АО «Иридиум»

РУКОВОДСТВО АДМИНИСТРАТОРА

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

RU.УГСФ.00003-01 90 01

Листов 247

2026

АННОТАЦИЯ

Настоящий документ содержит руководство администратора по безопасной 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, РЕД ОС и РОСА.

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;
- порядок настройки транспортных правил;
- порядок обеспечения регистрации событий безопасности;
- порядок резервного копирования и восстановления системы;
- порядок обслуживания системы.

Описание порядка работы в клиентской части под управлением ОС Linux, Windows, Android и клиентской части для работы через веб-браузер (Веб-клиент) 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);

– RU.УГСФ.00003-01 34 05 Руководство пользователя. Автоматизированное рабочее место абонента электронной почты «DeepMail» (Клиентская часть для работы через веб-браузер).

СОДЕРЖАНИЕ

1 Общие сведения 9
1.1 Условия, необходимые для функционирования изделия 11
1.1.1 Требования к техническим средствам 11
1.1.2 Требования к программным средствам 12
2 Установка и настройка сервера 13
2.1 Общие сведения об архитектуре 13
2.2 Геораспределение 14
2.2.1 Локация 14
2.2.2 Хост 14
2.2.3 Хранилище 14
2.2.4 Сервис 15
2.2.5 Репликация 15
2.3 Роли и составляющие управляющего сервера (DM1ha) 16
2.4 Почтовая нода (DM2node, DM3node) 17
2.5 Подготовка к установке 18
2.5.1 Требования к операционной системе 18
2.5.2 Предварительные шаги 19
2.5.3 Подготовка управляющего сервера DM1ha 19
2.5.4 Подготовка почтовых нод 19
2.6 Настройка управляющего сервера (DM1ha) 20
2.6.1 Распаковка дистрибутива 20
2.6.2 Редактирование файла инвентаризации (inventory) 20
2.6.3 Последовательный запуск плейбуков Ansible 29
2.7 Настройка почтовых нод 31
2.7.1 Установка DEB-пакета 31
2.7.2 Инициализация DeepMail 31
2.8 Первичная настройка DeepMail 32
2.9 Проверка работоспособности 43
2.10 Дальнейшие шаги 43
3 Администрирование почтового сервера 44
3.1 Вход в веб-интерфейс администратора и основные элементы управления 44
3.1.1 Пользовательские настройки учетной записи администратора 50
3.1.2 Смена (обновление) пароля 51
3.1.3 Работа с файловым менеджером 51

3.2 Раздел «Система» ... 59
3.2.1 Лицензирование ... 60
3.2.2 Панель управления ... 61
3.2.2.1 Карточка хоста ... 63
3.2.2.2 Мониторинг удаленного сервера ... 64
3.2.2.3 Управление удаленным сервером ... 68
3.2.2.4 Добавление хоста ... 70
3.2.3 Репозиторий ... 73
3.2.4 Локации ... 74
3.2.4.1 Редактирование локации ... 76
3.2.4.2 Состав локации ... 77
3.2.4.3 Настройка репликации ... 78
3.2.4.4 Удаление локации ... 80
3.2.5 Хранилища ... 80
3.2.6 Профили ... 81
3.2.6.1 Настройка корзин первого и второго уровня и восстановление удаленных писем ... 84
3.2.6.2 Настройка ретрансляции ... 85
3.2.7 Прочее ... 87
3.2.7.1 Уведомления о квоте ... 87
3.2.7.2 Политики паролей ... 89
3.3 Раздел «Журналы» ... 91
3.3.1 Журналы ... 92
3.3.2 Аудит ... 96
3.4 Раздел «Пользователи» ... 98
3.4.1 Инструмент «Объявление» ... 100
3.4.2 Инструмент «Пользователи» («Список пользователей») ... 101
3.4.2.1 Добавление нового пользователя ... 103
3.4.2.2 Редактирование данных пользователей ... 107
3.4.2.3 Блокировка пользователей ... 111
3.4.2.4 Удаление пользователя ... 112
3.4.2.5 Добавление общего почтового ящика ... 112
3.4.2.6 Редактирование и удаление общих почтовых ящиков ... 114
3.4.3 Инструмент «Псевдонимы» ... 115
3.4.3.1 Системный псевдоним ... 117

3.4.3.2 Создание статического псевдонима 118
3.4.3.3 Создание динамического псевдонима 120
3.4.3.4 Редактирование псевдонима 123
3.4.3.5 Удаление псевдонима 123
3.4.4 Инструмент «Токены аутентификации» 123
3.4.4.1 Добавление токена аутентификации (новый ADMIN-токен) 125
3.4.4.2 Удаление токена аутентификации из глобального списка 127
3.4.5 Инструмент «Группы» 127
3.4.5.1 Создание новой группы 129
3.4.5.1.1 Система прав 135
3.4.5.1.1.1 Глобальные права группы пользователей 136
3.4.5.1.1.2 Доменные права группы пользователей 138
3.4.5.1.1.3 Личные права группы пользователей 139
3.4.5.1.2 Двухфакторная аутентификация в системе 140
3.4.5.2 Редактирование списка пользователей, добавленных в группу 141
3.4.5.3 Редактирование настроек группы 142
3.4.5.4 Удаление группы 143
3.4.6 Инструмент «Ресурсы» 143
2.4.6.1 Создание нового ресурса 144
2.4.6.2 Редактирование ресурса 146
2.4.6.3 Удаление ресурса 146
3.4.7 Инструмент «Почтовые домены» 147
2.4.7.1 Действия с почтовыми доменами 148
2.4.7.1.1 Добавление нового почтового домена 148
2.4.7.1.2 Изменение почтового домена 151
2.4.7.1.3 Удаление почтового домена 152
2.4.7.1 Администратор (менеджер) почтового домена 152
2.4.7.2 Настройка автоматического ответа для почтового домена 152
2.4.7.3 Управление пользователями домена 153
2.4.7.4 Управление псевдонимами пользователей почтового домена 154
2.4.7.5 Альтернативный почтовый домен 155
2.4.7.5.1 Создание альтернативного почтового домена 156
2.4.7.5.2 Удаление альтернативного почтового домена 156
2.4.7.6 DNS-записи почтового домена и генерация ключей DKIM 157
3.4.8 Инструмент «Контроллеры домена» 160

3.4.8.1 Подключение контроллера домена ... 161
3.4.8.2 Синхронизация контроллеров домена ... 163
3.4.8.3 Удаление контроллера домена ... 164
3.4.9 Инструмент «Мастер миграции» ... 164
2.4.9.1 Инструмент мастер миграции Exchange Web Services ... 165
2.4.9.1.1 Создание настроек миграции и подключение к EWS-серверу ... 166
2.4.9.1.2 Запуск миграции EWS-сервера ... 168
2.4.9.1.3 Удаление настроек миграции EWS ... 171
2.4.9.2 Инструмент мастер миграции классический IMAP ... 171
2.4.9.2.1 Создание настроек миграции и подключение к IMAP-серверу стороннего домена ... 173
2.4.9.1.4 Удаление настроек миграции для домена ... 174
3.4.10 Инструмент «Шаблоны пользователей» ... 174
3.4.11 Список переадресаций ... 177
3.5 Раздел «Безопасность» ... 179
3.5.1 Инструмент «Антиспам» ... 180
3.5.1.1 Настройка антиспама по тексту в письме ... 181
3.5.1.2 Настройка антиспама по черным и белым спискам ... 182
3.5.2 Инструмент «Поиск писем» ... 183
3.5.3 Инструмент «Правила доступа по IP» ... 186
3.5.4 Инструмент «Ограничения внешней отправки по IP» ... 188
3.5.5 Инструмент «Настройки SSL/TLS» ... 190
3.6 Раздел «Транспорт» ... 193
3.6.1 Реле ... 193
3.6.1.1 Создание релейного домена ... 194
3.6.1.2 Редактирование релейного домена ... 195
3.6.1.3 Удаление релейного домена ... 195
3.6.2 «Транспортные правила» ... 195
3.6.3 Почтовая очередь ... 198
3.7 Раздел «Моя учетная запись» ... 198
3.7.1 Инструмент «Делегирование» ... 199
3.7.1.1 WebDav ACL ... 200
3.7.1.2 Mail ACL ... 202
3.7.1.3 Отправка почты ... 205
3.7.2 Инструмент «Токены аутентификации» ... 206

3.7.3 Инструмент «Автоответ» 208
3.7.4 Инструмент «Учетные записи сторонних серверов» 209
3.7.5 Инструмент «Коллекции» 211
3.7.6 Инструмент «Настройка клиента» 213
3.8 Раздел «О DeepMail» 214
3.9 Телефония 215
3.10 RADIUS-серверы 216
3.11 Интерфейс командной строки (CLI) 217
3.12 Дополнительные правила фильтрации Sieve в DeepMail 218
3.13 Коды ошибок 223
4 Интеграция с системой мониторинга Zabbix 227
5 Обеспечение интеграции KSMG с DeepMail 231
6 Обеспечение логирования 234
7 Порядок резервного копирования и восстановления системы 236
8 Обслуживание системы 238
Перечень терминов 243
Перечень принятых сокращений 246

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: Альт, Astra Linux, Debian, Ubuntu и РЕД ОС;
- поддержка проприетарного протокола Microsoft – MAPI, оптимального для Outlook и Exchange Server;
- 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 миграции почтовых баз и учетных записей пользователей с любого почтового сервера, в том числе с Microsoft Exchange Server;
- возможность работы на российских системах виртуализации (ПК «Звезда», ПК «Иридиум»);
- защита от спама и вирусов с помощью интеграции с сертифицированными средствами;
- поддержка применения специализированного сервера аутентификации RADIUS для проверки паролей (подключение RADIUS-сервера и настройка аутентификации);
- 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);
- поддержка применения файлового хранилища пользовательских файлов с возможностью предоставления прав доступа к файлам другим пользователям системы (установка уровня доступа, установка пароля, добавление списка разрешенных IP-адресов и подсетей для доступа);
- 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 Кибер Бэкап для защиты данных;
- возможность применения функционала SIP-телефонии в рамках корпоративной PBX (выдача, ротация и выключение SIP-телефонии для пользователей системы, настройка диапазонов доменов, служебных номеров и маршрутизация вызовов посредством панели администратора);
- 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).

С версии 5.0 серверная часть «DeepMail» включает наиболее важные доработки:

- географически распределенная установка – возможность установки на нескольких площадках (локациях) с собственными параметрами подключения, с репликацией почтовых данных между ними, маршрутизацией писем на домашнюю площадку получателя и переключением почтовых клиентов на резервную площадку;

- переработана система прав доступа;

- добавлена политика паролей;

- добавлен журнал аудита;

- обновлена служба синхронизации со службами каталогов;

- реализован функционал управления объектами системы средствами командной строки;

- разработана единая система кодов ошибок;

- поддержка операционной системы РОСА;

- добавлен доступ к комплекту документации из панели администрирования.

1.1 Условия, необходимые для функционирования изделия

1.1.1 Требования к техническим средствам

Минимальная конфигурация инфраструктуры для установки серверной части в одной локации должна состоять из двух ВМ:

- на одной ВМ размещаются стеки Auth, WebDAV, Core, в которых сгруппированы сервисы хоста – это почтовая нода;

- на второй – база данных PostgreSQL, Redis, 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, РОСА.

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

АРМ «DeepMail» делится на две независимые части:

1) Клиентские приложения (клиенты) DeepMail (описание и порядок работы приведен в соответствующих руководствах):

- десктопный клиент (доступ к почте, календарям, задачам, контактам);
- веб-клиент (админ-панель, веб-клиент пользователя (доступ к почте, календарям, задачам, контактам, файлам));
- мобильные клиенты (доступ к почте, календарям, задачам, контактам);

2) Серверная часть DeepMail (Сервер) (балансировщик, хранилища, стеки и сервисы и др.):

- HAProxy (прием внешнего трафика);
- прикладные сервисы (front-service, smtp-service, imap-service, webdav, sftp, webmail, admin);
- контент, каталог и управление (auth-service, антиспам, ldap-service, DNS-резолвер, контроллер, миграция, бэкап);
- данные (PostgreSQL, хранилища Redis, хранилище NFS).

При инсталляции серверной части применяется принцип 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 развернута 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 ее восстановления (см. также пункт 1.1.1);
- 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.

2.2 Георасределение

При создании георасределенной почтовой системы установка серверной части АРМ «DeepMail» в выбранной конфигурации (рекомендуется отказоустойчивая) выполняется на нескольких локациях.

2.2.1 Локация

Локация – отдельная самодостаточная площадка установки DeepMail: географическая зона со своими хостами и хранилищами. PostgreSQL и Redis у локации могут быть свои или общие на все локации, выбор зависит от того, как у вас развернута инфраструктура. Домены и пользователи привязываются к локации, а сами почтовые данные (почта и календари/ контакты) реплицируются между локациями. Это дает близость данных к пользователям и устойчивость к отказу отдельной площадки.

Привязки хостов, хранилищ, доменов и контроллеров домена к локации устроены таким образом, что при удалении локации связанные с ней записи не удаляются, они просто теряют привязку и становятся «ничьими», пока их не привяжут к другой локации. Это защищает систему от случайной потери данных при изменении геомодели.

2.2.2 Хост

Хост – это сервер (узел), принадлежащий ровно одной локации. У хоста есть короткое имя-идентификатор в системе, список смонтированных хранилищ и признак конфигурации (актуальна ли конфигурация или сервер нужно пересобрать), привязка к локации (к какой площадке относится сервер).

Одна локация обычно содержит несколько хостов, которые делят общее сетевое хранилище площадки.

Когда у хоста меняется набор хранилищ, он помечается как «требующий пересборки», и система перестраивает его конфигурацию автоматически.

2.2.3 Хранилище

Хранилище – это место, где физически лежат данные площадки. Хранилище бывает двух типов:

1) mail – почтовые ящики (письма в нем хранятся в формате maildir);

2) dav – данные календарей и адресных книг (CalDAV/CardDAV).

У хранилища указан сетевой протокол доступа (например, NFS) и адрес. Внутри одной локации каждое хранилище общее для всех ее хостов – то есть несколько серверов площадки видят одну и ту же почту. Между локациями содержимое хранилищ синхронизирует репликация (описание приведено в 2.2.5).

2.2.4 Сервис

Сервис – это конкретный процесс на хосте: прием почты, отдача почты, обслуживание календарей, файловый доступ и т. п. У каждого сервиса есть профиль конфигурации, через который задаются его параметры, часть данных для этого берется из установочных файлов, размещенных на хосте, а часть формируется автоматически в момент запуска контейнеров сервисов при установке системы.

Для георасределения важно одно: сервисы работают на хостах, а хосты относятся к локации, поэтому каждый сервис «знает», на какой площадке он запущен, принимая при запуске ее параметры БД, Redis, часовой пояс, адреса зависимых сервисов и т. д.

Таким образом георасределенная система – это две или более локаций, между которыми система синхронизирует почту и данные календарей/ контактов. Если площадка установки одна, локация в системе тоже одна – это обычный «негеораспределенный» режим.

2.2.5 Репликация

Чтобы почта и данные календарей/ контактов были доступны не на одной, а на нескольких площадках, DeepMail постоянно синхронизирует их между локациями в фоновых процессах – за это отвечает DSA (DeepMail Storage Adapter) – фоновый агент, устанавливаемый на каждой площадке.

Репликация решает две задачи:

1) доступность при отказе площадки. Если основная локация недоступна, актуальная копия почты и календарей остается на резервной – данные не теряются и могут быть выданы пользователям;

2) близость данных. Можно держать копию ящиков ближе к пользователям другого региона.

Без репликации каждая локация была бы изолированным «островом», репликация связывает площадки в единую устойчивую систему.

На каждой площадке синхронизируются два каталога:

1) Почта – данные почтовых ящиков (формат maildir), размещенные в директории */mnt/deepmail/mail*;

2) Календари/ контакты – данные календарей и адресных книг (CalDAV/CardDAV), размещенные в директории */mnt/deepmail/dav*.

Внутри одной локации эти каталоги общие для всех ее серверов – они лежат на сетевом хранилище площадки. Их содержимое синхронизируют DSA соседних локаций, напрямую обращаясь друг с другом.

Репликация проходит в два этапа:

1) обмен списками файлов (индексами). Агенты сообщают друг другу, какие файлы и какой версии у них есть. Так каждая сторона понимает, чего у нее не хватает;

2) получение недостающих данных по запросу (сторона, у которой чего-то нет, запрашивает недостающее у «соседа»). Данные передаются только по необходимости, а не «все подряд».

Если один и тот же файл изменился на двух площадках одновременно, конфликт разрешается по принципу «выигрывает последняя версия».

DSA использует два сетевых порта – это важно для настройки межсетевых экранов между площадками:

- 8384 – управляющий канал (через него площадка настраивает только свой DSA);
- 22000 – канал обмена данными между DSA соседних площадок.

Важно! Между локациями обязательно должен быть открыт порт 22000, без него DSA «видят» друг друга как отключенных, и синхронизация не идет.

Важно! Администратор каждой локации настраивает только свой DSA.

Включение, узкие настройки и мониторинг репликации выполняет администратор посредством админ-панели (подробнее см. в 3.2.4.1).

2.3 Роли и составляющие 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 (запускает плейбуки). Позволяет автоматизировать настройку всех серверов по заданному сценарию. Каталог Ansible входит в состав дистрибутива DeepMail вместе с CLI-бинарниками;

- 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, права, политики, конфигурация и аудит;

- Redis – в системе их два: внешний кластер (системный) и контейнер внутри стека Core. Системный Redis-кластер локации (внешний, вне стеков DeepMail) – предназначен для сессий веб-входа, кэша повторных проверок входа, lockout-счетчиков, SSO-токенов веб-почты, rate-limit отправки. Адрес и пароль кластера хранятся в БД на уровне локации. Контейнер Redis-антиспам в стеке Core – предназначен только для antispam-service (нечеткие хэши и история проверок rspamd);

- 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.

2.4 Почтовая нода (DM2node, DM3node)

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

- auth-service – единая проверка учетных данных для всех протоколов;

- webdav-service – предоставляет доступ к календарям, адресным книгам и задачам по протоколам CalDAV/CardDAV, free-busy; доступ к коллекциям;

- resolver-service – резолвинг имен с DNSSEC; обслуживает другие контейнеры

- front-service – терминирует TLS, разбирает протоколы, проксирует к нужному сервису;

- admin-service – веб-интерфейс для администратора и личный кабинет, REST-API, фоновые задачи;

- webmail-service – Веб-клиент почты с SSO и плагинами календарей/контактов;

- imap-service – IMAP/POP3, локальная доставка по LMTP, правила Sieve, квоты, поиск;

- smtp-service – прием/отправка, очередь, транспорт, политики, MTA-STS/DANE;

- sftp-service – доступ к файловому хранилищу пользователя по SFTP/FTP/WebDAV;

- antispam-service – фильтрация сообщений, антивирусная проверка вложений, подпись DKIM/ARC исходящих с помощью Rspamd и ClamAV;

- migration-service – Перенос почты с внешних серверов (IMAP/EWS);

- ldap-service – синхронизация пользователей и контактов с контроллерами домена (AD / ALD Pro / FreeIPA / Samba) и наполнение общей адресной книги (GAB);

- redis – антиспамовый Redis в стеке, который используется только antispam-service (нечеткие хэши и история проверок rspamd).

Каждый сервис Сервера работает в собственном контейнере и решает одну задачу (прием почты, выдача по IMAP, проверка входа, антиспам, календари и т. д.). Сервисы взаимодействуют друг с другом и управляются общей обвязкой.

Все эти сервисы запущены в контейнерах Docker, что обеспечивает изоляцию и простоту обновления. Автозапуск выполняется агентом-раннером, который является общей обвязкой для всех сервисов – это первый процесс в контейнере (точка входа). Он работает все время, пока существует контейнер: на старте собирает конфигурацию и запускает «родной» процесс сервиса (Dovecot, Postfix, nginx и т. п.), потом следит за этим процессом.

Дополнительно к контейнерам сервисов в системе предусмотрены:

- контроллер хоста – оркестратор, работающий на каждом сервере: приводит набор контейнеров на сервере в соответствие с базой данных;

- DSA (DeepMail Storage Adapter) – фоновый агент межлокационной синхронизации почты и календарей (необходим только для геораспределенного варианта установки);

- резервное копирование – отдельное приложение восстановления.

2.5 Подготовка к установке

2.5.1 Требования к операционной системе

DeepMail разработан для работы на Astra Linux Special Edition 1.7 и 1.8 (релизы «Орел», «Воронеж», «Смоленск»). Также поддерживаются: «Альт Рабочая станция» (версии 9, 10), Debian 12 и выше, Ubuntu, РЕД ОС 8+, РОСА. В данном руководстве все примеры приведены для Astra Linux.

Важное замечание по безопасности: уровень защищенности операционной системы должен быть переведен 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.

2.5.2 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 размещен на DM1ha, например, в домашнем каталоге.

2.5.3 Подготовка управляющего сервера DM1ha

На DM1ha нужно установить два пакета, которые будут использоваться только на этапе установки, для этого в терминале ввести:

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*).

2.5.4 Подготовка почтовых нод

На каждой почтовой ноде (DM2node и, при трехсерверной 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 удаленные хранилища (*core, mail, dav, archive*), которые находятся на управляющем сервере.

2.6 Настройка управляющего сервера (DM1ha)

2.6.1 Распаковка дистрибутива

На DM1ha распакуйте архив и перейдите в каталог с плейбуками:

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

cd deepmail-server-5.0/*

2.6.2 Редактирование файла инвентаризации (inventory)

Перед запуском плейбуков необходимо заполнить inventory-файл. Все плейбуки управляются переменными указанными в *all.vars*. Переменные и их назначение приведены в таблице 2.

Таблица 2 – Переменные *all.vars*

Переменная	Назначение
install_packages	Ставить ли пакеты (postgresql, haproxy, docker.io…). Если узлы уже подготовлены – false
psql_pass	Пароль роли PostgreSQL deepmail. Должен совпадать с тем, что введете в wizard
redis_password	Пароль Redis-кластера
pgcluster_use	False – одиночный PostgreSQL; true – отказоустойчивый кластер etcd + patroni + haproxy + keepalived (нужно минимум 3 хоста в группе postgresql)
pgcluster_virtual_ip	Виртуальный IP keepalived'a перед PG-кластером (только при pgcluster_use=true)

Переменная	Назначение
keepalived_use	False – один HAProxy-фронт; true – два хоста с keepalived (нужно минимум 2 хоста в haproxy)
haproxy_address	Виртуальный адрес для keepalived перед HAProxy
core_storage_path/ mail_storage_path/ webdav_storage_path/ archive_storage_path	Пути монтирования NFS на хостах core. По умолчанию /mnt/deepmail/{core,mail,dav,archive}
nfs_*_storage_path	Пути на самих NFS-серверах (storage_core/mail/dav/archive)
auth_subnet/ webdav_subnet/ core_subnet/ noinet_subnet	docker-сети для каждого стека и «изолированной» сети

Inventory-файл – сердце конфигурации. В нем 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).

За основу берется файл *inventory-example.yml*, который содержит описание всех серверов в инфраструктуре и прочие данные, необходимые для установки. Скопируйте его и отредактируйте, для этого в терминале выполните команды:

- cp inventory-example.yml inventory.yml
- sudo nano inventory.yml

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 трех 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.

2.6.3 Последовательный запуск плейбуков Ansible

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

1)

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

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

2)

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

Плейбук *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 трех экземпляров на одном хосте – стандартная конфигурация для программной отказоустойчивости внутри одного узла (рекомендуется для тестов).

Для полноценной отказоустойчивой системы (не тестовой) рекомендуется установка трех отдельных группы хостов (redis-1, redis-2, redis-3) – каждая по одному узлу (можно посадить на одну ВМ для тестов).

На каждом узле: ставит docker, загружает образ *redis.tar.gz* из *dist/*, разворачивает *templates/redis-{1,2,3}.yml* в /etc/redis/redis-N/ и поднимает контейнер. Порт у каждого свой – 7001/ 7002/ 7003. После – на первом узле необходимо выполнить:

*docker exec -i redis-1 redis-cli --cluster create *
*redis-1:7001 redis-2:7002 redis-3:7003 *
--cluster-replicas 0 -a "<redis_password>" --cluster-yes

Это минимальный кластер, без реплик (3 мастера × 0 реплик). Рекомендуется поднимать 6 узлов с *--cluster-replicas 1* (плейбук под это надо расширить вручную).

3)

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

Плейбук *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. При необходимости дает HA через Keepalived.

В процессе выполнения команды плейбук готовит директорию */deepmail/ssl/* и сохраняет туда *cert.crt* и *cert.crt.key* из папки *certs/* размещенной рядом с плейбуком – это сертификаты, которыми HAProxy будет работать.

Важно! Для тестовых стендов применяются самоподписанные сертификаты. В условиях ввода в эксплуатацию необходимо перед запуском плейбука заменить сертификаты в папке *certs/* на собственные.

Для режима HA (когда в *inventory.yml* установлен параметр *keepalived_use=true*) в *inventory.yml* необходимо назначить два хоста в группе *haproxy*. На первом ставится *keepalived_master: true*, на остальных – *false*; *keepalived_interface* указывает имя физического интерфейса. Тогда плейбук ставит Keepalived, разворачивает *templates/keepalived.conf* (VRRP-инстанс на интерфейсе, виртуальный IP *haproxy_address*) и стартует Keepalived в автозагрузке. В шаблоне *haproxy.cfg* команда *bind* переключается с *inventory_hostname* на *haproxy_address* с флагом *transparent* (необходима прозрачная привязка к виртуальному IP).

4)

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

Одна команда реализует оба режима установки PostgreSQL:

- Одиночный – когда в *inventory.yml* установлен параметр *pgcluster_use=false*;
- Кластерный – когда в *inventory.yml* установлен параметр *pgcluster_use=true* (Минимум 3 хоста в группе *postgresql* с разными *etcd_nodename (datanode1/ datanode2/ datanode3)* и *pg_interface* (имя сетевого интерфейса для Keepalived).

При одиночном режиме установки плейбук *pg.yml* – устанавливает PostgreSQL на DM1ha, создает базу данных deepmail, пользователя deepmail и задаёт пароль из psql_pass. Также конфигурирует права доступа и выполняет необходимую инициализацию.

В кластерном режиме плейбук *pg.yml* устанавливает компоненты отказоустойчивости (Patroni, etcd для синхронизации, HAProxy и Keepalived для сети) и удаляется стандартный пакет PostgreSQL, чтобы не мешать работе. Выполняется настройка координации (etcd).

Настраивается и запускается *Patroni*, для его работы создаются нужные папки и настраивается русский язык (*locale*) en_US.UTF-8. Затем выполняется инициализация кластера (пауза 1 мин.) и запускаются балансировщик HAProxy и сервис Keepalived. Они поднимают общий виртуальный IP-адрес (*pgcluster_virtual_ip*). Включается специальная настройка ядра *net.ipv4.ip_nonlocal_bind=1*, которая позволяет этим службам слушать адрес еще до того, как он официально перейдет к ним.

Результат – единая точка входа *pgcluster_virtual_ip:5432* (через локальный HAProxy на каждом PG-хосте), к которой и подключается admin-service. В поле настроек «Postgres host» указывается именно этот виртуальный IP.

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*.

2.7 Настройка почтовых нод

2.7.1 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 займет 1-2 минуты. Во время нее выполняются пост-установочные скрипты, которые подготавливают необходимые каталоги и зависимости.

2.7.2 Инициализация DeepMail

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

В терминале введите команду:

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 веб-конфигуратор – «Deepmail Configurator». Следующие шаги выполняются через браузер.

2.8 Первичная настройка DeepMail

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

Вы увидите Deepmail Configurator – мастер, в котором выполняется первичная настройка серверной части: главное, что тут происходит – это создание локации и регистрация привязанного к ней хоста (удаленного сервера).

На главной странице конфигуратора необходимо выбрать сценарий настройки – упрощенный или расширенный (рисунок 1).

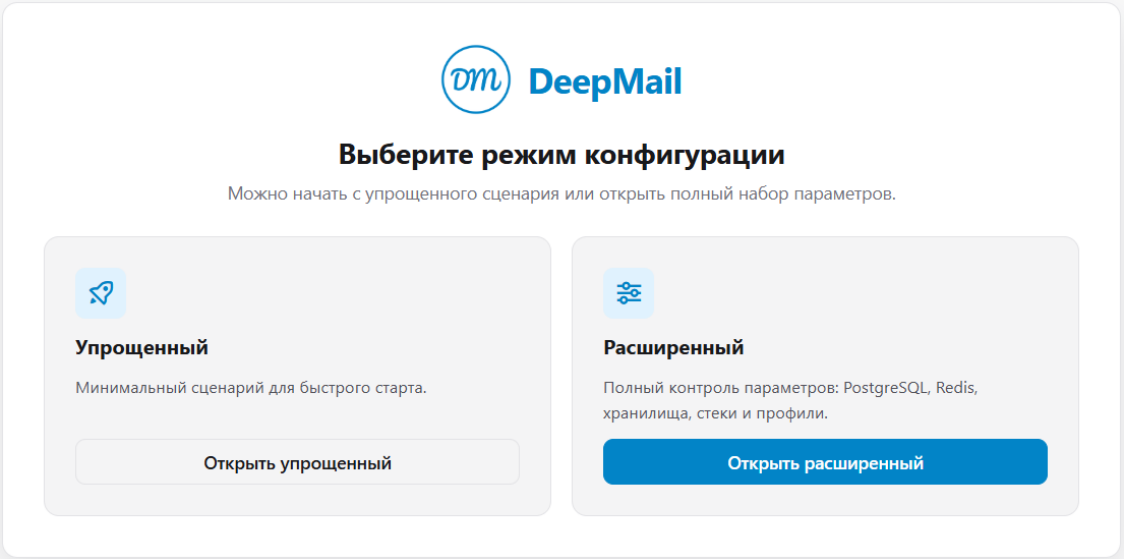


Рисунок 1 – Выбор режима конфигурации

Нажмите кнопку Открыть упрощенный или Открыть расширенный в соответствии с необходимостью.

Упрощенный режим предлагает для заполнения только базовые параметры, остальные настройки будут применены автоматически.

Параметры поделены на блоки с полями для заполнения, после заполнения обязательных полей запускается проверка конфигурации с отображением результатов в блоке «Валидация».

На рисунке 2 представлен упрощенный режим конфигурации.

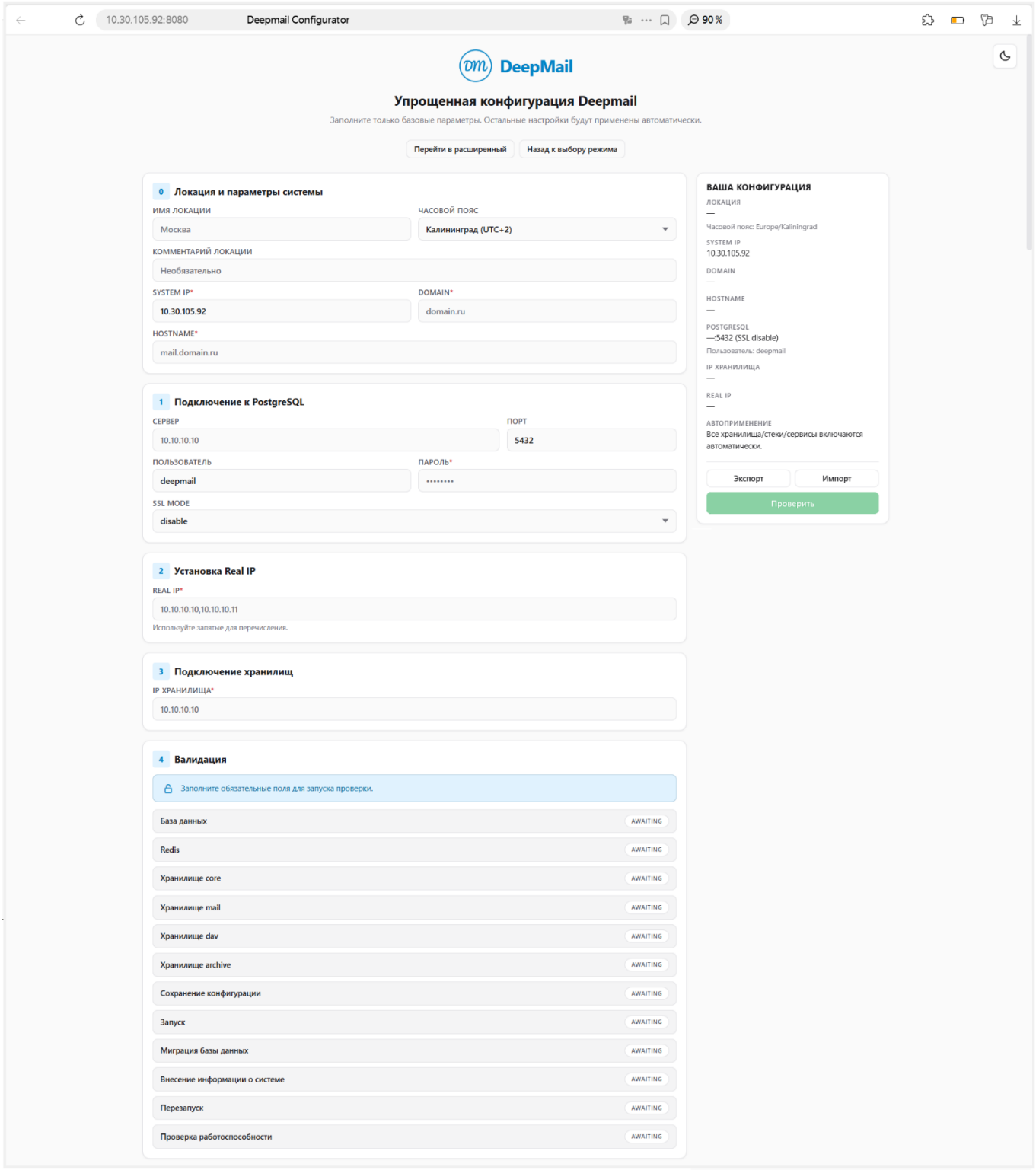


Рисунок 2 – Упрощенный режим конфигурации

Расширенный режим затрагивает все параметры подключения БД, хранилищ и необходимых сервисов, а также, при желании, в конфигураторе можно сразу настроить типовые профили сервисов перед запуском платформы, включая их расширенные параметры (рисунок 3).

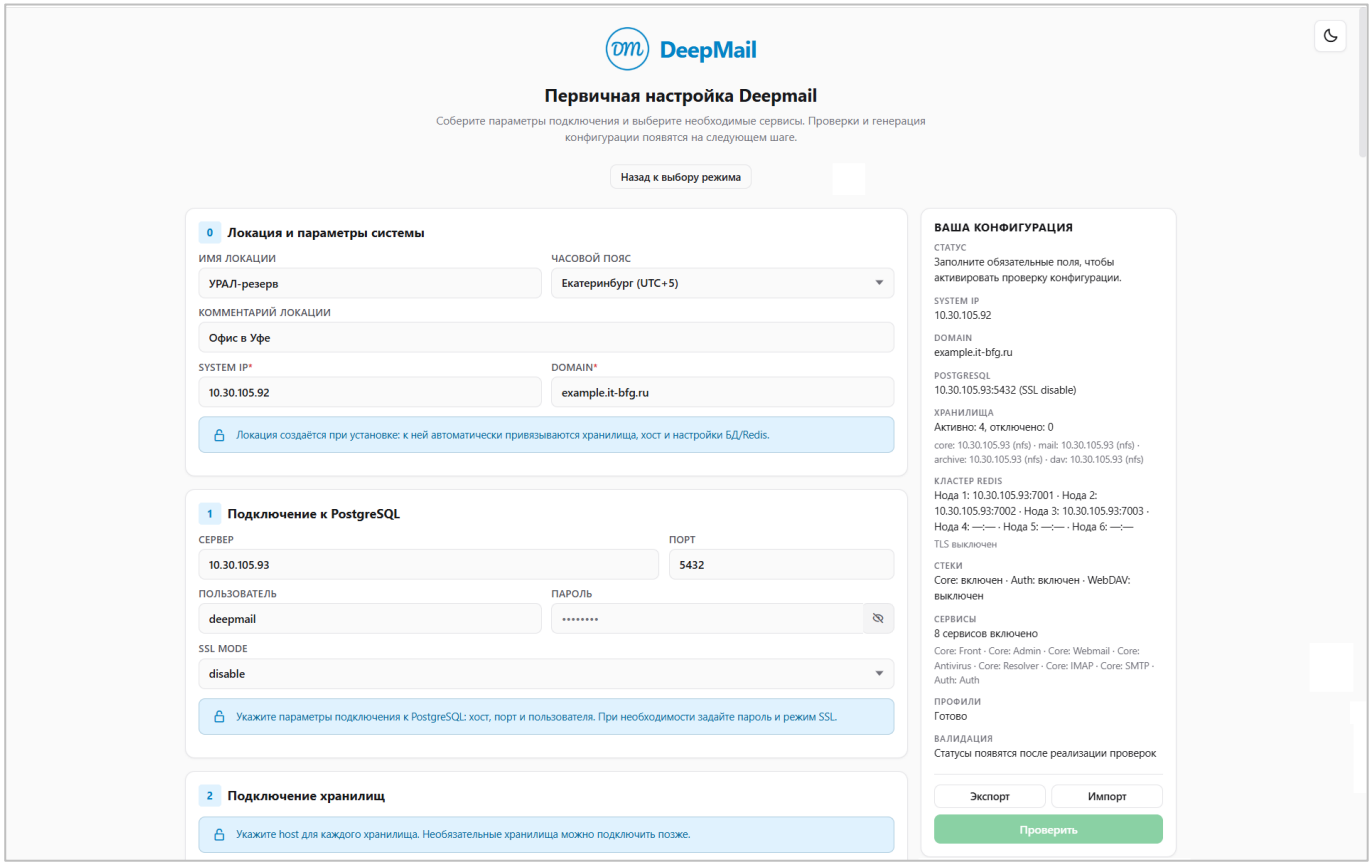


Рисунок 3 – Расширенный режим конфигурации

Кнопка  станет активной после того, как будут заполнены обязательные поля во всех блоках конфигуратора.

Далее отдельно рассмотрим состав блоков расширенного режима конфигуратора и заполнение параметров входящих в них.

Блок 0. Локация и параметры системы (см. рисунок 3).

Введите имя локации в соответствующее поле (обязательно для заполнения) – это имя будет отображаться в инструменте «Панель управления» при просмотре администратором подключенных хостов, обычно это название географической точки, например, «Москва». При необходимости впишите комментарий к локации (это справочная информация).

Выберите часовой пояс, раскрыв выпадающий список параметра «ЧАСОВОЙ ПОЯС» (рисунок 4).

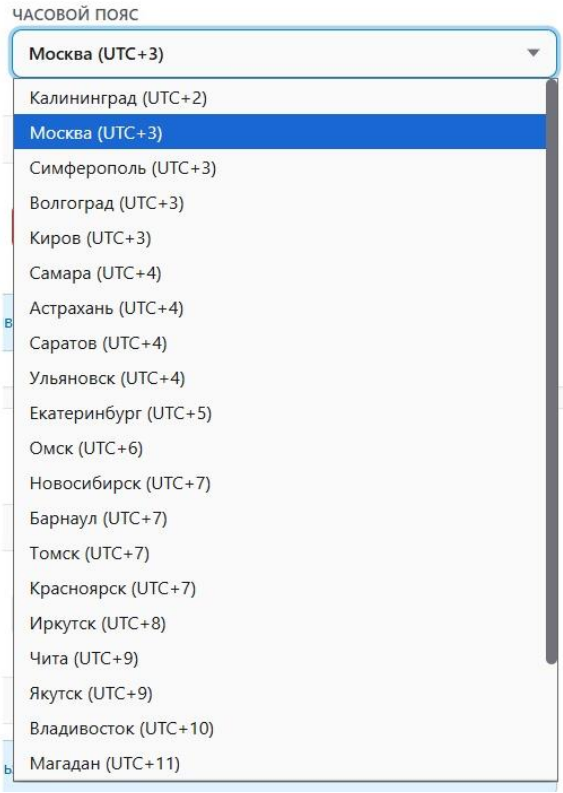


Рисунок 4 – Выбор часового пояса из выпадающего списка

Поле «SYSTEM IP» заполнится автоматически.

Укажите имя вашего будущего почтового домена в поле «DOMAIN» (например «example.ru»). Это имя будет использоваться для создания адресов электронной почты.

Блок 1. Подключение к PostgreSQL (см. рисунок 3).

Введите IP-адрес управляющего сервера DM1ha (IP одиночного PostgreSQL или виртуальный IP, если был кластерный режим установки PostgreSQL).

Порт *5432* и имя пользователя *deepmail* оставьте по умолчанию.

В поле пароль введите тот пароль, который вы задали в параметре *psql_pass* при редактировании файла инвентаризации (*inventory.yml*).

Задайте параметр «SSL MODE», выбрав значение из выпадающего списка (рисунок 5).

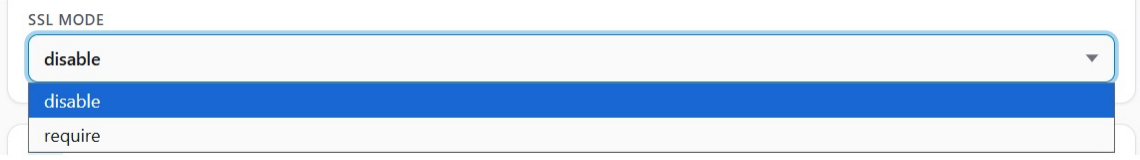


Рисунок 5 – Выбор значения параметра «SSL MODE»

Блок 2. Подключение хранилищ (рисунок 6).

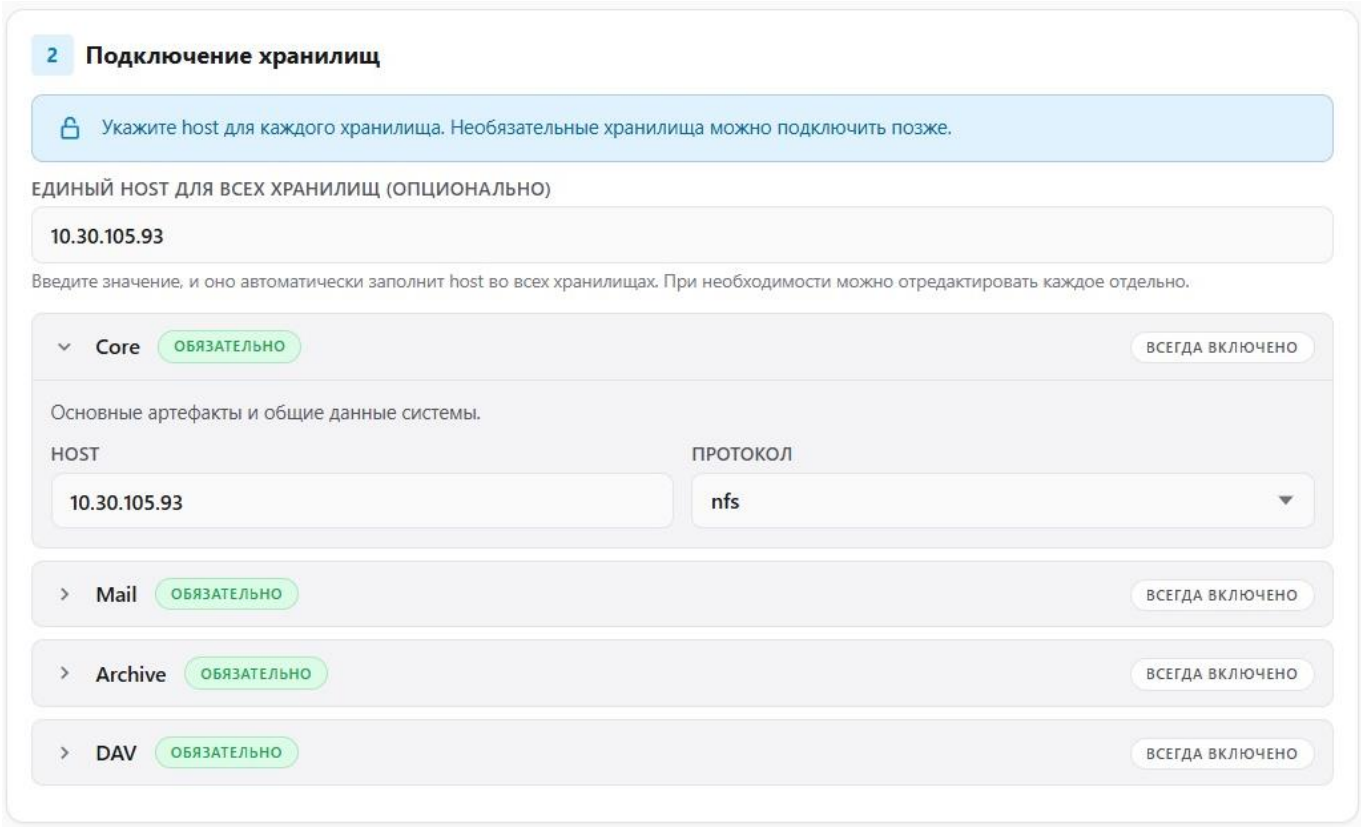


Рисунок 6 – Подключение хранилищ

Введите IP-адрес DM1ha в поле «ЕДИНЫЙ HOST ДЛЯ ВСЕХ ХРАНИЛИЩ (ОПЦИОНАЛЬНО)». Мастер автоматически подставит пути к хранилищам *Core*, *Mail*, *Archive*, *Dav*. По умолчанию эти каталоги будут примонтированы по протоколу *nfs* и использоваться для хранения всех данных.

Вы можете отдельно отредактировать параметры хранилищ. При необходимости можно задать другой хост и изменить протокол подключения для любого хранилища на local, если хранилище размещено локально (рисунок 7).

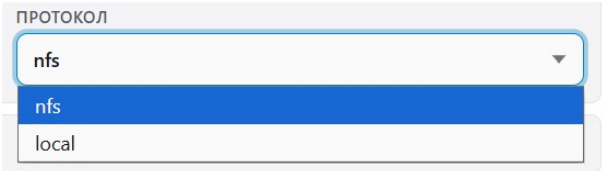


Рисунок 7 – Выбор протокола подключения хранилищ

Блок 3. Подключение к кластеру Redis (рисунок 8).

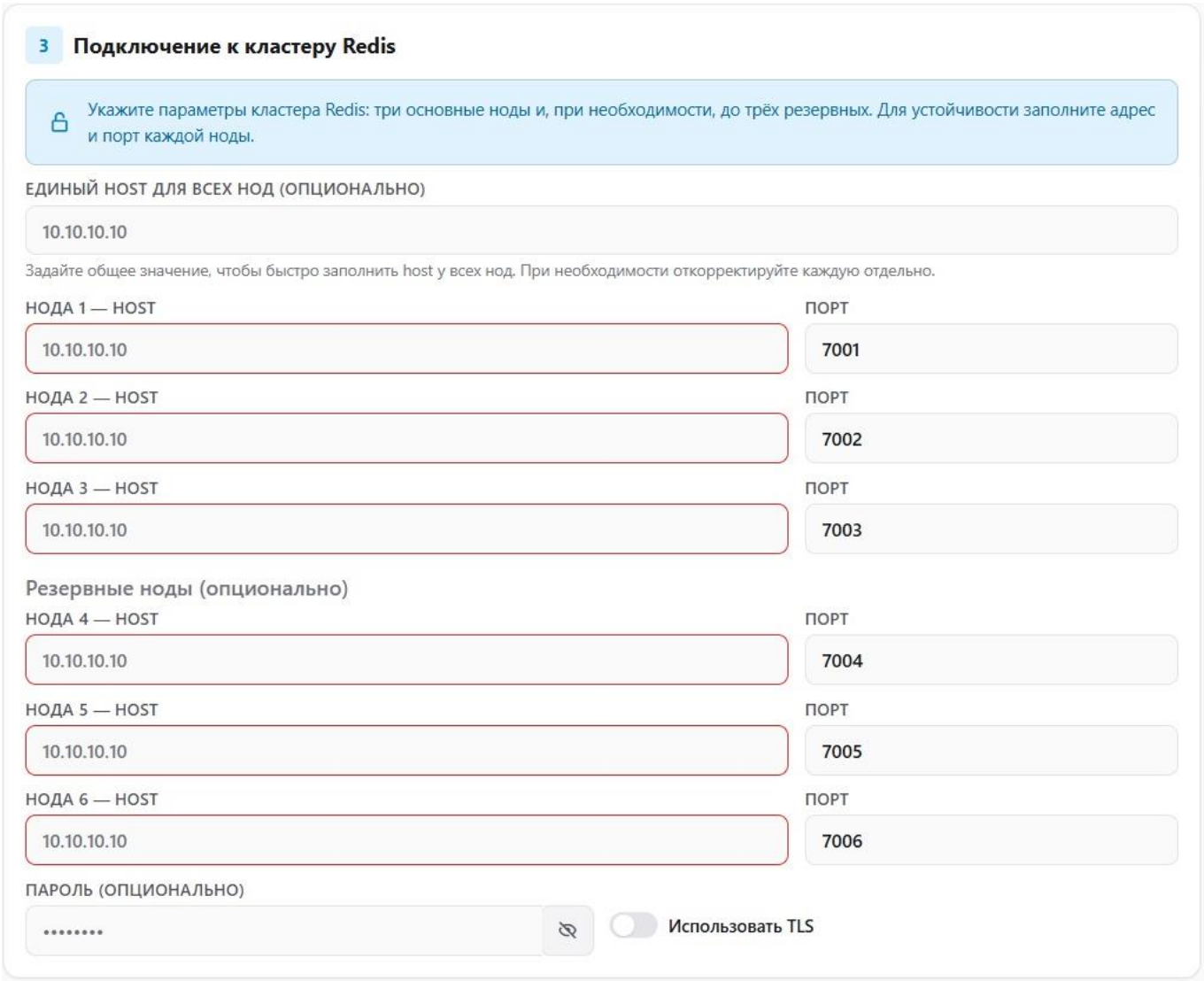


Рисунок 8 – Подключение к кластеру Redis

Укажите единый IP-адрес – IP DM1ha в поле «ЕДИНЫЙ HOST ДЛЯ ВСЕХ НОД (ОПЦИОНАЛЬНО)». Этот IP-адрес будет автоматически внесен во все поля.

Три контейнера Redis, запущенные на DM1ha, будут доступны по этому адресу. В случае если Redis развернут в полноценной отказоустойчивой конфигурации на трех разных ВМ – необходимо отредактировать IP трех нод отдельно вручную.

Также, если были добавлены дополнительные ноды Redis, для повышения устойчивости системы можно добавить дополнительные резервные IP.

Поля «ПОРТ» заполняются в соответствии с параметрами в файле *inventory.yml*.

В поле «ПАРОЛЬ (ОПЦИОНАЛЬНО)» введите пароль из параметра *redis_password* файла *inventory.yml*.

Если необходимо использовать TLS активируйте соответствующий чекбокс.

Блок 4. Стеки и сервисы (рисунок 9).

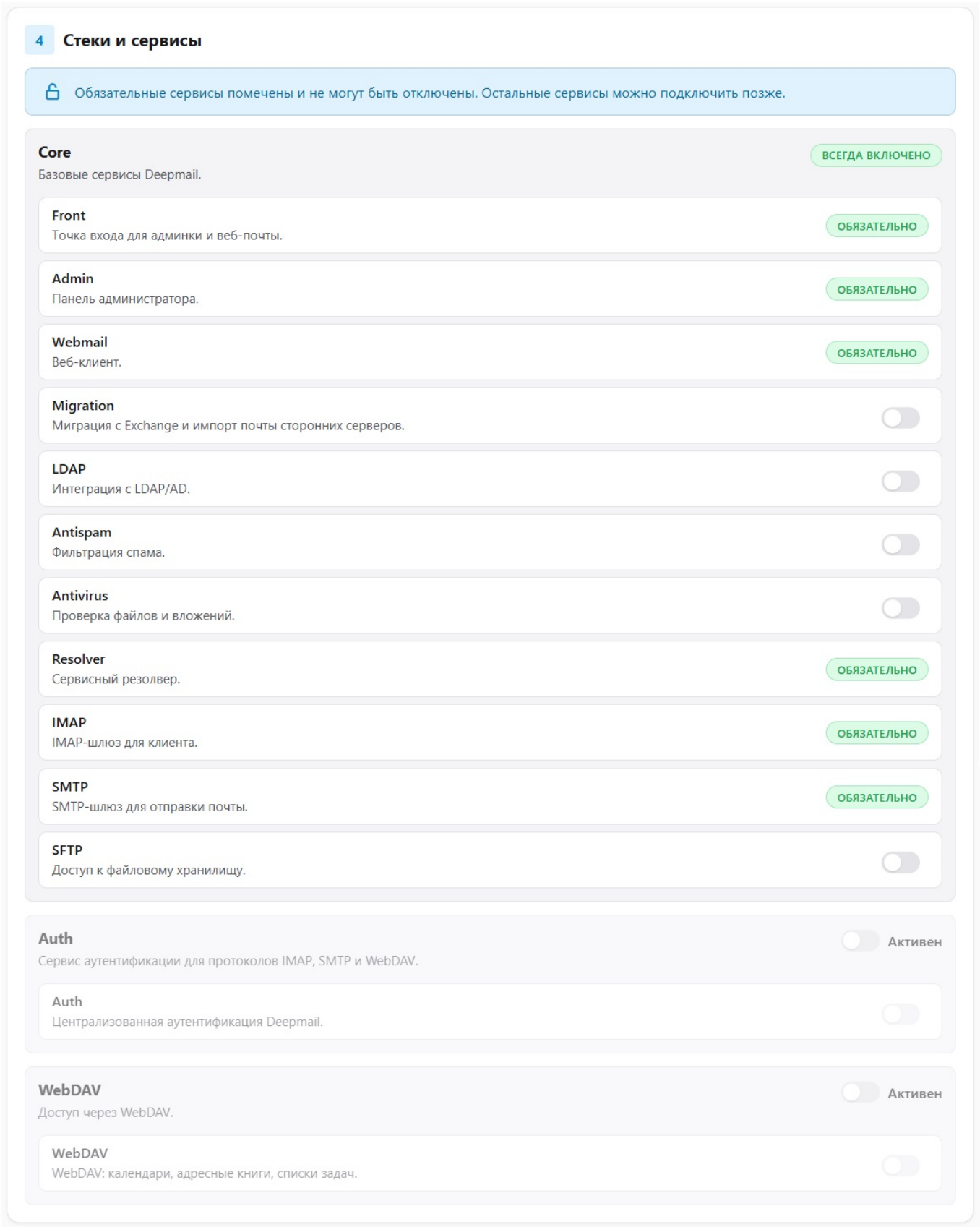


Рисунок 9 – Настройка стеков и сервисов

На этой странице перечислены все возможные сервисы DeepMail. Некоторые флажки уже установлены (Front, Admin, Webmail, Resolver, IMAP, SMTP).

Обязательно вручную установите флажки для сервисов Auth и WebDAV – они обеспечивают аутентификацию и работу календарей, контактов и задач.

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 (штатно используются ClamAV и Rspamd);
- SFTP – для доступа к файловому хранилищу по протоколу SFTP.

Блок 5. Настройка профилей.

В данном блоке выполняется настройка конфигурации профилей сервисов (IMAP/SMTP/SFTP/WebDAV) – устанавливаются лимиты, разрешения, и т.д. Изначально достаточно заполнить поля «ОБЩИЙ HOSTNAME» и «ОБЩИЙ REAL IP», эти данные автоматически будут вставлены в соответствующие поля всех профилей в блоке (рисунок 10).

В поле «ОБЩИЙ HOSTNAME» укажите полное доменное имя, которое пользователи будут вводить в настройках почтовых клиентов (в формате mail.<значение из поля «Domain» на шаге 1>).

В поле «ОБЩИЙ REAL IP» введите IP-адрес управляющего сервера DM1ha. Этот адрес будет использоваться HAProxy для приема входящих соединений. Остальные поля можно оставить без изменений, данные настройки будут доступны позже в админ-панели.

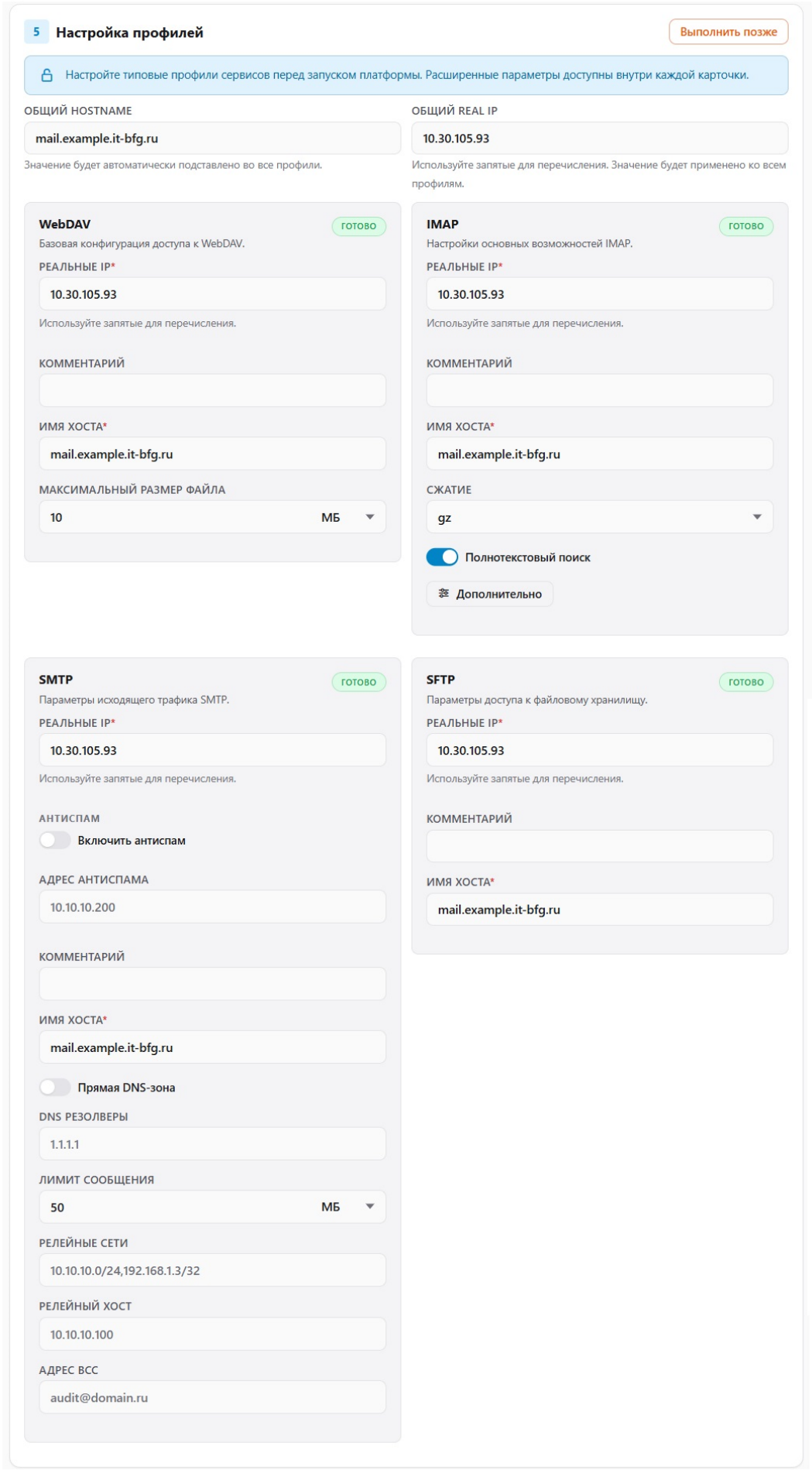


Рисунок 10 – Настройка профилей

Для профиля IMAP доступны дополнительные параметры – при нажатии в карточке профиля IMAP на кнопку Дополнительно (см. рисунок 10) появится карточка дополнительных настроек (рисунок 11).

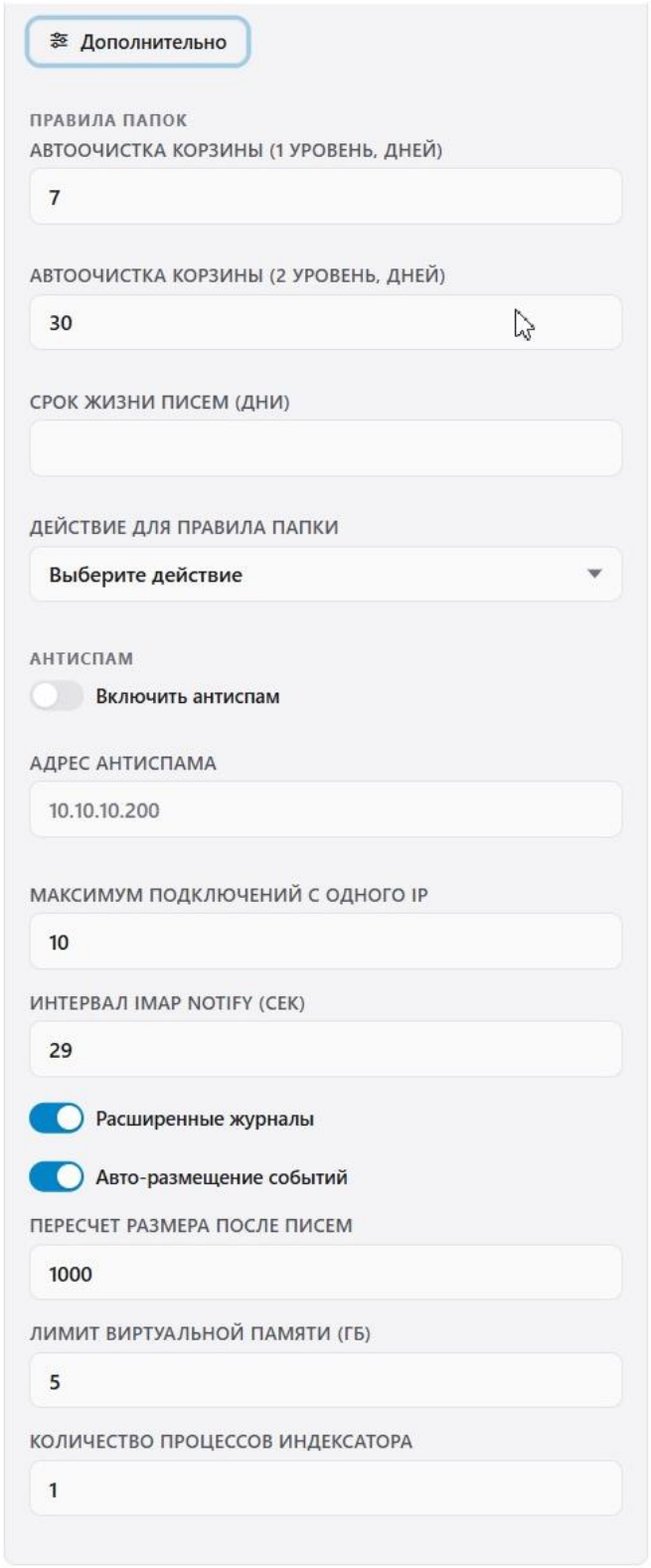


Рисунок 11 – Дополнительные настройки профиля IMAP

Данные настройки также можно выполнить позже при помощи инструмента «Профили» админ-панели (см. 3.2.6).

Блок 6. Валидация (рисунок 12).

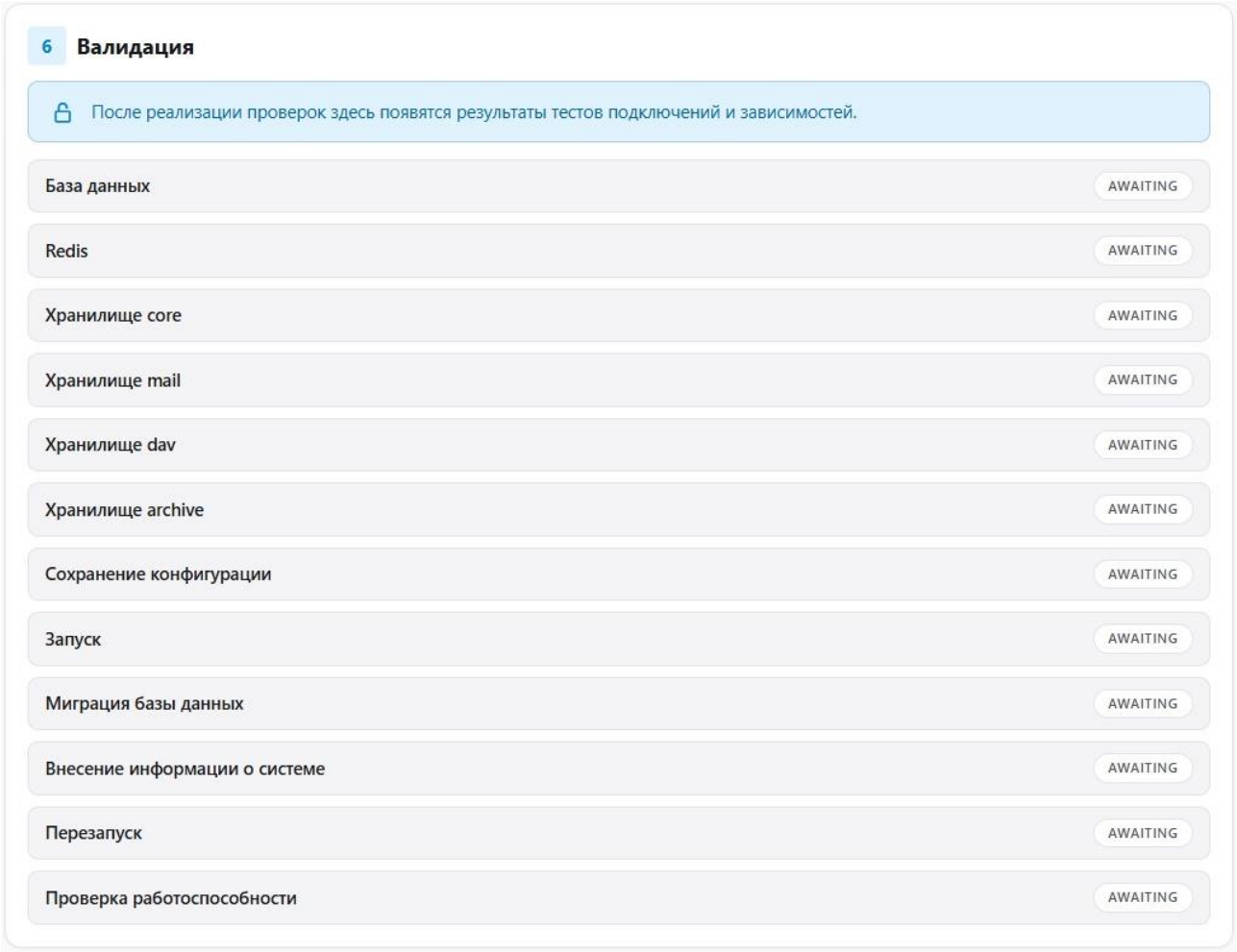


Рисунок 12 – Валидация

Нажмите кнопку «Проверить». Система последовательно протестирует: доступность PostgreSQL, Redis, подключение хранилищ, возможность запуска выбранных сервисов. Дождитесь, когда все пункты перейдут в статус «Success».

Если какой-то шаг завершился ошибкой – вернитесь к предыдущим настройкам и исправьте параметры.

После успешной проверки в конфигураторе появится кнопка «Завершить», после нажатия на которую система применит конфигурацию, перезапустит все контейнеры и станет доступен веб-интерфейс администратора, адрес для входа обычно *https://<IP_DM1ha>/ui/*.

2.9 Проверка работоспособности

После установки рекомендуется выполнить простые проверки:

- откройте веб-интерфейс администратора (см. подраздел 3.1), убедитесь, что в разделе «Система» → «Панель управления» присутствует локация и добавленный в нее сервер имеет статус «HEALTHY»;
- если вы разворачиваете конфигурацию из трех ВМ, добавьте вторую почтовую ноду (описание приведено в 3.2.2.4)
- 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).

2.10 Дальнейшие шаги

Установка завершена. Теперь вы можете приступить к администрированию системы:

- создавать почтовые домены и пользователей;
- подключать контроллеры домена для синхронизации учетных записей;
- настраивать маршрутизацию почты и правила фильтрации;
- организовывать резервное копирование;
- настраивать мониторинг через Zabbix (установка и конфигурирование системы мониторинга см. в разделе 4).

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

3 АДМИНИСТРИРОВАНИЕ ПОЧТОВОГО СЕРВЕРА

3.1 Вход в веб-интерфейс администратора и основные элементы управления

Для доступа к веб-интерфейсу администратора (далее – админ-панель) необходимо:

- открыть веб-браузер и в адресной строке ввести IP-адрес или имя почтового домена в формате «*https://<IP>*»;
- 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 13).

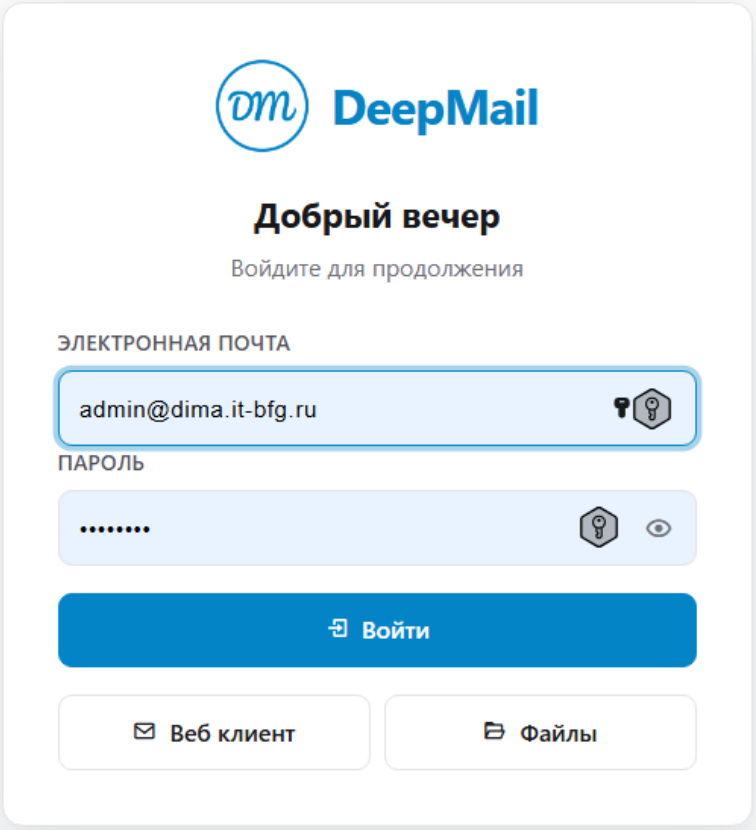
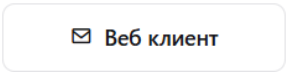


Рисунок 13 – Окно авторизации в админ-панель

Кнопки 

и 

предназначены для перехода в веб-клиент пользователя и в файловое хранилище соответственно.

Если логин или пароль были введены неверно в окне авторизации будет отображено сообщение о неверно введенных данных (рисунок 14).

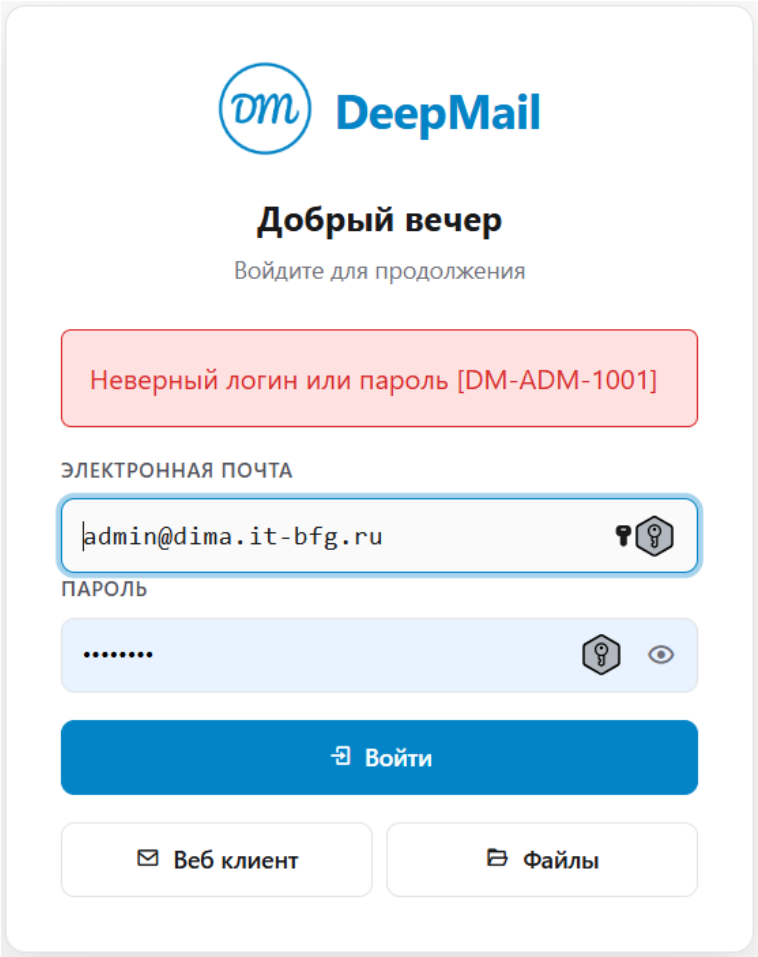


Рисунок 14 – Окно авторизации при неверно введенных учетных данных

При первом входе система потребует активации лицензии (рисунок 15).

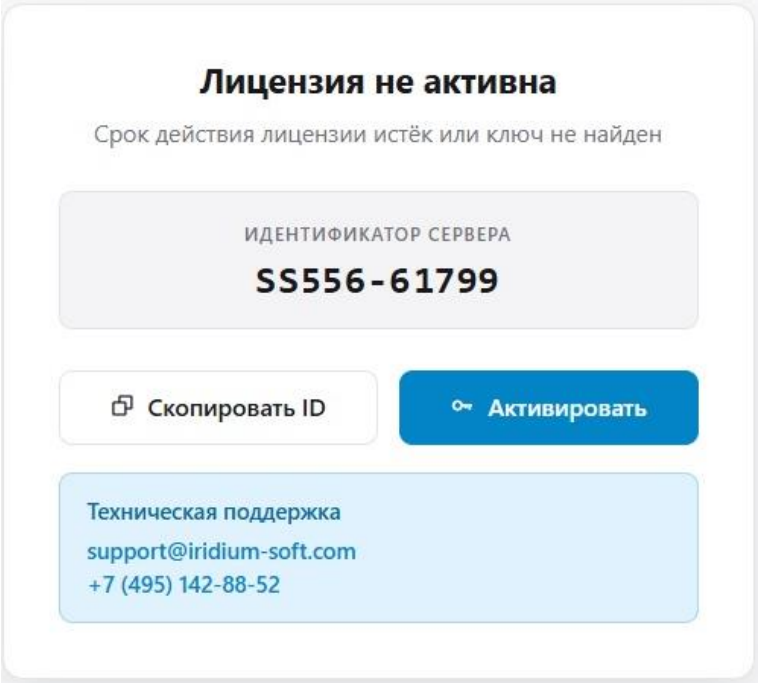
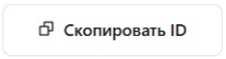


Рисунок 15 – Запрос активации лицензии

Если ключ не был получен ранее сообщите идентификатор сервера (номер лицензии) в техническую поддержку для получения лицензионного ключа. Кнопка 

позволяет скопировать номер лицензии в буфер обмена для вставки в запрос в СТП. Если у вас имеется лицензионный ключ, полученный вместе с дистрибутивом или напрямую от разработчика, нажмите кнопку 

и введите его в форму активации лицензии (рисунок 16).

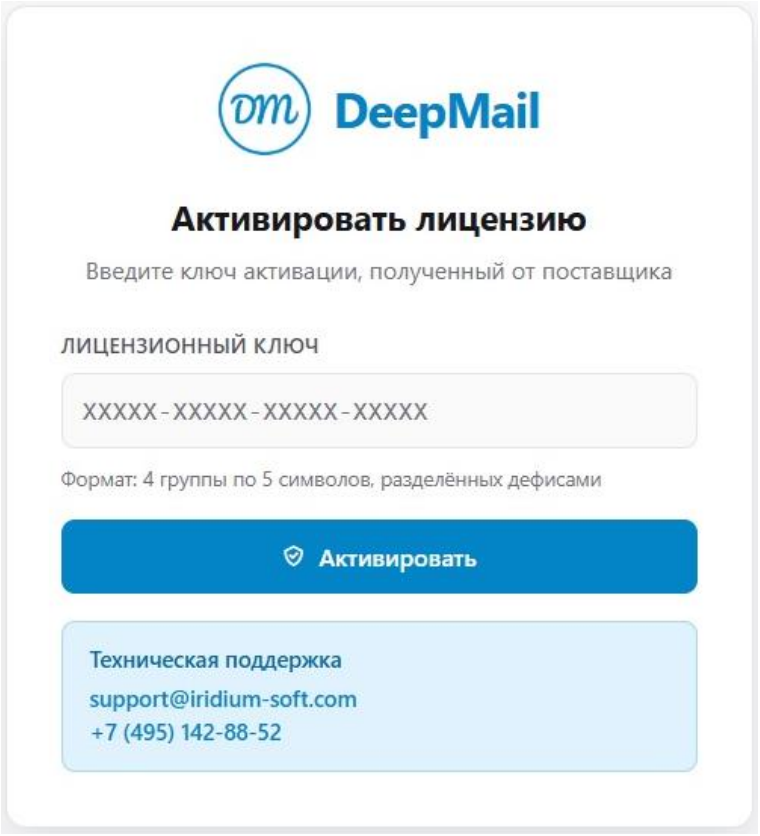


Рисунок 16 – Форма активации лицензии

После этого будет выполнена авторизация в веб-интерфейс администратора. При успешной авторизации в окне админ-панели будет отображена активная страница настроек пользователя УЗ администратора почтового сервера (рисунок 17).

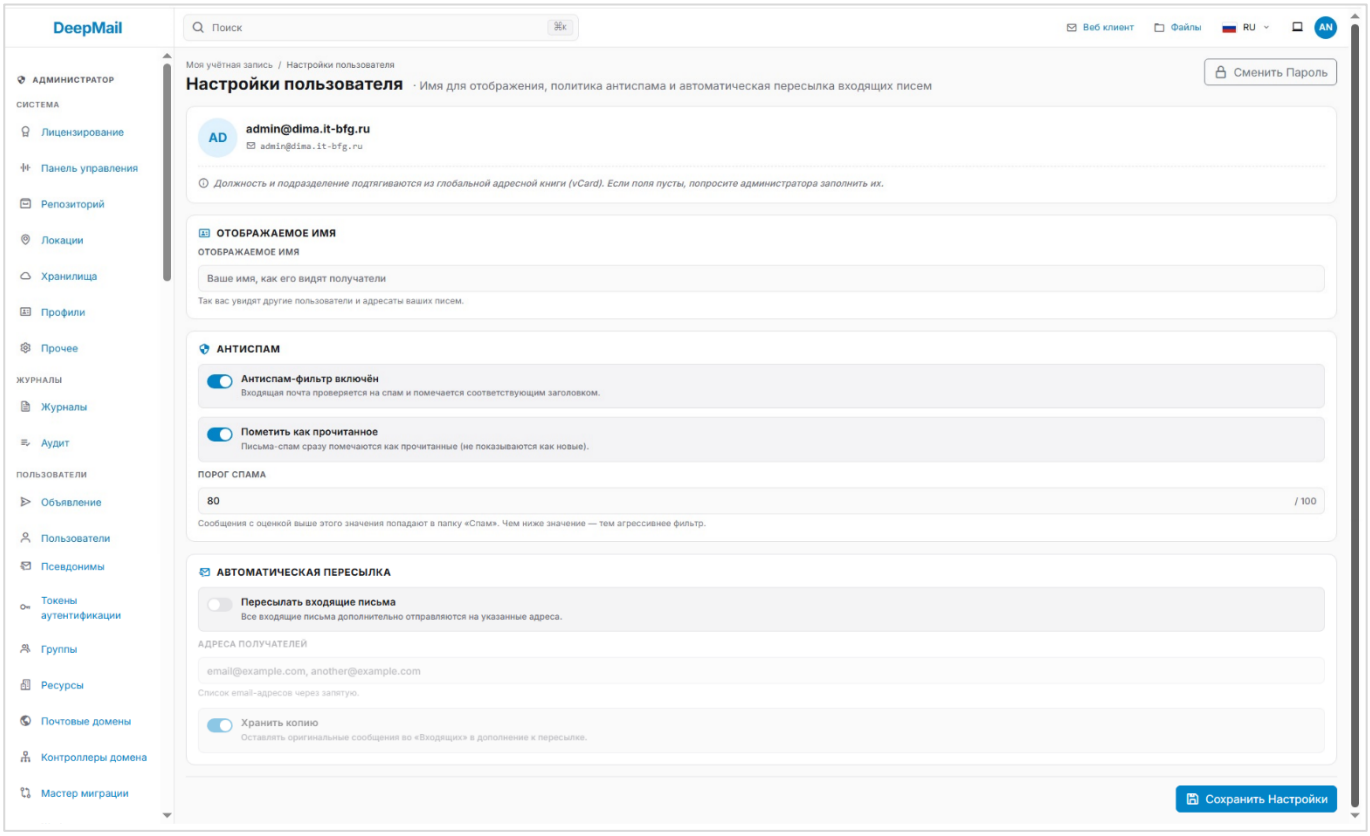


Рисунок 17 – Окно админ-панели с активной страницей настроек пользователя учетной записи администратора почтового сервера

В левой части окна размещена панель (см. рисунок 17) с кнопками инструментов управления почтовым сервером, при нажатии на которые выполняется переход на страницы настроек параметров почтовой системы, просмотра журналов, управления пользователями, параметрами безопасности и транспорта, а также управления параметрами учетной записи администратора. Инструменты сгруппированы в соответствующие разделы («Система», «Журналы», «Пользователи», «Безопасность», «Транспорт», «Моя учетная запись») (рисунок 18).

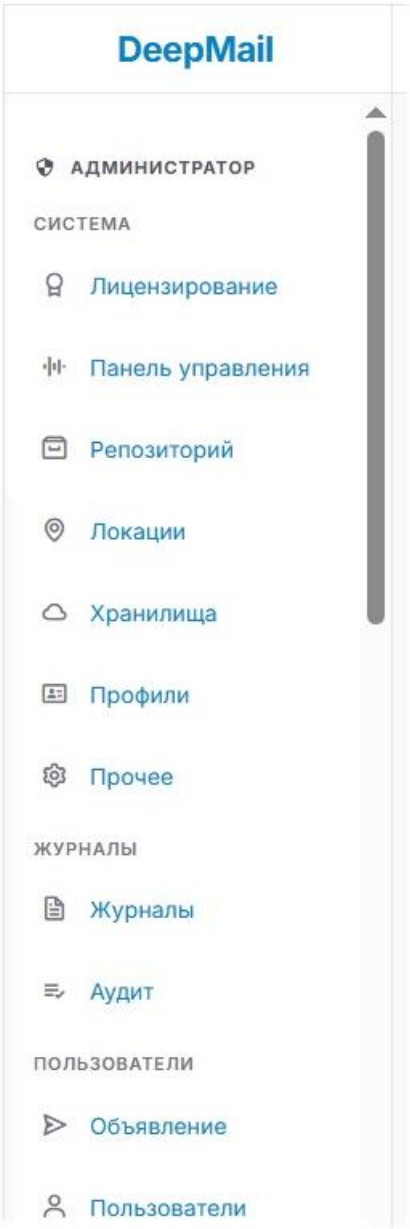


Рисунок 18 – Панель инструментов

Для перемещения по разделам панели инструментов используйте полосу прокрутки, размещенную слева, или прокрутите колесо мыши, передвинув курсор в область кнопок.

В верхней части админ-панели (см. рисунок 17) размещен инструмент поиска (рисунок 19), при помощи которого можно быстро найти определенный раздел, пользователя, домен и т.п.

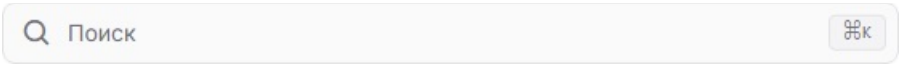


Рисунок 19 – Инструмент поиска – кнопка «Поиск»

При нажатии на кнопку «Поиск» открывается форма для введения поискового запроса (рисунок 20).

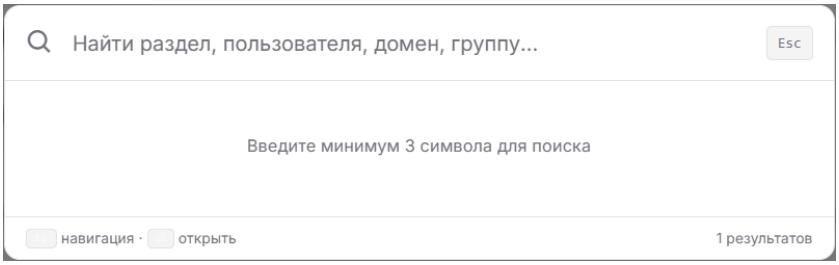


Рисунок 20 – Форма для введения поискового запроса

Начните вводить слово-запрос (или несколько слов) – в форме будут динамически отображаться результаты поиска (рисунок 21).

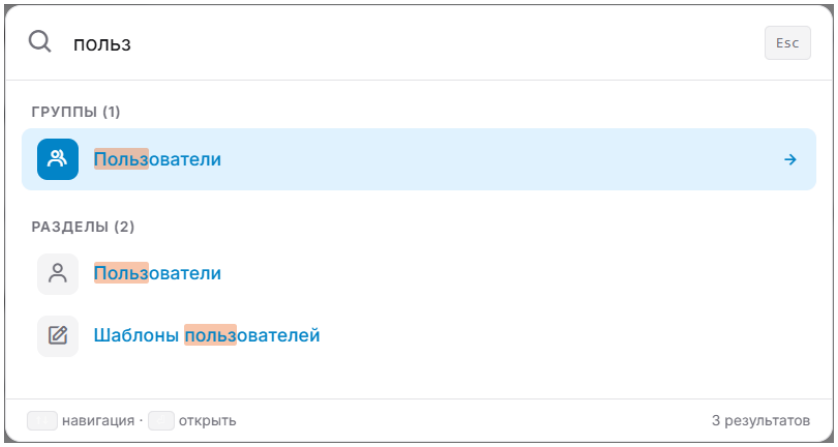


Рисунок 21 – Результаты поиска

Кликните по строке результата поиска с нужным значением – будет раскрыта соответствующая страница.

Справа в верхней части админ-панели (см. рисунок 17) размещены кнопки:

– Веб клиент – при нажатии выполняется переход на страницу авторизации в почтовый веб-клиент пользователя (порядок работы в веб-клиенте приведен в документе «Руководство пользователя. Автоматизированное рабочее место абонента электронной почты DeepMail (Клиентская часть для работы через веб-браузер)»);

– Файлы – при нажатии выполняется переход в файловое хранилище пользователя (порядок работы приведен в пункте 3.1.3);

– RU – кнопка выбора языка. В выпадающем меню доступны два языка – русский и английский, после выбора и обновления страницы все заголовки, кнопки, подсказки, предупреждения в админ-панели отображаются на выбранном языке.

Важно! Для корректной работы в веб-браузере должен быть отключен автоматический перевод содержания страниц на русский язык;

– – кнопка выбора темы оформления (по умолчанию «Системная»), с каждым кликом мыши по данной кнопке оформление админ-панели меняется на светлую тему, темную или возвращается к системной теме, при этом значок на кнопке переключения меняется: – «Светлая», – «Темная», – «Системная»);

– – кнопка меню учетной записи администратора. При нажатии на данную кнопку появляется выпадающее меню, содержащее команды для перехода на страницу настроек пользователя (администратора) (см. рисунок 17, см. пункт 3.1.1), обновления пароля (см. пункт 3.1.2) и выхода из админ-панели (рисунок 22).

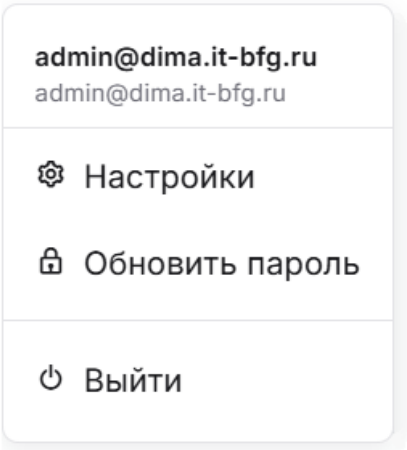


Рисунок 22 – Меню учетной записи администратора

3.1.1 Пользовательские настройки учетной записи администратора

Страница пользовательских настроек учетной записи администратора открывается при входе в админ-панель (рисунок 17). При нахождении на других страницах админ-панели для перехода на страницу настроек УЗ пользователя (администратора) необходимо раскрыть меню кнопки УЗ – (см. рисунок 17) и выбрать в нем команду «Настройки» (см. рисунок 22).

На странице пользовательских настроек администратор может:

– задать имя для отображения (то, как будет отображено его имя для других пользователей в почтовой переписке);

– настроить политику антиспама – включить/ отключить проверку своей входящей почты на спам, пометку подозрительных писем специальным заголовком, включить/ отключить пометку спам-писем сразу прочитанными (не будут отмечены в

списке входящих писем как новые), задать порог спама – это числовое значение (балл или рейтинг), при достижении которого электронное письмо отправляется в папку «Спам»;

- настроить автоматическую пересылку входящей корреспонденции – включить/ отключить пересылку входящих писем на дополнительный адрес (или несколько адресов) (значения адресов вводятся в специальное поле). Также можно включить/ отключить сохранение копии оригинального почтового сообщения в исходной папке «Входящие» в дополнение к его пересылке.

Для подтверждения настроек нажмите кнопку Сохранить Настройки (см. рисунок 17).

3.1.2 Смена (обновление) пароля

Администратор может в любой момент выполнить смену пароля, для этого необходимо нажать кнопку Сменить Пароль, размещенную в правом верхнем углу на странице настроек УЗ (см. рисунок 17) или выбрать команду «Обновить пароль» в меню кнопки УЗ (см. рисунок 22).

После нажатия кнопки или выбора команды откроется страница, где необходимо ввести новый пароль и подтвердить его (рисунок 23).

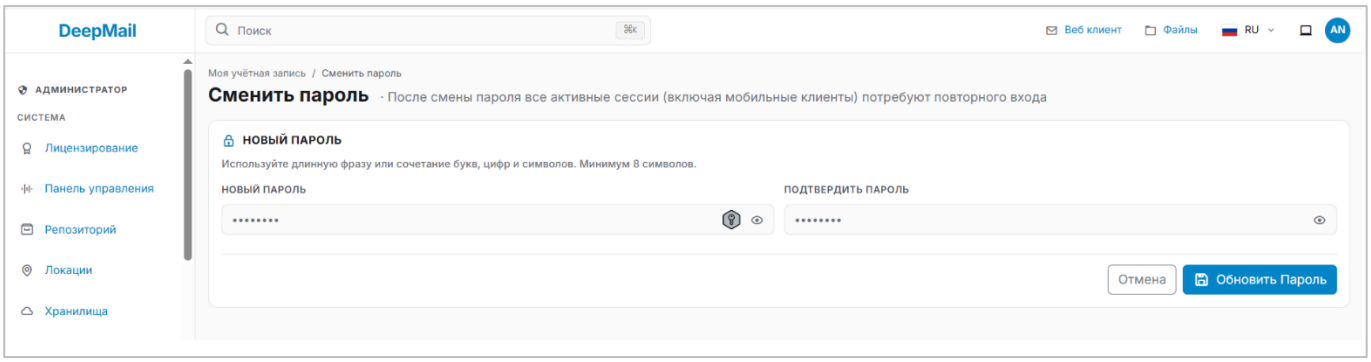


Рисунок 23 – Страница смены пароля

Для сохранения изменений нажмите кнопку Обновить Пароль. Для отказа от изменений нажмите кнопку Отмена.

3.1.3 Работа с файловым менеджером

Для перехода в режим работы с файловым менеджером DeepMail, необходимо нажать на кнопку Файлы в окне авторизации (см. рисунок 13) или кнопку Файлы, размещенную в верхнем правом углу админ-панели (см. рисунок 17), после чего откроется

окно аутентификации, в котором необходимо ввести свой логин и пароль и нажать кнопку Войти (рисунок 24).

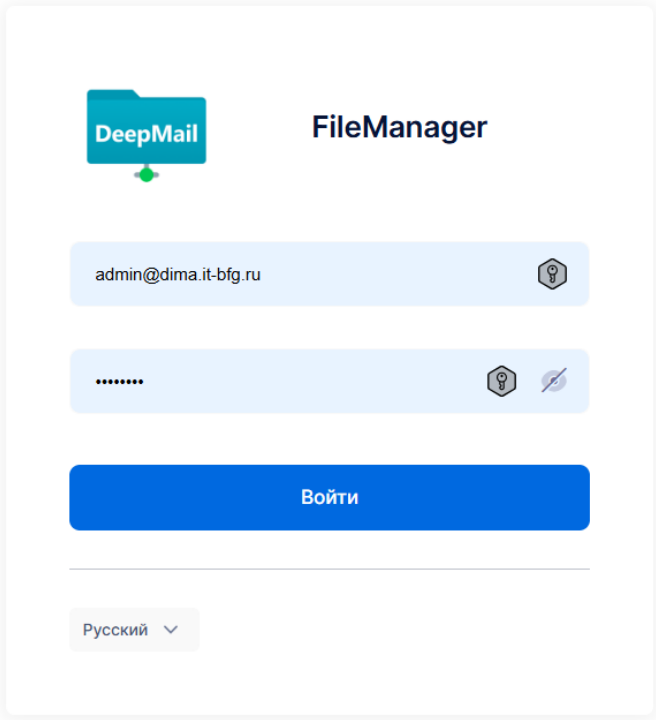


Рисунок 24 – Окно аутентификации в файловый менеджер DeepMail

Интерфейс файлового менеджера DeepMail предоставляет пользователю необходимые инструменты для работы с личным хранилищем файлов, которые включают функционал сохранения, каталогизации (создание папок, распределение файлов по папкам, копирование, перемещение и пр.) и предоставления доступа другим пользователям.

При входе в файловый менеджер на экран выводится главная страница раздела «Файлы», где отображается содержимое текущей директории (в случае отсутствия содержимого на странице будет отображено сообщение том, что директория пуста) (рисунок 25).

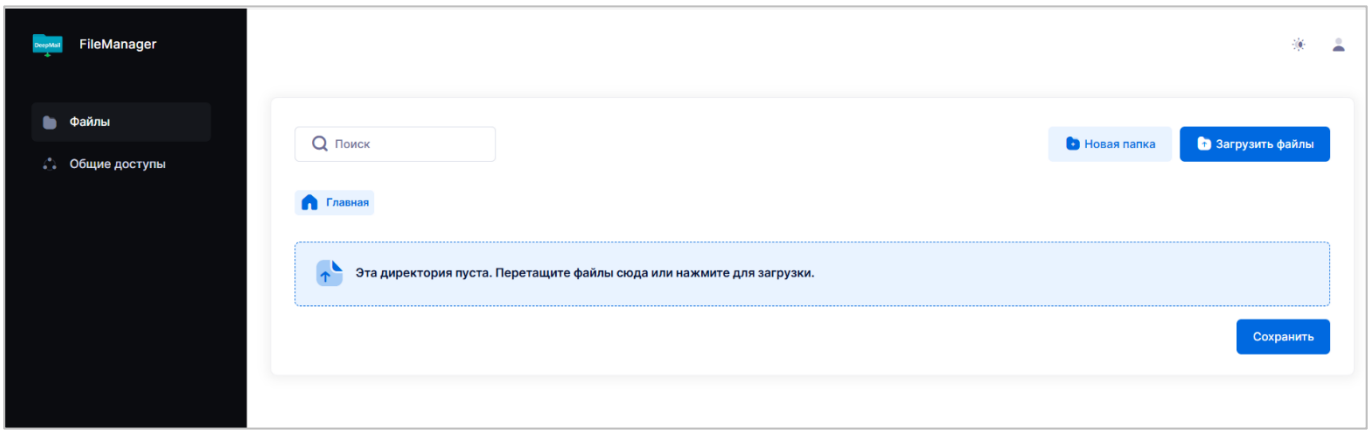


Рисунок 25 – Интерфейс файлового менеджера DeepMail

В правом верхнем углу размещены дополнительные элементы управления:

- – изменение темы оформления. При наведении курсора появляется меню выбора темы (рисунок 26);
- – управление учетной записью. При наведении курсора появляется меню с командами для перехода к настройкам профиля, смены пароля и выхода из аккаунта (рисунок 27).

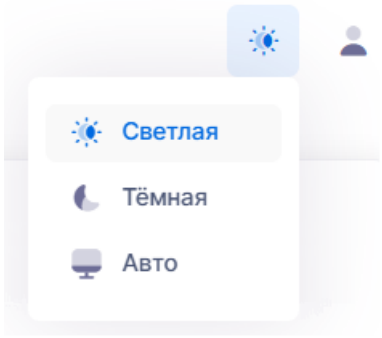


Рисунок 26 – Меню выбора темы оформления

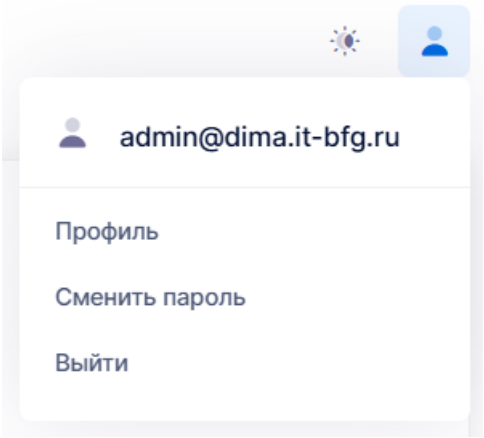


Рисунок 27 – Меню управления учетной записью

Слева на панели размещены кнопки переключения разделов (см. рисунок 25):

- «Файлы» – раздел для работы список файлов;
- «Общие доступы» – раздел для просмотра и управления доступами.

В верхней части находится строка поиска (см. рисунок 25), позволяющая быстро найти нужный файл по имени.

Список файлов представлен в виде таблицы с указанием имени, размера и даты последнего изменения. Пример отображения списка файлов, загруженных в файловое хранилище приведен на рисунке 28.

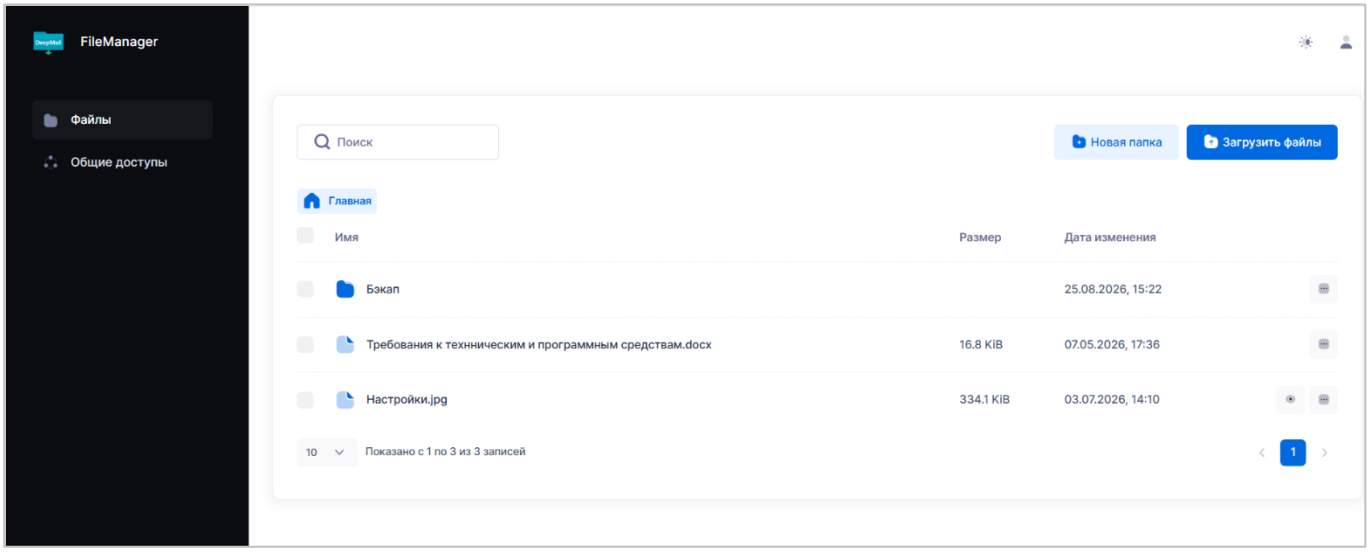
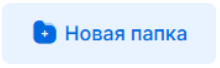


Рисунок 28 – Пример отображения файлов, загруженных в файловое хранилище

Чтобы добавить папку хранения файлов нажмите кнопку 

(см. рисунок 28). На странице появится поле для ввода имени папки (рисунок 29).

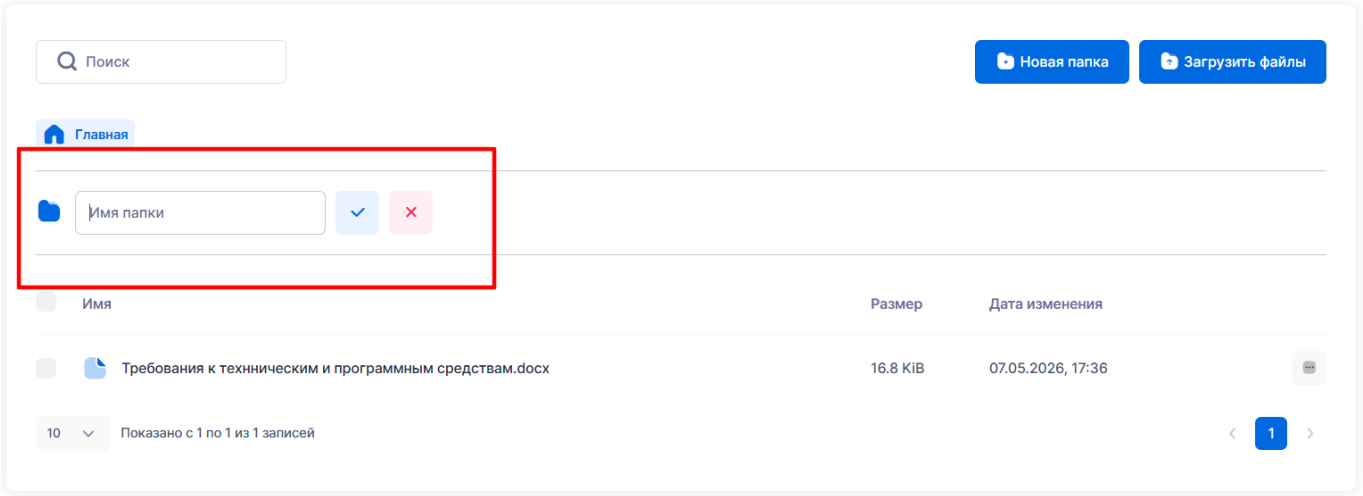


Рисунок 29 – Поле добавления новой папки

Введите имя новой папки и нажмите кнопку . Для отмены добавления папки нажмите кнопку .

Чтобы просмотреть содержимое папки щелкните мышью по ее имени в списке. В папках можно создавать подпапки. При переходе в них заголовок страницы будет содержать названия всех открытых директорий (рисунок 30).

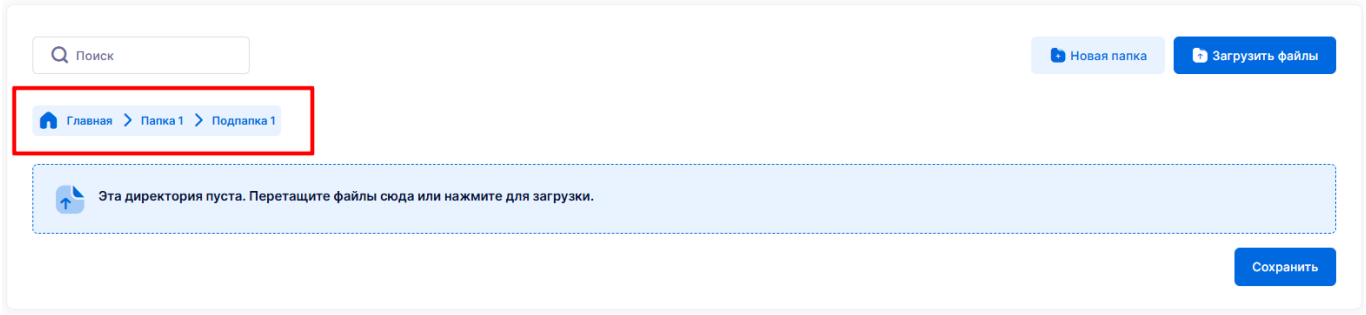


Рисунок 30 – Заголовок страницы

Для возврата в другую директорию наведите курсор на ее название в заголовке и выполните щелчок левой кнопкой мыши.

Чтобы загрузить файлы нажмите кнопку Загрузить файлы находясь в любой папке или на главной странице файлового менеджера (тогда файл будет добавлен в общий список файлов). Откроется окно загрузки файлов (рисунок 31).

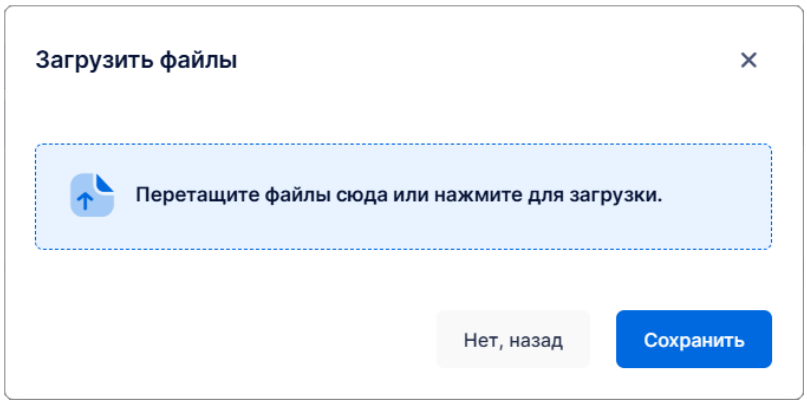


Рисунок 31 – Окно загрузки файлов

Перетащите необходимые файлы в специальную область или нажмите на нее для раскрытия окна выбора файлов в папках ПК. Затем нажмите кнопку Сохранить. Для отмены нажмите кнопку Нет, назад.

Для файлов и папок, добавленных в файловое хранилище, доступно меню управления, которое раскрывается нажатием на кнопку , размещенную слева в строке каждого файла (см. рисунок 28).

Меню содержит команды для переименования, перемещения или копирования, предоставления доступа (поделиться) и удаления файла/ папки (рисунок 32).

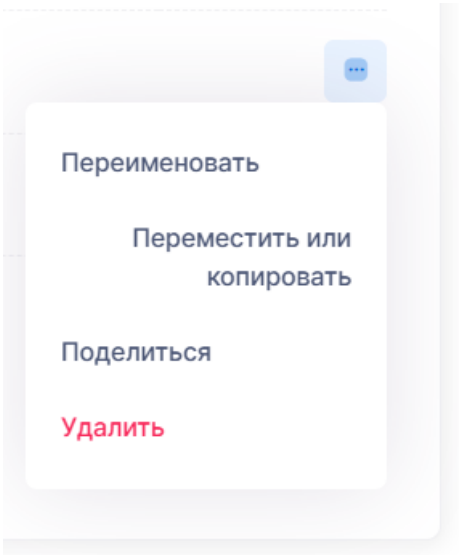


Рисунок 32 – Команды меню управления файла

При выборе команды «Переименовать» (см. рисунок 32) открывается отдельная форма для переименования (рисунок 33).

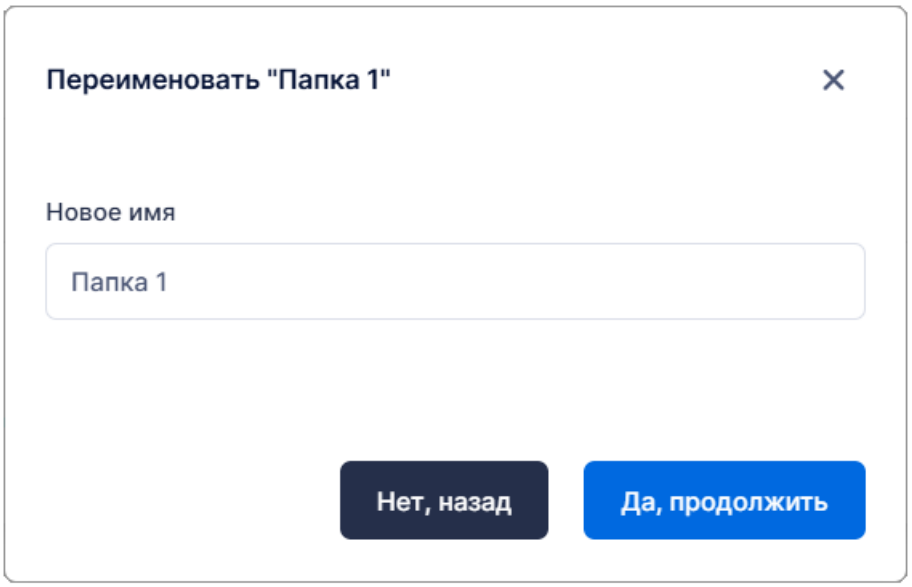


Рисунок 33 – Форма переименования файлов/ папок

Данная форма идентична как для файлов, так и для папок.

Введите новое наименование файла или папки в поле «Новое имя» и нажмите кнопку Да, продолжить. Для отказа нажмите кнопку Нет, назад.

При выборе команды «Переместить или копировать» (см. рисунок 32) открывается отдельная форма для выбора папки назначения, в которую будет перемещен или скопирован файл/ папка (рисунок 34).

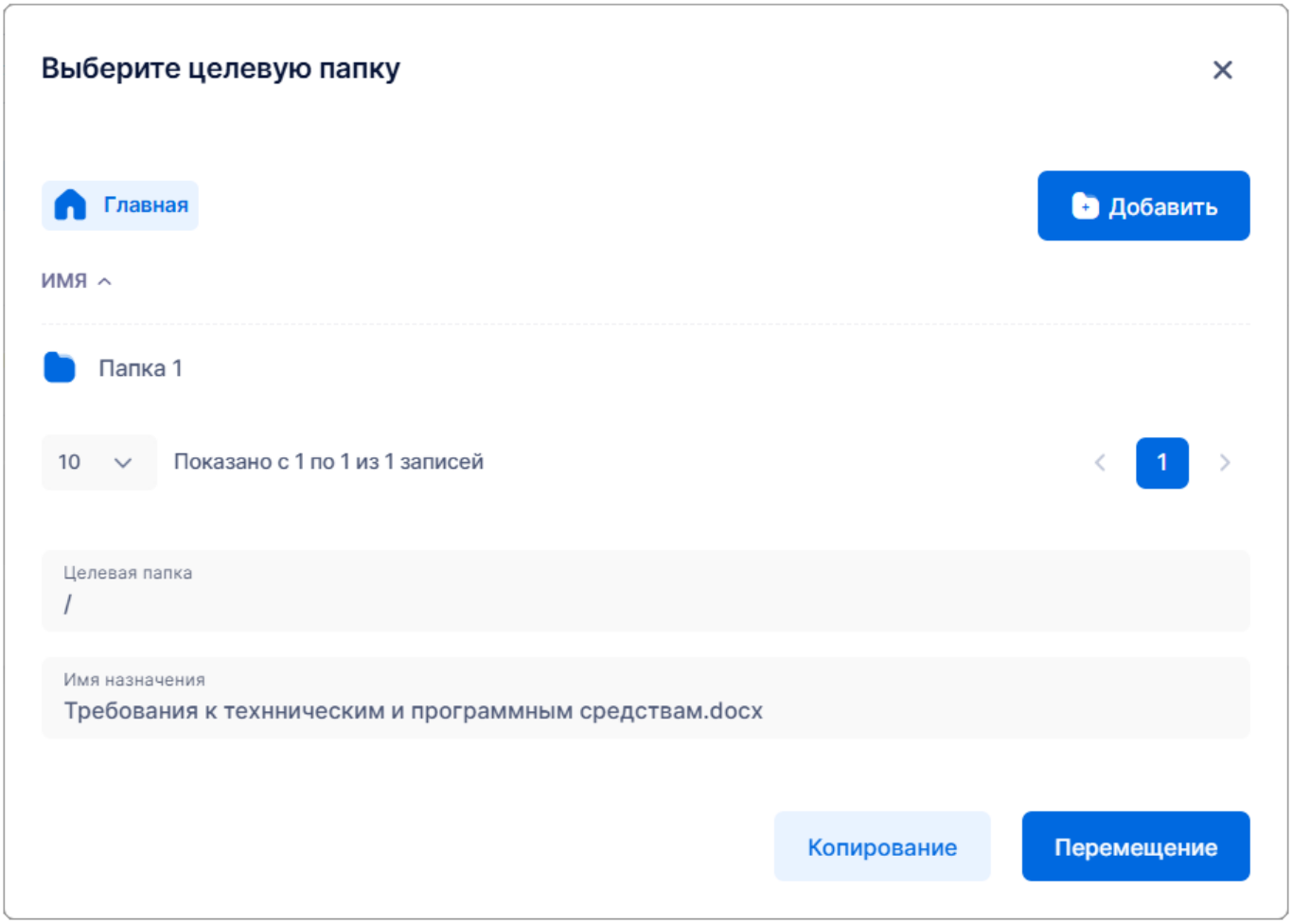


Рисунок 34 – Форма перемещения или копирования файлов/ папок

Данная форма идентична как для файлов, так и для папок.

Выберите целевую папку щелчком мыши по имени папки в списке (оно появится в поле «Целевая папка») или добавьте новую папку, нажав на кнопку Добавить.

Затем нажмите кнопку Копирование для того, чтобы файл (папка) был скопирован, или кнопку Перемещение для того, чтобы файл (папка) был перемещен в выбранную папку.

При вызове функции настройки доступа к файлу открывается форма, в которой необходимо задать параметры ссылки (рисунок 35).

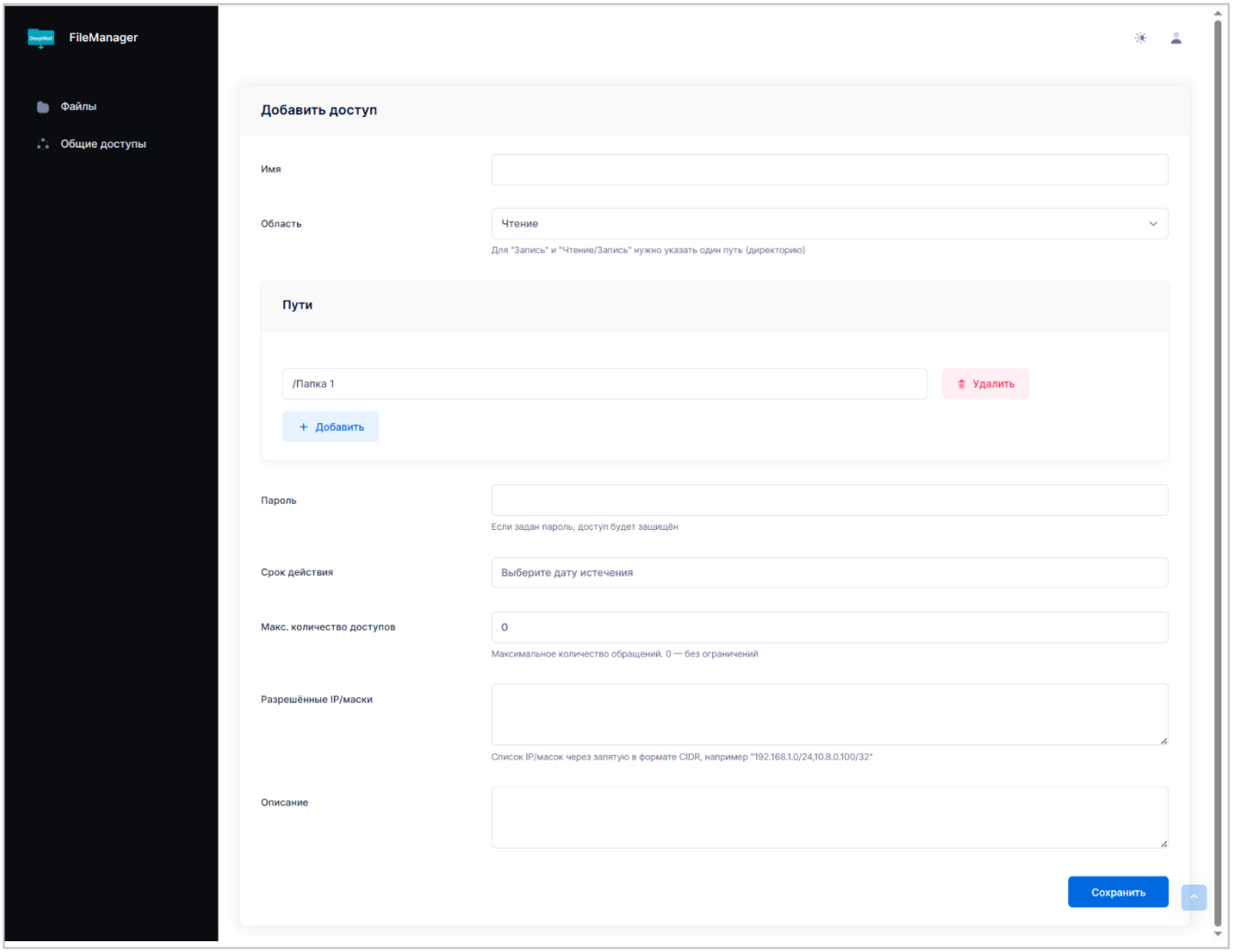


Рисунок 35 – Форма назначения параметров ссылки

В форме указываются:

- «Имя» – наименование ссылки, которое будет отображаться в разделе «Общие доступы»;

- «Область» – тип прав – «Чтение», «Запись» или «Чтение/Запись». Тип прав только «Запись» предназначен для предоставления прав добавления новых файлов в директорию, к которой предоставлен доступ, уже имеющееся содержимое директории будет не доступно для просмотра (чтения).

- «Пути» – путь (пути) к файлу, директории;

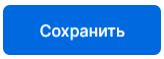
- «Пароль» – пароль, который необходимо будет ввести пользователю, чтобы воспользоваться правом доступа;

- «Срок действия» – ограничение срока действия ссылки (выберите дату окончания срока);

- «Макс. количество доступов» – ограничение максимального количества переходов по ссылке (0 – без ограничений);

- «Разрешенные IP/ Маски» – дополнительная защита ссылки доступа при помощи указания определенных IP-адресов или подсетей, которым можно подключаться по ней (указываются в формате CIDR);

- «Описание» – дополнительное поле для пояснения назначения ссылки.

Для сохранения настроек нажмите кнопку 

(см. рисунок 35).

3.2 Раздел «Система»

В разделе панели управления «Система» объединены следующие инструменты управления почтовым сервером:

- Лицензирование – статус, активация, список клиентских лицензий;

- Панель управления – карточки добавленных хостов с метриками, переход на страницу управления конкретным хостом (сервисы, перезагрузка, события);

- Репозиторий – загрузка и удаление образов сервисов (*.tar.gz) для обновления;

- Локации – геолокации, привязка доменов/ пользователей и настройка репликации DSA между локациями;

- Хранилища – NFS-таргеты для mail/ dav/ core/ archive, привязка к локациям;

- Профили – конфигурации IMAP/SMTP/WebDAV/SFTP-сервисов: можно создавать, редактировать, импортировать и экспортировать в JSON;

- Прочее – общесистемные настройки (уведомления о квоте, политика паролей).

Все эти инструменты относятся к функционалу инсталляции подкомпонентов почтового сервера (рисунок 36).

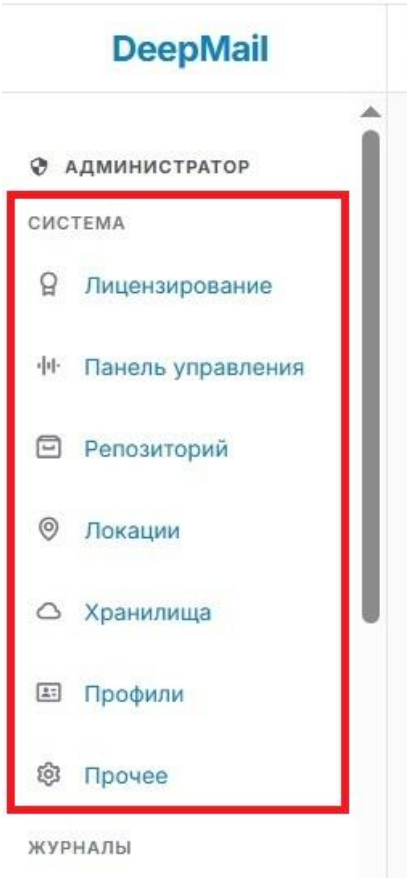


Рисунок 36 – Состав раздела «Система»

Для перехода на страницу настроек кликните мышью по соответствующей кнопке.

3.2.1 Лицензирование

На странице инструмента «Лицензирование» показаны данные серверной лицензии DeepMail – номер лицензии, номер лицензионного ключа, срок действия, количество активаций и статус.

И также тут отображена таблица пользователей системы с активными лицензиями (активированные в клиентских приложениях). Таблица содержит следующую информацию о клиентах с активной лицензией:

- «Электронная почта» – электронная почта пользователя;
- «Ключ» – номер лицензионного ключа клиента;
- «Создано» – дата получения лицензии клиентом;
- кнопка удаления – действие, разрешенное администратору применительно к данным клиента (рисунок 37).

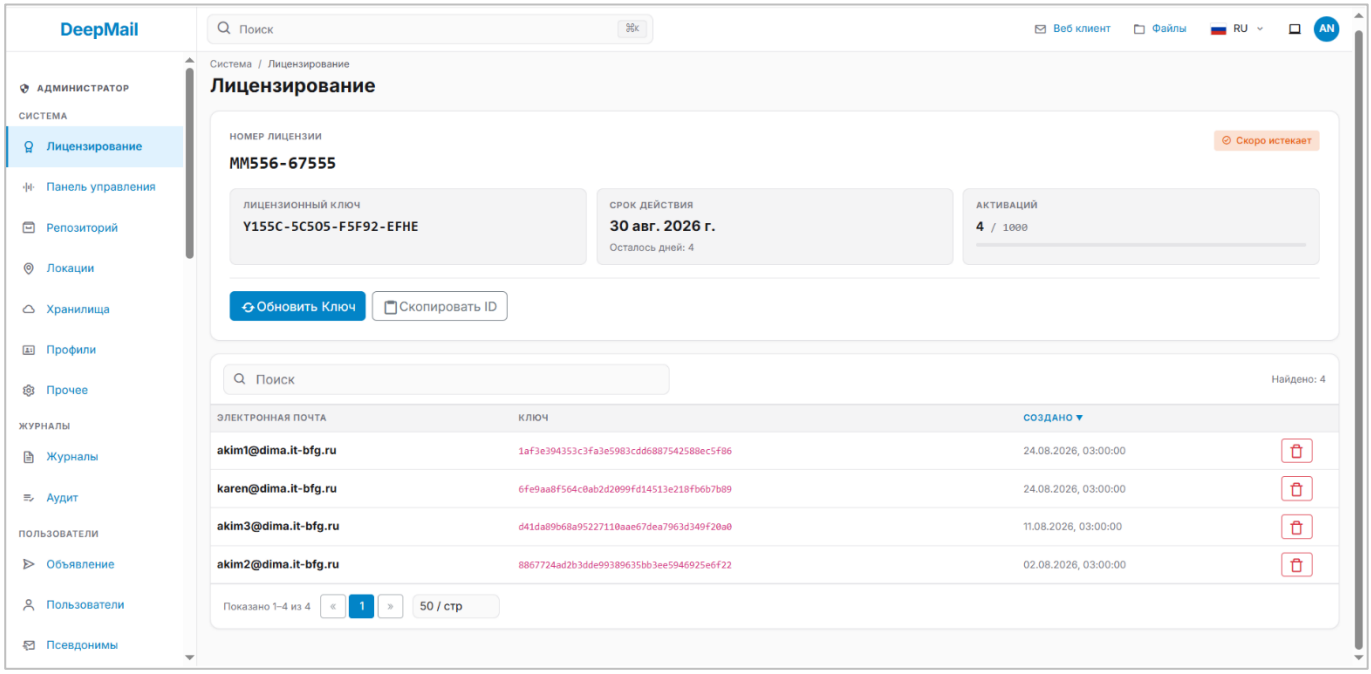


Рисунок 37 – Выбор инструмента «Система»

Функционал настроек лицензирования позволяет:

- обновить лицензионный ключ продукта – кнопка Обновить Ключ (после нажатия откроется форма активации лицензии (см. рисунок 16));
- скопировать номер лицензии – кнопка Скопировать ID (номер лицензии будет скопирован в буфер обмена, используется для запроса нового лицензионного ключа в СТП разработчика);
- удалить активированных клиентов – копка в строке определенного пользователя (после нажатия лицензия будет отозвана с клиента выбранного пользователя, при попытках входа пользователь будет видеть окно запроса лицензионного ключа).

3.2.2 Панель управления

Инструмент «Панель управления» предоставляет администратору возможность обзора уже добавленных хостов (удаленные сервера) и состояния их инфраструктуры, а также функционал добавления новых узлов и настройку их серверных параметров (рисунок 38).

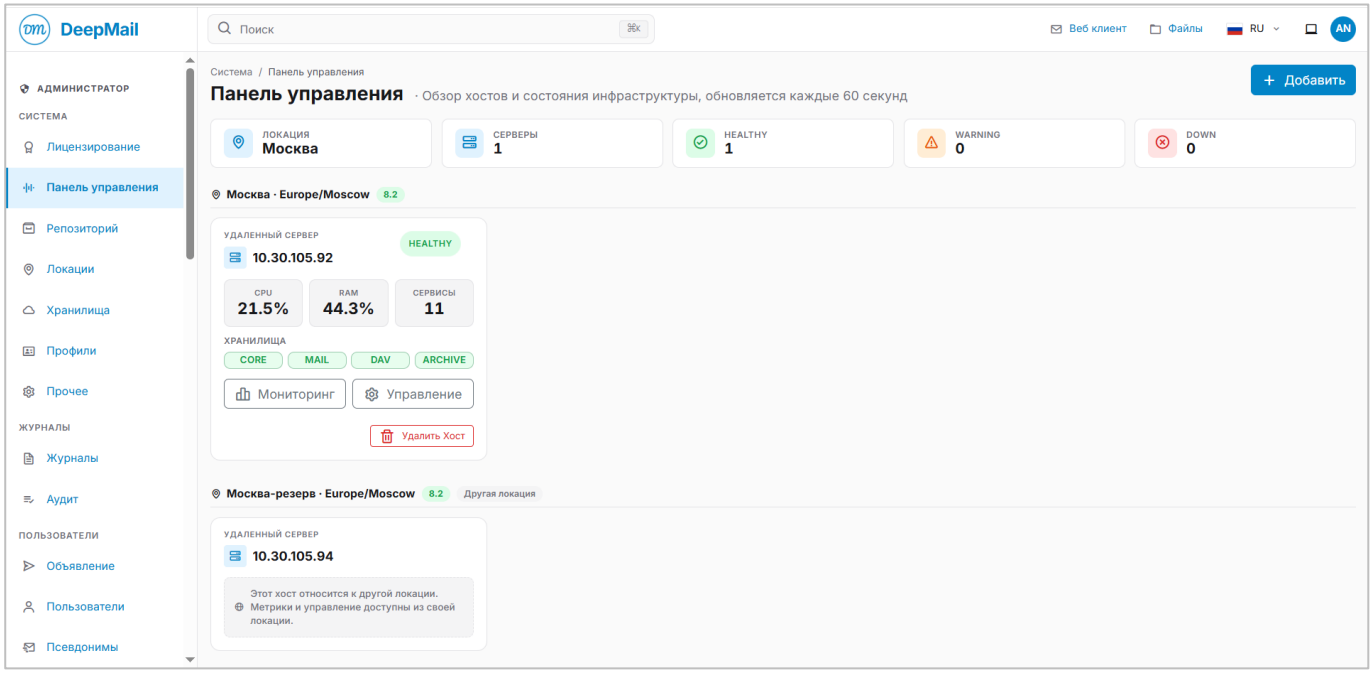


Рисунок 38 – Окно «Панель управления»

Все хосты сгруппированы по локациям: в верхней части страницы отображаются хосты «домашней» локации, в нижней части – резервные локации и их хосты.

Для каждой локации рядом с ее именем отображается метрика доступности (см. рисунок 38) в виде цветного значка с числовым значением, например 8.1. Метрики доступности локации могут быть:

- зеленый значок, числовое значение более 8.0 – доступен (Available);
- желтый значок, числовое значение от 8.0 до5.0 – ограниченно доступен (Limited);
- оранжевый значок, числовое значение от 5.0 до 2.0 – деградировал (Degraded);
- красный значок, числовое значение менее 2.0 или отсутствует – недоступен (Unavailable).

Интерфейс панели управления обеспечивает визуальный обзор ландшафта хостов «домашней» локации (той, в которой запущена админ-панель), позволяя контролировать ключевые метрики производительности каждого узла DeepMail, такие как загрузка процессора и использование оперативной памяти. На экране отображается сводка по добавленным в систему узлам с индикацией общего состояния для каждого, 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.

Также на странице инструмента «Панель управления» отображаются резервные хосты, принадлежащие другим локациям (при наличии других географических узлов), но их метрики и управление не доступны.

3.2.2.1 Карточка хоста

Каждый удаленный сервер отображен в интерфейсе панели управления отдельной карточкой хоста, которая представляет собой компактную информационную панель состояния (рисунок 39).

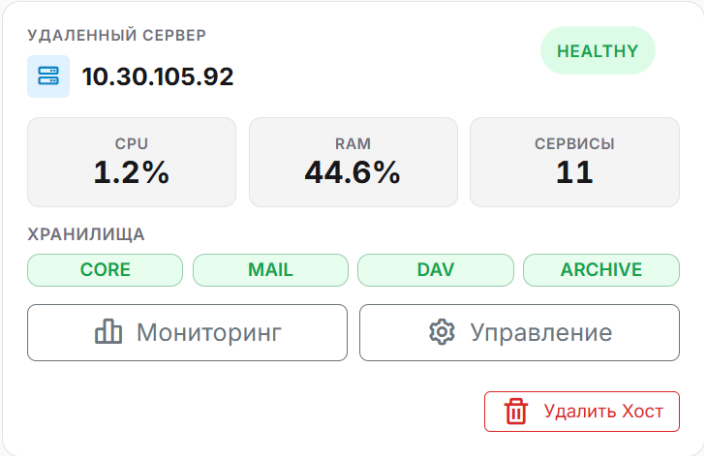


Рисунок 39 – Карточка хоста на странице панели управления

В центре внимания – ключевые показатели работоспособности и нагрузки узла DeepMail:

- имя хоста – IP-адрес (FQDN из БД);
- статус состояния – «HEALTHY» (зеленый) – исправен, сервер работает штатно, все проверки пройдены; «UNHEALTHY» и «WARNING» (оранжевый) – неработоспособен или ошибка, критическая ошибка сервиса, основная функция недоступна, хотя сам сервер может быть включен и отвечать на сетевые запросы или зафиксированы отклонения от нормы: высокая загрузка ЦП, мало свободного места на диске или задержки в ответах; «DOWN» (красный)– не отвечает или отключен, хост полностью недоступен по сети (пропал *ping*, закрыт доступ к портам), мониторинг не получает от него никаких сигналов; «PENDING» (серый)– ожидание или инициализация, состояние еще не определено, объект только что добавлен в систему мониторинга, и первая проверка либо выполняется прямо сейчас, либо стоит в очереди, либо это хост другой локации;
- текущая загрузка процессора и оперативной памяти (CPU/ RAM), а также количество активных сервисов;

– подключенные к ноде хранилища данных (CORE, MAIL, DAV, ARCHIVE) с индикаторами статуса – «healthy» (зеленый), «unhealthy» (оранжевый), «down» (красный), «no data» (серый).

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

3.2.2.2 Мониторинг удаленного сервера

При нажатии на кнопку 

откроется страница с метриками по мониторингу удаленного сервера. Данная страница представляет собой панель комплексного мониторинга инфраструктуры, сфокусированную на отслеживании производительности конкретного удаленного сервера для проверки состояния сетевых компонентов и использования ключевых ресурсов системы (рисунок 40).

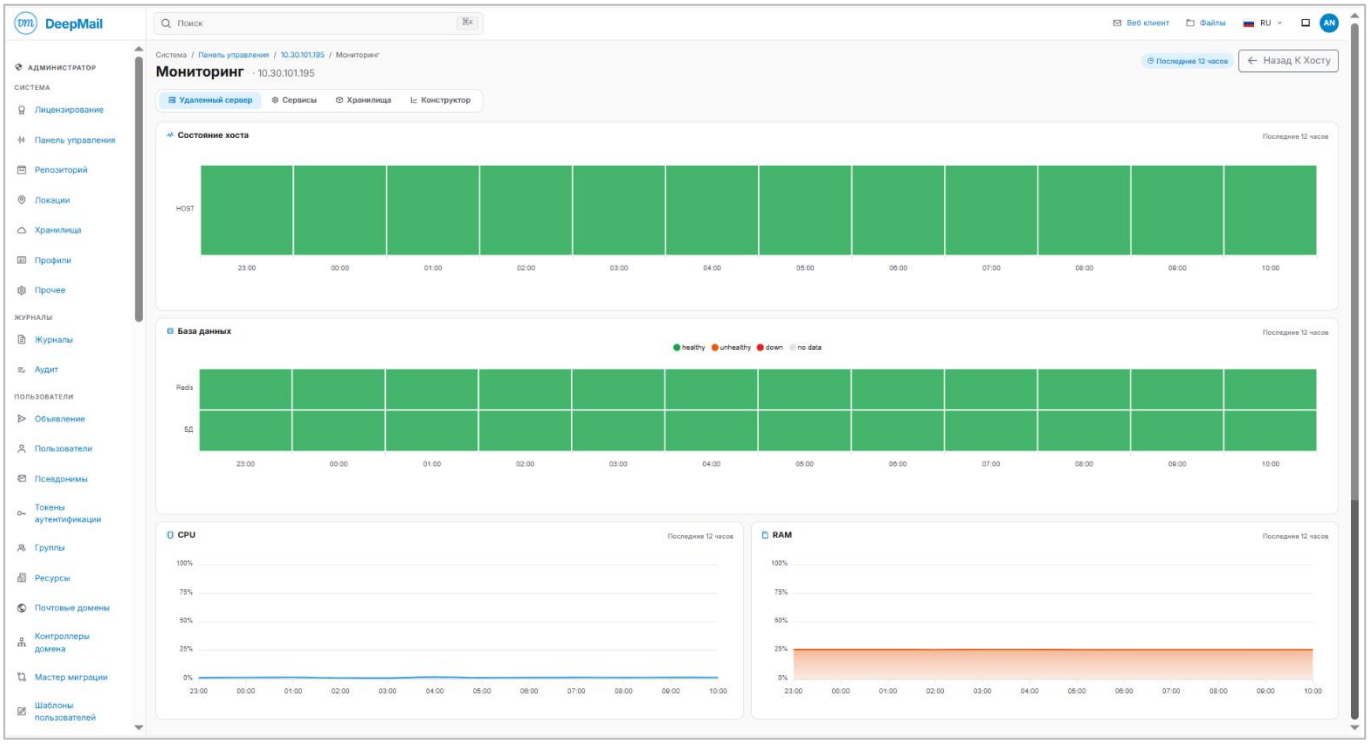


Рисунок 40 – Страница «Мониторинг»/ вкладка «Удаленный сервер»

Интерфейс разделен на логические блоки, обеспечивающие многоуровневый анализ состояния системы. Переключаясь на разные вкладки, можно отслеживать сводную информацию о хосте – вкладка «Удаленный сервер»; о сервисах сервера – вкладка «Сервисы»; а таже о состоянии хранилищ – вкладка «Хранилища». Это позволяет мгновенно оценить общую работоспособность узла.

Также для расширенного анализа доступен конструктор графиков – вкладка «Конструктор», где доступно построение и просмотр отельных графиков выбранных показателей за определенный период времени (дни).

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

Интерфейс мониторинга общего состояния удаленного сервера – вкладка «Удаленный сервер», помогает выявлять тренды и аномалии в работе хоста и в потреблении ресурсов. В верхней части вкладки (см. рисунок 40) представлена информация о состоянии хоста. В центральной части отображается состояние БД NFS и Redis. Затем внизу страницы размещены динамические графики загрузки ключевых ресурсов – процессора (CPU) и оперативной памяти (RAM). Графики CPU и RAM отображают изменения метрик за выбранный период (по умолчанию «последние 12 часов»). Все данные представлены в процентах использования, а временные метки стандартизированы в формате UTC для единообразия.

Интерфейс мониторинга сервисов – вкладка «Сервисы», представляет собой панель мониторинга состояния сервисов удаленного сервера, объединяющую информацию о работоспособности отдельных служб и потреблении ими системных ресурсов (рисунок 41).

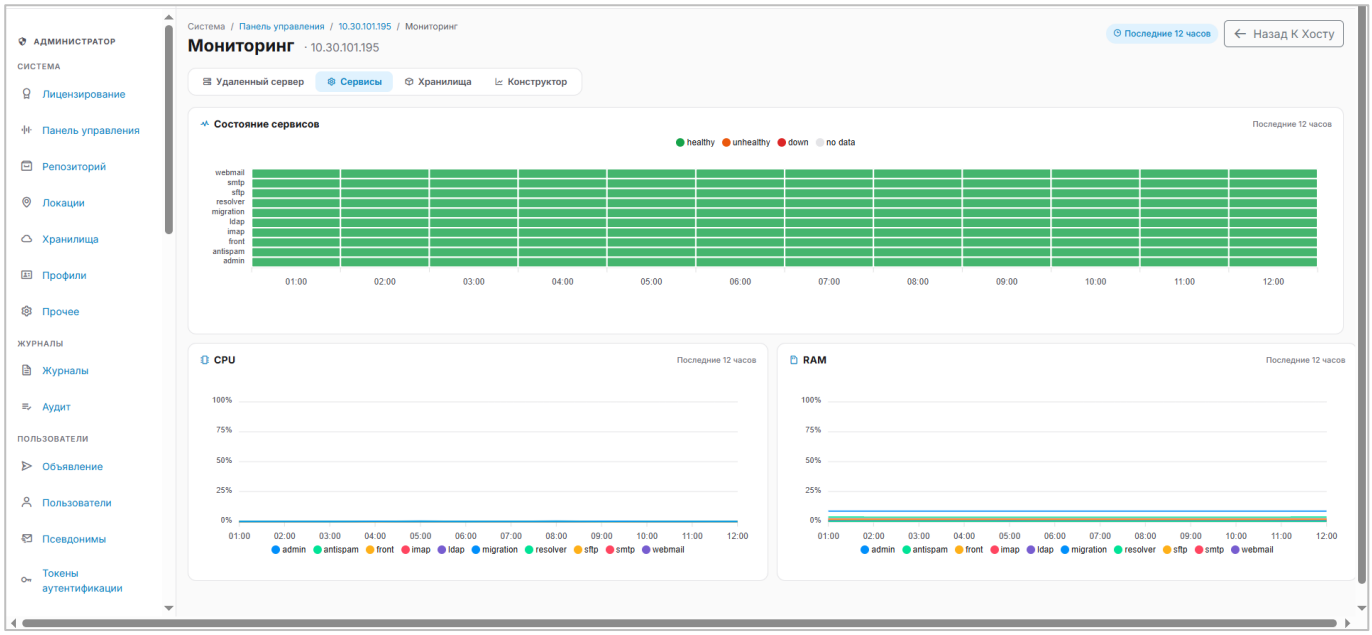


Рисунок 41 – Страница «Мониторинг»/ вкладка «Сервисы»

В верхней части страницы (см. рисунок 41) для каждого сервиса представлена цветовая временная шкала, визуализирующая историю его работоспособности за последние

12 часов. Цветовая индикация позволяет мгновенно оценить промежутки простоев и проблем в работе сервисов.

Нижняя часть страницы (см. рисунок 41) разделена на две синхронизированные по времени области. В левой части отображаются графики загрузки центрального процессора (CPU), в правой части – оперативной памяти (RAM), каждая кривая сервиса имеет свою цветовую индикацию. Графики в динамике показывают потребление ресурсов при работе сервисов за тот же 12-часовой период. Это позволяет моментально соотнести всплески или падения потребления ресурсов (внизу страницы) с изменениями статусов конкретных служб (вверху страницы).

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.

Интерфейс мониторинга хранилищ (рисунок 42) представляет собой панель мониторинга, обеспечивающую комплексный контроль над состоянием, производительностью и использованием дискового пространства на сервере.

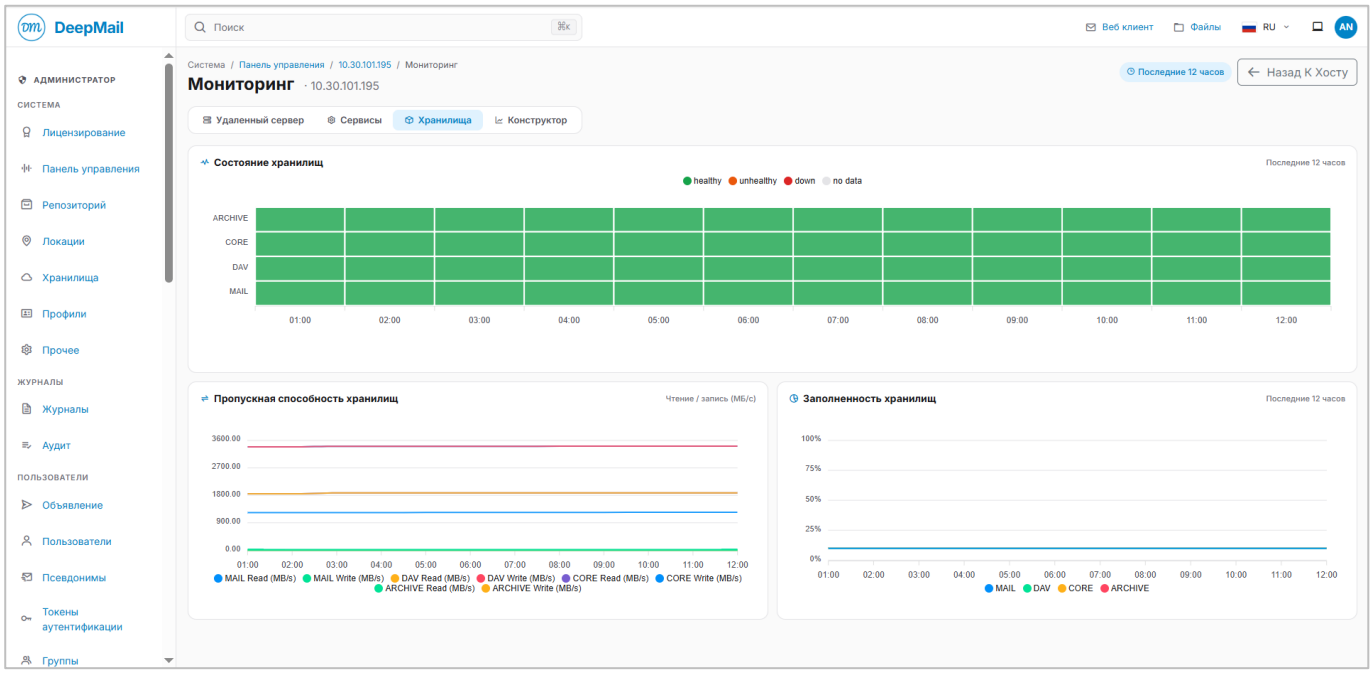


Рисунок 42 – Окно «Мониторинг»/ вкладка «Хранилища»

Экран визуально разделен на три ключевые секции (см. рисунок 42), 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, зеленый – «Healthy», красный – «Down»)

отображает историю их работоспособности. Это позволяет мгновенно определить периоды возникновения проблем с доступностью дисковых массивов.

В нижней части страницы левый блок посвящен мониторингу пропускной способности (см. рисунок 42). На детализированном графике показана динамика операций чтения и записи (в МБ/с) для каждого типа хранилища (например, ARCHIVE, MAIL). Это дает четкое понимание нагрузки на подсистему ввода-вывода и помогает выявлять аномальную активность.

Правый блок отображает заполненность хранилищ в процентах (см. рисунок 42). График демонстрирует, как изменялся объем занятого пространства на каждом из основных томов (CORE, MAIL, ARCHIVE) с течением времени, что критически важно для планирования ресурсов и предотвращения исчерпания дискового пространства.

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

Для построения пользовательского графика и детализированного просмотра отдельных параметров системы перейдите на вкладку «Конструктор» (рисунок 43).

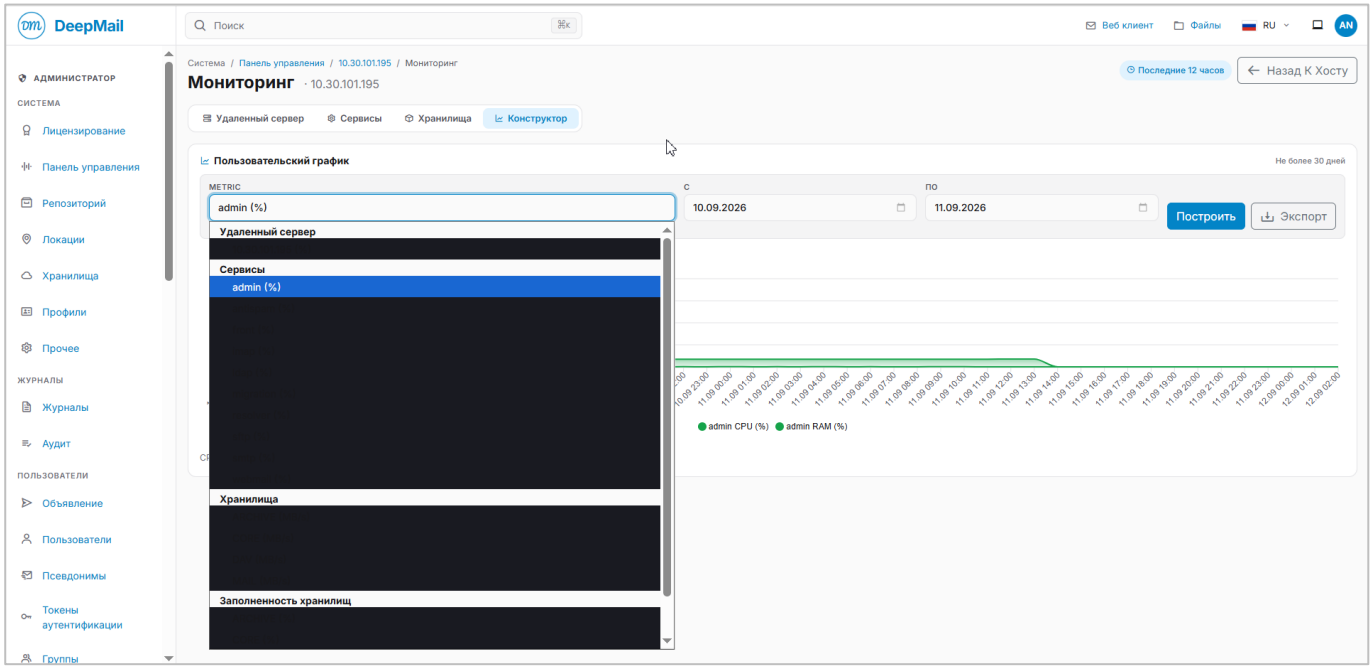


Рисунок 43 – Окно «Мониторинг»/ вкладка «Конструктор»

Выберите в поле «METRIC» из выпадающего списка значение параметра, для которого необходимо построить график, и установите даты начала и окончания временной шкалы графика. Затем нажмите на кнопку Построить, после этого на экране отобразится выстроенный по запросу график.

Для возврата на главную страницу выберите в заголовках страницы пункт «Панель управления», выделенный синим шрифтом (см. рисунок 43).

3.2.2.3 Управление удаленным сервером

Для управления удаленным сервером необходимо на странице «Панель управления» в карточке конкретного хоста нажать кнопку Управление (см. рисунок 39).

Управление удаленным сервером представляет собой централизованный интерфейс управления и мониторинга конкретного хоста DeepMail, объединяющий ключевые показатели его работоспособности и производительности, отображаемые в режиме реального времени (рисунок 44).

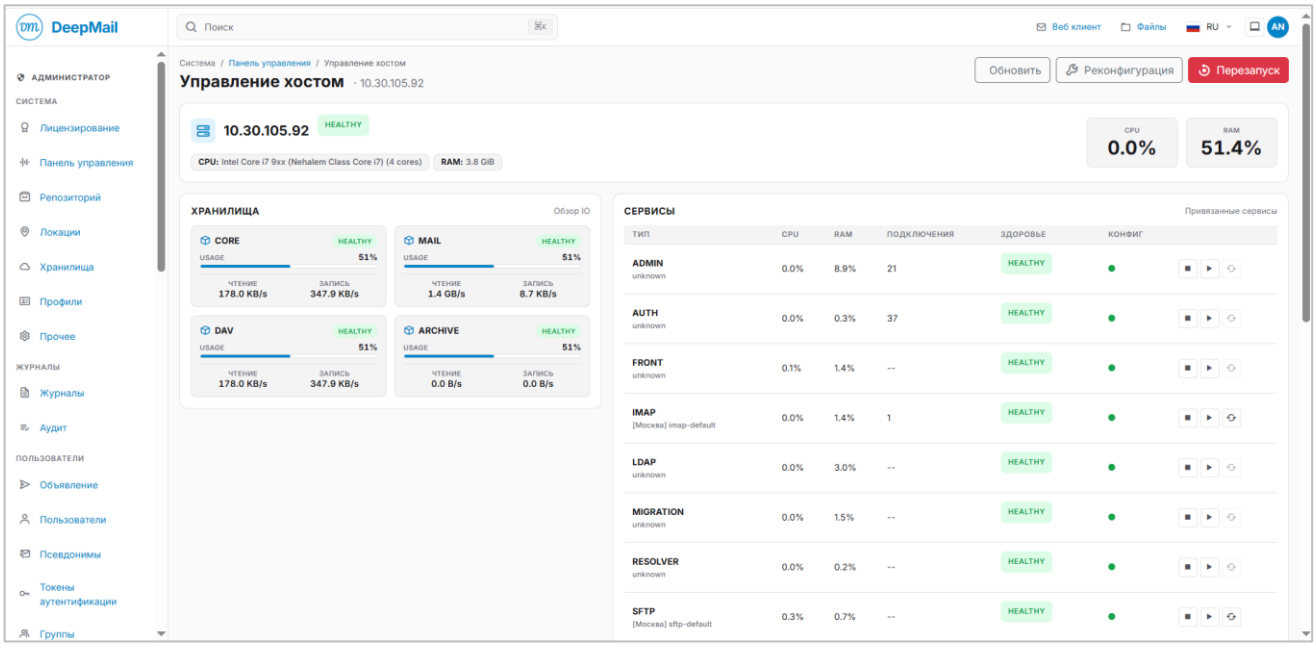


Рисунок 44 – Окно управления удаленным сервером

Вверху справа размещены кнопки Обновить (при нажатии выполняется переход на страницу обновления образов стеков и сервисов – «Планировщик обновлений»), Реконфигурация (при нажатии выполняется переход на страницу изменения параметров хоста), Перезапуск (при нажатии запускается полная перезагрузка узла, все отображаемые на экране метрики пропадают).

Также в верхней части отображается идентификатор хоста, общий статус (например «HEALTHY») общие значения загрузки процессора и памяти, а также физическая информация о процессоре и памяти – модель CPU и объем RAM.

Следом идет блок контроля хранилищ, где для каждого тома (CORE, MAIL, DAV, ARCHIVE) указано состояние и статус использования. 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, AUTH, SMTP, IMAP и т.д.) приведены точные значения потребления ресурсов CPU и оперативной памяти в процентах, количество активных сетевых подключений и индикатор «здоровья». Например, при централизованном изменении параметров профиля, примененного к сервисам SMTP, IMAP, WebDAV и SFTP индикатор в строке сервиса становится красным, это означает, что необходимо выполнить реконфигурацию хоста.

Все это дает администратору полную картину распределения ресурсов между компонентами системы и помогает быстро выявить проблемные службы.

В строке каждого сервиса доступны действия для остановки сервиса – кнопка  «Стоп»; для запуска – кнопка  «Старт»; и для сервисов с настраиваемыми профилями: IMAP, SMTP, WebDAV, SFTP доступна кнопка  «Сменить профиль», при нажатии на которую появится диалоговое окно для смены профиля (рисунок 45).

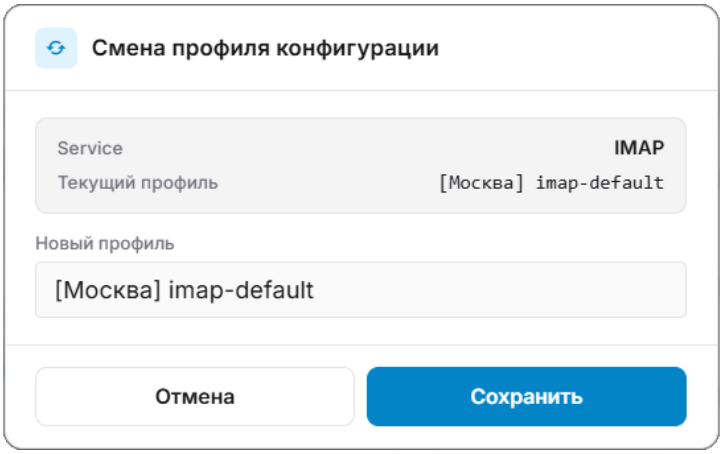
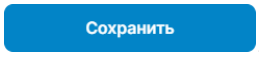


Рисунок 45 – Диалоговое окно смены профиля

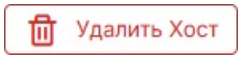
Щелчком мыши в поле «Новый профиль» вызывается выпадающий список, в котором можно выбрать другой профиль соответствующего типа. Для сохранения необходимо нажать кнопку 

.

Таким образом, функционал страницы «Управление хостом» обеспечивает комплексный оперативный обзор, сочетая сводные данные о здоровье узла с детальной

аналитикой по каждому сервису, что является основой для эффективного управления инфраструктурой.

Для возврата на главную страницу выберите в заголовках страницы пункт «Панель управления», выделенный синим шрифтом (см. рисунок 44).

Кнопка 

(см. рисунок 39) предназначена для удаления узла – удаляется запись о хосте из БД, но сам узел сети при этом не выключается – происходит так называемое удаление учетной записи в админ-панели. Реальное удаление выполняется через Ansible-плейбук или вручную на носителе хоста (ВМ, физический сервер).

3.2.2.4 Добавление хоста

Если вы разворачиваете систему на трех ВМ, после завершения первоначальной установки стеков на DM2node (см. 2.8), необходимо добавить еще один хост – вторую почтовую ноду (DM3node).

Важно! Перед добавлением ноды необходимо на ВМ нового хоста:

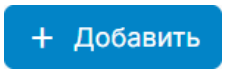
1) добавить базовые пакеты (*docker, rsyslog, nfs-common/nfs-utils*), запустить docker, NFS-точки должны быть досягаемы с хоста, IP-адрес добавлен в */etc/exports* нужных NFS-серверов (или соответствующие группы в файле инвентаризации (*inventory.yml*) должны быть обновлены и *storage.yaml/ install.yml* прогоняется еще раз);

2) установить пакет deepmail-server (*.deb/.rpm*);

3) запустить systemd-сервис deepmail – *systemctl enable --now deepmail*;

4) подгрузить docker-образы для выбранных стеков. Обязательные для Core: *admin-service*, *front-service*, *resolver-service*, *redis*. Опциональные внутри стека Core: *migration-service*, *ldap-service*, *webmail-service*, *imap-service*, *smtp-service*, *antispam-service* (если *antispam_enabled*), *clamav-service* (если *antivirus_enabled*). Для отдельных стеков – *auth-service*, *webdav-service*, *sftp-service*. Утилита *install.yml* грузит их шагами либо вручную командой – *docker load -i <image>.tar.gz*;

5) назначить локацию – у текущего хоста должна быть валидная локация (admin-service ее определяет по system_info). Если не назначена, то в окне мастера добавления почтовой ноды будет выведено сообщение о том, что локация не определена и кнопка проверки будет не доступна.

После подготовки ВМ в админ-панели на странице «Панель управления» нажмите кнопку 

(см. рисунок 38).

Откроется страница добавления конфигурации нового узла DeepMail – так называемый мастер добавления почтовой ноды. Окно мастера представляет собой интерфейс начальной настройки нового узла DeepMail в панели управления (рисунок 46).

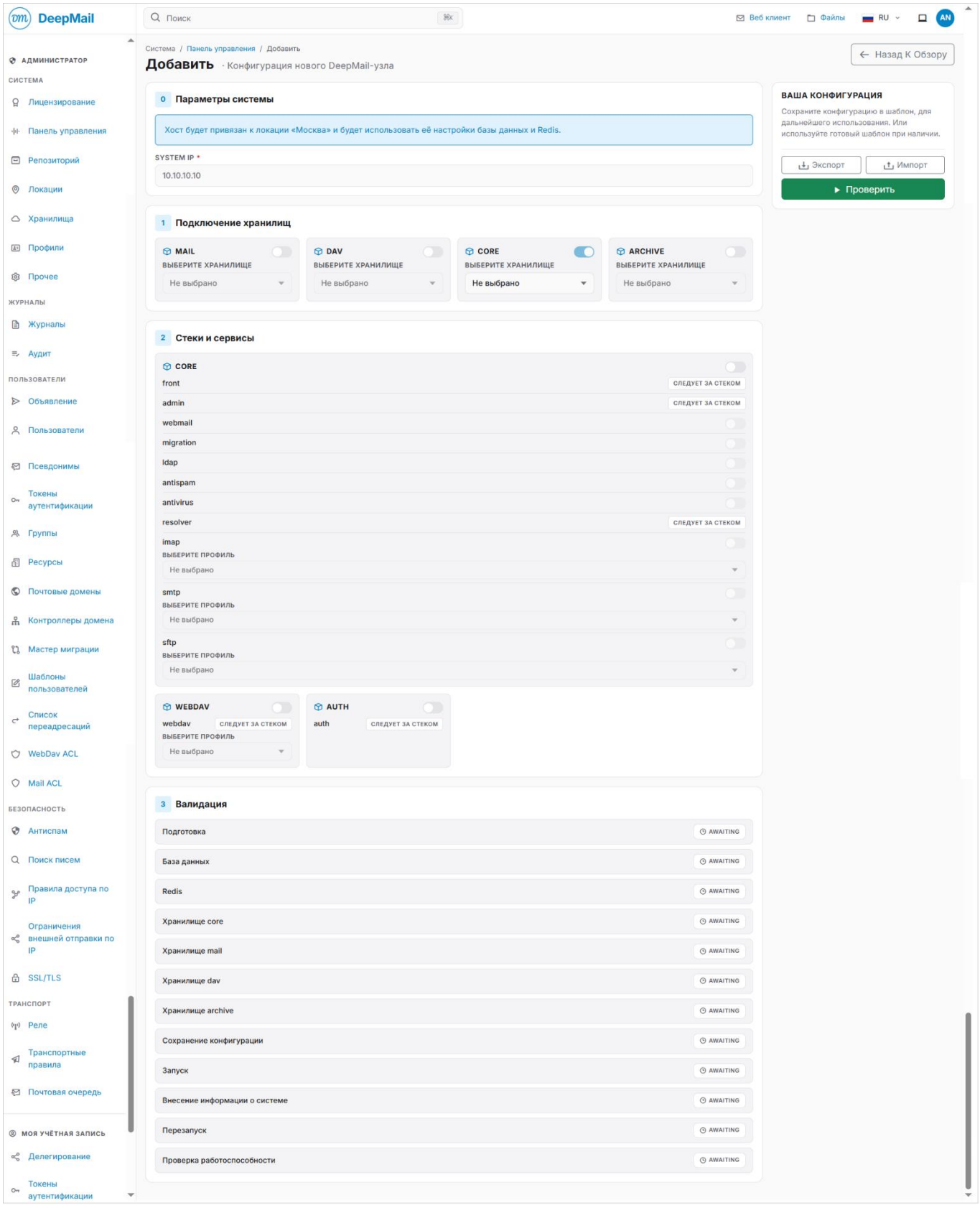


Рисунок 46 – Страница добавления конфигурации нового узла DeepMail

При добавлении нового хоста мастер использует текущую конфигурацию инсталляции как шаблон. Он автоматически считывает данные о подключении к БД, Redis и сети из текущей локации и применяет их к новому серверу. Новый хост автоматически привязывается к локации, в которой запущена админ-панель.

Важно! Переназначить локацию для хоста нельзя. Это выполняется только удалением хоста в админ-панели текущей локации и затем добавлением в админ-панели резервной локации.

В верхней части окна расположен блок параметров системы для указания IP-адреса узла. Справа 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 введенных параметров.

Основную часть интерфейса занимают разделы для подключения хранилищ, стеков и сервисов и для валидации.

Конфигуратор позволяет задать основные параметры для развертывания нового хоста – удаленного сервера. Заполните следующие параметры:

- в параметрах системы укажите System IP – адрес управляющего сервера DM1ha;
- включите чекбокс соответствующего хранилища для подключения хранилищ CORE (системные файлы), MAIL (почта), DAV (данные CalDAV/CardDAV), ARCHIVE (архив). CORE включен всегда по умолчанию, без него не будет выполнен старт *admin-service*. Выберите для каждого типа хранилища из выпадающего списка IP-адрес DM1ha;
- активируйте стеки и сервисы – как минимум *CORE*. Сервисы *front*, *admin* и *resolver* всегда включены если активирован стек *CORE* (в интерфейсе имеют метку «СЛЕДУЕТ ЗА СТЕКОМ»). Остальные сервисы включаются по необходимости. Здесь администратор может назначить конкретные профили конфигурации (наборы настроек – лимиты, политики, разрешения) для таких критически важных компонентов, как *imap, smtp*, *sftp* и *webdav*, выбрав имя нужного профиля в выпадающем списке «ВЫБЕРИТЕ ПРОФИЛЬ». При этом профили должны быть заранее добавлены в инструменте «Профили». Если профилей нужного типа нет заведите профиль, потом возвращайтесь (добавление профилей см. в 3.2.6).

Далее нажмите кнопку 

. Начнется процесс валидации, который 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 (ожидание), RUNNING (выполняется), SUCCESS (завершено успешно), что позволяет администратору в реальном времени наблюдать за ходом развертывания и валидации нового узла перед вводом его в эксплуатацию.

Дождитесь успешной валидации и нажмите ← Назад К Обзору (см. рисунок 46). Теперь в списке узлов будут отображаться две почтовые ноды: DM2node и DM3node. HAProxy автоматически начнет распределять нагрузку между ними, а если одна из нод перестанет отвечать – трафик будет перенаправлен на «живую» ноду.

3.2.3 Репозиторий

Серверная часть DeepMail обновляется не как монолит, а по-сервисно: каждый контейнер (*admin-service*, *front-service*, *imap-service* и т. д.) распространяется отдельным архивом образа – в виде *.tar.gz-архивов.

Инструмент админ-панели «Репозиторий» предоставляет интерфейс для управления централизованным хранилищем образов стеков и сервисов системы DeepMail (рисунок 47).

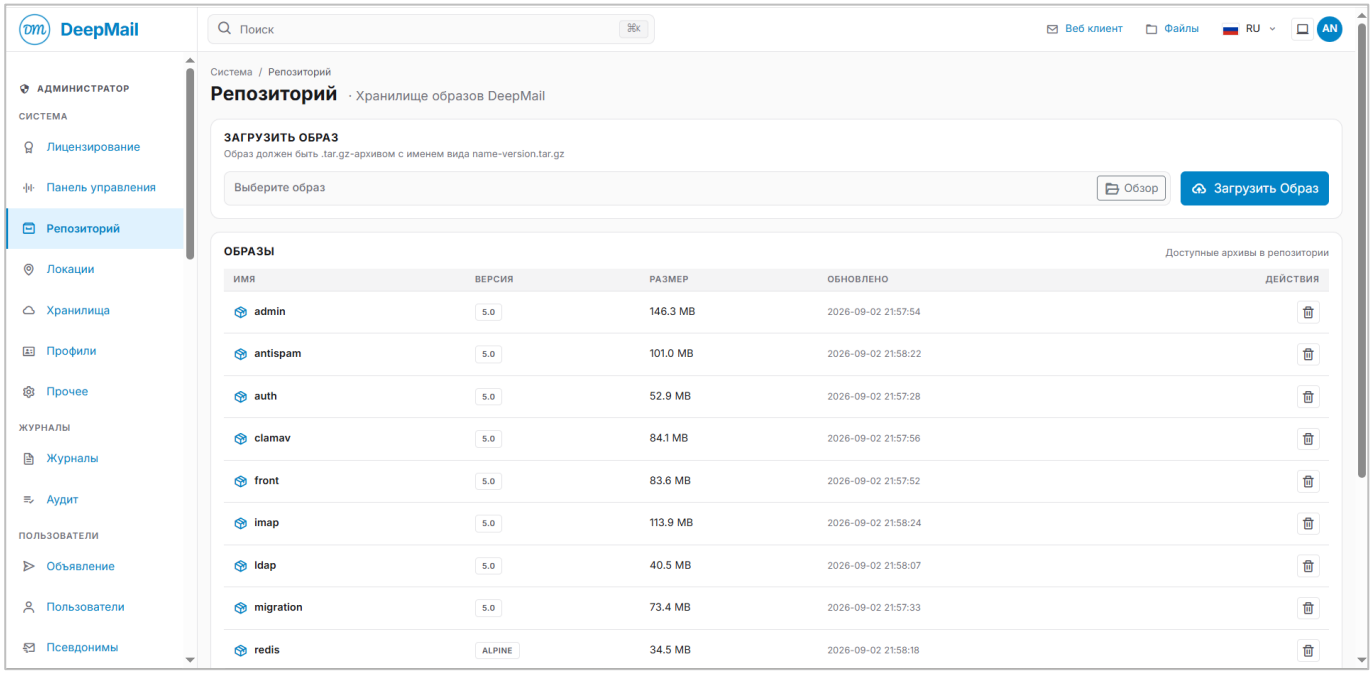
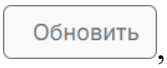


Рисунок 47 – Окно управления репозиториями

Физически архивы сервисов хранятся в специальной директории контейнера *admin-service*, а в админ-панели отображаются уже загруженные дистрибутивы всех сервисных компонентов (*admin*, *antispam*, *auth* и т.д.) и выполняется загрузка новых. Такой подход позволяет:

- загрузить новые *.tar.gz-архивы образов сервисов один раз в центральное место и потом устанавливать их на любой хост из админ-панели;
- видеть, какие версии архивов лежат в центральном хранилище;
- удалять устаревшие архивы, чтобы освободить место.

Само применение архива к хосту выполняется со страницы управления хостом (кнопка 

, см. 3.2.2.3).

Интерфейс репозитория разделен на две ключевые функциональные зоны.

В верхней части расположена область для загрузки новых образов в репозиторий. Администратор может выбрать готовый архив образа через поле «Выберите образ» (щелчок мыши в поле или по кнопке 

), выбрав его напрямую с локального диска ПК. Для подтверждения загрузки образа в репозиторий нажмите кнопку 

.

Важно! Архив обязательно должен иметь имя в формате *<имя>-<версия>.tar.gz*

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 Локации

Локация создается при помощи Deepmail Configurator (см. 2.8) и одновременно с этим в системе регистрируется хост, привязанный к ней. Смена привязки хоста к локации потом возможна только в процессе пересоздания (удалить хост, добавить заново) – в админ-панели этого сделать нельзя.

Инструмент «Локации» – это страница админ-панели для управления гео-распределенными узлами инсталляции – редактирование параметров локаций и их подключения к БД, привязка доменов и пользователей к локациям, назначение резервных локаций и настройка репликации между ними данных почты, календарей и контактов через DSA.

В интерфейсе администратора на странице «Локации» отображаются карточки локаций, добавленных в систему (рисунок 48).

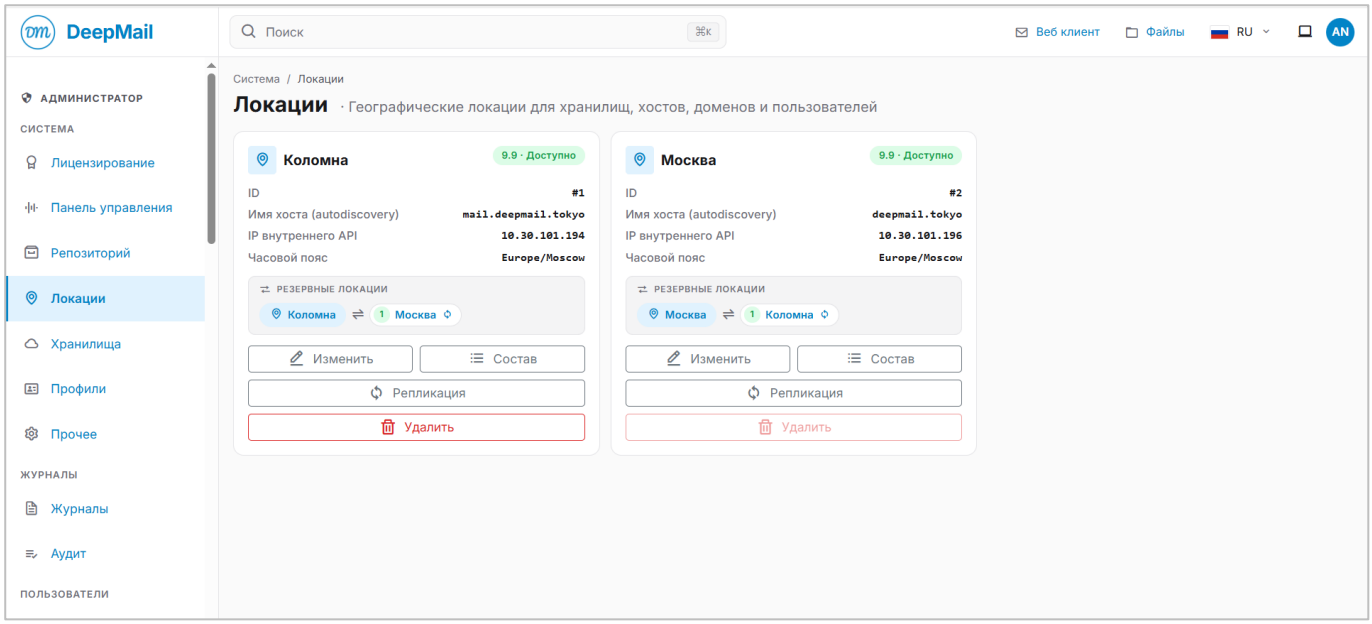


Рисунок 48 – Страница инструмента «Локации»

В каждой карточке локации отображаются следующие данные:

- имя локации;
- индикатор доступности – цветная плашка по GEO-Score: зеленая – «available» (≥ 8.0), желтая – «limited» (7.9≥ 5.0), оранжевая – «degraded» (4.9≥ 2.0), красная – «unavailable» (ниже 2.0);
- ID локации – персональный идентификатор;
- имя хоста – DNS-имя локации (используется только для autodiscovery клиентов);
- IP внутреннего API – IP-адрес, который используется для внутреннего API между сервисами (гео-доступность, следующий узел SMTP (next-hop));
- часовой пояс;
- резервные локации.

Далее в карточке размещены кнопки управления (см. рисунок 48):

- 

– редактирование параметров;

– Состав – просмотр и управление списками доменов и пользователей;

– Репликация – настройки DSA;

– Удалить – удаление локации.

3.2.4.1 Редактирование локации

Для редактирования параметров локации необходимо нажать в карточке локации на кнопку Изменить (см. рисунок 48). После этого откроется страница «Изменить локацию» (рисунок 49).

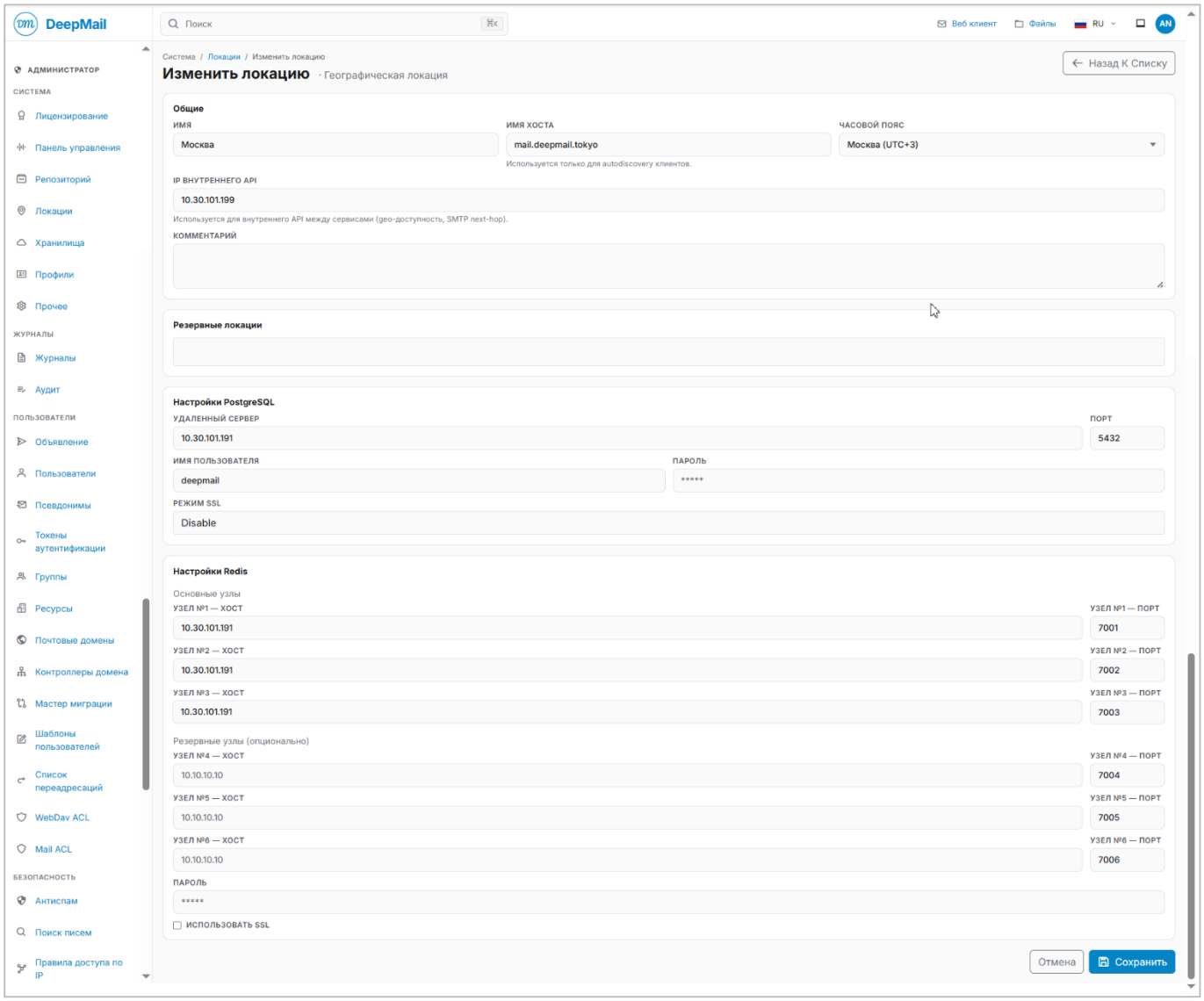


Рисунок 49 – Страница «Изменить локацию»

На данной странице отображены параметры локации, которые администратор при необходимости может отредактировать, изменив указанные значения в соответствующих полях.

Важнейшая функция, которая доступна администратору на этой странице – это назначение резервной локации. Для этого необходимо щелчком мыши в поле «Резервные локации» вызвать выпадающее меню и выбрать желаемый вариант из списка доступных локаций (рисунок 50).

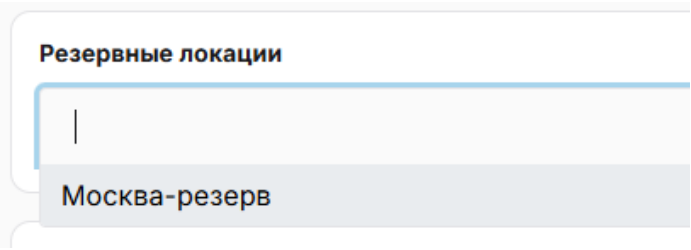


Рисунок 50 – Выбор резервной локации

Для сохранений изменений нажмите кнопку Сохранить, для отмены и выхода со страницы нажмите Отмена (см. рисунок 49).

3.2.4.2 Состав локации

При нажатии в карточке локации на кнопку Состав (см. рисунок 48) откроется инструмент администратора для привязки доменов и пользователей к локации (рисунок 51).

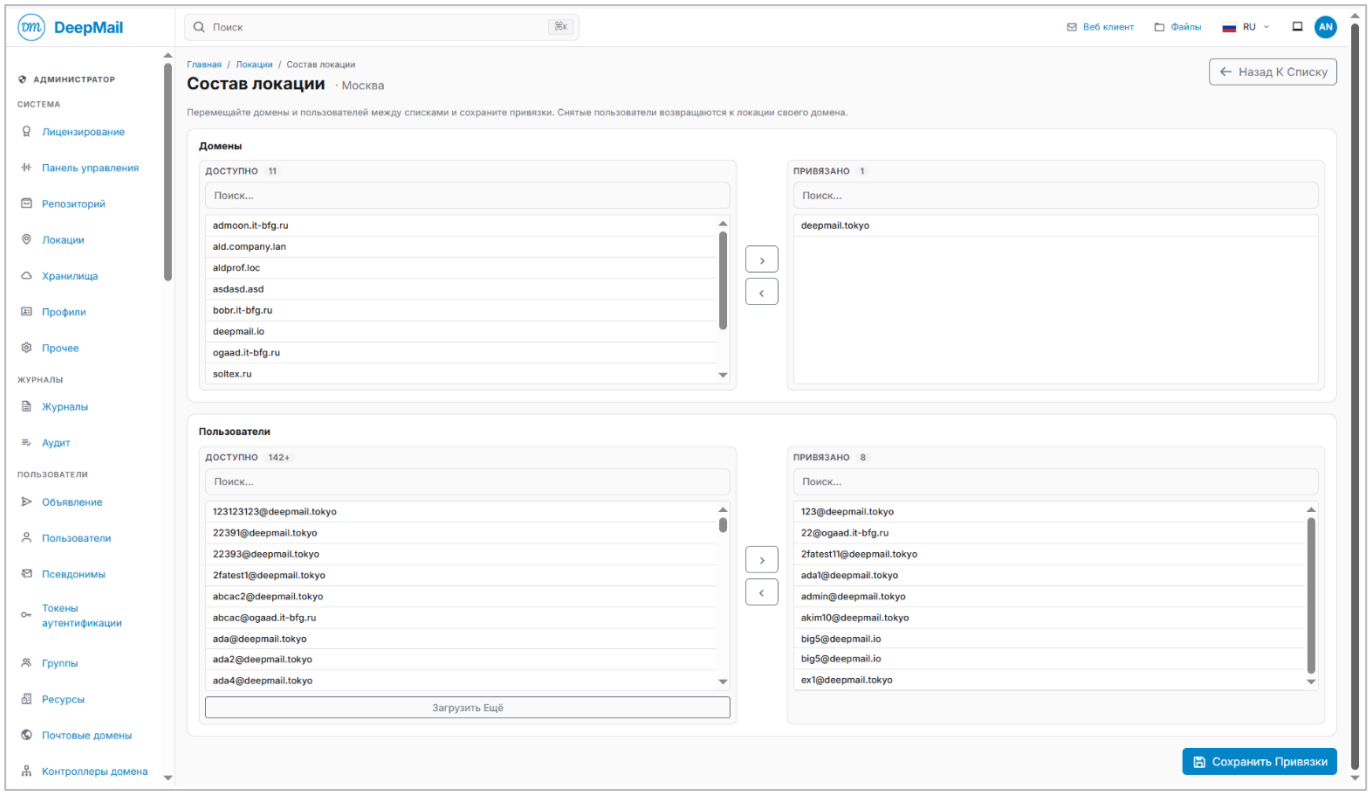


Рисунок 51 – Страница «Состав локации»

На странице отображены два блока «Домены» и «Пользователи» со списками – в правой части списки доменов и пользователей доступных к привязке, в левой части списки доменов и пользователей, привязанных к этой локации. Изначально в списках отображается максимум по 25 элементов, для отображения большего количества элементов (при наличии) необходимо нажать кнопку 

, размещенную внизу списка (см. рисунок 51).

Также для администратора доступен поиск – в строку поиска необходимо ввести минимум 3 символа.

Перемещение между списками выполняется выделением в списке нужных данных и затем нажатием на стрелки перемещения  или  (см. рисунок 51).

Отвязка пользователей и доменов от локации выполняется по следующей внутренней логике:

- пользователь при отвязке получает для своей УЗ значение параметра «location_id» = -1, это означает, что локацию он будет «наследовать от домена».
- домен при отвязке получает в параметре «location_id» значение = NULL, это означает что он становится «глобальным доменом» и может быть в любой локации.

Таким образом администратор может при необходимости перенести часть пользователей с одной локации на другую – передвинуть нужных пользователей из одного списка в другой, их «location_id» обновится. При их следующей авторизации в почтовый ящик *admin-service* использует БД новой локации.

3.2.4.3 Настройка репликации

При помощи репликации выполняется настройка передачи данных *mail* и *DAV* между локациями через DSA. Используется этот инструмент для того, чтобы при гео-распределении одни и те же письма, события и контакты пользователей были доступны на всех узлах почтовой системы (см. также пункт 2.2.5).

В DeepMail DSA-демон работает на одной из машин локации (обычно на ведущем хосте) и через REST API синхронизирует данные:

- *mail* – /mnt/deepmail/mail (почтовые ящики Dovecot);
- *DAV* – /mnt/deepmail/dav (коллекции календарей/ адресных книг).

При нажатии в карточке локации на кнопку 

(см. рисунок 48) откроется страница «Репликация» (рисунок 52).

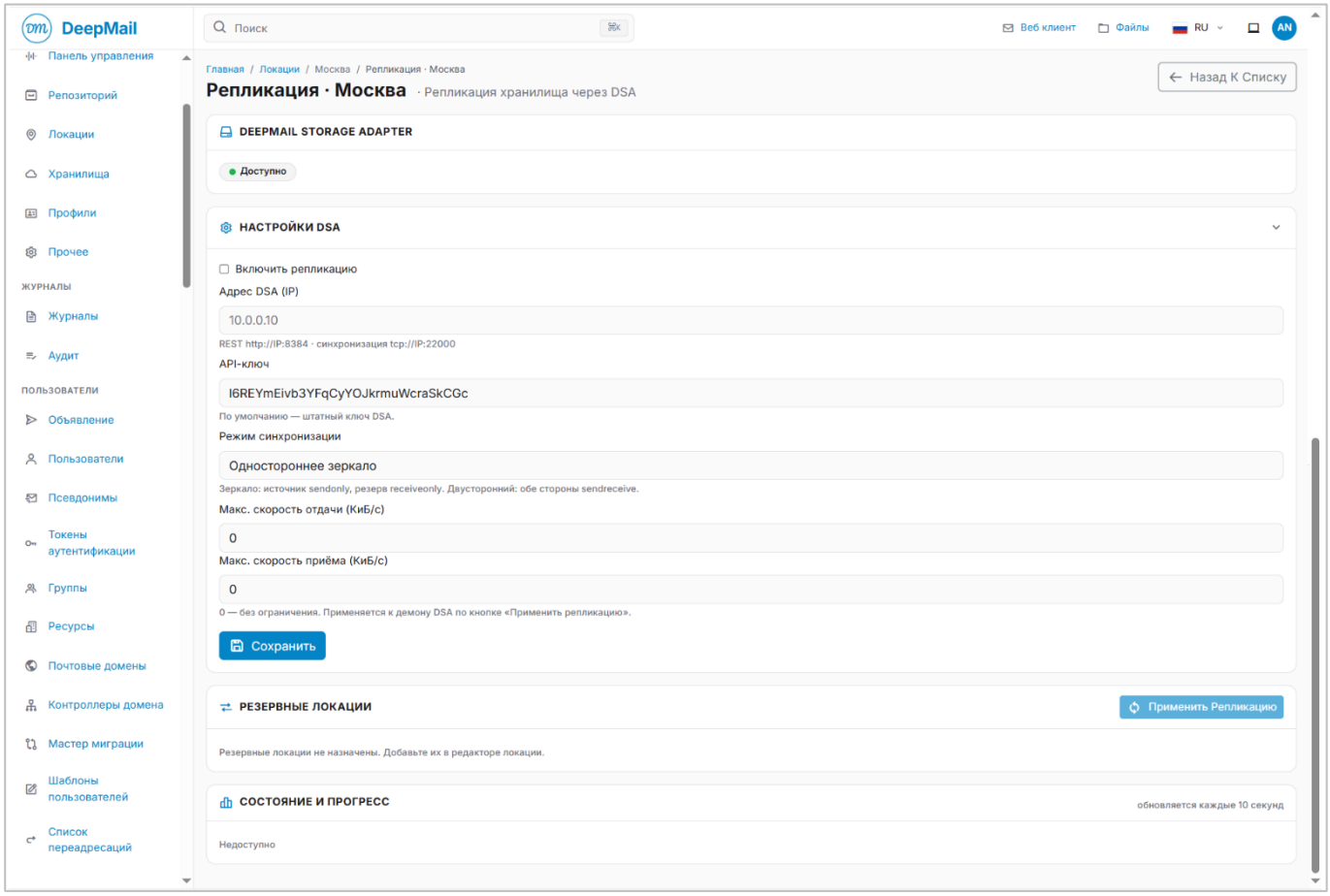


Рисунок 52 – Страница «Репликация»

На данной странице размещены несколько информационных блоков и ключевой блок настроек:

- «DEEPMAIL STORAGE ADAPTER» – информация доступности DSA;
- «НАСТРОЙКИ DSA» – основной блок настроек репликации;
- «РЕЗЕРВНЫЕ ЛОКАЦИИ» – информация о резервных локациях;
- «СОСТОЯНИЕ И ПРОГРЕСС» – информация о ходе репликации с отображением процентов синхронизации данных *mail* и *DAV*.

В блоке «НАСТРОЙКИ DSA» необходимо:

- отметить чекбокс «Включить репликацию» – включает или отключает участие этой локации в обмене данными;
- поле «Адрес DSA (IP)» – IP машины с DSA. Если порт не указан – по умолчанию: 8384;
- поле «API key» – ключ X-API-Key для запросов к DSA. Если не задан – используется дефолтный ключ;

- параметр «Режим синхронизации» – «Одностороннее зеркало» (one-way: отсюда уходят данные, в резерве только хранятся) или «Двусторонний (active-active)» (обе стороны отдают и принимают данные);

- параметр «Макс. скорость отдачи (Киб/с)» – Лимит исходящей скорости репликации. Значение «0» = без ограничения;

- параметр «Макс. скорость приёма (Киб/с)» – Лимит входящей скорости репликации. Значение «0» = без ограничения.

Затем нажмите 

, в верху страницы появится сообщение о том, что настройки репликации сохранены.

Далее в блоке «РЕЗЕРВНЫЕ ЛОКАЦИИ» нажмите кнопку 

. Кнопка будет доступна только если для локации назначена резервная площадка.

В блоке «СОСТОЯНИЕ И ПРОГРЕСС» появятся проценты синхронизации данных *mail* и *DAV*.

Важно! Для резервной локации также должна быть включена и настроена репликация (перейдите на страницу репликации в карточке резервной локации и выполните настройки).

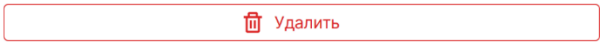
3.2.4.4 Удаление локации

Удаление локации будет заблокировано, если к ней привязан хотя бы один хост, сначала надо удалить все привязанные хосты.

Также перед удалением локации необходимо:

- если локация была резервом для других локаций, убрать ее из списка резервных;

- отвязать пользователей от локации.

После этого локацию можно удалить. Для удаления локации нажмите в карточке локации на кнопку 

(см. рисунок 48).

3.2.5 Хранилища

Интерфейс управления хранилищами (рисунок 53) представляет собой панель управления подключенными хранилищами в системе DeepMail, обеспечивающую централизованный контроль над дисковыми ресурсами.

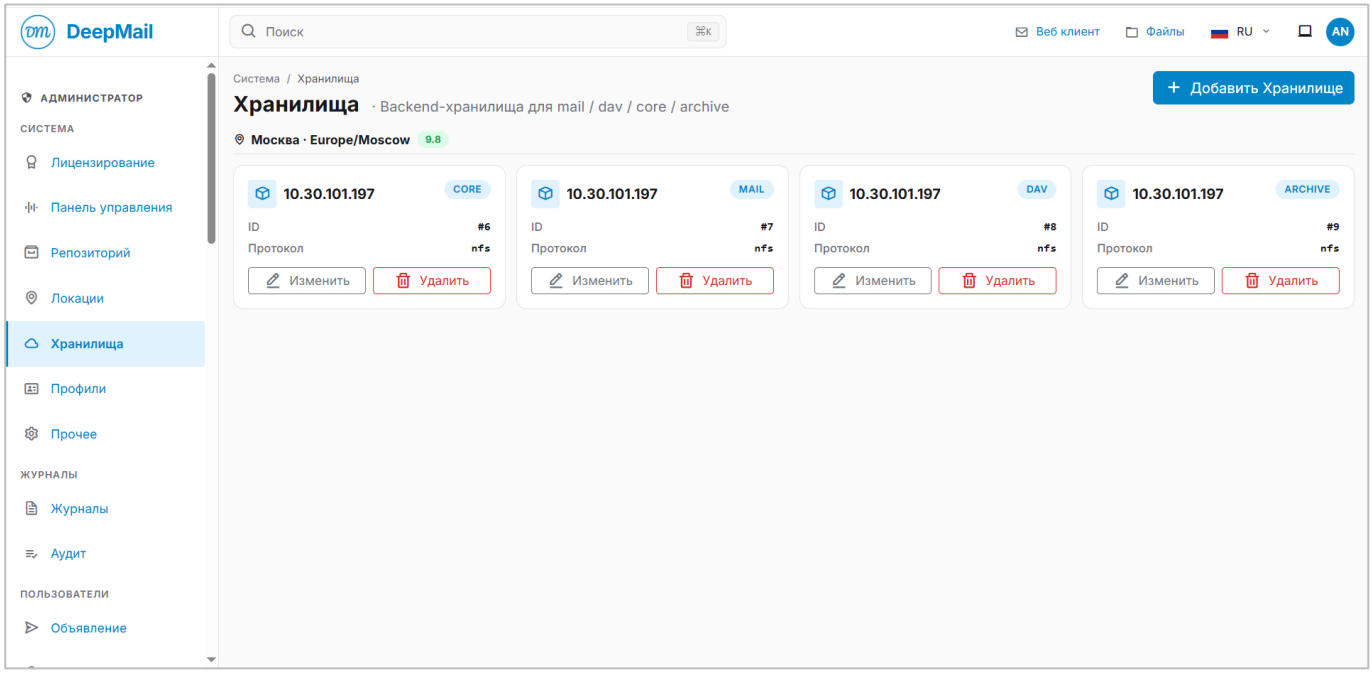
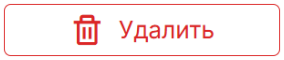


Рисунок 53 – Окно управления хранилищами

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 хранилище привязано.

Под каждым типом хранилища списком выводятся конкретные точки подключения (ID) с указанием используемого сетевого протокола (например, NFS). В карточке каждого элемента доступны кнопка 

(для смены типа, протокола, IP удаленного сервера или локации) и кнопка 

(для отключения конкретного хранилища).

В правом верхнем углу находится кнопка 

позволяющая добавить новое хранилище.

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

3.2.6 Профили

Профили – это наборы параметров для сервисов IMAP, SMTP, WebDAV и SFTP. Один и тот же сервис может работать на разных хостах с разными профилями и соответственно применять к почтовым ящикам разный набор параметров (например, установлены разные лимиты, маршруты, очереди, правила папок и т.п.).

Интерфейс управления профилями представляет собой панель управления профилями конфигурации в системе DeepMail, предназначенную для централизованного создания, редактирования и выполнения настроек сервисов IMAP, SMTP, WebDAV и SFTP (рисунок 54).

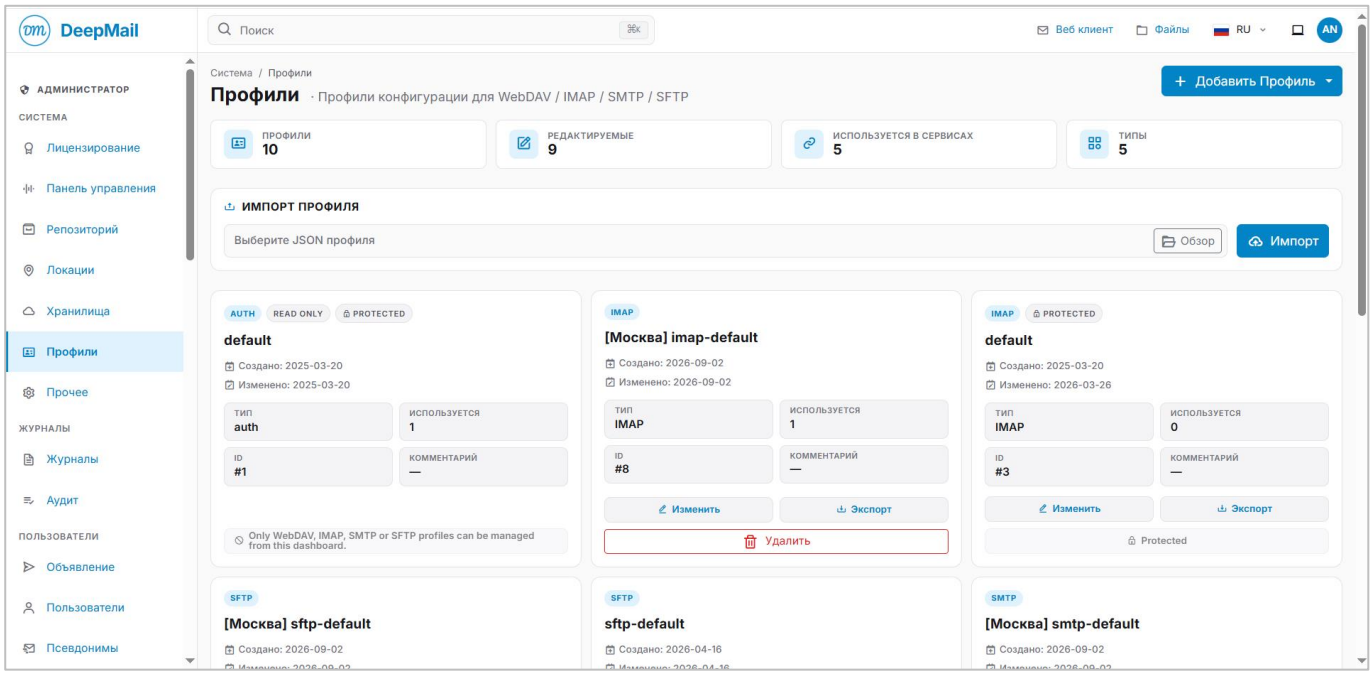


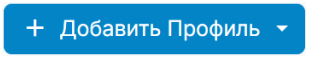
Рисунок 54 – Окно управления профилями

Панель разделена на три функциональные зоны. В верхней части отображается общая информация о количестве профилей – сколько всего созданных профилей в системе, сколько редактируемых, сколько профилей используется в сервисах и сколько типов профилей создано (профиль AUTH (5й тип) создается при инсталляции системы и не может быть добавлен, отредактирован, экспортирован или удален).

Затем размещена зона, посвященная импорту профилей. Она позволяет загрузить ранее экспортированный JSON-файл с настройками, используя кнопку Обзор, и затем применить их для создания профиля, нажав кнопку Импорт. Это удобно для тиражирования одинаковых настроек на разных узлах, восстановления конфигураций или их передачи.

И ниже расположен список существующих профилей. Для каждого профиля указана служебная информация: дата создания, последнего изменения, тип, количество сервисов в которых он используется, ID и 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. После изменения профиля необходимо выполнить реконфигурацию всех хостов, к которым он привязан (см. 3.2.2.3).

Для добавления нового профиля необходимо в правом верхнем углу окна нажать кнопку 

и выбрать соответствующий профиль: WebDav, SMTP, IMAP или SFTP, после чего заполнить поля формы создания профиля и нажать кнопку 

(рисунок 55).

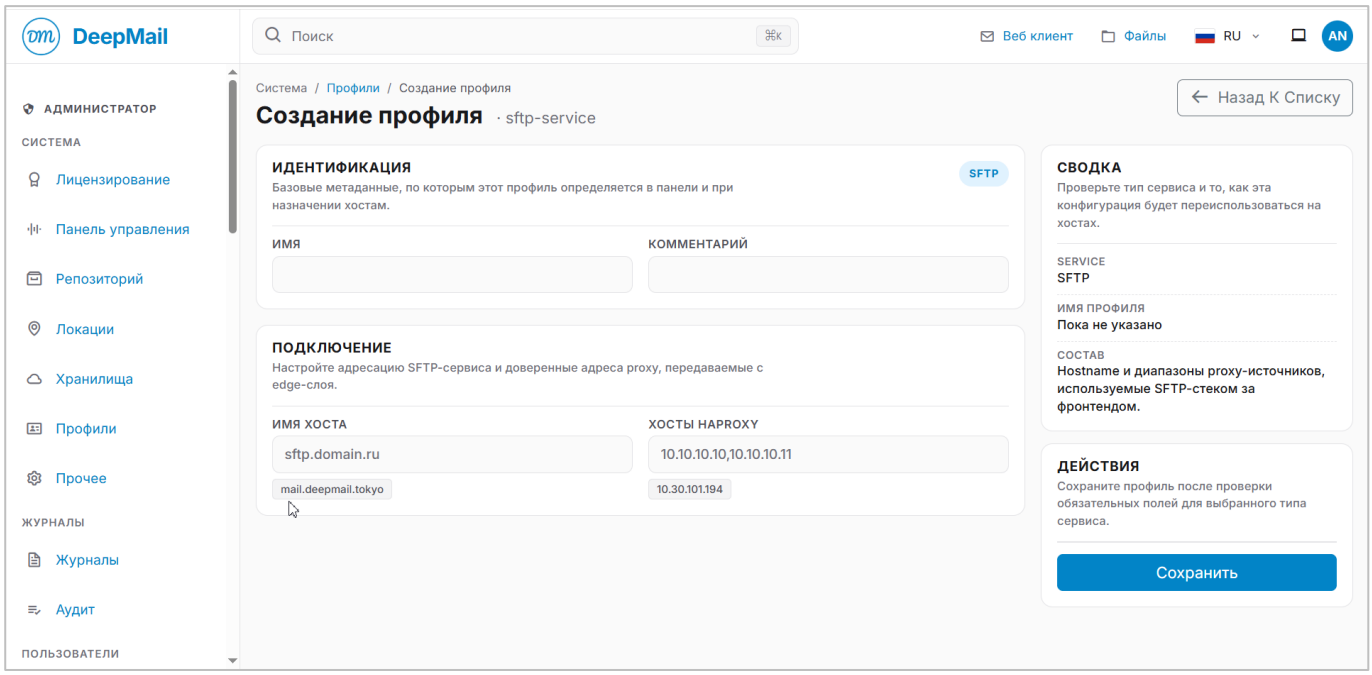
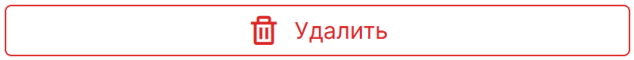


Рисунок 55 – Форма создания профиля

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, экспорта или удаления существующих профилей необходимо в карточке профиля нажать кнопку 

, 

или 

соответственно. Последний оставшийся профиль выбранного типа удалить нельзя, администратор увидит соответствующее предупреждение.

3.2.6.1 Настройка корзин первого и второго уровня и восстановление удаленных писем

В DeepMail реализована двухуровневая система хранения удаленных пользователями 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 */var/deepmail/mail/exemple@exemple.ru/Trash* почтового ящика пользователя. Когда пользователь очищает эту корзину, письма не удаляются безвозвратно, а перемещаются во второй, скрытый уровень – папку */var/deepmail/mail/exemple@exemple.ru/Recoverable*, которая находится в структуре того же ящика. В папке */var/deepmail/mail/exemple@exemple.ru/Recoverable/Deleted Items* находятся удаленные письма из корзины первого уровня. Доступ к этому уровню возможен только на уровне файловой системы сервера и требует привилегий администратора.

Параметры автоматической очистки обоих уровней задаются в IMAP-профиле через интерфейс управления профилями админ-панели. 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 хостов, использующих данный профиль.

Для настройки корзин первого и второго (скрытая корзина) уровней, куда попадают письма из обычной корзины после ее очистки, требуется в карточке профиля IMAP (см. рисунок 54) нажать кнопку 

и в открывшемся окне настроить параметры автоочистки корзин в блоке «Правила папок» (рисунок 56).

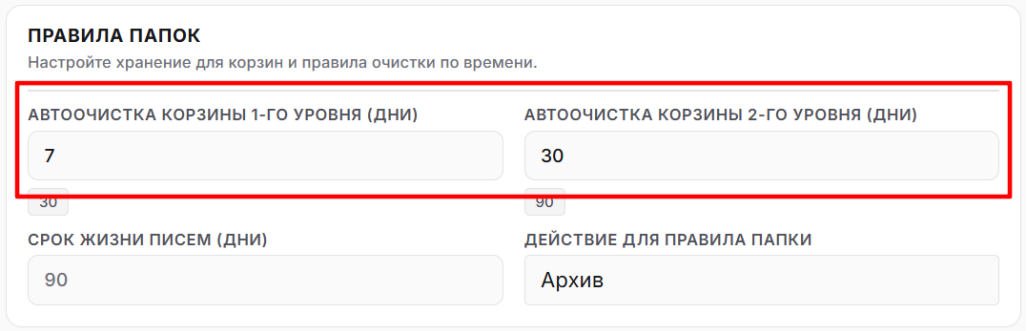


Рисунок 56 – Настройка параметров автоочистки корзин

Если возникает необходимость восстановить письма из скрытой корзины, администратору необходимо выполнить следующие действия на сервере, где размещен 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 надежного восстановления данных при сохранении полного контроля над правами доступа и сроками хранения информации.

3.2.6.2 Настройка ретрансляции

Для настройки ретрансляционных сетей, требуется в карточке профиля SMTP нажать кнопку 

и в открывшемся окне настроить параметры ретрансляционных сетей выбранного профиля SMTP, заполнив поле «Ретрансляционные сети» в блоке «Маршрутизация» (рисунок 57).

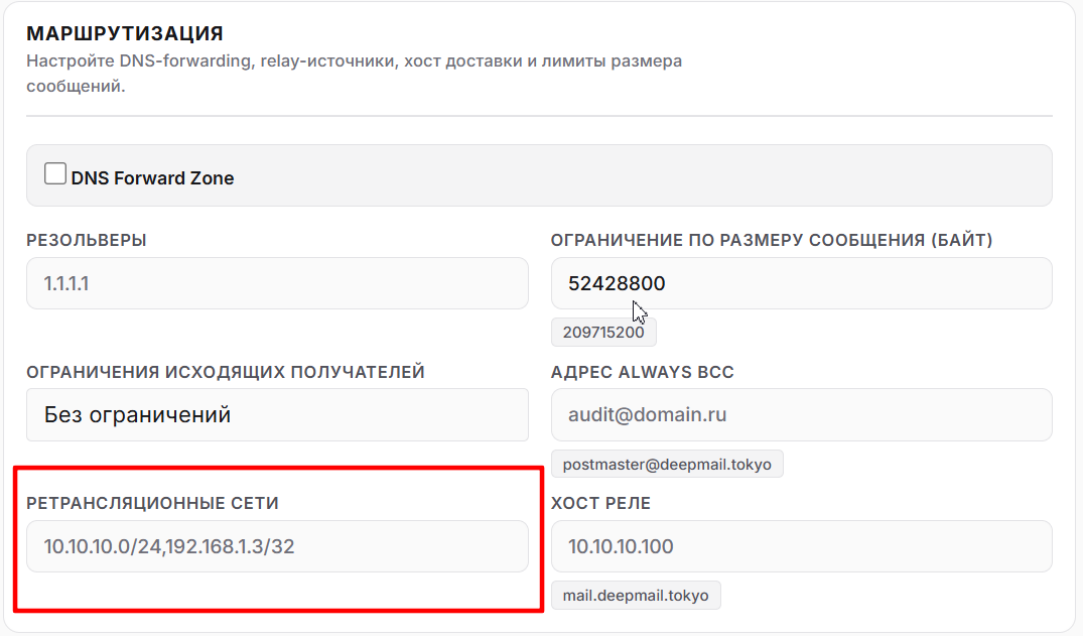


Рисунок 57 – Блок «Маршрутизация»/ поле «Ретрансляционные сети»

В поле «РЕТРАНСЛЯЦИОННЫЕ СЕТИ» необходимо указать необходимые сети *<IP-адрес>/24,<IP-адрес>/32*, например *10.10.10.0/24,192.168.1.3/32*.

Важно! IP-адреса указываются через запятую без пробелов.

В поле «ХОСТ РЕЛЕ» должно быть заполнено значение, например *10.10.10.100*.

В случае, если используется антиспам RSPAMD, дополнительно необходимо скорректировать в файле *deepmail.env* (*mnt/deepmail/core/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*.

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

deepmail stop

deepmail start.

3.2.7 Прочее

При нажатии в разделе «Система» кнопки «Прочее» (см. рисунок 36) открывается страница админ-панели «Прочие настройки», которая содержит ссылки на общесистемные настройки (рисунок 58).

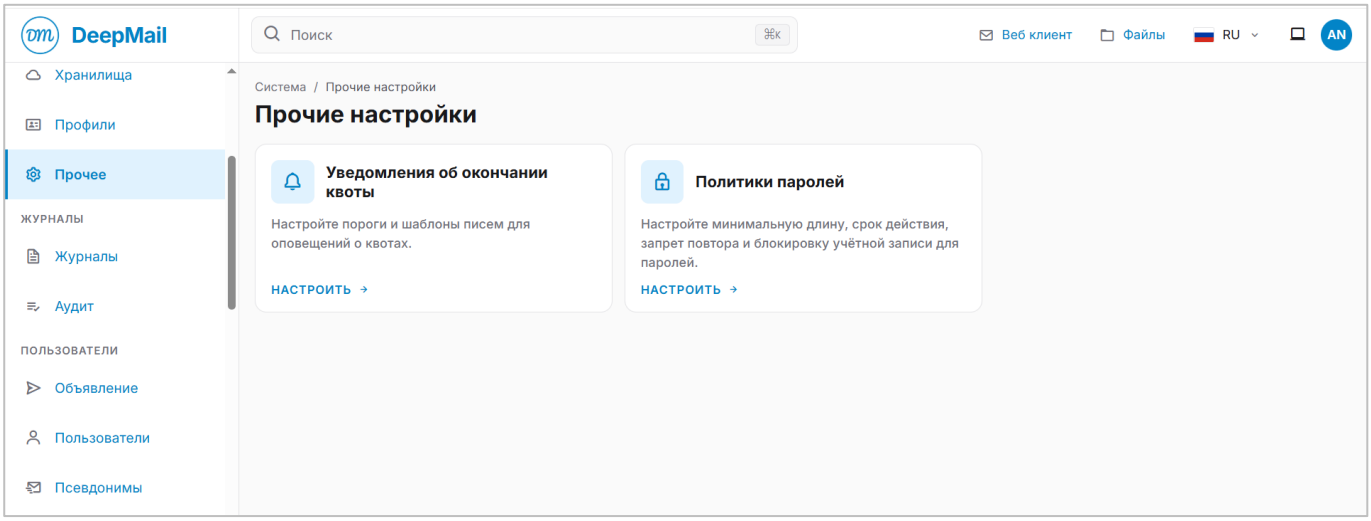


Рисунок 58 – Страница «Прочие настройки»

На текущий момент прочие настройки включают следующие инструменты:

- «Уведомления об окончании квоты» – настройка порогов достижения лимитов квоты почтового ящика;
- «Политики паролей» – настройки обеспечения безопасности доступа при применении паролей для УЗ пользователей.

Для перехода на страницы инструментов необходимо нажать соответствующую кнопку.

3.2.7.1 Уведомления о квоте

Учетной записи каждого пользователя присвоен параметр «quota_notify_level» в БД (от 0 до 3). После каждой проверки заполненности почтового ящика сравнивается фактический процент заполнения квоты с установленными администратором порогами L1/L2/L3:

- если процент пересек порог в сторону увеличения – система отправляет письмо с уведомлением, значение параметра «quota_notify_level» для УЗ поднимается на соответствующее значение;
- если процент пересек порог в сторону уменьшения (пользователь почистил ящик) – значение параметра «quota_notify_level» опускается обратно;

– при повторном превышении того же порога уведомление не дублируется пока не было «отката» через очистку.

Это необходимо, чтобы не «спамить» пользователю каждый раз, когда он балансирует на грани порога.

Функционал инструмента «Уведомления о квоте» дает возможность настройки порогов заполнения почтовых ящиков пользователей, по достижении которых система автоматически направит письма с уведомлением пользователям и/или администраторам.

На странице админ-панели «Уведомления о квоте» отображена форма с полями для заполнения (рисунок 59).

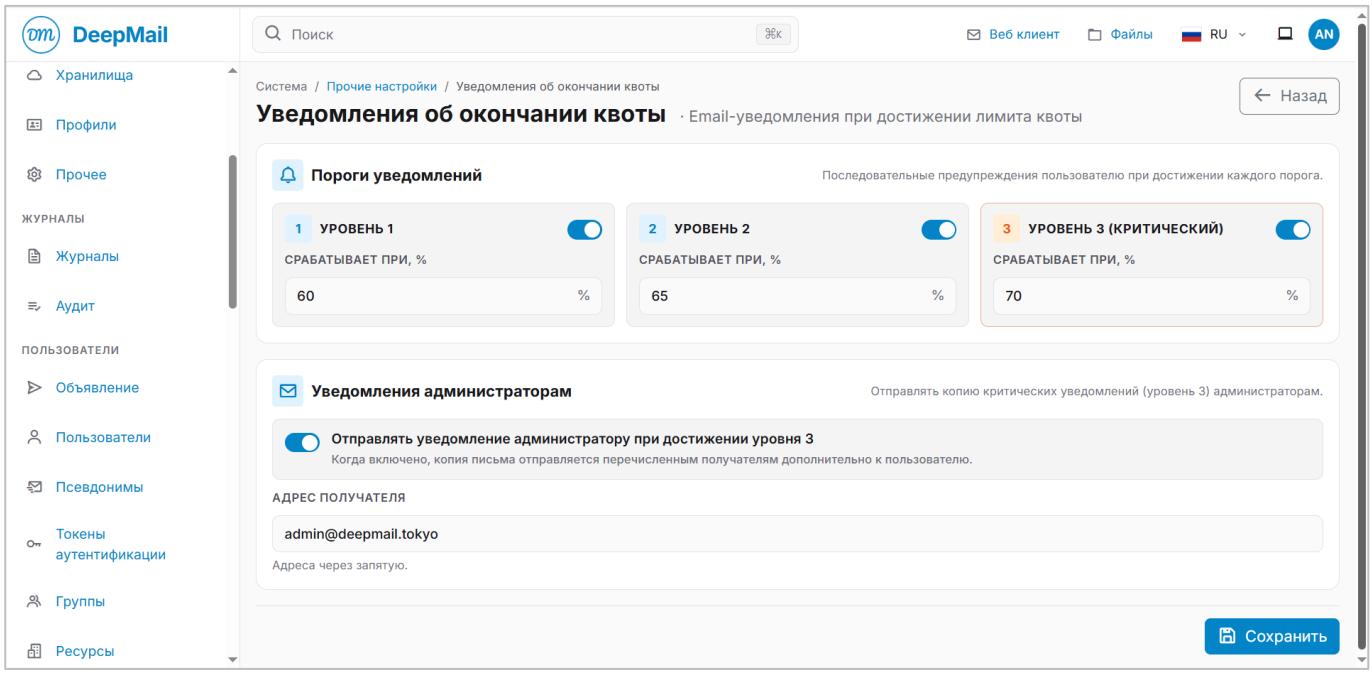


Рисунок 59 – Страница «Уведомления об окончании квоты»

В блоке «Пороги уведомлений» размещены следующие элементы настроек:

– «Уровень 1» – чекбокс включения и поле для ввода значения первого порога (L1) в процентах от квоты;

– «Уровень 2» – чекбокс включения и поле для ввода значения второго порога (L2) в процентах от квоты;

– «Уровень 3» – чекбокс включения и поле для ввода значения третьего порога (L3) в процентах от квоты. Это критический уровень заполнения почтового ящика.

В блоке «Уведомления администраторам» размещены следующие элементы настроек:

– чекбокс «Отправлять уведомление администратору при достижении уровня 3» – включает отправку копии письма с уведомлением для администраторов при критическом уровне (L3). На L1/L2 администраторам ничего не направляется;

- «Адрес получателя» – поле для ввода email-адресов администраторов, адреса указываются через запятую.

Значения процентов – это целые числа от 1 до 99. По умолчанию все три уровня отключены.

Примеры вариантов применения:

1) Уведомления получают только администраторы – отключить уровни 1 и 2 (уведомления пользователю не отправляются), включить только уровень 3 + включить «Отправлять админам на уровне 3» с адресами IT-отдела.

2) Постепенное оповещение – включить три уровня с установленными значениями L1 – 50%, L2 – 70%, L3 – 90%, пользователь получает три уведомления; администраторы оповещаются только при достижении критического уровня L3.

3.2.7.2 Политики паролей

Инструмент «Политики паролей» – это реализация функций безопасности таких как:

- Запрет повторного использования паролей;
- Ограничение минимальной длины пароля;
- Срок действия пароля, по истечении которого требует его смена;
- Блокировка входа на заданное время при определенном количестве неуспешных попыток ввода пароля.

Страница админ-панели «Политики паролей» содержит соответствующие функциям блоки с полями для заполнения (рисунок 60).

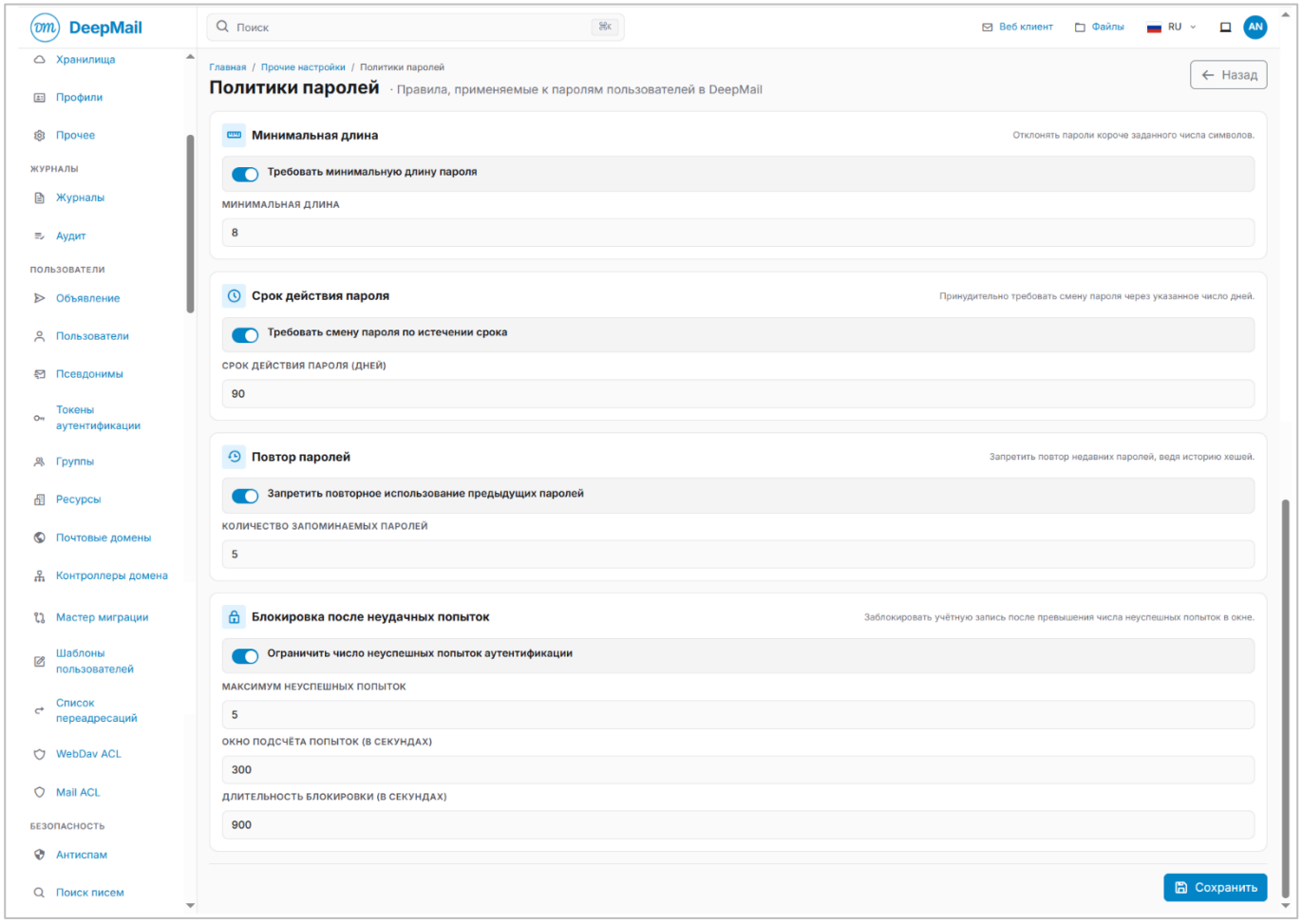


Рисунок 60 – страница «Политики паролей»

«Минимальная длина» – включается чекбоксом «Требовать минимальную длину пароля» и затем в поле «МИНИМАЛЬНАЯ ДЛИНА» вводится количество символов (если пользователь введет при смене пароля меньше символов, то пароль не будет принят);

«Срок действия пароля» – включается чекбоксом «Требовать смену пароля по истечении срока» и затем в поле «СРОК ДЕЙСТВИЯ ПАРОЛЯ (ДНЕЙ)» указывается количество дней, по истечении которых система запросит смену пароля. Вход в почтовый ящик или админ-панель (для администраторов) без смены пароля будет невозможен;

«Повтор паролей» – включается чекбоксом «Запретить повторное использование предыдущих паролей» и затем в поле «КОЛИЧЕСТВО ЗАПОМИНАЕМЫХ ПАРОЛЕЙ» указывается значение, которое определяет глубину истории паролей пользователя. Это необходимо для того, чтобы пользователь не мог бесконечно «переключаться» между двумя-тремя простыми паролями, обходя систему безопасности;

«Блокировка после неудачных попыток» – включается чекбоксом «Ограничить число неуспешных попыток аутентификации». Затем в поле «МАКСИМУМ НЕУСПЕШНЫХ ПОПЫТОК» указывается количество попыток ввода аутентификационной информации,

после которого система будет заблокирована. В поле «ОКНО ПОДСЧЕТА ПОПЫТОК (В СЕКУНДАХ)» вводится продолжительность временного интервала, в течение которого система подсчитывает неудачные попытки входа. Этот параметр работает не сам по себе, а всегда в паре с полем «МАКСИМУМ НЕУСПЕШНЫХ ПОПЫТОК». Вместе они образуют правило: «Если пользователь введет неверный пароль X раз в течение Y секунд, его учетная запись будет заблокирована». И в завершение, в поле «ДЛИТЕЛЬНОСТЬ БЛОКИРОВКИ (В СЕКУНДАХ)» указывается значение временного интервала, в течение которого система будет заблокирована и только по истечении которого пользователь снова сможет попробовать аутентифицироваться в систему.

После включения необходимых чекбоксов и заполнения соответствующих полей для сохранения настроек нажмите кнопку 

(см. рисунок 60).

3.3 Раздел «Журналы»

В разделе панели управления «Журналы» размещены инструменты администратора, в которых фиксируются и предоставляются для анализа два независимых потока записей логированной информации с разным назначением: «Журналы» и «Аудит» (рисунок 61).

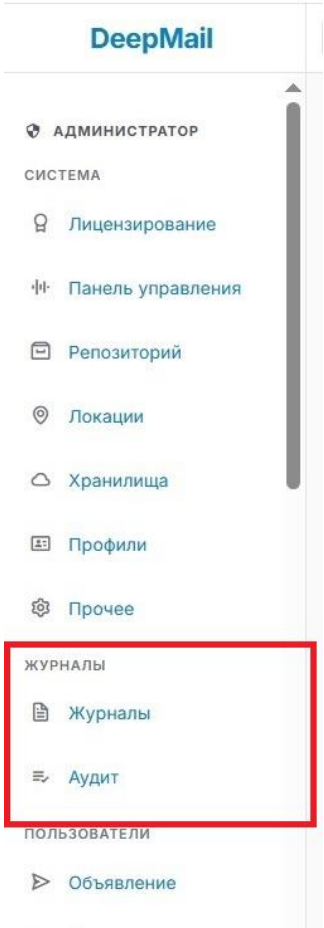


Рисунок 61 – Раздел «Журналы»

Инструмент «Журналы» – это файловые журналы сервисов (*Postfix, Dovecot, nginx, rspamd, admin-service* и др.) со всех хостов. С доступными действиями – поиск, фильтры по уровням и периоду, потоковый просмотр в реальном времени, выгрузка в виде архива *.tar.gz.

Инструмент «Аудит» – это структурированный журнал действий администраторов из БД *admin-service*: кто, когда, с какого IP, над каким объектом и с каким результатом выполнял действия. Сводка предоставляется за последние 24 часа, присутствуют фильтры, раскрытие деталей с дампом изменений. Доступ к аудиту имеют только глобальные администраторы.

Примеры применения инструментов:

- «Почему письмо не было доставлено?» – войти в инструмент «Журналы», выбрать источник – «smtp-service.log», фильтр по «queue_id».
- «Кто заблокировал пользователя?» – войти в инструмент «Аудит», установить фильтр «target=email, action=user.block».
- «Что менял конкретный администратор за неделю?» – войти в инструмент «Аудит», установить фильтр «actor» + диапазон дат.
- «Что писал сервис при ошибке из аудита?» – войти в инструмент «Аудит», чтобы найти время и объект (target); войти в инструмент «Журналы», чтобы посмотреть логи сервисов в этот момент.

3.3.1 Журналы

Инструмент «Журналы» централизованно показывает все журналы сервисов DeepMail со всех хостов инсталляции. Администратору предоставлены следующие возможности:

- поиск данных в текущих «живых» журналах и архивах за указанный период времени;
- просмотр в режиме реального времени логов одного источника на конкретном хосте;
- выгрузка архива журналов в формате*.tar.gz для передачи в поддержку или анализа записей.

Таким образом интерфейс позволяет оперативно анализировать события сервисов системы и сохранять их для последующего аудита или передачи в системы класса SIEM.

Окно страницы «Журналы» разделено на три функциональные области (рисунок 62).

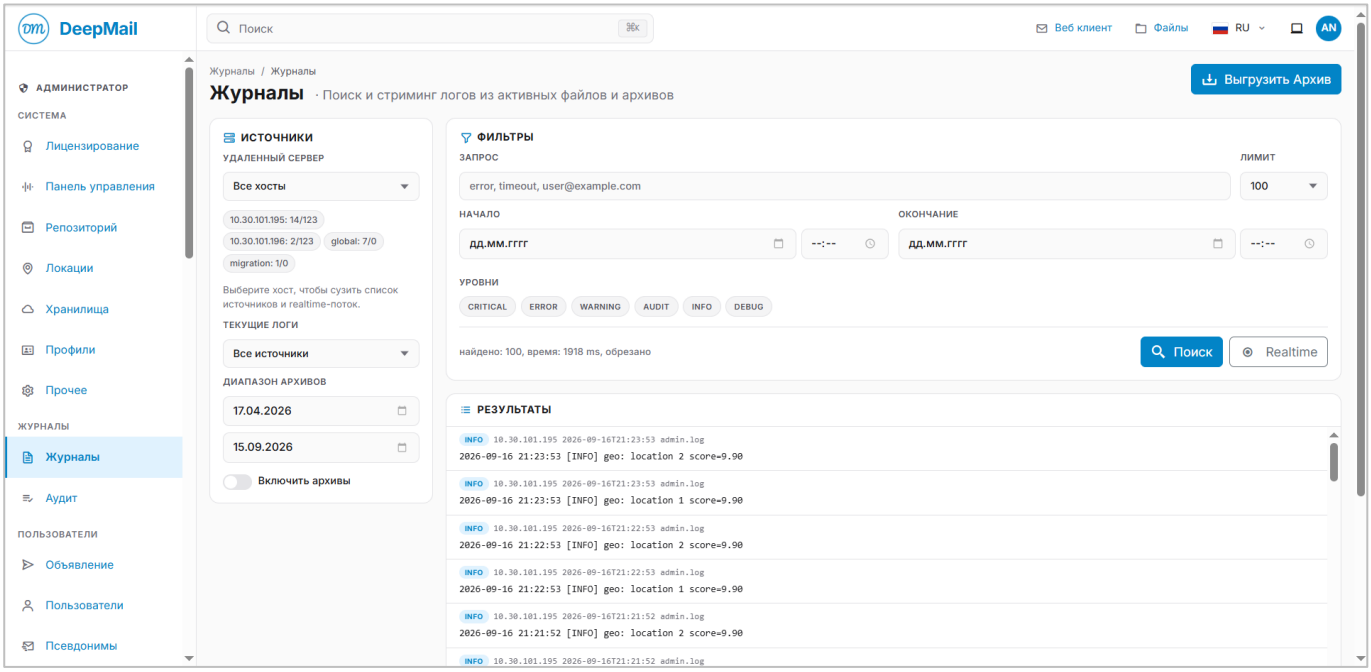


Рисунок 62 – Страница Журналы (просмотр логов сервисов)

В левой части находится блок «Источники» (см. рисунок 62), где предоставлен выбор либо всех узлов инфраструктуры, либо отдельных удаленных серверов с их IP-адресами (например, 10.30.101.195), а также служебные источники global (системные события) и migration (логи миграции). Рядом с каждым отдельным 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.

Поле «Текущие логи» содержит выпадающий список, в котором можно выбрать в качестве источника данных лог определенного сервиса, что позволит получить еще более узкую информацию для анализа.

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.

В блоке «Фильтры» (см. рисунок 62) содержатся элементы управления тем, что искать:

- поле «ЗАПРОС» – для ввода поисковых запросов (простой текст) по строкам журналов;
- поле «ЛИМИТ» – из выпадающего списка необходимо выбрать максимальное число выводимых результатов: 100 (по умолчанию), 300, 500 или 1000;
- поля «Начало» и «Окончание» – диапазон дат и времени. Выбор осуществляется нажатием на кнопки и ;

- параметр «Уровни» – фильтр по семантике лог-сообщения. Доступны следующие фильтры:

а) «Critical» – серьезные сбои, требующие немедленного внимания (отвал базы, нехватка диска и т.п.);

б) «Error» – операция не выполнилась: отказ доставки, ошибка авторизации, исключение в *admin-service*;

в) «Warning» – что-то пошло не идеально, но обработано: retry, soft-fail, fallback;

г) «Audit» – точечные значимые события (вход администратора, изменение объекта). Это не полный аудит – для полного журнала есть «Аудит»;

д) «Info» – обычный поток событий (запуски, синхронизации, переходы состояний);

е) «Debug» – детальные сообщения. Видны, только если у сервиса соответствующий уровень логирования включен.

Уровни определяются по тегу [<уровень>] в строке журнала или по характерным маркерам формата (зависит от сервиса). При нажатии кнопки уровня она «загорается» цветовым индикатором, например ERROR / ERROR, INFO / INFO и др.

В нижней части блока «Фильтры» (см. рисунок 62) отображаются служебные сведения: общее количество найденных строк, время выполнения запроса (в миллисекундах) и примечание об обрезании длинных строк. Также там размещены две копки:

- Поиск – после нажатия выполняется разовый поиск по выбранным источникам и архивам с применением установленных фильтров. Выводит в результатах количество строк равное значению, установленному в поле «Лимит»;

- Realtime – потоковый просмотр одного источника на одном хосте через SSE. Кнопка доступна, только когда выбраны конкретный хост и конкретный источник (не «Все хосты» или «Все источники»). Архивы в этом режиме игнорируются – в результаты выводятся новые строки, появляющиеся в активной области. Чтобы прекратить, нажмите кнопку Остановить Realtime, которая появится после запуска потокового просмотра, или уйдите со страницы.

В нижней части страницы в блоке «Результаты» выводится журнал записей, соответствующих выбранным источникам и фильтрам. Каждая строка результата содержит:

- цветной бейдж уровня (аналогичный кнопкам уровней в блоке «Фильтры» – «Critical», «Error», «Warning», «Audit», «Info», «Debug»);

- IP-адрес узла;
- метку даты и времени в формате ISO (если ее удалось извлечь из строки);
- имя файла журнала (например, admin.log)
- детальное сообщение – может содержать: 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 нажмите кнопку Выгрузить Архив (см. рисунок 62). Откроется модальное окно «Выгрузить архив» (рисунок 63).

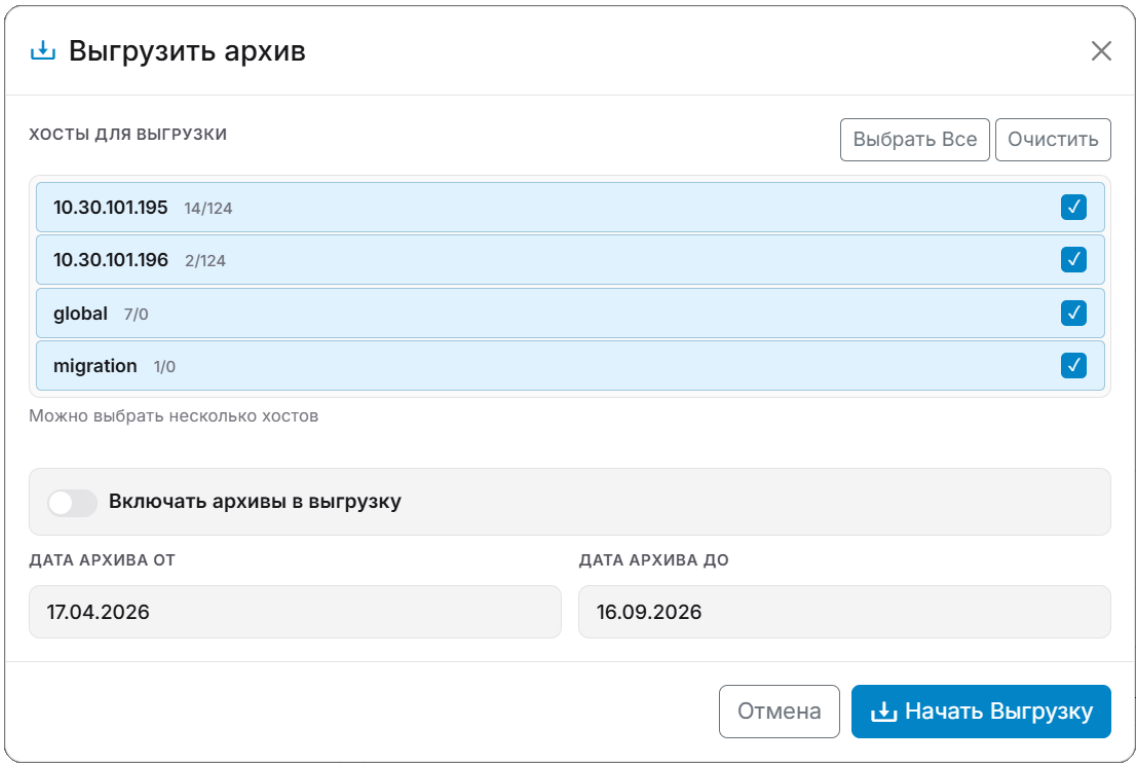


Рисунок 63 – Модальное окно настройки выгрузки журналов

В этом окне представлены для выбора те же хосты, что и на главном экране. Для каждого хоста 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 чекбокс «Включать архивы в выгрузку» – если он установлен, в выгрузку попадут и архивные записи за указанный период, и текущие логи. Далее задается диапазон дат «Дата архива от» и «Дата архива до» – этим ограничивается временной интервал выгружаемых событий (применяется, только если включен чекбокс «Включать архивы в выгрузку»).

После настройки параметров нажатие кнопки 

инициирует создание архива *tar.gz. Система соберет все записи, соответствующие выбранным хостам и диапазону дат, и выполнит выгрузку архива с логами, который сохраняется в папке «Загрузки» на ПК. Эта функция особенно полезна для предоставления журналов службе технической поддержки, для интеграции с внешними анализаторами или для выполнения требований по хранению логов.

3.3.2 Аудит

Инструмент «Аудит» – это журнал фиксации значимых действий администраторов. Например, сюда записываются все правки объектов через UI и CLI, переключения политик, выгрузки логов, входы и сбросы паролей.

На странице инструмента «Аудит» сразу отображается «результат» – «Журнал аудита» всех действий администраторов.

В верхней части размещен информационный блок, содержащий следующие данные:

- «Всего записей» – общее количество записей в журнале (за все время);
- «За последние 24ч» – новые записи, зафиксированные в течении последних 24х часов;
- «Активных админов (24ч)» – количество администраторов, совершающих действия в системе за последние 24 часа: уникальные значения «actor» за последние сутки;
- «Ошибок (24ч)» – количество зафиксированных ошибок за последние 24 часа: записи со статусом, отличным от «success», за последние сутки.

Значения в информационном блоке обновляются при загрузке, чтобы пересчитать – перезагрузите страницу.

Ниже размещена область вывода действий.

В отличие от инструмента «Журналы», «Журнал аудита»:

- имеет структурированный табличный вид, а также вывод для каждой строки дополнительных полей – «ПАРАМЕТРЫ ДЕЙСТВИЯ» (actor, action, target, status и др.) и «ДЕТАЛИ»;
- хранится бессрочно (cleanup-cron не настроен; решение пользователя);
- не зависит от того, успел ли сервис записать строку в лог-файл.

Технически каждая запись фиксируется двойной записью (dual-write): одновременно в БД (таблица audit_log) и в файл /logs/global/audit.log. Страница «Журнал аудита» считывает из БД файл, который работает даже при недоступности БД, и его же можно открыть на

странице «Журналы» (хост root или global, источник audit.log, уровень «Audit»). Формат строки в файле:

[DD/MM/YYYY HH:MM:SS] [AUDIT] actor=<email> ip=<addr> action=<name> target=<value> status=<state> detail=<payload>

Право доступа к странице «Журнал аудита» имеют только глобальные администраторы или те, кому назначены права «audit.manage». Доменные администраторы и обычные пользователи аудит не видят. Чтение файла /logs/global/audit.log через инструмент «Журналы» открыто шире, учитывайте это при разделении прав.

Таблица журнала аудита состоит из следующих столбцов:

- «ВРЕМЯ» – дата и время записи (в формате UTC);
- «АДМИНИСТРАТОР» – email администратора с аватаром (инициалы) и IP;
- «ДЕЙСТВИЕ» – бейдж действия (цвет зависит от типа (см. ниже);
- «ЦЕЛЬ» – моноширинная подпись объекта, на который было направлено действие;
- «СТАТУС» – бейдж статуса: «SUCCESS» (зеленый), «ERROR» (красный), «PARTIAL» (желтый, операция выполнена не полностью – например, массовое действие с частичными отказами);
- «ПОДРОБНО» – превью первых символов колонки «ДЕТАЛИ», которая отображается в дополнительной области при разворачивании строки.

Типы и цвета бейджей действий представлены в таблице 3.

Таблица 3 – Типы и цвета бейджей действий

Тип (семейство) действия	**Цвет**	**Примеры**
*.create, *.add*	синий (акцент)	user.create, relay.create, group.members.add
*.update, *.edit*, *.set*	оранжевый	user.edit, domain.edit, user.password.set
*.delete	красный	relay.delete, mailqueue.delete_all
*.block	красный	user.block
*.unblock	зеленый	user.unblock
другое (neutral)	серый	mailqueue.flush, system.logs.export, dcontroller.resync

Цвета бейджей действий – это визуальная подсказка администратору, а не классификация политики. Конкретное действие классифицируется по суффиксу/ фрагменту: *.create / содержит *.add → create, *.update / *.edit* / *.set* → update и т.д.

При клике на строку открывается дополнительная область с двумя колонками:

- слева «ПАРАМЕТРЫ ДЕЙСТВИЯ» – key-value-сводка: точные значения «job_id», «actor», «ip», «action», «status», «target», «created_at».
- справа «ДЕТАЛИ» – форматированный блок. Если содержимое – JSON, оно отображается с подсветкой/ переносами; если простой текст или диф полей – как есть.

В колонке «ДЕТАЛИ» обычно содержится:

- для типа действия *.create – значения полей нового объекта (audit_values() в коде);
- для типа действия *.edit – список изменений до/после (audit_diff());
- для типа действия *.delete – снимок удаляемого объекта;
- для действий, не относящихся к CRUD – контекст конкретного события (например, service_id=… queue_id=… для массового flush).

3.4 Раздел «Пользователи»

Самый обширный раздел настроек в системе – это раздел «Пользователи». На данный момент в нем 13 инструментов:

- Объявление;
- Пользователи;
- Псевдонимы;
- Токены аутентификации;
- Группы;
- Ресурсы;
- Почтовые домены;
- Контроллеры домена;
- Мастер миграции;
- Шаблоны пользователей;
- Список переадресаций;
- WebDAV ACL;
- Mail ACL (рисунок 64).

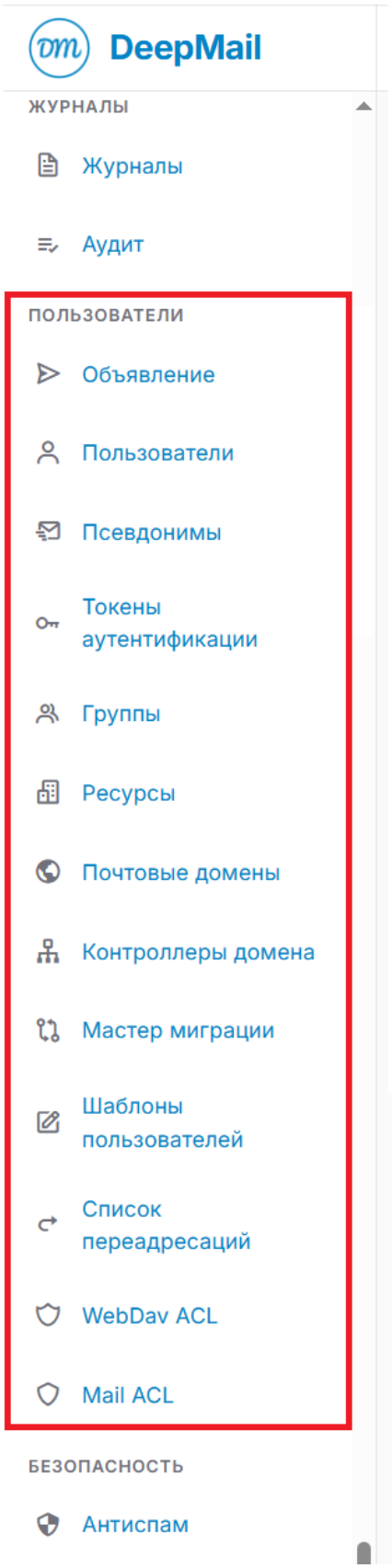


Рисунок 64 – Раздел «Пользователи»

Модули панели управления пользователями взаимосвязаны согласно логике доменной структуры или принадлежности к определенному пользователю. При завершении настройки зависимого объекта (например, почтового псевдонима) администратор перенаправляется из

текущего раздела («Пользователи»/ «Псевдонимы») в родительский контекст («Пользователи»/ «Домены»). Или при создании токена аутентификации для конкретного пользователя («Пользователи»/ «Токены аутентификации») администратор перенаправляется в личный кабинет этого пользователя («Моя учетная запись»/ «Токены аутентификации»). Такой подход оптимизирует работу поскольку администратору не нужно совершать дополнительных навигационных действий для проверки результата.

3.4.1 Инструмент «Объявление»

Инструмент «Объявление» предназначен для создания и отправки публичных объявлений пользователям почтовой системы.

Для перехода к инструменту необходимо в меню админ-панели выбрать пункт «Объявление» (см. рисунок 64).

Откроется страница, предназначенная для создания и отправки публичных объявлений (рисунок 65).

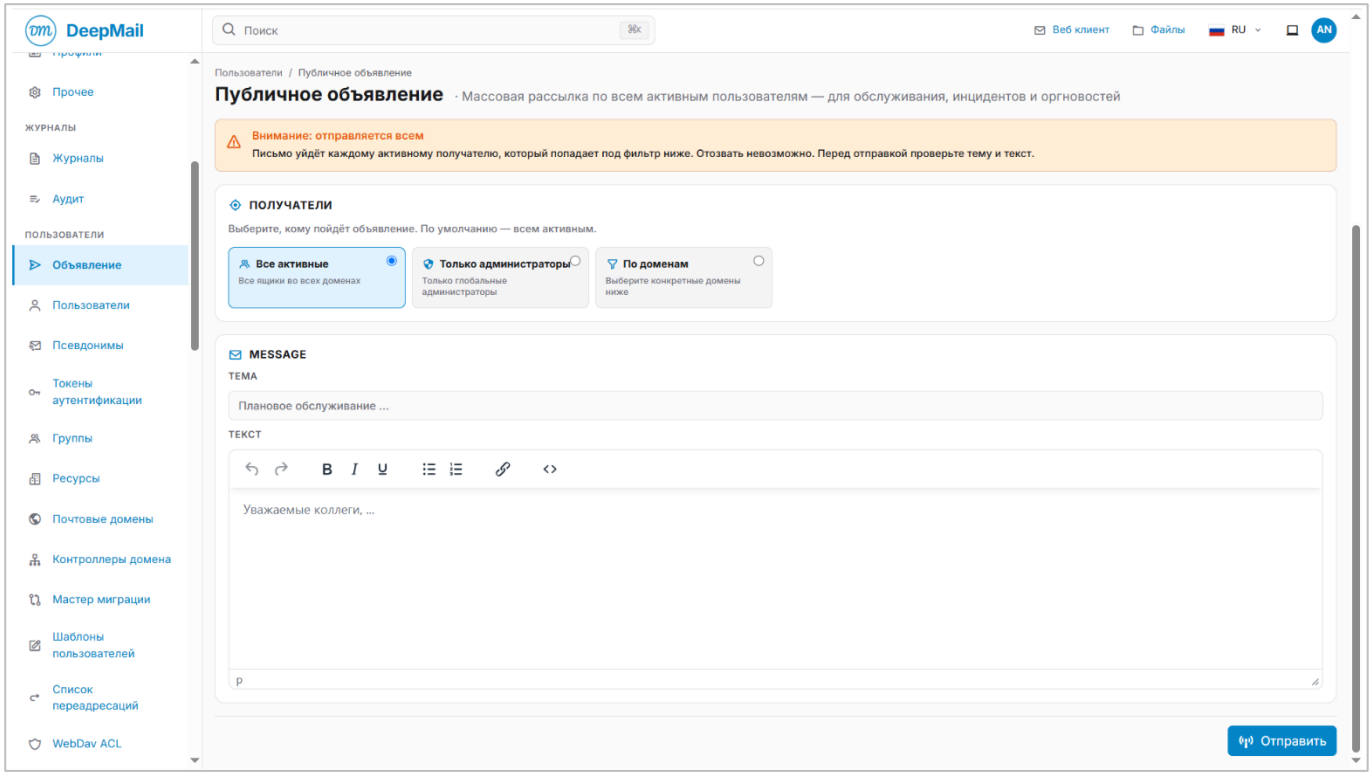


Рисунок 65 – Окно «Публичное объявление»

Страница разделена на два функциональных блока:

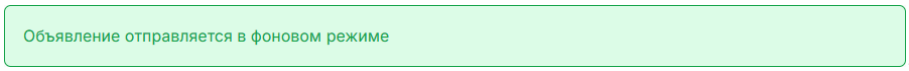
1) «ПОЛУЧАТЕЛИ» – выбор адресатов – «Все активные» (все ящики всех доменов), «Только администраторы» (получателями будут только пользователи с ролью «Глобальный администратор»), «По доменам» (выбор конкретного домена);

2) «MASSAGE» – поля ввода темы и текста объявления;

Выберите в блоке «ПОЛУЧАТЕЛИ» адресатов публичного объявления, в блоке «MASSAGE» укажите тему объявления, добавьте содержание в соответствующие поля и нажмите кнопку 

.

Важно! Внимательно проверьте отмеченные и введенные данные. Отозвать отправленное объявление невозможно.

В случае успешной рассылки объявления на странице появится сообщение 

.

3.4.2 Инструмент «Пользователи» («Список пользователей»)

При выборе в меню админ-панели пункта «Пользователи» (см. рисунок 64) открывается страница «Список пользователей», в которой отображена сводная информация о пользователях всех доменов почтовой системы (рисунок 66).

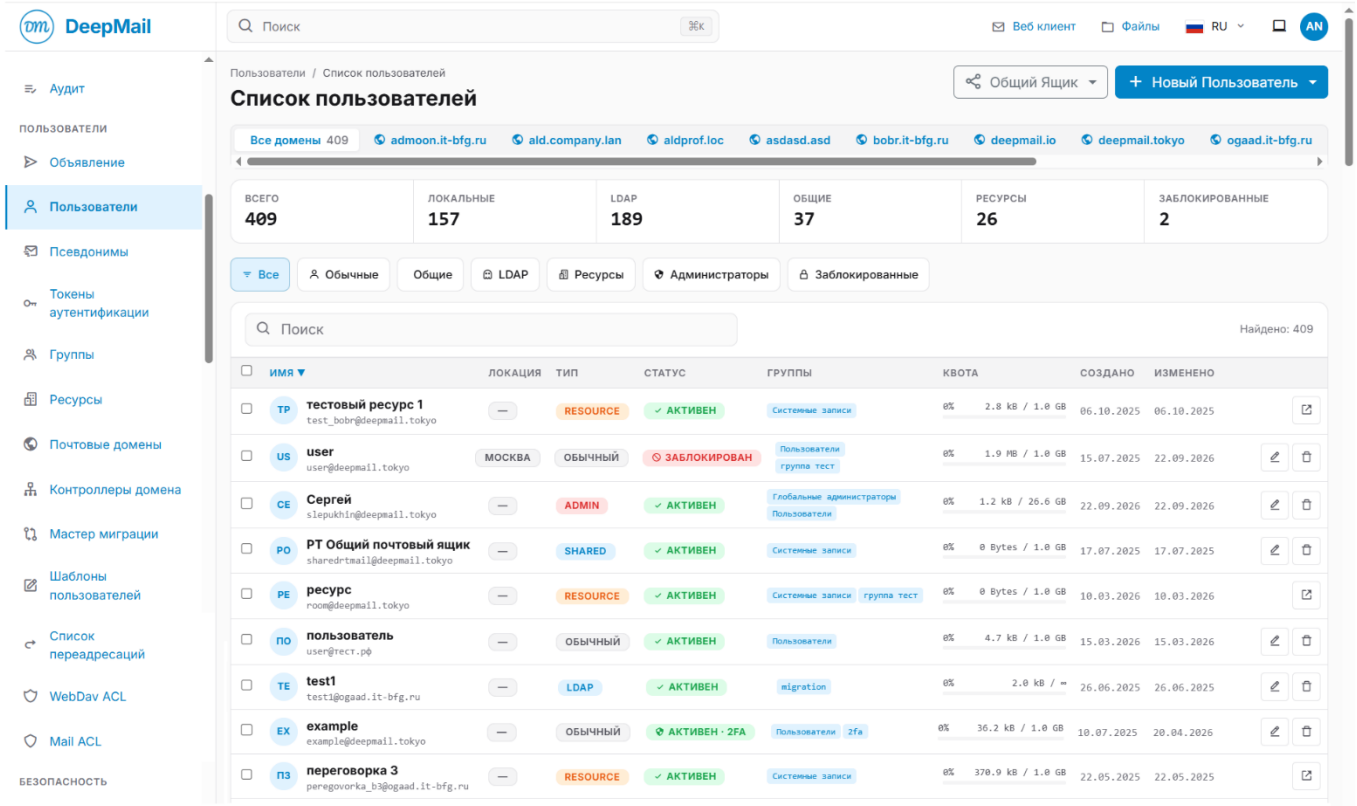


Рисунок 66 – Инструмент «Пользователи»/ страница «Список пользователей»

Инструмент предназначен для управления УЗ пользователей почтовой системы, включая общие почтовые ящики. Также в списке отображаются УЗ ресурсов, но управление ими осуществляется при помощи отдельного инструмента «Ресурсы» (см. 3.4.6).

В верхней части страницы размещена область информации с общими данными по всем доменам:

- «ВСЕГО» – общее число УЗ в почтовой системе;
- «ЛОКАЛЬНЫЕ» – не виртуальные и не общие почтовые ящики;
- «LDAP» – виртуальные УЗ (синхронизированные через контроллер домена);
- «ОБЩИЕ» – общие почтовые ящики;
- «РЕСУРСЫ» – почтовые ящики ресурсов;
- «ЗАБЛОКИРОВАННЫЕ» – заблокированные УЗ.

По умолчанию на странице показаны все УЗ добавленные в систему, для удобства администратору доступна система фильтрации:

- выбор конкретного домена для вывода списка пользователей на странице – нажмите на имя домена в строке с перечисленными доменами в верхней части страницы (например – deepmail.io, см. рисунок 66);
- выбор типа УЗ или статуса «Заблокирован», для показа в списке только соответствующих пользователей – нажмите необходимую кнопку над таблицей пользователей (например – Обычные, Ресурсы, Заблокированные и т.д., см. рисунок 66);
- сортировка списка пользователей по email (прямой или обратный алфавитный порядок) – нажмите на заголовок столбца ИМЯ ▼ (см. рисунок 66).

Также доступен поиск в списке (строка поиска над таблицей (см. рисунок 66), минимальный запрос – 3 символа).

В столбцах таблицы (см. рисунок 66) отображаются графические иконки типов, статусов и групп УЗ:

- ЛОКАЦИЯ – — (означает, что локация наследуется от домена), МОСКВА и т.п.;
- ТИП – ОБЫЧНЫЙ, ADMIN, SHARED и др.;
- СТАТУС – ✓ АКТИВЕН, ⦸ ЗАБЛОКИРОВАН, MASTER.
- ГРУППЫ – Пользователи, Глобальные администраторы и др.

Функционал инструмента «Пользователи» позволяет администратору добавлять новые УЗ пользователей и общих почтовых ящиков, редактировать их данные и удалять их из системы.

3.4.2.1 Добавление нового пользователя

Для добавления новой УЗ пользователя необходимо на странице «Список пользователей» нажать кнопку 

(см. рисунок 66), раскроется выпадающее меню со списком доступных доменов (рисунок 67).

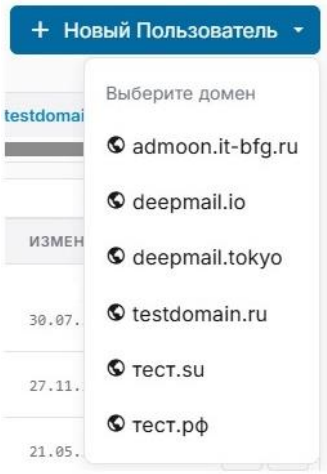


Рисунок 67 – Список доменов при добавлении УЗ пользователя

Выберите необходимый домен, после чего откроется форма добавления нового пользователя с привязкой к выбранному ранее домену (рисунок 68).

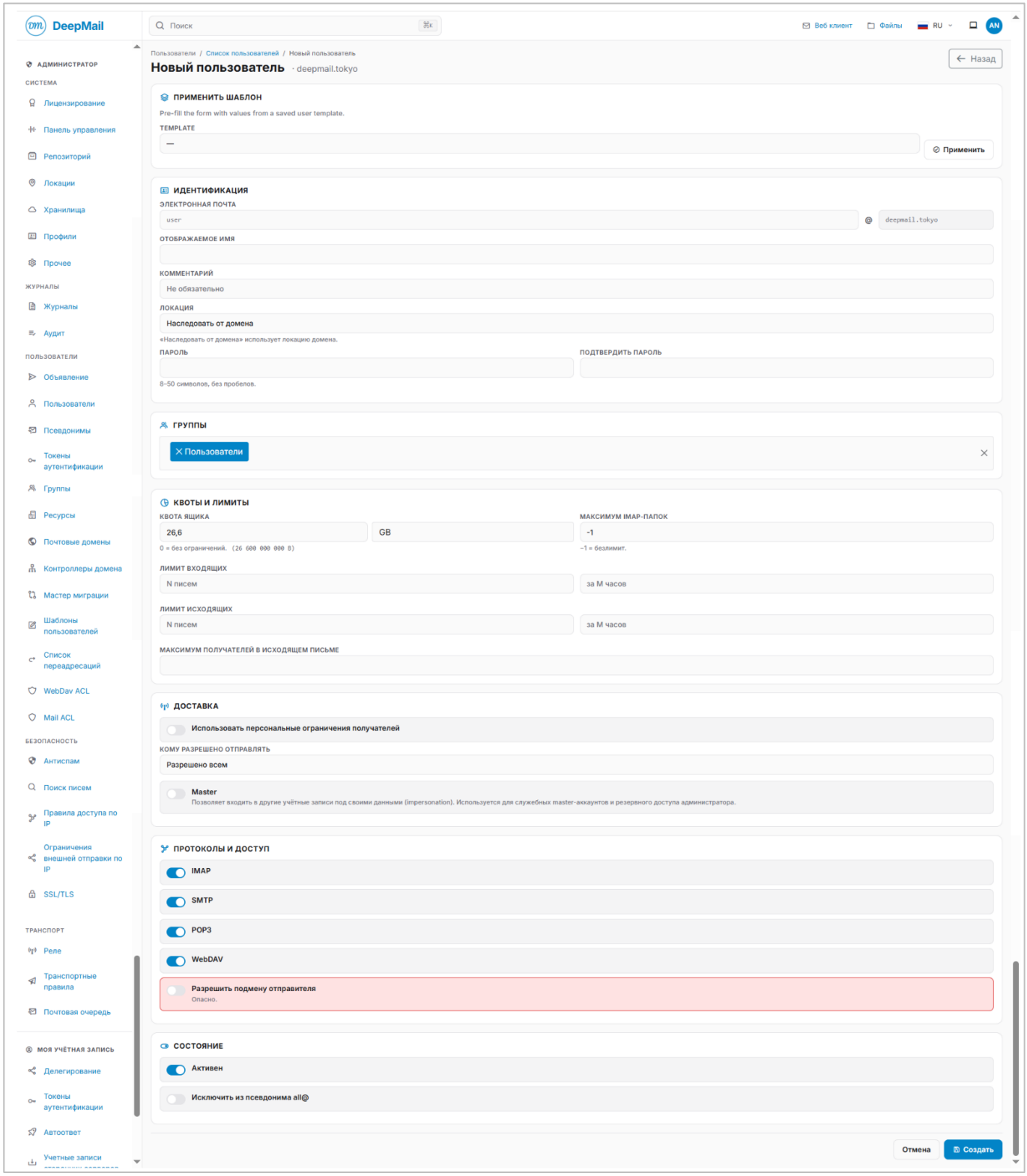


Рисунок 68 – Форма добавления нового пользователя

Примечание: Форма откроется только если у домена не превышен лимит количества пользователей. Если лимит превышен, откроется страница «Пользователи» со списком УЗ выбранного домена с сообщением «Слишком много пользователей для домена: <имя домена>».

Для автоматизации заполнения параметров, например при добавлении множества пользователей, для которых необходимо установить типовой набор прав (квоты, лимиты и

протоколы подключений, к новой УЗ) можно применить предварительно созданный шаблон (подробнее про шаблоны пользователей см. в 3.4.10). Щелчком мыши в поле «TEMPLATE» выберите необходимый шаблон и нажмите кнопку 

(см. рисунок 68). Параметры настроек будут установлены в соответствии с выбранным шаблоном, останется только заполнить идентификационную информацию.

Блок «ИДЕНТИФИКАЦИЯ» (см. рисунок 68) – это ключевой блок, в котором указываются:

- ЭЛЕКТРОННАЯ ПОЧТА – email нового пользователя, заполняется локальная часть (логин), доменная часть установлена автоматически и не доступна для редактирования;
- ОТОБРАЖАЕМОЕ ИМЯ – имя, которое будет отображаться в переписке вместо email;
- ЛОКАЦИЯ – географическая принадлежность УЗ. По умолчанию наследуется от домена, но можно назначить индивидуально, выбрав из списка доступных (раскрывается щелчком мыши в поле);
- ПАРОЛЬ – пароль для первичного входа в систему, затем меняется пользователем самостоятельно;
- КОММЕНТАРИЙ – информационное поле (не обязательное к заполнению). В текстовое поле можно внести любую служебную информацию, связанную с почтовым ящиком – например, дату создания, ответственного сотрудника или особые условия использования.

В блоке «ГРУППЫ» (см. рисунок 68) указываются наименования групп (выбор из списка доступных), в которые будет входить пользователь и соответственно наследовать их права или получать соответствующие рассылки. По умолчанию для всех новых пользователей установлена группа «Пользователи».

Примечание: Группу «Глобальные администраторы» может установить только пользователь сам являющийся глобальным администратором.

Блок «КВОТЫ И ЛИМИТЫ» (см. рисунок 68) предназначен для установки следующих параметров:

- КВОТА ЯЩИКА – по умолчанию для всех новых пользователей автоматически устанавливается квота домена. При необходимости установите индивидуальное значение, в случае изменения доменной политики индивидуальная квота не изменится;

– МАКСИМУМ IMAP-ПАПОК – ограничение на количество почтовых папок, которые пользователь сможет создать самостоятельно (значение -1 означает отсутствие ограничений);

– ЛИМИТ ВХОДЯЩИХ – ограничение количества входящих сообщений, которые смогут поступать в почтовый ящик пользователя за определенный временной промежуток (*n* входящих писем за *m* часов);

– ЛИМИТ ИСХОДЯЩИХ – ограничение количества исходящих сообщений, которые пользователь сможет отправлять за определенный временной промежуток (*n* исходящих писем за *m* часов);

– МАКСИМУМ ПОЛУЧАТЕЛЕЙ В ИСХОДЯЩЕМ ПИСЬМЕ – ограничение максимального количества адресов, которые пользователь сможет добавить в поле «Кому» в одном исходящем письме.

В блоке «ДОСТАВКА» (см. рисунок 68) устанавливаются следующие настройки:

– чекбокс «Использовать персональные ограничения получателей» включает для пользователя индивидуальные ограничения перекрывая доменные;

– поле «КОМУ РАЗРЕШЕНО ОТПРАВЛЯТЬ» предназначено для выбора политики ограничения отправки почты – либо «РАЗРЕШЕНО ВСЕМ» (на любой электронный адрес), либо «ТОЛЬКО ВНУТРИ СИСТЕМЫ» (только на электронные адреса пользователей всех доменов, либо «ТОЛЬКО ВНУТРИ ДОМЕНА» (только на электронные адреса пользователей домена, к которому принадлежит УЗ);

– чекбокс «MASTER» – делает УЗ привилегированным master-аккаунтом с правами суперпользователя, которому позволено входить в почтовые ящики пользователей под своими учетными данными (обычно применяется для служебных ящиков и для резервного доступа администраторов).

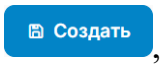
Блок «ПРОТОКОЛЫ И ДОСТУП» (см. рисунок 68) предназначен для выбора протоколов, в соответствии с которыми пользователю будет доступен функционал почтовой системы. Например, если пользователю не требуется доступ к календарям и адресным книгам, то включать чекбокс «WebDAV» не надо.

Администратор может разрешить пользователю редактировать электронный адрес отправителя в создаваемых исходящих письмах, для этого необходимо включить чекбокс «Разрешить подмену отправителя» (см. рисунок 68).

Важно! Применение функционала разрешения подмены отправителя может быть опасным! Включайте данную настройку только доверенным пользователям и в случае крайней необходимости.

Блок «СОСТОЯНИЕ» (см. рисунок 68) предназначен для включения следующих параметров:

- чекбокс «АКТИВЕН» – активирует (если включен) или блокирует (если выключен) УЗ пользователя (подробнее см. в 3.4.2.3);
- чекбокс «Исключить из псевдонима all@» – исключает адрес пользователя из группы псевдонима (алиаса) «all@<домен>». Это означает, что пользователю не будут направляться копии писем, адресованные «всем» (участникам группы «all»).

После заполнения всех необходимых параметров нажмите кнопку 

, для отказа от создания нового пользователя нажмите кнопку

(см. рисунок 68).

Система применяет настройки без необходимости перезагрузки сервисов, что обеспечивает оперативность администрирования.

3.4.2.2 Редактирование данных пользователей

Чтобы отредактировать данные или выполнить дополнительные настройки УЗ пользователей необходимо нажать в таблице со списком пользователей в строке выбранного пользователя кнопку  (см. рисунок 66).

Откроется форма «Изменить пользователя» (рисунок 87).

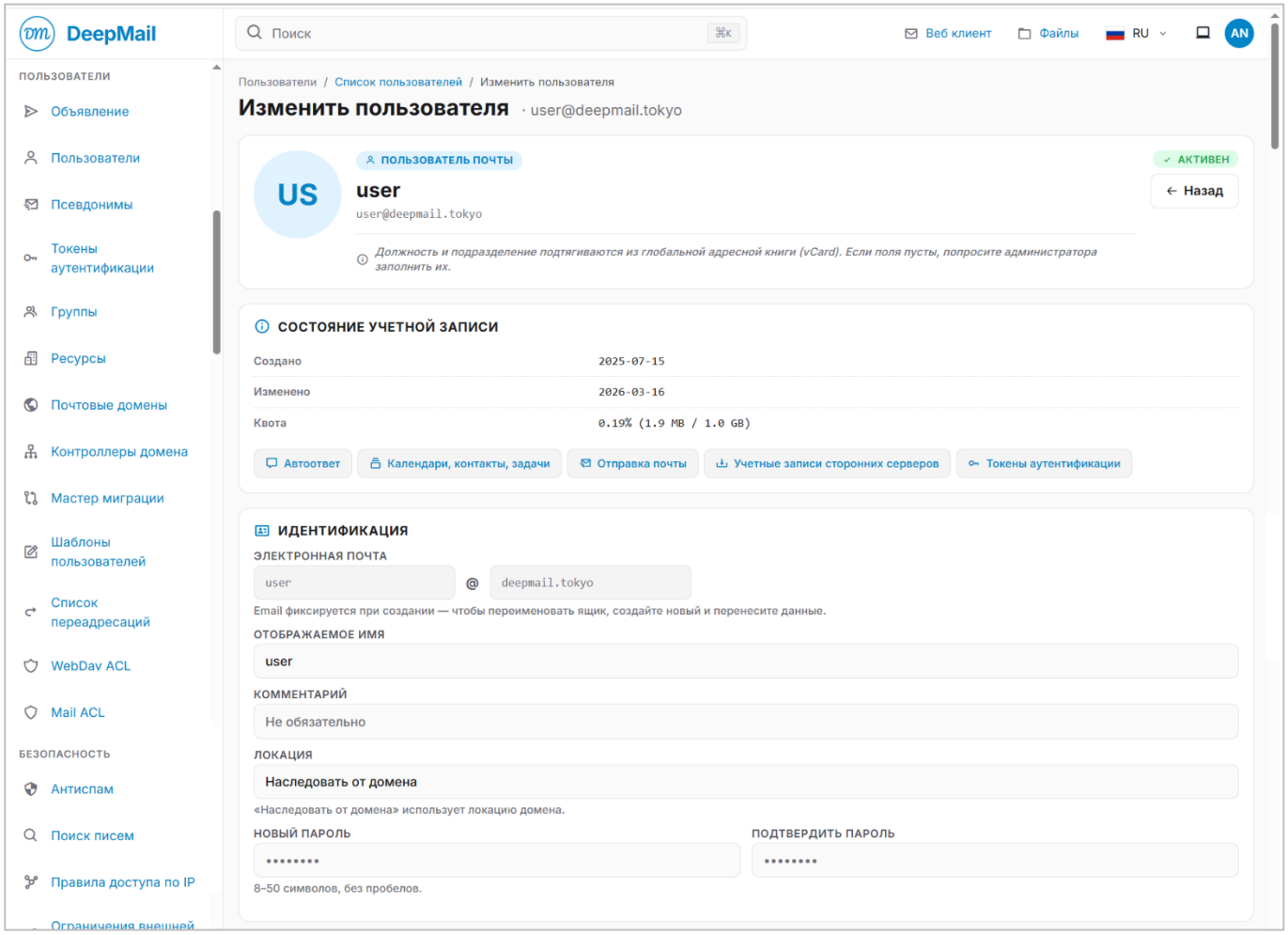


Рисунок 69 – Форма «Изменить пользователя»

Важно! Электронный адрес пользователя отредактировать нельзя, он фиксируется при создании УЗ. Чтобы переименовать почтовый ящик необходимо создать новую УЗ пользователя и перенести данные.

Помимо первоначальных параметров доступных для настройки УЗ при добавлении пользователя (см. 3.4.2.1) в данной форме присутствуют дополнительные блоки расширенных настроек.

В интерфейсе редактирования учетной записи пользователя блок «СОСТОЯНИЕ УЧЕТНОЙ ЗАПИСИ» (см. рисунок 87) 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 УЗ, дата внесения изменений в учетные данные. Ниже приводятся значения использования квоты, показывая какой объем дискового пространства уже занят письмами, а какой остается доступным. Основное значение выводится в процентах, в скобках указано значение в байтах из X доступных (например,

80.1 kB / 1.0 GB), что позволяет быстро оценить, не приближается ли ящик к установленному лимиту. Также в этом блоке доступны функциональные кнопки:

- Автоответ – установка автоматических ответов на время занятости (отсутствия) пользователя (описание управления автоответами приведено в 3.7.3);
- Календари, контакты, задачи – переход к управлению коллекциями (календари, контакты, задачи) – администратор может добавить или удалить календарь, адресную книгу или папку задач пользователя, а также выдать доступ к данным коллекций редактируемой УЗ другим пользователям (описание управления коллекциями приведено в 3.7.5);
- Отправка почты – переход к настройкам делегирования прав на отправку почты от имени пользователя, чья УЗ выбрана на редактирование (Описание добавления приведено в 3.7.1.2 3.7.2);
- Учетные записи сторонних серверов – переход к добавлению УЗ сторонних серверов, при их наличии у пользователя (например УЗ сервера Yandex, Gmail и т.п) (описание добавления УЗ сторонних серверов приведено в 3.7.4);
- Токены аутентификации – переход к управлению токенами аутентификации (описание настроек токенов аутентификации приведено в 3.7.2).

Важно! Нажимая перечисленные кнопки в интерфейсе редактирования УЗ пользователей, администратор переходит к инструментам управления именно УЗ выбранного на редактирование пользователя – в раздел «Моя учетная запись» редактируемого пользователя и выполняет настройки от его лица. Это необходимо в случае, если политика безопасности предприятия запрещает выполнение подобных настроек обычным пользователям самостоятельно, но применение данного функционала востребовано при работе сотрудников. Переход к инструментам настройки таких же параметров собственной УЗ администратора выполняется нажатием кнопок в разделе «Моя учетная запись» в панели управления (см. 3.7).

Блок «ДВУХФАКТОРНАЯ АУТЕНТИФИКАЦИЯ» предназначен для мониторинга и административного управления дополнительным уровнем защиты почтового ящика (рисунок 70).

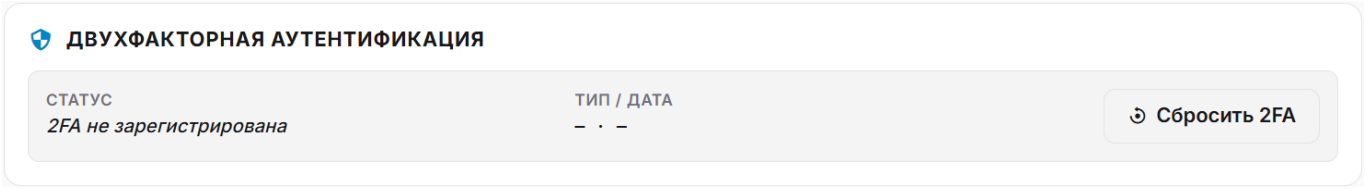
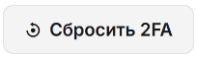


Рисунок 70 – Блок «ДВУХФАКТОРНАЯ АУТЕНТИФИКАЦИЯ»

Здесь администратор видит текущее состояние двухфакторной аутентификации: сообщение «2FA не зарегистрирована» указывает на то, что пользователь еще не настроил одноразовые коды, либо настройка была сброшена. Когда двухфакторная аутентификация активна, в столбце «ТИП / ДАТА» отображается соответствующая информация о типе зарегистрированной 2FA и дата, когда была выполнена регистрация (например, «TOTP · 21 May 2026, 17:48»).

Включение необходимости применения 2FA для УЗ пользователя при входе в почтовый ящик активируется политикой группы, в которой состоит пользователь – т.е. УЗ должна быть добавлена в группу, для которой настроена политика 2FA (настройку 2FA см. в 3.4.5.1.2).

Кнопка 

позволяет администратору принудительно перезагрузить двухфакторную аутентификацию для данного почтового ящика. Это необходимо, если пользователь потерял QR-код, 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 дает администратору централизованный контроль над доступом, позволяя быстро восстанавливать УЗ без потери данных, сохраняя при этом общую политику безопасности.

В блоке «АНТИСПАМ» включается антиспам-фильтр, необходимость отметки спам-сообщений прочитанными, а также устанавливается порог спама (чем меньше значение указано, тем более агрессивно выполняется фильтрация) (рисунок 71).



Рисунок 71 – Блок «АНТИСПАМ»

В блоке «АВТОПЕРЕСЫЛКА» настраиваются параметры переадресации писем, поступающих в адрес редактируемого пользователя (рисунок 72).



Рисунок 72 – Блок «АВТОПЕРЕСЫЛКА»

Для настройки включите чекбокс «Включить переадресацию», укажите адреса получателей, на которые необходимо пересылать входящую почту пользователя, а также при необходимости сохранения копии писем в папке «Входящие» включите чекбокс «Оставлять копию во входящих».

После внесения необходимых изменений и дополнительных настроек нажмите кнопку Сохранить. Для отмены изменений нажмите кнопку Отмена.

3.4.2.3 Блокировка пользователей

Администратор может заблокировать УЗ пользователей системы (включая LDAP-синхронизированные). УЗ общих почтовых ящиков и УЗ ресурсов не подлежат блокировке, из можно только удалить.

При блокировке УЗ продолжает существовать в системе, но пользователь такой УЗ не сможет авторизоваться в почтовую систему.

Для блокировки УЗ необходимо открыть форму редактирования, нажав в таблице со списком пользователей в строке выбранного пользователя кнопку (см. рисунок 66).

В открывшейся форме «ИЗМЕНИТЬ ПОЛЬЗОВТЕЛЯ» при помощи прокрутки колеса мыши перейти в блок «СОСТОЯНИЕ» и выключить чекбокс «АКТИВЕН» (см. рисунок 68).

Затем нажмите кнопку Сохранить. Форма редактирования закроется, статус пользователя в таблице изменится с ✓ АКТИВЕН на ⦸ ЗАБЛОКИРОВАН (см. рисунок 66).

Для разблокировки пользователя необходимо нажать кнопку 

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

.

3.4.2.4 Удаление пользователя

Для удаления пользователя необходимо нажать в таблице со списком пользователей в строке выбранного пользователя кнопку  (см. рисунок 66)., и подтвердить удаление в открывшемся модальном окне (рисунок 73).

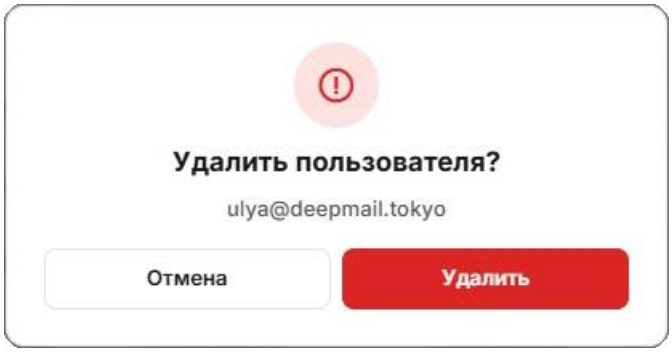


Рисунок 73 – Модальное окно подтверждения удаления УЗ пользователя

3.4.2.5 Добавление общего почтового ящика

Общий почтовый ящик – это УЗ виртуального пользователя с внутренним признаком *sharedmailbox*. Пользователи, которым предоставлен доступ к общему почтовому ящику, видят всю входящую почту, направленную в его адрес, а также могут отправлять письма от имени общего почтового ящика.

Для добавления УЗ общего почтового ящика необходимо на странице «Список пользователей» нажать кнопку 

(см. рисунок 66), раскроется выпадающее меню со списком доступных доменов (рисунок 74).

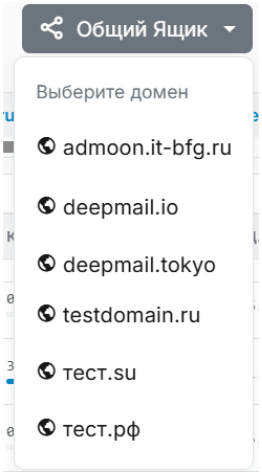


Рисунок 74 – Список доменов при добавлении общего ящика

Выберите необходимый домен, после чего откроется форма добавления нового общего ящика с привязкой к выбранному ранее домену (рисунок 75).

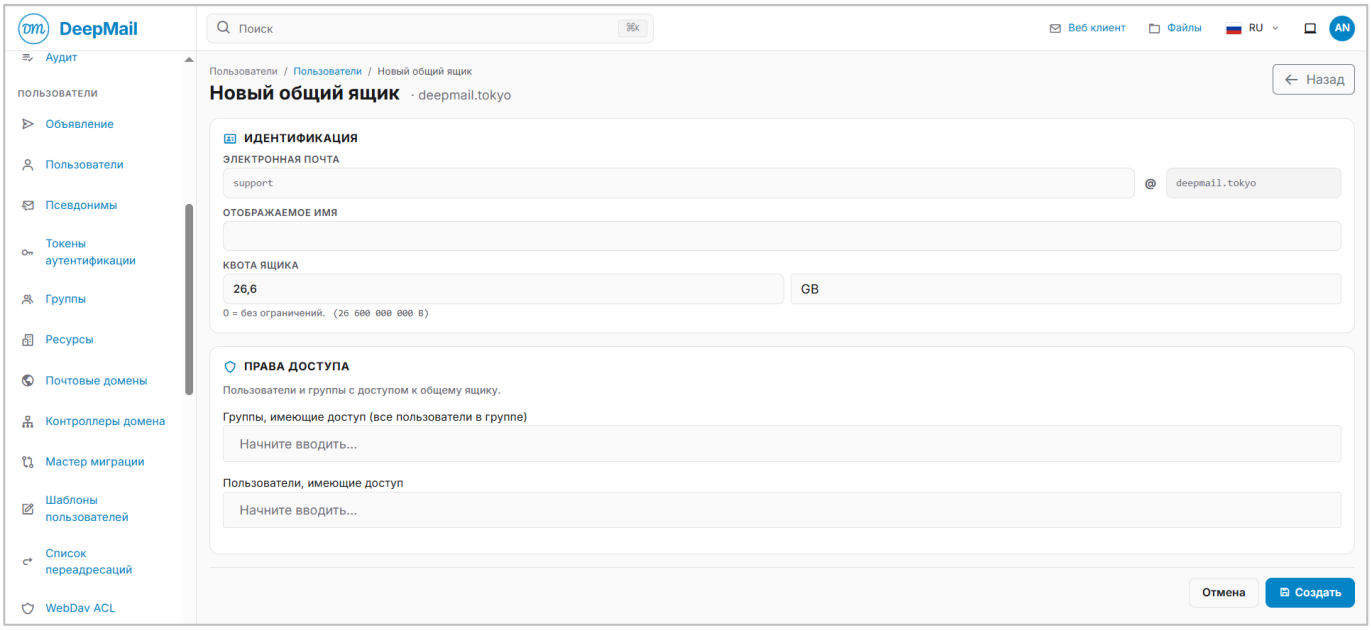


Рисунок 75 – Форма добавления нового общего ящика

В форме два блока для заполнения:

1) «ИДЕНТИФИКАЦИЯ» – заполните локальную часть (логин) электронной почты (доменная часть заполнена автоматически и недоступна для редактирования), отображаемое имя (имя почтового ящика, которое будет отображаться в переписке вместо email), укажите значение квоты почтового ящика (единицы квоты также доступны для выбора);

2) «ПРАВА ДОСТУПА» – выбор групп (все пользователи выбранной группы) и отдельных пользователей, которым будут предоставлены права доступа к создаваемому общему ящику. Начните вводить значения в соответствующие поля и система предложит список доступных вариантов.

После заполнения всех необходимых параметров нажмите кнопку Создать, для отказа от создания нового общего ящика нажмите кнопку Отмена (см. рисунок 75).

Созданный общий почтовый ящик появится в таблице на странице «Список пользователей». В столбце «ТИП» УЗ общих почтовых ящиков помечены иконкой SHARED (см. рисунок 66).

3.4.2.6 Редактирование и удаление общих почтовых ящиков

Чтобы отредактировать данные или выполнить дополнительные настройки УЗ общего почтового ящика необходимо нажать в таблице со списком пользователей в строке выбранного ящика кнопку (см. рисунок 66).

Откроется форма «Изменить общий ящик» (рисунок 76).

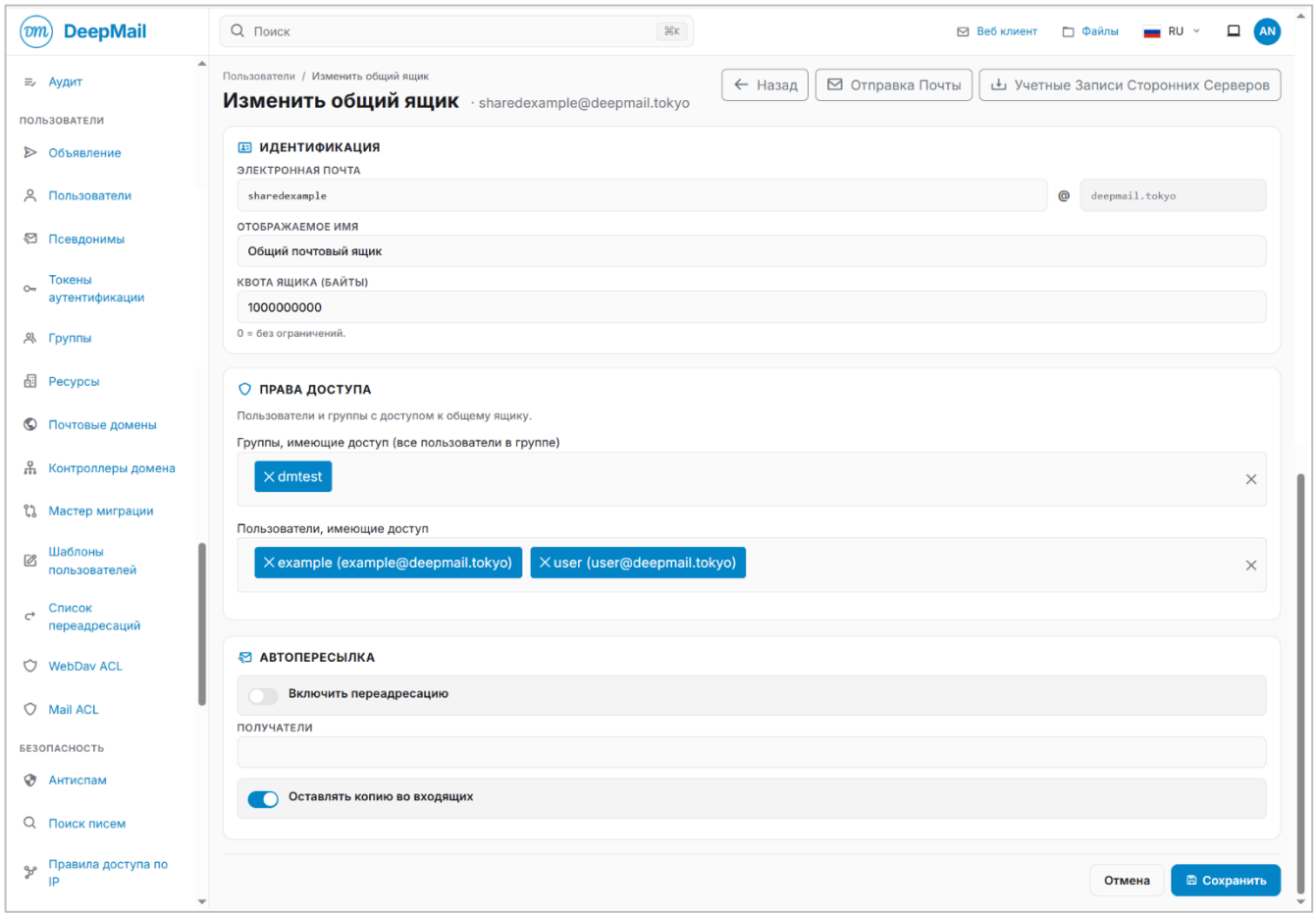


Рисунок 76 – Форма «Изменить общий ящик»

В отличие от редактирования пользователей электронную почту общего ящика можно отредактировать (локальную часть).

В данной форме дополнительно к первоначальным настройкам, доступным при создании нового общего ящика (см. 3.4.2.5), добавлен блок «АВТОПЕРЕСЫЛКА», в котором можно включить переадресацию писем на адреса определенных получателей, если необходимо оставлять копию в папке «Входящие» общего ящика, то включите соответствующий чекбокс.

Также в верхней части страницы редактирования общего ящика размещены кнопки:

– Отправка Почты – переход к настройкам делегирования прав на отправку почты от имени общего ящика, УЗ которого выбрана на редактирование;

– Учетные Записи Сторонних Серверов – переход к добавлению УЗ сторонних серверов, например если у общего почтового ящика есть УЗ сервера Yandex, Gmail и т.п.

Важно! Нажимая перечисленные кнопки в интерфейсе редактирования УЗ общего ящика, администратор переходит к инструментам управления именно настройками выбранного на редактирование ящика – в раздел «Моя учетная запись» редактируемого общего ящика и выполняет настройки «от его лица».

После внесения необходимых изменений и дополнительных настроек нажмите кнопку Сохранить. Для отмены изменений нажмите кнопку Отмена (см. рисунок 76).

Удаление общих почтовых ящиков выполняется аналогично удалению УЗ пользователей (см. 3.4.2.4).

3.4.3 Инструмент «Псевдонимы»

Сервер позволяет добавлять виртуальные почтовые адреса – псевдонимы (также называют алиасы) пользователю, нескольким пользователям или целой группе, при этом сообщения, приходящие на адрес псевдонима, будут автоматически отсылаться на все аккаунты, к которым он привязан. Фактически псевдоним не имеет собственного почтового ящика – он только маршрутизирует входящие сообщения.

Псевдоним также может быть создан для почтового домена, в DeepMail такие псевдонимы называются альтернативные домены. Управляются они из карточки конкретного домена (см. 2.4.7.5).

При выборе в меню админ-панели пункта «Псевдонимы» (см. рисунок 64) открывается страница «Псевдонимы», в которой отображена сводная информация о псевдонимах пользователей всех доменов почтовой системы (рисунок 77).

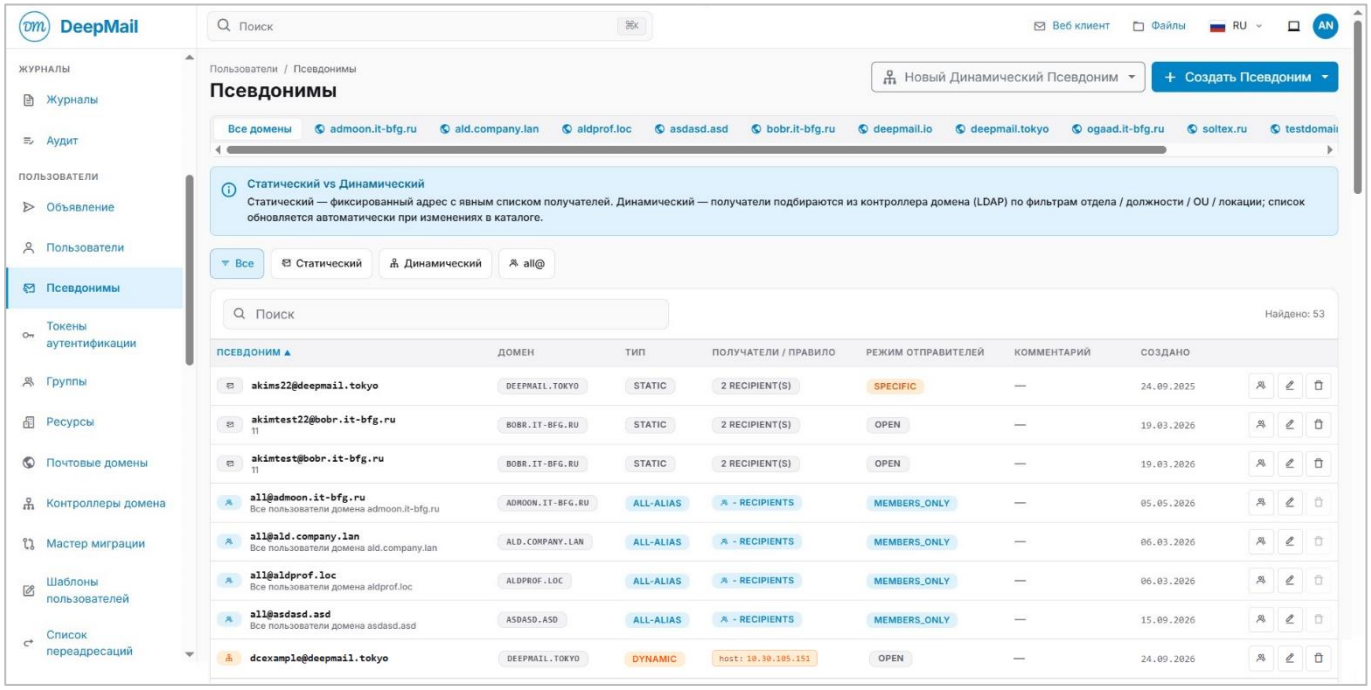


Рисунок 77 – Страница инструмента «Псевдонимы»

По умолчанию на странице отображается таблица со списком псевдонимов пользователей всех доменов почтовой системы. Для удобства администратору доступна система фильтрации:

- выбор конкретного домена для вывода списка пользователей на странице – нажмите на имя домена в строке с перечисленными доменами в верхней части страницы (например – deepmail.io, см. рисунок 77);

- выбор типа псевдонима – Статический (фиксированный адрес с конкретным списком получателей), Динамический (список получателей формируется на основе данных из контроллера домена) или all@ (алиасы «*all@<домен>*» – все пользователи домена) – нажмите соответствующую кнопку над таблицей (см. рисунок 77);

- сортировка списка псевдонимов по email (прямой или обратный алфавитный порядок) – нажмите на заголовок столбца ПСЕВДОНИМ ▲ (см. рисунок 77).

Также доступен поиск в списке (строка поиска над таблицей (см. рисунок 77), минимальный запрос – 3 символа).

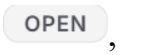
Для эффективного восприятия информации в столбцах таблицы (см. рисунок 77) отображаются различные графические иконки типов псевдонимов, получателей (правил) и режимов отправителей:

- ПСЕВДОНИМ –  (статический алиас),  (системный алиас),  (динамический алиас) – иконка рядом с именем псевдонима, символизирующая его тип;

- ДОМЕН – принадлежность к домену;

- ТИП –  (статический),  (динамический по фильтрам DC),  (системный (все пользователи домена));

- ПОЛУЧАТЕЛИ/ ПРАВИЛО –  (количество получателей пересылки), ,  (подключение к DC).

- РЕЖИМ ОТПРАВИТЕЛЕЙ – , ,  (кто может отправлять письма на адрес псевдонима).

Для просмотра списка пользователей подключенных к псевдониму необходимо нажать кнопку  в строке псевдонима в таблице (см. рисунок 77). Откроется страница «Участники псевдонима» со списком пользователей (рисунок 78).

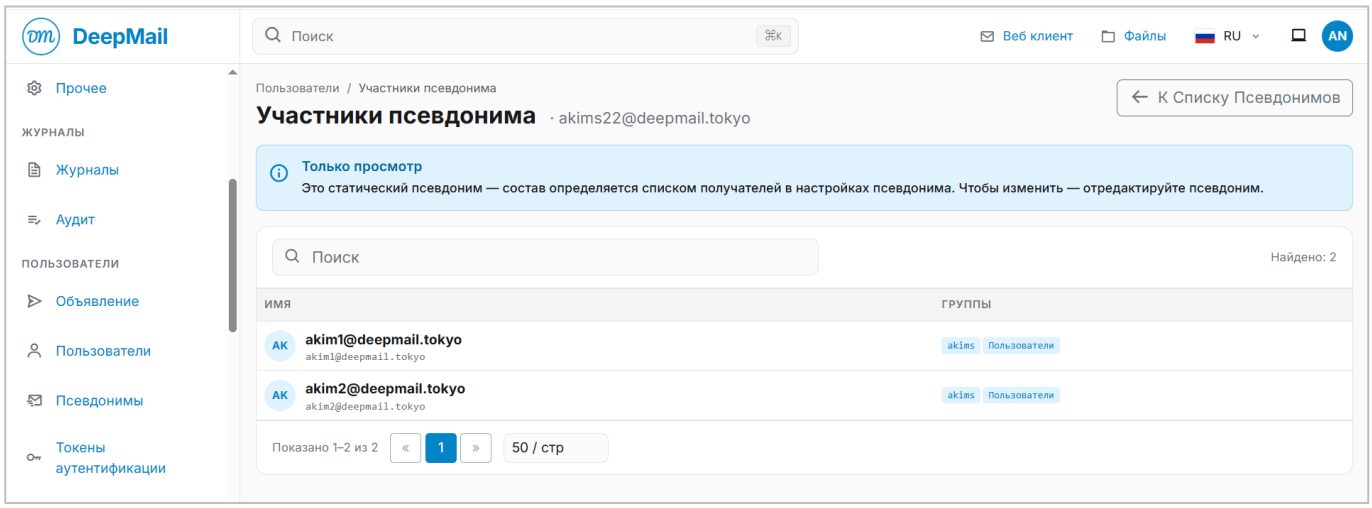


Рисунок 78 – Страница «Участники псевдонима»

Это нередактируемый список, предназначенный только для просмотра.

Функционал инструмента «Псевдонимы» позволяет администратору добавлять новые алиасы, редактировать их данные и удалять их из системы.

3.4.3.1 Системный псевдоним

Каждый добавленный в почтовую систему домен автоматически имеет встроенный алиас «*all@<domain>*». Письма, полученные на этот адрес, рассылаются всем активным пользователям домена, кроме тех, для кого в настройках (в форме добавления или при редактировании) включен параметр «Исключить из псевдонима all@» (см. 3.4.2.1).

В списке псевдонимов системный алиас помечен иконкой  (см. рисунок 77).

Удалить системный псевдоним нельзя, кнопка  для системных алиасов в списке псевдонимов неактивна (см. рисунок 77).

При редактировании таких псевдонимов изменить можно только отображаемое имя, режим отправителей и необходимость отображения его адреса в глобальной адресной книге.

3.4.3.2 Создание статического псевдонима

Статический псевдоним – алиас с конкретным списком получателей копий корреспонденции, который формируется вручную администратором при создании или редактировании псевдонима. Псевдоним может быть привязан как к одному, так и к нескольким пользователям. Можно указывать и внутренние и внешние (не сервера DeepMail) адреса.

В списке псевдонимов статический алиас помечен иконкой  (см. рисунок 77).

Для создания нового статического псевдонима нажмите на странице «Псевдонимы» кнопку 

(см. рисунок 77) и выберите в появившемся списке желаемый домен (рисунок 79).

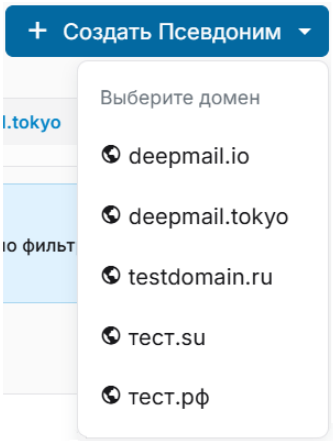


Рисунок 79 – Пример списка доступных доменов при создании статического псевдонима

Откроется форма создания нового статического псевдонима – «Создать псевдоним» (рисунок 80).

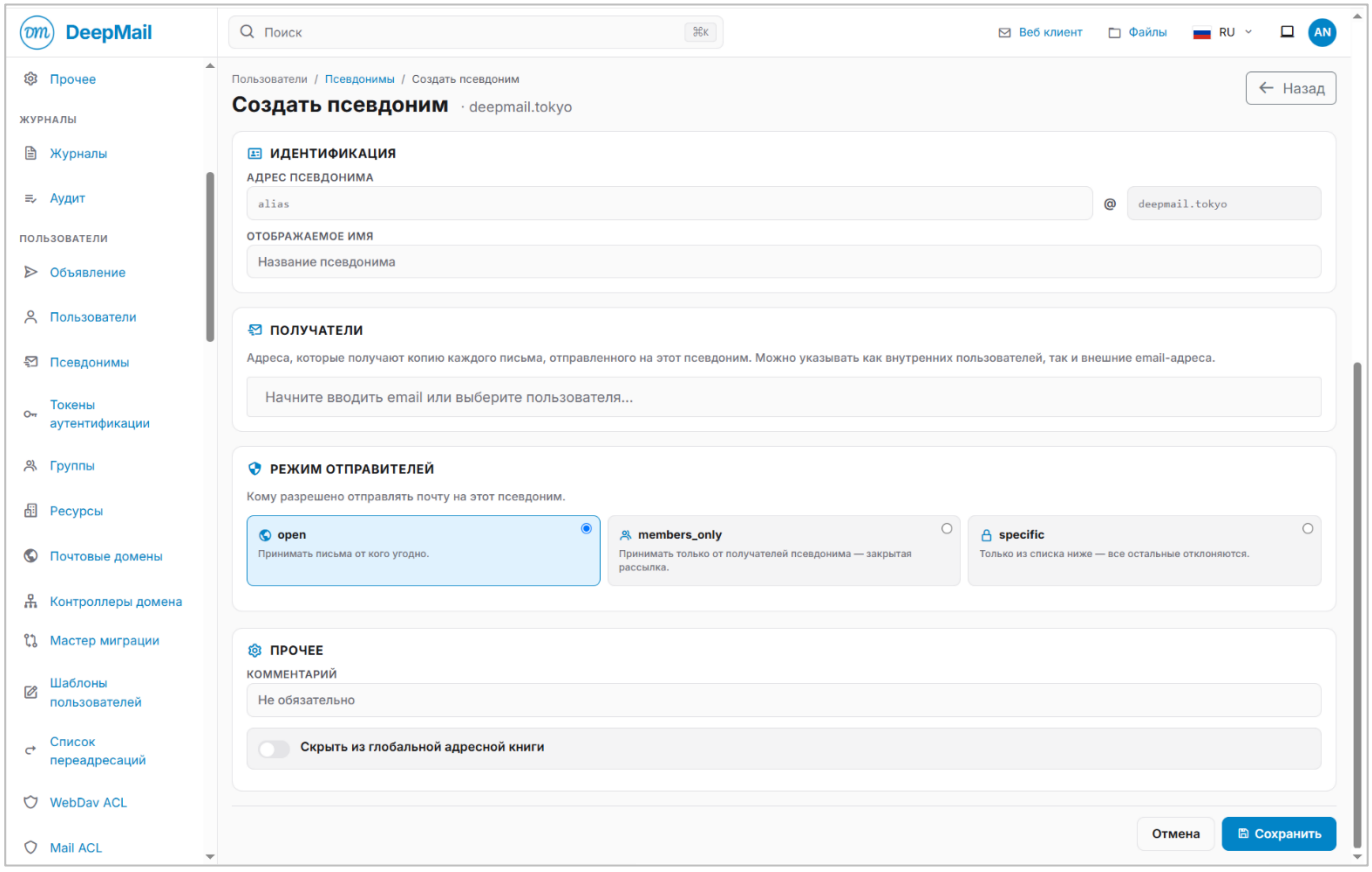


Рисунок 80 – Форма «Создать псевдоним»

Форма «Создать псевдоним» разделена на несколько функциональных блоков с полями для заполнения:

1) ИДЕНТИФИКАЦИЯ:

- поле «АДРЕС ПСЕВДОНИМА» – заполните локальную часть электронной почты псевдонима (доменная часть заполнена автоматически и недоступна для редактирования);
- поле «ОТОБРАЖАЕМОЕ ИМЯ» – имя виртуального почтового ящика, которое будет отображаться в переписке вместо email.

2) ПОЛУЧАТЕЛИ – электронные адреса, на которые будут отправляться копии писем, пришедшие на адрес псевдонима.

3) РЕЖИМ ОТПРАВИТЕЛЕЙ – выбор параметров для ограничения приема писем – «open» (система будет принимать письма в адрес псевдонима от любого пользователя), «members_only» (система будет принимать письма в адрес псевдонима только от его участников – закрытая рассылка), «specific» (система будет принимать письма в адрес псевдонима только от пользователей из списка разрешенных). При выборе режима «specific» в блоке появится дополнительное поле «РАЗРЕШЕННЫЕ ОТПРАВИТЕЛИ» для ввода адресов, которым будет разрешено отправлять письма в адрес псевдонима.

4) ПРОЧЕЕ – блок для ввода каких-либо комментариев к создаваемому псевдониму, а также для включения необходимости отображения или скрытия адреса псевдонима в глобальной адресной книге.

После ввода всех необходимых данных нажмите кнопку Сохранить. Для отмены нажмите кнопку Отмена (см. рисунок 80).

Созданный псевдоним отобразится в списке псевдонимов домена и также на странице домена будет отображено сообщение о создании псевдонима (рисунок 81).

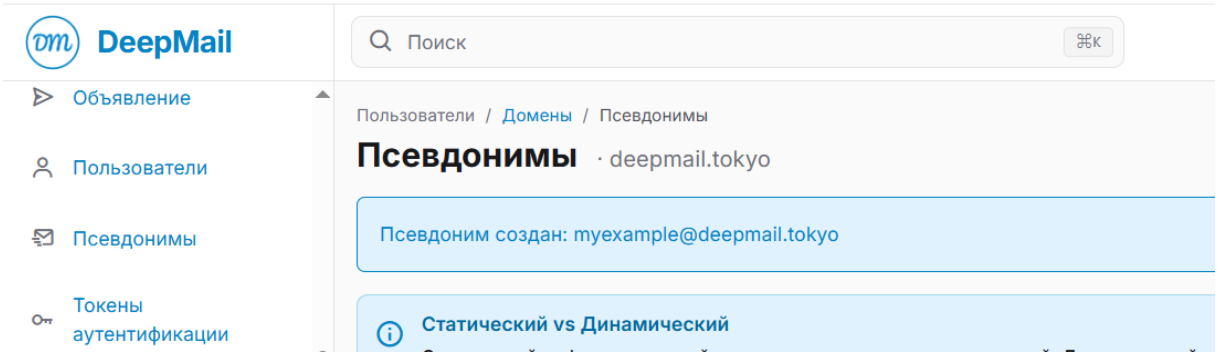


Рисунок 81 – Пример сообщения о создании псевдонима

3.4.3.3 Создание динамического псевдонима

Динамический псевдоним – алиас список получателей, которого формируется на основе данных из контроллера домена (протокол LDAP) на основе заданных фильтров (отделы, должности, локации и т.п.). Список обновляется автоматически при LDAP-синхронизации.

В списке псевдонимов динамический алиас помечен иконкой (см. рисунок 77).

Для создания нового динамического псевдонима нажмите на странице «Псевдонимы» кнопку Новый Динамический Псевдоним (см. рисунок 77) и выберите в появившемся списке желаемый домен (рисунок 82).

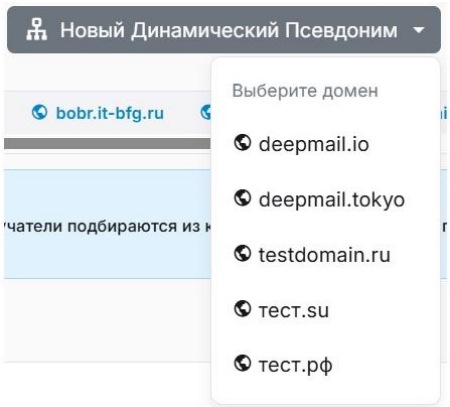


Рисунок 82 – Пример списка доступных доменов при создании динамического псевдонима

Откроется форма создания нового динамического псевдонима – «Создать динамический псевдоним» (рисунок 83).

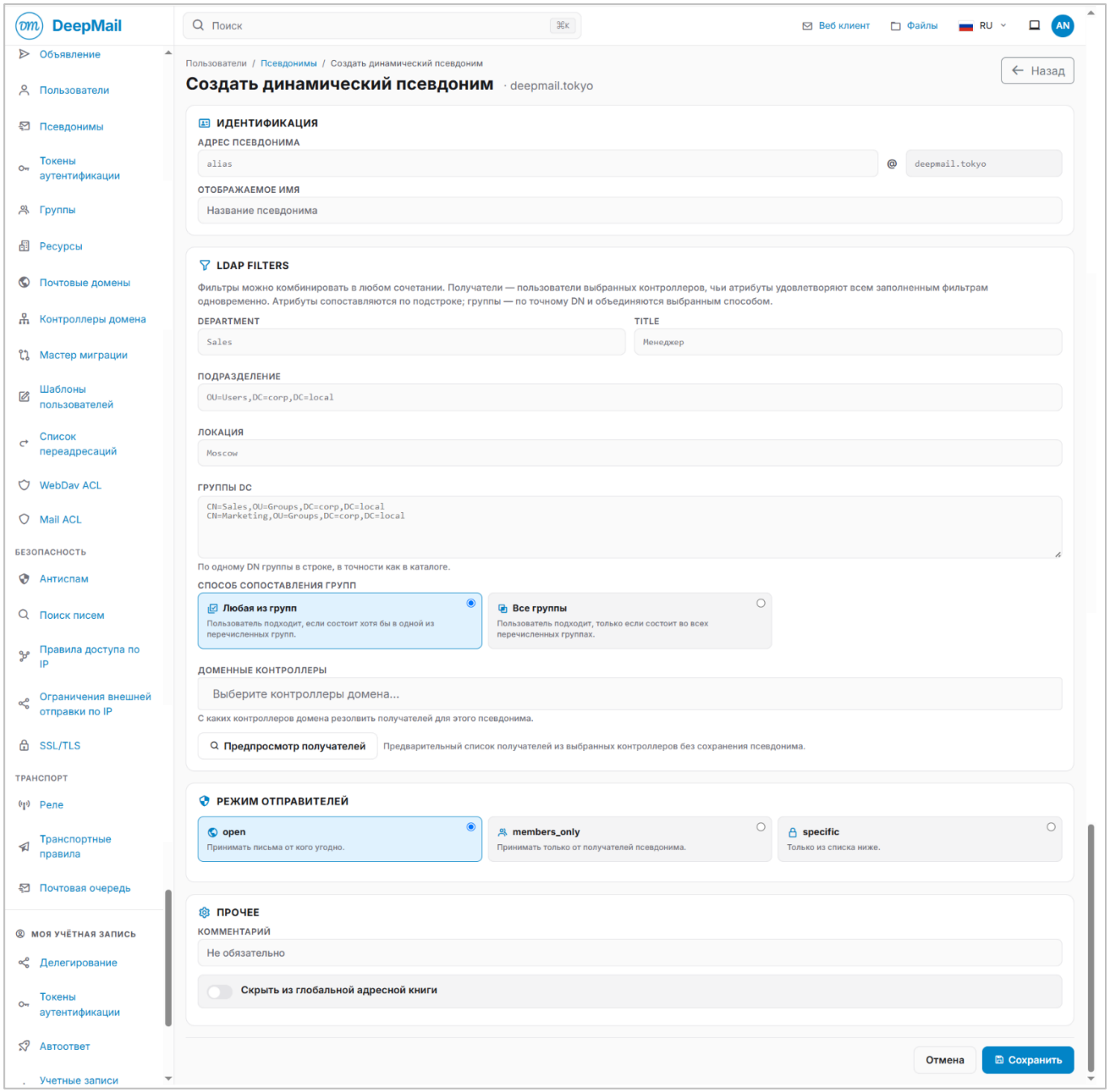


Рисунок 83 – Форма «Создать динамический псевдоним»

Форма «Создать динамический псевдоним» разделена на несколько функциональных блоков с полями для заполнения:

1) ИДЕНТИФИКАЦИЯ:

- поле «АДРЕС ПСЕВДОНИМА» – заполните локальную часть электронной почты псевдонима (доменная часть заполнена автоматически и недоступна для редактирования);
- поле «ОТОБРАЖАЕМОЕ ИМЯ» – имя виртуального почтового ящика, которое будет отображаться в переписке вместо email.

2) LDAP FILTERS: значения атрибутов (Department – отдел, Title – должность, Organizational unit – подразделение, Location – локация, Domain controllers – группы DC) в службе каталогов предприятия, в соответствии с которыми будут отбираться получатели подписанные на создаваемый псевдоним. Необходимо заполнить хотя бы одно из полей.

Тут же необходимо выбрать способ сопоставления групп DC – отметьте либо параметр «Любая из групп» (пользователь будет определен как подходящий, если он состоит хотя бы в одной из групп) либо параметр «Все группы» (пользователь будет определен как подходящий, если он состоит во всех перечисленных группах).

Затем необходимо выбрать конкретный контроллер для подключения выборки – при щелчке мыши в поле «ДОМЕННЫЙ КОНТРОЛЛЕР» раскроется список для выбора добавленных в систему контроллеров домена (добавление контроллера домена см. в 3.4.8.1).

Кнопка Предпросмотр получателей предназначена для проверки подключения к выбранному контроллеру домена и вывода предварительного списка получателей «ПОТЕНЦИАЛЬНЫЕ УЧАСТНИКИ», отобранных в соответствии с установленными фильтрами. При этом псевдоним пока не сохраняется в системе.

3) РЕЖИМ ОТПРАВИТЕЛЕЙ – выбор параметров для ограничения приема писем – «open» (система будет принимать письма в адрес псевдонима от любого пользователя), «members_only» (система будет принимать письма в адрес псевдонима только от его участников – закрытая рассылка), «specific» (система будет принимать письма в адрес псевдонима только от пользователей из списка разрешенных). При выборе режима «specific» в блоке появится дополнительное поле «РАЗРЕШЕННЫЕ ОТПРАВИТЕЛИ» для ввода адресов, которым будет разрешено отправлять письма в адрес псевдонима.

4) ПРОЧЕЕ – блок для ввода каких-либо комментариев к создаваемому псевдониму, а также для включения необходимости отображения или скрытия адреса псевдонима в глобальной адресной книге.

После ввода всех необходимых данных нажмите кнопку Сохранить. Для отмены нажмите кнопку Отмена (см. рисунок 83).

Созданный псевдоним отобразится в списке псевдонимов домена и также на странице домена будет отображено сообщение о создании псевдонима (рисунок 81).

3.4.3.4 Редактирование псевдонима

Чтобы отредактировать псевдоним необходимо в списке псевдонимов в строке выбранного алиаса нажать кнопку  (см. рисунок 77). Откроется форма редактирования псевдонима, соответствующая его типу, состоящая из тех же блоков и полей, что и форма создания псевдонима. Для редактирования доступны все поля кроме поля «АДРЕС ПСЕВДОНИМА».

После внесения необходимых изменений нажмите кнопку 

, для отмены нажмите кнопку

.

3.4.3.5 Удаление псевдонима

Чтобы отредактировать псевдоним необходимо в списке псевдонимов в строке выбранного алиаса нажать кнопку  (см. рисунок 77) и подтвердить действие в открывшемся модальном окне.

Кнопка удаления неактивна для системных псевдонимов.

3.4.4 Инструмент «Токены аутентификации»

Токен аутентификации – это уникальная зашифрованная строка символов, которая служит электронным «пропуском». Вместо того чтобы при каждом запросе отправлять логин и пароль (что небезопасно), клиент один раз получает токен после входа в систему и затем предъявляет его.

Токен – это альтернатива паролю для программного доступа:

- к IMAP/ SMTP/ CalDAV/ CardDAV/ SFTP-серверам – пользователь авторизуется, вводя email и токен вместо пароля;
- к HTTP API admin-service – при запросе на сервер токен будет в заголовке в заголовке Authorization: Bearer <token>.

Преимущества над паролем:

- соблюдение информационной безопасности;
- можно выпустить много токенов (разные приложения – разные токены);
- можно отозвать один токен не трогая другие;

– можно привязать к IP (Authorized IP) – токен будет валиден только отправленный с определенного источника;

– нет зависимости от смены пароля пользователя.

Инструмент админ-панели «Токены аутентификации» – глобальный список всех API-токенов в инсталляции с возможностью выпустить ADMIN-токен от имени любого пользователя.

Доступ к данному инструменту имеют только глобальные администраторы (рисунок 84).

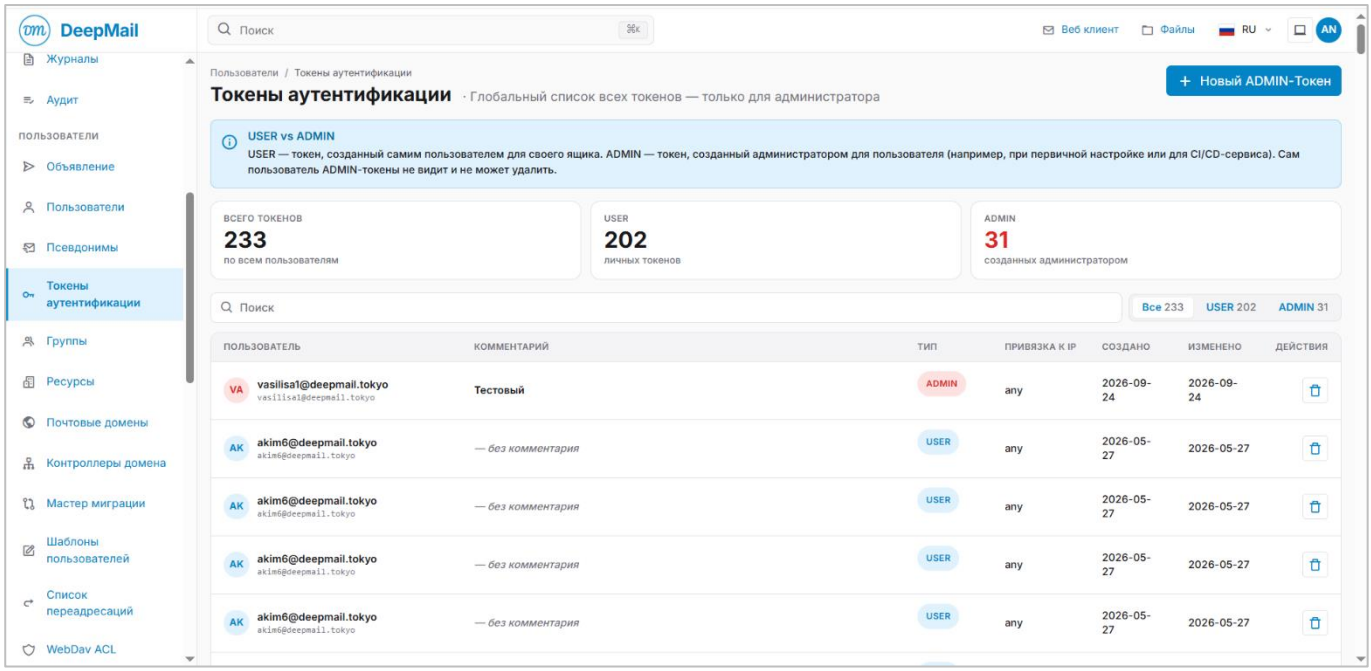


Рисунок 84 – Страница инструмента «Токены аутентификации»

DeepMail различает два типа токенов:

1) USER-токен – выпускает сам пользователь в своем клиенте («личном кабинете»). В списке инструмента администратора в столбце «ТИП» помечены иконкой USER (см. рисунок 84);

2) ADMIN-токен – выпускает глобальный администратор от имени любого пользователя через страницу инструмента «Токены аутентификации». Сам пользователь в своем личном кабинете этот токен не увидит. В списке инструмента администратора в столбце «ТИП» помечены иконкой ADMIN (см. рисунок 84).

Страница «Токены аутентификации» предоставляет администратору следующий функционал:

– обзор сводной информации – «ВСЕГО ТОКЕНОВ» (данные по всем пользователям), «USER» (личные токены пользователей, которые они добавили сами), «ADMIN» (токены пользователей созданные администратором);

– создание новых ADMIN-токенов – кнопка + Новый ADMIN-Токен;

– обзор списка пользователей, у которых имеются токены аутентификации. Для удобства над таблицей размещена строка поиска;

– удаление токенов аутентификации – кнопка в строке пользователя в списке.

3.4.4.1 Добавление токена аутентификации (новый ADMIN-токен)

Для добавления нового ADMIN-токена необходимо на странице «Токены аутентификации» нажать кнопку + Новый ADMIN-Токен (см. рисунок 84).

Откроется страница «Новый ADMIN-токен» (рисунок 85).

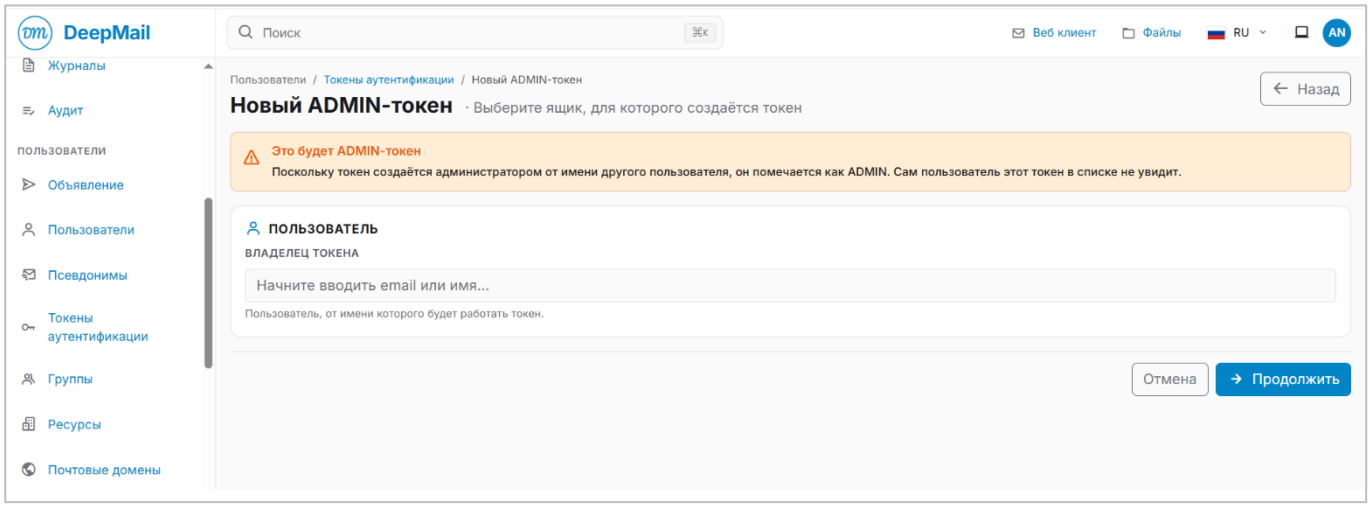


Рисунок 85 – Страница «Новый ADMIN-токен»

На данной странице необходимо выбрать пользователя, для которого будет создан токен – введите его email в поле «ВЛАДЕЛЕЦ ТОКЕНА» (при начале ввода система предлагает варианты, если совпадений нет, значит такого пользователя не существует) и затем нажмите кнопку → Продолжить.(см. рисунок 85).

После этого система выполнит переход на страницу «Создать токен аутентификации» для УЗ выбранного пользователя (рисунок 86).

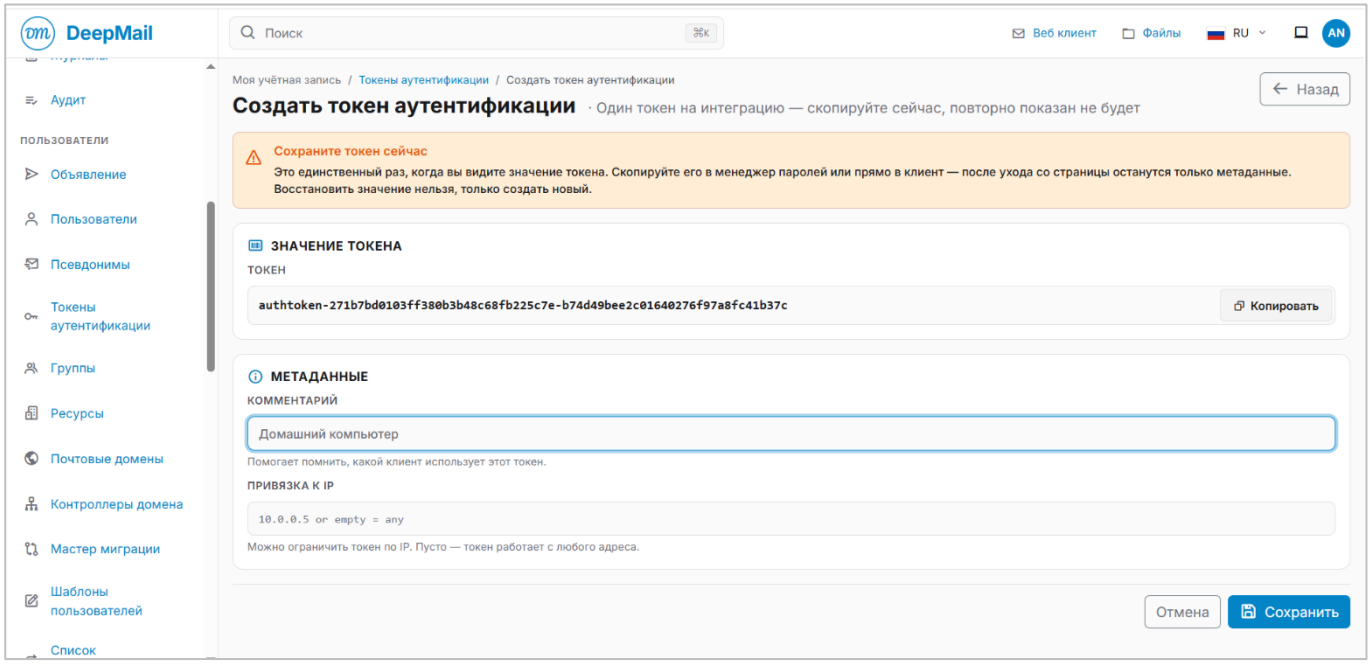


Рисунок 86 – Страница «Создать токен аутентификации»

На данной странице в блоке «ЗНАЧЕНИЕ ТОКЕНА» уже сгенерирован новый токен. Нажмите кнопку Копировать и сохраните значение для вставки в менеджер паролей или в клиентское приложение при аутентификации.

Важно! Восстановить токен нельзя! После ухода со страницы значение токена больше нигде не отображается, в записи останутся только метаданные. При утрате необходимо будет создать новый токен.

В блоке «МЕТАДАННЫЕ» можно внести комментарий, а также указать IP-адрес, к которому будет привязан токен, например если необходимо разрешить применение токена только на определенном устройстве. Если поле «ПРИВЯЗКА К IP» не заполнено, то токен будет работать на любом устройстве.

После сохранения токена и ввода необходимых данных нажмите кнопку Сохранить, для отмены нажмите кнопку Отмена (см. рисунок 86).

После этого будет открыта страница «Токены аутентификации» раздела «Моя учетная запись» пользователя, для которого был создан ADMIN-токен. Карточка созданного ADMIN-токена отмечена иконкой ADMIN (рисунок 87).

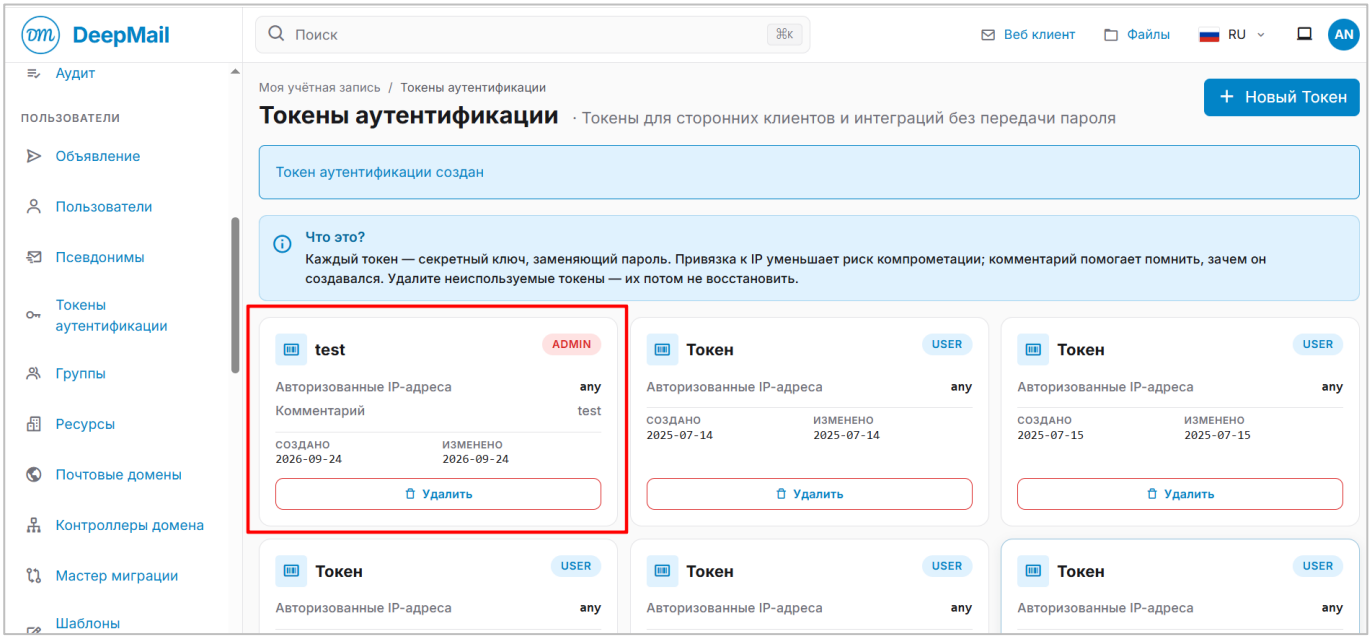


Рисунок 87 – Страница «Токены аутентификации» раздела «Моя учетная запись» пользователя/ карточка ADMIN-токена

3.4.4.2 Удаление токена аутентификации из глобального списка

Для удаления токена аутентификации из глобального списка токенов необходимо на странице инструмента «Токены аутентификации» в строке выбранного пользователя нажать кнопку  (см. рисунок 84) и затем подтвердить удаление.

3.4.5 Инструмент «Группы»

Инструмент «Группы» предоставляет администратору функционал управления группами пользователей. Группа в DeepMail – это контейнер прав и одновременно опциональный «рассылочный набор» (если включены общие коллекции). Пользователь может состоять в нескольких группах, при этом права всех групп пользователя объединяются.

Для перехода к инструменту «Группы» необходимо в меню админ-панели выбрать пункт «Группы» (см. рисунок 64).

В результате выбора на экране появится страница «Группы», содержащая список групп пользователей всех почтовых доменов (рисунок 88).

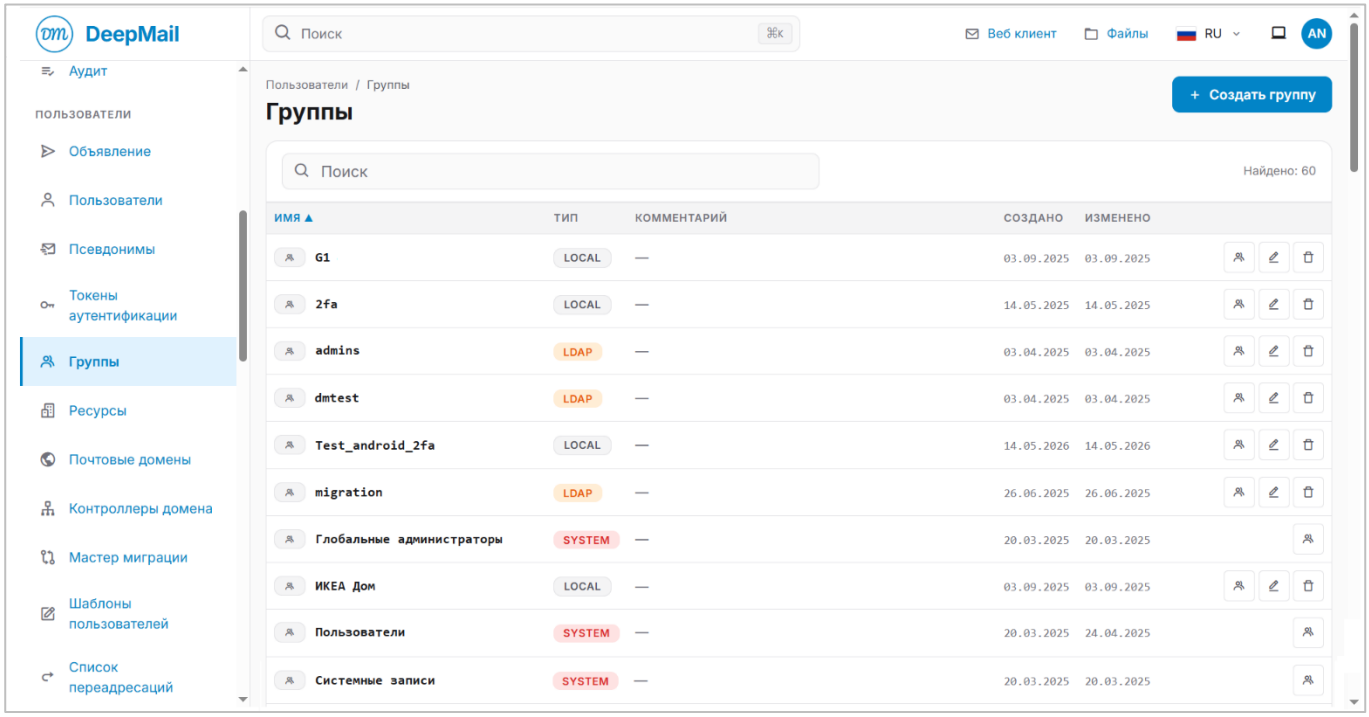


Рисунок 88 – Страница инструмента «Группы»

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 соответствии с системой прав (описание системы прав приведено в 3.4.5.1.1).

После инсталляции DeepMail имеет три системные группы:

– «Глобальные администраторы» (Global Admins) – для этой группы по умолчанию включен специальный параметр – «* – wildcard», который трактуется как «разрешено все». Удалять или снимать wildcard у этой группы нельзя. Любого участника этой группы система пускает в любой раздел и разрешает любое действие;

– «Пользователи» (Users) – группа, в которую по умолчанию включаются все новые УЗ. Никаких прав администрирования не несет – это просто обычный пользователь, со всеми личными правами;

– «Системные записи» (Shared mailbox marker) – техническая группа, в которую по умолчанию включаются общие почтовые ящики. В выпадающих списках UI она скрыта.

Все остальные группы создает администратор в инструменте «Группы» админ-панели.

3.4.5.1 Создание новой группы

Для создания новой группы на странице инструмента «Группы» нажмите кнопку + Создать группу. В результате откроется страница с формой создания группы (рисунок 89).

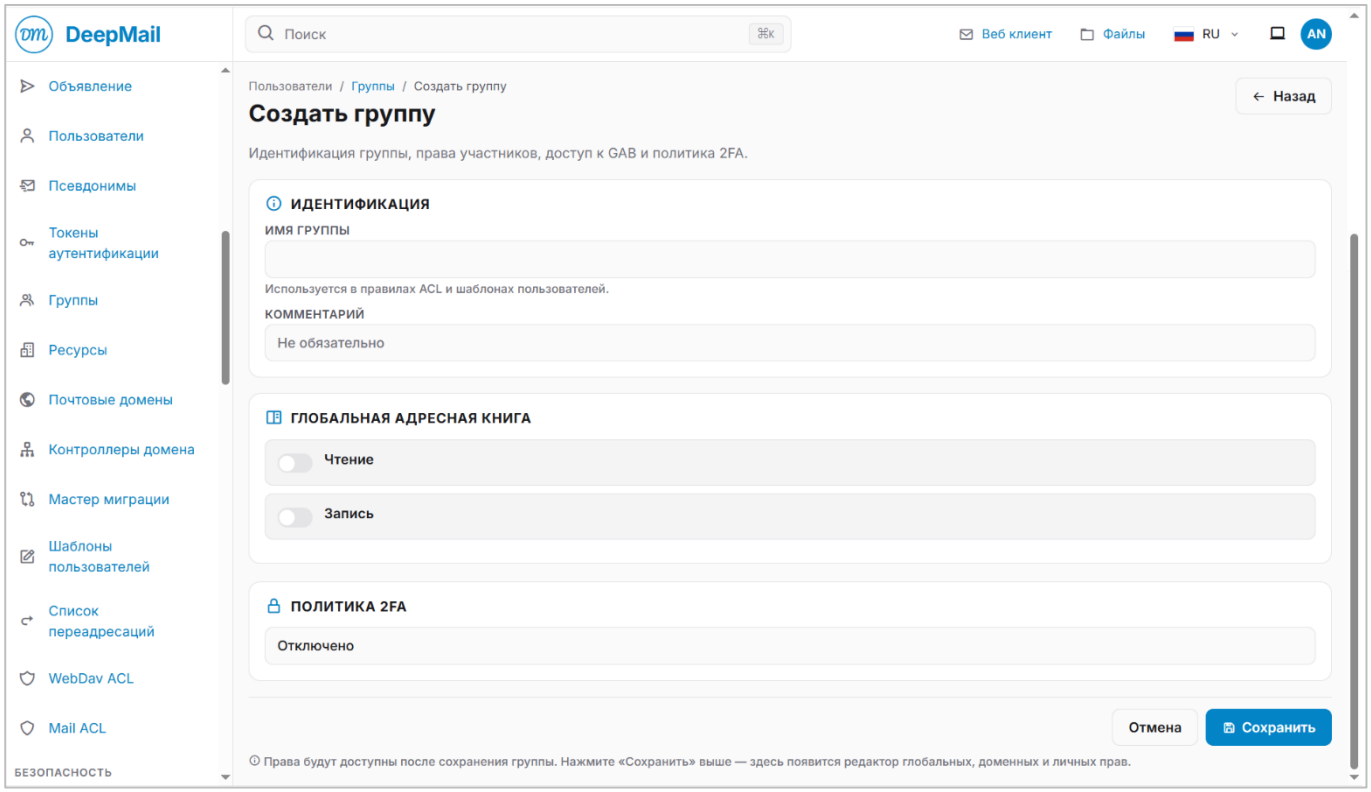


Рисунок 89 – Форма «Создать группу»

В форме «Создать группу» необходимо указать имя группы, комментарий, назначить права на доступ к глобальной адресной книге участникам группы, отметив соответствующие чек-боксы.

При необходимости включения пользователям дополнительной проверки при авторизации в почтовый ящик (двухфакторной аутентификации (подробнее про 2FA см. в 3.4.5.1.2)) в блоке «ПОЛИТИКА 2FA» щелкните в поле со значением «Отключено» и в выпадающем списке выберите значение «TOTP» (рисунок 90).

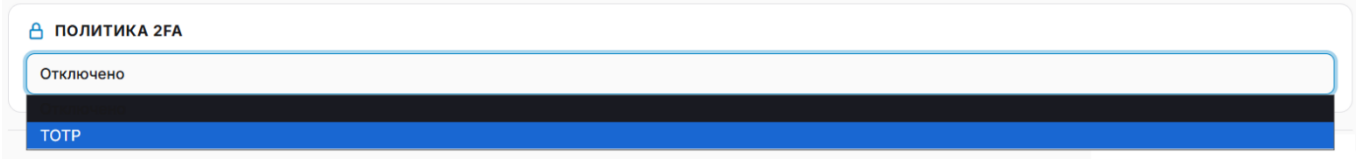
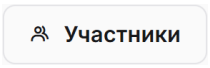


Рисунок 90 – Включение двухфакторной аутентификации

Это первоначальная форма с базовыми блоками, для дальнейшего добавления участников в группу и настройку глобальных, доменных и личных прав необходимо нажать кнопку 

(см. рисунок 89).

После этого откроется страница «Изменить группу», в которой дополнительно к базовым блокам появляется блок «ПРАВА УЧАСТНИКОВ» и кнопка добавления участников 

(рисунок 91).

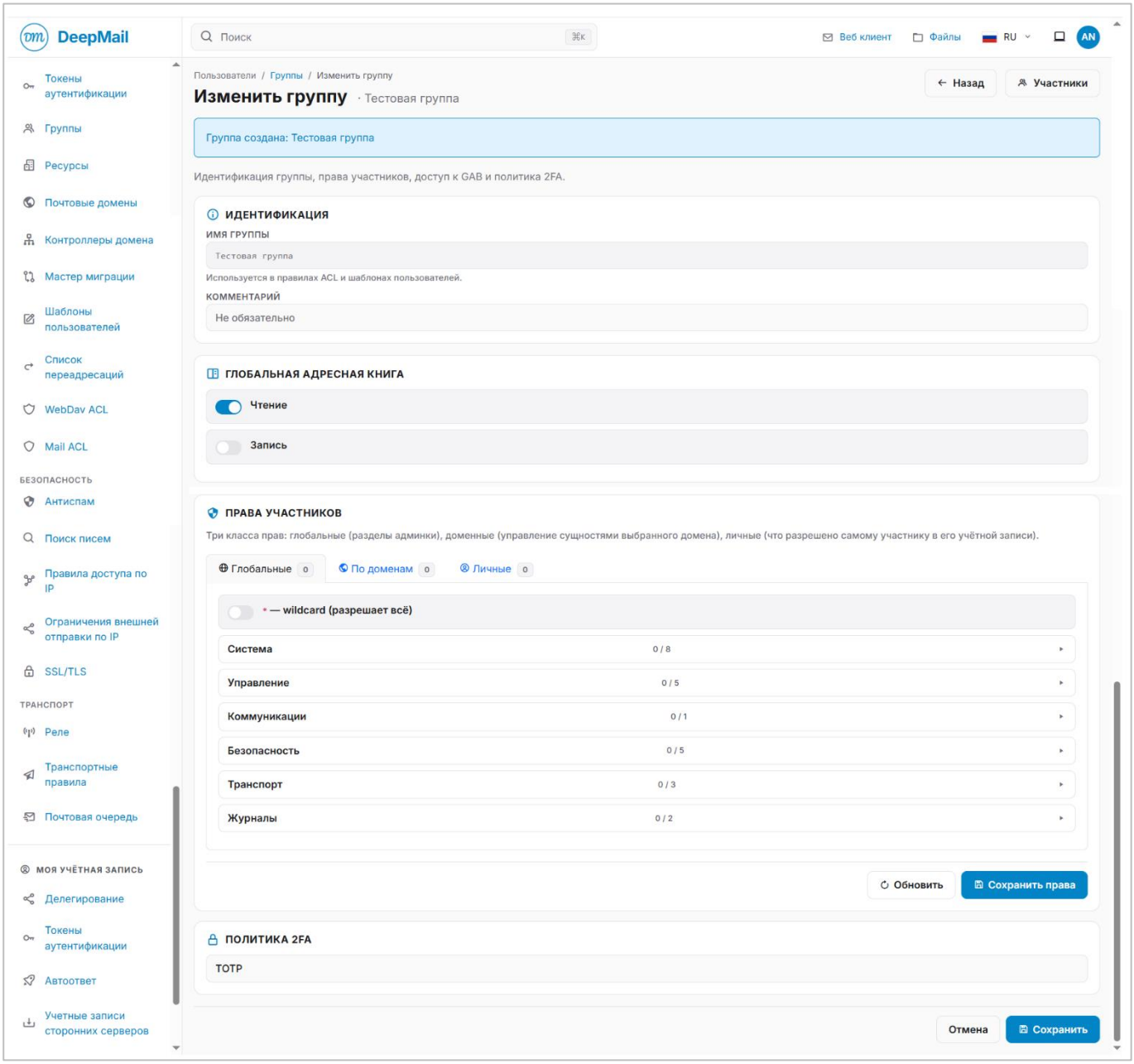


Рисунок 91 – Страница «Изменить группу»

В блоке «ПРАВА УЧАСТНИКОВ» три вкладки, которые соответствуют классу прав, реализованных в АРМ «DeepMail» (описание системы прав см. в 3.4.5.1.1). Рядом с названием каждой вкладки отображается счетчик количества прав, которые включены/ отключены в соответствии с правилами вкладки (изначально на всех 0) (рисунок 92).

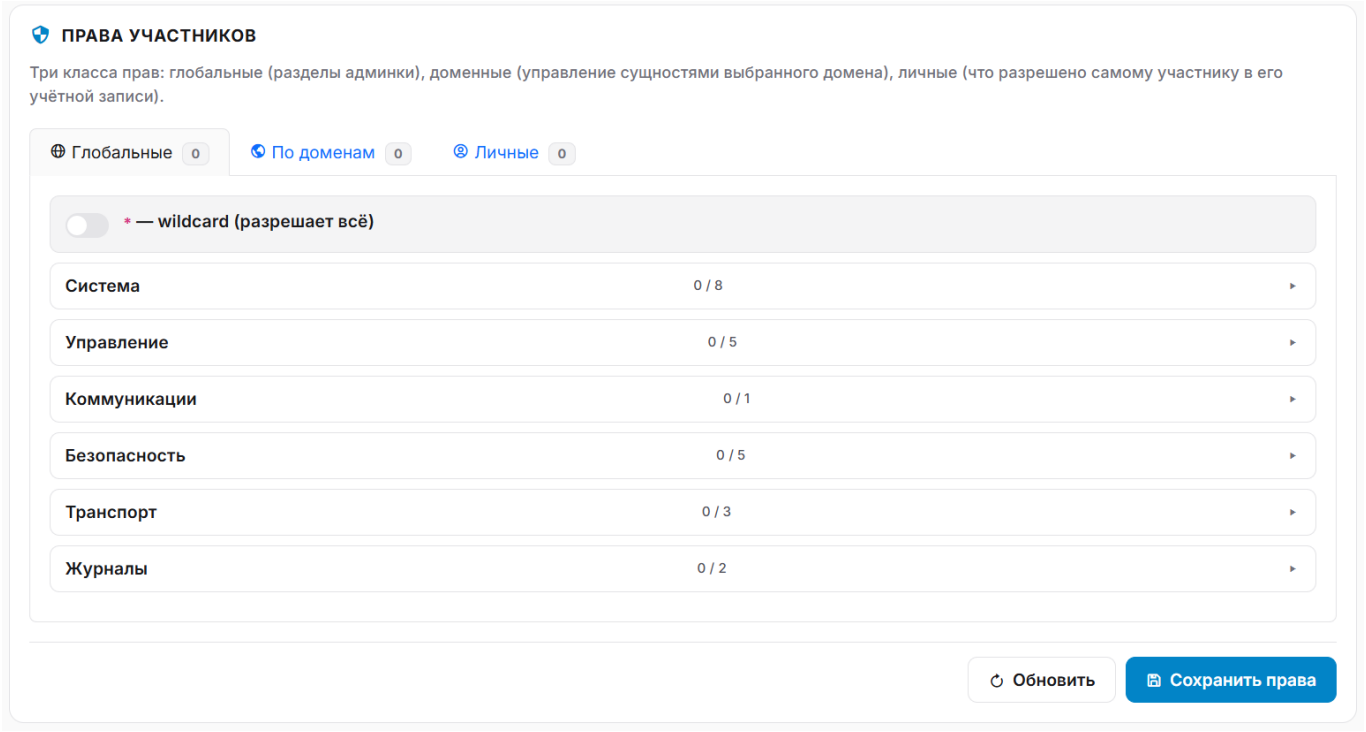


Рисунок 92 – Блок «ПРАВА УЧАСТНИКОВ»

На вкладке «Глобальные» все права по умолчанию отключены (в наименовании вкладки отображается 0 включенных (см. рисунок 92)).

Счетчик в каждой строке раздела (на рисунке 92 – 0/8, 0/5, 0/1 и т.д.) – это количество включенных прав к общему количеству прав в разделе. Для выбора прав разверните необходимый раздел, щелкнув мышью по его строке, и включите соответствующие чекбоксы (рисунок 93).

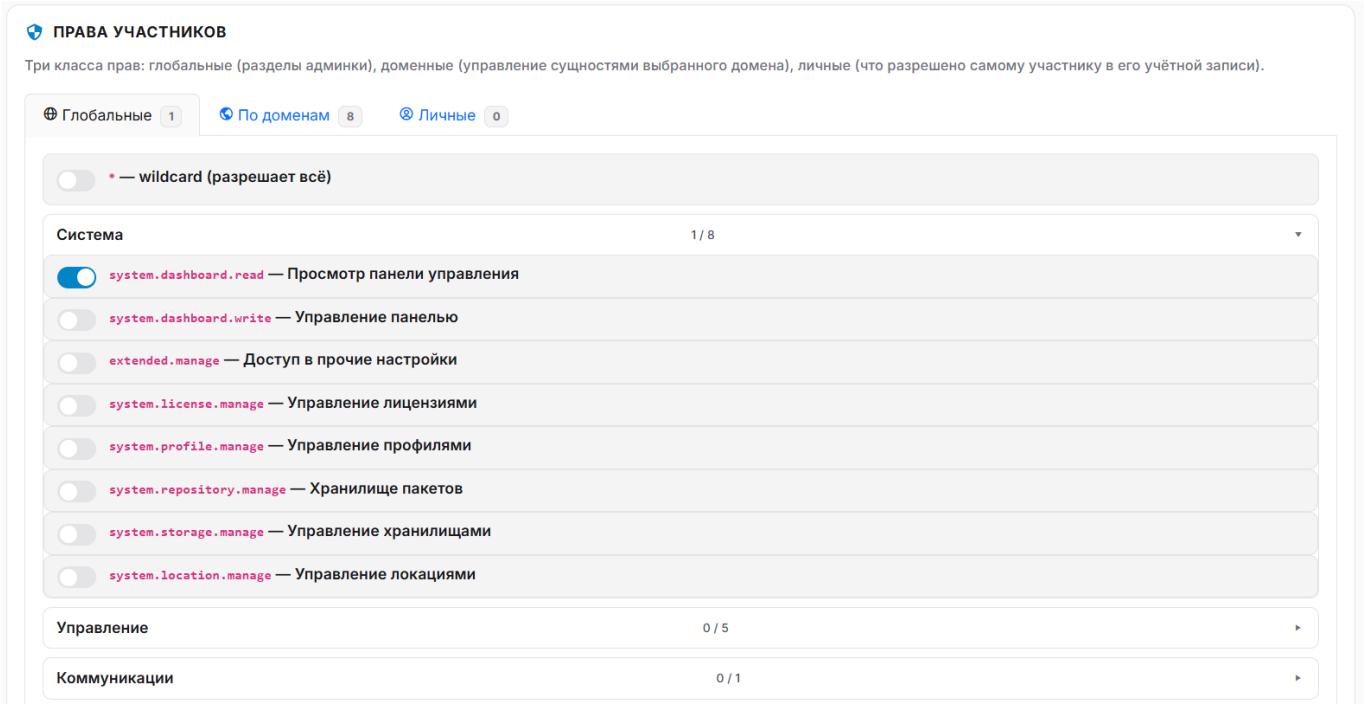


Рисунок 93 – Пример включения разрешения на просмотр раздела «Панель управления»

Подробнее о глобальных правах см. в 3.4.5.1.1.1.

На вкладке «По доменам» для добавления прав необходимо сначала добавить домен, в котором будут назначены разрешения (рисунок 94).

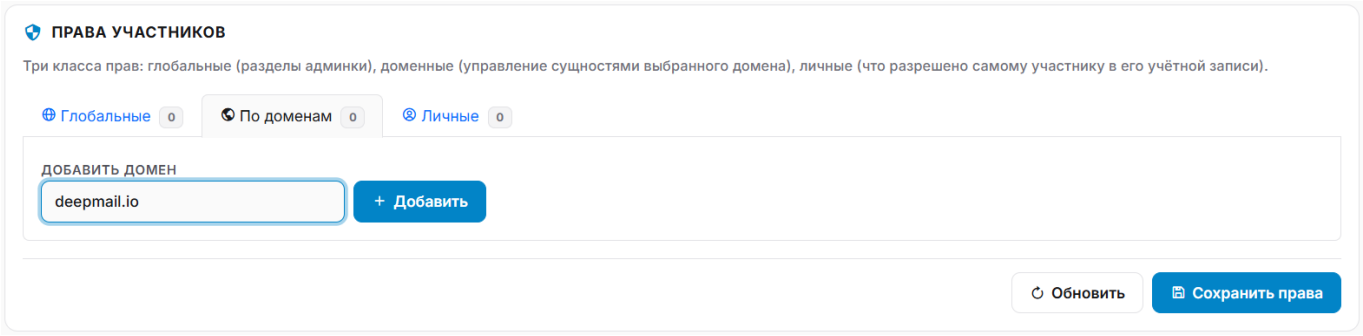


Рисунок 94 – Добавление домена для назначения доменных прав

Щелчком мыши в поле «ДОБАВИТЬ ДОМЕН» раскройте выпадающий список и выберите необходимый домен из предложенных (в списке все домены добавленные в систему) и затем нажмите кнопку + Добавить (см. рисунок 94). После этого откроется список доменных прав (рисунок 95).

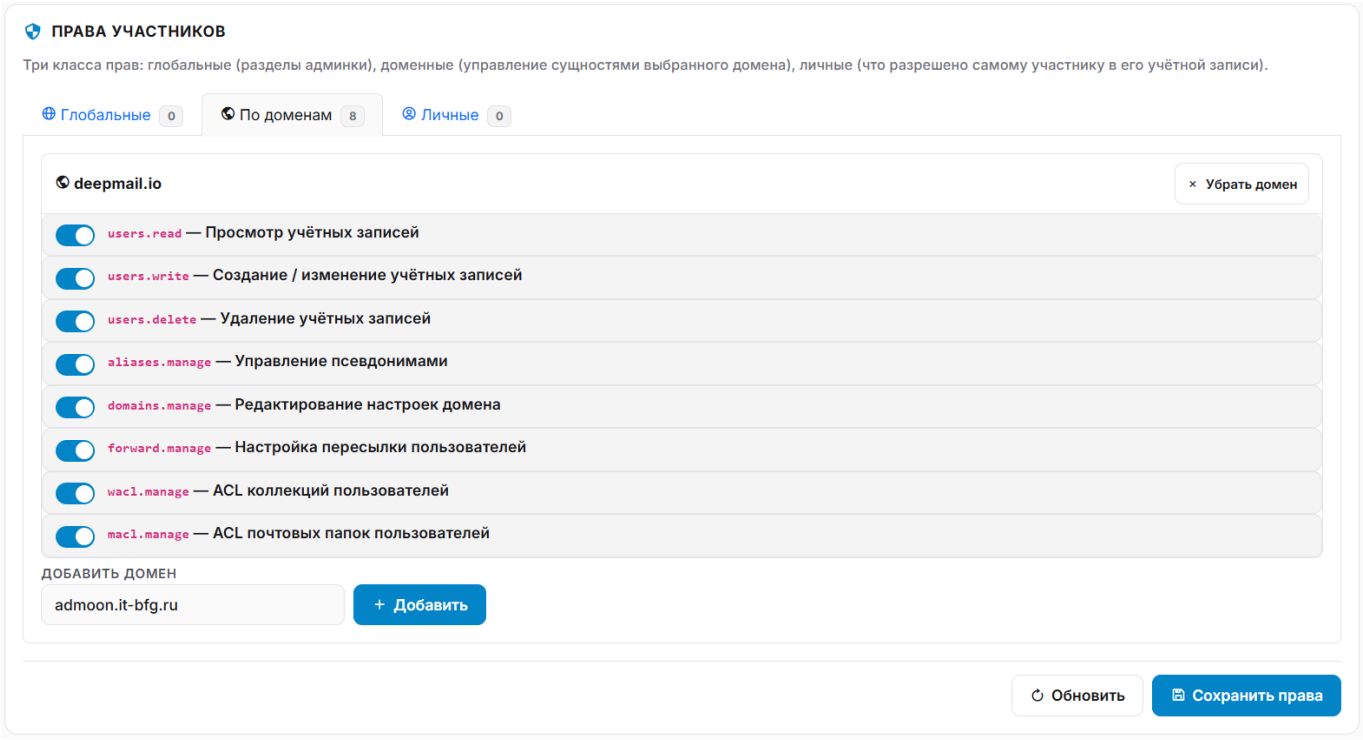
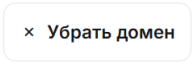


Рисунок 95 – Список доменных прав

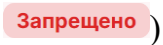
Доменные права по умолчанию все включены (в наименовании вкладки отображается 0 отключенных) (см. рисунок 95). Для отмены разрешения определенных действий отключите соответствующие чекбоксы.

Подробнее о доменных правах см. в 3.4.5.1.1.2.

Если необходимо отменить все права на домен, нажмите кнопку 

(см. рисунок 95).

На вкладке «Личные» по умолчанию все права включены (в наименовании вкладки отображается 0 отключенных). Для удобства личные права распределены по категориям применения, в строке права отображается иконка 

(при отключении 

) (рисунок 96).

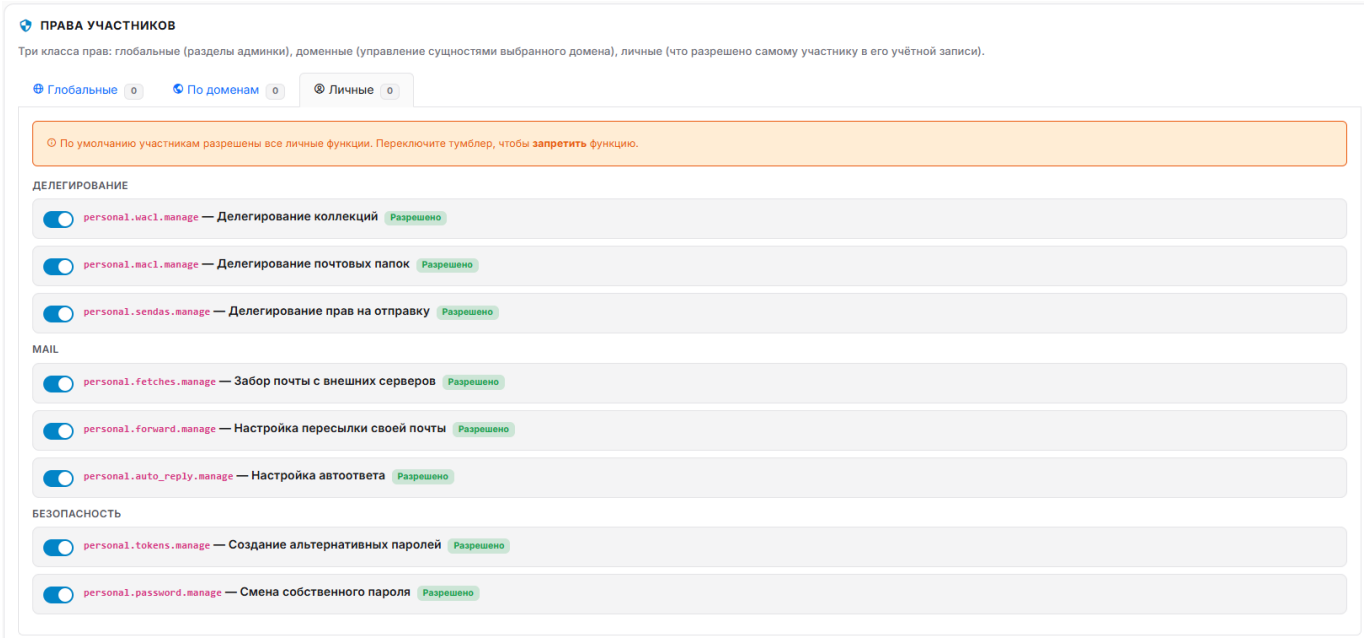


Рисунок 96 – Список личных прав

Подробнее о личных правах см. в 3.4.5.1.1.3.

После выполнения необходимых настроек прав для сохранения нажмите кнопку 

(см. рисунок 92).

Теперь можно добавить участников группы, для этого нажмите кнопку 

(см. рисунок 91). Откроется страница «Редактор группы» на которой отображено два поля:

- «В группе» – список пользователей, включенных в группу;
- «Доступные пользователи» – список пользователей, доступных для добавления в группу (рисунок 97).

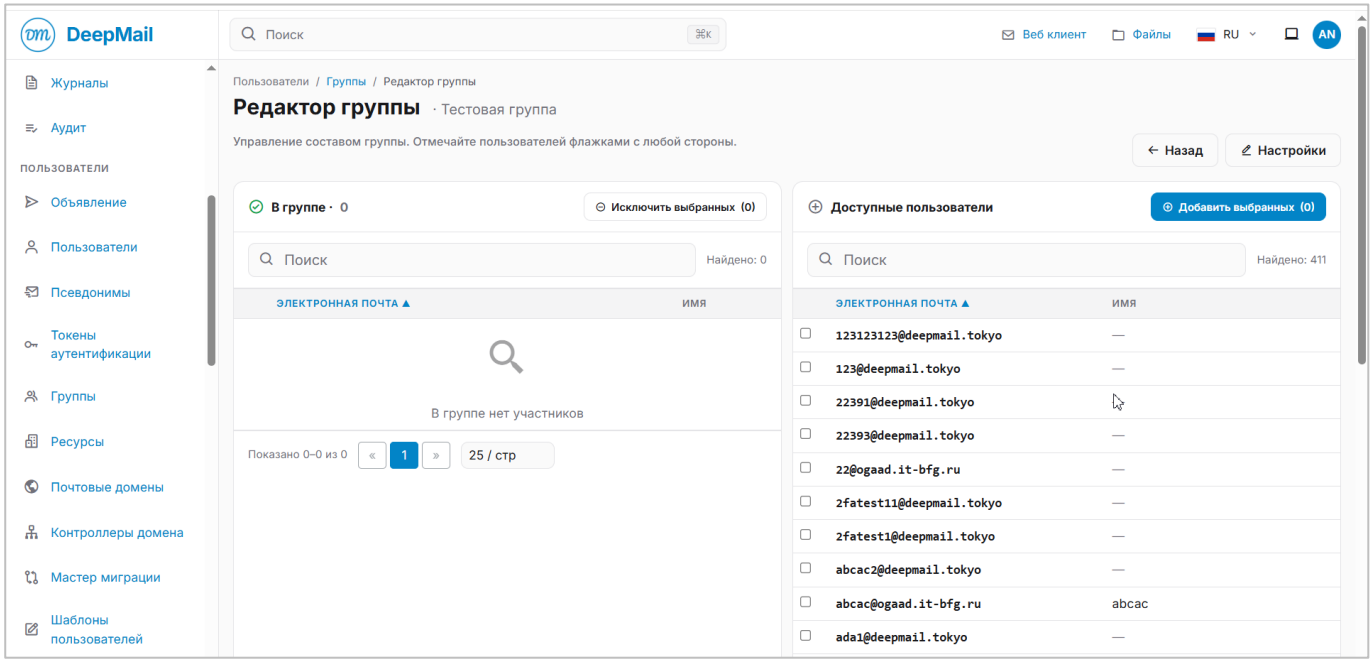


Рисунок 97 – Редактор группы

Отметьте пользователей в списке «Доступные пользователи» и нажмите кнопку Добавить выбранных (3) (счетчик на кнопке – количество выбранных пользователей).

Для возвращения на страницу «Изменить группу» и продолжения настройки прав и других параметров нажмите кнопку Настройки, для завершения настроек и перехода на страницу «Группы» нажмите кнопку ← Назад (см. рисунок 97).

3.4.5.1.1 Система прав

Каждое право в DeepMail – это именованный ключ (users.write, system.dashboard.read, personal.forward.manage и т.д.), который пользователь получает через добавление его УЗ в определенную группу. То есть у группы – набор выданных прав, у пользователя – членство в одной или нескольких группах. Эффективный набор прав пользователя – это объединение прав всех его групп.

В DeepMail реализовано три класса прав – глобальные (административные права, которые разрешают право доступа и управления функционалом, соответствующих разделов админ-панели), доменные (также административные права на управление сущностями выбранного домена), личные (пользовательские – разрешения пользователю на управление и настройку некоторых функций собственной УЗ).

Существует особая роль – глобальные администраторы – это системная группа (Global Admins), для которой применен специальный параметр – «* – wildcard», который трактуется как «разрешено все», и все глобальные права, и все доменные на всех доменах.

Важно! Удалять или снимать параметр «* – wildcard» у этой группы нельзя, иначе можно остаться без доступа в инсталляцию.

Альтернативный независимый атрибут – флаг *global_admin=True* для конкретного пользователя. Когда он установлен, проверка прав сразу дает наивысший приоритет на любой административный запрос. Права пользователя не зависят от его членства в группах или назначенных ролей. Флаг устанавливается исключительно через административный CLI или API. Изменение через админ-панель недоступно для предотвращения случайной блокировки доступа.

Все права, кроме вышеуказанного атрибута, назначаются через группы (см. 3.4.5.1). После сохранения изменений права применяются с первого следующего HTTP-запроса пользователя, выполнять повторную авторизацию в системе не требуется.

3.4.5.1.1.1 Глобальные права группы пользователей

Открывают доступ к разделам админ-панели и общесистемные действия. Выдаются только «глобально».

Ключи глобальных прав и описание разрешений при включении данных параметров приведены в таблице 4.

Таблица 4 – Ключи и их описание (глобальные)

Ключ	Описание разрешений
Раздел «Система»	
system.dashboard.read	Просмотр панели управления (Dashboard, Locations, Storages, Profiles, Repository, System logs)
system.dashboard.write	Действия в Dashboard: рестарт хостов, обновление образов, реконфигурация
extended.manage	Раздел «Прочее» и расширенные настройки (SSL/TLS, поиск писем, IP-правила, шаблоны пользователей)
system.license.manage	Управление лицензиями

Ключ	Описание разрешений
system.profile.manage	Управление профилями подключения (IMAP/SMTP/SFTP/WebDAV)
system.repository.manage	Хранилище пакетов (образы сервисов)
system.storage.manage	Управление хранилищами (NFS-таргеты)
system.location.manage	Управление локациями и репликацией
Управление	
groups.manage	Управление группами и правами
user_templates.manage	Управление шаблонами пользователей
dc.manage	Управление контроллерами домена (LDAP/AD/Samba/FreeIPA/ALD Pro)
migration.manage	Мастер миграции почты (IMAP/EWS)
resources.manage	Управление ресурсами (переговорные, транспорт)
Коммуникация	
announcement.manage	Массовые рассылки объявлений
Безопасность	
antispam.manage	Управление антиспамом (rspamd WebUI)
mail_search.manage	Глобальный поиск писем по ящикам пользователей
ip_rules.manage	Управление правилами доступа по IP
external_ip.manage	Управление ограничениями внешней отправки по IP
ssl.manage	Управление SSL/TLS-сертификатом инсталляции
Транспорт	
relay.manage	Управление реле
transport_rules.manage	Управление транспортными правилами
mail_queue.manage	Управление почтовой очередью
Журналы	
system_logs.manage	Системные логи

Ключ	Описание разрешений
audit.manage	Аудит действий администраторов

3.4.5.1.1.2 Доменные права группы пользователей

Доменные права группы пользователей управляют сущностями домена. Каждое право можно выдать «всем доменам» (добавив их последовательно), а можно выдавать права точечно – выключить определенные права в отдельных доменах (рисунок 98).

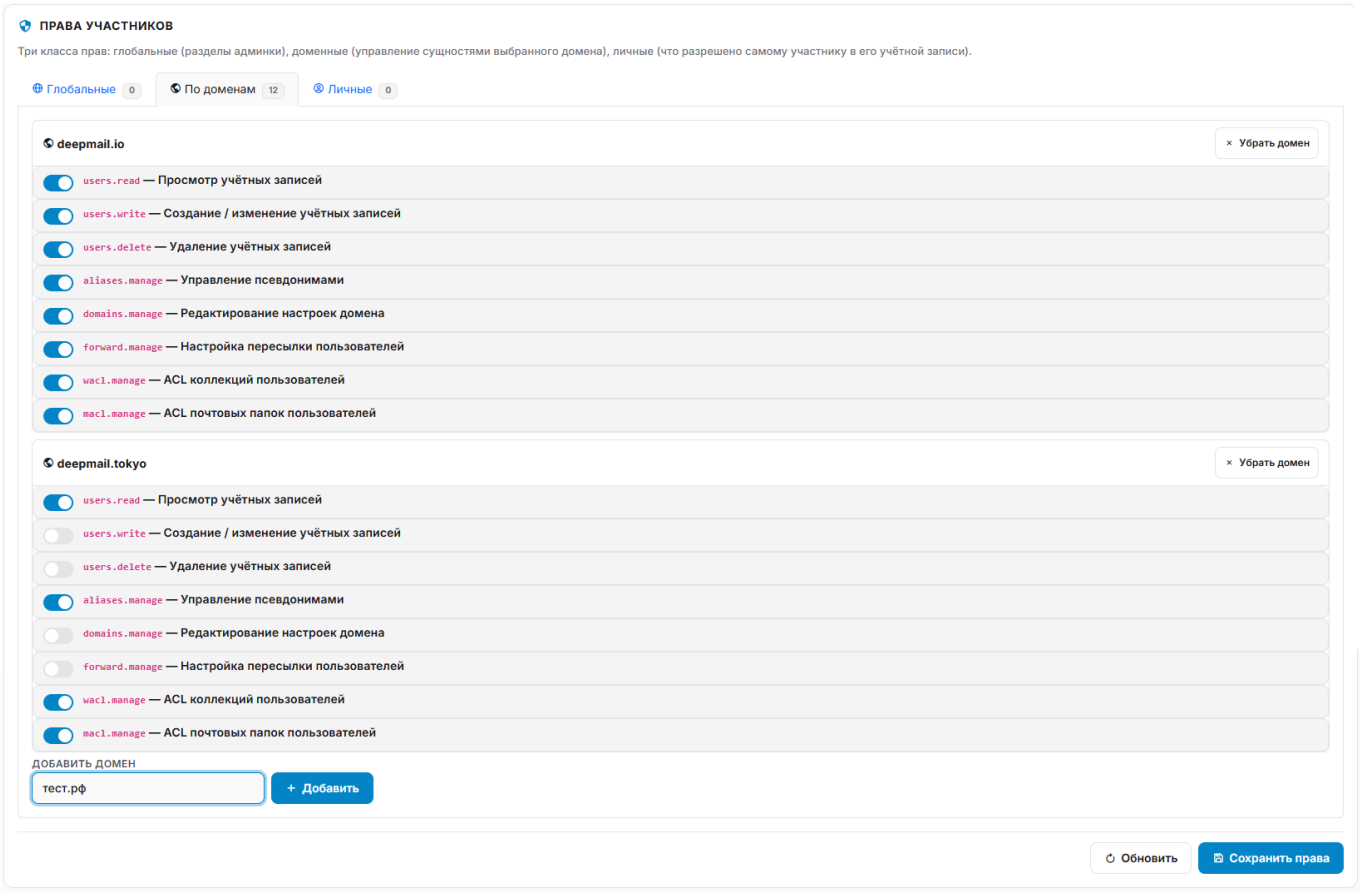


Рисунок 98 – Включение доменных прав

Таким образом у одной и той же группы можно создать разный профиль доступа в разных доменах: например, разрешить просмотр списков пользователей во всех доменах, но создавать и изменять УЗ только в домене «example.com».

Ключи доменных прав и их описание приведены в таблице 5.

Таблица 5 – Ключи и их описание (доменные)

Ключ	Категория применения	Описание разрешений
users.read	Пользователи	Просмотр УЗ пользователей домена
users.write	Пользователи	Создание и изменение УЗ
users.delete	Пользователи	Удаление УЗ
aliases.manage	Пользователи	Управление псевдонимами домена
domains.manage	Домен	Редактирование настроек самого домена (квоты, лимиты, DKIM, автоответ)
forward.manage	Пользователи	Настройка пересылки у пользователей домена
wacl.manage	Пользователи	Управление WebDAV ACL на коллекции пользователей домена
macl.manage	Пользователи	Управление Mail ACL на почтовые папки пользователей домена

3.4.5.1.1.3 Личные права группы пользователей

Личные права группы пользователей регулируют, что разрешено самому участнику группы в его личном кабинете. По умолчанию каждое право включено – то есть пользователь по умолчанию может все. Запрет выставляется выключением чекбокса на нужное право в одной из его групп: если хотя бы в одной группе пользователя чекбокс права, действие запрещено (правило «deny-wins»).

Ключи личных прав и их описание приведены в таблице 6.

Таблица 6 – Ключи и их описание (личные)

Ключ	Категория применения	Описание разрешений
personal.wacl.manage	Делегирование	Делегирование своих коллекций (календари, адресные книги, задачи)
personal.macl.manage	Делегирование	Делегирование почтовых папок
personal.sendas.manage	Делегирование	Делегирование прав на отправку (SendAs / OnBehalfOf)
personal.collections.manage	DAV	Создание дополнительных DAV-коллекций (помимо системных)
personal.fetches.manage	Почта	Забор почты с внешних серверов (POP3/IMAP fetch)

Ключ	Категория применения	Описание разрешений
personal.forward.manage	Почта	Настройка пересылки своей почты
personal.auto_reply.manage	Почта	Настройка автоответа
personal.tokens.manage	Безопасность	Создание альтернативных паролей (токенов)
personal.password.manage	Безопасность	Смена собственного пароля

3.4.5.1.2 Двухфакторная аутентификация в системе

АРМ «DeepMail» поддерживает двухфакторную аутентификацию (2FA) при входе пользователей в почтовые ящики 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, например, такого как Google Authenticator, Yandex Ключ и другие.

Администратору предоставляются инструменты для централизованного управления функцией 2FA. Включение и отключение настройки 2FA доступно на уровне групповых настроек. 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.

Чтобы активировать 2FA администратору необходимо создать группу (см. 3.4.5.1) с настроенной политикой двухфакторной аутентификации (см. рисунок 90) и добавить в нее пользователей, для которых требуется дополнительная мера защиты при входе в почтовый ящик.

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 к серверу полученный токен, который заменяет пароль. Это позволяет не запрашивать код 2FA при каждом обращении к системе.

В случае необходимости администратор может сбросить уникальный ключ для любого пользователя, что приведет к необходимости повторной настройки приложения-аутентификатора с новым QR-кодом. Сброс 2FA выполняется в режиме редактирования УЗ конкретного пользователя (см. 3.4.2.2).

3.4.5.2 Редактирование списка пользователей, добавленных в группу

Для редактирования списка пользователей включенных в группу необходимо нажать на странице инструмента «Группы» в строке выбранной группы кнопку  (см. рисунок 88).

Откроется страница «Редактор группы» со списками уже включенных в группу пользователей и пользователей, доступных для включения (рисунок 99).

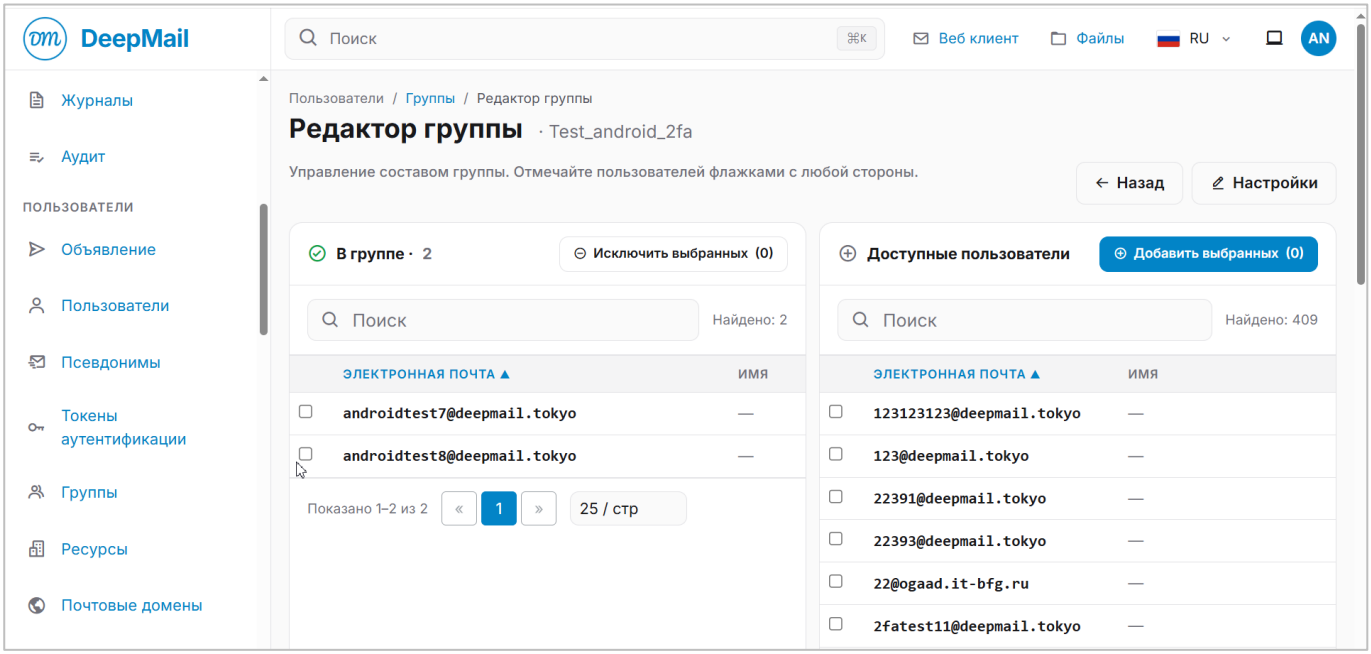


Рисунок 99 – Окно редактирования списка пользователей группы

Выбирайте необходимых пользователей в списках и исключайте или добавляйте пользователей в группу при помощи кнопок Исключить выбранных (1) и Добавить выбранных (3) соответственно.

Для завершения настроек и возврата на страницу «Группы» нажмите кнопку ← Назад, для перехода на страницу «Изменить группу» нажмите кнопку Настройки (см. рисунок 99).

3.4.5.3 Редактирование настроек группы

Для редактирования настроек на странице инструмента «Группы» в строке выбранной группы нажмите кнопку (см. рисунок 88).

Откроется страница «Изменить группу» аналогичная как при создании группы (см. рисунок 91).

После внесения необходимых изменений или дополнительных настроек нажмите кнопку Сохранить. Для отмены изменений нажмите кнопку Отмена (см. рисунок 91).

3.4.5.4 Удаление группы

Для удаления на странице инструмента «Группы» нажмите кнопку  (см. рисунок 88), расположенную в строке группы.

Подтвердите удаление в открывшемся модальном окне (рисунок 100).

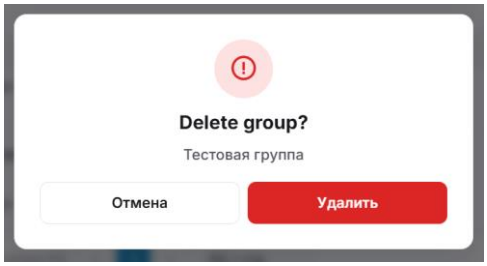


Рисунок 100 – Модальное окно для подтверждения удаления группы

3.4.6 Инструмент «Ресурсы»

Система позволяет централизованно управлять ресурсами организации (помещения, оборудование, транспорт) посредством автоматизации процесса бронирования добавленных в систему УЗ ресурсов.

Фактически в DeepMail каждый ресурс – это особая УЗ пользователя со служебным параметром *is_resource=True*, с почтовым ящиком (но как обычный не используется) и календарем, которыми автоматически управляет назначенный менеджер. Чтобы забронировать ресурс необходимо создать событие в календаре и добавить в качестве участника УЗ ресурса, при этом выполняется либо автоматическое согласие/ отклонение участия по правилам менеджера, либо назначенный менеджер ресурса может принять или отклонить участие вручную. В случае если ресурс доступен для брони, организатор события получит подтверждение об успешном бронировании. В случае если ресурс не доступен, организатор получит уведомление об отказе в бронировании.

Для административного управления ресурсами организации (создание, изменение параметров, удаление) предназначен инструмент «Ресурсы». Чтобы перейти к нему в меню админ-панели необходимо выбрать пункт «Ресурсы» (см. рисунок 64).

Откроется страница «Список ресурсов» (рисунок 101).

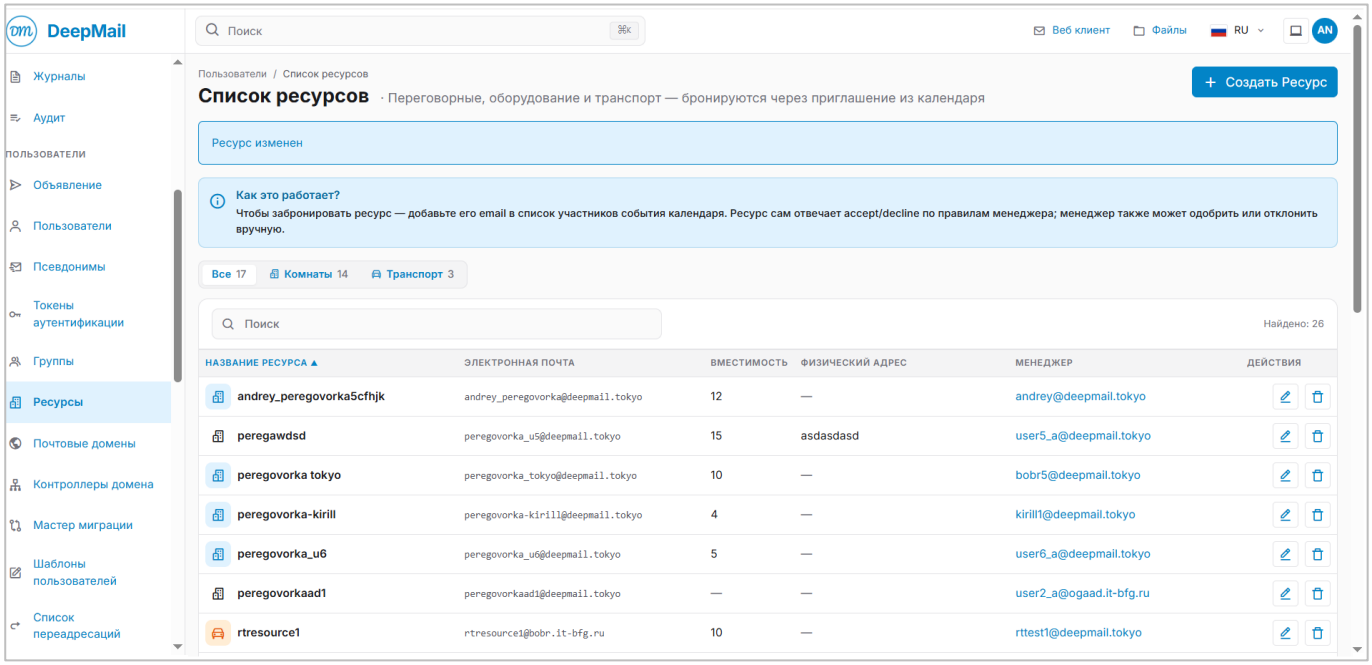


Рисунок 101 – Страница «Список ресурсов»

На странице представлен реестр доступных для бронирования ресурсов: переговорных комнат (оборудования) и транспорта. Для администратора доступны различные функциональные элементы сортировки по типу ресурсов (кнопки Все 17, Комнаты 14, Транспорт 3) и строка поиска (Поиск) в списке УЗ имеющихся ресурсов (см. рисунок 101).

2.4.6.1 Создание нового ресурса

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

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 контроль занятости ресурсов.

Для создания нового ресурса необходимо на странице «Список ресурсов» нажать кнопку + Создать Ресурс (см. рисунок 101).

Откроется страница с формой «Создать ресурс» (рисунок 102).

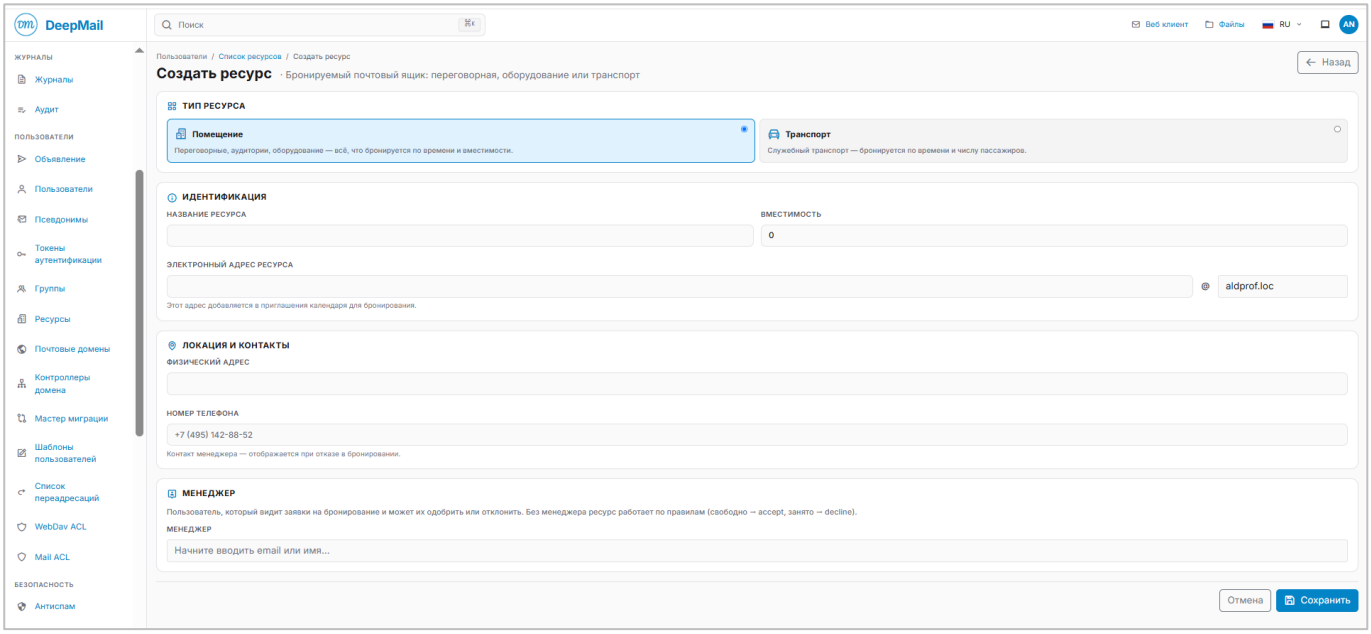


Рисунок 102 – Форма «Создать ресурс»

В появившейся форме в блоке «ТИП РЕСУРСА» необходимо выбрать тип создаваемого ресурса: «Помещение» или «Транспорт».

В блоке «ИДЕНТИФИКАЦИЯ» укажите наименование ресурса, вместимость и адрес электронной почты ресурса (локальную часть введите вручную, доменную выберите из выпадающего списка, щелкнув мышью в поле после знака «@») (см. рисунок 102).

В блоке «ЛОКАЦИЯ И КОНТАКТЫ» укажите фактический адрес размещения ресурса и контактный номер телефона менеджера ресурса (номер телефона будет отображаться в ответном сообщении при отказе в бронировании).

В блоке «МЕНЕДЖЕР» укажите УЗ (эл. адрес) пользователя ответственного за ресурс, ему будет доступен просмотр заявок на бронирование ресурса, и он сможет принимать или отклонять заявки. В данном блоке можно добавить только одну УЗ пользователя, если требуется назначение еще одного ответственного за ресурс, администратор может выдать права доступа на коллекцию ресурса от имени УЗ назначенного менеджера в инструменте «Пользователи» (редактирование УЗ менеджера , кнопка Календари, контакты, задачи – см. 3.4.2.2).

После внесения всех данных нажмите кнопку Сохранить. Для отмены нажмите кнопку Отмена (см. рисунок 102).

На странице «Ресурсы» появится системное сообщение «Ресурс создан», а созданный ресурс отобразится в списке.

2.4.6.2 Редактирование ресурса

Для редактирования необходимо нажать кнопку  в строке определенного ресурса (см. рисунок 101). Откроется страница «Изменить ресурс» (рисунок 103).

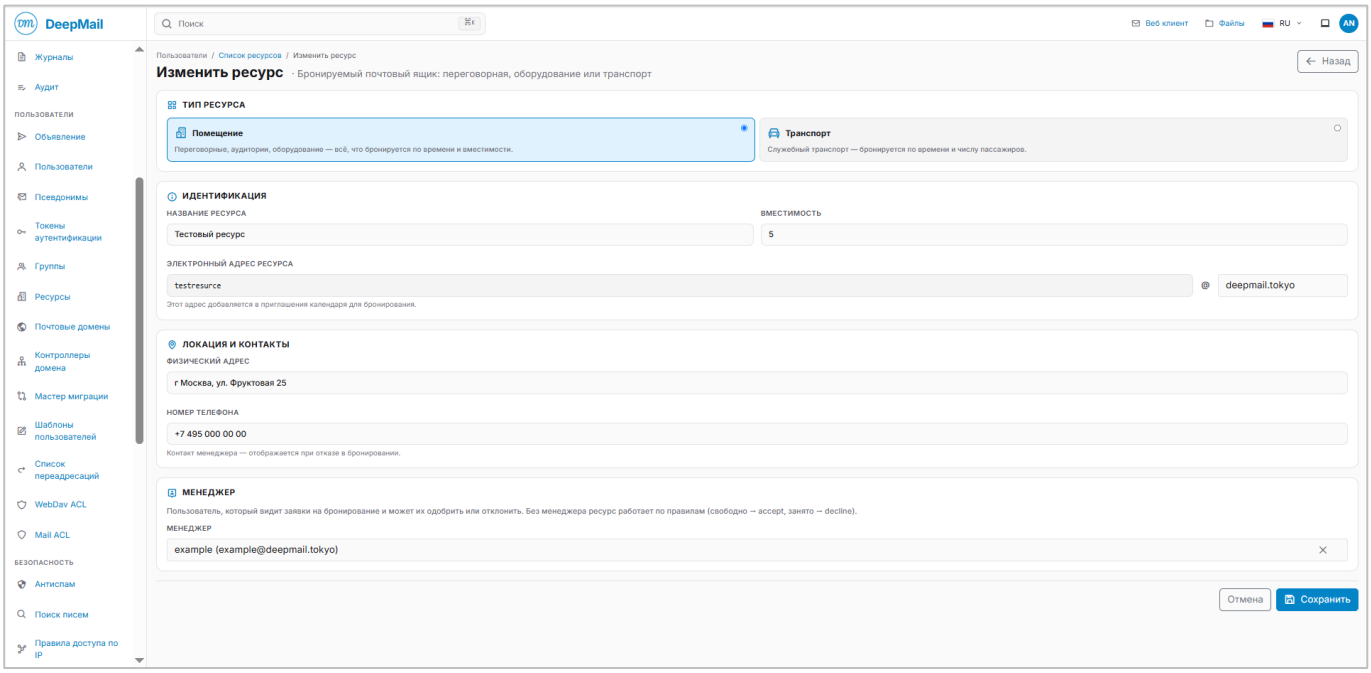


Рисунок 103 – Форма «Изменить ресурс»

В данной форме не доступен к изменению только электронный адрес ресурса, все остальные параметры можно поменять.

После внесения изменений нажмите кнопку 

. Для отмены нажмите кнопку

(см. рисунок 103).

На странице «Ресурсы» появится системное сообщение «Ресурс изменен».

2.4.6.3 Удаление ресурса

Для удаления ресурса необходимо нажать кнопку  в строке определенного ресурса (см. рисунок 101), и подтвердить удаление в открывшемся модальном окне.

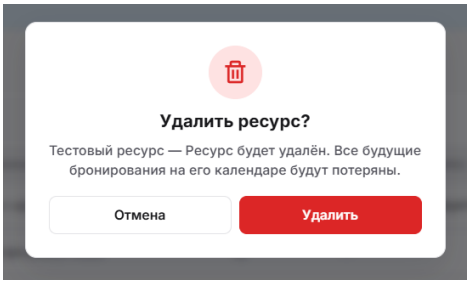


Рисунок 104 – Подтверждение удаления ресурса

При дополнительном запросе подтверждения действия – подтвердите его.

На странице «Ресурсы» появится системное сообщение «Ресурс удален».

3.4.7 Инструмент «Почтовые домены»

Инструмент «Почтовые домены» – страница списка доменов инсталляции с настройками квот, лимитов, доступов, DKIM-ключами, автоответом, псевдонимами и альтернативными именами, а также функционалом добавления, изменения и удаления доменов.

Для перехода на страницу «Список доменов» необходимо в меню админ-панели необходимо выбрать пункт «Почтовые домены» (см. рисунок 64).

На стартовой странице администратор видит обобщенную статистику по всем доменам: общее количество доменов, общее число почтовых ящиков и псевдонимов. Эти цифровые индикаторы позволяют быстро оценить масштаб инфраструктуры.

Каждый почтовый домен, обслуживаемый сервером DeepMail, отображен в интерфейсе страницы «Список доменов» отдельной карточкой домена, которая представляет собой компактную информационную панель с набором функциональных элементов для управления конкретным доменом (рисунок 105).

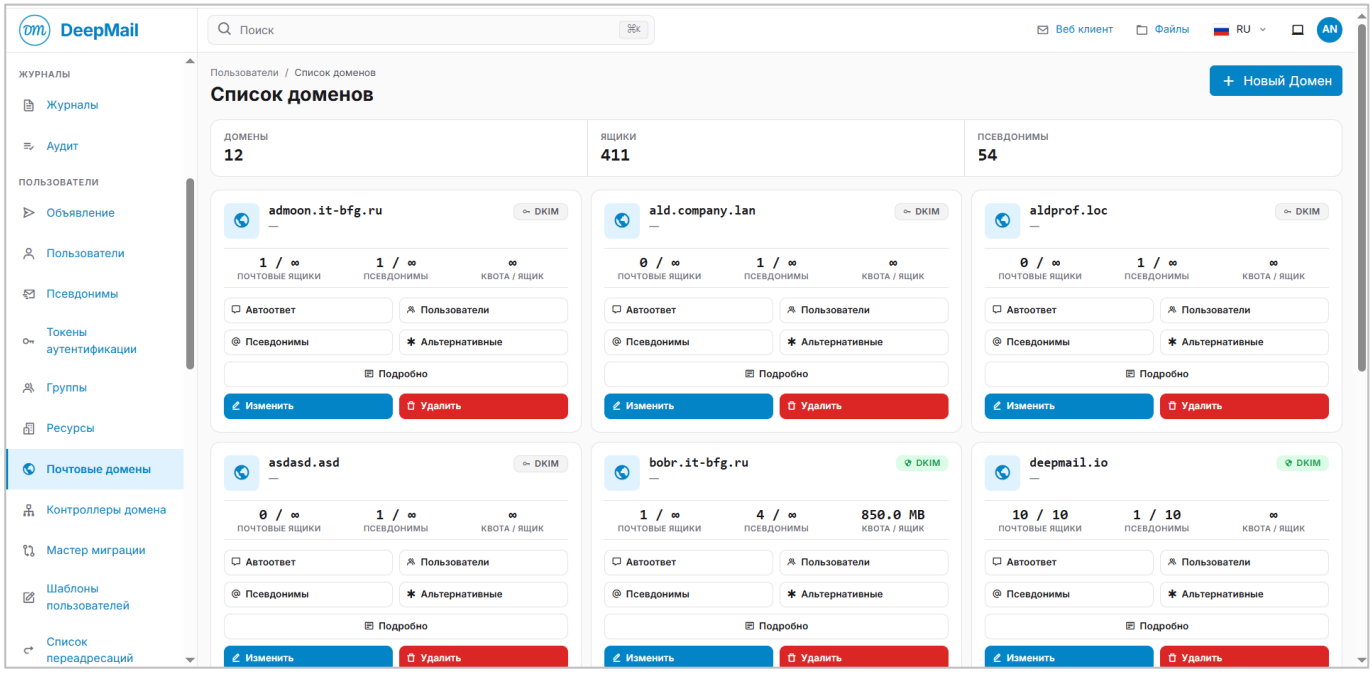


Рисунок 105 – Окно «Список доменов»

В верхней части карточки домена отображается его имя с комментарием (при наличии, если нет, то стоит «—») и иконка статуса: при отсутствии подключенного DKIM-ключа

DKIM, сигнализируя о необходимости настройки подписи; если подпись настроена отображается DKIM.

Ниже размещен блок с текущими значениями лимитов и потребления ресурсов. Для каждого домена отображается количество занятых почтовых ящиков относительно максимально разрешенного (например, 1 из бесконечности), число созданных псевдонимов и установленная квота на дисковое пространство (∞ означает отсутствие ограничения).

В нижней части карточки расположены кнопки быстрого перехода к основным операциям управления доменом:

- «Автоответ» – ведет к конфигурации автоответчика, который может быть включен для всех ящиков домена;
- «Пользователи» – открывает список учетных записей, созданных в домене, позволяя управлять ящиками;
- «Псевдонимы» – переход на страницу управления псевдонимами данного домена;
- «Альтернативные» служит для добавления альтернативных имен домена – дополнительных имен, на которые также будет приниматься почта;
- «Подробно» – открытие расширенной карточки домена, содержащей полный набор настроек;
- «Изменить» – редактирование основных параметров домена (например, квот, профилей SMTP/ IMAP);
- «Удалить» – полное удаление домена из системы.

Таким образом, интерфейс страницы «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.

2.4.7.1 Действия с почтовыми доменами

2.4.7.1.1 Добавление нового почтового домена

Для добавления нового почтового домена необходимо на странице «Список доменов» нажать кнопку + Новый Домен (см. рисунок 105). После этого будет выполнен переход к форме добавления нового почтового домена «Новый домен» (рисунок 106).

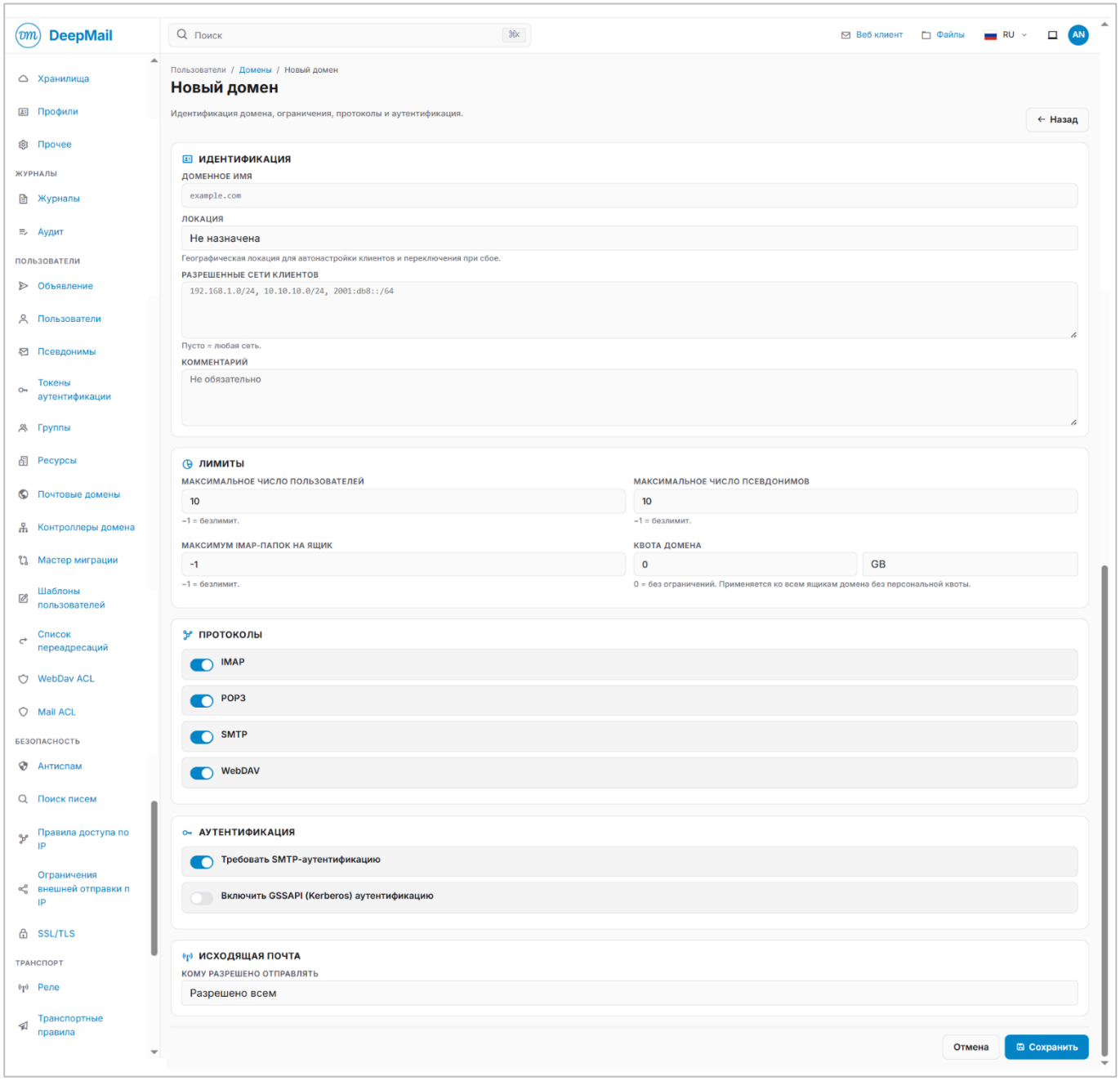


Рисунок 106 – Страница «Новый домен»

Страница создания домена объединяет несколько блоков, позволяющих администратору гибко настраивать параметры почтового домена, управлять сетевыми интерфейсами, протоколами, правами отправки и вести служебные заметки. Каждый блок отвечает за определенный аспект конфигурации, а их совокупность обеспечивает полный контроль над поведением домена.

В блоке «ИДЕНТИФИКАЦИЯ» задаются базовые характеристики домена:

- ДОМЕННОЕ ИМЯ – доменная часть адреса эл. почты, которая будет использоваться для формирования адресов электронной почты пользователей этого домена (часть адреса после @);

- ЛОКАЦИЯ – имя локации, к которой относится домен, если пустое, то локация не назначена. К локации привязаны пользователи и хранилища;

- РАЗРЕШЕННЫЕ СЕТИ КЛИЕНТОВ – список IPv4/IPv6 CIDR. Если задано – пользователи домена могут авторизоваться в систему только из этих сетей. Пустое – без ограничения;

- КОММЕНТАРИЙ – необязательное поле для заметок или комментариев. Сохраненные заметки хранятся вместе с конфигурацией домена и могут быть просмотрены другими администраторами, что облегчает совместную работу и документирование.

В блоке «ЛИМИТЫ» определяются ограничения:

- «МАКСИМАЛЬНОЕ ЧИСЛО ПОЛЬЗОВАТЕЛЕЙ» позволяет установить жесткий лимит, предотвращающий неконтролируемое создание учетных записей;

- «МАКСИМАЛЬНОЕ ЧИСЛО ПСЕВДОНИМОВ» – ограничивает количество одновременно активных псевдонимов для одного почтового ящика;

- «МАКСИМУМ IMAP-ПАПК НА ЯЩИК» – задает квоту на количество папок, которые пользователь может создать в своем почтовом ящике;

- «КВОТА ДОМЕНА» – задает ограничение на дисковое пространство, доступное всем ящикам домена – значение «∞» означает отсутствие ограничений.

В блоке «ПРОТОКОЛЫ» настраивается набор протоколов, доступных для домена. 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 приема почты по протоколу SMTP;

- WebDAV – поддержка CalDAV и CardDAV для синхронизации календарей и контактов.

Блок «АУТЕНТИФИКАЦИЯ» предназначен для настройки правил авторизации для отправки почты:

- «Требовать SMTP-аутентификацию» определяет, обязаны ли пользователи проходить аутентификацию перед отправкой писем через SMTP – отключение этого требования может использоваться для внутренних доверенных сетей;

– «Включить GSSAPI (Kerberos) аутентификацию» – включает поддержку аутентификации Kerberos (GSSAPI) для почтовых клиентов, что позволяет использовать единый вход в доменной среде (т.е. пользователь вводит логин и пароль единоразово при входе в ОС, при запуске почтового клиентского приложения привычная аутентификация не потребуется).

Блок «ИСХОЯЩАЯ ПОЧТА» содержит поле «КОМУ РАЗРЕШЕНО ОТПРАВЛЯТЬ», в нем задают политику исходящей почты. Щелчком мыши в поле раскрывается список настроек:

– «Разрешено всем» – установлено по умолчанию – пользователи домена могут отправлять письма всем (без ограничений);

– «Только внутри домена» – пользователи домена могут отправлять письма только внутри своего домена (только адресатам того же домена);

– «Только внутри системы» – только внутри инсталляции почтовой системы (свой домен и другие домены на том же сервере, но не на внешние адреса).

Все изменения в настройках домена применяются после нажатия кнопки 

. 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.

2.4.7.1.2 Изменение почтового домена

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

(см. рисунок 105). После этого будет выполнен переход на страницу «Изменить домен» с формой, идентичной форме создания нового домена. В данной форме можно внести изменения в параметры домена, кроме доменного имени. Для сохранения – нажать кнопку 

.

В результате на странице «Список доменов» появится сообщение «Домен сохранен <имя домена>».

2.4.7.1.3 Удаление почтового домена

Для удаления почтового домена необходимо нажать кнопку 

(см. рисунок 105), расположенную в карточке выбранного домена.

Подтвердите удаление домена в открывшемся модальном окне (рисунок 107).

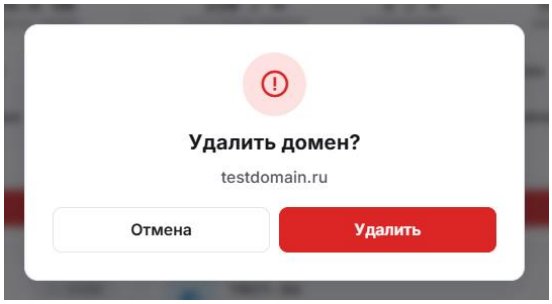


Рисунок 107 – Подтверждение удаления домена

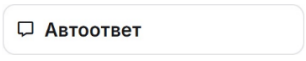
Важно! Операция удаления домена запускает каскадное удаление всех пользователей домена, псевдонимы и контакты в глобальной адресной книге. Перед удалением уведомите пользователей об этом и выполните бэкап – операция необратима.

2.4.7.1 Администратор (менеджер) почтового домена

Для управления почтовым доменом необходимо назначить администратора (или менеджера) почтового домена. Отдельной сущности в АРМ «DeepMail» для этого не предусмотрено, назначение администраторов домена выполняется при помощи делегирования прав пользователю на определенный домен.

Создайте группу с доменными правами на конкретный домен (оставьте все права включенными или отключите некоторые, в соответствии с потребностью) и добавьте в нее необходимых пользователей (описание создания группы, управление правами и добавление пользователей в группу см. в 3.4.5.1).

2.4.7.2 Настройка автоматического ответа для почтового домена

Для настройки автоматического ответа для выбранного почтового домена необходимо в окне «Список доменов» нажать в карточке выбранного домена кнопку 

(см. рисунок 105). После этого будет выполнен переход к форме редактирования параметров автоматического ответа «Автоматический ответ домена», в которой необходимо активировать чекбокс «Включить автоответ для домена», внести тему и текст автоответа, а

также дату начала и окончания работы автоответчика. После внесения всей информации нажать кнопку Сохранить (рисунок 108).

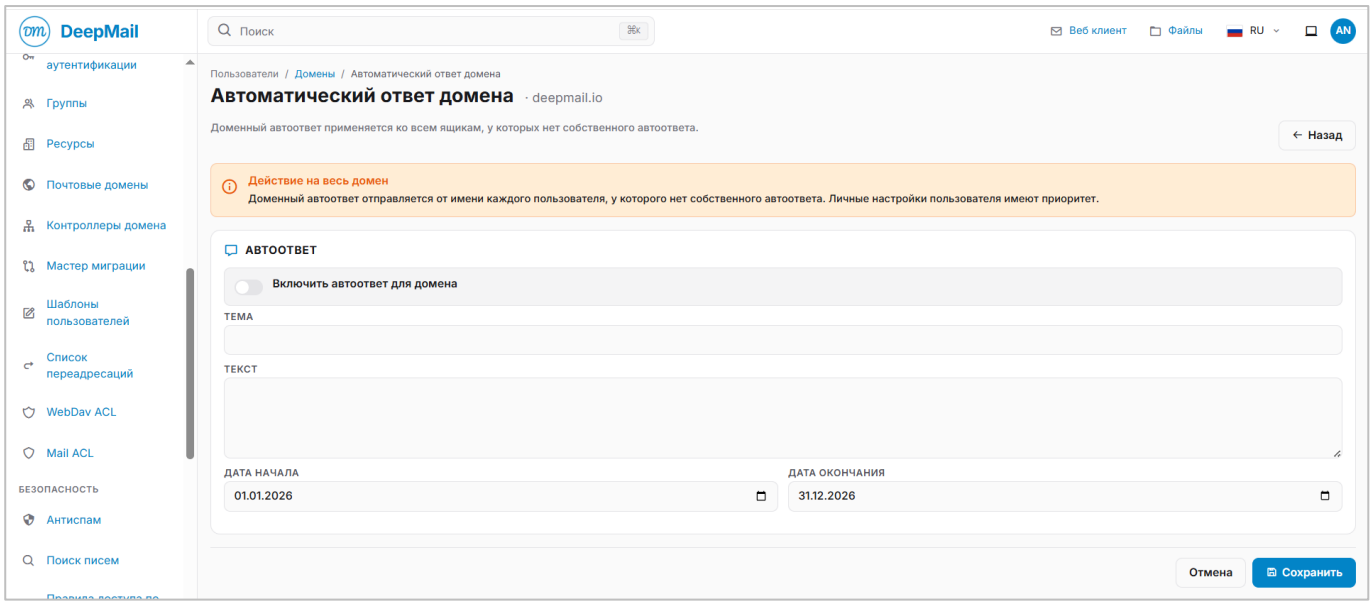


Рисунок 108 – Форма «Автоматический ответ домена»

Данная настройка применяется ко всем письмам в адрес пользователей выбранного домена, «поверх» личных автоответов пользователей. Если необходимо принудительно отключить доменную политику – выключите чекбокс «Включить автоответ для домена».

2.4.7.3 Управление пользователями домена

Управление пользователями из карточки домена осуществляется в пределах одного конкретного 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 необходимо нажать в карточке выбранного домена кнопку Пользователи (см. рисунок 105).

Откроется страница «Пользователи» с поименным списком УЗ пользователей выбранного домена, отображенным в табличном виде (рисунок 109).

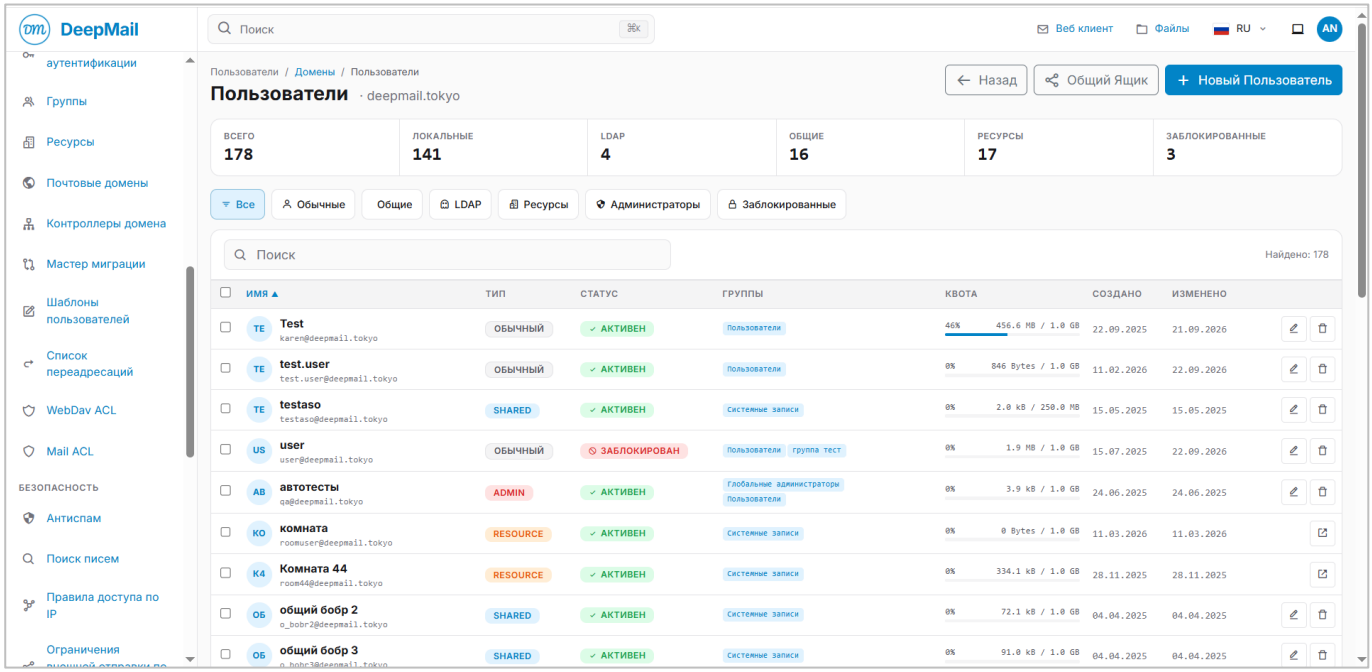


Рисунок 109 – Страница «Пользователи»

Интерфейс и функционал страницы полностью совпадают с интерфейсом и функционалом общесистемного инструмента «Пользователи» (страница «Список пользователей»), но в данном окне все касается пользователей выбранного домена – описание и принципы работы см. в 3.4.2.

2.4.7.4 Управление псевдонимами пользователей почтового домена

Управление псевдонимами пользователей из карточки домена осуществляется в пределах одного конкретного почтового домена. Можно добавлять, изменять данные и удалять псевдонимы.

Для вызова формы управления псевдонимами пользователей необходимо нажать в карточке выбранного домена кнопку @ Псевдонимы (см. рисунок 105).

Откроется страница «Псевдонимы» со списком псевдонимов пользователей выбранного домена, отображенным в табличном виде (рисунок 110).

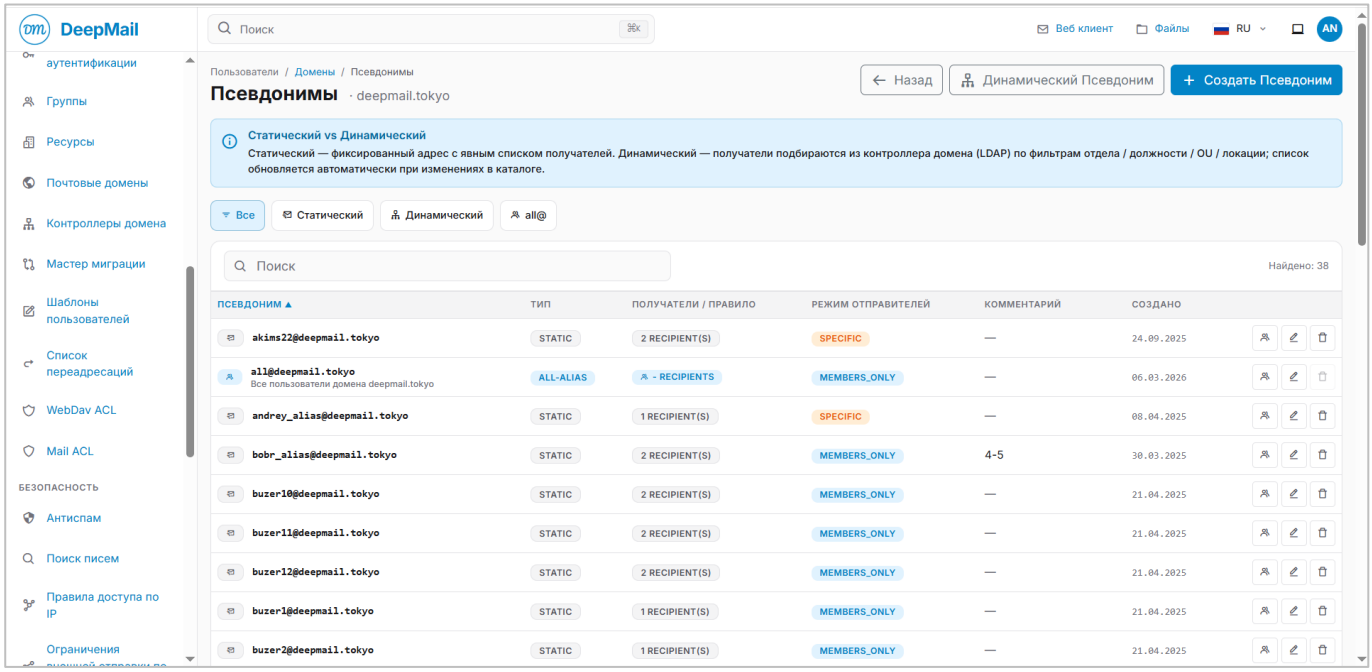


Рисунок 110 – Страница «Псевдонимы»

Интерфейс и функционал страницы полностью совпадают с интерфейсом и функционалом общесистемного инструмента «Псевдонимы», но в данном окне все данные представлены касаемо пользователей выбранного домена – описание и принципы работы см. в 3.4.3.

2.4.7.5 Альтернативный почтовый домен

Сервер позволяет настраивать альтернативные имена (псевдонимы) почтового домена, при этом почта доходит до пользователей как по основному имени домена, так и по всем альтернативным именам. Например, домену «example.com» можно добавить альтернативное имя «example.ru», тогда почта, направленная в адрес «ivan@example.ru», придет в почтовый ящик «ivan@example.com».

Для просмотра списка альтернативных имен почтового домена необходимо в окне «Список доменов» в карточке выбранного домена нажать кнопку 

, (см. рисунок 105).

На экране откроется страница «Список альтернативных доменов» со списком уже добавленных дополнительных доменных имен (при наличии, в случае отсутствия будет отображено сообщение о том, что альтернативных доменов нет) (рисунок 111).

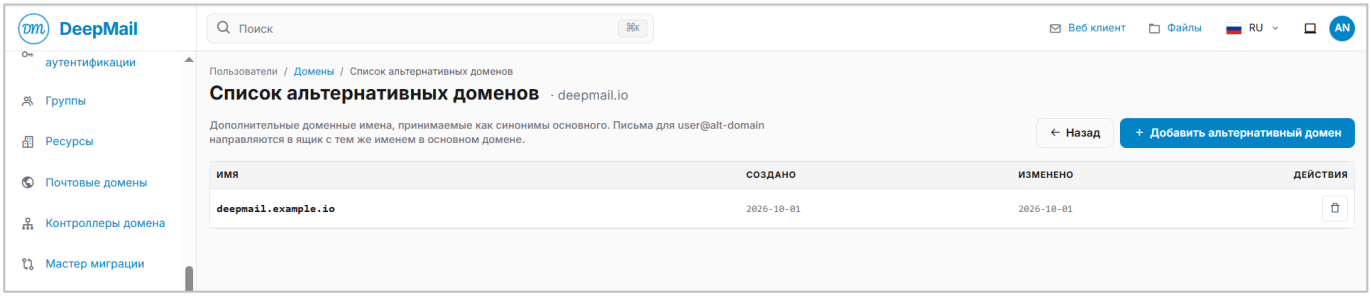


Рисунок 111 – Страница «Список альтернативных доменов» со списком дополнительных доменных имен

Функционал страницы позволяет администратору добавлять новые альтернативные имена домена и удалять уже имеющиеся.

2.4.7.5.1 Создание альтернативного почтового домена

Для создания альтернативного имени почтового домена необходимо на странице «Список альтернативных доменов» нажать кнопку + Добавить альтернативный домен (см. рисунок 111). В открывшейся форме указать имя альтернативного домена и нажать кнопку Сохранить (рисунок 112).

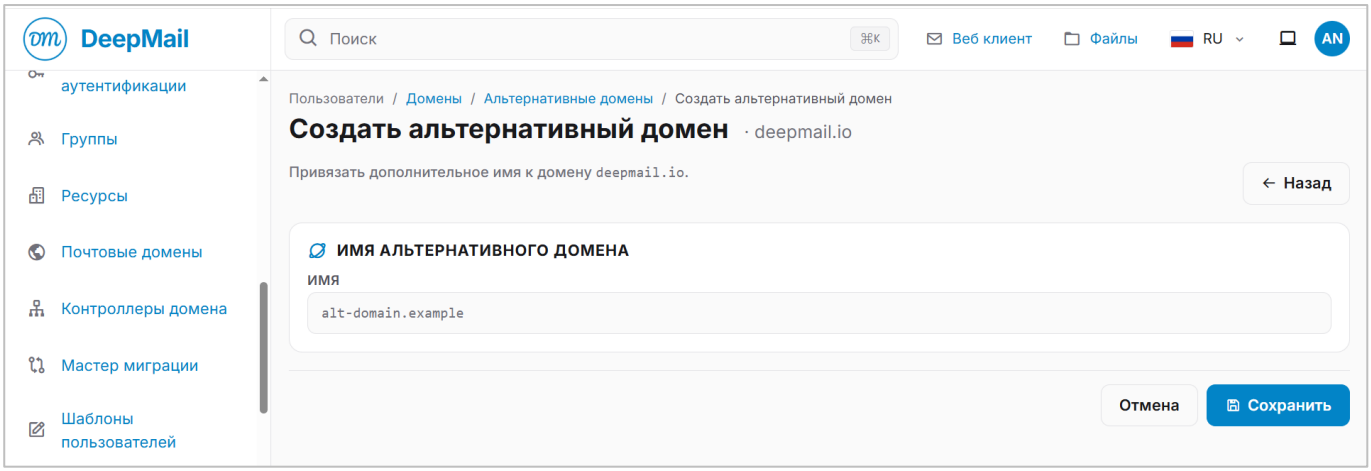


Рисунок 112 – Форма «Создать альтернативный домен»

Форма создания закроется, на странице «Список альтернативных доменов» появится сообщение «Альтернативный домен создан: <имя домена>», а дополнительное имя домена будет добавлено в таблицу со списком альтернативных доменов.

2.4.7.5.2 Удаление альтернативного почтового домена

Для удаления альтернативного почтового домена необходимо в окне «Список альтернативных доменов» нажать кнопку , расположенную в строке альтернативного

домена (см. рисунок 111), и подтвердить удаление в открывшемся модальном окне (при необходимости дополнительного подтверждения действия – подтвердите его). На странице «Список альтернативных доменов» появится сообщение «Альтернативный домен удален: <имя домена>».

2.4.7.6 DNS-записи почтового домена и генерация ключей DKIM

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

DNS-записи почтового домена – это специальные настройки в системе доменных имен (DNS), которые сообщают всему интернету, какой сервер должен обрабатывать почту для вашего домена, и подтверждают, что пользователи домена имеют право отправлять письма от его имени.

MX (Mail Exchanger) – запись указывает на сервер, который принимает входящую почту для вашего домена. Например, когда кто-то пишет письмо на адрес «ivan@example.ru», сервер получателя смотрит в DNS-записи «example.ru», находит MX-запись и понимает на какой сервер надо доставить письмо. У MX-записи есть приоритет, если указано несколько серверов, почта сначала пойдет на тот, у кого число приоритета меньше.

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 (DKIM) – метод e-mail аутентификации. Технология 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 «черные списки».

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.

Для просмотра DNS-записей домена необходимо в окне «Список доменов» на панели выбранного домена нажать кнопку 

(см. рисунок 105).

В результате откроется страница «Подробности домена» (рисунок 113).

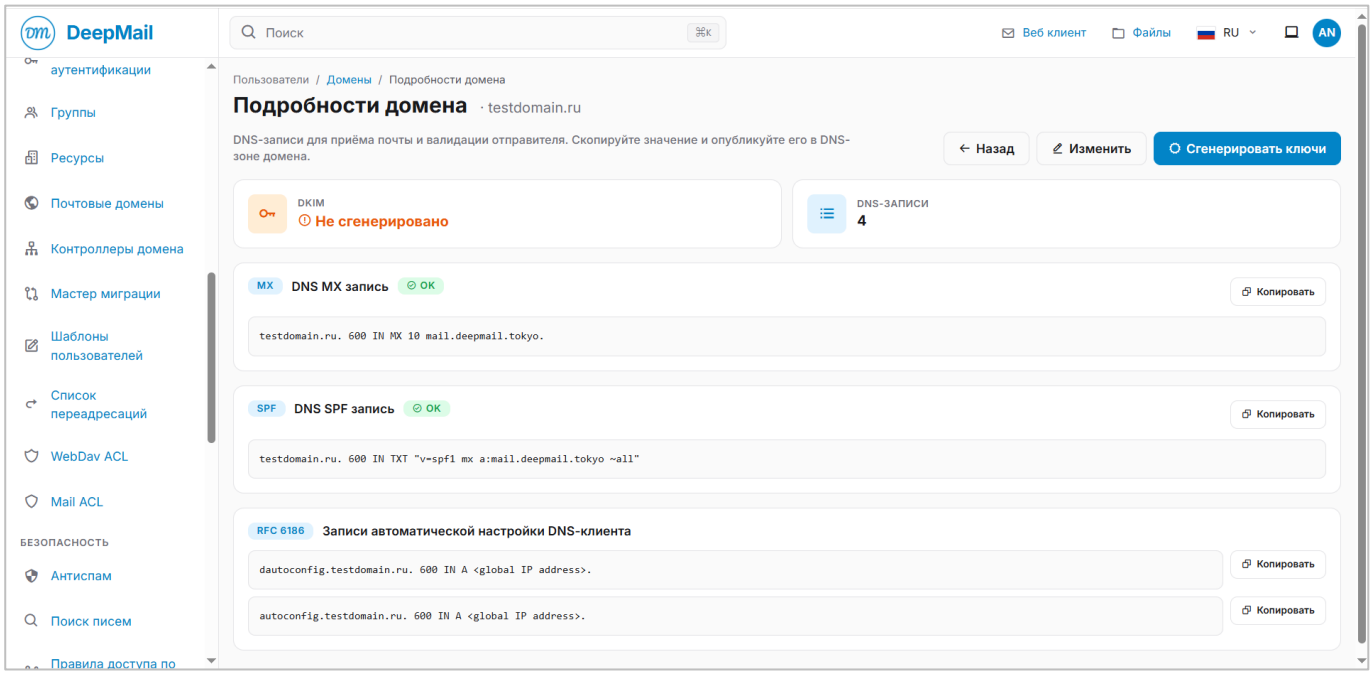


Рисунок 113 – Страница «Подробности домена»

В данной форме приведены DNS-записи, которые нужно прописать в DNS-зоне:

- «DNS MX запись» – для приема почты;
- «DNS SPF-запись» – TXT, разрешает отправку с IP;
- «Записи автоматической настройки DNS-клиента» – для почтовых клиентов.

Записи на странице «Подробности домена» (см. рисунок 113) приводятся в виде, готовом к копированию в зону DNS.

На рисунке 113 приведена начальная форма страницы «Подробности домена», когда ключи DKIM еще не сгенерированы. Для генерации ключей нажмите кнопку 

(см. рисунок 113) и подтвердить действие нажав в открывшемся модальном окне кнопку 

(рисунок 114).

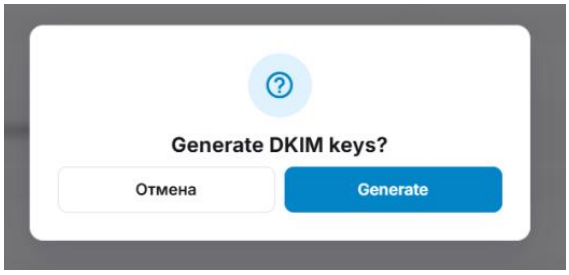


Рисунок 114 – Подтверждение генерации ключей DKIM

Также необходимо дополнительно подтвердить действие на странице (рисунок 115).

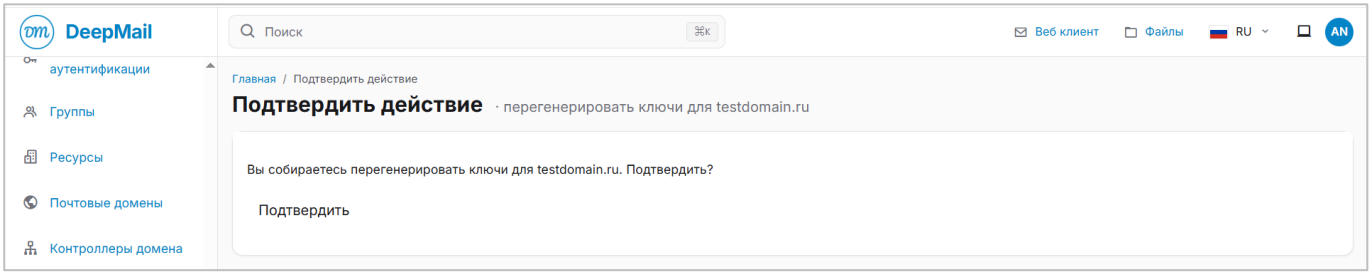


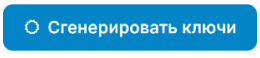
Рисунок 115 – Подтверждение действия на странице

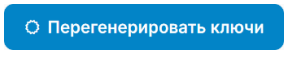
После генерации ключа на странице «Подробности домена» появятся дополнительные блоки:

- «Публичный ключ DKIM» – публичный ключ для создания цифровой подписи сообщений, гарантирующей их подлинность;
- «DNS DKIM запись» – TXT с публичным ключом;
- «DNS DMARC запись», которая определяет политику сервера получателя в отношении сообщений, отправленных с домена, но не прошедших аутентификацию (рисунок 116).



Рисунок 116 – Автоматическое добавление DKIM ключа в запись

Кнопка 

заменяется кнопкой 

(предназначена для замены имеющейся пары на новую пару ключей DKIM).

При настройке DNS почтового домена форматы данных для настройки рекомендуется брать из таблицы 7.

В таблице 7 приведены необходимые DNS-записи с общепринятыми обозначениями:

- «yourdomain» – имя почтового домена;

- «xxx.xxx.xxx.xxx» – IP-адрес;
- «DIM_KEY» – ваш DKIM key.

Таблица 7 – 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	-

3.4.8 Инструмент «Контроллеры домена»

Инструмент «Контроллеры домена» – это инструмент подключения DeepMail к внешним LDAP/ AD-каталогам для синхронизации пользователей. Из них создаются виртуальные пользователи (им присваивается параметр *is_virtual=True*), которые не имеют локального пароля и аутентифицируются через запрос к DC ОС.

DeepMail поддерживает 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 3.4.8.1).

Для перехода к подключению контроллеров домена необходимо в меню админ-панели необходимо выбрать пункт «Контроллеры домена» (см. рисунок 64).

В окне «Контроллеры домена» отображается перечень обслуживаемых доменов (это домены, список пользователей которых сформирован из подключенного контроллера) и список подключенных контроллеров домена, в верхней области страницы отображены общие количественные показатели (рисунок 117).

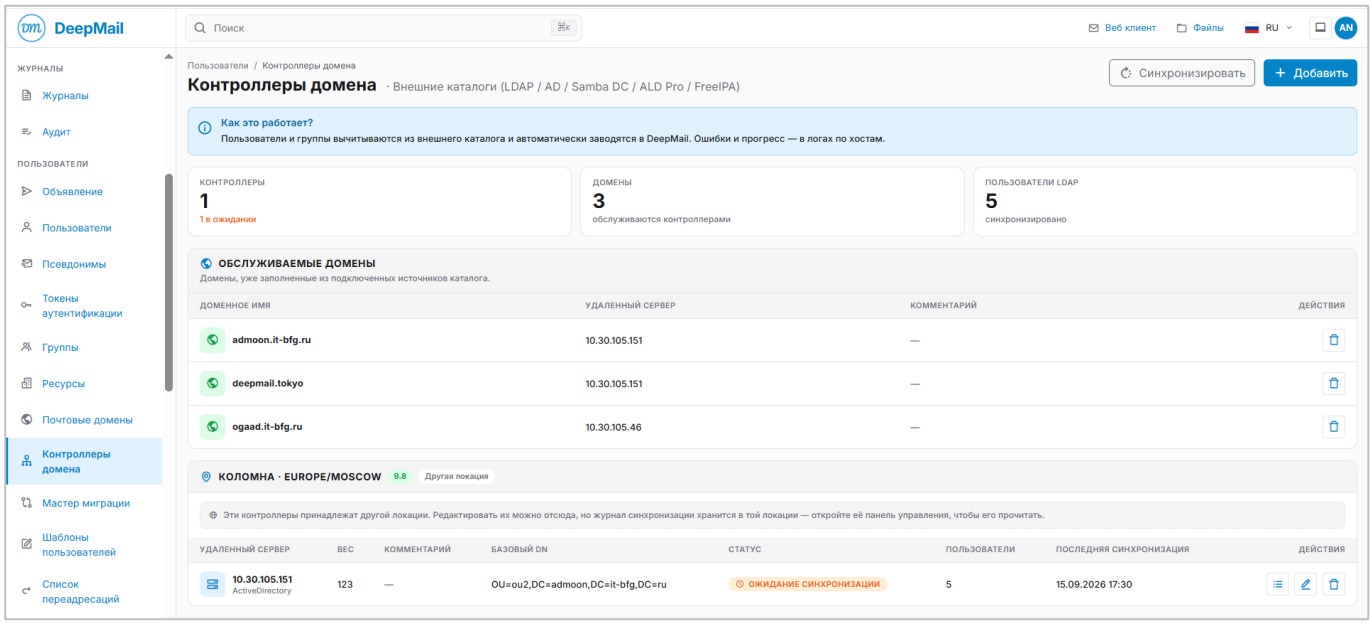
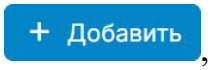


Рисунок 117 – Окно «Контроллеры домена»

Для просмотра журналов (логов) подключенных контроллеров необходимо в списке контроллеров домена нажать кнопку  (см. рисунок 117).

3.4.8.1 Подключение контроллера домена

Для подключения контроллера домена необходимо нажать кнопку 

, расположенную в правом верхнем углу страницы «Контроллеры домена» (см. рисунок 117). В результате на экране появится форма «Добавить контроллер домена», в которой необходимо указать параметры контроллера (рисунок 118).

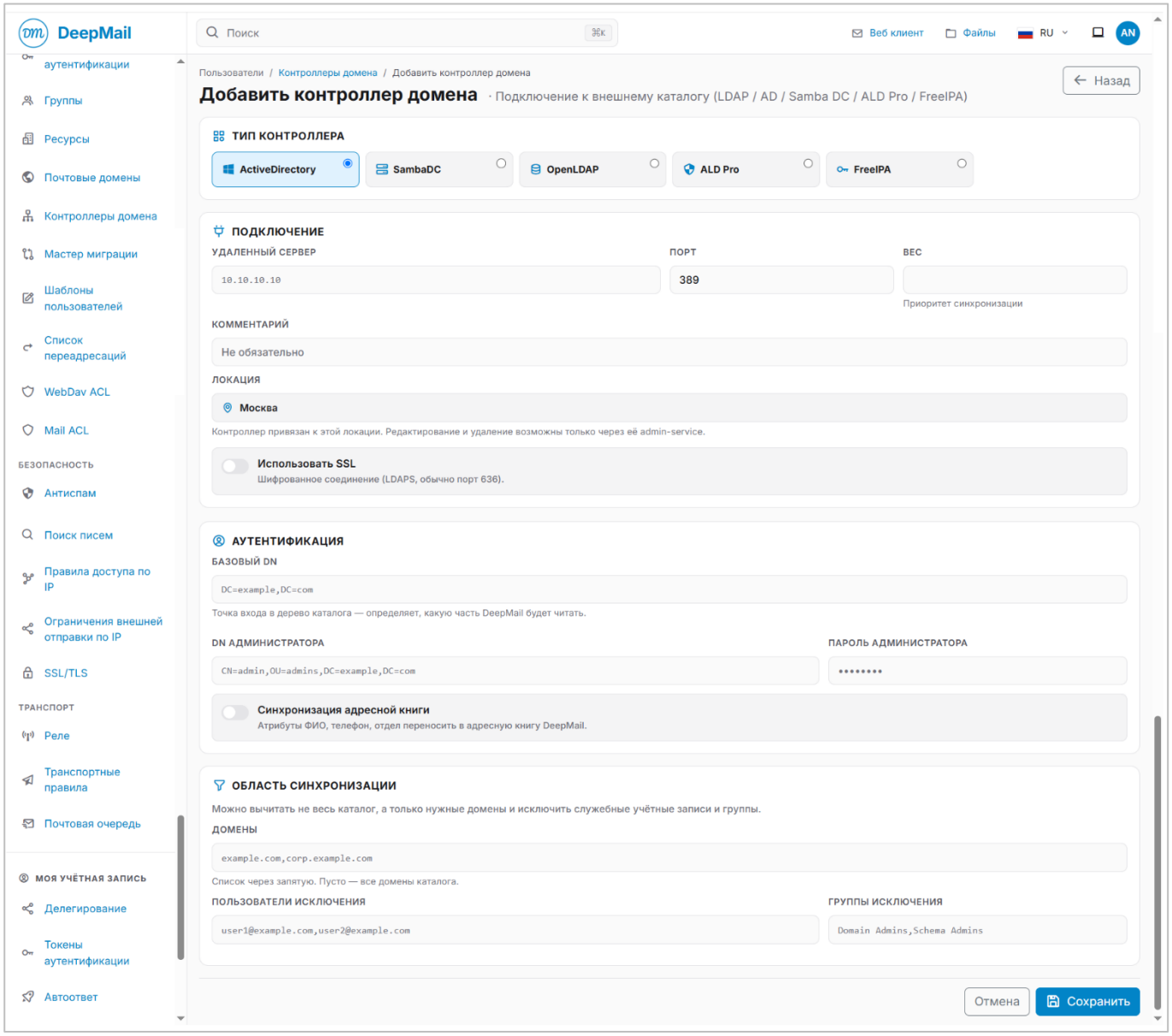


Рисунок 118 – Настройка параметров подключения контроллера домена

В блоке «ТИП КОНТРОЛЛЕРА» отметьте тип подключаемого контроллера домена:

- Active Directory (в ОС Windows);
- Samba DC (Linux-эквивалент);
- OpenLDAP (открытая БД);
- ALD Pro (российский AD-аналог);
- FreeIPA (в ОС Linux).

В блоке «ПОДКЛЮЧЕНИЕ» укажите следующие параметры контроллера:

- в поле «УДАЛЕННЫЙ СЕРВЕР» – IP-адрес контроллера домена;
- в поле «ПОРТ» – порт подключения (обычно 389 (LDAP) или 636 (LDAPS), по умолчанию указан 389);

- в поле «ВЕС» – числовое значение приоритета синхронизации (чем ниже значение, тем выше приоритет);

- поле «КОММЕНТАРИЙ» – информационные заметки (необязательное поле);

- поле «ЛОКАЦИЯ» – географическая привязка контроллера;

- чекбокс «Использовать SSL» – включите, если необходимо шифровать соединение.

В блоке «АУТЕНТИФИКАЦИЯ» необходимо:

- указать параметры для базового доменного имени (Базовый DN) и администратора (DN администратора);

- указать пароль администратора удаленного домена;

- включить чекбокс «Синхронизация адресной книги» если необходимо перенести соответствующие данные в адресную книгу на сервере DeepMail.

В блоке «ОБЛАСТЬ СИНХРОНИЗАЦИИ» необходимо:

- в поле «ДОМЕНЫ» указать домены, которые необходимо считывать из каталога;

- в поле «ПОЛЬЗОВАТЕЛИ ИСКЛЮЧЕНИЯ» указать пользователей, данные которых будут игнорироваться при синхронизации;

- в поле «ГРУППЫ ИСКЛЮЧЕНИЯ» указать группы, данные которых будут игнорироваться при синхронизации.

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.

Для сохранения настроек необходимо нажать кнопку 

(см. рисунок 118).

3.4.8.2 Синхронизация контроллеров домена

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

, при этом информация о подключенных доменах и контроллерах отобразится на странице «Контроллеры домена» (см. рисунок 118).

В начале подключения контроллер домена имеет статус «Ожидание синхронизации», затем статус меняется на «Подключение» или «Синхронизация». Если авторизация

пройдена, подключение выполнено, то статус становится «Успешно». 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.

Информацию о процессе подключения домена и о передаче данных можно посмотреть, нажав кнопку просмотра логов (см. рисунок 117).

Для изменения настроек подключения необходимо нажать кнопку (см. рисунок 117), и внести изменения в появившуюся форму.

3.4.8.3 Удаление контроллера домена

Для удаления контроллера домена необходимо нажать кнопку (см. рисунок 117), и подтвердить удаление в открывшейся модальном окне.

3.4.9 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 адмін-панели необходимо выбрать пункт «Мастер миграции» (см. рисунок 64).

Страница инструмента «Мастер миграции» 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 (рисунок 119).

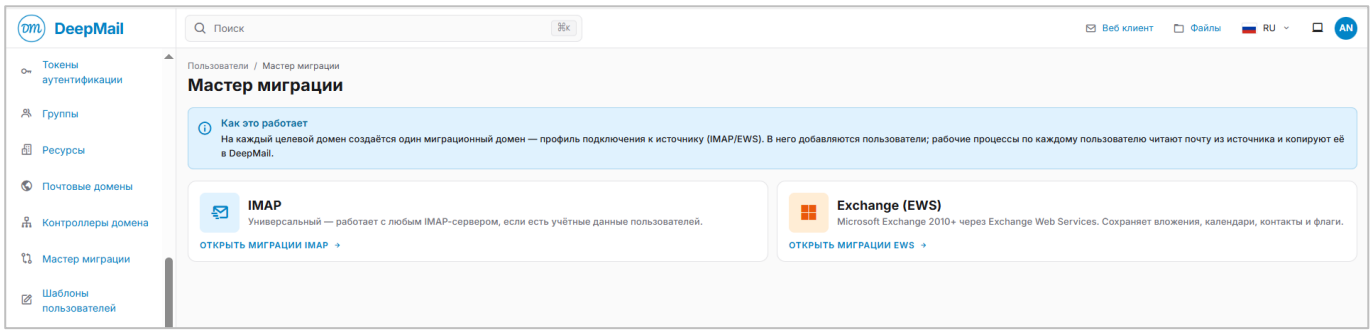


Рисунок 119 – Инструмент «Мастер миграции»

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.

Режим Exchange (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.

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.

2.4.9.1 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 отображаются карточки 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 120).

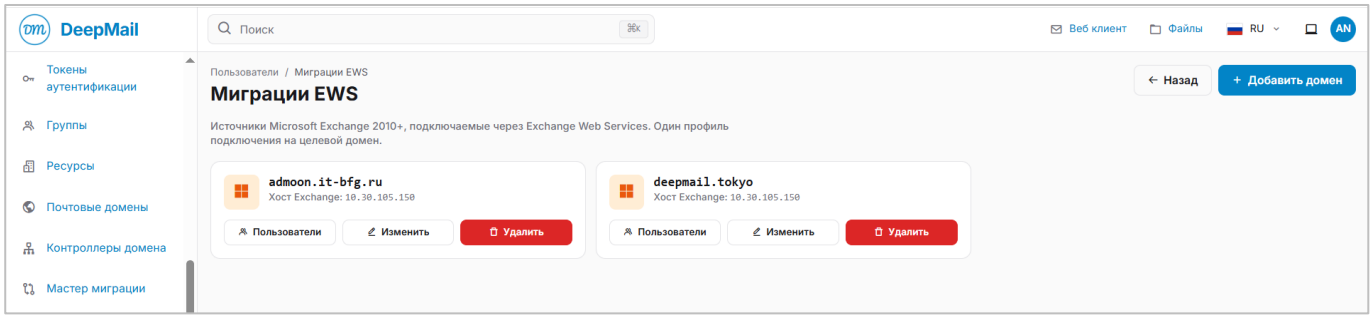


Рисунок 120 – Окно «Миграции EWS»

2.4.9.1.1 Создание настроек миграции и подключение к EWS-серверу

Для добавления домена, с которого требуется перенести данные, необходимо в окне мастера миграции EWS нажать кнопку + Добавить домен (см. рисунок 120), после чего откроется страница создания профиля миграции «Новый EWS-домен миграции» (рисунок 121).

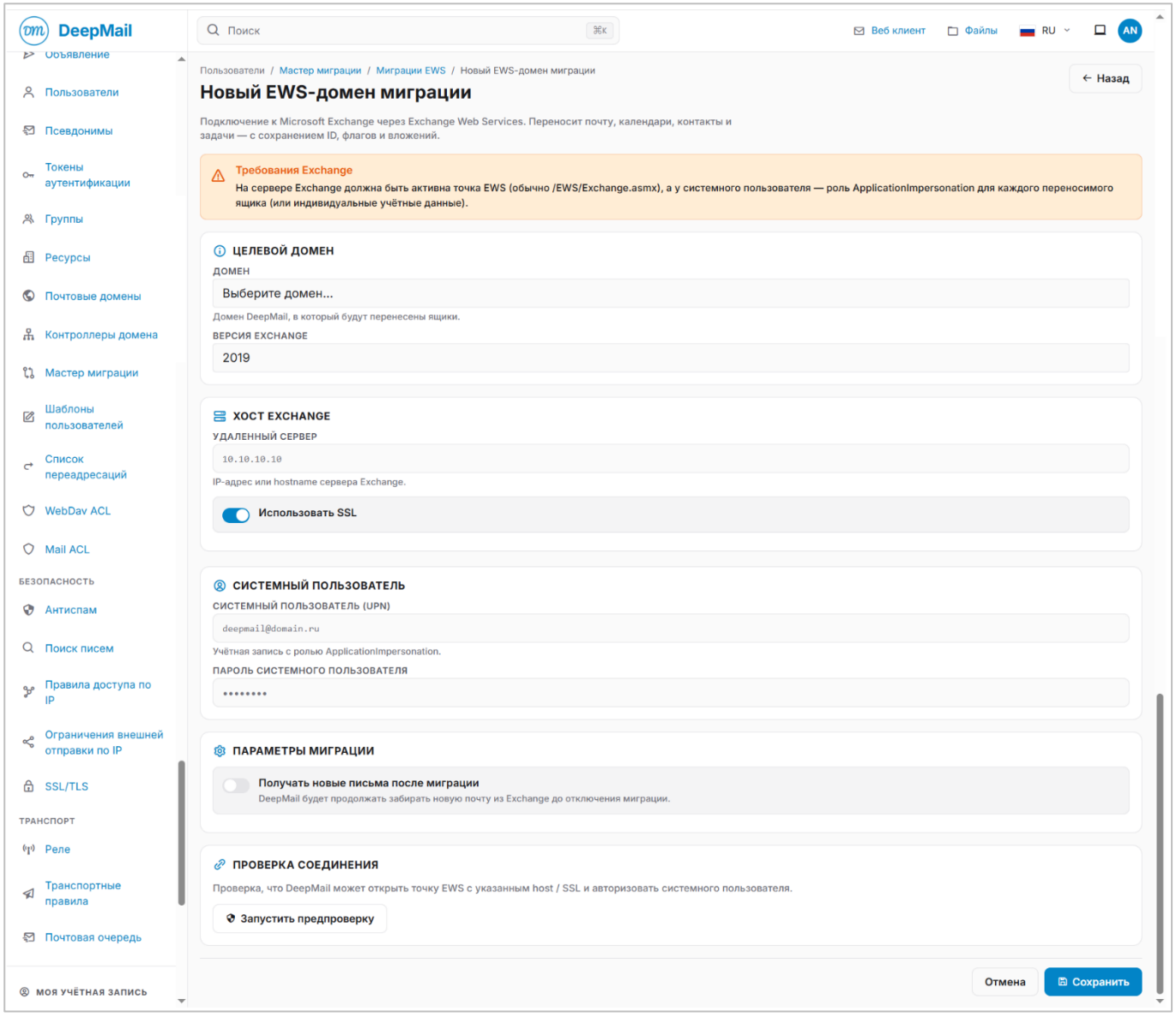


Рисунок 121 – Окно «Создание профиля миграции» EWS

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).

Важно! Внимательно прочитайте и выполните требования к Exchange указанные на странице настроек.

В верхней части страницы расположен блок «ЦЕЛЕВОЙ ДОМЕН» сполями для заполнения:

- «ДОМЕН» – выпадающий список, в котором выбирается целевой почтовый домен DeepMail, в который будут переноситься почтовые ящики. Это связывает создаваемый профиль миграции с конкретным доменом назначения, определяя, в какую структуру будут импортированы почтовые данные;
- «ВЕРСИЯ EXCHANGE» – указывается версия ПО Microsoft Exchange, с которого будут перенесены данные. 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 ее автоматически, но явный выбор повышает надежность.

В блоке «ХОСТ EXCHANGE» указывается IP-адрес или полное доменное имя сервера Exchange. Это обязательный параметр, по которому мастер миграции будет устанавливать соединение. Ниже расположен чекбокс «Использовать SSL»: его активация включает шифрование трафика между DeepMail и Exchange по протоколу HTTPS, что рекомендуется для безопасной передачи учетных данных и содержимого почтовых ящиков.

Ключевым элементом настройки является блок «СИСТЕМНЫЙ ПОЛЬЗОВАТЕЛЬ». Для миграции требуется учетная запись, обладающая правами ApplicationImpersonation, что позволяет серверу DeepMail действовать от имени любого пользователя в целевом домене. В поле «СИСТЕМНЫЙ ПОЛЬЗОВАТЕЛЬ (UPN)» вводится адрес электронной почты этой учетной записи (например, migration@domain.ru), а в поле «ПАРОЛЬ СИСТЕМНОГО ПОЛЬЗОВАТЕЛЯ» – его пароль. Без корректных учетных данных мастер не сможет получить доступ к почтовым ящикам пользователей на стороне сервера Microsoft Exchange.

Чекбокс «Получать новые письма после миграции» управляет поведением системы в отношении сообщений, которые могут поступить на Exchange в процессе переноса. Если чекбокс включен, 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.

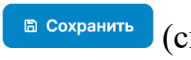
В блоке «ПРОВЕРКА СРЕДИНЕНИЯ» находится кнопка «Запустить предпроверку». Предпроверка должна быть выполнена первой: она проверяет доступность EWS-сервиса, корректность учетных данных и возможность обнаружения почтовых ящиков указанного домена. Только после успешного завершения предпроверки имеет смысл сохранять профиль и переходить к управлению списком пользователей.

В форме будет отображен статус предпроверки, где динамически отображается ход выполнения проверок. 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 учетная 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 (зеленая отметка) или ошибкой (красная). Только после прохождения всех трех 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.

После завершения предпроверки нажмите кнопку 

(см. рисунок 121). Форма создания профиля домена миграции закроется, на странице «Миграции EWS» появится карточка созданного профиля.

2.4.9.1.2 Запуск миграции EWS-сервера

Чтобы запустить миграцию для выбранного домена необходимо на странице «Миграции EWS» в карточке профиля нажать кнопку

(см. рисунок 120), и в открывшейся форме «Список пользователей для миграции» сделать необходимые настройки (см. рисунок 122).

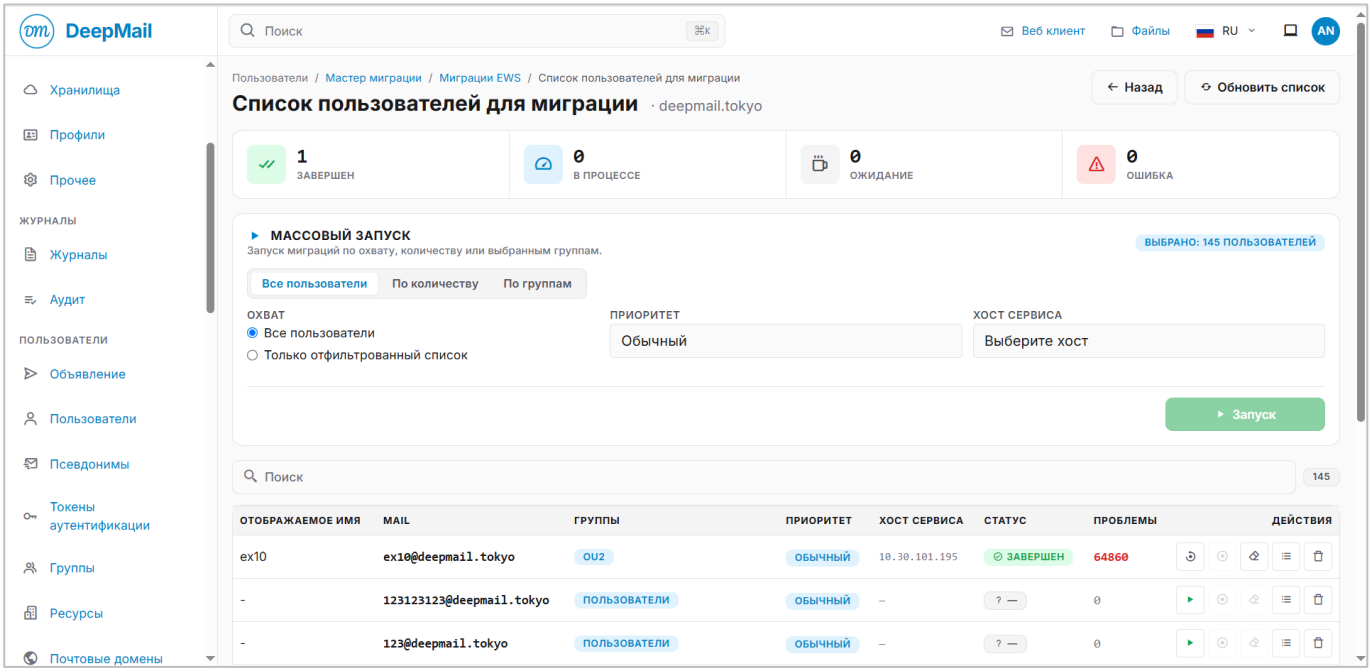


Рисунок 122 – Окно «Список пользователей для миграции»

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 сервер DeepMail.

В верхней части экрана всегда отображается имя домена, к которому относится текущая миграция, чтобы администратор четко понимал, с какими УЗ работает. Также тут расположена кнопка 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.

В нижней области находится панель управления списком. Над списком 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 задает 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 распределенной среде администратор может направить нагрузку на определенный сервер, выбрав его из выпадающего списка. Завершается настройка нажатием кнопки 

, после чего система начинает перенос данных, а статусы пользователей в списке начинают обновляться.

В верхней части страницы отображается общее количество пользователей домена и четыре цветных индикатора с подписями «Завершен», «В процессе», «Ожидание» 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 (запуск миграции для одного пользователя, перезапуск, очистить, журналы, удалить).

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 

. Если требуется перенести не всех сразу, применяется поиск или фильтр по статусу, а в блоке массового запуска выбирается охват «Только отфильтрованный список». Затем задается приоритет и хост, после чего нажатием кнопки 

стартует выполнение задачи. Статусы ящиков последовательно переходят из «Ожидание» в «В процессе», а затем в «Завершен» или «Ошибка». В случае ошибки администратор может просмотреть детали журнала логов (например, неверные учетные 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 перенесенные 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.

2.4.9.1.3 Удаление настроек миграции EWS

Чтобы удалить настройки миграции EWS для выбранного домена необходимо в окне мастера миграции EWS нажать кнопку Удалить (см. рисунок 120), и в открывшемся модальном окне 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.

2.4.9.2 Инструмент мастер миграции классический IMAP

Окно «Миграции IMAP» содержит список сторонних доменов (при наличии), подключенных к серверу АРМ «DeepMail» с отображением статуса подключения и кнопками действий (рисунок 123).

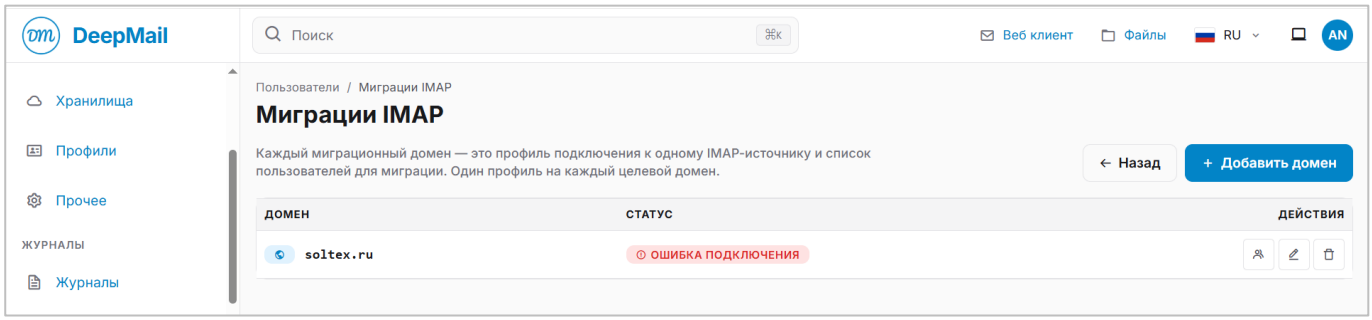


Рисунок 123 – Окно «Миграции IMAP»

Для изменения настроек миграции необходимо в строке домена нажать кнопку (см. рисунок 123). В результате откроется страница с формой изменения параметров домена IMAP-миграции с настройками миграции, доступными для редактирования.

Для просмотра списка пользователей, чьи аккаунты требуется перенести в новый домен, необходимо нажать кнопку (см. рисунок 123). В результате на экране отобразится форма «Список пользователей для миграции» (рисунок 124).

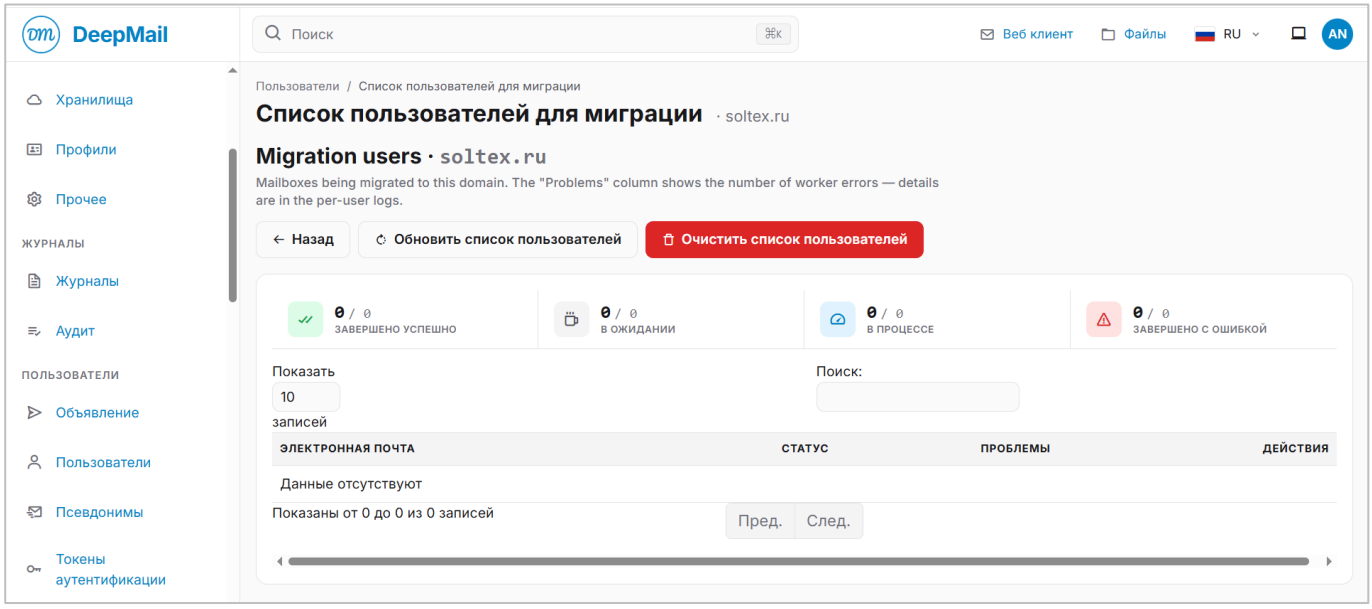


Рисунок 124 – Список для миграции

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.

Обновить информацию о статусе миграции можно с помощью кнопки Обновить список пользователей (см. рисунок 124).

Удалить пользователей из списка можно с помощью кнопки Очистить список пользователей (см. рисунок 124).

2.4.9.2.1 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 119).

Откроется страница с формой настройки миграции IMAP (рисунок 125).

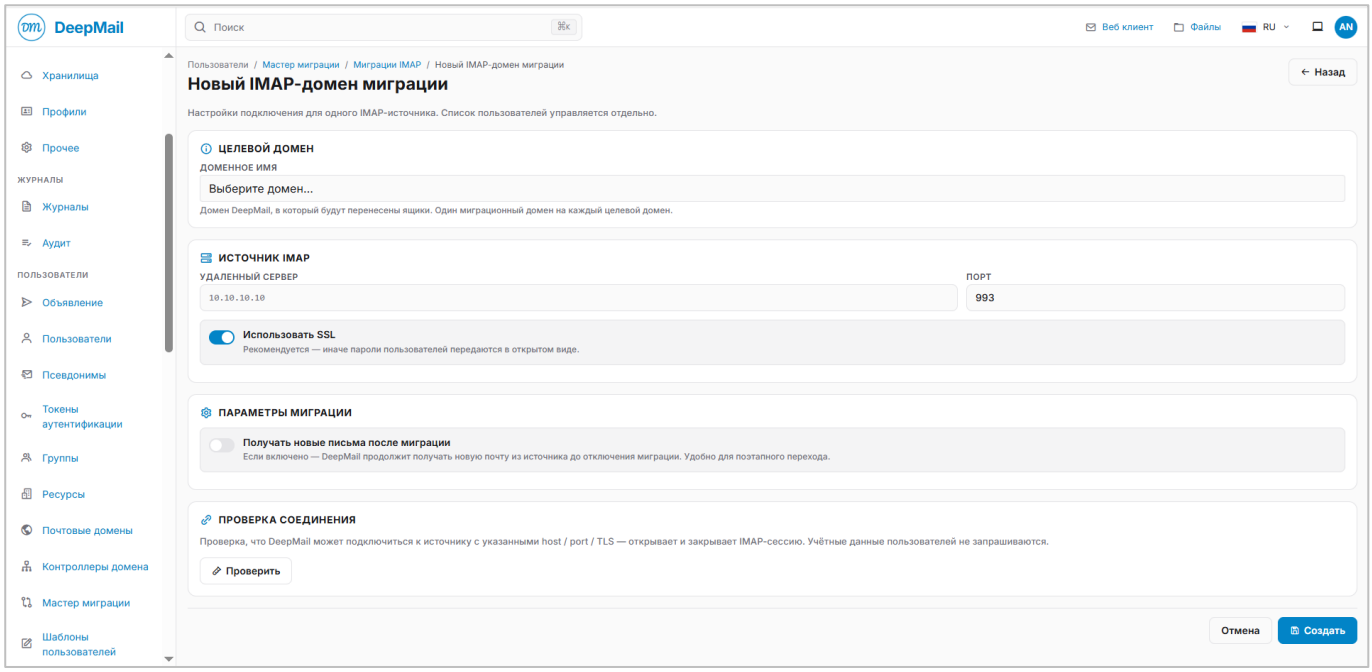


Рисунок 125 – Настройка миграции IMAP

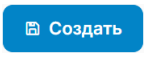
Настройка миграции состоит из следующих блоков:

- «ЦЕЛЕВОЙ ДОМЕН» – выпадающий список, в котором выбирается целевой почтовый домен DeepMail, в который будут переноситься почтовые ящики. Это связывает создаваемый профиль миграции с конкретным доменом назначения, определяя, в какую структуру будут импортированы почтовые данные;
- «ИСТОЧНИК IMAP» – настройка подключения к серверу по IMAP, тут указывается IP-адрес стороннего сервера. Это обязательный параметр, по которому мастер миграции будет устанавливать соединение. Ниже расположен чекбокс «Использовать SSL»: его активация включает шифрование трафика между DeepMail и сторонним сервером по протоколу HTTPS, что рекомендуется для безопасной передачи учетных данных и содержимого почтовых ящиков;
- «ПАРАМЕТРЫ МИГРАЦИИ» – чекбокс «Получать новые письма после миграции» управляет поведением системы в отношении сообщений, которые могут поступить на сторонний сервер в процессе переноса. Если чекбокс включен, 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;

- «ПРОВЕРКА СОЕДИНЕНИЯ» – при нажатии на кнопку 

выполняется проверка того, что DeepMail может подключиться к источнику с введенными параметрами подключения.

После успешной проверки для сохранения настроек нажмите кнопку 

(см. рисунок 125).

2.4.9.1.4 Удаление настроек миграции для домена

Чтобы удалить настройки миграции для выбранного домена необходимо в окне мастера миграции нажать кнопку  (см. рисунок 123), и в открывшемся модальном окне 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.

3.4.10 Инструмент «Шаблоны пользователей»

Инструмент «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 админ-панели необходимо выбрать пункт «Шаблоны пользователей» (см. рисунок 64).

На странице шаблонов пользователей в центральной части экрана будут расположены карточки существующих шаблонов (при наличии) (рисунок 126).

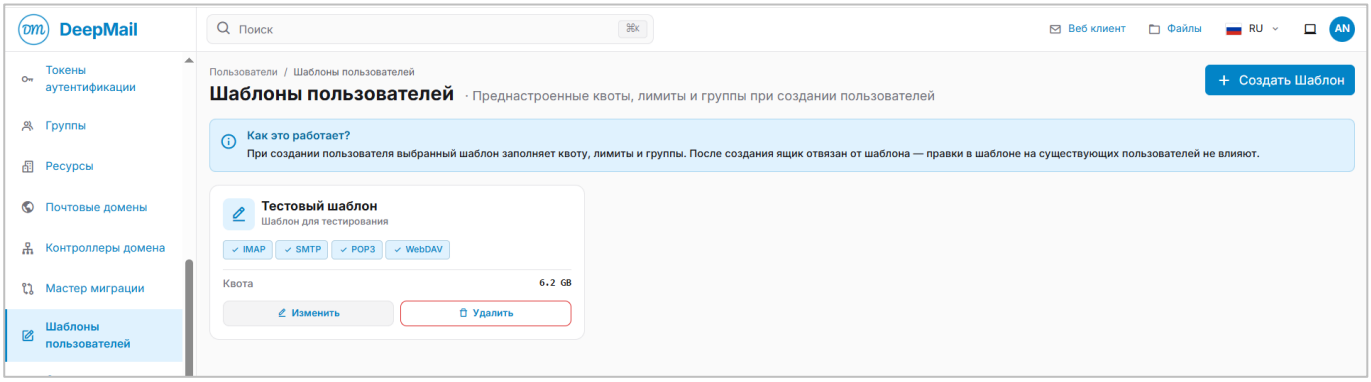
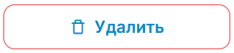


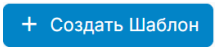
Рисунок 126 – Страница шаблонов пользователей

Для каждого шаблона отображаются его имя и краткий комментарий, поясняющий назначение, иконки настроенных протоколов и размер квоты, также в карточке присутствует кнопка

, позволяющая открыть форму редактирования параметров выбранного шаблона и кнопка 

для удаления шаблона.

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 нем параметры будут автоматически применены к ящику, что значительно экономит время и снижает риск ошибок.

Для добавления шаблона необходимо нажать на кнопку 

(см. рисунок 126), после чего откроется страница с формой настроек шаблона, в которой находятся общие настройки, настройки квот и лимитов, протоколов и параметров доступа (рисунок 127).

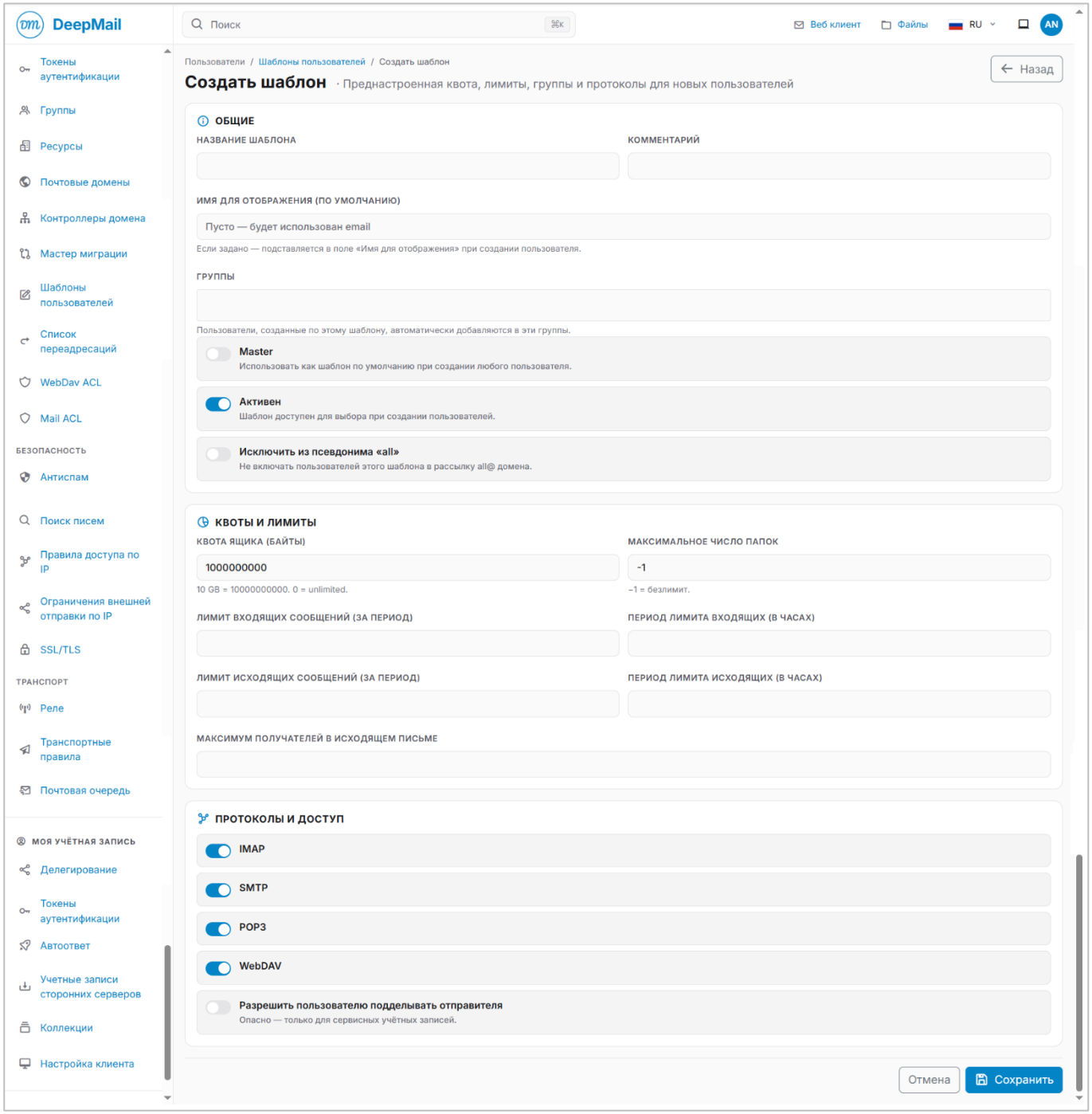


Рисунок 127 – Настройка Шаблона пользователей – Функции и квоты

В блоке «ОБЩИЕ» (см. рисунок 127) задаются базовые атрибуты шаблона. В поле «НАЗВАНИЕ ШАБЛОНА» вносится уникальное имя, по которому администратор будет идентифицировать набор настроек (например, «Сотрудник», «Внешний партнер»). «КОММЕНТАРИЙ» позволяет добавить краткое описание, поясняющее назначение шаблона. «ИМЯ ДЛЯ ОТОБРАЖЕНИЯ (ПО УМОЛЧАНИЮ)» задает имя, которое будет подставляться по умолчанию в поле «ИМЯ ДЛЯ ОТОБРАЖЕНИЯ» в форме создания новых ящиков. В поле «ГРУППЫ» администратор может указать, в какие группы каталога будет автоматически включен пользователь при создании по данному шаблону.

Дополнительно предусмотрены чекбоксы:

- «Master» – назначает шаблон используемым по умолчанию для всех новых пользователей (т.е. форма создания нового пользователя при открытии сразу будет заполнена по данному шаблону);
- «Активен» – определяет, будет ли шаблон доступен для выбора в писке шаблонов;
- «Исключить из псевдонима «all» – позволяет исключить учетную запись, созданную по данному шаблону, из общей группы рассылки, охватывающей всех пользователей домена.

Блок «КВОТЫ И ЛИМИТЫ» (см. рисунок 127) содержит параметры ресурсных ограничений. Тут задается 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 определенный период (в часах), а также задать максимум получателей в одном исходящем письме.

Ниже расположен блок настройки доступных протоколов и прав. Флажки «IMAP», «SMTP», «POP3», «WebDAV» позволяют предопределить, какие протоколы будут включены для пользователя.

Отдельная опция «Разрешить пользователю подделывать отправителя» дает возможность менять адрес в поле «От» при отправке.

После внесения необходимых изменений и дополнительных настроек нажмите кнопку 

(см. рисунок 127).

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 учетной записи, что обеспечивает единообразие конфигурации и ускоряет массовое создание пользователей.

3.4.11 Список переадресаций

Инструмент «Список переадресаций» позволяет администратору настроить пересылку писем пользователей на адреса других доверенных пользователей.

Для настройки переадресаций необходимо в меню админ-панели необходимо выбрать пункт «Список переадресаций» (см. рисунок 64). Откроется страница инструмента «Список переадресаций» (рисунок 128).

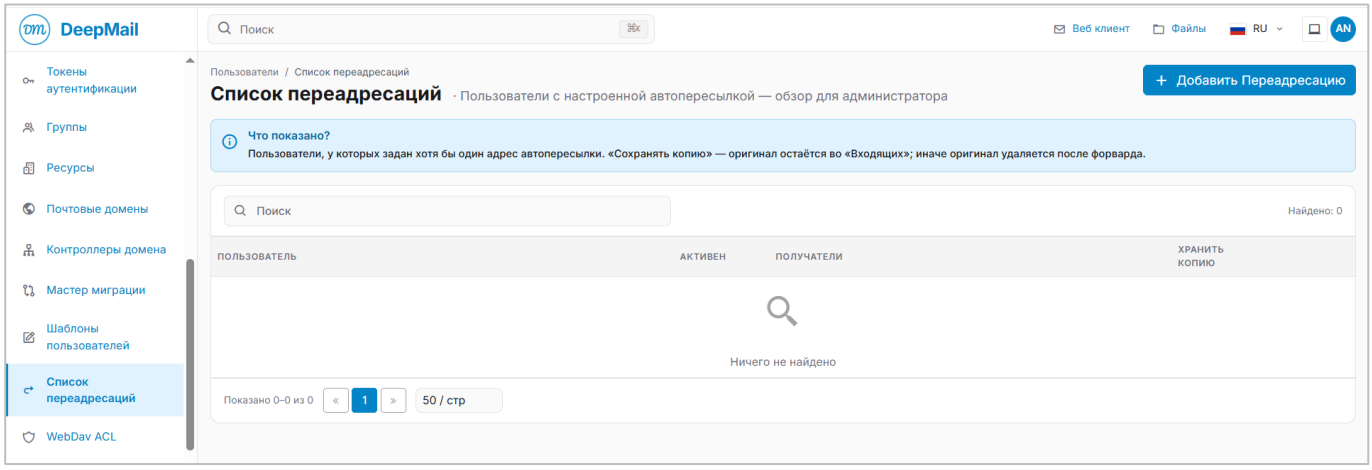


Рисунок 128 – Инструмент «Список переадресаций»

Для настройки переадресации необходимо на странице инструмента «Список переадресаций» нажать кнопку + Добавить Переадресацию, после чего откроется страница с формой «Добавить переадресацию» для настройки переадресаций (рисунок 129).

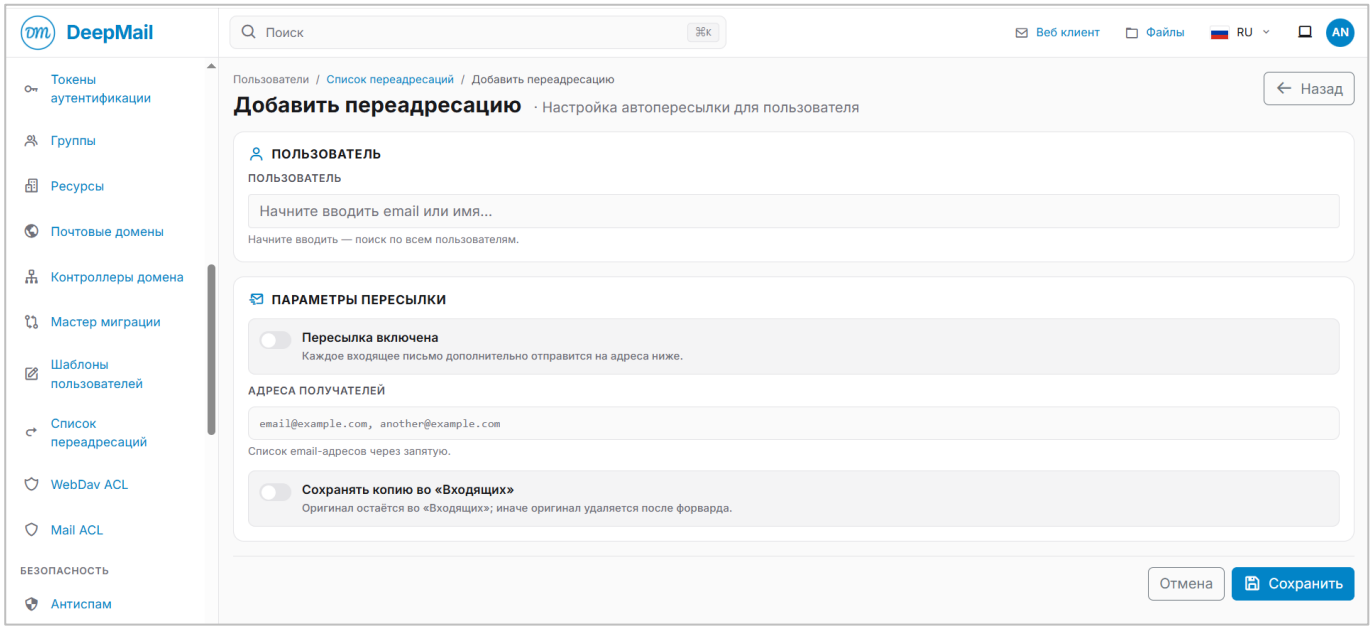


Рисунок 129 – Настройка переадресаций

В данной форме необходимо заполнить поля:

- «ПОЛЬЗОВАТЕЛЬ» – электронный адрес пользователя чья корреспонденция будет переадресовываться;
- «АДРЕСА ПОЛУЧАТЕЛЕЙ» – электронные адреса пользователей, на которые будут переадресовываться письма (один или несколько через запятую).

Для активации переадресации необходимо включить чекбокс «Пересылка включена» (см. рисунок 129).

При необходимости сохранения копий писем в почтовом ящике первоначального получателя необходимо включить параметр «Сохранять копию во «Входящих» (при включении оригинал письма останется в исходной папке «Входящие», если отключен, то оригинал удаляется после пересылки).

Для завершения настройки переадресации нажмите кнопку Сохранить (см. рисунок 129).

На странице «Список переадресаций» появится сообщение о том, что переадресация добавлена, в списке появится добавленная переадресация ().

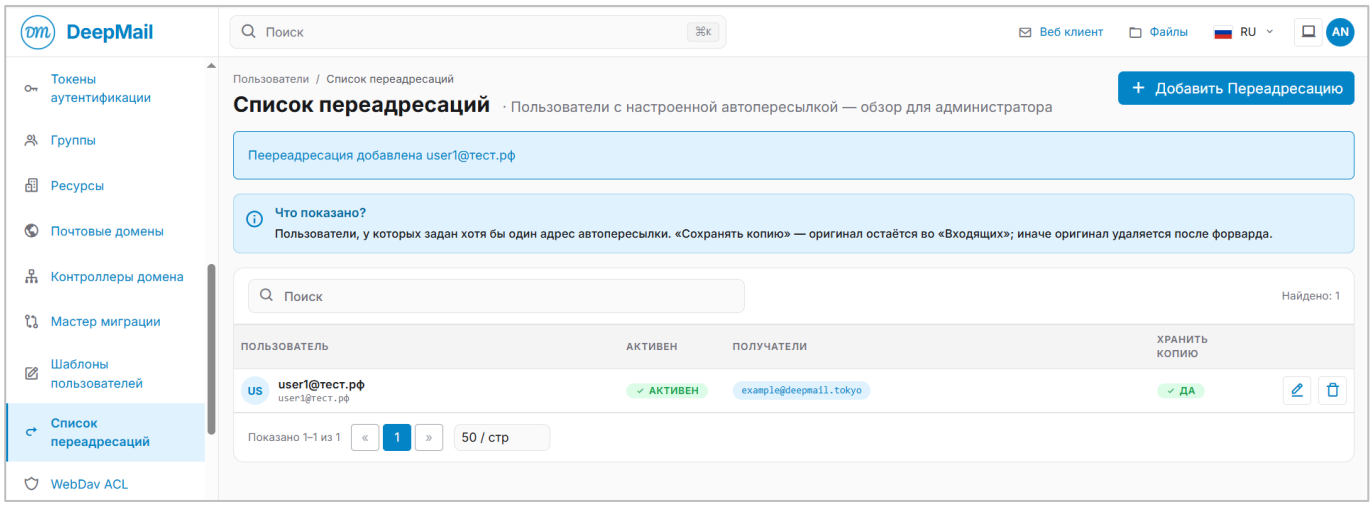


Рисунок 130 – Страница «Список переадресаций» с добавленной переадресацией

3.5 Раздел «Безопасность»

Раздел «Безопасность» – это инструменты, отвечающие за защиту почтовой инсталляции:

- «Антиспам» – переход в WebUI rspamd (в новой вкладке) для просмотра статистики, истории сканирования и ручной проверки писем;
- «Поиск писем» – асинхронный IMAP-поиск по ящикам пользователей, а также выгрузка результатов и возможность удалить найденные сообщения;
- «Правила доступа по IP» – реакция Postfix на входящие SMTP-соединения с указанных IP: REJECT, REDIRECT, DISCARD, HOLD, OK;
- «Ограничения внешней отправки по IP» – «черный список» IP-источников, с которых запрещена отправка «наружу» (внутренняя переписка при этом работает);
- «Настройки SSL/TLS» – сертификат, который инсталляция предъявляет клиентам. (рисунок 131).

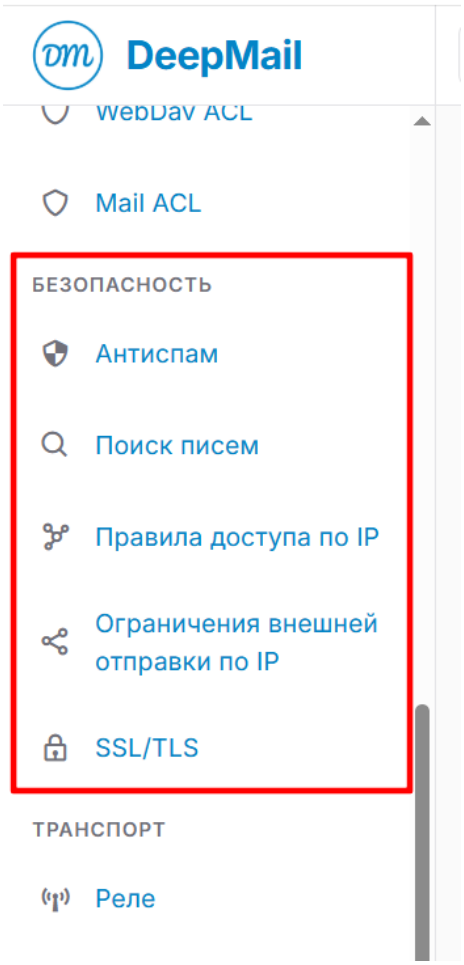


Рисунок 131 – Раздел «Безопасность»

3.5.1 Инструмент «Антиспам»

Для перехода к инструменту работы с системой спам-фильтрации необходимо в меню админ-панели выбрать пункт «Антиспам» (см. рисунок 131).

В результате откроется новая страница системы фильтрации спама RSPAMD, содержащая статистические данные и информацию о параметрах спам-фильтрации (рисунок 132).

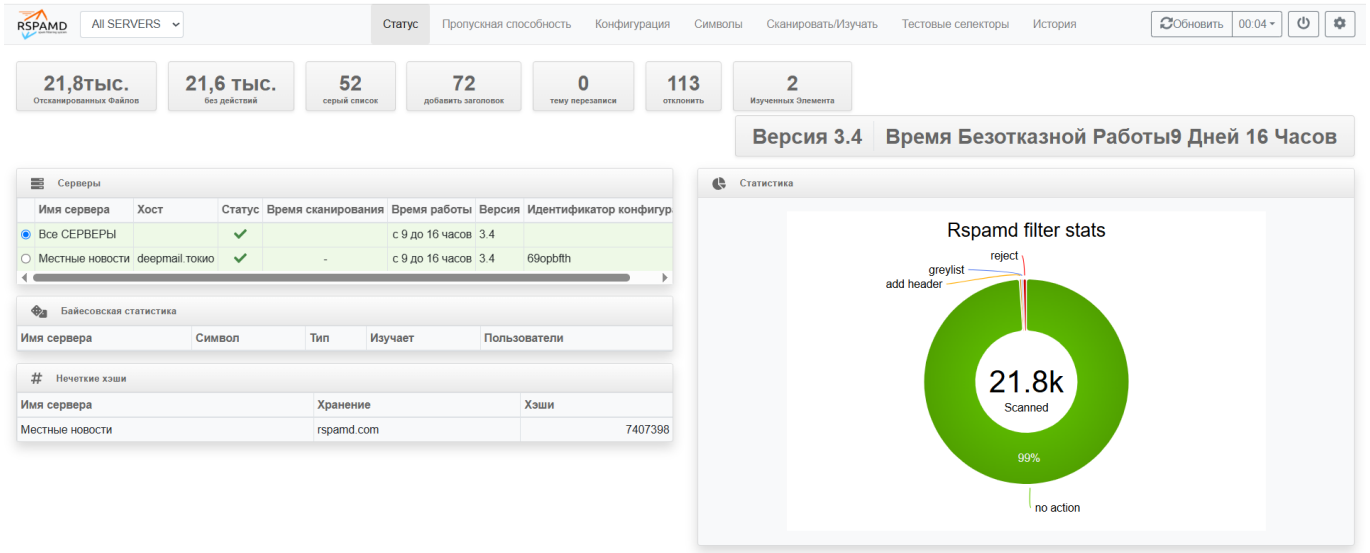


Рисунок 132 – Окно системы RSPAMD

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 133).

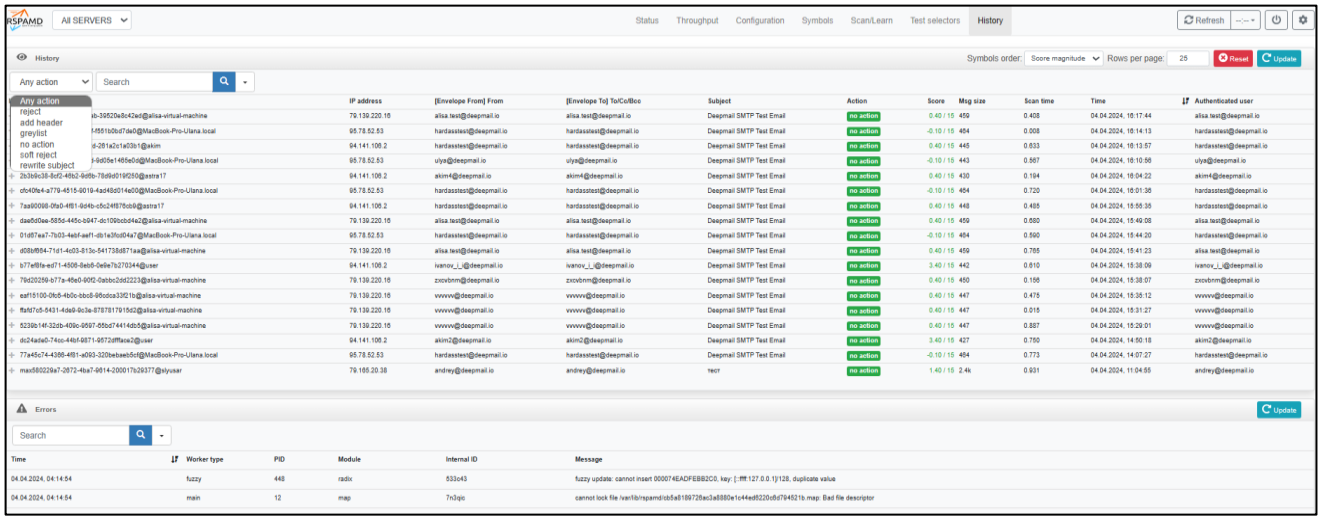


Рисунок 133 – Окно системы RSPAMD, вкладка «History»

3.5.1.1 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.

3.5.1.2 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.

Конфигурационные 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.

3.5.2 Инструмент «Поиск писем»

Инструмент «Поиск писем» позволяет администратору искать сообщения по почтовым ящикам пользователей и при необходимости удалять найденные письма. Это полезно, например, при расследовании инцидентов (массовая рассылка через скомпрометированный ящик, утечка чувствительных данных, фишинговая волна и пр.).

Для перехода к инструменту поиска писем необходимо в меню админ-панели выбрать пункт «Поиск писем» (см. рисунок 131).

Интерфейс представляет собой инструмент для расширенного поиска по почтовому архиву, организованный по принципу управления задачами поиска (рисунок 134).

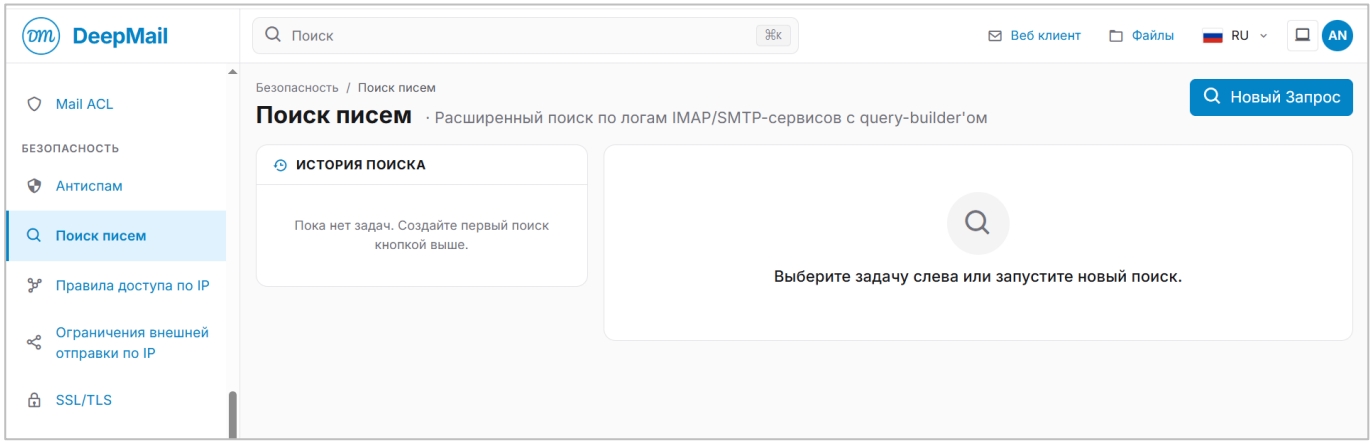
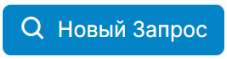


Рисунок 134 – Интерфейс «Поиск писем» без задач в истории поиска

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

Правая, основная рабочая область, на приведенном рисунке содержит приглашение к действию: предложение выбрать задачу из истории или начать новый поиск.

Кнопка 

является ключевым элементом, запускающим процесс создания сложного поискового запроса, с возможностью задания множества критериев (метаданных, периода, отправителей, тем и т.д.).

После нажатия открывается модальное окно «Сформировать запрос» (рисунок 135).

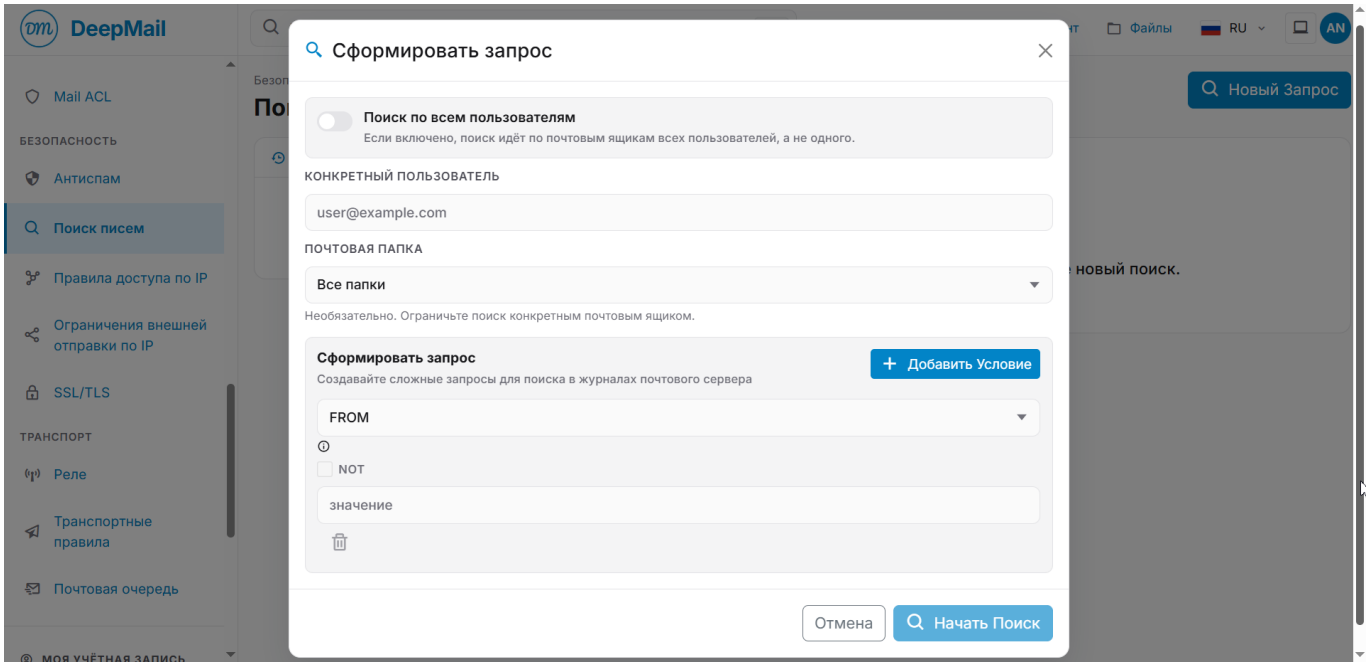


Рисунок 135 – Модальное окно «Сформировать запрос»

Выполняйте поиск по всем пользователям или конкретному пользователю, по конкретным почтовым папкам заполнив соответствующие поля в форме.

В блоке «Сформировать запрос» внесите условия поиска – выберите из выпадающего списка. При наведении на значок ⓘ появляется подсказка для выбранного условия.

Кнопка + Добавить Условие (см. рисунок 135) позволяет добавить еще одну область для ввода критериев отбора писем.

После ввода всех условий нажмите кнопку Начать Поиск (см. рисунок 135).

Модальное окно «Сформировать запрос» закроется и на странице инструмента «Поиск писем» справа отобразится результат, а в левой части добавится запись истории поиска (рисунок 136).

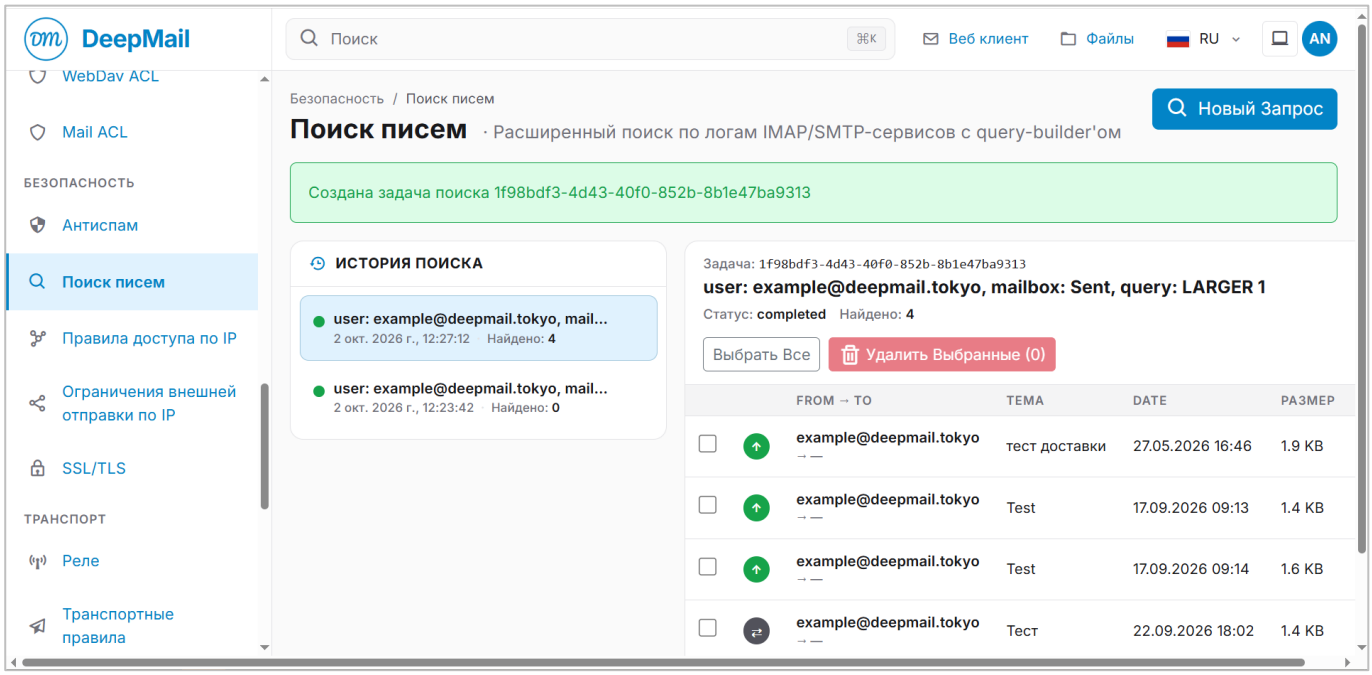


Рисунок 136 – Страница инструмента «Поиск писем» с результатом поиска

Для немедленного удаления писем необходимо выделить отдельные письма или нажать кнопку Выбрать Все (для выбора всех найденных писем) и затем нажать кнопку Удалить Выбранные (1).

Также администратор может просмотреть данные найденных писем щелкнув по строке в результатах поиска. На экране отобразится информация о получателе, метаданные, маршрутизация, данные антиспама, пересылки версия клиентского приложения, с которого отправлено письмо и текст письма (рисунок 137).

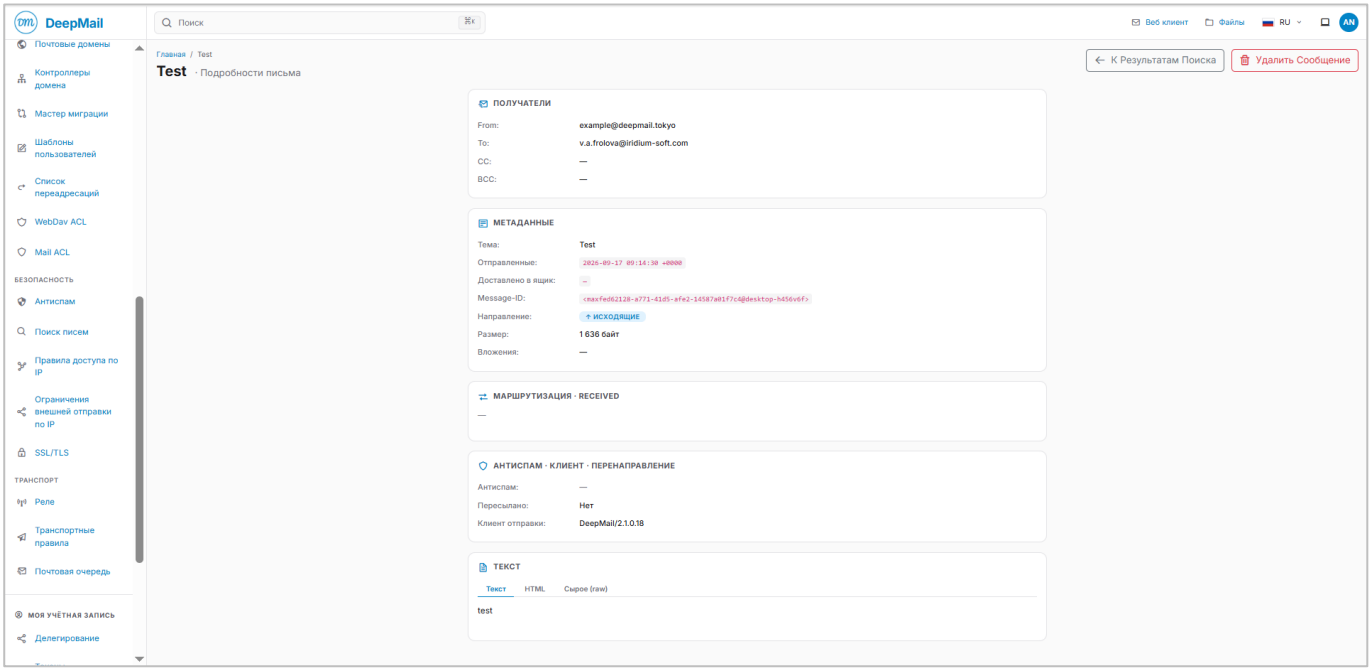


Рисунок 137 – Присмотр данных найденного письма

Для удаления просматриваемого сообщения нажмите кнопку Удалить Сообщение. Для возврата на странице «Поиск писем» нажмите кнопку ← К Результатам Поиска (см. рисунок 137).

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

3.5.3 Инструмент «Правила доступа по IP»

В пункте «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 определенных адресов, и таким образом реализовать гибкую политику безопасности, фильтрации или перенаправления трафика.

Для перехода к инструменту необходимо в меню адмін-панели выбрать пункт «Правила доступа по IP» (см. рисунок 131). Откроется страница «Правила доступа по IP» (рисунок 138).

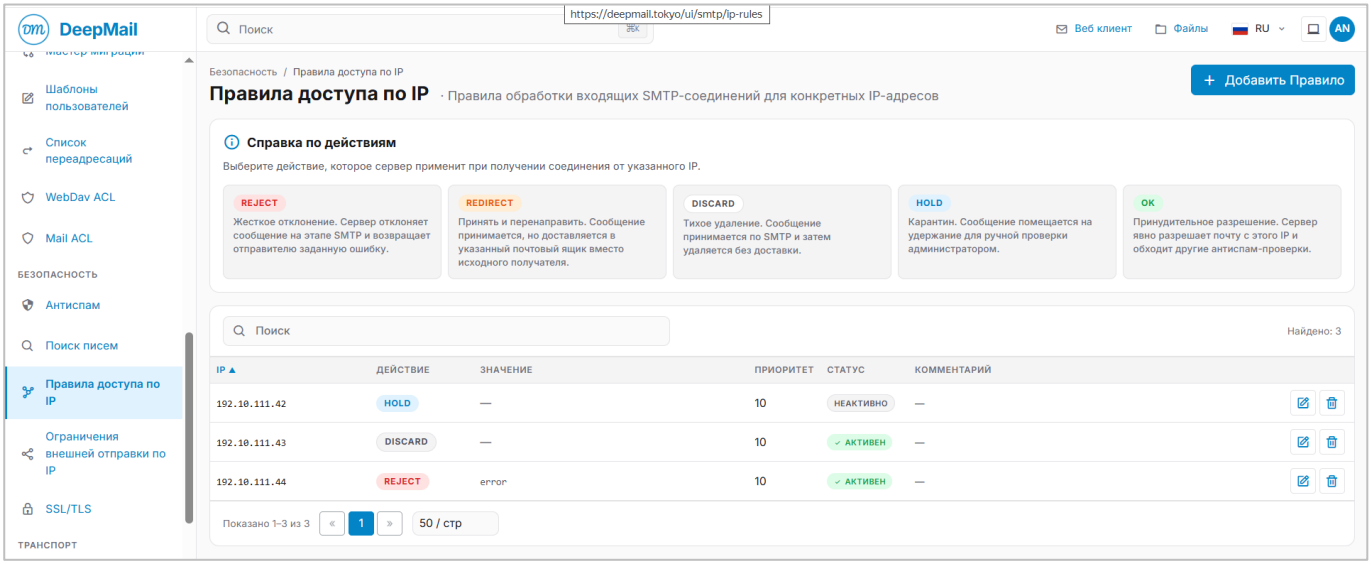


Рисунок 138 – Окно «Правила доступа по IP»

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 приеме 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 «черных 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), иконка выбранного действия, значение (например, текст ошибки для REJECT или целевой адрес для

REDIRECT), приоритет, статус активности, комментарий. Для каждого правила доступны действия – кнопка  для редактирования и кнопка  для удаления.

Для добавления правила нажмите кнопку 

(см. рисунок 138). Откроется форма «Создать правило IP» (рисунок 139).

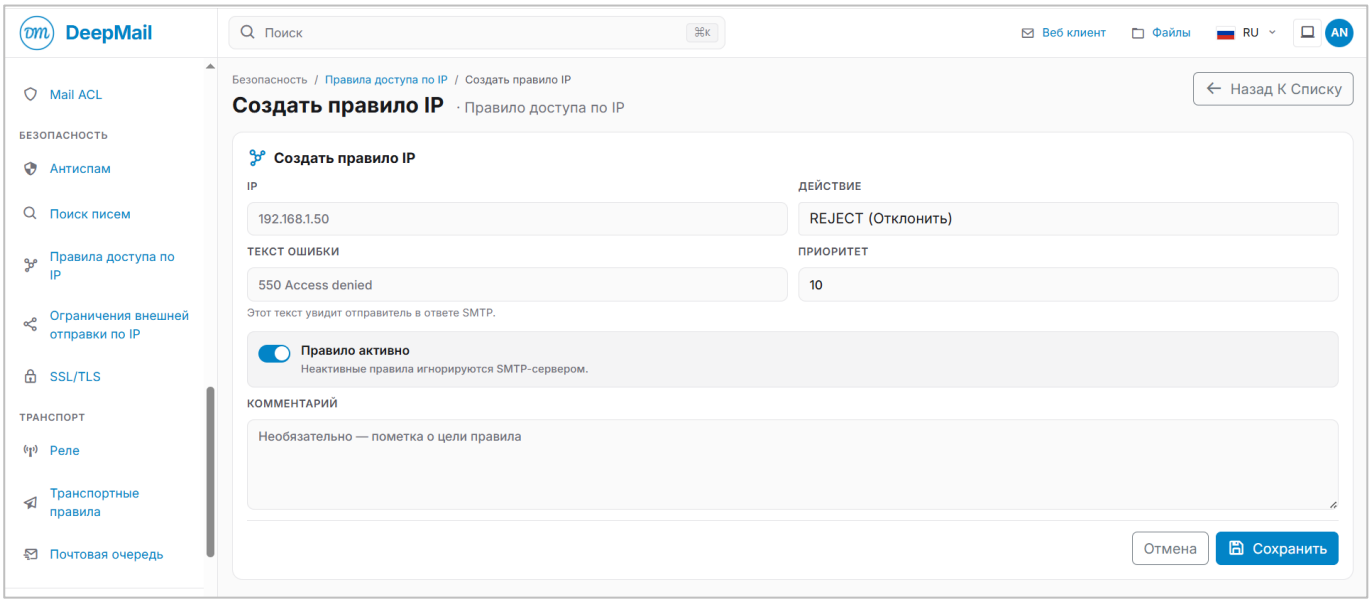
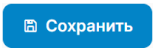


Рисунок 139 – Форма «Создать правило IP»

Заполните поля формы и нажмите кнопку 

. Созданное правило появится в списке правил на странице «Правила доступа по IP».

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.

3.5.4 Инструмент «Ограничения внешней отправки по IP»

Инструмент «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

Для перехода к инструменту необходимо в меню адмін-панели выбрать пункт «Ограничения внешней отправки по IP» (см. рисунок 131). Откроется страница «Ограничения внешней отправки по IP» (рисунок 140).

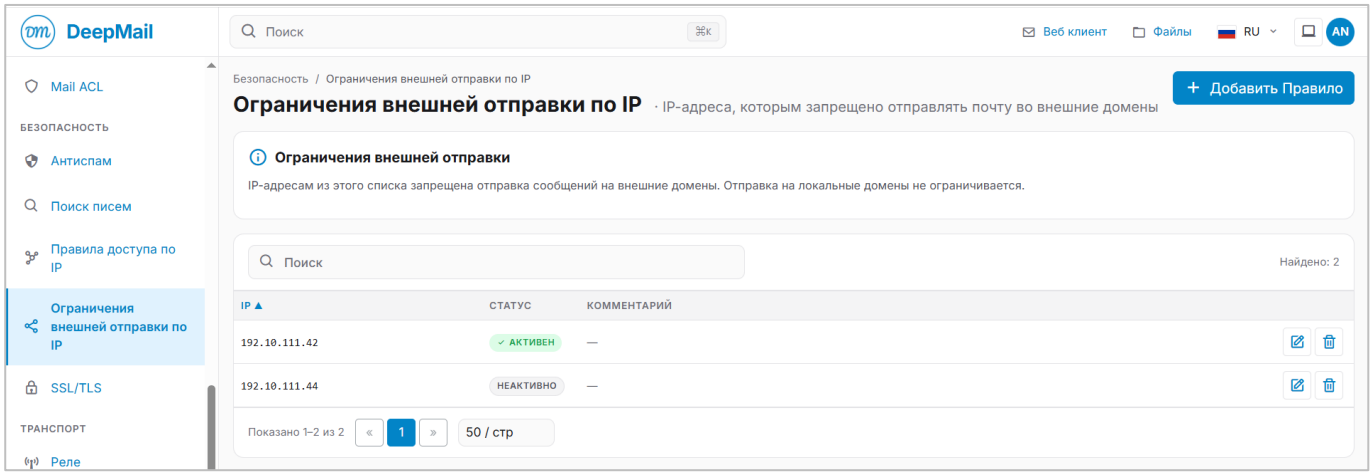


Рисунок 140 – Страница «Ограничение внешней отправки по IP»

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), иконка статуса активности (Активен/ Неактивен) и комментарий. Для каждого IP предусмотрены действия – кнопка  для редактирования и кнопка  для удаления. Поиск по списку позволяет быстро находить нужные записи.

Для добавления правила нажмите кнопку 

(см. рисунок 140). Откроется форма «Создать правило внешней отправки» (рисунок 141).

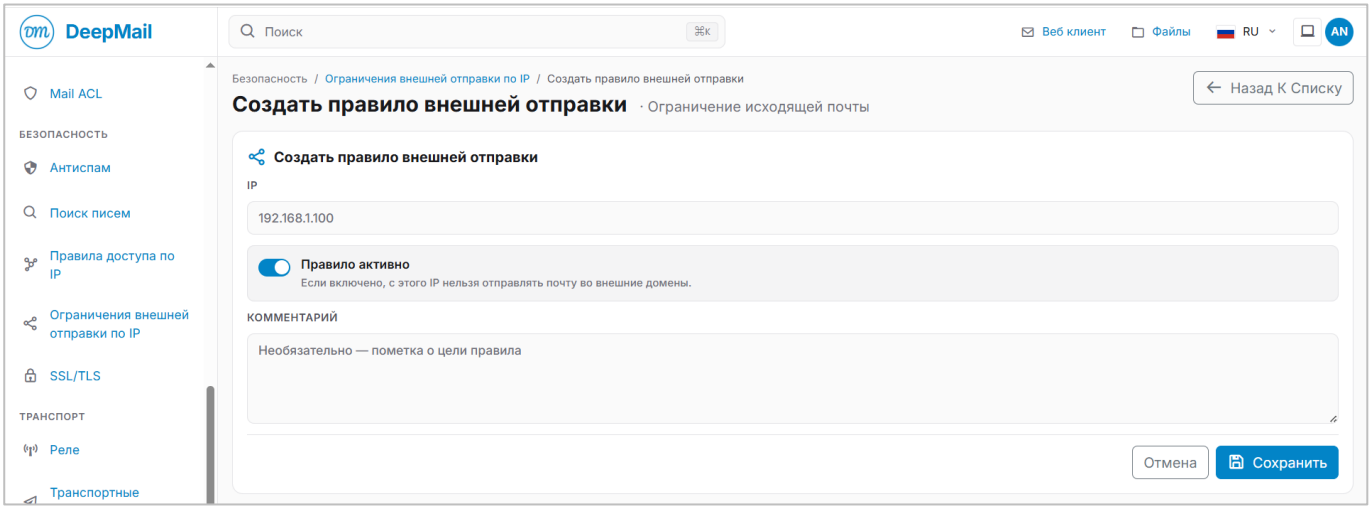


Рисунок 141 – Форма создания правила внешней отправки

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 «Правило активно».

Для завершения нажмите кнопку Сохранить (см. рисунок 141). Созданное правило появится в списке правил на странице «Ограничение внешней отправки по IP».

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

3.5.5 Инструмент «Настройки SSL/TLS»

Для перехода к настройкам SSL/TLS необходимо в меню админ-панели выбрать пункт «Настройки SSL/TLS» (см. рисунок 131).

На экране отобразится окно «Настройки SSL/TLS» (рисунок 142).

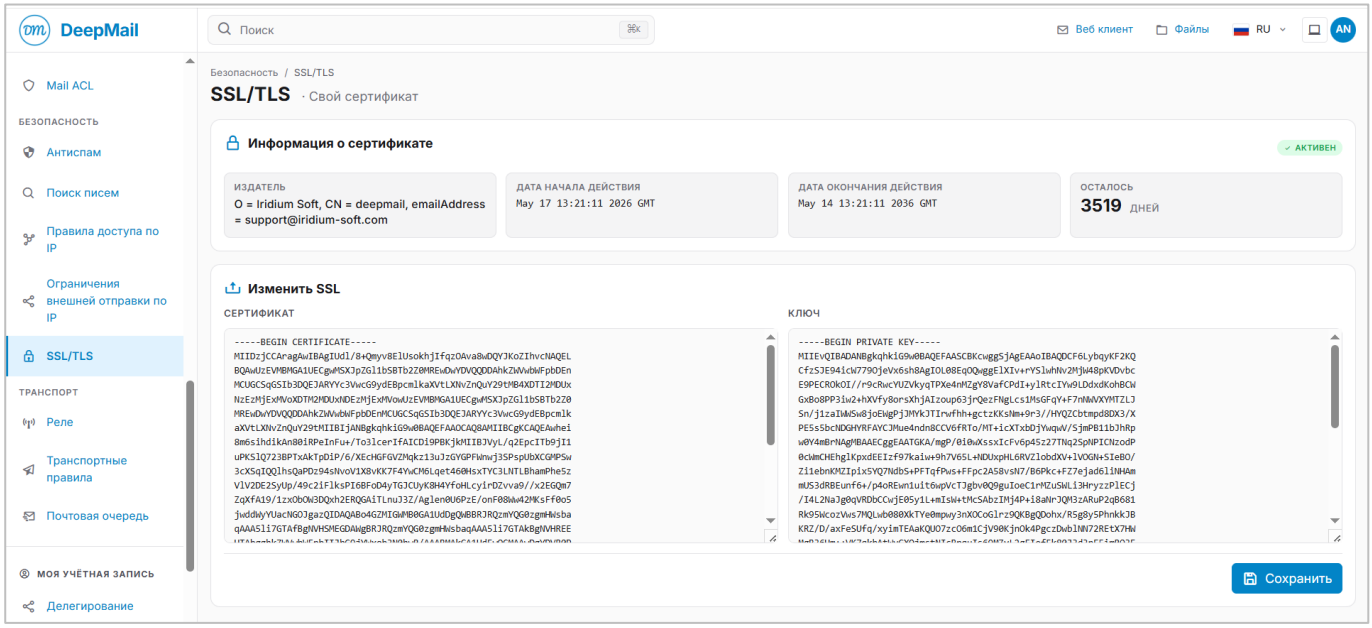


Рисунок 142 – Окно инструмента «Настройки SSL/TLS»

На странице представлена информация о действующем сертификате SSL/TLS – издатель, дата начала, дата окончания и количество оставшихся дней действия сертификата.

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 142) 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 «SSL/TLS обновлен».

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 143).

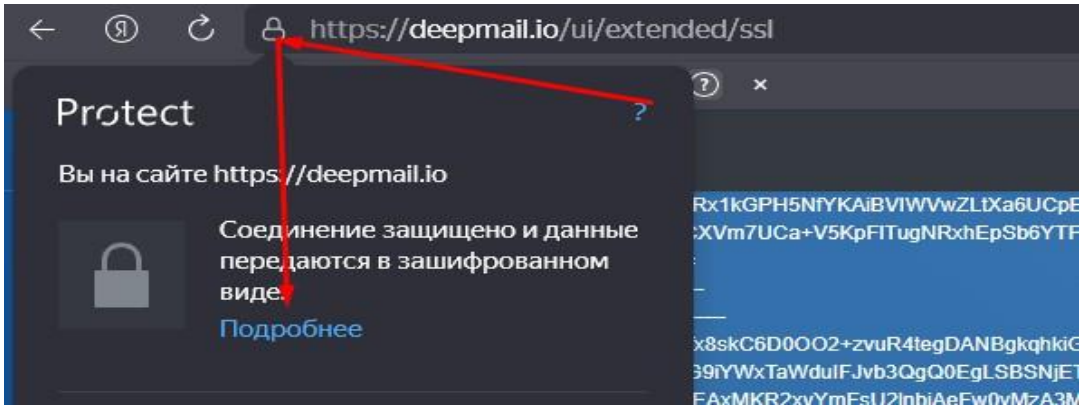


Рисунок 143 – Проверка обновления сертификатов

3.6 Раздел «Транспорт»

Раздел «Транспорт» интерфейса администратора содержит три инструмента: «Реле», «Транспортные правила», «Почтовая очередь» (рисунок 144).

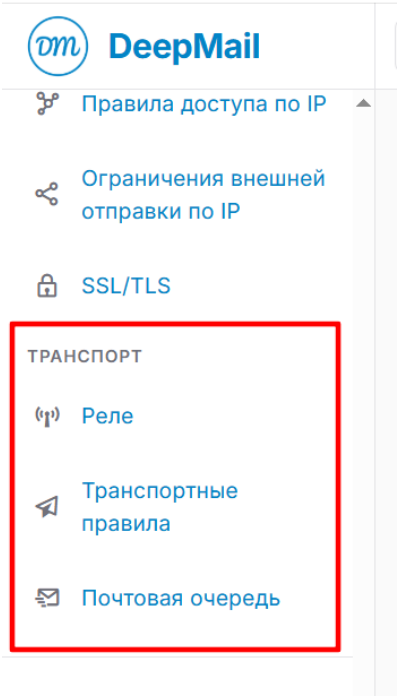


Рисунок 144 – Раздел «Транспорт»

3.6.1 Реле

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

Для настройки пересылки почты через сервер-посредник необходимо меню админ-панели выбрать пункт «Реле» (см. рисунок 144).

Откроется страница инструмента «Реле», которая содержит список настроенных релейных доменов (рисунок 145).

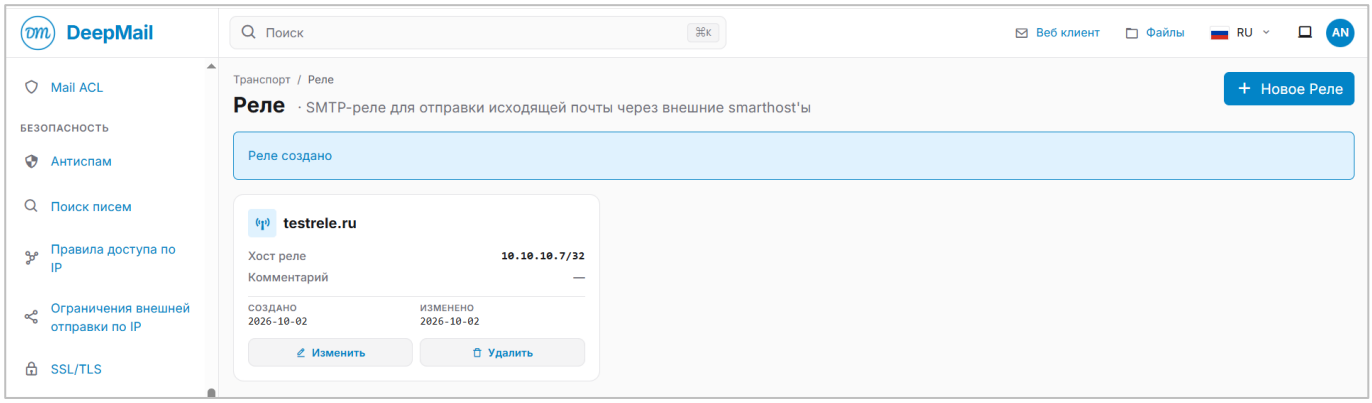


Рисунок 145 – Окно «Список релейных доменов»

3.6.1.1 Создание релейного домена

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

(см. рисунок 145).

В появившейся форме создания реле указать:

- «ИМЯ РЕЛЕ» – доменное имя исходного сервера, которое хотим использовать для релейного домена;
- «ХОСТ РЕЛЕ» – IP-адрес HAProxy удаленного хоста (реле) (рисунок 146).

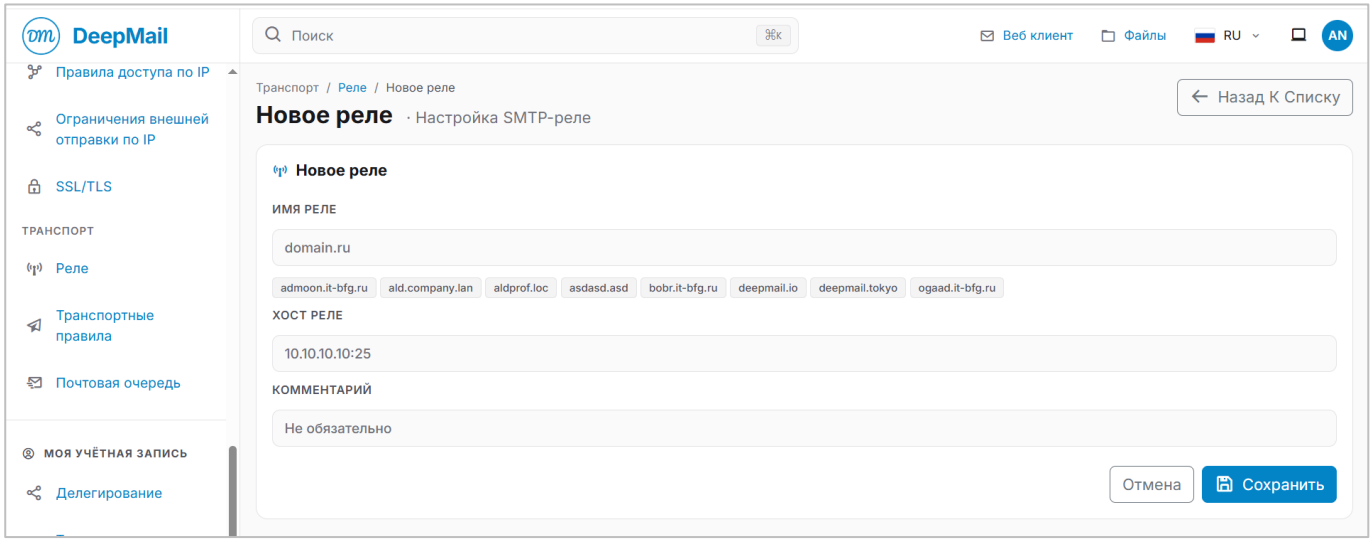


Рисунок 146 – Форма «Новый релейный домен»

Для завершения создания и сохранения параметров необходимо нажать кнопку 

(см. рисунок 146).

Для того чтобы почта пересылалась через созданное реле, необходимо внести настройки ретрансляции в профиле SMTP – см. 3.2.6.2.

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

3.6.1.2 Редактирование релейного домена

Для редактирования релейного домена необходимо в окне со списком релейных доменов нажать кнопку 

(см. рисунок 145). После этого откроется форма «Изменить реле» (рисунок 147).

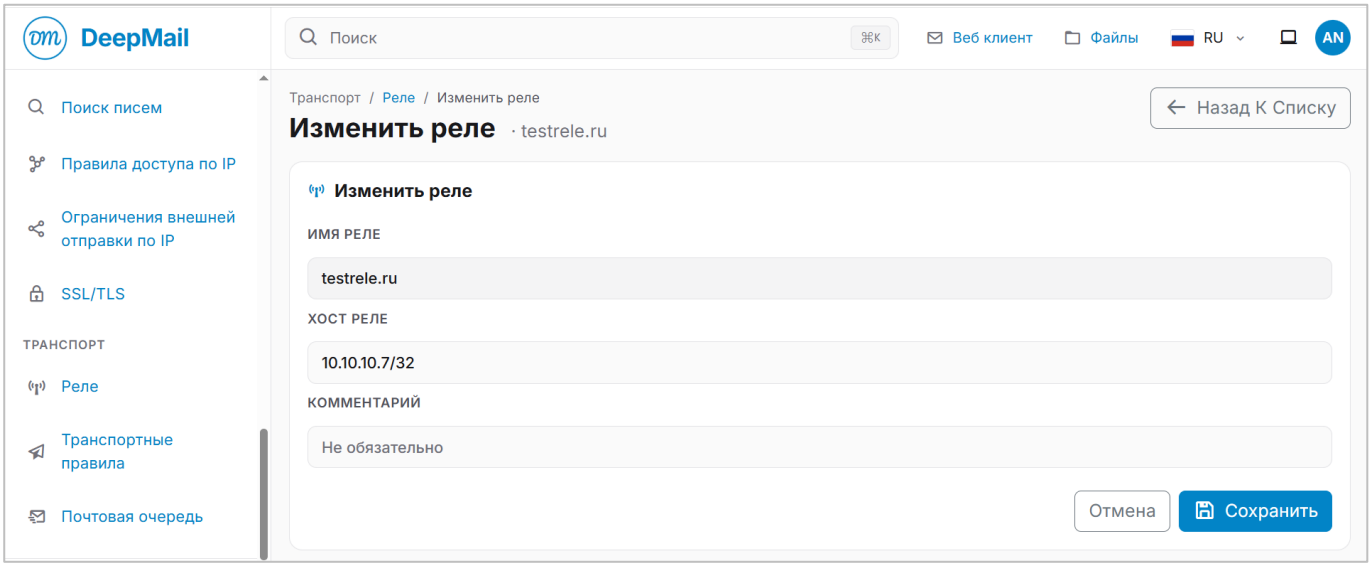
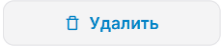


Рисунок 147 – Форма «Изменить реле»

Внесите изменения в поля появившейся формы, и нажмите кнопку 

(см. рисунок 147).

3.6.1.3 Удаление релейного домена

Для удаления релейного домена необходимо в окне со списком релейных доменов нажать кнопку 

(см. рисунок 145) и затем подтвердить удаление в открывшемся модальном окне.

3.6.2 «Транспортные правила»

Транспортные правила в DeepMail – это правила потока обработки почты. Не смотря на название «Транспортные» они не задают маршрутизацию писем по получателям, а только

устанавливают необходимость копирования либо блокировки при доставке и отправлении почтовых сообщений.

Инструмент «Транспортные правила» позволяет обрабатывать проходящие через организацию сообщения по заданным правилам. Эти правила действуют «поверх» обычного потока SMTP-доставки.

Чтобы настроить транспортные правила необходимо в меню админ-панели выбрать пункт «Транспортные правила» (см. рисунок 144).

Откроется страница «Транспортные правила», которое содержит список настроенных правил (рисунок 148).

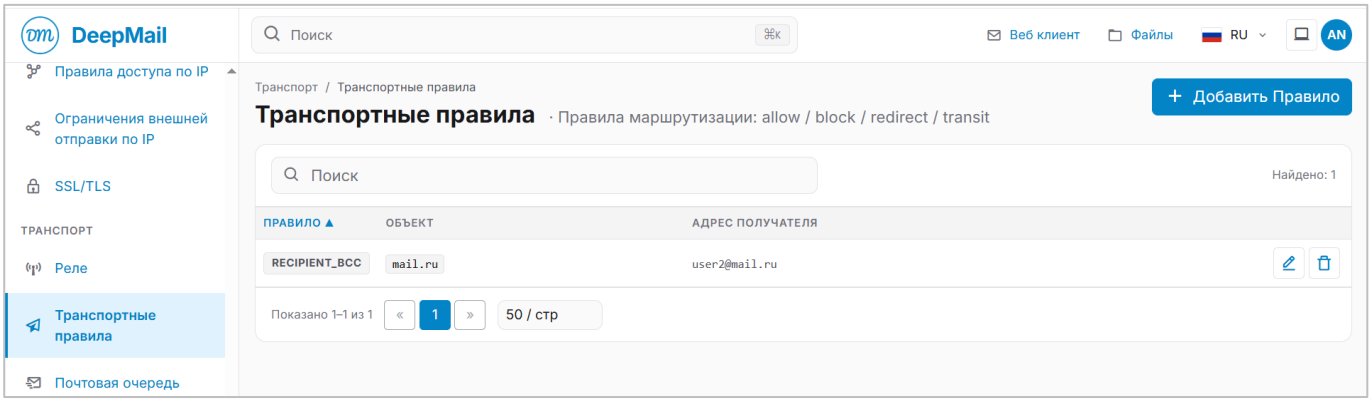


Рисунок 148 – Страница «Транспортные правила»

На странице отображен список уже созданных правил с элементами управления в строке каждого правила – кнопка  для редактирования и кнопка  для удаления.

BCC – слепые копии писем на дополнительные адреса (по отправителю, получателю или всем подряд).

Block – (блокировка отправителей) отказ принять или отправить почту от определенных адресов.

Чтобы создать новое правило нажмите кнопку 

. Откроется страница с формой «Добавить правило» (рисунок 149).

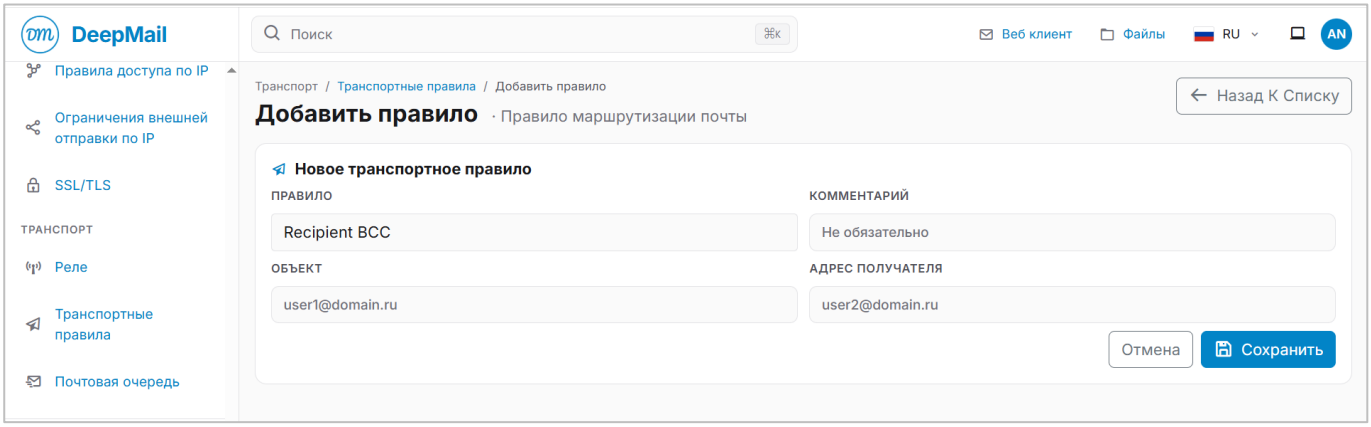


Рисунок 149 – Окно «Настройка транспортных правил»

В форме необходимо заполнить поля:

- ПРАВИЛО – выбрать из выпадающего списка название правила;
- КОММЕНТАРИЙ – пояснения, заметки (необязательно для заполнения);
- ОБЪЕКТ – на кого (на что) действует правило;
- АДРЕС ПОЛУЧАТЕЛЯ – адрес, куда отправляется копия.

В АРМ «DeepMail» реализованы следующие типы правил:

- «Recipient BCC» – письма, полученные на адрес, заданный в поле «ОБЪЕКТ», копируются на адрес, указанный в поле «АДРЕС ПОЛУЧАТЕЛЯ»;
- «Sender BCC» – письма, отправленные с адреса, заданного в поле «ОБЪЕКТ», копируются на адрес, указанный в поле «АДРЕС ПОЛУЧАТЕЛЯ»;
- «Always BCC» – письма, полученные или отправленные на адрес, заданный в поле «ОБЪЕКТ», копируются на адрес, указанный в поле «АДРЕС ПОЛУЧАТЕЛЯ»;
- «Sender Block» – письма, отправленные с адреса, заданного в поле «ОБЪЕКТ», будут отклоняться для отправки (блокироваться). Поле «АДРЕС ПОЛУЧАТЕЛЯ» при этом обязательно к заполнению, но значение его не важно (должно быть просто валидным), поэтому рекомендуется указывать служебный email.

Важно! Сообщения при выполнении правил BCC не пересылаются, а именно копируются в исходном состоянии.

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

Для завершения создания правила нажмите кнопку 

(см. рисунок 149).

3.6.3 Почтовая очередь

Интерфейс управления почтовой очередью (рисунок 150) представляет собой панель мониторинга и управления очередью исходящей почты на указанном SMTP-сервисе.

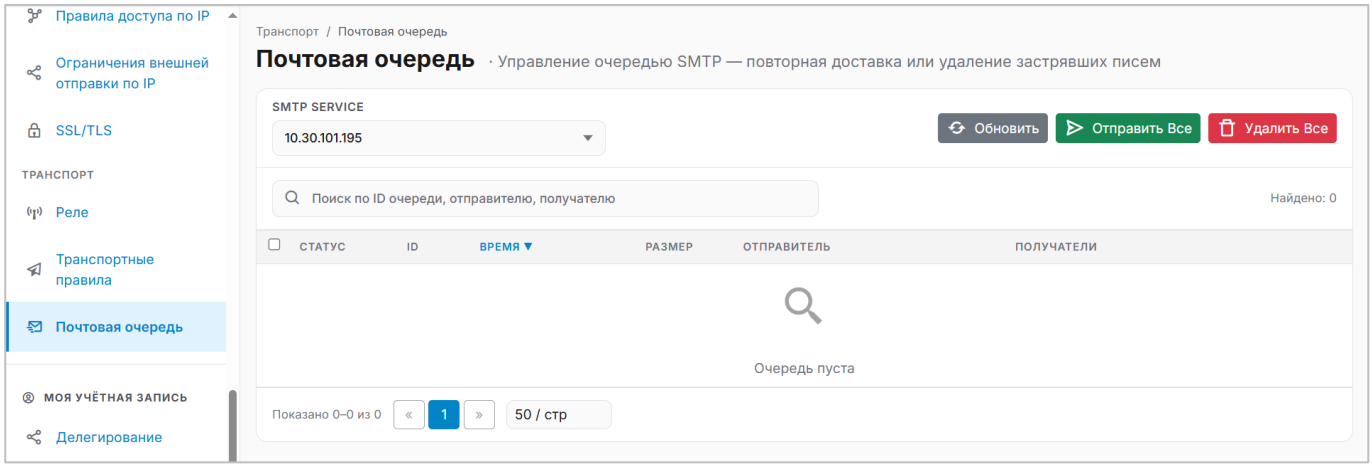


Рисунок 150 – Панель управления почтовой очередью

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. На рисунке показан момент, когда данные отсутствуют, что означает, что очередь пуста, о чем и свидетельствует информационная запись на экране.

Над таблицей расположены элементы управления для выбора IP-адреса SMTP-сервиса и кнопки для массовых операций:

- Обновить – обновление данных в таблице;
- Отправить Все – принудительная отправка всех писем в очереди;
- Удалить Все – 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.

3.7 Раздел «Моя учетная запись»

В данном разделе размещены пользовательские инструменты DeepMail, которые доступны администратору, для выполнения персональных настроек своего почтового аккаунта, а также при переходе из системных инструментов при выборе УЗ пользователей, администратор может выполнять настройки от лица выбранного пользователя. Например, из

инструмента «Пользователи» при редактировании УЗ можно настроить доступ к календарю для обычного пользователя системы – администратор войдет в раздел «Моя учетная запись» выбранного пользователя (см. 3.4.2.2).

На рисунке 151 представлен состав раздела «Моя учетная запись».

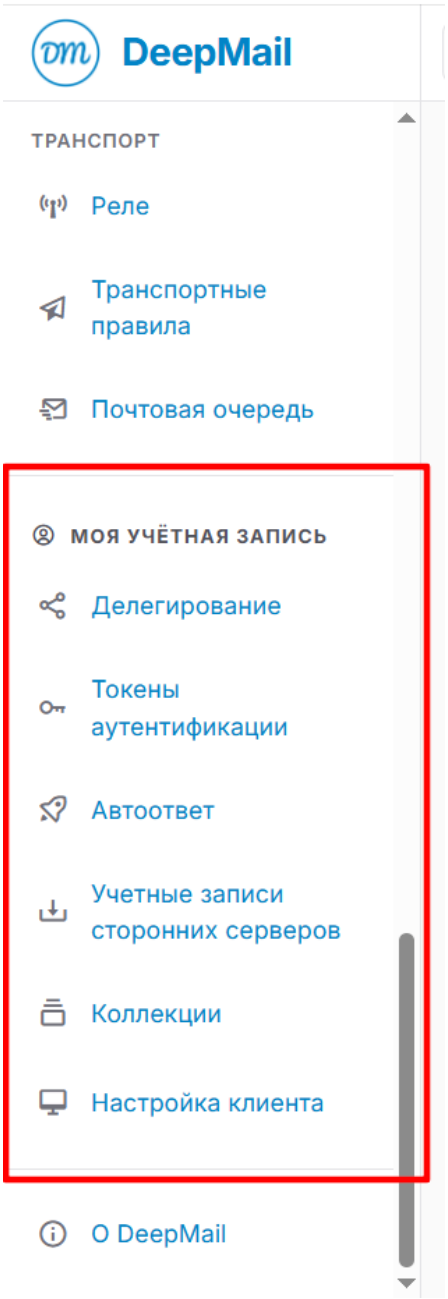


Рисунок 151 – Раздел «Моя учетная запись»

3.7.1 Инструмент «Делегирование»

Инструмент «Делегирование» содержит три подраздела настроек:

1) «WebDav ACL» – делегирование доступа к календарям, адресным книгам и спискам задач;

2) «Mail ACL» – предоставление доступа к конкретным почтовым папкам;

3) «Отправка почты» – предоставление прав отправки почты от своего имени (рисунок 152).

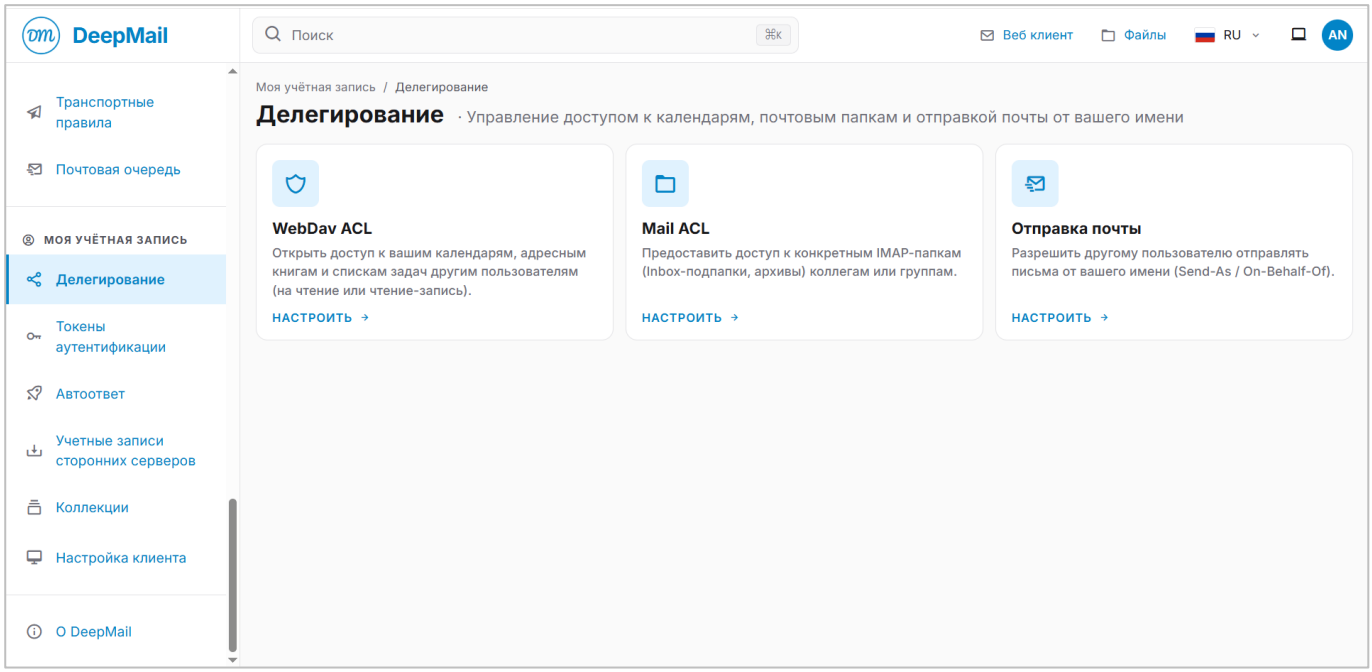


Рисунок 152 – Инструмент «Делегирование доступа»

3.7.1.1 WebDav ACL

Для перехода к настройке делегирования доступа к календарям, адресным книгам и папкам задач необходимо в разделе «Моя учетная запись» выбрать «Делегирование» и затем нажать «WebDav ACL» (см. рисунок 152).

На экране отобразится окно «WebDav ACL» со списком делегатов, если права уже назначались (рисунок 153).

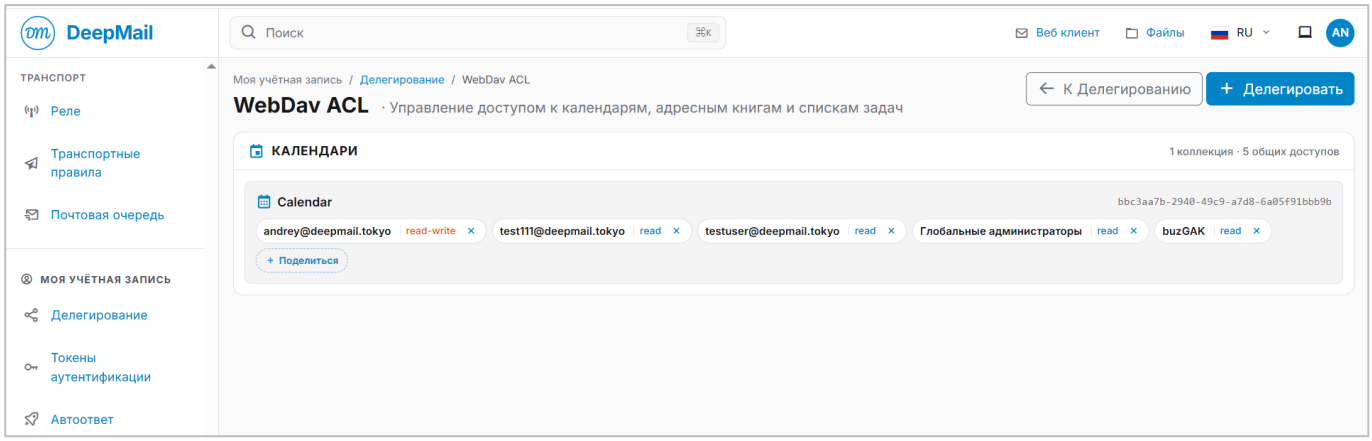
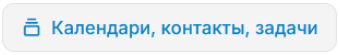
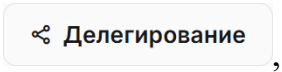


Рисунок 153 – Окно параметров «WebDav ACL»

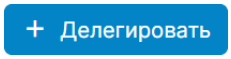
ACL (Access Control List) – механизм для гибкой маршрутизации трафика на основе условий. В контексте WebDav ACL определяет правила, по которым запросы с данными календарей, контактов и задач направляются к WebDAV-серверу

Администратор может управлять правами доступа на собственные календари, адресные книги и списки задач, так и управлять правами от имени обычного пользователя (см. 3.4.2.2). Для управления делегированием прав от имени пользователя необходимо в меню админ-панели выбрать инструмент «Пользователи», перейти к редактированию пользователя, нажав кнопку  (см. рисунок 66) и в окне редактирования в блоке «СОСТОЯНИЕ УЧЕТНОЙ ЗАПИСИ» нажать кнопку 

(см. рисунок 87). Будет выполнен переход в «Коллекции» пользователя (описание работы с инструментом «Коллекции» см. в 3.7.5), где, нажав кнопку 

, будет выполнен переход на страницу «WebDav ACL» выбранного пользователя. Дальнейшие действия идентичны работе с собственным «WebDav ACL».

Делегирование осуществляется в рамках одного домена.

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

(см. рисунок 153), после чего откроется страница предоставления прав «Делегировать коллекцию» (рисунок 154).

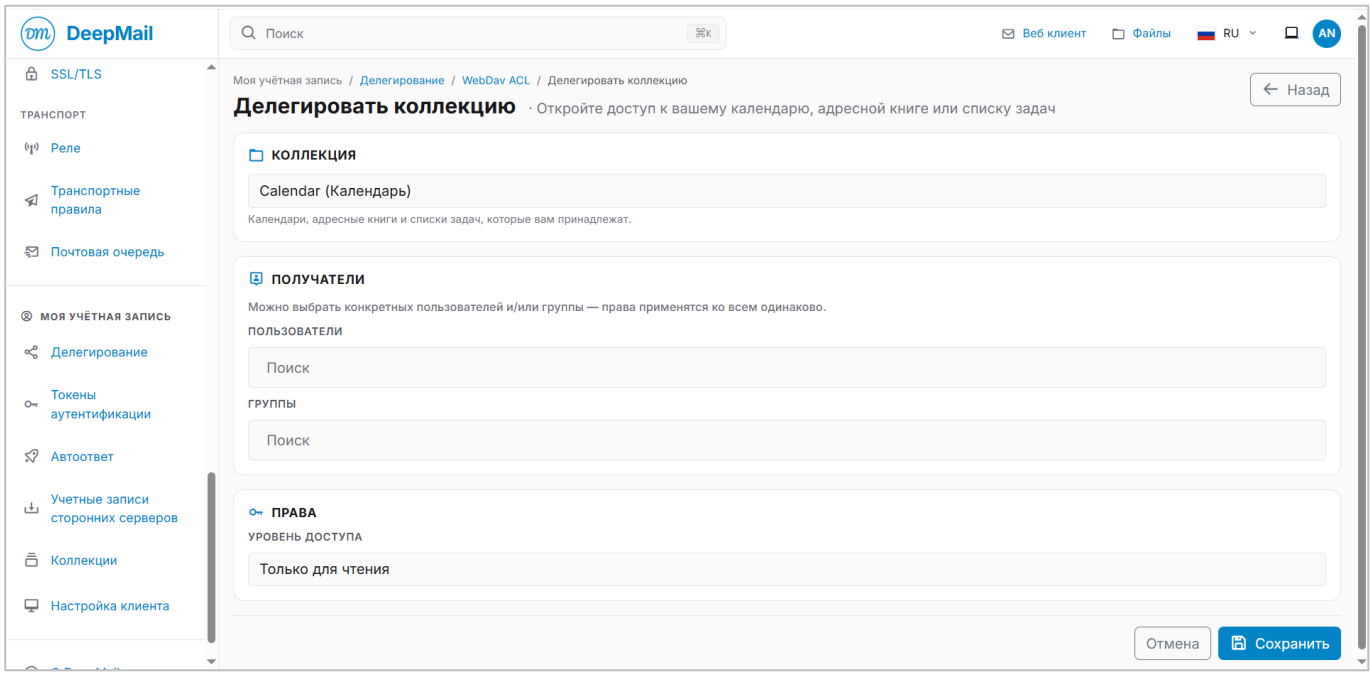


Рисунок 154 – Настройка делегирования

В открывшемся окне необходимо заполнить поля:

- КОЛЛЕКЦИЯ – выбрать из выпадающего списка доступные объекты (папки) для делегирования прав на них;

- ПОЛЬЗОВАТЕЛИ – пользователь (или несколько пользователей), которому будет предоставлен доступ к выбранной коллекции;

- ГРУППЫ – группа (или несколько групп) пользователей, которой 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 и веб-версию (описание действий приведено в соответствующих руководствах пользователя на клиентские приложения DeepMail).

Для сохранения внесенных изменений необходимо нажать кнопку Сохранить (см. рисунок 154).

3.7.1.2 Mail ACL

Mail ACL – это инструмент предоставления прав к почтовым папкам. Для перехода к нему необходимо в разделе «Моя учетная запись» выбрать инструмент «Делегирование» и затем нажать «Mail ACL» (см. рисунок 152).

Интерфейс «Mail ACL» предоставляет администратору инструменты для управления списками контроля доступа к почтовым папкам пользователя (рисунок 155).

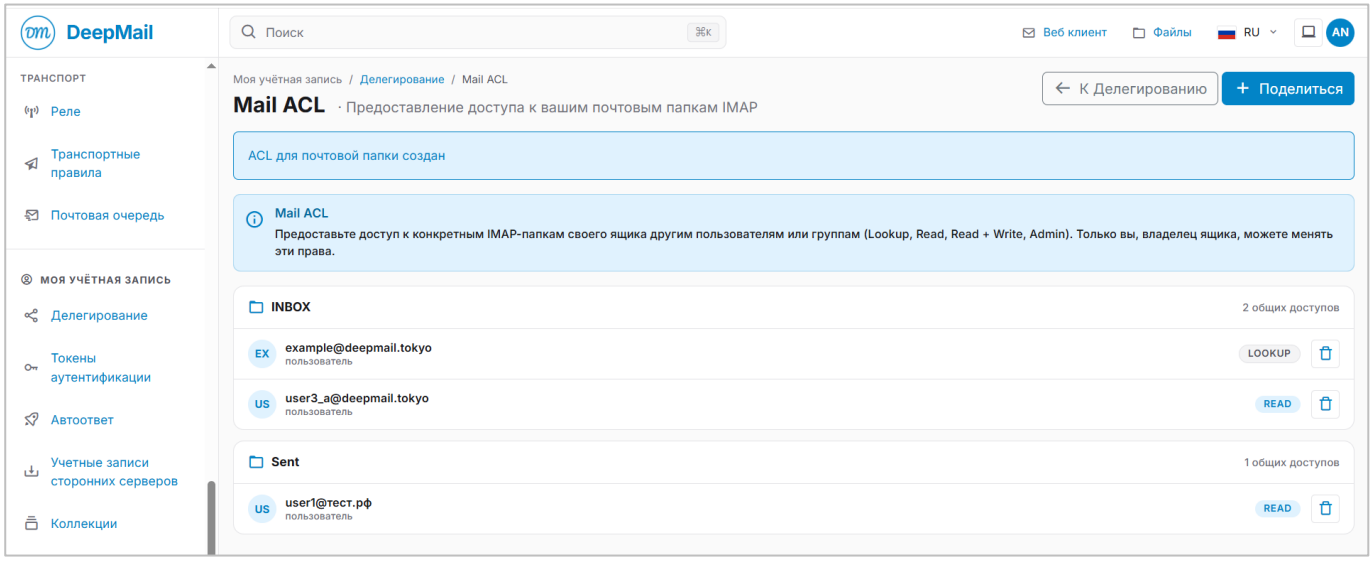


Рисунок 155 – Настройка делегирования Mail ACL

На странице отображаются данные предоставленных прав доступа, сгруппированные по почтовым папкам. В верхней части каждой группы (папки) отображается сводная статистика: количество общих доступов. В каждой строке указана УЗ пользователя или группа, которым предоставлены права, иконка типа прав, а также кнопка удаления делегации .

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

(см. рисунок 155), после чего откроется страница с формой делегирования почтовой папки (рисунок 156).

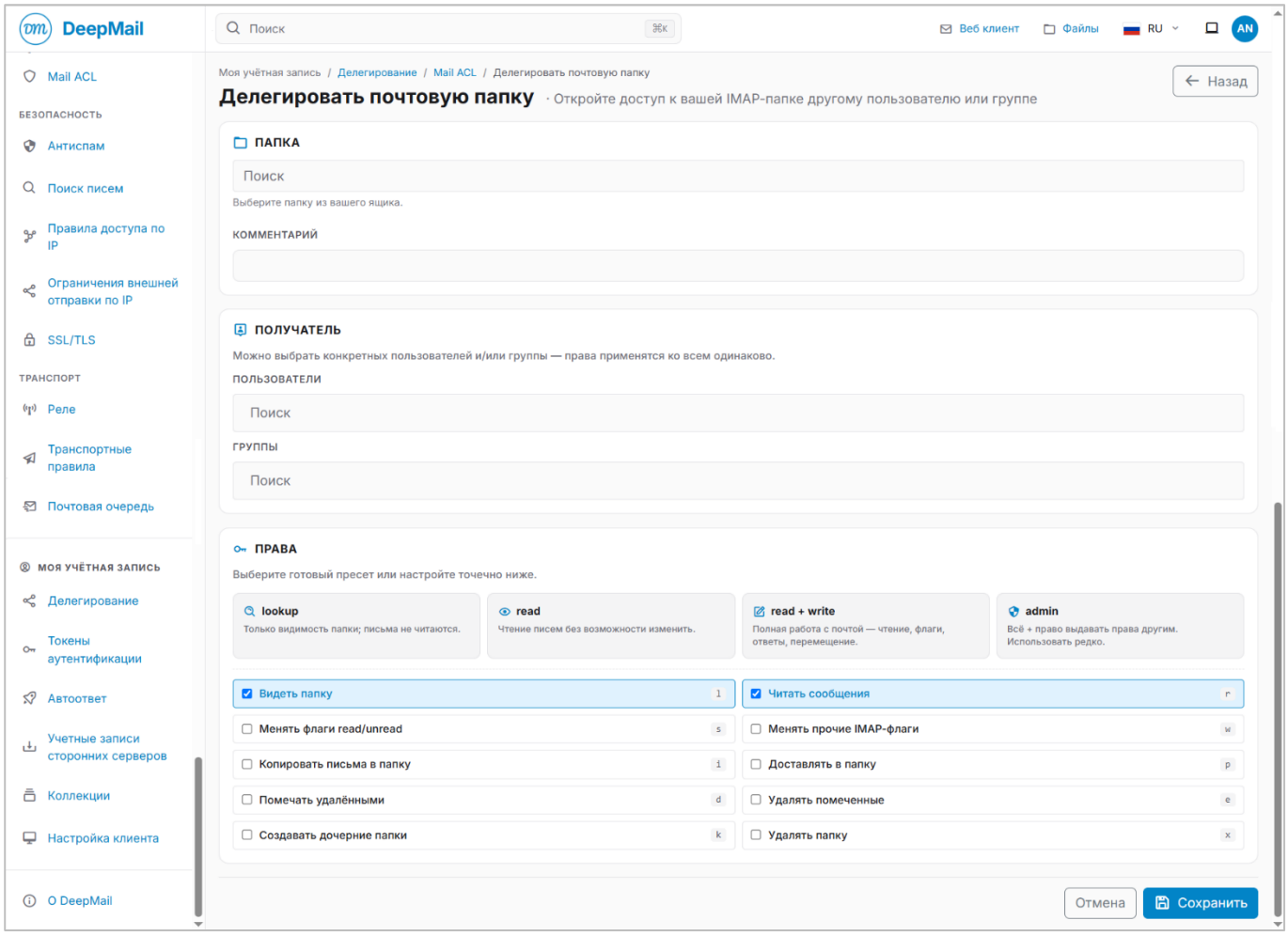


Рисунок 156 – Форма делегирования почтовой папки

В интерфейсе управления правами доступа к папкам «Mail ACL» администратор может гибко настраивать, кто и какие действия может выполнять с его собственными почтовыми папками, а также с почтовыми папками конкретного пользователя (переход в «Mail ACL» из инструмента «Пользователи» (см. 3.4.2.2)).

Форма настроек прав доступа к папкам содержит три основных блока:

1) ПАПКА – указывается название папки (например, INBOX или любая пользовательская папка) и комментарий (произвольное примечание);

2) ПОЛУЧАТЕЛЬ – в поле «ПОЛЬЗОВАТЕЛИ» указывается один или несколько пользователей, которым будет предоставлен доступ к выбранной папке; в поле «ГРУППЫ» указывается одна или несколько групп, которым будет предоставлен доступ к выбранной папке. Это может быть, например, секретарь, которому требуется доступ к папкам руководителя, или группа сотрудников, отвечающих за определенный проект;

3) ПРАВА – можно выбрать готовый пресет (набор прав – lookup, read, read+write, admin) или выбрать права по желанию отметив соответствующие чекбоксы (см. рисунок 156). Сами права представляют собой набор десяти дискретных разрешений, каждое из которых кодируется одной буквой в стандартной строке ACL.

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 папок в почтовом ящике получателя прав и открываться по имени;
- Менять флаги read/unread (s) – дает возможность отмечать сообщения как прочитанные и непрочитанные (изменять статус прочтения);
- Копировать письма в папку (i) – разрешает вставку в папку новых сообщений;
- Помечать удаленными (d) – позволяет ставить флаг удаления;
- Создавать дочерние папки (k) – позволяет создавать подпапки внутри данной;
- Читать сообщения (r) – дает возможность читать письма и просматривать содержимое папки;
- Менять прочие IMAP-флаги (w) – позволяет устанавливать прочие флаги (кроме Seen и Deleted);
- Доставлять в папку (p) – дает возможность доставлять почту напрямую (полезно для общих входящих папок);
- Удалять помеченные (e) – разрешает окончательную чистку удаленных писем;
- Удалять папку (x) – дает право удалить саму папку.

Такой подход позволяет точно контролировать доступ к почтовым папкам, обеспечивая безопасность и удобство совместной работы.

Для сохранения внесенных изменений необходимо нажать кнопку Сохранить (см. рисунок 156).

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 (можно дать секретарю право читать и изменять флаги, но запретить удаление папок), или для централизованного управления правами через группы администраторов (например, предоставить технической группе полный доступ для администрирования на папки определенного пользователя).

3.7.1.3 Отправка почты

Инструмент «Отправка почты» предназначен для делегирования прав на отправку почтовых сообщений пользователя в режиме SEND-AS (с полной подменой отправителя – получатель увидит письмо так, будто отправили его вы) и/ или ON-BEHALF-OF (от вашего имени – получатель увидит в письме имя (адрес) реального отправителя с пометкой «направлено от имени <ваше имя>». Для перехода к нему необходимо в разделе «Моя учетная запись» выбрать инструмент «Делегирование» и затем нажать «Отправка почты» (см. рисунок 152).

В появившемся окне «Отправка почты» в соответствующем поле (или в обоих полях) укажите адрес электронной почты пользователя, которому делегируются права, и нажмите кнопку Сохранить (рисунок 157).

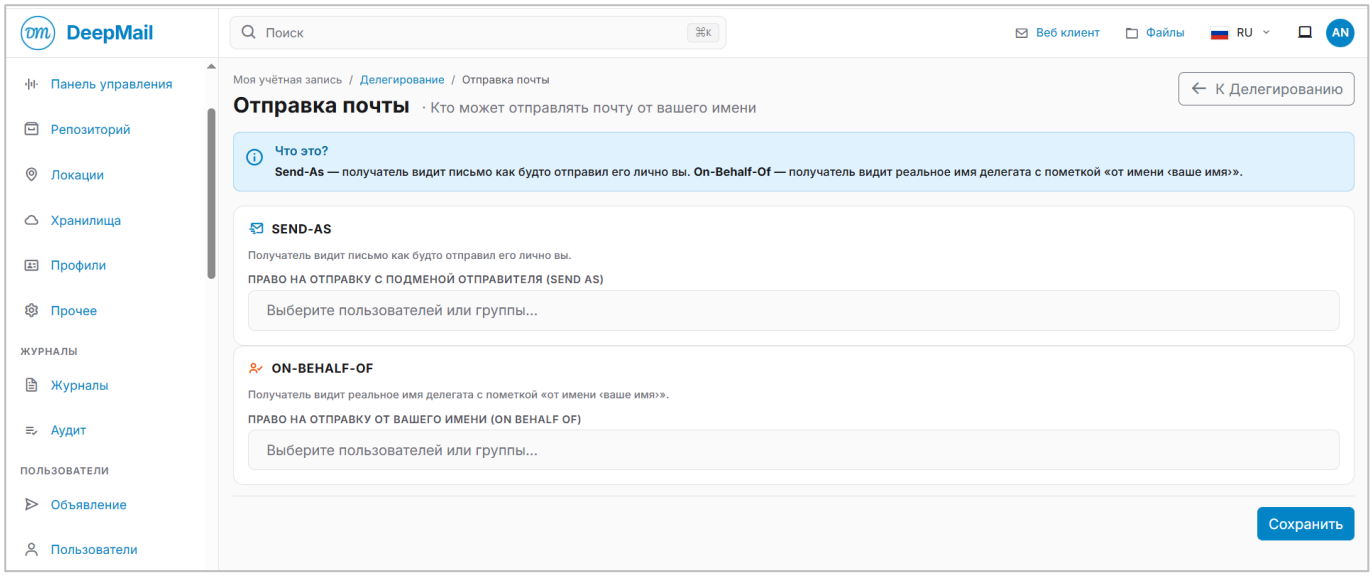


Рисунок 157 – Окно «Отправка почты»

3.7.2 Инструмент «Токены аутентификации»

Инструмент «Токены аутентификации» позволяет завести отдельные «пароли» для конкретных Клиентов и скриптов. Каждый токен – это уникальный «секрет», которым можно пользоваться вместо основного пароля для входа в IMAP, SMTP, WebDAV и подключения к API. Также при помощи токенов можно, например, предоставлять временный доступ к своему почтовому ящику для других пользователей – созданный токен передается пользователю, который авторизуясь в Клиент или веб-клиент с данным токеном в качестве пароля и адресом электронной почты пользователя-владельца токена, получает полный доступ к почтовым данным этой УЗ, при удалении токена доступ к почте УЗ блокируется.

Зачем это нужно:

- Безопасность – если Клиент будет скомпрометирован, достаточно отозвать один токен, основной пароль остается валидным, а остальные Клиенты продолжают работать;
- Изоляция – каждой интеграции – свой токен (видно, кто чем пользуется);
- Привязка к IP – токен можно ограничить адресом, с которого им можно пользоваться (например, IP домашнего сервера);
- Доступ из CI/скриптов – для скрипта удобнее использовать long-lived токен, чем интерактивно вводимый пароль.

Для создания такого ключа необходимо в разделе «Моя учетная запись» выбрать инструмент «Делегирование» и затем нажать «Токены аутентификации» (см. рисунок 152).

На экране отобразится страница инструмента «Токены аутентификации» с карточками предоставленных ключей, если они уже назначались (рисунок 158).

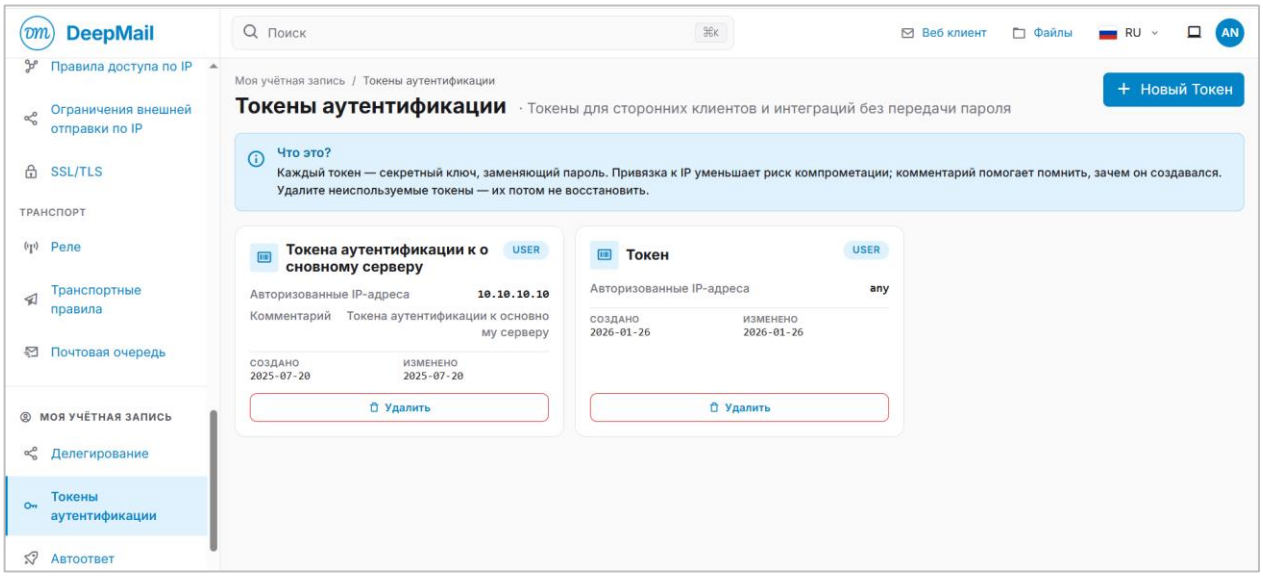


Рисунок 158 – Страница инструмента «Токены аутентификации»

Чтобы создать новый токен необходимо нажать кнопу + Новый Токен, расположенную в правом верхнем углу страницы «Токены аутентификации» (см. рисунок 158).

Откроется страница с формой создания нового токена (рисунок 159).

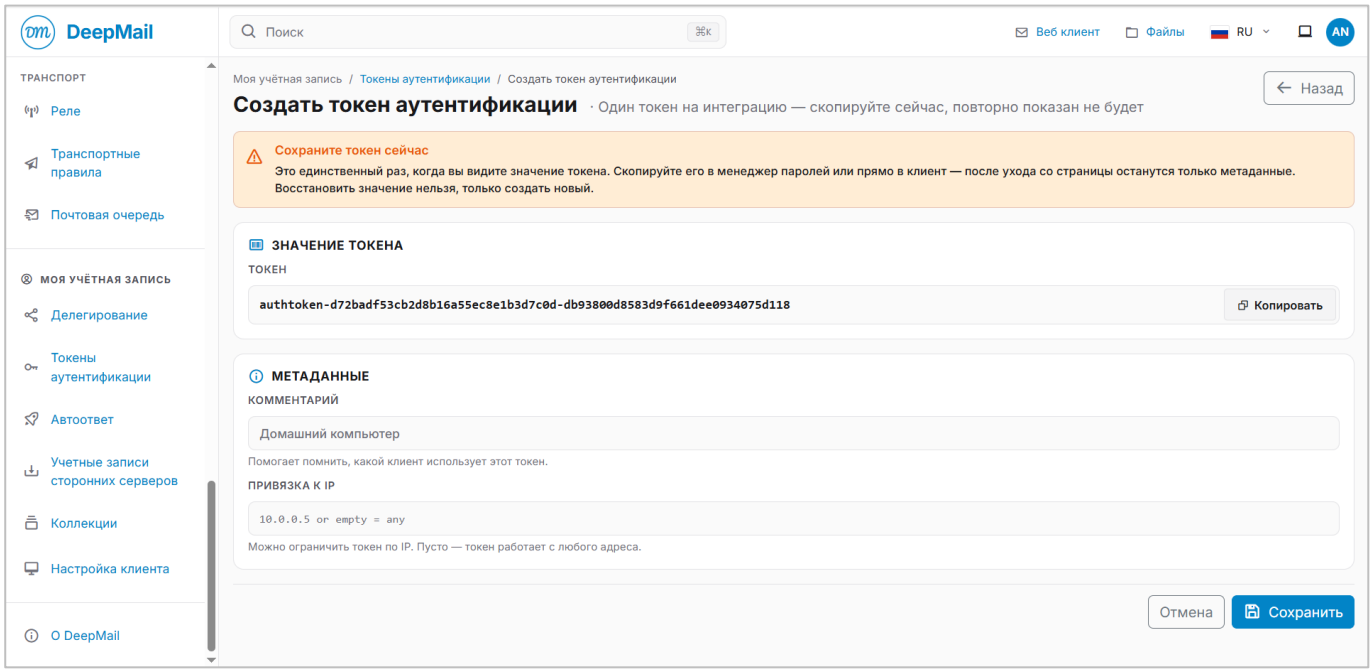


Рисунок 159 – Страница «Создать токен аутентификации»

В данной форме будет отображено автоматически сформированное значение токена.

Важно! Значение токена необходимо скопировать и сохранить, так как это единственный раз, когда оно будет отображено, после сохранения для просмотра будут доступны только метаданные.

В блоке «Метаданные» можно указать комментарий – пояснение к создаваемому токену (например «Почта на работе», «Скрипт rsync»), а также в поле «ПРИВЯЗКА К IP» указываются ограничения по IP для работы токена (если поле не заполнено, то токен будет работать с любого адреса).

Для завершения создания токена необходимо нажать кнопку Сохранить (см. рисунок 159).

Так создается USER-токен администратора, в карточке токена будет иконка USER (см. рисунок 158).

Администратор может создавать токены от лица обычных пользователей системы – ADMIN-токен. Создание таких токенов выполняется в системном инструменте «Токены аутентификации» (см. 3.4.4). В карточке токена будет иконка ADMIN.

Для удаления токена необходимо в его карточке нажать кнопку 

(рисунок 158). После удаления восстановить токен аутентификации нельзя.

3.7.3 Инструмент «Автоответ»

Инструмент «Автоответ» позволяет создавать, включать и выключать автоответчик на время отпуска, командировки, болезни, временного отсутствия и т.п. При поступлении входящего сообщения письмо-ответ уходит автоматически, входящее сообщение при этом попадает в почтовый ящик как обычно.

Для создания автоответчика необходимо в разделе «Моя учетная запись» выбрать инструмент «Автоответ» (см. рисунок 152).

В появившемся окне «Автоматический ответ» необходимо активировать чекбокс «Автоответчик включен» и заполнить следующие поля:

- ТЕМА – тема письма-автоответа;
- СООБЩЕНИЕ АВТООТВЕТА – текст письма;
- НАЧАЛО ОТПУСКА – дата начала работы автоответчика (с которой начнет отправляться автоответ на входящие письма);
- КОНЕЦ ОТПУСКА – дата окончания работы автоответчика (рисунок 160).

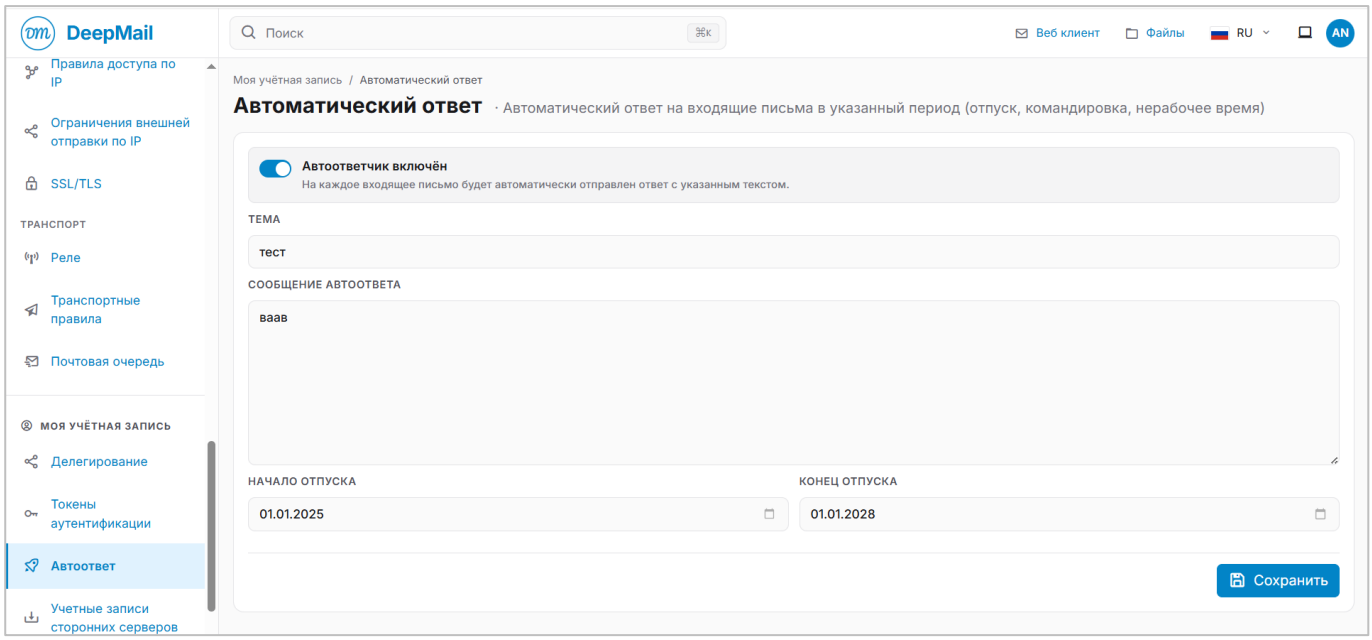


Рисунок 160 – Окно инструмента «Автоматический ответ»

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

Для отключения автоответчика вручную (до окончания срока его действия) необходимо выключить чекбокс «Автоответчик включен» (см. рисунок 160).

3.7.4 Инструмент «Учетные записи сторонних серверов»

Учетная запись стороннего сервера – это УЗ, принадлежащая внешнему серверу (например Yandex, Gmail и т.п.)

Для управления учетными записями сторонних серверов необходимо перейти к инструменту «Учетные записи сторонних серверов», выбрав его в разделе «Моя учетная запись» (см. рисунок 151).

Страница инструмента «Учетные записи сторонних серверов» предоставляет администратору возможность обзора уже добавленных внешних учетных записей (при наличии) и добавления новых (рисунок 161).

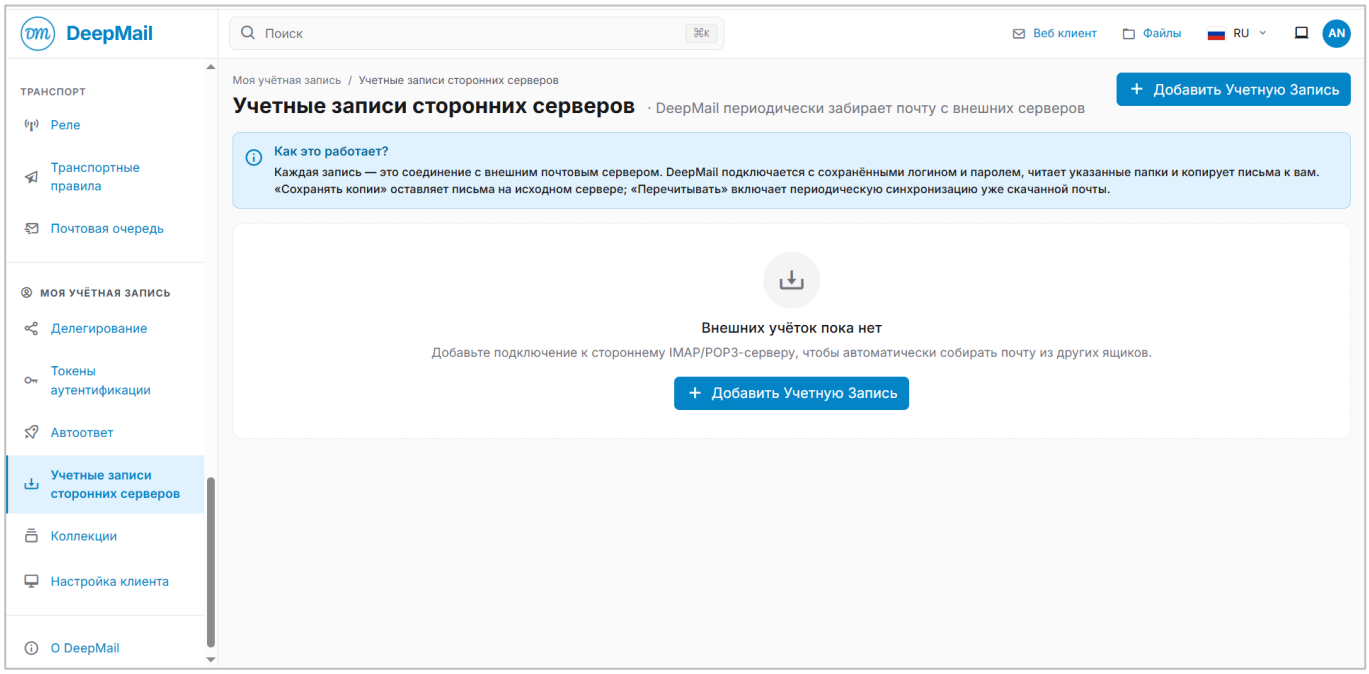


Рисунок 161 – Страница инструмента «Учетные записи сторонних серверов»

Каждая запись на данной странице – это соединение с внешним почтовым сервером. Система DeepMail подключается к стороннему серверу с сохраненным в настройках логином и паролем, считывает информацию во внешнем почтовом ящике и копирует письма в почтовый ящик пользователя DeepMail. Пользователь видит сторонние данные как отдельную УЗ с собственной структурой почтовых папок.

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

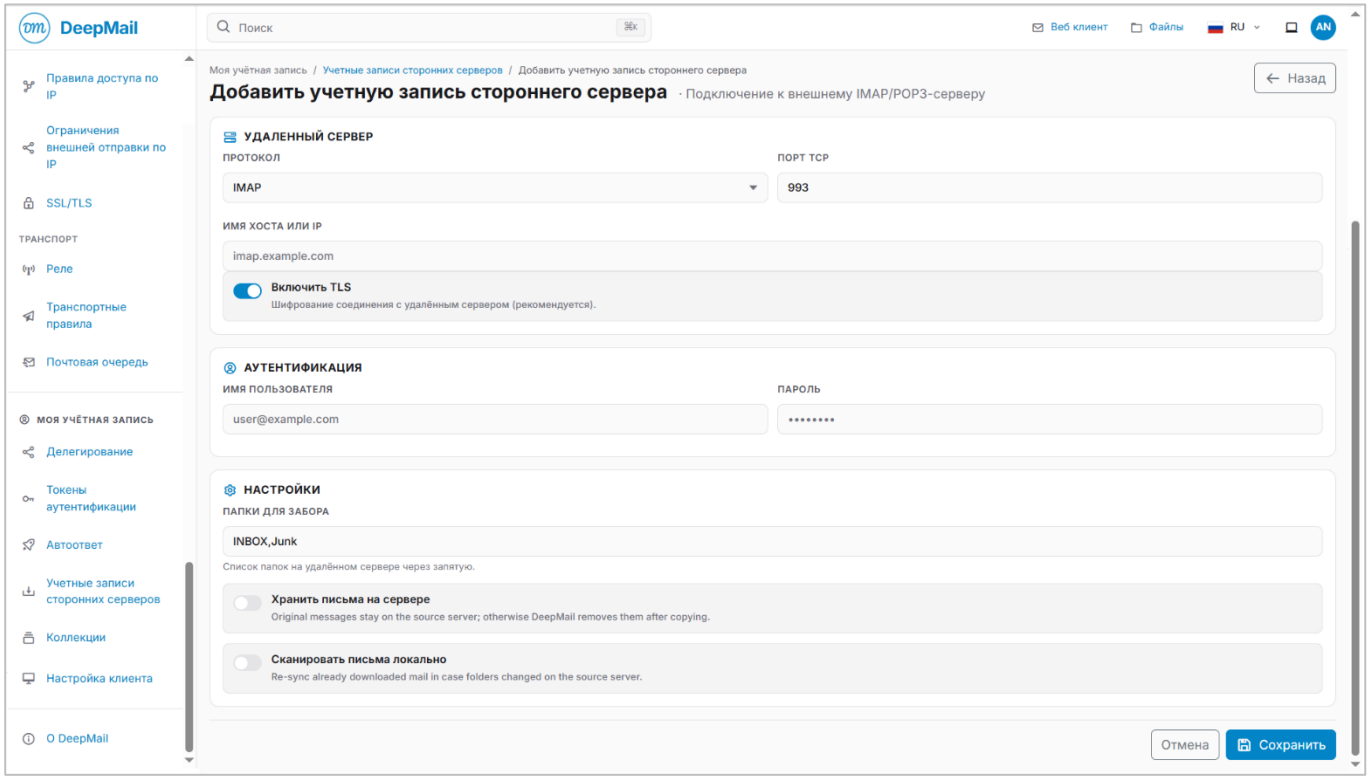


Рисунок 162 – Окно добавления параметров стороннего сервера

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;
- «Включить TLS» – протокол, обеспечивающий безопасную передачу данных;
- «Имя пользователя» – электронный адрес, зарегистрированный на внешнем сервере;
- «Пароль» – пароль, установленный для УЗ стороннего сервера. Для некоторых серверов применяется специальный зашифрованный пароль, для его получения необходимо выполнить определенные настройки в личном кабинете внешней УЗ;
- папки для получения на сервер DeepMail (по умолчанию «Входящие» и «Спам»);
- при необходимости включите чекбокс «Хранить письма на сервере» (если включено. То оригинал письма остается на сервере, если выключено, то оригинал удаляется с исходного сервера после сохранения на сервере DeepMail);
- при необходимости включите чекбокс «Сканировать письма локально» для выполнения периодической синхронизации уже скачанной почты.

Для завершения нажмите кнопку Сохранить. Для отмены нажмите кнопку Отмена (см. рисунок 162).

3.7.5 Инструмент «Коллекции»

Для управления параметрами календарей, адресных книг и списков задач пользователя необходимо перейти к инструменту «Коллекции», выбрав его в разделе «Моя учетная запись» (см. рисунок 151).

На странице инструмента «Коллекции» отображаются все имеющиеся у пользователя календари, адресные книги и списки задач, группированные по соответствующим блокам (рисунок 163).

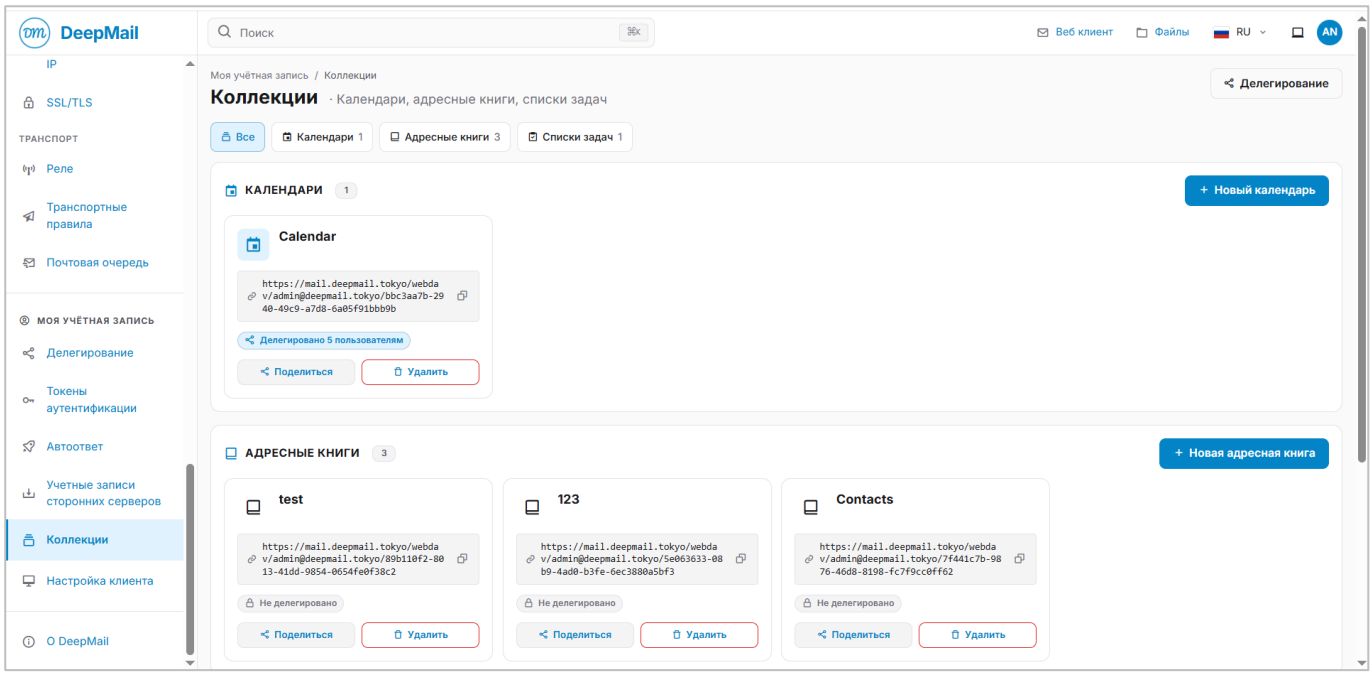


Рисунок 163 – Окно инструмента «Календари»

В блоке «Календари» отображены карточки всех календарей учетной записи, а также карточки календарей, делегированных этой УЗ, в том числе и календарь ресурса, если пользователь является его менеджером (см. 3.4.6).

В блоке «Адресные книги» отображены карточки всех папок контактов учетной записи, а также папок контактов, делегированных этой УЗ.

В блоке «Списки задач» отображены карточки всех папок задач учетной записи, а также папок задач, делегированных этой УЗ.

Инструмент позволяет создавать и удалять существующие папки календарей, контактов и задач пользователя, а также предоставлять к ним доступ.

Для создания календаря необходимо на странице инструмента «Коллекции» в блоке «КАЛЕНДАРИ» нажать кнопку 

(см. рисунок 163).

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

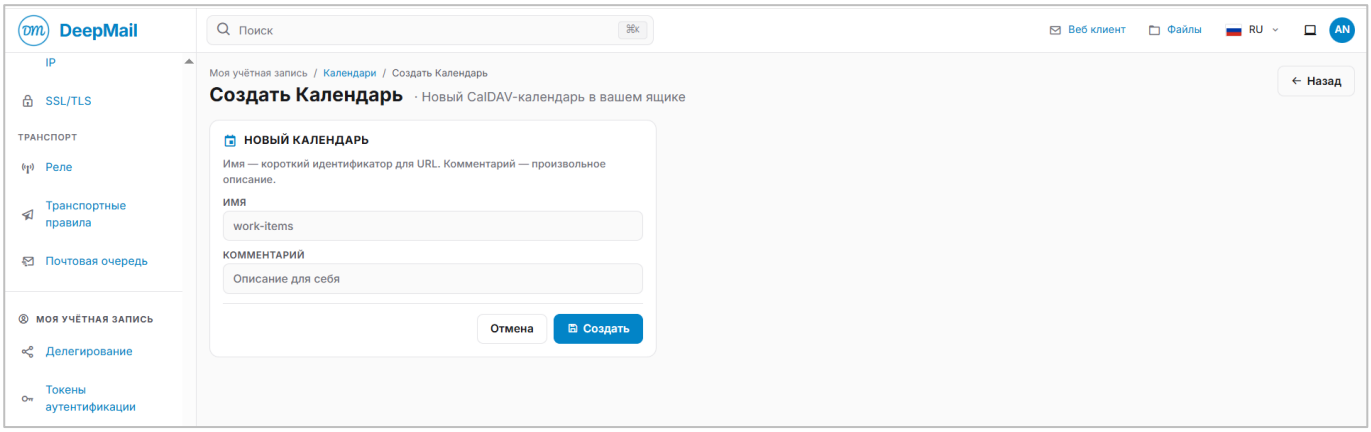


Рисунок 164 – Окно «Создать календарь»

Для завершения создания календаря нажмите кнопку Создать.

Для создания адресной книги необходимо на странице инструмента «Коллекции» в блоке «АДРЕСНЫЕ КНИГИ» нажать кнопку + Новая адресная книга (см. рисунок 163).

Откроется форма «Создать адресную книгу», в которой необходимо ввести имя адресной книги и, если нужно, добавить комментарий (рисунок 165).

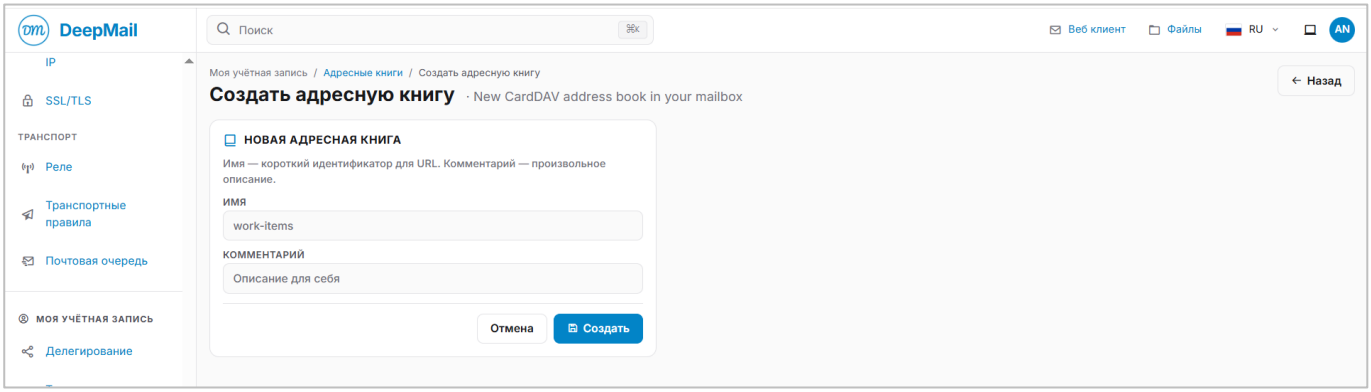


Рисунок 165 – Окно «Создать адресную книгу»

Для завершения создания адресной книги нажмите на кнопку Создать.

Чтобы создать папку задач необходимо на странице инструмента «Коллекции» в блоке «СПИСКИ ЗАДАЧ» нажать кнопку + Новый список задач (см. рисунок 163).

Откроется страница с формой создания нового списка задач, в которой необходимо ввести имя папки задач и, при необходимости, оставить комментарий (рисунок 166).

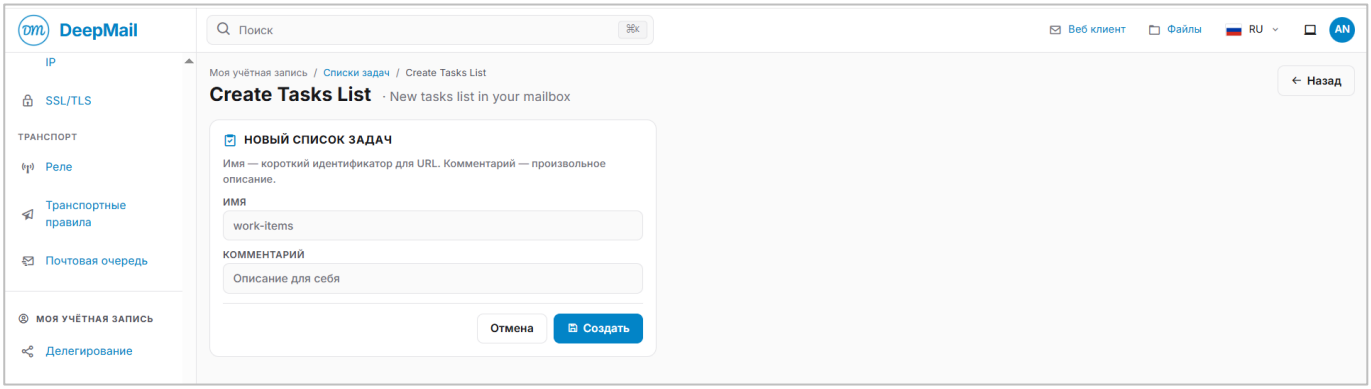


Рисунок 166 – Форма «Создать список задач»

Для завершения создания папки задач нажмите на кнопку Создать.

При нажатии в карточке календаря, адресной книги или списак задач на кнопку Поделиться (см. рисунок 163) будет выполнен переход на страницу «WebDav ACL» для делегирования прав доступа к выбранной папке (см. 3.7.1.1). В карточке отображается количество делегаций (например Делегировано 5 пользователям).

Чтобы удалить календарь, адресную книгу или список задач необходимо нажать кнопку Удалить, размещенную в карточке выбранной папки (см. рисунок 163).

3.7.6 Инструмент «Настройка клиента»

Инструмент «Настройка клиента» – это «справка» с параметрами подключения для внешних почтовых и календарных приложений (например, Outlook, Thunderbird, мобильные клиенты, веб-почта сторонних провайдеров и т.д.). Тут представлены все нужные адреса, порты и протоколы – копируйте и вставляйте в Клиент.

Чтобы перейти в инструмент «Настройка клиента», выберете его в разделе «Моя учетная запись» (см. рисунок 151). После этого на экране отобразится страница «Настройка клиента» (рисунок 167).

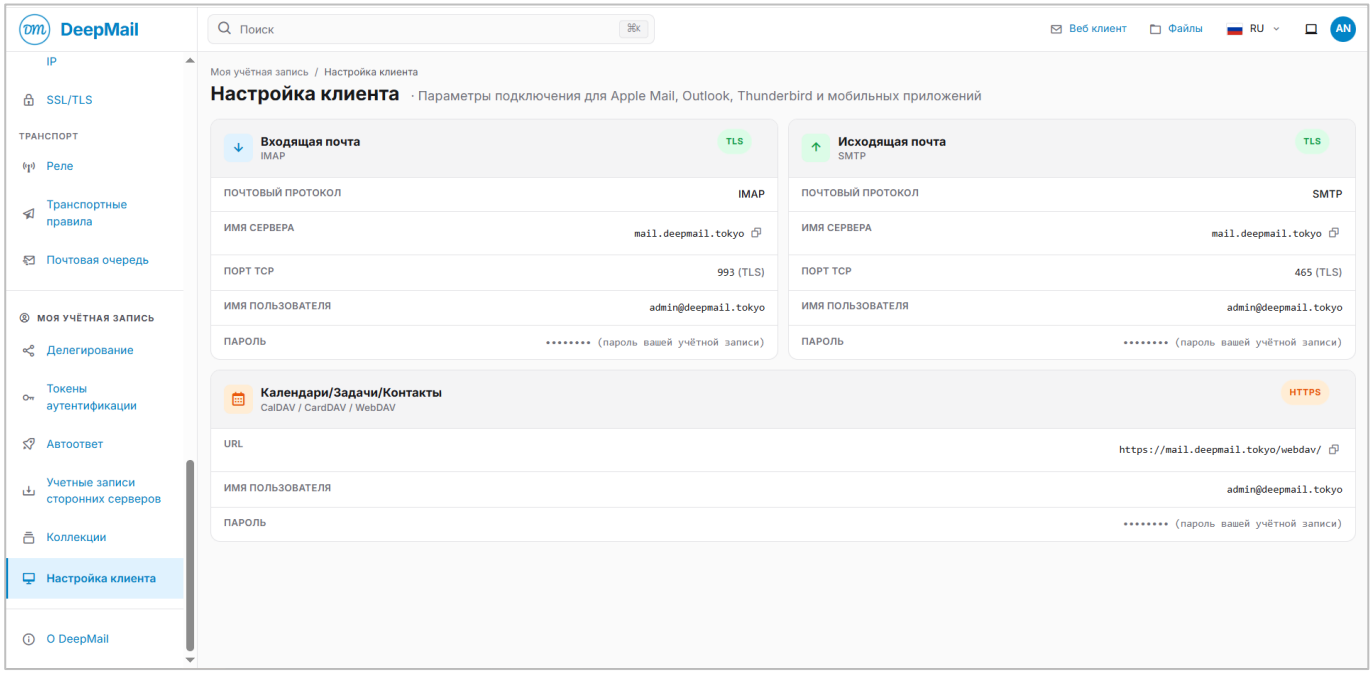


Рисунок 167 – Инструмент «Настройка клиента»

Для удобства копирования ключевых параметров в карточках есть кнопка .

3.8 Раздел «О DeepMail»

В разделе «О DeepMail» представлена информация о продукте (Серверная часть «DEEPMAIL модуль взаимодействия»), о версии ПО и о его разработчике (включая контактную информацию) (рисунок 168).

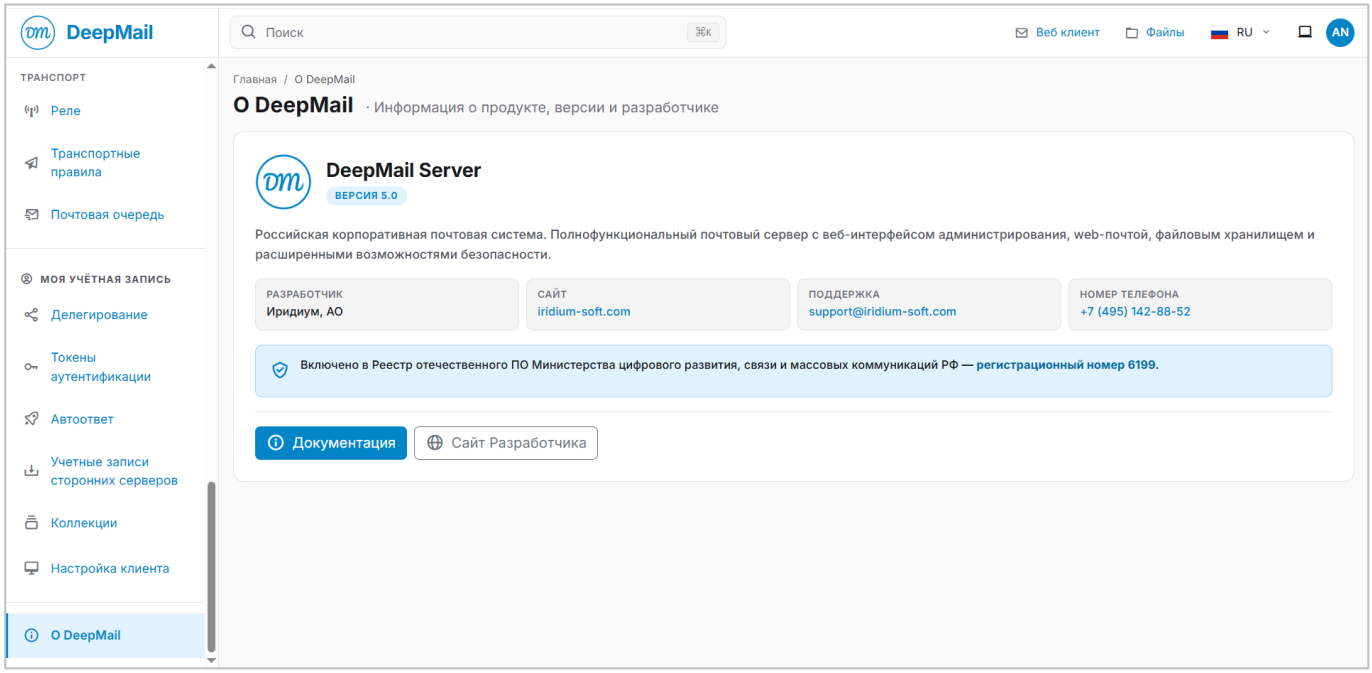


Рисунок 168 – Раздел «О DeepMail»

Также на странице есть функциональные элементы:

- 

– кнопка доступа к документации на АРМ «DeepMail» (руководство администратора, руководства пользователей, функциональные характеристики);

- 

– кнопка перехода на сайт разработчика.

3.9 Телефония

В АРМ «DeepMail» реализована возможность применения функционала SIP-телефонии в рамках корпоративной PBX. Панель администратора содержит инструменты для включения, ротации и выключения SIP-телефонии пользователям системы, а также набор инструментов для настройки диапазонов подключаемых доменов, служебных номеров и маршрутизации вызовов, управления внешними номерами и просмотра истории звонков.

Для перехода к настройкам телефонии необходимо на главной панели управления выбрать раздел «Телефония» (рисунок 169).

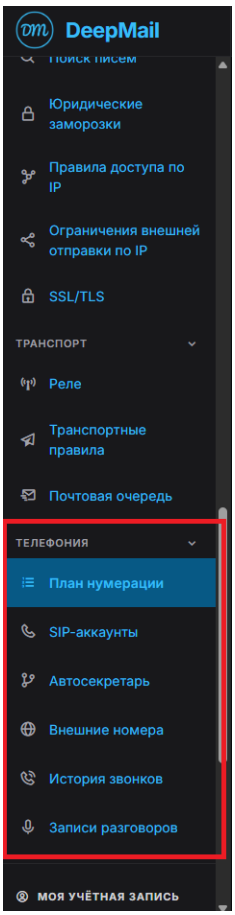


Рисунок 169 – Раздел «Телефония»

Затем выбрать необходимый подраздел настроек. На рисунке 170 представлена панель администратора для управления SIP-аккаунтами.

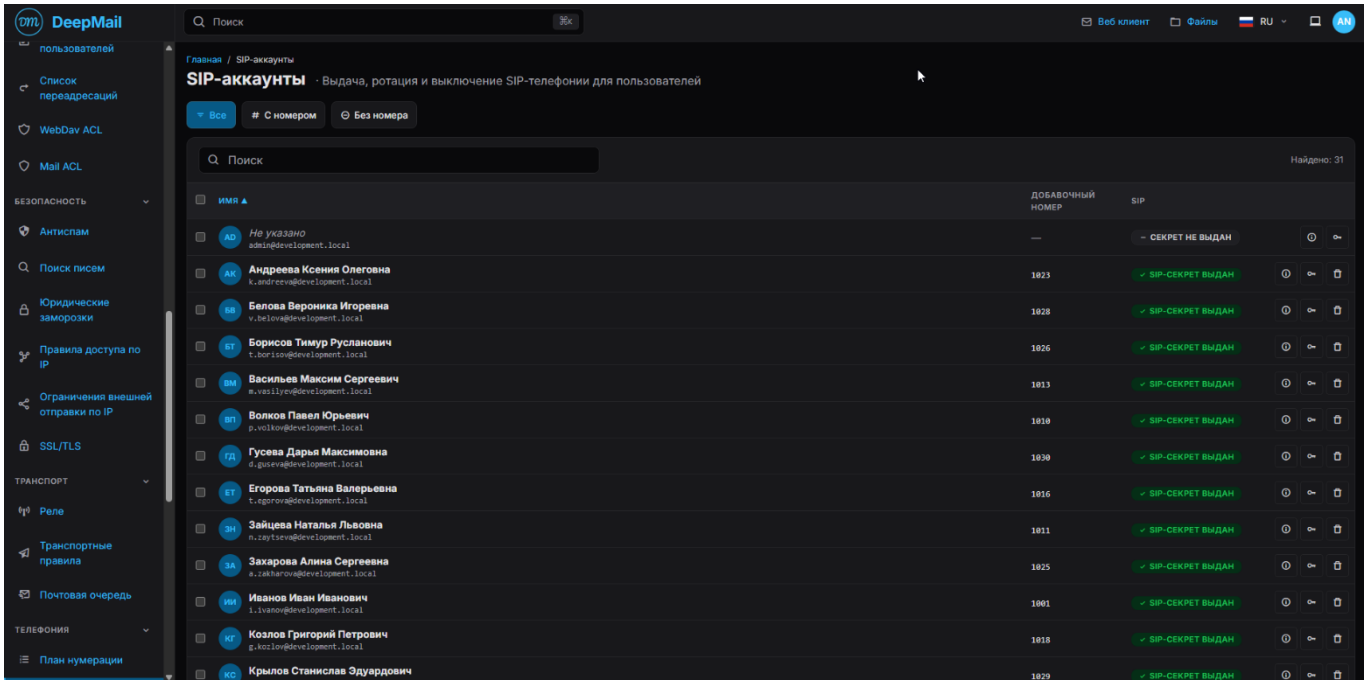


Рисунок 170 – Панель администратора для управления SIP-аккаунтами

3.10 RADIUS-серверы

В АРМ «DeepMail» реализована возможность применения специализированного сервера аутентификации RADIUS для проверки паролей. Для перехода к управлению RADIUS необходимо на главной панели администрирования выбрать раздел «RADIUS-серверы» (рисунок 171).

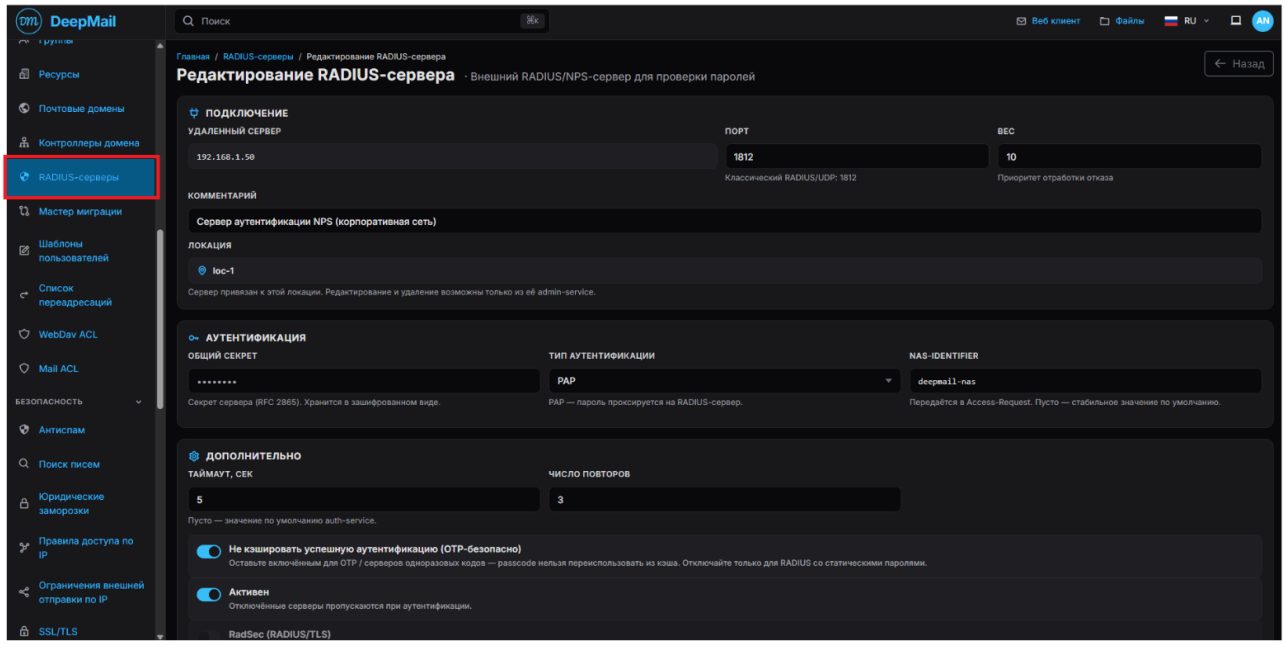


Рисунок 171 – Раздел «RADIUS-серверы»

Администратору доступны функции подключения RADIUS-сервера, настройка аутентификации и другие дополнительные настройки.

3.11 Интерфейс командной строки (CLI)

Для просмотра счетчиков статистики на уровне сервера, домена и пользователя применяется интерфейс командной строки – CLI (рисунок 172).

```
root@ub20:~# deepmail metrics current
=== Host usage ===
Metric                          Value  Updated
deepmail_host_ram_usage_percent  44.33  03 Dec 12:05:07
deepmail_host_cpu_usage_percent  3.80   03 Dec 12:05:07

=== Host health ===
Metric                       Status          Value  Updated
deepmail_host_health_status  status=healthy  3      03 Dec 12:04:07

=== Containers ===
Name       CPU   RAM   Health   Connections  Updated
admin      0.11  7.12  healthy  38           03 Dec 12:04:31
antispam   0.16  5.11  healthy  -            03 Dec 12:04:31
antivirus  0.14  0.40  down     -            03 Dec 12:04:31
auth       0.00  0.26  healthy  37           03 Dec 12:04:31
fetchmail  0.01  0.84  healthy  -            03 Dec 12:04:31
front      0.27  2.19  healthy  -            03 Dec 12:04:31
imap       0.38  2.43  healthy  7            03 Dec 12:04:31
ldap       0.00  0.66  healthy  -            03 Dec 12:04:31
resolver   0.00  0.45  healthy  -            03 Dec 12:04:31
smtp       0.75  2.08  healthy  1            03 Dec 12:04:31
webdav     0.00  0.55  healthy  2            03 Dec 12:04:31
webmail    0.01  1.66  healthy  0            03 Dec 12:04:31

=== Storage metrics ===
Metric                          Labels        Value         Updated
deepmail_storage_read_bytes     name=archive  77848.00      03 Dec 12:04:55
deepmail_storage_read_bytes     name=core     364697985.00  03 Dec 12:04:55
deepmail_storage_read_bytes     name=mail     7729603.00    03 Dec 12:04:55
deepmail_storage_write_bytes    name=archive  0.00          03 Dec 12:04:55
deepmail_storage_write_bytes    name=core     363479266.00  03 Dec 12:04:55
deepmail_storage_write_bytes    name=dav      363479266.00  03 Dec 12:04:55
deepmail_storage_used_percents  name=core     33.70         03 Dec 12:04:55
deepmail_storage_read_bytes     name=dav      364697985.00  03 Dec 12:04:55
deepmail_storage_used_percents  name=mail     33.70         03 Dec 12:04:55
deepmail_storage_used_percents  name=dav      33.70         03 Dec 12:04:55
deepmail_storage_write_bytes    name=mail     485719.00     03 Dec 12:04:55
deepmail_storage_used_percents  name=archive  33.70         03 Dec 12:04:55

=== Storage health ===
Target                          Status                        Value  Updated
deepmail_storage_health_status  name=core, status=healthy     3      03 Dec 12:04:07
```

Рисунок 172 – 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.

3.12 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 дает 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.

3.13 Коды ошибок

Когда что-то идет не так – пользователь не может войти, письмо не доставляется, календарь не синхронизируется, реплика данных не сошлась – DeepMail отмечает каждый такой сбой коротким человекочитаемым кодом. Эти коды видны в логах, в интерфейсе администратора и в JSON-ответах внутренних API. Они помогают сразу понять, в каком сервисе и какого рода случился сбой, не разбираясь в содержимом сообщения.

Каждый код формируется по следующей схеме:

DM – <СЕРВИС> – <КАТЕГОРИЯ><НОМЕР>

Таким образом даже первоначально, увидев код, можно понять примерную проблему.

Пример и пояснение структуры кода ошибки:

DM-AUTH-1203

```
  |      |   | | |
  |      |   | | └─ 003 – порядковый номер внутри пары «сервис + категория»
  |      |   | └── 2 – ошибка в этой категории и сервисе
  |      |   └──── 1 – категория «аутентификация»
  |      └──────── AUTH – префикс сервиса auth-service
  └─────────────── DM – фиксированный префикс «DeepMail»
```

Префикс после DM – это короткое имя сервиса, который зарегистрировал ошибку. Список префиксов, их соотношение с сервисами и значение сообщений представлены в таблице 8.

Таблица 8 – Список префиксов сервисов

Префикс в коде	Сервис	Что обычно сообщает
COM	Общие / сквозные	Кросс-сервисные сбои (валидация ввода, БД недоступна, Redis недоступен, расшифровка общего конфига)
ADM	admin-service	Интерфейс администратора, REST API, отображение всего инцидента в UI
AUTH	auth-service	Проверка пароля, токена, 2FA
IMAP	imap-service	IMAP, Sieve, ACL, квоты, поиск по почте
SMTP	smtp-service	Прием, отправка, маршрутизация SMTP, очередь
DAV	webdav-service	CalDAV/ CardDAV, событие в календаре, контакты, free-busy
LDAP	ldap-service	Синхронизация пользователей из AD/ LDAP
MIG	migration-service	Миграция почты по IMAP и EWS
SFTP	sftp-service	Файловая область пользователя (SFTP/ FTP/ WebDAV)
CTL	deepmail-controller	Контроллер хоста, оркестрация сервисов
RUN	deepmail-runner	Раннер для пересборки/ перерендера конфигов
DSA	deepmail-storage-adapter	Репликация данных между локациями

Первая цифра после префикса сервиса – это категория сбоя. Значения этой цифры одинаковы для всех сервисов (таблица 9).

Таблица 9 – Список категорий сбоев

Значение в коде	Категория	Что произошло
1	Аутентификация	Пользователь не подтвердил, кто он: неверный пароль, неверный или истекший токен, неверный 2FA-код, просроченная сессия
2	Авторизация/ доступ	Пользователь известен, но прав нет: нет прав администратора, IMAP/ SMTP отключен, метод не разрешен
3	Валидация ввода	Запрос синтаксически или семантически неверен: некорректные данные в форме, не указано обязательное поле, тело слишком велико
4	Не найдено	Запрошенного объекта нет: пользователь, домен, запись, путь, файл
5	Конфликт состояния	Объект уже существует или несовместимое состояние: «уже подключено», «не инициализировано»
6	Лимит/ квота/ лицензия	Превышено ограничение: лимит пользователей, истекшая лицензия, превышена квота, слишком частые попытки
7	Внешняя зависимость	Сбой в смежном компоненте: контроллер не отвечает, DSA, Redis недоступен, БД не отвечает, таймаут
9	Внутренняя ошибка	Баг или непредвиденный сбой на стороне DeepMail (необработанное исключение)

Цифры 0 и 8 зарезервированы и в текущей версии не используются.

Если кратко: 1-3 – это проблема на стороне клиента/ пользователя, 4-5 – расхождение со состоянием системы, 6 – лимиты, 7 – смежники, 9 – баг на стороне разработки.

Далее для более точной расшифровки кода необходимо обратиться в реестр кодов ошибок. Полный реестр всех известных кодов с их точными значениями представлен в файле ERROR_CODES.md, который размещен в корне репозитория DeepMail.

Важно! Эти коды ошибок – это «внутренние» коды DeepMail, они не уходят к внешним клиентам и не передаются в нативные протоколы DeepMail-сервисов, а предназначаются только для внутренней диагностики.

Каждый код виден сразу в нескольких местах:

- в логах сервиса;
- в интерфейсе администратора (в уведомлениях, на странице ошибки, в журнале аудита);
- JSON-ответы API;
- в CLI;

В админ-панели иногда может отображаться код «чужого» сервиса (например DM-CTL-.. (код контроллера) а не DM-ADM-.. о том что в интерфейсе администратора что-то случилось). Это сделано специально: пользователь увидит реальную сторону инцидента, и поддержка обратится сразу в логи нужного сервиса.

Когда в логе отображается несколько кодов разных сервисов подряд – это нормально и очень полезно: видна цепочка сервисов и где конкретно что-то «сломалось». Например: DM-ADM-7005 («ошибка DSA») – значит, admin-service сделал шаг репликации, но DSA вернул ошибку; искать ее корень нужно в логах DSA.

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.

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

Таблица 10 – 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	+	+	+	+	+	+	

Примечания:

1) Статус контейнера – это Alive/dead (up/down) каждого сервиса через Docker API.

2) CPU – это потребление CPU контейнера.

3) RAM – это потребление памяти контейнера.

4) Входящий/исходящий трафик – это объём входящих/исходящих байтов по сети.

5) Drop/Error Network – это отслеживание ошибок и потерь пакетов в сетевом стеке каждого контейнера.

6) 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 админ-панели перейдите в раздел «Система» и выберите «Профили». Откройте профиль SMTP для редактирования, нажав кнопку

в карточке 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 «ХОСТ РЕЛЕ» укажите: *192.168.92.157*. Сохраните изменения нажав кнопку 

.

Выполните реконфигурацию хоста профиля (см. 3.2.2.3)».

Добавьте релейный домен, перейдя в главном меню в раздел «Транспорт» → инструмент «Реле» (см. 3.6.1.1). В окне добавления нового релейного домена укажите:

- в поле «Имя релейного домена» – *ksmgexample.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, появляются 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. Таким образом обеспечивается целостность и доступность ПО.

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 приведен перечень основных задач с рекомендуемой периодичностью и кратким описанием действий (таблицы 11–14).

Таблица 11 – 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

Таблица 12 – 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

Область	Действие	Периодичность
Резервное копирование	Контроль выполнения запланированных задач резервного копирования (снапшоты ВМ, дампы БД, копии конфигураций). Проверка целостности резервных копий.	Еженедельно
Анализ производительности	Просмотр долгосрочных графиков CPU/RAM (период 7 дней) для выявления трендов и аномалий.	Еженедельно

Таблица 13 – 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

Таблица 14 – Ежеквартальные операции

Область	Действие	Периодичность
Обновление версии DeepMail	Плановое обновление платформы до актуальной версии (при наличии значительных релизов). Предварительное тестирование в изолированной среде.	Ежеквартально
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 15.

Таблица 15 – Термины и определения

Термин	Определение
CLI-бинарник	это готовая к запуску компьютерная программа, которая работает в интерфейсе командной строки (CLI).
SIP-телефония	Голосовая связь через интернет на основе протокола SIP, 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
Георасределенная система	— это две или несколько локаций, между которыми система синхронизирует почту и данные календарей/контактов
Дистрибутив	Форма распространения программного обеспечения, обычно содержащая программу-установщик (для выбора режимов и параметров установки) и набор файлов, содержащих отдельные части программного средства
Домен (или доменное имя)	Уникальное имя, служащее для идентификации области расположения ресурса (веб – сайта) в сети Интернет
Иконка	Графическое изображение элемента пользовательского интерфейса (меню, кнопки, значка, списка и т.д.)
Кластер	Группа компьютеров, серверов или процессоров, объединённых высокоскоростными каналами связи, представляющая с точки зрения пользователя единый аппаратный ресурс

Термин	Определение
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
Локация	Отдельная площадка установки DeepMail: географическая зона со своими серверами и хранилищами
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
Оркестратор	Программный компонент, который автоматически управляет, координирует и масштабирует компьютерные приложения, контейнеры или сервисы
Плейбук	Сценарий автоматизации – файл (обычно с расширением *.yml)
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	Совокупность средств и методов, обеспечивающая передачу информации, между пользователем и программно-аппаратным обеспечением, в удобной для пользователя форме
Резолвинг	Перевод доменного имени сайта в IP-адрес

Термин	Определение
Реплика	Копия данных (почта, календари, контакты), принадлежащих пользователям одной локации, сохраненная в хранилище другой локации
Репозиторий	Хранилище (каталог), в котором хранятся какие-либо данные, например установочные пакеты, образы сервисов, снапшоты (моментальные снимки) системы
Сообщения	Сообщения, передаваемые по электронной почте на базе ПО DeepMail
Спам	Массовая рассылка корреспонденции рекламного характера (нежелательных сообщений) лицам, не выразившим желания ее получить
Стек	Группа сервисных контейнеров (набор сервисов), которые можно запускать и останавливать независимо друг от друга
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
Чекбокс	Флажок, переключатель, переводящий функцию в состояние включено/ выключено

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;

ACL – англ. Access Control List – список контроля доступа;

API – англ. Application Programming Interface – простыми словами, это набор правил и инструментов, которые позволяют одной программе общаться с другой;

CLI – англ. Command-Line Interface – интерфейс командной строки;

CRUD – англ. аббревиатура, обозначающая четыре базовые функции работы с данными – **C**reate (Создание), **R**ead (Чтение), **U**pdate (Обновление), **D**elete (Удаление);

DC – англ. Domain Controller – контроллер домена;

DEB – англ. Debian package **–** формат установочных файлов, используемый в операционной системе Linux, а точнее в дистрибутивах на основе Debian;

DNS – англ. Domain Name System – система доменных имен;

DSA – англ. DeepMail Storage Adapter – фоновый агент, который выполняет репликацию данных между локациями;

HA – англ. High Availability – высокая доступность;

HTTP – англ. HyperText Transfer Protocol – стандартный протокол для передачи гипертекстовых документов в интернете;

IMAP – англ. Internet Message Access Protocol – протокол прикладного уровня для доступа к электронной почте;

IP – англ. Internet Protocol – фундаментальный протокол, который отвечает за доставку данных в интернете;

KSMG – англ. Kaspersky Security Management Gateway – программное решение от «Лаборатории Касперского» для защиты периметра сети и фильтрации интернет-трафика;

LDAP – англ. Lightweight Directory Access Protocol – протокол прикладного уровня для доступа к службе каталогов;

MAPI – англ. Messaging Application Programming Interface – проприетарный протокол Microsoft, который обеспечивает глубокую интеграцию между почтовым клиентом и сервером;

PBX – англ. Private Branch Exchange – офисная телефонная станция;

REST API – англ. Representational State Transfer Application Programming Interface – это способ, с помощью которого одна программа может «общаться» с другой через интернет по протоколу HTTP;

SIP – SIP-телефония, англ. Session Initiation Protocol – технология, которая позволяет совершать звонки через интернет;

SMTP – англ. Simple Mail Transfer Protocol – сетевой протокол, предназначенный для передачи электронной почты в сетях TCP/IP;

SSE – англ. Server-Sent Events – это технология, которая позволяет серверу отправлять данные браузеру в режиме реального времени через одно длинное HTTP-соединение;

SSL – англ. Secure Socket Layer – криптографический протокол, который защищает данные при передаче по сети;

TLS – англ. Transport Layer Security – современный стандарт защиты данных в интернете;

UI – англ. User Interface – интерфейс пользователя.