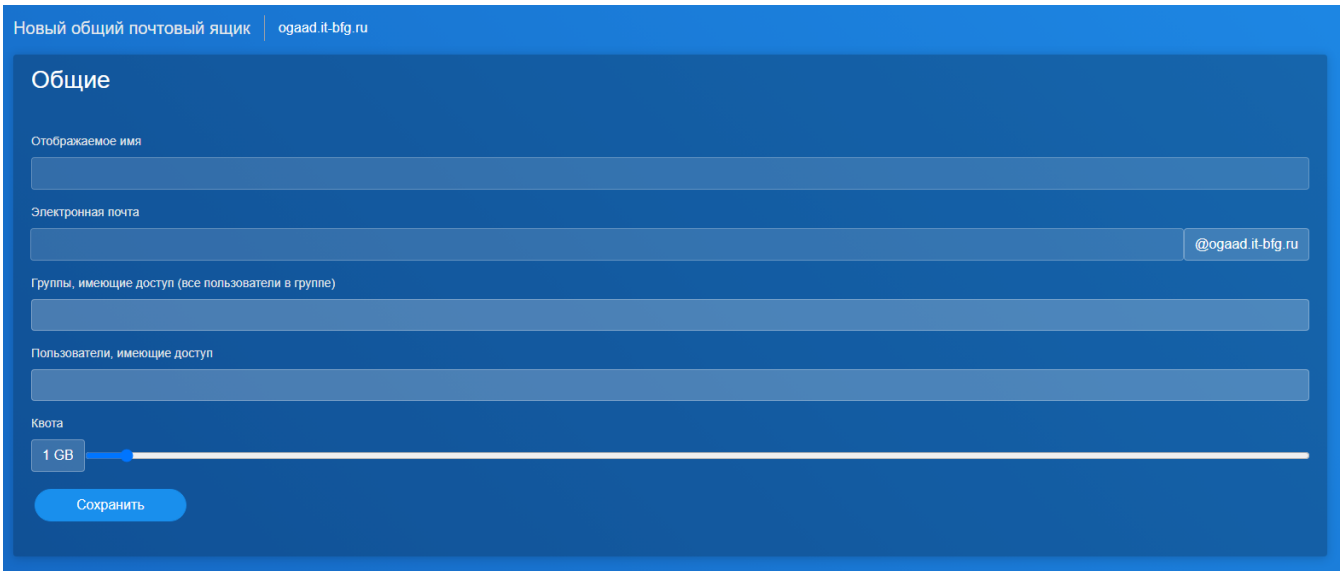


Рисунок 127 – Окно создания нового общего почтового ящика

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 127).

В списке пользователей в столбце «Функции» добавленный почтовый ящик отмечен как «Общий почтовый ящик» (рисунок 128).

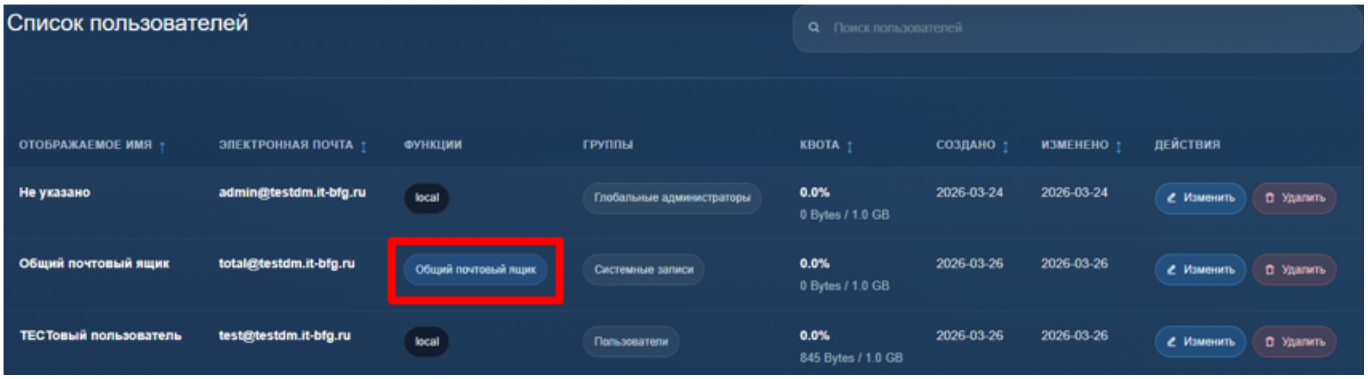


Рисунок 128 – Общий почтовый ящик в списке пользователей

3.10.7.2 Редактирование общего почтового ящика

Для перехода к форме редактирования общего почтового ящика необходимо нажать кнопку Изменить, расположенную в списке пользователей, в строке общего почтового ящика, столбец «Действия» (см. рисунок 128).

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 Удалить, расположенную в списке пользователей, в строке общего почтового ящика, столбец «Действия» (см. рисунок 128) 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;
- «Mail ACL», предназначенный для настройки прав к общим папкам или делегированным почтовым папкам;
- «Список переадресаций», предназначенный для настройки переадресации писем с почтовых ящиков (рисунок 129).

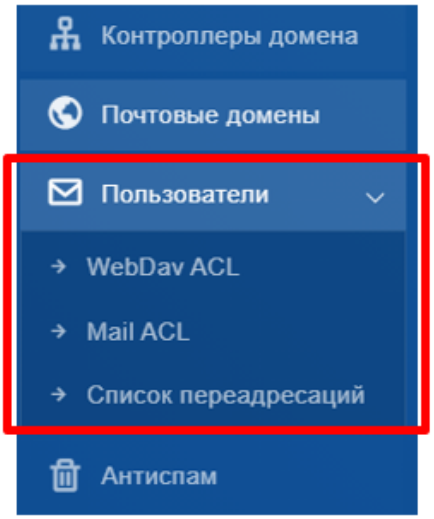


Рисунок 129 – Инструмент «Пользователи»

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 129).

На экране отобразится окно «Пользователи WebDav ACL», в котором приведена информация о настроенных правах делегирования для конкретных пользователей (рисунок 130).

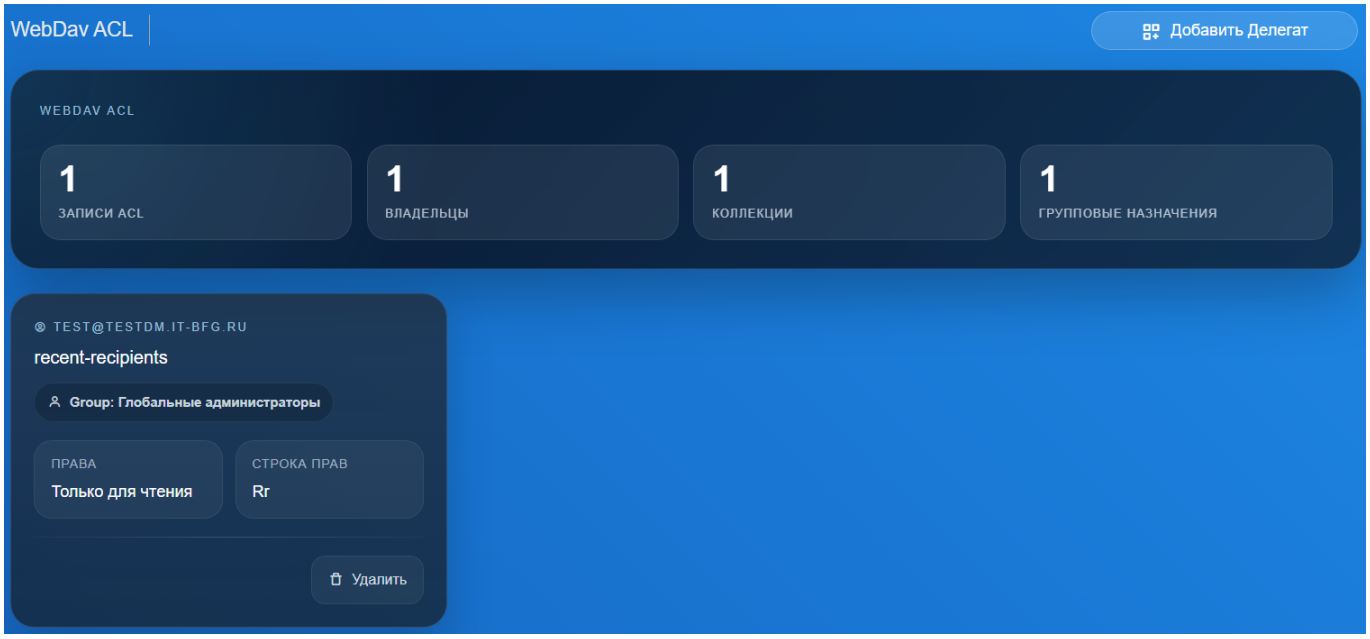
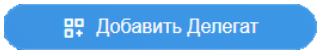


Рисунок 130 – Окно «WebDav ACL»

Делегирование осуществляется в рамках одного домена.

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

(см. рисунок 130), после чего откроется окно настройки делегирования «Добавить делегат» (рисунок 131).

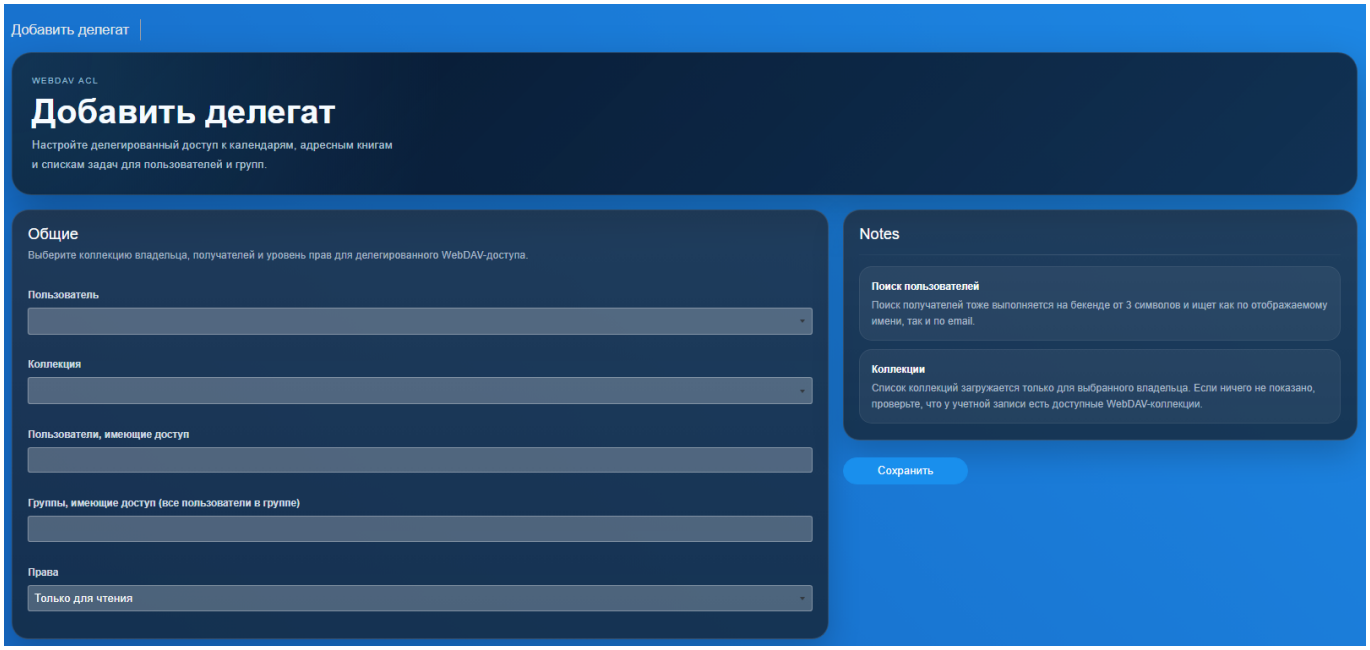


Рисунок 131 – Настройка делегирования

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).

Для сохранения внесенных изменений необходимо нажать кнопку Сохранить.

3.11.2 Пользователи Mail ACL

Интерфейс «Mail ACL» предоставляет администратору инструменты для управления списками контроля доступа к почтовым папкам пользователя (рисунок 132).

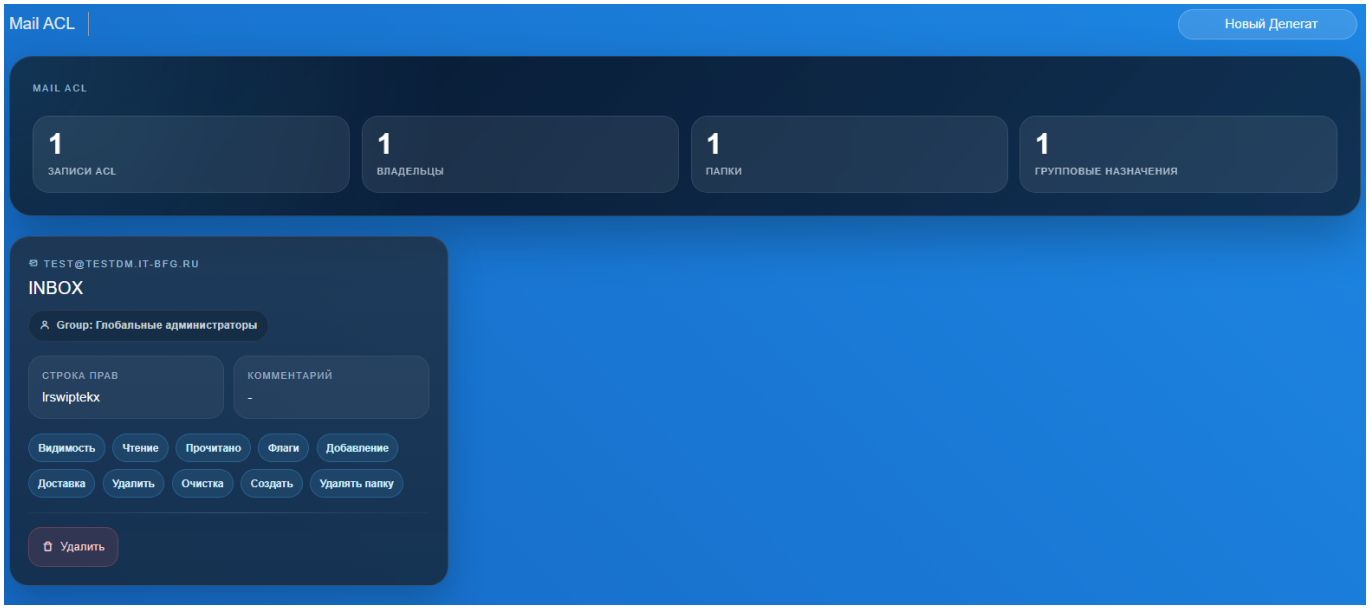
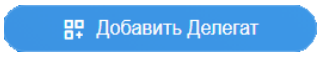


Рисунок 132 – Настройка делегирования Mail ACL

В верхней части отображается сводная статистика: количество записей ACL, число владельцев папок и количество групповых назначений. Центральная область перечисляет конкретные назначения прав, а также указывает группу, которой эти права предоставлены.

Ниже представлена таблица прав, где строка «lrswiptekx» является стандартной строкой ACL, каждая буква которой обозначает определённое разрешение: l (список), r (чтение), s (просмотр флагов), w (запись), i (вставка), p (отправка), t (удаление), e (удаление папки), k (создание папки), x (администрирование). Для удобства настройки предусмотрены кнопки быстрого назначения типовых прав: «Ведомость» (управление метаданными), «Чтение», «Прочитано» (отметка о прочтении), «Флаги», «Добавление», «Доставка», «Удалить», «Очистка», «Создать» (папку), «Удалить папку». Кнопка «Удалить» позволяет полностью отозвать права для выбранной записи.

Таким образом, интерфейс позволяет гибко делегировать доступ к почтовым папкам, задавая комбинации разрешений для отдельных пользователей или групп. Это особенно полезно для организации совместной работы, когда, например, секретарю требуется доступ к папкам руководителя, или для централизованного управления правами через группы администраторов.

Чтобы делегировать права необходимо в окне «Mail ACL» нажать кнопку 

(рисунок 132), после чего откроется окно настройки делегирования «Добавить делегат» (рисунок 133), в котором будут разделы общих настроек (рисунок 134), настроек папок (рисунок 135) и заметки (рисунок 136).

Рисунок 133 – Добавить делегат Mail ACL

В интерфейсе управления правами доступа к папкам (Mail ACL) администратор может гибко настраивать, кто и какие действия может выполнять с почтовыми папками конкретного пользователя.

Форма общих настроек назначения прав открывается после выбора целевой учетной записи и позволяет задать три основных параметра: «Пользователь» (владелец папки, для которой настраивается доступ), «Почтовая папка» (путь к папке, например, INBOX или любая пользовательская папка) и «Комментарий» (произвольное примечание) (рисунок 134).

Рисунок 134 – Общая настройка Mail ACL

Затем в полях «Пользователи, имеющие доступ» и «Группы, имеющие доступ» администратор добавляет учетные записи или группы, которым предоставляются права (см. рисунок 134). Это может быть, например, секретарь, которому требуется доступ к папкам руководителя, или группа сотрудников, отвечающих за определённый проект.

Сами права представляют собой набор десяти дискретных разрешений (рисунок 135, рисунок 136), каждое из которых кодируется одной буквой в стандартной строке ACL.

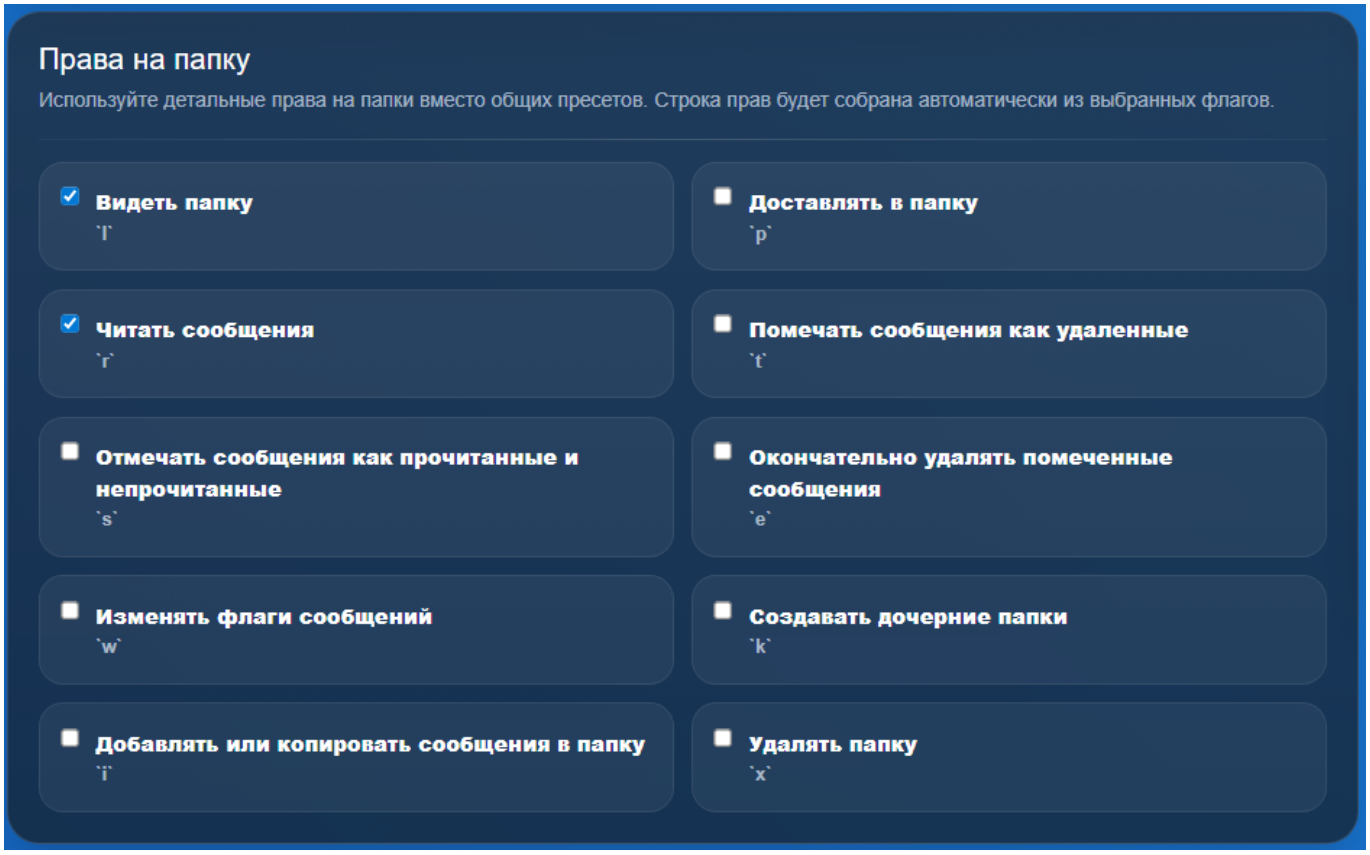


Рисунок 135 – Настройка прав на папку Mail ACL

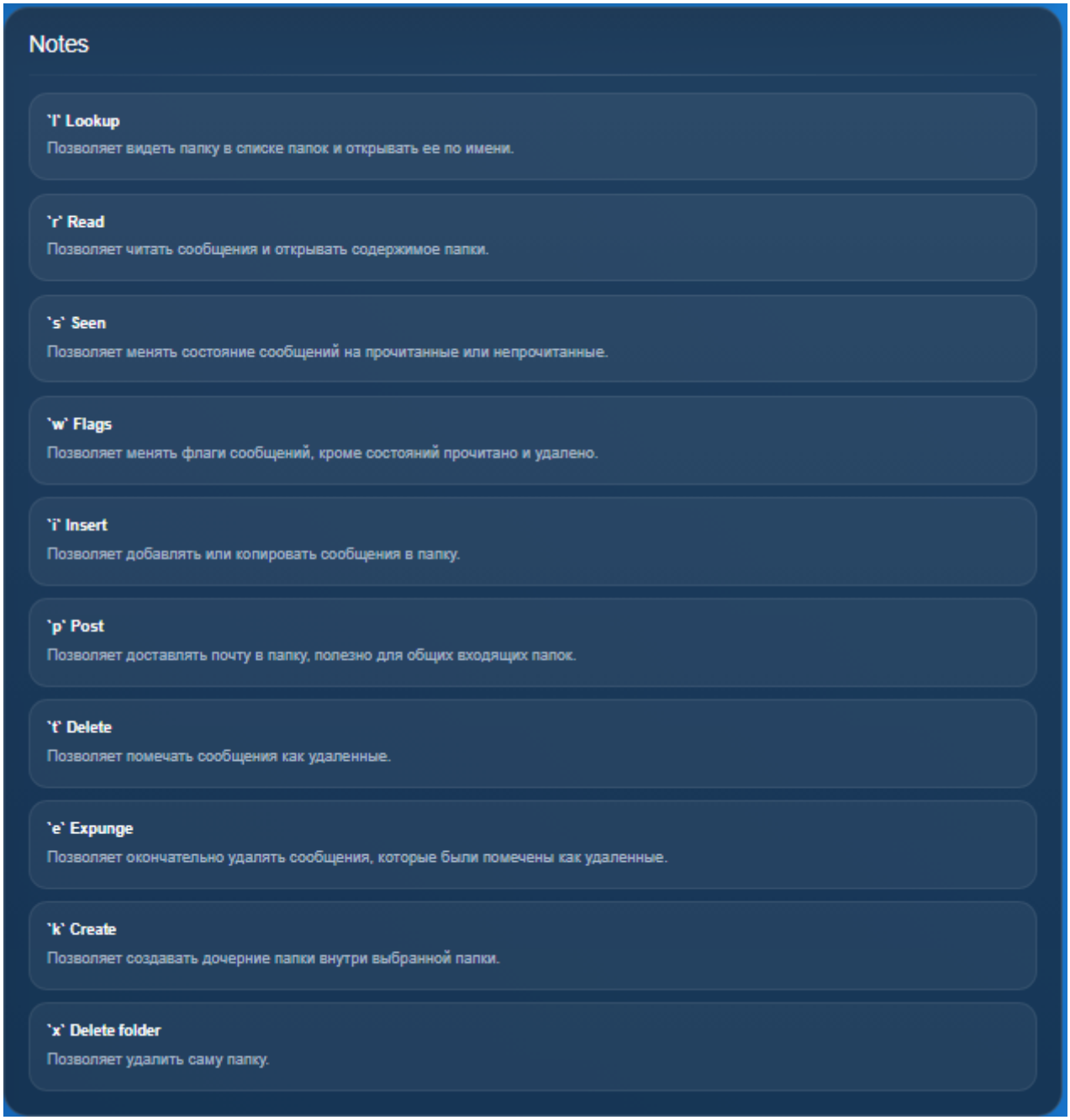


Рисунок 136 – Mail ACL заметки

Интерфейс предоставляет два способа управления этими правами: визуальный выбор через флажки и прямое редактирование строки. В панели «Права на папку» все разрешения представлены в виде чекбоксов с понятными описаниями. Администратор может включить или отключить каждое из них:

- Видеть папку (l) – позволяет папке отображаться в списке и открываться по имени.
- Читать сообщения (r) – даёт возможность читать письма и просматривать содержимое папки.
- Отмечать сообщения как прочитанные и непрочитанные (s) – разрешает изменять статус прочтения.

– Изменять флаги сообщений (w) – позволяет устанавливать любые флаги (кроме Seen и Deleted).

– Добавлять или копировать сообщения в папку (i) – разрешает вставку новых сообщений.

– Доставлять в папку (p) – даёт возможность доставлять почту напрямую (полезно для общих входящих папок).

– Помечать сообщения как удалённые (t) – позволяет ставить флаг удаления.

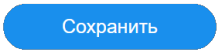
– Окончательно удалять помеченные сообщения (e) – разрешает окончательную чистку удалённых писем.

– Создавать дочерние папки (k) – позволяет создавать подпапки внутри данной.

– Удалять папку (x) – даёт право удалить саму папку.

При изменении чекбоксов строка прав автоматически формируется из выбранных букв, что исключает ошибки ручного ввода. Альтернативно, если администратору известна строка (например, lrswiptekx для полных прав), он может скопировать её непосредственно в соответствующее поле. Кнопка «Удалить» в карточке назначения позволяет отозвать все права для выбранного пользователя или группы.

Такой подход позволяет точно контролировать доступ к почтовым папкам, обеспечивая безопасность и удобство совместной работы. Например, можно дать секретарю право читать и изменять флаги, но запретить удаление папок, а технической группе – полный доступ для администрирования.

Для сохранения внесенных изменений необходимо нажать кнопку 

.

3.11.3 Список переадресаций

Для настройки переадресаций необходимо в меню интерфейса администратора выбрать «Пользователи» → «Список переадресаций» (рисунок 137).

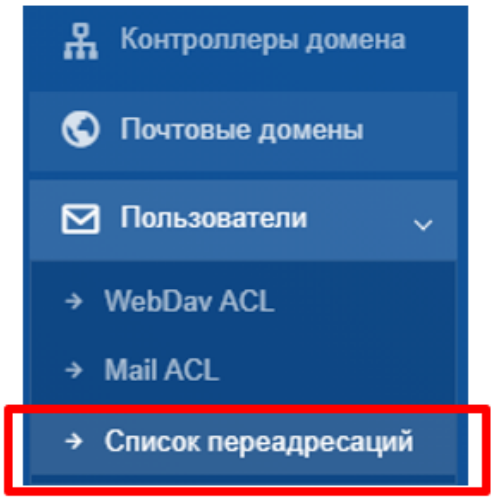
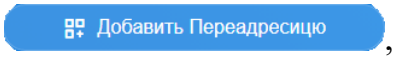


Рисунок 137 – Инструмент «Список переадресаций»

Для настройки переадресации необходимо в окне со списком переадресаций нажать кнопку 

, после чего откроется окно «Добавить переадресацию» для настройки переадресаций (рисунок 138).

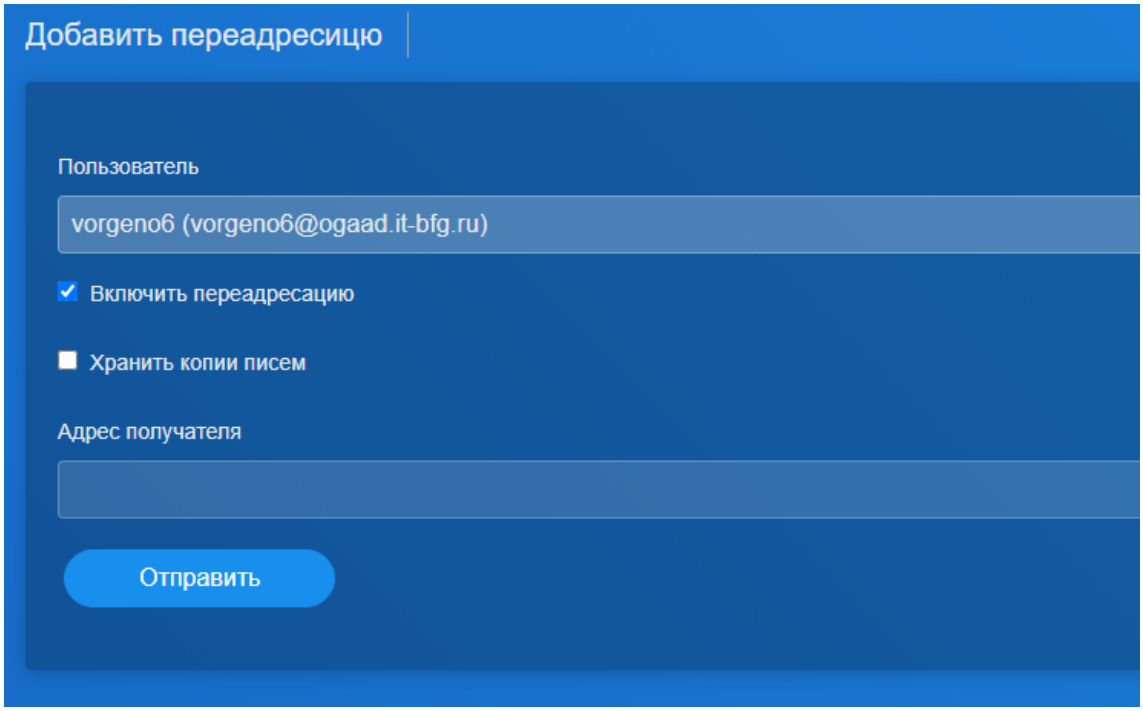


Рисунок 138 – Настройка переадресаций

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 Отправить (см. рисунок 138).

3.12 Инструмент «Антиспам»

Для перехода к инструменту работы со спам-фильтром необходимо в меню интерфейса администратора выбрать «Антиспам» (рисунок 139).

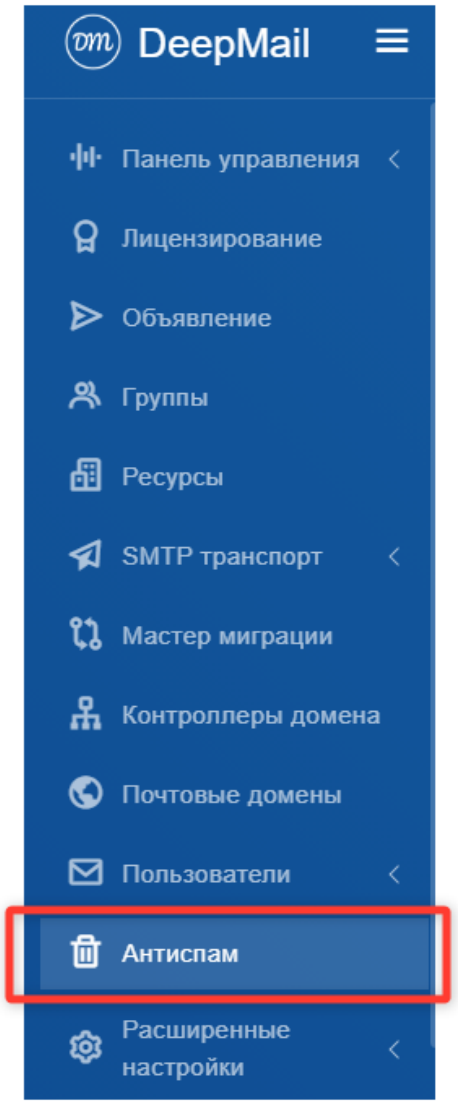


Рисунок 139 – Инструмент «Антиспам»

В результате появится окно системы фильтрации спама RSPAMD, содержащее статистические данные и информацию о параметрах спам-фильтрации (рисунок 140).

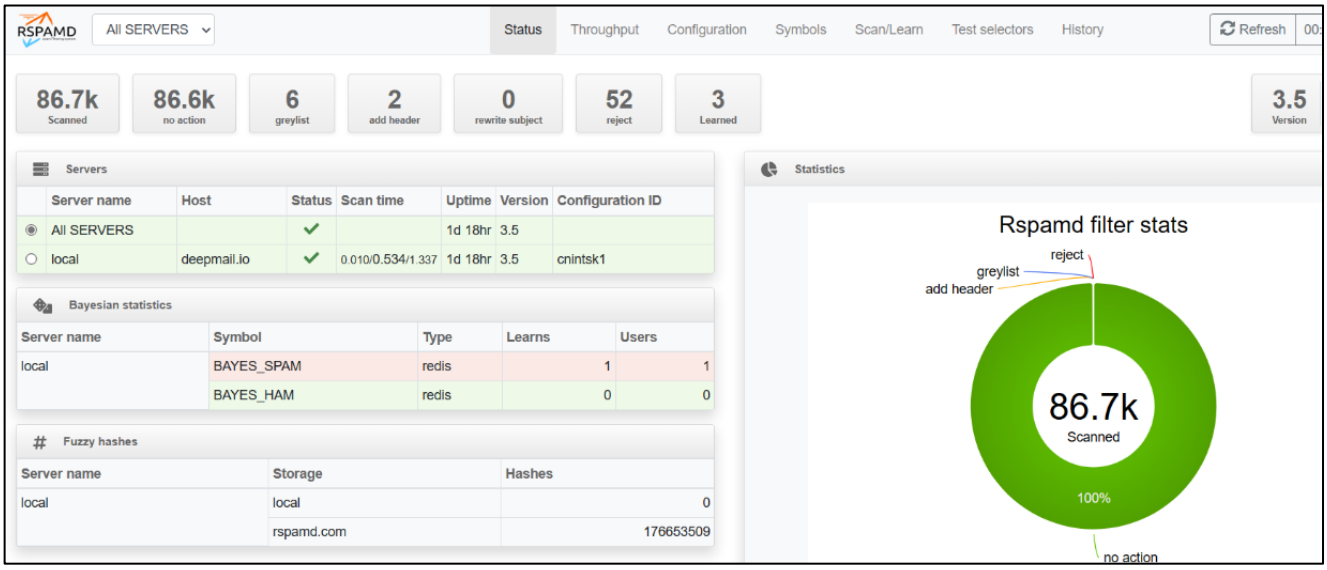


Рисунок 140 – Окно системы RSPAMD

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 141).

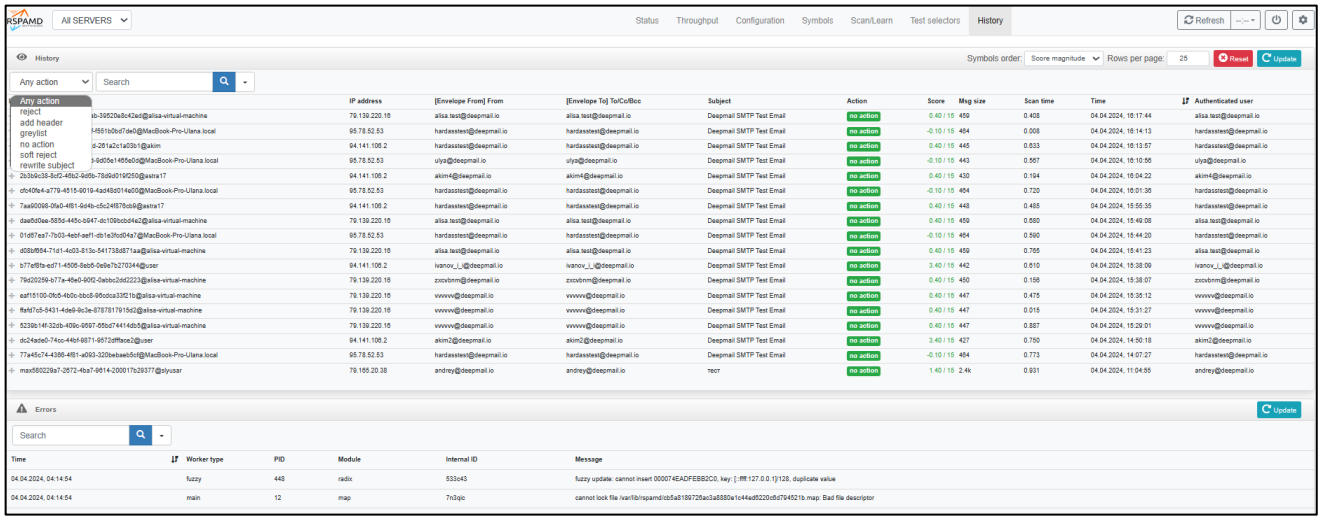


Рисунок 141 – Окно системы RSPAMD, вкладка «History»

3.12.1 Настройка антиспама по тексту в письме

Для настройки блокировки входящих писем, по определенным словам, в теле письма, необходимо создать файл *body_blockllist.map* в директории */mnt/deepmail/core/filter/maps/*.

Далее необходимо открыть файл и сформировать текст в следующем формате:

#Первое правило

Exemple first

#Второе правило

Exemple second

Где *Exemple first* и *Exemple second* является словами, по которым будет блокироваться входящие письма. Соответственно для точечной настройки правил, требуется вносить соответствующие слова, по которым будет блокироваться входящая почта.

3.12.2 Настройка антиспама по черным и белым спискам

В системе DeepMail для фильтрации спама используется Rspamd. Для тонкой настройки фильтрации администратор может создавать собственные черные и белые списки адресов отправителей и доменов. Это позволяет гарантированно пропускать письма от надежных отправителей (белый список) или блокировать нежелательную корреспонденцию (черный список) еще до применения статистических алгоритмов.

Конфигурационных файлы списков размещаются в каталоге переопределений конфигурации Rspamd:

mkdir -p /mnt/deepmail/core/overrides/rspamd

touch /mnt/deepmail/core/overrides/rspamd/blacklist.map

touch /mnt/deepmail/core/overrides/rspamd/whitelist.map

blacklist.map – список адресов и доменов, письма от которых должны блокироваться.

whitelist.map – список адресов и доменов, письма от которых должны пропускаться без проверки (или с пониженным весом спама).

Формат записей при редактировании белового и черного списков может содержать:

Полный электронный адрес: *user@example.com*

Домен (без символа @): *example.com*

Пример содержимого blacklist.map:

text

spammer@mail.ru

bad-domain.org

**@temp-mail.org*

Пример содержимого whitelist.map:

text

trusted-partner.com

admin@my-company.ru

После добавления или изменения записей не требуется перезапускать Rspamd, если файлы подключены через map с автоматической перезагрузкой. Однако в DeepMail по умолчанию используется стандартная процедура перезапуска нод для гарантированного применения конфигурации. Строки, начинающиеся с #, игнорируются (можно использовать для комментариев).

После редактирования файлов необходимо перезапустить ноды DeepMail, чтобы Rspamd перечитал конфигурацию:

deepmail stop

deepmail start

Примечание: Команда *deepmail stop/start* останавливает и запускает все сервисы, что может вызвать временную недоступность почтовой системы. Планируйте такие действия в периоды наименьшей нагрузки.

Рекомендуется вести списки аккуратно, не добавляйте слишком много записей без необходимости – это может замедлить обработку почты. Периодически требуется контролировать актуальность белых списков, удаляя устаревшие домены.

Для доменов, которые должны быть всегда в белом списке (например, корпоративные), рекомендуется использовать запись в виде *@domain.com*, чтобы пропускать все адреса этого домена.

Следуя этой инструкции, вы сможете гибко управлять фильтрацией спама в DeepMail и обеспечить надежную защиту почтовой системы.

3.13 Инструмент «Поиск писем»

Для перехода к инструменту поиска писем необходимо в меню интерфейса администратора выбрать «Поиск писем» (рисунок 142).

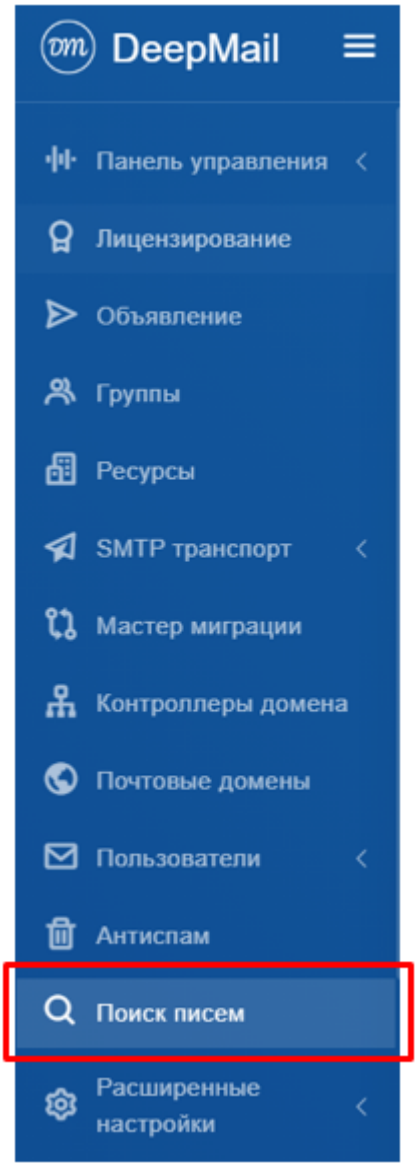


Рисунок 142 – Инструмент «Поиск писем»

Интерфейс представляет собой инструмент для расширенного поиска по почтовому архиву, организованный по принципу управления задачами (рисунок 143).

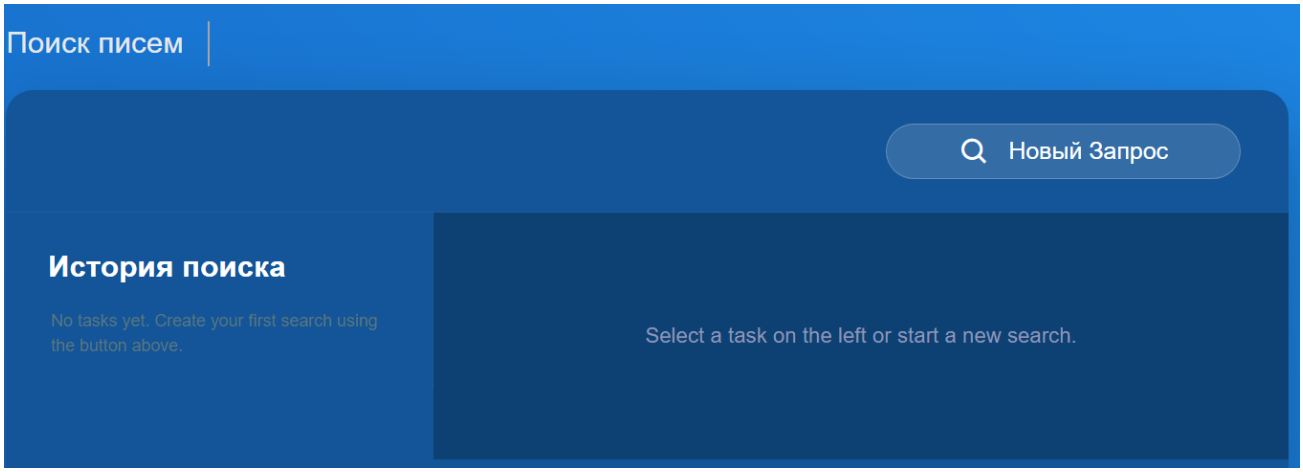


Рисунок 143 – Интерфейс «Поиск писем»

Окно разделено на две основные панели. Левая сторона отведена под историю поисковых запросов, где будут отображаться сохранённые или ранее выполненные задачи. В начальном состоянии она пуста, предлагая пользователю создать первый запрос.

Правая, основная рабочая область, в текущий момент содержит приглашение к действию: предложение выбрать задачу из истории или начать новый поиск. Кнопка «Новый Запрос» является центральным элементом, запускающим процесс создания сложного поискового запроса, вероятно, с возможностью задания множества критериев (метаданных, периода, отправителей, тем и т.д.).

Таким образом, интерфейс предназначен для выполнения нестандартных, возможно, массовых или регулярных поисковых операций в почтовой системе, обеспечивая структурированный подход через сохранение и повторное использование поисковых сценариев.

3.14 Инструмент «Расширенные настройки»

Инструмент администрирования «Расширенные настройки» содержит подразделы: «Настройки SSL/TSL», «Настройки конфигурации» и «Шаблоны пользователей» (рисунок 144).

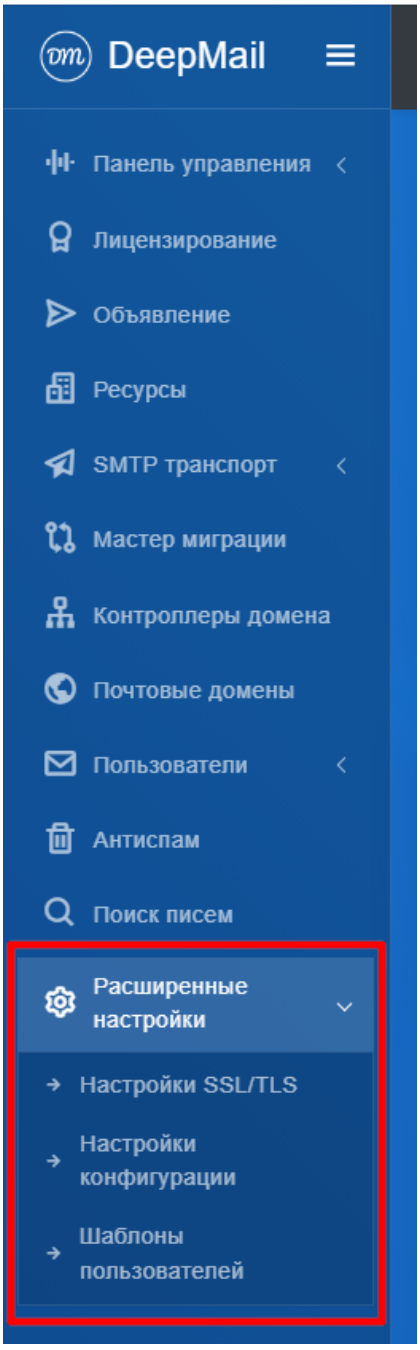


Рисунок 144 – «Расширенный настройки»

3.14.1 «Настройки SSL/TLS»

Для перехода к настройкам SSL/TLS необходимо в меню «Расширенные настройки» интерфейса администратора выбрать «Настройки SSL/TLS» (рисунок 145).

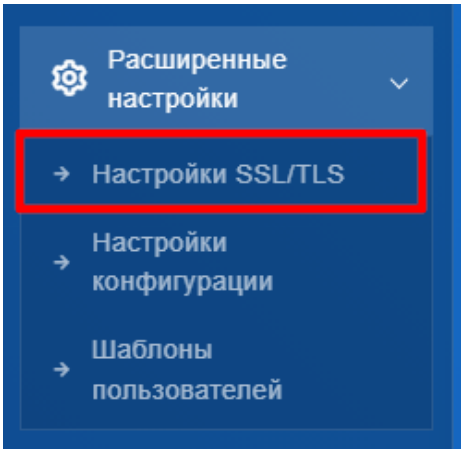


Рисунок 145 – «Настройки SSL/TLS»

На экране отобразится окно «Настройки SSL/TLS» (рисунок 146).

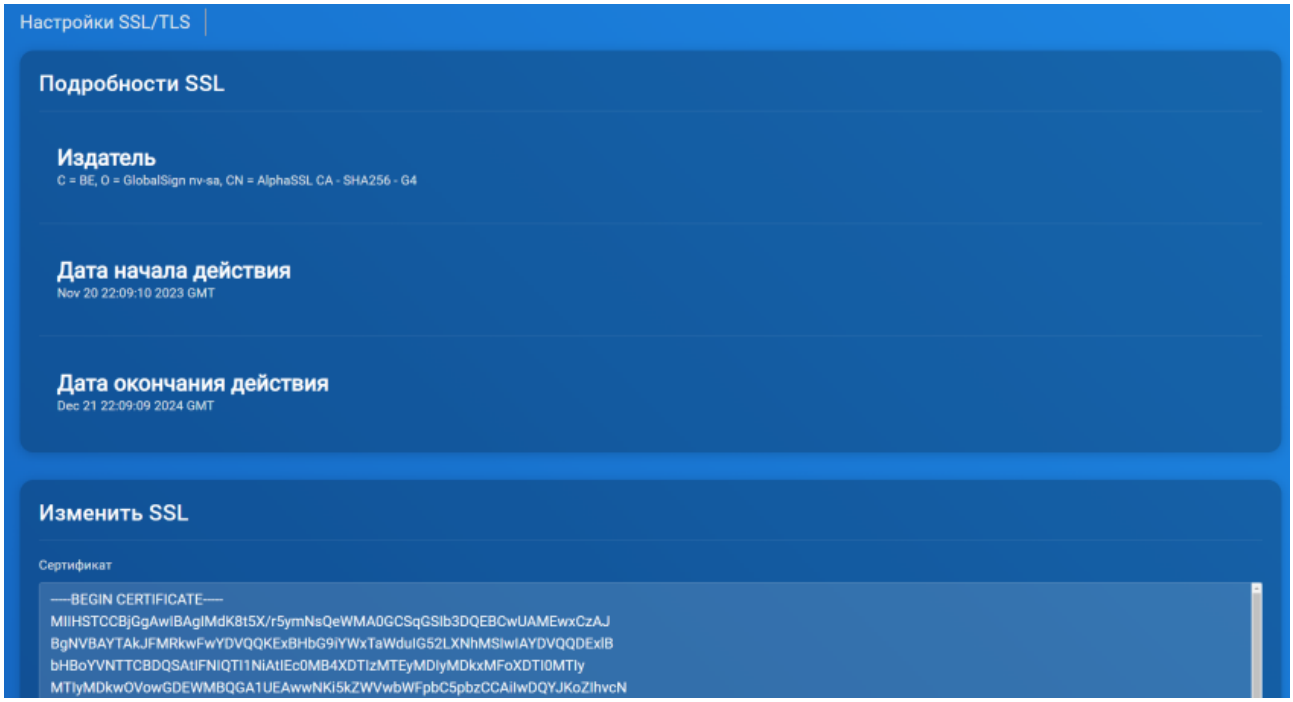


Рисунок 146 – Окно инструмента «Настройки SSL/TLS»

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:

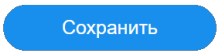
-----END CERTIFICATE-----

, а ключ:

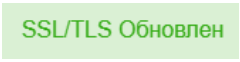
-----END PRIVATE KEY-----

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 146) 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 147).

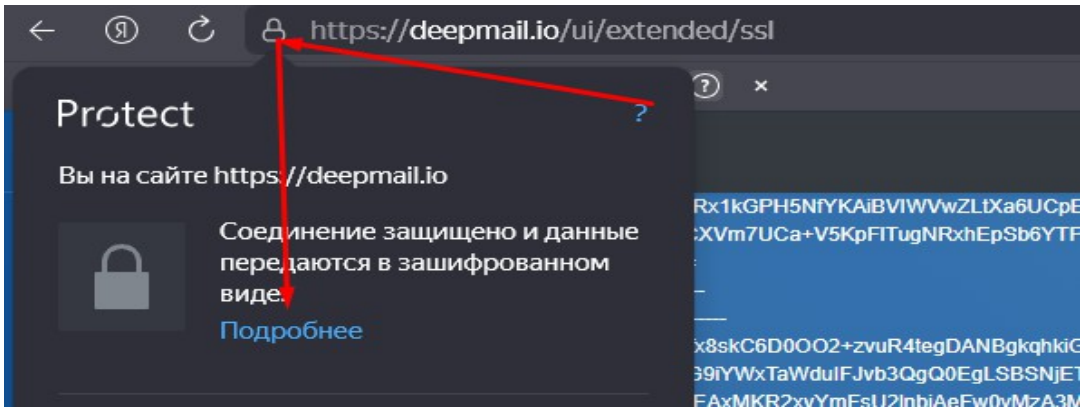


Рисунок 147 – Проверка обновления сертификатов

3.14.2 «Настройка конфигурации»

Для перехода к настройкам конфигурации необходимо в меню «Расширенные настройки» интерфейса администратора выбрать инструмент «Настройки конфигурации» (рисунок 148).

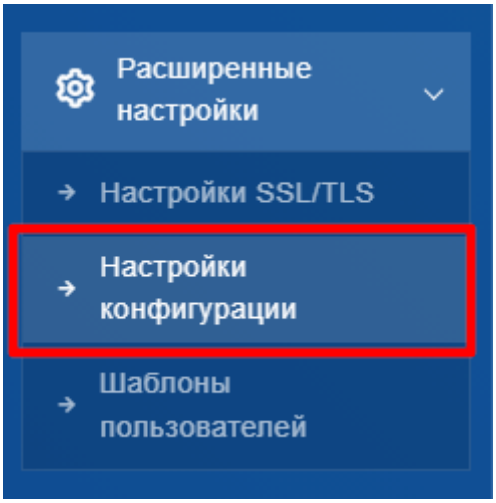


Рисунок 148 – Инструмент «Настройки конфигурации»

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 149).

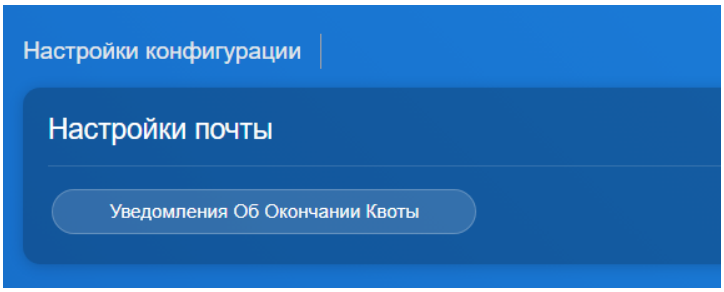


Рисунок 149 – Окно «Настройка конфигурации| Настройка почты», кнопка «Уведомление Об Окончании Квоты»

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

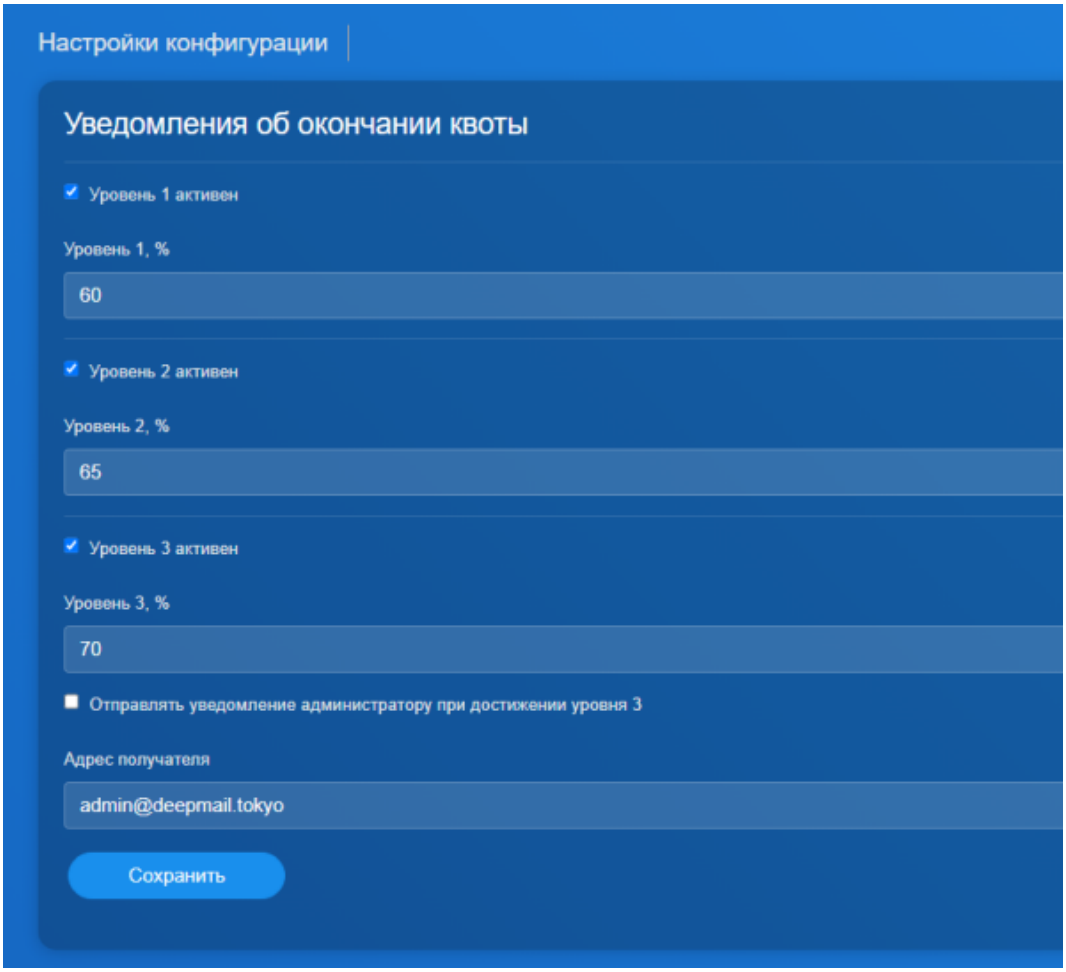


Рисунок 150 – Настройка параметров уведомлений об окончании квоты

3.14.3 «Шаблоны пользователей»

Раздел «Шаблоны пользователей» позволяет администратору создавать, просматривать и управлять наборами предварительно настроенных параметров, которые можно применять к новым почтовым ящикам. Это ускоряет массовое создание учётных записей и гарантирует единообразие настроек для групп пользователей.

Для перехода к настройкам конфигурации необходимо в меню «Расширенные настройки» выбрать инструмент «Шаблоны пользователей» (рисунок 151).

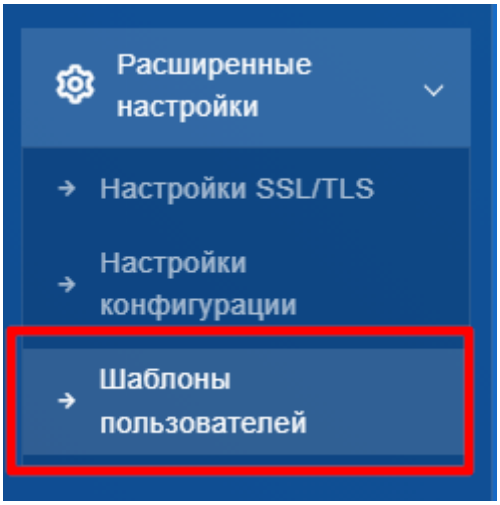


Рисунок 151 – Инструмент «Шаблоны пользователей»

После перехода на страницу шаблонов пользователей в центральной части экрана будет расположена таблица, в которой перечислены все существующие шаблоны (при наличии) (рисунок 152)

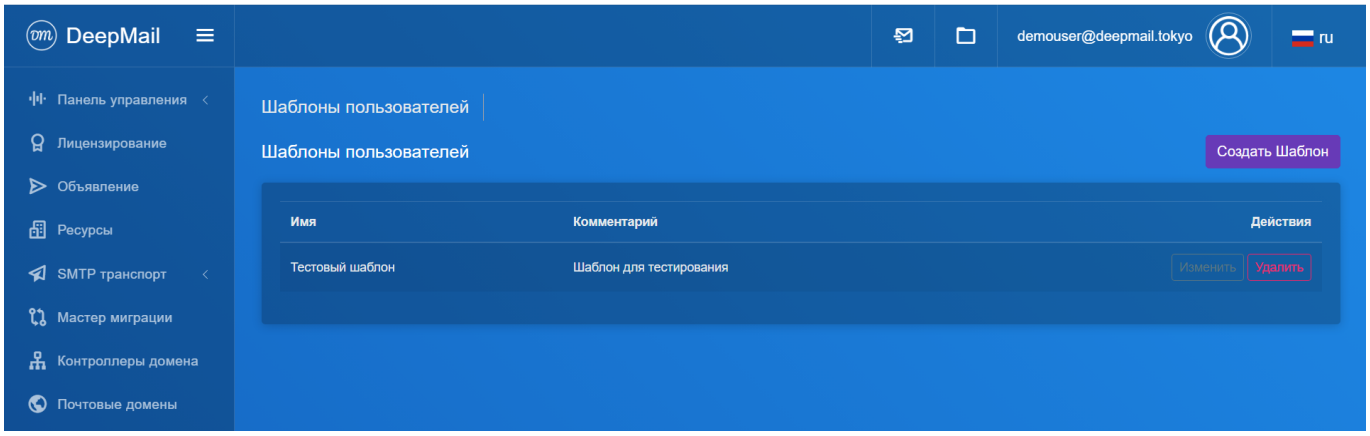


Рисунок 152 – Таблица шаблонов пользователей

Для каждого шаблона отображаются его имя и краткий комментарий, поясняющий назначение, а в столбце «Действия» присутствует кнопка «Изменить», позволяющая открыть форму редактирования параметров выбранного шаблона. Над таблицей находится кнопка Создать Шаблон, при нажатии на которую открывается форма для определения нового шаблона с указанием имени, комментария и всех необходимых настроек (квоты, права доступа, разрешённые протоколы и т.д.). Кнопка «Удалить» (расположенная в строке шаблона) служит для удаления выбранного шаблона после подтверждения действия.

Использование шаблонов позволяет централизованно управлять типовыми конфигурациями: например, можно создать шаблон «Сотрудник» с квотой 5 ГБ и доступом ко всем протоколам, шаблон «Внешний партнёр» с ограничениями на отправку и шаблон

«Техническая учётная запись» с повышенными правами. При создании нового пользователя администратор может просто выбрать нужный шаблон, и все заданные в нём параметры будут автоматически применены к ящику, что значительно экономит время и снижает риск ошибок.

Для добавления шаблона необходимо нажать на Создать Шаблон, после чего откроется окно настроек шаблона, в котором находятся общие настройки (рисунок 153) и настройка функций и квот (рисунок 154).

Рисунок 153 – Настройка Шаблона пользователей – общие настройки

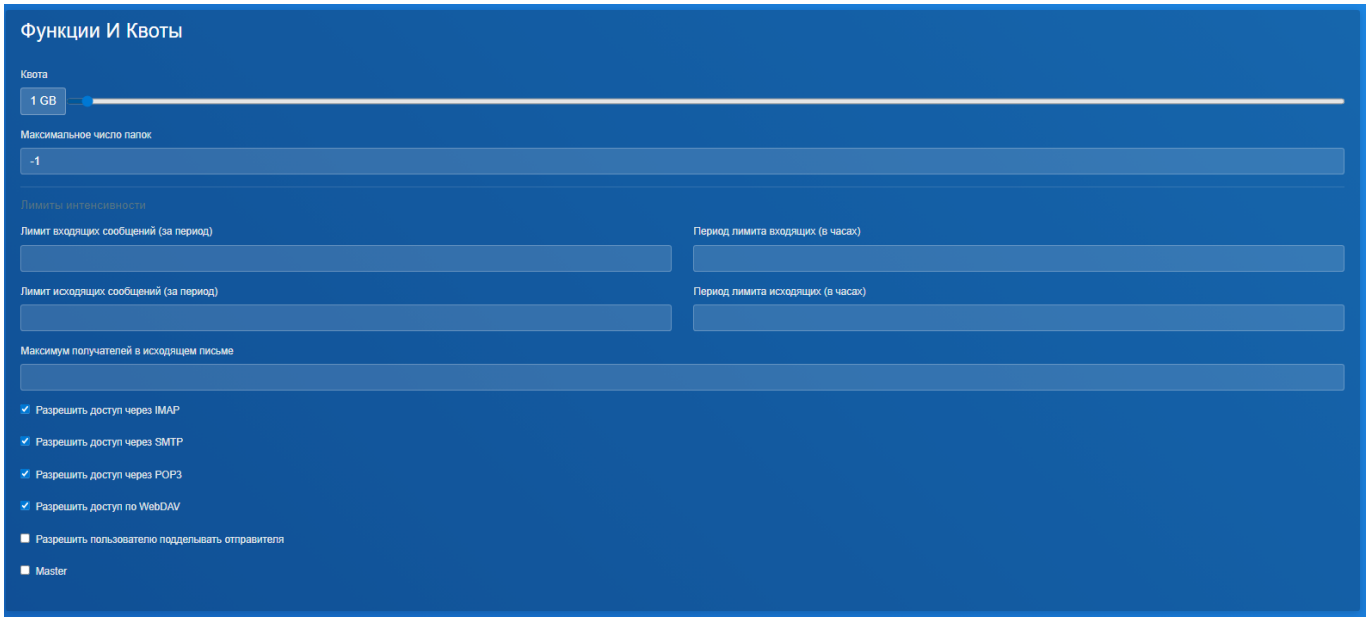


Рисунок 154 – Настройка Шаблона пользователей – Функции и квоты

В разделе «Общие» (см. рисунок 153) задаются базовые атрибуты шаблона. Поле «Название шаблона» содержит уникальное имя, по которому администратор будет идентифицировать набор настроек (например, «Сотрудник», «Внешний партнёр»). «Комментарий» позволяет добавить краткое описание, поясняющее назначение шаблона.

«Отображаемое имя» задаёт имя, которое будет подставляться по умолчанию для новых ящиков. В поле «Группы» администратор может указать, в какие группы каталога будет автоматически включён пользователь при создании по данному шаблону. Дополнительно предусмотрены флажки: «Активен» определяет, будет ли ящик активен сразу после создания, а «Исключить из псевдонима «all» позволяет исключить учетную запись из общей группы рассылки, охватывающей всех пользователей домена.

Раздел «Функции и квоты» (см. рисунок 154) содержит параметры ресурсных ограничений и прав доступа. В блоке квот задаётся максимальный размер почтового ящика в гигабайтах и максимальное количество папок (значение -1 означает отсутствие ограничений). Лимиты интенсивности позволяют установить пороговые значения для защиты от злоупотреблений: администратор может ограничить количество входящих и исходящих сообщений за определённый период (в часах), а также задать максимум получателей в одном исходящем письме.

Ниже расположены настройки доступных протоколов и прав. Флажки «Разрешить доступ через IMAP», «Разрешить доступ через SMTP», «Разрешить доступ через POP3», «Разрешить доступ по WebDAV» позволяют предопределить, какие протоколы будут включены для пользователя. Отдельная опция «Разрешить пользователю подделывать отправителя» даёт возможность менять адрес в поле «От» при отправке. Флаг «Master» предоставляет учётной записи права суперпользователя, что обычно используется для служебных или административных ящиков.

После сохранения шаблона он появляется в общем списке и может быть выбран при создании нового почтового ящика. Все параметры, заданные в шаблоне, будут автоматически применены к учётной записи, что обеспечивает единообразие конфигурации и ускоряет массовое создание пользователей.

3.15 Инструмент «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 155).

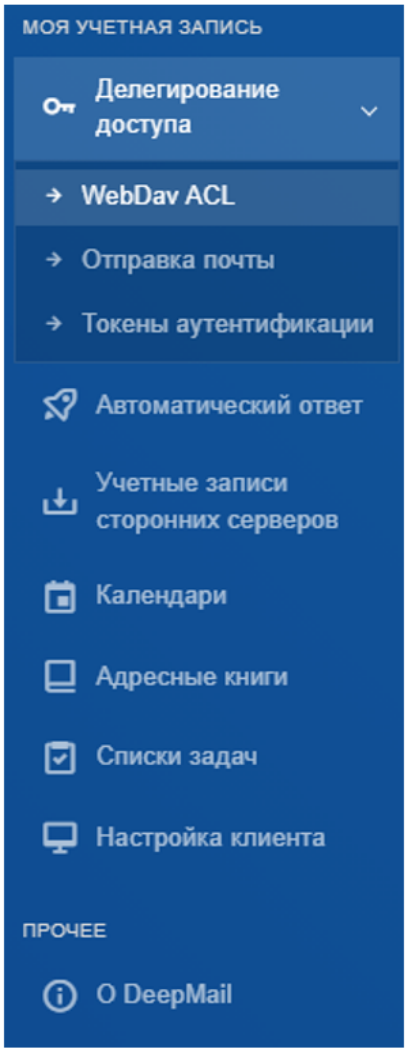


Рисунок 155 – Раздел «Моя учетная запись»

3.15.1 Инструмент «Делегирование доступа»

Инструмент «Делегирование доступа» содержит инструменты «WebDav ACL», «Отправка почты» и «Токены аутентификации» (рисунок 156).

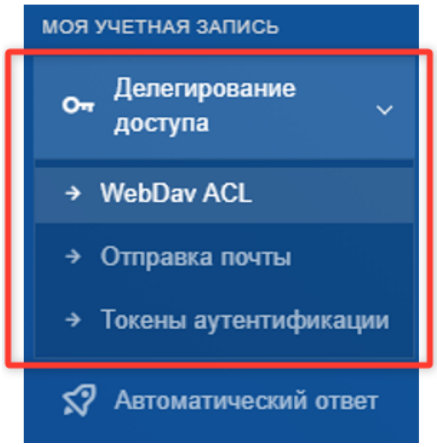


Рисунок 156 – Инструмент «Делегирование доступа»

3.15.1.1 «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 156).

На экране отобразится окно «Пользователи| WebDav ACL» со списком делегатов, если права уже назначались (рисунок 157).

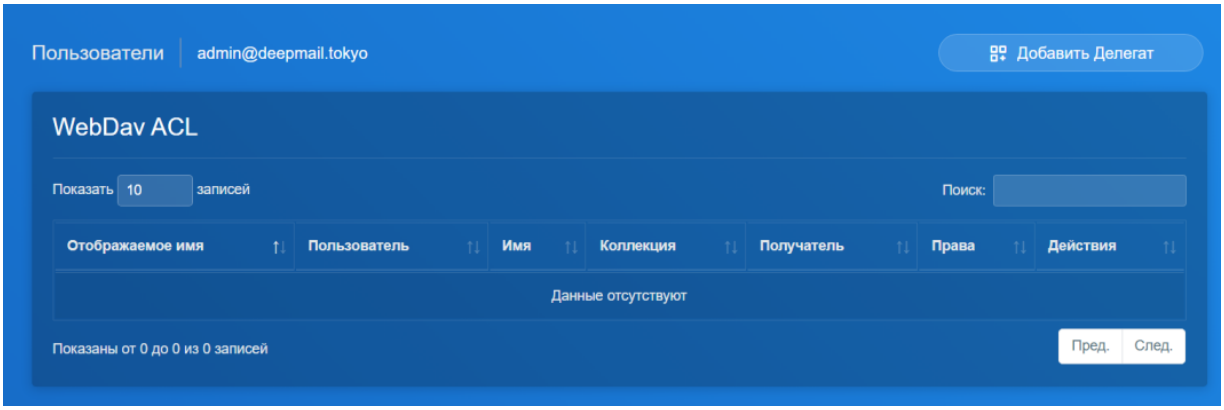
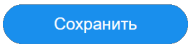


Рисунок 157 – Окно параметров «WebDav ACL»

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

3.15.1.2 «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 156).

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

(рисунок 158).

Рисунок 158 – Окно «Отправка почты»

3.15.1.3 «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 156).

На экране отобразится окно «Токены аутентификации» со списком предоставленных ключей, если они уже назначались (рисунок 159).

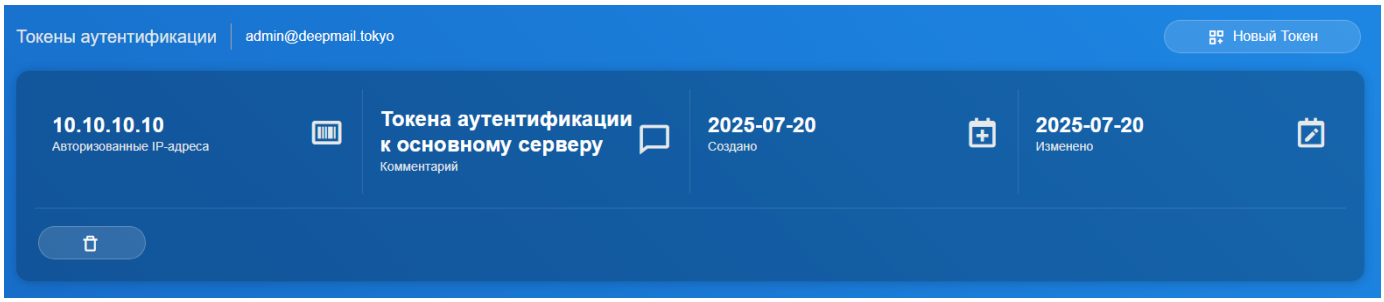


Рисунок 159 – Окно «Токены аутентификации»

Чтобы создать токен необходимо нажать кнопу «Новый Токен», расположенную в правом верхнем углу окна «Токены аутентификации» (см. рисунок 159). 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.

3.15.2 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 160).

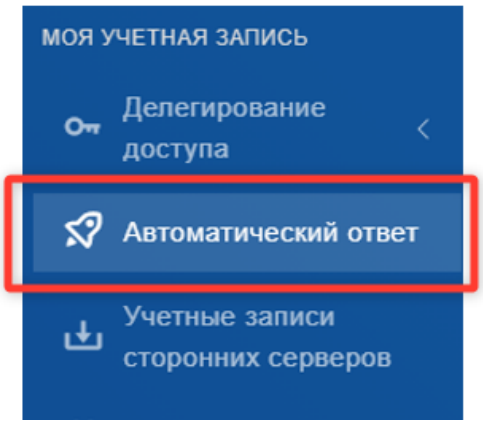


Рисунок 160 – «Автоматический ответ»

В появившемся окне «Автоматический ответ» указать следующие параметры:

- заголовок автоответа;
- сообщение автоответа;
- начало отпуска;
- конец отпуска (рисунок 161).

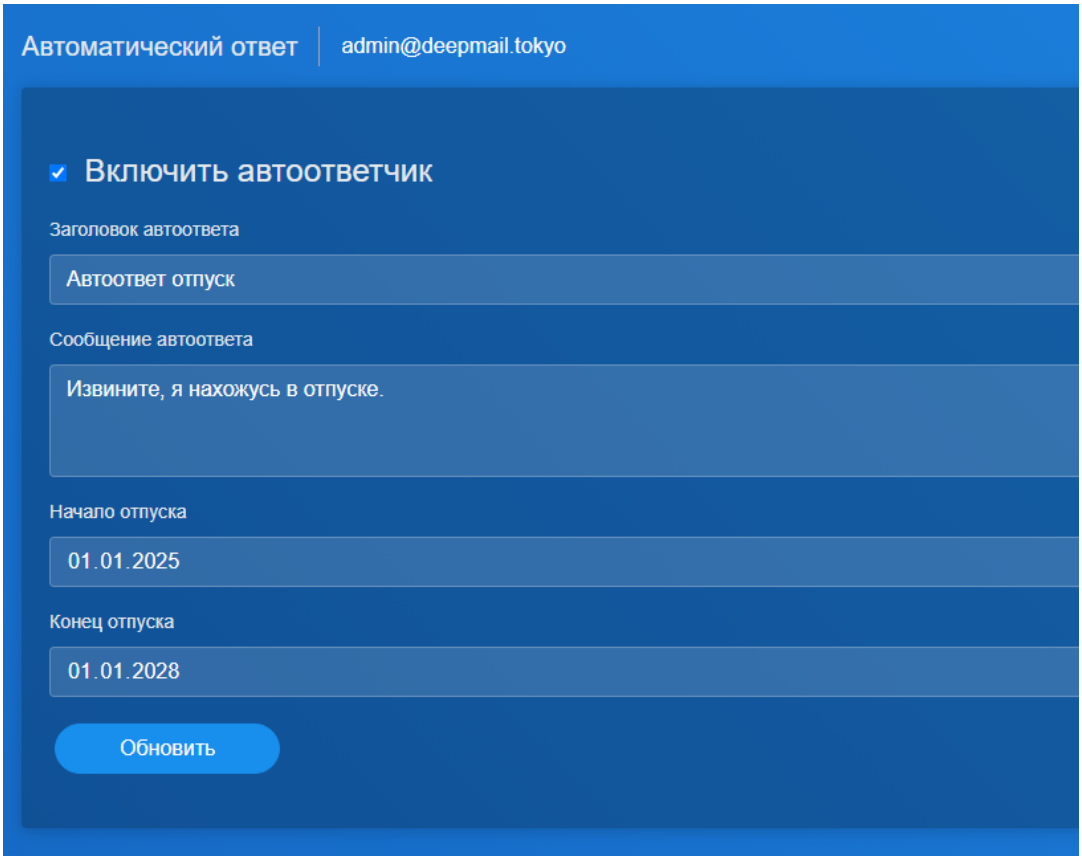


Рисунок 161 – Окно инструмента «Автоматический ответ»

Примечание. Автоответ приходит в адрес одного пользователя один раз в день.

3.15.3 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 155).

Чтобы добавить детали подключения к стороннему серверу необходимо нажать кнопку «Добавить Учетную Запись», откроется форма добавления учетной записи стороннего сервера (рисунок 162).

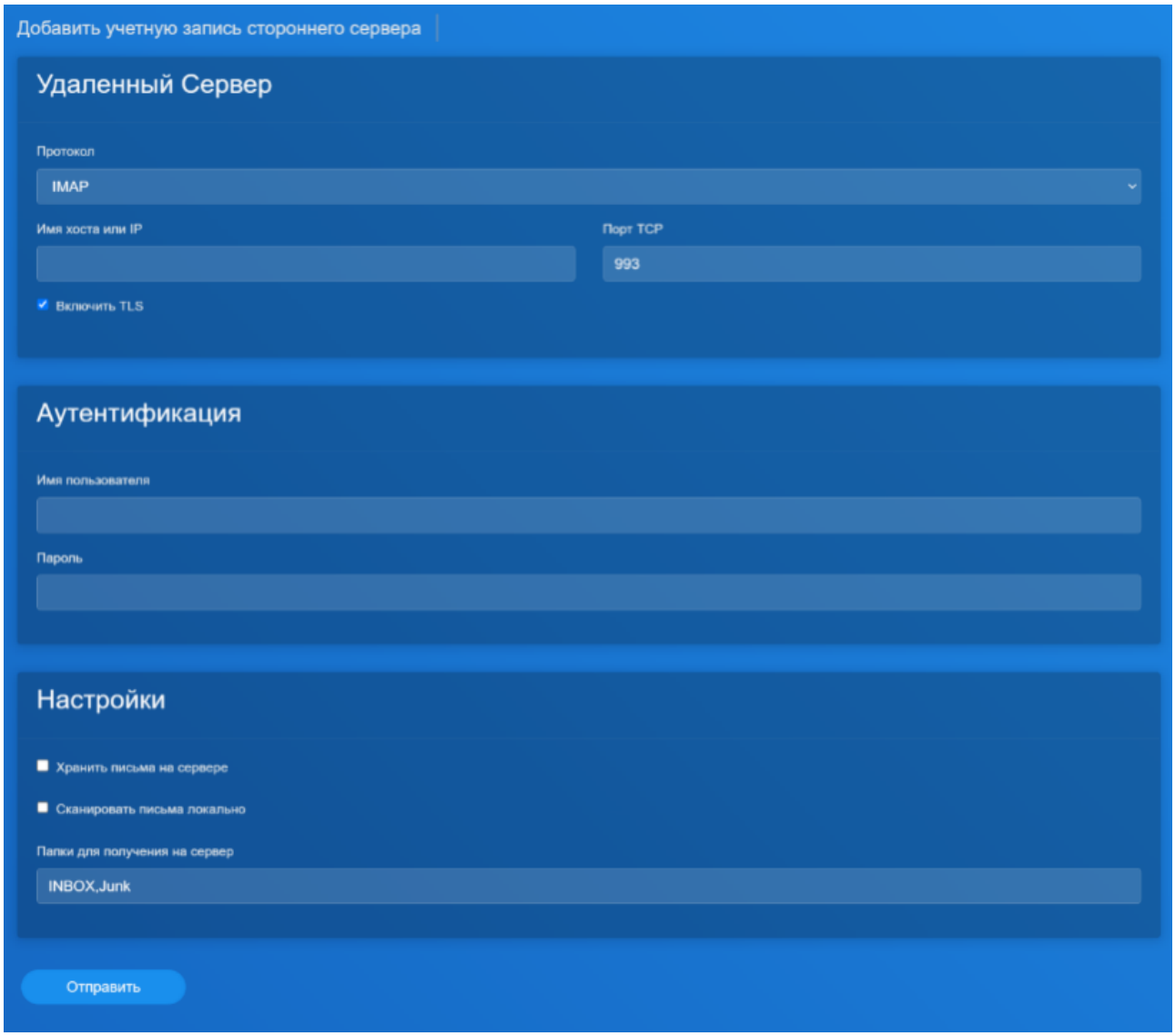


Рисунок 162 – Окно добавления параметров стороннего сервера

В появившейся форме укажите 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»).

Для завершения нажмите кнопку Отправить.

3.15.4 Инструмент «Календари»

Для управления параметрами календарей пользователя необходимо перейти к инструменту «Календари», выбрав его в разделе «Моя учетная запись» (см. рисунок 155).

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 163).

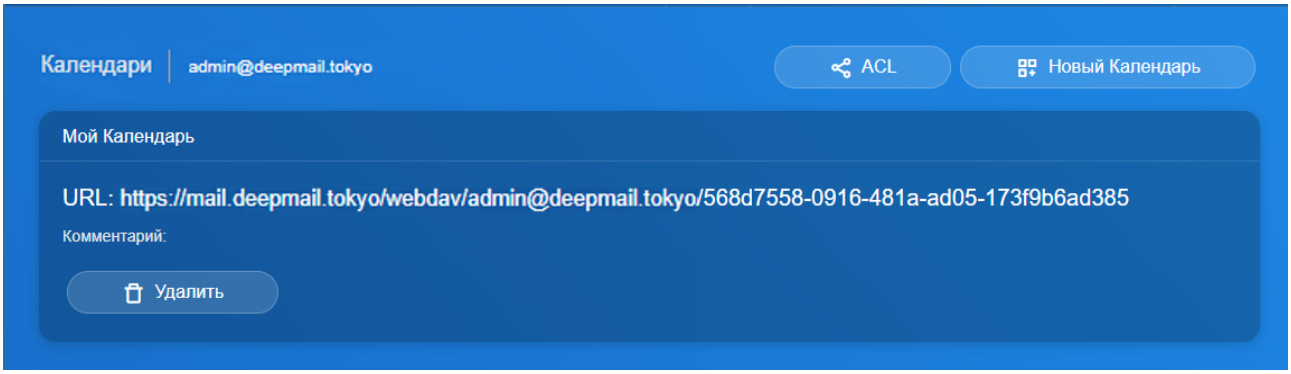
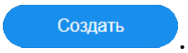


Рисунок 163 – Окно инструмента «Календари»

Для создания календаря необходимо в окне инструмента «Календари» нажать кнопку Новый Календарь (см. рисунок 163).

Откроется форма «Создать календарь», в которой необходимо ввести имя календаря и, если нужно, добавить комментарий (рисунок 164).

Рисунок 164 – Окно «Создать календарь»

Для завершения создания календаря нажмите на кнопку 

.

При нажатии в окне инструмента «Календари» на кнопку 

(см. рисунок 163) будет выполнен переход к окну «Пользователи| WebDav ACL» для делегирования прав доступа (см. 3.15.1.1).

3.15.5 Инструмент «Адресные книги»

Для управления данными адресных книг пользователя необходимо перейти к инструменту «Адресные книги», выбрав его в разделе «Моя учетная запись» (см. рисунок 155).

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 165).

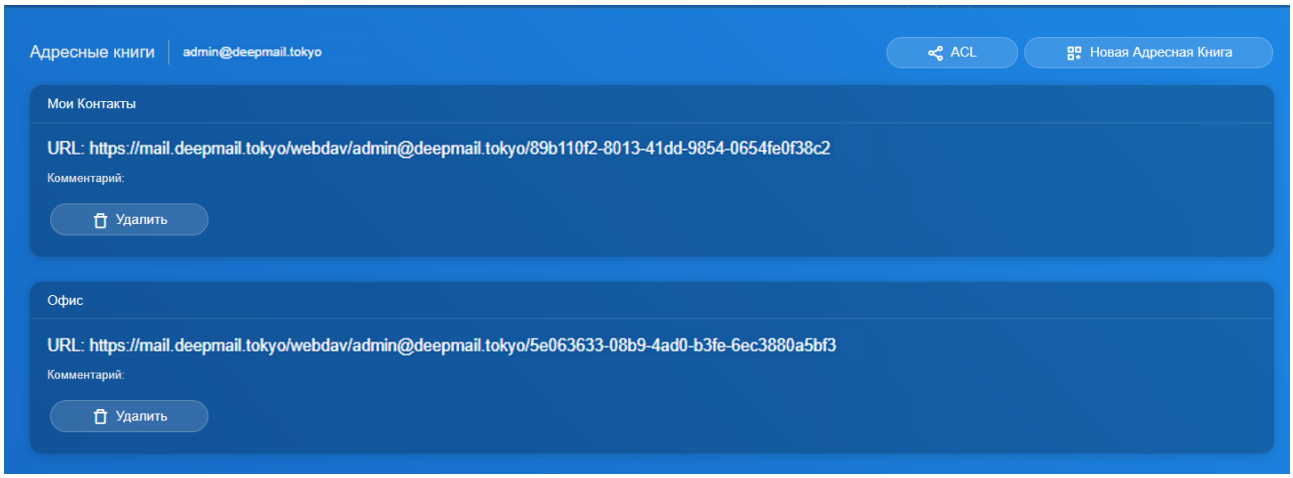


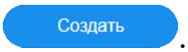
Рисунок 165 – Окно инструмента «Адресные книги»

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

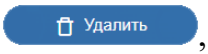
(см. рисунок 165).

Откроется форма «Создать адресную книгу», в которой необходимо ввести имя адресной книги и, если нужно, добавить комментарий (рисунок 166).

Рисунок 166 – 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 165).

При нажатии в окне инструмента «Адресные книги» на кнопку 

(см. рисунок 165) будет выполнен переход к окну «Пользователи| WebDav ACL» для делегирования прав доступа (см. 3.15.1.1).

3.15.6 Инструмент «Списки задач»

Для управления задачами пользователя необходимо перейти к инструменту «Списки задач», выбрав его в разделе «Моя учетная запись» (см. рисунок 155).

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 167).

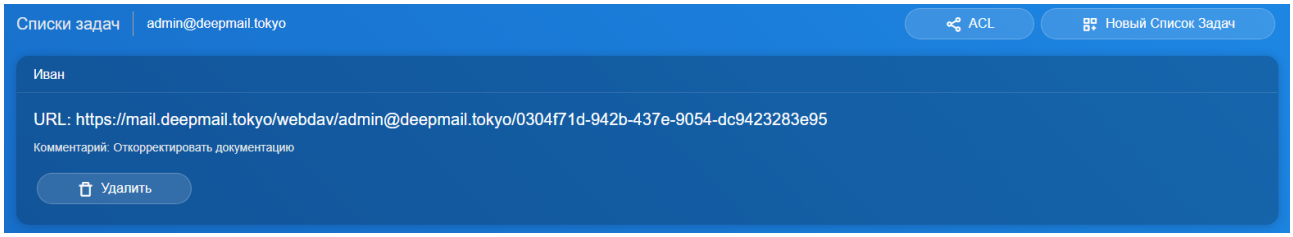
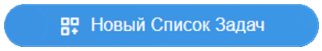


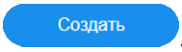
Рисунок 167 – Инструмент «Списки задач»

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

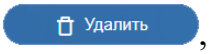
(см. рисунок 167).

Откроется форма «Создать список задач» в которой необходимо ввести имя папки задач и, при необходимости, оставить комментарий (рисунок 168).

Рисунок 168 – Форма «Создать список задач»

Для завершения создания папки задач нажмите на кнопку 

.

Чтобы удалить папку задач необходимо в окне инструмента «Адресные книги» нажать кнопку 

, размещенную на панели выбранной папки (см. рисунок 167).

При нажатии в окне инструмента «Списки задач» на кнопку 

(см. см. рисунок 167) будет выполнен переход к окну «Пользователи| WebDav ACL» для делегирования прав доступа (см. 3.15.1.1).

3.15.7 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 155). После этого на экране отобразится окно «Настройка клиента| Настройте свой почтовый клиент» (рисунок 169).

Рисунок 169 – Инструмент «Настройка клиента»

3.16 Интерфейс командной строки (CLI)

Для просмотра счетчиков статистики на уровне сервера, домена и пользователя применяется интерфейс командной строки (CLI – Command Line Interface) (рисунок 170).

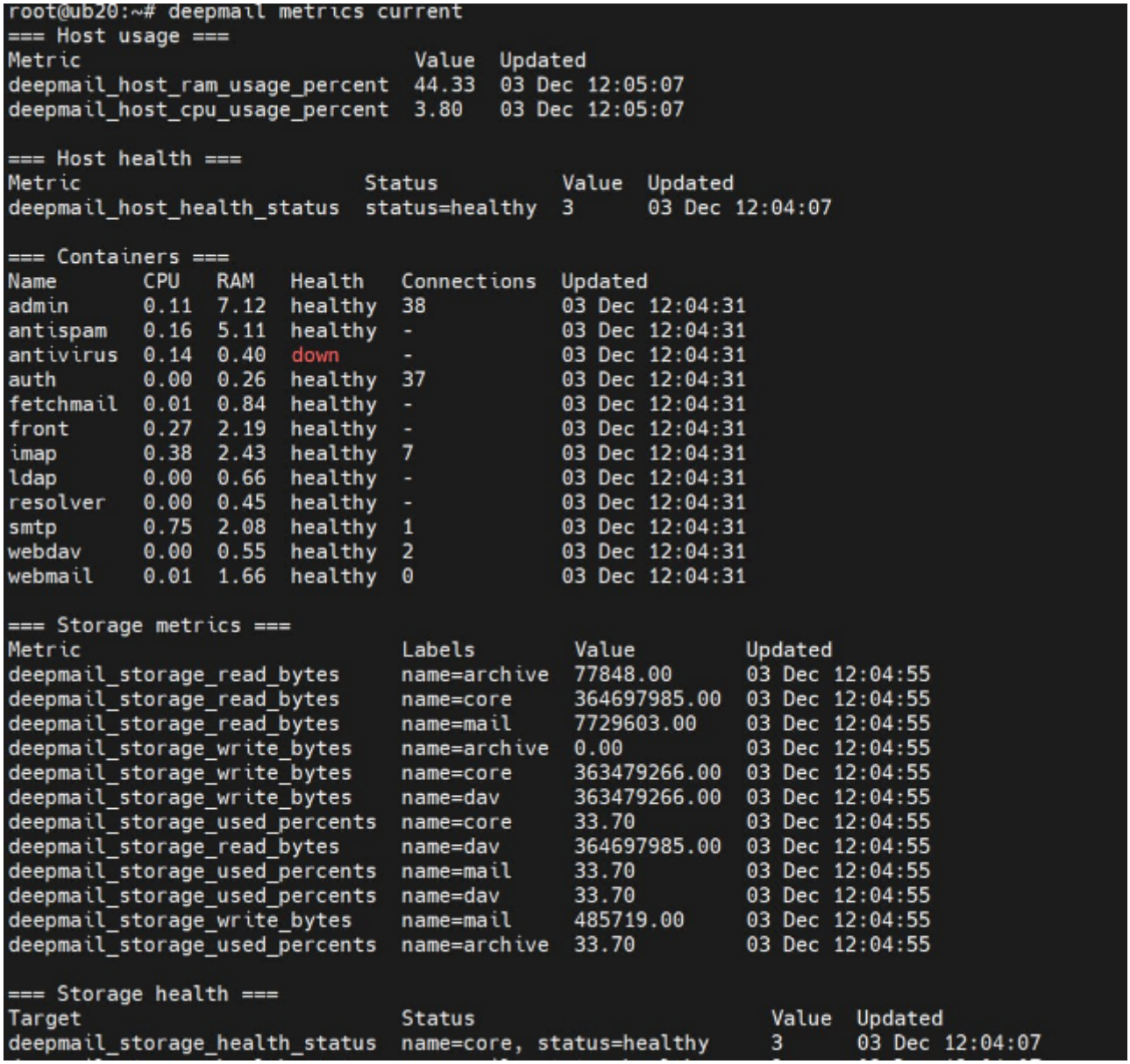


Рисунок 170 – Интерфейс командной строки

Для вывода статистических данных требуется выполнить команду:

depmail metrics current

В выводе команды отображаются ключевые метрики работоспособности и производительности системы DeepMail, сгруппированные по категориям:

- использование ресурсов сервера – загрузка оперативной памяти и процессора.
- состояние здоровья хоста – общий статус работоспособности сервера;
- метрики контейнеров – потребление ресурсов (CPU, RAM), статус здоровья и количество сетевых подключений для каждого сервиса DeepMail;
- дисковые операции и использование хранилища – объемы чтения/ записи и процент занятого пространства для различных типов данных (почта, архивы, конфигурации);
- состояние хранилищ – статус здоровья каждого смонтированного хранилища.

Вывод предоставляет комплексный снимок состояния системы в реальном времени, позволяющий оценить нагрузку, выявить проблемные сервисы (например, недоступные контейнеры) и контролировать использование дискового пространства.

Для управления настройками сервера доступен API – интерфейс. Перейти к описанию API – методов можно, набрав в адресной строке браузера «https:// https://<ip>/api/v1/», где <ip> IP адрес сервера DeepMail. Для выполнения описанных API – методов можно использовать «Swagger UI» или инструмент командной строки «curl».

3.16.1 Дополнительные правила фильтрации Sieve в DeepMail

Система DeepMail предоставляет администратору мощный механизм для расширения встроенной обработки почтовых сообщений с помощью языка фильтрации Sieve. В отличие от пользовательских правил, которые создаются через веб-интерфейс и предназначены для индивидуальных нужд, правила Sieve позволяют реализовать сложную серверную логику, применяемую ко всем письмам после основных обработчиков (антиспам, автоответчики, автоматическое размещение событий). Это даёт возможность гибко управлять почтовым потоком на уровне, недоступном обычным пользователям.

Файл с правилами размещён по пути */mnt/deepmail/core/overrides/dovecot/rules.sieve*. При запуске сервисов DeepMail система проверяет наличие этого файла. Если он существует, то автоматически подключается в Dovecot как sieve_after, что означает выполнение данных правил после всех стандартных, но перед окончательной доставкой письма в почтовый ящик пользователя. Любое изменение содержимого файла требует перезапуска всей системы командой *deepmail restart* для применения новых настроек. Важно помнить, что синтаксическая ошибка в файле приведёт к тому, что Sieve-скрипт не загрузится, и письма будут обрабатываться только стандартными правилами.

Dovecot в составе DeepMail поддерживает множество расширений Sieve, которые необходимо объявлять в начале файла с помощью директивы *require*. Среди наиболее полезных для администратора можно выделить:

- *fileinto* — перемещение письма в указанную папку; с параметром :create папка будет автоматически создана, если её не существует;

- *mailbox* — позволяет работать с почтовыми ящиками (обычно используется вместе с fileinto);

- *imap4flags* — управление флагами сообщений, такими как *\Seen* (прочитано), *\Flagged* (важное), *\Deleted* (удалено);

- *envelope* — доступ к конвертным адресам (реальным отправителю и получателю, которые могут отличаться от заголовков);

- regex — использование регулярных выражений для проверки заголовков и других частей письма;

- *relational* и *comparator-i;ascii-numeric* — числовые сравнения (больше, меньше, равно);

- *date* — проверка даты письма (например, день недели, месяц);

- *mime* — анализ MIME-структуры письма и вложений (тип содержимого, имя файла);

- *copy* — копирование письма в папку без удаления оригинала;

- *reject* — отклонение письма с возвратом заданного сообщения отправителю;

- *editheader* — добавление или удаление заголовков письма;

- *spamtest / spamtestplus* — оценка спам-рейтинга (обычно в процентах);

- *variables* — использование переменных и подстановок;

- *vacation / vacation-seconds* — автоматические ответы об отсутствии.

Все используемые расширения должны быть перечислены в *require,* к примеру:

sieve

require ["fileinto", "mailbox", "imap4flags", "regex", "variables"];

Базовый синтаксис Sieve следующий: после объявления расширений следуют правила, каждое из которых имеет вид *if <условие> { <действия>; }*. Условия могут быть простыми или составными с помощью операторов *allof* (логическое И), *anyof* (логическое ИЛИ) и *not* (отрицание). Каждое действие заканчивается точкой с запятой. Важно помнить, что если после выполнения действий не вызвана команда *stop*, то письмо после всех правил также попадёт в папку «Входящие». Поэтому для перемещения письма в целевую папку без дублирования необходимо после *fileinto* указывать *stop*.

Далее представлены примеры практических правил базового синтаксиса Sieve:

а) Сортировка писем по отправителю

Предположим, необходимо все письма от руководства компании перемещать в папку «Руководство», а письма из списков рассылки — в папку «Рассылки». Скрипт будет выглядеть так:

sieve

require ["fileinto", "mailbox"];

 # Письма от руководства

if header :contains "From" "@management.company.com" {

```
    fileinto :create "Руководство";
    stop;
}
# Письма из списков рассылки (имеют заголовок List-Id)
if header :contains "List-Id" "" {
    fileinto :create "Рассылки";
    stop;
}
```

Если письмо не подошло ни под одно условие, оно останется во «Входящих».

б) Блокировка опасных вложений

Организация может запретить получение писем с исполняемыми вложениями (файлы с расширением .exe). Такие письма можно перемещать в специальную папку «Заблокировано» и помечать как прочитанные:

```
sieve
require ["fileinto", "mailbox", "mime", "imap4flags"];

if header :mime :anychild :param "filename" :matches "Content-Disposition" "*.exe" {
    setflag "\\seen";              # пометить как прочитанное
    fileinto :create "Blocked";    # переместить в папку Blocked
    stop;
}
```

в) Автоматическая пометка важных писем

Письма, содержащие в теме слово «срочно», можно автоматически помечать флагом «важное» (в почтовых клиентах такие письма обычно выделяются цветом):

```
sieve
require ["imap4flags"];

if header :contains "Subject" "срочно" {
    addflag "\\flagged";
}
```

Необходимо обратить внимание, что здесь нет *stop*, поэтому письмо также попадёт во «Входящие», но уже с флагом важности.

г) Сортировка тикетов по проекту

Если в системе заявок используются темы вида «[PROJ-12345] Описание проблемы», можно автоматически раскладывать такие письма по папкам в зависимости от проекта:

```
sieve
require ["fileinto", "mailbox", "regex"];
if header :regex "Subject" "\\[PROJ-([0-9]+)\\]" {
   fileinto :create "Tickets/PROJ";
   stop;
}
```

Здесь регулярное выражение извлекает номер заявки, но для простоты мы помещаем все письма в одну папку *Tickets/PROJ*. При необходимости можно использовать переменные, чтобы создавать папки с разными номерами.

д) Копирование писем от важных клиентов

Иногда требуется сохранять копию всей переписки с определённым клиентом в архивной папке, не мешая основной доставке.

```
sieve
require ["copy", "fileinto", "mailbox"];

if header :contains "From" "@important-client.com" {
   fileinto :copy :create "ClientArchive";
   # stop не вызываем, чтобы письмо дошло и в обычную папку
}
```

е) Отклонение писем от нежелательных отправителей

Письма с определённого адреса можно отклонять сразу на уровне SMTP, отправляя отправителю уведомление:

```
sieve
require ["reject"];
if header :is "From" "spammer@bad.com" {
   reject "Сообщения от данного адреса не принимаются нашей организацией";
   stop;
}
```

ж) Фильтрация по спам-рейтингу

Если DeepMail интегрирован с антиспам-системой, которая добавляет заголовок с оценкой (например, X-Spam-Score), можно использовать расширение spamtestplus:

```
sieve
require ["spamtestplus", "relational", "comparator-i;ascii-numeric", "fileinto", "mailbox", "imap4flags"];

if spamtest :percent :value "gt" :comparator "i;ascii-numeric" "90" {
   setflag "\\seen";
   fileinto :create "Junk";
   stop;
}
```

Это правило перемещает в папку «*Junk*» письма со спам-рейтингом выше 90 процентов, помечая их как прочитанные.

з) Использование переменных для динамической сортировки

С помощью расширения *variables* можно извлекать части адреса или темы и использовать их для создания папок:

```
sieve
require ["variables", "fileinto", "mailbox"];

if header :matches "From" "*@*" {
   set "domain" "${2}";
   fileinto :create "ByDomain/${domain}";
   stop;
}
```

В этом примере все письма будут раскладываться по папкам, названным по домену отправителя (например, *ByDomain/deepmail.ru*).

Администратору в процессе настройки важно помнить:

- директива *require* обязательна для каждого используемого расширения и должна располагаться в самом начале файла;

- имена папок чувствительны к регистру. Папка *Archive* и *archive* — это разные папки;

- для создания вложенных папок используется разделитель «/», например, *Work/Projects/2025*;

- если в правиле не указан *stop,* письмо после выполнения действий будет также доставлено в папку «Входящие». Для перемещения письма в целевую папку без дублирования всегда используйте *stop*;

- при использовании *fileinto :create* папка создаётся автоматически, если её не было. Без *:create* перемещение в несуществующую папку вызовет ошибку;

- файл *rules.sieve* должен быть синтаксически валидным. Проверить правильность можно с помощью утилиты sievec (если она установлена) или путем наблюдения за логами Dovecot после перезапуска.

Дополнительные правила Sieve дают администратору практически неограниченные возможности по кастомизации обработки почты на серверном уровне. От простой сортировки по отправителям до сложной фильтрации на основе содержимого вложений, регулярных выражений и спам-рейтинга — всё это реализуется через один текстовый файл. При этом пользовательские настройки остаются нетронутыми, а сама система сохраняет высокую производительность. Освоив Sieve, вы сможете автоматизировать рутинные задачи и повысить безопасность почтовой инфраструктуры.

4 ИНТЕГРАЦИЯ С СИСТЕМОЙ МОНИТОРИНГА ZABBIX

В рамках интеграции с системой мониторинга Zabbix 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. Также доступно настроить SNMP-агента для удалённого мониторинга.

В поставляемом с дистрибутивом АРМ «DeepMail» 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 5 приведены данные по основным сервисам и метрикам, которые настроены в шаблоне *zabbix_deepmail-2.0-4.yaml* для мониторинга.

Таблица 5 – 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.

Для настройки без настроенного шаблона Zabbix необходимо выполнить следующие действия.

Этап 1: Установка и базовая настройка Zabbix Agent 2 на ноде DeepMail

- выполните подключение к ноде DeepMail по протоколу SSH;
- обновите индекс пакетов и установите zabbix-agent2:

apt-get update

apt-get install zabbix-agent2 -y

- активируйте службу zabbix-agent2 и разрешите её автоматический запуск при загрузке системы;

systemctl enable --now zabbix-agent2

Этап 2: Настройка прав доступа для пользователя Zabbix

- предоставьте агенту Zabbix права на взаимодействие с Docker;

usermod -aG docker zabbix

- для выполнения проверок внутри контейнеров предоставьте пользователю zabbix права на выполнение команд с повышенными привилегиями;
- отредактируйте файл /etc/sudoers с помощью команды visudo:

visudo

- Добавьте в конец файла следующую строку:

text

zabbix ALL=(ALL:ALL) NOPASSWD: ALL

- Примечание: Использование NOPASSWD может быть изменено в соответствии с политиками безопасности. Для повышения безопасности рекомендуется ограничить список разрешенных команд.

Этап 3: Конфигурация Zabbix Agent 2

- измените файл конфигурации агента /etc/zabbix/zabbix_agent2.conf.

nano /etc/zabbix/zabbix_agent2.conf

- убедитесь, что заданы следующие параметры (замените ip_zabbix_server и your_hostname на актуальные значения):

Server=ip_zabbix_server

ServerActive=ip_zabbix_server

Hostname=your_hostname

UserParameter=deepmail.postqueue,bash /etc/deepmail/mailq-count.sh 2> /dev/null

- создайте директорию для скриптов DeepMail (если она не существует):

mkdir -p /etc/deepmail

- создайте файл скрипта /etc/deepmail/mailq-count.sh:

nano /etc/deepmail/mailq-count.sh

- добавьте в файл следующее содержимое:

#!/bin/bash

echo $(docker exec -i deepmail-smtp mailq | grep -v "Mail queue is empty" | grep -c '^[0-9A-Z]')

- установите права на выполнение для скрипта:

chmod +x /etc/deepmail/mailq-count.sh

- перезапустите службу Zabbix Agent 2 для применения изменений.

systemctl restart zabbix-agent2

Этап 4: Настройка на сервере Zabbix

- авторизуйтесь в веб-интерфейсе сервера Zabbix;

- перейдите в раздел Data collection > Templates;

- нажмите кнопку Import и загрузите файл шаблона zabbix_deepmail-2.0.yaml;

- перейдите в раздел Data collection > Hosts;

- создайте новый узел, указав в поле Host name значение, точно соответствующее параметру Hostname из конфигурации агента;

- свяжите созданный узел с соответствующим интерфейсом (как правило, Zabbix agent) и укажите IP-адрес ноды DeepMail;

- на странице редактирования созданного узла (Host) во вкладке Templates добавьте шаблон с именем "deepmail-all";

- сохраните изменения.

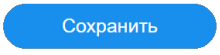
Для проверки результата необходимо убедиться, что в разделе Monitoring > Hosts для добавленного узла в столбце Availability значок Zabbix agent имеет зеленый цвет, что свидетельствует об успешном подключении.

5 ОБЕСПЕЧЕНИЕ ИНТЕГРАЦИИ KSMG С DEEPMAIL

5.1 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.

5.2 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*.

5.3 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

5.4 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».

5.5 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

5.6 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

Для подключения функционала «Антиспам» необходимо настроить соединение с KSMG по протоколу Milter.

Для настройки со стороны DeepMail требуется:

- авторизоваться в административный интерфейс;
- в левой панели развернуть раздел «Панель управления»;

- выбрать подраздел «Профили», в строке с типом профиля SMTP нажать кнопку  в последнем столбце;

- прокрутить вниз окно редактирования профиля, убедиться, что установлен чек-бокс «Антиспам активен (milter)», а в поле «Адрес антиспама (milter)» указать адрес сервера KSMG;

- сохранить конфигурацию нажав кнопку «Сохранить».

Важно! протокол Milter в DeepMail работает на порту 11332. Необходимо провести соответствующую настройку в KSMG (указать адрес порта 11332), согласно статье https://support.kaspersky.ru/ksmg/2.1va/239703.

Рекомендуем обратиться дополнительно в поддержку Касперского для получения актуальной инструкции. После проведения указанных действий в интерфейсе KSMG отобразятся письма с DeepMail.

5.7 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.

5.8 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.

6 ОБЕСПЕЧЕНИЕ ЛОГИРОВАНИЯ

В АРМ DeepMail реализован функционал регистрации событий информационной безопасности системы. Для удобства администраторов безопасности отслеживание логов возможно непосредственно в интерфейсе панели администратора (описание приведено в п.3.2.2) и через просмотр файлов логов, размещенных в специальной директории.

Для просмотра лог-файлов DeepMail необходимо перейти в директорию */var/log/deepmail.*

Базовые логи находятся в следующих файлах:

- admin.log (логи действий администратора);
- collections.log (логи коллекций);
- authentication.log (логи аутентификации на сервер);
- license.log (лог лицензирования);
- restart.log (логи включения и выключения сервера);
- service.log (логи ошибок реконфигурации сервисов).

Логи сервисов:

- deepmail-auth.log (логи сервиса аутентификации);
- deepmail-imap.log (логи сервиса imap, отвечающего за забор почты с сервера);
- deepmail-redis.log (логи сервиса redis, отвечающего за хранение сессий);
- deepmail-webdav (логи сервиса webdav, отвечающего за работу коллекций);
- deepmail-antispam.log (логи сервиса антиспама);
- deepmail-fetchmail.log (логи сервиса fetchmail, отвечающего за забор почты с удаленных почтовых серверов);
- deepmail-ldap.log (логи сервиса ldap, отвечающего за взаимодействие с контроллерами доменов);
- deepmail-webmail.log (логи сервиса webmail, отвечающего за работу веб-клиента);
- deepmail-admin.log (логи admin сервиса, отвечающего за совокупное взаимодействие сервисов и работоспособность сервера);
- deepmail-front.log (логи сервиса front, отвечающего за работоспособность веб-консоли);
- deepmail-oletools.log (логи сервиса oletools, отвечающего за сканирование вложений и проверку макросов);
- deepmail-smtp.log (логи сервиса smtp, отвечающего за хождение почты);

– deepmail-resolver.log (логи сервиса resolver, отвечающего за кэш DNS).

Дополнительные логи:

– ldap_ip.log (логи контроллера домена, появлются при синхронизации с контроллером домена);

– migration_user@domain.ru.log (логи миграции пользователя, появляются после выполнения процедуры миграции).

Также в директории */var/log/deepmail* размещена папка *archive*, в которой лежат архивированные логи за предыдущие дни.

7 ПОРЯДОК РЕЗЕРВНОГО КОПИРОВАНИЯ И ВОССТАНОВЛЕНИЯ СИСТЕМЫ

АРМ DeepMail не включает встроенного механизма автоматического резервного копирования. Ответственность за сохранность данных лежит на администраторе, который должен организовать регулярное копирование критически важных компонентов с помощью инфраструктурных средств (например, штатных утилит операционной системы, систем резервного копирования или снимков файловых систем). Для полного восстановления работоспособности почтовой системы необходимо резервировать три основных компонента: базу данных PostgreSQL, хранилище почтовых ящиков и конфигурационные файлы.

База данных PostgreSQL содержит метаданные пользователей, настройки доменов, правила фильтрации, псевдонимы и другую служебную информацию. Для её резервного копирования рекомендуется использовать утилиту pg_dumpall, которая создаёт дамп всех баз данных кластера. Команду следует выполнять от имени пользователя postgres, предварительно остановив или минимизировав нагрузку на систему (например, в период наименьшей активности). Пример команды:

pg_dumpall -U postgres > /backup/postgres/pg_dumpall_$(date +%Y%m%d).sql

Дамп рекомендуется хранить в отдельном каталоге, а также копировать его на удалённый носитель.

Хранилище почтовых ящиков физически располагается в каталоге /mnt/deepmail/mail/. В этой директории находятся все письма, вложения, структура папок и настройки пользователей. Для копирования почтовых данных можно использовать rsync или tar. Например, создание полного архива:

tar -czf /backup/mail_$(date +%Y%m%d).tar.gz /mnt/deepmail/mail/

Для ежедневного инкрементального копирования удобно применять *rsync -av --delete /mnt/deepmail/mail/ /backup/mail_daily/*. При использовании снимков файловой системы (LVM, ZFS) можно делать мгновенные копии без остановки сервисов, но важно обеспечить целостность данных.

Конфигурационные файлы включают настройки самой системы, пользовательские скрипты и параметры окружения. Обязательному резервированию подлежат файлы в /mnt/deepmail/core/deepmail.env, а также каталог /etc/deepmail/ (если он используется). Их следует копировать при каждом изменении конфигурации, сохраняя версионность.

Для восстановления системы необходимо сначала подготовить среду: установить DeepMail заново (если требуется) и убедиться, что версия программного обеспечения соответствует той, на которой создавались резервные копии. Далее в определённом порядке восстанавливаются компоненты. Сначала восстанавливается база данных: при помощи утилиты psql загружается дамп, например:

psql -U postgres -f /backup/postgres/pg_dumpall_YYYYMMDD.sql

Затем возвращаются почтовые ящики: архив распаковывается в каталог /mnt/deepmail/mail/, после чего необходимо рекурсивно исправить права владельца (пользователь mail, группа man) и установить корректные права доступа (например, *chown -R mail:man /mnt/deepmail/mail/ u find /mnt/deepmail/mail/ -type d -exec chmod 700 {} \;*). После этого восстанавливаются конфигурационные файлы и перезапускаются сервисы DeepMail. Завершающим шагом является проверка работоспособности: тестовый вход пользователя, отправка и получение письма.

Рекомендуется регулярно проверять целостность резервных копий, выполняя тестовое восстановление на отдельном стенде, и автоматизировать процесс с помощью скриптов, запускаемых по расписанию (cron).

8 ОБСЛУЖИВАНИЕ СИСТЕМЫ

Обслуживание сервера DeepMail осуществляется через единый центр управления, который консолидирует функции администрирования, мониторинга и информационной безопасности в рамках общего веб-интерфейса. Такой подход позволяет администратору выполнять все рутинные операции по поддержанию работоспособности системы без необходимости обращения к командной строке или ручного редактирования конфигурационных файлов.

Встроенные инструменты мониторинга обеспечивают возможность отслеживания нагрузки и ключевых метрик системы в режиме реального времени. Интерфейс мониторинга наглядно отображает статус всех подключенных сервисов, хостов и хранилищ в одном окне, что позволяет администратору оперативно оценивать общую картину работоспособности инфраструктуры. Система автоматически контролирует состояние сервисов и при обнаружении сбоев предпринимает попытки восстановления подключения или перезапуска компонентов с незамедлительным уведомлением оператора.

Для тиражирования настроек между различными узлами предусмотрена возможность использования готовых шаблонов, что позволяет в несколько кликов развертывать новые узлы и применять одинаковые параметры конфигурации. Все параметры баз данных и хранилищ настраиваются через веб-интерфейс панели управления. При необходимости изменения конфигурации почтовых сервисов администратор работает с профилями SMTP и IMAP, где задаются параметры работы с почтовым трафиком, включая настройки антиспама, антивируса и ретрансляции сообщений.

Система поддерживает подключение различных типов хранилищ (CORE, MAIL, DAV, ARCHIVE) через сетевые протоколы, такие как NFS. В интерфейсе управления хранилищами отображается иерархия всех дисковых ресурсов с возможностью детального управления каждым подключением. Администратор может контролировать заполненность хранилищ в процентах, отслеживать скорость операций чтения и записи, а также своевременно реагировать на приближение к критическим значениям занятого пространства.

Для контроля за исходящей корреспонденцией предусмотрена панель управления почтовой очередью. В ней отображаются письма, ожидающие отправки, с указанием идентификатора, времени постановки в очередь, размера, статуса доставки, отправителя и получателя. Администратор имеет возможность выполнять массовые операции:

принудительно отправлять все накопившиеся сообщения или полностью очищать очередь при возникновении проблем с доставкой.

В панели управления репозиторием хранятся образы всех сервисных компонентов системы. Администратор может загружать новые версии образов, отслеживать актуальность установленных компонентов и при необходимости удалять устаревшие дистрибутивы для освобождения дискового пространства. Для каждого образа отображается его имя, версия, размер и дата последнего обновления.

При возникновении ошибок или нештатных ситуаций администратор использует системные журналы, расположенные в каталоге */var/log/deepmail/*. Анализ логов позволяет выявить причины сбоев в работе сервисов, проблемы с доставкой почты или ошибки при взаимодействии с внешними системами. При необходимости возможен экспорт истории событий для последующего анализа или передачи в службу технической поддержки.

Для поддержания стабильной работы сервера рекомендуется выполнять следующие действия на регулярной основе:

- контролировать заполненность дисковых хранилищ и своевременно расширять их при необходимости;
- отслеживать актуальность антивирусных баз и версий программных компонентов;
- анализировать почтовые очереди на предмет застоявшихся сообщений;
- проверять логи на наличие повторяющихся ошибок или предупреждений;
- выполнять резервное копирование критичных данных согласно утвержденному регламенту.

Система автоматически пытается восстановить работоспособность сервисов при обнаружении проблем. Если автоматические механизмы не приводят к желаемому результату, администратор может выполнить реконфигурацию отдельных сервисов через веб-интерфейс или, в крайнем случае, осуществить перезапуск всей системы с использованием команд *deepmail stop* и *deepmail start* на соответствующих узлах.

Администратору доступны функции управления лицензиями сервера и клиентских подключений. В соответствующем разделе панели управления отображается информация о текущем статусе лицензий, количестве используемых и доступных лицензий, а также сроках их действия. При приближении даты окончания действия лицензии система выводит соответствующие уведомления.

Для обеспечения сохранности данных предусмотрены механизмы экспорта и импорта конфигураций профилей в JSON-формате, что позволяет создавать резервные копии

настроек и восстанавливать их при необходимости. Также система поддерживает возможность ведения истории изменений критически важных параметров, что помогает при расследовании инцидентов или восстановлении после ошибочных действий администратора.

Для обеспечения стабильной и безопасной работы сервера DeepMail администратору необходимо выполнять комплекс регулярных регламентных операций. Ниже приведён перечень основных задач с рекомендуемой периодичностью и кратким описанием действий.

Ежедневные операции

Область	Действие	Периодичность
Мониторинг состояния	Проверка панели управления на наличие критических уведомлений (статусы хостов, сервисов, хранилищ). Оценка нагрузки CPU, RAM, дисковой активности.	Ежедневно
Почтовые очереди	Контроль размера очереди SMTP. При обнаружении «зависших» писем — принудительная отправка или очистка через веб-интерфейс.	Ежедневно
Логи ошибок	Быстрый просмотр системных журналов */var/log/deepmail/* на предмет новых критических ошибок (например, сбоев аутентификации, проблем с доставкой).	Ежедневно

Еженедельные операции

Область	Действие	Периодичность
Заполненность хранилищ	Анализ графиков заполненности томов CORE, MAIL, DAV, ARCHIVE. Планирование расширения дискового пространства при превышении порога (рекомендуется 80–85%).	Еженедельно
Актуальность антивирусных баз	Проверка даты последнего обновления антивирусных сигнатур (при использовании встроенного антивируса или KSMG). При необходимости — ручное обновление.	Еженедельно
Резервное копирование	Контроль выполнения запланированных задач резервного копирования (снапшоты	Еженедельно

Область	Действие	Периодичность
	ВМ, дампы БД, копии конфигураций). Проверка целостности резервных копий.	
Анализ производительности	Просмотр долгосрочных графиков CPU/RAM (период 7 дней) для выявления трендов и аномалий.	Еженедельно

Ежемесячные операции

Область	Действие	Периодичность
Обновление компонентов	Проверка наличия новых версий образов в репозитории DeepMail. Планирование обновления сервисов (admin, smtp, imap и др.) в соответствии с политикой организации.	Ежемесячно
Аудит безопасности	Просмотр логов авторизации и подозрительных попыток входа. Анализ активности пользователей с высокими привилегиями.	Ежемесячно
Очистка устаревших данных	Оценка необходимости окончательного удаления писем из корзины второго уровня (Recoverable) в соответствии с политикой хранения. Настройка параметров автоочистки в IMAP-профиле.	Ежемесячно
Проверка лицензий	Контроль срока действия лицензий сервера и клиентских подключений. Планирование продления.	Ежемесячно
Тестирование восстановления	Выборочная проверка возможности восстановления данных из резервных копий (например, восстановление одного почтового ящика).	Ежемесячно

Ежеквартальные операции

Область	Действие	Периодичность
Обновление версии DeepMail	Плановое обновление платформы до актуальной версии (при наличии	Ежеквартально

Область	Действие	Периодичность
	значительных релизов). Предварительное тестирование в изолированной среде.	
Оптимизация хранилищ	Реорганизация томов (дефрагментация, миграция на более производительные носители) при необходимости.	Ежеквартально
Инвентаризация конфигураций	Проверка и актуализация профилей SMTP/IMAP, параметров ретрансляции, фильтров. Удаление неиспользуемых профилей.	Ежеквартально
Повторная оценка политик безопасности	Анализ настроек двухфакторной аутентификации, парольных политик, прав доступа. Корректировка в соответствии с новыми требованиями. Сканирование уязвимостей.	Ежеквартально

Дополнительные рекомендации:

- все изменения конфигурации перед применением в продуктивной среде рекомендуется тестировать на стенде, идентичном продуктивному;
- для критических обновлений (особенно затрагивающих ядро системы) следует создавать полные снапшоты всех узлов;
- ведение журнала регламентных работ (дата, ответственный, выполненные действия, результат) помогает при расследовании инцидентов;
- при возникновении нештатных ситуаций, не описанных в данном разделе, следует обращаться к технической документации или в службу поддержки.

Выполнение описанных регламентных операций позволяет поддерживать высокую доступность, производительность и безопасность почтовой системы DeepMail на протяжении всего жизненного цикла.

ПЕРЕЧЕНЬ ТЕРМИНОВ

Определения терминов, применяемых в настоящем документе, приведены в таблице 6.

Таблица 6 – 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;

2FA – англ. «two-factor authentication» – двухфакторная аутентификация.