ООО «НОВЫЕ ОБЛАЧНЫЕ ТЕХНОЛОГИИ»

Программное обеспечение «Корпоративная система электронной почты и планирования совместной работы команд «Mailion»

Руководство администратора

RU.29144487.506900.001 98

На 533 листах

Москва
2024

СОДЕРЖАНИЕ

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

В настоящем документе применяют следующие сокращения с соответствующими расшифровками (см. Таблица 1).

Таблица 1 – Перечень сокращений, терминов и определений

Сокращение, термин	Расшифровка и определение
A-запись	Address, одна из ключевых ресурсных записей, используется для связи домена с IP-адресом сервера
AD	Microsoft Active Directory, служба каталогов, разработанная Microsoft для доменных сетей Windows
AOF	Append Only File, свойство компьютерного хранилища данных, позволяющее добавлять новые данные в хранилище, при этом существующие данные остаются неизменными
API	Application Programming Interface, программный интерфейс приложения
CA	Certification Authority, центр сертификации
CLI	Command Line Interface, интерфейс командной строки
DNS	Domain Name System, система доменных имен
Docker	Программное обеспечение для автоматизации развертывания и управления приложениями в средах с поддержкой контейнеризации, контейнеризатор приложений
DOS	Dispersed Object Store, распределенное объектное хранилище
FCM	Firebase Cloud Messaging, служба, которая упрощает обмен сообщениями между мобильными и серверными приложениями
FQDN	Fully Qualified Domain Name, полное доменное имя, иногда также называемое абсолютным доменным именем. Это доменное имя, которое указывает точное местоположение домена в древовидной иерархии системы доменных имен (DNS). Включает в себя имена всех родительских доменов иерархии DNS
GAL	Global Address List, глобальная адресная книга
KSE	Kaspersky Scan Engine, серверное решение для защиты от вредоносного ПО
LDAP	Lightweight Directory Access Protocol, облегченный протокол доступа к каталогам, открытый стандартизированный протокол, применяемый для работы с различным реализациям служб каталогов, в том числе и Active Directory

Сокращение, термин	Расшифровка и определение
MX	Mail Exchanger, тип DNS-записи, предназначенный для маршрутизации электронной почты с использованием протокола SMTP
OSI	Open System Interconnection, модель сетевых протоколов, описывающая взаимодействие сетевых устройств
PTR-запись	Pointer, противоположность A-записи для DNS. Связывает IP-адрес сервера с его каноническим именем (доменом). Применяется для фильтрации почты
RPO	Recovery point objective, максимальный период за который могут быть потеряны данные. Время восстановления файлов из резервного хранилища не должно превышать показателя RPO
SIEM	Security information and event management, управление событиями и информацией о безопасности – класс программных продуктов, предназначенных для сбора и анализа информации о событиях безопасности
SLA	Service Level Agreement, формальный договор между заказчиком и потребителем, содержащий описание услуг, обязанностей и сторон, а также согласованный уровень качества предоставляемых услуг
SPN	Service Principal Name, уникальный идентификатор экземпляра сервиса. SPN используется аутентификацией Kerberos для сопоставления экземпляра сервиса с учетной записью сервиса (service logon account)
Standalone	Конфигурация установки ПО «Mailion» без отказоустойчивости
Бэкап (backup)	Резервное копирование
ДУ	Директория установки
Нода	Виртуальная или физическая машина, на которой разворачиваются и запускаются контейнеры
ООО	Общество с ограниченной ответственностью
ОС	Операционная система
Панель администрирования	Панель администрирования «Mailion»
ПК	Персональный компьютер
ПО	Программное обеспечение
ПО «Mailion»	Программное обеспечение «Корпоративная система электронной почты и планирования совместной работы команд «Mailion»
СУБД	Система управления базами данных

Сокращение, термин	Расшифровка и определение
УЦ	Удостоверяющий центр
ЦОД	Центр обработки данных

1 ОБЩИЕ СВЕДЕНИЯ

1.1 Назначение

Mailion – корпоративная почтовая система нового поколения на базе микросервисной архитектуры, обеспечивающая обмен электронными сообщениями, планирование рабочего времени, интеллектуальный поиск информации и работу с адресными книгами. Система отличается высокой отказоустойчивостью, способна на быстрое самовосстановление и масштабируемость в зависимости от нагрузок.

В состав продукта входят:

- Почтовая система Mailion для обмена электронными сообщениями, совместной работы с календарями, хранения адресных книг и индексации данных;
- Настольный почтовый клиент «МойОфис Почта» для работы с электронными сообщениями, календарями, задачами и адресными книгами на операционных системах Linux и Windows.

1.2 Структура ПО «Mailion»

Структура ПО «Mailion» представляет собой набор сервисов, обеспечивающих работу системы и взаимодействие между подсистемами ПО «Mailion».

Сервисы (представленные в виде установочных ролей) описаны в разделе 2.2.1.

Общая логическая схема ПО «Mailion» приведена на рисунке (см. Рисунок 1).

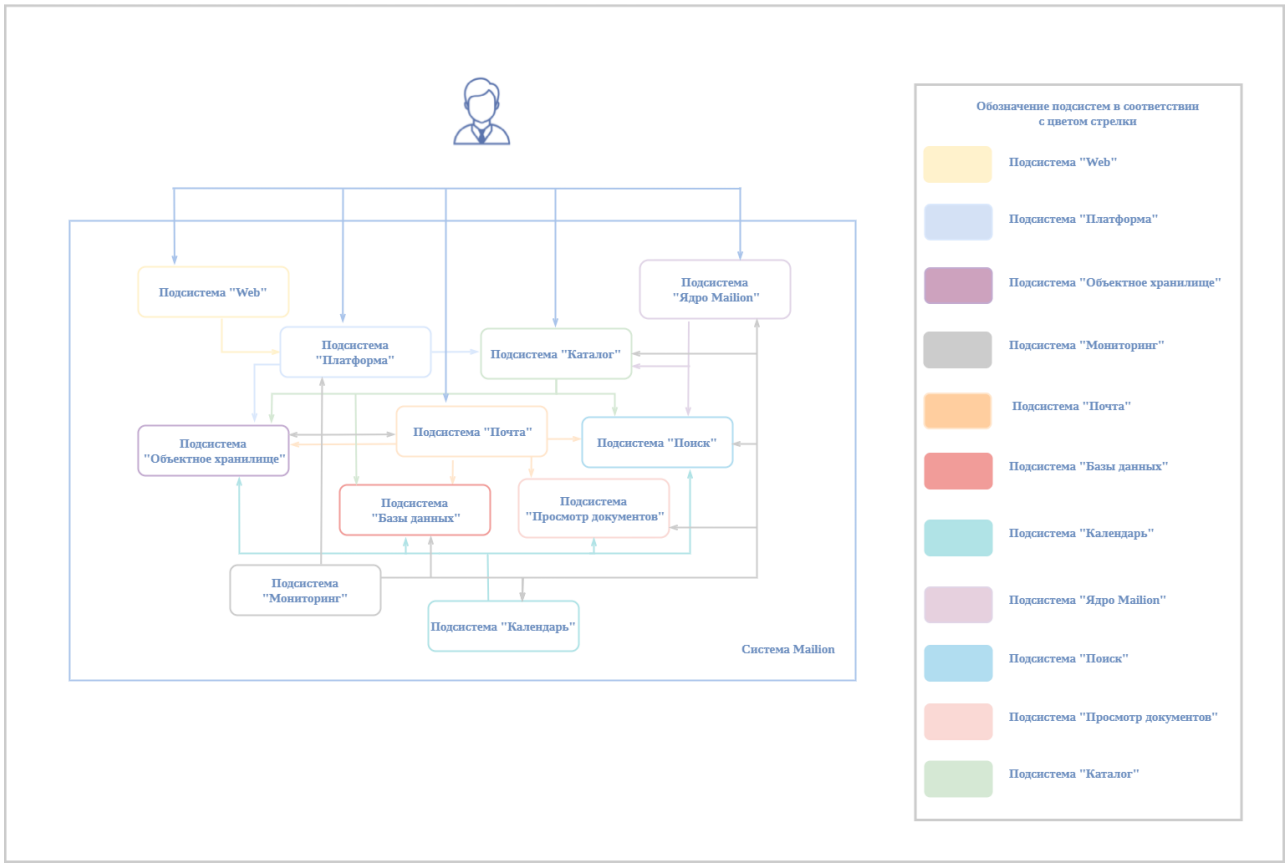


Рисунок 1 – Общая логическая схема ПО «Mailion»

Детальная логическая схема ПО «Mailion» приведена на рисунке (см. Рисунок 2).

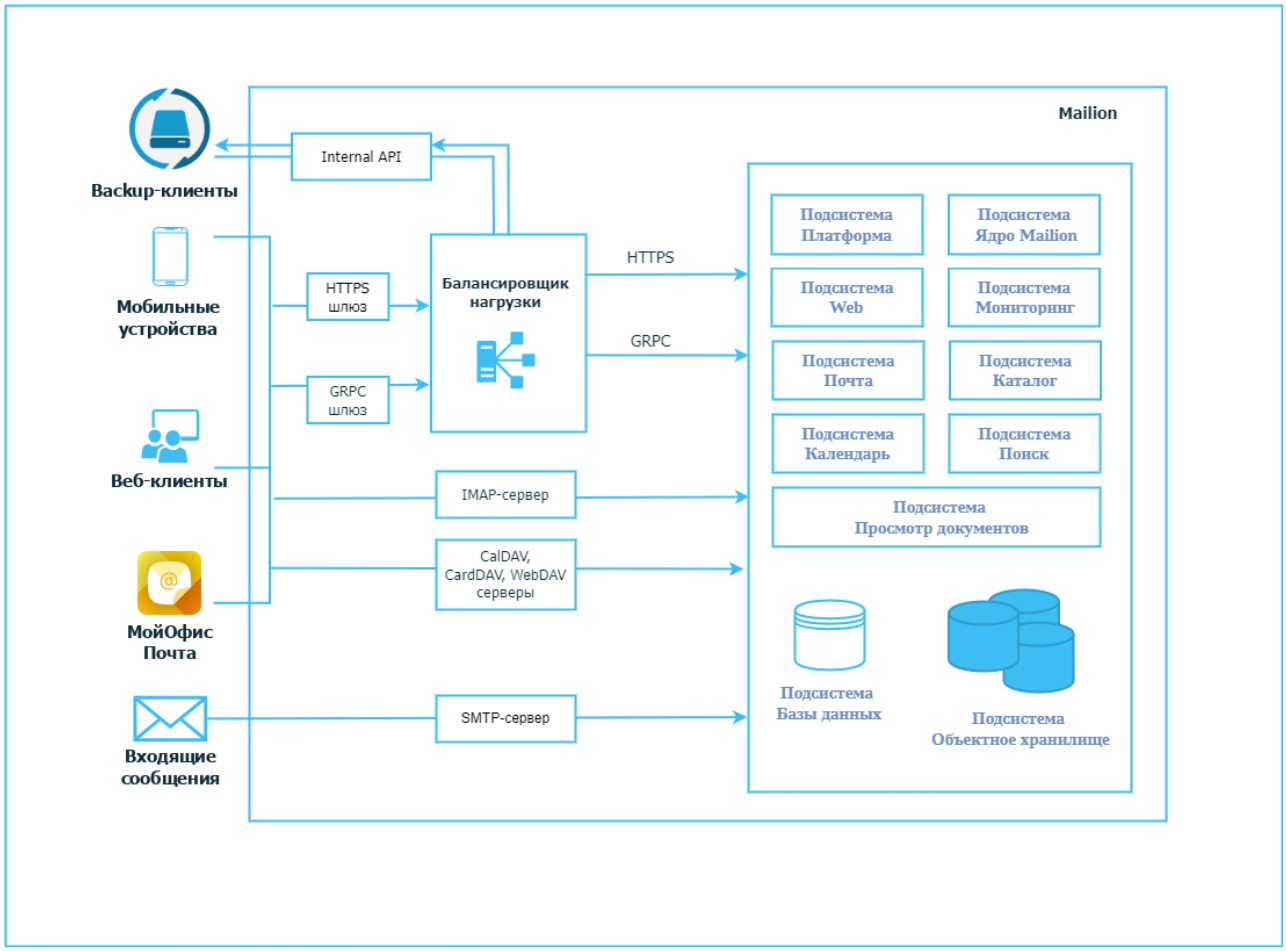


Рисунок 2 – Детальная логическая схема ПО «Mailion»

1.3 Уровень подготовки пользователя и администратора

Пользователь Административной панели «Mailion» должен обладать следующими навыками:

– знание одного (или нескольких) веб-браузеров, используемых в организации (см. раздел 1.4.2);
– знание стандартных офисных приложений;
– знание операционной системы (ОС) Linux;
– администрирование информационных систем.

Администратор ПО «Mailion» должен соответствовать следующим требованиям:

1. Знание основ сетевого администрирования:
   – сетевая модель OSI и стек протоколов TCP/IP;

- IP-адресация и маски подсети;
- маршрутизация: статическая и динамическая;
- протокол обеспечения отказоустойчивости шлюза (VRRP);

2. Опыт работы с подсистемами виртуализации на уровне эксперта:
   - работа с подсистемой контейнерной виртуализации (Docker/Podman);
   - работа с одной из подсистем серверной виртуализации на базе гипервизоров Hyper-V, VMware vSphere ESXi, KVM;
   - навык администрирования операционной системы (ОС) Linux с помощью консоли;
   - опыт работы со службой доменных имен (DNS):
     - знание основных терминов (DNS, IP-адрес и так далее);
     - понимание принципов работы DNS (корневые серверы, TLD-серверы, серверы имен доменов, разрешающий сервер имен и так далее);
     - знание типов записи и запросов DNS;
3. Знание видов архитектуры, а также основных компонентов инфраструктуры открытых ключей (PKI), к которым относятся:
   - закрытый и открытый ключи;
   - сертификат открытого ключа;
   - регистрационный центр (RA);
   - сертификационный центр (CA);
   - хранилище сертификатов (CR);
4. Практический опыт администрирования на уровне эксперта:
   - Redis;
   - NATS;
   - Prometheus;
   - MongoDB;
   - Postfix;
5. Опыт работы с подсистемой централизованного управления Ansible.
6. Опыт работы со стандартными офисными приложениями.

1.4 Системные требования

Перечень системных требований к аппаратному и программному обеспечению приведен в разделах 1.4.1, 1.4.2 и 1.4.3.

1.4.1 Базовый продукт (дистрибутив) «Mailion», серверная часть

1.4.1.1 Аппаратные требования

Ниже представлены описание ролей групп серверов, стандартные расчеты аппаратной части, расчет на 10 000 пользователей, требования к сетевой и дисковой подсистеме.

1.4.1.1.1 Описание групп сервера

В таблице 2 приведено обоснование выделения машин под группы сервера.

Таблица 2 – Описание групп сервера

Имя группы сервера	Обоснование выделения машин
ucs_frontend	Веб-сервера Mailion и прокси-сервисы клиентских протоколов. Хранят также веб-статический контент. Должны быть выделены, так как являются пограничными серверами между внешними сетями и внутренними службами системы или могут быть размещены за пограничным web application firewall
ucs_mail	Сервера, выполняющие приём и отправку писем. Являются точкой, граничащей между внешними сетями и внутренними службами. Рекомендуется не совмещать с веб и прокси серверами, чтобы при отказе или атаке не терять работоспособность в полном объёме. Могут быть размещены за пограничным web application firewall
ucs_apps	Сервера основной группы микросервисов, реализующих основной функционал системы
ucs_balancers	
ucs_calendar	
ucs_catalog	Сервера группы микросервисов, реализующих функционал Каталога. Рекомендуется разделение с остальными ролями для обособления в части безопасности. Нагрузка на эту группу повышенная, так как не только пользователи, но и приложения имеют различные уровни доступа, что постоянно проверяется внутри системы
ucs_converter	Сервера группы подготовки предпросмотра документов, конвертации разных форматов в форматы, готовые для отображения в браузере. Отделены от основной функциональности для обеспечения

Имя группы сервера	Обоснование выделения машин
	толерантности к отказу, так как работают напрямую с пользовательскими данными, в которых сложно выполнить предпроверку корректности этих данных и отсутствия уязвимостей
ucs_search	Сервера группы поискового движка, обеспечивающего поиск по письмам, вложениям, каталогу, справке. Индексирование данных ресурсоёмкая задача. Чтобы не делать один огромный сервер, поисковые данные могут быть шардированны, чтобы запросы обрабатывались сразу несколькими экземплярами поиска
ucs_etcd	Сервера группы очередей и хранилищ данных о работе региона. Не имеют тенденции к масштабированию, потому выделены отдельно. Требуют очень быстрые и никем не занятые, с точки зрения обращений, диски
ucs_mq	
ucs_mongodb	Сервера группы баз данных. Требовательны к ресурсам и к гарантиям их наличия
ucs_redis_cache	Сервера группы кэширующих баз данных. Выделены для гарантии обеспечения требуемых ресурсов
ucs_redis_data	
dispersed_object_store	Сервера группы объектного хранилища. Основное хранилище всей системы
ucs_infrastructure	Сервер группы инфраструктуры. Служит для хранения образов инсталляции, сбора журналов доступа и ошибок работы системы, метрик, обеспечивает мониторинг всей системы. Должен быть обособлен для внешнего наблюдения за системой. Его работа не блокирует работу системы

1.4.1.1.2 Стандартные расчеты аппаратной части

Минимальные требования для установки ПО «Mailion» без отказоустойчивости (Mailion «Standalone») приведены в таблице 3.

В а ж н о – Режим и последующая настройка параметров на оборудовании без поддержки отказоустойчивости предоставляется в целях демонстрации функциональности ПО «Mailion». **Данный режим не поддерживается и к использованию не рекомендуется.**

Таблица 3 – Минимальные требования (установка без отказоустойчивости)

Имя группы сервера	**VCPU**	**RAM, Gb**	**HDD, Gb (без учета ОС)**	**SSD, Gb**	**Количество виртуальных машин**	**VCPU**	**RAM, Gb**	**HDD, Gb (для ОС)**	**SSD, Gb**
	на каждую роль					**итого на группу**			
Mailion «Standalone»					1	12	32	50	50
				ИТОГО:	**1**	**12**	**32**	**50**	**50**

Минимальные требования для установки ПО «Mailion» для отказоустойчивой (кластерной) установки приведены в таблице 4.

Таблица 4 – Минимальные требования (отказоустойчивая установка)

Имя группы сервера	**VCPU**	**RAM, Gb**	**HDD, Gb (без учета ОС)**	**SSD, Gb**	**Количество виртуальных машин**	**VCPU**	**RAM, Gb**	**HDD, Gb**	**SSD, Gb**
	на каждую роль					**итого на группу**			
ucs_frontend	6	6	10	10	2	12	12	20	20
ucs_mail									
ucs_apps	8	8	10		2	16	16	20	
ucs_catalog									
ucs_calendar									

Имя группы сервера	VCPU	RAM, Gb	HDD, Gb (без учета ОС)	SSD, Gb	Количество виртуальных машин	VCPU	RAM, Gb	HDD, Gb	SSD, Gb
	на каждую роль					итого на группу			
ucs_balancers									
ucs_converter									
ucs_search	16	18	10	15	3	48	54	30	45
ucs_etcd									
ucs_mongodb									
ucs_redis_cache									
ucs_mq									
ucs_redis_data									
dispersed_object_ store	3	4	20	4	4	12	12	80	16
ucs_infrastructure	4	8	100		1	4	8	100	
				ИТОГО:	**12**	**92**	**102**	**250**	**81**

Рекомендованные требования для установки ПО «Mailion» на отказоустойчивом оборудовании приведены в таблице 4.

Таблица 5 – Рекомендованные требования (отказоустойчивая установка)

Имя группы сервера	VCPU	RAM, Gb	HDD, Gb (без учета ОС)	SSD, Gb	Количество виртуальных машин	VCPU	RAM, Gb	HDD, Gb	SSD, Gb
	на каждую роль					итого на группу			
ucs_frontend	4	4	10		2	8	8	20	

Имя группы сервера	VCPU	RAM, Gb	HDD, Gb (без учета ОС)	SSD, Gb	Количество виртуальных машин	VCPU	RAM, Gb	HDD, Gb	SSD, Gb
	на каждую роль					итого на группу			
ucs_mail	4	4		10	4	16	16		40
ucs_catalog	8	8	10		2	16	16	20	
ucs_apps	8	8	10		2	16	16	20	
ucs_calendar									
ucs_balancers									
ucs_search	4	8		30	3	12	24		90
ucs_converter	4	8		30	3				
ucs_etcd	8	16		30	3	24	48		90
ucs_mongodb									
ucs_mq									
dispersed_object_store	4	4	60	10	4	16	16	240	40
ucs_redis_data	8	8		10	3	24	24		30
ucs_redis_cache									
ucs_infrastructure	4	8	200		1	4	8	200	
				ИТОГО:	**26**	**144**	**184**	**510**	**290**

1.4.1.1.3 Расчет требований для 10 000 пользователей

Расчет требований для 10 000 пользователей ПО «Mailion» приведен в таблице 6.

Таблица 6 – Расчет требований для 10 000 пользователей

Примечания	Имя группы сервера	VCPU	RAM, Gb	HDD, Gb (без учета ОС)	SSD, Gb	Количество виртуальных машин	VCPU	RAM, Gb	HDD, Gb	SSD, Gb
		на каждую роль					итого на группу			
Веб-сервера Mailion и прокси-сервисы клиентских протоколов, работающие в DMZ	ucs_frontend	6	6	50	50	2	12	12	100	100
ВМ, выполняющие приём и отправку писем, работающие в DMZ	ucs_mail									
Блок ВМ приложений, обеспечивающих основную функциональность	ucs_apps	8	8	50	0	2	16	16	100	0
	ucs_balancers									
	ucs_calendar									
Блок ВМ приложений Каталога	ucs_catalog									
Блок ВМ подсистемы предпросмотра документов	ucs_converter									

Примечания	Имя группы сервера	VCPU	RAM, Gb	HDD, Gb (без учета ОС)	SSD, Gb	Количество виртуальных машин	VCPU	RAM, Gb	HDD, Gb	SSD, Gb
		на каждую роль					итого на группу			
Блок ВМ поисковой подсистемы	ucs_search	**8**	**32**	**50**	**256**	**3**	**24**	**96**	**150**	**768**
ВМ группы очередей и хранилищ данных о работе региона	ucs_etcd	**16**	**32**	**50**	**201**	**3**	**48**	**96**	**150**	**603**
	ucs_mq									
ВМ группы баз данных	ucs_mongodb									
ВМ группы хранилищ	dispersed_object_store	**4**	**8**	**3471**	**24**	**4**	**16**	**32**	**13883**	**95**
ВМ группы кэширующих баз данных	ucs_redis_cache	**8**	**8**	**0**	**50**	**3**	**24**	**24**	**0**	**150**
	ucs_redis_data									
ВМ инфрастуктуры. Является хранилищем всех образов инсталяции, сервером мониторинга, логколлектором	ucs_infrastructure	**4**	**8**	**300**	**0**	**1**	**4**	**8**	**300**	**0**

Примечания	Имя группы сервера	VCPU	RAM, Gb	HDD, Gb (без учета ОС)	SSD, Gb	Количество виртуальных машин	VCPU	RAM, Gb	HDD, Gb	SSD, Gb
		на каждую роль					итого на группу			
ИТОГО:						18	144	284	14684	1716

Параметры расчета приведены в таблице 7.

Таблица 7 – Параметры расчета

Параметр	Значения	Заполнить	Комментарий
Количество пользователей	10000	да	
Квота на ящик, Гб	1	да	
Избыточность данных DOS: d-сегменты	2	да	Количество сегментов самих данных, при использовании кодов Рида-Соломона, которые будут записаны в хранилище
Избыточность данных DOS: p-сегменты	1	да	Количество избыточных сегментов, при использовании кодов Рида-Соломона, которые будут записаны в хранилище
Фактор репликации данных DOS	3	да	Фактор репликации для индексов DOS (количество полных копий записи индекса)
Фактор репликации данных метаданных	3	да	Фактор репликации для метаданных (заголовки, участники и пр.) СУБД Mailion
Процент заполнения квоты ящика	100,00%	нет	
Избыточность данных DOS (d+p)	3	нет	Итоговая избыточность хранилища
Количество писем, шт	20971520	нет	

Дополнительные пояснения приведены в таблице 8.

Таблица 8 – Дополнительные пояснения

Данные, помеченные цветом	Пояснения
	Для данных в ячейках, отмеченных этим цветом, нужно 2 или более блочных устройств. Рекомендуются физические устройства, которые не требуют резервирования на уровне RAID массива на хостовой системе
	Все ресурсы указаны с расчётом работы ОС ВМ

1.4.1.1.4 Требования к дисковой подсистеме

Требования к дисковой подсистеме приведены в таблице 9.

Таблица 9 – Характеристики дисков

Тип диска	min IOPS read	min IOPS write	IOPS/GB read	IOPS/GB write	latency (clat) ms
HDD	300	150	1	1	<12
SSD	200000	80000	1700	700	<1

1.4.1.1.5 Требования к сетевой подсистеме

Между серверами (виртуальными машинами) должен быть канал в 1 Гб/с и предельное время ожидания (Network latency) 5-7 ms.

1.4.1.2 Программные требования

Требования к программному обеспечению для места оператора, на котором производится установка, приведены в таблицах 10, 11.

Таблица 10 – Требования к программному обеспечению для места оператора

Требование	Описания	
Поддерживаемые браузеры	Перечень поддерживаемых браузеров приведен в разделе 1.4.2	
Python3	v. 3.6+	
Модули Python	jmespath	
	jinja2	Необходима версия выше, чем v.2.10
	ansible	2.11 или новее, но до 2.12
	netaddr	python3-netaddr
	dnspython	
	hvac	
	pymongo	Не ниже версии 3.12
Дополнительные пакеты	mongodb-mongosh	Необходима версия 1.6.2_amd64.deb https://www.mongodb.com
	epel-release	Extra Packages Enterprise Linux, https://docs.fedoraproject.org/en-US/epel/

П р и м е ч а н и е – Перед установкой должен быть скачан и смонтирован образ Mailion (см. раздел 2.1).

Таблица 11 – Требования к программному обеспечению для серверов, на которые производится установка

Требование	Описания
ОС	Операционная система специального назначения «Astra Linux Special Edition» РУСБ.10015-01 1.7 – Орёл (базовый); Операционная система специального назначения «Astra Linux Special Edition» РУСБ.10015-01 1.7 – Воронеж (усиленный); Операционная система специального назначения «Astra Linux Special Edition» РУСБ.10015-01 1.7 – Смоленск (с ограничениями)
Стандартные репозитории ОС	Подключение всех стандартных репозиториев ОС либо их зеркал во внутренней сети для установок в закрытом контуре
Репозитории elrepo и docker-ce, ppa:canonical-kernel-team/ppa	Подключение репозиториев **elrepo** (http://elrepo.org) и **docker-ce** (https://download.docker.com/linux/centos/docker-ce.repo) для установки соответствующих пакетов ядра Linux и ПО **Docker**, не входящих в состав поставки для установок в закрытом контуре
Доступ	Для каждого сервера, на котором выполняется установка, должен быть обеспечен SSH-доступ: – с sudo привилегиями (ALL=(ALL) NOPASSWD: ALL); – без пароля (доступ по ключу)
Рекомендации по версии ядра Linux	Требуется ядро mainline (обновляется по умолчанию, если не передан флаг **UPGRADE_KERNEL=false**). С более старыми версиями ядер (lts) работоспособность не гарантируется из-за особенностей **Docker** (требуется полная поддержка cgroup2 в ядре)

1.4.2 Базовый продукт (дистрибутив) «Mailion», веб-интерфейс

Требования к аппаратному и программному обеспечению приведены в таблице 12.

Таблица 12 – Требования к аппаратному и программному обеспечению

Базовый продукт	Аппаратные требования		Программные требования
	минимальные	**рекомендуемые**	**Поддерживаемые ОС и браузеры**
Mailion.Web	• процессор – x86/x64 с тактовой частотой 1,6 ГГц; • оперативная память – 2 Гбайт; • свободное место на диске – 3 Гбайт для установки; • разрешение экрана монитора – 1280 x 720; • клавиатура, мышь; • подключение к Интернету (минимум LTE)	• процессор – x64 с тактовой частотой 3,0 ГГц и выше; • оперативная память – 8 Гбайт; • свободное место на диске – 3 Гбайт для установки; • разрешение экрана монитора – 1920 x 1080 и выше; • клавиатура, мышь; • подключение к Интернету (минимум LTE)	Операционные системы: • Windows 7 и выше; • macOS Ventura 13 и выше; • Ubuntu 18.04 (64-разрядная версия) и выше; • Debian 10 и выше; • Fedora Linux 38 и выше; • Alt Linux 8 СП; • «Альт Рабочая станция» версии 10; • RedOS 7.3; • Astra Linux 1.7. Браузеры: • Safari 16+; • Chrome 110+; • Firefox 121+; • Edge 107+; • Yandex 23+

1.4.3 Базовый продукт (дистрибутив) «МойОфис Почта», настольный клиент

В таблице 13 приведены аппаратные требования для настольных клиентов «МойОфис Почта».

Таблица 13 – Аппаратные требования для настольных клиентов «МойОфис Почта»

Базовый продукт (дистрибутив)	Минимальные требования	Рекомендуемые требования
«МойОфис Почта», настольный клиент	– процессор x64 с тактовой частотой 1,0 ГГц; – оперативная память 2 Гб; – пространство для установки на жестком диске 3 Гбайт; – монитор с разрешением 1024x768; – клавиатура, мышь	– процессор x64 с тактовой частотой 2,0 ГГц и выше; – оперативная память 4 Гбайт и выше; – пространство для установки на жестком диске 5 Гбайт и выше; – монитор с разрешением 1920x1080 и выше; – клавиатура, мышь

В таблице 14 приведен список поддерживаемых ОС для настольных клиентов «МойОфис Почта».

Таблица 14 – Поддерживаемые ОС для настольных клиентов «МойОфис Почта»

Базовый продукт (дистрибутив)	Платформа	Версии операционных систем
«МойОфис Почта», настольный клиент	Microsoft Windows	– Microsoft Windows 10 (64-разрядная версия); – Microsoft Windows 11 (64-разрядная версия)

Базовый продукт (дистрибутив)	Платформа	Версии операционных систем
	Linux	– Альт СП (64-разрядная версия) (ФСТЭК); – Альт Рабочая станция 10.X, K 10.X (64-разрядная версия); – Astra Linux Common Edition, релиз 2.12.X (64-разрядная версия)*; – Astra Linux Special Edition, релиз 1.6 (64-разрядная версия); – Astra Linux Special Edition, релиз 1.7 «Орел» уровень защищенности – базовый (64-разрядная версия); – Astra Linux Special Edition, релиз 1.7 «Воронеж» уровень защищенности – усиленный (64-разрядная версия); – Astra Linux Special Edition, релиз 1.7 «Смоленск» уровень защищенности – максимальный (64-разрядная версия); – РОСА Хром 12 Рабочая станция (64-разрядная версия); – РЕД ОС 7.3 Рабочая станция (64-разрядная версия). ** В связи с прекращением разработки ОС возможны ограничения в работе отдельных функций «МойОфис Почта»*
	Дополнительное программное обеспечение	
	Необходимо наличие КриптоПро CSP 5.0.12000	

1.5 Требования к работе DNS

1.5.1 Организация работы сервисов разрешения имен

Во время установки производится настройка и запуск локального кэширующего DNS-сервера (**unbound**) на машинах группы **ucs_etcd**. Он используется для запросов только внутри инсталляции и подключается для контейнеров и самих серверов через соответствующие параметры групповых переменных. С настройками инсталлятора по умолчанию серверы будут перенастроены на работу через **unbound** и не будут принимать параметры серверов разрешения имен по **DHCP**. Поэтому важно направить **unbound** на внутренние DNS-серверы компании, если есть такая необходимость. По умолчанию **unbound** настроен на перенаправление запросов на адреса 8.8.8.8 и 1.1.1.1.

1.5.2 Разрешение имен на машине оператора

Перед установкой необходимо убедиться, что на машине оператора доступен и подключен DNS-сервер, в котором созданы записи, согласно разделу 1.5.3.1. Должны быть доступны DNS-записи для машин группы **ucs_db**. При необходимости на машине оператора необходимо отредактировать файл `/etc/hosts` и внести в него соответствующие сопоставления имен и адресов. Пример приведен ниже.

В а ж н о – Здесь и далее: **<install_domain_name>** – это доменное имя инсталляции, описанное в разделе 2.2.2.3.2.

```
192.168.0.1 ucs-db-1.<install_domain_name>
192.168.0.1 mongodb.ucs-db-1.<install_domain_name>
.......
192.168.0.n ucs-db-n.<install_domain_name>
192.168.0.n mongodb.ucs-db-n.<install_domain_name>
```

Проверить разрешение имени машины в адрес можно с помощью команды:

```
> dig A mongodb.ucs-db-1.<install_domain_name>
; <<>> DiG 9.18.1-1ubuntu1.2-Ubuntu <<>> A mongodb.ucs-db-
1.<install_domain_name>
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 45369
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1
```

```
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;mongodb.ucs-db-1.<install_domain_name>. IN A

;; ANSWER SECTION:
mongodb.ucs-db-1.<install_domain_name>. 900 IN CNAME ucs-db-
1.<install_domain_name>.
ucs-db-1.<install_domain_name>. 900 IN A  192.168.0.1

;; Query time: 23 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Tue Jan 10 15:56:32 MSK 2023
;; MSG SIZE  rcvd: 95
```

Секция **ANSWER SECTION** показывает, что имя разрешается в адрес:

```
mongodb.ucs-db-1.<install_domain_name>. 900 IN CNAME ucs-db-
1.<install_domain_name>.
ucs-db-1.<install_domain_name>. 900 IN        A   192.168.0.1
```

1.5.3 Формирование внешних доменных имен инсталляций

При установке системы есть возможность указывать метод формирования доменных имен инсталляции. Шаблон, который формирует итоговый вариант всех DNS-записей, на которых будет работать инсталляция, принимает на вход два параметра:

- значение переменной: **mailion_external_domain** – отображает основной домен, на котором будет работать инсталляция;
- значение переменной: **mailion_domain_module** – отображает способ формирования доменного имени.

Пример работы шаблона приведен в таблице 15.

Таблица 15 – Примеры работы шаблона

mailion_domain_module	Имя ссылки	mailion_external_domain	Результат
{service}.{domain}	Auth	test.example.com	auth.test.example.com
{service}-{domain}	Auth	test.example.com	auth-test.example.com
{service}-xz-1.{domain}	Auth	test.example.com	auth-xz-1.test.example.com

Таким образом, можно гибко настраивать принцип формирования доменных имен инсталляции. Это может пригодиться, например, если имеется Wildcard SSL сертификат на доменное имя **example.com** и ***.example.com**, но нет на ***.test.example.com**. Можно установить **mailion_domain_module** в значение **{service}-{domain}** и получить домены третьего уровня, которые подходят под текущий Wildcard SSL сертификат.

1.5.4 Необходимые DNS-записи

1.5.4.1 Внешние DNS-записи

В таблицах 16, 17 приведены все необходимые внешние DNS-записи, требуемые для инсталляции. Данная таблица сформирована для параметра **mailion_domain_module** со значением **{service}.{domain}** (т.е. формирование ссылок через точку к указанному домену). Если выбран другой метод формирования, необходимо соотнести его со значениями в таблицах ниже.

Таблица 16 – Сведения о внешних DNS-записях

Имя записи	Тип записи	Значение	Комментарии
api	CNAME	@	
auth	CNAME	@	
autoconfig	CNAME	@	
avatars	CNAME	@	
caldav	CNAME	@	
carddav	CNAME	@	
db	CNAME	@	
@	A	<ucs_frontend_vip>	Значение должно быть равно VIP-адресу между серверами с ролью **ucs_frontend** или адресу самого сервера этой группы, если производится установка без отказоустойчивости
@	TXT	"v=spf1 mx a:relay.<mailion_external_domain> ~all"	Необходимо указать сформированное имя, с учетом значения в словаре **mailion_external_domain**

Имя записи	Тип записи	Значение	Комментарии
@	MX	10 <mx1>	MX-запись указывает на A-запись в которой содержится адрес первого сервера из группы **ucs_mail**
@	MX	10 <mx2>	MX-запись указывает на A-запись в которой содержится адрес второго сервера из группы **ucs_mail** (и т.д.)
grpc	CNAME	@	
imap	CNAME	@	
mail	CNAME	@	
mail._domainkey	TXT	"v=DKIM1; k=rsa; p=<DKIM_KEY>"	Значение **DKIM_KEY** определяется на этапе установки
mx1	A	<ucs_mail_mx[0]>	Внешний IP-адрес, по которому доступен первый сервер из группы **ucs_mail**
mx2	A	<ucs_mail_mx[1]>	Внешний IP-адрес, по которому доступен второй сервер из группы **ucs_mail** (и т.д.)
preview	CNAME	@	
relay	A	<ucs_mail_relay_vip>	Значение должно быть равно VIP-адресу между серверами с ролью ucs_mail или адресу самого сервера этой группы, если производится установка без отказоустойчивости
resources	CNAME	@	
secured	CNAME	@	
smtp	A	<ucs_mail_vip>	
_adsp._domainkey	TXT	"dkim=all"	

Таблица 17 – Сведения о внешних DNS-записях

Имя записи	Тип	Приоритет	Вес	Порт	Адрес
_autodiscover._tcp	SRV	0	0	443	<mailion_external_domain>.
_caldavs._tcp	SRV	0	0	6787	caldav.<mailion_external_domain>.
_carddavs._tcp	SRV	0	0	6787	carddav.<mailion_external_domain>.

Имя записи	Тип	Приоритет	Вес	Порт	Адрес
_grpcsec._tcp	SRV	0	0	3142	grpc.<mailion_external_domain>.
_imap._tcp	SRV	0	0	143	imap.<mailion_external_domain>.
_imaps._tcp	SRV	10	0	993	imap.<mailion_external_domain>.
_smtps._tcp	SRV	10	0	465	smtp.<mailion_external_domain>.
_submission._tcp	SRV	0	0	587	smtp.<mailion_external_domain>.
_submissions._tcp	SRV	10	0	465	smtp.<mailion_external_domain>.

Примеры написания DNS-записей приведены в Приложении А. Пример написания внешних DNS-записей.

1.5.4.2 Внутренние DNS-записи

Все DNS-записи, используемые для работы самой системы внутри контура установки, формируются через “.” (точку) относительно вписанного в файл **inventory** имени сервера и создаются в **unbound** автоматически на основе переменной **ansible_default_ipv4**.

Это поведение можно переопределить, если заполнить все адреса вручную на основе примеров в файле групповых переменных или если не использовать **Ansible** и заполнить все необходимые записи во внешнем DNS-сервере. При подобном варианте необходимо создать «A»-записи для каждого сервера, вписанного в файл **inventory**, а также CNAME адреса на все поддомены (“*”) к каждому серверу, вписанному в **inventory**.

Пример заполнения таких записей приведен в таблице 18.

Таблица 18 – Пример заполнения

Имя записи	Тип записи	Значение
infra-01	A	10.10.1.110
*.infra-01	CNAME	infra-01

В а ж н о – **unbound** не должен быть доступен из внешней сети.

Использование **unbound** необязательно. Если при заполнении файла с параметрами групповых переменных выставляется параметр **mailion_use_unbound: False**, то **unbound** будет установлен, но не будет принимать участия в работе ПО «Mailion».

1.6 Рекомендации

1.6.1 Рекомендации по разметке дисков

При разметке дисков требуется учитывать следующее:

– все рекомендуемые аппаратные требования приведены в разделе 1.4.1.1, в соответствии с приведенными в разделе таблицами для разных типов установки будут разные требования по выделяемому дисковому пространству;
– для всех серверов рекомендуется оставлять не менее 20 Гб на корневой раздел для штатной работы ОС.
– для роли **ucs_infrastructure** или инсталляции в режиме «Standalone» рекомендуется выделить 50 Гб на корневой раздел, так как во время установки все образы инсталляции предварительно копируются в локальное хранилище docker (`/var/lib/docker/`);
– для всех серверов рекомендуется выделять отдельный раздел /srv, в который происходит установка компонентов системы, и переполнение которого не приведет к аварийной работе самой ОС. В этот раздел также могут быть направлены копии журналов работы компонентов, при соответствующей настройке лог-коллектора, что потребует дополнительного дискового пространства;
– для сервера роли **dispersed_object_store** рекомендуется выделять независимые диски HDD для серверной части и диски SSD под метаданные. Например:
  - **/srv/docker/dispersed_object_store/data/metadata/** – SSD, индексы документов и сегментов;
  - **/srv/docker/dispersed_object_store/data/disk1/{blob,rocksdb}** – HDD1, бэкенд1 – блоб и индекс бэкенда;
  - **/srv/docker/dispersed_object_store/data/disk2/{blob,rocksdb}** – HDD2, бэкенд2 – блоб и индекс бэкенда;
– распределение сегментов (data segments) + (parity segments):
  - сумма data segments + parity segments не должна превышать количества независимых дисков в серверной части хранилища;
  - не менее 2 + 1 независимых дисков в серверной части хранилища;

- для кластера из трех машин минимально допустимые значения – 2 (data segments) + 1 (parity segments) сегментов.

1.7 Ограничения

1.7.1 Ограничения при выполнении кластерной установки

При кластерной установке ПО «Mailion» можно выделить отдельный сервер для каждой роли или совместить несколько ролей на одном сервере. Необходимо учитывать, что некоторые серверные роли могут быть не совместимы с другими ролями.

Пример совместимости ролей приведен в таблице 19.

Таблица 19 – Совместимости ролей

Имя роли сервера	Совместимость с другими ролями сервера
ucs_calendar	Совместимы с другими ролями
ucs_balancers	
ucs_mq	
ucs_mail	Несовместимы с ролями **ucs_mongodb**, **ucs_etcd**, **ucs_redis_cache**, **ucs_redis_data**
ucs_apps	
ucs_catalog	
ucs_converter	
ucs_etcd	Несовместимы с ролями **ucs_apps**, **ucs_mail**, **ucs_converter**, **ucs_catalog**
ucs_mongodb	
ucs_redis_cache	
ucs_redis_data	
ucs_frontend	Несовместимы с другими ролями
ucs_search	
dispersed_object_store	
ucs_infrastructure	

В а ж н о – Не рекомендуется совмещать серверные роли при установке.

1.7.2 Ограничение по работе с файлом inventory

В файл `hosts.yml` вносятся только полностью определенные имена доменов (FQDN). Эти имена будут использоваться во время и после установки системы для обращения к внутренним сервисам. Часть логики установщика использует их для формирования доменных имен и адресов сервисов.

1.7.3 Ограничение по работе с Ansible

В подсистеме управления конфигурациями не должно быть предыдущих конфигурационных файлов самой подсистемы. В том числе конфигурационного файла, который по умолчанию устанавливается с пакетом (например, `/etc/ansible/ansible.cfg`). Такой файл требуется удалить либо перезаписать образцом из поставляемого ПО. Подробнее см. в https://docs.ansible.com/ansible/latest/reference_appendices/config.html#the-configuration-file.

Важно самостоятельно установить необходимые модули python из раздела 1.4.1.2, так как они не являются частью поставки системы.

1.7.4 Ограничение по работе с системами виртуализации

Следующие системы виртуализации поддерживаются для обеспечения работы ПО «Mailion»:

- VMware;
- KVM.

1.7.5 Ограничение по работе с хостами MX

Каждый хост MX должен иметь PTR-запись для обеспечения правильной фильтрации писем антиспам-системой.

1.7.6 Ограничение при заполнении файлов переменных

При заполнении инвентарного файла имя **tier** (#SECTION 2) должно всегда начинаться с «ucs_».

1.7.7 Ограничение при использовании данных внешнего каталога

Необходимо использовать учетные данные внешнего LDAP-каталога для авторизации и отправки писем в ПО «Mailion». Если пользователь хочет отправить письмо на адрес **test@installation.net**, то письмо не отправится, так как на домене **installation.net** нет почтового сервиса. Поэтому необходимо заменить доменную часть в Email при отправке письма.

Например, в ПО «Mailion» создан домен **ipa.example.installation.net**, на нем есть почтовый сервис и он связан с **example.ru** через поле **x_external_names** в базе данных. Соответственно, отправить письмо необходимо на **test@ipa.example.installation.net**.

В а ж н о – Если этот пользователь еще не был создан в ПО «Mailion» (а при отправке письма на почту из внешнего каталога в ПО «Mailion» создается пользователь, если он еще не был синхронизирован), то для того, чтобы была возможность в будущем под ним авторизоваться, необходимо использовать для входа не адрес **test@ipa.example.installation.net**, на который осуществлялась отправка письма, а **test@installation.net** по причине того, что такой Email заведен во внешнем каталоге.

1.7.8 Поддерживаемые языки интерфейса

– Русский.
– Английский.

Настольное приложение «МойОфис Почта» также поддерживает следующие языки интерфейса:

– испанский;
– португальский;
– французский.

1.7.9 Поддерживаемые веб-браузеры

Перечень поддерживаемых веб-браузеров приведен в разделе 1.4.2.

1.7.10 Парольная политика

При формировании любого пароля (во время создания записи администратора, тенанта, пользователя, ресурса, сотрудника и т. д.) используются правила по умолчанию, приведенные в таблице 20. Парольная политика, заданная по умолчанию, может быть изменена администратором.

Таблица 20 – Ограничения пароля по умолчанию

Параметр	Значение
Длина пароля	от 8 до 128 символов
Минимальное необходимое количество прописных букв	1
Минимальное необходимое количество строчных букв	1
Минимальное необходимое количество цифр	1
Минимальное необходимое количество специальных символов (например, !$%&@)	1

Текущие принятые по умолчанию политики находятся в настройках конфигурации сервиса **talaos**:

```
"default_password_policies": {
        "hash_type": 1,
        "max_len": 128,
        "min_digits": 1,
        "min_len": 8,
        "min_lower_case_letters": 1,
        "min_special_characters": 1,
        "min_upper_case_letters": 1
    }
```

1.8 Типовые схемы установки

ПО «Mailion» может быть представлено следующими типами установки:

– standalone (один виртуальный сервер в рамках одного физического сервера);
– распределенная standalone (несколько виртуальных серверов в рамках одного физического сервера);
– кластерная (все роли устанавливаются на разные виртуальные сервера или физические сервера).

2 ПЕРВИЧНАЯ УСТАНОВКА

2.1 Состав дистрибутива

Дистрибутив Mailion поставляется в виде файла образа ISO с именем `Mailion_1.9.iso`.

Образ дистрибутива предварительно монтируется командой:

```
mount Mailion_1.9.iso /mnt/disk
```

В состав дистрибутива ПО «Mailion» входят:

1. Установщик рабочего места оператора (`mailion_ansible_bin_1.9.run`).
2. Установщик окружения для проведения установки, включающий все необходимые образы и пакеты (`mailion_infra_1.9.run`).
3. Файлы EULA (End-user license agreement).
4. Файлы TPL (Third-party license).

Для самостоятельной установки настольного приложения «МойОфис Почта» с поддержкой криптографической защиты данных доступны следующие дистрибутивы (см. Таблица 21):

Таблица 21 – Список дистрибутивов ПО «МойОфис Почта»

ОС	Дистрибутивы
Windows	MyOffice_Mail_PSN_Windows_2.8G.msi
Linux	MyOffice_Mail_PSN_x64_2.8G.sh myofficemail-2.8G-x86_64.deb myofficemail-2.8G.x86_64.rpm

2.2 Подготовка к установке

В данном разделе приведена последовательность действий, которую необходимо произвести перед установкой Mailion.

2.2.1 Описание ролей Ansible для преднастройки серверов перед установкой

Ansible применяется для автоматизации настройки и развёртывания сервисов. Список ролей Ansible для ПО «Mailion» приведен в таблице 22.

Таблица 22 – Описание общих ролей Ansible для преднастройки серверов перед установкой

Наименование роли	Описание
authorized_keys	Добавляет указанные ssh-ключи для выбранных пользователей на серверы группы **play_hosts**
hostname	Устанавливает **hostname** для выбранных серверов
SELinux	Проверяет режим работы **SELinux** и переключает его в режим «enforcing» П р и м е ч а н и е – Только для дистрибутивов с пакетным менеджером **yum**.
packagemanager	Настраивает пакетный менеджер
locale	Устанавливает параметры **locale** на серверах
timezone	Устанавливает часовой пояс на серверах
sshd	Производит настройку службы удаленного доступа **sshd**
chrony	Устанавливает и настраивает службу синхронизации времени **chronyd** П р и м е ч а н и е – Только для ОС на базе Red Hat.
timesyncd	Устанавливает и настраивает службу синхронизации времени **timesyncd** П р и м е ч а н и е – Только для ОС Astra Linux.
sysctl	Устанавливает требуемые параметры ядра на серверах
limits	Настраивает параметры ограничений на серверах
kernel_ml	Устанавливает пакет **kernel_ml** последнего доступного ядра
kernel_ml_deb	Устанавливает пакет **kernel_ml** последнего доступного ядра для ubuntu
rsyslog	Устанавливает и настраивает сервис сбора журналов
docker	Устанавливает и настраивает **Docker**, подключает к **docker registry**
unbound	Устанавливает и настраивает кэширующий DNS-сервер
iptables	Устанавливает и настраивает службы межсетевого экрана с параметрами, требуемыми для конкретной роли
resolv	Производит настройку файла **resolv.conf**
package_tools	Добавляет требуемые пакеты для работы ПО «Mailion» в целевую ОС

Роли, используемые для подготовки ПО «Mailion», описаны далее в таблице 23.

Таблица 23 – Описание ролей, используемых при подготовке ПО «Mailion»

Наименование роли	Описание
keepalived	Устанавливает и запускает службу, реализующую протокол VRRP
cAdvisor	Устанавливает сервис **cAdvisor**, осуществляющий сбор метрик работы контейнеров
node_exporter	Устанавливает сервис **node_exporter**, осуществляющий сбор метрик работы сервера
node_cert_exporter	Мониторинг срока действия сертификатов
node_filestat_exporter	Мониторинг появления дампов памяти
blackbox_exporter	Мониторинг доступности веб-интерфейса
syslog_ng	Устанавливает сервис централизованного сбора журналов работы системы
logrotate	Настраивает ротацию хранимых журналов работы системы
ca	Устанавливает и настраивает сервис внутреннего центра сертификации
alertmanager	Устанавливает и настраивает сервис оповещений о событиях мониторинга
devkalion	Устанавливает и настраивает сервис автообнаружения сервисов инсталляции для мониторинга
gesiona	Устанавливает и настраивает сервис, экспортирующий список сервисов инсталляции для сервиса мониторинга
prometheus	Устанавливает и настраивает сервис мониторинга
grafana	Устанавливает и настраивает сервис отображения данных мониторинга инсталляции
kunkka	Устанавливает и настраивает сервис отображения данных о запущенных контейнерах на каждом сервере и их конфигурационных файлов
plugin_certificate	Роль, выписывающая сертификат для сборки клиентских приложений **outlook plugin**
etcd	Устанавливает базу данных **etcd**
hydra	Устанавливает и настраивает сервис обнаружения и балансировки нагрузки gRPC
nats	Устанавливает и настраивает **NATS**
nats_exporter	Сбор метрик мониторинга с **NATS**
mongodb	Устанавливает и настраивает документоориентированную СУБД

Наименование роли	Описание
mongodb.mailion_migration	Устанавливает миграции данных сервисов в базах **MongoDB**
mongodb_exporter	Сбор метрик мониторинга с **MongoDB**
dorofej	Роль работы с модулем **Ansible**, реализующим первичную миграцию СУБД
redis	Устанавливает и настраивает кластер хранилищ **Redis**
theseus	Устанавливает и настраивает сервис работы с учетными данными
perseus	Устанавливает и настраивает сервис хранения контактов
erakles	Устанавливает и настраивает сервис работы с сущностями
odusseus	Устанавливает и настраивает сервис работы с регионами
talaos	Устанавливает и настраивает сервис работы с тенантами
daidal	Устанавливает и настраивает сервис работы с доменами
minos	Устанавливает и настраивает сервис работы с сессиями
ektor	Устанавливает и настраивает сервис работы со связями, сущностями
pasifae	Устанавливает и настраивает сервис подсказок при поиске
dispersed_object_store	Устанавливает и настраивает объектное хранилище, предоставляющее gRPC-интерфейс для хранения бинарных данных и метаданных
achill	Устанавливает и настраивает сервис работы с аватарками
jod	Устанавливает и настраивает сервис для конвертации документов
pregen	Устанавливает и настраивает сервис для конвертации документов
cvm	Устанавливает и настраивает сервис для конвертации документов
cu	Устанавливает и настраивает сервис для конвертации документов
sdd	Устанавливает и настраивает сервис для конвертации документов
meepo	Устанавливает и настраивает сервис генерации превью
mailbek	Устанавливает и настраивает сервис проксирования запросов к шардированным данным на экземплярах поисковой системы
dirbek	Сервис поиска по каталогу
helpbek	Устанавливает и настраивает поисковый сервис по имеющейся веб-документации инсталляции
tripoli	Устанавливает и настраивает единый индексно-поисковый сервис
rspamd	Устанавливает и настраивает сервис антиспама

Наименование роли	Описание
zeus	Устанавливает и настраивает сервис, отвечающий за шаблонизацию и настройку работы с письмами
paranoid	Устанавливает и настраивает сервис, реализующий протоколы **Postfix Policy Delegation** и **Nginx HTTP Auth**
woof	Устанавливает и настраивает сервис, реализующий метод search протокола LDAP для резолвинга групповых адресов, алиасов, получения списка доменов со стороны **postfix**
ariadne	Сервис аутентификации для MTA
lmtp	Устанавливает и настраивает сервис, реализующий протокол **lmtp**
postfix	Устанавливает роль для развертывания почтового сервера (**MTA**)
nginx	Устанавливает и настраивает сервер nginx в режиме **smtp**
kongur	Устанавливает и настраивает сервис, отвечающий за работу календарных событий
mars	Сервис для взаимодействия со ПО Squadus (создание и редактирование чатов и конференций)
kex	Устанавливает и настраивает сервис проксирования запросов к внешним календарям
thoth	Устанавливает и настраивает сервис сохранения полей
ares	Устанавливает и настраивает сервис для взаимодействия с системами видеоконференций
othrys	Устанавливает и настраивает взаимодействия с внешними календарными серверами
elysion	Устанавливает и настраивает сервис выполнения асинхронных работ в календаре
mosquito	Устанавливает и настраивает сервис, предоставляющий абстракцию pub/sub над **AMQP**
viper	Устанавливает и настраивает сервис для сохранения писем в системе
razor	Устанавливает и настраивает сервис для отправки писем по шаблону с локализацией
weaver	Устанавливает и настраивает сервис для построения всего сообщения (его web-представления) или его части (для **IMAP**)
marker	Устанавливает и настраивает сервис для управления тегами
hog	Устанавливает и настраивает сервис для получения и сохранения настроек пользователей

Наименование роли	Описание
beef	Устанавливает и настраивает сервис для сохранения и получения метаданных писем
mixer	Устанавливает и настраивает сервис для получения объектов веб-интерфейсом
atlas	Устанавливает и настраивает сервис для отправки почтовых сообщений
kronos	Устанавливает и настраивает сервис, предназначенный для регистрации задач на отложенное исполнение операций
clotho	Устанавливает и настраивает сервис для хранения истории изменений объектов и тегов
orpheus	Устанавливает и настраивает сервис проксирования аутентификации и поиска сущностей
iason	Устанавливает и настраивает сервис контроля за регистрацией внешних пользователей
cleanup	Производит полное удаление выбранных компонентов (при необходимости)
imap	Устанавливает и настраивает сервис, реализующий протокол **IMAP**
cox	Устанавливает и настраивает **proxy grpc** сервис
house	Устанавливает и настраивает веб-сервер
ararat	Устанавливает и настраивает сервис для работы десктопных и мобильных клиентов с календарем по протоколу CalDAV/CardDAV
leda	Устанавливает и настраивает ldap прокси сервер
sophokles	Устанавливает и настраивает сервис авторизации
dafnis	Устанавливает и настраивает сервис квот
iolaos	Устанавливает и настраивает сервис создания динамических групп
homeros	Устанавливает и настраивает сервис аудита действий пользователя
adonis	Устанавливает и настраивает сервис для административных функций ministerium
etcd.etcd_backup	Настройка автоматического резервного копирования для **etcd**
mongodb.mongodb_backup	Настройка автоматического резервного копирования для **MongoDB**
sreindexer	Настройка инструмента для переиндексации поиска
nats.nats_backup	Настройка автоматического резервного копирования **NATS**
themis	Устанавливает и настраивает сервис для генерации ссылок или занятость пользователей

2.2.2 Подготовка инфраструктуры установки

Для подготовки инфраструктуры установки должны быть проведены следующие действия (последовательность не важна):

– Установка хранилища образов **Docker** (**docker_registry**) на машине **ucs_infrastructure**, см. раздел 2.2.2.1.
– Установка подсистемы управления конфигурациями (**Ansible**) на машине оператора, см. раздел 2.2.2.2.

2.2.2.1 Установка хранилища образов Docker (docker_registry)

Установка производится на сервере с ролью **ucs_infrastructure**. Перед началом установки проверить, что вход выполнен под пользователем **root**.

Для установки необходимо:

1. Скопировать файл `mailion_infra_1.9.run` в домашний директорий пользователя.
2. Запустить скрипт установки:

```
bash mailion_infra_1.9.run
```

3. Дождаться проверки целостности файла и его распаковки.

```
Verifying archive integrity...100% MD5 checksums are OK. All good.
Uncompressing Co Infrastructure Node Package [RELEASE]100%
```

4. Согласиться на продолжение установки, нажать «Y».

```
Do you want to continue? [y/N] y
```

5. Указать тип контейнерной виртуализации (**docker** или **podman**, см. варианты установки в разделе 2.3).

```
choose container_management_tool ('docker' or 'podman')*:
```

6. Во время установки на экране пользователя будет отображен список выполненяемых операций и их статус:

```
.................................................          ........
Check if container with registry is available              [  OK  ]
Ensure that registry configuration directory exists        [CHANGE]
Ensure that docker-registry env file exists                [CHANGE]
Check if old registry data directory exists                [  OK  ]
Ensure that registry data directory exists                 [CHANGE]
```

```
Ensure that container with registry is available              [CHANGE]
Ensure that docker-registry is running                        [  OK  ]
Extracting registry archive...                                [  OK  ]
Remove dangling and outdated images                           [  OK  ]
.....................................................         ........
```

Необходимо убедиться, что элементы списка содержат статус **[OK]** или **[CHANGE]**, это свидетельствует об успешной установке компонента.

При получении статуса **[FAIL]** для любого из компонентов необходимо обратиться в техническую поддержку.

Установка хранилища образов **Docker** (**docker_registry**) будет считаться успешно завершенной в случае успешной установки всех компонент.

2.2.2.2 Установка конфигурационных файлов Ansible для развертывания ПО «Mailion»

Установка производится на рабочем месте оператора. Перед началом установки необходимо проверить следующие условия:

- вход выполнен под пользователем **root** или под пользователем **sudo** с привилегиями **yum** (**dnf**);
- машина, на которой выполняется установка, соответствует требованиям, приведенным в разделе 1.4;
- с выбранного сервера есть возможность доступа по SSH к другим серверам, на которых выполняется установка;
- система управления конфигурациями **Ansible** установлена, другие конфигурационные файлы **Ansible** не присутствуют в системе;
- необходимые модули установлены в системе, их версии соответствуют требованиям.

В а ж н о – В подсистеме управления конфигурациями не должно быть предыдущих конфигурационных файлов самой подсистемы. В том числе конфигурационного файла, который по умолчанию устанавливается с пакетом (например, `/etc/ansible/ansible.cfg`). Такой файл требуется удалить либо перезаписать образцом из поставляемого ПО. Подробнее см. в разделе https://docs.ansible.com/ansible/latest/reference_appendices/config.html#the-configuration-file.

Перед установкой важно самостоятельно установить необходимые модули python из раздела 1.4.1.2, так как они не являются частью поставки системы.

Для установки необходимо:

1. Скопировать файл `mailion_ansible_bin_1.9.run` в домашнюю директорию пользователя.
2. Запустить скрипт установки:

```
bash mailion_ansible_bin_1.9.run
```

3. Согласиться на продолжение установки, нажать на клавишу «**Y**».

```
Do you want to continue?  [y/N] y
```

4. Во время установки на экране пользователя будет отображен список выполняемых операций и их статус:

```
.............................                                    ........
Create playbooks symlink                                         [  OK  ]
Create group_vars directory                                      [  OK  ]
Create group_vars/all symlink                                    [  OK  ]
Create host_vars directory                                       [  OK  ]
Create certificates directory                                    [  OK  ]
Create certificates symlink                                      [  OK  ]
.............................                                    ........
```

Необходимо убедиться, что элементы списка содержат статус **[OK]** – это свидетельствует об успешной установке компонента.

При получении сообщения **[FAIL]** для любого из компонентов необходимо обратиться в техническую поддержку.

Установка конфигурационных файлов **Ansible** будет считаться успешно завершенной в случае успешной установки всех компонент.

2.2.2.3 Установка ПО «Mailion» с машины оператора

К началу данного этапа директория инсталляции `~/install_mailion/` должна выглядеть следующим образом (см. Рисунок 3):

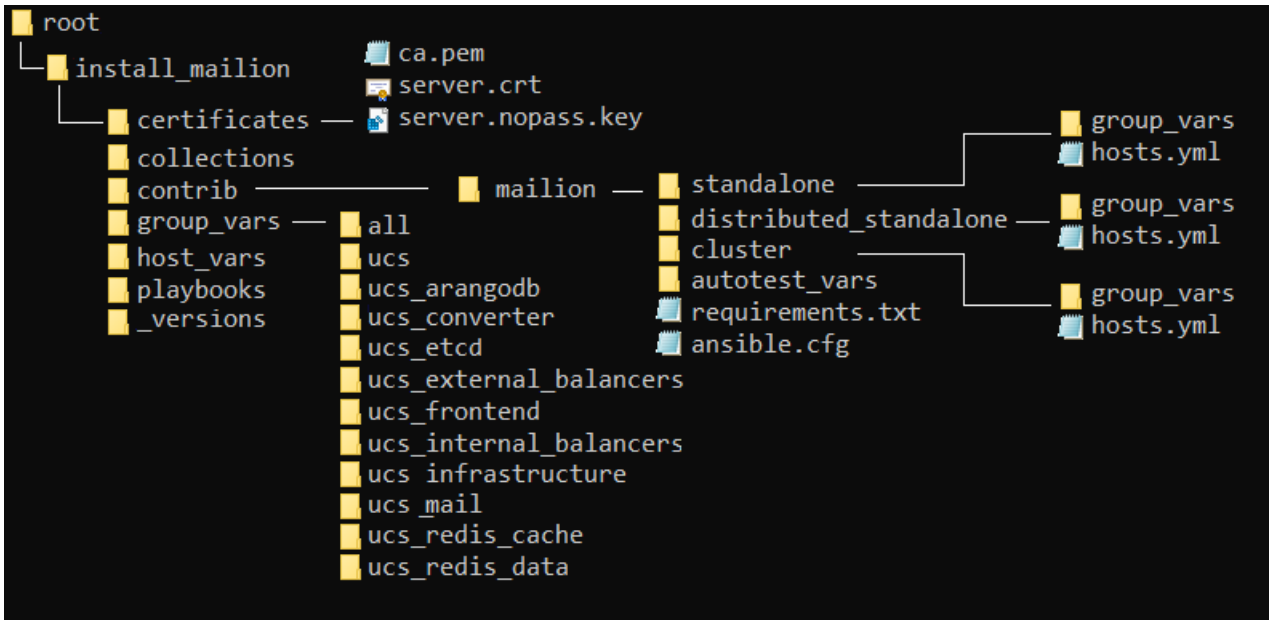


Рисунок 3 – Структура папок перед началом инсталляции

В инсталляторе представлены предзаполненные файлы конфигураций (установка описана в разделе 2.2.2.2), которые помогут в настройке необходимого функционала будущей системы. В директории `~/contrib/mailion/` находятся три директории, соответствующие возможным конфигурациям установки:

- `~/contrib/mailion/cluster` (кластерная конфигурация);
- `~/contrib/mailion/standalone` («Standalone»);
- `~/contrib/mailion/distributed_standalone` (распределенная конфигурация «Standalone»).

Так как целевое назначение системы – крупная отказоустойчивая инсталляция, в данном документе будет описана **кластерная конфигурация установки**.

При установке конфигурации «**Standalone**» необходимо воспроизвести аналогичные этапы установки, описанные в данном разделе. Отличие будет заключаться в названии папки, в которой находится конфигурационный файл для данной конфигурации.

Перед установкой необходимо перейти в каталог `~/install_mailion/` с помощью команды:

```
cd ~/install_mailion
```

П р и м е ч а н и е – Данный каталог будет являться корневой точкой установки

2.2.2.3.1 Копирование файла ansible.cfg

Необходимо скопировать конфигурационный файл ansible из папки `~/contrib/mailion/ansible.cfg` в корневой раздел директории установки с помощью команды:

```
cp contrib/mailion/ansible.cfg .
```

2.2.2.3.2 Конфигурирование файла hosts.yml

Для подготовки файла **inventory** (`~/hosts.yml`) необходимо произвести следующие действия:

1. Предварительно скопировать его из директории с заполненными шаблонами `~/contrib/mailion/<config>`, где `<config>` – конфигурация установки. Для конфигурации **cluster** следует воспользоваться следующей командой:

```
cp contrib/mailion/cluster/hosts.yml .
```

   В а ж н о – Для конфигурации «**Standalone**» необходимо использовать `hosts.yml` из директории `contrib/mailion/standalone`. Для распределенной конфигурации «**Standalone**» необходимо использовать `hosts.yml` из директории `contrib/mailion/distributed_standalone`.

2. Открыть файл `hosts.yml` в редакторе и заменить все текстовые вхождения «**installation.example.net**» на доменное имя инсталляции (имя должно быть в нижнем регистре). Важно не менять данные имена до «**.installation.example.net**», можно изменять только количество нод.

В а ж н о – В файл `hosts.yml` вносятся только полностью определенные имена доменов (FQDN). Эти имена будут использоваться во время и после установки системы для обращения к внутренним сервисам. Часть логики установщика использует их для формирования доменных имен и адресов сервисов.

3. Если на машине оператора планируется использовать несколько инсталляций Mailion, то необходимо заменить в файле `hosts.yml` имя группы **ucs_setup** (из ## SECTION 2) на имя текущей инсталяции (префикс **ucs_** следует оставить в имени, например: **ucs_mailion**). Аналогичным образом нужно поменять значение переменной **tier** (см. Рисунок 4).

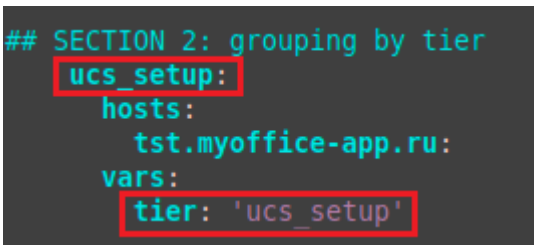


Рисунок 4 – Настройка **ucs_setup**

2.2.2.3.3 Копирование папки групповых переменных

Для подготовки директории `~/group_vars` необходимо произвести следующие действия:

1. Создать в папке групповых переменных (`~/group_vars`) каталог для серверов с именем `<install_name>` группы инсталляции из файла `hosts.yml`. Имя данной папки обязательно должно совпадать с именем инсталляции из секции ## SECTION 2 (по умолчанию – **ucs_setup**, либо измененное имя).

```
cd group_vars
mkdir <install_name>
```

2. Для **кластерной** установки скопировать в папку групповых переменных (`~/group_vars`) каталог с переменными для заполнения:

```
cp -r contrib/mailion/cluster/group_vars/ucs_setup/*
group_vars/<install_name>
```

Для установки **standalone** необходимо скопировать конфигурационный файл из папки `contrib/mailion/standalone`.

```
        cp -r contrib/mailion/standalone/group_vars/ucs_setup/*
group_vars/<install_name>
```

2.2.2.3.4 Конфигурирование файла main.yml

Открыть файл `main.yml` из каталога `group_vars/<install_name>` (см. раздел 2.2.2.3.2) и отредактировать значение параметров, которые находятся в комментариях. Набор параметров для минимальной настройки можно найти в разделе 2.2.5.1.

В случае если данная инсталяция Mailion будет использоваться для восстановления из резервной копии предыдущей инсталяции, то необходимо задать ID региона данной инсталяции в переменной `dorofej_region_id`.

При необходимости хранения паролей в зашифрованном виде следует зашифровать содержимое файла `main.yml` с помощью команды:

```
    ansible-vault encrypt group_vars/ucs_setup/main.yml --ask-vault-pass
```

Затем ввести пароль для шифрования. Для удобства можно использовать файл с парольной фразой. Для этого необходимо создать текстовый файл с паролем. В таком случае команда будет следующей:

```
    ansible-vault encrypt group_vars/ucs_setup/main.yml --vault-password-
file=.filesecret
```

Чтобы отменить шифрование файла необходимо в команде опцию **encrypt** изменить на **decrypt**. Чтобы отредактировать зашифрованный файл, следует выполнить команду:

```
    ansible-vault edit group_vars/ucs_setup/main.yml --vault-password-
file=.filesecret* (или --ask-vault-pass)
```

2.2.2.3.5 Конфигурирование файла ministerium.yml

Открыть файл `ministerium.yml` из каталога размещения и отредактировать значение параметров, которые находятся в комментариях. Примеры заполнения параметров можно найти в разделе 2.2.5.1. Подробная инструкция присутствует в разделе 7.

2.2.3 Установка и обновление пакетов Python

Требуется наличие программного обеспечения, описанное в разделе 1.4.1.2, для чего необходимо на машине оператора установить или обновить следующие пакеты:

– Установка или обновление каталога пакетов python:

```
python3 -m pip install --upgrade pip==20.3.4
```

– Установка модуля ansible-core (версия может отличаться):

```
pip3 install --no-cache-dir hvac ansible-core==2.11.9
```

– Установка необходимых зависимостей:

```
pip3 install --no-cache-dir -r
~/install_mailion/contrib/mailion/requirements.txt
```

2.2.4 Размещение SSL-сертификатов для шифрования

Имена сертификатов могут быть произвольными, но они потребуются для дальнейшего заполнения параметров групповых переменных, поэтому важно их запомнить. В файле групповых переменных `extra_vars.yml`, создание которого было описано в разделе 2.2.2.3.3, заполнены имена сертификатов по умолчанию. Если назвать файлы сертификатов соответствующим образом, то менять имена в переменных не нужно.

Состав необходимых сертификатов:

1. Сертификат внешнего домена `server.crt`.
2. Ключ внешнего домена `server.nopass.key`.
3. Цепочка сертификатов промежуточных центров сертификации (CA) внешнего домена `ca.pem`.

Формат файла: в конце файла не должно быть пустой строки.

```
cat certificates/server.crt

-----BEGIN CERTIFICATE-----
...
-----END CERTIFICATE-----
```

Необходимо скопировать файлы сертификатов (`ca.pem`, `server.crt`, `server.nopass.key`) в папку:

```
~/install_mailion/certificates/
```

Имена ключей групповых переменных находятся в переменных **mailion_external_cert_filename**, **mailion_external_key_filename**, **mailion_external_ca_filename**:

```
mailion_external_cert_filename: "server.crt"
mailion_external_key_filename: "server.nopass.key"
mailion_external_ca_filename: "ca.pem"
```

В а ж н о – При установке ПО «Mailion» есть возможность использования сертификатов центра Let's Encrypt на усмотрение администратора установки. Разработчик ПО «Mailion» не несет ответственности за получение, обновление и управление сертификатами Let's Encrypt.

В а ж н о – В случае использования самоподписанного сертификата в конфигурационный файл необходимо добавить флаг: **mailion_use_self_signed_external_certificate: true**.

2.2.5 Настройка основных параметров установки

2.2.5.1 Минимальные параметры установки

Минимальные параметры, обязательные для заполнения:

- ansible_user;
- codec_secret_key;
- dispersed_object_store_management_token;
- grafana_admin_password;
- house_ldapauth_password_salt;
- hydra_get_service_list_token;
- jwt_key;
- keepalived_vrrp_instances;

- mailion_cluster, mailion_domain_module, mailion_external_domain, mailion_installation_admin_password, mailion_integrations, mailion_internal_web_auth, mailion_max_users, mailion_service_accounts, mailion_supported_domains, mailion_tenants;
- mongodb_root_password, mongodb_secured_key, mongodb_management_users;
- nats_authorization_password, nats_cluster_authorization_password;
- redis_cluster_replicas, redis_dafnis_password, redis_dowal_password, redis_ektor_password, redis_erakles_password, redis_euripides_password, redis_hog_password, redis_homeros_password, redis_leda_password, redis_minos_password, redis_rspamd_password, redis_sdd_password, redis_viper_password;
- rspamd_kse_endpoints, rspamd_dkim_hosts, rspamd_web_password;
- servus;
- sophokles_access_token;
- theseus_cipher_key;
- tls_certs_remote_token_key;
- unbound_forward_addresses.

Структура и способы заполнения указанных параметров приведены в разделах ниже.

2.2.5.1.1 Настройка параметров установки ansible_user

Настройка параметров приведена в таблице 24.

Таблица 24 – Настройка параметров ansible_user

Параметр	Тип данных	Описание
ansible_user:	Str	Имя пользователя, под которым установщику будут доступны серверы инсталляции по **ssh**

Пример корректно настроенного параметра:

```
ansible_user: "root"
```

2.2.5.1.2 Настройка параметров codec_secret_key

Настройка параметров приведена в таблице 25.

Таблица 25 – Настройка параметров codec_secret_key

Параметр	Тип	Описание
codec_secret_key:		Словарь параметров секретов для формирования шифрованной ссылки
rcr:	Str	Используется для формирования ссылки на проксирование данных внутри системы
secret_link:	Str	Используется для формирования ссылки на проксируемые ресурсы
values_codec	Str	Значение

Пример корректно настроенного параметра:

```
codec_secret_key:
  rcr: "O1Wk7ha80M1qfvq8UtuZg918AZyh+q65s68dKvXwVTQ="
  secret_link: "69rUgWgrLbV50CiAEK78AJIrLoWBGHGwYCX25phh3yg="
  values_codec: "ggxhfxrjshb034fosedfwd3d"
```

2.2.5.1.3 Настройка параметров dispersed_object_store

Настройка параметров приведена в таблице 26.

Таблица 26 – Настройка параметров dispersed_object_store

Параметр	Тип	Описание
dispersed_object_store_management_token: ""	Str	Токен доступа для управления через API сервиса

Пример корректно настроенного параметра:

```
dispersed_object_store_management_token: "Aig2utoavi6iageiltas"
```

2.2.5.1.4 Настройка параметра Docker

Настройка параметров приведена в таблице 27.

Таблица 27 – Настройка параметров Docker

Параметр	Тип	Описание
docker_daemon_parameters:		Параметры демона **docker**
bip:	Str	Подсеть и маска для **docker**
dns:	List	Список строк с адресами DNS-серверов
mtu:	Int	Значение **MTU** для сетевого интерфейса **docker**

Пример корректно настроенного параметра:

```
docker_daemon_parameters:
  bip: "172.17.0.1/16"
  dns:
      - "8.8.8.8"
      - "1.1.1.1"
  mtu: 1412
```

2.2.5.1.5 Настройка параметров grafana

Настройка параметров приведена в таблице 28.

Таблица 28 – Настройка параметров grafana

Параметр	Тип	Описание
grafana_admin_password:	Str	Пароль администратора grafana

Пример корректно настроенного параметра:

```
grafana_admin_password: "Ooj0Inahgh2Ixailoxie"
```

2.2.5.1.6 Настройка house

Настройка параметров приведена в таблице 29.

Таблица 29 – Настройка параметров house

Параметр	Тип	Описание
house_ldapauth_password_salt:	Str	Соль для хеширования паролей при LDAP-авторизации

Пример корректно настроенного параметра:

```
house_ldapauth_password_salt: ")6_]*|,)(bJ;PN"
```

2.2.5.1.7 Настройка hydra

Настройка параметров приведена в таблице 30.

Таблица 30 – Настройка параметров hydra

Параметр	Тип	Описание
hydra_get_service_list_token:	Str	Токен для обращения в API сервиса

Пример корректно настроенного параметра:

```
hydra_get_service_list_token: "maiquauzuwooQu9ooR7x"
```

2.2.5.1.8 Настройка параметров jwt_key

Настройка параметров приведена в таблице 31.

Таблица 31 – Настройка параметров jwt_key

Параметр	Тип	Описание
jwt_key:		Параметры **jwt_key**
priv:	Str	Закрытый ключ
pub:	Str	Публичный ключ

Пример корректно настроенного параметра:

```
jwt_key:
  priv: |
    -----BEGIN RSA PRIVATE KEY-----
    MIIEowIBAAKCAQEA063xN82YOtJBq8sfd79bJ+4W9QEdOueQljPziN4JdYntS381
```

```
    AqxOA4Ud886S4LdwCN2KSpuh7QSHkzjzH9AlDrHCYShOfPAeHLMCBDszazr2IOc0
    Jaw3bHRfrM9Ilb+X4qdDE88Mfk+B/8Sa/xG2HJVy0Jjb4XoipwzEB900a+6zpnLT
    ..............
    q/kNt7YtrTBmrgpSzFMr0VD+x0Ftb9zhiFVLyVscVKEl67+TNlWahgzh14YF8xP8
    gb89coH114YUNfxN8lKURdY9QFNuZLF+x8xfL4CWwydSbtL7dFFK0HVowMt4tnoJ
    okthJ5JZNw+XZAXHS3NyuvbYmP+iqRuL2YAr2wIDAQABAoIBAGyNHs5HGHHRsOuw
    Uq3/k9aD8NKVjJnJ7/kQEnLlBjcHcpazMHQJnvpfRaqfBre0G1ok9sPH/rvTgK1U
    clKH2eSXgRhKgLf3Dtf6m2bULj0HN0FIydngh0F1EqK10vnvqfkN
    -----END RSA PRIVATE KEY-----
  pub: |
    -----BEGIN PUBLIC KEY-----
    MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA063xN82YOtJBq8sfd79b
    J+4W9QEdOueQljPziN4JdYntS381AqxOA4Ud886S4LdwCN2KSpuh7QSHkzjzH9Al
    DrHCYShOfPAeHLMCBDszazr2IOc0Jaw3bHRfrM9Ilb+X4qdDE88Mfk+B/8Sa/xG2
    HJVy0Jjb4XoipwzEB900a+6zpnLTq/kNt7YtrTBmrgpSzFMr0VD+x0Ftb9zhiFVL
    yVscVKEl67+TNlWahgzh14YF8xP8gb89coH114YUNfxN8lKURdY9QFNuZLF+x8xf
    L4CWwydSbtL7dFFK0HVowMt4tnoJokthJ5JZNw+XZAXHS3NyuvbYmP+iqRuL2YAr
    2wIDAQAB
    -----END PUBLIC KEY-----
```

2.2.5.1.9 Настройка параметров keepalived

Настройка параметров приведена в таблице 32.

Таблица 32 – Настройка параметров keepalived

Параметр	Тип	Описание
keepalived_vrrp_instances		Параметры **keepalived**
ucs_frontend:		Параметры **ucs_frontend**
password:	Str	Пароль
virtual_ip	Str	Виртуальный IP для группы хостов **ucs_frontend**
ucs_mail:		Параметры **ucs_mail**
password:	Str	Пароль
virtual_ip	Str	Виртуальный IP для группы хостов **ucs_mail**

Пример корректно настроенного параметра:

```
keepalived_vrrp_instances:
  ucs_frontend:
    password: "UgohSh8i"
    virtual_ip: "192.168.10.10"
    ucs_mail:
```

```
    password: "keeB5ooH"
    virtual_ip: "192.168.10.10"
```

2.2.5.1.10 Настройка параметров mailion

Настройка параметров приведена в таблице 33.

Таблица 33 – Настройка параметров mailion

Параметр	Тип	Описание
mailion_cluster:	Bool	Флаг кластерной или «Standalone» инсталляции
mailion_domain_module	Special	Переменная для генерации эндпоинтов инсталляции (убедиться, что в значении используются разделители «-», а не «.»)
mailion_external_domain:	Str	Внешний домен инсталляции
mailion_installation_admin_password	Str	Пароль для администратора всей инсталляции (!)
mailion_integrations	Dict	Словарь, содержащий настройки интеграций
mailion_integrations.microsoft	Bool	Включение и отключение интеграции с решениями Microsoft
mailion_integrations.freeipa	Bool	Включение и отключение интеграции с FreeIpa
mailion_integrations.psn	Bool	Включение и отключение интеграции с PSN
mailion_integrations.google_oauth	Bool	Включение и отключение интеграции с Google OAuth
mailion_internal_web_auth	Dict	Словарь, содержащий настройки внутренней веб-аутентификации
mailion_internal_web_auth.enabled	Bool	Включение и отключение аутентификации для доступа к веб-интерфейсам инфраструктурных сервисов (мониторинг, grafana и т.д.)
mailion_internal_web_auth.password	Str	Пароль для аутентификации для доступа к веб-интерфейсам инфраструктурных сервисов
mailion_max_users:	Int	Максимальное количество пользователей в инсталляции
mailion_service_accounts	Dict	Словарь, содержащий пароли сервисов (values) и имена сервисов (keys)

Параметр	Тип	Описание
mailion_supported_domains	List	Список доменов, которые инсталляция будет поддерживать

Пример корректно настроенного параметра:

```
mailion_cluster: true
mailion_domain_module: "{service}.{domain}"
mailion_external_domain: "installation.example.net"
mailion_installation_admin_password: "oor3Iekichocaiphahr5"
mailion_integrations:
  aldpro: false
  freeipa: false
  google_oauth: false
  microsoft: false
  psn: false
  samba_dc: false
mailion_internal_web_auth:
  enabled: true
  password: "rfkg7shtasjfha6vnd"
mailion_max_users: 100
mailion_service_accounts:
  ararat: "Jo8be1pheicahmieV2oa"
  ares: "72gyV456uh9ARiYs8jBx"
  ariadne: "Um6heiNie2doeshee2sa"
  atlas: "Gaezohg1Ad3naf5ahpef"
  clotho: "Hyrq5iedwemdLNrV47KT"
  cox: "Ii0eeceen5ti1Oe6xaeb"
  dflink_plugin: "Gaezohg1Ad312345hpef"
  elysion: "le0eelePhooghougoopo"
  erakles: "Ui6ohDahLeitozughugh"
  hog: "shee8einoh4AivigePei"
  homeros: "ooph8Efu1eesu2quah1u"
  house: "ahb9Hai3Quaid4aed7an"
  imap: "feo6aita3El6aiMaeboh"
  kongur: "aa6eizooguPhene9uifu"
  kronos: "iphuTh0eiY2ook4aeph5"
  leda: "72YjiCQrnwUwCR32sVrL"
  lmtp: "aicae3yo7Aukaejeel2e"
  marker: "eer1edaeceeJu6naiPom"
  minos: "eshegh3iaR0fie0G"
```

```
  othrys: "eeth8Avohv8OpheeHieg"
  paranoid: "Yoa4eNgahm0aeChu8uWe"
  perseus: "Oogh9ahroow2eicaeng7"
  razor: "Ohquietikenu2Aeloh6E"
  theseus: "eileixietai0cahQu3ma"
  viper: "Feir8uewie4Ieshu4thi"
  woof: "at6Ohdapohaitahtho2j"
  zeus: "fa4Ohxaithee0yaeleit"
mailion_supported_domains: []
```

2.2.5.1.11 Настройка параметров MongoDB

Настройка параметров приведена в таблице 34.

Таблица 34 – Настройка параметров MongoDB

Параметр	Тип	Описание
mongodb_root_password:	Str	Пароль пользователя root для СУБД
mongodb_secured_key:	Str	Ключ для доступа к СУБД
mongodb_management_users:		Словарь. Каждый ключ словаря – пользователь
marker:		Ключ, имя пользователя
database:	Str	База для аутентификации (опционально)
password:	Str	Пароль для аутентификации
roles:		Список ролей (опционально)
- role:	Str	Роль пользователя
db	Str	Имя базы данных, для которой пользователю присваивается роль

Пример корректно настроенного параметра:

```
## MongoDB secrets
## Generate the password with `pwgen 16 1`
mongodb_root_password: "ohre4Rohngahshah"
## Generate the password with `pwgen 16 1`
mongodb_secured_key: "uGhie5ieweixae9C"
mongodb_management_users:
  achill:
```

```
  password: "cohh0Av2mai2aJae"
beef:
  password: "idohjie2Ikeice0I"
clotho:
  password: "wahcoovei0bahRu4"
daidal:
  password: "cheYichoongoh4gi"
erakles:
  password: "Uxeu4ieph1uix1ah"
hog:
  password: "rae0faeng1Seupee"
homeros:
  password: "xoopunaihuopae4J"
marker:
  password: "ohvufoosaeTeeCo3"
mongodb_exporter:
  password: "woo2Yual2saeboh1"
kongur:
  password: "ahmeayooH1yahlohreem"
kronos:
  password: "peiNguxud8ooThaiCahL"
odusseus:
  password: "oY9ja7ietheec6sahthe"
perseus:
  password: "xuoboop5Geneemei"
sophokles:
  password: "baexuli5oow8ohTh"
talaos:
  password: "Ahroozait4pesupohpho"
themis:
  password: "feef8euch8gaiwieRoig"
theseus:
  password: "ua8mu0uoj6uvieDu2gei
"thoth:
  password: "BooRah6oal9Naehai2ph"
```

2.2.5.1.12 Настройка параметров NATS

Настройка параметров приведена в таблице 35.

Таблица 35 – Настройка параметров NATS

Параметр	Тип	Описание
nats_authorization_password:	Str	Пароль для авторизации в **NATS**
nats_cluster_authorization_password:	Str	Пароль для **NATS cluster auth**

Пример корректно настроенных параметров:

```
nats_authorization_password: "Fiohoogh7Raobi4yeiSi"
nats_cluster_authorization_password: "ao1Iey7luRoh1ahf9eVe"
```

2.2.5.1.13 Настройка дополнительных параметров postfix

Настройка дополнительных параметров приведена в таблице 36.

Таблица 36 – Настройка дополнительных параметров postfix

Параметр	Тип	Описание
postfix_additional_mynetworks:	List	Список дополнительных сетей, из которых разрешена отправка через MTA инсталляции

Примечание – Если используется Exchange, то нужно добавить адреса в исключение для `postfix_additional_mynetworks` адресов Exchange.

Пример корректно настроенного параметра:

```
## POSTFIX configuration
### (optional) list of networks allowed to use this SMTP relay
# postfix_additional_mynetworks:
#  - "192.168.113.0/24"
```

2.2.5.1.14 Настройка параметров redis

Настройка параметров приведена в таблице 37.

Таблица 37 – Настройка параметров redis

Параметр	Тип	Описание
redis_cluster_replicas	Int	redis_cluster_replicas аналогичен параметру replicas redis-cli. См. официальную документацию https://redis.io/docs/manual/replication/. Для HA redis с slave, требуется минимум 6 машин с redis_cluster_replicas 1 и 9 машин с redis_cluster_replicas 2.
redis_dafnis_password	Str	Пароль для **redis_dafnis**
redis_dowal_password	Str	Пароль для **redis_dowal**
redis_ektor_password	Str	Пароль для **redis_ektor**
redis_erakles_password	Str	Пароль для **redis_erakles**
redis_euripides_password	Str	Пароль для **redis_euripides**
redis_hog_password	Str	Пароль для **redis_hog**
redis_homeros_password	Str	Пароль для **redis_homeros**
redis_leda_password	Str	Пароль для **redis_leda**
redis_minos_password	Str	Пароль для **redis_minos**
redis_rspamd_password	Str	Пароль для **redis_rspamd**
redis_sdd_password	Str	Пароль для **redis_sdd**
redis_viper_password	Str	Пароль для **redis_viper**

Пример корректно настроенных параметров:

```
redis_dafnis_password: "eexaiSheQuoivu1oo4ak"
redis_dowal_password: "oasu7nieNg0aeshaiphi"
redis_ektor_password: "eisach9eet8thaug9Ieg"
redis_erakles_password: "zae9iaL3ooth3ahphugh"
redis_euripides_password: "xi6Ohy8io5ku7veQuau7"
redis_hog_password: "dighaeX0hoov6aeJee3u"
redis_homeros_password: "chae7quah7Li2zohbe8o"
redis_leda_password: "Aiy6iiyeiZo2caaleofe"
redis_minos_password: "quie2jiG2CeucooShahG"
redis_rspamd_password: "Iughoo2iuS2Xew1die4p"
```

```
redis_sdd_password: "fohphow6eat1aekod5Oh"
redis_viper_password: "Tee9han6ienaYoSievoo"
```

2.2.5.1.15 Настройка параметров resolv

Настройка параметров приведена в таблице 38.

Таблица 38 – Настройка параметров resolv

Параметр	Тип	Описание
resolv_nameservers:	List	Список строк с адресами DNS-серверов для настройки файла **resolv.conf**

Пример корректно настроенного параметра:

```
resolv_nameservers:
  - "192.168.1.1"
  - "192.168.1.2"
  - "192.168.1.3"
```

2.2.5.1.16 Настройка параметров rspamd

Настройка параметров приведена в таблице 39.

Таблица 39 – Настройка параметров rspamd

Параметр	Тип	Описание
rspamd_dkim_hosts:		Параметры антиспама
		Параметры **dkim_hosts**
<your_external_domain>		Имя внешнего домена, который необходимо подписывать DKIM-ключом
dkim_key:	Str	DKIM-ключ
rspamd_web_password:	Str	Пароль от веб-интерфейса

Пример корректно настроенного параметра:

```
rspamd_dkim_hosts:
    installation.example.net:
      dkim_key: |
        -----BEGIN PRIVATE KEY-----
        MIIEvwIBADANBgkqhkiG9w0BAQEFAASCBKkwggSlAgEAAoIBAQC3euVQm/Djy1z1
        JhbTC5Cs99HmrgN6DldM5xivTyhopgkGlHXIoWaKfvt3wKm/Pzah2/BkcTXtDa3w
        E70bmjVXFX2xkXG5DAuY9ChnX6+xWYCeBUeRsMSnWdyoNBwFK9rjE2vZ+u3OzLhz
        wP6PuIyigV7A3D9Mtok0XA3iH/7G+99ARjxhj8hCkYEqEsR688uU1JNeztTfkte+
```

```
        mz6n7w8AO2jdpdG8wRqjvj4B4H0MaaP7R4y/UopZ+UP0RAbm7KryOjgC15uLou9Y
        Yg9ym0VkcaIOvc0xQT7Zk13yf8vIuVS/6yhO3FcKYB4mx0Szz1RpU2ueyvD2COSj
        C+2uZsPFAgMBAAECggEBAK6+xEH2kwFRAPKWWSydGigySl4KI1OO7wRWIMNuf4zT
        fUsf/+GaHoAPGk7eVozHlq+nOhdfXz2rRpqdIgF06BJNbI2+ePIFj9IXz5dMoZcm
        KAHYA2a1VUYRpr8oCfu+3dRg/dn4S58miRHtoESfPonS7rx9x2e3fYs5lRtk35EA
        Wp5Vy+2U36cKIJLVtAOvzRbGl9SLjPAvuc/WKGda2lA7HBlhep/Yrm0RUoH//5Px
        fJwLVSy34B31Fx1wZk80aVquXCv644GbR89RIQttziHg9q4g/wyZ5/+ZG/967kim
        tKDS8PWhAK5pjUHS9cED/hjs+ITlNCI4qKf2zj2XSqECgYEA3X9zmzAw9JLnelZN
        3oVM/boqtwfPgnO6Y98inDMsecAICWLCAsEsWYY90IB3FQCXJXVrGTxKnHa3S0fR
        MTX5xx3Rta5SWf88jUQCmZEuxHBeIEN9JKebKC97rKIlIJmYJ8PVZ8c6LAvMgmYc
        sd+GyjJAmV+N7j5Eo8tXmZCCuK0CgYEA1A9t7P6GjXQQFrIk81+x+0JHmIN+DPKs
        eyR6avDfd32HIq2dPCMmjCAl7EFbfOPVNx9rZvLrEWtTkgU8DYBPlZ955EJORi9l
        eqYeOKwhWLUMgwHyWlEJZPeY3o31TF1NwNG16Qy98h4zr2SUaTuCdccoNWAc0GuI
        rA1Gjn7AonkCgYEAuMpgFJS8Aw+cdwARrxffB7+Na23kvZz3X+ME6PP4owqGqe3u
        loW7DmVkpNLIhokbkHDJjSAzzx1sBi5AZKH3ZRuHnd91bQf36JNY5+2r6s8keB5W
        BYKfe4NB1uDfwLbjrik/nXklGyIs2I2AWxV1SrNqGYsSyjTA5zX6O2/I33ECgYBS
        eO23jgWmXc0kBoR4Ym9F2LEfj4QmZPrPqZAypxtBzYAQ7JSKHuGO/bHCAGkkWTdD
        COUsVK03SRZnY8HHPm+1MSCmtWLbyPMekByQzeDqLv9+s/MdTQbqTaEWbP9Jg8AJ
        jYXB7UKyNyzCucs+YfaK97mbiJWsOSYeQ8t8/67LgQKBgQCk4q/D5Cq5Fqalbk/0
        jyEQAmHgrhWEJO2bECGjGIJ13/Hj3bbQ3znfPUDf9MLDtrveGu4YdspL3S4yahLO
        EXxXPgwHCDLqamx5vj4QKFPFQEHXv68RK6RKhw7m2IeyI/7nsHPvjZhNZI4ulSTN
        CLCjuiw8tvIafY26wKDylpvnRQ==
        -----END PRIVATE KEY-----

  rspamd_web_password: "iePixieTaf4IriequieX"
```

2.2.5.1.17 Настройка параметров servus

Настройка параметров приведена в таблице 40.

Таблица 40 – Настройка параметров servus

Параметр	Тип	Описание
servus:	Str	Параметры **servus**

Пример корректно настроенного параметра:

```
servus: "Iefae4yoh4rohceepoli"
```

2.2.5.1.18 Настройка параметров sophokles

Настройка параметров приведена в таблице 41.

Таблица 41 – Настройка параметров sophokles

Параметр	Тип	Описание
sophokles_access_token:	Str	Токен для сервиса авторизации **minos** и **sophokles**

Пример корректно настроенного параметра:

```
sophokles_access_token: "IeWoh9eateihuvoxekah":
```

2.2.5.1.19 Настройка параметров theseus

Настройка параметров приведена в таблице 42.

Таблица 42 – Настройка параметров theseus

Параметр	Тип	Описание
theseus_cipher_key:	Str	Ключ шифрования **theseus**

Пример корректно настроенного параметра:

```
theseus_cipher_key: "RWVmb21pZXhvbmFpYzZvaHlhaTR6aURhd2VpZzhlZW4="
```

2.2.5.1.20 Настройка параметров unbound

Настройка параметров приведена в таблице 43.

Таблица 43 – Настройка параметров unbound

Параметр	Тип	Описание
unbound_access_control:	Dict	Параметры доступа к управлению **unbound**
network1	Str	Подсеть, из которой разрешен доступ к кэширующему **DNS**
unbound_enable_autowildcard:	Bool	Флаг использования автоматического формирования DNS-записей внутренних адресов на базе серверов в файле **inventory** и их значений переменной **ansible_default_ipv4**

Параметр	Тип	Описание
unbound_forward_addresses:	List	Список строк внешних DNS-сервисов, на которые будут перенаправляться запросы **unbound** серверов

Пример корректно настроенного параметра:

```
unbound_enable_autowildcard: false
unbound_access_control:
  network1: "192.168.1.0/24"
unbound_forward_addresses:
  - "8.8.8.8"
  - "1.1.1.1"
```

2.2.5.1.21 Настройка параметров CA

Настройка параметров приведена в таблице 44.

Таблица 44 – Настройка параметров CA

Параметр	Тип	Описание
tls_certs_remote_token_key:	Str	Ключ для доступа к API внутреннего **Certificate Authority**

Пример корректно настроенного параметра:

```
tls_certs_remote_token_key: "afba15d0def55ca6e57efb481f8232a5"
```

2.2.5.1.22 Настройка параметров viper

Настройка параметров приведена в таблице 45.

Таблица 45 – Настройка параметров viper

Параметр	Тип	Описание
viper_calendar_settings_sender_white_list:	List	Список отправителей, которые могут присылать календарные письма за участника события (например, сервисные ящики noreply).
regexp:	Str	Выбор отправителей по регулярному выражению
sender_in_reply_to	Bool	Добавить отправителя в **reply_to**

Параметр	Тип	Описание
Переменные для ограничения индексации писем		
viper_rate_limit_mail_indexer_enable	Bool	Если **true**, то механизм ограничения индексации включен
viper_rate_limit_mail_indexer_events_ per_sec	Int	Ограничение на количество запросов в секунду (RPS)
viper_rate_limit_mail_indexer_burst	Int	Размер разрешенного единовременного всплеска событий. Данная переменная нужна для обработки пиковой нагрузки. Значение может быть больше ограничения на количество запросов в секунду (RPS). Практическое применение этого параметра заключается в ограничении количества одновременно обрабатываемых событий
viper_rate_limit_mail_indexer_max_delay_sec	Int	Максимальное время, на которое может блокироваться обработка события при реиндексации. Если это время превышено, попытка индексации будет происходить позже, когда нагрузка станет меньше. Для отключения проверки максимальной задержки следует установить значение 0
Переменные для ограничения индексации вложений писем		
viper_rate_limit_attachment_indexer_enable	Bool	Если **true**, то механизм ограничения индексации включен
viper_rate_limit_attachment_indexer_events_ per_sec	Int	Ограничение на количество запросов в секунду (RPS)
viper_rate_limit_attachment_indexer_burst	Int	Размер разрешенного единовременного всплеска событий. Данная переменная нужна для обработки пиковой нагрузки. Значение может быть больше ограничения на количество запросов в секунду (RPS). Практическое применение этого параметра заключается в ограничении количества одновременно обрабатываемых событий
viper_rate_limit_attachment_indexer_max_ delay_sec	Int	Максимальное время, на которое может блокироваться обработка события при реиндексации. Если это время превышено, попытка индексации будет происходить позже, когда нагрузка станет меньше. Для отключения проверки максимальной задержки следует установить значение 0

Пример корректно настроенного параметра:

```
viper_calendar_settings_sender_white_list:
- regexp: "[^@]+@calendar.example.ru$"
  sender_in_reply_to: true
- regexp: "^calendar@calendar.example.ru$"
  sender_in_reply_to: false

viper_rate_limit_mail_indexer_enable: false
viper_rate_limit_mail_indexer_events_per_sec: 100
viper_rate_limit_mail_indexer_burst: 50
viper_rate_limit_mail_indexer_max_delay_sec: 300
viper_rate_limit_attachment_indexer_enable: false
viper_rate_limit_attachment_indexer_events_per_sec: 100
viper_rate_limit_attachment_indexer_burst: 50
viper_rate_limit_attachment_indexer_max_delay_sec: 300
```

2.2.5.1.23 Настройка параметров ntp

Настройка параметров приведена в таблице 46.

Таблица 46 – Настройка параметров ntp

Параметр	Тип	Описание
ntp_servers:	List	Список **ntp** серверов
ntp_listen_on_default_v4	Bool	Определяет какие сетевые адреса открывает **ntpd**
ntp_listen_on_default_v6	Bool	Определяет какие сетевые адреса открывает **ntpd**
ntp_clients_inventory_access	Bool	Ограничивает все хосты из inventory по флагу **nomodify notrap**
ntp_clients:	List	Список хостов/адресов для ограничения
name:	Str	Имя хоста или адреса
access:	Str	Флаг доступа
ntp_driftfile_directory	Str	Путь к файлу данных **ntp**
ntp_custom_config	Dict	Выборочная конфигурация **ntp**

2.2.5.1.24 Настройка параметров chrony

Настройка параметров приведена в таблице 47.

Таблица 47 – Настройка параметров chrony

Параметр	Тип	Описание
ntp_servers:	List	Список **ntp** серверов

2.2.6 Настройка межсетевого экранирования

В а ж н о – Во время установки на все серверы **автоматически** будет установлена служба управления межсетевым экраном **iptables** и настроены правила, ограничивающие входящий доступ по всем портам, кроме тех, которые занимают запущенные контейнеры на соответствующих серверах, и разрешены заданными правилами экрана.

Установленные правила межсетевого экрана приведены в таблице 48.

Таблица 48 – Установленные правила межсетевого экрана

Серверы	Таблица	Состояние	Порт	Протокол	Интерфейс	Разрешение
Серверы группы ucs	INPUT					DROP
	FORWARD					DROP
	OUTPUT					ACCEPT
	INPUT	RELATED, ESTABLISHED				ACCEPT
	INPUT			ICMP		ACCEPT
	INPUT				lo	ACCEPT
	INPUT	NEW	SSH	TCP		ACCEPT
	INPUT				docker0 или cni-podman0*	ACCEPT
	INPUT		2376	TCP		ACCEPT
	INPUT		9100	TCP		ACCEPT
Серверы группы ucs_etcd	INPUT					DROP
	FORWARD					DROP
	OUTPUT					ACCEPT
	INPUT	RELATED, ESTABLISHED				ACCEPT

Серверы	Таблица	Состояние	Порт	Протокол	Интерфейс	Разрешение
	INPUT			ICMP		ACCEPT
	INPUT				lo	ACCEPT
	INPUT	NEW	SSH	TCP		ACCEPT
	INPUT				docker0 или cni-podman0*	ACCEPT
	INPUT		2376	TCP		ACCEPT
	INPUT		9100	TCP		ACCEPT
	INPUT	NEW	53	UDP		ACCEPT
Серверы группы ucs_infrastructure	INPUT					DROP
	FORWARD					DROP
	OUTPUT					ACCEPT
	INPUT	RELATED, ESTABLISHED				ACCEPT
	INPUT			ICMP		ACCEPT
	INPUT				lo	ACCEPT
	INPUT	NEW	SSH	TCP		ACCEPT
					docker0 или cni-podman0*	ACCEPT
	INPUT		2376	TCP		ACCEPT
	INPUT		9100	TCP		ACCEPT
	INPUT		53	TCP		ACCEPT
	INPUT		53	UDP		ACCEPT
Серверы группы ucs_frontend	INPUT					DROP
	FORWARD					DROP
	OUTPUT					ACCEPT
	INPUT	RELATED, ESTABLISHED				ACCEPT
	INPUT			ICMP		ACCEPT
	INPUT				lo	ACCEPT
	INPUT	NEW	SSH	TCP		ACCEPT
					docker0 или cni-podman0*	ACCEPT
	INPUT		2376	TCP		ACCEPT
	INPUT		9100	TCP		ACCEPT
	INPUT			VRRP		ACCEPT

Серверы	Таблица	Состояние	Порт	Протокол	Интерфейс	Разрешение
Серверы группы ucs_mail	INPUT					DROP
	FORWARD					DROP
	OUTPUT					ACCEPT
	INPUT	RELATED, ESTABLISHED				ACCEPT
	INPUT			ICMP		ACCEPT
	INPUT				lo	ACCEPT
	INPUT	NEW	SSH	TCP		ACCEPT
					docker0 или cni-podman0*	ACCEPT
	INPUT		2376	TCP		ACCEPT
	INPUT		9100	TCP		ACCEPT
	INPUT			VRRP		ACCEPT

* если используется контейнерная виртуализация **podman**.

2.2.6.1 Настройки правил внешнего межсетевого экрана

Во время установки происходит настройка межсетевого экрана внутри контура инсталляции. Тем не менее очень важно обеспечить дополнительную защиту системы с внешней стороны по отношению к контуру инсталляции.

Во внешний контур должны быть доступны только следующие порты:

– порты на виртуальные IP серверов с ролью **ucs_frontend**:

- 80/tcp;
- 143/tcp;
- 443/tcp;
- 993/tcp;
- 3142/tcp;
- 6787/tcp;
- 389/tcp;
- 389/udp;
- 636/tcp;
- 636/udp;

– порты на виртуальные IP серверов с ролью **ucs_mail**:
  - 465/tcp;
  - 587/tcp;
– порты на реальные IP серверов **ucs_mail**:
  - 25/tcp.

2.3 Запуск установки

Для установки на контейнеры **docker** необходимо запустить следующую команду:

```
ansible-playbook playbooks/main.yml --diff
```

Для установки на контейнеры **podman** необходимо запустить следующую команду:

```
ansible-playbook playbooks/main.yml --skip-tags=cadvisor --extra-vars
'{"container_management_tool": "podman"}'  --extra-vars
'{"podman_container_no_hosts": "true"}' -e '{"confd_max_memory": "100M"}' -e
'{"pregen_max_memory": "100M"}' -e '{"cvm_max_memory": "2000M"}' --diff
```

Если использовалось шифрование паролей, описанное в разделе 2.2.2.3, то к команде установки необходимо добавить ключи **--vault-password-file=.filesecret** или **--ask-vault-pass**.

После этого запускаются роли, описанные в разделе 2.2.1.

В а ж н о – После установки Mailion по умолчанию включен увеличенный уровень логирования. По этой причине дисковое пространство будет значительно уменьшаться. Чтобы отключить данную функциональность, необходимо на машине оператора в файле `~/install_mailion/group_vars/ucs/main.yml` в строке 1888 удалить опцию `syslog_ng_external_all_services: true`. Сделать это возможно с помощью следующей команды:

```
sed 's|syslog_ng_external_all_services: true|#syslog_ng_external_all_services:
true|g' -i ~/install_mailion/group_vars/ucs/main.yml
```

Далее необходимо повторно перезапустить сервис syslog_ng:

```
~/install_mailion# ansible-playbook playbooks/mailion/logging.yml -v
```

2.4 Проверка корректности установки

Для проверки корректности установки необходимо запустить установленный ПО «Mailion»:

1. Открыть в поддерживаемом веб-браузере страницу по адресу, который указывался в **mailion_external_domain**.
2. Использовать для входа учетные данные созданных пользователей.
3. Если вход был выполнен под пользователем, то необходимо отправить письмо самому себе внутри ПО «Mailion». Если вход выполнен под администратором, то сначала нужно создать пользователя (при условии, что он не был создан плейбуком **ministerium**).
4. Если письмо успешно отправилось и пришло – установка настроена корректно.

2.4.1 Добавление дополнительных доменов для обслуживания инсталляцией

В ПО «Mailion» реализована поддержка дополнительных доменов. Чтобы добавить дополнительный домен необходимо включить его в список **mailion_supported_domain**:

```
mailion_supported_domains:
  - "example.com"
```

Затем необходимо добавить dkim-ключ к домену в словарь **rspamd_dkim_hosts**:

```
rspamd_dkim_hosts:
  domain2.example.net:
    dkim_key: |
......
```

После этого с машины оператора из папки с инсталлятором необходимо выполнить команду:

```
ansible-playbook playbooks/ucs/main.yml --tags postfix,rspamd --limit ucs_mail
--diff
```

Эта команда запустит роль **postfix** с функцией **mx** и добавит указанные домены для **MTA**, а также добавит dkim-ключи для доменов в **rspamd**.

2.5 Установка клиента «МойОфис Почта»

2.5.1 Установка программы на ОС Windows

Установку ПО «МойОфис Почта» на рабочее место с ОС Windows можно выполнить из командной строки в режиме «тихой» установки.

Перед началом установки ПО «МойОфис Почта» выполните следующие действия:

1. Убедитесь, что на рабочем месте пользователя, на котором будет осуществляться установка ПО «МойОфис Почта», разрешен удаленный доступ с правами администратора с рабочего места системного администратора.
2. Разместите дистрибутив ПО «МойОфис Почта» или в сетевой папке, доступной на рабочем месте пользователя, или в локальной папке на рабочем месте пользователя.
3. Войдите удаленно с помощью стандартной программы ОС Windows «Подключение к удаленному рабочему столу» на рабочее место пользователя, на котором будет осуществляться установка ПО «МойОфис Почта».

Подключение необходимо выполнять под учетной записью пользователя с правами администратора.

Примечание – Для обновления приложения на ОС Windows предварительно удалите текущую версию приложения (см. раздел 15.1), а затем установите версию 2.8 так, как это описано в данном разделе.

2.5.1.1 Установка с помощью MSI-пакета

Для «тихой» установки ПО «МойОфис Почта» запустите в командной строке ОС Windows от имени администратора следующую команду:

```
msiexec.exe /i <путь к дистрибутиву>
```

В таблице ниже представлено подробное описание параметров установки.

Таблица 49 – Параметры установки ПО «МойОфис Почта»

Параметр	Описание
/i или /package	Установить ПО «МойОфис Почта».
<путь к дистрибутиву>	Расположение и имя файла пакета установки.

Параметр	Описание
INSTALL_DIRECTORY_PATH=[path]	Абсолютный путь, указывающий место установки. Если используется параметр **INSTALL_DIRECTORY_NAME**, то этот параметр игнорируется.
INSTALL_DIRECTORY_NAME=[name]	Название папки для установки, которая будет создана в папке **Program Files**.
DESKTOP_SHORTCUT={true,false}	Создать/не создавать ярлык на рабочем столе. По умолчанию **true**.
START_MENU_SHORTCUT={true,false}	Создать/не создавать ярлык в меню «Пуск». По умолчанию **true**.
INSTALL_MAINTENANCE_SERVICE= {true,false}	Включить/отключить установку сервиса поддержки Maintenance Service. По умолчанию **true**.
REMOVE_DISTRIBUTION_DIR= {true,false}	Удалить/не удалять папку с дистрибутивом **distribution** из существующей установки. По умолчанию **true**.
PREVENT_REBOOT_REQUIRED= {true,false}	Запретить/не запрещать перезагрузку компьютера в процессе установки. Включение данного параметра может привести к неполной установке ПО. По умолчанию **false**.
OPTIONAL_EXTENSIONS={true,false}	Включить/отключить установку расширений. По умолчанию **true**.
EXTRACT_DIR=[directory]	Папка для распаковки файлов приложения. Файлы распаковываются в указанную папку, и установка приложения не производится. Все остальные параметры установки игнорируются.
/m	Создать MIF-файл состояния.
/q, /quiet и /passive	Параметры отображения: – **/q** и **/quiet** – «тихий» режим, без взаимодействия с пользователем. – **/passive** – автоматический режим. Только указатель хода выполнения.
/norestart, /forcerestart и /promptrestart	Параметры перезагрузки: – **/norestart** – останавливает перезагрузку устройства после завершения установки. Используется по умолчанию. – **/promptrestart** – запрашивает пользователя, если требуется перезагрузка.

Параметр	Описание
	– **/forcerestart** – перезапускает устройство после завершения установки.
/L или /log	Генерировать лог-файл (ведение журнала). Параметры: – **/L** – путь к файлу журнала. – **i** – занесение в журнал сообщений о состоянии. – **w** – занесение в журнал некритических предупреждений. – **e** – занесение в журнал сообщений об ошибках. – **a** – занесение в журнал выполнения действий. – **r** – занесение в журнал записей со сведениями о действиях. – **u** – занесение в журнал запросов пользователей. – **c** – занесение в журнал исходных параметров пользовательского интерфейса. – **m** – занесение в журнал нехватки памяти. – **p** – занесение в журнал свойств терминала. – **v** – занесение в журнал подробных сведений. Для использования параметра **v** следует задавать **/L*v**. – **+** – добавление в существующий файл. – **!** – сброс в журнал каждой строки. – ***** – занесение в журнал всех сведений, кроме параметра **v**. Это подстановочный знак. – **Имя_файла_журнала.txt** – имя и путь к текстовому файлу журнала.

Пример:

```
msiexec.exe /i "C:\Дистрибутивы\MyOffice_Mail_PSN_Windows_2.8G.msi"
INSTALL_DIRECTORY_PATH="C:\MyOfficeMail\"
DESKTOP_SHORTCUT=false
INSTALL_MAINTENANCE_SERVICE=false
/quiet
```

2.5.2 Установка приложения на ОС Linux

Для обновления приложения на ОС Linux предварительно удалите текущую версию приложения (см. раздел 15.2), а затем установите версию 2.8 так, как это описано в данном

разделе.

2.5.2.1 Установка дистрибутива sh

Перед началом установки разместите исполняемый файл дистрибутива **MyOffice_Mail_PSN_x64_2.8G.sh** в сетевой папке, доступной на рабочем месте пользователя, или в локальной папке на рабочем месте пользователя.

Если установка будет осуществляться локально, откройте терминал.

Если установка будет осуществляться удаленно, выполните следующие действия:

1. Убедитесь, что на рабочее место пользователя, на котором будет осуществляться установка ПО «МойОфис Почта», разрешен удаленный доступ по SSH с рабочего места системного администратора.
2. Войдите удаленно с помощью SSH-клиента на рабочее место пользователя, на котором будет осуществляться установка ПО «МойОфис Почта».

Для установки ПО «МойОфис Почта» выполните следующие действия:

1. С помощью команды **cd** перейдите в папку, в которой расположен исполняемый файл дистрибутива.
2. Добавьте необходимые права исполняемому файлу дистрибутива:

```
chmod +x ./MyOffice_Mail_PSN_x64_2.8G.sh
```

3. Запустите выполнение файла дистрибутива:

```
./MyOffice_Mail_PSN_x64_2.8G.sh
```

4. Укажите **1**, чтобы начать процесс установки (см. Рисунок 5).

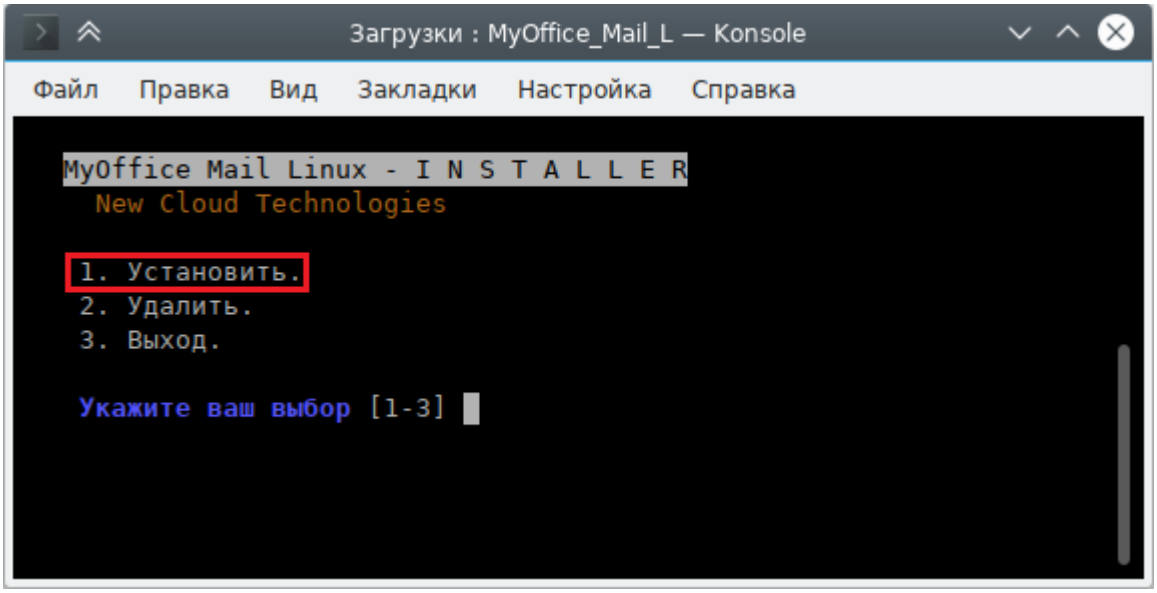


Рисунок 5 – Выбор основного сценария действий

5. Укажите **1**, чтобы прочитать лицензионное соглашение (см. Рисунок 6).
6. Укажите **2**, чтобы принять лицензионное соглашение и установить программу.

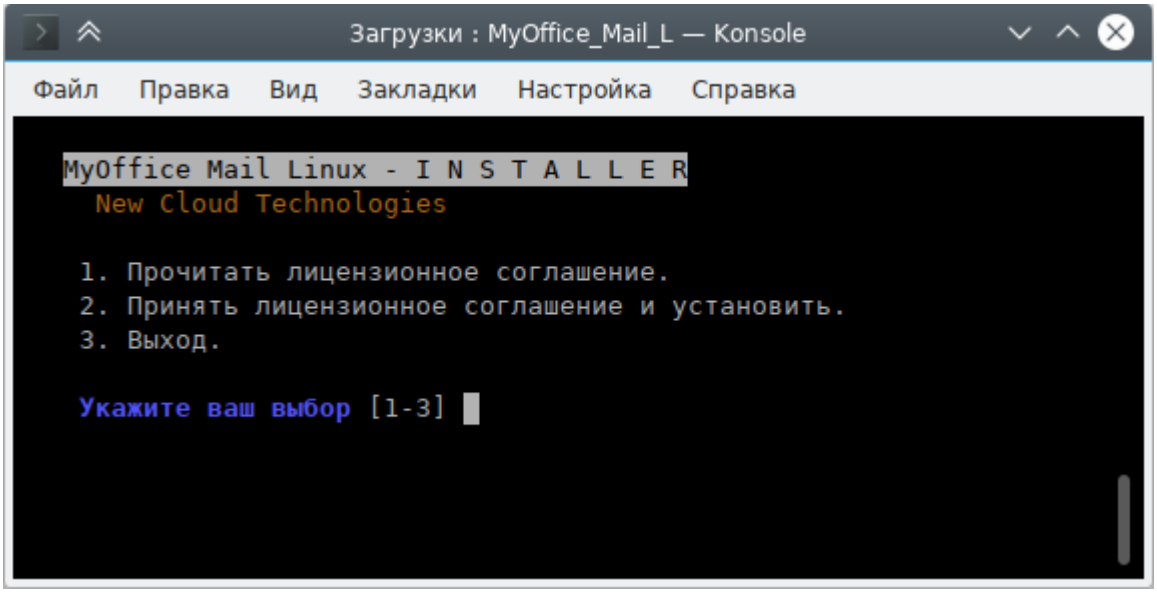


Рисунок 6 – Лицензионное соглашение и начало установки

7. При необходимости укажите папку для установки программы (см. Рисунок 7).

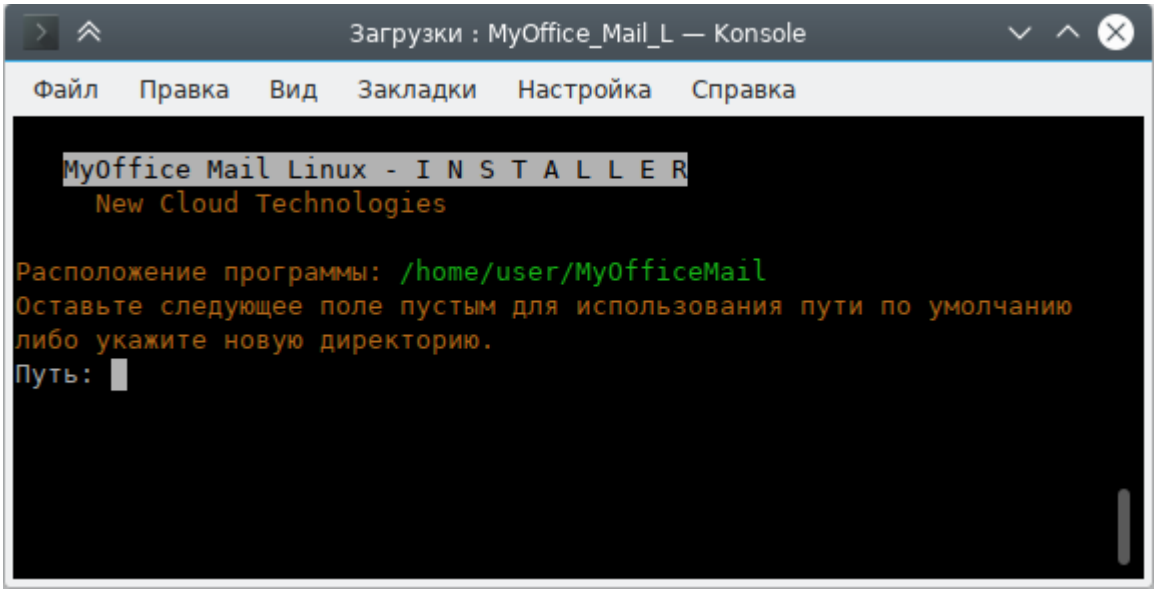


Рисунок 7 – Выбор папки для установки

8. Дождитесь полной установки компонентов программы (см. Рисунок 8).

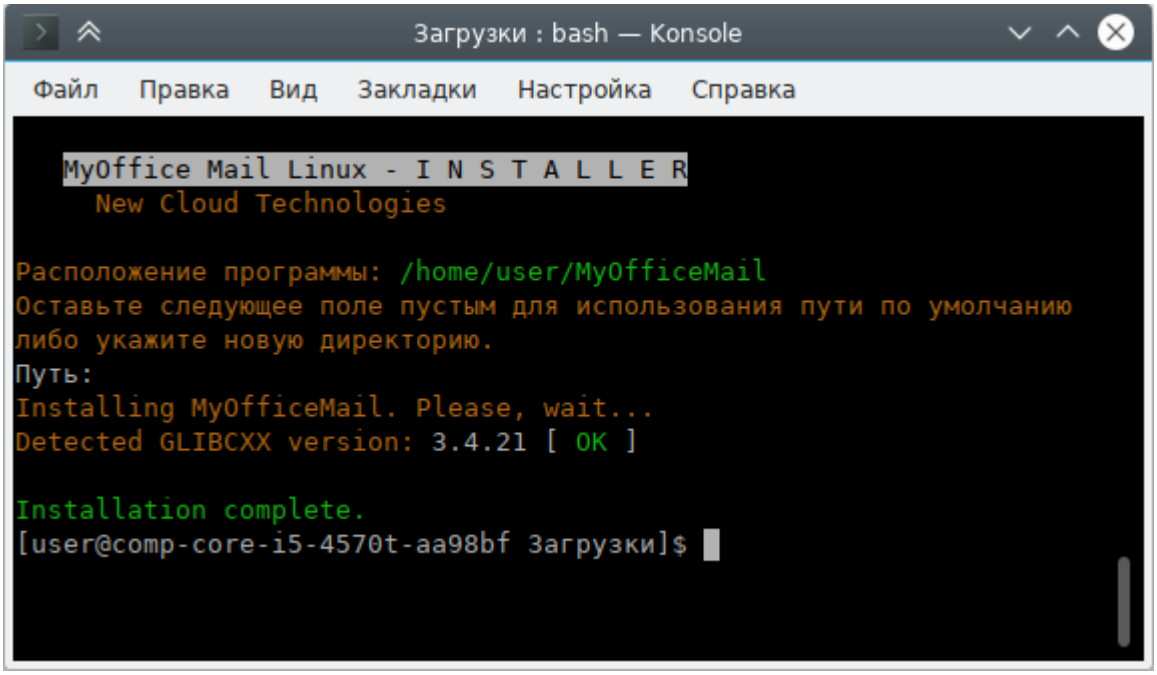


Рисунок 8 – Установка завершена успешно

2.5.2.2 Установка дистрибутива rpm

2.5.2.2.1 Установка rpm с помощью терминала

Установку или обновление приложения «МойОфис Почта» на ОС Linux (дистрибутив **myofficemail-2.8G.x86_64.rpm**) можно выполнить с помощью терминала или программы, предназначенной для установки пакетов.

Перед началом установки разместите файл дистрибутива приложения «МойОфис Почта» в локальной папке.

Если обновление приложения «МойОфис Почта» выполняется на ОС с окружением рабочего стола GNOME, Cinnamon или MATE, удалите конфигурационные файлы предыдущей версии приложения, расположенные в домашнем каталоге пользователя.

Чтобы установить или обновить приложение «МойОфис Почта» посредством терминала, с помощью команды `cd` перейдите в каталог, в котором размещен файл дистрибутива.

Для установки или обновления приложения «МойОфис Почта» с помощью файла дистрибутива с расширением **.rpm** выполните следующую команду:

```
sudo rpm -iU myofficemail-2.8G.x86_64.rpm
```

2.5.2.2.2 Установка rpm с помощью приложения установки

Чтобы установить или обновить приложение «МойОфис Почта» с помощью программы, предназначенной для установки пакетов, выполните следующие действия:

1. Запустите программу для установки пакетов одним из следующих способов:
   – Единожды/дважды щелкните мышью по файлу дистрибутива приложения «МойОфис Почта».

– Щелчком правой кнопки мыши откройте контекстное меню файла дистрибутива приложения «МойОфис Почта» и выберите пункт **Открыть в** [наименование программы] / **Открыть с помощью** [наименование программы] / **Открыть с помощью другого приложения** (см. Рисунок 9).

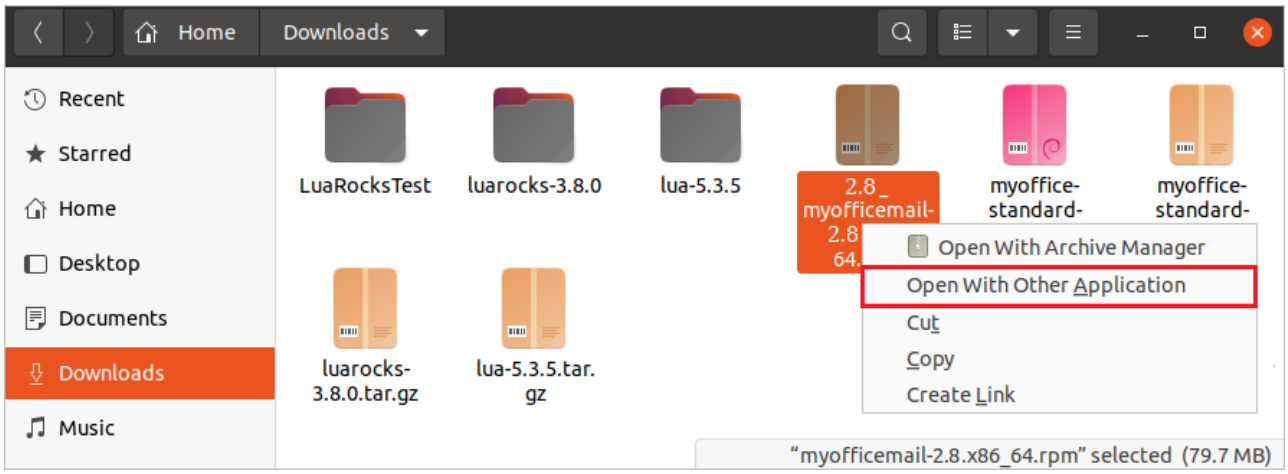


Рисунок 9 – Пример контекстного меню дистрибутива «МойОфис Почта»

Выберите приложение установки (см. Рисунок 10).

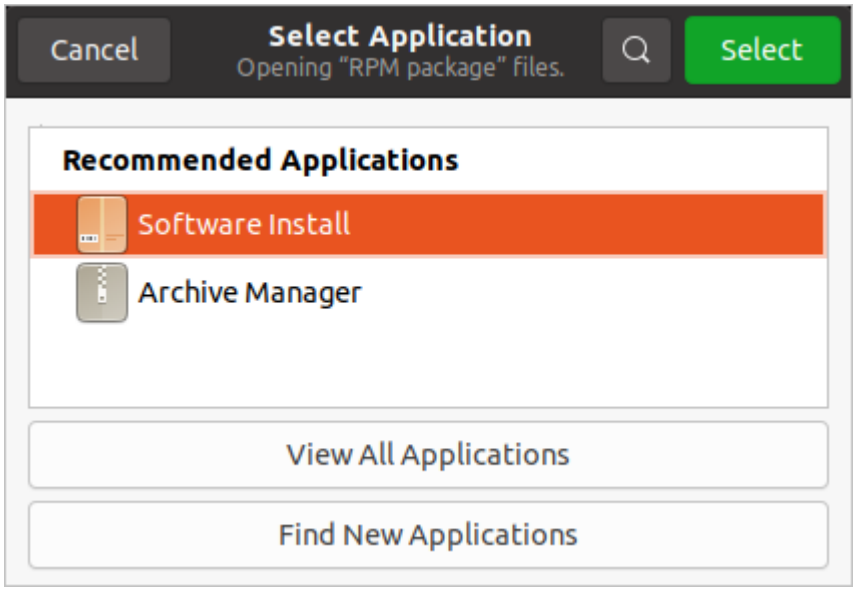


Рисунок 10 – Выбор приложения для открытия пакета **rpm**

2. Для последующей установки приложения «МойОфис Почта» следуйте указаниям программы установки.

2.5.2.3 Установка дистрибутива deb

2.5.2.3.1 Установка дистрибутива deb из проводника

Установку или обновление приложения «МойОфис Почта» на ОС Astra Linux Special Edition (дистрибутив **myofficemail-2.8G-x86_64.deb**) можно выполнить из проводника.

Откройте папку, содержащую файл дистрибутива приложения «МойОфис Почта».

Запустите установку одним из следующих способов:

– Двойным кликом мыши на файле дистрибутива.

– Правой клавишей мыши откройте контекстное меню и выберите **Открыть**.

На экране появится панель подготовки к инсталляции (см. Рисунок 11).

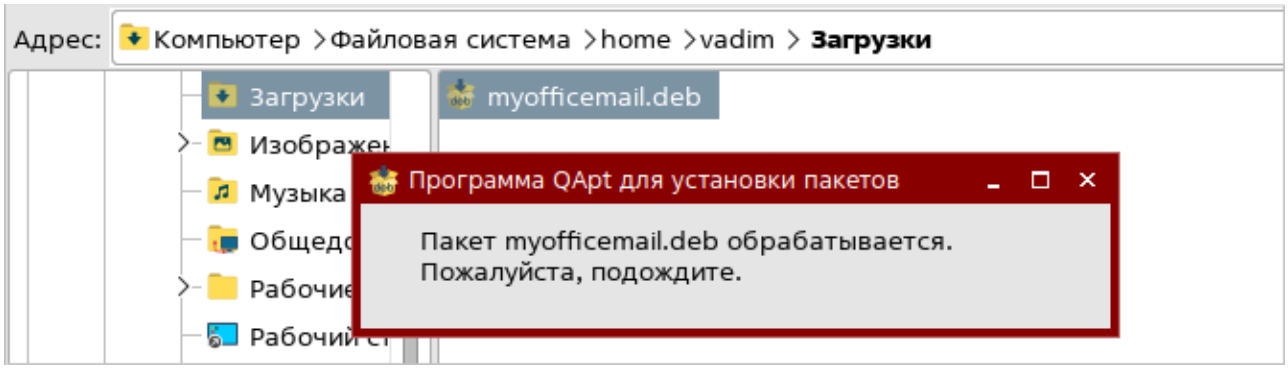


Рисунок 11 – Подготовка к установке

Далее на экране появится основной диалог инсталляции приложения (см. Рисунок 12).

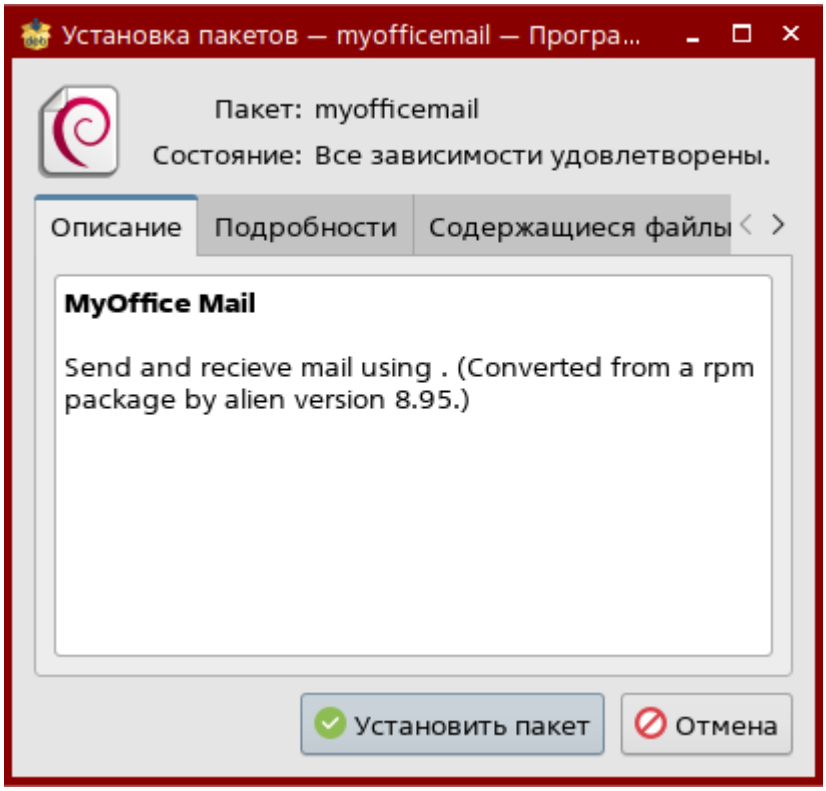


Рисунок 12 – Диалог установки приложения

Нажмите **Установить пакет**, введите пароль администратора (см. Рисунок 13).

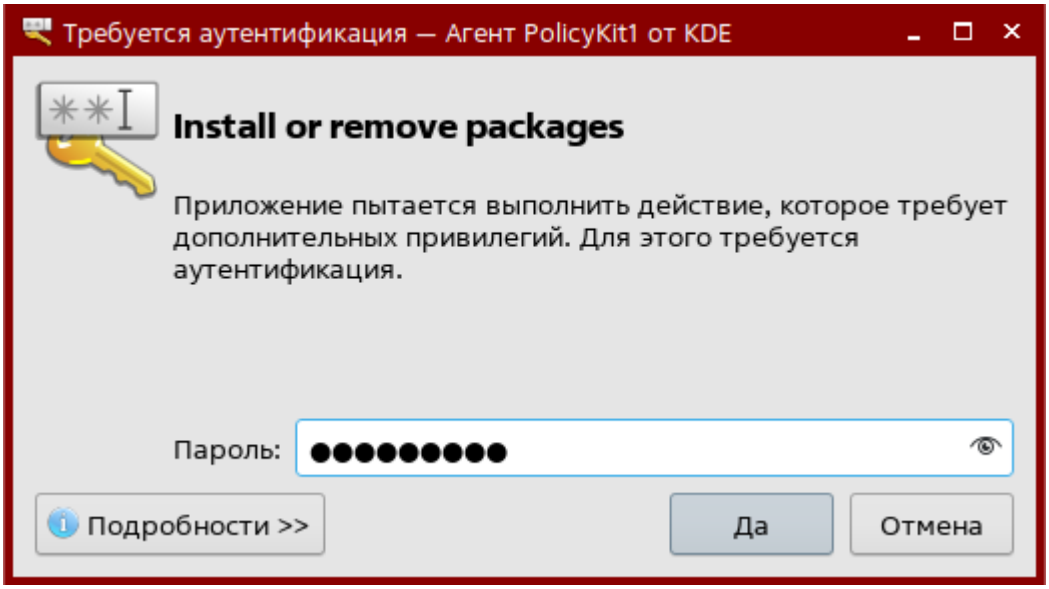


Рисунок 13 – Ввод пароля администратора

Нажмите **Да**, процесс установки начнется, на экране появится панель завершения (см. Рисунок 14).

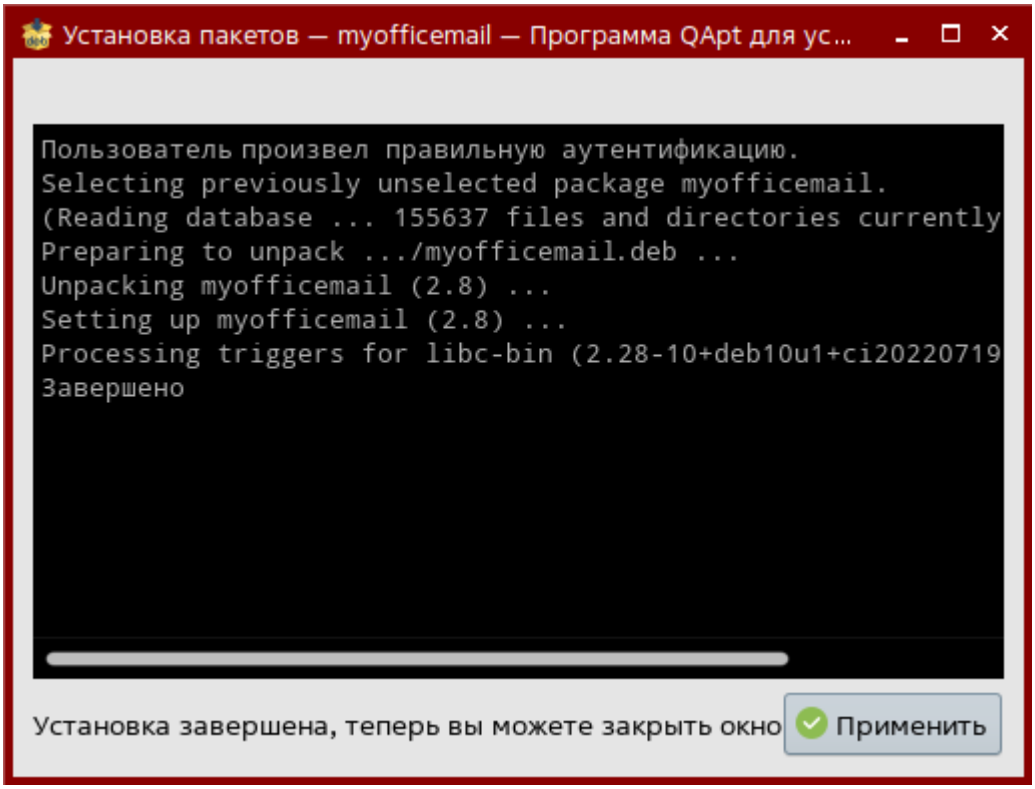


Рисунок 14 – Панель завершения инсталляции

Инсталляция завершена, нажмите кнопку **Применить**, в системном меню в разделе **Офис** появится приложение «МойОфис Почта» (см. раздел 5.3).

2.5.2.3.2 Установка дистрибутива deb из консоли

Установку или обновление приложения «МойОфис Почта» на ОС Astra Linux Special Edition (дистрибутив **myofficemail-2.8G-x86_64.deb**) можно выполнить с помощью терминала.

Перед началом установки разместите файл дистрибутива приложения «МойОфис Почта» в локальной папке.

Для установки или обновления приложения «МойОфис Почта» выполните следующий набор команд:

```
astrauser@astra-pc:~$ cd home/astrauser/Downloads
astrauser@astra-pc:~/Downloads$
astrauser@astra-pc:~/Downloads$ chmod 777 myofficemail-2.8G-x86_64.deb
astrauser@astra-pc:~/Downloads$ sudo dpkg -i myofficemail-2.8G-x86_64.deb
[sudo] пароль для astrauser:
Выбор ранее не выбранного пакета myofficemail.
(Чтение базы данных ... на данный момент установлено 198107 файлов и
каталогов.)
Подготовка к распаковке myofficemail-2.8G-x86_64.deb ...
Распаковывается myofficemail (2.8) ...
Распаковывается пакет myofficemail (2.8) ...
Обрабатываются триггеры для libc-bin (2.28-10+deb1-
u2+ci20230227150+astra5) ///
astrauser@astra-pc:~/Downloads$
```

2.6 Установка в составе других продуктов ПО «МойОфис»

Установка в составе других продуктов ПО «МойОфис» не выполняется.

3 ОБНОВЛЕНИЕ С ПРЕДЫДУЩИХ ВЕРСИЙ

Обновления возможны с версии 1.8.2. Список компонентов приведен в разделе 2.1.

Перед обновлением необходимо в файлах `group_vars/ucs_setup/*` проверять наличие новых переменных (где `ucs_setup` – название инсталяции). Новые переменные находятся в файлах `contrib/mailion/cluster/group_vars/ucs_setup/*` (для «Standalone» инсталляции в `contrib/mailion/standalone/group_vars/ucs_setup/*`).

Обновление ПО «Mailion» осуществляется аналогично установке новой версии (см. раздел 2).

В а ж н о – Перед обновлением необходимо в файле **contrib/mailion/cluster/group_vars/ucs_Имя_Инсталяции/version.yml** изменить значение переменной **mailion_release_name** на значение, аналогичное номеру актуального релиза.

4 ДОПОЛНИТЕЛЬНЫЕ ВОЗМОЖНОСТИ И РЕКОМЕНДАЦИИ ПО УСТАНОВКЕ

4.1 Настройка Redis TLS

Последовательность действий:

1. Изначально необходимо установить Mailion без поддержки TLS, установив параметр `redis_sentinel_single_installation_enabled` в значение `true`. Это необходимо для того, чтобы для каждого сервиса, использующего `redis`, создавался отдельный экземпляр `redis sentinel`, при этом впоследствии все экземпляры `redis sentinel` переключаются в режим TLS, за исключением `redis sentinel` для сервиса `rspamd` (см. исключение, пункт 6).
2. Сгенерировать TLS-сертификаты для всех серверов `redis` (см. исключение, пункт 6), включая все `sentinel`. Сертификаты должны быть подписаны корневым сертификатом, который будет доступен в клиентах (сервисах, подключающихся к `redis` по TLS) – для верификации `redis`, также сертификаты должны включать IP-адреса сервисов `redis`, на которых будут серверы `redis` (IP SANs – https://serverfault.com/a/611121).
3. Настроить все сервера `redis`, включая `redis sentinel`, на работу с TLS.
4. Настроить сервисы с поддержкой TLS для `redis`.
5. Перезапустить сервисы.
6. Обратить внимание на исключение для rspamd: `redis_sentinel_rspamd` / `redis_rspamd` – оставить как есть, без TLS.

4.1.1 Генерация сертификатов и запуск контейнеров с сертификатами

Для генерации сертификатов в нужном формате необходимо добавить следующие изменения в коллекцию `nct.redis` для ролей `redis` и `sentinel`:

1. Добавить переменные для TLS в файлы `redis/defaults/main.yml` и `sentinel/defaults/main.yml`:

```
redis_tls_certs_authority_name: "Intermediate main"
redis_tls_certs_generate_cert_auth_key_name: "services"
```

2. Добавить изменения в следующие файлы:
   – В файл `redis/tasks/main.yml` добавить "Reset vars", "Create TLS certs", "Set TLS directories for mount volumes", "Set container volumes", заменить "Start redis container":

```
- name: "Install python dependencies"
  ansible.builtin.include_role:
    name: "init"
  when: >
    (redis_packages is not defined) or
    ((redis_packages.changed is defined) and (not redis_packages.changed))

- name: "Reset vars"
  ansible.builtin.set_fact:
    redis_tls_volumes: []
    redis_volumes: []

 - name: "Create TLS certs"
  ansible.builtin.include_role:
    name: "nct.certs.tls_certs"
  vars:
    tls_certs_authority_name: "{{ redis_tls_certs_authority_name }}"
    tls_certs_copy_ca: true
    tls_certs_create_certs: true
    tls_certs_generate_cert_auth_key_name:
"{{ redis_tls_certs_generate_cert_auth_key_name if ca_multiroot else '' }}"
    tls_certs_generate_cert_domain_name: "redis.{{ inventory_hostname }}"
    tls_certs_generate_cert_domain_aliases: ["{{ ansible_nic_ipv4_address }}"]
    tls_certs_generate_cert_key_algorithm: "rsa"
    tls_certs_generate_cert_key_size: 2048
    tls_certs_generate_cert_profile: "both"

- name: "Set TLS directories for mount volumes"
  ansible.builtin.set_fact:
    redis_tls_volumes:
      - "{{ tls_ca }}:/etc/pki/tls/certs/{{ tls_ca_name }}:ro"
      - "{{ tls_cert_client }}:/etc/pki/tls/certs/{{ tls_cert_client_name }}:ro"
      - "{{ tls_cert_server }}:/etc/pki/tls/certs/{{ tls_cert_server_name }}:ro"
      - "{{ tls_key }}:/etc/pki/tls/private/{{ tls_key_name }}:ro"

...

- name: "Set container volumes"
  ansible.builtin.set_fact:
    redis_volumes:
      - "{{ vars['redis_' + redis_id + '_conf_dir'] }}:/etc/redis"
      - "{{ vars['redis_' + redis_id + '_data_dir'] }}:/data"
      - "{{ vars['redis_' + redis_id + '_cluster_conf_dir'] }}:/etc/redis-
cluster"

- name: "Start redis container"
  ansible.builtin.include_role:
    name: "nct.tools.container_launcher"
  vars:
    service_container_management_tool: "{{ redis_container_management_tool }}"
    service_name: "redis_{{ redis_id }}"
    service_image_name: "redis"
    service_image_registry: "{{ redis_image_registry }}"
    service_image_tag: "{{ redis_image_tag }}"
```

```
    service_container_state: "started"
    service_container_log_driver: "{{ redis_container_log_driver | default(omit)
}}"
    service_container_log_options: "{{ redis_container_log_options |
default(omit) }}"
    service_container_cpus: "{{ redis_container_cpu_limit | default(omit) }}"
    service_container_memory: "{{ redis_container_memory_limit |
default(omit) }}"
    service_published_ports:
      - "{{ redis_port }}:{{ redis_port }}"
      - "{{ redis_replication_port }}:{{ redis_replication_port }}"
    service_env:
      TZ: "{{ system_timezone }}"
      REDIS_PASSWORD: "{{ redis_password }}"
    service_volumes: "{{ redis_tls_volumes + redis_volumes }}"
    service_container_command: "{{ redis_command }}"
    when: >
        (redis_static_conf.changed) or (molecule_test_mode is not defined) or
        (not molecule_test_mode) or (redis_sensitive_conf1.changed) or
        (redis_sensitive_conf2.changed) or (redis_sensitive_conf3.changed) or
        (redis_sensitive_conf4.changed)
    service_container_restart: >-
      {{-
        (redis_static_conf.changed) or
        (redis_sensitive_conf1.changed) or
        (redis_sensitive_conf2.changed) or
        (redis_sensitive_conf3.changed) or
        (redis_sensitive_conf4.changed) or
        (tls_certs_generate_cert_force_update | default(omit))
      -}}
    service_published_ports:
      - "{{ redis_sentinel_port }}:{{ redis_sentinel_port }}"
    service_volumes: "{{ redis_sentinel_tls_volumes + redis_sentinel_volumes }}"
    service_container_command: "redis-sentinel /etc/redis/sentinel.conf"
```

– В файл `sentinel/tasks/main.yml` добавить "Reset vars", "Create TLS certs", "Set TLS directories for mount volumes", заменить "Start redis container":

```
- name: "Reset vars"
  ansible.builtin.set_fact:
    redis_sentinel_tls_volumes: []

  - name: "Create TLS certs"
  ansible.builtin.include_role:
    name: "nct.certs.tls_certs"
  vars:
    tls_certs_authority_name: "{{ redis_tls_certs_authority_name }}"
    tls_certs_copy_ca: true
    tls_certs_create_certs: true
    tls_certs_generate_cert_auth_key_name:
"{{ redis_tls_certs_generate_cert_auth_key_name if ca_multiroot else '' }}"
    tls_certs_generate_cert_domain_name: "redis.{{ inventory_hostname }}"
    tls_certs_generate_cert_domain_aliases: ["{{ ansible_nic_ipv4_address }}"]
    tls_certs_generate_cert_key_algorithm: "rsa"
    tls_certs_generate_cert_key_size: 2048
    tls_certs_generate_cert_profile: "both"

- name: "Set TLS directories for mount volumes"
  ansible.builtin.set_fact:
```

```
    redis_tls_volumes:
      - "{{ tls_ca }}:/etc/pki/tls/certs/{{ tls_ca_name }}:ro"
      - "{{ tls_cert_client }}:/etc/pki/tls/certs/{{ tls_cert_client_name }}:ro"
      - "{{ tls_cert_server }}:/etc/pki/tls/certs/{{ tls_cert_server_name }}:ro"
      - "{{ tls_key }}:/etc/pki/tls/private/{{ tls_key_name }}:ro"

...

- name: "Start container"
  ansible.builtin.include_role:
    name: "nct.tools.container_launcher"
  vars:
    service_container_management_tool:
"{{ redis_sentinel_container_management_tool }}"
    service_name: "redis_sentinel_{{ redis_sentinel_name }}"
    service_image_name: "redis"
    service_image_registry: "{{ redis_image_registry }}"
    service_image_tag: "{{ redis_image_tag }}"
    service_container_state: "started"
    service_container_log_driver: "{{ redis_sentinel_container_log_driver |
default(omit) }}"
    service_container_log_options: "{{ redis_sentinel_container_log_options |
default(omit) }}"
    service_container_restart: >-
      {{-
        (sentinel_auth_pass.changed) or
        (sentinel_default_conf.changed) or
        (sentinel_requirepass.changed) or
        (sentinel_static_conf.changed) or
        (tls_certs_generate_cert_force_update | default(omit))
      -}}
    service_published_ports:
      - "{{ redis_sentinel_port }}:{{ redis_sentinel_port }}"
    service_volumes: "{{ redis_sentinel_tls_volumes + redis_sentinel_volumes }}"
    service_container_command: "redis-sentinel /etc/redis/sentinel.conf"
```

– В файл `sentinel/tasks/configure_sentinel.yml` добавить "Reset vars", "Set container volumes":

```
- name: "Reset vars"
  ansible.builtin.set_fact:
    redis_sentinel_volumes: []

- name: "Configure sentinel : create directories required by containers and get
variables"
....

- name: "Set container volumes"
  ansible.builtin.set_fact:
    redis_sentinel_volumes:
      - "{{ vars['redis_sentinel_' + redis_sentinel_name +
'_conf_dir'] }}:/etc/redis"
```

– В файл `sentinel/tasks/sanitize_sentinel.yml` добавить "Reset vars", "Create TLS certs", "Set TLS directories for mount volumes", "Set container volumes", заменить "Start redis container":

```
- name: "Reset vars"
  ansible.builtin.set_fact:
    redis_sentinel_tls_volumes: []

- name: "Sanitize sentinel : create directories required by containers and get
variables"
...

- name: "Create TLS certs"
  ansible.builtin.include_role:
    name: "nct.certs.tls_certs"
  vars:
    tls_certs_authority_name: "{{ redis_tls_certs_authority_name }}"
    tls_certs_copy_ca: true
    tls_certs_create_certs: true
    tls_certs_generate_cert_auth_key_name:
"{{ redis_tls_certs_generate_cert_auth_key_name if ca_multiroot else '' }}"
    tls_certs_generate_cert_domain_name: "redis.{{ inventory_hostname }}"
    tls_certs_generate_cert_domain_aliases: ["{{ ansible_nic_ipv4_address }}"]
    tls_certs_generate_cert_key_algorithm: "rsa"
    tls_certs_generate_cert_key_size: 2048
    tls_certs_generate_cert_profile: "both"

- name: "Set TLS directories for mount volumes"
  ansible.builtin.set_fact:
    redis_tls_volumes:
      - "{{ tls_ca }}:/etc/pki/tls/certs/{{ tls_ca_name }}:ro"
      - "{{ tls_cert_client }}:/etc/pki/tls/certs/{{ tls_cert_client_name }}:ro"
      - "{{ tls_cert_server }}:/etc/pki/tls/certs/{{ tls_cert_server_name }}:ro"
      - "{{ tls_key }}:/etc/pki/tls/private/{{ tls_key_name }}:ro"

- name: "Set container volumes"
  ansible.builtin.set_fact:
    redis_sentinel_volumes:
      - "{{ vars['redis_sentinel_' + redis_sentinel_name +
'_conf_dir'] }}:/etc/redis"

...

- name: "Start container"
  ansible.builtin.include_role:
    name: "nct.tools.container_launcher"
  vars:
    service_container_management_tool:
"{{ redis_sentinel_container_management_tool }}"
    service_name: "redis_sentinel_{{ redis_sentinel_name }}"
    service_image_name: "redis"
    service_image_registry: "{{ redis_image_registry }}"
    service_image_tag: "{{ redis_image_tag }}"
    service_container_state: "started"
    service_container_log_driver: "{{ redis_sentinel_container_log_driver |
default(omit) }}"
    service_container_log_options: "{{ redis_sentinel_container_log_options |
default(omit) }}"
```

```
    service_container_cpus: "{{ redis_sentinel_container_cpu_limit |
default(omit) }}"
    service_container_memory: "{{ redis_sentinel_container_memory_limit |
default(omit) }}"
    service_container_restart: true # we always restart after sanitizing
    service_published_ports:
      - "{{ redis_sentinel_port }}:{{ redis_sentinel_port }}"
    service_volumes: "{{ redis_sentinel_tls_volumes + redis_sentinel_volumes }}"
    service_container_command: "{{ redis_command }}
{{ redis_sentinel_sanitized_params }}"
```

3. Запустить плейбук обновления ролей `redis` и `redis_sentinel` с перегенерацией сертификатов:

```
ansible-playbook -i inventory/<your_inventory>.yml playbooks/mailion/infra.yml \
    --extra-vars "ansible_user=<your_ansible_user>" \
    --extra-vars "tls_certs_generate_cert_force_update=true" \
    --tags redis_cache,redis_data \
    --diff --limit ucs_redis_cache,ucs_redis_data
```

4. После обновления ролей `redis` и `redis_sentinel` с перегенерацией сертификатов на хостах групп `ucs_redis_cache`, `ucs_redis_data` сертификаты будут находиться в каталогах `/srv/tls/certs` и `/srv/tls/private`:
   - `redis.<domain>-main-client.pem`
   - `redis.<domain>-main-server.pem`
   - `redis.<domain>-main-key.pem`
   - `...<domain>-main-ca.pem`

4.1.2 Настройка Redis и Sentinel для работы по TLS

Для добавления параметров TLS для Redis и Sentinel следует выполнить команды:

1. Отредактировать файл `/srv/docker/<redis_<имя_сервиса>/conf/redis.conf` для сервисов Redis.
2. Отредактировать файл `/srv/docker/<redis_sentinel_<имя_сервиса>/conf/sentinel.conf` для сервисов Redis Sentinel.
3. Добавить параметры TLS в конфигурационный файл и сохранить.
4. В файлах `redis.conf` и `sentinel.conf` необходимо указать следующие параметры:

```
port 0
tls-auth-clients no
```

```
tls-ca-cert-file "/etc/pki/tls/certs/<имя файла tls-ca-cert-file>"
tls-cert-file "/etc/pki/tls/certs/<имя файла tls-cert-file>"
tls-cluster yes
tls-key-file "/etc/pki/tls/private/<имя файла tls-key-file>"
tls-port <redis_port> или <redis_sentinel_port>
tls-replication yes
```

Пример конфигурации с TLS для Redis и Sentinel:

```
port 0
tls-auth-clients no
tls-ca-cert-file "/etc/pki/tls/certs/intermediate_main.pem"
tls-cert-file "/etc/pki/tls/certs/redis.redis-sentinel-docker-astra-
1.molecule.stageoffice.ru-intermediate_main-server.pem"
tls-cluster yes
tls-key-file "/etc/pki/tls/private/redis.redis-sentinel-docker-astra-
1.molecule.stageoffice.ru-intermediate_main-key.pem"
tls-port <redis_port> или <redis_sentinel_port>
tls-replication yes
# Generated by CONFIG REWRITE
...
```

5. Запустить команду внутри каждого контейнера с Redis и Sentinel:
   - для контейнеров Redis без аутентификации:

```
docker exec -ti redis_<service_name> redis-cli -p <redis_port> CONFIG REWRITE
```

   - для контейнеров Redis с аутентификацей:

```
docker exec -ti redis_<service_name> redis-cli -p <redis_port> --no-auth-warning
-a <redis_password> CONFIG REWRITE
```

   - для контейнеров Redis Sentinel без аутентификации:

```
docker exec -ti redis_sentinel_<service_name> redis-cli -p <redis_port> CONFIG
REWRITE
```

   - для контейнеров Redis Sentinel с аутентификацей:

```
docker exec -ti redis_sentinel_<service_name> redis-cli -p <redis_port> --no-
auth-warning -a <redis_password> CONFIG REWRITE
```

После выполнения данных команд нужно учитывать, что в конфигурационные файлы Redis, Redis Sentinel будет заново добавлена чувствительная информация, которая убирается запуском плейбука:

```
ansible-playbook -i inventory/<your_inventory>.yml playbooks/mailion/infra.yml \
    --extra-vars "ansible_user=<your_ansible_user>" \
    --extra-vars "redis_sentinel_sanitized_enabled=1" \
    --tags redis_sanitize \
    --diff --limit ucs_redis_cache,ucs_redis_data
```

4.1.3 Настройка сервисов с поддержкой TLS для Redis

Чтобы сервисы обращались к Redis и Sentinel по TLS, необходимо изменить конфигурацию сервисов для секции `redis`:

– Зайти на хосты, где расположен сервис.

– Открыть конфигурационный файл сервиса для редактирования:

```
vim /srv/docker/<имя_сервиса>/conf/config.json
```

– Добавить параметр `"use_tls": true` в секцию `redis`.

– Сохранить изменения.

В таблице 50 для каждого сервиса указана группа хостов. Проверить имена хостов можно по группе в файле `inventory/<your_inventory>.yml`.

Таблица 50 – Группа хостов для сервисов

Сервис	Группа хостов
ares	ucs_caledar
homeros	ucs_catalog
leda	ucs_frontend
erakles	ucs_catalog
viper	ucs_apps
ektor	ucs_catalog
mars	ucs_calendar
hog	ucs_apps

Сервис	Группа хостов
minos	ucs_catalog
euripides	ucs_catalog
rspamd	-
dafnis	ucs_catalog, ucs_calendar
dowal	ucs_apps

Пример файла `config.json`:

```
"redis": {
    "addresses": [
    "redis.mailion-obst-1.redis.stageoffice.ru:26379",
    "redis.mailion-obst-2.redis.stageoffice.ru:26379",
    "redis.mailion-obst-3.redis.stageoffice.ru:26379"
  ],
  "dial_timeout": "3s",
  "master_name": "minos",
  "max_retries": 0,
  "password": "",
  "pool_size": 25,
  "read_timeout": "10s",
  "redis_mode": "sentinel",
  "use_tls": true,
  "write_timeout": "10s"
},
```

4.1.4 Перезапуск сервисов

Для перезапуска всех контейнеров с Redis и Redis Sentinel нужно зайти на хосты групп `ucs_redis_cache` и `ucs_redis_data` и выполнить:

```
docker restart $(docker ps -qf "name=^redis_")
```

Далее перезапустить сервисы на каждом хосте (см. раздел 4.1.3):

```
docker restart <service_name>
```

После рестарта контейнеров применятся новые настройки с TLS для Redis и Redis Sentinel.

4.2 Доступ к веб-интерфейсам вспомогательных систем для управления ПО «Mailion»

4.2.1 Rspamd

Rspamd – система управления антиспамом (конфигурация правил рейтингов, история обработки). Веб-интерфейс Rspamd доступен по адресу `http://rspamd.<mail_inventory_hostname>:11334/`.

Где `<mail_inventory_hostname>` – FQDN хоста из группы **ucs_mail** (см. Рисунок 15).

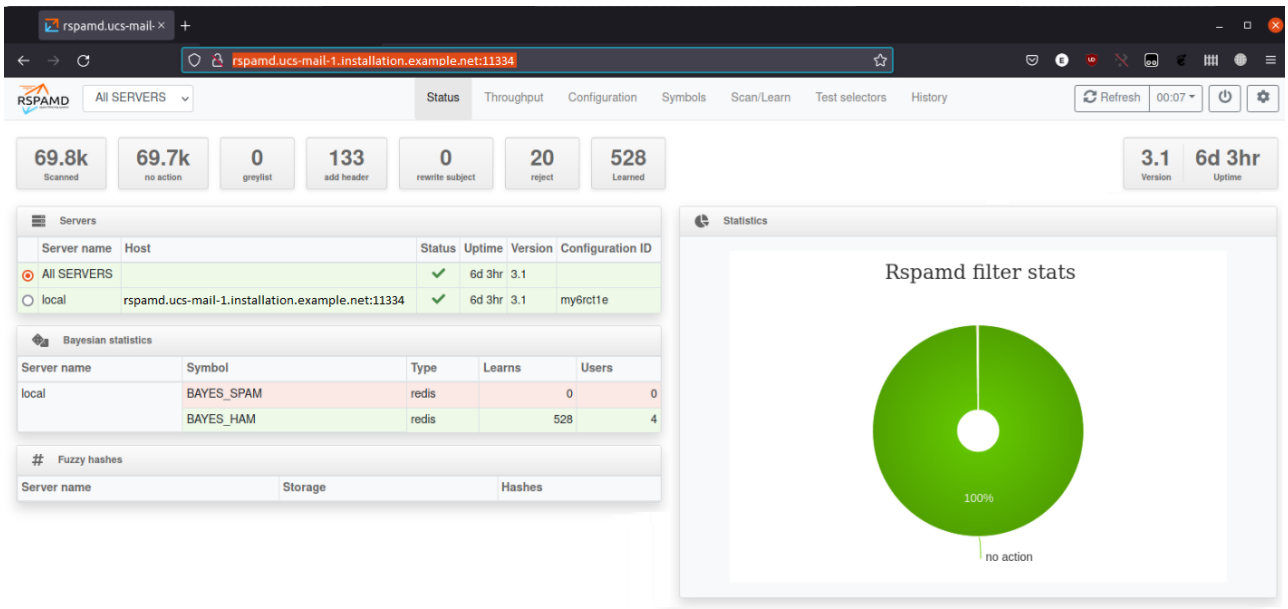


Рисунок 15 – Веб-интерфейс Rspamd

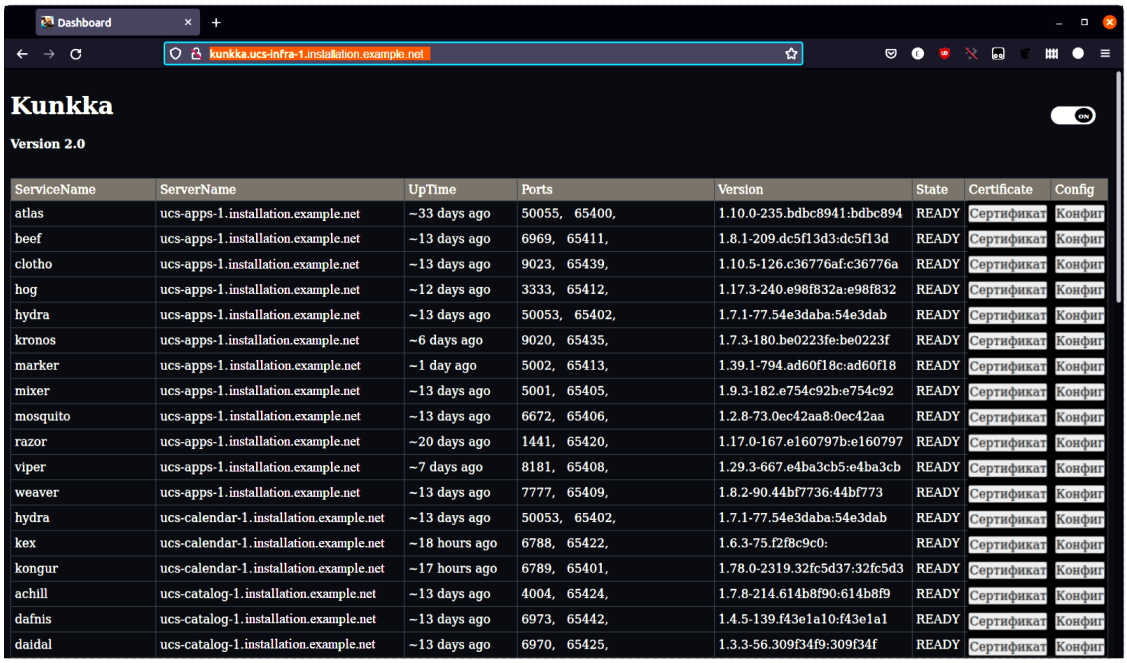
Доступ в Rspamd необходимо осуществлять по протоколу HTTP из внутренней сети инсталляции.

Для доступа к веб-интерфейсу потребуется пароль, который указан в переменной **rspamd_web_password**.

4.2.2 Kunkka

Kunkka – веб-страница с отображением подсистем на серверах. Веб-интерфейс Kunkka доступен по адресу `http://kunkka.<infrastructure_inventory_hostname>/`.

Где `<infrastructure_inventory_hostname>` – FQDN хоста группы **ucs_infrastructure** (см. Рисунок 16).



ServiceName	ServerName	UpTime	Ports	Version	State	Certificate	Config
atlas	ucs-apps-1.installation.example.net	~33 days ago	50055, 65400,	1.10.0-235.bdbc8941:bdbc894	READY	Сертификат	Конфиг
beef	ucs-apps-1.installation.example.net	~13 days ago	6969, 65411,	1.8.1-209.dc5f13d3:dc5f13d	READY	Сертификат	Конфиг
clotho	ucs-apps-1.installation.example.net	~13 days ago	9023, 65439,	1.10.5-126.c36776af:c36776a	READY	Сертификат	Конфиг
hog	ucs-apps-1.installation.example.net	~12 days ago	3333, 65412,	1.17.3-240.e98f832a:e98f832	READY	Сертификат	Конфиг
hydra	ucs-apps-1.installation.example.net	~13 days ago	50053, 65402,	1.7.1-77.54e3daba:54e3dab	READY	Сертификат	Конфиг
kronos	ucs-apps-1.installation.example.net	~6 days ago	9020, 65435,	1.7.3-180.be0223fe:be0223f	READY	Сертификат	Конфиг
marker	ucs-apps-1.installation.example.net	~1 day ago	5002, 65413,	1.39.1-794.ad60f18c:ad60f18	READY	Сертификат	Конфиг
mixer	ucs-apps-1.installation.example.net	~13 days ago	5001, 65405,	1.9.3-182.e754c92b:e754c92	READY	Сертификат	Конфиг
mosquito	ucs-apps-1.installation.example.net	~13 days ago	6672, 65406,	1.2.8-73.0ec42aa8:0ec42aa	READY	Сертификат	Конфиг
razor	ucs-apps-1.installation.example.net	~20 days ago	1441, 65420,	1.17.0-167.e160797b:e160797	READY	Сертификат	Конфиг
viper	ucs-apps-1.installation.example.net	~7 days ago	8181, 65408,	1.29.3-667.e4ba3cb5:e4ba3cb	READY	Сертификат	Конфиг
weaver	ucs-apps-1.installation.example.net	~13 days ago	7777, 65409,	1.8.2-90.44bf7736:44bf773	READY	Сертификат	Конфиг
hydra	ucs-calendar-1.installation.example.net	~13 days ago	50053, 65402,	1.7.1-77.54e3daba:54e3dab	READY	Сертификат	Конфиг
kex	ucs-calendar-1.installation.example.net	~18 hours ago	6788, 65422,	1.6.3-75.f2f8c9c0:	READY	Сертификат	Конфиг
kongur	ucs-calendar-1.installation.example.net	~17 hours ago	6789, 65401,	1.78.0-2319.32fc5d37:32fc5d3	READY	Сертификат	Конфиг
achill	ucs-catalog-1.installation.example.net	~13 days ago	4004, 65424,	1.7.8-214.614b8f90:614b8f9	READY	Сертификат	Конфиг
dafnis	ucs-catalog-1.installation.example.net	~13 days ago	6973, 65442,	1.4.5-139.f43e1a10:f43e1a1	READY	Сертификат	Конфиг
daidal	ucs-catalog-1.installation.example.net	~13 days ago	6970, 65425,	1.3.3-56.309f34f9:309f34f	READY	Сертификат	Конфиг

Рисунок 16 – Веб-интерфейс Kunkka

Для доступа может потребоваться логин «admin» и пароль, хранящийся в переменной **mailion_internal_web_auth.password**.

4.2.3 Prometheus

Prometheus – система мониторинга. Веб-интерфейс Prometheus доступен по адресу `http://prometheus.<infrastructure_inventory_hostname>/`.

Где `<infrastructure_inventory_hostname>` – FQDN хоста группы **ucs_infrastructure** (см. Рисунок 17).

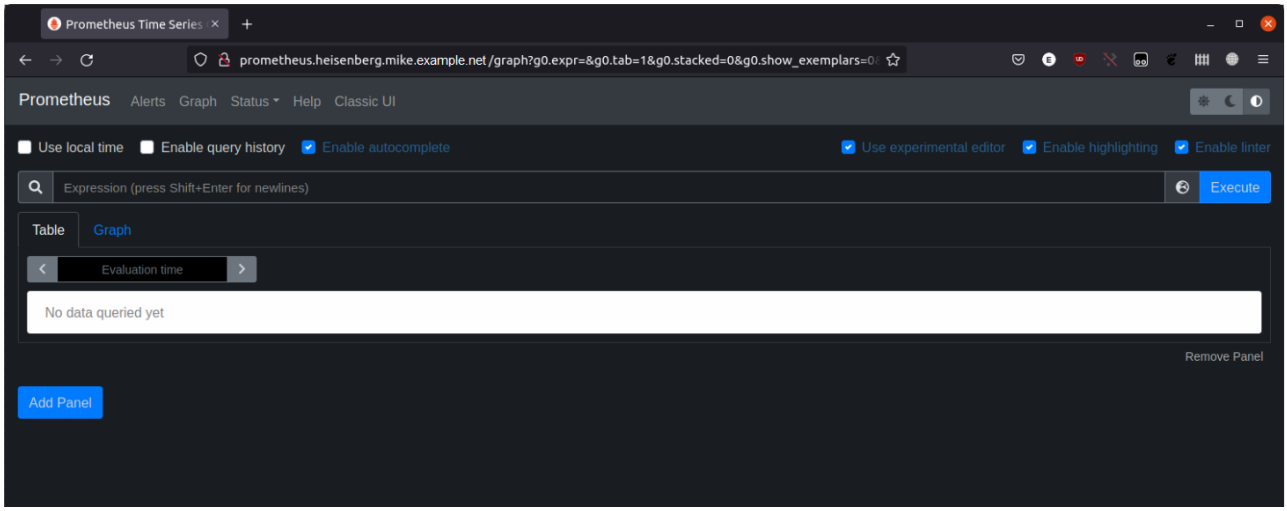


Рисунок 17 – Веб-интерфейс Prometheus

Для доступа может потребоваться логин «admin» и пароль, хранящийся в переменной **mailion_internal_web_auth.password**.

4.2.4 Alertmanager

Alertmanager – система алертинга. Веб-интерфейс Alertmanager доступен по адресу `http://alertmanager.<infrastructure_inventory_hostname>/`.

Где `<infrastructure_inventory_hostname>` – FQDN хоста группы **ucs_infrastructure** (см. Рисунок 18).

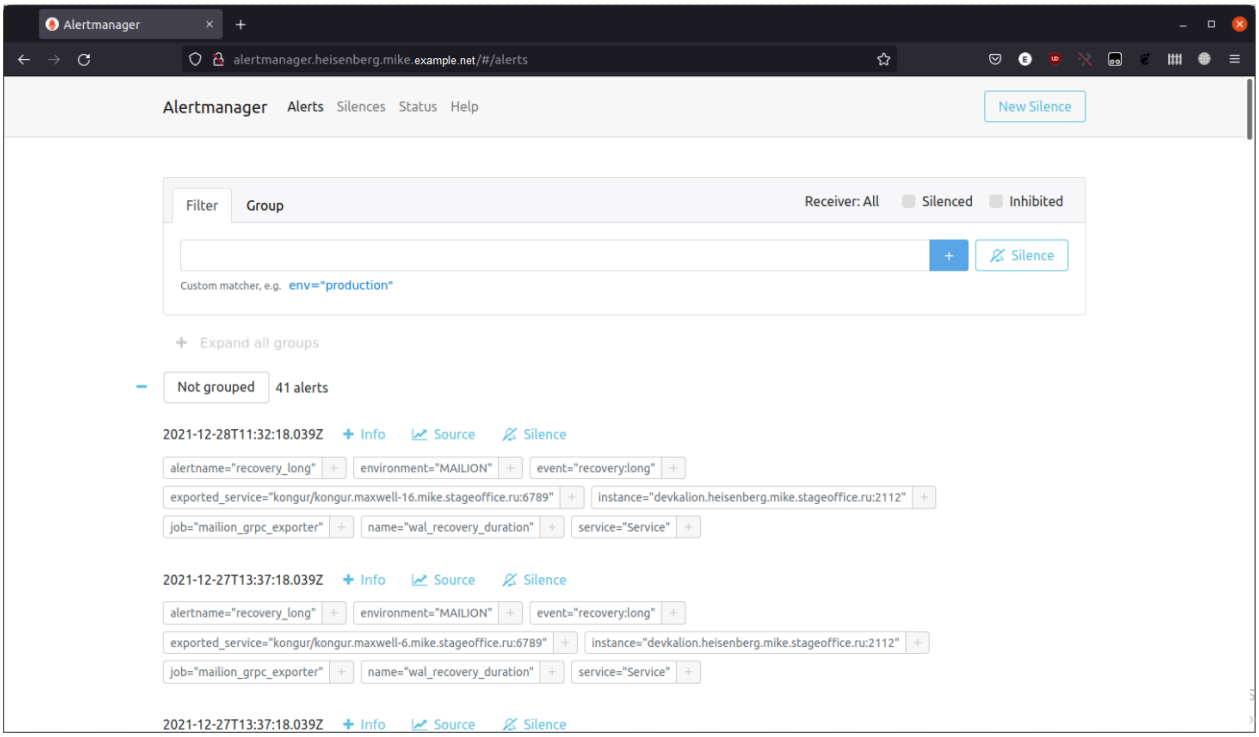


Рисунок 18 – Веб-интерфейс Alertmanager

Для доступа может потребоваться логин «admin» и пароль, хранящийся в переменной **mailion_internal_web_auth.password**.

4.2.5 Grafana

Grafana – система отображения метрик. Веб-интерфейс Grafana доступен по адресу `http://grafana.<infrastructure_inventory_hostname>`.

Где `<infrastructure_inventory_hostname>` – FQDN хоста группы **ucs_infrastructure** (см. Рисунок 19).

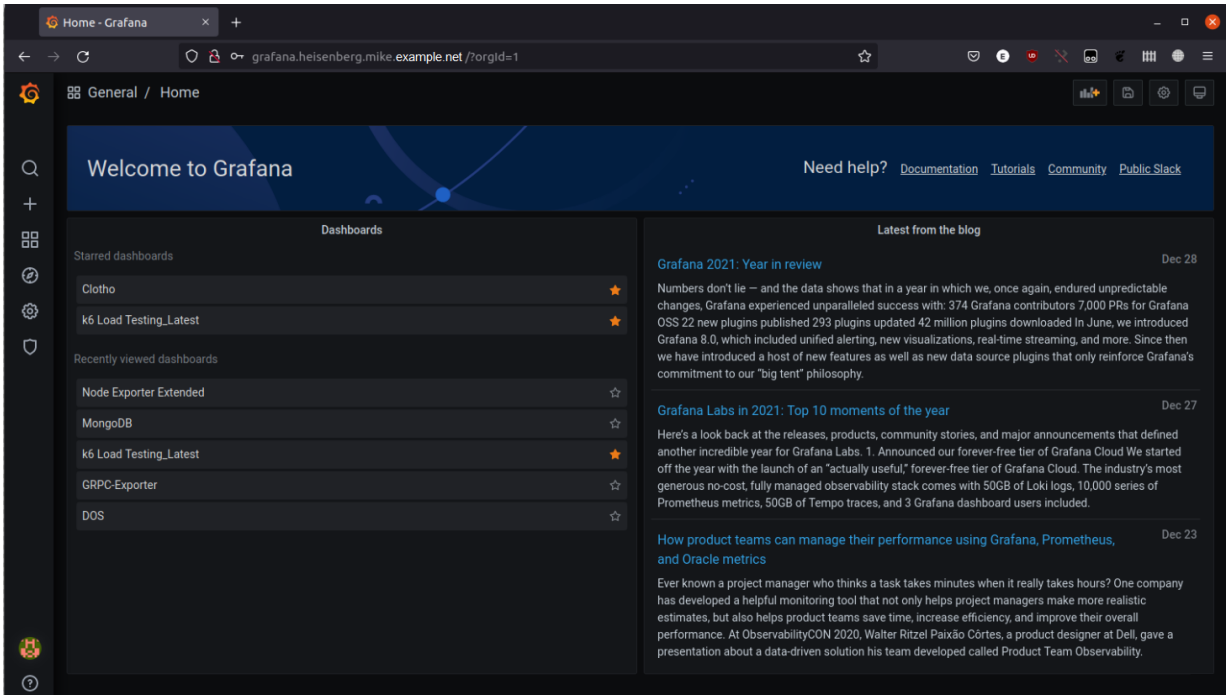


Рисунок 19 – Веб-интерфейс Grafana

Для доступа может потребоваться логин «admin» и пароль, хранящийся в переменной **grafana_admin_password**.

4.3 Настройка взаимодействия со службой каталогов

Для настройки интеграции с одним из каталогов (Microsoft Active Directory, FreeIPA, ALD Pro, РЕД АДМ и Samba DC) до инсталляции необходимо в соответствующем словаре указать уникальный ключ, в котором будут храниться параметры интеграции. Ключ можно сгенерировать с помощью команды «**pwgen 25 1**».

Настройки интеграции необходимо прописать в файле **group_vars/ucs_setup/main.yml**. Пользователь, который прописывается в секции **bind_user** в данном конфигурационном файле, должен иметь права доступа на чтение к дереву Microsoft Active Directory, FreeIPA, ALD Pro и Samba DC.

Корректно заполненные параметры приведены ниже.

```
integrations:
 microsoft:
   "IS7YluhZ318G7Sm89SkkfZbO":
     ads:
       base_dn: "dc=example,dc=net"
```

```
      bind_user: "example\\aduser"
      bind_password: "adUserPassword"
      name: "AD"
      servers:
        - endpoint: "dc.example.net:636"
          tls:
            ca_filename: "ca_example.net.pem"
            cert_file: ""
            key_file: ""
          use_tls: true
      use_dc: false
    exchanges:
      exchange_version: "Exchange2013_SP1"
      ca_filename: ""
freeipa:
  "zuif6jeifiQueey5ahWatoo0o":
    dcs:
      base_dn: "dc=ipa-example,dc=net"
      bind_user: "uid=admin,cn=users,cn=accounts,dc=ipa-example,dc=net"
      bind_password: "adminPassword"
      name: "FreeIPA"
      servers:
        - endpoint: "freeipa.ipa-example.net:389"
          tls:
            ca_filename: ""
            cert_file: ""
            key_file: ""
          use_tls: false
      use_dc: false
samba_dc:
  "PeZh0WisXah5thooWhoo9bgG":
    smb:
      base_dn: "DC=samba-dc-test,DC=example,DC=com"
      bind_user: "Administrator"
      bind_password: "ahTh6uu7sah4so1C"
      name: "SAMBA_DC"
      servers:
        - endpoint: "samba-dc-test.example.com:389"
          tls:
            ca_filename: ""
            cert_file: ""
```

```
            key_file: ""
          use_tls: false
      use_dc: false
 aldpro:
   "ALDh9ZisXah5thooWhoo9bgZ":
     ald:
       base_dn: "DC=domain,DC=test"
       bind_user: "admin"
       bind_password: "ahTh6uu7sah4so1C"
       name: "ALDPRO"
       servers:
         - endpoint: "aldpro-test.example.com:389"
           tls:
             ca_filename: ""
             cert_file: ""
             key_file: ""
           use_tls: false
       use_dc: false
```

Для включения интеграции с Microsoft Active Directory необходимо указать в групповых переменных:

```
mailion_integrations:
 microsoft: true
```

Для включения интеграции с FreeIPA необходимо указать в групповых переменных:

```
mailion_integrations:
 freeipa: true
```

Для включения интеграции с ALD Pro необходимо указать в групповых переменных:

```
mailion_integrations:
 aldpro: true
```

Для включения интеграции с Samba DC необходимо указать в групповых переменных:

```
mailion_integrations:
 samba_dc: true
```

Поддержка каталога РЕД АДМ осуществляется без заполнения параметров в конфигурационном файле.

В настройках для Microsoft Active Directory добавлена возможность конфигурировать используемую версию Exchange. Для этого используется переменная **exchange_version**. Она будет влиять на поддерживаемую версию Exchange, с которой идут запросы в EWS API. Данная переменная находится в разделе **exchanges**.

```
microsoft:
   ..................
   ads:
   ..................
   exchanges:
     ...................
     exchange_version: "Exchange2013_SP1"
```

Доступны следующие варианты:

– "Exchange2010";

– "Exchange2010_SP1";

– "Exchange2010_SP2";

– "Exchange2013";

– "Exchange2013_SP1".

Если переменная не задана, то по умолчанию будет использовано значение "Exchange2013_SP1".

В настройках Exchange присутствует поле **tls_min_version**. Оно содержит минимальную приемлемую версию TLS для работы с сервисами.

Данная настройка является обязательной для установки (значение по умолчанию не задано), без нее сервисы работать не будут.

Расположение переменной в файле конфигурации:

```
integrations:
  ..................
  microsoft:
    ..................
    exchanges:
      ...................
      servers:
          tls_min_version: "..."
```

В настройках Exchange обязательным является поле **ca_filename**. Оно содержит имя файла сертификата, который необходимо скопировать в папку `~/install_mailion/certificates/` перед инсталляцией (см. раздел 2.2.4).

Расположение переменной **ca_filename** в файле конфигурации:

```
microsoft:
   ..................
   ads:
   ..................
   exchanges:
     ...................
     ca_filename: ""
```

4.4 Настройка антивирусного программного обеспечения

В ПО «Mailion» **Rspamd** поддерживает несколько сторонних антивирусных модулей, в том числе KSE (Kaspersky). Настройка данного модуля осуществляется через переменные роли **Rspamd**. Подробное описание этих ролей приведено в таблицах 51 и 52.

Таблица 51 – Настройка Rspamd role vars

Параметр	Пример заполнения	Описание
rspamd:		
kse_use_https:	false	Использование **https** для подключения к серверам Касперского
kse_endpoints:	[]	Адреса серверов Касперского для обновления сигнатур (Обязательно наличие инсталляции KSE внутри компании)
kse_timeout:	"5.0"	Максимальный период времени для сканирования объекта
kse_scan_mime_parts:	true	Включение сканирования вложений
kse_use_files:	false	Отключение file mode в пользу TCP Stream. Не рекомендуется менять значение на true, режим file mode используется только для случаев наличия быстрой **tmpfs**
kse_max_size:	2048000	Максимальный размер файла для сканирования

Включение модуля антивирусной защиты Kaspersky осуществляется через групповые переменные инсталлятора ПО «Mailion» при наличии установленного в компании Сервера управления «Касперский антивирус».

Таблица 52 – Настройка Rspamd role vars

Параметр	Пример заполнения	Описание
rspamd:		
kse_enabled	true	Включение модуля Касперский для **rsmapd**
kse_endpoints:	"kaspersky.example.net:8085"	Список серверов управления антивирусной защитой Касперский

В а ж н о – Продукт Kaspersky Scan Engine не является частью поставки ПО «Mailion».

4.5 Настройка сервиса imap

Для корректной работы сервиса imap необходимо убедиться, что файл конфигурации `/srv/docker/imap/conf/config.json` содержит следующие параметры:

```
{
...
"beef_client_cache": {"disable": true},
"tag_object_cache": {"disable": true},
...
"disable_audit": true,
...
}
```

4.6 Настройка сервиса Vault

Сервис хранения ключей Vault поддерживает многосерверный режим для обеспечения высокой доступности. Этот режим защищает от сбоев в работе за счет запуска нескольких серверов хранилища. Режим высокой доступности включается автоматически при использовании хранилища данных, которое его поддерживает.

Vault работает в такой схеме, когда все инстансы кластера развернуты и работоспособны, при этом только один инстанс активен (активный инстанс vault, все остальные standby – в режиме ожидания). Он принимает запросы на чтение/запись, остальные инстансы остаются в режиме ожидания и перенаправляют все запросы на активный инстанс. Если активный инстанс выходит из строя, кластер сам выбирает новый активный хост, и система продолжает работать.

Все данные (секреты) автоматически синхронизируются и хранятся на всех трех инстансах. Количество инстансов Vault в кластере должно быть нечетным.

4.6.1 Установка сервиса Vault

Необходимо установить Vault на хосты vault1, vault2, vault3, при этом сам Vault не запускать и не распечатывать.

Для этого необходимо установить и запустить первый инстанс Vault.

В а ж н о – Установка Vault-сервера **осуществляется до установки остальных компонент** ПО «Mailion» один раз, в дальнейшем не нужно выполнять установку Vault, если она уже была выполнена или если нет рекомендаций по переустановке.

4.6.1.1 Этапы установки

1. Подготовить DNS-запись, по которой будет происходить обращение к сервису Vault.
2. Убедиться в доступности портов 8200, 8201 или других, если планируется их использовать на машине, которая будет предназначена для развертывания Vault.
3. Необходимо подготовить три файла для корректной работы сервиса Vault. Все файлы должны быть выпущены на доменное имя, подготовленное в предыдущем пункте, либо должны поддерживать Wildcard SSL сертификат, в который входит доменное имя из предыдущего пункта.

Пример – Если доменное имя **vault.example.ru**, то сертификаты должны быть выпущены либо на домен **vault.example.ru**, либо на ***.example.ru**. В последнем случае допустимо использовать сертификаты, уже подготовленные для инсталляции Mailion (см. раздел 2.2.4):

- CA сертификат, подписанный доверенным удостоверяющим центром (необходимо использовать для корректной работы);
- сертификат сервера, подписанный подготовленным в предыдущем пункте приватным ключом CA;
- приватный ключ для сертификата из предыдущего пункта.

4. Подготовленные ранее сертификаты необходимо расположить в директории коллекции **nct.certs/roles/tls_certs/files/**. Данная директория будет создана после распаковки установщика.
5. Необходимо обновить файл **inventory** и указать в нем созданные файлы. Пример секции в конфигурационном файле:

```
vault_tls:
  enabled: true
  certs:
    ca_filename: "<Имя CA файла>"
    cert_filename: "<Имя файла сертификата сервера>"
    key_filename: "<Имя файла ключа сервера>"
```

6. Выполнить команду установки:

```
install-mailion playbooks/mailion/vault.yml --tags=mln_vault -i <Путь к файлу inventory>
```

7. Необходимо распаковать сервис Vault. Для этого перейти в веб-браузере по адресу Vault-сервиса с указанием порта и схемы (пример: https://vault.example.ru:8200). На странице будет предложено задать несколько параметров:
   - Key shares – количество ключей, которое будет сгенерировано;
   - Key threshold – количество ключей из сгенерированных, которое понадобится для распаковки Vault. Не может быть больше, чем Key shares.

8. Задать значения и инициализировать сервис. Будет предложено сохранить сгенерированные значения ключей для распаковки и токен для root-доступа на сервер в файл.

   В а ж н о – Необходимо обязательно сохранить файл! В случае рестарта сервиса Vault без ключей для распаковки его будет невозможно восстановить, так как все данные будут зашифрованы. Также для настройки понадобится root token, его можно будет перевыпустить, используя ключи для распаковки.

9. Ввести сохраненные ключи для распаковки, пока сервер не будет распакован полностью.

4.6.1.2 Настройка Vault AppRole и доступа к кластеру для приложений

Для настройки Vault AppRole и доступа к кластеру необходимо запустить команду:

```
install-mailion playbooks/mailion/vault.yml --tags=mln_vault_init -i <Путь к файлу inventory> -e vault_init_address=<Полный адрес до Vault-сервера вместе с портом и схемой> -e vault_init_token=<Root токен, сохраненный на этапе инициализации Vault-сервера>
```

Данная команда создает AppRole и необходимые политики доступа на Vault-сервере, также она инициализирует пустой секрет по нужному пути.

В выводе данной команды будет указан токен **APP_ROLE_TOKEN** для доступа на Vault-сервер для приложений ПО «Mailion», который нужно сохранить. Срок действия данного токена – 1 год. Для перевыпуска токена можно запустить команду еще раз.

4.6.1.3 Инициализация секретов

Чтобы создать список секретов, необходимо выполнить следующие действия:

1. Проанализировать файл inventory и сохранить результат в файл с помощью команды:

```
grep -rni 'vault:.*' <Путь к директории с inventory файлами> | grep -o 'vault:.*' | sed 's/vault://g' | tr -d '\"' |  sort -h | uniq > first.txt
```

2. Проанализировать файл inventory на предмет других секретов с помощью команды:

```
grep -rnio 'vault_secrets\[.*\]' <Путь к директории с inventory файлами>  | grep
-o '\[.*\]' | tr -d "[,']" | sort -h | uniq > second.txt
```

3. Сформировать финальный список секретов, которые необходимо внести в Vault. Для этого выполнить команду:

```
cat first.txt second.txt | sort -h | uniq > final_secret_list.txt
```

Сформированный файл будет содержать список секретов, которые необходимо внести в Vault. Значения для секретов заполняются самостоятельно.

4. Также необходимо проанализировать inventory файл на наличие открытых паролей, указанных в открытом виде. В случае наличия таковых, можно поменять значения для них на маскированные значения и добавлять свои секреты в Vault.
5. В веб-браузере зайти на сервис Vault, используя полный адрес с портом.
6. Авторизоваться, используя root токен, полученный на этапе инициализации сервиса Vault.
7. Перейти во вкладку **Secrets**, в списке секретов перейти на **mailion** и далее на **installation**. Путь для секретов – **mailion/installation**.
8. Нажать кнопку **Create new version** и заполнить в соответствии с полученными ранее секретами.
9. Создать секрет **vault_token** в качестве значения, указать токен для доступа приложений, полученный ранее на этапе настройки Vault AppRole (см. раздел 4.6.1.2).
10. Для удобства можно заполнить в виде файла в формате JSON. Для этого есть специальная кнопка **JSON**, нужно ее включить.

4.6.1.4 Настройка .ansible.cfg для доступа к развернутому Vault-серверу

Для настройки необходимо отредактировать файл **~/.ansible.cfg** на той машине, с которой планируется запускать установку ПО «Mailion», добавив следующую секцию:

```
[hashi_vault_collection]
token_path = /Users/user/projects/secrets/
token_file = vault.token # Внутри файла необходимо указать токен для приложений,
полученный ранее на этапе настройки Vault AppRole
```

```
url = https://vault.server.company:8200 # URL, где будет доступен hosted vault -
в случае с HA vault достаточно одного из инстансов
```

4.6.1.5 Подготовка inventory файла

Для дальнейшей установки ПО «Mailion» необходимо подготовить inventory файл. При использовании Vault необходимо использовать `main.yml.hosted_vault`. Данный файл конфигурациии достаточно хорошо документирован, описание использования каждой секции подробно описано в комментариях.

Пример:

```
## ANSIBLE configuration
## remote SSH user with correct permissions
ansible_user: "root"
################################################################################
#####################
# данный файл содержит актуальный пример настроек переменных
# в случае установки Mailion вместе с hosted vault
################################################################################
###########

################################################################################
###########
# данная секция обеспечивает
# интеграцию ansible с hosted vault сервером
# для интеграции
# необходимо включить переменные:
# use_hashi_vault_secrets,
# use_hashi_vault_ad_secrets
.............................
```

4.6.2 Установка на другие хосты

Установка на другие хосты (vault2, vault3) осуществляется стандартным способом скачивания Vault-дистрибутива с docker-контейнера, на котором запущен первый Vault-инстанс:

```
ssh infra # зайти на машину, на которой запущен докер-контейнер с первым Vault-инстансом
sudo docker cp vault:/usr/local/bin/vault /tmp/vault
sudo chmod a+r /tmp/vault
exit
ssh vault2
scp infra:/tmp/vault vault
sudo mv /tmp/vault /usr/local/bin/
./vault --version
```

4.6.3 Создание доменных имен

Опционально: для каждого из хостов на DNS-серверах разворачиваемой инфраструктуры создать доменные имена:

– vault1.stageoffice.ru;

– vault2.stageoffice.ru;

– vault3.stageoffice.ru.

Для этого перед установкой ПО «Mailion» необходимо добавить в файл (пример: ./папка_инсталяции/group_vars/ucs_Имя_Стенда/main.yml) следующие опции:

```
- type: "transparent"
    zone: "vault1.stageoffice.ru"
    local_data:
      - domain: "vault1.stageoffice.ru"
        type: "A"
        ip: "192.168.0.1"
  - type: "transparent"
    zone: "vault2.stageoffice.ru"
    local_data:
      - domain: "vault2.stageoffice.ru"
        type: "A"
```

```
      ip: "192.168.0.2"
  - type: "transparent"
    zone: "vault3.stageoffice.ru"
    local_data:
      - domain: "vault3.stageoffice.ru"
        type: "A"
        ip: "192.168.0.3"
```

На серверах с Vault рекомендуется добавить в файле **/etc/hosts** следующие записи:

```
192.168.0.1 vault1.stageoffice.ru
192.168.0.2 vault2.stageoffice.ru
192.168.0.3 vault3.stageoffice.ru
```

Секции IP-адресов необходимо установить на соответствующие устанавливаемой конфигурации.

4.6.4 Генерация CA сертификата

Необходимо выпустить Wildcard SSL сертификат под домен для инсталляции ПО «Mailion» в аккредитованном центре сертификации. Либо использовать уже имеющийся Wildcard SSL сертификат аккредитованного CA и формировать доменные имена третьего уровня исходя из имени домена, на который он был выдан.

В результате должны получиться три файла:

– server.crt;

– server.key;

– ca.pem.

4.6.5 Создание сертификатов для каждого инстанса

Для работы Vault необходимы сертификаты в формате PEM. Ключи могут уже быть в формате PEM, но им просто будет присвоено имя .crt или .key.

Если они начинаются с -----BEGIN и есть возможность прочитать их в текстовом редакторе (они используют base64, который читается в ASCII, а не в двоичном формате), то они находятся в формате PEM.

Если файлы в двоичном формате:

```
#для server.crt необходимо использовать:
openssl x509 -inform DER -outform PEM -in server.crt -out server_crt.pem

#для server.key необходимо использовать:
openssl rsa -inform DER -outform PEM -in server.key -out server_key.pem
```

Чтобы настроить параметр **tls_cert_file** в секции **listener** на использование сертификата CA, объедините основной сертификат (server.crt) и сертификат CA (ca.pem) в одном файле server.pem:

```
cat server.crt ca.pem > server.pem
```

В результате файл server.pem должен содержать сертификат и цепочку корневого сертификата:

```
cat server.pem
-----BEGIN CERTIFICATE-----
...
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
...
-----END CERTIFICATE-----
```

После этого необходимо скопировать сертификаты, созданные на предыдущем шаге, в пути установки Vault и изменить владельцев и права доступа:

```
cp ./server_key.pem ./server.pem ./ca.pem /opt/vault/tls
chown root:root /opt/vault/tls/ca.pem
chown root:root /opt/vault/tls/server.pem
chown root:vault /opt/vault/tls/server_key.pem
chmod 0644 /opt/vault/tls/ca.pem
chmod 0644 /opt/vault/tls/server.pem
chmod 0644 /opt/vault/tls/server_key.pem
```

В а ж н о – Для управления верификацией используется переменная **othrys_insecure_skip_verify: true**. Значение **false** включает верификацию недоверенных сертификатов, значение **true** игнорирует ее.

4.6.6 Настройка конфигурационного файла Vault для каждого инстанса

Для каждого из хостов, где установлен Vault необходимо создать один и тоже конфигурационный файл с разницей только в том, что необходимо указать доменное имя хоста и IP-адрес, по которому Vault будет доступен.

В а ж н о – Во всех секциях, где необходимо указать TLS сертификаты, нужно указать сертификат/ключ, а также CA сертификат, созданные на предыдущем шаге.

Для первого инстанса Vault, запущенного, как docker-контейнер, предварительно рекомендуется сделать резервную копию директории **/srv/docker/vault**.

Далее необходимо отредактировать конфигурационный файл по пути **/srd/docker/vault/conf/config.hcl** способом, аналогичным другим инстансам. После того как он будет отредактирован, необходимо перезапустить контейнер с помощью команды **sudo docker restart vault**.

```
ssh infra # машина в кластере Mailion, на которой запущен первый Vault-инстанс
cat << HERE > /srv/docker/vault/config/vault.hcl
cluster_addr = "https://192.168.0.1:8201
api_addr = "https://192.168.0.1:8200
disable_mlock = true
ui = true

 listener "tcp" {
  address = "0.0.0.0:8200"
  tls_client_ca_file = "/opt/vault/tls/ca.pem"
  tls_cert_file = "/opt/vault/tls/server.pem"
  tls_key_file = "/opt/vault/tls/server_key.pem"
 }

# секция raft содержит в себе ссылки на _все_ инстансы Vault,
# доступные в кластере (включая инстанс, который установлен на данном хосте)
 storage "raft" {
  path = "/opt/vault/data"
  node_id = "vault1.stageoffice.ru"

 retry_join {
  leader_tls_servername = "vault1.stageoffice.ru"
  leader_api_addr = "https://192.168.0.1:8200
```

```
  leader_ca_cert_file = "/opt/vault/tls/ca.pem"
  leader_client_cert_file = "/opt/vault/tls/server.pem"
  leader_client_key_file = "/opt/vault/tls/server_key.pem"
 }
 retry_join {
  leader_tls_servername = "vault2.stageoffice.ru"
  leader_api_addr = "https://192.168.0.2:8200
  leader_ca_cert_file = "/opt/vault/tls/ca.pem"
  leader_client_cert_file = "/opt/vault/tls/server.pem"
  leader_client_key_file = "/opt/vault/tls/server_key.pem"
 }
 retry_join {
  leader_tls_servername = "vault3.stageoffice.ru"
  leader_api_addr = "https://192.168.0.3:8200
  leader_ca_cert_file = "/opt/vault/tls/ca.pem"
  leader_client_cert_file = "/opt/vault/tls/server.pem"
  leader_client_key_file = "/opt/vault/tls/server_key.pem"
 }
}
HERE
ssh vault2
[root@vault1] cat << HERE > /etc/vault.d/vault.hcl
cluster_addr  = "https://192.168.0.1:8201
api_addr      = "https://192.168.0.1:8200
disable_mlock = true

ui = true

listener "tcp" {
  address             = "0.0.0.0:8200"
  tls_client_ca_file  = "/opt/vault/tls/ca.pem"
  tls_cert_file       = "/opt/vault/tls/server.pem"
  tls_key_file        = "/opt/vault/tls/server_key.pem"
}

# секция raft содержит в себе ссылки на _все_ инстансы Vault,
# доступные в кластере (включая инстанс, который установлен на данном хосте)
storage "raft" {
  path    = "/opt/vault/data"
  node_id = "vault2.stageoffice.ru"
```

```
  retry_join {
    leader_tls_servername   = "vault1.stageoffice.ru"
    leader_api_addr         = "https://192.168.0.1:8200
    leader_ca_cert_file     = "/opt/vault/tls/ca.pem"
    leader_client_cert_file = "/opt/vault/tls/server.pem"
    leader_client_key_file  = "/opt/vault/tls/server_key.pem"
  }
  retry_join {
    leader_tls_servername   = "vault2.stageoffice.ru"
    leader_api_addr         = "https://192.168.0.2:8200
    leader_ca_cert_file     = "/opt/vault/tls/ca.pem"
    leader_client_cert_file = "/opt/vault/tls/server.pem"
    leader_client_key_file  = "/opt/vault/tls/server_key.pem"
  }
  retry_join {
    leader_tls_servername   = "vault3.stageoffice.ru"
    leader_api_addr         = "https://192.168.0.3:8200
    leader_ca_cert_file     = "/opt/vault/tls/ca.pem"
    leader_client_cert_file = "/opt/vault/tls/server.pem"
    leader_client_key_file  = "/opt/vault/tls/server_key.pem"
  }
}
HERE
```

4.6.7 Рестарт, распечатка первого инстанса Vault

Когда конфигурационные файлы готовы, необходимо вернуться на первый узел (vault1) и запустить сервис Vault с помощью команды:

```
ssh infra
docker restart vault
#  зайти в web-интерфейс и распечатать
```

4.6.8 Запуск и распечатка остальных инстансов Vault

Для всех остальных нод кластера необходимо запустить и распечатать сервис Vault.

В а ж н о – Инициализация для данных инстансов не требуется.

```
ssh vault2
sudo apt-get install screen
screen # мы будем использовать screen для запуска Vault в режиме сервиса
# вы также можете создать systemd unit для этого и запускать Vault-сервис через
systemd
# следуйте руководству вашего Linux-дистрибутива о том, как создавать новые
systemd сервисы

sudo vault server
^D # выход из screen сессии
vault operator unseal
```

Для распечатки необходимо следовать процедуре, описанной в разделе 4.6.7. Использовать те же ключи распечатки, которые использовали для распечатки первого инстанса. Пример **systemd** конфигурации для сервиса Vault (выполняется с помощью команды **nano /etc/systemd/system/vault.service**):

```
[Unit]
Description=a tool for managing secrets
Documentation=https://vaultproject.io/docs/
After=network.target
ConditionFileNotEmpty=/etc/vault.d/vault.hcl

[Service]
User=vault
Group=vault
ExecStart=/usr/local/bin/vault server -config=/etc/vault.d/vault.hcl
ExecReload=/usr/local/bin/kill --signal HUP $MAINPID
CapabilityBoundingSet=CAP_SYSLOG CAP_IPC_LOCK
Capabilities=CAP_IPC_LOCK+ep
SecureBits=keep-caps
NoNewPrivileges=yes
KillSignal=SIGINT
```

```
[Install]
WantedBy=multi-user.target
```

Запуск через systemd:

```
systemctl daemon-reload
systemctl enable --now vault.service
systemctl start  vault.service
systemctl status vault.service
```

4.6.9 Верификация работы кластера

На данном этапе сформирован кластер из трех нод. Для верификации необходимо вернуться на вторую ноду и проверить состояние кластера.

Необходимо авторизоваться с токеном, который был получен ранее:

```
ssh vault2
vault login
Token (will be hidden):
Success! You are now authenticated. The token information displayed below
is already stored in the token helper. You do NOT need to run "vault login"
again. Future Vault requests will automatically use this token.
```

Затем проверить статус хранилища:

```
[root@vault1]# vault operator raft list-peers
Node                    Address             State       Voter
----                    -------             -----       -----
vault1.stageoffice.ru   192.168.0.1:8201    leader      true
vault2.stageoffice.ru   192.168.0.2:8201    follower    true
vault3.stageoffice.ru   192.168.0.3:8201    follower    true
```

По статусу видно три сервера, один из которых в статусе лидера, а два других – ведомые.

4.7 Настройка аудита событий в формате CEF

Чтобы настроить регистрацию событий пользователя для аудита в формате CEF, необходимо внести в конфигурационный файл (по умолчанию `~/install_mailion/group_vars/ucs_setup/main.yml`) следующие изменения:

1. Включить функцию регистрации событий в формате CEF:

```
mailion_global_cef_enabled: true
```

2. Указать для сервиса **homeros** уровень журналирования TRACE, добавив следующий параметр:

```
homeros_log_level: "trace"
```

   П р и м е ч а н и е – Если подключение настраивается на внешнюю SIEM-систему, то выполнять пункт 2 не требуется.

3. Указать адрес и порт внешней SIEM-системы с помощью следующего параметра:

```
homeros_cef_siem_endpoints:
  - "<адрес>:<порт>"
```

   Если необходимо, чтобы события сохранялись в журнал сервиса **homeros**, следует указать адрес и порт, который будет настроен на контейнер **syslog_ng** (по умолчанию 172.17.0.1:514), при этом события для аудита будут записываться на машину группы хостов **ucs_infrastructure** в каталог `~/srv/logs/ucs_setup/homeros/homeros.log`. Пример:

```
homeros_cef_siem_endpoints:
  - "172.17.0.1:514"
```

Если установка была сделана без этих изменений, то для применения настроек необходимо выполнить следующую команду из каталога `~/install_mailion`:

```
ansible-playbook -i hosts.yml playbooks/mailion.yml \
--tags homeros,house,cox \
--diff
```

4.8 Рекомендации по безопасности

Если система установлена не в закрытом контуре и брандмауэр разрешает осуществлять исходящие соединения в сеть Интернет, то на машине оператора рекомендуется прописать следующие настройки в конфигурационном файле `~/install_mailion/group_vars/<install_name>/main.yml`:

```
unbound_local_zones:
 - type: "transparent"
   zone: "grafana.com"
   local_data:
     - domain: "grafana.com"
       type: "A"
       ip: "192.168.115.63"

 - type: "transparent"
   zone: "raw.githubusercontent.com"
   local_data:
     - domain: "raw.githubusercontent.com"
       type: "A"
       ip: "192.168.115.63"

 - type: "transparent"
   zone: "api.segment.io"
   local_data:
     - domain: "api.segment.io"
        type: "A"
        ip: "192.168.115.63"

 - type: "transparent"
   zone: "maps.rspamd.com"
   local_data:
     - domain: "maps.rspamd.com"
        type: "A"
        ip: "192.168.115.63"
```

Вместо IP-адреса 192.168.115.63 необходимо указать IP-адрес любой машины из группы **ucs_infrastructure**.

Далее необходимо обновить параметры конфигурации сервиса **unbound**:

```
 ~/install_mailion#  ansible-playbook  -i  hosts.yml  playbooks/common.yml  --
tags=unbound --diff
```

4.8.1 Рекомендации по безопасности веб-интерфейса

В целях обеспечения безопасности рекомендуется установить запрет на индексацию поисковыми системами главной страницы веб-интерфейса Mailion. Для этого на машине оператора необходимо внести исправления в код сервиса **house** следующей командой:

```
# sed '/Pragma "no-cache"/a \        \X-Robots-Tag "none"' -i
~/install_mailion/collections/ansible_collections/nct/platform/roles/house/templ
ates/apps/ucs/*.conf.j2
```

В а ж н о – Восемь пробелов между символами \ и \ в команде должны быть сохранены (при копировании из PDF через буфер клавиатуры последовательные пробелы заменяются одним).

Затем необходимо выполнить повторное развертывание сервиса **house** следующей командой:

```
# ansible-playbook playbooks/mailion/frontend.yml -t house --diff
```

5 ПОДГОТОВКА К РАБОТЕ

5.1 Доступ к ПО «Mailion»

Пользователи получают доступ к ПО «Mailion» с помощью веб-браузера (см. раздел 1.4.2) или настольного приложения «МойОфис Почта».

5.2 Запуск системы

Для запуска ПО «Mailion» необходимо выполнить следующие действия:

1. Открыть веб-браузер при активном сетевом подключении.
2. Ввести адрес ПО «Mailion» в адресную строку веб-браузера. После этого осуществится переход к окну авторизации.
3. Выполнить авторизацию. Подробная информация об авторизации в ПО «Mailion» приведена в документе «Программное обеспечение «Корпоративная система электронной почты и планирования совместной работы команд «Mailion». Руководство оператора» RU.29144487.506900.001 34.

Для подготовки к работе с настольным приложением «МойОфис Почта» необходимо выполнить следующие шаги:

1. Проверить выполнение системных требований и, при необходимости, обратиться к системному администратору.
2. Установить следующее программное обеспечение:
   – КриптоПро CSP 5.0.12000;
   – Библиотеку КриптоПро PKCS#11;
   – КриптоПро ЭЦП Browser plug-in.

   После установки запустить приложение «Инструменты КриптоПро», ввести лицензию и установить сертификаты УЦ.

   Подробная информация по взаимодействию с КриптоПро CSP представлена в соответствующей эксплуатационной документации на изделие СКЗИ ЖТЯИ.00101-02.

3. Если подготовка к работе с приложением «МойОфис Почта» осуществляется на ОС Windows, в `registry` необходимо сделать следующие изменения: в ветке `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\CryptoPro\Cryptography\CurrentVersion\PKCS11\slot0` (для 64-разрядной ОС) или `HKEY_LOCAL_MACHINE\SOFTWARE\CryptoPro\Cryptography\CurrentVersion\PKCS11\slot0` (для 32-разрядной ОС) создать строковый параметр с именем **Firefox**, не меняя остальные значения.
4. Установить приложение «МойОфис Почта» так, как это описано в разделе 2.5.
5. Запустить приложение и ввести данные той учетной записи, от имени которой будет осуществляться работа на текущем компьютере.
6. Добавить личный сертификат авторизованного пользователя так, как это описано в разделе 2.1.1 документа «Программное обеспечение «Корпоративная система электронной почты и планирования совместной работы команд «Mailion». Руководство оператора» RU.29144487.506900.001 34.

5.3 Проверка работоспособности системы

ПО «Mailion» считается работоспособным, если в результате действий пользователя, изложенных в разделах 5.1 и 5.2, на экране монитора отобразилась стартовая страница для входа в ПО «Mailion» без выдачи сообщений о сбое в работе (см. Рисунок 20).

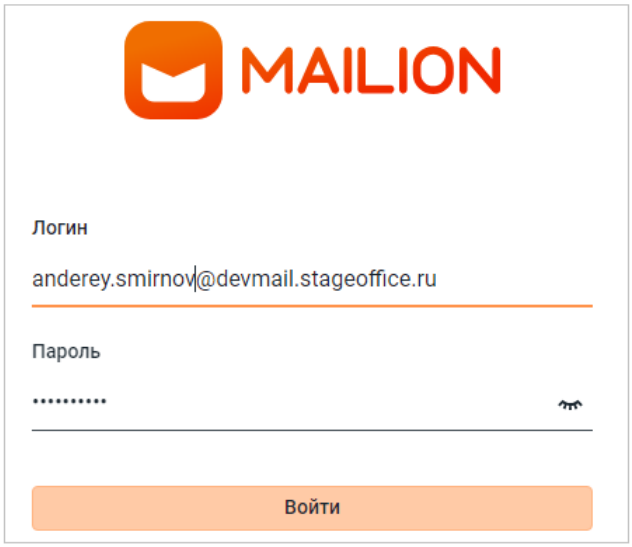


Рисунок 20 – Стартовая страница для входа в ПО «Mailion»

В случае нескольких неудачных попыток входа возможность логина будет заблокирована на 10 минут (см. Рисунок 21).

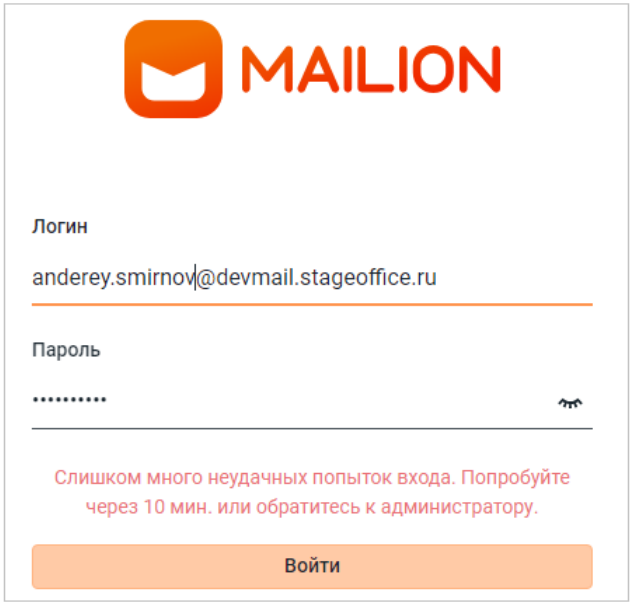


Рисунок 21 – Неудачная попытка входа

Приложение «МойОфис Почта» для ОС Windows считается работоспособным, если в результате действий, изложенных в разделе 2.5.1, на рабочем столе (см. Рисунок 22) и в главном меню ОС отображается ярлык, при активации которого программа корректно открывается без выдачи сообщений о сбое в работе.

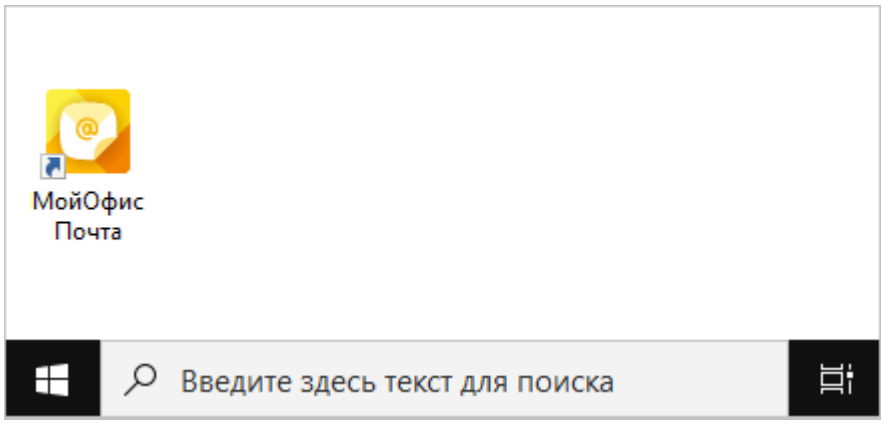


Рисунок 22 – Ярлык ПО «МойОфис Почта» на рабочем столе ОС Windows

Приложение «МойОфис Почта» для ОС Linux считается работоспособным, если в результате действий, изложенных в разделе 2.5.2, в меню приложений ОС (см. Рисунки 23, 24) отображается ярлык, при активации которого программа корректно открывается без выдачи сообщений о сбое в работе.

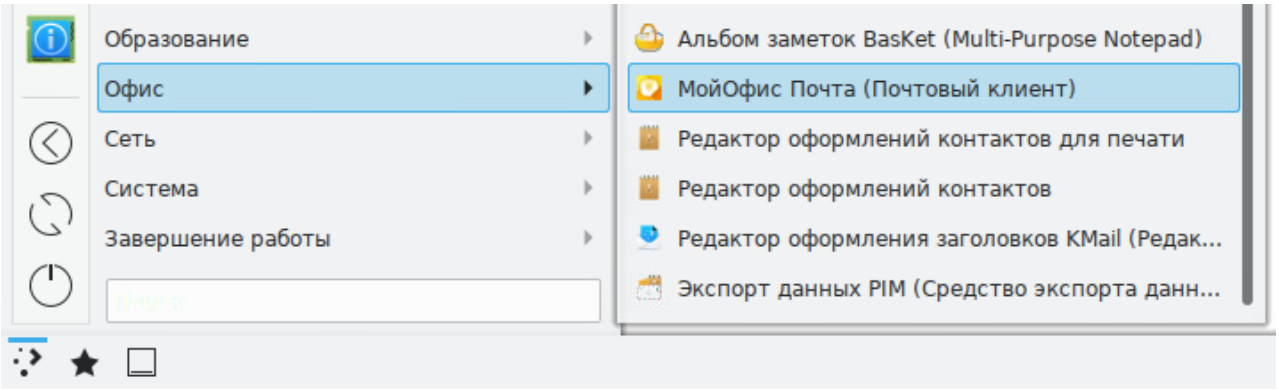


Рисунок 23 – Ярлык ПО «МойОфис Почта» в меню приложений ОС Linux

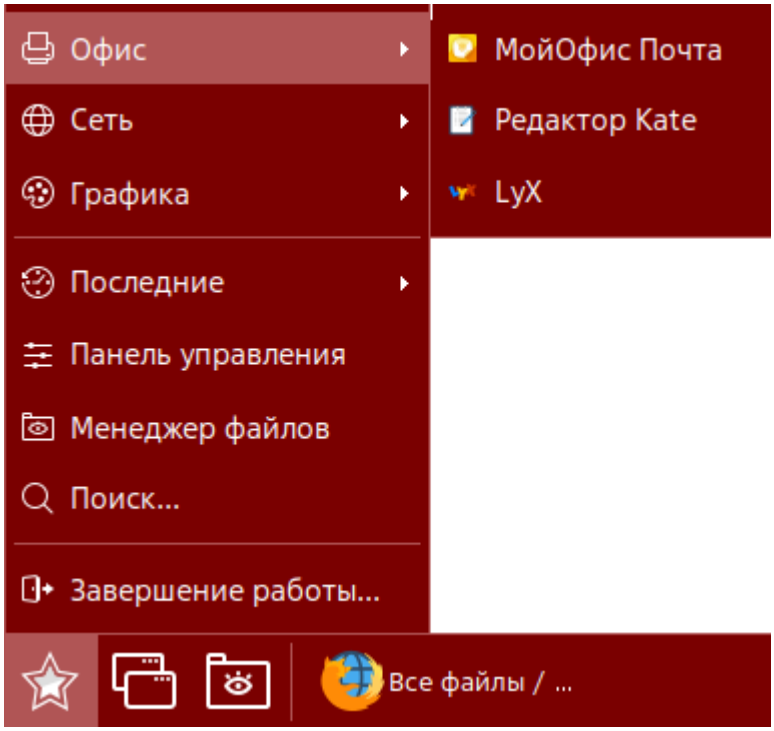


Рисунок 24 – Ярлык ПО «МойОфис Почта» в меню приложений ОС Astra Linux Special Edition

6 РАБОТА В ПАНЕЛИ АДМИНИСТРИРОВАНИЯ

После авторизации в ПО «Mailion» пользователю с правами администратора доступна работа в приложении **Панель администрирования** ПО «Mailion».

Для перехода к работе с панелью администрирования ПО «Mailion» необходимо нажать на значок  в меню приложений (см. Рисунок 25).

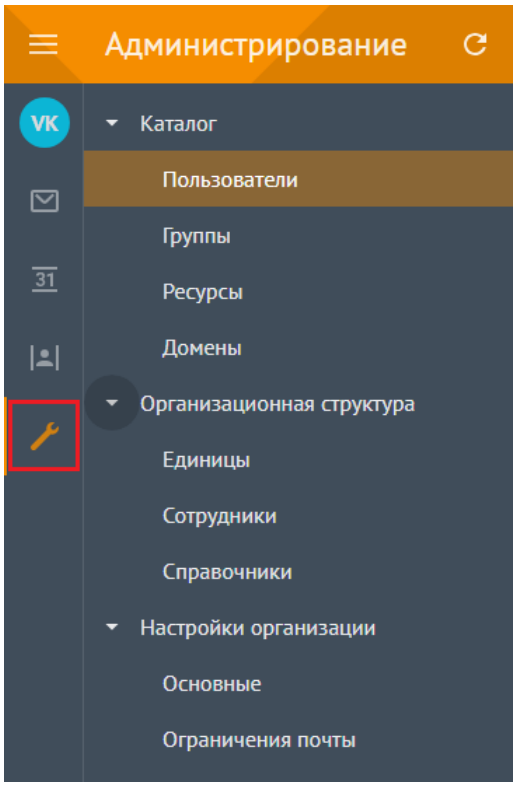


Рисунок 25 – Переход к **Панели администрирования**

6.1 Интерфейс приложения Панель администрирования

Интерфейс приложения **Панель администрирования** включает следующие элементы (см. Рисунок 26):

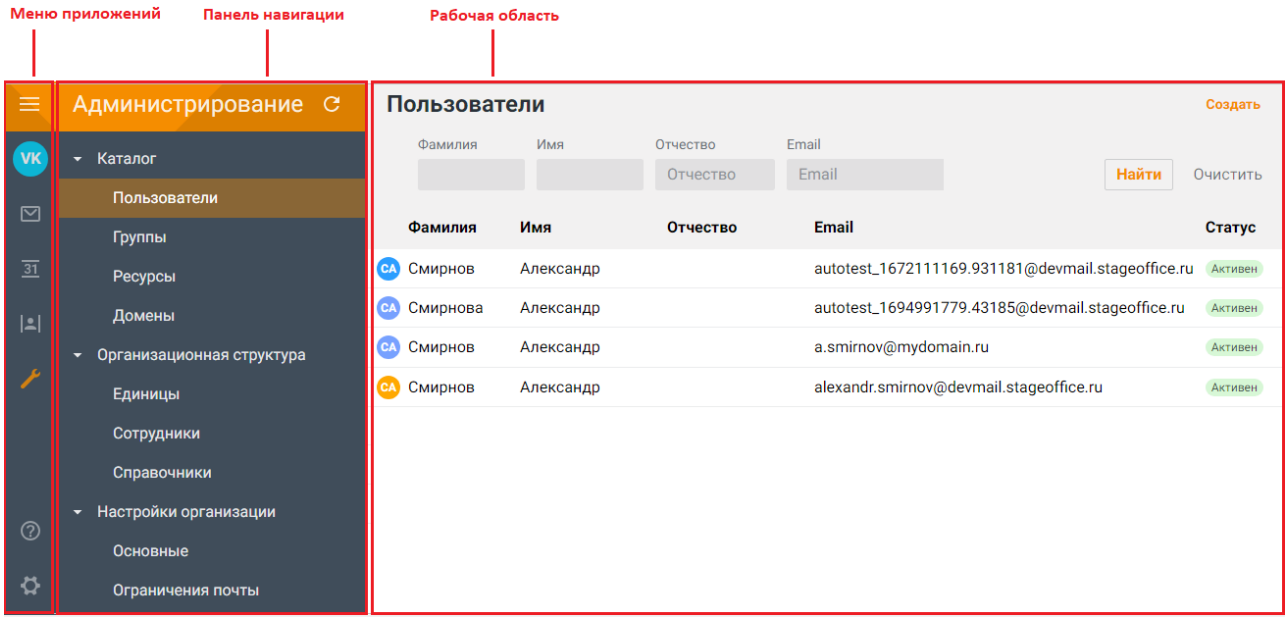


Рисунок 26 – Интерфейс приложения **Панель администрирования**

1. Меню приложений.
2. Панель навигации, содержащую:
   - вкладку **Каталог** с разделами:
     - Пользователи;
     - Группы;
     - Ресурсы;
     - Домены.
   - вкладку **Организационная структура** с разделами:
     - Единицы;
     - Сотрудники;
     - Справочники.
   - вкладку **Настройки организации** с разделами:
     - Основные;
     - Ограничения почты.

3. Рабочая область с содержимым выбранного раздела.

В верхней области **Панели администрирования** находится область с полями для поисковых запросов (см. Рисунок 27).

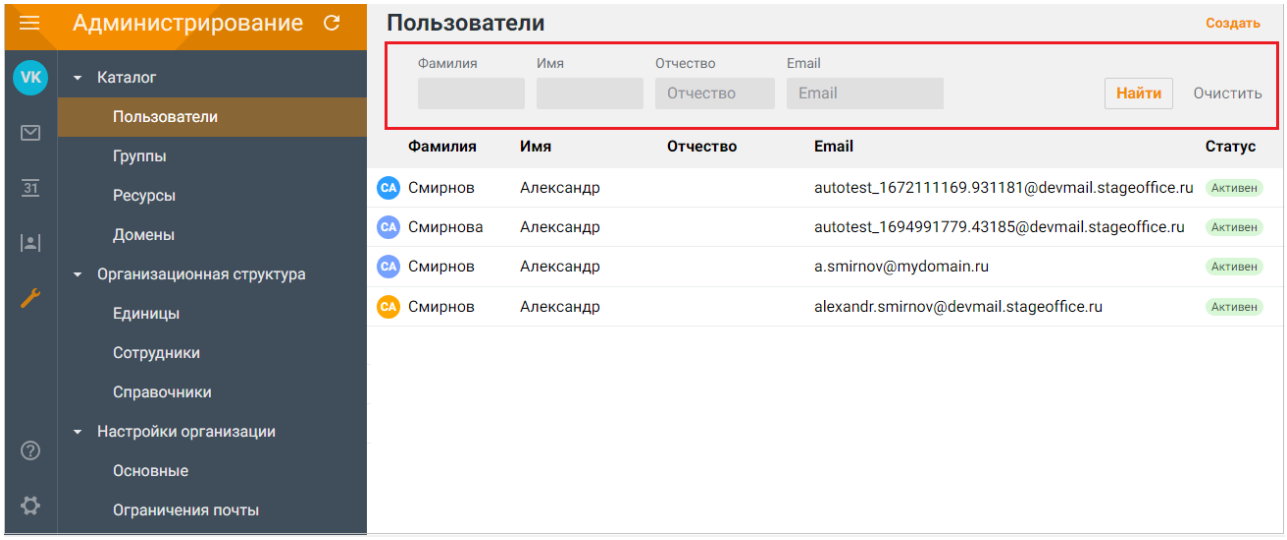


Рисунок 27 – Просмотр полей для поиска

При переходе на другую вкладку или отображении записи объекта результаты поиска сохраняются. Сброс результатов поиска осуществляется только при нажатии на кнопку **Очистить** или на кнопку **Найти** с пустым поисковым запросом.

6.2 Управление пользователями

6.2.1 Просмотр списка пользователей

Для просмотра списка пользователей необходимо авторизоваться в ПО «Mailion» и перейти в раздел **Пользователи**. На экране отобразится таблица со списком пользователей (см. Рисунок 28).

Таблица пользователей содержит следующие столбцы:

– Фамилия;
– Имя;
– Отчество;
– E-mail;
– Статус;
– Должность;

– Отдел;
– Город;
– Логин.

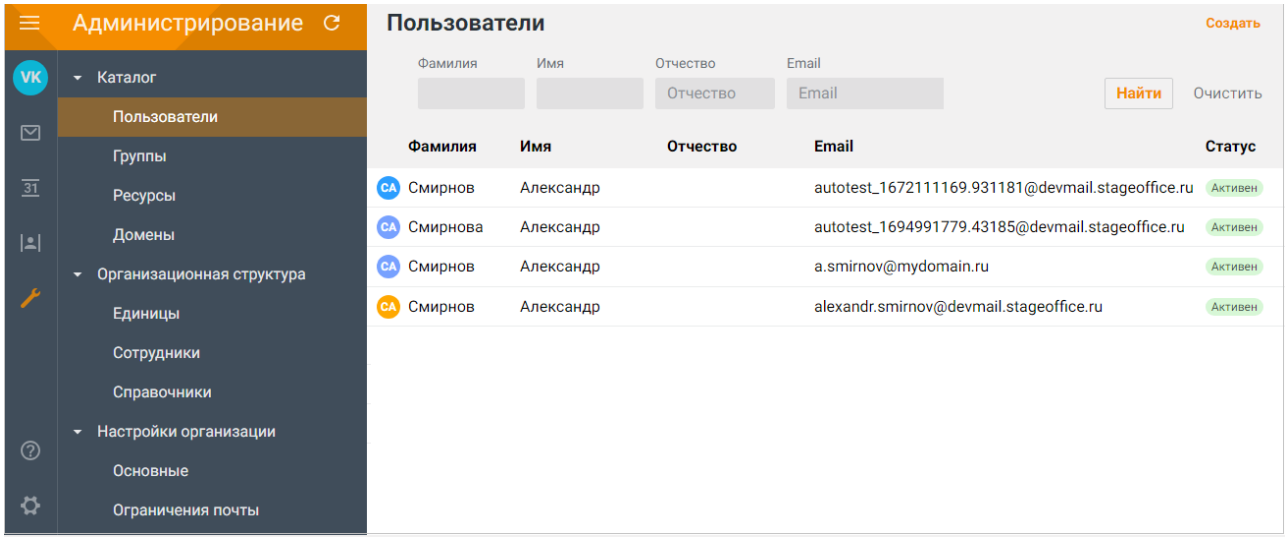


Рисунок 28 – Просмотр списка пользователей

По нажатию на строку откроется список групп пользователя.

6.2.2 Просмотр записи о пользователе

Чтобы просмотреть подробную запись о пользователе, необходимо нажать на соответствующую строку и перейти на вкладку **Данные** (см. Рисунок 29).

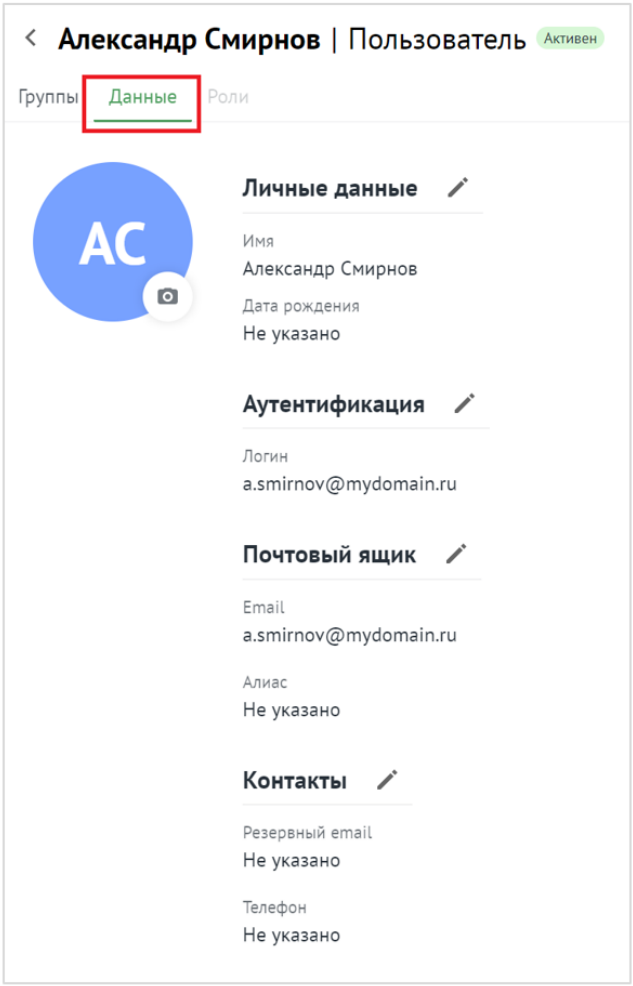


Рисунок 29 – Информация о пользователе на вкладке **Данные**

На этой же вкладке доступно редактирование записи о пользователе (см. раздел 6.2.12).

6.2.3 Создание пользователя

Для создания нового пользователя в разделе **Пользователи** необходимо нажать на кнопку **Создать** и в открывшейся форме выполнить следующие действия (см. Рисунок 30):

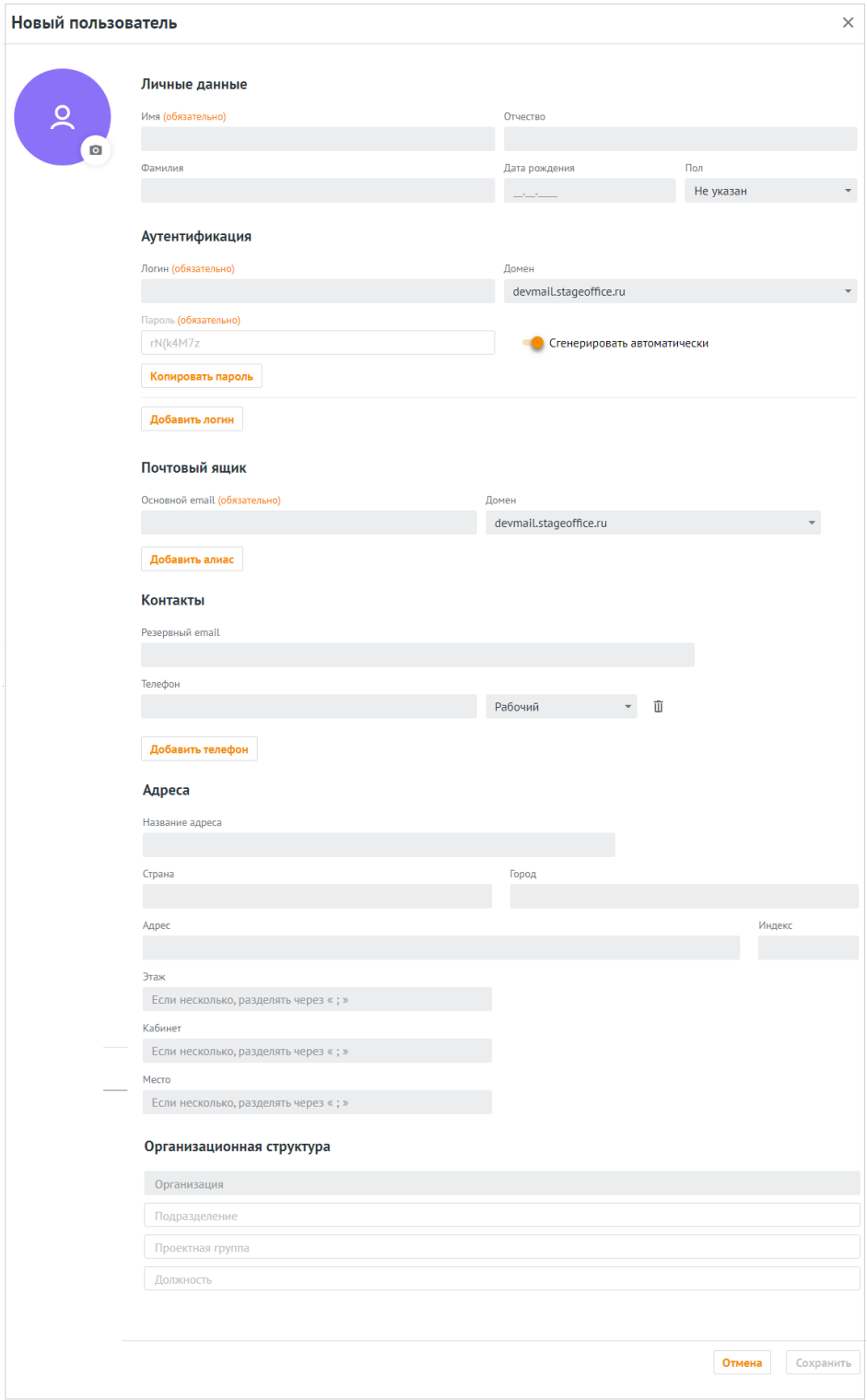


Рисунок 30 – Создание нового пользователя

1. Заполнить поля блока **Личные данные** вручную с клавиатуры:
   – Имя;
   – Фамилия (опционально);
   – Отчество (опционально);
   – Дата рождения (опционально);
   – Пол (опционально, выбрать из раскрывающегося списка).
2. Заполнить поля блока **Аутентификация** вручную с клавиатуры:
   – Логин. Можно ввести логин на латинице или кириллице;
   – Домен. Выбор из списка;
   – Пароль. Можно придумать новый пароль пользователя и подтвердить его либо использовать пароль, предложенный автоматическим генератором. Поле ручного ввода пароля содержит подсказку, описывающую текущую рекомендацию по парольной политике, установленной по умолчанию (см. раздел 1.7.10; см. Рисунок 31):

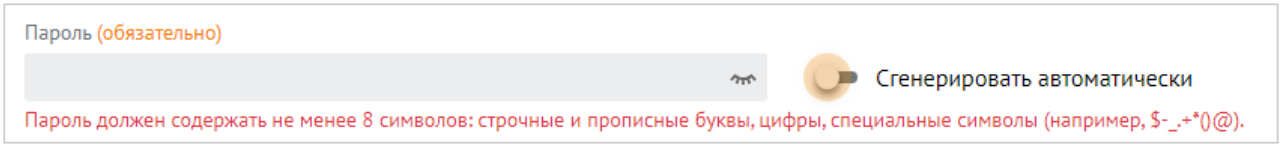


Рисунок 31 – Поле ввода пароля с подсказкой

П р и м е ч а н и е – Допускается использование не более 10 учетных записей для одного пользователя.

3. Заполнить поле блока **Почтовый ящик** вручную с клавиатуры:
   – Основной E-mail. Можно ввести E-mail на латинице или кириллице;
   – Домен. Выбор из списка;
   – Алиас. Для этого необходимо нажать на кнопку **Добавить алиас**.

   П р и м е ч а н и е – Допускается использование не более 11 адресов электронной почты для одного пользователя.

4. Заполнить поля блока **Контакты** (опционально) вручную с клавиатуры:
   – Резервный E-mail;
   – Телефон;
   – Тип телефона (выбрать из раскрывающегося списка).

П р и м е ч а н и е – Допускается использование не более 10 номеров телефонов различного назначения для одного пользователя.

5. Заполнить блок **Адреса** (опционально) вручную с клавиатуры:
   – Название адреса;
   – Страна;
   – Город;
   – Адрес;
   – Индекс;
   – Этаж;
   – Кабинет;
   – Место.
6. Заполнить поля блока **Организационная структура** (опционально) вручную с клавиатуры:
   – Организация;
   – Подразделение;
   – Проектная группа;
   – Должность.

   В а ж н о – Для заполнения полей данного блока необходимо предварительно создать объекты организационной структуры (см. раздел 6.6).
7. Нажать на кнопку **Сохранить** для создания пользователя с указанными данными или на кнопку **Отмена** для отмены создания пользователя.

В а ж н о – В случае сбоя в процессе добавления пользователя данные сохраняются в системе для того, чтобы впоследствии запись можно было просмотреть, дополнить, а также включить в группы рассылки. Если данные сохранятся не в полном объеме, то для полноценной работы в системе необходимо удалить и создать пользователя заново. Или заполнить недостающие данные с помощью расширенного администрирования (см. раздел 7).

6.2.4 Поиск пользователя

Для поиска пользователя необходимо выполнить следующие действия:

1. В разделе **Пользователи** заполнить одно или несколько полей **Фамилия**, **Имя**, **Отчество**, **Email** данными искомого пользователя. В каждое поле можно ввести данные полностью или только несколько символов, по которым осуществится поиск.
2. Нажать на кнопку **Найти** или клавишу **Enter**. На экране отобразится список найденных пользователей по заданным критериям (см. Рисунок 32).

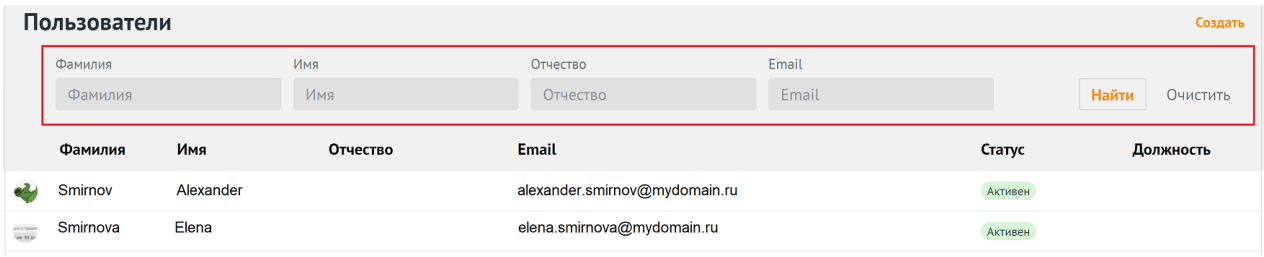


Рисунок 32 – Поиск группы рассылки

3. По нажатию на строку откроется список групп рассылок, в которых находится данный пользователь (см. Рисунок 33).

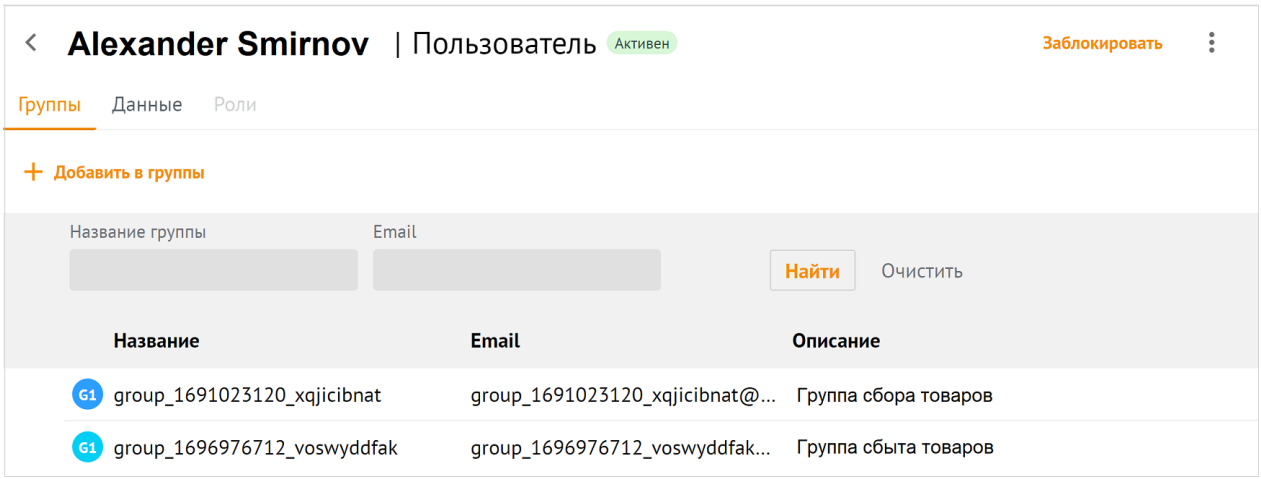


Рисунок 33 – Список групп рассылок пользователя

6.2.5 Блокировка пользователя

Для блокировки пользователя необходимо воспользоваться одним из следующих способов:

1. В списке пользователей выбрать курсором необходимую запись, нажать на возникшую в строке кнопку **Заблокировать** (см. Рисунок 34).

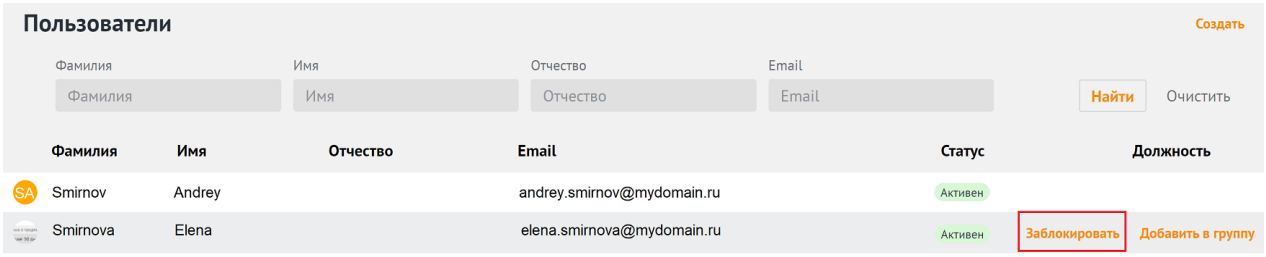


Рисунок 34 – Блокировка пользователя из списка пользователей

2. В списке пользователей нажать на строку пользователя, в открывшейся панели нажать кнопку **Заблокировать** (см. Рисунок 35).

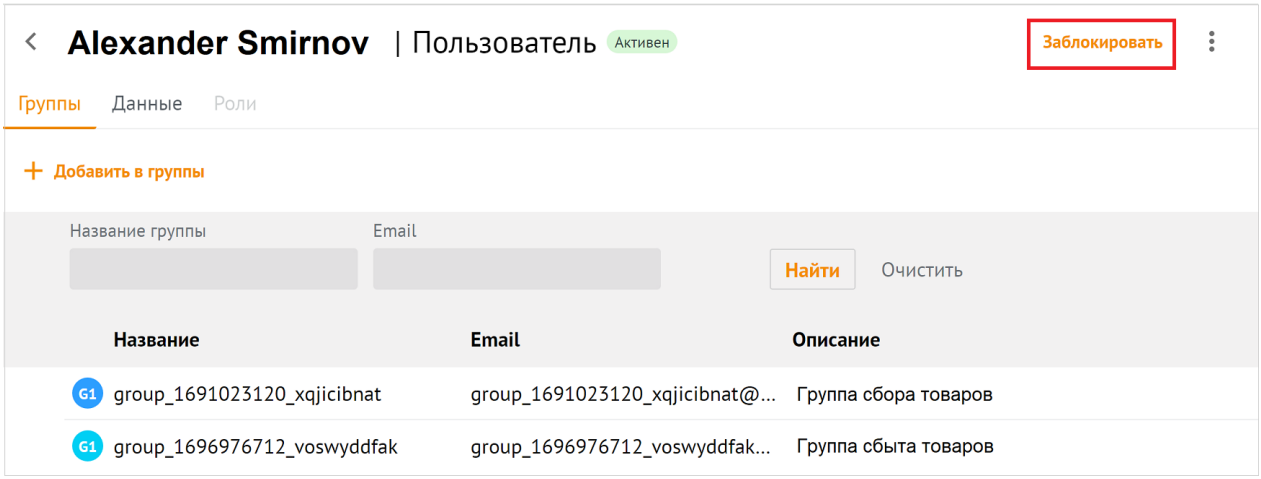


Рисунок 35 – Блокировка пользователя из панели пользователя

После нажатия на кнопку **Заблокировать** на экране возникнет панель для ввода комментария (см. Рисунок 36). После нажатия на кнопку **Заблокировать** пользователь будет заблокирован.

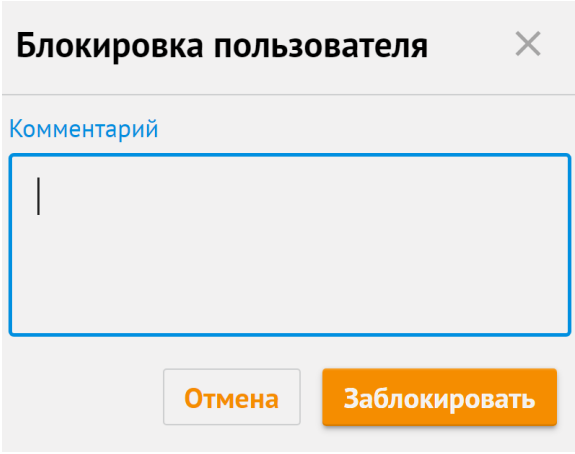


Рисунок 36 – Комментарий к блокировке пользователя

6.2.6 Разблокировка пользователя

Для разблокировки пользователя необходимо воспользоваться одним из следующих способов:

1. В списке пользователей выбрать курсором необходимую запись заблокированного пользователя, нажать на возникшую в строке кнопку **Разблокировать** (см. Рисунок 37).

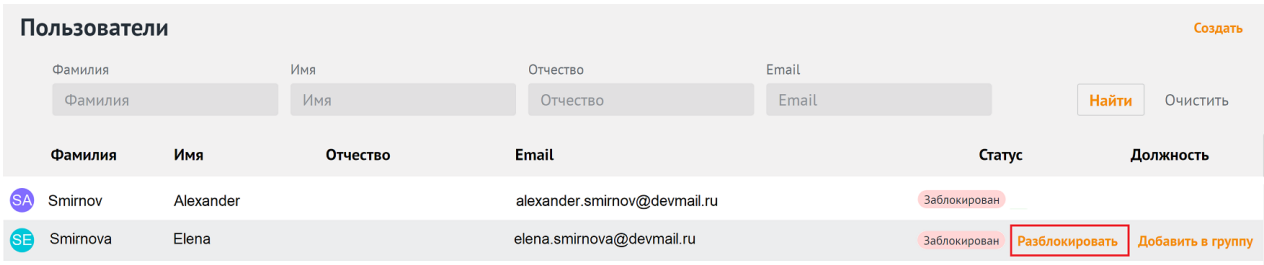


Рисунок 37 – Разблокировка пользователя из списка пользователей

2. В списке пользователей нажать на строку заблокированного пользователя, в открывшейся панели нажать кнопку **Разблокировать** (см. Рисунок 38).

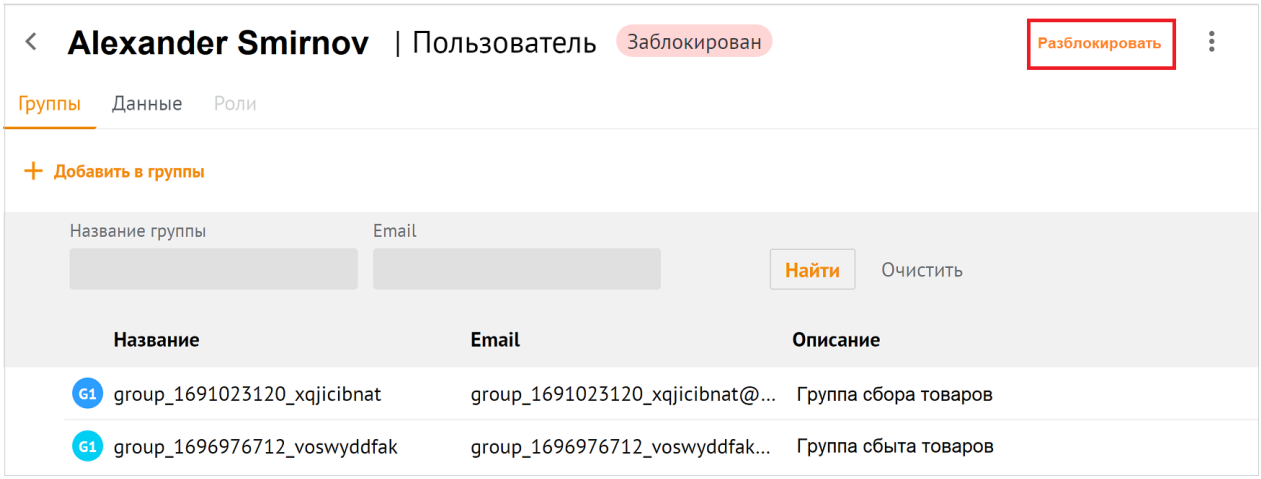


Рисунок 38 – Разблокировка пользователя из панели пользователя

После нажатия на кнопку **Разблокировать** на экране возникнет панель для подтверждения (см. Рисунок 39). После нажатия на кнопку **Разблокировать** пользователь будет активирован.

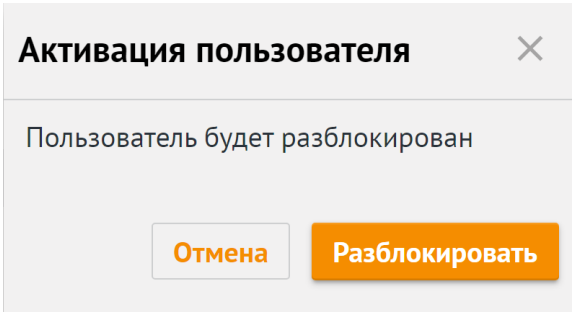


Рисунок 39 – Подтверждение разблокировки пользователя

6.2.7 Удаление пользователя

Для удаления пользователя необходимо выполнить следующие действия:

1. Выбрать пользователя из общего списка и нажать на значок ⋮.
2. Нажать на **Удалить** (см. Рисунок 40).

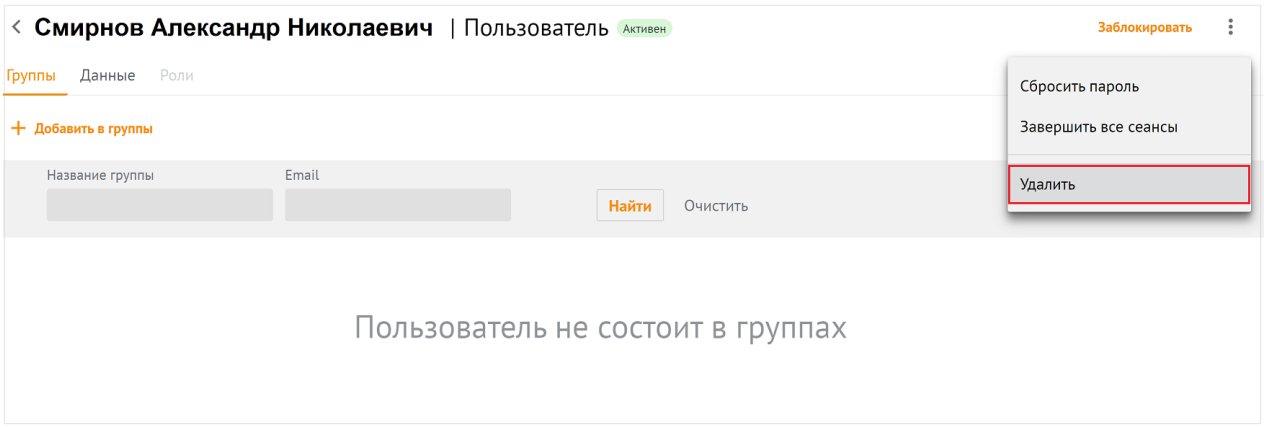


Рисунок 40 – Удаление пользователя

3. В окне подтверждения удаления необходимо нажать на кнопку **Удалить** (см. Рисунок 41).

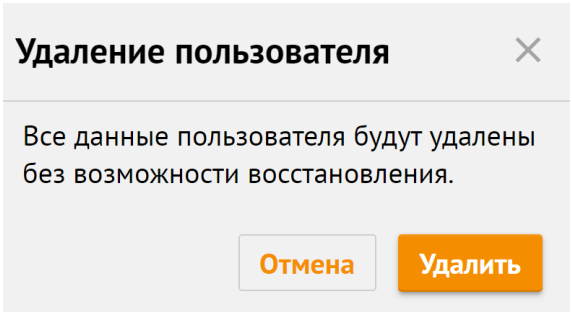


Рисунок 41 – Подтверждение удаления пользователя

6.2.8 Сброс пароля пользователя

Для сброса пароля пользователя необходимо выбрать пользователя из общего списка и нажать на **Сбросить пароль** (см. Рисунок 42).

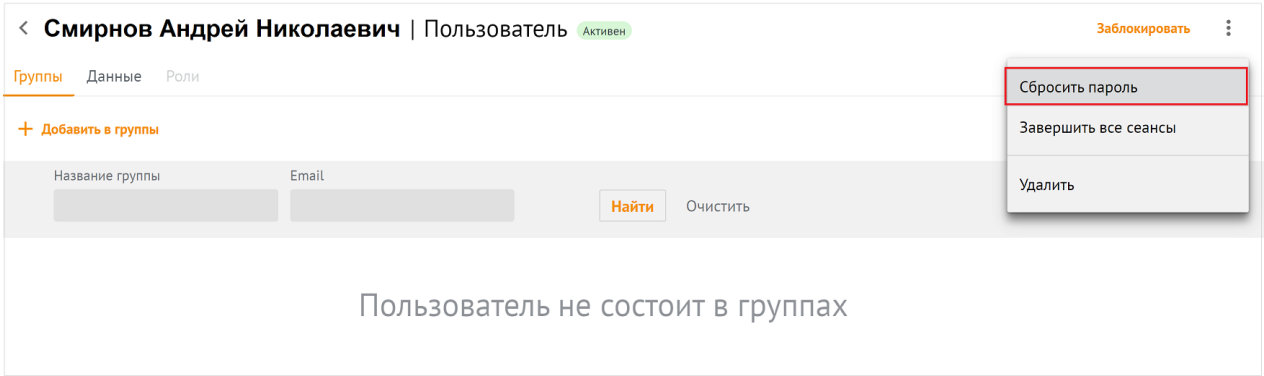


Рисунок 42 – Сброс пароля пользователя

После нажатия на кнопку **Сбросить пароль**, администратор должен ввести новый пароль пользователя и подтвердить его, либо использовать пароль, предложенный автоматическим генератором (см. Рисунок 43).

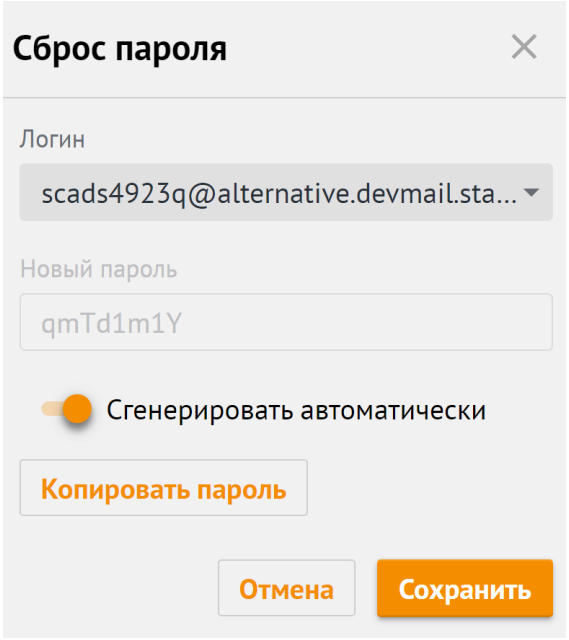


Рисунок 43 – Сгенерировать пароль автоматически

6.2.9 Завершение всех сеансов пользователя

Для завершения всех сеансов пользователя необходимо выбрать пользователя из общего списка и нажать на **Завершить все сеансы** (см. Рисунок 44).

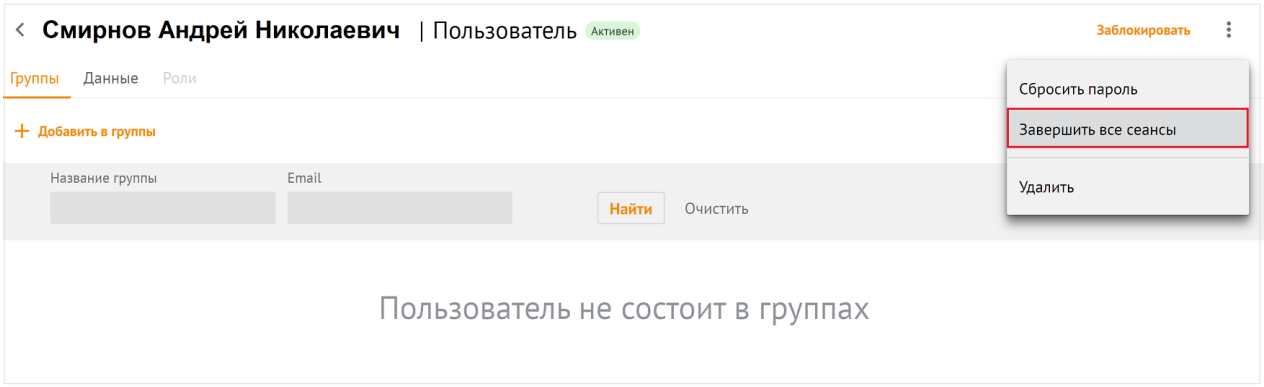


Рисунок 44 – Сброс пароля пользователя

После этого все сеансы пользователя на всех устройствах, кроме данного, будут завершены, а в левом нижнем углу окна отобразится сообщение **Все сеансы завершены**.

6.2.10 Добавление пользователей в группы рассылки

6.2.10.1 Добавление пользователя из панели свойств

Для добавления пользователя в группу рассылки из панели свойств пользователя необходимо выполнить следующие действия:

1. В списке пользователей выбрать пользователя, нажать **Добавить в группы** (см. Рисунок 45).

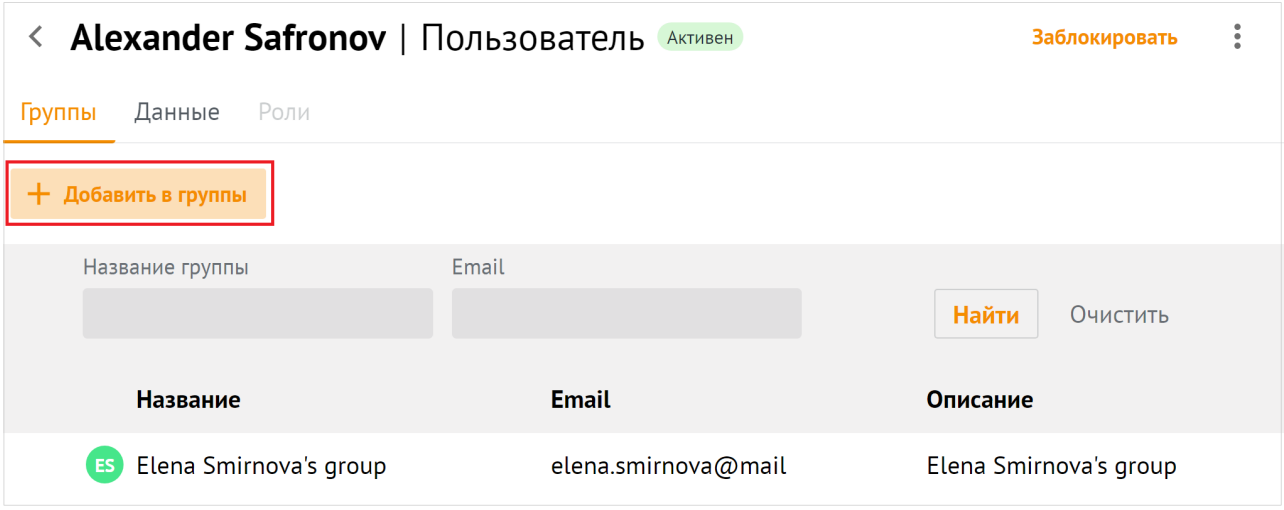


Рисунок 45 – Добавление пользователя в группу рассылки из списка пользователей

2. В появившемся списке групп выделить флагами необходимые группы, нажать **Добавить в группы** (см. Рисунок 46).

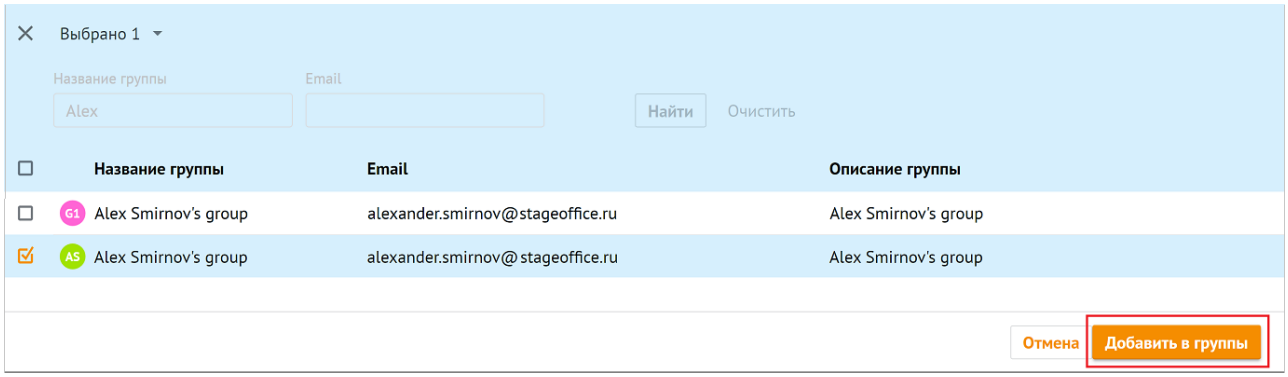


Рисунок 46 – Выбор групп рассылки для добавления пользователя

В а ж н о – Для добавления пользователя в несколько групп рассылки нужно установить галочку напротив нескольких групп рассылки.

В левом нижнем углу возникнет сообщение: **Пользователь добавлен в группы**.

6.2.10.2 Добавление пользователя из списка пользователей

Для добавления пользователя в группу рассылки из списка пользователей необходимо выполнить следующие действия:

1. В списке пользователей навести курсор на строку пользователя, выбрать **Добавить в группу** (см. Рисунок 47).

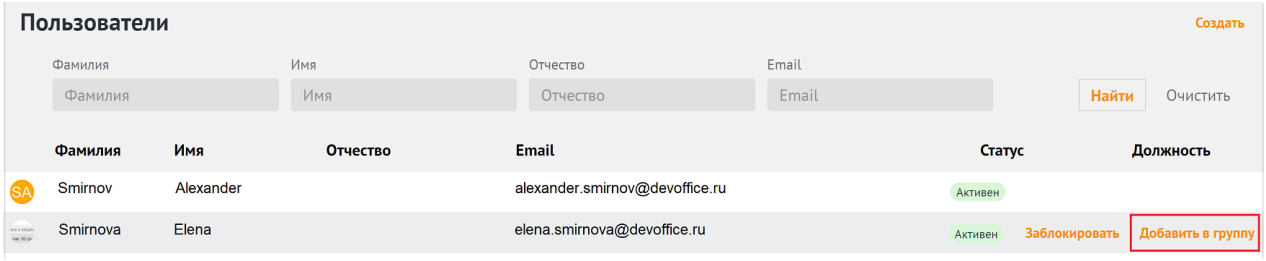


Рисунок 47 – Добавление пользователя в группу рассылки из списка пользователей

2. В появившемся списке групп выделить флагами необходимые группы, нажать **Добавить в группы** (см. Рисунок 48).

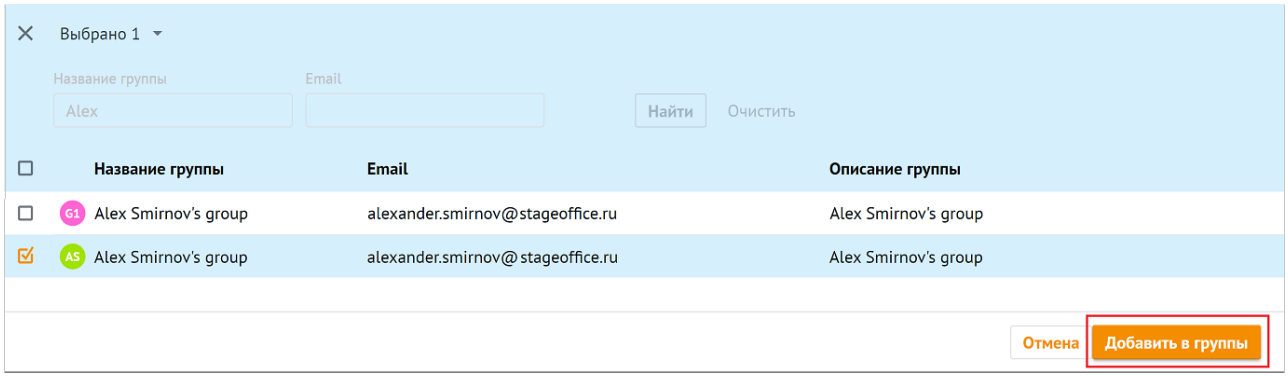


Рисунок 48 – Выбор групп рассылки для добавления пользователя

В а ж н о – Для добавления пользователя в несколько групп рассылки нужно установить галочку напротив нескольких групп рассылки.

В левом нижнем углу возникнет сообщение: **Пользователь добавлен в группы**.

6.2.10.3 Добавление пользователя из списка групп

Для добавления пользователя в группу рассылки из списка групп необходимо выполнить одно из следующих действий:

1. В списке групп навести курсор на интерсующую группу рассылки, нажать на **Добавить участников** (см. Рисунок 49).

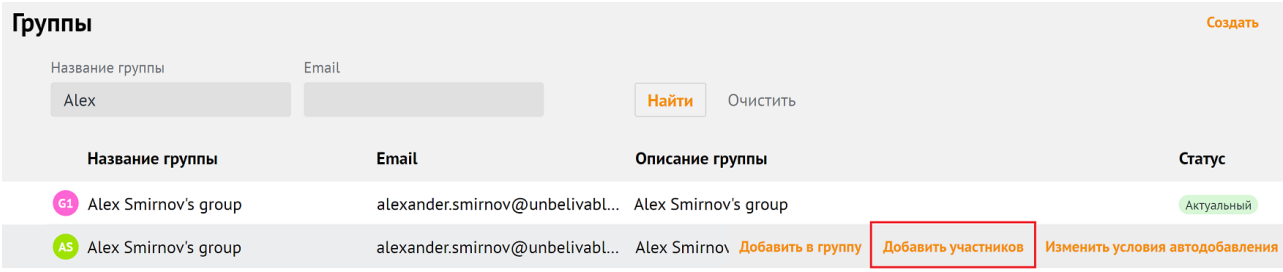


Рисунок 49 – Выбор участника для добавления в группы рассылки

2. На экране откроется панель **Добавление участников**. В открывшемся окне установить флажки для тех пользователей, которых требуется добавить в группу рассылки и нажать на кнопку **Добавить в группы**.

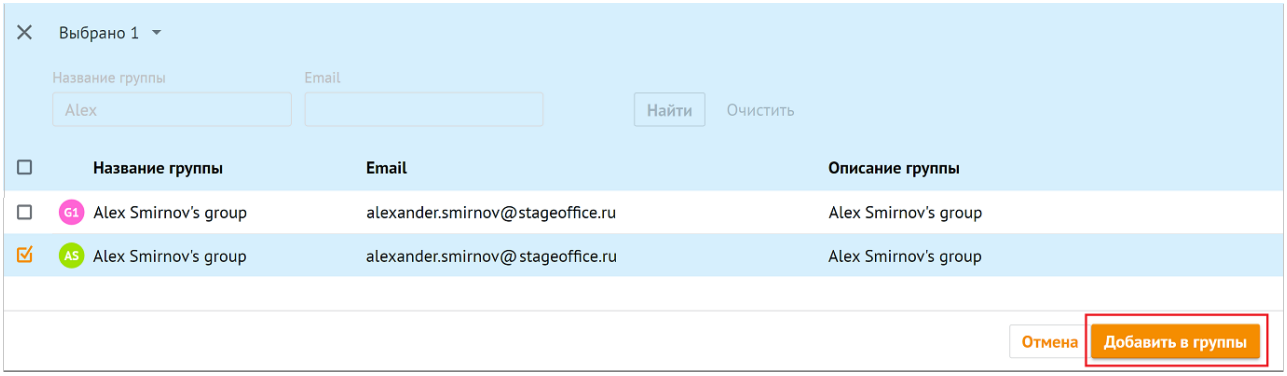


Рисунок 50 – Выбор групп рассылки для добавления пользователя

В а ж н о – Для добавления пользователя в несколько групп рассылки нужно установить галочку напротив нескольких групп рассылки.

В левом нижнем углу возникнет сообщение: **Пользователь добавлен в группы**.

6.2.11 Исключение пользователей из группы рассылки

Для исключения пользователя из группы рассылки необходимо воспользоваться одним из следующих способов:

1. Выбрать соответствующего пользователя в списке пользователей и нажать на кнопку **Удалить из группы** (см. Рисунок 51).

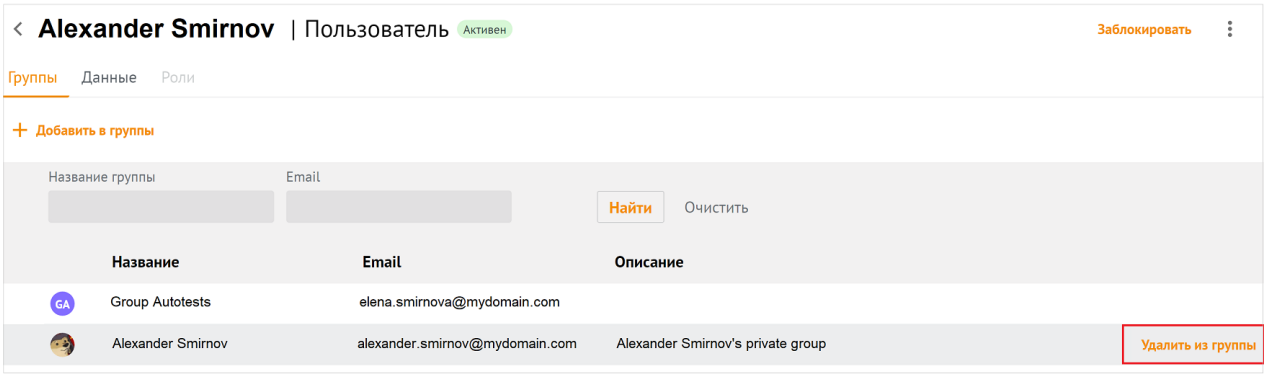


Рисунок 51 – Удаление участника из группы рассылки

2. Открыть группу рассылки, выбрать соответствующего пользователя в группе и нажать на кнопку **Удалить из группы** (см. Рисунок 52).

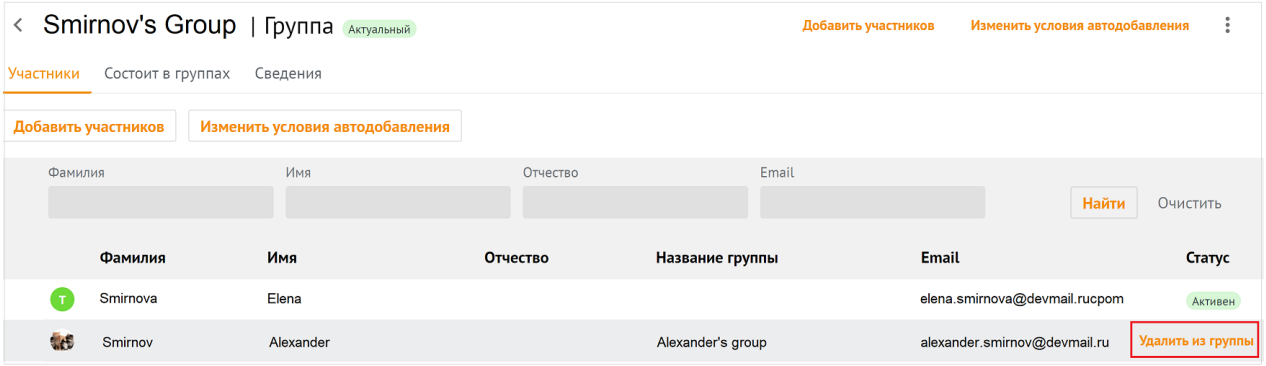


Рисунок 52 – Удаление участника из группы рассылки

В левом нижнем углу возникнет сообщение: **Участники удалены из группы**.

6.2.12 Редактирование данных пользователя

Для редактирования данных пользователя необходимо в разделе **Пользователи** перейти на вкладку **Данные** (см. Рисунок 53).

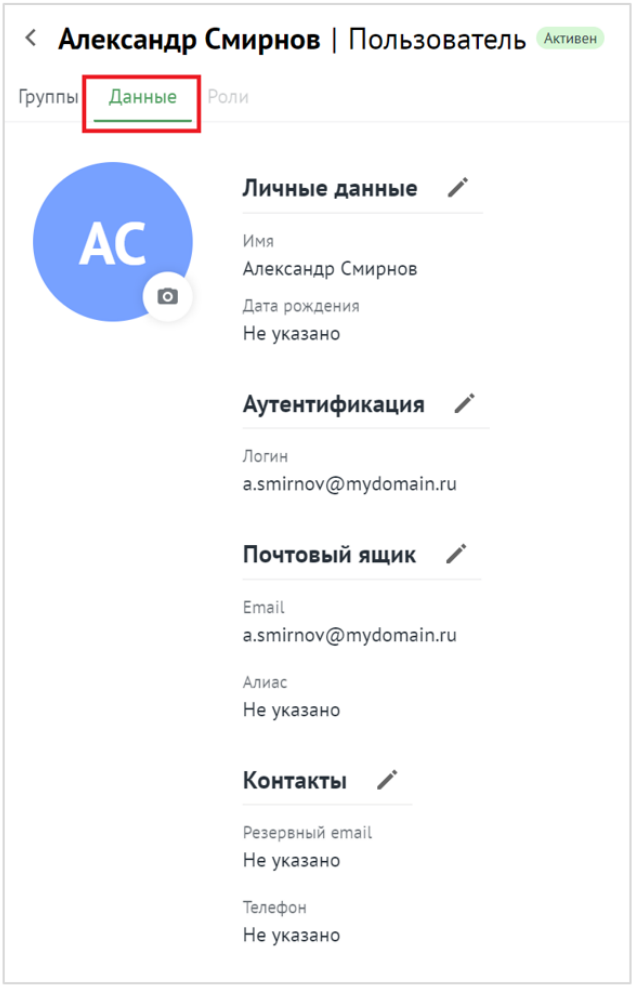


Рисунок 53 – Информация о пользователе на вкладке **Данные**

В результате отобразится информация, заполненная администратором при создании пользователя. При нажатии на иконку выбранный блок становится редактируемым (см. Рисунок 54).

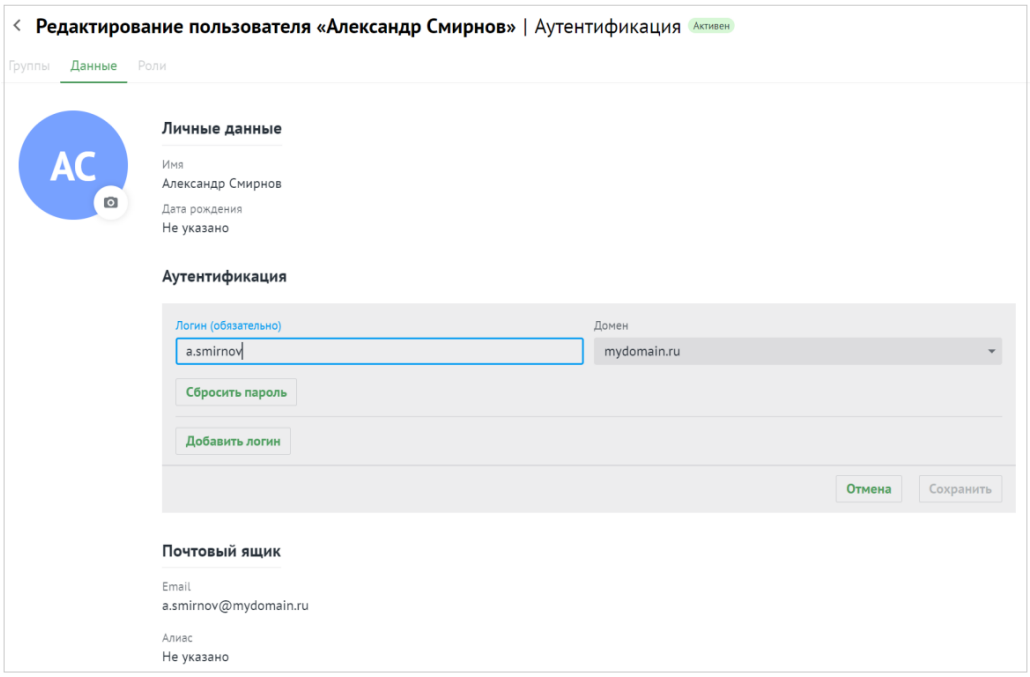


Рисунок 54 – Редактирование информации о пользователе

При необходимости следует нажать на иконку напротив соответствующего блока, отредактировать данные и нажать кнопку **Сохранить** или нажать на кнопку **Отмена**, чтобы отменить изменения.

6.3 Управление группами рассылки

6.3.1 Просмотр групп рассылки

Для просмотра существующей группы в **Панели администрирования** необходимо выбрать раздел **Группы**. В рабочей области откроется перечень существующих групп (см. Рисунок 55). Об активной группе представлена следующая информация:

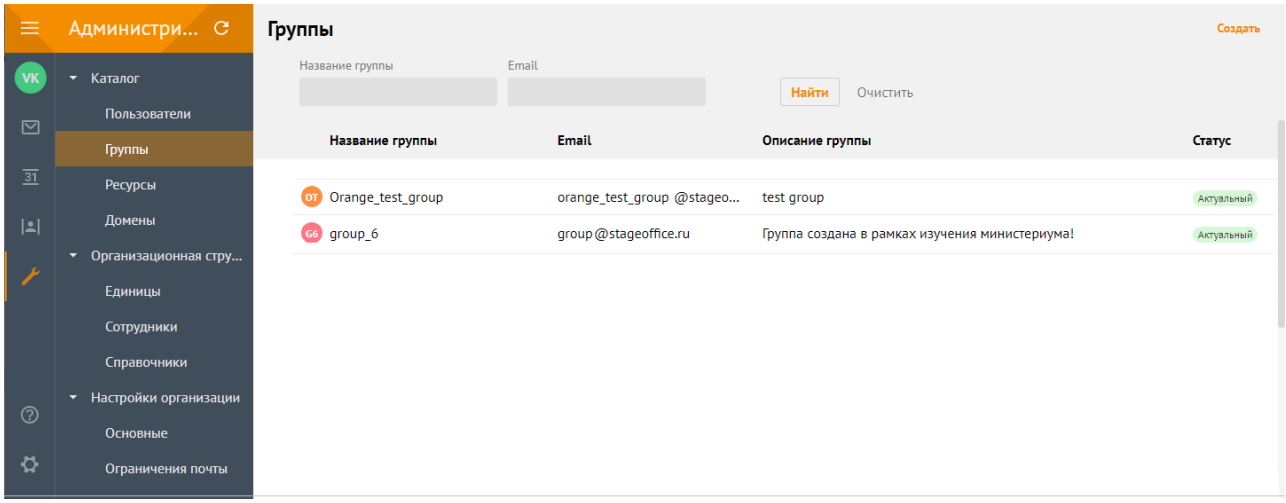


Рисунок 55 – Просмотр списка существующих групп рассылки

– Название группы рассылки.
– E-mail.
– Описание группы рассылки.
– Статус.

Для просмотра участников группы необходимо нажать на строку с именем группы, на экране появится панель, приведенная на рисунке 56.

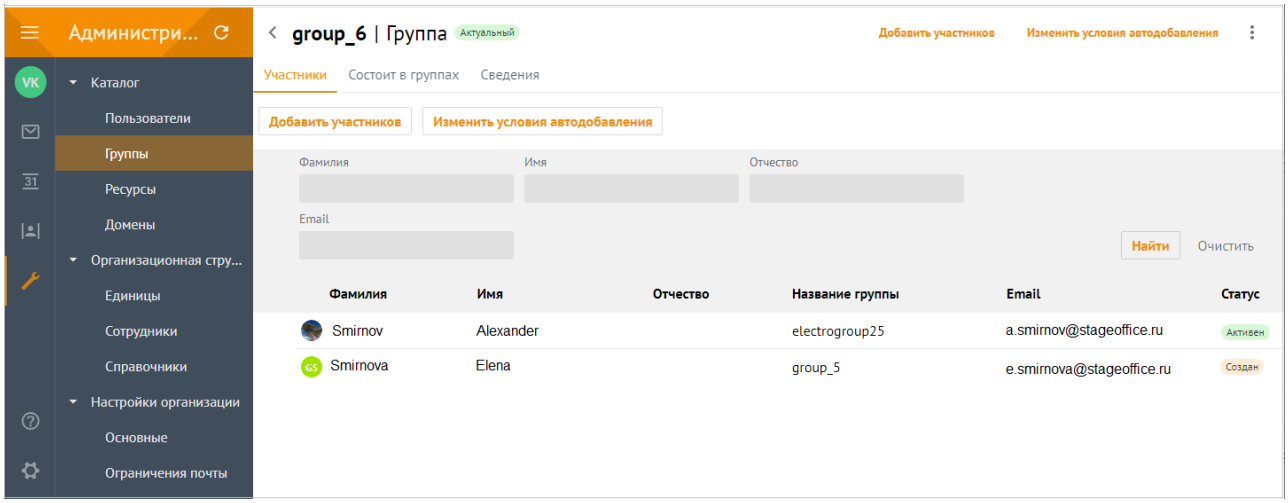


Рисунок 56 – Просмотр содержимого группы рассылки

6.3.2 Просмотр записи о группе

Чтобы просмотреть подробную запись о группе, необходимо открыть список групп, выбрать необходимую группу и перейти на вкладку **Сведения** (см. Рисунок 57).

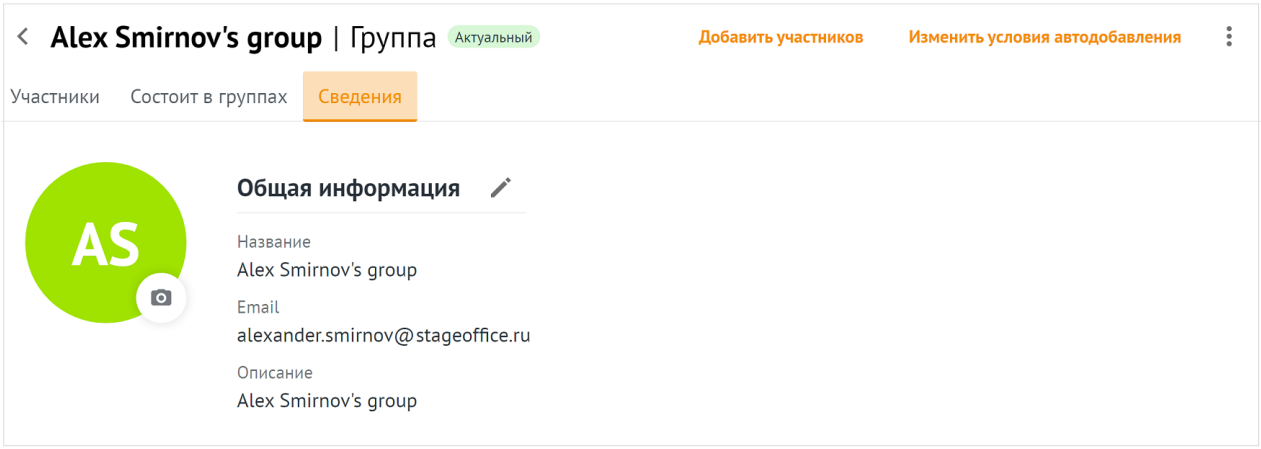


Рисунок 57 – Информация о группе

При нажатии на кнопку  откроется панель редактирования записи о группе (см. раздел 6.3.7).

6.3.3 Создание группы рассылки

Для создания группы рассылки необходимо выполнить следующие действия:

1. В разделе **Группы** нажать на кнопку **Создать** (см. Рисунок 58).

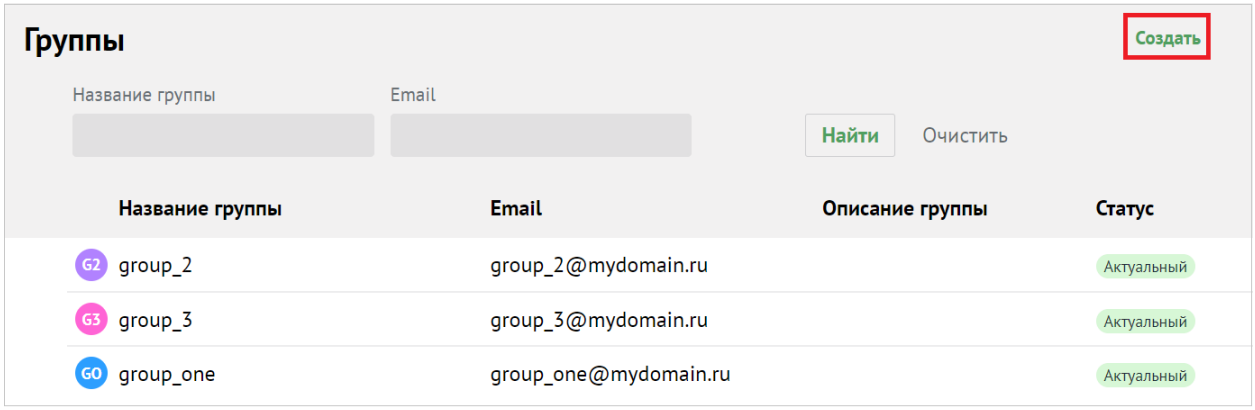


Рисунок 58 – Создание группы рассылки

2. В открывшейся форме создания группы необходимо заполнить следующие поля (см. Рисунок 59):

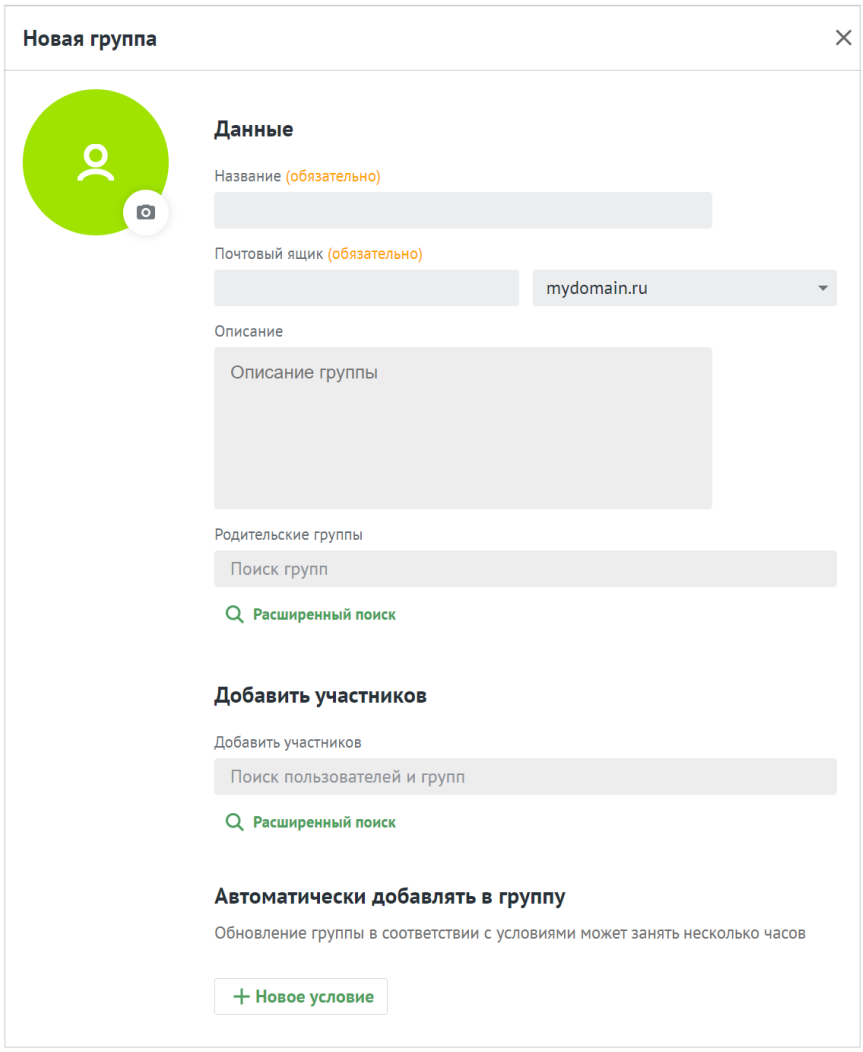


Рисунок 59 – Создание группы рассылки

– Поле **Название группы рассылки** обязательно к заполнению.

– Поле **Почтовый ящик** обязательно к заполнению. Если введенный почтовый ящик уже существует, то поле **Почтовый ящик** подсветится красным цветом и под ним отобразится сообщение. Необходимо изменить название почтового ящика. В ином случае, после заполнения всех полей, группу сохранить не удастся, кнопка **Сохранить** будет неактивна (см. Рисунок 60).

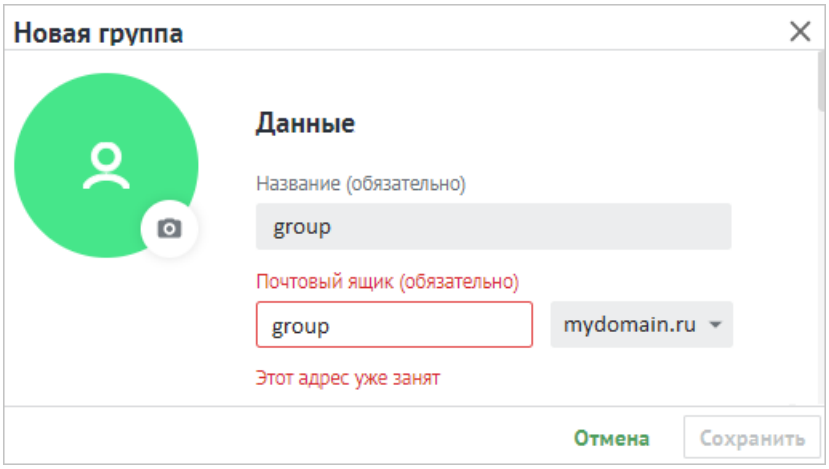


Рисунок 60 – Использование существующего названия почтового ящика

– Описание группы рассылки (опционально).
– Поле **Родительские группы** заполнить вручную или найти с помощью кнопки (**Расширенный поиск**);
  - установить курсор мыши на соответствующую группу и нажать **Добавить в группы** (см. Рисунок 61);

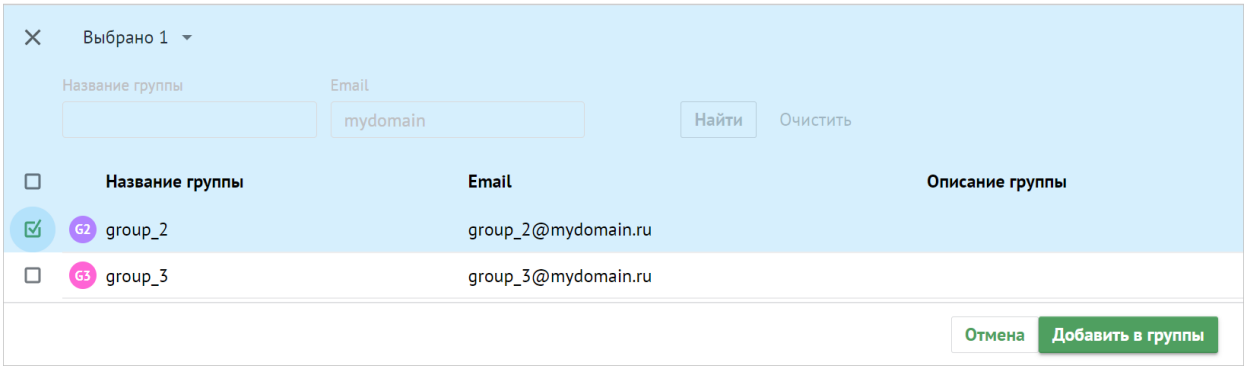


Рисунок 61 – Добавление в группы

- выбрать группы с помощью отметки из перечня групп и нажать кнопку **Добавить в группы** (см. Рисунок 62);

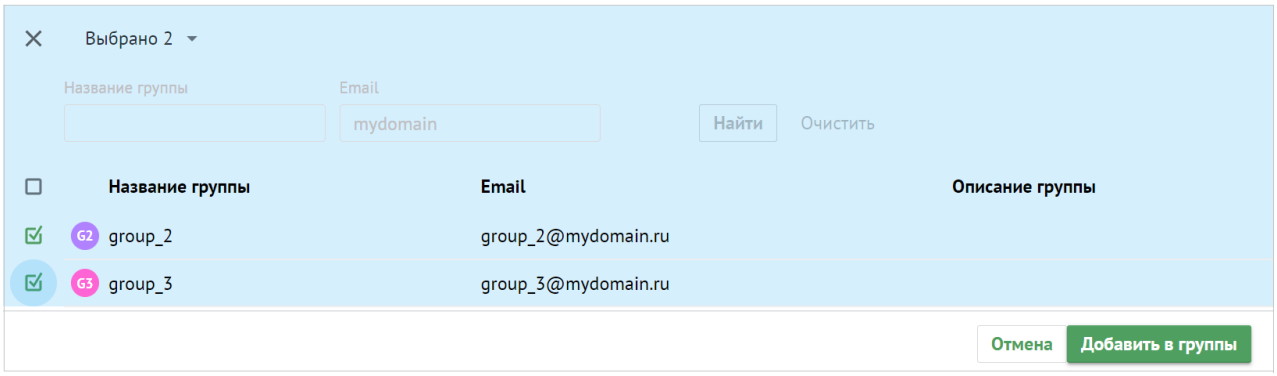


Рисунок 62 – Добавление в группы

- нажать на < в левом верхнем углу окна **Добавление в группы**, чтобы вернуться к созданию группы;

– Поле **Добавить участников** заполнить аналогично полю **Родительские группы**.

– Добавьте одно или несколько условий группе нажатием на кнопку + **Новое условие**. Подробная информация о добавлении условия приведена в разделе 6.3.8.

Для создания группы с указанными данными необходимо нажать на кнопку **Сохранить**. Для отмены создания группы нажать на кнопку **Отмена**.

6.3.4 Поиск группы рассылки

Для поиска группы рассылки необходимо выполнить следующие действия:

1. Перейти в раздел **Группы**.
2. В строку поиска ввести несколько символов из названия искомой группы.
3. Нажать на кнопку **Найти** или клавишу **Enter**.

4. Выбрать необходимую группу рассылки из динамически формируемого списка в области отображения найденных групп (см. Рисунок 63).

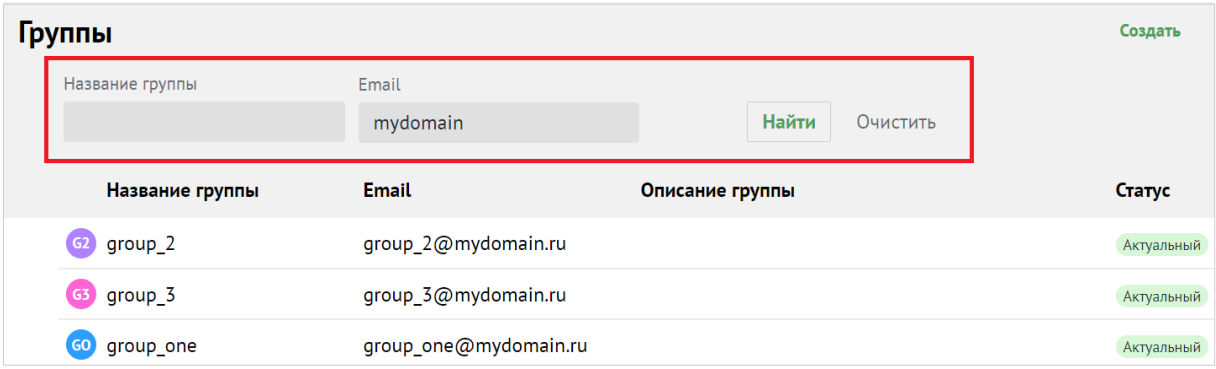


Рисунок 63 – Поиск группы рассылки

6.3.5 Добавление группы рассылки в другую группу

Для добавления группы рассылки в другую группу необходимо выполнить следующие действия:

1. В списке групп навести курсор на строку нужной группы и выбрать **Добавить в группу** (см. Рисунок 64).

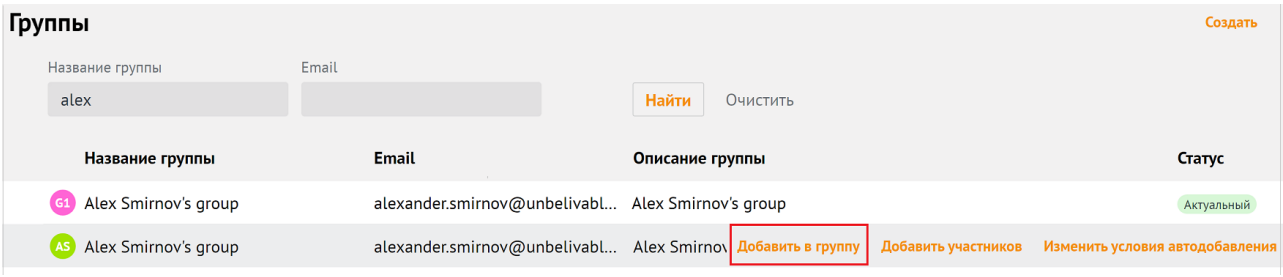


Рисунок 64 – Добавление группы рассылки в другую группу

2. В появившемся списке групп выделить флагами необходимые группы, нажать **Добавить в группы** (см. Рисунок 65).

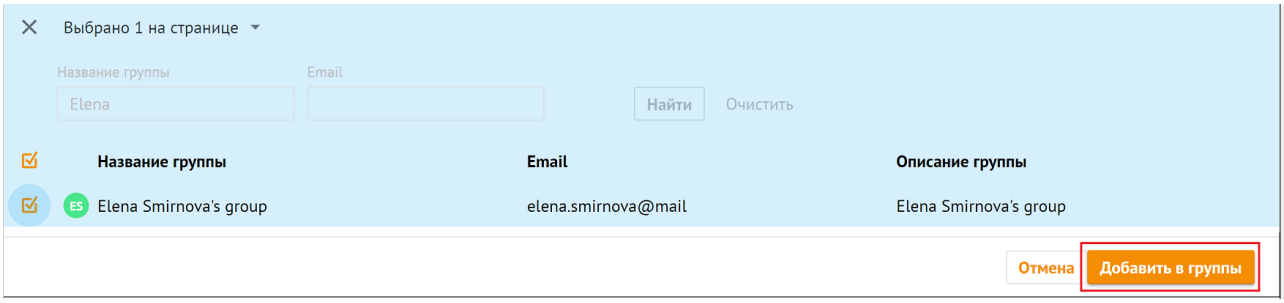


Рисунок 65 – Выбор групп рассылки для добавления группы

В левом нижнем углу возникнет сообщение: **Группа добавлена в группы**.

6.3.6 Удаление групп рассылки

Для удаления группы рассылки необходимо выбрать группу рассылки из списка и нажать на иконку ⋮, а затем на **Удалить** (см. Рисунок 66).

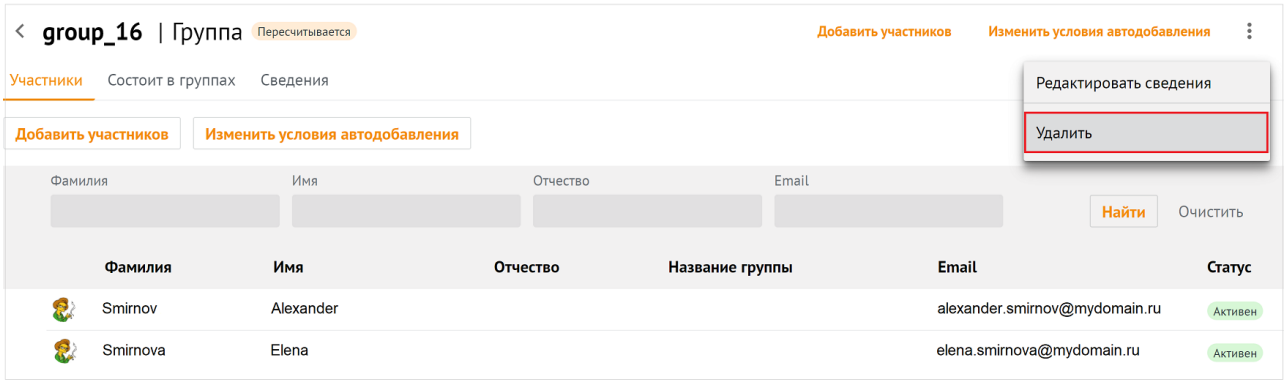


Рисунок 66 – Удаление группы рассылки

Подтвердить удаление группы рассылки, после чего группа будет удалена.

6.3.7 Редактирование группы рассылки

Для редактирования группы рассылки необходимо выполнить одно из следующих действий:

1. Перейти в раздел **Группы**, в списке выбрать необходимую группу, в контекстном меню нажать **Редактировать сведения** (см. Рисунок 67).

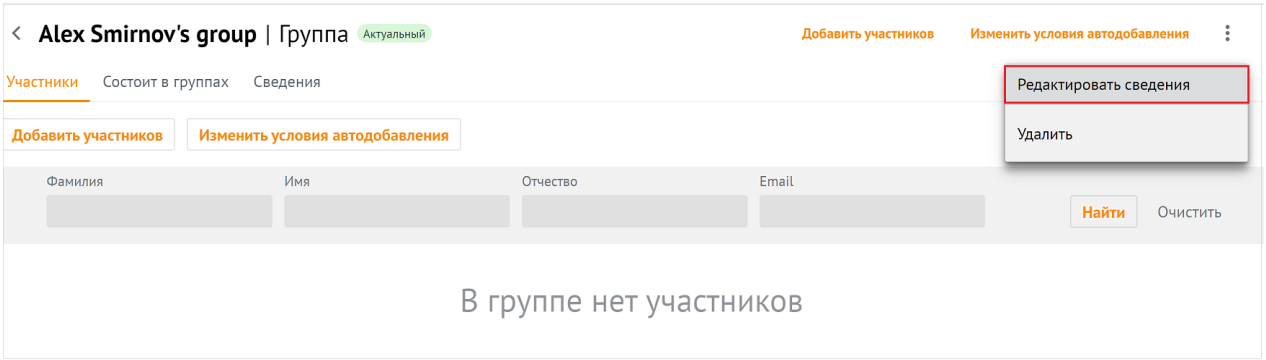


Рисунок 67 – Редактирование группы рассылки

2. Перейти в раздел **Группы**, в списке выбрать необходимую группу, выбрать закладку **Сведения**, в открывшейся форма нажать (см. Рисунок 68).

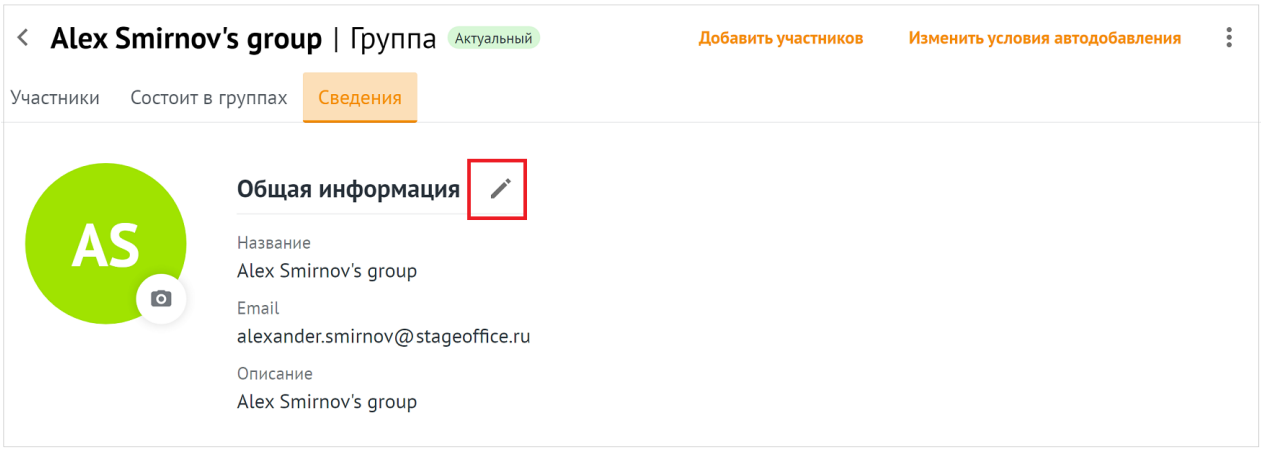


Рисунок 68 – Редактирование группы рассылки

На экране появится панель редактирования группы. Для сохранения изменений следует нажать на кнопку **Сохранить**. Для отмены внесенных изменений использовать кнопку **Отмена** (см. Рисунок 69).

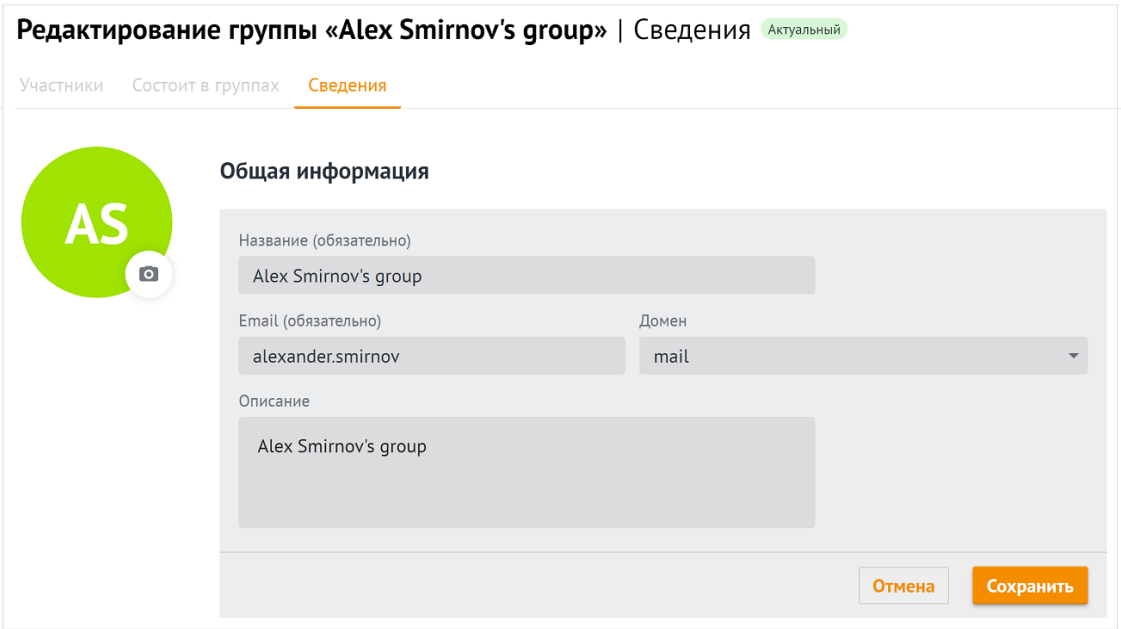


Рисунок 69 – Панель редактирования группы рассылки

6.3.8 Настройка динамических групп рассылки

Администратор может добавлять, настраивать и удалять правила автоматического добавления в группы рассылки.

Для добавления правил автоматического добавления необходимо выполнить следующие действия:

1. В разделе **Группы** выбрать соответствующую группу из списка.
2. Вызвать окно настроек правил автодобавления нажатием на кнопку **Изменить условия автодобавления** (см. Рисунок 70).

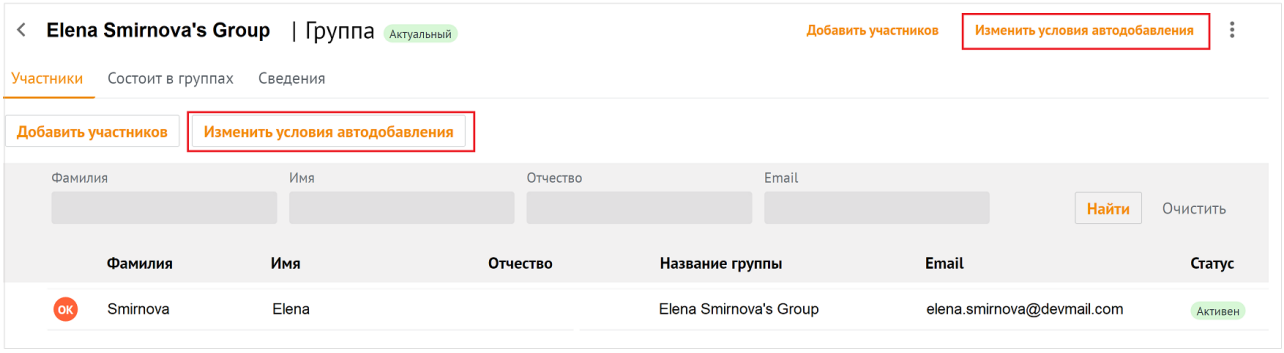


Рисунок 70 – Изменить условия автодобавления

На экране откроется панель настроек правил автоматического добавления (см. Рисунок 71).

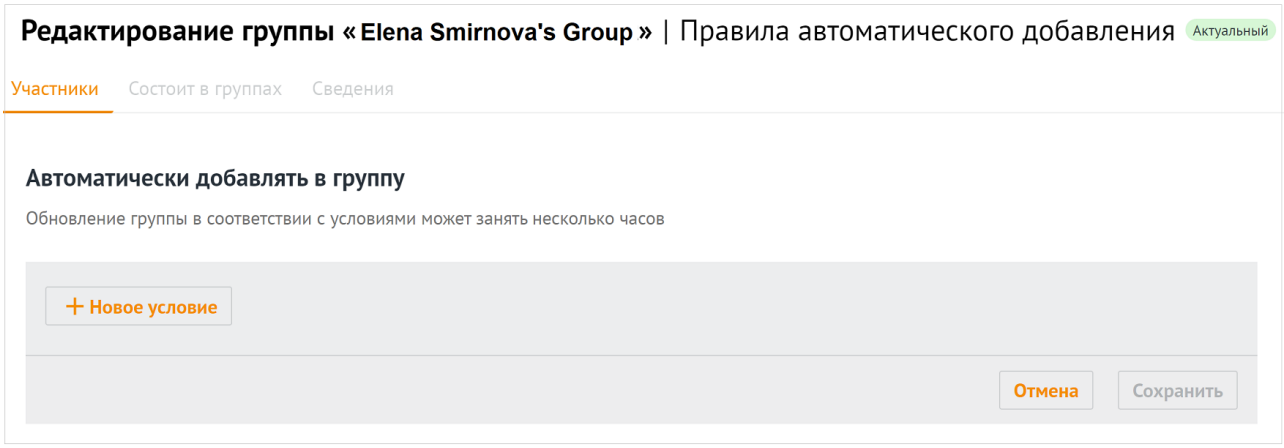


Рисунок 71 – Панель правил автоматического добавления в группу

3. Нажать на кнопку **+ Новое условие**.

4. Выбрать из списка поле условия автодобавления (**Организация**, **Подразделение**, **Должность**, **Город**, **Пол**, **Имя**, **Фамилия**). Если в группу добавляется второе условие, отобразится дополнительное поле выбора типа логической операции:
   – И – пользователи добавятся, если выполняются оба условия.
   – ИЛИ – пользователи добавятся, если выполнится одно из двух условий.
5. Выбрать из списка оператор сравнения: **содержит текст/не содержит текст**.
6. Указать текст для сравнения.
7. Нажать на кнопку **Сохранить**.

Состав группы обновится только после пересчета добавленных пользователей. В зависимости от количества пользователей в системе операция может занять до нескольких часов. Пользователи отобразятся как участники группы рассылки только после завершения пересчета. После обновления в группе также могут остаться статичные пользователи.

Условия применяются сверху вниз в соответствии с правилами алгебры логики. Чтобы изменить порядок выполнения условий необходимо выполнить следующие действия:

1. Выбрать соответствующее условие и нажать на кнопку ⋮ (**Еще**) напротив строки.
2. Выбрать значение:
   – «↑» (**Переместить выше**);
   – «↓» (**Переместить ниже**).

Чтобы удалить правило, необходимо нажать на кнопку ⋮ (**Еще**) и на кнопку **Удалить**.

6.4 Управление ресурсами

6.4.1 Создание ресурса

Чтобы создать новую запись о пространстве для встречи, необходимо выполнить следующие действия:

1. Нажать на кнопку **+ Создать** в списке ресурсов.
2. Задать параметры создаваемого пространства для встречи:
   – Заполнить блок **Общая информация**:
   - Ввести название пространства для встречи. Поле **Название** обязательно для заполнения.

- Ввести текст описания пространства для встречи.
- Указать минимальное количество участников пространства для встречи в поле **Вместимость**. По умолчанию задано значение 1.
- Ввести адрес электронной почты. Если доменов несколько, в поле справа от поля **Электронная почта** нажать на кнопку (**Развернуть**) и выбрать домен.

3. Заполнить поля блока **Контакты**: Название адреса, Страна, Город,Адрес, Индекс, Этаж, Кабинет, Место.
4. Заполнить блок **Аутентификация**:
   – Ввести логин. Если доменов несколько, в поле справа от поля **Логин** следует нажать на кнопку (**Развернуть**) и выбрать домен.
   – Ввести и повторить пароль, либо использовать пароль, предложенный автоматическим генератором. Поле ручного ввода пароля содержит подсказку, описывающую текущую рекомендацию по парольной политике, установленной по умолчанию (см. раздел 1.7.10; см. Рисунок 72):

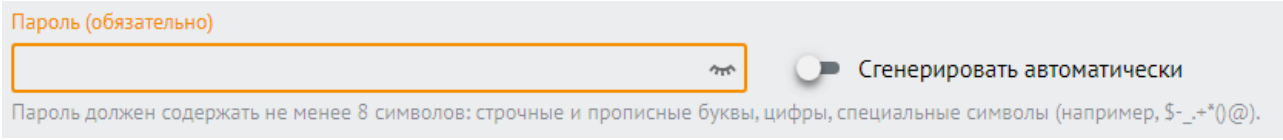


Рисунок 72 – Поле ввода пароля с подсказкой

   – Заполнить блок **Настройки бронирования**:
     - Выбрать подтверждение: **Автоматическое** или **Вручную владельцем или управляющим** и установить переключатель на соответствующей строке.
     - Указать минимальное количество участников пространства для встречи в поле **Условия для автоматического подтверждения**. По умолчанию задано значение 1.
5. Нажать на кнопку **Сохранить**.

В а ж н о – Если указанная комбинация значений поля **Email** и его домена ранее была присвоена другому пространству для встречи, то следует ввести уникальные сочетания и повторно нажать на кнопку **Сохранить**.

6.4.2 Просмотр данных о пространстве для встречи

Для просмотра данных о пространстве для встречи необходимо выполнить следующие действия:

1. Открыть раздел **Ресурсы**.
2. Выбрать запись в таблице ресурсов.
3. Просмотреть запись о пространстве для встречи:
   – аватар – круглый значок, установленный по умолчанию или выбранный пользователем;
   – блок **Общая информация** – сведения о названии ресурса, описание, вместимость и адрес электронной почты;
   – блок **Контакты** – сведения о названии, адресе, стране, городе, индексе, этаже, кабинете и месте;
   – блок **Аутентификация** – сведения о логине;
   – блок **Настройки бронирования** – сведения о подтверждении и минимальном количестве участников.

6.4.3 Поиск ресурса

Для поиска ресурса необходимо выполнить следующие действия:

1. Перейти в раздел **Ресурсы**.
2. Заполнить поля в области поиска. При необходимости можно раскрыть больше полей и заполнить их, для этого необходимо нажать на иконку .
3. Нажать на кнопку **Найти** или клавишу **Enter**.

6.4.4 Редактировать запись о пространстве для встречи

1. Нажать на кнопку (**Редактировать**) в записи пространства для встречи.
2. Внести изменения (для редактирования недоступно поле **Электронная почта**).
3. Нажать на кнопку **Сохранить**.

6.4.5 Фильтрация ресурсов

Чтобы отфильтровать список ресурсов, необходимо выполнить следующие действия:

1. Ввести поисковый запрос в нужное поле на панели фильтрации (например, ввести имя искомого пространства для встречи в поле **Название**). Для получения всех доступных полей фильтрации нажать на кнопку . Активируются кнопки **Найти** и **Очистить**.
2. Нажать на кнопку **Найти**.
3. Чтобы сбросить настройки фильтрации, нажать на кнопку **Очистить**.

6.4.6 Удаление ресурса

Чтобы удалить пространства для встреч, необходимо выполнить следующие действия:

1. Нажать на кнопку (**Удалить**) в записи о пространстве для встречи.
2. Нажать на кнопку **Удалить**.

В а ж н о – Пространства для встречи удаляются безвозвратно.

6.5 Управление доменами

6.5.1 Создание домена

Чтобы создать новый домен, необходимо выполнить следующие действия:

1. Нажать кнопку **+ Добавить домен** в окне отображения доменов.
2. Заполнить поля блока **Общая информация**:
   – ввести название домена (обязательно для заполнения);
   – ввести текст описания домена;
   – при необходимости установить флажок **Показывать в качестве приоритетного при добавлении новых пользователей**.

3. При необходимости заполнить поля блока **Напоминание о продлении срока регистрации**, предварительно сняв флажок **Не напоминать** (см. Рисунок 73):

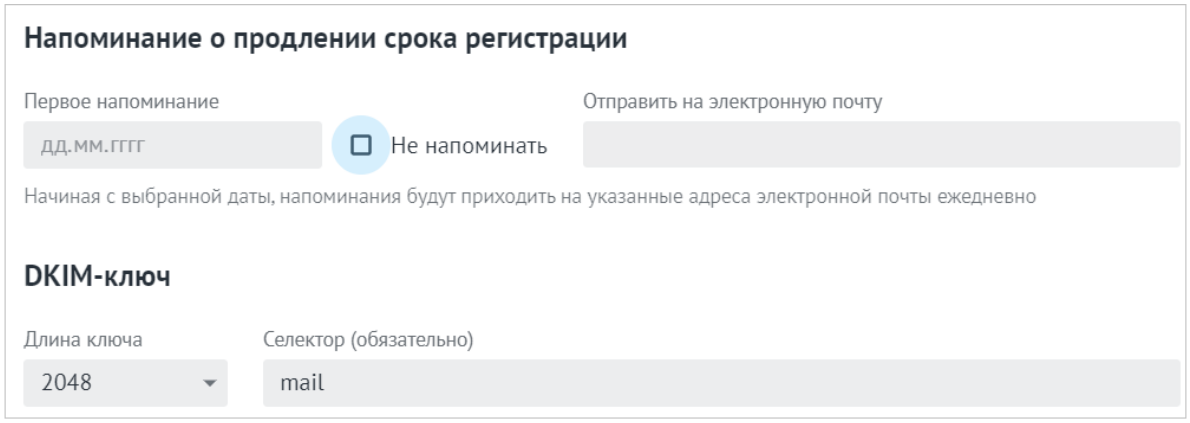


Рисунок 73 – Поля блока **Напоминание о продлении срока регистрации**

– в поле **Первое напоминание** ввести дату в формате ДД.ММ.ГГГГ или выбрать дату в календаре, который отображается при нажатии в поле ввода;
– в поле **Отправить на электронную почту** ввести адрес(-а) электронной почты для отправления напоминаний.

В а ж н о – Если напоминания о продлении срока регистрации домена не нужны, следует оставить флажок **Не напоминать** установленным.

4. Заполнить поля блока **DKIM-ключ**:
   – в поле **Длина ключа** выбрать значение из раскрывающегося списка;
   – в поле **Селектор** (обязательно для заполнения) по умолчанию стоит префикс *mail*, рекомендуется его использовать.
5. Нажать кнопку **Сохранить**.

Отображаемые в разделе **Администрирование** домены можно создавать как средствами графического интерфейса, так и через CLI (см. раздел 7).

6.5.2 Поиск домена

Для поиска домена необходимо выполнить следующие действия:

1. Перейти в раздел **Домены**.
2. Заполнить поля в области поиска. При необходимости можно раскрыть больше полей и заполнить их, для этого необходимо нажать на иконку .

3. Нажать на кнопку **Найти** или клавишу **Enter**.

6.5.3 Просмотр данных о домене

В разделе **Домены** отображается перечень созданных доменов с теми или иными характеристиками. Для просмотра данных о домене необходимо выбрать соответствующую строку и нажать на нее.

Отобразится запись о домене, в которой содержится вся необходимая информация. На этой же вкладке доступно редактирование записи о домене (см. раздел 6.5.4).

6.5.4 Редактировать запись о домене

Чтобы отредактировать запись о домене, необходимо выполнить следующие действия:

1. Нажать на кнопку (**Редактировать**) напротив соответствующего блока с информацией.
2. Внести изменения и нажать на кнопку **Сохранить**.

6.5.5 Фильтрация доменов

Чтобы отфильтровать список доменов, необходимо выполнить следующие действия:

1. Ввести поисковый запрос в нужное поле на панели фильтрации (например, ввести имя домена в поле **Домен**, выбрать домены по дате напоминания о продлении). Для получения всех доступных полей фильтрации нажать на кнопку .
2. Нажать на кнопку **Найти**.
3. Чтобы сбросить настройки фильтрации, нажать на кнопку **Очистить**.

6.5.6 Удаление домена

Чтобы удалить домен в списке записей, необходимо установить галочку напротив соответствующей записи о домене и нажать на **Удалить** в левом верхнем углу экрана.

Чтобы удалить домен в записи о домене, необходимо выполнить следующие действия:

1. Открыть запись о домене нажатием на соответствующую строку.
2. Нажать на кнопку **Удалить домен** в левом верхнем углу экрана.

В а ж н о – Домены удаляются безвозвратно.

6.6 Управление единицами организационной структуры

В приложениях **Mailion**: **Почта**, **Календарь**, **Контакты**, **Профиль пользователя** можно создавать и редактировать организационные единицы (организации, подразделения и проектные группы организации).

В а ж н о – Создание организации доступно только с помощью интерфейса командной строки. Подробная информация приведена в разделе 7.9.

В разделе отображаются либо единицы с типом **Подразделение**, либо единицы с типом **Проектная группа**. Для переключения между типами единиц организационной структуры необходимо воспользоваться фильтром **Тип подразделения** (по умолчанию выбрано значение – **Подразделение**). Вне зависимости от выбранного типа единиц таблица отображает все организационные единицы компании – родительские и дочерние.

После удаления дочернего объекта с помощью команды вкладки **Дочерние подразделения**/**Дочерние проектные группы** запись об этом объекте сохранится в разделе **Единицы организационной структуры**, но ее связь с родительским объектом будет разорвана (родительский объект не будет указан в качестве вышестоящей единицы).

6.6.1 Создание организационной единицы

Чтобы создать организационную единицу, необходимо выполнить следующие действия:

1. Вызвать форму создания и редактирования организационной единицы одним из следующих способов:
   – Нажать на кнопку **+ Создать** в таблице единиц и выбрать класс единицы **Структурное подразделение**.
   – Нажать на кнопку **+ Создать подразделение** при создании первой записи в таблице подразделений и групп в окне **Единицы организационной структуры**. Класс единицы выбирать не нужно.
2. Задать параметры создаваемой единицы:
   – Установить отметку напротив типа единицы в блоке **Выбор типа подразделения – Структурное подразделение** или **Проектная группа**.
   – Ввести название единицы, ее вид (отдел, департамент и т. п. – для подразделения или оперативная группа, команда и т. п. – для проектной группы) и при необходимости описание.
   – Ввести организацию в блоке полей, обозначающих место единицы в организационной структуре компании, затем ввести родительские единицы и руководителей. Нажать клавишу **Enter**. Для всех единиц можно ввести только одну организацию и несколько руководителей. Для подразделения и для проектной группы можно указать только одну родительскую единицу.
   – Ввести название местоположения, страну, город, индекс, адрес, координаты, этаж и номер места в офисе в блоке полей, описывающих местоположение единицы.
3. Нажать на кнопку **Сохранить**.

Можно создать дочернюю единицу для родительской единицы. Для этого можно воспользоваться командами меню таблицы единиц или кнопками вкладки **Дочерние подразделения**/**Дочерние проектные группы**.

6.6.2 Просмотр данных

Чтобы просмотреть организационную единицу, необходимо выполнить следующие действия:

1. Открыть раздел **Единицы** организационной структуры.
2. Выбрать запись в таблице, нажав на нее.
3. Просмотреть доступные сведения:
   – **Данные** – сведения, введенные администратором в форме создания и редактирования единицы.
   – **Дочерние подразделения** (для единиц с типом **Подразделение**) или **Дочерние проектные группы** (для единиц с типом **Проектная группа**) – список дочерних единиц, входящих в выбранное подразделение/проектную группу.
   – **Сотрудники** – список сотрудников, относящихся к выбранной единице.

Чтобы просмотреть вкладки **Дочерних подразделений**/**Дочерних проектных групп** и **Сотрудников** непосредственно из таблицы необходимо навести курсор на подразделение в таблице и выбрать команду **Дочерние подразделения** или **Сотрудники**.

В а ж н о – Поля **Организация** и **Вышестоящее подразделение** для дочерних единиц заполняются автоматически в соответствии с данными родительской единицы.

6.6.3 Редактирование организационной единицы

Вызвать форму создания и редактирования организационной единицы можно одним из способов:

– Нажать на кнопку **Редактировать** в записи о единице.
– Навести курсор на подразделение в таблице единиц/дочерних единиц. В появившемся меню навести курсор на команду **Редактировать**.

После этого необходимо внести изменения и нажать на кнопку **Сохранить**.

6.6.4 Поиск единицы организационной структуры

Для поиска единицы организационной структуры необходимо выполнить следующие действия:

1. Перейти в раздел **Единицы**.
2. Заполнить поля в области поиска.
3. Нажать на кнопку **Найти** или клавишу **Enter**.

6.6.5 Создание дочерней единицы

Чтобы создать дочернюю единицу, необходимо выполнить следующие действия:

1. Вызвать форму создания и редактирования дочерней единицы одним из следующих способов:
   – Навести курсор на подразделение в таблице единиц и нажать на кнопку **Создать дочернее подразделение**.
   – Нажать на кнопку **+ Создать новое подразделение** / **+ Создать новую проектную группу** на вкладке **Дочерние подразделения** / **Дочерние проектные группы**. Если на вкладке нет ни одной записи, кнопка расположится в центре экрана. Если в таблице присутствует хотя бы одна запись, то кнопка расположится над панелью фильтрации таблицы.
2. Задать параметры дочерней единицы:
   – Добавить аватар.
   – Установить отметку напротив типа единицы в блоке **Выбор** типа подразделения – **Структурное подразделение** или **Проектная группа**.
   – Ввести название единицы, вид (отдел, департамент и т. п. – для подразделения или оперативная группа, команда и т. п. – для проектной группы) и при необходимости описание.
   – В блоке полей, обозначающих место единицы в организационной структуре компании, поля организации и вышестоящих подразделений будут заполнены автоматически данными родительской единицы. Перечислить руководителей для дочерней единицы. Нажать клавишу **Enter**.

– В блоке полей, описывающих местоположение единицы, ввести название местоположения, страну, город, индекс, адрес, координаты, этаж и номер места в офисе.

3. Нажать на кнопку **Сохранить**.

6.6.6 Удаление дочерней единицы

Чтобы выделить все просмотренные записи таблицы, следует использовать отметки ☑ в первом столбце шапки таблицы. Так как списки в **Рабочей области** не разбиваются на страницы, все записи, заведенные в системе, загружаются динамически по мере того, как пользователь перемещается к концу списка. Поэтому выбор всех записей осуществляется только для записей, загруженных в ходе просмотра. Например, если пользователь просмотрел 30 записей, то он сможет выбрать 30 записей, если просмотрел 100 – сможет выбрать 100 записей и т.д.

Чтобы удалить дочернюю единицу, необходимо выполнить следующие действия:

1. Навести курсор на запись, нажать на кнопку ⋮ (**Еще**) и выбрать команду **Удалить**. Чтобы удалить несколько записей, необходимо установить отметки ☑ в строках у записей и нажать на кнопку **Удалить**. Чтобы удалить все просмотренные записи, необходимо установить отметку ☑ в первом столбце шапки таблицы и нажать на кнопку **Удалить**.
2. Нажать на кнопку **Удалить**.

В а ж н о – Организационная единица удаляется безвозвратно из списка единиц и записей о сотрудниках, которые к ней относятся. После удаления записи исчезают должности, входящие в эту единицу. Ее дочерние подразделения при этом сохраняются в таблице подразделений, но нарушается иерархия единиц (исчезает родительское подразделение, разрываются связи с дочерними единицами). В записях о пользователе в приложении **Mailion Контакты** при этом исчезают поля **Должность** и **Подразделение**.

6.6.7 Удаление организационной единицы

Чтобы удалить организационную единицу, необходимо навести курсор на запись в таблице единиц, нажать кнопку ⋮ (**Еще**) и выбрать команду **Удалить** либо нажать на кнопку ⋮ (**Еще**) и выбрать команду **Удалить**.

Чтобы удалить несколько записей, в таблице единиц необходимо установить отметки и нажать на кнопку **Удалить**. Чтобы удалить все просмотренные записи, в таблице единиц необходимо установить отметку в первом столбце шапки и нажать на кнопку **Удалить**.

6.7 Управление сотрудниками

6.7.1 Добавление нового сотрудника

Чтобы добавить нового сотрудника, необходимо выполнить следующие действия:

1. Нажать на кнопку **+ Новый сотрудник**.
2. В открывшейся форме добавления нового сотрудника необходимо заполнить следующие поля:
   – Заполнить блок **Личные данные**: ввести имя, фамилию, отчество, дату рождения и выбрать пол сотрудника. Поле **Имя** обязательно для заполнения.
   – Заполнить блок **Аутентификация**:
   - Ввести логин. Если доменов несколько, в поле справа от поля **Логин** нажать на кнопку (**Развернуть**) и выбрать домен.
   - Ввести и повторить пароль, либо использовать пароль, предложенный автоматическим генератором. Поле ручного ввода пароля содержит подсказку, описывающую текущую рекомендацию по парольной политике, установленной по умолчанию (см. раздел 1.7.10; см. Рисунок 74):

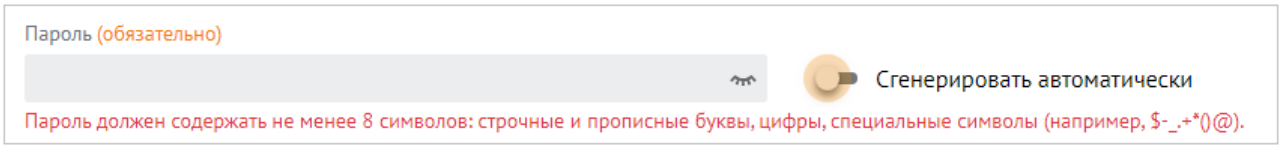


Рисунок 74 – Поле ввода пароля с подсказкой

– Заполнить блок **Почтовый ящик**:
  - В поле **Основной email** (обязательно для заполнения) ввести почтовый ящик сотрудника. Если доменов несколько, то в поле справа от поля **Логин** необходимо нажать на кнопку (**Развернуть**) и выбрать домен.
  - При необходимости добавить алиас сотрудника нажатием кнопки + (**Добавить алиас**).
– Заполнить блок **Контакты**:
  - Заполнить поле **Резервный email**.
  - Ввести телефон, при необходимости несколько, и выбрать категорию из раскрывающегося списка:
    - Домашний;
    - Рабочий;
    - Для СМС;
    - Для голосовых звонков;
    - Факс;
    - Мобильный;
    - Для видеозвонков;
    - Пейджер;
    - Телетайп.
– Заполнить блок **Адреса**. Заполнить данными сотрудника поля **Название адреса**, **Страна**, **Город**, **Адрес**, **Индекс**, **Этаж**, **Кабинет**, **Место**.
– Заполнить поле **Организация**. После этого для заполнения станут доступны поля **Подразделение**, **Проектная группа** и **Должность**.

3. Нажать на кнопку **Сохранить**.

6.7.2 Редактирование записи о сотруднике

Чтобы отредактировать информацию о сотруднике, необходимо выполнить следующие действия:

1. Перейти на вкладку **Сведения** или нажать на кнопку **Еще** и выбрать пункт **Редактировать сведения**.
2. Изменить информацию в соответствующих полях.

После этого внести изменения и нажать на кнопку **Сохранить**.

6.7.3 Поиск сотрудника

Поиск сотрудника осуществляется в разделе **Сотрудники** аналогично информации, приведенной в разделе 6.3.4, начиная с пункта 2.

6.7.4 Удаление сотрудника

Чтобы удалить сотрудника, необходимо установить курсор на соответствующей строке и выбрать команду **Удалить**. В окне подтверждения нажать кнопку **Удалить**.

6.8 Управление справочниками

Пользователь с правами администратора в справочниках **Должности** и **Адреса** имеет возможность создавать и редактировать должности и адреса сотрудников, чтобы впоследствии назначать сотрудникам и ресурсам адреса и должности из этих справочников.

6.8.1 Создание записи в справочнике

Чтобы создать запись в справочнике на вкладке **Должности**, необходимо выполнить следующие действия:

1. Нажать на кнопку **+Новая должность**.
2. Задать параметры создаваемой записи:
   - Ввести название должности.
   - Ввести описание должности (при необходимости).
   - Ввести организации, подразделения и/или проектные группы, к которым относится создаваемая должность, и нажать клавишу **Enter**.
3. Нажать на кнопку **Сохранить**.

После этого данная должность будет доступна для выбора при создании нового сотрудника и отображаться при просмотре сведений о пользователе.

Чтобы создать запись в справочнике на вкладке **Адреса**, необходимо выполнить следующие действия:

1. Нажать на кнопку **+Новый адрес**.
2. Задать параметры создаваемой записи:
   – Ввести текст адреса.
   – При необходимости ввести название страны, региона или района, города или населенного пункта, улицы дома и индекса.
3. Нажать на кнопку **Сохранить**.

После этого адрес будет доступен для выбора при создании нового сотрудника и отобразится при просмотре сведений о пользователе.

6.8.2 Поиск записи в справочнике

Поиск должности или адреса осуществляется в разделе **Справочник** аналогично информации, приведенной в разделе 6.3.4, начиная с пункта 2.

6.8.3 Редактирование записи в справочнике

Чтобы отредактировать запись о должности или адресе в справочнике, необходимо выполнить следующие действия:

1. Навести курсор на запись на вкладке **Должность** или **Адрес** и выбрать команду **Редактировать**.
2. Изменить значения полей и/или добавить новые.
3. Нажать на кнопку **Сохранить**.

6.8.4 Удалить запись в справочнике

Записи удаляются безвозвратно. Должность является признаком организационной единицы, поэтому при удалении записи о единице, относящейся к должности, запись о должности будет также удалена – как из таблицы справочника, так и из записей о сотрудниках, относящихся к этой единице. В записях о пользователе в приложении **Mailion Контакты** при этом исчезают поля **Должность** и **Подразделение**.

Чтобы удалить запись, необходимо навести на запись курсор и выбрать команду **Удалить**.

Чтобы удалить несколько записей, необходимо установить отметки и нажать на кнопку **Удалить**.

Чтобы удалить все просмотренные записи, необходимо установить отметку в первом столбце шапки таблицы и нажать на кнопку **Удалить**.

6.9 Управление настройками организации

6.9.1 Основные настройки

Для отображения названия организации и отображения/редактирования региональных настроек следует перейти в раздел **Настройки организации** / **Основные** (см. Рисунок 75).

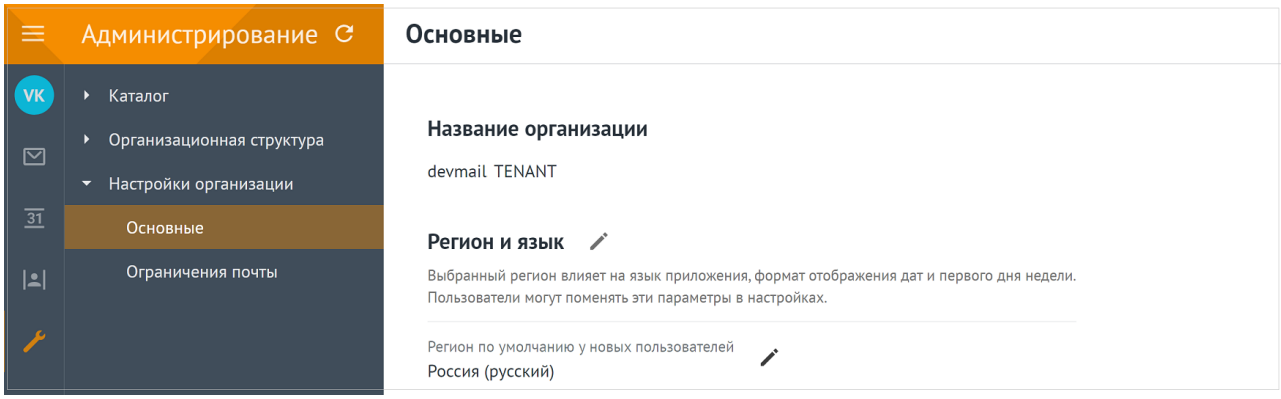


Рисунок 75 – Основные настройки организации (название и регион)

Для изменения региональных настроек необходимо нажать , на экране откроется панель выбора региона и языка (см. Рисунок 76).

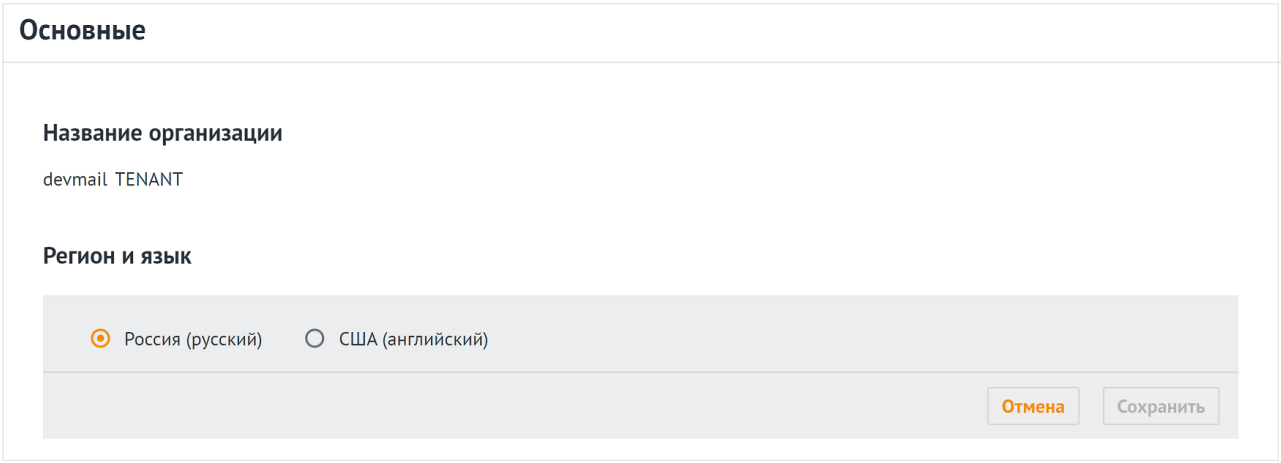


Рисунок 76 – Редактирование региональных настроек

6.9.2 Ограничения почты

Панель администрирования позволяет настраивать параметры ограничения размеров сообщений для переписки как внутри организации, так и для работы с внешними контактами:

– максимальный размер сообщения для переписки внутри организации;
– максимальный размер входящего сообщения для переписки с внешними контактами;
– максимальный размер исходящего сообщения для переписки с внешними контактами.

Для отображения и редактирования данных значений следует перейти в раздел **Настройки организации** / **Ограничения почты** (см. Рисунок 77).

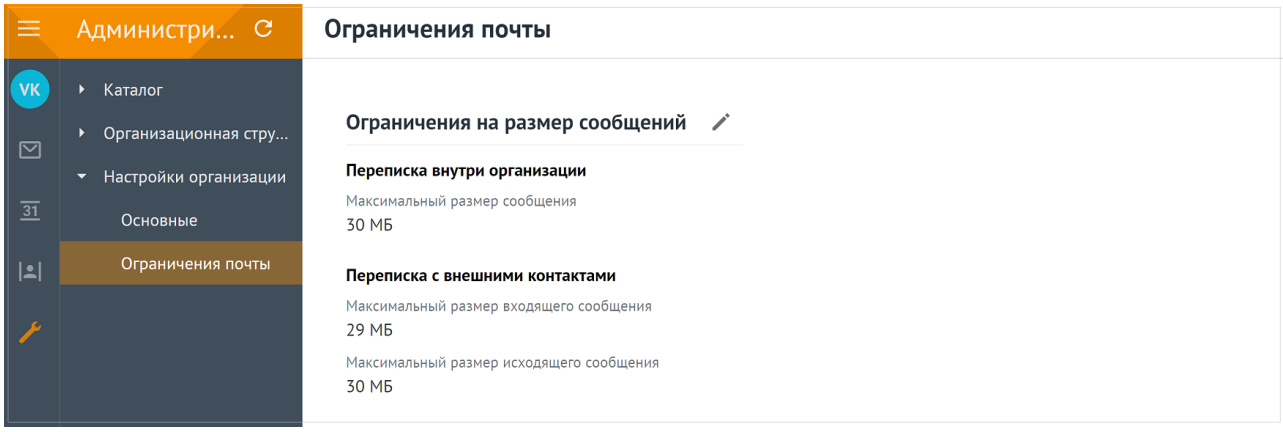


Рисунок 77 – Отображение ограничений размеров почтовых сообщений

Для изменения ограничений необходимо нажать , на экране откроется форма редактирования максимальных размеров сообщений (см. Рисунок 78).

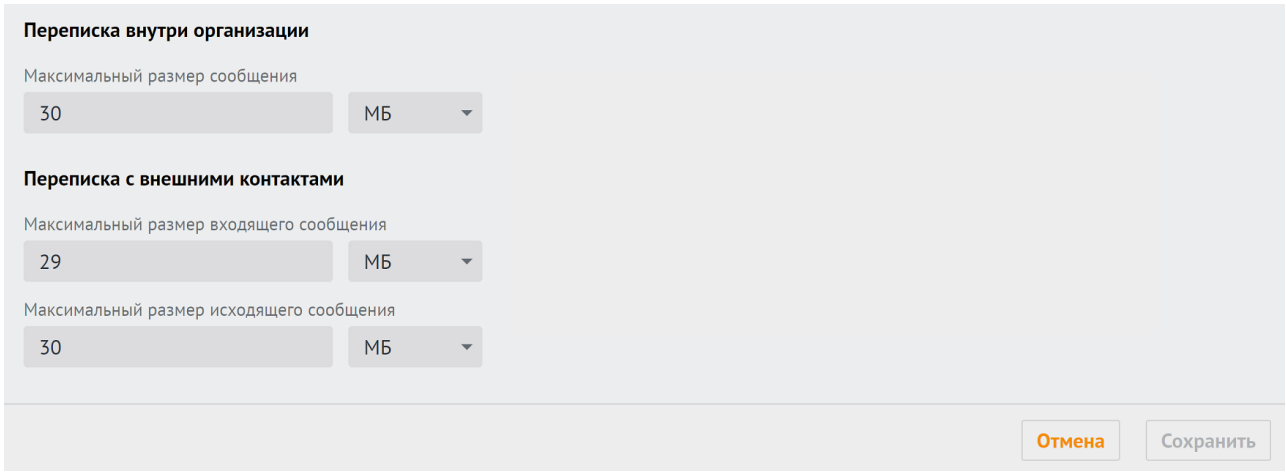


Рисунок 78 – Редактирование ограничений на размер почтовых сообщений

7 РАСШИРЕННОЕ АДМИНИСТРИРОВАНИЕ С ПОМОЩЬЮ ИНТЕРФЕЙСА КОМАНДНОЙ СТРОКИ

В а ж н о – Для выполнения указанных ниже запросов должен быть установлен интерфейс командной строки для расширенного администрирования ПО «Mailion». При установке ПО «Mailion» он автоматически устанавливается на сервер с ролью **ucs_infrastructure**.

Интерфейс командной строки для расширенного администрирования ПО «Mailion» реализует CLI интерфейс для взаимодействия Mailion с серверной частью.

7.1 Информация для работы с интерфейсом командной строки

7.1.1 Установка

При установке ПО «Mailion» интерфейс командной строки **ministerium** для расширенного администрирования автоматически устанавливается на сервер с ролью **ucs_infrastructure**.

При необходимости установки на машину оператора необходимо использовать команду:

```
sudo yum install nct_ministerium
```

7.1.2 Просмотр команд

В а ж н о – Все команды, прописываемые в интерфейсе командной строки вручную, набираются в одну строку. Команды, приведенные в данном руководстве, для более наглядного представления написаны в виде столбца.

Для просмотра списка всех команд интерфейса командной строки необходимо использовать запрос:

```
nct_ministerium --help
```

Для просмотра конкретной команды необходимо использовать запрос:

```
nct_ministerium <command> --help
```

Доступные команды, выполняемые с помощью интерфейса командной строки, приведены в Приложении Б. Команды, выполняемые с помощью интерфейса командной строки, и их описание.

7.1.3 Получение сертификатов админом тенанта для работы с nct_ministerium

Администратор тенанта может получить сертификат и конфиг для **ministerium** от администратора инсталляции. Администратор инсталляции может зайти на сервер с ролью **ucs_infrastructure** и оттуда скопировать на свою рабочую станцию сертификаты и конфиг для передачи администратору тената любым удобным способом.

Необходимо наличие доступа с рабочей станции администратора тенанта до сервера, где развернут сервис Cox (**installation.example.net:3142**).

Пример получения сертификатов:

```
// подготовка каталога для файлов в домашней папке пользователя, под которым производится подключение на сервер
cd /home/user/
mkdir ministerium

// копирование сертификатов и конфига
cp /srv/tls/certs/ucs-infra-1.installation.example.net-main-ca.pem /home/user/ministerium
cp /srv/tls/certs/ministerium.ucs-infra-1.installation.example.net-main-client.pem /home/user/ministerium
cp /srv/tls/keys/ministerium.ucs-infra-1.installation.example.net-main-key.pem /home/user/ministerium
cp /srv/ministerium/config.json /home/user/ministerium

// удаление из конфига логина и пароля администратора инсталляции
vim /home/user/ministerium/config.json
// Позже администратор тенанта должен самостоятельно заполнить эти поля своими учетными данными.
// "admin": {
//        "login": "",
//        "password": ""
//    },

// создание архива
tar czf "ministerium.tar.gz" -c ministerium/

// копирование на рабочую станцию, данная команда указана с учетом того, что выполняется с рабочей станции
scp user@ucs-infra-1.installation.example.net:/home/user/ministerium.tar.gz .
```

7.1.4 Основные роли для администрирования ПО «Mailion» с помощью интерфейса командной строки

Администратор инсталляции – лицо, ответственное за развертывание инсталляции ПО «Mailion» и ее конфигурирование. Он управляет регионами, тенантами и администраторами тенантов.

В а ж н о – Администратор инсталляции создается при первичном развертывании системы. Удаление его с помощью интерфейса командной строки для расширенного администрирования невозможно.

Пользователь с ролью администратора тенанта – лицо, ответственное за конфигурирование настроек ПО «Mailion». Например:

– изменение парольной политики тенанта;
– создание пользователей;
– работа в **Панели администрирования**;
– создание ресурсов и т.д.

В а ж н о – Перед созданием администратора тенанта должны быть выполнены следующие условия: создан тенант (см. раздел. 7.3.1); создана группа ALL в тенанте (см. раздел 7.3.2); создан GAL-пользователь в тенанте (см. раздел 7.3.4).

Подробная информация о создании и удалении администратора тенанта приведена в разделах 7.3.5 и 7.26. Информация о добавлении роли администратора тенанта к уже созданному пользователю приведена в разделе 7.3.7.

7.2 Установка общей квоты на тенант администратором инсталляции

С помощью расширенного администрирования можно установить общую квоту на тенант (в данном релизе квотой лимитируется только почтовый ящик).

В а ж н о – Установить общую квоту может только пользователь с ролью администратора инсталляции.

Для этого необходимо выполнить запрос:

```
nct_ministerium update_total_quotas
--admin.login <...>
--admin.password <...>
```

```
--tenant_total.max_size 40gb
--config ministerium.json
--tenant_id 2a3b8043-70ef-4a59-a395-9e28cc5c2685
```

Описание параметров запроса приведено в таблице 53.

Таблица 53 – Описание параметров запроса на установку общей квоты

Параметр	Тип	Обязательный	Описание
admin.login	Str	+	Логин администратора тенанта
admin.password	Str	+	Пароль администратора тенанта
tenant_total.max_size	Str	+	Размер общей квоты тенанта
config	Str	+	Конфигурационный файл с параметрами сервиса Cox и настройками tls. Формируется автоматически на сервере с ролью ucs_infrastructure и находится по пути /srv/ministerium/config.json
tenant_id	Str	+	Идентификатор тенанта

Пример ответа:

```
{
  "changed": true,
  "failed": false,
  "msg": "ok"
}
```

Администратор инсталляции может получить размер общей квоты, выделенной на тенант, выполнив запрос:

```
nct_ministerium get_total_quotas
--admin.login <...>
--admin.password <...>
--config ministerium.json
--tenant_id 2a3b8043-70ef-4a59-a395-9e28cc5c2685
```

Описание параметров запроса приведено в таблице 54.

Таблица 54 – Описание параметров запроса на установку общей квоты

Параметр	Тип	Обязательный	Описание
admin.login	Str	+	Логин администратора тенанта
admin.password	Str	+	Пароль администратора тенанта
config	Str	+	Конфигурационный файл с параметрами сервиса Cox и настройками tls. Формируется автоматически на сервере с ролью ucs_infrastructure и находится по пути /srv/ministerium/config.json

Параметр	Тип	Обязательный	Описание
tenant_id	Str	+	Идентификатор тенанта

Пример ответа:

```
{
  "Response": {
    "changed": false,
    "failed": false,
    "msg": "ok"
  },
  "mail_total_quota": null,
  "tenat_total_quota": {
    "max_size": 42949672960
  }
}
```

В а ж н о – Администратор инсталляции не может ни устанавливать почтовую квоту **mail_total_quota**, ни получать ее текущее значение.

7.3 Операции над тенантом

Тенант создается для того, чтобы использовать систему в корпоративных целях. У администратора тенанта есть права на создание пользователей, групп, доменов и другие возможности, описанные в данном разделе.

Тенант представляет собой одну компанию и является учетной записью организации.

7.3.1 Создание тенанта

Для создания тенанта необходимо выполнить запрос:

```
nct_ministerium create_tenant \
--config ministerium.json \
--display_name 'Tenant Test' \
--default_locale ru_RU \
--password.min_upper_case_letters 1 \
--password.min_lower_case_letters 1 \
--password.min_digits 1 \
--password.min_special_characters 1 \
--password.default_hash_type 1 \
--password.expiration_duration '31536000000000us' \
--password.expiration_remind '31535999999999us' \
--password.last_number_must_differ 0
```

Описание параметров запроса приведено в таблице 55.

Таблица 55 – Описание параметров запроса на создание тенанта

Параметр	Тип	Обязательный	Описание
config	Str	+	Конфигурационный файл с параметрами сервиса Cox и настройками tls. Формируется автоматически на сервере с ролью ucs_infrastructure и находится по пути /srv/ministerium/config.json
display_name	Str	+	Имя тенанта
default_locale	Str	+	Локаль тенанта по умолчанию
password.default_hash_type	Int	+	Тип хэша паролей по умолчанию для пользователей тенанта
password.expiration_duration	Str	+	Срок действия паролей пользователей тенанта (задается в микросекундах)
password.password_ expiration_remind	Str	+	Срок действия напоминания об истечении срока действия паролей (должен быть меньше expiration_duration)
password.last_number_must_ differ	Int	+	Количество уникальных паролей в истории паролей пользователя
Параметры парольной политики:			
password.min_upper_case_ letters	Int	-	Минимальное количество прописных букв
password.min_lower_case_ letters	Int	-	Минимальное количество строчных букв
password.min_digits	Int	-	Минимальное количество цифр
password.min_special_ characters	Int	-	Минимальное количество специальных символов

Пример ответа:

```
{
  "Response": {
    "msg": "ok",
    "changed": true
  },
  "id": "ef28480f-0ee4-4f0c-af67-59f100727f31"
}
```

В а ж н о – В случае если указан хотя бы один параметр парольной политики, в обязательном порядке должны быть указаны остальные. В случае если параметры парольной политики не были указаны совсем, по умолчанию будет применена парольная политика ФСТЭК.

Далее необходимо проверить, что тенант был успешно создан. Для этого следует выполнить запрос на получение информации о созданном тенанте по его идентификатору:

```
nct_ministerium get_tenant
--config ministerium.json
--admin.login <...>
--admin.password <...>
--tenant_id ef28480f-0ee4-4f0c-af67-59f100727f31
```

где **tenant_id** является идентификатором тенанта.

Пример ответа:

```
{
  "Response": {
    "msg": "ok",
    "changed": true
  },
  "tenant": {
    "id": "ef28480f-0ee4-4f0c-af67-59f100727f31",
    "display_name": "Tenant Test",
    "locale": "ru_RU",
    "password_policies": {
      "hash_type": 1,
      "password_expiration": {
        "unixmicro": 31536000000000
      }
    }
  }
}
```

7.3.2 Настройка уведомлений об истечении срока жизни пароля

С помощью расширенного администрирования можно настроить отправку уведомлений на почту пользователей о том, что время действия их пароля истекает. Для этого необходимо выполнить запрос:

```
nct_ministerium create_credential_expire_notification_task
--admin.login <>
--admin.password <>
--locale ru_RU
--mail_from <>
--recurrence_rule.by_hour <>
--recurrence_rule.by_minute <>
--recurrence_rule.by_second <>
```

```
--recurrence_rule.frequency daily
--recurrence_rule.interval <>
--recurrence_rule.count
--retry_policy.count <>
--retry_policy.delay <>
--tenant_id <>
```

Описание параметров запроса приведено в таблице 56.

Таблица 56 – Описание параметров запроса на создание уведомления

Параметр	Тип	Обязательный	Описание
admin.login	Str	+	Логин администратора тенанта
admin.password	Str	+	Пароль администратора тенанта
locale	Str	+	Локаль тенанта
mail_from	Str	+	Email пользователя
recurrence_rule.by_hour	Str	+	Время отправки (в формате UTC) (Ограничение: необходимо указывать время минус три часа от настоящего. Например, если нужно указать 9 часов, необходимо задать 6 часов)
recurrence_rule.by_minute	Str	+	Минута отправки
recurrence_rule.by_second	Str	+	Секунда отправки
recurrence_rule.frequency	Str	-	Периодичность выполнения. Допустимые значения: yearly, monthly, weekly, daily, hourly, minutely, secondly
recurrence_rule.interval	Str	-	Интервал повтора отправки
recurrence_rule.count	Str	-	Точное количество раз отправки уведомления. Данная команда перебивает настройки параметра **recurrence_rule.frequency daily**.
retry_policy.count	Str	-	Количество повторов
retry_policy.delay	Str	-	Время перед повтором
tenant_id	Str	+	Идентификатор тенанта

После этого необходимо выполнить запрос на обновление тенанта:

```
nct_ministerium update_tenant
--admin.login <...>
--admin.password <...>
--tenant_id <...>
--password.min_upper_case_letters 1 \
--password.min_lower_case_letters 1 \
--password.min_digits 1 \
--password.min_special_characters 1 \
--password.expiration_duration
--password.expiration_remind
```

Описание параметров запроса приведено в таблице 57.

Таблица 57 – Описание параметров запроса на обновление тенанта

Параметр	Тип	Обязательный	Описание
admin.login	Str	+	Логин администратора тенанта
admin.password	Str	+	Пароль администратора тенанта
tenant_id	Str	+	Идентификатор тенанта
password.expiration_duration	Str	+	Срок действия паролей пользователей тенанта (задается в микросекундах)
password.expiration_remind	Str	+	Срок действия напоминания об истечении срока действия паролей (должен быть меньше expiration_duration)
Параметры парольной политики:			
password.min_upper_case_letters	Int	-	Минимальное количество прописных букв
password.min_lower_case_letters	Int	-	Минимальное количество строчных букв
password.min_digits	Int	-	Минимальное количество цифр
password.min_special_characters	Int	-	Минимальное количество специальных символов

П р и м е ч а н и е – При обновлении тенанта можно отключить установку надежности пароля, передав в параметрах парольной политики значения "0".

Пример ответа на данные команды:

```
{
  "Response": {
    "msg": "ok",
```

```
    "changed": true
}
```

7.3.3 Создание группы ALL для тенанта

Группа ALL обязательно должна быть создана для каждого тенанта. Для нее должны выполняться следующие условия:

- существующую связь между сущностью тенанта и группой ALL удалить нельзя;
- сущность из другого тенанта не может быть дочерней для группы ALL данного тенанта;
- группу ALL тенанта удалить нельзя;
- нельзя делать группу ALL дочерней для любой другой группы, каждый пользователь тенанта является дочерней сущностью по отношению к этой группе.

Для создания группы ALL для тенанта необходимо выполнить запрос:

```
nct_ministerium create_group_all
--config ministerium.json
--admin.login <...>
--admin.password <...>
--tenant_id ef28480f-0ee4-4f0c-af67-59f100727f31
```

Описание параметров запроса приведено в таблице 58.

Таблица 58 – Описание параметров запроса на создание группы ALL для тенанта

Параметр	Тип	Обязательный	Описание
config	Str	+	Конфигурационный файл с параметрами сервиса Cox и настройками tls. Формируется автоматически на сервере с ролью ucs_infrastructure и находится по пути /srv/ministerium/config.json
admin.login	Str	+	Логин администратора тенанта
admin.password	Str	+	Пароль администратора тенанта
tenant_id	Str	+	Идентификатор тенанта

Пример ответа:

```
{
  "msg": "ok",
  "changed": true
}
```

7.3.4 Создание GAL-пользователя в тенанте

GAL-пользователь – это системный пользователь, владелец глобальной адресной книги и тегов в системе. Он автоматически добавляется к тенанту в момент создания. В глобальную адресную книгу, или GAL (Global Address List), попадают контакты пользователей внутри тенанта. Информация о создании пользовательских тегов приведена в разделе 7.4.

В а ж н о – Перед созданием GAL-пользователя должен быть создан тенант.

Для создания GAL-пользователя необходимо выполнить запрос:

```
nct_ministerium create_gal_user \
--config ministerium.json \
--admin.login <...> \
--admin.password <...> \
--locale ru_RU \
--region_id 004bfd74-e829-4224-a28c-620b265b5bc1 \
--tenant_id ef28480f-0ee4-4f0c-af67-59f100727f31
```

Описание параметров запроса приведено в таблице 59.

Таблица 59 – Описание параметров запроса на создание группы ALL для тенанта

Параметр	Тип	Обязательный	Описание
config	Str	+	Конфигурационный файл с параметрами сервиса Cox и настройками tls. Формируется автоматически на сервере с ролью ucs_infrastructure и находится по пути /srv/ministerium/config.json
admin.login	Str	+	Логин администратора тенанта
admin.password	Str	+	Пароль администратора тенанта
locale	Str	+	Локаль тенанта
region_id	Str	+	Идентификатор региона
tenant_id	Str	+	Идентификатор тенанта

Пример ответа:

```
{
  "Response": {
    "msg": "ok",
    "changed": true
  },
  "id": "45addbaf-0c91-4a0c-aae1-e8e3923d0545"
}
```

7.3.5 Создание администратора тенанта

Для создания администратора тенанта необходимо выполнить следующие действия:

1. Выполнить запрос на получение GAL-тегов (тегов глобальной адресной книги) тенанта:

```
nct_ministerium get_tenant_gals \
--config ministerium.json \
--admin.login <...> \
--admin.password <...> \
--tenant_id ef28480f-0ee4-4f0c-af67-59f100727f31
```

Описание параметров запроса приведено в таблице 60.

Таблица 60 – Описание параметров запроса на получение GAL-тегов тенанта

Параметр	Тип	Обязательный	Описание
config	Str	+	Конфигурационный файл с параметрами сервиса Cox и настройками tls. Формируется автоматически на сервере с ролью ucs_infrastructure и находится по пути /srv/ministerium/config.json
admin.login	Str	+	Логин администратора тенанта
admin.password	Str	+	Пароль администратора тенанта
tenant_id	Str	+	Идентификатор тенанта

Пример ответа:

```
{
  "Response": {
    "msg": "ok",
    "changed": true
  },
  "gals": [
    {
      "id": {
        "id": "11cd3c1a-9f14-4810-acc6-4a7b2aacb540",
        "region_id": "004bfd74-e829-4224-a28c-620b265b5bc1"
      },
      "path": [
        "gal"
      ]
    }
  ]
}
```

где **gals.id.id** – идентификатор GAL-тега.

2. Выполнить запрос на создание администратора тенанта:

```
nct_ministerium create_tenant_admin \
--config ministerium.json \
--admin.login <...> \
```

```
--admin.password <...> \
--tenant_id ef28480f-0ee4-4f0c-af67-59f100727f31 \
--region_id 004bfd74-e829-4224-a28c-620b265b5bc1 \
--gal_tags 11cd3c1a-9f14-4810-acc6-4a7b2aacb540 \
--login admin2.tenant2_test \
--password 'BnYs6j*Hw_TT$X)MsD59' \
--profile.first_name Admin2 \
--profile.last_name Test
```

Описание параметров запроса приведено в таблице 61.

Таблица 61 – Описание параметров запроса на создание администратора тенанта

Параметр	Тип	Обязательный	Описание
config	Str	+	Конфигурационный файл с параметрами сервиса Cox и настройками tls. Формируется автоматически на сервере с ролью ucs_infrastructure и находится по пути /srv/ministerium/config.json
admin.login	Str	+	Логин администратора тенанта
admin.password	Str	+	Пароль администратора тенанта
tenant_id	Str	+	Идентификатор тенанта
region_id	Str	+	Идентификатор региона
gal_tags	Str	+	Идентификаторы GAL-тегов
login	Str	+	Логин создаваемого администратора тенанта
password	Str	+	Пароль создаваемого администратора тенанта
profile.first_name	Str	+	Имя создаваемого администратора тенанта
profile.last_name	Str	+	Фамилия создаваемого администратора тенанта

Пример ответа:

```
{
  "Response": {
    "msg": "ok",
    "changed": true
  },
  "id": "aa7287ad-b22d-4a2e-aaf7-f123d71ad7e8"
}
```

где **id** – идентификатор созданного администратора тенанта.

3. Выполнить запрос на получение созданного администратора тенанта по его идентификатору:

```
nct_ministerium list_entities \
--config ministerium.json \
--admin.login <...> \
--admin.password <...> \
--id aa7287ad-b22d-4a2e-aaf7-f123d71ad7e8
```

Пример ответа:

```
{
  "Response": {
    "msg": "ok"
  },
  "Entities": [
    {
      "id": "aa7287ad-b22d-4a2e-aaf7-f123d71ad7e8",
      "type": 1, ### USER ###
      "tenant_id": "ef28480f-0ee4-4f0c-af67-59f100727f31",
      "region_id": "004bfd74-e829-4224-a28c-620b265b5bc1",
      "roles": [
        "54718e3a-6c7b-5c9f-b4de-a897c356cb5e", ### admin_tenant ###
        "c4b1f72c-672d-5ace-8a6d-96edc21227de"  ### user_regular ###
      ],
      "logins": [
        {
          "id": "918d0b5b-72b6-5f28-b563-4c80511d0787",
          "entity_id": "aa7287ad-b22d-4a2e-aaf7-f123d71ad7e8",
          "login": "admin2.tenant2_test",
          "auth_type": 1
        }
      ],
      "Payload": {
        "User": {
          "locale": "ru_RU"
        }
      },
      "status": 2 ### ACTIVE ###
    }
  ]
}
```

Для удаления администратора тенанта необходимо выполнить действия, приведенные в разделе 7.26.

7.3.6 Создание пользователя тенанта

В а ж н о – Перед созданием пользователя тенанта должен быть создан администратор тенанта.

Для создания пользователя тенанта необходимо выполнить следующие действия:

1. Выполнить запрос на получение GAL-тегов тенанта:

```
nct_ministerium get_tenant_gals
--config ministerium.json
--admin.login <...>
--admin.password <...>
--tenant_id 8c13a034-48f5-44e6-9a60-afecda033437
```

Описание параметров запроса приведено в таблице 62.

Таблица 62 – Описание параметров запроса на получение GAL-тегов тенанта

Параметр	Тип	Обязательный	Описание
config	Str	+	Конфигурационный файл с параметрами сервиса Cox и настройками tls. Формируется автоматически на сервере с ролью ucs_infrastructure и находится по пути /srv/ministerium/config.json
admin.login	Str	+	Логин администратора тенанта
admin.password	Str	+	Пароль администратора тенанта
tenant_id	Str	+	Идентификатор тенанта

Пример ответа:

```
{
  "Response": {
    "msg": "ok",
    "changed": true
  },
  "gals": [
    {
      "id": {
        "id": "3eac9972-c634-4e5b-858a-1043386b4045",
        "region_id": "004bfd74-e829-4224-a28c-620b265b5bc1"
      },
      "path": [
        "gal"
      ]
    }
  ]
}
```

где **gals.id.id** – идентификатор GAL-тега.

2. Выполнить запрос на создание пользователя тенанта:

```
nct_ministerium create_user
--admin.login <...>
--admin.password <...>
--tenant_id 8c13a034-48f5-44e6-9a60-afecda033437
--region_id 004bfd74-e829-4224-a28c-620b265b5bc1
--gal_tags 3eac9972-c634-4e5b-858a-1043386b4045
--login test@domain.ru
```

```
--password ')wx8y(LSpb_8$Duzq1HD'
--E-mail test@domain.ru
--profile.first_name Name
--profile.last_name Family
```

Описание параметров запроса приведено в таблице 63.

Таблица 63 – Описание параметров запроса на создание пользователя тенанта

Параметр	Тип	Обязательный	Описание
config	Str	+	Конфигурационный файл с параметрами сервиса Cox и настройками tls. Формируется автоматически на сервере с ролью ucs_infrastructure и находится по пути /srv/ministerium/config.json
admin.login	Str	+	Логин администратора тенанта
admin.password	Str	+	Пароль администратора тенанта
tenant_id	Str	+	Идентификатор тенанта
region_id	Str	+	Идентификатор региона
gal_tags	Str	+	Идентификаторы GAL-тегов
login	Str	+	Логин создаваемого пользователя тенанта
password	Str	+	Пароль создаваемого пользователя тенанта
E-mail	Str	+	Почтовый ящик создаваемого пользователя тенанта
profile.first_name	Str	+	Имя создаваемого пользователя тенанта
profile.last_name	Str	+	Фамилия создаваемого пользователя тенанта

Пример ответа:

```
{
    "Response": {
      "msg": "ok",
      "changed": true
    },
    "id": "5798aad7-a922-435d-9d8d-ea0818093cc5"
}
```

где **id** – идентификатор созданного пользователя.

3. Выполнить запрос на получение созданного пользователя по его идентификатору:

```
nct_ministerium list_entities
--config ministerium.json
--admin.login <...>
--admin.password <...>
--id aa7287ad-b22d-4a2e-aaf7-f123d71ad7e8
```

Пример ответа:


```
{
  "Response": {
    "msg": "ok"
  },
  "Entities": [
    {
      "id": "5798aad7-a922-435d-9d8d-ea0818093cc5",
      "type": 1,  ### USER ###
      "tenant_id": "8c13a034-48f5-44e6-9a60-afecda033437",
      "region_id": "004bfd74-e829-4224-a28c-620b265b5bc1",
      "roles": [
        "c4b1f72c-672d-5ace-8a6d-96edc21227de"   ### user_regular ###
      ],
      "E-mails": [
        {
          "id": "34df5090-3cd8-5a86-9490-0f91ebe8253d",
          "E-mail": "test@domain.ru"
          "domain_id": "fae98b71-29e5-52ba-ab28-3b4a66643ef1",
          "entity_id": "5798aad7-a922-435d-9d8d-ea0818093cc5",
          "primary": true
        }
      ],
      "logins": [
        {
          "id": "34df5090-3cd8-5a86-9490-0f91ebe8253d",
          "entity_id": "5798aad7-a922-435d-9d8d-ea0818093cc5",
          "login": "test@domain.ru"
          "auth_type": 1
        }
      ],
      "Payload": {
        "User": {
          "locale": "ru_RU"
        }
      },
      "status": 2  ### ACTIVE ###
    }
  ]
}
```


Описание параметров ответа приведено в таблице 64.

Таблица 64 – Описание параметров ответа на запрос на получение созданного пользователя по его идентификатору

Параметр	Тип	Обязательный	Описание
Entities.type	Int	+	Значение должно быть равно 1 (USER)
Entities.tenant_id	Str	+	Значение должно быть равно значению, указанному при создании пользователя
Entities.region_id	Str	+	Значение должно быть равно значению, указанному при

Параметр	Тип	Обязательный	Описание
			создании пользователя
Entities.roles	Str	+	Список ролей должен включать user_regular роль
Entities.E-mails.E-mail	Str	+	Значение должно быть равно значению, указанному при создании пользователя
Entities.E-mails.primary	Bool	+	Значение должно быть равно true
Entities.logins.login	Str	+	Значение должно быть равно значению, указанному при создании пользователя
Entities.Payload.User.locale	Str	+	Если при создании пользователя не была указана локаль, то ее значение должно быть равно значению локали, указанному при создании тенанта
Entities.status	Int	+	Значение должно быть равно 2 (ACTIVE)

В а ж н о – При сбое создания пользователя см. раздел 7.8.

7.3.7 Добавление роли администратора тенанта пользователю

Для добавления роли администратора тенанта необходимо выполнить следующие действия:

1. Выполнить запрос на получение данных пользователя до добавления роли:

```
nct_ministerium list_entities
--admin.login <...>
--admin.password <…>
--id 7b9d0558-f9b9-475b-9c52-1d63a30c3ed6
```

Пример ответа:

```
{
  "Response": {
    "msg": "ok"
  },
  "Entities": [
    {
      "id": "7b9d0558-f9b9-475b-9c52-1d63a30c3ed6",
      "type": 1,
      "tenant_id": "8c13a034-48f5-44e6-9a60-afecda033437",
      "region_id": "004bfd74-e829-4224-a28c-620b265b5bc1",
      "roles": [
```

```
        "c4b1f72c-672d-5ace-8a6d-96edc21227de"
      ],
      .....
    }
  ]
}
```

где "Response.msg": "ok" – признак успешности, а Entities[0].roles – роли пользователя.

2. Выполнить запрос из шага 1 и проверить роли пользователя до добавления новой роли. У пользователя должна быть только одна роль **user_regular**.
3. Выполнить запрос на добавление роли администратора тенанта для созданного пользователя (см. раздел 7.3.8):

```
nct_ministerium set_tenant_administrator
--config /srv/ministerium/config.json
--user_id 7b9d0558-f9b9-475b-9c52-1d63a30c3ed6
```

Пример ответа:

```
{
  "msg": "ok"
}
```

, где "Response.msg": "ok" – признак успешности.

4. Выполнить запрос из шага 1 и проверить роли пользователя. У пользователя должно быть две роли **user_regular** и **admin_tenant**.

7.3.8 Управление администраторами тенанта

Управление администраторами тенанта осуществляется с помощью команд:

– добавление роли администратора **set_tenant_administrator**;

– удаление роли администратора **unset_tenant_administrator**;

– получение списка администраторов тенанта **list_tenant_administrator**.

Описание общих параметров запросов **set_tenant_administrator**, **unset_tenant_administrator**, **list_tenant_administrator** приведено в таблице 65.

Таблица 65 – Описание общих параметров запросов управления администраторами тенанта

Параметр	Тип	Обязательный	Описание
admin.login	string	+	Логин администратора тенанта
admin.password	string	+	Пароль администратора тенанта

Параметр	Тип	Обязательный	Описание
cox.balancer_endpoint	string	+	Endpoint балансировщика нагрузки сервиса
cox.compression	string	-	Метод сжатия данных (варианты: **none**, **gzip**), по умолчанию **none**
cox.endpoint	string	+	Endpoint сервиса
cox.load_balanced	boolean	-	Использовать соединение с балансировщиком
cox.request_timeout	duration	-	Тайм-аут запроса к сервису (по умолчанию 2 секунды)
cox.service_name	string	-	Имя сервиса балансировщика
cox.use_tls	boolean	+	TLS-сертификат
cox.use_tls_balancer	boolean	-	Защищенная передача данных при подключении к балансировщику
tls_settings.ca_file	string	+	Путь к CA файлу
tls_settings.client_cert_file	string	+	Путь к файлу сертификата клиента
tls_settings.key_file	string	+	Путь к файлу с ключом клиента
token-name	string	+	Имя токена для подключения
user_id	string	+	Идентификатор пользователя

1. Пример добавления роли администратора **set_tenant_administrator**:

```
nct_ministerium set_tenant_administrator
--admin.login <...>
--admin.password <...>
--cox.balancer_endpoint=hydra.ucs-apps-1.installation.example.net:50053
--cox.compression=none
--cox.endpoint=grpc-mydomain.ru:3142
--cox.load_balanced=false
--cox.request_timeout=10s
--cox.service_name=cox
--cox.use_tls=true
--cox.use_tls_balancer=false
--tls_settings.ca_file .../certs/ca.pem
--tls_settings.key_file .../certs/client_key.pem
--token-name ucs-access-token
--user_id 7b9d0558-f9b9-475b-9c52-1d63a30c3ed6
```

Параметр **user_id** содержит идентификатор пользователя, который будет добавлен в качестве администратора тенанта.

2. Пример удаления роли администратора **unset_tenant_administrator**:

```
nct_ministerium unset_tenant_administrator
--admin.login <...>
--admin.password <...>
```

```
--cox.balancer_endpoint=hydra.ucs-apps-1.installation.example.net:50053
--cox.compression=none
--cox.endpoint=grpc-mydomain.ru:3142
--cox.load_balanced=false
--cox.request_timeout=10s
--cox.service_name=cox
--cox.use_tls=true
--cox.use_tls_balancer=false
--tls_settings.ca_file .../certs/ca.pem
--tls_settings.key_file .../certs/client_key.pem
--token-name ucs-access-token
--user_id 7b9d0558-f9b9-475b-9c52-1d63a30c3ed6
```

Параметр **user_id** содержит идентификатор пользователя, который будет удален из списка администраторов тенанта.

3. Пример получения списка администраторов тенанта **list_tenant_administrator**:

```
nct_ministerium list_tenant_administrator
--admin.login <...>
--admin.password <...>
--cox.balancer_endpoint=hydra.ucs-apps-1.installation.example.net:50053
--cox.compression=none
--cox.endpoint=grpc-mydomain.ru:3142
--cox.load_balanced=false
--cox.request_timeout=10s
--cox.service_name=cox
--cox.use_tls=true
--cox.use_tls_balancer=false
--tls_settings.ca_file .../certs/ca.pem
--tls_settings.key_file .../certs/client_key.pem
--token-name ucs-access-token
--tenant_id 7b9d0558-f9b9-475b-9c52-1d63a30c3ed6
```

Параметр **tenant_id** содержит идентификатор тенанта, для которого будет получен список администраторов.

7.3.9 Настройка квот в тенанте

Чтобы задать ограничения размеров отдельного почтового сообщения, общего объема почтовых сообщений в почтовом ящике или ограничить суммарный размер вложений в письме, в ПО «Mailion» используется механизм определения квот. Квоты могут быть назначены на разных уровнях – на уровне тенанта, а также на уровне отдельного пользователя. Квоты, заданные на уровне пользователя, имеют преимущество перед квотами на уровне тенанта.

В а ж н о – Настройки квот в тенанте может выполнить только пользователь с ролью администратора тенанта.

Для настройки квот используются команды, приведенные в таблице 66.

Таблица 66 – Команды для настройки квот

Доступные команды	Описание
create_tenant_quotas_profile	Создать квоты профиля тенанта
create_user_quotas_profile	Создать квоты профиля пользователя. Используются параметры: – "MAIL_COUNT_LIMIT" – количество писем за указанный период; – "MAIL_COUNT_TIME_LIMIT" – период в секундах. Например, если MAIL_COUNT_LIMIT=2 и MAIL_COUNT_TIME_LIMIT=60, то пользователь не сможет отправить больше двух писем в минуту
delete_tenant_quotas_profile	Удалить квоты профиля тенанта
get_recount_quotas_processes	Получить все запущенные процессы пересчета квот
get_user_quotas_profile	Получить квоты профиля пользователя
recount_quotas	Начать процесс напоминания о пересчете квот для одиночного объекта или всех объектов в тенанте
remove_user_quotas_profile	Удалить квоты профиля пользователя
stop_recount_quotas	Остановить процесс пересчета квоты. Некоторые объекты могли иметь непредвиденные упоминания о квотах
update_tenant_quotas_profile	Обновить квоты профиля тенанта
update_user_quotas_profile	Обновить квоты профиля пользователя
get_total_quotas	Получить размер общей квоты, выделенной на тенант
update_total_quotas	Обновить общую квоту

7.3.9.1 Создание квот профиля

Пример запроса на создание квот профиля тенанта:

```
nct_ministerium create_tenant_quotas_profile
--admin.login <…>
--admin.password <…>
--tenant_id 9d5dc502-51d8-4dc0-a7a8-0856639ec0d1
--quotas {\"ONE_MAIL_SIZE\": \"1M\"}
--cox.balancer_endpoint=hydra.ucs-apps-1.installation.example.net:50053
--cox.compression=none
--cox.endpoint=grpc-mydomain.ru:3142
--cox.load_balanced=false
--cox.request_timeout=10s
--cox.service_name=cox
--cox.use_tls=true
```

```
--cox.use_tls_balancer=false
--tls_settings.ca_file .../certs/ca.pem
--tls_settings.client_cert_file .../certs/client_crt.pem
--tls_settings.key_file .../certs/client_key.pem
```

Описание параметров запроса на создание квот профиля тенанта приведено в таблице 67.

Таблица 67 – Описание параметров запроса на создание квот профиля тенанта

Параметр	Тип	Обязательный	Описание
admin.login	Str	+	Логин администратора тенанта
admin.password	Str	+	Пароль администратора тенанта
tenant_id	Str	+	Идентификатор тенанта
quotas	Str	+	Список квот для пользователей: – ONE_MAIL_SIZE (размер письма); – ALL_MAILS_SIZE (размер всех писем); – ALL_MAIL_ATTACHMENTS_SIZE (размер всех вложений в письме)
cox.balancer_endpoint	Str	+	Endpoint балансировщика нагрузки сервиса
cox.compression	Str	+	Метод сжатия данных (варианты: **none**, **gzip**), по умолчанию **none**
cox.endpoint	Str	+	Endpoint сервиса
cox.load_balanced	Bool	+	Балансировщик нагрузки сервиса
cox.request_timeout	Str	+	Тайм-аут запроса к сервису
cox.service_name	Str	+	Имя сервиса
cox.use_tls	Bool	+	TLS-сертификат
cox.use_tls_balancer	Bool	+	Защищенная передача данных при подключении к балансировщику
tls_settings.ca_file	Str	+	Путь к CA файлу
tls_settings.client_cert_file	Str	+	Путь к файлу сертификата клиента
tls_settings.key_file	Str	+	Путь к файлу с ключом клиента

Пример ответа на данный запрос:

```
{
  "msg": "ok",
  "changed": true
}
```

7.3.9.2 Удаление квот профиля

Пример запроса на удаления квот профиля тенанта:

```
nct_ministerium delete_tenant_quotas_profile
--admin.login <…>
--admin.password <…>
--tenant_id 9d5dc502-51d8-4dc0-a7a8-0856639ec0d1
--cox.balancer_endpoint=hydra.ucs-apps-1.installation.example.net:50053
--cox.compression=none
--cox.endpoint=grpc-mydomain.ru:3142
--cox.load_balanced=false
--cox.request_timeout=10s
--cox.service_name=cox
--cox.use_tls=true
--cox.use_tls_balancer=false
--tls_settings.ca_file .../certs/ca.pem
--tls_settings.client_cert_file .../certs/client_crt.pem
--tls_settings.key_file .../certs/client_key.pem
```

Описание параметров запроса на удаление квот профиля тенанта приведено в таблице 68.

Таблица 68 – Описание параметров запроса на удаление квот профиля тенанта

Параметр	Тип	Обязательный	Описание
admin.login	string	+	Логин администратора тенанта
admin.password	string	+	Пароль администратора тенанта
tenant_id	string	+	Идентификатор тенанта
cox.balancer_endpoint	string	+	Endpoint балансировщика нагрузки сервиса
cox.compression	string	+	Метод сжатия данных (варианты: **none**, **gzip**), по умолчанию **none**
cox.endpoint	string	+	Endpoint сервиса
cox.load_balanced	boolean	+	Балансировщик нагрузки сервиса
cox.request_timeout	string	+	Тайм-аут запроса к сервису
cox.service_name	string	+	Имя сервиса
cox.use_tls	boolean	+	TLS-сертификат
cox.use_tls_balancer	boolean	+	Защищенная передача данных при подключении к балансировщику
tls_settings.ca_file	string	+	Путь к CA файлу
tls_settings.client_cert_file	string	+	Путь к файлу сертификата клиента

Параметр	Тип	Обязательный	Описание
tls_settings.key_file	string	+	Путь к файлу с ключом клиента

Пример ответа на данный запрос:

```
{
  "msg": "ok",
  "changed": true
}
```

7.3.9.3 Обновление квот профиля

Пример запроса на обновление квот профиля тенанта:

```
nct_ministerium update_tenant_quotas_profile
--admin.login <…>
--admin.password <…>
--tenant_id 9d5dc502-51d8-4dc0-a7a8-0856639ec0d1
--quotas {\"ONE_MAIL_SIZE\": \"15M\", \"ALL_MAILS_SIZE\": \"35M\",
\"ALL_MAIL_ATTACHMENTS_SIZE\": \"15M\"}
--cox.balancer_endpoint=hydra.ucs-apps-1.installation.example.net:50053
--cox.compression=none
--cox.endpoint=grpc-mydomain.ru:3142
--cox.load_balanced=false
--cox.request_timeout=10s
--cox.service_name=cox
--cox.use_tls=true
--cox.use_tls_balancer=false
--tls_settings.ca_file .../certs/ca.pem
--tls_settings.client_cert_file .../certs/client_crt.pem
--tls_settings.key_file .../certs/client_key.pem
```

Описание параметров запроса на обновление квот профиля приведено в таблице 69.

Таблица 69 – Описание параметров запроса на обновление квот профиля

Параметр	Тип	Обязательный	Описание
admin.login	Str	+	Логин администратора тенанта
admin.password	Str	+	Пароль администратора тенанта
tenant_id	Str	+	Идентификатор тенанта
quotas	Str	+	Список квот для пользователей: – ONE_MAIL_SIZE (размер письма); – ALL_MAILS_SIZE (размер всех писем); – ALL_MAIL_ATTACHMENTS_SIZE (размер всех вложений в письме)
cox.balancer_endpoint	Str	+	Endpoint балансировщика нагрузки сервиса

Параметр	Тип	Обязательный	Описание
cox.compression	Str	+	Метод сжатия данных (варианты: **none**, **gzip**), по умолчанию **none**
cox.endpoint	Str	+	Endpoint сервиса
cox.load_balanced	Bool	+	Балансировщик нагрузки сервиса
cox.request_timeout	Str	+	Тайм-аут запроса к сервису
cox.service_name	Str	+	Имя сервиса
cox.use_tls	Bool	+	TLS-сертификат
cox.use_tls_balancer	Bool	+	Защищенная передача данных при подключении к балансировщику
tls_settings.ca_file	Str	+	Путь к CA файлу
tls_settings.client_cert_file	Str	+	Путь к файлу сертификата клиента
tls_settings.key_file	Str	+	Путь к файлу с ключом клиента

Пример ответа на данный запрос:

```
{
  "msg": "ok",
  "changed": true
}
```

7.3.9.4 Создание квот профиля пользователя

Пример запроса на создание квот профиля пользователя:

```
nct_ministerium create_user_quotas_profile
--admin.login <…>
--admin.password <…>
--tenant_id 01068ade-1cce-4125-ab6b-91d977ecf85b
--entity_id 8b3c878b-9e26-440f-84db-aabce7e5e75f
--quotas {\"ONE_MAIL_SIZE\": \"1M\", \"ALL_MAILS_SIZE\": \"1M\",
\"ALL_MAIL_ATTACHMENTS_SIZE\": \"1M\"}
--cox.balancer_endpoint=hydra.ucs-apps-1.installation.example.net:50053
--cox.compression=none
--cox.endpoint=grpc-mydomain.ru:3142
--cox.load_balanced=false
--cox.request_timeout=10s
--cox.service_name=cox
--cox.use_tls=true
--cox.use_tls_balancer=false
--tls_settings.ca_file .../certs/ca.pem
--tls_settings.client_cert_file .../certs/client_crt.pem
--tls_settings.key_file .../certs/client_key.pem
```

Описание параметров запроса на создание квот профиля пользователя приведено в таблице 70.

Таблица 70 – Описание параметров запроса на создание квот профиля пользователя

Параметр	Тип	Обязательный	Описание
admin.login	Str	+	Логин администратора тенанта
admin.password	Str	+	Пароль администратора тенанта
tenant_id	Str	+	Идентификатор тенанта
entity_id	Str	+	Идентификатор пользователя
quotas	Str	+	Список квот для пользователей: – ONE_MAIL_SIZE (размер письма); – ALL_MAILS_SIZE (размер всех писем); – ALL_MAIL_ATTACHMENTS_SIZE (размер всех вложений в письме)
cox.balancer_endpoint	Str	+	Endpoint балансировщика нагрузки сервиса
cox.compression	Str	+	Метод сжатия данных (варианты: **none**, **gzip**), по умолчанию **none**
cox.endpoint	Str	+	Endpoint сервиса
cox.load_balanced	Bool	+	Балансировщик нагрузки сервиса
cox.request_timeout	Str	+	Тайм-аут запроса к сервису
cox.service_name	Str	+	Имя сервиса
cox.use_tls	Bool	+	TLS-сертификат
cox.use_tls_balancer	Bool	+	Защищенная передача данных при подключении к балансировщику
tls_settings.ca_file	Str	+	Путь к CA файлу
tls_settings.client_cert_file	Str	+	Путь к файлу сертификата клиента
tls_settings.key_file	Str	+	Путь к файлу с ключом клиента

Пример ответа на данный запрос:

```
{
  "msg": "ok",
  "changed": true
}
```

7.3.9.5 Удаление квот профиля пользователя

Пример запроса на удаление квот профиля пользователя:

```
nct_ministerium remove_user_quotas_profile
--admin.login <…>
--admin.password <…>
--tenant_id 01068ade-1cce-4125-ab6b-91d977ecf85b
--entity_id e1257024-5dc4-446a-abae-e15eb4273297
--cox.balancer_endpoint=hydra.ucs-apps-1.installation.example.net:50053
--cox.compression=none
--cox.endpoint=grpc-mydomain.ru:3142
--cox.load_balanced=false
--cox.request_timeout=10s
--cox.service_name=cox
--cox.use_tls=true
--cox.use_tls_balancer=false
--tls_settings.ca_file .../certs/ca.pem
--tls_settings.client_cert_file .../certs/client_crt.pem
--tls_settings.key_file .../certs/client_key.pem
```

Описание параметров запроса на удаление квот профиля приведено в таблице 71.

Таблица 71 – Описание параметров запроса на обновление квот профиля пользователя

Параметр	Тип	Обязательный	Описание
admin.login	Str	+	Логин администратора тенанта
admin.password	Str	+	Пароль администратора тенанта
tenant_id	Str	+	Идентификатор тенанта
entity_id	Str	+	Идентификатор пользователя
cox.balancer_endpoint	Str	+	Endpoint балансировщика нагрузки сервиса
cox.compression	Str	+	Метод сжатия данных (варианты: **none**, **gzip**), по умолчанию **none**
cox.endpoint	Str	+	Endpoint сервиса
cox.load_balanced	Bool	+	Балансировщик нагрузки сервиса
cox.request_timeout	Str	+	Тайм-аут запроса к сервису
cox.service_name	Str	+	Имя сервиса
cox.use_tls	Bool	+	TLS-сертификат
cox.use_tls_balancer	Bool	+	Защищенная передача данных при подключении к балансировщику
tls_settings.ca_file	Str	+	Путь к CA файлу
tls_settings.client_cert_file	Str	+	Путь к файлу сертификата клиента

Параметр	Тип	Обязательный	Описание
tls_settings.key_file	Str	+	Путь к файлу с ключом клиента

Пример ответа на данный запрос:

```
{
  "msg": "ok",
  "changed": true
}
```

7.3.9.6 Обновление квот профиля пользователя

Пример запроса на обновления квот профиля пользователя:

```
nct_ministerium update_user_quotas_profile
--admin.login <…>
--admin.password <…>
--tenant_id 01068ade-1cce-4125-ab6b-91d977ecf85b
--entity_id 0e1e6928-bf56-460e-a8b7-b16c681913d7
--quotas {\"ONE_MAIL_SIZE\": \"2M\", \"ALL_MAILS_SIZE\": \"2M\",
\"ALL_MAIL_ATTACHMENTS_SIZE\": \"2M\"}
--cox.balancer_endpoint=hydra.ucs-apps-1.installation.example.net:50053
--cox.compression=none
--cox.endpoint=grpc-mydomain.ru:3142
--cox.load_balanced=false
--cox.request_timeout=10s
--cox.service_name=cox
--cox.use_tls=true
--cox.use_tls_balancer=false
--tls_settings.ca_file .../certs/ca.pem
--tls_settings.client_cert_file .../certs/client_crt.pem
--tls_settings.key_file .../certs/client_key.pem
```

Описание параметров запроса на обновление квот профиля приведено в таблице 72.

Таблица 72 – Описание параметров запроса на обновление квот профиля пользователя

Параметр	Тип	Обязательный	Описание
admin.login	Str	+	Логин администратора тенанта
admin.password	Str	+	Пароль администратора тенанта
tenant_id	Str	+	Идентификатор тенанта
entity_id	Str	+	Идентификатор пользователя
quotas	Str	+	Список квот для пользователей: – ONE_MAIL_SIZE (размер письма); – ALL_MAILS_SIZE (размер всех писем); – ALL_MAIL_ATTACHMENTS_SIZE (размер всех вложений в письме)

Параметр	Тип	Обязательный	Описание
cox.balancer_endpoint	Str	+	Endpoint балансировщика нагрузки сервиса
cox.compression	Str	+	Метод сжатия данных (варианты: **none**, **gzip**), по умолчанию **none**
cox.endpoint	Str	+	Endpoint сервиса
cox.load_balanced	Bool	+	Балансировщик нагрузки сервиса
cox.request_timeout	Str	+	Тайм-аут запроса к сервису
cox.service_name	Str	+	Имя сервиса
cox.use_tls	Bool	+	TLS-сертификат
cox.use_tls_balancer	Bool	+	Защищенная передача данных при подключении к балансировщику
tls_settings.ca_file	Str	+	Путь к CA файлу
tls_settings.client_cert_file	Str	+	Путь к файлу сертификата клиента
tls_settings.key_file	Str	+	Путь к файлу с ключом клиента

Пример ответа на данный запрос:

```
{
  "msg": "ok",
  "changed": true
}
```

7.3.9.7 Получение квот профиля

Пример запроса на получение квот профиля пользователя:

```
nct_ministerium get_user_quotas_profile
--admin.login <…>
--admin.password <…>
--tenant_id 01068ade-1cce-4125-ab6b-91d977ecf85b
--entity_id b8740313-c64e-427f-8635-ecbb083d2435
--cox.balancer_endpoint=hydra.ucs-apps-1.installation.example.net:50053
--cox.compression=none
--cox.endpoint=grpc-mydomain.ru:3142
--cox.load_balanced=false
--cox.request_timeout=10s
--cox.service_name=cox
--cox.use_tls=true
--cox.use_tls_balancer=false
--tls_settings.ca_file .../certs/ca.pem
--tls_settings.client_cert_file .../certs/client_crt.pem
--tls_settings.key_file .../certs/client_key.pem
```

Описание параметров запроса приведено в таблице 73.

Таблица 73 – Описание параметров запроса на получение квот профиля пользователя

Параметр	Тип	Обязательный	Описание
admin.login	Str	+	Логин администратора тенанта
admin.password	Str	+	Пароль администратора тенанта
tenant_id	Str	+	Идентификатор тенанта
entity_id	Str	+	Идентификатор пользователя
cox.balancer_endpoint	Str	+	Endpoint балансировщика нагрузки сервиса
cox.compression	Str	+	Метод сжатия данных (варианты: **none**, **gzip**), по умолчанию **none**
cox.endpoint	Str	+	Endpoint сервиса
cox.load_balanced	Bool	+	Балансировщик нагрузки сервиса
cox.service_name	Str	+	Имя сервиса
cox.use_tls_balancer	Bool	+	Защищенная передача данных при подключении к балансировщику
tls_settings.ca_file	Str	+	Путь к CA файлу
tls_settings.client_cert_file	Str	+	Путь к файлу сертификата клиента
tls_settings.key_file	Str	+	Путь к файлу с ключом клиента

Пример ответа:

```
{
  "Response": {
    "msg": "ok",
    "changed": true
  },
  "quotas_limits": {
    "ALL_MAILS_SIZE": "1G"
  },
  "quotas": {}
}
```

7.3.9.8 Установка общей квоты тенанта на почту

Пользователь с ролью администратора тенанта может установить общую квоту тенанта на почту. Если данная квота не установлена, то лимитировать размер почтовой квоты на тенант будет общая квота тенанта, установленная администратором инсталляции (см. раздел 7.2).

Пример запроса на установку общей почтовой квоты:

```
nct_ministerium update_total_quotas
--admin.login ***
--admin.password ***
--mail_total.active_quotas ALL_MAILS_SIZE
--mail_total.max_size 40gb
--config ministerium.json
--tenant_id 2a3b8043-70ef-4a59-a395-9e28cc5c2685
```

Описание параметров запроса приведено в таблице 74.

Таблица 74 – Описание параметров запроса на установку общей почтовой квоты

Параметр	Тип	Обязательный	Описание
admin.login	Str	+	Логин администратора тенанта
admin.password	Str	+	Пароль администратора тенанта
mail_total.active_ quotas	Str	+	Перечень квот, участвующих в подсчете почтовой квоты
mail_total.max_size	Str	+	Размер почтовой квоты тенанта
config	Str	+	Конфигурационный файл с параметрами сервиса Cox и настройками tls. Формируется автоматически на сервере с ролью ucs_infrastructure и находится по пути /srv/ministerium/config.json
tenant_id	Str	+	Идентификатор тенанта

Пример ответа:

```
{
  "changed": true,
  "failed": false,
  "msg": "ok"
}
```

7.3.9.9 Получение общей квоты на тенант и общей квоты тенанта на почту

Пользователь с ролью администратора тенанта может получить размер общей квоты на тенант и общей квоты тенанта на почту.

Пример запроса на получение размера общей квоты на тенант и общей квоты тенанта на почту:

```
nct_ministerium get_total_quotas
--admin.login ***
--admin.password ***
```

```
--config ministerium.json
--tenant_id 2a3b8043-70ef-4a59-a395-9e28cc5c2685
```

Описание параметров запроса приведено в таблице 75.

Таблица 75 – Параметры запроса на получение размера общей квоты

Параметр	Тип	Обязательный	Описание
admin.login	Str	+	Логин администратора тенанта
admin.password	Str	+	Пароль администратора тенанта
config	Str	+	Конфигурационный файл с параметрами сервиса Cox и настройками tls. Формируется автоматически на сервере с ролью ucs_infrastructure и находится по пути /srv/ministerium/config.json
tenant_id	Str	+	Идентификатор тенанта

Пример ответа:

```
{
  "Response": {
    "changed": false,
    "failed": false,
    "msg": "ok"
  },
  "mail_total_quota": {
    "max_size": 42949672960,
    "active_quotas": [
      2
    ]
  },
  "tenant_total_quota": {
    "max_size": 42949672960
  }
}
```

7.3.9.10 Нулевая квота пользователя

Если задана общая квота тенанта, то при создании пользователя в ней может не хватить места на его квоту. В таком случае для нового пользователя будет создан профиль квот, где его квота будет равна нулю. Он не будет занимать место в общей квоте тенанта, но не сможет писать или получать письма.

Чтобы узнать перечень пользователей, получивших нулевую квоту, необходимо выполнить запрос:

```
get_users_with_zero_quota
--config cfg.json
--tenant_id <>
--admin.login <>
--admin.password <>
```

Описание параметров запроса приведено в таблице 76.

Таблица 76 – Описание параметров запроса на просмотр пользователей с нулевой квотой

Параметр	Тип	Обязательный	Описание
config	Str	+	Конфигурационный файл с параметрами сервиса Cox и настройками tls. Формируется автоматически на сервере с ролью ucs_infrastructure и находится по пути /srv/ministerium/config.json
admin.login	Str	+	Логин администратора тенанта
admin.password	Str	+	Пароль администратора тенанта
tenant_id	Str	+	Идентификатор тенанта

Пример ответа:

```
{
  "Response": {
    "changed": false,
    "failed": false,
    "msg": "ok"
  },
  "users_ids": {"id1", "id2", ...}
}
```

7.3.10 Установка лимитов почты в тенанте

Лимиты почты в тенанте устанавливаются следующей командой:

```
nct_ministerium update_tenant_limits
--admin.login ***
--admin.password ***
--tenant_id ***
--limits '{"ONE_MAIL_SIZE_OUTGOING": "30MB",
"ONE_MAIL_SIZE_INCOMING": "30MB",
"ALL_MAIL_ATTACHMENTS_SIZE_INCOMING": "25MB",
"ALL_MAIL_ATTACHMENTS_SIZE_OUTGOING": "25MB",
"ONE_MAIL_SIZE_OUTGOING_EXTERNAL": "30MB",
"ALL_MAIL_ATTACHMENTS_SIZE_OUTGOING_EXTERNAL": "25MB",
"ONE_MAIL_SIZE_INCOMING_EXTERNAL": "30MB",
"ALL_MAIL_ATTACHMENTS_SIZE_INCOMING_EXTERNAL": "25MB"}'
```

Описание параметров запроса приведено в таблице 77.

Таблица 77 – Описание параметров запроса на удаление администратора тенанта

Параметр	Тип	Обязательный	Описание
admin.login	Str	+	Логин администратора тенанта
admin.password	Str	+	Пароль администратора тенанта
tenant_id	Str	+	Идентификатор тенанта
limits	Str	+	Настройки лимитов

Значения полей параметра `limits`:

- `ONE_MAIL_SIZE_OUTGOING`: максимальный размер исходящего сообщения;
- `ONE_MAIL_SIZE_INCOMING`: максимальный размер входящего сообщения;
- `ALL_MAIL_ATTACHMENTS_SIZE_INCOMING`: максимальный суммарный размер всех вложений письма для входящих сообщений;
- `ALL_MAIL_ATTACHMENTS_SIZE_OUTGOING`: максимальный суммарный размер всех вложений письма для исходящих сообщений;
- `ONE_MAIL_SIZE_OUTGOING_EXTERNAL`: максимальный размер внешнего исходящего сообщения;
- `ALL_MAIL_ATTACHMENTS_SIZE_OUTGOING_EXTERNAL`: максимальный суммарный размер всех вложений письма для внешних исходящих сообщений;
- `ONE_MAIL_SIZE_INCOMING_EXTERNAL`: максимальный размер внешнего входящего сообщения;

– ALL_MAIL_ATTACHMENTS_SIZE_INCOMING_EXTERNAL: максимальный суммарный размер всех вложений письма для внешних входящих сообщений.

7.3.11 Удаление тенанта

Для удаления тенанта необходимо выполнить запрос на удаление тенанта:

```
nct_ministerium delete_tenant
--admin.login <…>
--admin.password <...>
--tenant_id ef28480f-0ee4-4f0c-af67-59f100727f31
--cox.balancer_endpoint=hydra.<domain>:<port>
--cox.endpoint=<domain>:<port>
--cox.load_balanced=false
--cox.request_timeout=10s
--cox.service_name=cox
--cox.use_tls=true
--cox.use_tls_balancer=false
--tls_settings.ca_file <…/ca.pem>
--tls_settings.client_cert_file <…/client_crt.pem>
--tls_settings.key_file <…/client_key.pem>
```

Описание параметров запроса приведено в таблице 78.

Таблица 78 – Описание параметров запроса на удаление тенанта

Параметр	Тип	Обязательный	Описание
admin.login	Str	+	Логин администратора тенанта
admin.password	Str	+	Пароль администратора тенанта
tenant_id	Str	+	Идентификатор тенанта
cox.balancer_endpoint	Str	+	Endpoint балансировщика нагрузки сервиса
cox.endpoint	Str	+	Endpoint сервиса
cox.load_balanced	Bool	+	Балансировщик нагрузки сервиса
cox.request_timeout	Str	+	Тайм-аут запроса к сервису
cox.service_name	Str	+	Имя сервиса
cox.use_tls	Bool	+	TLS-сертификат
cox.use_tls_balancer	Bool	+	Защищенная передача данных при подключении к балансировщику
tls_settings.ca_file	Str	+	Путь к CA файлу
tls_settings.client_cert_file	Str	+	Путь к файлу сертификата клиента
tls_settings.key_file	Str	+	Путь к файлу с ключом клиента

Важно – На момент удаления тенанта в нем не должно быть доменов и пользователей. При выполнении команды удаления тенант не удаляется физически, а помечается для удаления. После выполнения команды удаления тенант становится недоступным в системе, но физически продолжает существовать.

7.3.12 Учетная запись для резервного копирования

У обычных учетных записей, даже у администраторов, нет прав на выполнение операций резервного копирования и восстановления. Для выполнения этих операций необходимо использовать специальные учетные записи – **«backuper тенанта»** и/или **«backuper инсталляции»**.

Так же как и учетная запись администратора инсталляции, при первоначальной установке автоматически создается специальный пользователь **«backuper»** с правами на резервное копирование инсталляции. Он может делать резервные копии и восстановление всех данных инсталляции. Пароль для этой учетной записи задается через новый параметр Mailion `mailion_installation_backuper_password`.

Администратор тенанта может создать специального пользователя **«backuper тенанта»**. Этот пользователь сможет делать резервные копии и восстановление всех данных этого тенанта. Создать его можно с помощью команды **ministerium**:

```
nct_ministerium create_tenant_backuper
--config ministerium.json
--admin.login <...>
--admin.password <...>
--tenant_id ef28480f-0ee4-4f0c-af67-59f100727f31
--region_id 004bfd74-e829-4224-a28c-620b265b5bc1
--gal_tags 11cd3c1a-9f14-4810-acc6-4a7b2aacb540
--login admin2.tenant2_test
--password 'BnYs6j*Hw_TT$X)MsD59'
--profile.first_name Admin2
--profile.last_name Test
```

Описание параметров запроса приведено в таблице 79.

Таблица 79 – Описание параметров запроса на создание бэкапера тенанта

Параметр	Тип	Обязательный	Описание
config	Str	+	Конфигурационный файл с параметрами сервиса Cox и настройками tls. Формируется автоматически на сервере с ролью ucs_infrastructure и находится по пути /srv/ministerium/config.json
admin.login	Str	+	Логин администратора тенанта
admin.password	Str	+	Пароль администратора тенанта
tenant_id	Str	+	Идентификатор тенанта
region_id	Str	+	Идентификатор региона
gal_tags	Str	+	Идентификаторы GAL-тегов
login	Str	+	Логин создаваемого бэкапера тенанта
password	Str	+	Пароль создаваемого бэкапера тенанта
profile.first_name	Str	+	Имя создаваемого бэкапера тенанта
profile.last_name	Str	+	Фамилия создаваемого бэкапера тенанта

7.3.13 Удаление письма у всех получателей в рамках тенанта

Важно – Удаление письма выполняется пользователем с ролью администратора тенанта.

Для удаления письма у всех получателей в рамках тенанта необходимо выполнить следующие действия:

1. В представлении **Почта** необходимо выбрать письмо из любой папки. Подробная информация приведена в документе «Программное обеспечение «Корпоративная система электронной почты и планирования совместной работы команд «Mailion». Руководство оператора» RU.29144487.506900.001 34.
2. При открытии письма в консоли браузера формируется запрос **build_message**. Необходимо скопировать идентификаторы письма из сообщения вида:

```
{"msg":{"id":"61c45c6c-937f-4065-a204-04b0e0091dbb","region_id":"2dbacea3-5889-4021-8f38-bc2214dd7423"}}
```

3. Выполнить запрос на удаление письма:

```
nct_ministerium delete_all_related_messages_by_message_id
--config nct-ministerium.json
--message_id 61c45c6c-937f-4065-a204-04b0e0091dbb
--region_id 2dbacea3-5889-4021-8f38-bc2214dd7423
--tenant_id 01068ade-1cce-4125-ab6b-91d977ecf85b
```

Описание параметров запроса приведено в таблице 80.

Таблица 80 – Описание параметров запроса на удаление письма

Параметр	Тип	Обязательный	Описание
message_id	Str	+	Идентификатор сообщения, которое необходимо удалить
region_id	Str	+	Регион, в котором находится сообщение
tenant_id	Str	+	Идентификатор тенанта, в рамках которого удаляются сообщения

Пример ответа:

```
{
  "Response": {
    "msg": "ok",
    "changed": true
  }
}
```

После этого выбранное письмо удалится.

7.4 Создание пользовательских GAL-тегов

Пользовательский GAL-тег – это тег глобальной адресной книги, который обозначает категорию, метку или дополнительные атрибуты, присваиваемые контактам.

В а ж н о – Перед созданием пользовательских GAL-тегов должен быть создан администратор тенанта.

Чтобы создать пользовательские теги, предварительно необходимо создать пользователя. Для создания пользовательских GAL-тегов необходимо выполнить следующие действия:

1. Выполнить запрос на создание пользовательского GAL-тега:

```
nct_ministerium create_tenant_gal_tag
--config ministerium.json
--path february_03_gal_tag
--tenant_id 8c13a034-48f5-44e6-9a60-afecda033437
```

Описание параметров запроса приведено в таблице 81.

Таблица 81 – Описание параметров запроса на получение созданного пользователя по его идентификатору

Параметр	Тип	Обязательный	Описание
config	Str	+	Конфигурационный файл с параметрами сервиса Cox и настройками tls. Формируется автоматически на сервере с ролью ucs_infrastructure и находится по пути /srv/ministerium/config.json
path	Str	+	Путь к GAL-тегу
tenant_id	Str	+	Идентификатор тенанта

Пример ответа:

```
{
  "Response": {
    "msg": "ok",
    "changed": true
  },
  "gal": {
    "id": {
      "id": "559368c3-2ee4-43a4-966d-0904341f05f0",
      "region_id": "004bfd74-e829-4224-a28c-620b265b5bc1"
    },
    "path":
     [
      "april_26_gal_tag"
    ]
  }
}
```

где **gal.id.id** – идентификатор GAL-тега.

2. Выполнить запрос на получение GAL-тегов тенанта:

```
nct_ministerium get_tenant_gals
--config ministerium.json
--tenant_id 8c13a034-48f5-44e6-9a60-afecda033437
```

Пример ответа:

```
{
   "Response": {
     "msg": "ok",
     "changed": true
   },
   "gals": [
     ...
     {
       "id": {
         "id": "559368c3-2ee4-43a4-966d-0904341f05f0",
         "region_id": "004bfd74-e829-4224-a28c-620b265b5bc1"
       },
```

```
      "path": [
        "april_26_gal_tag"
      ] },
    ...
  ]
}
```

Для добавления пользователя в GAL-тег необходимо использовать команду **add_users_to_gal_tag**.

7.5 Работа с импортированными контактами

7.5.1 Импортирование контактов

Импорт контактов производится командой **add_contacts_to_gal_tag**.

```
nct_ministerium add_contacts_to_gal_tag \
--admin.login *** \
--admin.password *** \
--gal_id *** \
--contacts_file gal_contacts_1.json \
--cox.balancer_endpoint=hydra.ucs-apps-1.zulu.example.ru:50053 \
--cox.compression=none \
--cox.endpoint=grpc-devmail.example.ru:3142 \
--cox.load_balanced=false \
--cox.request_timeout=10s \
--cox.service_name=cox \
--cox.use_tls=true \
--cox.use_tls_balancer=false \
--tls_settings.ca_file /***/ca.pem \
--tls_settings.client_cert_file /***/client_crt.pem \
--tls_settings.key_file /***/client_key.pem \
--v
```

Параметр **contacts_file** содержит имя файла формата JSON, который содержит записи для импорта.

Пример:

```
{
    "first_name": "galcontact-test-name-1",
    "last_name": "galcontact-test-last-1",
    "middle_name": "galcontact-test-middle-1",
    "locale": "RU",
    "department": "IT",
    "title": "Developer",
    "organization": "Org1",
    "phones": [
        {
            "value": "89181234567",
            "preferable": true,
            "type": [
```

```
                2
            ]
        }
    ],
    "gender": 1,
    "birthday": "2023-12-31",
    "emails": [
        {
            "value": "galcontact.test.1@example.ru",
            "preferable": true,
            "type": 2
        }
    ],
    "addresses": [
        {
            "name": "addr1",
            "country": "RU",
            "region": "23",
            "city": "KRD",
            "zip_code": "350000",
            "address": "K",
            "floor": "3",
            "room": "42",
            "workplace": "15",
            "preference": 1,
            "type": "HOME"
        }
    ],
    "description": "Description1"
}
{
    "first_name": "galcontact-test-name-2",
     ....................................
}
```

Описание параметров запроса на импорт контактов приведено в таблице 82.

Таблица 82 – Описание параметров запроса на импорт контактов

Параметр	Тип	Обязательный	Описание
admin.login	Str	+	Логин администратора тенанта
admin.password	Str	+	Пароль администратора тенанта
gal_id	Str	+	Идентификатор GAL
contacts_file	Str	+	Имя файла (формат JSON), содержащего записи для импорта
cox.balancer_endpoint	Str	+	Endpoint балансировщика нагрузки сервиса
cox.compression	Str	+	Метод сжатия данных (варианты: **none**, **gzip**), по умолчанию **none**
cox.endpoint	Str	+	Endpoint сервиса
cox.load_balanced	Bool	+	Балансировщик нагрузки сервиса

Параметр	Тип	Обязательный	Описание
cox.request_timeout	Str	+	Тайм-аут запроса к сервису
cox.service_name	Str	+	Имя сервиса
cox.use_tls	Bool	+	TLS-сертификат
cox.use_tls_balancer	Bool	+	Защищенная передача данных при подключении к балансировщику
tls_settings.ca_file	Str	+	Путь к CA файлу
tls_settings.client_cert_file	Str	+	Путь к файлу сертификата клиента
tls_settings.key_file	Str	+	Путь к файлу с ключом клиента

Пример ответа:

```
{
  "changed": true,
  "failed": false,
  "msg": "ok"
}
```

7.5.2 Удаление импортированных контактов

Удаление импортированных контактов производится командой **delete_gal_contact**.

```
nct_ministerium delete_gal_contact \
--admin.login *** \
--admin.password *** \
--gal_id *** \
--contact_emails galcontact.test.2@example.ru,galcontact.test.3@example.ru \
--contact_ids 1531959f-8fd0-47f7-8fa1-cefa12da93be,bb25ef42-4728-49d0-8156-
109ee69e0adc \
--cox.balancer_endpoint=hydra.ucs-apps-1.zulu.example.ru:50053 \
--cox.compression=none \
--cox.endpoint=grpc-devmail.example.ru:3142 \
--cox.load_balanced=false \
--cox.request_timeout=10s \
--cox.service_name=cox \
--cox.use_tls=true \
--cox.use_tls_balancer=false \
--tls_settings.ca_file /***/ca.pem \
--tls_settings.client_cert_file /***/client_crt.pem \
--tls_settings.key_file /***/client_key.pem \
--v
```

Описание параметров запроса на удаление импортированных контактов приведено в таблице 83.

Таблица 83 – Описание параметров запроса на удаление импортированных контактов

Параметр	Тип	Обязательный	Описание
admin.login	Str	+	Логин администратора тенанта
admin.password	Str	+	Пароль администратора тенанта
gal_id	Str	+	Идентификатор GAL
contact_emails	Str	+	Список импортированных контактов (через запятую)
contact_ids	Str	+	Идентификаторы импортированных контактов (через запятую)
cox.balancer_endpoint	Str	+	Endpoint балансировщика нагрузки сервиса
cox.compression	Str	+	Метод сжатия данных (варианты: **none**, **gzip**), по умолчанию **none**
cox.endpoint	Str	+	Endpoint сервиса
cox.load_balanced	Bool	+	Балансировщик нагрузки сервиса
cox.request_timeout	Str	+	Тайм-аут запроса к сервису
cox.service_name	Str	+	Имя сервиса
cox.use_tls	Bool	+	TLS-сертификат
cox.use_tls_balancer	Bool	+	Защищенная передача данных при подключении к балансировщику
tls_settings.ca_file	Str	+	Путь к CA файлу
tls_settings.client_cert_file	Str	+	Путь к файлу сертификата клиента
tls_settings.key_file	Str	+	Путь к файлу с ключом клиента

Пример ответа:

```
{
  "changed": true,
  "failed": false,
  "msg": "ok"
}
```

7.5.3 Поиск импортированных контактов

Поиск импортированных контактов производится командой **search_gal_contact**.

```
nct_ministerium search_gal_contact \
--admin.login *** \
--admin.password *** \
--gal_id *** \
--contact_emails galcontact.test.2@example.ru,galcontact.test.3@example.ru \
--cox.balancer_endpoint=hydra.ucs-apps-1.zulu.example.ru:50053 \
--cox.compression=none \
--cox.endpoint=grpc-devmail.example.ru:3142 \
--cox.load_balanced=false \
--cox.request_timeout=10s \
--cox.service_name=cox \
--cox.use_tls=true \
--cox.use_tls_balancer=false \
--tls_settings.ca_file /***/ca.pem \
--tls_settings.client_cert_file /***/client_crt.pem \
--tls_settings.key_file /***/client_key.pem \
--v
```

Описание параметров запроса на поиск импортированных контактов приведено в таблице 84.

Таблица 84 – Описание параметров запроса на поиск импортированных контактов

Параметр	Тип	Обязательный	Описание
admin.login	Str	+	Логин администратора тенанта
admin.password	Str	+	Пароль администратора тенанта
gal_id	Str	+	Идентификатор GAL
contact_emails	Str	+	Список импортированных контактов (через запятую)
cox.balancer_endpoint	Str	+	Endpoint балансировщика нагрузки сервиса
cox.compression	Str	+	Метод сжатия данных (варианты: **none**, **gzip**), по умолчанию **none**
cox.endpoint	Str	+	Endpoint сервиса
cox.load_balanced	Bool	+	Балансировщик нагрузки сервиса
cox.request_timeout	Str	+	Тайм-аут запроса к сервису
cox.service_name	Str	+	Имя сервиса
cox.use_tls	Bool	+	TLS-сертификат
cox.use_tls_balancer	Bool	+	Защищенная передача данных при подключении к балансировщику

Параметр	Тип	Обязательный	Описание
tls_settings.ca_file	Str	+	Путь к CA файлу
tls_settings.client_cert_file	Str	+	Путь к файлу сертификата клиента
tls_settings.key_file	Str	+	Путь к файлу с ключом клиента

Пример ответа:


```
{
  "Response": {
    "changed": true,
    "failed": false,
    "msg": "ok"
  },
  "contacts": [
    {
      "id": "0e3ab1ef-a817-46dd-acc3-d350f8e40a6a",
      "first_name": "Алексей",
      "last_name": "Алексеев",
      "middle_name": "Алексеевич",
      "locale": "RU",
      "department": "IT",
      "title": "Тестировщик",
      "organization": "Org1",
      "phones": [
        {
          "value": "89181234567",
          "preferable": true,
          "type": [
            2
          ]
        }
      ],
      "birthday": "2023-12-31",
      "emails": [
        {
          "value": "alekseyalekseev@example.ru",
          "preferable": true,
          "type": 2
        }
      ],
      "addresses": [
        {
          "name": "addr1",
          "country": "RU",
          "region": "23",
          "city": "KRD",
          "zip_code": "350000",
          "address": "K",
          "floor": "3",
          "room": "42",
          "workplace": "15",
          "preference": 1,
          "type": "HOME"
        }
      ]
```

```
    },
    {
      "id": "2b4fd14d-b77e-40a9-a006-cfa8b4634c1f",
      "first_name": "Денис",
      "last_name": "Денисов",
      "middle_name": "Денисович",
      "emails": [
        {
          "value": "denisdenisov@example.ru"
        }
      ]
    }
  ]
}
```

7.6 Настройка двухфакторной аутентификации

В а ж н о – Настройка двухфакторной аутентификации выполняется пользователем с ролью администратора тенанта.

Если администратор настроит двухфакторную аутентификацию на весь тенант без исключения, то в последствии он не сможет отключить данную настройку или каким-то образом ею управлять. Поэтому первым шагом в настройке двухфакторной аутентификации необходимо выполнить исключение администратора тенанта из перечня пользователей, попадающих под действие команды двухфакторной аутентификации.

Чтобы администратору тенанта добавить себя в исключение, необходимо выполнить команду:

```
nct_ministerium two_factor_auth_update_login_params
--admin.login ***
--admin.password ***
--login user@domain.ru
--second_factor_login_status LIST_DISABLED
```

Описание параметров приведено в таблице 85.

Таблица 85 – Описание параметров исключения пользователя

Параметр	Тип	Обязательный	Описание
admin.login	Str	+	Логин администратора тенанта
admin.password	Str	+	Пароль администратора тенанта
login	Str	+	Идентификатор логина
second_factor_ login.status	Str	+	Статус работы двухфакторной аутентификации для логина

От значений аргумента **second_factor_login.status** зависит статус работы двухфакторной аутентификации:

– DEFAULT – аналогично параметрам, заданным для тенанта;

– LIST_ENABLED – спрашивать всегда, кроме случая, когда запрос второго фактора для тенанта полностью отключен;

– LIST_DISABLED – никогда не запрашивать второй фактор.

Пример ответа:

```
{
  "changed": true,
  "failed": false,
  "msg": "ok"
}
```

Для настройки двухфакторной аутентификации пользователей необходимо выполнить следующие действия:

1. Установить параметры двухфакторной аутентификации тенанта:

```
nct_ministerium update_tenant
--config ministerium_demo.json
--admin.login <…>
--admin.password <…>
--tenant_id 1ddccc69-e32e-461f-9cba-1421c52a81b9
--second_factor_params.algorithm SHA256
--second_factor_params.digits 6
--second_factor_params.period_time 30
--second_factor_params.status ENABLED_FOR_ALL
--second_factor_params.sync_step 2
--second_factor_params.type TOTP
```

Описание параметров запроса приведено в таблице 86.

Таблица 86 – Описание параметров двухфакторной аутентификации тенанта

Параметр	Тип	Обязательный	Описание
config	Str	+	Конфигурационный файл с параметрами сервиса Cox и настройками tls. Формируется автоматически на сервере с ролью ucs_infrastructure и находится по пути /srv/ministerium/config.json
admin.login	Str	+	Логин администратора тенанта
admin.password	Str	+	Пароль администратора тенанта
tenant_id	Str	+	Идентификатор тенанта

Параметр	Тип	Обязательный	Описание
second_factor_params.algorithm	Str	+	Выбор алгоритма хеширования одноразового пароля (SHA1, SHA256, SHA512). Рекомендуется использовать алгоритм SHA1
second_factor_params.digits	Str	+	Длина одноразового пароля. Рекомендуется установить длину в 6 символов
second_factor_params.period_time	Str	Обязательный для типа TOTP, для HOTP не требуется	Время жизни одноразового пароля. Рекомендуется установить 30 секунд
second_factor_params.status	Str	+	Статус работы двухфакторной аутентификации
second_factor_params.sync_step	Str	+	Максимальная разница между значением счетчика на сервере и у пользователя
second_factor_params.type	Str	+	Тип второго фактора, TOTP (одноразовый пароль на основе времени) или HOTP (одноразовый пароль на основе хеш-функции)

Важно – Клиентские приложения чаще всего используют параметры, установленные по умолчанию. Необходимо использовать рекомендуемые параметры, указанные в таблице.

От значений аргумента **second_factor_params.status** зависит статус работы двухфакторной аутентификации:

– DISABLED – выключена;

– ENABLED_FOR_ALLOWED_LIST – включена для определенных пользователей;

– ENABLED_FOR_ALL – включена для всех пользователей.

Пример ответа:

```
{
  "changed": true,
  "failed": false,
  "msg": "ok"
}
```

2. Сбросить пользователю второй фактор, если он утратил к нему доступ:

```
nct_ministerium two_factor_auth_reset_user
--config ministerium.json
```

```
--admin.login <…>
--admin.password <…>
--entity_id
```

Описание параметров запроса приведено в таблице 87.

Таблица 87 – Описание параметров двухфакторной аутентификации тенанта

Параметр	Тип	Обязательный	Описание
config	Str	+	Конфигурационный файл с параметрами сервиса Cox и настройками tls. Формируется автоматически на сервере с ролью ucs_infrastructure и находится по пути /srv/ministerium/config.json
admin.login	Str	+	Логин администратора тенанта
admin.password	Str	+	Пароль администратора тенанта
entity_id	Str	+	Идентификатор пользователя, для которого необходимо сбросить второй фактор

Пример ответа:

```
{
  "changed": true,
  "failed": false,
  "msg": "ok"
}
```

7.7 Создание домена

Домен представляет собой локальный каталог ПО «Mailion» и служит для аутентификации пользователей.

Для создания домена необходимо выполнить следующие действия:

1. Выполнить запрос на создание домена без делегирования:

```
nct_ministerium create_domain
--config ministerium.json
--admin.login <...>
--admin.password <...>
--tenant_id ef28480f-0ee4-4f0c-af67-59f100727f31
--features.is_authorization=true
--features.is_mail=true
--features.is_service=true
--hostname mydomain.ru
```

Описание параметров запроса приведено в таблице 88.

Таблица 88 – Описание параметров запроса на создание домена без делегирования

Параметр	Тип	Обязательный	Описание
config	Str	+	Конфигурационный файл с параметрами сервиса Cox и настройками tls. Формируется автоматически на сервере с ролью ucs_infrastructure и находится по пути /srv/ministerium/config.json
admin.login	Str	+	Логин администратора тенанта
admin.password	Str	+	Пароль администратора тенанта
tenant_id	Str	+	Идентификатор тенанта
features.is_authorization	Bool	+	Если значение true, домен можно использовать для авторизации
features.is_mail	Bool	+	Если значение true, домен может принимать почтовые сообщения
features.is_service	Bool	+	Если значение true, домен можно использовать для авторизации по умолчанию
hostname	Str	+	Имя домена

Пример ответа:

```
{
  "msg": "ok",
  "changed": true
}
```

2. Выполнить запрос на получение параметров созданного домена:

```
nct_ministerium find_domain
--config ministerium.json
--admin.login <...>
--admin.password <...>
--hostname mydomain.ru
```

Описание параметров запроса приведено в таблице 89.

Таблица 89 – Описание параметров запроса на получение параметров созданного домена

Параметр	Тип	Обязательный	Описание
config	Str	+	Конфигурационный файл с параметрами сервиса Cox и настройками tls. Формируется автоматически на сервере с ролью ucs_infrastructure и находится по пути /srv/ministerium/config.json
admin.login	Str	+	Логин администратора тенанта

Параметр	Тип	Обязательный	Описание
admin.password	Str	+	Пароль администратора тенанта
hostname	Str	+	Имя домена

Пример ответа:

```
{
  "Response": {
    "msg": "ok"
  },
  "domains": [
    {
      "id": "c87f1fc3-23d5-520c-9049-b14aae2aa53b",
      "hostname": "mydomain.ru",
      "tenant_id": "ef28480f-0ee4-4f0c-af67-59f100727f31",
      "features":
      {
        "is_mail": true,
        "is_authorization": true,
        "is_service": true
      }
    }
  ]
}
```

Описание параметров ответа приведено в таблице 90.

Таблица 90 – Описание параметров ответа

Параметр	Тип	Обязательный	Описание
domains.hostname	Str	+	Значение должно быть равно значению, указанному при создании домена
domains.tenant_id	Str	+	Значение должно быть равно значению, указанному при создании домена
domains.features.is_mail	Bool	+	Значение должно быть равно значению, указанному при создании домена
domains.features.is_authorization	Bool	+	Значение должно быть равно значению, указанному при создании домена
domains.features.is_service	Bool	+	Значение должно быть равно значению, указанному при создании домена

Домен с делегированием связан с внешним доменом заказчика для осуществления аутентификации пользователей и синхронизации информации о профилях пользователя.

3. Для создания домена необходимо выполнить запрос на создание домена с делегированием:

```
nct_ministerium create_domain
--config ministerium.json
--admin.login <…>
```

```
--admin.password <…>
--tenant_id 833f618c-bfb0-4679-9761-d1a58480bca9
--hostname mydomain.ru
--features.is_authorization=true
--features.is_mail=true
--features.is_service=true
--features.is_delegated
--external.delegate_id 73b04a5a-47c4-4a59-86dd-6c1b195bc485
--external.domain_alias dc.mydomain.local
--external.default_region_id "2dbacea3-5889-4021-8f38-bc2214dd7423"
```

Описание параметров запроса приведено в таблице 91.

Таблица 91 – Описание параметров запроса на создание домена с делегированием

Параметр	Тип	Обязательный	Описание
config	Str	+	Конфигурационный файл с параметрами сервиса Cox и настройками tls. Формируется автоматически на сервере с ролью ucs_infrastructure и находится по пути /srv/ministerium/config.json
admin.login	Str	+	Логин администратора тенанта
admin.password	Str	+	Пароль администратора тенанта
tenant_id	Str	+	Идентификатор тенанта
hostname	Str	-	Имя домена
features.is_authorization	Bool	+	Если значение true, домен можно использовать для авторизации
features.is_mail	Bool	+	Если значение true, домен может принимать почтовые сообщения
features.is_service	Bool	+	Если значение true, домен можно использовать для авторизации по умолчанию
features.is_delegated	Bool	-	Если значение true, домен делегирован внешней системе
external.delegate_id	Str	-	Идентификатор делегата, используемый для внешней авторизации
external.domain_alias	Str	-	Имя контроллера делегируемого домена
external.default_region_id	Str	-	Идентификатор региона по умолчанию для автоматического создания пользователей

Пример ответа:

```
{
  "changed": true,
```

```
  "failed": false,
  "msg": "ok"
}
```

7.8 Создание первичной организационной структуры

Организационная структура – это иерархический набор контейнеров, используемый для упорядочивания и группировки объектов почтовой системы. Организационная структура может включать несколько Организаций, которые, в свою очередь, могут включать **Структурные подразделения** и **Проектные группы** (см. Рисунок 79). Объект Организационной структуры необходимо создать для получения возможности создания объектов **Организаций**.

Рисунок 79 – Примерная схема организационной структуры

В а ж н о – Может быть создано несколько иерархий оргструктур с различными названиями.

Изменение полей оргструктуры никак не влияет на поля элементов, входящих в нее, или их порядок. Организации внутри оргструктуры могут менять порядок нахождения в иерархии. При удалении оргструктуры входящие в нее организации не удаляются.

Для создания первичной организационной структуры необходимо выполнить следующие действия:

1. Выполнить запрос на создание оргструктуры, используя полученные данные:

```
nct_ministreuim save_org_structure_element
--config ministerium.json
--admin.login <…>
--admin.password <…>
--element '{"name": {"value": "Название оргструктуры"}, "description": {"value":
"Описание орг.структуры "}, "tenant_id": "tenant_id"}
--element_type 'ORG_STRUCTURE'
```

Описание параметров запроса приведено в таблице 92.

Таблица 92 – Описание параметров запроса на создание оргструктуры

Параметр	Тип	Обязательный	Описание
config	Str	+	Конфигурационный файл с параметрами сервиса Cox и настройками tls. Формируется автоматически на сервере с ролью ucs_infrastructure и находится по пути /srv/ministerium/config.json
admin.login	Str	+	Логин администратора тенанта
admin.password	Str	+	Пароль администратора тенанта
element	Str	+	Элемент организационной структуры для сохранения. Требуемые поля: – ORG_STRUCTURE(id, tenant_id, name, description), – ORGANIZATION(id, tenant_id, name, type, description, logo_identifier, address, phone, countries, leaders, avatar), – UNIT(id, tenant_id, name, type, description, address, phone, leaders, avatar), – GROUP(same with unit), – OCCUPATION(id, tenant_id, name, description, org_group, org_unit, organization), – COMPETENCE(id, tenant_id, name, description, qualifications)
element_type	Str	+	Тип элемента в оргструктуре на выбор

2. Выполнить запрос на установку связи с тенантом:

```
nct_ministerium add_org_structure_link
--config ministerium.json
--admin.login <…>
--admin.password <…>
--parent_id tenant_id
--parent_type "TENANT"
```

```
--child_id ORG_STRUCTURE_id
--child_type "ORG_STRUCTURE"
```

Описание параметров запроса приведено в таблице 93.

Таблица 93 – Описание параметров запроса на установку связи с тенантом

Параметр	Тип	Обязательный	Описание
config	Str	+	Конфигурационный файл с параметрами сервиса Cox и настройками tls. Формируется автоматически на сервере с ролью ucs_infrastructure и находится по пути /srv/ministerium/config.json
admin.login	Str	+	Логин администратора тенанта
admin.password	Str	+	Пароль администратора тенанта
parent_id	Str	+	Идентификатор родительского элемента в оргструктуре
parent_type	Str	+	Тип родительского элемента оргструктуры
child_id	Str	+	Идентификатор дочернего элемента в оргструктуре
child_type	Str	+	Тип дочернего элемента оргструктуры

После создания объекта оргструктуры в Панели администрирования «Mailion» станет доступна функция создания организаций и подразделений.

7.9 Создание организации

Администратор может создать несколько организаций.

В а ж н о – Нельзя создать организации с одинаковым именем в рамках одной оргструктуры.

Удалить организацию нельзя до тех пор, пока все входящие в нее организационные единицы или группы не будут удалены.

В а ж н о – Выполнять команду необходимо от имени администратора тенанта.

Для создания организации необходимо выполнить следующий запрос:

```
nct_ministerium save_org_structure_element
--admin.login <…>
--admin.password <…>
--element {"tenant_id": "01068ade-1cce-4125-ab6b-91d977ecf85b", "type":
{"value": "ЗАО"}, "name": {"value": "Организация Название организации"}}
--element_type ORGANIZATION
--cox.balancer_endpoint=hydra.ucs-apps-1.installation.example.net:50053
```

```
--cox.compression=none
--cox.endpoint=grpc-installation.example.net:3142
--cox.load_balanced=false
--cox.request_timeout=10s
--cox.service_name=cox
--cox.use_tls=true
--cox.use_tls_balancer=false
--tls_settings.ca_file /builds/0/mail-back-tests/certs/ca.pem
--tls_settings.client_cert_file /builds/0/mail-back-tests/certs/client_crt.pem
--tls_settings.key_file /builds/0/mail-back-tests/certs/client_key.pem
```

Описание параметров запроса приведено в таблице 94.

Таблица 94 – Описание параметров запроса на создание организации

Параметр	Тип	Обязательный	Описание
admin.login	Str	+	Логин администратора тенанта
admin.password	Str	+	Пароль администратора тенанта
element	Str	+	Данные сохраняемого объекта оргструктуры (строка в формате JSON)
element_type	Str	+	Тип элемента в оргструктуре на выбор
cox.balancer_endpoint	Str	+	Endpoint балансировщика нагрузки сервиса
cox.compression	Str	+	Метод сжатия данных (варианты: **none**, **gzip**), по умолчанию **none**
cox.endpoint	Str	+	Endpoint сервиса
cox.load_balanced	Bool	+	Балансировщик нагрузки сервиса
cox.request_timeout	Str	+	Тайм-аут запроса к сервису
cox.service_name	Str	+	Имя сервиса
cox.use_tls	Bool	+	TLS-сертификат
cox.use_tls_balancer	Str	+	Защищенная передача данных при подключении к балансировщику
tls_settings.ca_file	Bool	+	Путь к CA файлу
tls_settings.client_cert_file	Str	+	Путь к файлу сертификата клиента
tls_settings.key_file	Str	+	Путь к файлу с ключом клиента

Пример ответа:

```
{
  "Response": {
    "msg": "ok",
```

```
    "changed": true
  },
  "Id": "e7057610-b04d-4528-9218-db3e7b229fd5"
}
```

7.10 Операции над пользователями, группами и ресурсами

При первой попытке создания пользователя, группы или ресурса с помощью интерфейса командной строки предусмотрено автоматическое выполнение следующих запросов:

– создание пользователя;

– создание E-mail;

– создание логина;

– создание пароля и токена к логину;

– добавление роли;

– активация.

При неудачном выполнении какого-либо из шагов необходимо выполнить запросы вручную. Примеры выполнения запросов приведены ниже:

1. Создание пользователя:

```
nct_ministerium create_user
--admin.login <...>
--admin.password <…>
--email <...>
--login <...>
--password IbpvOqD(8)i90YL+U7Jx
--region_id 05fc39ce-9b06-4437-ae09-f1276468a0b9
--tenant_id ff11f0a0-dcd5-4392-8a34-b18036640a08
--gal_tags 91e3f772-4828-5da3-957e-73fdbc07ae8d
--profile.first_name <имя пользователя>
--profile.last_name <фамилия пользователя>
--cox.balancer_endpoint=hydra.ucs-apps-1.yankee.installation.example.net:50053
--cox.compression=none
--cox.endpoint=grpc-yankee.installation.example.net:3142
--cox.load_balanced=false
--cox.request_timeout=10s
--cox.service_name=cox
--cox.use_tls=true
--cox.use_tls_balancer=false
--tls_settings.ca_file /home/ps/work/first/mail-back-tests/certs/ca.pem
--tls_settings.client_cert_file /home/ps/work/first/mail-back-
tests/certs/client_crt.pem
--tls_settings.key_file /home/ps/work/first/mail-back-tests/certs/client_key.pem
```

Описание параметров запроса приведено в таблице 95.

Таблица 95 – Описание параметров запроса на создание пользователя

Параметр	Тип	Обязательный	Описание
admin.login	Str	+	Логин администратора тенанта
admin.password	Str	+	Пароль администратора тенанта
email	Str	+	Основной электронный адрес
login	Str		Логин пользователя
password	Str	+	Пароль для логина пользователя
region_id	Str	+	Идентификатор региона
tenant_id	Str	+	Идентификатор тенанта
gal_tags	Str	+	Идентификаторы GAL-тегов
profile.first_name	Str	+	Имя создаваемого пользователя
profile.last_name	Str	+	Фамилия создаваемого пользователя
cox.balancer_endpoint	Str	+	Endpoint балансировщика нагрузки сервиса
cox.compression	Str	+	Метод сжатия данных (варианты: **none**, **gzip**), по умолчанию **none**
cox.endpoint	Str	+	Endpoint сервиса
cox.load_balanced	Bool	+	Балансировщик нагрузки сервиса
cox.request_timeout	Str	+	Тайм-аут запроса к сервису
cox.service_name	Str	+	Имя сервиса
cox.use_tls	Bool	+	TLS-сертификат
cox.use_tls_balancer	Bool	+	Защищенная передача данных при подключении к балансировщику
tls_settings.ca_file	Str	+	Путь к CA файлу
tls_settings.client_cert_file	Str	+	Путь к файлу сертификата клиента
tls_settings.key_file	Str	+	Путь к файлу с ключом клиента

В а ж н о – При первом шаге создается объект (пользователь). При ошибке выполнения данного шага следующие запросы также не будут выполнены.

2. Создание E-mail:

```
nct_ministerium add_email
--admin.login <...>
--admin.password <…>
--email <...>
```

```
--entity_id 540712cd-0723-4dd3-9424-0912322eebbd
--cox.balancer_endpoint=hydra.ucs-apps-1.installation.example.net:50053
--cox.compression=none --cox.endpoint=grpc-mydomain.ru:3142
--cox.load_balanced=false --cox.request_timeout=10s --cox.service_name=cox
--cox.use_tls=true
--cox.use_tls_balancer=false
--tls_settings.ca_file /home/ps/work/first/mail-back-tests/certs/ca.pem
--tls_settings.client_cert_file /home/ps/work/first/mail-back-
tests/certs/client_crt.pem
--tls_settings.key_file /home/ps/work/first/mail-back-tests/certs/client_key.pem
```

Описание параметров запроса приведено в таблице 96.

Таблица 96 – Описание параметров запроса на создание E-mail

Параметр	Тип	Обязательный	Описание
admin.login	Str	+	Логин администратора тенанта
admin.password	Str	+	Пароль администратора тенанта
entity_id	Str	+	Идентификатор пользователя
cox.balancer_endpoint	Str	+	Endpoint балансировщика нагрузки сервиса
cox.compression	Str	+	Метод сжатия данных (варианты: **none**, **gzip**), по умолчанию **none**
cox.load_balanced	Bool	+	Балансировщик нагрузки сервиса
cox.use_tls	Str	+	TLS-сертификат
tls_settings.ca_file	Str	+	Путь к CA файлу
tls_settings.client_cert_file	Str	+	Путь к файлу сертификата клиента
tls_settings.key_file	Str	+	Путь к файлу с ключом клиента

3. Создание логина:

```
nct_ministerium create_login
--login <login>
--entity_id <entity_id>
```

Описание параметров запроса приведено в таблице 97.

Таблица 97 – Описание параметров запроса на создание логина

Параметр	Тип	Обязательный	Описание
login	Str	+	Имя логина
entity_id	Str	+	Идентификатор пользователя

4. Создание пароля и токена к логину:

```
nct_ministerium create_password
--login_id <additional_login.id>
--password <password> ...
```

Описание параметров запроса приведено в таблице 98.

Таблица 98 – Описание параметров запроса на создание пароля и токена к логину

Параметр	Тип	Обязательный	Описание
login_id	Str	+	Идентификатор логина
password	Str	+	Пароль к логину

5. Создание профиля:

```
nct_ministerium update_user_profile
--admin.login <...>
--admin.password <…>
--entity_id 08c9f17d-d110-4567-96d4-e2c1c15e96a3
--gal_region_id
--gal_tags
--create=false
--profile.birthday 1970-10-19
--profile.addresses [{"name": "address name", "country": "address country",
"region": "address region", "city": "address city", "zip_code": "zip
code", "address": "address address", "floor": "8", "room": "674", "workplace":
"904", "coordinates": {"latitude": 47.3394, "longitude": 34.00219},
"preference": 14, "type": "address type"}]
--profile.department department_1650447499
--profile.first_name <...>
--profile.gender <MALE/FEMALE>
--profile.last_name <...>
--profile.locale en_US
--profile.middle_name <...>
--profile.phones <WORK: <...>,HOME: <...>>
--profile.preferable_phone <...>
--profile.title title_1650447499
--cox.balancer_endpoint=hydra.ucs-apps-1.installation.example.net:50053
--cox.compression=none
--cox.endpoint=grpc-mydomain.ru:3142
--cox.load_balanced=false
--cox.request_timeout=10s
--cox.service_name=cox
--cox.use_tls=true
--cox.use_tls_balancer=false
--tls_settings.ca_file /home/ps/work/first/mail-back-tests/certs/ca.pem
--tls_settings.client_cert_file /home/ps/work/first/mail-back-
tests/certs/client_crt.pem
--tls_settings.key_file /home/ps/work/first/mail-back-
tests/certs/client_key.pem
```

Описание параметров запроса приведено в таблице 99.

Таблица 99 – Описание параметров запроса на создание профиля

Параметр	Тип	Обязательный	Описание
admin.login	Str	+	Логин администратора тенанта
admin.password	Str	+	Пароль администратора тенанта
entity_id	Str	+	Идентификатор пользователя профиля
gal_region_id	Str	+	Идентификатор региона, в котором создан GAL-тег
gal_tags	Str	+	Идентификаторы GAL-тегов
create	Str	-	Создание нового профиля
profile.birthday	Str	+	Дата рождения, в формате: ГГГГ-ММ-ДД
profile.addresses	Str	+	Список адресов пользователя профиля
profile.department	Str	+	Наименование подразделения компании профиля
profile.first_name	Str	+	Имя создаваемого пользователя профиля
profile.gender	Str	+	Пол пользователя профиля
profile.last_name	Str	+	Фамилия создаваемого пользователя профиля
profile.locale	Str	+	Локаль профиля
profile.middle_name	Str	+	Отчество пользователя профиля
profile.phones	Str	+	Список телефонных адресов пользователя профиля
profile.preferable_phone	Str	+	Признак предпочтительного номера пользователя профиля
profile.title	Str	+	Должность пользователя профиля
cox.balancer_endpoint	Str	+	Endpoint балансировщика нагрузки сервиса
cox.compression	Str	+	Метод сжатия данных (варианты: **none**, **gzip**), по умолчанию **none**
cox.endpoint	Str	+	Endpoint сервиса

Параметр	Тип	Обязательный	Описание
cox.load_balanced	Bool	+	Балансировщик нагрузки сервиса
cox.request_timeout	Str	+	Тайм-аут запроса к сервису
cox.service_name	Str	+	Имя сервиса
cox.use_tls	Bool	+	TLS-сертификат
cox.use_tls_balancer	Bool	+	Защищенная передача данных при подключении к балансировщику
tls_settings.ca_file	Str	+	Путь к CA файлу
tls_settings.client_cert_file	Str	+	Путь к файлу сертификата клиента
tls_settings.key_file	Str	+	Путь к файлу с ключом клиента

6. Добавление роли:

```
nct_ministerium update_roles
--admin.login <...>
--admin.password <…>
--entity_id 8c88d3b1-2c01-4dc7-bfe0-9182e291444c
--add_roles 54718e3a-6c7b-5c9f-b4de-a897c356cb5e
--remove_roles
--cox.balancer_endpoint=hydra.ucs-apps-1.installation.example.net:50053
--cox.compression=none
--cox.endpoint=grpc-mydomain.ru:3142
--cox.load_balanced=false
--cox.request_timeout=10s
--cox.service_name=cox
--cox.use_tls=true -
--cox.use_tls_balancer=false
--tls_settings.ca_file /home/ps/work/first/mail-back-tests/certs/ca.pem
--tls_settings.client_cert_file /home/ps/work/first/mail-back-
tests/certs/client_crt.pem
--tls_settings.key_file /home/ps/work/first/mail-back-tests/certs/client_key.pem
```

Описание параметров запроса приведено в таблице 100.

Таблица 100 – Описание параметров запроса на добавление роли

Параметр	Тип	Обязательный	Описание
admin.login	Str	+	Логин администратора тенанта
admin.password	Str	+	Пароль администратора тенанта
entity_id	Str	+	Идентификатор пользователя профиля
add_roles	Str	+	Добавление ролей
remove_role	Str	+	Удаление ролей

Параметр	Тип	Обязательный	Описание
cox.balancer_endpoint	Str	+	Endpoint балансировщика нагрузки сервиса
cox.compression	Str	+	Метод сжатия данных (варианты: **none**, **gzip**), по умолчанию **none**
cox.endpoint	Str	+	Endpoint сервиса
cox.load_balanced	Bool	+	Балансировщик нагрузки сервиса
cox.request_timeout	Str	+	Тайм-аут запроса к сервису
cox.service_name	Str	+	Имя сервиса
cox.use_tls	Bool	+	TLS-сертификат
cox.use_tls_balancer	Str	+	Защищенная передача данных при подключении к балансировщику
tls_settings.ca_file	Bool	+	Путь к CA файлу
tls_settings.client_cert_file	Str	+	Путь к файлу сертификата клиента
tls_settings.key_file	Str	+	Путь к файлу с ключом клиента

7. Активация:

```
nct_ministerium change_status
--entity_id <entity_id>
--status <status> ...
```

Описание параметров запроса приведено в таблице 101.

Таблица 101 – Описание параметров запроса на активацию

Параметр	Тип	Обязательный	Описание
entity_id	Str	+	Идентификатор статуса
status	Str	+	Статус

В а ж н о – У несозданных объектов необходимо вручную выполнить те запросы, которые остались невыполненными автоматически.

7.11 Ограничение бронирования списком пользователей

Добавление разрешенных пользователей и групп, разрешенных для ресурса:

```
nct_ministerium add_allowed_users_and_groups_to_resource
--config "/home/.../dev/ministerium.json"
--entity_ids "b2e27539-1997-40cd-a294-3f7c96801b96,3c311490-f0c4-4e32-ae60-
```

```
081bc51ac9c3"
--resource_id 106eb48a-2133-4c6e-87ca-179dc8e101e9
--v
```

Описание параметров запроса приведено в таблице 102.

Таблица 102 – Описание параметров запроса на удаление администратора тенанта

Параметр	Тип	Обязательный	Описание
config	Str	+	Конфигурационный файл
entity_ids	Str	+	Список идентификаторов разрешенных пользователей
resource_id	Str	+	Идентификатор ресурса

Удаление разрешенных пользователей и групп, разрешенных для ресурса:

```
nct_ministerium remove_allowed_users_and_groups_to_resource
--config "/home/.../dev/ministerium.json"
--entity_ids "b2e27539-1997-40cd-a294-3f7c96801b96,3c311490-f0c4-4e32-ae60-
081bc51ac9c3"
--resource_id 106eb48a-2133-4c6e-87ca-179dc8e101e9
--v
```

Описание параметров запроса приведено в таблице 103.

Таблица 103 – Описание параметров запроса на удаление администратора тенанта

Параметр	Тип	Обязательный	Описание
config	Str	+	Конфигурационный файл
entity_ids	Str	+	Список идентификаторов разрешенных пользователей
resource_id	Str	+	Идентификатор ресурса

Получение списка разрешенных пользователей и групп, разрешенных для ресурса:

```
nct_ministerium get_allowed_users_and_groups_to_resource
--config "/home/.../dev/ministerium.json"
--resource_id 106eb48a-2133-4c6e-87ca-179dc8e101e9
--v
```

Описание параметров запроса приведено в таблице 104.

Таблица 104 – Описание параметров запроса на удаление администратора тенанта

Параметр	Тип	Обязательный	Описание
config	Str	+	Конфигурационный файл
resource_id	Str	+	Идентификатор ресурса

7.12 Делегирование управления группами

Администратор тенанта может делегировать произвольному пользователю права на управление составом участников и редактирование данных группы.

Для этого необходимо выполнить запрос на выдачу прав на управление группой, назначив пользователю соответствующую роль:

```
nct_ministerium shared_access_grant
--admin.login <…>
--admin.password <…>
--emails autotest_1680079691.97499@installation.exaple.net,
autotest_1680079700.613669@installation.exaple.net,autotest_1680079668.730608@in
stallation.exaple.net,autotest_1680079682.528347@installation.exaple.net,autotes
t_1680079359.89922@installation.exaple.net,autotest_1680079373.50339@installatio
n.exaple.net,autotest_1680079536.010099@installation.exaple.net
--delegate_email test_group_delegate_2@installation.exaple.net
--sharing_roles
GROUP_ADMINISTRATOR,GROUP_ADMINISTRATOR,GROUP_ADMINISTRATOR,GROUP_ADMINISTRATOR,
GROUP_ADMINISTRATOR,GROUP_ADMINISTRATOR,GROUP_ADMINISTRATOR
--cox.balancer_endpoint=hydra.ucs-apps-1.installation.exaple.net:50053
--cox.compression=none
--cox.endpoint=grpc-installation.exaple.net:3142
--cox.load_balanced=false
--cox.request_timeout=10s
--cox.service_name=cox
--cox.use_tls=true
--cox.use_tls_balancer=false
--tls_settings.ca_file /home/user/mail-back-tests/certs/ca.pem
--tls_settings.client_cert_file /home/user/mail-back-tests/certs/client_crt.pem
--tls_settings.key_file /home/user/mail-back-tests/certs/client_key.pem
```

Описание параметров запроса на выдачу прав на управление группой в таблице 105.

Таблица 105 – Описание параметров запроса на выдачу прав на управление группой

Параметр	Тип	Обязательный	Описание
admin.login	Str	+	Логин администратора тенанта
admin.password	Str	+	Пароль администратора тенанта
emails	Str	+	Email пользователя/пользователей, которым будут делегированы права управления группой
delegate_email		+	Email группы, права на управление которой необходимо делегировать пользователю/пользователям
sharing_roles		+	Выбор из разрешенных к назначению ролей: − GROUP_EDITOR (Редактор группы); − GROUP_ADMINISTRATOR (Администратор группы)

Параметр	Тип	Обязательный	Описание
cox.balancer_endpoint	Str	+	Endpoint балансировщика нагрузки сервиса
cox.compression	Str	+	Метод сжатия данных (варианты: **none**, **gzip**), по умолчанию **none**
cox.endpoint	Str	+	Endpoint сервиса
cox.load_balanced	Bool	+	Балансировщик нагрузки сервиса
cox.request_timeout	Str	+	Тайм-аут запроса к сервису
cox.service_name	Str	+	Имя сервиса
cox.use_tls	Bool	+	TLS-сертификат
cox.use_tls_balancer	Bool	+	Защищенная передача данных при подключении к балансировщику
tls_settings.ca_file	Str	+	Путь к CA файлу
tls_settings.client_cert_file	Str	+	Путь к файлу сертификата клиента
tls_settings.key_file	Str	+	Путь к файлу с ключом клиента

Примечание – При делегировании управления группой нескольким пользователям необходимо указать такое же количество ролей в соответствующем порядке.

Пример ответа:

```
{
  "Response": {
    "changed": true,
    "failed": false,
    "msg": "ok"
  }
}
```

Важно – Процесс выдачи прав на управление группой может занять до одной минуты. По истечении данного времени пользователю станут доступны функции назначенной роли.

Чтобы отозвать права у пользователя/пользователей необходимо выполнить запрос:

```
nct_ministerium shared_access_revoke
--admin.login <…>
--admin.password <…>
--delegate_email group_1681355902_pwbgdstsxr@installation.exaple.net
--emails autotest_1681355888.981403@installation.exaple.net
```

Описание параметров запроса на отзыв прав в таблице 106.

Таблица 106 – Описание параметров запроса на отзыв прав

Параметр	Тип	Обязательный	Описание
admin.login	Str	+	Логин администратора тенанта
admin.password	Str	+	Пароль администратора тенанта
delegate_email		+	Email делегированной на управление группы
emails	Str	-	Email пользователя/пользователей, права на управление группой у которых будут отозваны

Примечание – Если необходимо отозвать права у всех пользователей, которым предварительно они были назначены, то следует оставить поле **emails** пустым.

Пример ответа:

```
{
  "Response": {
    "changed": true,
    "failed": false,
    "msg": "ok"
  }
}
```

7.13 Создание динамической группы

Динамическая группа позволяет определить параметры автоматического добавления пользователей. Для создания динамической группы, требуется созданная организационная группа.

Для создания организационной группы необходимо выполнить запрос:

```
nct_ministerium create_group
-- config ministerium.json
--admin.login <...>
--admin.password <...>
--tenant_id <...>
--region_id <...>
--gal_tags <...>
--gal_region_id <...>
--profile.name "Group Test"
--profile.description "Group Description"
```

Описание параметров запроса приведено в таблице 107.

Таблица 107 – Описание параметров запроса на создание организационной группы

Параметр	Тип	Обязательный	Описание
config	Str	+	Конфигурационный файл с параметрами сервиса Cox и настройками tls. Формируется автоматически на сервере с ролью ucs_infrastructure и находится по пути /srv/ministerium/config.json
admin.login	Str	+	Логин администратора тенанта
admin.password	Str	+	Пароль администратора тенанта
tenant_id	Str	+	Идентификатор тенанта
region_id	Str	+	Идентификатор региона
gal_tags	Str	+	Идентификаторы GAL-тегов
gal_region_id	Str	+	Идентификатор региона GAL
profile.name	Str	+	Имя создаваемой группы
profile.description	Str	+	Описание создаваемой группы

Пример ответа:

```
{
  "Response": {
    "msg": "ok",
    "changed": true
  },
  "id": "a4f1d34a-4072-407c-8001-876d7e6912e6"
}
```

После этого необходимо выполнить запрос на создание динамической группы:

```
nct_ministerium make_dynamic_group
--config ministerium.json
--admin.login <...>
--admin.password <...>
--group_id a4f1d34a-4072-407c-8001-876d7e6912e6
--filter '{"left": {"operation": {"left": {"attribute": "ORGANIZATION_NAME"},
"operation": "CONTAINS", "right": {"str": "MyOffice"}}}, "operation": "AND",
"right": {"operation": {"left": {"operation": {"left": {"attribute":
"OCCUPATION_NAME"}, "operation": "CONTAINS", "right": {"str": "Customer
Care"}}}, "operation": "OR", "right": {"operation": {"left": {"attribute":
"OCCUPATION_NAME"}, "operation": "NOT_CONTAINS", "right": {"str":
"Support"}}}}}}'
```

Описание параметров запроса приведено в таблице 108.

Таблица 108 – Описание параметров запроса на создание динамической группы

Параметр	Тип	Обязательный	Описание
config	Str	+	Конфигурационный файл с параметрами сервиса Cox и настройками tls. Формируется

Параметр	Тип	Обязательный	Описание
			автоматически на сервере с ролью ucs_infrastructure и находится по пути /srv/ministerium/config.json
admin.login	Str	+	Логин администратора тенанта
admin.password	Str	+	Пароль администратора тенанта
group_id	Str	+	Идентификатор организационной группы
filter	Str	+	Правила для динамической группы в формате JSON

Пример правил для создания фильтрации в динамической группе:

```
{
    "left": {
        "operation": {
            "left": {
                "attribute": "ORGANIZATION_NAME"
            },
            "operation": "CONTAINS",
            "right": {
                "str": "Company.example"
            }
        }
    },
    "operation": "AND",
    "right": {
        "operation": {
            "left": {
                "operation": {
                    "left": {
                        "attribute": "OCCUPATION_NAME"
                    },
                    "operation": "CONTAINS",
                    "right": {
                        "str": "Customer Care"
                    }
                }
            },
            "operation": "OR",
            "right": {
                "operation": {
                    "left": {
                        "attribute": "OCCUPATION_NAME"
                    },
                    "operation": "NOT_CONTAINS",
                    "right": {
                        "str": "Support"
                    }
                }
            }
        }
    }
}
```

Данный фильтр добавляет в группу пользователей из организации «Company.example», с должностью, название которой содержит значение «Customer Care» или не содержит значения «Support».

Примечание – Если в массиве есть хотя бы один оператор or, то условия объединяются в группы по правилам приоритетности логических операций. При этом список все рано остается плоским, а количество групп условий будет равно n + 1, где n – количество операторов or. Все объекты от одного разделителя or до другого разделителя or представляют собой группу условий, объединенных оператором and.

Допустимые значения параметра **operation**:

```
'EQUALS' - равенство операндов
'NOT_EQUALS' - неравенство операндов
'GREATER' - левый операнд больше правого
'LESS' - левый операнд меньше правого
'GREATER_OR_EQUAL' - левый операнд больше или равен правому
'LESS_OR_EQUAL' - левый операнд меньше или равен правому
'CONTAINS' - левый операнд содержит правый
'NOT_CONTAINS' - левый операнд не содержит правый
'AND' - левый и правый операнды истинны
'OR' - левый или правый операнд истинен
```

Допустимые значения параметра **attribute**:

```
'ORGANIZATION_STRUCTURE_NAME' - имя организационной структуры
'ORGANIZATION_NAME' - имя организации
'ORGANIZATIONAL_UNIT_NAME' - имя организационной единицы
'ORGANIZATIONAL_GROUP_NAME' - имя организационной группы
'OCCUPATION_NAME' - название должности
'COMPETENCE_NAME' - название компетенции
'FIRST_NAME' - имя пользователя
'LAST_NAME' - фамилия пользователя
'GENDER' - гендерная принадлежность пользователя
  - 'MALE' - муж.
  - 'FEMALE' - жен.
'CITY' - название города
'BIRTHDAY' - день рождения
'ID' - идентификатор субъекта (пользователя, группы, ресурса и т. д.)
```

Пример ответа на запрос создания динамической группы:

```
{
  "msg": "ok",
  "changed": true
}
```

7.14 Массовое создание пользователей в каталоге

В а ж н о – Массовое создание пользователей выполняется пользователем с ролью администратора тенанта.

Массовое создание пользователей в каталоге осуществляется с помощью импорта пользователей в систему из файла, выгруженного заранее из внешнего каталога или созданного любым другим способом.

Для импорта пользователей из файла необходимо выполнить следующие действия:

1. Подготовить два файла:
   – Файл настроек процедуры импорта **import_config.json**. Пример файла настроек приведен в приложении (см. раздел «Файл настроек импорта пользователей» в Приложении В).
   – Файл импорта, содержащий импортируемых в систему пользователей, в формате JSON (**user_profiles.json**) или CSV (**user_profiles.csv**). Пример заполняемых полей в файле приведен в разделе 7.14.1.

   П р и м е ч а н и е – Для каждого отдельного пользователя перед импортом система выполняет поиск пользователя по электронным адресам почты (emails) и логинам (logins). Если найдено совпадение, то вместо создания нового пользователя выполняется обновление данных. Обновляются все поля пользователя, за исключением электронных адресов и логинов – они будут добавлены.

2. Выполнить команду запуска импорта **import_users**. Перед выполнением непосредственного импорта выполнить первоначальную проверку данных, предоставляемых для импорта и настроек подключения к ПО «Mailion»:
   – Выполнить непосредственный запуск импорта пользователей:

```
nct_ministerium import_users --config import_config.json
```

Описание параметров запроса приведено в таблице 109.

Таблица 109 – Описание параметров запроса на импорт пользователей

Параметр	Тип	Обязательный	Описание
config	Str	+	Конфигурационный файл с параметрами сервиса Cox и настройками tls. Формируется автоматически на сервере с ролью

			ucs_infrastructure и находится по пути /srv/ministerium/config.json

Пример ответа:

```
{
  "Response": {
    "msg": "ok",
    "changed": true
  },
  "responses": [
    {
      "msg": "validation done, users to import: 1"
    },
    {
      "msg": "import procedure summary: total reported results: 1, errors: 0,
success: 1",
      "changed": true
    }
  ]
}
```

– Выполнить запрос на проверку файла импорта, конфигурации и подключения к ПО «Mailion», но без запуска самого импорта:

```
nct-ministerium import_users
--config import_config.json
--check
```

Проверка файла производится по схеме, которая подробно описывает ограничения системы, существующие на структуру и поля данных пользователя. Схема в формате JSON Schema приведена в приложении (см. раздел «Схема записи пользователя» в Приложении В).

В а ж н о – Процедура импорта будет возможна, если все пользователи в файле импорта пройдут проверку по этой схеме.

Описание параметров запроса приведено в таблице 110.

Таблица 110 – Описание параметров запроса на проверку файла импорта, конфигурации и подключения к ПО «Mailion»

Параметр	Тип	Обязательный	Описание
config	Str	+	Конфигурационный файл с параметрами сервиса Cox и настройками tls. Формируется автоматически на сервере с ролью ucs_infrastructure и находится по пути /srv/ministerium/config.json
check	Str	+	Выполнение базовых проверок перед отправкой данных на сервер.

Пример ответа:


```
{
  "Response": {
    "msg": "ok"
  },
  "responses": [
    {
      "msg": "validation done, users to import: 1"
    }
  ]
}
```


Примечание – Команда **import_users** реализована таким образом, что поддерживает неоднократный запуск с одними и теми же параметрами, включая файл импорта.

3. Выполнить запрос на получение списка глобальных адресных книг, чтобы определить в какой GAL-тег определить создаваемых пользователей:

```
nct-ministerium get_tenant_gals --config get_tenant_gals.json
```

Описание параметров запроса приведено в таблице 111.

Таблица 111 – Описание параметров запроса на получение GAL-тегов тенанта

Параметр	Тип	Обязательный	Описание
config	Str	+	Конфигурационный файл с параметрами сервиса Cox и настройками tls. Формируется автоматически на сервере с ролью ucs_infrastructure и находится по пути /srv/ministerium/config.json

Пример ответа:


```
{
  "Response": {
    "msg": "ok",
    "changed": true
  },
  "gals": [
    {
      "id": {
        "id": "1c22be2e-1e2f-5f6d-bec5-842c5d48e9d3",
        "region_id": "1dbacea3-5889-4021-8f38-bc2214dd7423"
      },
      "path": [
        "gal"
      ]
    },
    {
      "id": {
        "id": "1d34a52f-c510-40e7-b6ac-d6cae0753184",
```

```
        "region_id": "1dbacea3-5889-4021-8f38-bc2214dd7423"
      },
      "path": [
        "gal_1k"
      ]
    },
    {
      "id": {
        "id": "194ea408-9087-4bec-855e-ff8e82fdab8a",
        "region_id": "1dbacea3-5889-4021-8f38-bc2214dd7423"
      },
      "path": [
        "custom_gal"
      ]
    }
  ]
}
```


Пример файла настроек **get_tenant_gals.json** приведен в приложении (см. раздел «Список глобальных адресных книг» в Приложении В).

7.14.1 Подготовка файла импорта

В а ж н о – Файл импорта может быть предоставлен только в форматах JSON Lines и CSV.

Формат JSON является основным для системы и позволяет наиболее полно описать пользователя системы.

Описание параметров файла импорта **user_profiles.json** приведено в таблице 112.

Таблица 112 – Описание параметров файла импорта **user_profiles.json**

Параметр	Тип	Обязательный	Описание
correlation_id	Str	+	Пользовательский идентификатор, уникальный в пределах файла импорта
first_name	Str	+	Имя пользователя
last_name	Str	-	Фамилия пользователя
middle_name	Str	-	Отчество пользователя
gender	Str	-	Пол пользователя
birthday	Str	-	Дата рождения, в формате: ГГГГ-ММ-ДД
locale	Str	-	Код локализации

Параметр	Тип	Обязательный	Описание
department	Str	-	Наименование подразделения компании
title	Str	-	Должность
reserve_email	Str	-	Резервный адрес электронной почты
addresses	Str	-	Список адресов пользователя
addresses.name	Str	-	Наименование адреса
addresses.country	Str	-	Страна
addresses.region	Str	-	Регион
addresses.city	Str	-	Город
addresses.zip_code	Str	-	Почтовый индекс
addresses.address	Str	-	Адрес
addresses.floor	Str	-	Этаж
addresses.room	Str	-	Комната
addresses.workplace	Str	-	Рабочее место
addresses.coordinates	Str	-	Географические координаты
addresses.coordinates.latitude	Str	+	Широта. Обязательно к заполнению, если заполнено поле **addresses.coordinates**
addresses.coordinates.longitude	Str	+	Долгота. Обязательно к заполнению, если заполнено поле **addresses.coordinates**
addresses.preference	Str	-	Уровень предпочтения для использования адреса
addresses.type	Str	-	Тип адреса
phones	Str	-	Список телефонных адресов
phones.number	Str	-	Номер телефона
phones.preferable	Str	-	Признак предпочтительного номера
phones.type	Str	-	Список типов номера
emails	Str	+	Список электронных адресов пользователя
emails.email	Str	+	Электронный адрес
emails.primary	Str	+	Признак основного адреса

Параметр	Тип	Обязательный	Описание
logins	Str	+	Список логинов пользователя
logins.login	Str	+	Логин
logins.password	Str	+	Пароль

В а ж н о – Каждый отдельный пользователь проверяется по JSON-схеме записи пользователя, приведенной в приложении (см. раздел «Схема записи пользователя» в Приложении В).

Файл импорта в формате CSV позволяет импортировать пользователей с ограниченным набором данных.

Описание параметров файла импорта **user_profiles.csv** приведено в таблице 113.

Таблица 113 – Описание параметров файла импорта **user_profiles.csv**

Параметр	Обязательный	Описание
correlation_id	+	Пользовательский идентификатор, уникальный в пределах файла импорта
first_name	+	Имя пользователя
email	+	Основной электронный адрес и логин
password	+	Пароль для логина, заданного полем **email**

7.14.2 Примеры сообщений системы

Пример успешного импорта одного пользователя из одного предоставленного в файле импорта:

```
nct-ministerium import_users
--config import_config.json
import file verification starts, it will take some time {"client-request-id":
"84e8b091-29cf-46a3-8883-f14e3cb1360e", "command": "import_users"}
user imported {"client-request-id": "84e8b091-29cf-46a3-8883-f14e3cb1360e",
"command": "import_users", "correlation_id": "f1b97e81-e4a3-4ebd-ba59-
e4b864ef4797", "status": "ok", "total": 1}
{
  "Response": {
    "msg": "ok",
    "changed": true
  },
  "responses": [
    {
      "msg": "validation done, users to import: 1"
    },
```

```
    {
      "msg": "import procedure summary: total reported results: 1, errors: 0,
success: 1",
      "changed": true
    }
  ]
}
```

Описания сообщений приведены в таблице 114.

Таблица 114 – Описание сообщений системы

Сообщение	Описание
import file verification starts, it will take some time	Процесс локальной проверки файла импорта запущен. Такая проверка осуществляется при каждом запуске, до отправки файла импорта на сервер. Время проверки зависит от количества пользователей, переданных для импорта, и может занимать значительное время
user imported	Пользователь успешно импортирован. Об этом говорит маркер «ok» в поле «status». Идентификатор импортируемой записи пользователя сообщается в поле «correlation_id». В поле «total» показывается общее количество полученных ответов от сервера обо всех пользователях, успешно импортированных и не импортированных
validation done, users to import	Проверка файла импорта прошла успешно и обнаружен один пользователь для импорта. Это сообщение отобразится только в том случае, если все пользователи прошли проверку по схеме записи пользователя, описанной в приложении (см. раздел «Схема записи пользователя» в Приложении В)
import procedure summary	Итог импорта, сообщает количество пользователей, которые были обработаны системой, количество пользователей с ошибками и количество успешно импортированных пользователей. В любом случае количество, указанное в полях «users to import» и «total reported results», должно быть одинаковым

7.14.3 Возможные ошибки при импорте пользователей

Описания возможных ошибок при импорте пользователя приведены в таблице 115.

Таблица 115 – Описание возможных ошибок

Название ошибки	Вид в интерфейсе командной строки	Описание

Ошибка декодирования JSON	{
	"msg": "import file validation: decode next user: decode JSON: invalid character '}' looking for beginning of value",
	"failed": true
	}
		Сообщение выводится в случае, если утилита не может декодировать файл импорта, в этом случае необходимо проверить корректность синтаксиса JSON или CSV

Название ошибки	Вид в интерфейсе командной строки	Описание

Ошибка при проверке записи пользователя по схеме	{
	"msg": "import file validation: user correlation ID: : correlation_id: String length must be greater than or equal to 1",
	"failed": true
	}
		Сообщение транслирует информацию о том, что обязательное поле "correlation_id" отсутствует или имеет пустое значение

Ошибка в адресе электронной почты	{
	"msg": "import file validation: user correlation ID: f1b97e81-e4a3-4ebd-ba59-e4b864ef4797: emails.0.email: Does not match format 'email'",
	"failed": true
	}
		Сообщение выводится в случае, если пользователь с идентификатором (correlation_id) "f1b97e81-e4a3-4ebd-ba59-e4b864ef4797" не прошел проверку по схеме. У этого пользователя в первой структуре, описывающей электронные адреса, отсутствует или имеет некорректный формат поле "email"

Ошибка в логине	{
	"msg": "import file validation: user correlation ID: f1b97e81-e4a3-4ebd-ba59-e4b864ef4797: logins.0.login: String length must be greater than or equal to 1",
	"failed": true
	}
		Аналогично предыдущему примеру, но отсутствует поле "login" у первой структуры в списке логинов (logins)

Ошибка, дубликат электронного адреса	{
	"msg": "import file validation: duplicate email found: 433bfcea-5adf-49ee-88e5-cfca9a575b6b@example.com (users correlation IDs: f1b97e81-e4a3-4ebd-ba59-e4b864ef4797, 1d567e35-31ce-461e-8a35-5efd2012362c)",
	"failed": true
	}
		Еще один пример проверки, выполняемой перед отправкой файла импорта на сервер.
		Здесь говорится о том, что у записей пользователя с идентификаторами (correlation_id) "f1b97e81-e4a3-4ebd-ba59-e4b864ef4797" и "1d567e35-31ce-461e-8a35-5efd2012362c" найдено повторение электронного адреса, его значение: "433bfcea-5adf-49ee-88e5-cfca9a575b6b@example.com".
		Необходимо исправить электронный адрес у одного из пользователей

Ошибка, возникшая в процессе импорта пользователя на стороне сервера	$ nct-ministerium import_users --config import_config.json import file verification starts, it will take some time {"client-request-id": "09ed4436-41e9-475f-b741-7ae81237cc8f", "command": "import_users"}	Пример ошибки, возникшей в процессе импорта пользователя на стороне сервера, например по причине отказа сетевого окружения

Название ошибки	Вид в интерфейсе командной строки	Описание

	user error {"client-request-id": "09ed4436-41e9-475f-b741-7ae81237cc8f", "command": "import_users", "correlation_id": "f1b97e81-e4a3-4ebd-ba59-e4b864ef4797", "status": "error", "error": "upsert user: save profile: common.Error(module:PERSEUS code:5000 msg:\"ERAKLES_ERROR\")", "total": 1}
	{
	"Response": {
	"msg": "ok",
	"changed": true
	},
	"responses": [
	{
	"msg": "validation done, users to import: 1"
	},
	{
	"msg": "import procedure summary: total reported results: 1, errors: 1, success: 0",
	"changed": true
	}
	]
	}	

	user error	В этом сообщении говорится о том, что пользователь с идентификатором, указанным в поле "correlation_id", не был импортирован. На это указывает маркер "error" в поле "status" и наличие поля "error", которое содержит сообщение об ошибке со стороны системы. Соответственно, этот пользователь будет добавлен в файл, указанный в параметре "rejected_users_path", или в файл с именем по умолчанию
Ошибка проверки локали в записи пользователя	{ "msg": "import file validation: user correlation ID: f1b97e81-e4a3-4ebd-ba59-	Пример ошибки, которая выдается, если локаль (locale) в записи пользователя не задана или задана

Название ошибки	Вид в интерфейсе командной строки	Описание
	e4b864ef4797, check user locale: language: tag is not well-formed", "failed": true }	некорректно. Пример правильного значения: ru_RU, en_US

Возможен сценарий, при котором файл импорта выгружается несколько раз с какими-либо уточнениями из системы-источника и каждый раз (кроме первого) происходит обновление пользователя в ПО «Mailion». Кроме повторного запуска с исправленными/уточненными данными в исходном файле импорта также допускается импорт файла **rejected_users.json**, после исправлений ошибок о которых система оповестила в процессе импорта. Для этого путь к файлу **rejected_users.json** нужно указать в параметре user_data_path, не допустив при этом пересечения имени с параметром **rejected_users_path**.

Примечание – Пользователи, не импортированные или частично импортированные в систему, записываются в файл **rejected_users.json**. При этом для каждого такого пользователя система выдаст сообщение об ошибке на экран. Найти конкретного пользователя в файле **rejected_users.json** можно по **correlation_id**.

7.15 Массовое создание групп в каталоге

Важно – Массовое создание пользователей выполняется пользователем с ролью администратора тенанта.

Массовое создание групп в каталоге осуществляется с помощью импорта групп из файла в формате **JSON** или **CSV**, выгруженного из внешнего каталога заранее (см. раздел 7.15.6) или созданного любым другим способом.

Импорт групп из файла в систему осуществляется в два этапа:

– непосредственно импорт групп (см. раздел 7.15.1);

– импорт связей данных групп (см. раздел 7.15.2).

7.15.1 Импорт групп

Для выполнения первого этапа необходимо выполнить следующие действия:

1. Подготовить два файла:
   – Файл настроек процедуры импорта **settings.json**. Пример файла настроек приведен в приложении (см. раздел «Файл настроек импорта групп» в Приложении В).
   – Файл импорта, содержащий импортируемые в систему группы, в формате JSON (**groups.json**) или CSV (**groups.csv**). Пример заполняемых полей в файлах приведен в разделе 7.15.3.

   П р и м е ч а н и е – Для каждой отдельной группы, перед импортом, система выполняет поиск группы по электронным адресам почты (emails) и логинам (logins). Если найдено совпадение, то вместо создания новой группы выполняется обновление данных. Обновляются все поля группы, за исключением электронных адресов и логинов – они будут добавлены. В результате импорта также может измениться основной электронный адрес на вновь импортированный. То есть, вновь импортированный станет основным (primary).

2. Выполнить команду запуска импорта **import_groups**. Перед выполнением непосредственного импорта необходимо выполнить первоначальную проверку данных, предоставляемых для импорта и настроек подключения к ПО «Mailion»:
   – Выполнить непосредственный запуск импорта групп:

```
nct_ministerium import_groups
--config settings.json
```

Описание параметров запроса приведено в таблице 116.

Таблица 116 – Описание параметров запроса на импорт групп

Параметр	Тип	Обязательный	Описание
config	Str	+	Конфигурационный файл с параметрами сервиса Cox и настройками tls. Формируется автоматически на сервере с ролью ucs_infrastructure и находится по пути /srv/ministerium/config.json

Пример ответа:


```
{
  "Response": {
    "msg": "ok",
    "changed": true
  },
  "responses": [
    {
      "msg": "validation done, groups to import: 1"
    },
    {
      "msg": "import procedure summary: total reported results: 1, errors: 0,
success: 1",
      "changed": true
    }
  ]
}
```


– Выполнить запрос на проверку файла импорта, конфигурации и подключения к ПО «Mailion», но без запуска самого импорта:

```
nct-ministerium import_groups
--config groups.json
--check
```

Проверка файла производится по схеме, которая подробно описывает ограничения системы, существующие на структуру и поля данных группы. Схема в формате JSON Schema приведена в приложении (см. раздел «Схема записи группы» в Приложении В).

В а ж н о – Процедура импорта будет возможна, если все группы в файле импорта пройдут проверку по этой схеме.

Описание параметров запроса приведено в таблице 117.

Таблица 117 – Описание параметров запроса на проверку файла импорта, конфигурации и подключения к ПО «Mailion»

Параметр	Тип	Обязательный	Описание
config	Str	+	Конфигурационный файл с параметрами сервиса Cox и настройками tls. Формируется автоматически на сервере с ролью ucs_infrastructure и находится по пути /srv/ministerium/config.json
check	Str	+	Выполнение всех проверок, которые делает сервер системы, отвечающий за импорт

Пример ответа:


```
{
  "Response": {
    "msg": "ok"
  },
  "responses": [
    {
      "msg": "validation done, groups to import: 1"
    }
  ]
}
```


Примечание – Команда **import_groups** реализована таким образом, что поддерживает неоднократный запуск с одними и теми же параметрами, включая файл импорта.

3. Выполнить запрос на получение списка глобальных адресных книг, чтобы определить в какой GAL-тег определить создаваемые группы:

```
nct-ministerium get_tenant_gals
--config get_tenant_gals.json
```

Описание параметров запроса приведено в таблице 118.

Таблица 118 – Описание параметров запроса на получение GAL-тегов тенанта

Параметр	Тип	Обязательный	Описание
config	Str	+	Конфигурационный файл с параметрами сервиса Cox и настройками tls. Формируется автоматически на сервере с ролью ucs_infrastructure и находится по пути /srv/ministerium/config.json

Пример ответа:


```
{
  "Response": {
    "msg": "ok",
    "changed": true
  },
  "gals": [
    {
      "id": {
        "id": "1c22be2e-1e2f-5f6d-bec5-842c5d48e9d3",
        "region_id": "1dbacea3-5889-4021-8f38-bc2214dd7423"
      },
      "path": [
        "gal"
      ]
    },
    {
      "id": {
```

```
        "id": "1d34a52f-c510-40e7-b6ac-d6cae0753184",
        "region_id": "1dbacea3-5889-4021-8f38-bc2214dd7423"
      },
      "path": [
        "gal_1k"
      ]
    },
    {
      "id": {
        "id": "194ea408-9087-4bec-855e-ff8e82fdab8a",
        "region_id": "1dbacea3-5889-4021-8f38-bc2214dd7423"
      },
      "path": [
        "custom_gal"
      ]
    }
  ]
}
```


Пример файла настроек **get_tenant_gals.json** приведен в приложении (см. раздел «Список глобальных адресных книг» в Приложении В).

7.15.2 Импорт связей групп

Для выполнения второго этапа – импорта связей групп необходимо выполнить следующие действия:

1. Подготовить два файла:
   – Файл настроек процедуры импорта **settings.json**. Пример файла настроек для связей групп приведен в приложении (см. раздел «Файл настроек для импорта связей групп» в Приложении В).
   – Файл импорта, содержащий импортируемые в систему группы, в формате JSON (**groups_links.json**) или CSV (**groups_links.csv**). Пример заполняемых полей в файле приведен в разделе 7.15.3.
2. Выполнить команду запуска импорта **import_groups_links**. Перед выполнением непосредственного импорта выполнить первоначальную проверку данных, предоставляемых для импорта и настроек подключения к ПО «Mailion»:
   – Выполнить непосредственный запуск импорта пользователей:

```
nct_ministerium import_groups_links
--config settings.json
```

Описание параметров запроса приведено в таблице 119.

Таблица 119 – Описание параметров запроса на импорт связей групп

Параметр	Тип	Обязательный	Описание
config	Str	+	Конфигурационный файл с параметрами сервиса Cox и настройками tls. Формируется автоматически на сервере с ролью ucs_infrastructure и находится по пути /srv/ministerium/config.json

Пример ответа:

```
{
  "Response": {
    "msg": "ok",
    "changed": true
  },
  "responses": [
    {
      "msg": "validation done, groups links to import: 1"
    },
    {
      "msg": "import procedure summary: total reported results: 1, errors: 0,
success: 1",
      "changed": true
    }
  ]
}
```

– Выполнить запрос на проверку файла импорта, конфигурации и подключения к ПО «Mailion», но без запуска самого импорта:

```
nct-ministerium import_groups_links
--config groups.json
--check
```

Проверка файла производится по схеме, которая подробно описывает ограничения системы, существующие на структуру и поля данных группы. Схема в формате JSON Schema приведена в приложении (см. раздел «Схема записи связей групп» в Приложении В).

В а ж н о – Процедура импорта будет возможна, если все связи групп в файле импорта пройдут проверку по этой схеме.

Описание параметров запроса приведено в таблице 120.

Таблица 120 – Описание параметров запроса на проверку файла импорта, конфигурации и подключения к ПО «Mailion»

Параметр	Тип	Обязательный	Описание
config	Str	+	Конфигурационный файл с параметрами сервиса

Параметр	Тип	Обязательный	Описание
			Cox и настройками tls. Формируется автоматически на сервере с ролью ucs_infrastructure и находится по пути /srv/ministerium/config.json
check	Str	+	Выполнение всех проверок, которые делает сервер системы, отвечающий за импорт

Пример ответа:

```
{
  "Response": {
    "msg": "ok"
  },
  "responses": [
    {
      "msg": "validation done, groups links to import: 1"
    }
  ]
}
```

7.15.3 Подготовка файла импорта

Формат JSON является основным для системы и позволяет наиболее полно описать группу.

Описание параметров файла импорта **groups.json** приведено в таблице 121.

Таблица 121 – Описание параметров файла импорта **groups.json**

Параметр	Тип	Обязательный	Описание
correlation_id	Str	+	Идентификатор группы. Должен быть уникален в пределах файла импорта. Система ссылается на этот идентификатор при информировании пользователя об успешности импорта отдельной группы или об ошибках, возникших в процессе импорта. Может быть произвольной строкой, например идентификатор группы в системе, из которой производится перенос групп или случайно сгенерированный UUID
name	Str	+	Название группы
description	Str	-	Описание группы
email	Str	+	Электронная почта группы

Файл импорта в формате CSV позволяет импортировать группы с ограниченным набором данных.

Описание параметров файла импорта **groups.csv** приведено в таблице 122.

Таблица 122 – Описание параметров файла импорта **groups.csv**

Параметр	Обязательный	Описание
correlation_id	+	Идентификатор группы. Должен быть уникален в пределах файла импорта. Система ссылается на этот идентификатор при информировании пользователя об успешности импорта отдельной группы или об ошибках, возникших в процессе импорта. Может быть произвольной строкой, например, идентификатор группы в системе, из которой производится перенос групп или случайно сгенерированный UUID
name	+	Название группы
description	-	Описание группы
email	+	Электронная почта группы

7.15.4 Примеры сообщений системы

Пример успешного импорта связей групп:

```
Oct 26 13:09:49.890     info    ministerium/import_group_links.go:128   import
file verification starts, it will take some time {"client-request-id":
"cd227e3f-65a6-4b2c-8310-a34a170cf3dc", "command": "import_groups_links"}
Oct 26 13:09:54.071     info    ministerium/import_group_links.go:226   group
link imported     {"client-request-id": "cd227e3f-65a6-4b2c-8310-a34a170cf3dc",
"command": "import_groups_links", "correlation_id": "link external id1",
"status": "ok"}
Oct 26 13:09:54.072     info    ministerium/import_group_links.go:226   group
link imported     {"client-request-id": "cd227e3f-65a6-4b2c-8310-a34a170cf3dc",
"command": "import_groups_links", "correlation_id": "link external id2",
"status": "ok"}
Oct 26 13:09:54.072     info    ministerium/import_group_links.go:226   group
link imported     {"client-request-id": "cd227e3f-65a6-4b2c-8310-a34a170cf3dc",
"command": "import_groups_links", "correlation_id": "link external id3",
"status": "ok"}
{
  "Response": {
    "changed": true,
    "failed": false,
    "msg": "ok"
  },
  "responses": [
    {
      "changed": false,
      "failed": false,
      "msg": "validation done, group links to import: 3"
    },
```

```
    {
      "changed": true,
      "failed": false,
      "msg": "import procedure summary: total reported results: 3, errors: 0,
success: 3"
    }
  ]
}
```

Описания сообщений приведены в таблице 123.

Таблица 123 – Описание сообщений системы

Сообщение	Описание
import file verification starts, it will take some time	Сообщение говорит о том, что процесс локальной проверки файла импорта запущен. Такая проверка осуществляется при каждом запуске, до отправки файла импорта на сервер. Время проверки зависит от количества групп, переданных для импорта, и может занимать значительное время.
group link imported	Связь группы успешно импортирована. Об этом говорит маркер «ok» в поле «status». Идентификатор импортируемой записи группы сообщается в поле «correlation_id». В поле «total» показывается общее количество полученных ответов от сервера обо всех связях групп, успешно импортированных и не импортированных
validation done, group links to import	Проверка файла импорта прошла успешно и обнаружена одна связь группы для импорта. Это сообщение отобразится только в том случае, если все связи группы прошли проверку по схеме, описанной в приложении (см. раздел «Схема записи группы» в Приложении В)
import procedure summary	Итог импорта, сообщает количество групп, которые были обработаны системой, количество групп с ошибками и количество успешно импортированных групп

7.15.5 Возможные ошибки при импорте групп

Описания возможных ошибок при импорте групп приведены в таблице 124.

Таблица 124 – Описание возможных ошибок

Название ошибки	Вид в интерфейсе командной строки	Описание

Ошибка декодирования JSON	{
	"msg": "import file validation: decode next group: decode JSON: invalid character '}' looking for beginning of value",
	"failed": true
	}
		Сообщение выводится в случае, если утилита не может декодировать файл импорта, в этом случае необходимо проверить корректность синтаксиса JSON или CSV

Название ошибки	Вид в интерфейсе командной строки	Описание

Ошибка при проверке записи группы по схеме	{
	"msg": "import file validation: group correlation ID: : correlation_id: String length must be greater than or equal to 1",
	"failed": true
	}
		Сообщение транслирует информацию о том, что обязательное поле "correlation_id" отсутствует или имеет пустое значение

Ошибка в адресе электронной почты	{
	"msg": "import file validation: group correlation ID: f1b97e81-e4a3-4ebd-ba59-e4b864ef4797: emails.0.email: Does not match format 'email'",
	"failed": true
	}
		Сообщение выводится в случае, если группа с идентификатором (correlation_id) "f1b97e81-e4a3-4ebd-ba59-e4b864ef4797" не прошла проверку по схеме

Ошибка в логине	{
	"msg": "import file validation: group correlation ID: f1b97e81-e4a3-4ebd-ba59-e4b864ef4797: logins.0.login: String length must be greater than or equal to 1",
	"failed": true
	}
		Аналогично предыдущему примеру, но отсутствует поле "login" у первой структуры в списке логинов (logins)

Ошибка, дубликат электронного адреса	{
	"msg": "import file validation: duplicate email found: 433bfcea-5adf-49ee-88e5-cfca9a575b6b@example.com (users correlation IDs: f1b97e81-e4a3-4ebd-ba59-e4b864ef4797, 1d567e35-31ce-461e-8a35-5efd2012362c)",
	"failed": true
	}
		Еще один пример проверки, выполняемой перед отправкой файла импорта на сервер.
		Здесь говорится о том, что у записей группы с идентификаторами (correlation_id) "f1b97e81-e4a3-4ebd-ba59-e4b864ef4797" и "1d567e35-31ce-461e-8a35-5efd2012362c" найдено повторение электронного адреса, его значение: "433bfcea-5adf-49ee-88e5-cfca9a575b6b@example.com". Необходимо исправить электронный адрес у одного из пользователей

Ошибка, возникшая в процессе импорта группы на стороне сервера	$ nct-ministerium import_groups --config import_config.json import file verification starts, it will take some time {"client-request-id": "09ed4436-41e9-475f-b741-7ae81237cc8f", "command": "import_users"} user error {"client-request-id": "09ed4436-41e9-475f-b741-7ae81237cc8f", "command": "import_groups", "correlation_id": "f1b97e81-	Пример ошибки, возникшей в процессе импорта группы на стороне сервера, например по причине отказа сетевого окружения

Название ошибки	Вид в интерфейсе командной строки	Описание

	e4a3-4ebd-ba59-e4b864ef4797", "status": "error", "error": "upsert user: save profile: common.Error(module:PERSEUS code:5000 msg:\"ERAKLES_ERROR\")", "total": 1}
	{
	"Response": {
	"msg": "ok",
	"changed": true
	},
	"responses": [
	{
	"msg": "validation done, users to import: 1"
	},
	{
	"msg": "import procedure summary: total reported results: 1, errors: 1, success: 0",
	"changed": true
	}
	]
	}	

	group error	В этом сообщении говорится о том, что группа с идентификатором, указанным в поле "correlation_id" не была импортирована. На это указывает маркер "error" в поле "status" и наличие поля "error", которое содержит сообщение об ошибке со стороны системы. Соответственно эта группа будет добавлена в файл, указанный в параметре "rejected_groups_path" или в файл с именем по умолчанию

Возможен сценарий, при котором файл импорта выгружается несколько раз с какими-либо уточнениями из системы-источника и каждый раз (кроме первого) происходит обновление группы в системе ПО «Mailion». Кроме повторного запуска с исправленными/уточненными данными в исходном файле импорта также допускается импорт файла **rejected_groups.json**, после исправлений ошибок о которых система оповестила в процессе импорта. Для этого путь к файлу **rejected_groups.json** нужно указать в

параметре user_data_path, не допустив при этом пересечения имени с параметром **rejected_groups_path**.

П р и м е ч а н и е – Группы, не импортированные или частично импортированные в систему, записываются в **rejected_groups.json**. При этом для каждой такой группы система выдаст сообщение об ошибке на экран. Найти конкретную группу в файле **rejected_groups.json** можно по **correlation_id**.

7.15.6 Автоматизация переноса групп и их связей из LDAP-каталогов в каталог ПО «Mailion»

При автоматизации экспорта необходимых групп и их связей из LDAP-каталога администратор использует утилиты, позволяющие выполнить следующие действия:

– отфильтровать необходимые для импорта в каталог ПО «Mailion» группы, задав фильтры LDAP Search;
– сохранить файл с результатами операции LDAP Search в формате LDIF (поддерживаются только записи **changetype: add**, записи **changetype: modify** не поддерживаются).

Пример команды экспорта из каталога Microsoft Active Directory (AD):

```
ldifde -f OUTPUT.LDF
-b администратор test-forest *
-s 10.1.1.50 -d "dc=test-forest,dc=local"
-r "(objectClass=group)"
```

Пример команды экспорта из каталога OpenLDAP/FreeIPA (командная строка Linux):

```
ldapsearch
-H ldap://10.1.1.50:389 -x
-D 'test-forest\администратор'
-w '****'
-b 'dc=test-forest,dc=local'
-s sub
-a always '(objectClass=group)' '*' > OUTPUT.LDF
```

В а ж н о – Особенности экспорта из LDAP-каталога при помощи утилиты ldifde: такую утилиту обязательно нужно использовать без опции "-m". **nct_ldif_converter** не обрабатывает **changetype**, отличный от **add**.

Для автоматизации импорта в каталог ПО «Mailion» предназначена утилита **nct_ldif_converter**. Полученный файл в формате LDIF может быть использован при запуске данной утилиты.

Пример корректной записи в LDIF файле (changetype: add):

```
dn: CN=TestGroup1,CN=Users,DC=test-forest,DC=local
changetype: add
objectClass: top
objectClass: group
cn: TestGroup1
description: PervayaGruppa opisanie
member: CN=GLOBALgroup,CN=Users,DC=test-forest,DC=local
member: CN=TestGroup2,CN=Users,DC=test-forest,DC=local
member: CN=UserTest1 a,CN=Users,DC=test-forest,DC=local
distinguishedName: CN=TestGroup1,CN=Users,DC=test-forest,DC=local
instanceType: 4
whenCreated: 20220725234749.0Z
whenChanged: 20220726211521.0Z
uSNCreated: 18915
info: PervayaGruppa zametka
memberOf: CN=GLOBALgroup,CN=Users,DC=test-forest,DC=local
memberOf: CN=TestGroup4,CN=Users,DC=test-forest,DC=local
memberOf: CN=TestGroup3,CN=Users,DC=test-forest,DC=local
uSNChanged: 19160
name: TestGroup1
objectGUID:: WjCoO3Tf40GUOw9s8N+ytw==
objectSid:: AQUAAAAAAAUVAAAAVUO/Hdot23E9GJS5aAQAAA==
sAMAccountName: TestGroup1
sAMAccountType: 268435457
groupType: 8
objectCategory: CN=Group,CN=Schema,CN=Configuration,DC=test-forest,DC=local
dSCorePropagationData: 20220803000327.0Z
dSCorePropagationData: 16010101000001.0Z
mail: PervayaGruppa@lan.ru
```

Пример команды запуска утилиты **nct_ldif_converter**:

```
nct_ldif_converter
-s OUTPUT.LDF
```

где -s указывает на путь к файлу в формате LDIF.

С помощью **nct_ldif_converter** сформируется два файла:

– **groups.json**, записи в формате JSON Lines, описывающие сами группы;

– **links.json**, записи, описывающие связи групп, также в формате JSON Lines.

При необходимости файлы **groups.json** и **links.json** можно отредактировать, после чего использовать при выполнении команд **import_groups** (см. раздел 7.15.1) и **import_groups_links** (см. раздел 7.15.2) соответственно.

7.16 Массовое создание ресурсов в каталоге

В а ж н о – Массовое создание ресурсов выполняется пользователем с ролью администратора тенанта или администратора инсталляции.

Массовое создание ресурсов в каталоге осуществляется с помощью импорта ресурсов в систему из файла, выгруженного заранее из внешнего каталога.

Для импорта ресурсов из файла необходимо выполнить следующие действия:

1. Подготовить два файла:
   – Файл настроек процедуры импорта **settings.json**. Пример файла настроек приведен в приложении (см. раздел «Файл настроек импорта ресурсов» в Приложении В).
   – Файл импорта, содержащий импортируемых в систему пользователей, в формате JSON (**resources.json**) или CSV (**resources.csv**). Пример заполняемых полей в файле приведен в разделе 7.14.1.

   П р и м е ч а н и е – Для каждого отдельного ресурса перед импортом система выполняет поиск пользователя по электронным адресам почты (emails) и логинам (logins). Если найдено совпадение, то вместо создания нового ресурса выполняется обновление данных. Обновляются все поля ресурса, за исключением электронных адресов и логинов – они будут добавлены.

2. Выполнить команду запуска импорта **import_resources**. Перед выполнением непосредственного импорта выполнить первоначальную проверку данных, предоставляемых для импорта и настроек подключения к ПО «Mailion»:
   – Выполнить непосредственный запуск импорта ресурсов:

```
nct_ministerium settings.json --config settings.json
```

Описание параметров запроса приведено в таблице 125.

Таблица 125 – Описание параметров запроса на импорт ресурсов

Параметр	Тип	Обязательный	Описание
config	Str	+	Конфигурационный файл с параметрами сервиса Cox и настройками tls. Формируется автоматически на сервере с ролью ucs_infrastructure и находится по пути /srv/ministerium/config.json

Пример ответа:

```
{
  "Response": {
    "msg": "ok",
    "changed": true
  },
  "responses": [
```

```
    {
      "msg": "validation done, resources to import: 1"
    },
    {
      "msg": "import procedure summary: total reported results: 1, errors: 0,
success: 1",
      "changed": true
    }
  ]
}
```

– Выполнить запрос на проверку файла импорта, конфигурации и подключения к ПО «Mailion», но без запуска самого импорта:

```
nct-ministerium import_users
--config settings.json
--check
```

Проверка файла производится по схеме, которая подробно описывает ограничения системы, существующие на структуру и поля данных ресурса. Схема в формате JSON Schema приведена в приложении (см. раздел «Схема записи ресурса» в Приложении В).

В а ж н о – Ресурс не будет успешно импортирован, если он не удовлетворяет этой схеме.

Описание параметров запроса приведено в таблице 126.

Таблица 126 – Описание параметров запроса на проверку файла импорта, конфигурации и подключения к ПО «Mailion»

Параметр	Тип	Обязательный	Описание
config	Str	+	Конфигурационный файл с параметрами сервиса Cox и настройками tls. Формируется автоматически на сервере с ролью ucs_infrastructure и находится по пути /srv/ministerium/config.json
check	Str	+	Выполнение всех проверок, которые делает сервер системы, отвечающий за импорт

Пример ответа:

```
{
  "Response": {
    "changed": false,
    "failed": false,
    "msg": "ok"
  },
  "responses": [
    {
      "changed": false,
```

```
      "failed": false,
      "msg": "validation done, resources to import: 1"
    }
  ]
}
```


Примечание – Команда **import_resources** реализована таким образом, что поддерживает неоднократный запуск с одними и теми же параметрами, включая файл импорта.

3. Выполнить запрос на получение списка глобальных адресных книг, чтобы определить в какой GAL-тег определить создаваемые ресурсы:

```
nct-ministerium get_tenant_gals --config get_tenant_gals.json
```

Описание параметров запроса приведено в таблице 127.

Таблица 127 – Описание параметров запроса на получение GAL-тегов тенанта

Параметр	Тип	Обязательный	Описание
config	Str	+	Конфигурационный файл с параметрами сервиса Cox и настройками tls. Формируется автоматически на сервере с ролью ucs_infrastructure и находится по пути /srv/ministerium/config.json

Пример ответа:


```
{
  "Response": {
    "msg": "ok",
    "changed": true
  },
  "gals": [
    {
      "id": {
        "id": "1c22be2e-1e2f-5f6d-bec5-842c5d48e9d3",
        "region_id": "1dbacea3-5889-4021-8f38-bc2214dd7423"
      },
      "path": [
        "gal"
      ]
    },
    {
      "id": {
        "id": "1d34a52f-c510-40e7-b6ac-d6cae0753184",
        "region_id": "1dbacea3-5889-4021-8f38-bc2214dd7423"
      },
      "path": [
        "gal_1k"
      ]
    },
    {
      "id": {
        "id": "194ea408-9087-4bec-855e-ff8e82fdab8a",
```

```
        "region_id": "1dbacea3-5889-4021-8f38-bc2214dd7423"
      },
      "path": [
        "custom_gal"
      ]
    }
  ]
}
```

Пример файла настроек **get_tenant_gals.json** приведен в приложении (см. раздел «Список глобальных адресных книг» в Приложении В).

7.16.1 Подготовка файла импорта

В а ж н о – Файл импорта может быть предоставлен только в форматах JSON Lines и CSV.

Формат JSON является основным для системы и позволяет наиболее полно описать параметры ресурсов.

Описание параметров файла импорта **user_profiles.json** приведено в таблице 128.

Таблица 128 – Описание параметров файла импорта **user_profiles.json**

Параметр	Тип	Обязательный	Описание
correlation_id	Str	+	Пользовательский идентификатор. Должен быть уникален в пределах файла импорта. Система ссылается на этот идентификатор при информировании пользователя об успешности импорта или об ошибках, возникших в процессе импорта. Может быть произвольной строкой, например, идентификатор ресурса в системе, из которой производится перенос пользователей или случайно сгенерированный UUID
name	Str	+	Имя ресурса
description	Str	-	Описание ресурса
capacity	Str	+	Максимальная вместимость
email	Str	+	Адрес почты ресурса с доменом
location_name	Str	-	Название адреса
country	Str	-	Страна
city	Str	-	Город
address	Str	-	Адрес

Параметр	Тип	Обязательный	Описание
zip_code	Str	-	Индекс
floor	Str	-	Этаж
room	Str	-	Кабинет
workplace	Str	-	Рабочее место
login	Str	+	Логин ресурса (с доменом или нет)
password	Str	+	Пароль
autobook	Str	-	Автоматическое бронирование ресурса
minimal_ participation_ number	Str	+	Минимальное количество участников

В а ж н о – Каждый отдельный объект ресурса проверяется по JSON-схеме записи пользователя, приведенной в приложении (см. раздел «Схема записи ресурса» в Приложении В).

Файл импорта в формате CSV позволяет импортировать объекты ресурсов с ограниченным набором данных.

Описание параметров файла импорта **user_profiles.csv** приведено в таблице 129.

Таблица 129 – Описание параметров файла импорта **user_profiles.csv**

Параметр	Обязательный	Описание
correlation_id	+	Идентификатор ресурса, уникальный в пределах файла импорта
name	+	Название ресурса
email	+	Основной электронный адрес и логин
password	+	Пароль для логина, заданного полем **email**

7.16.2 Примеры сообщений системы

Пример успешного импорта ресурса в файле импорта:

```
ucs_ministerium import_resources --
config /home/user/ministerium/resource_settings.json
Sep 13 17:34:06.076     info    ministerium/import_resources.go:147     import
file verification starts, it will take some time {"client-request-id":
"d2de1455-21d4-4762-9999-b095fdb94d2f", "command": "import_resources"}
Sep 13 17:34:11.470     info    ministerium/import_resources.go:248     resource
imported       {"client-request-id": "d2de1455-21d4-4762-9999-b095fdb94d2f",
```

```
"command":"import_resources", "correlation_id": "00025fe9-1fb5-4fda-a6ac-
c8fb5572b88f", "status": "ok"}
{
  "Response": {
    "changed": true,
    "failed": false,
    "msg": "ok"
  },
  "responses": [
    {
      "changed": false,
      "failed": false,
      "msg": "validation done, resources to import: 1"
    },
    {
      "changed": true,
      "failed": false,
      "msg": "import procedure summary: total reported results: 1, errors: 0,
success: 1"
    }
  ]
}
```


Описания сообщений приведены в таблице 130.

Таблица 130 – Описание сообщений системы

Сообщение	Описание
import file verification starts, it will take some time	Процесс локальной проверки файла импорта запущен. Такая проверка осуществляется при каждом запуске, до отправки файла импорта на сервер. Время проверки зависит от количества пользователей, переданных для импорта, и может занимать значительное время
resource imported	Сообщение о том, что ресурс успешно импортирован. Об этом говорит маркер «ok» в поле «status». Идентификатор импортируемой записи сообщается в поле «correlation_id»
validation done, resources to import	Сообщает о том, что проверка файла импорта прошла успешно и обнаружен один ресурс для импорта. Это сообщение появится только в том случае, если все ресурсы прошли проверку по схеме
import procedure summary	Итог импорта, сообщает количество ресурсов, которые были обработаны системой, количество ресурсов с ошибками и количество успешно импортированных ресурсов

7.16.3 Возможные ошибки при импорте объектов ресурсов

Описания возможных ошибок при импорте объектов ресурсов приведены в таблице 131.

Таблица 131 – Описание возможных ошибок

Название ошибки	Вид в интерфейсе командной строки	Описание

Ошибка декодирования JSON	{
	"msg": "import file validation: decode next user: decode JSON: invalid character '}' looking for beginning of value",
	"failed": true
	}
		Сообщение выводится в случае, если утилита не может декодировать файл импорта, в этом случае необходимо проверить корректность синтаксиса JSON или CSV

Повторяющийся correlation ID	{
	"changed": false,
	"failed": true,
	"msg": "import file validation: duplicate correlation_id found: 00025fe9-1fb5-4fda-a6ac-c8fb5572b88f"
	}
		Сообщение выводится в случае, если две записи ресурса в файле имеют одинаково заполненное поле correlation ID

Пустой correlation ID	{
	"changed": false,
	"failed": true,
	"msg": "import file validation: resource correlation ID: : resource CorrelationId is empty"
	}
		Сообщение выводится в случае, если поле correlationID не заполнено

Ошибка создания Email	{
	"Response": {
	"changed": true,
	"failed": false,
	"msg": "ok"
	},
	"responses": [
	{
	"changed": false,
	"failed": false,
	"msg": "validation done, resources to import: 1"
	},
	{
	"changed": true,
	"failed": false,
	"msg": "import procedure summary: total reported results: 1, errors: 1, success: 0"
	}
	]
		Сообщение выводится в случае ошибки создания Email

Название ошибки	Вид в интерфейсе командной строки	Описание
	}	

Возможен сценарий, при котором файл импорта выгружается несколько раз с какими-либо уточнениями из системы-источника и каждый раз (кроме первого) происходит обновление объектов ресурсов в ПО «Mailion». Кроме повторного запуска с исправленными/уточненными данными в исходном файле импорта также допускается импорт файла **rejected_resources.json**, после исправлений ошибок о которых система оповестила в процессе импорта. Для этого путь к файлу **rejected_resources.json** нужно указать в параметре user_data_path, не допустив при этом пересечения имени с параметром **rejected_resources_path**.

Примечание – Ресурсы, не импортированные в систему или частично импортированные, записываются в **rejected_resources.json**. При этом для каждого такого объекта ресурса система выдаст сообщение об ошибке на экран. Найти конкретный объект ресурса в файле **rejected_resources.json** можно по **correlation_id**.

7.17 Синхронизация календаря с Exchange

Синхронизация событий календаря с Exchange происходит с периодичностью, заданной в параметре `limits` сервиса **Hog** (в секундах):

```
"limits": {
    "sync_process_chunk_time_limit": 300
}
```

По умолчанию период синхронизации составляет 300 секунд.

Управление синхронизацией производится командами **ministerium**.

7.17.1 Включение/выключение синхронизации для домена

Пример запроса:

```
nct_ministerium update_domain \
--config ministerium.json \
--id= <...> \
--features.is_mail=true \
--features.is_authorization=true \
```

```
--features.is_service=true \
--external.is_sync_enabled=false
```

Описание параметров команды управления синхронизацией для домена приведено в таблице 132.

Таблица 132 – Параметры команды управления синхронизацией для домена

Параметр	Тип	Обязательный	Описание
config	Str	+	Путь к файлу конфигурации
id	Str	+	Идентификатор домена
features.is_mail	Bool	+	Если значение **true**, домен может принимать почтовые сообщения
features.is_authorization	Bool	+	Если значение **true**, домен можно использовать для авторизации
features.is_service	Bool	+	Если значение **true**, домен можно использовать для авторизации по умолчанию
external.is_sync_enabled	Bool	+	Включение/отключение синхронизации: – **false** – выключена; – **true** – включена

Пример ответа:

```
{
  "changed": true,
  "failed": false,
  "msg": "ok"
}
```

7.17.2 Блокировка синхронизации для конкретного пользователя

Пример запроса:

```
nct_ministerium set_sync_block_setting_for_user \
--config <...> \
--login <...> \
--setBlock=true \
--enableImmidiately=false
```

Описание параметров команды блокировки синхронизации для конкретного пользователя приведено в таблице 133.

Таблица 133 – Параметры команды блокировки синхронизации для конкретного пользователя

Параметр	Тип	Обязательный	Описание
config	Str	+	Путь к файлу конфигурации
login	Str	+	Логин пользователя
setBlock	Bool	+	Установка блокировки синхронизации (для тенанта или пользователя): – **true** – блокировка установлена; – **false** – блокировка снята
enableImmidiately	Bool	+	Снять/установить флажки в настройках: – **false** – флажки сняты; – **true** – флажки установлены

Пример ответа:

```
{
  "Response": {
    "changed": true,
    "failed": false,
    "msg": "ok"
  },
  "changed_entity_id": "ид измененного пользователя"
}
```

7.17.3 Блокировка синхронизации для тенанта

Пример запроса:

```
nct_ministerium set_sync_block_setting_for_all_users_in_tenant \
--config <...> \
--tenantId <...> \
--setBlock=true \
--enableImmidiately=false
```

Описание параметров команды блокировки синхронизации для тенанта приведено в таблице 134.

Таблица 134 – Параметры команды блокировки синхронизации для тенанта

Параметр	Тип	Обязательный	Описание
config	Str	+	Путь к файлу конфигурации
tenantId	Str	+	Идентификатор тенанта

Параметр	Тип	Обязательный	Описание
setBlock	Bool	+	Установка блокировки синхронизации (для тенанта или пользователя): – **true** – блокировка установлена; – **false** – блокировка снята
enableImmidiately	Bool	+	Снять/установить флажки в настройках: – **false** – флажки сняты; – **true** – флажки установлены

Пример ответа:

```
{
  "changed": true,
  "failed": false,
  "msg": "ok"
}
```

Для синхронизации событий приглашений (чтобы приглашения попадали в календарную сетку) необходимо в приложении Exchange включить настройку **Параметры** > **Показать все параметры** > **Календарь** > **Автоматически обрабатывать запросы и отклики от внешних отправителей** (см. Рисунок 80).

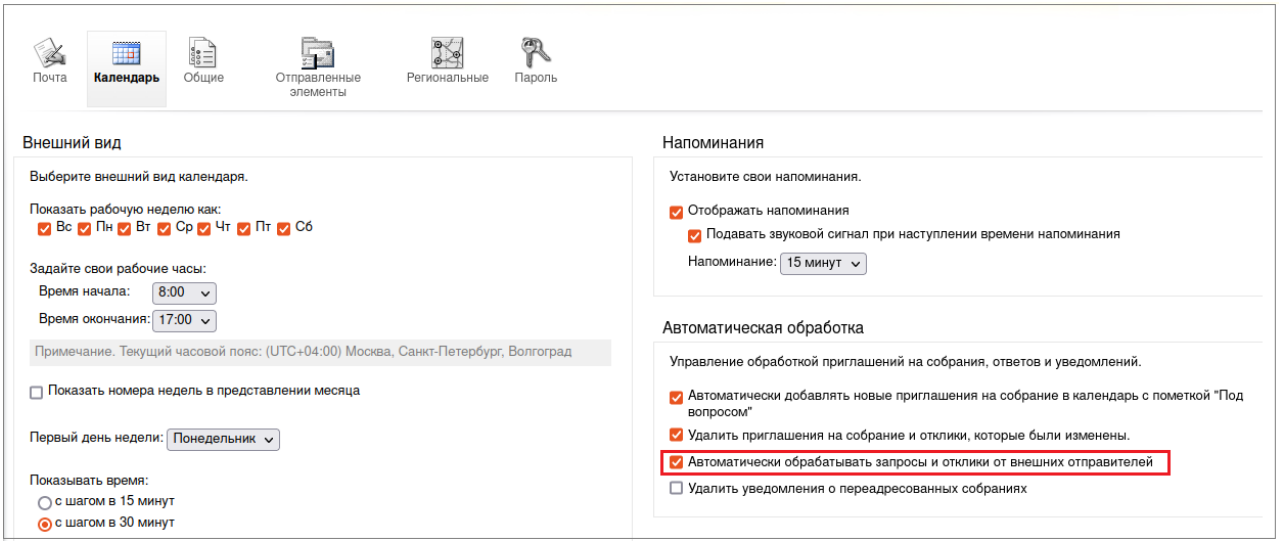


Рисунок 80 – Вкладка настройки календаря в Exchange

7.17.4 Выбор источника календаря для синхронизации

Данная команда выполняется для делегированного пользователя и задает источник календарных данных для синхронизации. Например, если делегированный пользователь ни разу не проходил аутентификацию в Mailion, то при создании события, где он будет участником, данные о его занятости будут извлекаться из Exchange (**calendar_source_type = CALENDAR_TYPE_UNSPECIFIED**). Если же аутентификация была пройдена, то значение **calendar_source_type** поменяется на **CALENDAR_TYPE_MAILION**.

Если требуется поменять источник календаря на Exchange, то следует выполнить команду **set_calendar_source**, задав для параметра **calendar_source_type** значение **CALENDAR_TYPE_EXCHANGE**.

Пример запроса:

```
nct_ministerium set_calendar_source \
--config <...> \
--user_id efad31ad-6ff3-4aea-8c4a-ce3e44248b56 \
--calendar_source_type CALENDAR_TYPE_EXCHANGE \
--v
```

Описание параметров команды выбора источника календаря приведено в таблице 135.

Таблица 135 – Параметры команды выбора источника календаря

Параметр	Тип	Обязательный	Описание
config	Str	+	Путь к файлу конфигурации
user_id	Str	+	Идентификатор пользователя
calendar_source_type	Str	+	CALENDAR_TYPE_UNSPECIFIED – источник не определен; CALENDAR_TYPE_MAILION – источником календаря является Mailion; CALENDAR_TYPE_EXCHANGE – источником календаря является Exchange

Пример ответа:

```
{
  "changed": true,
  "failed": false,
  "msg": "ok"
}
```

7.18 Настройка миграции данных календаря

В а ж н о – Для миграции данных необходимо использовать Microsoft Exchange версии 2010 и выше.

Для запуска миграции календаря необходимо выполнить следующие действия:

1. Зайти на машину через SSH, например `ssh <username>@<host>`, где `<host>` – имя хоста из inventory, где расположен сервис **kex**.
2. Выполнить команду `docker exec -ti kex bash`.
3. Внутри контейнера с **kex** перейти в каталог **/usr/local/bin** (`cd /usr/local/bin`), где находятся утилиты для миграции календаря:
   – **ucs-exch-to-mln-migrator** (подробнее о запуске миграции календаря из Microsoft Exchange в ПО «Mailion» см. в разделе 7.18.1);
   – **ucs-mln-to-exch-migrator** (подробнее о запуске миграции календаря из ПО «Mailion» в Microsoft Exchange см. в разделе 7.18.2).
4. Внутри контейнера **kex** перейти в каталог **/etc/ucs/kex** (`cd /etc/ucs/kex`), где находятся конфигурационные файлы для миграции календаря:
   – /etc/ucs/kex/calendar_exch_to_mln_migrator.json;
   – /etc/ucs/kex/calendar_mln_to_exch_migrator.json.

В а ж н о – **Выполнение миграции вместе с включенной синхронизацией невозможно. Перед началом миграции необходимо отключить синхронизацию.** Примеры команд для отключения синхронизации приведены в разделе 7.17.

7.18.1 Миграция данных календаря из Microsoft Exchange в ПО «Mailion»

Мигратор представляет собой отдельный исполняемый файл. Для запуска мигратора необходимо выполнить запрос:

```
./ucs-exch-to-mln-migrator
-from user@user@ad.example.net \
-to user@user@installation.example.net \
-ignore-errors=true \
-from-time 2022-07-17T15:04:05Z \
-to-time time 2023-07-17T15:04:05Z \
-c /path/to/config.json
```

В а ж н о – Миграция пользователей должна производиться только в одноименные учетные записи.

Описание параметров запроса приведено в таблице 136.

Таблица 136 – Параметры запроса на вызов мигратора

Параметр	Тип	Обязательный	Описание
from	Str	+	Почтовый адрес пользователя Microsoft Exchange, чьи календарные данные будут мигрировать. Пример записи пользователя в данном параметре для однодоменной делегации: user@ad.example.net. Пример записи пользователя в данном параметре для мультидоменной делегации: – пользователь Microsoft Exchange – user@ad.example.net; – пользователь ПО «Mailion» – user@installation.example.net
to	Str	+	Почтовый адрес пользователя Mailion, на который мигрируют календарные данные. Пример записи пользователя в данном параметре для однодоменной делегации: user@ad.example.net. Пример записи пользователя в данном параметре для мультидоменной делегации: – пользователь Microsoft Exchange – user@ad.example.net; – пользователь ПО «Mailion» – user@installation.example.net
ignore-errors	Bool	+	Значение по умолчанию **true**. Отвечает за продолжение работы мигратора в случае ошибок (ошибки попадают в журнал работы системы; пример записи в журнале работы системы приведен ниже). Если значение **false**, процесс миграции останавливается при первой ошибке
from-time	Str	-	Параметр для указания даты, начиная с которой необходимо перенести события из календаря. Пример формата времени: 2015-07-17T15:04:05Z (RFC3339)
to-time	Str	-	Параметр для указания даты, до которой необходимо перенести события из календаря. Пример формата времени: 2015-07-17T15:04:05Z (RFC3339)
c	Str	+	Путь к файлу конфигурации (по умолчанию `internal/config/config.local.json`)

В а ж н о – Можно указать только один параметр времени: **from-time** или **to-time**. Временной промежуток может быть не более двух лет. При указании одного из параметров второй будет вычислен автоматически путем прибавления или вычитания двух лет.

Пример отчета о завершении миграции календаря:

```
{
    "migration": {
        "trace_id": string, (trace id миграции, чтобы можно было посмотреть
логи)
        "date": "2024-03-13 18:39:41.496800048 +0300 MSK m=+6.098483637", (дата,
когда был запущен мигратор)
        "migration_mode": { (Режим запуска мигратора)
            "type": "all"/"period", (За все время/За определенный период
времени)
            "ignore_errors": bool, (Режим игнорирования ошибок)
            "from": "DD.MM.YYYY HH:MM:SS", (Опционально - если выбран тип
"period")
            "to": "DD.MM.YYYY HH.MM.SS" (Опционально - если выбран тип "period)
            },
        "mailion_email": "test_user@se.stageoffice.ru",
        "exchange_email": "test_user@ad.stageoffice.ru",
        "errors": { (Ошибки)
            "num_folders": 0, (Количество "папок" с ошибками)
            "folders"" {}
        }.
        "all_objects_in_mailion_before_migration": 0 (Количество объектов ДО
миграции в Mailion)
        "all_synced_objects": 12, (ТО, что синхронизировалось при актуальном
запуске)
        "all_objects_in_exhange": 12, (ТО-ВЕ: Все объекты в указанном периоде)
        "all_errors_count": 0 (exchange = errors? + all_synced + already_synced)
        "migration_progress": 100 (Процент смигрированных объектов)
    },
    "current_status": { (Текущий статус)
        "exchange": {
            "folders": { (Количество "папок" (имеется в виду календарей, включая
те, в которых есть ТО-DO))
                "Задачи": {
                    "num_objects": 0, (Количество объектов)
                    "ews_id"
"AAMkAGNkMjYzMjQ0LTUzMzAtNDhhMy04YzQyLTkxZGU3NzZkNjgyJ+U6H4cR6at4RdJZOWeAAAAK/pB
AAA=" (Индентификатор в EWS)
                },
                "Календарь": {
                    "num_objects": 12, (Количество объектов)
                    "ews_id":
"AAMkAGNkMjYzMjQ0LTUzMzAtNDhYvcFAQAf+J+U6H4cR6at4RdJZOWeAAAAK/o8AAA="
 (Идентификатор в EWS)
                }
            },
            "num_folders": 2 (Количество "папок")
        },
        "mailion": {
            "folders": { (Количество "папок" (имеется в виду календарей, включая
те, в которых есть ТО-DO))
                "Задачи": {
```

```
                    "num_objects": 0 (Количество объектов)
                },
                "Календарь": {
                    "num_objects": 12 (Количество объектов)
                }
            },
            "num_folders": 2 (Количество "папок")
        }
    }
}
```

Примеры ошибок при миграции календаря:

– Неподдерживаемый формат события, уровень ERROR:

```
2023-11-28T11:41:19.883  ERR  errreporter/impl.go:23  convert calendar item to
event: uid is nil: mexa error [ErrorResponseUnexpectedNil]
{"service_endpoint":"ucs-apps-1.testoffice.ru:6788"}
```

– Неподдерживаемое вложение в событии, уровень ERROR:

```
2023-11-28T11:41:19.883  ERR  errreporter/impl.go:18  Reference contains invalid
type of SpanReference: {}  {"service_endpoint":"kex.ucs-apps-
1.yankee.stageoffice.ru:6788"}
```

– Неверно указан UPN или email мигрируемого пользователя, уровень FATAL:

```
2024-03-21T12:29:18.243  FTL  exch-to-mln-migrator/main.go:127  import calendars
and events  {"service_identity":"kex","service_endpoint":"kex.ucs-apps-
1.testoffice.ru:6788","error":"provided emails belong to different users","err-
location":"/home/admin-msk/kex/cmd/exch-to-mln-migrator/main.go:183"}
```

– Неверно указаны `impersonation_username` и `impersonation_password` в конфигурации мигратора:

```
2024-03-21T12:31:41.312  FTL  exch-to-mln-migrator/main.go:127  import calendars
and events  {"service_identity":"kex","service_endpoint":"kex.ucs-apps-
1.zulu.stageoffice.ru:6788","error":"import calendars: get calendars from
exchange: get deleted items folder: ews service: [GetFolder]: get folder with
ews: RoundTripWithAction: 401 Unauthorized: mexa error
[ErrorAccessDenied]","err-location":"gitlab.stageoffice.ru/!u!c!s-
!c!o!m!m!o!n/mexa@v0.26.5/soap/client.go:241"}
```

Пример конфигурационного файла приведен в приложении (см. раздел «Конфигурационный файл для миграции календаря из Microsoft Exchange в ПО «Mailion» в Приложении В).

7.18.2 Миграция данных календаря из ПО «Mailion» в Microsoft Exchange

Мигратор представляет собой отдельный исполняемый файл. Для запуска мигратора необходимо выполнить запрос:

```
./ucs-mln-to-exch-migrator \
-from user@user@installation.example.net \
-to user@user@ad.example.net \
-ignore-errors=true \
-from-time 2023-07-17T15:04:05Z \
-c /path/to/config.json
```

Описание параметров запроса приведено в таблице 137.

Таблица 137 – Параметры запроса на вызов мигратора

Параметр	Тип	Обязательный	Описание
from	Str	+	Почтовый адрес пользователя Microsoft Exchange, чьи календарные данные будут мигрировать. Пример записи пользователя в данном параметре для однодоменной делегации: user@ad.example.net. Пример записи пользователя в данном параметре для мультидоменной делегации: – пользователь Microsoft Exchange – user@ad.example.net; – пользователь ПО «Mailion» – user@installation.example.net
to	Str	+	Почтовый адрес пользователя, на который мигрируют календарные данные. Пример записи пользователя в данном параметре для однодоменной делегации: user@ad.example.net. Пример записи пользователя в данном параметре для мультидоменной делегации: – пользователь Microsoft Exchange – user@ad.example.net; – пользователь ПО «Mailion» – user@installation.example.net
ignore-errors	Bool	+	Значение по умолчанию **true**. Отвечает за продолжение работы мигратора в случае ошибок (ошибки попадают в журнал работы системы; пример записи в журнале работы системы приведен ниже). Если значение **false**, процесс миграции останавливается при первой ошибке

Параметр	Тип	Обязательный	Описание
from-time	Str	-	Параметр для указания даты, начиная с которой необходимо перенести события из календаря
to-time	Str	-	Параметр для указания даты, до которой необходимо перенести события из календаря
c	Str	+	Путь к файлу конфигурации (по умолчанию `internal/config/config.local.json`)

В а ж н о – Можно указать один параметр времени: **from-time** или **to-time**. Если указан только параметр **from-time**, то перенесутся все события, начиная с указанной даты, и за последующие пять лет. Если указан только параметр **to-time**, то перенесутся все события с начала до указанной даты.

Пример записи в журнале работы системы:

```
./ 2023-07-18T19: 56: 18.342+0200INFOexch-to-mln-migrator/main.go: 151{
  "migration": {
    "date": "2023-07-18 19:56:10.06591495 +0200 CEST m=+2.050583246",
    "mailion_email": "bdad1@installation.example.net",
    "exchange_email": "bdad1@ad.example.net",
    "errors": {
      "num_folders": 1,
      "folders": {
        "AmazingCal": [
          {
            "error": "send request: 1: import event
AAMkADdhOGQ1YThmLWE1NTUtNDZmMy04NmExLTc4YjgxMmIwNDk5ZABGAAAAAABOC/xo0g9rQr2266gF
2feqBwDBZPRHK3THT7Vxk0lMFP/sAAASj75BAADBZPRHK3THT7Vxk0lMFP/sAAASj8YVAAA="
          },
          {
            "error": "send request: 2: import event
AAMkADdhOGQ1YThmLWE1NTUtNDZmMy04NmExLTc4YjgxMmIwNDk5ZABGAAAAAABOC/xo0g9rQr2266gF
2feqBwDBZPRHK3THT7Vxk0lMFP/sAAASj75BAADBZPRHK3THT7Vxk0lMFP/sAAASj8YUAAA="
          },
          {
            "error": "send request: 3: import event
AAMkADdhOGQ1YThmLWE1NTUtNDZmMy04NmExLTc4YjgxMmIwNDk5ZABGAAAAAABOC/xo0g9rQr2266gF
2feqBwDBZPRHK3THT7Vxk0lMFP/sAAASj75BAADBZPRHK3THT7Vxk0lMFP/sAAASj8YTAAA="
          }
        ],

      }
    }
  },
  "current_status": {
    "exchange": {
      "folders": {
        "AmazingCal": {
          "num_objects": 3,
          "ews_id":
"AAMkADdhOGQ1YThmLWE1NTUtNDZmMy04NmExLTc4YjgxMmIwNDk5ZAAuAAAAAABOC/xo0g9rQr2266g
F2feqAQDBZPRHK3THT7Vxk0lMFP/sAAASj75BAAA="
        },
```

```
        "Дни рождения": {
          "num_objects": 0,
          "ews_id":
"AQMkADdhOGQ1YThmLWE1NQEtNDZmMy04NmExLTc4YjgxMmIwNDk5AGQALgAAA04L/GjSD2tCvbbrqAX
Z96oBAMFk9EcrdMdPtXGTSUwU/+wAAAIBTAAAAA=="
        },
        "Задачи": {
          "num_objects": 0,
          "ews_id":
"AQMkADdhOGQ1YThmLWE1NQEtNDZmMy04NmExLTc4YjgxMmIwNDk5AGQALgAAA04L/GjSD2tCvbbrqAX
Z96oBAMFk9EcrdMdPtXGTSUwU/+wAAAIBEgAAAA=="
        },
        "Календарь": {
          "num_objects": 4,
          "ews_id":
"AQMkADdhOGQ1YThmLWE1NQEtNDZmMy04NmExLTc4YjgxMmIwNDk5AGQALgAAA04L/GjSD2tCvbbrqAX
Z96oBAMFk9EcrdMdPtXGTSUwU/+wAAAIBDQAAAA=="
        }
      },
      "num_folders": 4
    },
    "mailion": {
      "folders": {
        "AmazingCal": {
          "num_objects": 3,
          "ews_id":
"AAMkADdhOGQ1YThmLWE1NTUtNDZmMy04NmExLTc4YjgxMmIwNDk5ZAAuAAAAAABOC/xo0g9rQr2266g
F2feqAQDBZPRHK3THT7Vxk0lMFP/sAAASj75BAAA="
        },
        "Дни рождения": {
          "num_objects": 0,
          "ews_id":
"AQMkADdhOGQ1YThmLWE1NQEtNDZmMy04NmExLTc4YjgxMmIwNDk5AGQALgAAA04L/GjSD2tCvbbrqAX
Z96oBAMFk9EcrdMdPtXGTSUwU/+wAAAIBTAAAAA=="
        },
        "Календарь": {
          "num_objects": 4
        }
      },
      "num_folders": 3
    }
  }
}
```


Пример конфигурационного файла приведен в приложении (см. раздел «Конфигурационный файл для миграции календаря из ПО «Mailion» в Microsoft Exchange» в Приложении В).

В а ж н о – Событие мигрирует только для организатора и в календарь, выбранный по умолчанию.

7.19 Синхронизация почты

Однодоменный режим синхронизации почты с Exchange на Mailion – это временный режим работы на период переноса пользователей из Exchange в Mailion. Он подразумевает одновременную работу двух сервисов на одном домене и позволяет пользователям работать как с одной, так и с другой почтовой системой. Так как режим является временным, он должен работать до тех пор, пока вся необходимая почта не будет перемещена из одной системы в другую.

Однодоменный режим обеспечивает:

– авторизацию в Mailion пользователей, которые изначально были заведены в AD, – пользователь должен быть создан в Mailion при попытке авторизоваться или же при получении нового письма для этого пользователя;
– получение пользователями доступа к входящей почте как из одной, так и из другой системы. Пользователь получает мгновенный доступ к новой почте, которая была получена после начала работы однодоменного режима, но старые письма должны появиться со временем. Поэтому сохраняется возможность доступа к старой системе;
– отправление почты из личных почтовых ящиков пользователей как из одной, так и из другой системы.

Для переключения в данный режим требуется выполнить следующие действия:

1. Создать **технический домен** и делегацию на Exchange.
2. Создать пользователей из AD в Mailion (опционально).

Для того чтобы обеспечить вышеописанную функциональность, были разработаны два дополнительных способа синхронизации почты.

В однодоменном режиме MX запись продолжает указывать на Exchange, а значит вся входящая почта приходит только туда. Поэтому для синхронизации новой почты в Mailion создается новый домен, который называется **техническим** и MX запись которого указывает уже на Mailion. Этот домен используется для получения входящей почты из Exchange по правилам перенаправления, которые появляются при создании пользователя в Mailion.

Подразумевается, что в момент миграции и работы Mailion в однодоменном режиме пользователи будут пользоваться именно им и новую почту отправлять из Mailion. Таким образом, новую почту нужно синхронизировать с Exchange. Это делается средствами postfix-милтеров. Милтер **zeus** получает исходящую почту и с помощью средств EWS API сохраняет письмо в Exchange. Необходимо сохранять письма, отправляемые как через веб-интерфейс, так и через сторонние клиенты (такие как Thunderbird). Поэтому postfix-милтер – это единственное место, где письмо можно перехватить и сохранить.

Для миграции всех ранее созданных писем был создан специальный мигратор. Он позволяет перенести почту, папки, контакты, правила, события календаря из Exchange в Mailion. Мигратор запускается для каждого пользователя в отдельности и позволяет перемещать всю почту одного пользователя за один раз.

Мигратор поддерживает частичный перенос данных:

– за определенный период (позволяет указать дату начала и/или дату окончания);
– только определенные папки (позволяет указать одну или несколько папок для переноса).

Примечание – При настройке однодоменного режима используется понятие **технического/secondary домена**. Этот домен используется для синхронизации входящей почты из Exchange и для работы однодоменного режима в формате **сосуществования** (в этом случае почтовые ящики синхронизируются в реальном времени). Технический домен автоматически фильтруется и пропадает из выдачи подсказок при поиске, из профилей пользователей, из списка пользователей в веб-интерфейсе администратора.

7.19.1 Настройка миграции почты

Важно – Для миграции данных необходимо использовать Microsoft Exchange версии 2010 и выше.

Для запуска миграции почты необходимо выполнить следующие действия:

1. Зайти на машину через SSH, например **ssh <username>@<host>**, где **<host>** – имя хоста из inventory, где расположен сервис viper.
2. Выполнить команду **docker exec -ti viper bash**.

3. Внутри контейнера с viper перейти в каталог **cd /usr/local/bin**. В каталоге **/usr/local/bin** находится утилита для миграции почты: ucs-mail-mln-exch-migrator (подробнее о запуске миграции почты из ПО «Mailion» в Microsoft Exchange см. 7.19.4).
4. Внутри контейнера viper перейти в каталог **/etc/ucs/viper**. В нем находится конфигурационный файл для миграции почты: **/etc/ucs/viper/mail_exch_mln_migrator.json**.

Важно – **Выполнение миграции вместе с включенной синхронизацией невозможно. Перед началом миграции необходимо отключить синхронизацию.** Примеры команд для отключения синхронизации приведены ниже.

Пример команды отключения синхронизации для домена:

```
nct_ministerium update_domain \
--config ministerium.json
--id= <...>
--features.is_mail=true \
--features.is_authorization=true \
--features.is_service=true \
--external.is_sync_enabled=false \
```

Описание параметров отключения синхронизации для домена приведено в таблице 138.

Таблица 138 – Параметры отключения синхронизации для домена

Параметр	Тип	Обязательный	Описание
config	Str	+	Путь к файлу конфигурации
id	Str	+	Идентификатор домена
features.is_mail	Bool	+	Если значение **true**, домен может принимать почтовые сообщения
features.is_authorization	Bool	+	Если значение **true**, домен можно использовать для авторизации
features.is_service	Bool	+	Если значение **true**, домен можно использовать для авторизации по умолчанию
external.is_sync_ enabled	Bool	+	Включение/отключение синхронизации. Если значение **false**, то выключена. Если значение **true**, то включена

Пример ответа:

```
{
  "changed": true,
  "failed": false,
  "msg": "ok"
}
```

Пример команды отключения синхронизации для конкретного пользователя:

```
nct_ministerium set_sync_block_setting_for_user \
--config <путь до конфигурационного файла>
--login <...>
--setBlock=true \
--enableImmidiately=false
```

Описание параметров отключения синхронизации для конкретного пользователя приведено в таблице 139.

Таблица 139 – Параметры отключения синхронизации для конкретного пользователя

Параметр	Тип	Обязательный	Описание
config	Str	+	Путь до конфигурационного файла
login	Str	+	Логин пользователя
setBlock	Bool	+	Установка блокировки синхронизации (для тенанта или пользователя). Если значение **true**, то заблокирована, **false** – разблокирована
enableImmidiately	Bool	+	Снять/проставить галочки в настройках. Если значение **false**, то галочки сняты, **true** – галочки установлены

Пример ответа:

```
{
  "Response": {
    "changed": true,
    "failed": false,
    "msg": "ok"
  },
  "changed_entity_id": "ид измененного пользователя"
}
```

Пример команды отключения синхронизации для тенанта:

```
nct_ministerium set_sync_block_setting_for_all_users_in_tenant \
--config <путь до конфигурационного файла>
--tenantId <...>
--setBlock=true \
--enableImmidiately=false \
```

Описание параметров отключения синхронизации для тенанта приведено в таблице 140.

Таблица 140 – Параметры отключения синхронизации для тенанта

Параметр	Тип	Обязательный	Описание
config	Str	+	Путь до конфигурационного файла
login	Str	+	Логин пользователя
tenantId	Str	+	Идентификатор тенанта
enableImmidiately	Bool	+	Снять/проставить галочки в настройках. Если значение **false**, то галочки сняты, **true** – галочки установлены

Пример ответа:

```
{
  "changed": true,
  "failed": false,
  "msg": "ok"
}
```

7.19.2 Миграция данных почты из Microsoft Exchange в ПО «Mailion»

Мигратор представляет собой отдельный исполняемый файл. Для вызова мигратора необходимо выполнить запрос:

```
./ ucs-mail-exch-mln-migrator
-c mail_exch_mln_migrator.json
-from userexch1@installation.example.net
-to usermln2@installation.example.net
-direction to-mln
```

Описание параметров запроса приведено в таблице 141.

Таблица 141 – Описание параметров запроса на вызов мигратора

Параметр	Тип	Обязательный	Описание
from	Str	+	Почтовый адрес (mailbox name) пользователя Microsoft Exchange, чьи почтовые данные будут мигрировать
to	Str	+	Почтовый адрес (mailbox name) пользователя Mailion, на который мигрируют данные почты
c	Str	+	Путь к конфигурационному файлу (по умолчанию `internal/config/config.local.json`)
direction	Str	+	Направление миграции может быть либо `to-ex` либо `to-mln`, в случае миграции из Microsoft Exchange в ПО «Mailion» указывать `to-mln`

Параметр	Тип	Обязательный	Описание
start		-	Параметр для указания даты, начиная **с** которой необходимо перенести письма. Формат: 2006-01-02
end		-	Параметр для указания даты, **до** которой необходимо перенести письма. Формат: 2006-01-02
use-sync-state	Bool		Параметр для создания файла `.sync-state`, который хранит состояние мигрируемых данных. По умолчанию состояние **true**. Пример: при повторной миграции почтовых данных мигратор не будет дублировать мигрируемые объекты, так как в файле `.sync-state` хранятся те данные, которые успешно мигрировали и находятся в Mailion

Особенности миграции:

– если указан хотя бы один из параметров **start** и **end**, то миграция будет происходит относительно этой даты;

– если параметры **start** и **end** не указаны, то в месте, откуда запускается мигратор, появится файл `.sync-state`, в котором будут сохраняться данные, позволяющие при перезапуске продолжить миграцию с момента остановки ранее запущенной миграции. Это работает только в случае, если мигратор запускается без указания дат;

– параметры **start** и **end** относятся только к письмам, миграция правил и подписей будет осуществлена за все время вне зависимости от указания дат.

Пример конфигурационного файла приведен в приложении (см. раздел «Конфигурационный файл для миграции почты из Microsoft Exchange в ПО «Mailion», из ПО «Mailion» в Microsoft Exchange» в Приложении В).

П р и м е ч а н и е – При миграции данных почты из Microsoft Exchange в ПО «Mailion» также происходит миграция всех созданных пользователем текстовых подписей и почтовых правил.

7.19.3 Поддерживаемые правила при миграции данных почты

При миграции данных почты из Microsoft Exchange в ПО «Mailion» поддерживается перенос правил (фильтров) со следующими условиями:

– получено в течение указанного периода;

– моего имени нет в поле «Кому»;
– мое имя присутствует в поле «Копия»;
– мое имя содержится в поле «Кому»;
– в списке получателей указано только мое имя;
– мое имя присутствует в строке «Кому» или «Копия»;
– адрес получателя содержит эти слова»;
– адрес отправителя содержит»;
– тема содержит эти слова»;
– получатель ...;
– получено от ...;
– с вложением.

При миграции данных почты из Microsoft Exchange в ПО «Mailion» поддерживается перенос правил со следующими действиями:

– пометить сообщение как прочтенное;
– перенаправлять сообщения;
– пересылать сообщения;
– пометить как нежелательное;
– удалять сообщение;
– перемещать сообщения в папку.

При миграции присутствуют следующие ограничения:

1. Если почтовое правило было изменено в Microsoft Exchange, то при повторной миграции данных почты из Microsoft Exchange правило не изменится в ПО «Mailion».
2. В ПО «Mailion» отсутствует:
   – поддержка исключения из правил;
   – условие «Для всех входящих»;
   – действие «Применить ко всем сообщениям», но есть функционал применения правила к папке;
   – классификация сообщений: тип, категория, конфиденциальность, флаг;
   – поддержка нескольких уровней важности: у сообщений в ПО «Mailion» один уровень важности, а в Microsoft Exchange три (в веб-интерфейсе ПО «Mailion» три уровня важности, но в сервисе этот параметр имеет тип **bool**);

– функционал голосовых сообщений.
– функционал отправки SMS-сообщений.

7.19.4 Миграция данных почты из ПО «Mailion» в Microsoft Exchange

Мигратор представляет собой отдельный исполняемый файл. Для запуска мигратора необходимо выполнить запрос:

```
./ ucs-mail-mln-exch-migrator \
-c mail_exch_mln_migrator.json \
-from usermln1@installation.example.net \ и куда он будет стыковаться
-to userexch1@installation.example.net \
-use-sync-state=false \
-folders "folder" \
-direction to-ex
```

При запуске миграции создается файл `.sync-state`. Он содержит сведения, необходимые для продолжения миграции с того момента, на котором она закончилась в предыдущий раз. Данный файл создается в папке, в которой производится запуск миграции. Чтобы начать миграцию с самого начала, можно удалить `.sync-state`, либо использовать флаг `-use-sync-state=false`, который позволит игнорировать данный файл. Несмотря на наличие флага, файл синхронизации будет создаваться в любом случае.

При использовании временного периода, который задается параметрами `from` и `to`, миграция в любом случае запустится с самого начала.

Описание параметров запроса приведено в таблице 142.

Таблица 142 – Описание параметров запроса на вызов мигратора

Параметр	Тип	Обязательный	Описание
from	Str	+	Почтовый адрес (mailbox name) пользователя ПО «Mailion», чьи почтовые данные будут мигрировать
to	Str	+	Почтовый адрес (mailbox name) пользователя Microsoft Exchange, на почтовый ящик которого мигрируют данные почты
c	Str	+	Путь к конфигурационному файлу (по умолчанию `internal/config/config.local.json`)
use-sync-state	Bool	+	Отключение синхронизации во время миграции, обязательный параметр, значение `false`
folders	Str	-	Список папок

Параметр	Тип	Обязательный	Описание
direction	Str	+	Направление миграции может быть либо `to-ex` либо `to-mln`, в случае миграции в Microsoft Exchange из ПО «Mailion» указывать `to-ex`
ignore-errors	Bool	-	Значение по умолчанию **true**. Отвечает за продолжение работы мигратора в случае ошибок (ошибки попадают в журнал работы системы. Пример записи в журнале работы системы приведен ниже). Если значение **false**, процесс миграции останавливается при первой ошибке

Пример отчета о завершении миграции почты:

```
{
    "Migration": {
        "trace-id": string, (trace id миграции, чтобы можно было посмотреть
логи) +
        "date": "2024-03-13 18:39:41.496800048 +0300 MSK m=+6.098483637", (дата,
когда был запущен мигратор)
        "migration_progress": int, (Процент смигрированных писем)
((all_synced_objects + all_already_synced_objects)/all_objects_in_exchange)
        "migration_mode": { (Режим запуска мигратора) +
            "type": "all"/"period", (За все время/За определенный период
времени)
            "date_start": "DD.MM.YYYY HH:MM:SS", (Опционально - если выбран тип
"period")
            "date_end": "DD.MM.YYYY HH:MM:SS" (Опционально - если выбран тип
"period")
            },
        "mailion_email": "test_user@se.stageoffice.ru",
        "exchange_email": "test_user@ad.stageoffice.ru",
        "mails": { (Примечание: в случае миграции за все время выводится общее
количество писем в Exchange, в случае за период - столько, сколько
смигрировалось) +
            "all_objects_in_exchange": 74, (TO-BE: Все письма в указанном
периоде)
            "all_object_in_mailion_before_migration": 53, (Количество писем ДО
миграции в ящике Mailion)
            "all_synced_objects": 0, (То, что синхронизировалось при актуальном
запуске)
            "all_already_synced_objects": 49, (Все письма, смигрированные за
период. Примечание: данное поле возникает при повторной миграции при условии,
что уже были смигрированы какие-то объекты)
            "all_errors_count": 25 (exchange = errors? + all_synced +
already_synced)
            },
        "signatures": {
            "all_objects_in_exchange": 10, (Все подписи, которые есть в
Exchange)
            "all_object_in_mailion_before_migration": 3, (Подписи, которые есть
в Mailion ДО миграции)
            "all_synced_objects": 7, (То, что синхронизировалось при актуальном
запуске)
            "all_already_synced_objects": 0, (Все подписи, смигрированные за
период. Примечание: данное поле возникает при повторной миграции при условии,
что уже были смигрированы какие-то объекты)
```

```
            "all_errors_count": 25 (exchange = errors? + all_synced +
already_synced)
        },
        "rules": {
            "all": 6, (Все почтовые правила, которые есть в Exchange)
            "successfully_created": 5, (Почтовые правила в Mailion после
миграции)
            "already_existed": 1, (Правила, которые уже есть в Mailion)
            "failed": 1, (Не мигрировавшие правила)
            "failed_rules": 25 [ {
                "ID": "RRYAABoyu7A=", (Идентификатор правила)
                "Name": "Тест", (Наименование правила)
                "ErrorMessage": "fill with conditions: rule have a not
implemented conditions: [WithinSizeRange]" (Сообщение об ошибке)
            } ]
        }
    },
    "signatures": {

        }
   "folders": {
        "AAMkADkwYjc4Zjg/ONrAQBBGa9SxwTHSqrp6ZgSQNeHAAAAAAEJAAA=": {
            "exchange-folder-path": "Отправленные",
            "mln-folder-path": "Sent",
            "objects-in-exchange": 24,
            "object-in-mailion-before": 27,
            "synced-objects": 0,
            "already-synced": 25,
            "was-created": false,
            "errors": [{
                "message-id":
"AAMkADkwYjc4ZjgzLWYwNwTHSqrp6ZgSQNeHAABkNwIeAAA=",
                "subject": "lol 20",
                "from": "andrey.smirnov@testoffice.ru",
                "created": "2024-03-05T14:13:22Z",
                "error": "some error"
            }, {
                "message-id":"AAMkADAEJAABBGa9SxwTHSqrp6ZgSQNeHAABkNwIdAAA=",
                "subject": "qq",
                "from": "test_user@ad.stageoffice.ru",
                "created": "2024-03-05T13:49:49Z",
                "error": "some error"
            },
            ...
            {
                "message-id": "AAMkADkwYjc4ZjgzLWYwNeHAAA2TxkCAAA=",
                "subject": "lol",
                "from": "test_user@ad.stageoffice.ru",
                "to": ["test_user@ad.stageoffice.ru"],
                "created": "2023-11-17T06:41:10Z",
                "error": "exchange-message-id=[AAMkTxkCAAA=] internet-message-
id=[\u003ce11eeac67e@ad.stageoffice.ru\u003e] message-size=[5.0 kB] from-
email=[sergey.smirnov@testoffice.ru] to-emails=[sergey.smirnov@testoffice.ru]
subject=[lol] created=[2023-11-17T06:41:10Z]: add tag for existing mail:
common.Error(module:MARKER code:6009 msg:\"list of objects must not be empty\")"
            }]
        },
        "AAMkADkwYjc4ZnmgSbNAXTjP=": {
            "exchange-folder-path": "Удаленные",
            "mln-folder-path": "",
```

```
            "objects-in-exchange": 23,
            "object-in-mailion-before": 0,
            "synced-objects": 0,
            "already-synced": 0,
            "was-created": false,
            "errors": [{
                "error": "folder should not be synced"
            }]
        },
        "AAMkADkwYjc4ZAAAAAELAAA=": {
            "exchange-folder-path": "Исходящие",
            "mln-folder-path": "",
            "objects-in-exchange": 0,
            "object-in-mailion-before": 0,
            "synced-objects": 0,
            "already-synced": 0,
            "was-created": false,
            "errors": []
        }
        ...
}
```


Примеры ошибок при миграции почты:

– Сервис не смог выполнить логаут (миграция больше 5 минут), уровень ERROR:


```
2024-01-12T13:47:11.109  ERR
ru_stageoffice_gitlab_ucs_common_auth_v2/authenticate_service.go:52  logout
{"service":"viper","error":"delete session: common.Error(module:MINOS code:2002
msg:\"INVALID_TOKEN\")","err-
location"
:"external/ru_stageoffice_gitlab_ucs_common_auth_v2/authenticate.go:191"}
```


– Ошибка с тайм-аутом (попытка мигрировать письмо с вложением больше 5 Мб), уровень ERROR:


```
2024-02-16T21:32:02.321  ERR  viper_client/retry.go:49  Retry send after error
{"error":"EOF","attempt":1}
2024-02-16T21:32:02.322  ERR  viper_client/retry.go:49  Retry send after error
{"error":"EOF","attempt":2}
2024-02-16T21:32:02.323  ERR  viper_client/retry.go:49  Retry send after error
{"error":"EOF","attempt":3}
2024-02-16T21:32:03.323  ERR  viper_client/retry.go:49  Retry send after error
{"error":"EOF","attempt":4}
2024-02-16T21:32:04.323  ERR  viper_client/retry.go:49  Retry send after error
{"error":"EOF","attempt":5}
2024-02-16T21:32:05.324  ERR  migrator/migrator.go:1473  failed to save message
in viper  {"direction":"from-Exchange", ......,"to-mln-
user":"test_user@exlab.su"}
```


– Не переливаются письма за определенный период, уровень ERROR:


```
2023-12-15T16:50:58.627+0300    ERROR   xyncmodel/model_sync_me.go:106  xync
user data  {"service_identity": "viper", "service_endpoint": "viper.ucs-apps-
1.zulu.stageoffice.ru:8181", "grpc.service": "xync.v1.Xync", "grpc.method":
"SyncMe", "session-id": "742d7d20-be65-5ba0-b676-1e5a3b778713", "client-request-
id": "751fbd8d-7d92-4459-b11f-efeed4f34fef.846d661f-cb06-4ad4-803c-
```

```
0e3f54094b8d", "user-ip": "10.80.52.41", "actor-id": "5c903909-1eed-48c4-9578-
4253ce978c62", "trace-request-id": "7cde88b73715202e", "span-request-id":
["459c367aeaec3ba7"], "victim-id": ["5c903909-1eed-48c4-9578-4253ce978c62"],
"user-id": "5c903909-1eed-48c4-9578-4253ce978c62", "error": "sync data for user:
sync exchange folder
'AAMkAGU4YTU2MTZiLWYzNTgtNDQxNS1hNDM2LTQ5NjA1OGEyOTZhMgAuAAAAAAAQdAGHFbdWToIhSIU
lCp1dAQDyjrLB3AdZR4E776IDUsu+AAAAZXsoAAA=' to marker tag (ID=3f142c45-b313-45a7-
8448-62429e702847, RegionID=2dbacea3-5889-4021-8f38-bc2214dd7423): runtime
error: invalid memory address or nil pointer dereference", "err-location":
"xyncer/xyncer_imp.go:350"}
```


– Включена синхронизация писем, уровень FATAL:


```
2023-08-15T09:17:30.719+0300 fatal ucs-mail-mln-exch-migrator/main.go:148 failed
to migrate {"from-ad-user": "test_user@ad.stageoffice.ru", "to-mln-user":
"test_user@se.stageoffice.ru", "error": "check is sync enabled: mail
synchronization is enabled; event synchronization is enabled", "err-location":
"gitlab.stageoffice.ru/UCS-PLATFORM/viper/cmd/ucs-mail-mln-exch-
migrator/migrator/migrator.go:286"}
```


– Сервис Hog недоступен:


```
"error":"get user data and user settings: get hog user settings: get settings:
common.Error(module:HOG code:1000 msg:\"get user info: wrapping nil error\")
```


Пример конфигурационного файла приведен в приложении (см. раздел «Конфигурационный файл для миграции почты из Microsoft Exchange в ПО «Mailion», из ПО «Mailion» в Microsoft Exchange» в Приложении В).

7.19.5 Возможная проблема с миграцией почты

После перехода Mailion на более безопасный способ запуска контейнеров от имени обычного (не root) пользователя возникла проблема с миграцией: она останавливается после 100 писем (по умолчанию) и завершается ошибкой, содержащей `wrapping nil error`.

Данная ошибка связана с файлом `.sync-state`, который мигратор пытается создать в корневой директории от имени обычного пользователя.

Чтобы исправить эту проблему, необходимо:

1. Если мигратор запускается из docker-контейнера, то следует изменить команду запуска, в качестве параметра указав рабочую папку, доступную для записи не-root пользователю.

   Пример для папки `/tmp`:

   ```
   docker run \
        ... \
   ```

```
-w /tmp \
... \
hub/viper:latest /usr/loca/bin/ucs-mail-mln-exch-migrator \
  -c /etc/ucs/viper/mail_exch_mln_migrator.json \
  -from $(mln_login) \
  ...
```

2. Если мигратор запускается как отдельный бинарный файл, то необходимо убедиться, что у пользователя, от имени которого производится запуск, достаточно прав на запись в каталог, из которого запускается мигратор.

7.19.6 Автоматическое создание учетной записи по первому письму

Функционал автоматического создания учетной записи по первому письму по умолчанию выключен. В случае необходимости его можно включить в конфигурационном файле сервисов Zeus и Paranoid, поменяв значение соответствующих параметров на **true**.

Zeus:

```
register_external_users=true
```

Paranoid:

```
create_mailion_users_for_mail_recipients=true
```

7.19.7 Автоматическое создание правила перенаправления писем

Функционал автоматического создания правила перенаправления по умолчанию выключен в пользу настройки перенаправления со стороны Exchange. В случае необходимости его можно включить в конфигурационном файле сервиса Hog, поменяв значение параметра `hog_use_redirect_rules` на **true**.

```
hog_use_redirect_rules=true
```

7.19.8 Настройка перенаправления писем со стороны Exchange

1. Настройка правила перенаправления писем с помощью Exchange Management Shell

Для настройки правил перенаправления через Exchange Management Shell (EMS) используется командлет `Set-Mailbox`. Данный командлет следует применять только для одного почтового ящика.

В данном примере настройки правила перенаправления электронная почта доставляется в почтовый ящик пользователя `Test User`, кроме того, все отправленные пользователю `Test User` сообщения пересылаются на указанный внешний адрес электронной почты.

```
Set-Mailbox -Identity "Test User" -DeliverToMailboxAndForward $true -
ForwardingSMTPAddress "testuser@se.stageoffice.ru"
```

Примечание – При установке для параметра `-DeliverToMailboxAndForward` значения `$false` сообщения будут перенаправляться только на указанный адрес. Чтобы отключить это правило, нужно указать: `-DeliverToMailboxAndForward $false -ForwardingSMTPAddress $null`. Для параметра `-ForwardingSMTPAddress` указывается почтовый ящик с техническим доменом.

В данном примере настройки правила перенаправления все сообщения электронной почты, отправленные в почтовый ящик `Test User` сотрудника `Test Company`, пересылаются одному из его коллег:

```
Set-Mailbox -Identity "Test User" -ForwardingAddress "mrtest@ad.stageoffice.com"
```

Для проверки существования правила перенаправления необходимо выполнить следующую команду:

```
Get-Mailbox "Test User" | Format-List
testuser@testdomain.com,DeliverToMailboxandForward
```

2. **Настройка правила перенаправления писем в Центре администрирования Exchange**

В центре администрирования Exchange перейти в раздел **Почтовые ящики получателей** (см. Рисунок 81).

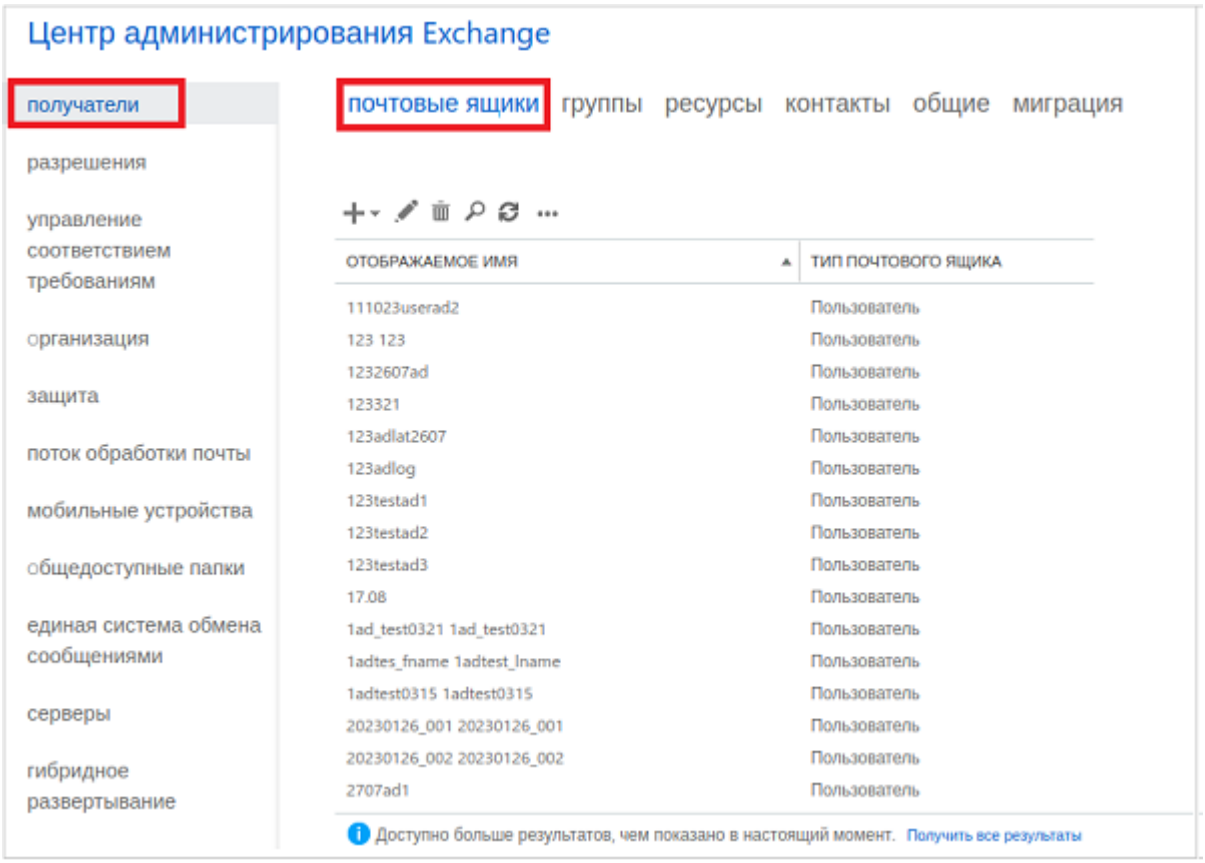


Рисунок 81 – Центр администрирования Exchange

В списке почтовых ящиков пользователей открыть почтовый ящик, для которого требуется настроить перенаправление почты.

В открывшемся окне перейти в раздел **Функции почтового ящика > Поток обработки почты > Просмотреть сведения** (см. Рисунок 82).

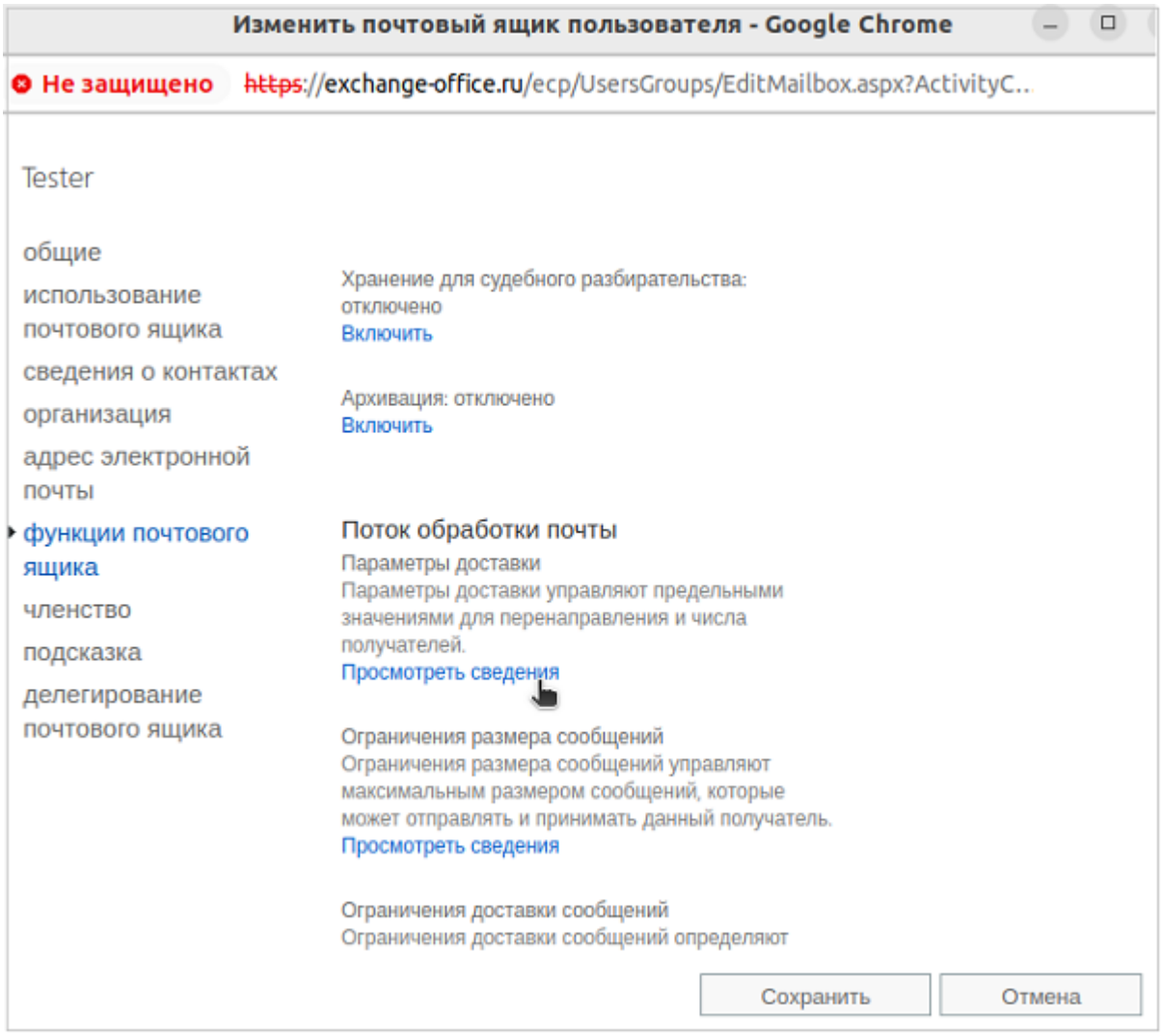


Рисунок 82 – Свойства почтового ящика пользователя

Установить флажок **Включить перенаправление**, ввести получателя с почтовым ящиком Exchange / выбрать получателя, нажав на кнопку **Обзор**, и нажать **ОК** (см. Рисунок 83).

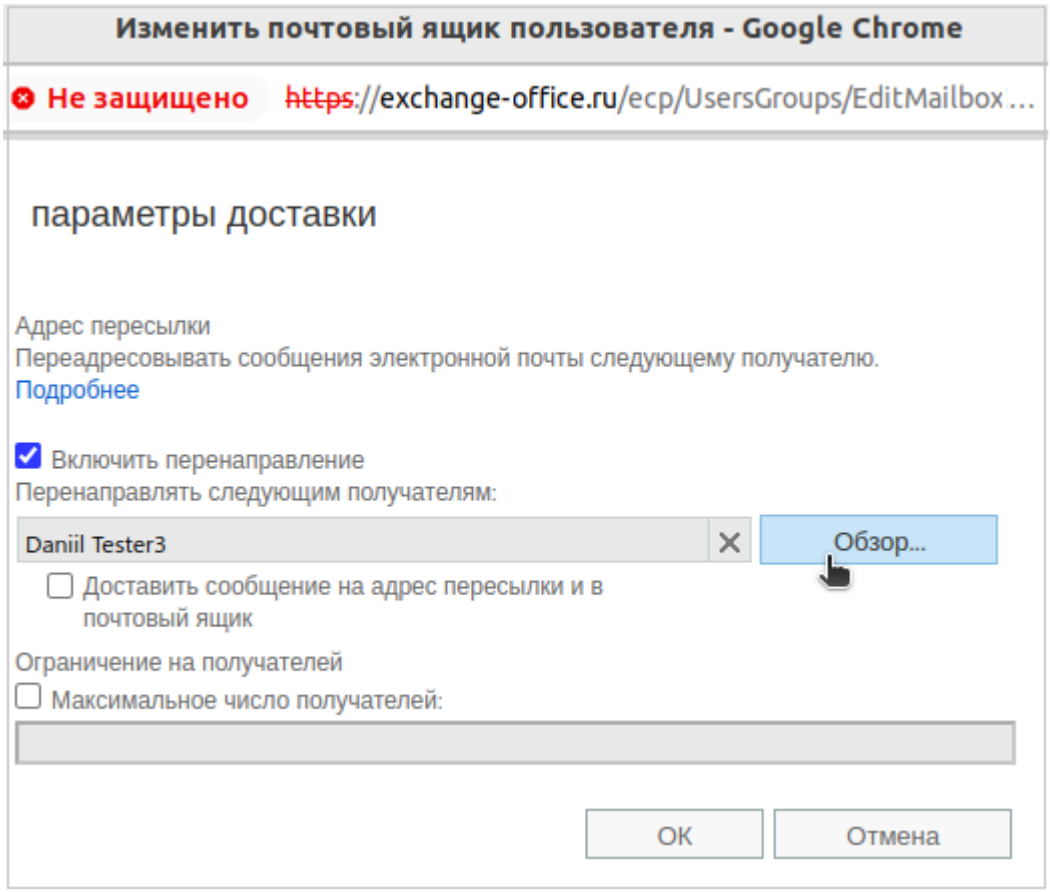


Рисунок 83 – Параметры доставки сообщений

В а ж н о – Через Центр администрирования Exchange можно настроить правило перенаправления только для пользователей, имеющих почтовый ящик в организации Exchange. Для создания правила перенаправления почты на адрес электронной почты за пределами Exchange следует использовать командную консоль EMS.

П р и м е ч а н и е – Перенаправление для группы пользователей включается только в момент миграции почтовых ящиков этих пользователей в Mailion. Не рекомендуется включать перенаправление для пользователей, которые еще не заведены в Mailion.

7.19.9 Перенаправление автоответа

Перенаправление автоответа, уведомлений о прочтении/доставке, уведомлений от ресурсов из Exchange в Mailion требует настройки со стороны Exchange:

- Все AD-пользователи были созданы через команду **ministerium** `create_delegated_users`, правила перенаправления созданы с помощью командлета `Set-Mailbox` (через Exchange Management Shell).
- С помощью командлета `Set-RemoteDomain` значение параметра `-AllowedOOFType` технического домена было изменено на `InternalLegacy`. Это необходимо для того, чтобы сообщения автоответа перенаправлялись в Mailion.

В а ж н о – Ограничения: если учетная запись, для которой требуется включить автоответ, уже перенесена в Mailion и настроено перенаправление (см. раздел 7.19.8), то автоответ необходимо настраивать только в Mailion; для Microsoft Exchange 2010 разработчиком заявлено известное ограничение – при настроенном перенаправлении функционал автоовета не поддерживается.

7.20 Миграция внешних пользователей

Для создания пользователя из внешнего каталога используется команда **create_delegated_users**.

Пример команды создания пользователя из внешнего каталога:

```
nct_ministerium create_delegated_users \
--config "...config/ministerium.json" \
--emails external.user@external_catalog.su \
--force_remove_outlook_rule_blob=true \
--enable_sync=true \
--v
```

Описание параметров запроса приведено в таблице 143.

Таблица 143 – Описание параметров запроса на вызов мигратора

Параметр	Тип	Обязательный	Описание
config	Str	+	Путь к файлу конфигурации

Параметр	Тип	Обязательный	Описание
emails	Str	+	Почтовые адреса внешних пользователей (перечисляются через запятую)
force_remove_outlook_rule_blob	Bool	+	Флаг удаления объекта правил MS Outlook: – **true** – все отключенные правила MS Outlook будут удалены; – **false** – метод **adonis.CreateDelegatedUsers** вернет ошибку OUTLOOK_RULE_EXISTS
enable_sync	Bool	+	Флаг включения синхронизации почты и календаря. Значение по умолчанию – **false**

Пример ответа:

```
{
  "Response": {
    "changed": false,
    "failed": false,
  },
  "succeed": [
    {
      "emails": [
        "external.user@external_catalog.su",
        "external.user@eycp_external_catalog.su"
      ],
      "login": "external.user@external_catalog.su",
      "entityId": "b2890986-92b4-42bc-847f-5e16e8a49695"
    }
  ],
  "failed": []
}
```

7.21 Миграция идентификаторов из внешних каталогов

Для миграции уникального идентификатора для делегированных пользователей из внешних каталогов необходимо:

1. Запустить ansible playbook с командой `update_tenant` и дополнительными переменными:

```
ansible-playbook playbooks/mailion/external_id_migration.yml \
     -e "external_command=update_tenant" \
     -e "tenant_admin_login=USR" \
     -e "tenant_admin_pass=PASS" \
     -e "tenant_admin_id=TENANT_ID"
```

Команда `update_tenant` обновляет внешний идентификатор для всех делегированных пользователей, которые однозначно соотносятся с учетной записью внешнего каталога.

В результате выполнения команды формируется отчет вида: `report_{date}.txt`.

В отчете могут присутствовать следующие разделы:

- `multiple ldap correlation` – один пользователь Mailion может быть соотнесен с несколькими пользователями из внешнего каталога;
- `no ldap correlation` – для пользователя Mailion не найдено ни одного соотносящегося пользователя из внешнего каталога;
- `no extended domain` – по доменной части пользователя Mailion не находится ни одной делегации в доменах тенанта;
- `multiple users on one ldap relation` – более одного пользователя Mailion возможно соотнести с одним пользователем из внешнего каталога;
- `successfully synced` – успешно синхронизированные пользователи;
- `unspecified delegate ID. Please add to config` – делегация найдена, но ее параметры не добавлены в конфигурацию мигратора;
- `multiple delegations found for one login` – один пользователь Mailion может быть соотнесен с пользователями из различных внешних каталогов;
- `users on db update error` – пользователь должен был быть обновлен, но произошла ошибка записи в базу данных.

2. Запустить ansible playbook с командой `update_users_external_id` и дополнительными переменными:

```
ansible-playbook playbooks/mailion/external_id_migration.yml \
    -e "external_command=update_users_external_id" \
    -e "tenant_admin_login=USR" \
    -e "tenant_admin_pass=PASS" \
    -e "tenant_admin_id=TENANT_ID" \
    -e "external_user_login=USER_LOGINS"
```

Команда `update_users_external_id` позволяет разрешить некоторые конфликты синхронизации идентификаторов и выполнить миграцию для определенного пользователя или списка пользователей. Для того чтобы синхронизировать определенного пользователя или пользователя, который не может быть синхронизирован через `update_tenant`, необходимо учесть следующие условия:

1. Необходимо, чтобы у пользователя в Mailion был логин, в котором правая часть соотносится с делегированным доменом, а по его левой части может быть найден только один пользователь во внешнем каталоге согласно строке поиска в конфигурации. При отсутствии такого логина его необходимо создать, а левую часть рекомендуется выбрать согласно маппингу атрибута на поле "`login`".
2. Если для пользователя Mailion соотносится несколько пользователей одного внешнего каталога, то такой пользователь может быть синхронизирован только с изменением поисковой строки в конфиге, чтобы находился именно он.
3. Если для пользователя Mailion соотносится несколько пользователей различных внешних каталогов (что является редким случаем), то для синхронизации стоит удалить все его логины и создать логин согласно описанию выше для команды `update_users_external_id`.

7.22 Управление делегированием учетных записей

В а ж н о – Управление доступом к почте пользователя выполняется пользователем с ролью администратора тенанта.

Предоставление доступа к почте пользователя может быть выполнено с разными уровнями доступа. Доступ к почте задается с помощью параметра **permissions_by_emails**, при этом существует три уровня доступа:

- 0 – уровень доступа с правами «Не разрешено» (Cannot). Пользователь, которому предоставлены права доступа к почте, получает права совладельца на все почтовые папки, календари и адресные книги, но не может писать письма от имени делегированной учетной записи.
- 1 – уровень доступа с правами «От имени» (OnBehalf). Пользователь, которому предоставлены права доступа к почте, получает права совладельца на все почтовые

папки, календари и адресные книги, также он может отправлять письма от имени делегированной учетной записи, но со своей учетной записи.

– 2 – уровень доступа с правами «Напрямую» (SendAs). Пользователь, которому предоставлены права доступа к почте, получает права совладельца на все почтовые папки, календари и адресные книги, также он может отправлять письма от имени делегированной учетной записи.

7.22.1 Предоставление доступа к почте пользователя с правами «Не разрешено»

Для предоставления доступа к почте пользователя с правами «Не разрешено» необходимо выполнить запрос:

```
nct_ministerium set_shared_access \
--admin.login <…>
--admin.password <…>
--cox.balancer_endpoint=hydra.ucs-apps-1.installation.example.net:50053 \
--cox.compression=none \
--cox.endpoint=grpc-installation.example.net:3142 \
--cox.load_balanced=false \
--cox.request_timeout=10s \
--cox.service_name=cox \
--cox.use_tls=true \
--cox.use_tls_balancer=false \
--delegate_email user1@example.net\
--emails user2@example.net\
--permissions_by_emails 0 \
--tls_settings.ca_file ca.pem \
--tls_settings.client_cert_file client_cert.pem \
--tls_settings.key_file client_key.pem
```

Описание параметров запроса приведено в таблице 144.

Таблица 144 – Описание параметров запроса на доступ к почте пользователя с правами «Не разрешено» (Cannot)

Параметр	Тип	Обязательный	Описание
admin.login	Str	+	Логин администратора тенанта
admin.password	Str	+	Пароль администратора тенанта
cox.balancer_endpoint	Str	+	Endpoint балансировщика нагрузки сервиса
cox.compression	Str	+	Метод сжатия данных (варианты: **none**, **gzip**), по умолчанию **none**
cox.endpoint	Str	+	Endpoint сервиса
cox.load_balanced	Bool	+	Балансировщик нагрузки сервиса
cox.request_timeout	Str	+	Тайм-аут запроса к сервису

Параметр	Тип	Обязательный	Описание
cox.service_name	Str	+	Имя сервиса
cox.use_tls	Bool	+	TLS-сертификат
cox.use_tls_balancer	Bool	+	Защищенная передача данных при подключении к балансировщику
delegate_email	Str	+	Учетная запись, которую необходимо делегировать пользователю
emails	Str	+	Учетная запись пользователя, которому делегируют
permissions_by_emails	Str	+	Разрешения для политики отправки почты для настройки доступа к почте: 0 – разрешение «Не разрешено» (Cannot), 1 – разрешение «От имени» (OnBehalf), 2 – разрешение «Напрямую» (SendAs)
tls_settings.ca_file	Str	+	Путь к CA файлу
tls_settings.client_cert_file	Str	+	Путь к файлу сертификата клиента
tls_settings.key_file	Str	+	Путь к файлу с ключом клиента

Пример ответа:

```
{
  "Response": {
    "changed": true,
    "failed": false,
    "msg": "ok"
  }
}
```

7.22.2 Предоставление доступа к почте пользователя с правами «От имени»

Для предоставления доступа к почте пользователя с правами «От имени» (с сохранением реального отправителя) необходимо выполнить запрос:

```
nct_ministerium set_shared_access \
--admin.login <…>
--admin.password <…>
--cox.balancer_endpoint=hydra.ucs-apps-1.installation.example.net:50053 \
--cox.compression=none \
--cox.endpoint=grpc-installation.example.net:3142 \
--cox.load_balanced=false \
--cox.request_timeout=10s \
--cox.service_name=cox \
--cox.use_tls=true \
--cox.use_tls_balancer=false \
```

```
--delegate_email user1@example.net\
--emails user2@example.net\
--permissions_by_emails 1 \
--tls_settings.ca_file ca.pem \
--tls_settings.client_cert_file client_cert.pem \
--tls_settings.key_file client_key.pem
```

Описание параметров запроса приведено в таблице 145.

Таблица 145 – Описание параметров запроса на доступ к почте пользователя с правами «От имени» (OnBehalf)

Параметр	Тип	Обязательный	Описание
admin.login	Str	+	Логин администратора тенанта
admin.password	Str	+	Пароль администратора тенанта
cox.balancer_endpoint	Str	+	Endpoint балансировщика нагрузки сервиса
cox.compression	Str	+	Метод сжатия данных (варианты: **none**, **gzip**), по умолчанию **none**
cox.endpoint	Str	+	Endpoint сервиса
cox.load_balanced	Bool	+	Балансировщик нагрузки сервиса
cox.request_timeout	Str	+	Тайм-аут запроса к сервису
cox.service_name	Str	+	Имя сервиса
cox.use_tls	Bool	+	TLS-сертификат
cox.use_tls_balancer	Bool	+	Защищенная передача данных при подключении к балансировщику
delegate_email	Str	+	Учетная запись, которую необходимо делегировать пользователю
emails	Str	+	Учетная запись пользователя, которому делегируют
permissions_by_emails	Str	+	Разрешения для политики отправки почты для настройки доступа к почте: 0 – разрешение «Не разрешено» (Cannot), 1 – разрешение «От имени» (OnBehalf), 2 – разрешение «Напрямую» (SendAs)
tls_settings.ca_file	Str	+	Путь к CA файлу
tls_settings.client_cert_file	Str	+	Путь к файлу сертификата клиента
tls_settings.key_file	Str	+	Путь к файлу с ключом клиента

Пример ответа:

```
{
  "Response": {
  "changed": true,
    "failed": false,
    "msg": "ok"
 }
}
```

7.22.3 Предоставление доступа к почте пользователя с правами «Напрямую»

Для предоставления доступа к почте пользователя с правами «Напрямую» (без указания реального отправителя) необходимо выполнить запрос:

```
nct_ministerium set_shared_access \
--admin.login <…>
--admin.password <…>
--cox.balancer_endpoint=hydra.ucs-apps-1.installation.example.net:50053 \
--cox.compression=none \
--cox.endpoint=grpc-installation.example.net:3142 \
--cox.load_balanced=false \
--cox.request_timeout=10s \
--cox.service_name=cox \
--cox.use_tls=true \
--cox.use_tls_balancer=false \
--delegate_email user1@example.net\
--emails user2@example.net\
--permissions_by_emails 1 \
--tls_settings.ca_file ca.pem \
--tls_settings.client_cert_file client_cert.pem \
--tls_settings.key_file client_key.pem
```

Описание параметров запроса приведено в таблице 146.

Таблица 146 – Описание параметров запроса на доступ к почте пользователя с правами «Напрямую» (SendAs)

Параметр	Тип	Обязательный	Описание
admin.login	Str	+	Логин администратора тенанта
admin.password	Str	+	Пароль администратора тенанта
cox.balancer_endpoint	Str	+	Endpoint балансировщика нагрузки сервиса
cox.compression	Str	+	Метод сжатия данных (варианты: **none**, **gzip**), по умолчанию **none**
cox.endpoint	Str	+	Endpoint сервиса
cox.load_balanced	Bool	+	Балансировщик нагрузки сервиса
cox.request_timeout	Str	+	Тайм-аут запроса к сервису

Параметр	Тип	Обязательный	Описание
cox.service_name	Str	+	Имя сервиса
cox.use_tls	Bool	+	TLS-сертификат
cox.use_tls_balancer	Bool	+	Защищенная передача данных при подключении к балансировщику
delegate_email	Str	+	Учетная запись, которую необходимо делегировать пользователю
emails	Str	+	Учетная запись пользователя, которому делегируют
permissions_by_emails	Str	+	Разрешения для политики отправки почты для настройки доступа к почте: 0 – разрешение «Не разрешено» (Cannot), 1 – разрешение «От имени» (OnBehalf), 2 – разрешение «Напрямую» (SendAs)
tls_settings.ca_file	Str	+	Путь к CA файлу
tls_settings.client_cert_file	Str	+	Путь к файлу сертификата клиента
tls_settings.key_file	Str	+	Путь к файлу с ключом клиента

Пример ответа:

```
{
  "Response": {
    "changed": true,
    "failed": false,
    "msg": "ok"
 }
}
```

7.22.4 Отзыв доступа к делегированной учетной записи у всех делегатов

Чтобы отозвать доступ к делегированной учетной записи у всех делегатов, необходимо выполнить следующие действия:

1. Выполнить запрос на отзыв доступа к делегированной учетной записи у всех делегатов:

```
nct_ministerium unset_shared_access \
--admin.login <…>
--admin.password <…>
--cox.balancer_endpoint=hydra.ucs-apps-1.installation.example.net:50053 \
--cox.compression=none \
--cox.endpoint=grpc-installation.example.net:3142 \
--cox.load_balanced=false \
```

```
--cox.request_timeout=10s \
--cox.service_name=cox \
--cox.use_tls=true \
--cox.use_tls_balancer=false \
--delegate_email user1@example.net\
--tls_settings.ca_file ca.pem \
--tls_settings.client_cert_file client_cert.pem \
--tls_settings.key_file client_key.pem
```

Описание параметров запроса приведено в таблице 147.

Таблица 147 – Описание параметров запроса на отзыв доступа к делегированной учетной записи у всех делегатов

Параметр	Тип	Обязательный	Описание
admin.login	Str	+	Логин администратора тенанта
admin.password	Str	+	Пароль администратора тенанта
cox.balancer_endpoint	Str	+	Endpoint балансировщика нагрузки сервиса
cox.compression	Str	+	Метод сжатия данных (варианты: **none**, **gzip**), по умолчанию **none**
cox.endpoint	Str	+	Endpoint сервиса
cox.load_balanced	Bool	+	Балансировщик нагрузки сервиса
cox.request_timeout	Str	+	Тайм-аут запроса к сервису
cox.service_name	Str	+	Имя сервиса
cox.use_tls	Bool	+	TLS-сертификат
cox.use_tls_balancer	Bool	+	Защищенная передача данных при подключении к балансировщику
delegate_email	Str	+	Учетная запись, которую необходимо делегировать пользователю
tls_settings.ca_file	Str	+	Путь к CA файлу
tls_settings.client_cert_file	Str	+	Путь к файлу сертификата клиента
tls_settings.key_file	Str	+	Путь к файлу с ключом клиента

Пример ответа:

```
{
  "Response": {
    "changed": true,
    "failed": false,
    "msg": "ok"
   }
}
```

2. Выполнить запрос на проверку наличия делегатов:

```
nct_ministerium get_entities_with_shared_access \
--admin.login <…>
--admin.password <…>
--cox.balancer_endpoint=hydra.ucs-apps-1.installation.example.net:50053 \
--cox.compression=none \
--cox.endpoint=grpc-installation.example.net:3142 \
--cox.load_balanced=false \
--cox.request_timeout=10s \
--cox.service_name=cox \
--cox.use_tls=true \
--cox.use_tls_balancer=false \
--entity_email user1@example.net\
--tls_settings.ca_file ca.pem \
--tls_settings.client_cert_file client_cert.pem \
--tls_settings.key_file client_key.pem
```

Описание параметров запроса приведено в таблице 148.

Таблица 148 – Описание параметров запроса на проверку наличия делегатов

Параметр	Тип	Обязательный	Описание
admin.login	Str	+	Логин администратора тенанта
admin.password	Str	+	Пароль администратора тенанта
cox.balancer_endpoint	Str	+	Endpoint балансировщика нагрузки сервиса
cox.compression	Str	+	Метод сжатия данных (варианты: **none**, **gzip**), по умолчанию **none**
cox.endpoint	Str	+	Endpoint сервиса
cox.load_balanced	Bool	+	Балансировщик нагрузки сервиса
cox.request_timeout	Str	+	Тайм-аут запроса к сервису
cox.service_name	Str	+	Имя сервиса
cox.use_tls	Bool	+	TLS-сертификат
cox.use_tls_balancer	Bool	+	Защищенная передача данных при подключении к балансировщику
delegate_email	Str	+	Учетная запись, которую необходимо делегировать пользователю
entity_email	Str	+	Идентификатор пользователя, делегирующего свою учетную запись
tls_settings.ca_file	Str	+	Путь к CA файлу
tls_settings.client_cert_file	Str	+	Путь к файлу сертификата клиента
tls_settings.key_file	Str	+	Путь к файлу с ключом клиента

Пример ответа:

```
{
  "Response": {
    "changed": false,
    "failed": false,
    "msg": "ok"
  },
  "Entities": null,
  "Count": 0
}
```

7.22.5 Отзыв доступа к делегированной учетной записи у определенного делегата

Чтобы отозвать доступ к делегированной учетной записи у определенного делегата, необходимо выполнить следующие действия:

1. Выполнить запрос на отзыв доступа к делегированной учетной записи у определенного делегата:

```
nct_ministerium unset_shared_access \
--admin.login <…>
--admin.password <…>
--cox.balancer_endpoint=hydra.ucs-apps-1.installation.example.net:50053 \
--cox.compression=none \
--cox.endpoint=grpc-installation.example.net:3142 \
--cox.load_balanced=false \
--cox.request_timeout=10s \
--cox.service_name=cox \
--cox.use_tls=true \
--cox.use_tls_balancer=false \
--delegate_email user1@example.net\
--emails user2@example.net\
--tls_settings.ca_file ca.pem \
--tls_settings.client_cert_file client_cert.pem \
--tls_settings.key_file client_key.pem
```

Описание параметров запроса приведено в таблице 149.

Таблица 149 – Описание параметров запроса на отзыв доступа к делегированной учетной записи у определенного делегата

Параметр	Тип	Обязательный	Описание
admin.login	Str	+	Логин администратора тенанта
admin.password	Str	+	Пароль администратора тенанта
cox.balancer_endpoint	Str	+	Endpoint балансировщика нагрузки сервиса
cox.compression	Str	+	Метод сжатия данных (варианты: **none**, **gzip**), по умолчанию **none**

Параметр	Тип	Обязательный	Описание
cox.endpoint	Str	+	Endpoint сервиса
cox.load_balanced	Bool	+	Балансировщик нагрузки сервиса
cox.request_timeout	Str	+	Тайм-аут запроса к сервису
cox.service_name	Str	+	Имя сервиса
cox.use_tls	Bool	+	TLS-сертификат
cox.use_tls_balancer	Bool	+	Защищенная передача данных при подключении к балансировщику
delegate_email	Str	+	Учетная запись, которую необходимо делегировать пользователю
emails	Str	+	Учетная запись пользователя, которому делегируют
tls_settings.ca_file	Str	+	Путь к CA файлу
tls_settings.client_cert_file	Str	+	Путь к файлу сертификата клиента
tls_settings.key_file	Str	+	Путь к файлу с ключом клиента

Пример ответа:

```
{
  "Response": {
    "changed": true,
    "failed": false,
    "msg": "ok"
  }
}
```

2. Выполнить запрос на проверку наличия делегатов:

```
nct_ministerium get_entities_with_shared_access \
--admin.login <…>
--admin.password <…>
--cox.balancer_endpoint=hydra.ucs-apps-1.installation.example.net:50053 \
--cox.compression=none \
--cox.endpoint=grpc-installation.example.net:3142 \
--cox.load_balanced=false \
--cox.request_timeout=10s \
--cox.service_name=cox \
--cox.use_tls=true \
--cox.use_tls_balancer=false \
--entity_email user1@example.net\
--tls_settings.ca_file ca.pem \
--tls_settings.client_cert_file client_cert.pem \
--tls_settings.key_file client_key.pem
```

Описание параметров запроса приведено в таблице 150.

Таблица 150 – Описание параметров запроса на проверку наличия делегатов

Параметр	Тип	Обязательный	Описание
admin.login	Str	+	Логин администратора тенанта
admin.password	Str	+	Пароль администратора тенанта
cox.balancer_endpoint	Str	+	Endpoint балансировщика нагрузки сервиса
cox.compression	Str	+	Метод сжатия данных (варианты: **none**, **gzip**), по умолчанию **none**
cox.endpoint	Str	+	Endpoint сервиса
cox.load_balanced	Bool	+	Балансировщик нагрузки сервиса
cox.request_timeout	Str	+	Тайм-аут запроса к сервису
cox.service_name	Str	+	Имя сервиса
cox.use_tls	Bool	+	TLS-сертификат
cox.use_tls_balancer	Bool	+	Защищенная передача данных при подключении к балансировщику
delegate_email	Str	+	Учетная запись, которую необходимо делегировать пользователю
entity_email	Str	+	Идентификатор пользователя, делегирующего свою учетную запись
tls_settings.ca_file	Str	+	Путь к CA файлу
tls_settings.client_cert_file	Str	+	Путь к файлу сертификата клиента
tls_settings.key_file	Str	+	Путь к файлу с ключом клиента

Пример ответа:


```
{
  "Response": {
    "changed": false,
    "failed": false,
    "msg": "ok"
  },
  "Entities": [
    {
      "id": "925c704b-1815-4250-890c-a4048feb748a",
      "type": 1,
      "tenant_id": "a3bbba13-686a-485b-8878-3d0642018cc8",
      "region_id": "2dbacea3-5889-4021-8f38-bc2214dd7423",
      "roles": [
        "c4b1f72c-672d-5ace-8a6d-96edc21227de"
      ],
      "emails": [
        {
          "id": "95622080-5064-5ee4-b6fb-26594a2f9387",
```

```
          "email": "user3@example.net"
          "domain_id": "6bb5e324-9e1f-5cde-9844-504d2465ddf2",
          "entity_id": "925c704b-1815-4250-890c-a4048feb748a",
          "primary": true
        }
      ],
      "logins": [
        {
          "id": "95622080-5064-5ee4-b6fb-26594a2f9387",
          "entity_id": "925c704b-1815-4250-890c-a4048feb748a",
          "login": "user3@example.net"
          "auth_type": 1,
          "attributes": {
            "domain_id": "6bb5e324-9e1f-5cde-9844-504d2465ddf2"
          },
          "SecondFactorParams": null
        }
      ],
      "Payload": {
        "User": {
          "locale": "ru_RU"
        }
      },
      "status": 2,
      "shared_access": {}
    }
  ],
  "Count": 1
}
```


7.22.6 Просмотр всех делегатов

Чтобы увидеть всех пользователей, которым делегирована учетная запись выбранного пользователя, необходимо выполнить запрос:

```
nct_ministerium get_entities_with_shared_access \
--admin.login <…>
--admin.password <…>
--cox.balancer_endpoint=hydra.ucs-apps-1.installation.example.net:50053 \
--cox.compression=none \
--cox.endpoint=grpc-installation.example.net:3142 \
--cox.load_balanced=false \
--cox.request_timeout=10s \
--cox.service_name=cox \
--cox.use_tls=true \
--cox.use_tls_balancer=false \
--entity_email user1@example.net\
--tls_settings.ca_file ca.pem \
--tls_settings.client_cert_file client_cert.pem \
--tls_settings.key_file client_key.pem
```

Описание параметров запроса приведено в таблице 151.

Таблица 151 – Описание параметров запроса на проверку всех пользователей, которым делегирована учетная запись

Параметр	Тип	Обязательный	Описание
admin.login	Str	+	Логин администратора тенанта
admin.password	Str	+	Пароль администратора тенанта
cox.balancer_endpoint	Str	+	Endpoint балансировщика нагрузки сервиса
cox.compression	Str	+	Метод сжатия данных (варианты: **none**, **gzip**), по умолчанию **none**
cox.endpoint	Str	+	Endpoint сервиса
cox.load_balanced	Bool	+	Балансировщик нагрузки сервиса
cox.request_timeout	Str	+	Тайм-аут запроса к сервису
cox.service_name	Str	+	Имя сервиса
cox.use_tls	Bool	+	TLS-сертификат
cox.use_tls_balancer	Bool	+	Защищенная передача данных при подключении к балансировщику
entity_email	Str	+	Идентификатор пользователя, делегирующего свою учетную запись
tls_settings.ca_file	Str	+	Путь к CA файлу
tls_settings.client_cert_file	Str	+	Путь к файлу сертификата клиента
tls_settings.key_file	Str	+	Путь к файлу с ключом клиента

Пример ответа:


```
{
  "Response": {
    "changed": false,
    "failed": false,
    "msg": "ok"
  },
  "Entities": [
    {
      "id": "925c704b-1815-4250-890c-a4048feb748a",
      "type": 1,
      "tenant_id": "a3bbba13-686a-485b-8878-3d0642018cc8",
      "region_id": "2dbacea3-5889-4021-8f38-bc2214dd7423",
      "roles": [
        "c4b1f72c-672d-5ace-8a6d-96edc21227de"
      ],
      "emails": [
        {
          "id": "95622080-5064-5ee4-b6fb-26594a2f9387",
          "email": "user2@example.net"
          "domain_id": "6bb5e324-9e1f-5cde-9844-504d2465ddf2",
```

```
          "entity_id": "925c704b-1815-4250-890c-a4048feb748a",
          "primary": true
        }
      ],
      "logins": [
        {
          "id": "95622080-5064-5ee4-b6fb-26594a2f9387",
          "entity_id": "925c704b-1815-4250-890c-a4048feb748a",
          "login": "user2@example.net"
          "auth_type": 1,
          "attributes": {
            "domain_id": "6bb5e324-9e1f-5cde-9844-504d2465ddf2"
          },
          "SecondFactorParams": null
        }
      ],
      "Payload": {
        "User": {
          "locale": "ru_RU"
        }
      },
      "status": 2,
      "shared_access": {}
    }
  ],
  "Count": 1
}
```


В случае отсутствия делегированных пользователей у учетной записи ожидается ответ вида:


```
{
  "Response": {
    "changed": false,
    "failed": false,
    "msg": "ok"
  },
  "Entities": null,
  "Count": 0
}
```


7.22.7 Просмотр всех делегированных учетных записей

Чтобы увидеть все делегированные учетные записи, необходимо выполнить запрос на проверку всех делегированных учетных записей выбранного пользователя:

```
nct_ministerium get_shared_entities \
--admin.login <…>
--admin.password <…>
--cox.balancer_endpoint=hydra.ucs-apps-1.installation.example.net:50053 \
--cox.compression=none \
--cox.endpoint=grpc-installation.example.net:3142 \
--cox.load_balanced=false \
--cox.request_timeout=10s \
```

```
--cox.service_name=cox \
--cox.use_tls=true \
--cox.use_tls_balancer=false \
--entity_email user2@example.net\
--tls_settings.ca_file ca.pem \
--tls_settings.client_cert_file client_cert.pem \
--tls_settings.key_file client_key.pem
```

Описание параметров запроса приведено в таблице 152.

Таблица 152 – Описание параметров запроса на проверку всех делегированных учетных записей выбранного пользователя

Параметр	Тип	Обязательный	Описание
admin.login	Str	+	Логин администратора тенанта
admin.password	Str	+	Пароль администратора тенанта
cox.balancer_endpoint	Str	+	Endpoint балансировщика нагрузки сервиса
cox.compression	Str	+	Метод сжатия данных (варианты: **none**, **gzip**), по умолчанию **none**
cox.endpoint	Str	+	Endpoint сервиса
cox.load_balanced	Bool	+	Балансировщик нагрузки сервиса
cox.request_timeout	Str	+	Тайм-аут запроса к сервису
cox.service_name	Str	+	Имя сервиса
cox.use_tls	Bool	+	TLS-сертификат
cox.use_tls_balancer	Bool	+	Защищенная передача данных при подключении к балансировщику
entity_email	Str	+	Email ползователя
tls_settings.ca_file	Str	+	Путь к CA файлу
tls_settings.client_cert_file	Str	+	Путь к файлу сертификата клиента
tls_settings.key_file	Str	+	Путь к файлу с ключом клиента

Пример ответа:


```
{
  "Response": {
    "changed": false,
    "failed": false,
    "msg": "ok"
  },
  "Entities": [
    {
      "id": "925c704b-1815-4250-890c-a4048feb748a",
      "type": 1,
      "tenant_id": "a3bbba13-686a-485b-8878-3d0642018cc8",
      "region_id": "2dbacea3-5889-4021-8f38-bc2214dd7423",
```

```
      "roles": [
        "c4b1f72c-672d-5ace-8a6d-96edc21227de"
      ],
      "emails": [
        {
          "id": "95622080-5064-5ee4-b6fb-26594a2f9387",
          "email": "user1@example.net"
          "domain_id": "6bb5e324-9e1f-5cde-9844-504d2465ddf2",
          "entity_id": "925c704b-1815-4250-890c-a4048feb748a",
          "primary": true
        }
      ],
      "logins": [
        {
          "id": "95622080-5064-5ee4-b6fb-26594a2f9387",
          "entity_id": "925c704b-1815-4250-890c-a4048feb748a",
          "login": "user1@example.net"
          "auth_type": 1,
          "attributes": {
            "domain_id": "6bb5e324-9e1f-5cde-9844-504d2465ddf2"
          },
          "SecondFactorParams": null
        }
      ],
      "Payload": {
        "User": {
          "locale": "ru_RU"
        }
      },
      "status": 2,
      "shared_access": {
        "permissions": {
          "d59ed675-0218-486c-8941-c245b3e3a306": {
            "account": {
              "role": 3
            },
            "mail": {
              "send_policy": 2
            }
          }
        }
      }
    }
  ],
  "Count": 1
}
```


В случае отсутствия делегированных учетных записей ожидается ответ вида:


```
{
  "Response": {
    "changed": false,
    "failed": false,
    "msg": "ok"
  },
  "Entities": null,
  "Count": 0
}
```

7.23 Поиск писем по заданным критериям

Важно – Поиск писем всех пользователей в тенанте по заданным критериям выполняется пользователем с ролью администратора тенанта.

Поиск писем всех пользователей в тенанте по заданным критериям выполняется с помощью команды **search_mails_by_tenant_id**.

Пример выполнения поиска письма по заданным критериям:

```
nct_ministerium search_mails_by_tenant_id \
--admin.login <…>
--admin.password <…>
--output_json /home/admin/certs/installation/output.json \
--query.text.operation=equals \
--query.text.value=семь \
--tenant_id 01068ade-1cce-4125-ab6b-91d977ecf85b \
--cox.balancer_endpoint=hydra.ucs-apps-1. installation.example.net:50053 \
--cox.compression=none \
--cox.endpoint=grpc-installation.example.net:3142 \
--cox.load_balanced=false \
--cox.request_timeout=10s \
--cox.service_name=cox \
--cox.use_tls=true \
--cox.use_tls_balancer=false \
--tls_settings.ca_file /home/user/ministerium_certs/installation/ca.pem \
--
tls_settings.client_cert_file /home/user/ministerium_certs/installation/client_c
rt.pem \
--tls_settings.key_file /home/user/ministerium_certs/installation/client_key.pem
\
```

Описание параметров поиска приведено в таблице 153.

Таблица 153 – Описание параметров поиска письма по заданным критериям

Параметр	Тип	Обязательный	Описание
admin.login	Str	+	Логин администратора тенанта
admin.password	Str	+	Пароль администратора тенанта
output_json	Str	+	Путь к файлу, в который будет записан результат поиска. Этот файл может быть использован в команде удаления (**delete_mails**) и указан в параметре **--source**
query.text.operation	Str	-	Поиск в тексте письма. Оператор запроса. Возможные значения: – less (меньше); – greater (больше); – in_range (в диапазоне); – equals (равно);

Параметр	Тип	Обязательный	Описание
			– contains (содержит)
query.text.value	Str	-	Значение поиска
tenant_id	Str	+	Идентификатор тенанта
cox.balancer_endpoint	Str	+	Endpoint балансировщика нагрузки сервиса
cox.compression	Str	+	Метод сжатия данных (варианты: **none**, **gzip**), по умолчанию **none**
cox.endpoint	Str	+	Endpoint сервиса
cox.load_balanced	Bool	+	Балансировщик нагрузки сервиса
cox.request_timeout	Str	+	Тайм-аут запроса к сервису
cox.service_name	Str	+	Имя сервиса
cox.use_tls	Bool	+	TLS-сертификат
cox.use_tls_balancer	Bool	+	Защищенная передача данных при подключении к балансировщику
tls_settings.ca_file	Str	+	Путь к CA файлу
tls_settings.client_cert_file	Str	+	Путь к файлу сертификата клиента
tls_settings.key_file	Str	+	Путь к файлу с ключом клиента

Пример ответа:

```
[
  {
    "user_id": "b8856ca4-2081-4fad-b2ca-e4029ac9fceb",
    "mails": [
      {
        "from": "ivan@installation.example.net"
        "to": "vasiliy@installation.example.net"
        "subject": "Hello!",
        "mail_id": "9d43a184-16ad-4714-b9e8-dae85722f668"
      }
    ]
  }
]
```

Все возможные параметры поиска приведены в таблице 154.

Таблица 154 – Описание всех параметров поиска

Параметр	Тип	Обязательный	Описание
admin.login	Str	+	Логин администратора тенанта
admin.password	Str	+	Пароль администратора тенанта

Параметр	Тип	Обязательный	Описание
compose_with_or			Объединение полей запроса с помощью ИЛИ. Значение по умолчанию И
cox.balancer_endpoint	Str	+	Endpoint балансировщика нагрузки сервиса
cox.compression	Str	+	Метод сжатия данных (варианты: **none**, **gzip**), по умолчанию **none**
cox.endpoint	Str	+	Endpoint сервиса
cox.load_balanced	Bool	+	Балансировщик нагрузки сервиса
cox.request_timeout	Str	+	Тайм-аут запроса к сервису
cox.service_name	Str	+	Имя сервиса
cox.use_tls	Bool	+	TLS-сертификат
cox.use_tls_balancer	Bool	+	Защищенная передача данных при подключении к балансировщику
help	Str	+	Помощь при выполнении команды **search_mails_by_tenant_id**
output_json	Str	+	Путь к файлу, в который будет записан результат поиска. Этот файл может быть использован в команде удаления (**delete_mails**) и указан в параметре **--source**
query.attachment_ names.operation	Str	-	Поиск по названию вложений. Оператор запроса. Возможные значения: – less (меньше); – greater (больше); – in_range (в диапазоне); – equals (равно); – contains (содержит)
query.attachment_ names.values	Str	-	Поиск по названию вложений
query.bcc.operation	Str	-	Оператор для поиска значения в поле письма «Скрытая копия». Оператор запроса. Возможные значения: – less (меньше); – greater (больше); – in_range (в диапазоне); – equals (равно); – contains (содержит)

Параметр	Тип	Обязательный	Описание
query.bcc.values	Str	-	Поиск указанного значения в поле письма «Скрытая копия»
query.cc.operation	Str	-	Оператор для поиска значения в поле письма «Копия». Оператор запроса. Возможные значения: – less (меньше); – greater (больше); – in_range (в диапазоне); – equals (равно); – contains (содержит)
query.cc.values	Str	-	Поиск указанного значения в поле письма «Копия»
query.created_ time.additional	Int	-	Время создания письма. Микросекунды UTC. Справа от диапазона, если операция равна «in_range», в противном случае игнорируется
query.created_time.operation	Str	-	Время создания письма. Оператор запроса. Возможные значения: – less (меньше); – greater (больше); – in_range (в диапазоне); – equals (равно); – contains (содержит)
query.created_ time.unixmicro	Int	-	Время создания письма. Микросекунды UTC. Операнд ИЛИ слева от диапазона
query.flag_draft	Str	-	Письмо помечено как «Черновик». Возможные значения: «true» или «false»
query.flag_flagged	Str	-	Письмо имеет метку-флаг. Возможные значения: «true» или «false»
query.flag_seen	Str	-	Письмо помечено как «Прочитано». Возможные значения: «true» или «false»
query.from.operation	Str	-	Оператор запроса для поиска значения в поле письма «От кого». Возможные значения: – less (меньше); – greater (больше);

Параметр	Тип	Обязательный	Описание
			– in_range (в диапазоне); – equals (равно); – contains (содержит)
query.from.values strings	Str	-	Поиск указанного значения в поле письма «От кого»
query.from_to_cc_text_ subject.operation	Str	-	Поиск указанного значения в заголовках «от кого», «кому», «копия», «тема» и в тексте письма. Оператор запроса. Возможные значения: – less (меньше); – greater (больше); – in_range (в диапазоне); – equals (равно); – contains (содержит)
query.from_to_cc_text_ subject.value	Str	-	Поиск указанного значения в заголовках «от кого», «кому», «копия», «тема» и в тексте письма
query.has_attachments	Str	-	Письмо имеет вложения. Возможные значения: «true» или «false»
query.importance.operation	Str	-	Фильтр по важности письма. Оператор запроса. Возможные значения: – less (меньше); – greater (больше); – in_range (в диапазоне); – equals (равно); – contains (содержит)
query.importance.value	Str	-	Фильтр по важности письма. Возможные поисковые значения: – low (низкий); – normal (нормальный); – high (высокий);
query.mail_size.additional	Str	-	Размер письма. Справа от диапазона, если операция равна «in_range», в противном случае игнорируется
query.mail_size.operation	Str	-	Размер письма. Оператор запроса. Возможные значения: – less (меньше); – greater (больше); – in_range (в диапазоне); – equals (равно); – contains (содержит)

Параметр	Тип	Обязательный	Описание
query.mail_size.value	Int	-	Размер письма. Операнд ИЛИ слева от диапазона
query.modified_ time.operation	Str	-	Время последнего редактирования письма. Оператор запроса. Возможные значения: – less (меньше); – greater (больше); – in_range (в диапазоне); – equals (равно); – contains (содержит)
query.modified_ time.additional	Int	-	Время последнего редактирования письма. Микросекунды UTC. Справа от диапазона, если операция равна «in_range», в противном случае игнорируется
query.modified_ time.unixmicro	Int	-	Время последнего редактирования письма. Микросекунды UTC. Операнд ИЛИ слева от диапазона
query.subject.operation	Str	-	Поиск в теме письма. Оператор запроса. Возможные значения: – less (меньше); – greater (больше); – in_range (в диапазоне); – equals (равно); – contains (содержит)
query.subject.value	Str	-	Поиск в теме письма
query.subject_and_ text.operation	Str	-	Поиск в теме письма и в тексте. Оператор запроса. Возможные значения: – less (меньше); – greater (больше); – in_range (в диапазоне); – equals (равно); – contains (содержит)
query.subject_and_ text.value	Str	-	Поиск значений в теме письма и в тексте
query.text.operation	Str	-	Поиск в тексте письма. Оператор запроса. Возможные значения: – less (меньше); – greater (больше); – in_range (в диапазоне);

Параметр	Тип	Обязательный	Описание
			– equals (равно); – contains (содержит)
query.text.value	Str	-	Поиск в тексте письма
query.to.operation	Str	-	Оператор для поиска значения в поле письма «Кому». Оператор запроса. Возможные значения: – less (меньше); – greater (больше); – in_range (в диапазоне); – equals (равно); – contains (содержит)
query.to.values	Str	-	Поиск указанного значения в поле письма «Кому»
tenant_id	Str	+	Идентификатор тенанта
tls_settings.ca_file	Str	+	Путь к CA файлу
tls_settings.client_cert_file	Str	+	Путь к файлу сертификата клиента
tls_settings.key_file	Str	+	Путь к файлу с ключом клиента
token-name	Str	+	Имя токена для подключения
c	Str	+	Цветной вывод на консоль
check	Str	+	Выполнить проверку без выполнения команды
config	Str	+	По умолчанию используется **nct_ministerium.yaml** или **nct_ministerium.json**, расположенный в PWD
diff	Str	+	Показать изменения
v	Str	+	Подробное ведение журнала

7.24 Поиск сведений о доставленных письмах

Поиск сведений о доставленных письмах выполняется с помощью команды **get_mail_events**.

Пример команды, реализующей поиск сведений о доставленных письмах:

```
nct_ministerium get_mail_events
  --config ministerium_local.json
```

```
--tenant_id 03337d37-3f34-4000-bb9c-4d8088dfe992
--timestamp_from 2024-01-18T19:42:07+03:00
```

Описание параметров поиска приведено в таблице 155.

Таблица 155 – Описание параметров команды поиска доставленных писем

Параметр	Тип	Обязательный	Описание
config	Str	+	Путь к файлу конфигурации
tenant_id	Str	+	Идентификатор тенанта, в рамках которого производится поиск сообщений
timestamp_from	Str	-	Начало периода, пример: 2024-01-18T19:42:07+03:00
timestamp_to	Str	-	Окончание периода, пример: 2024-01-18T19:42:07+03:00
message_id	Str	-	Идентификатор сообщения
email	Str	-	Почтовый адрес
user_id	Str	-	Идентификатор пользователя

Пример ответа:


```
{
  "Response": {
    "changed": false,
    "failed": false,
    "msg": "ok"
  },
  "mail_events": [
    {
      "timestamp": "2024-01-19T12:30:40.367+03:00",
      "event_type": "SAVED",
      "message_id": "a7d@local.example.ru",
      "sender_email": "admin@local.example.ru",
      "recipient_email": [
         "dedal.qq@local.example.ru"
      ],
      "message_size": 1439,
      "message_subject": "qq",
      "data": null
    },
    {
      "timestamp": "2024-01-19T12:23:18.724+03:00",
```

```
      "event_type": "SAVED",
      "message_id": "a7d@local.example.ru",
      "sender_email": "admin@local.example.ru",
      "recipient_email": [
         "dedal.qq@local.example.ru"
      ],
      "message_size": 1439,
      "message_subject": "qq",
      "data": null
    },
     ......
}
```


7.25 Массовое удаление писем

Важно – Удаление писем по списку выполняется пользователем с ролью администратора тенанта.

Для удаления писем по списку необходимо выполнить команду **delete_mails**. Для выполнения данной команды потребуется JSON файл с идентификаторами письма. Подготовить файл можно двумя способами:

1. Самостоятельно подготовить входной JSON файл с данными письма:

```
[
  {
    "user_id": "c6ce44a7-7d81-4598-a727-02852bd149c4",
    "mails": [
      {
        "mail_id": "3bcf4651-c98d-4d65-b04d-17c0ca05ec14"
      }
    ]
  }
]
```

2. Получить информацию для JSON файла из ответа на команду **search_mails_by_tenant_id**. Для этого выполнить запрос на поиск письма по заданным критериям с помощью команды **search_mails_by_tenant_id** (пример команды и описание параметров запроса приведены в разделе 7.23).
3. После этого необходимо выполнить команду **delete_mails**:

```
nct_ministerium delete_mails \
--admin.login <…>
--admin.password <…>
--source /home/user/mail_list.json \
```

```
--reject /home/user/rejected.json \
--cox.balancer_endpoint=hydra.ucs-apps-1.installation.example.net:50053 \
--cox.compression=none \
--cox.endpoint=grpc-installation.example.net:3142 \
--cox.load_balanced=false \
--cox.request_timeout=10s \
--cox.service_name=cox \
--cox.use_tls=true \
--cox.use_tls_balancer=false \
--tls_settings.ca_file /home/user/ca.pem \
--tls_settings.client_cert_file /home/user/client_crt.pem \
--tls_settings.key_file /home/user/client_key.pem \
```

Описание параметров запроса приведено в таблице 156.

Таблица 156 – Описание параметров запроса на удаление писем по заданным критериям

Параметр	Тип	Обязательный	Описание
admin.login	Str	+	Логин администратора тенанта
admin.password	Str	+	Пароль администратора тенанта
source	Str	+	Путь к json файлу со списком удаляемых писем
reject	Str	+	В этот файл сохраняются идентификаторы писем (mail_id) и причины (reason), по которым письмо не получилось удалить
cox.balancer_endpoint	Str	+	Endpoint балансировщика нагрузки сервиса
cox.compression	Str	+	Метод сжатия данных (варианты: **none**, **gzip**), по умолчанию **none**
cox.endpoint	Str	+	Endpoint сервиса
cox.load_balanced	Bool	+	Балансировщик нагрузки сервиса
cox.request_timeout	Str	+	Тайм-аут запроса к сервису
cox.service_name	Str	+	Имя сервиса
cox.use_tls	Bool	+	TLS-сертификат
cox.use_tls_balancer	Bool	+	Защищенная передача данных при подключении к балансировщику
tls_settings.ca_file	Str	+	Путь к CA файлу
tls_settings.client_cert_file	Str	+	Путь к файлу сертификата клиента
tls_settings.key_file	Str	+	Путь к файлу с ключом клиента

Пример ответа:

```
{
  "Response": {
```

```
    "changed": true,
    "failed": false,
    "msg": "ok"
  },
  "deleted": 1,
  "failed": 0
}
```


7.26 Удаление пользователя, группы и ресурса

Для удаления пользователя, группы и ресурса выполнить запрос **change_status** на смену статуса объекта:

```
nct-ministerium change_status
--entity_id <entity_id>
--status <MARK_DELETED> ...
```

Описание параметров запроса приведено в таблице 157.

Таблица 157 – Описание параметров запроса на смену статуса объекта

Параметр	Тип	Обязательный	Описание
entity_id	Str	+	Идентификатор пользователя
statuses	Str	+	Статусы

Примечание – Сущность будет помечена на удаление и впоследствии будет удалена в соответствии с retention policy механизмом сборки мусора (garbage collector).

7.27 Восстановление удаленных писем в почтовом ящике пользователя

Для восстановления удаленных писем в почтовом ящике пользователя необходимо выполнить следующие действия:

1. Выполнить запрос на поиск удаленных писем. С помощью данной команды осуществляется поиск писем пользователей на основании следующих фильтров:
   – идентификатор пользователя;
   – лимит на количество писем, необходимых для восстановления;
   – временной диапазон «с» и «до».

   Важно – Должен быть установлен минимум один фильтр.

Пример запроса на поиск удаленных писем:

```
./nct_ministerium get_deleted_mails
--config=config.json
--user_id 596c43b8-234d-4229-a138-b3f2e6555b0f
--limit 3
--timestamp_from 2012-11-01T22:08:41+00:00 --timestamp_to 2032-11-
01T22:08:41+00:00
```

Описание параметров запроса приведено в таблице 158.

Таблица 158 – Описание параметров запроса на поиск удаленных писем

Параметр	Тип	Обязательный	Описание
config	Str	+	Конфигурационный файл с параметрами сервиса Cox и настройками tls. Формируется автоматически на сервере с ролью ucs_infrastructure и находится по пути /srv/ministerium/config.json
user_id	Str	-	Идентификатор пользователя
limit	Str	-	Лимит на количество писем, необходимых для восстановления
timestamp_from timestamp_to	Str	-	Временной диапазон «с» и «до»

После этого в консоли администратора отобразится список найденных писем. Письма выведутся в порядке убывания по дате удаления, от более ранней к более поздней.

Пример ответа:

```
{
  "Response": {
    "changed": false,
    "failed": false,
    "msg": "ok"
  },
  "DeletedMails": [
    {
      "Id": "aflee084-c154-4aed-86df-0c8fa51e7fce",
      "Subject": "asd: событие было обновлено",
      "DeletedTime": "2023-01-24T17:23:13+03:00",
      "ReceivingTime": "2023-01-31T10:32:59+03:00"
    },
    {
      "Id": "1bb308de-a042-59c8-9002-c3dd6fef78f0",
      "Subject": "",
      "DeletedTime": "2023-01-24T17:01:10+03:00",
      "ReceivingTime": "2023-01-24T17:01:10+03:00"
    }
  ]
}
```

2. Выполнить восстановление удаленных писем, найденных с помощью команды из п. 1. Восстановление удаленных писем можно выполнить тремя способами:
   – Восстановить письмо по его идентификатору. С помощью данной команды можно восстановить одно письмо по известному идентификатору. Пример запроса на восстановление письма по его идентификатору:

```
./nct_ministerium restore_mails_by_mail_id
--config=config.json
--email_id 9b0873df-2829-49d7-b0ae-36ef8b52ae7e
```

Описание параметров запроса приведено в таблице 159.

Таблица 159 – Описание параметров запроса на восстановление письма по идентификатору

Параметр	Тип	Обязательный	Описание
config	Str	+	Конфигурационный файл с параметрами сервиса Cox и настройками tls. Формируется автоматически на сервере с ролью ucs_infrastructure и находится по пути /srv/ministerium/config.json
email_id	Str	+	Идентификатор письма пользователя

Пример ответа:

```
{
  "changed": true,
  "failed": false,
  "msg": "ok"
}
```

   – Восстановить письмо по лимиту на количество писем, необходимых для восстановления. С помощью данной команды можно восстановить определенное количество последних удаленных писем пользователей. Пример запроса на восстановление письма по лимиту на количество писем, необходимых для восстановления:

```
./nct_ministerium restore_mails_by_limit
--config=config.json
--limit 10
--user_id ddd4a809-ea14-407c-b4ea-60ac90214630
```

Описание параметров запроса приведено в таблице 160.

Таблица 160 – Описание параметров запроса на восстановление по лимиту на количество писем

Параметр	Тип	Обязательный	Описание
config	Str	+	Конфигурационный файл с параметрами сервиса Cox и настройками tls. Формируется автоматически на сервере с ролью ucs_infrastructure и находится по пути /srv/ministerium/config.json
limit	Str	-	Лимит на количество писем, необходимых для восстановления
user_id	Str	-	Идентификатор пользователя

Примечание – Если в этой команде указать параметры **limit** и **user_id**, то восстановится определенное количество последних удаленных писем конкретного пользователя. Если в этой команде указать только параметр **user_id**, то восстановятся все удаленные письма конкретного пользователя. Если в этой команде указать только параметр **limit**, то восстановится определенное количество последних удаленных писем всех пользователей.

Пример ответа:

```
{
  "changed": true,
  "failed": false,
  "msg": "ok"
}
```

– Восстановить письма, удаленные в определенный диапазон времени, указанный пользователем. С помощью данной команды можно восстановить последние удаленные письма пользователей в заданный диапазон времени. Пример запроса на восстановление писем, удаленных в заданный диапазон времени:

```
./nct_ministerium restore_mails_by_period
--config=config.json
--timestamp_from 2012-11-01T22:08:41+00:00 --timestamp_to 2032-11-
01T22:08:41+00:00
--user_id ddd4a809-ea14-407c-b4ea-60ac90214630
```

Описание параметров запроса приведено в таблице 161.

Таблица 161 – Описание параметров запроса на восстановление писем, удаленных в определенный диапазон времени, указанный пользователем

Параметр	Тип	Обязательный	Описание
config	Str	+	Конфигурационный файл с параметрами сервиса Cox и настройками tls. Формируется автоматически на сервере с ролью ucs_infrastructure и находится по пути /srv/ministerium/config.json
timestamp_from timestamp_to	Str	-	Временной диапазон «с» и «до»
user_id	Str	-	Идентификатор пользователя

Примечание – Если в этой команде указать параметры **timestamp_from**, **timestamp_to** и **user_id**, то восстановятся письма конкретного пользователя за определенный временной диапазон. Если в этой команде указать только параметры **timestamp_from** и **timestamp_to**, то восстановятся последние удаленные письма всех пользователей за определенный временной диапазон. Если в этой команде указать только параметр **user_id**, то восстановятся все удаленные письма конкретного пользователя.

Пример ответа:

```
{
  "changed": true,
  "failed": false,
  "msg": "ok"
}
```

7.28 Просмотр истории комментариев блокировки пользователей

Для просмотра истории комментариев блокировки пользователей необходимо выполнить запрос на просмотр истории комментариев:

```
nct_ministerium get_user_blocking_history
--admin.login <…>
--admin.password <…>
--entity_id <…>
--cox.balancer_endpoint=hydra.ucs-apps-1.installation.example.net:50053 \
--cox.compression=none \
--cox.endpoint=grpc-installation.example.net:3142 \
--cox.load_balanced=false \
--cox.request_timeout=10s \
--cox.service_name=cox \
```

```
--cox.use_tls=true \
--cox.use_tls_balancer=false \
--tls_settings.ca_file /home/user/ca.pem
--tls_settings.client_cert_file /home/user/client_crt.pem \
--tls_settings.key_file /home/user/client_key.pem \
```

Описание параметров запроса приведено в таблице 162.

Таблица 162 – Описание параметров запроса на просмотр истории комментариев

Параметр	Тип	Обязательный	Описание
admin.login	Str	+	Логин администратора тенанта
admin.password	Str	+	Пароль администратора тенанта
entity_id	Str	+	Идентификатор пользователя
cox.balancer_endpoint	Str	+	Endpoint балансировщика нагрузки сервиса
cox.compression	Str	+	Метод сжатия данных (варианты: **none**, **gzip**), по умолчанию **none**
cox.endpoint	Str	+	Endpoint сервиса
cox.load_balanced	Bool	+	Балансировщик нагрузки сервиса
cox.request_timeout	Str	+	Тайм-аут запроса к сервису
cox.service_name	Str	+	Имя сервиса
cox.use_tls	Bool	+	TLS-сертификат
cox.use_tls_balancer	Bool	+	Защищенная передача данных при подключении к балансировщику
tls_settings.ca_file	Str	+	Путь к CA файлу
tls_settings.client_cert_file	Str	+	Путь к файлу сертификата клиента
tls_settings.key_file	Str	+	Путь к файлу с ключом клиента

Пример ответа:


```
{
  "Response": {
    "changed": false,
    "failed": false,
    "msg": "ok"
  },
  "history_records": [
    {
      "id": "2358ec03-1caa-4bdb-9a40-2d274f24eb70",
      "tenant_id": "01068ade-1cce-4125-ab6b-91d977ecf85b",
      "actor_id": "e0e788c4-2b10-4375-86f6-1726b0c274a1",
      "user_id": "041ab13d-f419-4412-9670-ed0339b919ed",
      "timestamp": "2023-01-11T16:10:53+03:00",
      "action": "USER_BLOCKED"
    },
```

```
  {
    "id": "50106f1e-f37d-4518-ad0c-e7c4bdf51687",
    "tenant_id": "01068ade-1cce-4125-ab6b-91d977ecf85b",
    "actor_id": "e0e788c4-2b10-4375-86f6-1726b0c274a1",
    "user_id": "041ab13d-f419-4412-9670-ed0339b919ed",
    "timestamp": "2023-01-11T16:10:53+03:00",
    "action": "ADDED_BLOCKING_REASON",
    "reason": "huj nkl;"
  },
  {
    "id": "1fc85eaf-8763-4544-85fb-8689862c7524",
    "tenant_id": "01068ade-1cce-4125-ab6b-91d977ecf85b",
    "actor_id": "e0e788c4-2b10-4375-86f6-1726b0c274a1",
    "user_id": "041ab13d-f419-4412-9670-ed0339b919ed",
    "timestamp": "2023-01-11T16:11:02+03:00",
    "action": "ADDED_BLOCKING_REASON",
    "reason": "huj nkl;kiolp"
  },
  {
    "id": "10765bc9-5444-425d-9d47-8bfec8a3d7fb",
    "tenant_id": "01068ade-1cce-4125-ab6b-91d977ecf85b",
    "actor_id": "e0e788c4-2b10-4375-86f6-1726b0c274a1",
    "user_id": "041ab13d-f419-4412-9670-ed0339b919ed",
    "timestamp": "2023-01-11T16:11:12+03:00",
    "action": "USER_UNBLOCKED"
  },
  {
    "id": "c30e82e4-b130-430b-a138-4c36d091a4bd",
    "tenant_id": "01068ade-1cce-4125-ab6b-91d977ecf85b",
    "actor_id": "e0e788c4-2b10-4375-86f6-1726b0c274a1",
    "user_id": "041ab13d-f419-4412-9670-ed0339b919ed",
    "timestamp": "2023-01-11T16:13:34+03:00",
    "action": "USER_BLOCKED"
  },
  {
    "id": "95610aec-31da-470b-9e4b-22084cf4219d",
    "tenant_id": "01068ade-1cce-4125-ab6b-91d977ecf85b",
    "actor_id": "e0e788c4-2b10-4375-86f6-1726b0c274a1",
    "user_id": "041ab13d-f419-4412-9670-ed0339b919ed",
    "timestamp": "2023-01-11T16:13:35+03:00",
    "action": "ADDED_BLOCKING_REASON",
    "reason": "тгошьлбд"
  },
  {
    "id": "cecf645a-ee70-42b9-9d5a-5a5dc9255a7f",
    "tenant_id": "01068ade-1cce-4125-ab6b-91d977ecf85b",
    "actor_id": "e0e788c4-2b10-4375-86f6-1726b0c274a1",
    "user_id": "041ab13d-f419-4412-9670-ed0339b919ed",
    "timestamp": "2023-01-11T16:20:34+03:00",
    "action": "USER_UNBLOCKED"
  },
  {
    "id": "949780fb-2578-49d9-9a20-aecdc8544a0a",
    "tenant_id": "01068ade-1cce-4125-ab6b-91d977ecf85b",
    "actor_id": "e0e788c4-2b10-4375-86f6-1726b0c274a1",
    "user_id": "041ab13d-f419-4412-9670-ed0339b919ed",
    "timestamp": "2023-01-11T16:20:52+03:00",
    "action": "USER_BLOCKED"
  },
```

```
    {
      "id": "652cd651-b9bd-4fbd-bf91-5e8918b9fd14",
      "tenant_id": "01068ade-1cce-4125-ab6b-91d977ecf85b",
      "actor_id": "e0e788c4-2b10-4375-86f6-1726b0c274a1",
      "user_id": "041ab13d-f419-4412-9670-ed0339b919ed",
      "timestamp": "2023-01-11T16:20:53+03:00",
      "action": "ADDED_BLOCKING_REASON",
      "reason": "уамуамк"
    },
    {
      "id": "d8359c94-eeb3-40d7-8dbd-0a6ef669a074",
      "tenant_id": "01068ade-1cce-4125-ab6b-91d977ecf85b",
      "actor_id": "e0e788c4-2b10-4375-86f6-1726b0c274a1",
      "user_id": "041ab13d-f419-4412-9670-ed0339b919ed",
      "timestamp": "2023-01-11T16:21:58+03:00",
      "action": "USER_UNBLOCKED"
    },
    {
      "id": "f7ef3298-f455-4ddf-9359-d1e9a1485434",
      "tenant_id": "01068ade-1cce-4125-ab6b-91d977ecf85b",
      "actor_id": "e0e788c4-2b10-4375-86f6-1726b0c274a1",
      "user_id": "041ab13d-f419-4412-9670-ed0339b919ed",
      "timestamp": "2023-01-11T16:51:08+03:00",
      "action": "USER_BLOCKED"
    },
    {
      "id": "bd6d8af9-766d-4734-999f-b1238d84fc3e",
      "tenant_id": "01068ade-1cce-4125-ab6b-91d977ecf85b",
      "actor_id": "e0e788c4-2b10-4375-86f6-1726b0c274a1",
      "user_id": "041ab13d-f419-4412-9670-ed0339b919ed",
      "timestamp": "2023-01-11T16:51:10+03:00",
      "action": "ADDED_BLOCKING_REASON",
      "reason": "7890"
    }
  ]
}
```


7.29 Работа с корпоративными подписями

С помощью расширенного администрирования можно работать с корпоративными подписями всех пользователей в тенанте, конкретного пользователя или группы пользователей в рамках тенанта:

– создать корпоративную подпись, которая будет отображаться в перечне подписей;

– установить созданную корпоративную подпись как подпись по умолчанию;

– удалить подпись.

В а ж н о – Работа с подписями выполняется пользователем с ролью администратора тенанта.

Для создания корпоративной подписи необходимо выполнить следующие действия:

1. Подготовить файл подписи в формате HTML. Пример содержания такого файла:

```
<!DOCTYPE html>
<html>
<head>
</head>
<body>
<p>С уважением,</p>
<p><b>#full_fio#,</b>
<p><b>#department#,</b></p>
<p><b>тел.</b></p><p><b>#person_phone#</b></p>
<img src="http:///uploads/posts/2021-09/1631898903_20-risunok.jpg"/>
</body>
</html>
```

где #full_fio# – фамилия, имя, отчество пользователя (можно указать параметр #fio# – фамилия и инициалы), #department# – структурное подразделение, #title# – должность пользователя, #person_phone# – номер телефона.

В а ж н о – При добавлении изображения к подписи необходимо учитывать: изображение может быть добавлено как URL-адрес или путь к файлу на ПК администратора тенанта; ограничение размера изображения – не более 60 КБ.

2. Выполнить запрос на создание подписи для пользователей в рамках тенанта:

```
nct_ministerium apply_signature_template \
--admin.login <…>
--admin.password <…>
--signature_name <…>
--signature_is_default=true
--template_path /home/user/подпись.html
--source.tenant=false
--source.emails x@example.net
--tenant_id <…>
--cox.balancer_endpoint=hydra.ucs-apps-1.installation.example.net:50053 \
--cox.compression=none
--cox.endpoint=grpc-installation.example.net:3142 \
--cox.load_balanced=false
--cox.request_timeout=10s
--cox.service_name=cox
--cox.use_tls=true
--cox.use_tls_balancer=false
--tls_settings.ca_file /home/user/ca.pem
--tls_settings.client_cert_file/home/user/client_crt.pem
--tls_settings.key_file/home/home/user/client_key.pem
```

Описание параметров запроса приведено в таблице 163.

Таблица 163 – Описание параметров запроса на создание подписи

Параметр	Тип	Обязательный	Описание
admin.login	Str	+	Логин администратора тенанта

Параметр	Тип	Обязательный	Описание
admin.password	Str	+	Пароль администратора тенанта
signature_name	Str	+	Название подписи
signature_is_default	Bool	+	При значении **true** созданная подпись применяется как подпись по умолчанию. При значении **false** подпись создастся и добавится в перечень подписей, но не будет применена как подпись по умолчанию
template_path	Str	+	Путь к файлу подписи
source.tenant	Bool	+	При значении **true** созданная подпись применится для всех пользователей тенанта. При значении **false** созданная подпись предусматривается как подпись для конкретных пользователей или группы пользователей, их нужно указать в параметре **source.emails**
source.emails	Str	-	Email или email-ы пользователя или группы пользователей, для которых создается подпись. Если **source.tenant=false**, то параметр **source.emails** необходимо указать в запросе. Возможен также вариант указания только параметра **source.emails**, без использования параметра **source.tenant** в запросе. Email-ы необходимо указывать через запятую, без пробела.
tenant_id	Str	+	Идентификатор тенанта
cox.balancer_endpoint	Str	+	Endpoint балансировщика нагрузки сервиса
cox.compression	Str	+	Метод сжатия данных (варианты: **none**, **gzip**), по умолчанию **none**
cox.endpoint	Str	+	Endpoint сервиса
cox.load_balanced	Bool	+	Балансировщик нагрузки сервиса
cox.request_timeout	Str	+	Тайм-аут запроса к сервису
cox.service_name	Str	+	Имя сервиса
cox.use_tls	Bool	+	TLS-сертификат
cox.use_tls_balancer	Bool	+	Защищенная передача данных при подключении к балансировщику
tls_settings.ca_file	Str	+	Путь к CA файлу

Параметр	Тип	Обязательный	Описание
tls_settings.client_cert_file	Str	+	Путь к файлу сертификата клиента
tls_settings.key_file	Str	+	Путь к файлу с ключом клиента

Пример ответа:

```
{
  "Response": {
    "changed": true,
    "failed": false,
    "msg": "ok"
  },
  "success_user_count": 16
}
```

Если у пользователя отсутствуют некоторые данные для подготовки файла подписи (например, не заполнен телефон), то при просмотре подписи данное поле останется пустым. Администратору тенанта в ответе на команду отобразится поле **incomplete_users**, где в поле **missing_variables** будет приведен список переменных в файле подписи, которые остались незаполненными. Пример такого ответа:

```
{
  "Response": {
    "changed": true,
    "failed": false,
    "msg": "ok"
  },
  "incomplete_users": [
    {
      "id": "some_user_uuid",
      "email": "test@example.com"
      "missing_variables": [
        "department",
        "title",
        "person_phone"
      ]
    }
  ]
```

В случае ошибки добавления подписи для одного или нескольких пользователей, команда добавит подписи для всех, кроме ошибочных. Для последних в ответе отобразится поле **entities_with_errors**, где будет приведен список пользователей или групп пользователей с ошибкой добавления, содержащий идентификатор, тип (пользователь или группа), email и причину ошибки.

Пример такого ответа:

```
{
  "Response": {
    "changed": true,
```

```
    "failed": false,
    "msg": "ok"
  },
  "entities_with_errors": [
    {
      "id": "some_user_uuid",
      "mail": "test@example.com"
      "type": "user",
      "why": "user has no settings"
    }
  ]
```


где поле **why** обозначает причину ошибки. Значения могут быть следующие:

- user has no settings – пользователь или группа пользователей есть в базе данных как объект, но настроек в базе данных нет;
- no entity found with this email – если указан параметр **source.emails** и по заданному email пользователь или группа пользователей не были найдены;
- is inactive – пользователь или группа пользователей не активны;
- signature already exist – подпись с таким названием уже существует;
- max signatures count exceeded – у пользователя или группы пользователей достигнут лимит подписей;
- error getting group members – внутренняя ошибка получения пользователей из группы по email-у группы;
- internal error – неизвестная внутренняя ошибка, информация о ней может находиться в записях журналов работы системы.

Корпоративную подпись также можно удалить. Для этого необходимо выполнить запрос:

```
nct_ministerium delete_users_signature
--admin.login <…>
--admin.password <…>
--signature_name <…>
--tenant_id <…>
--source.tenant=false
--source.emails x@example.net
--cox.balancer_endpoint=hydra.ucs-apps-1.installation.example.net:50053
--cox.compression=none
--cox.endpoint=grpc-installation.example.net:3142
--cox.load_balanced=false
--cox.request_timeout=10s
--cox.service_name=cox
--cox.use_tls=true
--cox.use_tls_balancer=false
--tls_settings.ca_file /home/user/ca.pem
--tls_settings.client_cert_file/home/user/client_crt.pem
--tls_settings.key_file/home/home/user/client_key.pem
```

Описание параметров запроса приведено в таблице 164.

Таблица 164 – Описание параметров запроса на удаление подписи

Параметр	Тип	Обязательный	Описание
admin.login	Str	+	Логин администратора тенанта
admin.password	Str	+	Пароль администратора тенанта
signature_name	Str	+	Название подписи
template_path	Str	+	Путь к файлу подписи
tenant_id	Str	+	Идентификатор тенанта
source.tenant	Bool	+	При значении **true** созданная подпись применится для всех пользователей тенанта. При значении **false** созданная подпись предусматривается как подпись для конкретных пользователей или группы пользователей, их нужно указать в параметре **source.emails**
source.emails	Str	-	Email пользователя или группы пользователей, для которых создается подпись. Если **source.tenant=false**, то параметр **source.emails** необходимо указать в запросе. Возможен также вариант указания только параметра **source.emails**, без использования параметра **source.tenant** в запросе. Email-ы необходимо указывать через запятую, без пробела.
cox.balancer_endpoint	Str	+	Endpoint балансировщика нагрузки сервиса
cox.compression	Str	+	Метод сжатия данных (варианты: **none**, **gzip**), по умолчанию **none**
cox.endpoint	Str	+	Endpoint сервиса
cox.load_balanced	Bool	+	Балансировщик нагрузки сервиса
cox.request_timeout	Str	+	Тайм-аут запроса к сервису
cox.service_name	Str	+	Имя сервиса
cox.use_tls	Bool	+	TLS-сертификат
cox.use_tls_balancer	Bool	+	Защищенная передача данных при подключении к балансировщику
tls_settings.ca_file	Str	+	Путь к CA файлу
tls_settings.client_cert_file	Str	+	Путь к файлу сертификата клиента

Параметр	Тип	Обязательный	Описание
tls_settings.key_file	Str	+	Путь к файлу с ключом клиента

Пример ответа:

```
{
  "Response": {
    "changed": true,
    "failed": false,
    "msg": "ok"
  },
  "success_user_count": 1
}
```

7.30 Работа с черными и белыми списками отправителей

С помощью расширенного администрирования можно работать с черными и белыми списками отправителей: добавлять и удалять пользователей, обновлять перечень пользователей в списках. Таким образом, пользователь будет получать письма от отправителей из белого списка, а письма, отправленные пользователями из черного списка, буду направляться в папку **Корзина**.

В а ж н о – Работа с черными и белыми списками отправителей выполняется пользователем с ролью администратора тенанта.

Чтобы получить черный или белый список отправителей, необходимо выполнить запрос:

```
nct-ministerium get_senders \
--config <path to config> \
--admin.login <...> \
--admin.password <...> \
--tenant_id <...>
```

Описание параметров запроса приведено в таблице 165.

Таблица 165 – Описание параметров запроса на добавление отправителей в список

Параметр	Тип	Обязательный	Описание
config	Str	+	Конфигурационный файл с параметрами сервиса Cox и настройками tls. Формируется автоматически на сервере с ролью ucs_infrastructure и находится по пути /srv/ministerium/config.json

Параметр	Тип	Обязательный	Описание
admin.login	Str	+	Логин администратора тенанта
admin.password	Str	+	Пароль администратора тенанта
tenant_id	Str	+	Идентификатор тенанта

Пример ответа:

```
{
  "Response": {
    "changed": false,
    "failed": false,
    "msg": "ok"
  },
  "senders": [
    {
      "tenant_id": "…",
      "address": "…",
      "status": 1
    },
    {
      "tenant_id": "…",
      "address": "…",
      "status": 1
    },
    {
      "tenant_id": "…",
      "address": "…",
      "status": 2
    },
    {
      "tenant_id": "…",
      "address": "…",
      "status": 2
    }
    ...
  ]
}
```

7.30.1 Добавление отправителей в список

Чтобы добавить отправителей в черный или белый список, необходимо выполнить запрос:

```
nct-ministerium add_sender \
--config <path to config> \
--admin.login <...> \
--admin.password <...> \
--tenant_id <...> \
--address <...> \
--status <BLACKLIST>
```

Описание параметров запроса приведено в таблице 166.

Таблица 166 – Описание параметров запроса на добавление отправителей в список

Параметр	Тип	Обязательный	Описание
config	Str	+	Конфигурационный файл с параметрами сервиса Cox и настройками tls. Формируется автоматически на сервере с ролью ucs_infrastructure и находится по пути /srv/ministerium/config.json
admin.login	Str	+	Логин администратора тенанта
admin.password	Str	+	Пароль администратора тенанта
tenant_id	Str	+	Идентификатор тенанта
address	Str	+	Email или домен отправителей, которых необходимо добавить в список
status	Str	+	Статус отправителя: WHITELIST (белый список) или BLACKLIST (черный список)

Пример ответа:

```
{
  "Response": {
    "changed": true,
    "msg": "ok"
  }
```

Чтобы проверить наличие отправителя в списке, необходимо выполнить запрос на проверку:

```
nct-ministerium check_email \
--config <path to config> \
--admin.login <...> \
--admin.password <...> \
--tenant_id <...> \
--email <...>
```

Описание параметров запроса приведено в таблице 167.

Таблица 167 – Описание параметров запроса на проверку отправителей

Параметр	Тип	Обязательный	Описание
config	Str	+	Конфигурационный файл с параметрами сервиса Cox и настройками tls. Формируется автоматически на сервере с ролью ucs_infrastructure и находится по пути /srv/ministerium/config.json
admin.login	Str	+	Логин администратора тенанта

Параметр	Тип	Обязательный	Описание
admin.password	Str	+	Пароль администратора тенанта
tenant_id	Str	+	Идентификатор тенанта
email	Str	+	Основной электронный адрес

Пример ответа:

```
{
  "Response": {
    "changed": false,
    "failed": false,
    "msg": "ok"
  },
  "email_list": 2
}
```

7.30.2 Обновление списка отправителей

Чтобы обновить отправителей в списках, необходимо выполнить запрос:

```
nct-ministerium update_sender \
--config <path to config> \
--admin.login <...> \
--admin.password <...> \
--tenant_id <...> \
--address <...> \
--status <BLACKLIST>
```

Описание параметров запроса приведено в таблице 168.

Таблица 168 – Описание параметров запроса на обновление списка пользователей

Параметр	Тип	Обязательный	Описание
config	Str	+	Конфигурационный файл с параметрами сервиса Cox и настройками tls. Формируется автоматически на сервере с ролью ucs_infrastructure и находится по пути /srv/ministerium/config.json
admin.login	Str	+	Логин администратора тенанта
admin.password	Str	+	Пароль администратора тенанта
tenant_id	Str	+	Идентификатор тенанта
address	Str	+	Email или домен отправителей, которых необходимо добавить в список
status	Str	+	Статус отправителя: WHITELIST (белый список) или BLACKLIST (черный список)

Пример ответа:

```
{
  "Response": {
    "changed": true,
    "msg": "ok"
  }
```

Чтобы проверить наличие вновь добавленных отправителей в списке, необходимо выполнить проверку с помощью команды **check_email**, описанной в разделе 7.30.1.

7.30.3 Удаление отправителей из списка

Чтобы удалить отправителей из списков, необходимо выполнить запрос:

```
nct-ministerium delete_sender \
--config <path to config> \
--admin.login <...> \
--admin.password <...> \
--tenant_id <...> \
--address <...>
```

Описание параметров запроса приведено в таблице 169.

Таблица 169 – Описание параметров запроса на удаление отправителей в списках

Параметр	Тип	Обязательный	Описание
config	Str	+	Конфигурационный файл с параметрами сервиса Cox и настройками tls. Формируется автоматически на сервере с ролью ucs_infrastructure и находится по пути /srv/ministerium/config.json
admin.login	Str	+	Логин администратора тенанта
admin.password	Str	+	Пароль администратора тенанта
tenant_id	Str	+	Идентификатор тенанта
address	Str	+	Email или домен отправителей, которых необходимо добавить в список

Пример ответа:

```
{
  "Response": {
    "changed": true,
    "msg": "ok"
  }
```

Чтобы проверить наличие вновь добавленных отправителей в списке, необходимо выполнить проверку с помощью команды **check_email**, описанной в разделе 7.30.1.

8 СОПОСТАВЛЕНИЕ LDAP АТРИБУТОВ КАТАЛОГА

Для доменов, у которых настроена делегация на внешний LDAP каталог, может быть также настроено сопоставление атрибутов LDAP каталога на поля/атрибуты сущностей в каталоге Mailion. Такое отображение называется маппингом атрибутов. Домен делегируется на одно из подключений к внешнему LDAP каталогу, которое настраивается в конфигурации сервиса Orpheus. Также в сервисе Orpheus есть настройка маппингов по умолчанию, и каждое соединение с внешним каталогом в обязательном порядке имеет ссылку на маппинг по умолчанию. Имя маппинга по умолчанию может иметь произвольное значение, но обычно совпадает с именем каталога, на которое рассчитан этот маппинг: AD, OpenLDAP, FreeIPA, SambaDC, ALDPRO или REDADM. Маппинг по умолчанию можно переопределить через команды утилиты **nct_ministerium**, описанные далее. Можно задать другой маппинг по умолчанию (MAPPING_TYPE_PRESET) или загрузить полностью новый маппинг из файла для отдельного домена. Маппинги по умолчанию можно выгрузить в файл, отредактировать и загрузить как уникальный маппинг (MAPPING_TYPE_CUSTOM).

Чтобы подключиться к внешним каталогам, необходимо выполнить сопоставление данных, или маппинг данных. Сопоставление (маппинг) данных – это выстраивание соотношений между моделями данных, которые находятся в разных источниках или системах. В записи данные содержатся в парах атрибут-значение. Каждый атрибут имеет имя (или короткую форму имени) и принадлежит одному или нескольким объектным классам, то есть входит в их состав.

Маппинг LDAP атрибутов внешнего каталога и каталога ПО «Mailion» настраивается для доменов, делегированных на внешний LDAP каталог. Для каждого делегированного домена может быть настроен свой маппинг.

Маппинг необходимо настроить самостоятельно через файл (см. раздел 8.1) и передать с помощью команд (см. раздел 8.2).

8.1 Настройка маппинга через файл

Для упрощения работы и быстрого выполнения маппинга можно выполнить его настройку через файл-шаблон, доступный для любого внешнего каталога. Путь до этого файла передается в любую из команд (см. раздел 8.2), которая поддерживает добавление маппинга, и маппинг подтянется из этого файла.

Чтобы получить шаблон файла, необходимо выполнить запрос:

```
nct_ministerium get_default_ldap_attribute_mappings
--output_filepath AD.json
--preset_name AD
--admin.login <...>
--admin.password <...>
--cox.balancer_endpoint=hydra.ucs-apps-1.installation.example.net:50053
--cox.compression=none
--cox.endpoint=grpc-installation.example.net:3142
--cox.load_balanced=false
--cox.request_timeout=10s
--cox.service_name=cox
--cox.use_tls=true
--cox.use_tls_balancer=false
--tls_settings.ca_file ...
--tls_settings.client_cert_file ...
--tls_settings.key_file ...
```

Описание параметров запроса приведено в таблице 170.

Таблица 170 – Описание параметров запроса на получение файла-шаблона для маппинга

Параметр	Тип	Обязательный	Описание
output_filepath	Str	+	Путь до файла-шаблона для маппинга
preset_name	Str	+	Имя шаблона маппинга для необходимого каталога. Например, AD
admin.login	Str	+	Логин администратора
admin.password	Str	+	Пароль администратора
cox.balancer_endpoint	Str	+	Endpoint балансировщика нагрузки сервиса
cox.compression	Str	+	Метод сжатия данных (варианты: **none**, **gzip**), по умолчанию **none**
cox.endpoint	Str	+	Endpoint сервиса
cox.load_balanced	Bool	+	Балансировщик нагрузки сервиса
cox.request_timeout	Str	+	Тайм-аут запроса к сервису
cox.service_name	Str	+	Имя сервиса

Параметр	Тип	Обязательный	Описание
cox.use_tls	Bool	+	TLS-сертификат
cox.use_tls_balancer	Bool	+	Защищенная передача данных при подключении к балансировщику
tls_settings.ca_file	Str	+	Путь к CA файлу
tls_settings.client_cert_file	Str	+	Путь к файлу сертификата клиента
tls_settings.key_file	Str	+	Путь к файлу с ключом клиента

После этого необходимо открыть файл AD.json, в котором выполнить настройку полей. Пример данного файла:

```
{
  "attributes_mapping": {
    "avatar": "thumbnailPhoto",
    "department": "department",
    "first_name": "givenName",
    "first_name_alt": "givenName",
    "group_description": "description",
    "group_name": "displayName",
    "last_changed": "whenChanged",
    "last_name": "sn",
    "last_name_alt": "sn",
    "locale": "localeID",
    "login": "sAMAccountName",
    "mail": "mail",
    "middle_name": "middleName",
    "middle_name_alt": "middleName",
    "phone_number_work": "telephoneNumber",
    "principal_name": "userPrincipalName",
    "status": "userAccountControl",
    "title": "title"
  },
       "search_filter_user":    "(&(&(objectCategory=person)(objectClass=user))(|
(givenName={{.Name}}*)(sn={{.Name}}*)(middleName={{.Name}}*)
(sAMAccountName={{.Name}}*)(mail={{.Name}}*)))",
   "search_filter_group":  "(&(&(objectCategory=group)(|(groupType=8)(groupType=-
2147483646)(groupType=-2147483640))(mail=*)(!(msExchHideFromAddressLists=TRUE)))
(|(displayName={{.Name}}*)(description={{.Name}}*)(mail={{.Name}}*)))",
    "search_filter_resource":  "(&(|(msExchResourceMetaData=ResourceType:Room))(|
(givenName={{.Name}}*)(sn={{.Name}}*)(middleName={{.Name}}*)
(sAMAccountName={{.Name}}*)(mail={{.Name}}*)))",
           "search_filter_exact_user_by_name":      "(&(&(objectCategory=person)
(objectClass=user))(sAMAccountName={{.Name}}))",
          "search_filter_exact_user_by_email":      "(&(&(objectCategory=person)
(objectClass=user))(mail={{.Email}}))"
}
```

Описание параметров поля **attributes_mapping** приведено в таблице 171.

Таблица 171 – Описание параметров запроса на получение файла-шаблона для маппинга

Значение для ПО «Mailion»	Значение для AD	Описание атрибута
avatar	thumbnailPhoto	Фотография пользователя
department	department	Отдел пользователя
first_name	givenName	Имя пользователя
first_name_alt	givenName	Имя пользователя, если задано, имеет приоритет над first_name
group_description	description	Описание группы
group_name	displayName	Имя группы
last_changed	whenChanged	Время последнего изменения
last_name	sn	Фамилия пользователя
last_name_alt	sn	Фамилия пользователя, если задано, имеет приоритет над last_name
locale	localeID	Язык
login	sAMAccountName	Логин пользователя
mail	mail	Email пользователя
middle_name	middleName	Отчество пользователя
middle_name_alt	middleName	Отчество пользователя, если задано, имеет приоритет над middle_name
phone_number_work	telephoneNumber	Рабочий телефон пользователя
principal_name	userPrincipalName	Имя принципала. Принципал – сущность, заведенная в каталоге. Имя используется как логин, который нельзя изменять. Этот атрибут – особенность AD, но также присутствует во FreeIPA
status	userAccountControl	Статус пользователя
title	title	Должность пользователя

Описание полей фильтров:

1. **SearchFilterUser** – шаблон для LDAP-фильтра, с помощью которого будет производиться поиск пользователя во внешнем каталоге. С его помощью можно понять, как искать того или иного пользователя. Доступные переменные шаблона:
   – {{.Name}} – имя пользователя;
   – {{.Email}} – Email пользователя.

2. **SearchFilterGroup** – шаблон для LDAP-фильтра, с помощью которого будет производиться поиск группы во внешнем каталоге. Доступные переменные шаблона:
   – {{.Name}} – имя группы;
   – {{.Email}} – Email группы.
3. **SearchFilterResource** – шаблон для LDAP-фильтра, с помощью которого будет производиться поиск ресурса во внешнем каталоге. Доступные переменные шаблона:
   – {{.Name}} – имя ресурса;
   – {{.Email}} – Email ресурса.
4. **SearchFilterExactUserByName** – шаблон для LDAP-фильтра, с помощью которого будет производиться точный поиск пользователя по имени во внешнем каталоге. Доступные переменные шаблона:
   – {{.Name}} – имя пользователя.
5. **SearchFilterExactUserByEmail** – шаблон для LDAP-фильтра, с помощью которого будет производиться точный поиск пользователя по почтовому адресу во внешнем каталоге. Доступные переменные шаблона:
   – {{.Email}} – Email пользователя.
6. **SearchFilterById** – шаблон для LDAP-фильтра, с помощью которого будет производиться точный поиск пользователя по идентификатору во внешнем каталоге. Доступные переменные шаблона:
   – {{.ID}} – идентификатор пользователя.

8.2 Добавление маппинга через команды

Управление маппингом LDAP атрибутов осуществляется с помощью команд расширенного администрирования (см. раздел 7):

- **create_domain** – создание домена (см. раздел 8.2.1). Если в этом запросе добавляется делегирование домена, то можно сразу же задать маппинг.
- **add_domain_delegation** – добавление делегированного на внешний LDAP каталог домена (см. раздел 8.2.2).
- **update_domain_delegation** – обновление делегации домена (см. раздел 8.2.3).

– **set_same_domain_delegation** – обновление делегации домена (см. раздел 8.2.4).

В а ж н о – Для команд **add_domain_delegation** и **update_domain_delegation** опция для задания файла будет **--delegation.ldap_attributes_mapping.custom_from_file**.

8.2.1 Добавление маппинга при создании домена

Для добавления маппинга через команду создания домена необходимо выполнить запрос:

```
nct_ministerium create_domain
--tenant_id <...>
--hostname <...>
--external.default_region_id <...>
--external.delegate_id <...>
--external.domain_alias <...>
--external.domain_auth_name <...>
--external.domain_short_name <...>
--external.is_sync_enabled=true \
--external.ldap_attributes_mapping.custom_from_file "AD.json"
--features.is_authorization=true
--features.is_mail=true
--features.is_service=true
--is_prioritized=false
--admin.login <...>
--admin.password <...>
--cox.balancer_endpoint=hydra.ucs-apps-1.installation.example.net:50053
--cox.compression=none
--cox.endpoint=grpc-installation.example.net:3142
--cox.load_balanced=false
--cox.request_timeout=10s
--cox.service_name=cox
--cox.use_tls=true
--cox.use_tls_balancer=false
--tls_settings.ca_file ...
--tls_settings.client_cert_file ...
--tls_settings.key_file ...
```

Описание параметров запроса приведено в таблице 172.

Таблица 172 – Описание параметров запроса на создание домена

Параметр	Тип	Обязательный	Описание
--admin.login	string	+	Логин администратора
--admin.password	string	+	Пароль администратора
--cox.balancer_endpoint	string	+	Endpoint балансировщика нагрузки сервиса

Параметр	Тип	Обязательный	Описание
--cox.compression	string	+	Использование метода компрессии при соединении с сервисом: **none** (по умолчанию), **gzip**
--cox.endpoint	string	+	Endpoint для непосредственного соединения с сервисом
--cox.load_balanced	boolean	+	Использовать соединение с балансировщиком
--cox.request_timeout	duration	+	Тайм-аут запроса к сервису (по умолчанию 2 секунды)
--cox.service_name	string	+	Имя сервиса в балансировщике
--cox.use_tls	boolean	+	Использование TLS-сертификата
--cox.use_tls_balancer	boolean	+	Использование TLS-сертификата при соединении с балансировщиком
--external.auth_domains	strings	+	Список доменов авторизации для внешнего почтового домена
--external.default_region_id	string	-	Идентификатор региона по умолчанию для автоматического создания пользователей
--external.delegate_id	string	+	Идентификатор для использования при внешней авторизации
--external.delegation_catalog_type	int32	+	Если в качестве **mapping_type** установлено значение **MAPPING_TYPE_PRESET**, то используется готовый пресет исходя из следующего списка: **1** – ACTIVE_DIRECTORY, **2** – FREE_IPA, **3** – SAMBA_DC, **4** – RED_ADM, **5** – ALD_PRO
--external.domain_alias	string	+	Имя контроллера внешнего домена
--external.domain_auth_name	string	+	Длинная запись домена аутентификации
--external.domain_short_name	string	+	Краткая запись домена аутентификации

Параметр	Тип	Обязательный	Описание
--external.is_sync_enabled	boolean	+	Включение/отключение синхронизации с внешним доменом. Если значение **false**, то выключена. Если значение **true**, то включена
--external.ldap_attributes_ mapping.custom_from_file	string	-	Имя файла для загрузки пользовательского маппинга атрибутов. Если задано, другие атрибуты игнорируются
--external.ldap_attributes_ mapping.mapping	strings	+	Список атрибутов. Формат: `key1=value1,key2=value2,...` Где `key` – атрибут Mailion, `value` – внешний атрибут
--external.ldap_attributes_ mapping.mapping_type	string	+	Тип маппинга. Доступные значения: **MAPPING_TYPE_PRESET** (маппинг с помощью шаблона), **MAPPING_TYPE_CUSTOM** (маппинг, который необходимо заполнить самостоятельно)
--external.ldap_attributes_ mapping.search_filter_by_id	string	+	Фильтр шаблона LDAP для поиска объектов по идентификатору во внешнем каталоге. Пример: `(&(ipaUniqueID={{.ID}}))`
--external.ldap_attributes_ mapping.search_filter_exact_ user_by_email	string	+	Фильтр шаблона LDAP для точного поиска пользователей по почтовому адресу во внешнем каталоге. Пример: `(&(&(objectCategory=person) (objectClass=user)) (mail={{.Email}}))`
--external.ldap_attributes_ mapping.search_filter_exact_ user_by_name	string	+	Фильтр шаблона LDAP для точного поиска пользователей по имени во внешнем каталоге. Пример: `(&(&(objectCategory=person) (objectClass=user)) (sAMAccountName={{.Name}}))`
--external.ldap_attributes_ mapping.search_filter_group	string	+	Фильтр шаблона LDAP для поиска групп во внешнем

Параметр	Тип	Обязательный	Описание
			каталоге. Пример: `(&(&(objectCategory=group)(|(groupType=8)(groupType=-2147483646)(groupType=-2147483640))(mail=*)(!(msExchHideFromAddressLists=TRUE)))(|(displayName={{.Name}}*)(description={{.Name}}*)(mail={{.Name}}*)))`
--external.ldap_attributes_mapping.search_filter_resource	string	+	Фильтр шаблона LDAP для поиска ресурсов во внешнем каталоге. Пример: `(&(|(msExchResourceMetaData=ResourceType:Room))(|(extensionAttribute2={{.Name}}*)(extensionAttribute1={{.Name}}*)(givenName={{.Name}}*)(sn={{.Name}}*)(extensionAttribute3={{.Name}}*)(sAMAccountName={{.Name}}*)(mail={{.Name}}*)))`
--external.ldap_attributes_mapping.search_filter_user	string	+	Фильтр шаблона LDAP для поиска пользователей во внешнем каталоге. Пример: `(&(&(objectCategory=person)(objectClass=user))(|(extensionAttribute2={{.Name}}*)(extensionAttribute1={{.Name}}*)(givenName={{.Name}}*)(sn={{.Name}}*)(extensionAttribute3={{.Name}}*)(sAMAccountName={{.Name}}*)(mail={{.Name}}*)))`
--features.is_authorization	boolean	+	Домен может быть использован при авторизации
--features.is_mail	boolean	+	Если значение **true**, домен может принимать почтовые сообщения

Параметр	Тип	Обязательный	Описание
--features.is_saml	boolean	+	Если значение **true**, домен можно использовать для авторизации
--features.is_service	boolean	+	Если значение **true**, домен можно использовать для авторизации по умолчанию
--hostname	string	+	Имя домена
--is_prioritized	boolean	+	Приоретизированный домен
--tenant_id	string	+	Идентификатор тенанта
--tls_settings.ca_file	string	+	Путь к файлу CA
--tls_settings.client_cert_file	string	+	Путь к файлу сертификата клиента
--tls_settings.key_file	String	+	Путь к файлу ключа клиента
--token-name	string	+	Имя токена

После использования данного метода маппинг добавится из файла AD.json и сохранится в домене.

8.2.2 Добавление маппинга при настройке делегации домена

Для добавления маппинга при настройке делегированного на внешний LDAP каталог домена необходимо выполнить запрос:

```
nct_ministerium add_domain_delegation
--admin.login <...>
--admin.password <...>
--domain_id <...>
--delegation.default_region_id <...>
--delegation.delegate_id <...>
--delegation.domain_alias <...>
--delegation.is_sync_enabled=TRUE
--delegation.ldap_attributes_mapping.mapping_type=MAPPING_TYPE_PRESET
--delegation.ldap_attributes_mapping.mapping_preset_name=AD
--external.delegation.ldap_attributes_mapping.mapping_preset_name=AD
--cox.balancer_endpoint=hydra.ucs-apps-1.installation.example.net:50053
--cox.compression=none
--cox.endpoint=grpc-installation.example.net:3142
--cox.load_balanced=false
--cox.request_timeout=10s
--cox.service_name=cox
--cox.use_tls=true
--cox.use_tls_balancer=false
--tls_settings.ca_file ...
--tls_settings.client_cert_file ...
--tls_settings.key_file ...
```

Описание параметров запроса приведено в таблице 173.

Таблица 173 – Описание параметров запроса на создание домена

Параметр	Тип	Обязательный	Описание
--admin.login	string	+	Логин администратора
--admin.password	string	+	Пароль администратора
--cox.balancer_endpoint	string	+	Endpoint балансировщика нагрузки сервиса
--cox.compression	string	+	Использование метода компрессии при соединении с сервисом: **none** (по умолчанию), **gzip**
--cox.endpoint	string	+	Endpoint для непосредственного соединения с сервисом
--cox.load_balanced	boolean	+	Использовать соединение с балансировщиком
--cox.request_timeout	duration	+	Тайм-аут запроса к сервису (по умолчанию 2 секунды)
--cox.service_name	string	+	Имя сервиса в балансировщике
--cox.use_tls	boolean	+	Использование TLS-сертификата
--cox.use_tls_balancer	boolean	+	Использование TLS-сертификата при соединении с балансировщиком
--delegation.auth_domains	strings	+	Список доменов авторизации для внешнего почтового домена
--delegation.default_region_id	string	-	Идентификатор региона по умолчанию для автоматического создания пользователей
--delegation.delegate_id	string	+	Идентификатор для использования при внешней авторизации
--delegation.delegation_catalog_type	int32	+	Если в качестве **mapping_type** установлено значение **MAPPING_TYPE_PRESET**, то используется готовый пресет исходя из следующего списка: **1** – ACTIVE_DIRECTORY, **2** – FREE_IPA, **3** – SAMBA_DC,

Параметр	Тип	Обязательный	Описание
			4 – RED_ADM, **5** – ALD_PRO
--delegation.domain_alias	string	+	Имя контроллера внешнего домена
--delegation.domain_auth_name	string	+	Длинная запись домена аутентификации
--delegation.domain_short_name	string	+	Краткая запись домена аутентификации
--delegation.is_sync_enabled	boolean	+	Включение/отключение синхронизации с внешним доменом. Если значение **false**, то выключена. Если значение **true**, то включена
--delegation.ldap_attributes_mapping.custom_from_file	string	-	Имя файла для загрузки пользовательского маппинга атрибутов. Если задано, другие атрибуты игнорируются
--delegation.ldap_attributes_mapping.mapping	strings	+	Список атрибутов. Формат: `key1=value1,key2=value2,...` Где `key` – атрибут Mailion, `value` – внешний атрибут
--delegation.ldap_attributes_mapping.mapping_type	string	+	Тип маппинга. Доступные значения: **MAPPING_TYPE_PRESET** (маппинг с помощью шаблона), **MAPPING_TYPE_CUSTOM** (маппинг, который необходимо заполнить самостоятельно)
--delegation.ldap_attributes_mapping.search_filter_by_id	string	+	Фильтр шаблона LDAP для поиска объектов по идентификатору во внешнем каталоге. Пример: `(&(ipaUniqueID={{.ID}}))`
--delegation.ldap_attributes_mapping.search_filter_exact_user_by_email	string	+	Фильтр шаблона LDAP для точного поиска пользователей по почтовому адресу во внешнем каталоге. Пример: `(&(&(objectCategory=person)`

Параметр	Тип	Обязательный	Описание
			`(objectClass=user))(mail={{.Email}}))`
--delegation.ldap_attributes_mapping.search_filter_exact_user_by_name	string	+	Фильтр шаблона LDAP для точного поиска пользователей по имени во внешнем каталоге. Пример: `(&(&(objectCategory=person)(objectClass=user))(sAMAccountName={{.Name}}))`
--delegation.ldap_attributes_mapping.search_filter_group	string	+	Фильтр шаблона LDAP для поиска групп во внешнем каталоге. Пример: `(&(&(objectCategory=group)(|(groupType=8)(groupType=-2147483646)(groupType=-2147483640))(mail=*)(!(msExchHideFromAddressLists=TRUE)))(|(displayName={{.Name}}*)(description={{.Name}}*)(mail={{.Name}}*)))`
--delegation.ldap_attributes_mapping.search_filter_resource	string	+	Фильтр шаблона LDAP для поиска ресурсов во внешнем каталоге. Пример: `(&(|(msExchResourceMetaData=ResourceType:Room))(|(extensionAttribute2={{.Name}}*)(extensionAttribute1={{.Name}}*)(givenName={{.Name}}*)(sn={{.Name}}*)(extensionAttribute3={{.Name}}*)(sAMAccountName={{.Name}}*)(mail={{.Name}}*)))`
--delegation.ldap_attributes_mapping.search_filter_user	string	+	Фильтр шаблона LDAP для поиска пользователей во внешнем каталоге. Пример: `(&(&(objectCategory=person)(objectClass=user))(|(extensionAttribute2={{.Name}}*)(extensionAttribute1=`

Параметр	Тип	Обязательный	Описание
			{{.Name}}*) (givenName={{.Name}}*) (sn={{.Name}}*) (extensionAttribute3= {{.Name}}*) (sAMAccountName={{.Name}}*) (mail={{.Name}}*)))
--domain_id	string	+	Идентификатор домена
--tls_settings.ca_file	string	+	Путь к файлу CA
--tls_settings.client_cert_file	string	+	Путь к файлу сертификата клиента
--tls_settings.key_file	string	+	Путь к файлу ключа клиента
--token-name	string	+	Имя токена

8.2.3 Добавление маппинга при обновлении делегации в домене

Для добавления маппинга через обновление делегации в домене выполните запрос:

```
nct_ministerium update_domain_delegation
--admin.login  <...>
--admin.password  <...>
--domain_id  <...>
--delegation.default_region_id  <...>
--delegation.delegate_id  <...>
--delegation.domain_alias  <...>
--delegation.is_sync_enabled=TRUE <...>
--delegation.ldap_attributes_mapping.mapping_type MAPPING_TYPE_CUSTOM
--delegation.ldap_attributes_mapping.mapping
'avatar=thumbnailPhoto,department=department,first_name=givenName,first_name_alt
=extensionAttribute2,group_description=description,group_name=displayName,last_c
hanged=whenChanged,last_name=sn,last_name_alt=extensionAttribute1,locale=localeI
D,login=sAMAccountName,mail=mail,middle_name=extensionAttribute3,middle_name_alt
=extensionAttribute3,phone_number_work=telephoneNumber,principal_name=userPrinci
palName,status=userAccountControl,title=title'
--delegation.ldap_attributes_mapping.search_filter_exact_user_by_email
'(&(&(objectCategory=person)(objectClass=user))(mail={{.Email}}))'
--delegation.ldap_attributes_mapping.search_filter_exact_user_by_name
'(&(&(objectCategory=person)(objectClass=user))(sAMAccountName={{.Name}}))' \
--delegation.ldap_attributes_mapping.search_filter_group
'(&(&(objectCategory=group)(|(groupType=8)(groupType=-2147483646)(groupType=-
2147483640))(mail=*)(!(msExchHideFromAddressLists=TRUE)))(|
(displayName={{.Name}}*)(description={{.Name}}*)(mail={{.Name}}*)))'
--delegation.ldap_attributes_mapping.search_filter_resource '(&(|
(msExchResourceMetaData=ResourceType:Room))(|(extensionAttribute2={{.Name}}*)
(extensionAttribute1={{.Name}}*)(givenName={{.Name}}*)(sn={{.Name}}*)
(extensionAttribute3={{.Name}}*)(sAMAccountName={{.Name}}*)(mail={{.Name}}*)))'
--delegation.ldap_attributes_mapping.search_filter_user
'(&(&(objectCategory=person)(objectClass=user))(|(extensionAttribute2={{.Name}}
```

```
*)(extensionAttribute1={{.Name}}*)(givenName={{.Name}}*)(sn={{.Name}}*)
(extensionAttribute3={{.Name}}*)(sAMAccountName={{.Name}}*)(mail={{.Name}}*)))'
--cox.balancer_endpoint=hydra.ucs-apps-1.installation.example.net:50053
--cox.compression=none
--cox.endpoint=grpc-installation.example.net:3142
--cox.load_balanced=false
--cox.request_timeout=10s
--cox.service_name=cox
--cox.use_tls=true \
--cox.use_tls_balancer=false
--tls_settings.ca_file ...
--tls_settings.client_cert_file ...
--tls_settings.key_file ...
```

Описание параметров запроса приведено в таблице 174.

Таблица 174 – Описание параметров запроса на создание домена

Параметр	Тип	Обязательный	Описание
--admin.login	string	+	Логин администратора
--admin.password	string	+	Пароль администратора
--cox.balancer_endpoint	string	+	Endpoint балансировщика нагрузки сервиса
--cox.compression	string	+	Использование метода компрессии при соединении с сервисом: **none** (по умолчанию), **gzip**
--cox.endpoint	string	+	Endpoint для непосредственного соединения с сервисом
--cox.load_balanced	boolean	+	Использовать соединение с балансировщиком
--cox.request_timeout	duration	+	Тайм-аут запроса к сервису (по умолчанию 2 секунды)
--cox.service_name	string	+	Имя сервиса в балансировщике
--cox.use_tls	boolean	+	Использование TLS-сертификата
--cox.use_tls_balancer	boolean	+	Использование TLS-сертификата при соединении с балансировщиком
--delegation.auth_domains	strings	+	Список доменов авторизации для внешнего почтового домена
--delegation.default_region_id	string	+	Идентификатор региона по умолчанию для автоматического создания пользователей

Параметр	Тип	Обязательный	Описание
--delegation.delegate_id	string	+	Идентификатор для использования при внешней авторизации
--delegation.delegation_ catalog_type	int32	+	Если в качестве **mapping_type** установлено значение **MAPPING_TYPE_PRESET**, то используется готовый пресет исходя из следующего списка: **1** – ACTIVE_DIRECTORY, **2** – FREE_IPA, **3** – SAMBA_DC, **4** – RED_ADM, **5** – ALD_PRO
--delegation.domain_alias	string	+	Имя контроллера внешнего домена
--delegation.domain_auth_name	string	+	Длинная запись домена аутентификации
--delegation.domain_short_ name	string	+	Краткая запись домена аутентификации
--delegation.is_sync_enabled	boolean	+	Включение/отключение синхронизации с внешним доменом. Если значение **false**, то выключена. Если значение **true**, то включена
--delegation.ldap_attributes_ mapping.custom_from_file	string	-	Имя файла для загрузки пользовательского маппинга атрибутов. Если задано, другие атрибуты игнорируются
--delegation.ldap_attributes_ mapping.mapping	strings	+	Список атрибутов. Формат: `key1=value1,key2=value2,...` Где `key` – атрибут Mailion, `value` – внешний атрибут
--delegation.ldap_attributes_ mapping.mapping_type	string	+	Тип маппинга. Доступные значения: **MAPPING_TYPE_PRESET** (маппинг с помощью шаблона), **MAPPING_TYPE_CUSTOM** (маппинг, который необходимо заполнить самостоятельно)
--delegation.ldap_attributes_ mapping.search_filter_by_id	string	+	Фильтр шаблона LDAP для поиска объектов по

Параметр	Тип	Обязательный	Описание
			идентификатору во внешнем каталоге. Пример: `(&(ipaUniqueID={{.ID}}))`
--delegation.ldap_attributes_mapping.search_filter_exact_user_by_email	string	+	Фильтр шаблона LDAP для точного поиска пользователей по почтовому адресу во внешнем каталоге. Пример: `(&(&(objectCategory=person)(objectClass=user))(mail={{.Email}}))`
--delegation.ldap_attributes_mapping.search_filter_exact_user_by_name	string	+	Фильтр шаблона LDAP для точного поиска пользователей по имени во внешнем каталоге. Пример: `(&(&(objectCategory=person)(objectClass=user))(sAMAccountName={{.Name}}))`
--delegation.ldap_attributes_mapping.search_filter_group	string	+	Фильтр шаблона LDAP для поиска групп во внешнем каталоге. Пример: `(&(&(objectCategory=group)(|(groupType=8)(groupType=-2147483646)(groupType=-2147483640))(mail=*)(!(msExchHideFromAddressLists=TRUE)))(|(displayName={{.Name}}*)(description={{.Name}}*)(mail={{.Name}}*)))`
--delegation.ldap_attributes_mapping.search_filter_resource	string	+	Фильтр шаблона LDAP для поиска ресурсов во внешнем каталоге. Пример: `(&(|(msExchResourceMetaData=ResourceType:Room))(|(extensionAttribute2={{.Name}}*)(extensionAttribute1={{.Name}}*)(givenName={{.Name}}*)(sn={{.Name}}*)(extensionAttribute3={{.Name}}*)`

Параметр	Тип	Обязательный	Описание
			`(sAMAccountName={{.Name}}*)(mail={{.Name}}*)))`
--delegation.ldap_attributes_mapping.search_filter_user	string	+	Фильтр шаблона LDAP для поиска пользователей во внешнем каталоге. Пример: `(&(&(objectCategory=person)(objectClass=user))(|(extensionAttribute2={{.Name}}*)(extensionAttribute1={{.Name}}*)(givenName={{.Name}}*)(sn={{.Name}}*)(extensionAttribute3={{.Name}}*)(sAMAccountName={{.Name}}*)(mail={{.Name}}*)))`
--domain_id	string	+	Идентификатор домена
--tls_settings.ca_file	string	+	Путь к файлу CA
--tls_settings.client_cert_file	string	+	Путь к файлу сертификата клиента
--tls_settings.key_file	string	+	Путь к файлу ключа клиента
--token-name	string	+	Имя токена

Пример настройки полей приведен в разделе 8.1.

8.2.4 Создание делегации с типом «делегация на одинаковых доменах»

В новом тенанте нужно создать делегацию с типом «делегация на одинаковых доменах», для этого необходимо выполнить запрос:

```
nct_ministerium set_same_domain_delegation
--admin.login  <...>
--admin.password  <...>
--domain_id  <...>
--delegation.default_region_id  <...>
--delegation.delegate_id  <...>
--delegation.domain_alias  <...>
--delegation.is_sync_enabled=TRUE <...>
--delegation.ldap_attributes_mapping.mapping_type MAPPING_TYPE_CUSTOM
--delegation.ldap_attributes_mapping.mapping
'avatar=thumbnailPhoto,department=department,first_name=givenName,first_name_alt
=extensionAttribute2,group_description=description,group_name=displayName,last_c
hanged=whenChanged,last_name=sn,last_name_alt=extensionAttribute1,locale=localeI
```

```
D,login=sAMAccountName,mail=mail,middle_name=extensionAttribute3,middle_name_alt
=extensionAttribute3,phone_number_work=telephoneNumber,principal_name=userPrinci
palName,status=userAccountControl,title=title'
--delegation.ldap_attributes_mapping.search_filter_exact_user_by_email
'(&(&(objectCategory=person)(objectClass=user))(mail={{.Email}}))'
--delegation.ldap_attributes_mapping.search_filter_exact_user_by_name
'(&(&(objectCategory=person)(objectClass=user))(sAMAccountName={{.Name}}))' \
--delegation.ldap_attributes_mapping.search_filter_group
'(&(&(objectCategory=group)(|(groupType=8)(groupType=-2147483646)(groupType=-
2147483640))(mail=*)(!(msExchHideFromAddressLists=TRUE)))(|
(displayName={{.Name}}*)(description={{.Name}}*)(mail={{.Name}}*)))'
--delegation.ldap_attributes_mapping.search_filter_resource '(&(|
(msExchResourceMetaData=ResourceType:Room))(|(extensionAttribute2={{.Name}}*)
(extensionAttribute1={{.Name}}*)(givenName={{.Name}}*)(sn={{.Name}}*)
(extensionAttribute3={{.Name}}*)(sAMAccountName={{.Name}}*)(mail={{.Name}}*)))'
--delegation.ldap_attributes_mapping.search_filter_user
'(&(&(objectCategory=person)(objectClass=user))(|(extensionAttribute2={{.Name}}
*)(extensionAttribute1={{.Name}}*)(givenName={{.Name}}*)(sn={{.Name}}*)
(extensionAttribute3={{.Name}}*)(sAMAccountName={{.Name}}*)(mail={{.Name}}*)))'
--cox.balancer_endpoint=hydra.ucs-apps-1.installation.example.net:50053
--cox.compression=none
--cox.endpoint=grpc-installation.example.net:3142
--cox.load_balanced=false
--cox.request_timeout=10s
--cox.service_name=cox
--cox.use_tls=true \
--cox.use_tls_balancer=false
--tls_settings.ca_file ...
--tls_settings.client_cert_file ...
--tls_settings.key_file ...
```

Описание параметров запроса приведено в таблице 175.

Таблица 175 – Описание параметров запроса `set_same_domain_delegation`

Параметр	Тип	Обязательный	Описание
--admin.login	string	+	Логин администратора
--admin.password	string	+	Пароль администратора
--cox.balancer_endpoint	string	+	Endpoint балансировщика нагрузки сервиса
--cox.compression	string	+	Использование метода компрессии при соединении с сервисом: **none** (по умолчанию), **gzip**
--cox.endpoint	string	+	Endpoint для непосредственного соединения с сервисом
--cox.load_balanced	boolean	+	Использовать соединение с балансировщиком
--cox.request_timeout	duration	+	Тайм-аут запроса к сервису (по умолчанию 2 секунды)

Параметр	Тип	Обязательный	Описание
--cox.service_name	string	+	Имя сервиса в балансировщике
--cox.use_tls	boolean	+	Использование TLS-сертификата
--cox.use_tls_balancer	boolean	+	Использование TLS-сертификата при соединении с балансировщиком
--delegation.auth_domains	strings	+	Список доменов авторизации для внешнего почтового домена
--delegation.default_region_id	string	+	Идентификатор региона по умолчанию для автоматического создания пользователей
--delegation.delegate_id	string	+	Идентификатор для использования при внешней авторизации
--delegation.delegation_catalog_type	int32	+	Если в качестве **mapping_type** установлено значение **MAPPING_TYPE_PRESET**, то используется готовый пресет исходя из следующего списка: **1** – ACTIVE_DIRECTORY, **2** – FREE_IPA, **3** – SAMBA_DC, **4** – RED_ADM, **5** – ALD_PRO
--delegation.domain_alias	string	+	Имя контроллера внешнего домена
--delegation.domain_auth_name	string	+	Длинная запись домена аутентификации
--delegation.domain_short_name	string	+	Краткая запись домена аутентификации
--delegation.is_sync_enabled	boolean	+	Включение/отключение синхронизации с внешним доменом. Если значение **false**, то выключена. Если значение **true**, то включена
--delegation.ldap_attributes_mapping.custom_from_file	string	-	Имя файла для загрузки пользовательского маппинга атрибутов. Если задано, другие атрибуты игнорируются

Параметр	Тип	Обязательный	Описание
--delegation.ldap_attributes_mapping.mapping	strings	+	Список атрибутов. Формат: `key1=value1,key2=value2,...` Где `key` – атрибут Mailion, `value` – внешний атрибут
--delegation.ldap_attributes_mapping.mapping_type	string	+	Тип маппинга. Доступные значения: **MAPPING_TYPE_PRESET** (маппинг с помощью шаблона), **MAPPING_TYPE_CUSTOM** (маппинг, который необходимо заполнить самостоятельно)
--delegation.ldap_attributes_mapping.search_filter_by_id	string	+	Фильтр шаблона LDAP для поиска объектов по идентификатору во внешнем каталоге. Пример: `(&(ipaUniqueID={{.ID}}))`
--delegation.ldap_attributes_mapping.search_filter_exact_user_by_email	string	+	Фильтр шаблона LDAP для точного поиска пользователей по почтовому адресу во внешнем каталоге. Пример: `(&(&(objectCategory=person)(objectClass=user))(mail={{.Email}}))`
--delegation.ldap_attributes_mapping.search_filter_exact_user_by_name	string	+	Фильтр шаблона LDAP для точного поиска пользователей по имени во внешнем каталоге. Пример: `(&(&(objectCategory=person)(objectClass=user))(sAMAccountName={{.Name}}))`
--delegation.ldap_attributes_mapping.search_filter_group	string	+	Фильтр шаблона LDAP для поиска групп во внешнем каталоге. Пример: `(&(&(objectCategory=group)(|(groupType=8)(groupType=-2147483646)(groupType=-2147483640))(mail=*)(!(msExchHideFromAddressLists=TRUE)))(|(displayName={{.Name}}*)(description={{.Name}}*)(mail={{.Name}}*)))`

Параметр	Тип	Обязательный	Описание
--delegation.ldap_attributes_ mapping.search_filter_resource	string	+	Фильтр шаблона LDAP для поиска ресурсов во внешнем каталоге. Пример: `(&(|(msExchResourceMetaData=ResourceType:Room))(|(extensionAttribute2={{.Name}}*)(extensionAttribute1={{.Name}}*)(givenName={{.Name}}*)(sn={{.Name}}*)(extensionAttribute3={{.Name}}*)(sAMAccountName={{.Name}}*)(mail={{.Name}}*)))`
--delegation.ldap_attributes_ mapping.search_filter_user	string	+	Фильтр шаблона LDAP для поиска пользователей во внешнем каталоге. Пример: `(&(&(objectCategory=person)(objectClass=user))(|(extensionAttribute2={{.Name}}*)(extensionAttribute1={{.Name}}*)(givenName={{.Name}}*)(sn={{.Name}}*)(extensionAttribute3={{.Name}}*)(sAMAccountName={{.Name}}*)(mail={{.Name}}*)))`
--domain_id	string	+	Идентификатор домена
--secondary_domain_id	string	+	Идентификатор домена для установки вторичного технического домена для синхронизации почты Exchange
--tls_settings.ca_file	string	+	Путь к файлу CA
--tls_settings.client_cert_file	string	+	Путь к файлу сертификата клиента
--tls_settings.key_file	string	+	Путь к файлу ключа клиента
--token-name	string	+	Имя токена

Пример настройки полей приведен в разделе 8.1.

9 НАСТРОЙКА KERBEROS

Сетевой протокол Kerberos предназначен для обеспечения безопасной аутентификации.

Для корректной работы с Kerberos необходимы следующие условия:

1. Домен авторизации, соответствующий домену в AD, должен быть добавлен в Mailion (см. раздел 7.7).
2. В вышеуказанном домене у пользователя должен присутствовать логин.
3. UPN пользователя должен быть с тем же самым hostname, что и домен AD.
4. В Mailion должен быть заведен аутентификационный домен с делегатом на hostname AD.
5. Должны присутствовать записи для `api` типа A на домен инсталляции. Дополнительно необходимо убедиться, что существует правильная PTR-запись на домен инсталляции или `api` и нет лишних некорректных или устаревших записей.
6. В `trusted sites` достаточно записи `api`.

9.1 Поддержка kerberos для домена

Чтобы включить поддержку Kerberos для домена, необходимо выполнить следующие действия:

1. На контроллере домена через оснастку AD рабочей станции администратора ОС Windows создать служебных пользователей stagehttp (`stageimap/stagesmtp/stageldap/stagegrpc`) (см. Рисунок 84).

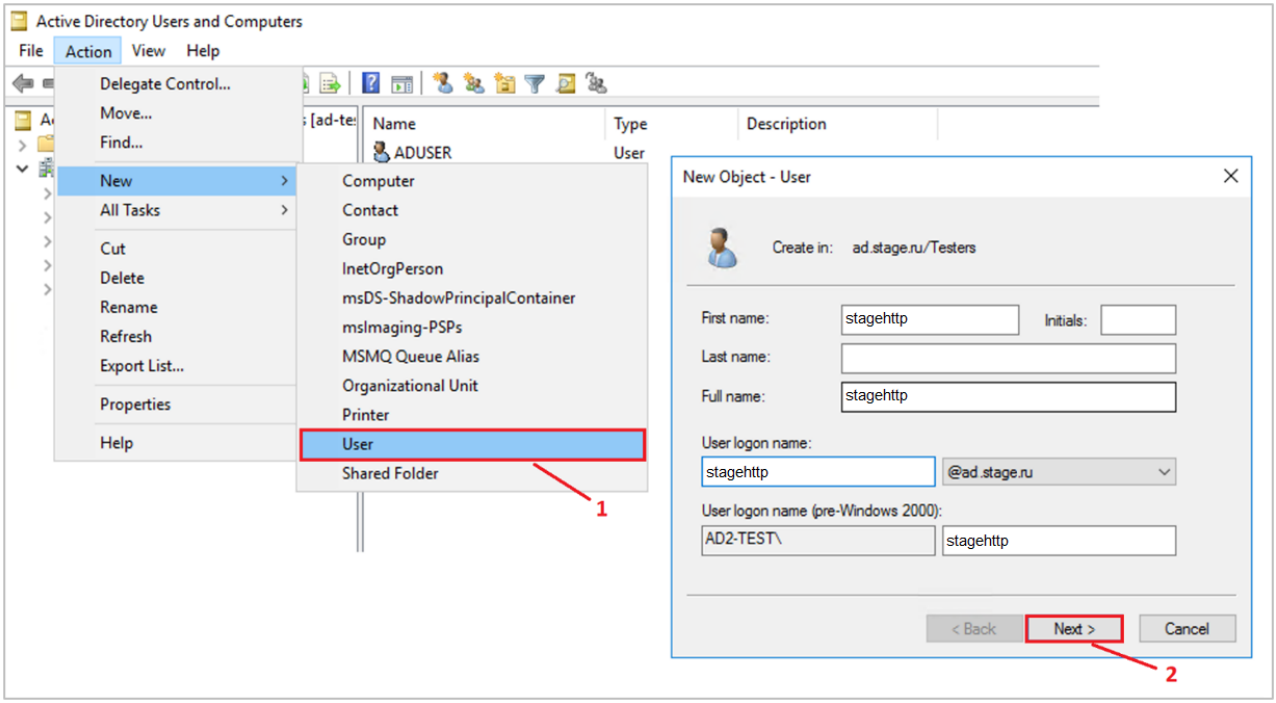


Рисунок 84 – Создание служебных пользователей

2. Запретить изменять пароль и установить пароль бессрочным (см. Рисунок 85).

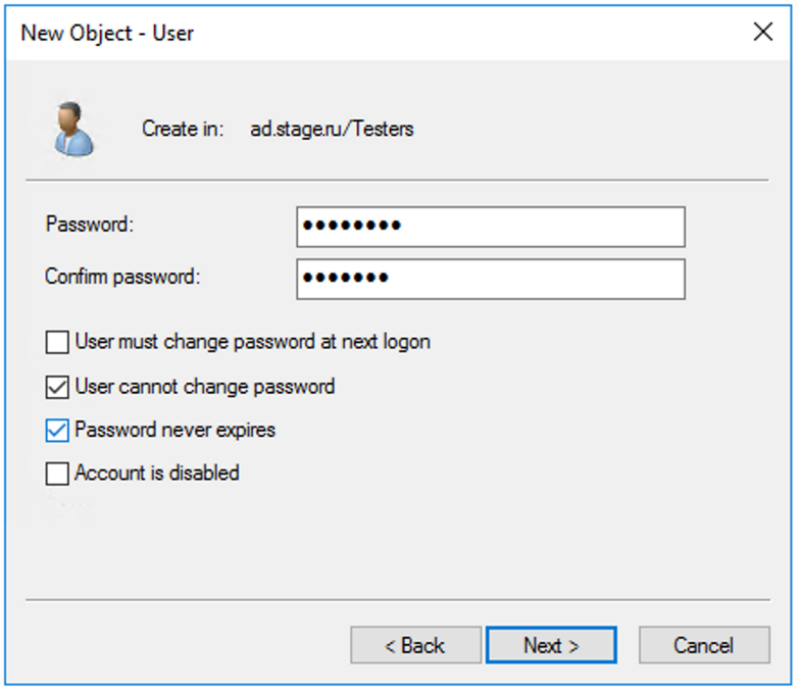


Рисунок 85 – Установка бессрочного пароля

3. Повторить для других пользователей аналогичным образом.

После этого необходимо выполнить настройки для каждого созданного пользователя. Сначала необходимо создать соответствие системного пользователя и уникального идентификатора экземпляра сервиса – Service Principal Name (SPN). В таблице 176 перечислено соответствие системного пользователя и его SPN.

Таблица 176 – Соответствие системного пользователя и его SPN

Системный пользователь	SPN
stagehttp	HTTP/api-testmail.domain.ru
stageimap	imap/imap-testmail.domain.ru
stagesmtp	smtp/smtp-testmail.domain.ru
stageldap	ldap/ldap-testmail.domain.ru
stagegrpc	grpc/grpc-testmail.domain.ru

Затем необходимо выполнить следующие действия (процесс рассмотрен на основе пользователя stagehttp):

1. Открыть командную строку или PowerShell (https://learn.microsoft.com/ru-ru/powershell/) от имени администратора ОС. Выполнить команду для регистрации SPN:

```
C:\Temp>setspn -A HTTP/api-testmail.domain.ru stagehttp
Регистрация ServicePrincipalNames для CN=stagehttp,CN=Users,DC=domain,DC=ru
        HTTP/api-testmail.domain.ru
Обновленный объект
```

2. Выполнить проверку и убедиться, что SPN создан и принадлежит пользователю stagehttp:

```
C:\Temp>setspn -L stagehttp
Зарегистрирован ServicePrincipalNames для CN=stagehttp,CN=Users,DC=domain,DC=ru
HTTP/api-testmail.domain.ru
```

3. Выполнить команду, чтобы сгенерировать keytab-файл. Данный файл будет содержать пары Kerberos принципалов и их ключей для зарегистрированного SPN. Необходимо выполнить для каждого системного пользователя:

   В а ж н о – Хост контроллера домена должен быть записан в верхнем регистре. Пример: AD2-TEST.DOMAIN.RU

```
C:\Temp> ktpass -princ HTTP/api-testmail.domain.ru@AD2-TEST.DOMAIN.RU -mapuser
stagehttp -crypto ALL -ptype KRB5_NT_PRINCIPAL -pass __PASSWORD__ -out C:
\Temp\stagehttp.keytab
```

   Если keytab-файл был создан повторно, то необходимо очистить тикеты в службе KDC (Центр распространения ключей) с помощью команды **klist purge**.

4. Перенести keytab-файл на рабочую машину администратора ОС, где установлена утилита для расширенного администрирования **nct-ministerium** (см. раздел 7) и выполнить команду ниже:

```
nct-ministerium save_keytab --config config.local.json --domain_id 'fae98b71-
29e5-52ba-ab28-3b4a66643ef1' --principal 'HTTP/api-testmail.domain.ru' --
keytab_path '/tmp/stagehttp.keytab'
```

5. Настроить клиент на авторизацию методом Kerberos/GSSAPI.
6. Для HTTP разрешить Kerberos в конфигурационном файле сервиса **house**. Пример секции в файле:

```
http://127.0.0.1:8080/session {
    .....
    kerberos
```

```
    sessions {
        login /create
        ......
    }
```

9.2 Настройка для веб-клиента

9.2.1 Настройка браузера для авторизации через Kerberos

Настройка браузера может быть произведена пользователем с ролью:

– локальный пользователь ОС Windows – пользователь с правами администратора;

– доменный пользователь ОС Windows – Пользователь AD, с ролью которого нужно будет авторизовываться в ОС Windows. Для доменных пользователей, авторизованных в ОС Windows, авторизация в ПО «Mailion» будет происходить автоматически. Для переключения в другой аккаунт пользователю необходимо перейти в другую доменную или локальную учетную запись в ОС Windows.

Авторизация доменных пользователей ОС Windows происходит как в Microsoft Outlook Web: потребуется домен, логин и пароль пользователя. Домен и логин пользователя указываются через слеш: AD\ADUSR25.

9.2.2 Проверка конфигурации Kerberos

Перед тем как осуществить настройку, необходимо выполнить проверку:

1. Посмотреть в конфигурационном файле наличие Kerberos:

```
 ...
    kerberos
    sessions
        { login /create
...
```

2. Посмотреть в консоль браузера, запрос `session/check` вместе со статусом 401 должен отдавать заголовок `WWW-Authenticate: Negotiate`.

9.2.3 Настройка ОС Windows

В а ж н о – Чтобы использовать Kerberos, необходимо включить рабочую станцию в домен. Версия Windows 10 Home не может быть включена в домен, необходимо использовать Windows 10 Pro.

Чтобы присоединить ПК к домену, необходимо (см. Рисунок 86):

1. В **Панели управления** выбрать «Система»/«Имя компьютера».
2. Нажать кнопку **Изменить...**
3. В пункте **Является членом** выбрать «домена» и указать домен (на рисунке в качестве примера указан `installation.example.net`).
4. Нажать **OK**.

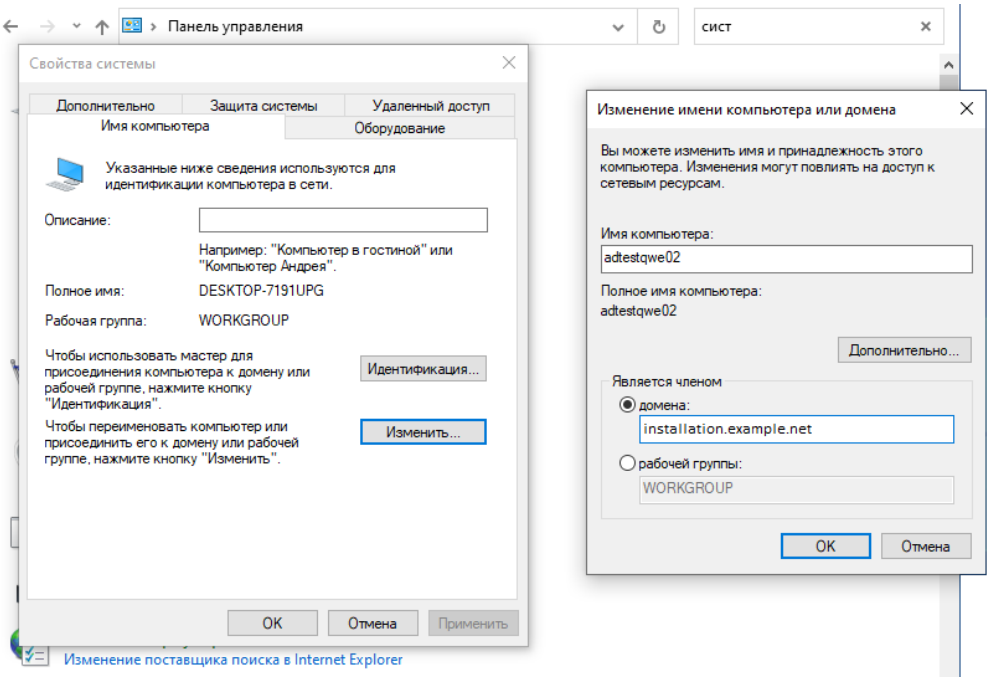


Рисунок 86 – Присоединение ПК к домену

9.2.4 Настройка браузеров в ОС Windows

9.2.4.1 Настройка в Internet Explorer

В а ж н о – Настройка в Internet Explorer обязательна.

Чтобы настроить Internet Explorer, необходимо выполнить следующие действия:

1. В браузере нажать на значок настройки и выбрать **Свойства браузера** (см. Рисунок 87).

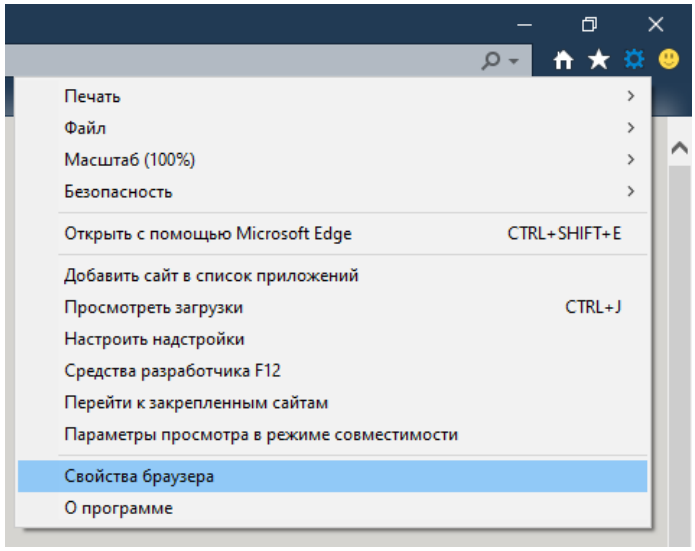


Рисунок 87 – Свойства браузера

2. На вкладке **Безопасность** необходимо выбрать зону **Местная интрасеть** и нажать кнопку **Сайты** (см. Рисунок 88).

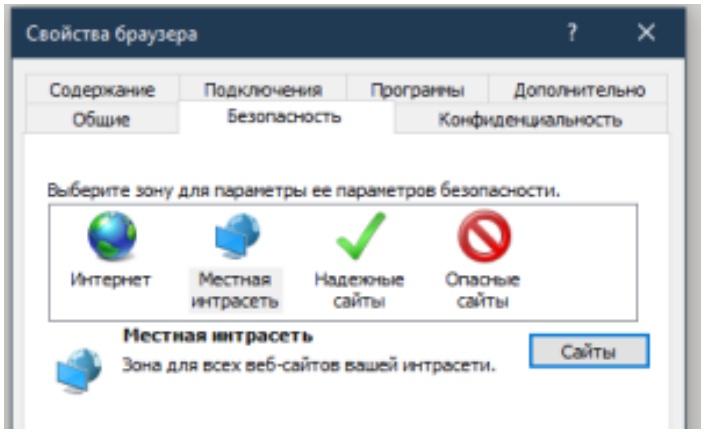


Рисунок 88 – Кнопка **Сайты**

3. Нажать кнопку **Дополнительно** (см. Рисунок 89).

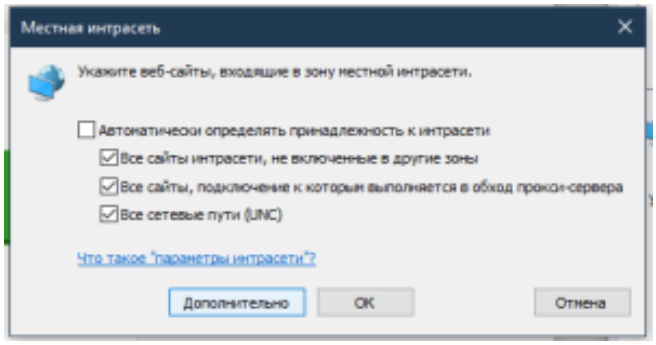


Рисунок 89 – Кнопка **Дополнительно**

4. Указать домен стенда, на котором будет проходить тестирование, и нажать кнопку **Добавить**.
5. На вкладке «Безопасность» выбрать зону «Местная интрасеть» и нажать кнопку **Custom level**. Выставить флаг «Автоматический логин только в Местной интрасети».
6. В окне **Свойства браузера** открыть вкладку **Дополнительно** и убедиться, что включена опция **Разрешить встроенную проверку подлинности Windows** (см. Рисунок 90).

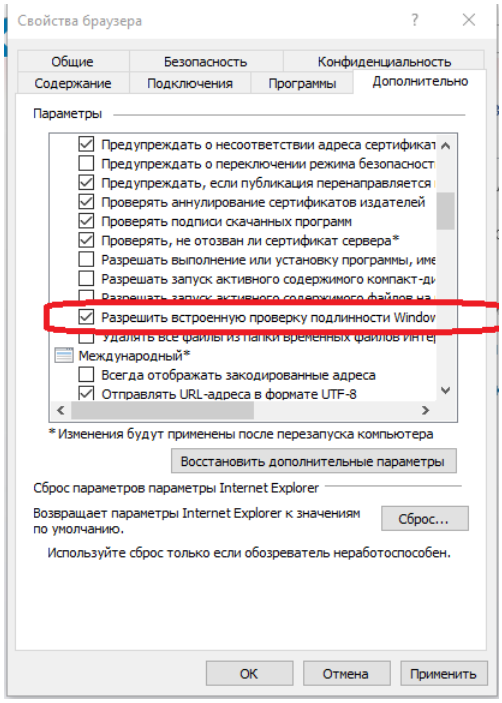


Рисунок 90 – Опция **Разрешить встроенную проверку подлинности Windows**

9.2.4.2 Настройка Google Chrome

В новых версиях Chrome автоматически определяется наличие поддержки Kerberos. Если используется устаревшая версия браузера, то его нужно запустить с дополнительным параметром. Для этого необходимо выполнить следующие действия:

1. Открыть командную строку и указать путь до файла запуска браузера:

```
"C:\Program Files\Google\Chrome\Application\chrome.exe"
```

2. Добавить параметр:

```
--auth-server-whitelist =«*. домен стенда»
```

3. Нажать **Enter**.

После этого откроется браузер Chrome.

9.2.4.3 Настройка Mozilla Firefox

В а ж н о – По умолчанию поддержка Kerberos в Firefox отключена.

Для настройки необходимо выполнить следующие действия:

1. В адресной строке браузера перейти на страницу `about:config`. Нажать кнопку **Принять риск и продолжить**.
2. Найти параметры:
   – network.negotiate-auth.trusted-uris;
   – network.automatic-ntlm-auth.trusted-uris;
   – network.negotiate-auth.delegation-uris.
3. Указать в этих параметрах домен стенда, на котором проходит тестирование.

9.2.5 Настройка приложений в ОС Windows

9.2.5.1 Thunderbird

Чтобы настроить Kerberos в приложении Thunderbird, необходимо выполнить следующие действия:

1. В Thunderbird из меню открыть **Параметры учетной записи** (см. Рисунок 91).

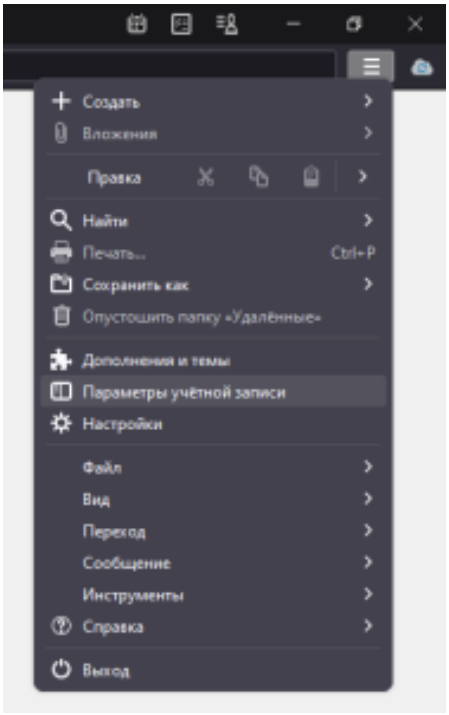


Рисунок 91 – Параметры учетной записи

2. На вкладке **Сервер исходящей почты (SMTP)** нажать кнопку **Добавить/Изменить** (см. Рисунок 92).

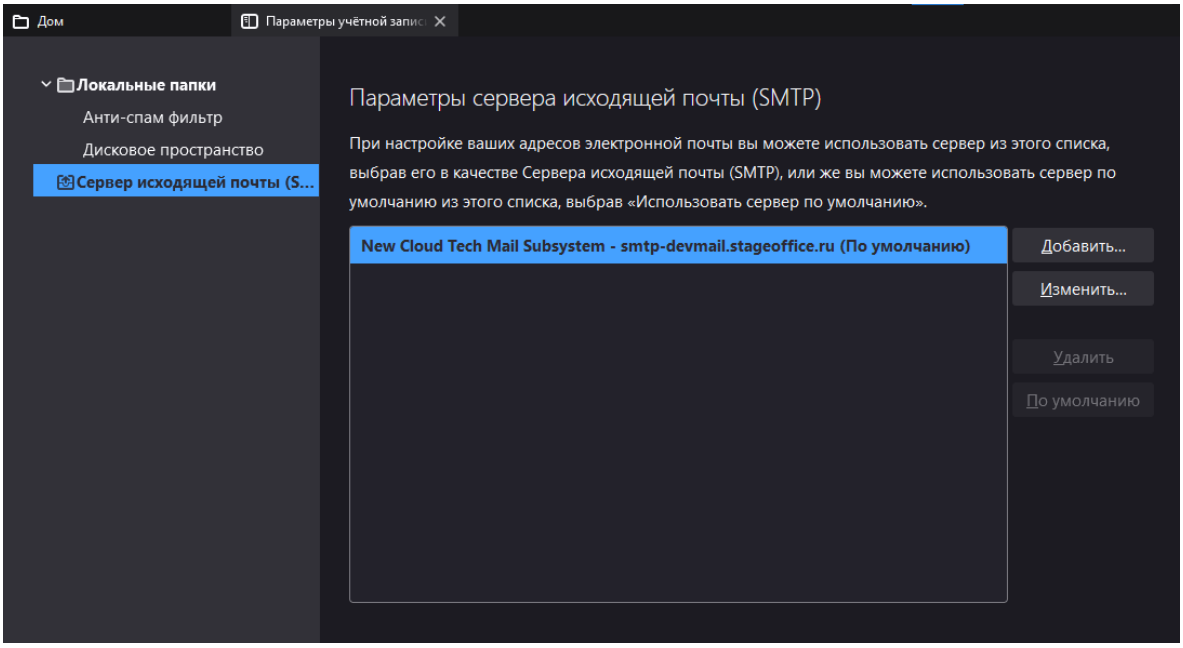


Рисунок 92 – Добавление сервера исходящей почты

3. В **Метод аутентификации** выбрать **Kerberos / GSSAPI**, заполнить оставшиеся необходимые поля и нажать кнопку **ОК** (см. Рисунок 93).

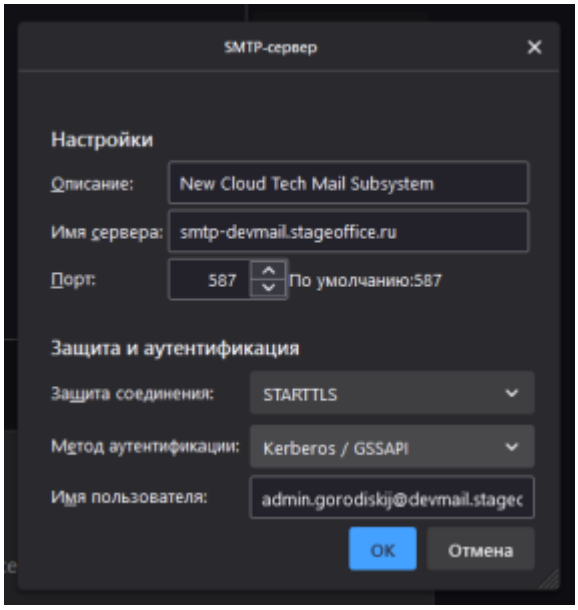


Рисунок 93 – Выбор метода **Kerberos / GSSAPI**

10 УРОВЕНЬ ДОСТУПНОСТИ ПО «MAILION»

ПО «Mailion» имеет уровень доступности 99.9% или «три девятки» при условии обновления системы четыре раза в год.

11 НАСТРОЙКА ОГРАНИЧЕНИЙ ДЛЯ ПОИСКА ПО ВЛОЖЕНИЯМ

Работа в ПО «Mailion» с большим объемом информации, с файлами, нагруженными текстом и вложениями, может привести к высокому потреблению ресурсов оперативной памяти и замедлению выполнения процессов сервисом **viper**.

Для избежания потенциальных проблем с перерасходом памяти и для ускорения процессов (например, миграции пользователей) были введены следующие ограничения:

– ограничение размера вложений для поиска;
– возможность отключения поиска по вложениям:
– ограничение скорости парсинга (автоматизированного сбора и структурирования текстовой информации из документа для поискового индекса) или ограничение числа потоков одновременного парсинга.

11.1 Ограничение размера вложений для поиска

Ограничение гарантирует, что сервис **viper** не будет не будет расходовать ресурсы памяти в большом объеме и оставит функцию поиска по вложениям для большинства пользователей. Таким образом, поиск будет осуществляться только по вложениям, размер которых не превышает 1 МБ.

Примечание – Настройка лимита сохраняется только в конфигурационных файлах внутри сервиса.

11.2 Отключение поиска по вложениям

Для избежания перегрузки ресурсов оперативной памяти и процессора была добавлена возможность отключить поиск по вложениям. Для этого для ansible-роли в конфигурационный файл сервиса **viper** добавлен параметр **viper_disable_attachment_indexing**.

При значении **true** сервис **viper** не будет индексировать вложения при сохранении писем, что приведет к снижению затрат на память и CPU.

Пример секции в конфигурационном файле:

```
viper_disable_attachment_indexing: true
```

11.3 Ограничение скорости парсинга

Для ограничения числа потоков, которые одновременно выполняют индексацию вложений, в конфигурационный файл сервиса **viper** ПО «Mailion» добавлен параметр **viper_client.tripoli.attach_parsing_thread_limit**.

Настройка данного параметра влияет на следующие показатели:

– на пик потребляемой памяти (чем меньше потоков, тем меньше одновременных вложений будет в памяти сервиса);

– на процессорное время, потребляемое сервисом **viper** (чем меньше ядер занято парсингом, тем больше времени остается для других сервисов или задач).

Если нагрузка от сервиса **viper** или нагрузка в виде большого количества писем с вложениями в секунду замедляет процессы, то для ограничения потребления ресурсов можно уменьшить этот параметр. При этом общая скорость индексации вложений соответственно уменьшится.

По умолчанию значение равно количеству доступных виртуальных ядер с той виртуальной машины на которой запущен сервис **viper**.

Пример секции в конфигурационном файле **inventory.yml**:

```
viper_client:
    tripoli:
        attach_parsing_thread_limit: 1
```

12 ИНСТРУКЦИЯ ПО ОБНОВЛЕНИЮ СЕРТИФИКАТОВ НА ФРОНТЕНД-СЕРВЕРАХ

Сертификаты для домена установки находятся в папке, где расположен установщик:

– certificates/server.crt – сертификат сервера;

– certificates/server.nopass.key – ключ сертификата сервера;

– certificates/ca.pem – сертификат или цепочка сертификатов УЦ.

Если имена сертификатов изменились, то необходимо изменить значения **group_vars** в файле group_vars/<installation_name>/main.yml:

```
setup:
   tls:
     cert_filename: <имя файла с сертификатом>
     key_filename:  <имя файла с ключом>
     ca_filename:   <файл с сертификатом или цепочкой сертификатов УЦ>
```

После чего запустить переустановку сервисов фронтенд-сервера следующей командой (независимо от изменения имен сертификатов):

```
ansible-playbook playbooks/main.yml [-i hosts_cluster.yml]
--diff
--limit ucs_frontend,ucs_mail,ucs_infrastructure
--tags cox,house,leda,ararat,imap,postfix
--extra-vars '{"reissue_certificates": true}'
--extra-vars '{"postfix_recreate": true}'
```

13 РЕЗЕРВНОЕ КОПИРОВАНИЕ И ВОССТАНОВЛЕНИЕ

В ПО «Mailion» предусмотрено резервное копирование и восстановление данных.

13.1 Dispersed object store

В конфигурационном файле Dispersed object store (DOS) каждой ноды должны быть заданы параметры резервного копирования:

```
"backup_engine": {
    "store_count": 1,                                    // не используется для
резервного копирования с лидером
    "path": "/srv/docker/dispersed_object_store/backup" // путь для хранения
резервных копий
}
```

В DOS существует два вида резервного копирования:

1. Локальное – резервная копия RocksDB на одной ноде, не зависит от типа установки.
2. Кластерное – набор локальных резервных копий всех нод, которые снимаются со всего кластера в одно время. Кластерные копии можно снять только с кластерной установки.

При работе с обоими видами резервного копирования необходимо учитывать следующие факторы:

– Для локальной (Standalone) и кластерной (отказоустойчивой) установки используется одно API. При снятии и восстановлении резервных копий необходимо работать с тем идентификатором, который вернул DOS.

– Идентификаторы локальных и кластерных копий имеют один тип и не зависят от типа инсталляции.

Для проведения восстановления необходимо перезапускать ноду в режиме восстановления. Для этого необходимо выполнить следующие действия:

1. Остановить ноду.
2. Поменять поле в файле конфигурации **server.recovery_mode = true**.
3. Запустить ноду.

После этого нода готова для восстановления. После проведения восстановления необходимо вернуть значения поля обратно на **false**.

В а ж н о – Нода в режиме восстановления подключается к кластеру так же, как и в нормальном режиме. Нода в режиме восстановления не обрабатывает клиентские запросы.

13.1.1 Снятие резервных копий

Команды для управления резервным копированием необходимо выполнить в любом из Docker-контейнеров DOS.

П р и м е ч а н и е – Docker-контейнер (Docker container) – это автономный исполняемый пакет программного обеспечения, который включает в себя все необходимое для запуска приложения: код, среду выполнения, системные инструменты, системные библиотеки и настройки.

Для этого необходимо перейти в любой из контейнеров с помощью команды:

```
docker exec -it dispersed_object_store bash
```

Следующая команда запустит создание кластерного резервирования для кластерной инсталляции или локального резервирования для Standalone инсталляции соответственно.

В кластерной конфигурации команда на создание кластерного резервирования вызывается только через «лидера» кластера (в терминологии DOS – нода, через которую осуществляется управление кластером). Необходимо, чтобы все ноды кластера успешно выполнили резервное копирование. Если хотя бы одна из нод не смогла сделать резервирование, то весь процесс не считается выполненным.

Запуск резервирования метаданных выполняется с помощью команды:

```
ucs_dispersed_object_store leader backup run -H dos.ucs-dos-shard-2.ucs-
developers.example.com -p 7400 --token=****** --
tls_settings.key_file=/srv/tls/keys/dos.ucs-dos-shard-1.ucs-
developers.example.com-main-key.pem --
tls_settings.client_cert_file=/srv/tls/certs/dos.ucs-dos-shard-1.ucs-
developers.example.com-main-client.pem --
tls_settings.ca_file=/srv/tls/certs/ucs-infra-1.ucs-developers.example.com-main-
ca.pem
```

Точное расположение SSL сертификатов и ключей можно посмотреть в конфигурационном файле **/etc/ucs/dispersed-object-store/config.json** в секции **tls_settings**.

При этом следует соблюдать следующие правила:

– не останавливать ноды для снятия резервных копий;

– поле **blocking** делает снятие резервных копий блокирующим или асинхронным. Для проверки статуса асинхронного процесса необходимо использовать команду проверки статуса резервирования (см. раздел 13.1.2);
– одновременно может сниматься только одна копия;
– для кластера снятие копии необходимо выполнять через «лидера»;
– для кластера можно сделать только кластерное резервирование;
– в качестве ответа на операцию снятия копии вернется сообщение, содержащее в себе идентификатор резервирования (JSON, значение поля **backup_time**);
– если операция снятия копии прошла с ошибками, то в ответном сообщении вернется поле **backup_time** = 0.

В ответе на успешный запрос резервирования поле **backup_time** содержит идентификатор операции. Ответ на выполнение **dos leader backup run**:

```
{
    "error":  {
        "module":  24,
        "code":  200,
        "msg":  "succeeded",
        "details":  []
    },
    "backup_time":  "1693763682", // идентификатор операции копирования
    "rsm_dump_path":
"/srv/docker/dispersed_object_store/backup/rsm_dump.1693763682.json"
}
```

13.1.2 Проверка статуса резервирования

Проверка статуса резервного копирования выполняется с помощью команды:

```
ucs-dispersed-object-store-client leader backup status -H dos.ucs-dos-shard-
2.ucs-developers.example.com -p 7400 --token=****** --
tls_settings.key_file=/srv/tls/keys/dos.ucs-dos-shard-1.ucs-
developers.example.com-main-key.pem --
tls_settings.client_cert_file=/srv/tls/certs/dos.ucs-dos-shard-1.ucs-
developers.example.com-main-client.pem --
tls_settings.ca_file=/srv/tls/certs/ucs-infra-1.ucs-developers.example.com-main-
ca.pem \
--backup_time 1693763682 \  // идентификатор операции резервного копирования
--verify=true               // флаг верификации операции
```

В случае кластерной инсталляции, команду необходимо запускать через «лидер» кластера.

Данная команда осуществляет проверку:

– возможности восстановления DOS из резервной копии;

– существования и успешности резервной копии;

– контрольных резервных копий на всех нодах.

Пример ответа на выполнение команды **dos leader backup status** в кластерной инсталляции:

```
{
    "error": {
        "module": 24,
        "code": 200,
        "msg": "succeeded",
        "details": []
    },
    "info": {
        "backup_time": "1693763682",
        "status": 1,
        "node_backups": {    // для кластерного резервирования указывает
локальные копии на всех нодах кластера. Для SA инсталляции будет пусто
            "1": {
                "status": 1,
                "rocksdb_info": {
                    "backup_id": 5,      // внутренний идентификатор
резервирования RocksDB
                    "timestamp": "1693763686",     // идентификатор локального
резервирования на данной ноде
                    "size": "223327490",
                    "num_files": 15
                },
                "backends": {
                    "1627464062": {
                        "blob": {
                            "blob_path":
"/srv/docker/dispersed_object_store/data/disk1/blob",
                            "rocksdb_info": {
                                "backup_id": 5,
                                "timestamp": "1693763689",
                                "size": "9459078",
                                "num_files": 13
                            },
                            "blob_backup_id": "5"
                        }
                    },
                    "4180084543": {
                        "blob": {
                            "blob_path":
"/srv/docker/dispersed_object_store/data/disk2/blob",
                            "rocksdb_info": {
                                "backup_id": 5,
                                "timestamp": "1693763690",
                                "size": "5857733",
                                "num_files": 14
                            },
                            "blob_backup_id": "5"
                        }
                    }
                }
            },
            "2": {
```

```
                "status": 1,
                "rocksdb_info": {
                    "backup_id": 5,
                    "timestamp": "1693763690",
                    "size": "156609579",
                    "num_files": 21
                },
                "backends": {
                    "2563458084": {
                        "blob": {
                            "blob_path":
"/srv/docker/dispersed_object_store/data/disk1/blob",
                            "rocksdb_info": {
                                "backup_id": 5,
                                "timestamp": "1693763700",
                                "size": "10226794",
                                "num_files": 14
                            },
                            "blob_backup_id": "5"
                        }
                    },
                    "3800749068": {
                        "blob": {
                            "blob_path":
"/srv/docker/dispersed_object_store/data/disk2/blob",
                            "rocksdb_info": {
                                "backup_id": 5,
                                "timestamp": "1693763705",
                                "size": "5939407",
                                "num_files": 10
                            },
                            "blob_backup_id": "5"
                        }
                    }
                }
            },
            "3": {
                "status": 1,
                "rocksdb_info": {
                    "backup_id": 5,
                    "timestamp": "1693763708",
                    "size": "201223876",
                    "num_files": 16
                },
                "backends": {
                    "360601927": {
                        "blob": {
                            "blob_path":
"/srv/docker/dispersed_object_store/data/disk2/blob",
                            "rocksdb_info": {
                                "backup_id": 5,
                                "timestamp": "1693763720",
                                "size": "6252619",
                                "num_files": 15
                            },
                            "blob_backup_id": "5"
                        }
                    },
                    "1202462078": {
```

```
                        "blob": {
                            "blob_path":
"/srv/docker/dispersed_object_store/data/disk1/blob",
                            "rocksdb_info": {
                                "backup_id": 5,
                                "timestamp": "1693763725",
                                "size": "9392734",
                                "num_files": 15
                            },
                            "blob_backup_id": "5"
                        }
                    }
                }
            },
            "4": {
                "status": 1,
                "rocksdb_info": {
                    "backup_id": 5,
                    "timestamp": "1693763729",
                    "size": "223651851",
                    "num_files": 15
                },
                "backends": {
                    "199161773": {
                        "blob": {
                            "blob_path":
"/srv/docker/dispersed_object_store/data/disk2/blob",
                            "rocksdb_info": {
                                "backup_id": 5,
                                "timestamp": "1693763742",
                                "size": "5719444",
                                "num_files": 14
                            },
                            "blob_backup_id": "5"
                        }
                    },
                    "661017583": {
                        "blob": {
                            "blob_path":
"/srv/docker/dispersed_object_store/data/disk1/blob",
                            "rocksdb_info": {
                                "backup_id": 5,
                                "timestamp": "1693763738",
                                "size": "10137511",
                                "num_files": 15
                            },
                            "blob_backup_id": "5"
                        }
                    }
                }
            }
        }
    }
}
```

13.1.3 Получение списка резервных копий

Для кластерной инсталляции команда возвращает список кластерных копий; выполнить ее можно только на лидере кластера. Для инсталляции Standalone команда возвращается список локальных копий.

Пример команды получения списка резервных копий:

```
ucs-dispersed-object-store-client leader backup list -H dos.ucs-dos-shard-4.ucs-
developers.example.com -p 7400 --token=******** --
tls_settings.key_file=/srv/tls/keys/dos.ucs-dos-shard-1.ucs-
developers.example.com-main-key.pem --
tls_settings.client_cert_file=/srv/tls/certs/dos.ucs-dos-shard-1.ucs-
developers.example.com-main-client.pem --
tls_settings.ca_file=/srv/tls/certs/ucs-infra-1.ucs-developers.example.com-main-
ca.pem
```

13.1.4 Восстановление из резервной копии

При потере или повреждении данных можно восстановить их из резервного копирования. Присутствуют следующие ограничения:

– Если данные были повреждены, то для их восстановления из резервных копий необходимо сначала удалить данные в основном хранилище.

– В данном релизе восстанавливаются все данные, кроме backend-данных.

Для восстановления данных в режиме Standalone необходимо выполнить следующие действия:

1. Остановить ноду.
2. Поменять поле в конфигурационном файле **server.recovery_mode = true**.
3. Запустить ноду.
4. Если не известен идентификатор (ID) backup, то его можно найти в списке backup.
5. Запустить команду по **restore** из backup.
6. Остановить ноду.
7. Поменять поле в конфиге.
8. Запустить ноду **server.recovery_mode = false**.

Пример команды **restore**:

```
ucs-dispersed-object-store-client leader backup restore \
-H 127.0.0.1 -p 20300 --token **** --servus_token **** \
--backup_time 1212121212 // идентификатор backup
```

Для восстановления данных в режиме отказоустойчивости необходимо выполнить следующие действия:

1. На машине оператора запустить установку DOS на новую ноду через Ansible с помощью команды:

```
ansible-playbook -i hosts.yml playbooks/mailion/core.yml --tags=dos
```

2. Остановить все ноды командой:

```
docker stop dispersed_object_store
```

3. Монтировать сетевые диски с резервными копиями DOS в **/srv/docker/dispersed_object_store/backup/** или копировать данные этой папки с сервера резервного копирования.
4. Копировать raft json **/srv/docker/dispersed_object_store/backup/rsm_dump.1693763682.json** с ноды лидера в директории для резервных копий остальных нод.
5. На всех нодах DOS в конфигурационный файл доса **/srv/docker/dispersed_object_store/conf/config.json** в секцию server добавить параметр **recovery_mode = true**.
6. Запустить DOS на всех нодах с помощью команды:

```
docker start dispersed_object_store
```

7. Запустить команду **restore** из резервных копий на «лидере».
8. Остановить все ноды.
9. Изменить поле в конфигурационном файле **server.recovery_mode = false** на всех нодах.
10. Запустить DOS на всех нодах с помощью команды:

```
docker start dispersed_object_store
```

Пример команды для восстановления из резервных копий при установке в режиме отказоустойчивости:

```
ucs-dispersed-object-store-client leader backup restore --token=****** --
servus_token ********************** -H dos.ucs-dos-shard-1.ucs-
developers.example.net -p 7400 --token=RhtgjcnmLe[f --
tls_settings.key_file=/srv/tls/keys/dos.ucs-dos-shard-1.ucs-
developers.example.net-main-key.pem --
tls_settings.client_cert_file=/srv/tls/certs/dos.ucs-dos-shard-1.ucs-
developers.example.net-main-client.pem --
tls_settings.ca_file=/srv/tls/certs/ucs-infra-1.ucs-developers.example.net-
main-ca.pem --backup_time 1693767209 \   // идентификатор резервирования
--local=false \                                          // восстановление
из кластерного резервирования (запускается на лидере кластера)
--remote_endpoints="dos.ucs-dos-shard-2.ucs-
developers.example.net:7400,dos.ucs-dos-shard-3.ucs-
developers.example.net:7400,dos.ucs-dos-shard-4.ucs-
developers.example.net:7400"    // восстанавливаем кластер из 3 нод [1,2,3];
команда запускалась с ноды [1]: перечисляем эндпойнты
```

13.1.5 Частичное восстановление из резервной копии для кластера

Для кластера существует возможность восстановить часть нод из резервной копии. Для этого необходимо выполнить следующие действия:

1. Получить статус резервирования (см. раздел 13.1.2).
2. В структуре **node_backups** для всех нод, которые необходимо восстановить, определить идентификаторы локальных копий (поле **timestamp**).
3. Перезапустить все требующие восстановления ноды в режиме восстановления.
4. На каждой ноде, которую необходимо восстановить, провести локальное восстановление. Необходимо использовать команду восстановления с флагом **--local=true**, а в качестве идентификатора указать **локальный идентификатор резервной копии** из структуры **node_backups**.

Пример сообщения в ответе:


```
{
    "error": {
        "module": 24,
        "code": 200,
        "msg": "succeeded",
        "details": []
    },
    "backups": [
        {
            "backup_time": "1634895238",
            "status": 1,
            "node_backups": {
                "1": {
                    "status": 1,
                    "rocksdb_info": {
                        "backup_id": 1,
                        "timestamp": "1634895238",
                        "size": "23785",
                        "num_files": 5
                    }
                },
                "2": {
                    "status": 1,
                    "rocksdb_info": {
                        "backup_id": 1,
                        "timestamp": "1634895238",
                        "size": "23785",
                        "num_files": 5
                    }
                },
                "3": {
                    "status": 1,
                    "rocksdb_info": {
                        "backup_id": 1,
                        "timestamp": "1634895239",
                        "size": "23785",
                        "num_files": 5
                    }
                }
            }
        }
    ]
}
```


Задание на автоматическое резервное копирование в планировщик задач может быть включено через конфигурирование инсталлятора с помощью переменной:

```
dispersed_object_store_backup_full_job_cron_enabled
```

Переменная принимает булевы значения: true (включено) или false (выключено).

13.2 Redis

Резервное копирование Redis не требуется, так как в большей части экземпляров Redis, используемых в ПО «Mailion», хранится кэш. Исключением является Redis для сервиса **dafnis** – в нем хранятся данные о квотах пользователей. Если резервная копия была сделана ранее, при восстановлении хранилища с квотами будут получены некорректные данные факта используемой квоты и ее расчета в системе. Поэтому в случае потери данных этого хранилища лучше использовать механизм пересчета квот через команду **recount_quotas** с помощью интерфейса командной строки.

13.2.1 Резервное копирование

Данные Redis находятся в каталоге **/srv/docker/redis/data/dump.rdb**. Необходимо выполнить следующие действия:

1. Для актуального состояния дампа необходимо сохранить состояние базы через **redis-cli**. Указать порт и пароль в следующей команде:

```
docker exec -ti redis redis-cli -p port -a password save
```

2. Остановить сервис redis, выполнив команду:

```
docker stop redis
```

3. Скопировать дамп **dump.rdb** в резервный каталог.

13.2.2 Восстановление

Для восстановления необходимо выполнить следующие действия:

1. Остановить образ Redis с помощью команды:

```
# docker stop redis
```

2. Убрать текущие файлы баз в рабочей директории:

```
# mv dump.rdb dump.rdb.old
# mv appendonly.aof appendonly.aof.old
```

3. Скопировать дамп **dump.rdb** в каталог с данными redis **/srv/docker/redis/data/** (необходимо проверить права на файл с базой).
4. Отключить AOF **appendonly no** в **/srv/docker/redis/conf/redis.conf**.

5. Запустить сервис Redis с помощью команды:

```
# docker start redis
```

6. Включить AOF, новый файл появится в каталоге **/srv/docker/redis/data/appendonly.aof**.

```
# docker exec -ti redis redis-cli -a password
127.0.0.1:6379> BGREWRITEAOF
Background append only file rewriting started
```

7. Остановить сервис Redis с помощью команды:

```
# docker stop redis
```

8. Включить AOF в конфиге redis **appendonly yes** в **/srv/docker/redis/conf/redis.conf**.
9. Запустить Redis с помощью команды:

```
# docker start redis
```

Примечание – Официальные инструкции по ссылке https://redis.io/topics/persistence.

13.3 MongoDB

13.3.1 Резервное копирование

Для резервного копирования MongoDB необходимо выполнить следующие действия:

1. Запустить скрипт для резервного копирования, который находится на машине инфраструктуры по пути **/srv/docker/mongodb/backup_scripts/mongodb_backup.sh**.
2. Резервное копирование запускается по расписанию через файл **/etc/cron.d/ansible_mongodb_backup**:

```
#Ansible: mongodb-backup
0 1 * * * root /srv/docker/mongodb/backup_scripts/mongodb_backup.sh
```

3. Дампы создаются в каталоге **/srv/backups/mongodb/**.

Примечание – Задание на автоматическое резервное копирование в планировщик задач включается с помощью переменной `mongodb_backup_cron_enabled: true`. По умолчанию включено.

Mongodump и mongorestore не могут быть частью стратегии резервного копирования для сегментированных кластеров 4.2+, в которых выполняются сегментированные транзакции, поскольку резервные копии, созданные с помощью mongodump, не поддерживают гарантии атомарности транзакций между сегментами.

Примечание – Инструкции по командам: https://docs.mongodb.com/manual/tutorial/backup-and-restore-tools/#basic-mongodump-operations, https://docs.mongodb.com/manual/tutorial/backup-and-restore-tools/#restore-a-database-with-mongorestore, https://docs.mongodb.com/database-tools/mongorestore/#mongodb-binary-bin.mongorestore.

Важно – При развертывании стенда с шардированием MongoDB нужна иная стратегия резервного копирования, не поставляемая на данный момент в продукте.

13.3.2 Восстановление

Для восстановления необходимо запустить команду, указав корректное имя образа для текущего релиза, пути до СУБД, учетных данных и путь к файлу с резервной копией:

```
docker run --rm \
    --name mongorestore \
    -v "/srv/tls/certs:/etc/pki/tls/certs/" \
    -v "/srv/backups/mongodb/:/data/backups" \
    172.31.0.22:5000/mongo:4.4.10-17
    mongorestore \
       "mongodb://root:user@mongodb.ucs-db-1.installation.example.net:27017 \
        mongodb.ucs-db-2.installation.example.net:27017 \
        mongodb.ucs-db-3.installation.example.net:27017/?\
           authSource=admin&replicaSet=ucs&tls=true&\
           tlsCAFile=/etc/pki/tls/certs/ucs-infra-1.installation.example.net-
main-ca.pem&\
           tlsCertificateKeyFile=/etc/pki/tls/certs/merged_mongodb.ucs-infra-
1.installation.example.net.pem" \
    --drop --gzip --archive='/data/backups/mongodb_dump_2023_11_01_0100.gz'
```

Примечание – При восстановлении на существующую базу нужно использовать ключ **--drop**, чтобы избежать ошибок с **duplicate key**. При восстановлении на чистый экземпляр запущенного сервиса **mongodb** ключ **--drop** не требуется. Если требуется восстановить коллекцию с текущим UUID, нужно использовать ключ **--drop** с **--preserveUUID**, иначе новой коллекции будет присвоен новый **UUID**. Подробнее: https://docs.mongodb.com/database-tools/mongorestore/#std-option-mongorestore.--preserveUUI.

13.4 Search

Для резервного копирования необходимо выполнить следующие действия:

1. Остановить сервис, дампы которого нужно сделать, – **dirbek** или **mailbek_search**.
2. Заархивировать каталог с данными:

```
tar -czpf имя_сервиса_data.tar.gz /srv/docker/имя_сервиса/data.
```

3. Скопировать архив на тестовый сервер поиска:

```
rsync -ax имя_сервиса_data.tar.gz root@searchstage.example.net:/tmp.
```

Все данные поисковых подсистем могут быть восстановлены через полный проход по всем объектам.

Данные кэша поиска по пользователям, письмам, событиям и пр. можно полностью пересоздать. Подробная информация приведена в разделах 13.4.1 и 13.4.2.

13.4.1 Ручная синхронизация данных в dirbek – поиске по пользователям

В состав поставки входит вспомогательный скрипт, с помощью которого можно провести переиндексацию пользователей в индексе поискового движка.

Вспомогательная утилита поставляется внутри контейнера **perseus**, соответственно, на любой машине с ролью **ucs_catalog**.

Для вызова команды на переиндексацию выполнить:

```
docker exec -it perseus ucs-perseus-dirmole-upsync -
c /etc/ucs/perseus/config.json
```

13.4.2 Ручная переиндексация почтовых ящиков или календарных событий в поиске

В состав поставки входит вспомогательный скрипт, с помощью которого можно провести переиндексацию ящиков или событий. Установка скрипта производится по пути **/bin/ucs-sreindexer** на машине с ролью **ucs_infrastructure**.

Перед тем как запустить переиндексацию, в конфигурационный файл необходимо внести логин и пароль администратора тенанта, в котором будет производиться переиндексация. Файл конфигурации находится по пути **/srv/docker/sreindexer/conf/config.yml.** Часть, которую необходимо изменить:

```
---
auth:
  basic:
    login: <…>
    password: <…>
```

При запуске скрипта можно вызвать справку использования с помощью команды:

```
[root@ucs-infra-1 ~]# /bin/ucs-sreindexer -h
Usage: ucs-sreindexer <scope> <your_tenant_id>
scopes:
mail - index all users mails
cal - index all users calendar events
```

Команда на реиндексацию всех почтовых ящиков:

```
[root@ucs-infra-1 ~]# /bin/ucs-sreindexer mail <tenant_id>
```

Команда на реиндексацию всех календарных событий:

```
[root@ucs-infra-1 ~]# /bin/ucs-sreindexer cal <tenant_id>
```

13.5 Настройка роли ApplicationImpersonation (Олицетворение)

В а ж н о – Для настройки потребуется доступ к Microsoft Exchange Management Shell, который будет подключен к настраиваемому серверу Microsoft Exchange.

Роль **ApplicationImpersonation** позволяет приложениям олицетворять пользователей в организации для выполнения задач от имени пользователя.

Олицетворение – это стандартная техника, которую службы используют для ограничения клиентского доступа к ресурсам домена службы. В Microsoft Exchange используется управление доступом на основе ролей (RBAC). Поэтому для возможности олицетворения приложения потребуется присвоить аккаунту приложения роль **ApplicationImpersonation** (предварительно приложению нужно создать аккаунт, если его нет). Помимо присвоения роли, возможно, потребуется ограничить область видимости для присвоенной аккаунту приложения роли (**ManagementScope**).

Для этого необходимо выполнить следующие действия:

1. Создать ограничения области видимости:

```
New-ManagementScope -Name:<scopeName> -RecipientRestrictionFilter:"<Filter>"
```

2. Присвоить роль **ApplicationImpersonation** и ограничение области видимости для этого присвоения:

```
New-ManagementRoleAssignment -Name:<Assignment name> -
Role:ApplicationImpersonation -User:<impersonationuser>
CustomRecipientWriteScope:<ManagementScope>
```

3. Проверить, какой фильтр указан в **ManagementScope**:

```
Get-ManagementScope | Format-list RecipientFilter,Identity
```

4. Проверить, какой **ManagementScope** указан для присвоенных ролей и каким аккаунтам присвоены роли:

```
Get-ManagementRoleAssignment -RoleAssigneeType User -Role
ApplicationImpersonation | Format-list
User,Role,EffectiveUserName,CustomRecipientWriteScope,DataObject,Identity
```

5. Изменить **ManagementScope** для присвоенной роли:

```
Set-ManagementRoleAssignment -Identity <identity> -CustomRecipientWriteScope
<scopeIdentity>
```

6. Изменить фильтр **ManagementScope**:

```
Set-ManagementScope -Identity <scopeIdentity> -
RecipientRestrictionFilter:"<Filter>"
```

7. ***Пример*** – Создать скоуп для управления почтовыми аккаунтами в OU "ad.installation.example.net/FS":

```
New-ManagementScope -Name "FS_Mailboxes" -RecipientRoot
"ad.installation.example.net/FS" -RecipientRestrictionFilter "RecipientType -eq
'UserMailbox'"
```

8. Создать роль и привязать ее к пользователю и скоупу:

```
New-ManagementRoleAssignment -Name "NMRassignment" -Role
"ApplicationImpersonation" -User "ADUSR01" -CustomRecipientWriteScope
"FS_Mailboxes"
```

13.6 Автоматизация записи информации (метаданных) о резервных копиях сервисов

Логика автоматизации реализована двумя скриптами интерпретатора командной строки **bash** – скриптом **setup.sh** для настройки cron и PostgreSQL и скриптом генерации записей в базе данных **parser.sh**.

Перед запуском скрипта настройки необходимо установить в систему PostgreSQL и отредактировать файл **environment** или оставить его по умолчанию, если в уже установленной базе данных PostgreSQL и в системе отсутствует пользователь **serviceuser** и база **servicedb**. Назначение переменных из этого файла описано в таблице 177.

Таблица 177 – Переменные файла environment

Переменная	Назначение
DATABASE	Имя базы данных, которая будет создана в PostgreSQL
USERNAME	Пользователь, который будет использоваться для автоматизации и доступа к базе DATABASE
PASSWORD	Пароль пользователя USERNAME
SCRIPT_INTERVAL	Время в минутах автоматического запуска скрипта parser.sh

Содержимое файла **environment**:

```
DATABASE=servicedb
USERNAME=serviceuser
PASSWORD=servicepass
SCRIPT_INTERVAL=1
```

Скрипт настройки (setup.sh):

```
DIR=$(dirname $0)
DIR=$(realpath $DIR)
pushd $DIR
 source environment

function remove() {
    execute_psql "DROP DATABASE $DATABASE;"
    execute_psql "DROP USER $USERNAME;"
    clear_crond
    userdel -r $USERNAME
    rm parser-history
}
```

```
function prepare_crond() {
    set -f
    LINE="*/$SCRIPT_INTERVAL * * * *\tbash $DIR/parser.sh"
    crontab -u $USERNAME -l > /tmp/parser-crond
    echo -e $LINE >> /tmp/parser-crond
    crontab -u $USERNAME /tmp/parser-crond
    rm -f /tmp/parser-crond
    set +f
}

function clear_crond() {
    crontab -u $USERNAME -l > /tmp/parser-crond
    grep -v $DIR/parser.sh /tmp/parser-crond > /tmp/parser-crond-remove
    crontab -u $USERNAME /tmp/parser-crond-remove
    rm -f /tmp/parser-crond-remove
    rm -f /tmp/parser-crond
}

function execute_psql() {
    sudo -u postgres psql -c "$@"
}

function create() {
    execute_psql "CREATE USER $USERNAME WITH PASSWORD '$PASSWORD';"
    execute_psql "CREATE DATABASE $DATABASE;"
    execute_psql "GRANT ALL PRIVILEGES ON DATABASE \"$DATABASE\" TO $USERNAME;"
    useradd -m $USERNAME -s /bin/bash
    chown $USERNAME:$USERNAME parser.sh
    pdpl-user -l 0:0 $USERNAME
    setfacl -m u:postgres:r /etc/parsec/macdb/$(sudo -u $USERNAME id -u)
    sudo -u $USERNAME psql -d $DATABASE -c "CREATE TABLE backup_list( record_id
SERIAL PRIMARY KEY, service_name TEXT, create_date TEXT, create_time TEXT,
file_name TEXT, generate_date TIMESTAMP);"
    prepare_crond
    touch parser-history
    chown $USERNAME:$USERNAME parser-history
}

SCRIPT=$0
ACTION=$1

if [ $UID -ne 0 ]; then
    echo This script must be run by root.
    exit 1
fi

if [[ $ACTION != remove && $ACTION != create ]]; then
    echo Usage:
    echo -e "\t$SCRIPT create|remove"
    echo -e "\tcreate - prepare database"
    echo -e "\tremove - delete script changes"
    exit 1
fi

$ACTION

popd
```

Скрипт настройки необходимо запускать от пользователя с привилегиями суперпользователя. Скрипт работает в двух режимах в зависимости от значения первого аргумента при вызове скрипта:

- **create** – создание пользователя в системе, который используется для авторизации по MAC в базе данных PostgreSQL, генерация правила для crontab (файл **/var/spool/cron/crontabs/$USERNAME**) и подготовка базы к работе (создание таблицы, создание пользователя, предоставление прав на базу);
- **remove** – удаление всех записей, баз и пользователей.

Скрипт парсинга (parser.sh):

```
SCRIPT=$(realpath $0)

pushd $(dirname $0)

source environment

DIR=/srv/backups/
HISTORY=parser-history

function get_field_from_last() {
    TEXT=$1
    DELIM=$2
    FIELD=$3

    echo $TEXT | rev | cut -d "$DELIM" -f$FIELD | rev
}

function parse_file() {
    FILE=$1
    SERVICE_NAME=$2

    LAST=$(get_field_from_last "$FILE" "_" 1)
    TIME=$(echo $LAST | cut -d '.' -f1)
    DATE=$(get_field_from_last "$FILE" "_" "2-4")
    NAME=$(get_field_from_last "$FILE" "_" "5-")

    echo parse file by name $NAME with date $DATE and time $TIME
    psql -d $DATABASE -c "INSERT INTO backup_list(service_name, create_date,
create_time, file_name, generate_date) VALUES ('$SERVICE_NAME', '$DATE',
'$TIME', '$NAME', NOW());"
}

function get_user_id() {
    USERNAME=$1

    echo $(getent passwd $USERNAME | cut -d ':' -f 3)
}

USERNAME_UID=$(get_user_id $USERNAME)
if [ $USERNAME_UID -ne $UID ]; then
    echo $SCRIPT
    echo -e "\tThis script must be executed by user $USERNAME"
```

```
    echo -e "\tsudo -u $USERNAME bash $SCRIPT"
    exit 1
fi

if [ ! -e $HISTORY ]; then
    touch $HISTORY
fi

for dir in $(ls $DIR); do
    for file in $(ls $DIR/$dir); do
        full="$dir/$file"
        have=$(grep -o $full $HISTORY)
        if [ -n "$have" ]; then
            continue
        fi
        parse_file $file $dir
        echo $full >> $HISTORY
    done
done

popd
```

Скрипт парсинга необходимо запускать от пользователя, который указан в переменной **USERNAME**:

```
sudo -u $USERNAME bash /opt/parser/parser.sh
```

14 АВТОМАТИЧЕСКОЕ КОНФИГУРИРОВАНИЕ КЛИЕНТА «МОЙОФИС ПОЧТА»

Автоконфигурация клиента включает следующие шаги:

1. Проверка наличия DNS A записи autoconfig.*.
2. При отсутствии результата от шага 1 – проверяется A запись autoconfig-*.
3. Выполняется POST запрос на найденный адрес с передачей логина и пароля пользователя, а в ответ приходят параметры конфигурации почтового клиента.

14.1 Адресные книги CardDAV

Пример секции файла, содержащей адресные книги:

```
"addressbooks": {
   "login": "user@example.net",
   "addressbookPasswordUri": "https://test.example.net",
   "addressbookUri":
"https://test.example.net /dav.php/addressbooks/user@example.net
},
```

Описание полей приведено в таблице 178.

Таблица 178 – Описание полей секции файла, содержащей адресные книги

Параметр	Тип	Описание
addressbookPasswordUri	Str	Специфическое поле для настольного клиента. URI домена
login	Str	Логин для доступа к CardDAV
addressbookUri	Str	URI DAV-коллекции книг

14.2 Календари CalDAV

Пример секции файла, содержащей календари:

```
"calendars": {
   "eventAttachSizeLimit": 2000000,
   "login "user@example.net",
   "calendarPasswordUri": "https://test.example.net"
   "calendarUri": "https://test.example.net /dav.php/calendars/user@example.net
},
```

Описание полей приведено в таблице 179.

Таблица 179 – Описание полей файла секции файла, содержащей календари

Параметр	Тип	Описание
calendarPasswordUri	Str	Специфическое поле для настольного клиента. URI домена
calendarUri	Str	URI DAV-коллекции календарей
login	Str	Логин для доступа к CalDAV
eventAttachSizeLimit	Str	Максимальный размер вложения в событие в байтах

14.3 Глобальная адресная книга LDAP

Пример секции файла, содержащей глобальную адресную книгу:

```
"ldap": {
   "exists": true,
   "binddn": "mail=user@example.net,ou=People,dc=test.example.net,dc=ru",
   "description": "Глобальная адресная книга",
   "basedn": "ou=IT,dc=test.example.net,dc=ru",
   "uri": "ldaps://test.example.net:636/",
   "searchFilter": "(objectclass=*)",
   "autocompleteFilter": "(|(displayName=*%v*)(mail=*%v*))",
   "fullname": "Test User"
},
```

Описание полей приведено в таблице 180.

Таблица 180 – Описание полей секции файла, содержащей календари

Параметр	Тип	Описание
exists	Str	Используется ли наш LDAP сервер как глобальная адресная книга
binddn	Str	DN подключения (Bind DN)
description	Str	Специфическое поле для настольного клиента. Описание книги
basedn	Str	База поиска
uri	Str	Uri LDAP сервера (включает протокол и порт)
searchFilter	Str	Фильтр поиска по книге
autocompleteFilter	Str	Фильтр для поиска в клиентском автокомплите
fullname	Str	Имя и фамилия пользователя из адресной книги, если есть, если нет, то false

В а ж н о – Scope для LDAP поиска будет subtree. Паролем будет являться пароль пользователя.

14.4 Настройки FCM

Пример секции файла, содержащей клиентские настройки FCM:

```
"fcm":
{
   "exists": true,
   "ios":
   {
      "api_key": "AIzaSyAFmtvX4xZB3SUSHlWn9Nsvl02yI4ulKK8",
      "app_id": "1:799400580219:ios:bf6f80e6feb4d4b29dfede",
      "messaging_sender_id": "799400580219",
       "project_id": "amail-push"
   },
   "android":
   {
      "api_key": "AIzaSyA4q_SeJKESXGEEFwM_wylha-Zy_fidATQ",
      "app_id": "1:799400580219:android:96051b1c3139ef31",
      "messaging_sender_id": "799400580219",
      "project_id": "amail-push"
   },
   "huawei": {},
}
```

Описание полей приведено в таблице 181.

Таблица 181 – Описание полей секции файла, содержащей клиентские настройки FCM

Параметр	Тип	Описание
exists	Str	Используется ли FCM

В а ж н о – Остальные поля используются мобильными клиентами, пояснения по их значениям необходимо уточнять у разработчиков мобильных клиентов.

14.5 Другие ответы сервера

Описание примеров сообщений об ошибке приведены в таблице 182.

Таблица 182 – Описание примеров сообщений об ошибке

Пример	Тело сообщения

Неправильный логин или пароль, код ответа 403	{
	"message": "You don't have the permission to access the requested resource. It is either read-protected or not readable by the server."
	}

Не передан Обязательный, код ответа 400	{"message": {"password": "password required"}}

Пример	Тело сообщения
Ошибка сервера, код ответа 500	{"message": "Internal Server Error"}

15 УДАЛЕНИЕ КЛИЕНТА «МОЙОФИС ПОЧТА»

15.1 Удаление приложения на ОС Windows

Удаление приложения «МойОфис Почта» можно выполнить с помощью Панели управления ОС Windows. Рассмотрим удаление на примере ОС Windows 10.

Чтобы удалить приложение, откройте меню «Пуск» Windows и выберите Панель управления.

В окне **Панель управления** выберите **Программы и компоненты**.

В списке программ (см. Рисунок 94) выберите приложение «МойОфис Почта» и нажмите кнопку **Удалить**.

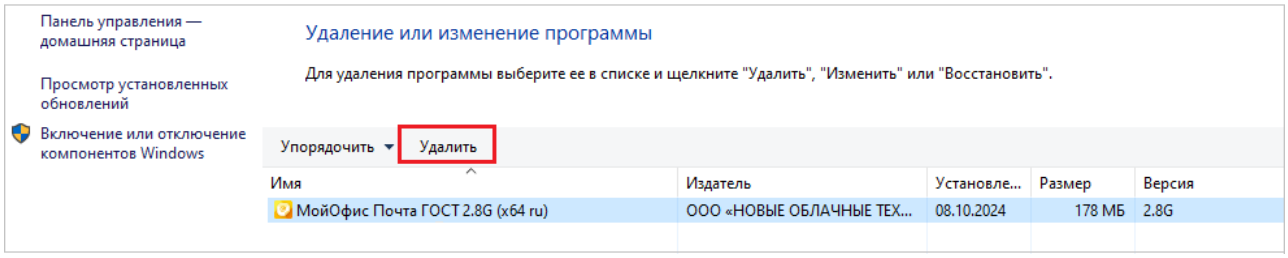


Рисунок 94 – Окно **Удаление или изменение программы**

В мастере удаления, представленном на рисунке 95, нажмите кнопку **Далее**.

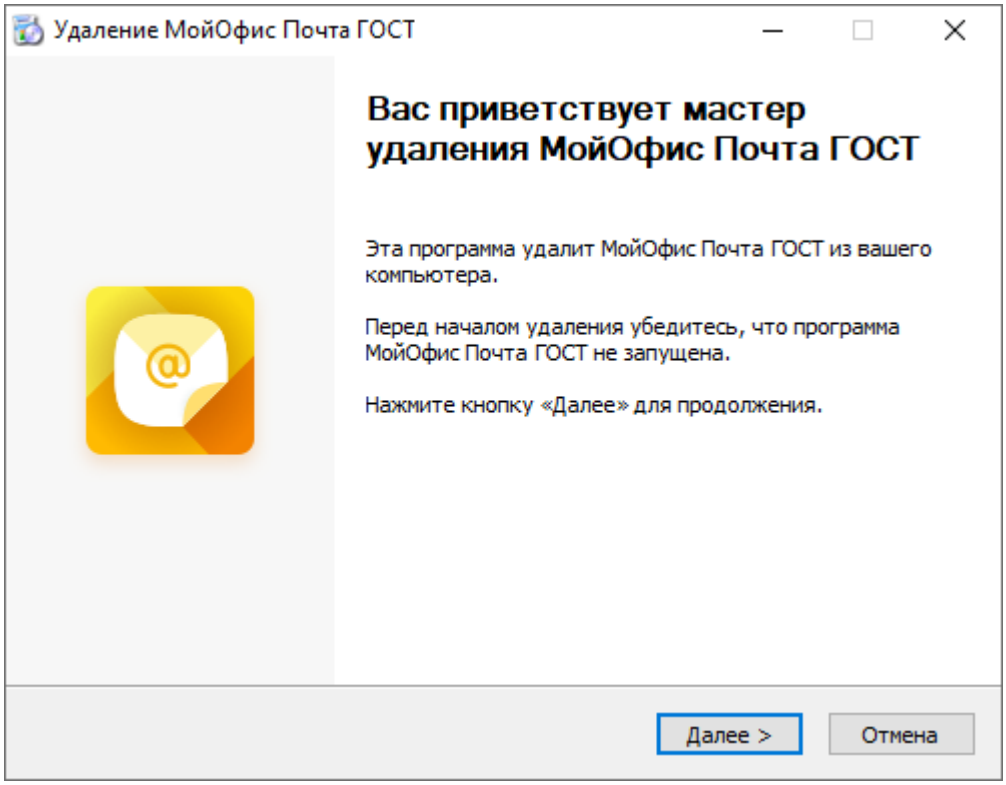


Рисунок 95 – Запрос на подтверждение удаления приложения

Дождитесь подготовки к удалению, нажмите кнопку **Удалить** (см. Рисунок 96).

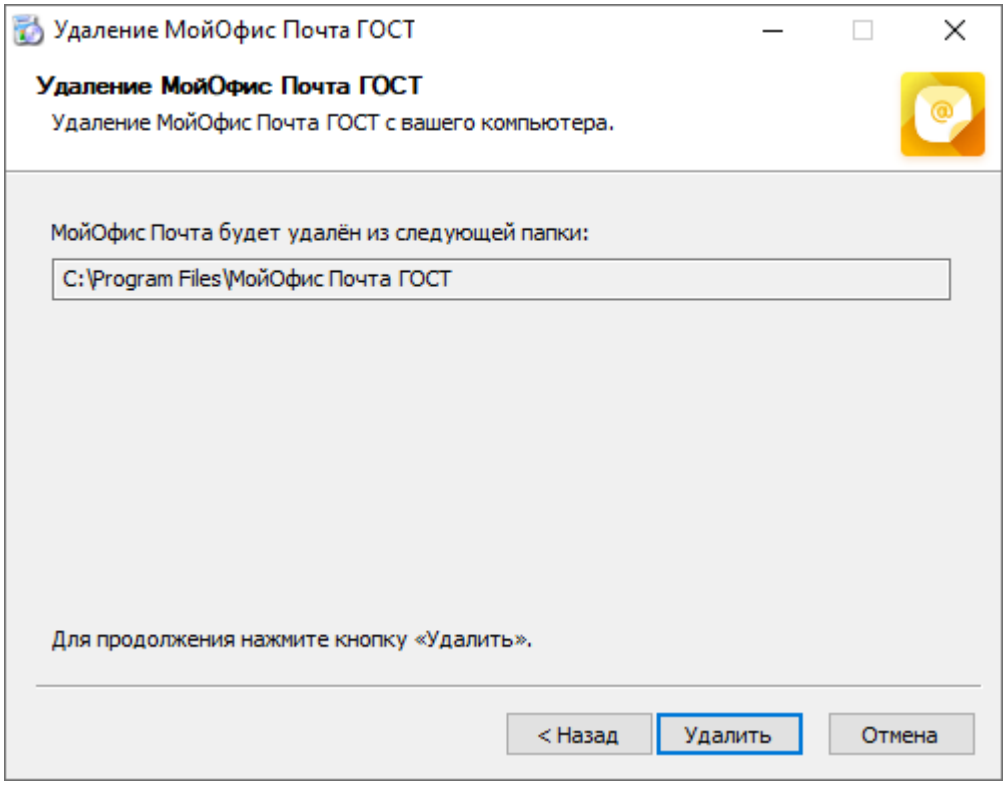


Рисунок 96 – Удаление компонентов приложения

На окончательном экране мастера удаления МойОфис Почта нажмите **Готово** (см. Рисунок 97).

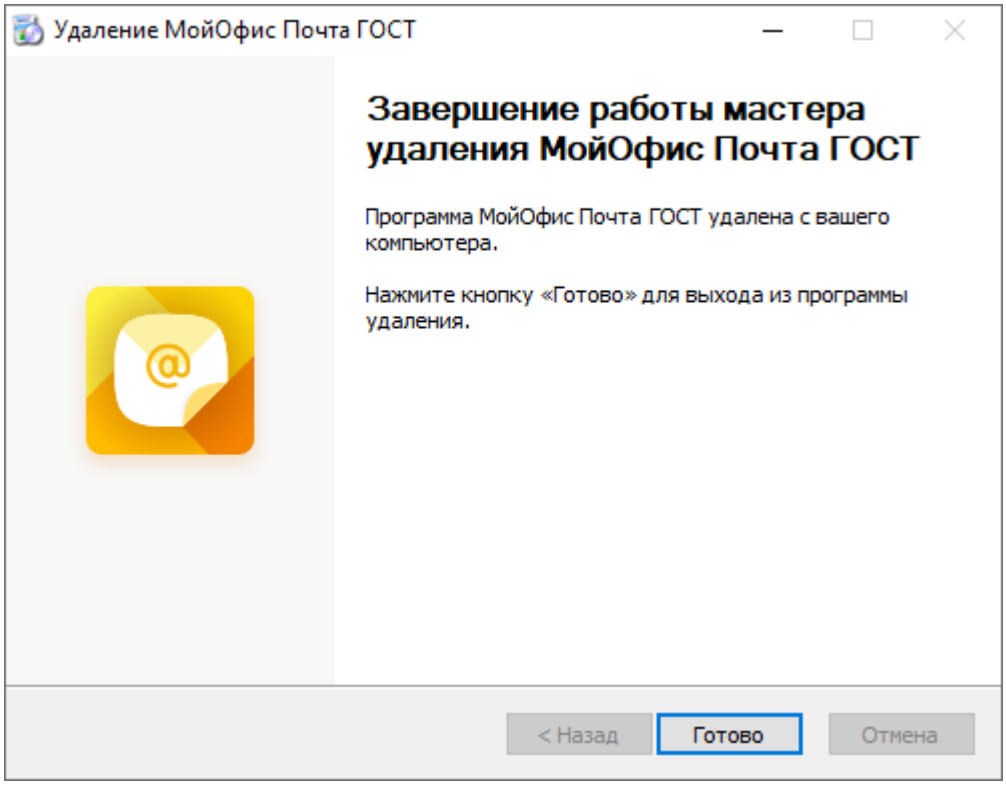


Рисунок 97 – Завершение работы мастера удаления

Если удаление приложения «МойОфис Почта» завершается успешно, строка приложения автоматически удаляется из списка программ.

15.2 Удаление приложения на ОС Linux

Для удаления приложения «МойОфис Почта», установленного с помощью файла дистрибутива с расширением **.rpm**, выполните следующую команду:

```
sudo rpm -e myofficemail
```

Для удаления приложения «МойОфис Почта», установленного с помощью файла дистрибутива с расширением **.deb**, выполните следующую команду:

```
sudo dpkg -r myofficemail
```

Для удаления приложения «МойОфис Почта», установленного с помощью файла дистрибутива с расширением **.sh**, выполните следующие действия:

1. Откройте терминал в папке, в которой находится файл дистрибутива «МойОфис Почта» **MyOffice_Mail_PSN_x64_2.8G.sh**.
2. При необходимости добавьте необходимые права исполняемому файлу дистрибутива, если вы не делали этого ранее:

```
chmod +x ./MyOffice_Mail_PSN_x64_2.8G.sh
```

3. Запустите выполнение файла дистрибутива:

```
./MyOffice_Mail_PSN_x64_2.8G.sh
```

4. Укажите **2**, чтобы начать процесс удаления приложения (см. Рисунок 98).

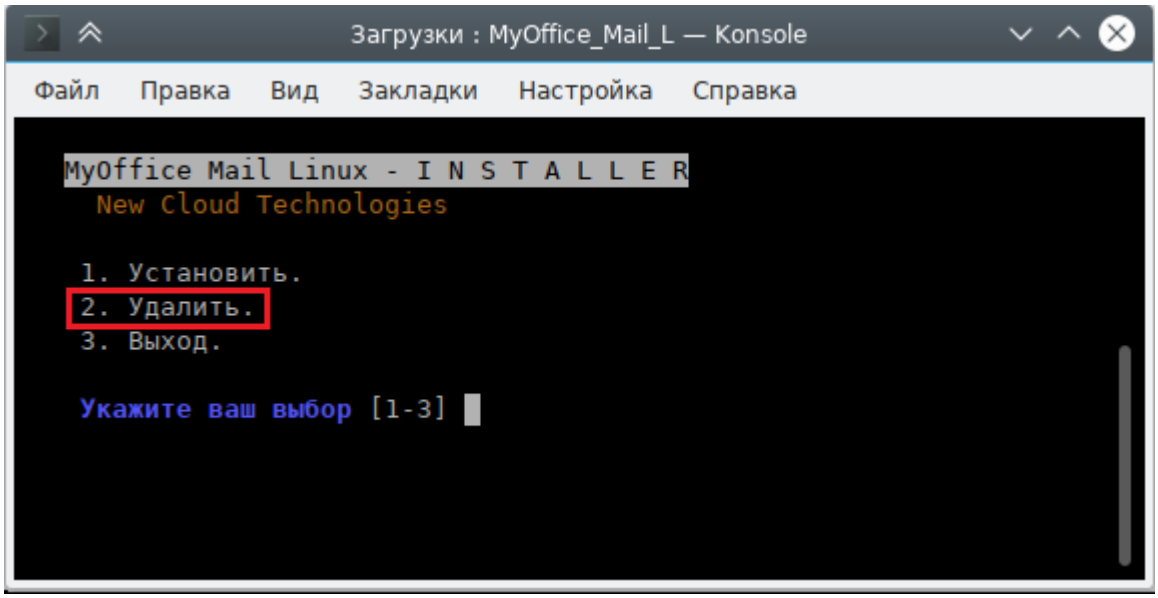


Рисунок 98 – Выбор основного сценария действий

5. Введите **yes**, чтобы согласиться с удалением приложения (см. Рисунок 99).

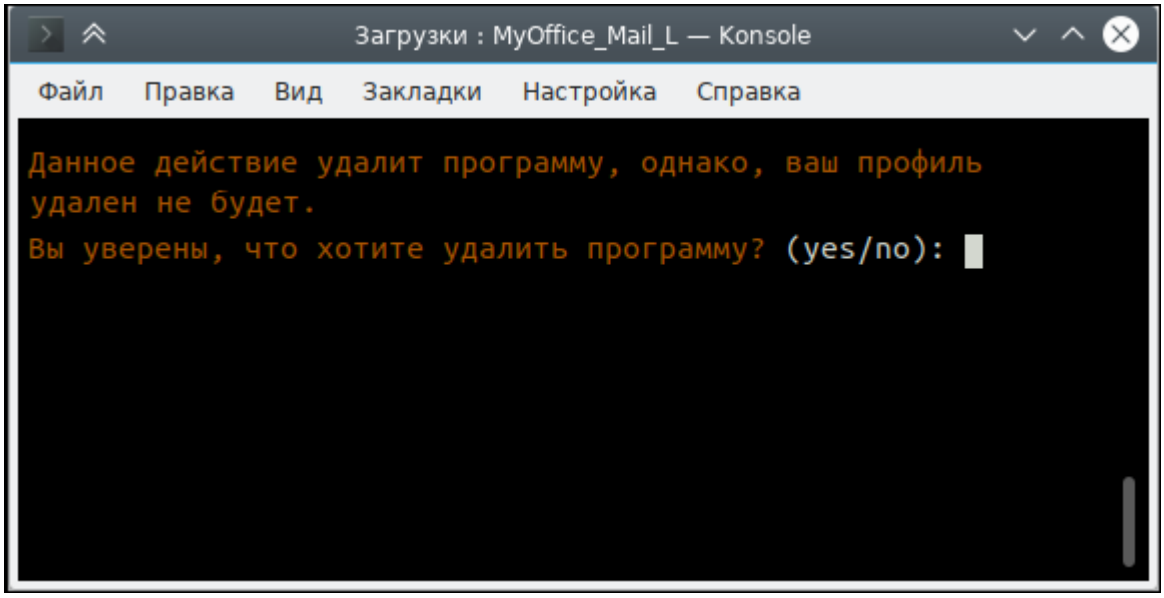


Рисунок 99 – Подтверждение удаления приложения

6. При необходимости укажите папку приложения (см. Рисунок 100).

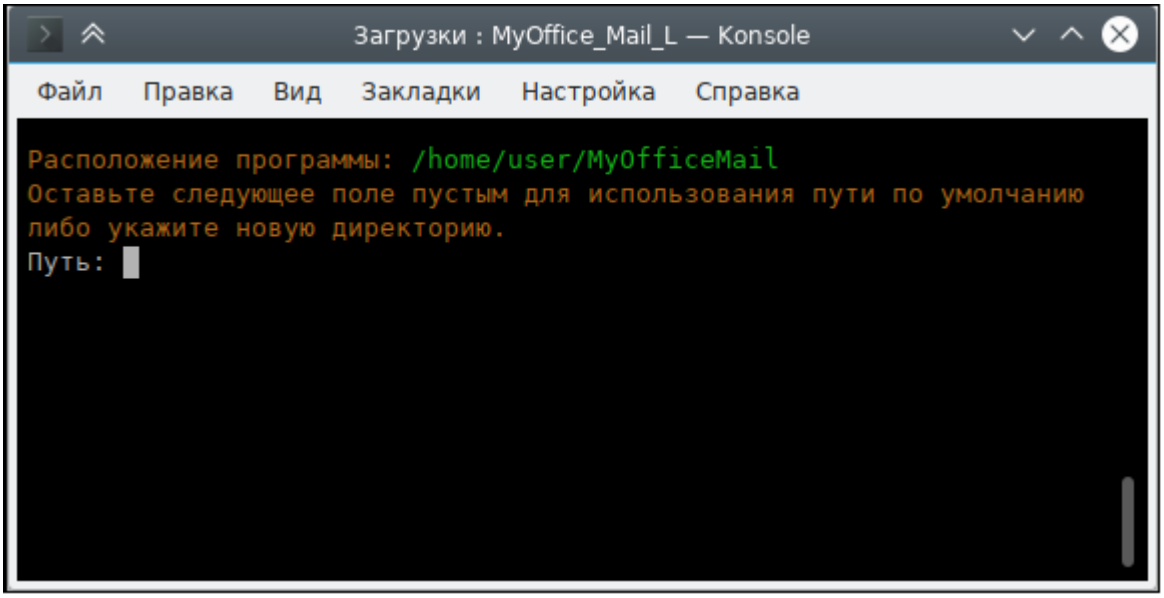


Рисунок 100 – Указание пути приложения

7. Приложение удалено.

16 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

16.1 Сбор и анализ логов

Syslog-ng – сервис централизованного сбора журналов работы системы, включающий в себя **Syslog-ng tier** и **Syslog-ng collector**. Более подробная информация о них приведена ниже.

16.1.1 Syslog-ng tier

На каждый сервер в поставке устанавливается экземпляр **syslog-ng**, который именуется как **tier syslog-ng**.

Данный экземпляр имеет следующие задачи:

- сбор всех данных, поступающих к нему по имени сервера или внутренним адресам через порт **514/udp**;
- переопределение заголовка **hostname** на имя сервера.

Журналы собираются по протоколу без гарантии доставки, так как предполагается, что внутри машины возникновение проблем с сетью достаточно мала.

Локальный **syslog-ng** в поставке имеет дополнительные настройки для того, чтобы:

- сохранять копии журналов локально;
- отправлять данные на единый коллектор **syslog-ng**;
- использовать буфер на диске для отправляемых данных (подробнее см. на официальном сайте разработчика https://www.syslog-ng.com/);
- настраивать параметры гарантии доставки (по умолчанию гарантия доставки отключена, подробнее см. на официальном сайте разработчика https://www.syslog-ng.com/).

16.1.2 Syslog-ng collector

Коллектор **syslog-ng** устанавливается на инфраструктурную машину.

Данный коллектор имеет следующие задачи:

– сбор всех журналов с сервисов, которые используются на инфраструктурной машине;
– прием и агрегирование журналов с других серверов системы, раскладывая их по отдельным директориям.

Журналы на коллектор отправляются по протоколу гарантирующему доставку на порт **601/tcp**.

Коллектор имеет дополнительные параметры:

– настройки количества соединений **tcp** (по умолчанию вычисляется по формуле);
– фильтрации для соединений с других серверов на базе имени сервера (опционально).

16.1.3 Доставка журналов до сервера логирования

Практически каждый сервис в поставке самостоятельно устанавливает соединение с сервером логирования и отправляет на него свои журналы. Дополнительно на сами контейнеры установлены правила отправки журналов на сервер логирования через **docker log-driver**.

Такое разделение вызвано следующими идеями:

– **log-driver** системы контейнеризации работает медленнее встроенного механизма за счет нескольких слоев перенаправления данных;
– **log-driver** системы контейнеризации используется для ПО с открытым исходным кодом, которые не умеют самостоятельно отправлять журналы на серверы логирования, устанавливая удаленное соединение по протоколу **syslog**;
– **log-driver** системы контейнеризации дополняет сборку журналов на случай, если сервис не может быть запущен и не успевает инициализировать соединение с серверов логирования.

16.1.4 Настройка параметров Syslog-ng

Описание настройки параметров **Syslog-ng** приведено в таблице 183.

Таблица 183 – Настройка параметров Syslog-ng

Параметр	Тип	Описание
syslog_ng:		Словарь параметров **syslog_ng**
disk_buffer:		Эта опция позволяет помещать исходящие сообщения в дисковый буфер места назначения, чтобы избежать потери сообщения в случае сбоя системы на стороне назначения
disk_buf_size:	Int	Максимальный размер дискового буфера в байтах. Минимальное значение – **1048576** байт. Если установить меньшее значение, минимальное значение будет использоваться автоматически (По умолчанию: **335544320**)
enabled:	Bool	Включить/Отключить дисковый буфер (По умолчанию: **False**)
mem_buf_size:	Int	Этот параметр содержит размер сообщений в байтах, который используется в части памяти дискового буфера. Используется только вместе с параметром **reliable: True**, параметр будет проигнорирован, если указано **reliable: False** (По умолчанию: **201326592**)
reliable:	Bool	Если значение этого параметра установлено в **True**, **syslog-ng** не может потерять журналы в случае перезагрузки/перезапуска, недоступности места назначения или сбоя **syslog-ng**. Это решение обеспечивает более медленный, но надежный вариант дискового буфера. Он создается и инициализируется при запуске и постепенно увеличивается по мере поступления новых сообщений. Если установлено значение **False**, будет использоваться обычный дисковый буфер. Это обеспечивает более быстрый, но менее надежный вариант дискового буфера (По умолчанию: **False**)
collector:		Эта опция определяет параметры настройки коллектора **syslog-ng**
service_ports:	List	Порты TCP/UDP для коллектора
hostname:	Str	Имя хоста для установки коллектора **syslog-ng**
image:		Эта опция определяет параметры настройки используемого образа
registry:	Str	Путь к образу в хранилище **docker-registry**

Параметр	Тип	Описание
tag:	Str	Имя тега образа
services:	Dict	Список сервисов для правил фильтрации логов
tier:		Эта опция определяет параметры хранения и отправки для локального **syslog-ng**
send_remote	Bool	Отправка журналов работы системы на коллектор
local_store:	Bool	Хранение логов на локальном сервере
service_ports:	List	Порт для отправки сообщений для локального **syslog-ng**

16.2 Антиспам

Rspamd – это продвинутая система фильтрации нежелательной почты, которая позволяет оценивать сообщения по ряду правил, включая регулярные выражения, статистический анализ и пользовательские сервисы, такие как черные списки URL. Каждое сообщение анализируется **Rspamd** и получает оценку вероятности нежелательной почты. В соответствии с этим показателем и настройками пользователя **Rspamd** рекомендует MTA применить к сообщению действие, например, передать, отклонить или добавить заголовок.

Rspamd в ПО «Mailion» используется как антиспам система, антивирус, а также сервис, подписывающий письма электронной подписью DKIM.

Rspamd подключается через MTA (**postfix**) в виде **milter** расширения. Общая схема подключения и работы **milter** и **MTA** (см. Рисунок 101):

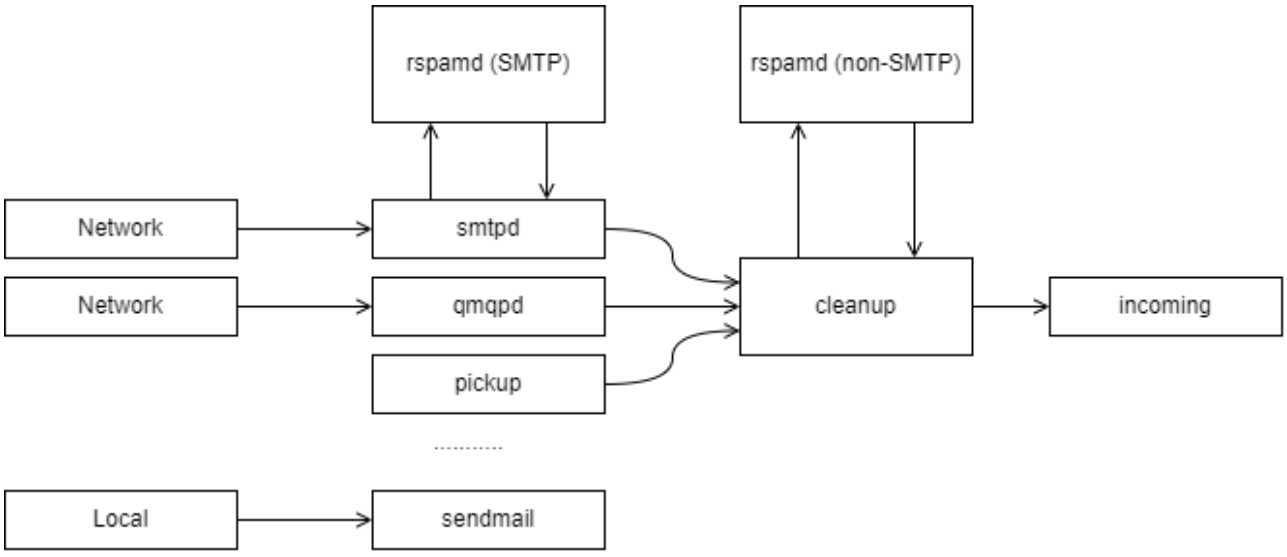


Рисунок 101 – Схема подключения и работы milter и MTA

Типы Milter:

– SMTP-only – обрабатывают почту, приходящую через **smtpd**. Обычно используется для отсеивания нежелательной почты и подписи почты от авторизованных клиентов;
– Non-SMTP – обрабатывает почту, поступающую через командную строку, qmqpd-сервер. Обычно используется для цифровой подписи почты.

Rspamd в ПО «Mailion» используется и как SMTP-only, и как non-SMTP milter.

Более подробную информацию про **Rspamd** можно найти на официальном сайте разработчика (https://rspamd.com/doc/index.html), про архитектуру **postfix** и работу **milter** в **postfix** – на официальном сайте **postfix** (http://www.postfix.org/OVERVIEW.html и http://www.postfix.org/MILTER_README.html).

Для настройки **Rspamd** в ПО «Mailion» следует использовать переменные роли **Rspamd**. Подробная информация о них описана в таблице 184.

Таблица 184 – Настройка переменных ролей Rspamd

Параметр	Пример заполнения	Описание
rspamd:		
connection:	“unix_socket”	Тип подключения (tcp, unix_socket)
dkim_hosts:		DKIM ключ(и) для домена(ов)
installation.example.net:		Заполняется с помощью вывода команды на инфраструктурной ноде docker run --rm -it localhost:5000/nct_rspamd:1.2 rspamadm dkim_keygen -b 2048 -s mail
dkim_key:	| -----BEGIN PRIVATE KEY----- ... -----END PRIVATE KEY-----	При наличии дополнительного внешнего домена добавляется еще один параметр **dkim_key**
dkim_selector:	“mail”	Переключатель функции DKIM ключа
plugins:		Настройка исключений плагина антиспам системы, реализующего технологию серых списков: https://rspamd.com/doc/modules/greylisting.html
greylist:		Серый список заполняется адресами mail-серверов и VIP, относящихся к ним

Параметр	Пример заполнения	Описание
whitelisted_ip:	- "10.10.1.10/32"	https://rspamd.com/doc/modules/ratelimit.html#module-configuration
ratelimit:		
enabled:	False	Включение плагина **ratelimit**
whitelisted_ip:	[]	Список адресов, на которые не действует **ratelimit**
to:		Общий лимит на всю почту (на получателя)
burst:	1000	
rate:	0.5	
to_ip:		Лимит на всю почту, получаемую с одного адреса-источника (на получателя)
burst:	100	
rate:	0.5	
bounce_to:		Общий лимит на **bounce** (на получателя)
burst:	5	
rate:	0.5	
bounce_to_ip:		Лимит на **bounce** из одного адреса-источника (на получателя)
burst:	5	
rate:	0.5	
user:		Лимит на всю почту (**на пользователя**)
burst:	0	
rate:	0.01666666667	
proxy_port:	11332	Прослушиваемый прокси-порт
service_port:	11333	Порт, прослушиваемый сервисом
use_tls:	false	Использование TLS для сетевых соединений
web_port:	11334	Порт, прослушиваемый веб-интерфейсом сервиса
web_password:	"passwd"	Пароль для доступа к веб-интерфейсу
configuration:		
composites:		**composites** используются для сложения (конкатенации) существующих правил и создания более комплексных правил: https://rspamd.com/doc/configuration/composites.html

Параметр	Пример заполнения	Описание
test_composite_1:		
expression:	"SYMBOL1 and SYMBOL2 and (not SYMBOL3 | not SYMBOL4 | not SYMBOL5)"	
score:	1.0	
group:	"some group"	
description:	"description 1"	
policy:	"leave"	
test_composite_2:		
expression:	"SYMBOL3 and SYMBOL4 and (not SYMBOL5 | not SYMBOL6 | not SYMBOL7)"	
score:	2.0	
group:	"some group"	
description:	"description 2"	
policy:	"remove_symbol"	

Для настройки, сбора статистики, журнала обработки писем и обучения **Rspamd** доступен веб-интерфейс, который будет доступен по адресам VM-группы **ucs_mail_mx**.

Например: ucs-mail-1.example.net:{{ rspamd.web_port }}.

В интерфейсе будут доступны вкладки **Status**, **Throughput**, **Configuration**, **Symbols**, **Scan/Learn**, **Test selectors**, **History**:

- **Status** отображает общую статистику работы **Rspamd**;
- **Throughput** предоставляет графики действий;
- **Configuration** предоставляет интерфейс работы с конфигурацией;
- **Symbols** предоставляет интерфейс работы с правилами;
- **Scan/Learn** предоставляет интерфейс сканирования и обучения **Rspamd**;
- **Test selectors** предоставляет интерфейс проверки и работы с селекторами **Rspamd**;
- **History** предоставляет интерфейс просмотра истории действий **Rspamd**.

16.3 Подключение антивирусного модуля KSE (Kaspersky)

Rspamd поддерживает несколько сторонних антивирусных модулей, в том числе Kaspersky. Настройка данного модуля осуществляется через переменные роли **Rspamd**, приведенные в таблице 185.

Таблица 185 – Настройка переменных ролей Rspamd

Параметр	Пример заполнения	Описание
rspamd_kse_use_https	false	Использование **https** для подключения к серверам Касперского
rspamd_kse_endpoints	"192.168.2.25:8085"	Адреса серверов Касперского для обновления сигнатур (обязательно наличие инсталляции KSE внутри компании)
rspamd_kse_timeout	"5.0"	Максимальный период времени для сканирования объекта
rspamd_kse_scan_mime_parts	true	Включение сканирования вложений
rspamd_kse_use_files	false	Отключение file mode в пользу TCP Stream. Не рекомендуется менять значение на true, режим file mode используется только для случаев наличия быстрой **tmpfs**
rspamd_kse_max_size	2048000	Максимальный размер файла для сканирования

Включение модуля антивирусной защиты Kaspersky осуществляется через групповые переменные инсталлятора ПО «Mailion» при наличии установленного в компании Сервера управления «Касперский антивирус».

Подробное описание этих ролей приведено приведено в таблице 186.

Таблица 186 – Настройка переменных ролей Rspamd

Параметр	Пример заполнения	Описание
rspamd_kse_enabled	true	Включение модуля Касперский для **Rspamd**
rspamd_kse_endpoints	"kaspersky.example.net:8085"	Список серверов управления антивирусной защитой Касперский

В а ж н о – Продукт Kaspersky Scan Engine не является частью поставки ПО «Mailion».

16.4 Аудит действий

Для получения событий из аудита необходимо выполнить запрос:

```
nct-ministerium --config juliett.json --c -
-v get_audit_events_by_app_name
--timestamp_from “2012-11-01T22:08:41+00:00”
--timestamp_to “2022-11-01T22:08:41+00:00”
--limit 10
--tenant_id c4972e94-2aff-49ce-4e40-f3c3268bea45
--actors_ids dfe7d654-96ef-454a-a41c-2e83385460b5
--app_name APP_NAME_CATALOG
```

Описание параметров запроса приведено в таблице 187.

Таблица 187 – Описание параметров запроса на получение аудита

Параметр	Тип	Обязательный	Описание
time	Str	+	Время регистрации события
tenant_id	Str	+	Идентификатор тенанта
actors_ids	Str	+	Идентификаторы учетных записей
app_name	Str	+	Имя приложения

16.4.1 Поиск событий безопасности пользователя

16.4.1.1 Вход в систему

Для входа в систему и создания сессии необходимо выполнить запрос:

```
nct-ministerium get_audit_events_by_methods_codes
--config ministerium.json
--admin.login <…>
--admin.password <…>
--methods_names  METHOD_MINOS_CREATE_SESSION
--tenant_id 01068ade-1cce-4125-ab6b-91d977ecf85b
--actors_ids 53c6173f-3e64-4112-93b0-c0c380b33a51
--timestamp_from 2022-09-16T00:00:00+00:00
--timestamp_to 2022-09-16T20:00:00+00:00
--limit 2
```

Описание параметров запроса приведено в таблице 188.

Таблица 188 – Описание параметров запроса на вход в систему и создания сессии

Параметр	Тип	Обязательный	Описание
admin.login	Str	+	Логин администратора тенанта

Параметр	Тип	Обязательный	Описание
admin.password	Str	+	Пароль администратора тенанта
method	Str	+	Метод API
tenant_id	Str	+	Идентификатор тенанта
actors_ids	Str	+	Идентификаторы учетных записей
time	Str	+	Время регистрации события

Пример ответа:


```
{
  "Response": {
    "changed": false,
    "failed": false,
    "msg": "ok"
  },
  "events": [
    {
      "request_id": "5a40de50-ac11-0009-0301-000000000000",
      "actor_id": "53c6173f-3e64-4112-93b0-c0c380b33a51",
      "method": {
        "code": "METHOD_MINOS_CREATE_SESSION",
        "name": "METHOD_MINOS_CREATE_SESSION"
      },
      "time": {
        "unixmicro": "1663337892000000",
        "zone": 10800,
        "zone_name": ""
      },
      "touches": null,
      "client_ip": "\u003cnil\u003e",
      "streamseq": "0"
    },
    {
      "request_id": "5a40de50-ac11-0009-0301-000000000000",
      "actor_id": "53c6173f-3e64-4112-93b0-c0c380b33a51",
      "method": {
        "code": "METHOD_MINOS_CREATE_SESSION",
        "name": "METHOD_MINOS_CREATE_SESSION"
      },
      "time": {
        "unixmicro": "1663337892000000",
        "zone": 10800,
        "zone_name": ""
      },
      "response": {
        "@type": "catalog.minos.v1.CreateSessionResponse",
        "error": {
          "module": "INTERNAL",
          "code": 200,
          "msg": "",
          "details": []
        },
        "access_token": "",
        "expire_at": null,
        "user_id": "",
```

```
        "duration": null,
        "need_change_credential": false,
        "quotas_state": [],
        "refresh_token": "",
        "auth_type": "RESERVED",
        "awaiting_second_factor": false,
        "secret_key": "",
        "blocked_for": "0"
      },
      "touches": null,
      "client_ip": "\u003cnil\u003e",
      "streamseq": "0"
    }
  ],
  "next": {
    "time": {
      "unixmicro": "1663337892000000",
      "zone": 10800
    },
    "requestId": "5a40de50-ac11-0009-0301-000000000000",
    "actorId": "53c6173f-3e64-4112-93b0-c0c380b33a51",
    "methodCode": "METHOD_MINOS_CREATE_SESSION"
  },
  "is_final": false
}
```


16.4.1.2 Смена пароля пользователя

Для смены пароля пользователя необходимо выполнить запрос:

```
nct_ministerium get_audit_events_by_methods_codes
--config ministerium.json
--admin.login <…>
--admin.password <…>
--methods_names METHOD_THESEUS_CHANGE_PASSWORD
--tenant_id 01068ade-1cce-4125-ab6b-91d977ecf85b
--actors_ids 53c6173f-3e64-4112-93b0-c0c380b33a51
--timestamp_from 2022-09-16T00:00:00+00:00
--timestamp_to 2022-09-16T20:00:00+00:00
--limit 2
```

Описание параметров запроса приведено в таблице 189.

Таблица 189 – Описание параметров запроса на смену пароля пользователя

Параметр	Тип	Обязательный	Описание
admin.login	Str	+	Логин администратора тенанта
admin.password	Str	+	Пароль администратора тенанта
method	Str	+	Метод API
tenant_id	Str	+	Идентификатор тенанта
actors_ids	Str	+	Идентификаторы учетных записей

Параметр	Тип	Обязательный	Описание
time	Str	+	Время регистрации события

Пример ответа:


```
{
  "Response": {
    "changed": false,
    "failed": false,
    "msg": "ok"
  },
  "events": [
    {
      "request_id": "5a40de50-ac11-0009-2d01-000000000000",
      "actor_id": "53c6173f-3e64-4112-93b0-c0c380b33a51",
      "method": {
        "code": "METHOD_THESEUS_CHANGE_PASSWORD",
        "name": "METHOD_THESEUS_CHANGE_PASSWORD"
      },
      "time": {
        "unixmicro": "1663338209000000",
        "zone": 10800,
        "zone_name": ""
      },
      "touches": null,
      "client_ip": "10.5.152.93",
      "streamseq": "0"
    },
    {
      "request_id": "5a40de50-ac11-0009-2d01-000000000000",
      "actor_id": "53c6173f-3e64-4112-93b0-c0c380b33a51",
      "method": {
        "code": "METHOD_THESEUS_CHANGE_PASSWORD",
        "name": "METHOD_THESEUS_CHANGE_PASSWORD"
      },
      "time": {
        "unixmicro": "1663338209000000",
        "zone": 10800,
        "zone_name": ""
      },
      "response": {
        "@type": "catalog.theseus.v1.ChangePasswordResponse",
        "error": {
          "module": "INTERNAL",
          "code": 200,
          "msg": "",
          "details": []
        }
      },
      "touches": null,
      "client_ip": "10.5.152.93",
      "streamseq": "0"
    }
  ],
  "next": {
    "time": {
      "unixmicro": "1663338209000000",
      "zone": 10800
```

```
    },
    "requestId": "5a40de50-ac11-0009-2d01-000000000000",
    "actorId": "53c6173f-3e64-4112-93b0-c0c380b33a51",
    "methodCode": "METHOD_THESEUS_CHANGE_PASSWORD"
  },
  "is_final": false
}
```


16.4.2 Поиск событий безопасности администратора

16.4.2.1 Операции над пользователем

16.4.2.1.1 Создание пользователя

Для создания пользователя необходимо выполнить запрос:

```
nct_ministerium get_audit_events_by_methods_codes
--config ministerium.json
--admin.login <…>
--admin.password <…>
--methods_names METHOD_THESEUS_CHANGE_PASSWORD
--tenant_id 01068ade-1cce-4125-ab6b-91d977ecf85b
--actors_ids 53c6173f-3e64-4112-93b0-c0c380b33a51
--timestamp_from 2022-09-16T00:00:00+00:00
--timestamp_to 2022-09-16T20:00:00+00:00
--limit 2
```

Описание параметров запроса приведено в таблице 190.

Таблица 190 – Описание параметров запроса на создание пользователя

Параметр	Тип	Обязательный	Описание
admin.login	Str	+	Логин администратора тенанта
admin.password	Str	+	Пароль администратора тенанта
method	Str	+	Метод API
tenant_id	Str	+	Идентификатор тенанта
actors_ids	Str	+	Идентификаторы учетных записей
time	Str	+	Время регистрации события

Пример ответа:


```
{
  "Response": {
    "changed": false,
    "failed": false,
    "msg": "ok"
```

```
  },
  "events": [
    {
      "request_id": "d2770df7-a32f-4542-a3e0-28ea4829bf94",
      "actor_id": "59ed9c03-0c75-47e2-ac12-eacf6f775431",
      "method": {
        "code": "METHOD_MINISTERIUM_CREATE_USER",
        "name": "METHOD_MINISTERIUM_CREATE_USER"
      },
      "time": {
        "unixmicro": "1663304717000000",
        "zone": 10800,
        "zone_name": ""
      },
      "request": {
        "@type": "type.googleapis.com/ministerium.v1.MinisteriumCommand",
        "name": "create_user",
        "input": "{\"tls_settings\":{\"ca_file\":\"/builds/0/mail-back-
tests/certs/ca.pem\",\"client_cert_file\":\"/builds/0/mail-back-
tests/certs/client_crt.pem\",\"server_cert_file\":\"\",\"key_file\":
\"/builds/0/mail-back-tests/certs/client_key.pem\",\"server_name_override\":
\"\",\"client_auth_type\":\"\",\"tls_min_version\":\"\",
\"prefer_server_cipher_suites\":false,\"use_tls_bundle\":false},\"cox\":
{\"endpoint\":\"grpc-install.example.net:3142\",\"balancer_endpoint\":
\"hydra.ucs-apps-1.install.example.net:50053\",\"balancer_endpoints\":null,
\"service_name\":\"cox\",\"load_balanced\":false,\"use_tls\":true,
\"use_tls_balancer\":false,\"request_timeout\":\"10s\",\"max_send_size\":\"0B\",
\"max_recv_size\":\"0B\",\"compression\":\"none\",\"is_external\":false},
\"token-name\":\"ucs-access-token\",\"admin\":{\"login\":
\"admin_tenant@install.example.net\",\"password\":\"bKv9jqZ9PSwqKD7s\"},
\"tenant_id\":\"01068ade-1cce-4125-ab6b-91d977ecf85b\",\"region_id\":\"2dbacea3-
5889-4021-8f38-bc2214dd7423\",\"login\":
\"autotest_1663293917.343707@install.example.net\",\"password\":
\"4TXoWASIMGD$_EY3*.ij\",\"email\":
\"autotest_1663293917.343707@install.example.net\",\"profile\":{\"first_name\":
\"Герасим\",\"last_name\":\"Одинцов\",\"middle_name\":\"\",\"locale\":\"\",
\"addresses\":\"\",\"department\":\"\",\"title\":\"\",\"phones\":[],
\"preferable_phone\":\"\",\"gender\":\"\",\"birthday\":\"\"},\"roles\":[],
\"gal_tags\":[\"0c22be2e-1e2f-5f6d-bec5-842c5d48e9d3\"],\"quotas\":{}}
      },
      "touches": null,
      "client_ip": "172.17.0.2",
      "streamseq": "0"
    },
    {
      "request_id": "57b87da0-62f9-4c38-a180-ebe8add7421b",
      "actor_id": "59ed9c03-0c75-47e2-ac12-eacf6f775431",
      "method": {
        "code": "METHOD_MINISTERIUM_CREATE_USER",
        "name": "METHOD_MINISTERIUM_CREATE_USER"
      },
      "time": {
        "unixmicro": "1663304718000000",
        "zone": 10800,
        "zone_name": ""
      },
      "request": {
        "@type": "type.googleapis.com/ministerium.v1.MinisteriumCommand",
        "name": "create_user",
```

```
        "input": "{\"tls_settings\":{\"ca_file\":\"/builds/0/mail-back-
tests/certs/ca.pem\",\"client_cert_file\":\"/builds/0/mail-back-
tests/certs/client_crt.pem\",\"server_cert_file\":\"\",\"key_file\":
\"/builds/0/mail-back-tests/certs/client_key.pem\",\"server_name_override\":
\"\",\"client_auth_type\":\"\",\"tls_min_version\":\"\",
\"prefer_server_cipher_suites\":false,\"use_tls_bundle\":false},\"cox\":
{\"endpoint\":\"grpc-install.example.net:3142\",\"balancer_endpoint\":
\"hydra.ucs-apps-1.install.example.net:50053\",\"balancer_endpoints\":null,
\"service_name\":\"cox\",\"load_balanced\":false,\"use_tls\":true,
\"use_tls_balancer\":false,\"request_timeout\":\"10s\",\"max_send_size\":\"0B\",
\"max_recv_size\":\"0B\",\"compression\":\"none\",\"is_external\":false},
\"token-name\":\"ucs-access-token\",\"admin\":{\"login\":
\"admin_tenant@install.example.net\",\"password\":\"bKv9jqZ9PSwqKD7s\"},
\"tenant_id\":\"01068ade-1cce-4125-ab6b-91d977ecf85b\",\"region_id\":\"2dbacea3-
5889-4021-8f38-bc2214dd7423\",\"login\":
\"autotest_1663293917.881039@install.example.net\",\"password\":
\"pJuPaw(lmbC2zAhOG3MS\",\"email\":
\"autotest_1663293917.881039@install.example.net\",\"profile\":{\"first_name\":
\"Нифонт\",\"last_name\":\"Медведев\",\"middle_name\":\"\",\"locale\":\"\",
\"addresses\":\"\",\"department\":\"\",\"title\":\"\",\"phones\":[],
\"preferable_phone\":\"\",\"gender\":\"\",\"birthday\":\"\"},\"roles\":[],
\"gal_tags\":[\"0c22be2e-1e2f-5f6d-bec5-842c5d48e9d3\"],\"quotas\":{}}
      },
      "touches": null,
      "client_ip": "172.17.0.2",
      "streamseq": "0"
    }
  ],
  "next": {
    "time": {
      "unixmicro": "1663304718000000",
      "zone": 10800
    },
    "requestId": "57b87da0-62f9-4c38-a180-ebe8add7421b",
    "actorId": "59ed9c03-0c75-47e2-ac12-eacf6f775431",
    "methodCode": "METHOD_MINISTERIUM_CREATE_USER"
  },
  "is_final": false
}
```


16.4.2.1.2 Обновление профиля пользователя

Для обновления профиля пользователя необходимо выполнить запрос:

```
nct_ministerium get_audit_events_by_methods_codes
--config ministerium.json
--admin.login <…>
--admin.password <…>
--methods_names METHOD_MINISTERIUM_UPDATE_USER_PROFILE
--tenant_id 01068ade-1cce-4125-ab6b-91d977ecf85b
--actors_ids 59ed9c03-0c75-47e2-ac12-eacf6f775431
--timestamp_from 2022-09-16T05:00:00+00:00
--timestamp_to 2022-09-16T06:00:00+00:00
--limit 2
```

Описание параметров запроса приведено в таблице 191.

Таблица 191 – Описание параметров запроса на обновление профиля пользователя

Параметр	Тип	Обязательный	Описание
admin.login	Str	+	Логин администратора тенанта
admin.password	Str	+	Пароль администратора тенанта
method	Str	+	Метод API
tenant_id	Str	+	Идентификатор тенанта
actors_ids	Str	+	Идентификаторы учетных записей
time	Str	+	Время регистрации события

Пример ответа:


```
{
  "Response": {
    "changed": false,
    "failed": false,
    "msg": "ok"
  },
  "events": [
    {
      "request_id": "873a1c4b-ef29-44af-8fba-cd4d005da0bc",
      "actor_id": "59ed9c03-0c75-47e2-ac12-eacf6f775431",
      "method": {
        "code": "METHOD_MINISTERIUM_UPDATE_USER_PROFILE",
        "name": "METHOD_MINISTERIUM_UPDATE_USER_PROFILE"
      },
      "time": {
        "unixmicro": "1663307004000000",
        "zone": 10800,
        "zone_name": ""
      },
      "request": {
        "@type": "type.googleapis.com/ministerium.v1.MinisteriumCommand",
        "name": "update_user_profile",
        "input": "{\"tls_settings\":{\"ca_file\":\"/builds/0/mail-back-
tests/certs/ca.pem\",\"client_cert_file\":\"/builds/0/mail-back-
tests/certs/client_crt.pem\",\"server_cert_file\":\"\",\"key_file\":
\"/builds/0/mail-back-tests/certs/client_key.pem\",\"server_name_override\":
\"\",\"client_auth_type\":\"\",\"tls_min_version\":\"\",
\"prefer_server_cipher_suites\":false,\"use_tls_bundle\":false},\"cox\":
{\"endpoint\":\"grpc-install.example.net:3142\",\"balancer_endpoint\":
\"hydra.ucs-apps-1.install.example.net:50053\",\"balancer_endpoints\":null,
\"service_name\":\"cox\",\"load_balanced\":false,\"use_tls\":true,
\"use_tls_balancer\":false,\"request_timeout\":\"10s\",\"max_send_size\":\"0B\",
\"max_recv_size\":\"0B\",\"compression\":\"none\",\"is_external\":false},
\"token-name\":\"ucs-access-token\",\"admin\":{\"login\":
\"admin_tenant@install.example.net\",\"password\":\"bKv9jqZ9PSwqKD7s\"},
\"entity_id\":\"ca6d8fca-f2bf-4ff4-a08e-987e23b99f4c\",\"profile\":
{\"first_name\":\"Адриан\",\"last_name\":\"Новиков\",\"middle_name\":
\"Викторович\",\"locale\":\"en_US\",\"addresses\":\"[{\\\"name\\\": \\\"Один
заложить.\\\", \\\"country\\\": \\\"Ямайка\\\", \\\"region\\\": \\\"Тульская
обл.\\\", \\\"city\\\": \\\"п. Токма\\\", \\\"zip_code\\\": \\\"132543\\\", \\
```

```
\"address\\\": \\\"пр. Тенистый, д. 682 стр. 62\\\", \\\"floor\\\": \\\"59\\\",
\\\"room\\\": \\\"72\\\", \\\"workplace\\\": \\\"760\\\", \\\"coordinates\\\":
{\\\"latitude\\\": 33.09753, \\\"longitude\\\": 15.37725}, \\\"preference\\\":
28, \\\"type\\\": \\\"work\\\"}]\",\"department\":\"department_1663296204\",
\"title\":\"title_1663296204\",\"phones\":[\"WORK:+72939806278\",\"HOME:8 658
438 44 22\"],\"preferable_phone\":\"+72939806278\",\"gender\":\"FEMALE\",
\"birthday\":\"1979-02-10\"},\"create\":false,\"gal_tags\":[],\"gal_region_id\":
\"\"}"
      },
      "touches": null,
      "client_ip": "172.17.0.2",
      "streamseq": "0"
    },
    {
      "request_id": "873a1c4b-ef29-44af-8fba-cd4d005da0bc",
      "actor_id": "59ed9c03-0c75-47e2-ac12-eacf6f775431",
      "method": {
        "code": "METHOD_MINISTERIUM_UPDATE_USER_PROFILE",
        "name": "METHOD_MINISTERIUM_UPDATE_USER_PROFILE"
      },
      "time": {
        "unixmicro": "1663307007000000",
        "zone": 10800,
        "zone_name": ""
      },
      "response": {
        "@type": "type.googleapis.com/ministerium.v1.MinisteriumCommand",
        "name": "update_user_profile",
        "output": "{\"changed\":true,\"failed\":false,\"msg\":\"ok\"}"
      },
      "touches": null,
      "client_ip": "172.17.0.2",
      "streamseq": "0"
    }
  ],
  "next": {
    "time": {
      "unixmicro": "1663307007000000",
      "zone": 10800
    },
    "requestId": "873a1c4b-ef29-44af-8fba-cd4d005da0bc",
    "actorId": "59ed9c03-0c75-47e2-ac12-eacf6f775431",
    "methodCode": "METHOD_MINISTERIUM_UPDATE_USER_PROFILE"
  },
  "is_final": false
}
```


16.4.2.1.3 Удаление пользователя

Для удаления пользователя необходимо выполнить запрос:

```
nct_ministerium get_audit_events_by_methods_codes
--config ministerium.json
--admin.login <…>
--admin.password <…>
--methods_names METHOD_ERAKLES_CHANGE_STATUS
--tenant_id 01068ade-1cce-4125-ab6b-91d977ecf85b
```

```
--actors_ids 59ed9c03-0c75-47e2-ac12-eacf6f775431
--timestamp_from 2022-09-16T12:34:00+00:00
--timestamp_to 2022-09-16T12:35:00+00:00
--limit 2
```

Описание параметров запроса приведено в таблице 192.

Таблица 192 – Описание параметров запроса на удаление пользователя

Параметр	Тип	Обязательный	Описание
admin.login	Str	+	Логин администратора тенанта
admin.password	Str	+	Пароль администратора тенанта
method	Str	+	Метод API
tenant_id	Str	+	Идентификатор тенанта
actors_ids	Str	+	Идентификаторы учетных записей
time	Str	+	Время регистрации события

Пример ответа:


```
{
  "Response": {
    "changed": false,
    "failed": false,
    "msg": "ok"
  },
  "events": [
    {
      "request_id": "60e48e50-ac11-0009-3500-000000000000",
      "actor_id": "59ed9c03-0c75-47e2-ac12-eacf6f775431",
      "method": {
        "code": "METHOD_ERAKLES_CHANGE_STATUS",
        "name": "METHOD_ERAKLES_CHANGE_STATUS"
      },
      "time": {
        "unixmicro": "1663331652000000",
        "zone": 10800,
        "zone_name": ""
      },
      "touches": null,
      "client_ip": "10.7.98.71",
      "streamseq": "0"
    },
    {
      "request_id": "60e48e50-ac11-0009-3700-000000000000",
      "actor_id": "59ed9c03-0c75-47e2-ac12-eacf6f775431",
      "method": {
        "code": "METHOD_ERAKLES_CHANGE_STATUS",
        "name": "METHOD_ERAKLES_CHANGE_STATUS"
      },
      "time": {
        "unixmicro": "1663331652000000",
        "zone": 10800,
```

```
        "zone_name": ""
      },
      "touches": null,
      "client_ip": "10.7.98.71",
      "streamseq": "0"
    }
  ],
  "next": {
    "time": {
      "unixmicro": "1663331652000000",
      "zone": 10800
    },
    "requestId": "60e48e50-ac11-0009-3700-000000000000",
    "actorId": "59ed9c03-0c75-47e2-ac12-eacf6f775431",
    "methodCode": "METHOD_ERAKLES_CHANGE_STATUS"
  },
  "is_final": false
}
```


16.4.2.2 Операции над доменом

16.4.2.2.1 Создание домена

Для создания домена необходимо выполнить запрос:

```
nct_ministerium get_audit_events_by_methods_codes
--config ministerium.json
--admin.login <…>
--admin.password <…>
--methods_names METHOD_DAIDAL_CREATE_DOMAIN
--tenant_id 01068ade-1cce-4125-ab6b-91d977ecf85b
--actors_ids 59ed9c03-0c75-47e2-ac12-eacf6f775431
--timestamp_from 2022-09-16T05:00:00+00:00
--timestamp_to 2022-09-16T06:00:00+00:00
--limit 2
```

Описание параметров запроса приведено в таблице 193.

Таблица 193 – Описание параметров запроса на создание домена

Параметр	Тип	Обязательный	Описание
admin.login	Str	+	Логин администратора тенанта
admin.password	Str	+	Пароль администратора тенанта
method	Str	+	Метод API
tenant_id	Str	+	Идентификатор тенанта
actors_ids	Str	+	Идентификаторы учетных записей
time	Str	+	Время регистрации события

Пример ответа:


```
{
  "Response": {
    "changed": false,
    "failed": false,
    "msg": "ok"
  },
  "events": [
    {
      "request_id": "3bb37f4c-ac11-0009-ad2c-000000000000",
      "actor_id": "59ed9c03-0c75-47e2-ac12-eacf6f775431",
      "method": {
        "code": "METHOD_DAIDAL_CREATE_DOMAIN",
        "name": "METHOD_DAIDAL_CREATE_DOMAIN"
      },
      "time": {
        "unixmicro": "1663306692000000",
        "zone": 10800,
        "zone_name": ""
      },
      "touches": null,
      "client_ip": "10.7.98.54",
      "streamseq": "0"
    },
    {
      "request_id": "3bb37f4c-ac11-0009-ad2c-000000000000",
      "actor_id": "59ed9c03-0c75-47e2-ac12-eacf6f775431",
      "method": {
        "code": "METHOD_DAIDAL_CREATE_DOMAIN",
        "name": "METHOD_DAIDAL_CREATE_DOMAIN"
      },
      "time": {
        "unixmicro": "1663306692000000",
        "zone": 10800,
        "zone_name": ""
      },
      "response": {
        "@type": "catalog.daidal.v1.CreateDomainResponse",
        "error": {
          "module": "INTERNAL",
          "code": 2001,
          "msg": "",
          "details": []
        },
        "id": ""
      },
      "touches": null,
      "client_ip": "10.7.98.54",
      "streamseq": "0"
    }
  ],
  "next": {
    "time": {
      "unixmicro": "1663306692000000",
      "zone": 10800
    },
    "requestId": "3bb37f4c-ac11-0009-ad2c-000000000000",
    "actorId": "59ed9c03-0c75-47e2-ac12-eacf6f775431",
    "methodCode": "METHOD_DAIDAL_CREATE_DOMAIN"
```

```
  },
  "is_final": false
}
```

16.4.2.2.2 Обновление домена

Для обновления домена необходимо выполнить запрос:

```
nct_ministerium get_audit_events_by_methods_codes
--config ministerium.json
--admin.login <…>
--admin.password <…>
--methods_names METHOD_MINISTERIUM_UPDATE_GROUP_PROFILE
--tenant_id 01068ade-1cce-4125-ab6b-91d977ecf85b
--actors_ids 59ed9c03-0c75-47e2-ac12-eacf6f775431
--timestamp_from 2022-09-16T05:00:00+00:00
--timestamp_to 2022-09-16T06:00:00+00:00
--limit 2
```

Описание параметров запроса приведено в таблице 194.

Таблица 194 – Описание параметров запроса на обновление домена

Параметр	Тип	Обязательный	Описание
admin.login	Str	+	Логин администратора тенанта
admin.password	Str	+	Пароль администратора тенанта
method	Str	+	Метод API
tenant_id	Str	+	Идентификатор тенанта
actors_ids	Str	+	Идентификаторы учетных записей
time	Str	+	Время регистрации события

Пример ответа:

```
{
  "Response": {
    "changed": false,
    "failed": false,
    "msg": "ok"
  },
  "events": [

      "request_id": "3bb37f4c-ac11-0009-b22c-000000000000",
      "actor_id": "59ed9c03-0c75-47e2-ac12-eacf6f775431",
      "method": {
        "code": "METHOD_DAIDAL_UPDATE_DOMAIN",
        "name": "METHOD_DAIDAL_UPDATE_DOMAIN"
      },
      "time": {
        "unixmicro": "1663306704000000",
        "zone": 10800,
        "zone_name": ""
```

```
      },
      "touches": null,
      "client_ip": "10.7.98.54",
      "streamseq": "0"
    },
    {
      "request_id": "3bb37f4c-ac11-0009-b22c-000000000000",
      "actor_id": "59ed9c03-0c75-47e2-ac12-eacf6f775431",
      "method": {
        "code": "METHOD_DAIDAL_UPDATE_DOMAIN",
        "name": "METHOD_DAIDAL_UPDATE_DOMAIN"
      },
      "time": {
        "unixmicro": "1663306704000000",
        "zone": 10800,
        "zone_name": ""
      },
      "response": {
        "@type": "catalog.daidal.v1.UpdateDomainResponse",
        "error": {
          "module": "INTERNAL",
          "code": 2001,
          "msg": "",
          "details": []
        }
      },
      "touches": null,
      "client_ip": "10.7.98.54",
      "streamseq": "0"
    }
  ],
  "next": {
    "time": {
      "unixmicro": "1663306704000000",
      "zone": 10800
    },
    "requestId": "3bb37f4c-ac11-0009-b22c-000000000000",
    "actorId": "59ed9c03-0c75-47e2-ac12-eacf6f775431",
    "methodCode": "METHOD_DAIDAL_UPDATE_DOMAIN"
  },
  "is_final": false
}
```


16.4.2.2.3 Удаление домена

Для удаления домена необходимо выполнить запрос:

```
nct_ministerium get_audit_events_by_methods_codes
--config ministerium.json
--admin.login <…>
--admin.password <…>
--methods_names METHOD_DAIDAL_DELETE_BY_IDS
--tenant_id 01068ade-1cce-4125-ab6b-91d977ecf85b
--actors_ids 59ed9c03-0c75-47e2-ac12-eacf6f775431
--timestamp_from 2022-09-16T05:00:00+00:00
--timestamp_to 2022-09-16T06:00:00+00:00
--limit 2
```

Описание параметров запроса приведено в таблице 195.

Таблица 195 – Описание параметров запроса на удаление домена

Параметр	Тип	Обязательный	Описание
admin.login	Str	+	Логин администратора тенанта
admin.password	Str	+	Пароль администратора тенанта
method	Str	+	Метод API
tenant_id	Str	+	Идентификатор тенанта
actors_ids	Str	+	Идентификаторы учетных записей
time	Str	+	Время регистрации события

Пример ответа:


```
{
  "Response": {
    "changed": false,
    "failed": false,
    "msg": "ok"
  },
  "events": [
    {
      "request_id": "3bb37f4c-ac11-0009-bc2c-000000000000",
      "actor_id": "59ed9c03-0c75-47e2-ac12-eacf6f775431",
      "method": {
        "code": "METHOD_DAIDAL_DELETE_BY_IDS",
        "name": "METHOD_DAIDAL_DELETE_BY_IDS"
      },
      "time": {
        "unixmicro": "1663306714000000",
        "zone": 10800,
        "zone_name": ""
      },
      "touches": null,
      "client_ip": "10.7.98.54",
      "streamseq": "0"
    },
    {
      "request_id": "3bb37f4c-ac11-0009-bc2c-000000000000",
      "actor_id": "59ed9c03-0c75-47e2-ac12-eacf6f775431",
      "method": {
        "code": "METHOD_DAIDAL_DELETE_BY_IDS",
        "name": "METHOD_DAIDAL_DELETE_BY_IDS"
      },
      "time": {
        "unixmicro": "1663306714000000",
        "zone": 10800,
        "zone_name": ""
      },
      "response": {
        "@type": "catalog.daidal.v1.DeleteByIDsResponse",
        "error": {
```

```
          "module": "INTERNAL",
          "code": 200,
          "msg": "",
          "details": []
        },
        "deleted_ids": [],
        "not_deleted": []
      },
      "touches": null,
      "client_ip": "10.7.98.54",
      "streamseq": "0"
    }
  ],
  "next": {
    "time": {
      "unixmicro": "1663306714000000",
      "zone": 10800
    },
    "requestId": "3bb37f4c-ac11-0009-bc2c-000000000000",
    "actorId": "59ed9c03-0c75-47e2-ac12-eacf6f775431",
    "methodCode": "METHOD_DAIDAL_DELETE_BY_IDS"
  },
  "is_final": false
}
```


16.4.2.3 Операции над ресурсом

16.4.2.3.1 Создание ресурса

Для создания ресурса необходимо выполнить запрос:

```
nct_ministerium get_audit_events_by_methods_codes
--config ministerium.json
--admin.login <…>
--admin.password <…>
--methods_names METHOD_MINISTERIUM_CREATE_RESOURCE
--tenant_id 01068ade-1cce-4125-ab6b-91d977ecf85b
--actors_ids 59ed9c03-0c75-47e2-ac12-eacf6f775431
--timestamp_from 2022-09-16T05:00:00+00:00
--timestamp_to 2022-09-16T06:00:00+00:00
--limit 2
```

Описание параметров запроса приведено в таблице 196.

Таблица 196 – Описание параметров запроса на создание ресурса

Параметр	Тип	Обязательный	Описание
admin.login	Str	+	Логин администратора тенанта
admin.password	Str	+	Пароль администратора тенанта
method	Str	+	Метод API
tenant_id	Str	+	Идентификатор тенанта

Параметр	Тип	Обязательный	Описание
actors_ids	Str	+	Идентификаторы учетных записей
time	Str	+	Время регистрации события

Пример ответа:


```
{
  "Response": {
    "changed": false,
    "failed": false,
    "msg": "ok"
  },
  "events": [
    {
      "request_id": "f7def38d-f6ec-41c2-838b-e0459bf2b854",
      "actor_id": "59ed9c03-0c75-47e2-ac12-eacf6f775431",
      "method": {
        "code": "METHOD_MINISTERIUM_CREATE_RESOURCE",
        "name": "METHOD_MINISTERIUM_CREATE_RESOURCE"
      },
      "time": {
        "unixmicro": "1663305042000000",
        "zone": 10800,
        "zone_name": ""
      },
      "request": {
        "@type": "type.googleapis.com/ministerium.v1.MinisteriumCommand",
        "name": "create_resource",
                "input":  "{\"tls_settings\":{\"ca_file\":\"/builds/0/mail-back-
tests/certs/ca.pem\",\"client_cert_file\":\"/builds/0/mail-back-
tests/certs/client_crt.pem\",\"server_cert_file\":\"\",\"key_file\":
\"/builds/0/mail-back-tests/certs/client_key.pem\",\"server_name_override\":
\"\",\"client_auth_type\":\"\",\"tls_min_version\":\"\",
\"prefer_server_cipher_suites\":false,\"use_tls_bundle\":false},\"cox\":
{\"endpoint\":\"grpc-install.example.net:3142\",\"balancer_endpoint\":
\"hydra.ucs-apps-1.install.example.net:50053\",\"balancer_endpoints\":null,
\"service_name\":\"cox\",\"load_balanced\":false,\"use_tls\":true,
\"use_tls_balancer\":false,\"request_timeout\":\"10s\",\"max_send_size\":\"0B\",
\"max_recv_size\":\"0B\",\"compression\":\"none\",\"is_external\":false},
\"token-name\":\"ucs-access-token\",\"admin\":{\"login\":
\"admin_tenant@install.example.net\",\"password\":\"bKv9jqZ9PSwqKD7s\"},
\"tenant_id\":\"01068ade-1cce-4125-ab6b-91d977ecf85b\",\"region_id\":\"2dbacea3-
5889-4021-8f38-bc2214dd7423\",\"email\":
\"resource_atangkcvob@install.example.net\",\"login\":\"\",\"password\":\"\",
\"type\":\"MEETING_ROOM\",\"profile\":{\"name\":
\"autotest_resource_1663294241\",\"description\":\"Пропаганда
четко._1663294241\",\"location\":\"г.    Казань_0.2871,0.4561\",\"geolocation\":
\"0.2471,0.5491\",\"company\":\"organization_1663294241\",\"department\":
\"department_1663294241\",\"capacity\":8},\"gal_tags\":[\"0c22be2e-1e2f-5f6d-
bec5-842c5d48e9d3\"],\"autobook\":true,\"work_status\":true,\"locale\":
\"en_US\"}"
      },
      "touches": null,
      "client_ip": "172.17.0.2",
      "streamseq": "0"
    },
```

```
    {
      "request_id": "f7def38d-f6ec-41c2-838b-e0459bf2b854",
      "actor_id": "59ed9c03-0c75-47e2-ac12-eacf6f775431",
      "method": {
        "code": "METHOD_MINISTERIUM_CREATE_RESOURCE",
        "name": "METHOD_MINISTERIUM_CREATE_RESOURCE"
      },
      "time": {
        "unixmicro": "1663305049000000",
        "zone": 10800,
        "zone_name": ""
      },
      "response": {
        "@type": "type.googleapis.com/ministerium.v1.MinisteriumCommand",
        "name": "create_resource",
           "output": "{\"Response\":{\"changed\":true,\"failed\":false,\"msg\":
\"ok\"},\"id\":\"3e5bb5f6-841b-4119-a9bb-480101759253\"}"
      },
      "touches": null,
      "client_ip": "172.17.0.2",
      "streamseq": "0"
    }
  ],
  "next": {
    "time": {
      "unixmicro": "1663305049000000",
      "zone": 10800
    },
    "requestId": "f7def38d-f6ec-41c2-838b-e0459bf2b854",
    "actorId": "59ed9c03-0c75-47e2-ac12-eacf6f775431",
    "methodCode": "METHOD_MINISTERIUM_CREATE_RESOURCE"
  },
  "is_final": false
}
```


16.4.2.3.2 Обновление ресурса

Для обновления ресурса необходимо выполнить запрос:

```
nct_ministerium get_audit_events_by_methods_codes
--config ministerium.json
--admin.login <…>
--admin.password <…>
--methods_names METHOD_MINISTERIUM_UPDATE_RESOURCE_PROFILE
--tenant_id 01068ade-1cce-4125-ab6b-91d977ecf85b
--actors_ids 59ed9c03-0c75-47e2-ac12-eacf6f775431
--timestamp_from 2022-09-16T05:00:00+00:00
--timestamp_to 2022-09-16T06:00:00+00:00
--limit 2
```

Описание параметров запроса приведено в таблице 197.

Таблица 197 – Описание параметров запроса на обновление ресурса

Параметр	Тип	Обязательный	Описание
admin.login	Str	+	Логин администратора тенанта

Параметр	Тип	Обязательный	Описание
admin.password	Str	+	Пароль администратора тенанта
method	Str	+	Метод API
tenant_id	Str	+	Идентификатор тенанта
actors_ids	Str	+	Идентификаторы учетных записей
time	Str	+	Время регистрации события

Пример ответа:


```
{
  "Response": {
    "changed": false,
    "failed": false,
    "msg": "ok"
  },
  "events": [
    {
      "request_id": "68cf1d91-addc-4c9b-beb1-f40ba61ad385",
      "actor_id": "59ed9c03-0c75-47e2-ac12-eacf6f775431",
      "method": {
        "code": "METHOD_MINISTERIUM_UPDATE_RESOURCE_PROFILE",
        "name": "METHOD_MINISTERIUM_UPDATE_RESOURCE_PROFILE"
      },
      "time": {
        "unixmicro": "1663306885000000",
        "zone": 10800,
        "zone_name": ""
      },
      "request": {
        "@type": "type.googleapis.com/ministerium.v1.MinisteriumCommand",
        "name": "update_resource_profile",
                "input":  "{\"tls_settings\":{\"ca_file\":\"/builds/0/mail-back-
tests/certs/ca.pem\",\"client_cert_file\":\"/builds/0/mail-back-
tests/certs/client_crt.pem\",\"server_cert_file\":\"\",\"key_file\":
\"/builds/0/mail-back-tests/certs/client_key.pem\",\"server_name_override\":
\"\",\"client_auth_type\":\"\",\"tls_min_version\":\"\",
\"prefer_server_cipher_suites\":false,\"use_tls_bundle\":false},\"cox\":
{\"endpoint\":\"grpc-install.example.net:3142\",\"balancer_endpoint\":
\"hydra.ucs-apps-1.install.example.net:50053\",\"balancer_endpoints\":null,
\"service_name\":\"cox\",\"load_balanced\":false,\"use_tls\":true,
\"use_tls_balancer\":false,\"request_timeout\":\"10s\",\"max_send_size\":\"0B\",
\"max_recv_size\":\"0B\",\"compression\":\"none\",\"is_external\":false},
\"token-name\":\"ucs-access-token\",\"admin\":{\"login\":
\"admin_tenant@install.example.net\",\"password\":\"bKv9jqZ9PSwqKD7s\"},
\"entity_id\":\"b012ff77-7555-4c39-9797-478a52bec6b5\",\"profile\":{\"name\":
\"autotest_resource_1663296085\",\"description\":\"Скрытый
решение._1663296085\",\"location\":\"ст.  Бийск_0.5581,0.6351\",\"geolocation\":
\"0.3011,0.1181\",\"company\":\"organization_1663296085\",\"department\":
\"department_1663296085\",\"capacity\":29},\"create\":false,\"gal_tags\":
[\"0c22be2e-1e2f-5f6d-bec5-842c5d48e9d3\"],\"gal_region_id\":\"2dbacea3-5889-
4021-8f38-bc2214dd7423\"}"
      },
      "touches": null,
```

```
      "client_ip": "172.17.0.2",
      "streamseq": "0"
    },
    {
      "request_id": "68cf1d91-addc-4c9b-beb1-f40ba61ad385",
      "actor_id": "59ed9c03-0c75-47e2-ac12-eacf6f775431",
      "method": {
        "code": "METHOD_MINISTERIUM_UPDATE_RESOURCE_PROFILE",
        "name": "METHOD_MINISTERIUM_UPDATE_RESOURCE_PROFILE"
      },
      "time": {
        "unixmicro": "1663306886000000",
        "zone": 10800,
        "zone_name": ""
      },
      "response": {
        "@type": "type.googleapis.com/ministerium.v1.MinisteriumCommand",
        "name": "update_resource_profile",
        "output": "{\"changed\":true,\"failed\":false,\"msg\":\"ok\"}"
      },
      "touches": null,
      "client_ip": "172.17.0.2",
      "streamseq": "0"
    }
  ],
  "next": {
    "time": {
      "unixmicro": "1663306886000000",
      "zone": 10800
    },
    "requestId": "68cf1d91-addc-4c9b-beb1-f40ba61ad385",
    "actorId": "59ed9c03-0c75-47e2-ac12-eacf6f775431",
    "methodCode": "METHOD_MINISTERIUM_UPDATE_RESOURCE_PROFILE"
  },
  "is_final": false
}
```


16.4.2.4 Операции над группами

16.4.2.4.1 Удаление группы

Для удаления группы необходимо выполнить запрос:

```
nct_ministerium get_audit_events_by_methods_codes
--config ministerium.json
--admin.login <…>
--admin.password <…>
--methods_names METHOD_MINISTERIUM_DELETE_GROUP
--tenant_id 01068ade-1cce-4125-ab6b-91d977ecf85b
--actors_ids 59ed9c03-0c75-47e2-ac12-eacf6f775431
--timestamp_from 2022-09-16T05:00:00+00:00
--timestamp_to 2022-09-16T06:00:00+00:00
--limit 2
```

Описание параметров запроса приведено в таблице 198.

Таблица 198 – Описание параметров запроса на удаление группы

Параметр	Тип	Обязательный	Описание
admin.login	Str	+	Логин администратора тенанта
admin.password	Str	+	Пароль администратора тенанта
method	Str	+	Метод API
tenant_id	Str	+	Идентификатор тенанта
actors_ids	Str	+	Идентификаторы учетных записей
time	Str	+	Время регистрации события

Пример ответа:


```
{
  "Response": {
    "changed": false,
    "failed": false,
    "msg": "ok"
  },
  "events": [
    {
      "request_id": "9f39cb5d-8dde-4b62-9921-dcf72eb238cc",
      "actor_id": "59ed9c03-0c75-47e2-ac12-eacf6f775431",
      "method": {
        "code": "METHOD_MINISTERIUM_DELETE_GROUP",
        "name": "METHOD_MINISTERIUM_DELETE_GROUP"
      },
      "time": {
        "unixmicro": "1663306828000000",
        "zone": 10800,
        "zone_name": ""
      },
      "request": {
        "@type": "type.googleapis.com/ministerium.v1.MinisteriumCommand",
        "name": "delete_group",
        "input": "{\"tls_settings\":{\"ca_file\":\"/builds/0/mail-back-
tests/certs/ca.pem\",\"client_cert_file\":\"/builds/0/mail-back-
tests/certs/client_crt.pem\",\"server_cert_file\":\"\",\"key_file\":
\"/builds/0/mail-back-tests/certs/client_key.pem\",\"server_name_override\":
\"\",\"client_auth_type\":\"\",\"tls_min_version\":\"\",
\"prefer_server_cipher_suites\":false,\"use_tls_bundle\":false},\"cox\":
{\"endpoint\":\"grpc-install.example.net:3142\",\"balancer_endpoint\":
\"hydra.ucs-apps-1.install.example.net:50053\",\"balancer_endpoints\":null,
\"service_name\":\"cox\",\"load_balanced\":false,\"use_tls\":true,
\"use_tls_balancer\":false,\"request_timeout\":\"10s\",\"max_send_size\":\"0B\",
\"max_recv_size\":\"0B\",\"compression\":\"none\",\"is_external\":false},
\"token-name\":\"ucs-access-token\",\"admin\":{\"login\":
\"admin_tenant@install.example.net\",\"password\":\"bKv9jqZ9PSwqKD7s\"},
\"group_id\":\"4779ebcb-0eb9-4b21-82c3-53afc79278f3\"}
      },
      "touches": null,
      "client_ip": "172.17.0.2",
      "streamseq": "0"
```

```
    },
    {
      "request_id": "9f39cb5d-8dde-4b62-9921-dcf72eb238cc",
      "actor_id": "59ed9c03-0c75-47e2-ac12-eacf6f775431",
      "method": {
        "code": "METHOD_MINISTERIUM_DELETE_GROUP",
        "name": "METHOD_MINISTERIUM_DELETE_GROUP"
      },
      "time": {
        "unixmicro": "1663306830000000",
        "zone": 10800,
        "zone_name": ""
      },
      "response": {
        "@type": "type.googleapis.com/ministerium.v1.MinisteriumCommand",
        "name": "delete_group",
        "output": "{\"changed\":true,\"failed\":false,\"msg\":\"ok\"}"
      },
      "touches": null,
      "client_ip": "172.17.0.2",
      "streamseq": "0"
    }
  ],
  "next": {
    "time": {
      "unixmicro": "1663306830000000",
      "zone": 10800
    },
    "requestId": "9f39cb5d-8dde-4b62-9921-dcf72eb238cc",
    "actorId": "59ed9c03-0c75-47e2-ac12-eacf6f775431",
    "methodCode": "METHOD_MINISTERIUM_DELETE_GROUP"
  },
  "is_final": false
}
```


16.4.2.4.2 Обновление профиля группы

Для обновления профиля группы необходимо выполнить запрос:

```
nct_ministerium get_audit_events_by_methods_codes
--config ministerium.json
--admin.login <…>
--admin.password <…>
--methods_names METHOD_MINISTERIUM_UPDATE_GROUP_PROFILE
--tenant_id 01068ade-1cce-4125-ab6b-91d977ecf85b
--actors_ids 59ed9c03-0c75-47e2-ac12-eacf6f775431
--timestamp_from 2022-09-16T05:00:00+00:00
--timestamp_to 2022-09-16T06:00:00+00:00
--limit 2
```

Описание параметров запроса приведено в таблице 199.

Таблица 199 – Описание параметров запроса на обновление профиля группы

Параметр	Тип	Обязательный	Описание
admin.login	Str	+	Логин администратора тенанта

Параметр	Тип	Обязательный	Описание
admin.password	Str	+	Пароль администратора тенанта
method	Str	+	Метод API
tenant_id	Str	+	Идентификатор тенанта
actors_ids	Str	+	Идентификаторы учетных записей
time	Str	+	Время регистрации события

Пример ответа:


```
{
  "Response": {
    "changed": false,
    "failed": false,
    "msg": "ok"
  },
  "events": [
    {
      "request_id": "e321df1d-61b3-4237-a7e3-a7964674d36a",
      "actor_id": "59ed9c03-0c75-47e2-ac12-eacf6f775431",
      "method": {
        "code": "METHOD_MINISTERIUM_UPDATE_GROUP_PROFILE",
        "name": "METHOD_MINISTERIUM_UPDATE_GROUP_PROFILE"
      },
      "time": {
        "unixmicro": "1663306825000000",
        "zone": 10800,
        "zone_name": ""
      },
      "request": {
        "@type": "type.googleapis.com/ministerium.v1.MinisteriumCommand",
        "name": "update_group_profile",
        "input": "{\"tls_settings\":{\"ca_file\":\"/builds/0/mail-back-
tests/certs/ca.pem\",\"client_cert_file\":\"/builds/0/mail-back-
tests/certs/client_crt.pem\",\"server_cert_file\":\"\",\"key_file\":
\"/builds/0/mail-back-tests/certs/client_key.pem\",\"server_name_override\":
\"\",\"client_auth_type\":\"\",\"tls_min_version\":\"\",
\"prefer_server_cipher_suites\":false,\"use_tls_bundle\":false},\"cox\":
{\"endpoint\":\"grpc-install.example.net:3142\",\"balancer_endpoint\":
\"hydra.ucs-apps-1.install.example.net:50053\",\"balancer_endpoints\":null,
\"service_name\":\"cox\",\"load_balanced\":false,\"use_tls\":true,
\"use_tls_balancer\":false,\"request_timeout\":\"10s\",\"max_send_size\":\"0B\",
\"max_recv_size\":\"0B\",\"compression\":\"none\",\"is_external\":false},
\"token-name\":\"ucs-access-token\",\"admin\":{\"login\":
\"admin_tenant@install.example.net\",\"password\":\"bKv9jqZ9PSwqKD7s\"},
\"entity_id\":\"4779ebcb-0eb9-4b21-82c3-53afc79278f3\",\"profile\":{\"name\":
\"group_1663296024_jftakbfbov\",\"description\":\"Торговля помолчать
предоставить исполнять сопровождаться горький кузнец.\"},\"create\":false,
\"gal_tags\":[],\"gal_region_id\":\"\"}"
      },
      "touches": null,
      "client_ip": "172.17.0.2",
      "streamseq": "0"
    },
    {
      "request_id": "e321df1d-61b3-4237-a7e3-a7964674d36a",
```

```
      "actor_id": "59ed9c03-0c75-47e2-ac12-eacf6f775431",
      "method": {
        "code": "METHOD_MINISTERIUM_UPDATE_GROUP_PROFILE",
        "name": "METHOD_MINISTERIUM_UPDATE_GROUP_PROFILE"
      },
      "time": {
        "unixmicro": "1663306827000000",
        "zone": 10800,
        "zone_name": ""
      },
      "response": {
        "@type": "type.googleapis.com/ministerium.v1.MinisteriumCommand",
        "name": "update_group_profile",
        "output": "{\"changed\":true,\"failed\":false,\"msg\":\"ok\"}"
      },
      "touches": null,
      "client_ip": "172.17.0.2",
      "streamseq": "0"
    }
  ],
  "next": {
    "time": {
      "unixmicro": "1663306827000000",
      "zone": 10800
    },
    "requestId": "e321df1d-61b3-4237-a7e3-a7964674d36a",
    "actorId": "59ed9c03-0c75-47e2-ac12-eacf6f775431",
    "methodCode": "METHOD_MINISTERIUM_UPDATE_GROUP_PROFILE"
  },
  "is_final": false
}
```


16.5 Перечень регистрируемых методов API

В таблицах 200 и 201 представлено соответствие реализованных бизнес-функций отправляемым API-запросам в рамках ПО «Mailion».

Таблица 200 – Перечень отслеживаемых запросов при функционировании сервиса homeros

Название события	Список запросов
Подсистема «Каталог»	
Создание пользователя/User Create	v1/erakles/create_entities v1/erakles/create_emails v1/erakles/create_logins v1/theseus/create_credentials v1/erakles/change_status v1/sophokles/subjects_init v1/perseus/save_profile

Название события	Список запросов
	Проверка логина: v1/erakles/get_entity_by_login Проверка email: v1/erakles/get_entities_by_emails Добавление в организацию: v1/arachne/link/operate Добавление аватара: v1/achill/get_all_avatars v1/achill/save_avatar Наличие ошибок в запросах: v1/erakles/change_status v1/erakles/delete_email v1/erakles/delete_login v1/achill/remove_avatar Фронтенд-рендеринг: v1/perseus/get_group_entities
Удаление пользователя/User Delete	v1/erakles/change_status Фронтенд-рендеринг: v1/perseus/get_group_entities
Создание локальной адресной книги	v1/marker/create_usertag Фронтенд-рендеринг: v1/marker/get_tags_by_ids v1/marker/get_tag_subtree
Переименование локальной адресной книги	v1/marker/rename_tag Фронтенд-рендеринг: v1/marker/get_tag_subtree v1/mixer/get_objects_sorted_filtered
Перемещение локальной адресной книги	v1/marker/rename_tag Фронтенд-рендеринг: v1/marker/get_tag_subtree v1/mixer/get_objects_sorted_filtered
Удаление локальной адресной книги	v1/marker/delete_usertag

Название события	Список запросов
	Фронтенд-рендеринг: v1/marker/get_tag_subtree v1/mixer/get_objects_sorted_filtered
Создание контакта в адресной книге	v1/perseus/create_contact Фронтенд-рендеринг: v1/mixer/get_objects_by_ids v1/dafnis/get_profile
Удаление контакта в адресной книге	v1/marker/remove_tags_from_objects Фронтенд-рендеринг: v1/mixer/get_objects_by_ids v1/dafnis/get_profile
Создание группы рассылки Создание группы/Create a Group	v1/erakles/create_entities v1/erakles/create_emails v1/perseus/save_profile Добавление аватара: v1/achill/save_avatar Фронтенд-рендеринг: v1/erakles/get_entities_by_emails v1/perseus/get_group_entities
Изменение группы рассылки Изменение группы/Change a Group	v1/perseus/update_profile Изменение аватара: v1/achill/get_all_avatars v1/achill/save_avatar v1/achill/remove_avatar Обновление параметра group: v1/perseus/get_profile v1/iolaos/get_dynamic_group_filling_status
Удаление группы рассылки Удаление группы/Delete a Group	v1/erakles/change_status
Шаринг аккаунта	v1/erakles/set_shared_access
Отменить шаринг аккаунта	v1/erakles/unset_shared_access
Добавление пользователя в группу/Add a User	v1/erakles/adopt_entities
Удаление пользователя из группы/Delete a User	v1/erakles/leave_from_group

Название события	Список запросов
	Фронтенд-рендеринг: v1/perseus/get_group_entities
Создание подразделения/Create a Subdivision	v1/arachne/organizational_unit/save v1/arachne/link/operate Фронтенд-рендеринг: v1/arachne/entities_list
Создание проектной группы/Create a Workgroup	v1/arachne/organizational_group/save Фронтенд-рендеринг: v1/arachne/entities_list
Создание новой должности в справочнике оргструктуры/Create Occupations	v1/arachne/occupation/save v1/arachne/link/operate Фронтенд-рендеринг: v1/arachne/occupations
Удаление подразделения/Delete an Subdivision	v1/arachne/organizational_unit/delete
Удаление проектной группы/Delete an Workgroup	v1/arachne/organizational_group/delete
Удаление должности в справочнике оргструктуры/Delete an Entity	v1/arachne/occupation/delete
Создание ресурса/Create a Resource	v1/erakles/create_entities v1/erakles/create_emails v1/erakles/create_logins v1/perseus/save_profile v1/theseus/create_credentials v1/erakles/change_status v1/sophokles/subjects_init Проверка логина: v1/erakles/get_entity_by_login Проверка email: v1/erakles/get_entities_by_emails Добавление аватара: v1/achill/get_all_avatars v1/achill/save_avatar Наличие ошибок в запросах: v1/erakles/change_status

Название события	Список запросов
	v1/erakles/delete_email v1/erakles/delete_login v1/achill/remove_avatar Фронтенд-рендеринг: v1/perseus/get_group_entities
Удаление ресурса/Delete a Resource	v1/erakles/change_status
Обновить ресурс/Update resource	v1/erakles/update_entity v1/perseus/update_profile Изменение логина: v1/erakles/delete_login v1/erakles/get_entity_by_login v1/erakles/create_logins v1/theseus/create_credentials Изменение аватара: v1/achill/get_all_avatars v1/achill/remove_avatar v1/achill/save_avatar
Выход из системы/Log Out	v1/minos/delete_all_sessions
Изменение пароля/Change a Password	v1/theseus/change_password Изменение пароля в профиле: v1/theseus/create_credentials
Изменение профиля пользователя/Change User Profile	v1/perseus/update_profile Изменение настроек: v1/erakles/update_entity Изменение логина: v1/erakles/get_entity_by_login v1/erakles/create_logins v1/theseus/create_credentials v1/erakles/delete_login Изменение email: v1/erakles/delete_email v1/erakles/get_entities_by_emails v1/erakles/create_emails Изменения в организационной структуре: v1/arachne/link/operate

Название события	Список запросов
	Изменение аватара: v1/achill/get_all_avatars v1/achill/remove_avatar v1/achill/save_avatar Изменение контактов: v1/erakles/update_entity v1/perseus/update_profile
Блокирование пользователя/Block a User	v1/erakles/change_status v1/erakles/set_blocking_reason
Настройка календаря/Calendar settings changed	v1/hog/update_calendar_schedule Изменение часового пояса: v1/hog/set_timezone Изменение событий приглашения: v1/hog/update_allow_ics_without_me Изменение напоминания о событиях: v1/hog/update_default_calendar_alarm Фронтенд-рендеринг: v1/hog/get_settings
Подсистема «Почта»	
Создание папки/Create a folder	v1/marker/create_usertag
Переименование папки/Rename folder	v1/marker/rename_tag
Удаление папки/Delete a folder	v1/marker/delete_usertag
Очистка папки «Удаленные»/Empty Trash	v1/marker/empty_tag_content
Отправка нового сообщения/Message Sent Сообщение успешно отправлено/Message Sent Successfully	v1/atlas/send_drafted v1/atlas/send_drafted_async
Отзыв сообщения/Message revoke	v1/atlas/revoke
Открыто|Сохранено вложение/Attachment opened| downloaded	attach/read doc_preview

Название события	Список запросов
Пересылка сообщения/Forward message	v1/atlas/send_drafted
Отметить прочитанным/Mark as read	marker/update_flag Фронтенд-рендеринг письма: mixer/get_objects_by_ids
Отметить непрочитанным/Mark as unread	marker/update_flag Фронтенд-рендеринг письма: mixer/get_objects_by_ids
Отметить как спам/Mark as Spam	v1/marker/delete_objects Фронтенд-рендеринг письма в новой папке: mixer/get_objects_by_ids
Копирование сообщения/Copy message	marker/add_tags_to_objects Фронтенд-рендеринг письма в новой папке: mixer/get_objects_by_ids
Перемещение сообщения/Move message	marker/move_tags_from_objects
Создание фильтра сообщений/Create message filter	v1/hog/add_rule Фронтенд-рендеринг настроек: hog/get_settings
Настройка автоматического ответа/Set automatic reply	atlas/save_template hog/update_auto_respond_event_invitations hog/edit_rule Сохранение настроек автоматического ответа: atlas hog/update_auto_respond_event_invitations hog/edit_rule Фронтенд-рендеринг настроек: hog/get_settings weaver/build_message dafnis/get_profile
Архивация сообщений/Archive message	marker/move_tags_from_objects Фронтенд-рендеринг письма в новой папке: mixer/get_objects_by_ids

Название события	Список запросов
Удаление сообщения/Message delete	marker/delete_objects Фронтенд-рендеринг письма в новой папке/исключение удаленного письма из списка писем: mixer/get_objects_by_ids
Вставка объекта в сообщение/Insert object into message body	attach/load_embed Передача двоичного кода вставленного объекта: attach/load_embed Фронтенд-рендеринг вставленного объекта: mixer/get_objects_by_ids

Таблица 201 – Перечень отслеживаемых команд IMAP

Команда IMAP	Описание события	Название события
CAPABILITY	Запрос списка возможностей сервера IMAP, таких как поддерживаемые аутентификационные методы и расширения протокола	
LOGOUT	Завершение сеанса работы с почтовым сервером IMAP	Выход из системы/Log Out
NOOP	Поддержание активного соединения с сервером	
LOGIN	Аутентификация пользователя на почтовом сервере с использованием имени пользователя и пароля	Аутентификация в системе/Authentication
AUTHENTICATE	Аутентификация пользователя с помощью различных механизмов, таких как PLAIN, LOGIN и CRAM-MD5, SASL	Аутентификация в системе/Authentication
LIST	Получение списка почтовых ящиков на сервере	
APPEND	Добавление нового сообщения в указанный почтовый ящик	
CREATE	Создание новой папки на сервере	Создание папки/Create folder
DELETE	Удаление указанной папки	Удаление папки/Delete folder
RENAME	Переименование указанной папки	Переименование папки/Rename folder

Команда IMAP	Описание события	Название события
SUBSCRIBE	Добавление указанного почтового ящика в список подписок пользователя	
UNSUBSCRIBE	Удаление указанного почтового ящика из списка подписок пользователя	
LSUB	Получение списка папок, на которые подписан пользователь	
SELECT	Выбор указанной папки для чтения сообщений	
EXAMINE	Открытие указанного почтового ящика для чтения сообщений без возможности изменения его состояния	
STATUS	Получение информации о состоянии указанного почтового ящика	
FETCH	Получение атрибутов сообщений из указанного почтового ящика	Загрузка сообщения/Fetch Message
CLOSE	Закрытие текущего почтового ящика; удаление сообщений, помеченных для удаления	Удаление сообщения/Message delete
CHECK	Проверка наличия новых сообщений в текущем почтовом ящике	
COPY	Копирование сообщения из одного почтового ящика в другой	Копирование сообщения/Copy message
STORE	Изменение флагов сообщений в указанном почтовом ящике	Отметить прочитанным/Mark as read
EXPUNGE	Удаление сообщений, помеченных для удаления, из текущего почтового ящика	Удаление сообщения/Message delete
SEARCH	Поиск сообщений в указанном почтовом ящике	
UNSELECT	Закрытие текущего почтового ящика без завершения сеанса работы с сервером	
NAMESPACE	Получение пространств имен для почтовых ящиков на сервере	
ID	Получение пространств имен для почтовых ящиков на сервере,	

Команда IMAP	Описание события	Название события
	включая информацию об IMAP-сервере (вендор, версия и т. д.)	
COMPRESS	Инициирование сжатия данных между клиентом и сервером	
MOVE	Перемещение сообщения из одного почтового ящика в другой	Перемещение сообщения/Move message
IDLE	Инициирование длительного ожидания на сервере до появления новых сообщений в указанном почтовом ящике	

16.6 Дополнительные меры защиты ПО «Mailion»

Для предотвращения несанкционированного доступа в отношении файлов конфигурации, относящихся к ПО «Mailion» и содержащихся в каталогах **/srv/docker/*/conf/*/**, рекомендуется обеспечить:

1. Разграничение прав доступа в помещение или стойку с установленными экземплярами ПО «Mailion» согласно составленному «белому списку» работников Клиента, обладающих необходимыми полномочиями.
2. Разграничение прав доступа для программного доступа в хостовую ОС согласно «белому списку» работников Клиента, обладающих необходимыми полномочиями.
3. Использование наложенных сертифицированных средств защиты от несанкционированного доступа.

По умолчанию в отношении каталога **/srv/docker/** установлены права доступа исключительно для суперпользователя, которые наследуются в отношении вложенных каталогов:

```
[root@ucs-infra-1 ~]# ls -ld /srv/docker/
drwxr-x---. 14 root root 189 Jan 10 13:21 /srv/docker/
```

Подробные сведения об администрировании в ОС Astra Linux Special Edition 1.7 представлены в документе «Операционная система специального назначения «Astra Linux Special Edition». Руководство администратора» РУСБ.10015-01 95 01.

17 КАТАСТРОФОУСТОЙЧИВОСТЬ

Установка почтовой системы Mailion предусматривает вариант, поддерживающий режим катастрофоустойчивости. Клиентам предоставляется возможность выбора необходимого варианта инсталляции.

Катастрофоустойчивый режим подразумевает наличие двух ЦОД для хранения инфраструктуры и данных. При временной недоступности или полном уничтожении основного ЦОД вследствие катастрофы происходит переключение работы почтовой системы и каталога на резервный ЦОД.

В а ж н о – Установка и настройка Mailion в режиме катастрофоустойчивости осуществляются силами сотрудников МойОфис.

17.1 Принцип действия

Катастрофоустойчивая установка Mailion состоит из двух Active-Passive кластеров – основного и резервного:

– данные почты хранятся в Dispersed Object Storage (DOS) и копируются на резервный кластер асинхронно, используя внутренние механизмы DOS;
– метаданные почты хранятся в MongoDB и копируются на резервный кластер асинхронно при помощи механизма Mongosync.

В обычном режиме работа происходит на основном кластере (см. Рисунок 102).

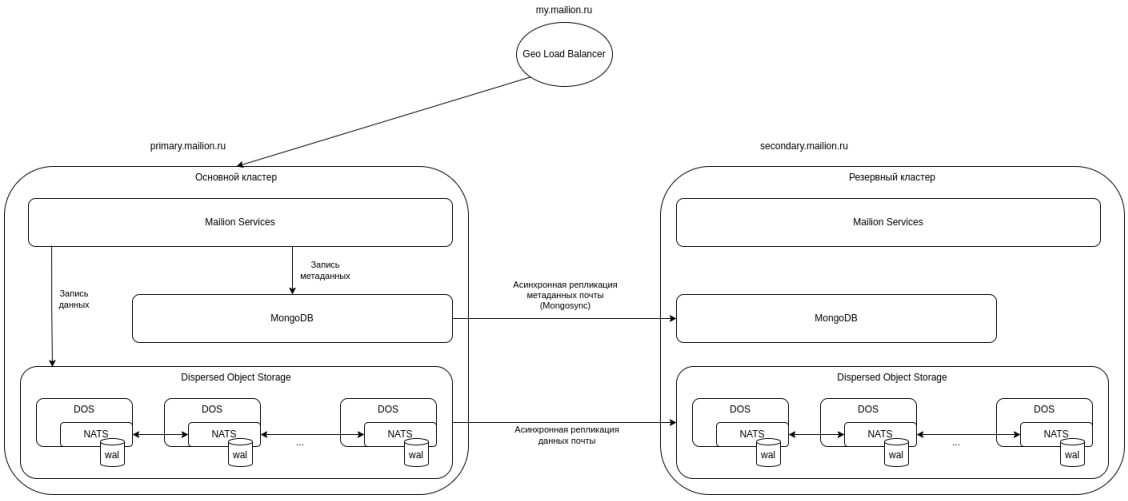


Рисунок 102 – Репликация базы данных между датацентрами

В случае выхода из строя основного кластера администратор переключает нагрузку на резервный кластер (см. Рисунок 103).

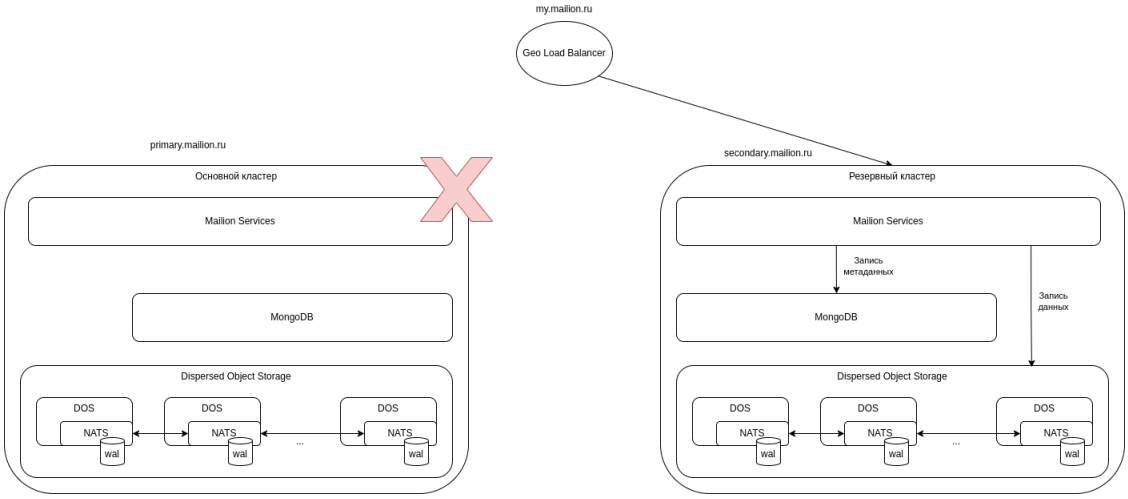


Рисунок 103 – Репликация базы данных между датацентрами

17.1.1 Катастрофоустойчивая установка DOS

Катастрофоустойчивая установка DOS использует копирование Write Ahead Log (WAL) с основного на резервный кластер для асинхронной синхронизации данных DOS:

- при записи данных на основной кластер метаинформация об операции записывается в WAL;
- WAL хранится в отказоустойчивой очереди NATS JetStream (https://docs.nats.io/nats-concepts/jetstream);
- копирование на резервный кластер производится с использованием NATS Replication Sourcing (https://docs.nats.io/running-a-nats-service/nats_admin/jetstream_admin/replication#sources);
- при обработке WAL на резервном кластере данные объекта запрашиваются с ноды основного кластера, которая имеет копию данного объекта, при этом данные объектов между кластерами передаются в уже сжатом виде;
- после получения данных с основного кластера метаданные и данные объекта записываются на резервный кластер.

17.1.1.1 Требования для катастрофоустойчивого развертывания DOS

Требования приведены в таблице 202.

Таблица 202 – Список требований для катастрофоустойчивого развертывания DOS

Требование	Описание

Добавление SSD для WAL DOS (размер зависит от нагрузки на основной кластер и максимального времени, которое система должна переживать недоступность резервного кластера без установки репликации заново)	На каждую ноду кластера добавить SSD. Размер SSD для ноды рассчитать исходя из следующей формулы:
	`size = (max_msgx * 370 / 1000 / 1024 / 1024) * 1.2  [Gb]`
	Формула для расчета max_msgx:
	`max_msgx = N * R * 24 * downtime_days`
	Где N – количество пользователей, R – среднее число писем в час на пользователя, downtime_days – максимальное количество дней, которое может быть недоступен резервный кластер.
	downtime_days = 3, R=100
	N=5000: max_msgx = 36 000 000, size = 15 Гб
	N=10 000: max_msgx = 72 000 000, size = 30 Гб
	N=100 000: max_msgx = 720 000 000, size = 300 Гб

Достаточная пропускная способность канала между кластерами	Выбор пропускной способности канала зависит от ожидаемой нагрузки и вычисляется по формуле: `N * R * S / (C * 3 600 000 000) (Гбит/с)` Где N – количество пользователей, R – среднее количество писем на пользователя в час, S – средний размер письма (в Кб), C – compression ratio (принять равным 2). Например, для 200 тыс. пользователей, получающих 100 писем в час, при размере письма 500 Кб получаем пропускную способность канала 1.4 Гбит / сек. тыс.
DNS-имена виртуальных машин DOS основного и резервного кластеров должны быть доступны из обоих кластеров	DNS-имена виртуальных машин DOS используются для асинхронного копирования данных с основного на резервный кластер, подключения с резервного кластера на основной, для копирования данных DOS
Идентичная топология виртуальных машин DOS основного и резервного кластеров	Основной и резервный кластеры должны иметь идентичную топологию виртуальных машин DOS: – количество виртуальных машин DOS; – количество дисков на виртуальную машину DOS (и пути монтирования дисков); – размер дисков на виртуальных машинах DOS.

17.1.1.2 Настройка катастрофоустойчивости для кластера без данных

Последовательность действий при настройке катастрофоустойчивости для кластера без данных приведена в таблице 203.

Таблица 203 – Настройка катастрофоустойчивости для кластера без данных

Шаг	Команды	Комментарий
Развертывание резервного кластера		
Настройка NTP для основного и резервного кластеров		Время на виртуальных машинах DOS на основном и резервном кластерах должно быть синхронизировано (с использованием NTP)

Добавление SSD mount point для всех нод на основном и резервном кластерах		Размер директории для WAL на каждой ноде зависит от сайзинга. При значении по умолчанию для dispersed_object_store_cross_dc_wal_stream_max_msgs составляет 11 Гб. Если данный параметр изменяется, то необходимо рассчитать необходимый размер директории по формуле:
		`size = (max_msgx * 370 / 1000 / 1024 / 1024) * 1.2 [Gb]`
		Формула для расчета max_msgx:
		`max_msgx = N * 100 * 24 * downtime_days`
		Где N – количество пользователей, 100 – среднее число писем в час на пользователя, downtime_days – максимальное количество дней, которое может быть недоступен резервный кластер.
		downtime_days = 3
		N=5000: max_msgx = 36 000 000, size = 15 Гб
		N=10 000: max_msgx = 72 000 000, size = 30 Гб
		N=100 000: max_msgx = 720 000 000, size = 300 Гб

Шаг	Команды	Комментарий

Добавление резервного кластера в конфигурацию основного кластера
 	
Добавление основного кластера в конфигурацию резервного кластера
	Запуск Ansible с параметрами для установки кластеров сразу с настроенной конфигурацией для будущей установки репликации. Ansible запускается на каждом кластере. При запуске на основном кластере указываются параметры резервного кластера в качестве удаленного кластера. При запуске на резервном кластере указываются параметры основного кластера в качестве удаленного кластера. Пример результирующей конфигурации DOS, которая будет сгенерирована с помощью Ansible:
	`"cross_dc": {`
	`"clusters": {`
	`"target": {`
	`"token": "secret-token",`
	`"api_urls": [`
	`"127.0.0.1:21106",`
	`"127.0.0.1:21206",`
	`"127.0.0.1:21306"`
	`]`
	`}`
	`},`
	`"api": {`
	`"listen_endpoint": "0.0.0.0:20106",`
	`"service_address": "127.0.0.1",`
	`"service_port": "20106",`
	`"use_tracer": false,`
	`"max_send_size": "32M",`
	`"max_recv_size": "32M"`
	`},`
	`"wal": {`
	`"type": "embedded",`
	`"dir": "/var/lib/dispersed-object-store/source/peer1/wal",`
	`"file_permissions": "0644",`
	`"dir_permissions": "0755",`
	`"subject_shards": 64,`
	`"service_endpoint":`
		dispersed_object_store_cross_dc_target_name – имя удаленного кластера
		
		dispersed_object_store_cross_dc_target_api_urls – список IP удаленного кластера
		
		dispersed_object_store_cross_dc_wal_stream_max_msgs – количество сообщений, которое будет храниться в replicated wal очереди (от этого параметра зависит, какое время основной кластер сможет пережить недоступность резервного кластера, а также размер WAL директории, которую необходимо примонтировать к каждому ноду). 1000 записей занимает около 370 Кб. Значение по умолчанию 25920000 = (3 * 100 * (60 * 60 * 24)) при нагрузке 100 RPS на кластер позволит переживать недоступность резервного кластера 3 дня и потребует 12 Гб для WAL (10 Гб на WAL плюс 2 Гб запас для того, чтобы WAL директория заполнялась не на 100%).
		
		dispersed_object_store_cross_dc_token – токен локального кластера
		
		dispersed_object_store_cross_dc_target_token – токен удаленного кластера

Шаг	Команды	Комментарий

	"127.0.0.1:20107",
	"cluster_endpoint":
	"127.0.0.1:20108",
	"gateway_endpoint":
	"127.0.0.1:20109",
	"stream_max_msgs": 25920000,
	"handler": {
	"timeout": "30s",
	"fatal_error_codes": [
	2000, 1115, 1112, 1111,
	1107, 1106, 1105, 1104, 102, 1101,
	1100,
	1026, 1007, 1004, 1015,
	1010, 1012, 1257
	]
	}
	},
	"token": "secret-token"
	}	

Установка репликации	Для основного кластера следует вызвать команду: ucs-dispersed-object-store-client dc add --target 'target_name'	Вместо target_name необходимо использовать значение, которое было добавлено в конфигурацию на шаге «Добавление резервного кластера в конфигурацию основного кластера»

17.1.1.3 Настройка катастрофоустойчивости для кластера с данными

Последовательность действий при настройке катастрофоустойчивости для кластера с данными приведена в таблице 204.

Таблица 204 – Настройка катастрофоустойчивости для кластера с данными

Шаг	Команды	Комментарий
Развертывание резервного кластера		

Шаг	Команды	Комментарий
Настройка NTP для основного и резервного кластеров		Время на виртуальных машинах DOS на основном и резервном кластерах должно быть синхронизировано (с использованием NTP)

Добавление SSD mount point для всех нод на основном и резервном кластерах		Размер директории для WAL на каждой ноде зависит от сайзинга. При значении по умолчанию для dispersed_object_store_cross_dc_wal_stream_max_msgs составляет 11 Гб. Если данный параметр изменяется, то необходимо рассчитать необходимый размер директории по формуле:
		`size = (max_msgx * 370 / 1000 / 1024 / 1024) * 1.2 [Gb]`
		Формула для расчета max_msgx:
		`max_msgx = N * 100 * 24 * downtime_days`
		Где N – количество пользователей, 100 – среднее число писем в час на пользователя, downtime_days – максимальное количество дней, которое может быть недоступен резервный кластер.
		downtime_days = 3
		N=5000: max_msgx = 36 000 000, size = 15 Гб
		N=10 000: max_msgx = 72 000 000, size = 30 Гб
		N=100 000: max_msgx = 720 000 000, size = 300 Гб

Добавление резервного кластера в конфигурацию основного кластера Добавление основного кластера в конфигурацию резервного кластера	Запуск Ansible с параметрами для установки кластеров сразу с настроенной конфигурацией для будущей установки репликации. Ansible запускается на каждом кластере. При запуске на основном кластере указываются параметры резервного кластера в качестве удаленного кластера. При запуске на резервном кластере указываются параметры основного кластера в качестве удаленного кластера.	dispersed_object_store_cross_dc_target_name – имя удаленного кластера dispersed_object_store_cross_dc_target_api_urls – список IP удаленного кластера dispersed_object_store_cross_dc_wal_stream_max_msgs – количество сообщений, которое будет храниться в

Шаг	Команды	Комментарий

	Пример результирующей конфигурации DOS, которая будет сгенерирована с помощью Ansible:
	`"cross_dc": {`
	`"clusters": {`
	`"target": {`
	`"token": "secret-token",`
	`"api_urls": [`
	`"127.0.0.1:21106",`
	`"127.0.0.1:21206",`
	`"127.0.0.1:21306"`
	`]`
	`}`
	`},`
	`"api": {`
	`"listen_endpoint": "0.0.0.0:20106",`
	`"service_address": "127.0.0.1",`
	`"service_port": "20106",`
	`"use_tracer": false,`
	`"max_send_size": "32M",`
	`"max_recv_size": "32M"`
	`},`
	`"wal": {`
	`"type": "embedded",`
	`"dir": "/var/lib/dispersed-object-store/source/peer1/wal",`
	`"file_permissions": "0644",`
	`"dir_permissions": "0755",`
	`"subject_shards": 64,`
	`"service_endpoint": "127.0.0.1:20107",`
	`"cluster_endpoint": "127.0.0.1:20108",`
	`"gateway_endpoint": "127.0.0.1:20109",`
	`"stream_max_msgs": 25920000,`
	`"handler": {`
	`"timeout": "30s",`
	`"fatal_error_codes": [`
	`2000, 1115, 1112, 1111, 1107, 1106, 1105, 1104, 102, 1101,`
		replicated wal очереди (от этого параметра зависит, какое время основной кластер сможет пережить недоступность резервного кластера, а также размер WAL директории, которую необходимо примонтировать к каждому ноду). 1000 записей занимает около 370 Кб. Значение по умолчанию 25920000 = (3 * 100 * (60 * 60 * 24)) при нагрузке 100 RPS на кластер позволит переживать недоступность резервного кластера 3 дня и потребует 12 Гб для WAL (10 Гб на WAL плюс запас 2 Гб для того, чтобы директория WAL заполнялась не на 100%).
		dispersed_object_store_cross_dc_token – токен локального кластера
		dispersed_object_store_cross_dc_target_token – токен удаленного кластера

Шаг	Команды	Комментарий
	1100, 1026, 1007, 1004, 1015, 1010, 1012, 1257] } }, "token": "secret-token" }	
Рестарт контейнеров DOS основного кластера (для загрузки новой конфигурации)		
Перевод резервного кластера в режим Bootstrap	ucs-dispersed-object-store-client leader set_cluster_mode --mode=BOOTSTRAP	Резервный кластер не будет обрабатывать WAL в этом режиме
Перевод всех нод основного кластера в режим Maintenance	ucs-dispersed-object-store-client leader set_node_mode --mode=MAINTENANCE	Будут заблокированы запись и чтение на основном кластере до снятия снапшота метаданных на шаге «Снятие бэкапа с основного кластера»
Включение репликации между кластерами	ucs-dispersed-object-store-client dc add --target=cluster_name	Начнется репликация между кластерами
Снятие бэкапа с основного кластера	ucs-dispersed-object-store-client leader backup run	Запись и чтение автоматически будут разрешены вскоре после запуска данной операции (до окончания полного бэкапа всех данных)
Восстановление резервного кластера из бэкапа, снятого с основного кластера	ucs-dispersed-object-store-client leader backup restore --backup_time xxxx \ --remote_endpoints ip1:port1,ip2:port2,ip3:port4	
Перевод резервного кластера в режим Normal	ucs-dispersed-object-store-client leader set_cluster_mode --mode=NORMAL	Кластер выйдет из режима Bootstrap и начнет обрабатывать WAL

17.1.1.4 Переключение с основного кластера на резервный в случае катастрофы

Последовательность действий при переключении с основного кластера на резервный приведена в таблице 205.

Таблица 205 – Переключение с основного кластера на резервный в случае катастрофы

Шаг	Команды	Комментарий
Переключение нагрузки на резервный кластер		
Удаление репликации на резервном кластере (опционально)	`ucs-dispersed-object-store-client dc delete --force`	– Если основной кластер временно недоступен и будет вскоре восстановлен, можно пропустить данный шаг. – Удаление репликации необходимо, только если основной кластер не будет восстановлен в течение поддерживаемого предела недоступности резервного кластера и будет необходимо создавать репликацию заново. – Если известно, что основной кластер будет недоступен продолжительное время, то удаление репликации сэкономит ресурсы, потребляемые на резервном кластере.

17.1.1.5 Плановое переключение с основного кластера на резервный (без катастрофы)

Последовательность действий при переключении с основного кластера на резервный без катастрофы приведена в таблице 206.

Таблица 206 – Переключение с основного кластера на резервный без катастрофы

Шаг	Команды	Комментарий
Переключение нагрузки на резервный кластер		Дополнительные шаги не требуются

17.1.1.6 Обратное переключение с резервного на основной кластер

Если основной кластер был недоступен больше поддерживаемого предела недоступности (определяется параметром **dispersed_object_store_cross_dc_wal_stream_max_msgs** при развертывании), то необходимо заново создать репликацию между кластерами по шагам, описанным в разделе 17.1.1.3, после этого следует произвести переключение нагрузки (см. раздел 17.1.1.5).

Если основной кластер был недоступен непродолжительное время, необходимо произвести плановое переключение нагрузки на основной кластер (см. раздел 17.1.1.5).

17.1.1.7 Мониторинг репликации

1. RPO (Recovery point objective)

Можно отслеживать логи всех серверов DOS с сообщением «processed replicated wal record», они будут содержать поля **replication_lag_seconds** и **replication_last_ts**.

Пример лога ноды DOS на резервном кластере:

```
10:40:54.0894   debug   nats/handler.go:117 processed replicated wal record
{"service_identity": "dos-1", "service_endpoint": "127.0.0.1:21100", "span-
request-id": ["8fa06a44-9d8f-43d9-87d2-ba9b7efc7bc8"], "trace-request-id":
["05035fe7-7a51-458e-9902-6408dcfced60"], "stream": "dos-target-follower",
"consumer": "dos-target-replication-1", "consumer_seq": 23,
"replication_lag_seconds": 98, "replication_last_ts": 1707907156455}
```

Описание полей логов мониторинга приведено в таблице 207.

Таблица 207 – Описание полей логов мониторинга

Поле	Описание	Подсчет значения для кластера	Что необходимо учитывать при трактовке метрики
replication_ last_ts	Последнее время создания объекта на основном кластере, которое было обработано сервером на резервном кластере	`min(replication_last_ts)` взять минимальное значение из всех, рапортуемых нодами DOS	Если нода перестала функционировать, ее нужно исключить из подсчета

Поле	Описание	Подсчет значения для кластера	Что необходимо учитывать при трактовке метрики
replication_lag_seconds	Лаг между временем записи объекта на основном кластере и его обработки на сервере резервного кластера. Печатается в секундах	`max(replication_lag_seconds)` взять максимальное значение из всех, рапортуемых нодами DOS	– Удобно использовать при быстрой оценке репликации на действующих кластерах. Для построения алертинга лучше использовать значение ***replication_last_ts***. – Если нода перестала функционировать, ее нужно исключить из подсчета. – Если резервный кластер перестал функционировать или принимать входящие реплицируемые сообщения, то данные этого поля, взятые из старых записей логов, будут содержать неверное значение. При этом лучше использовать ***replication_last_ts***.

2. Переполнение WAL на основном кластере

Основной кластер раз в 5 минут проверяет переполнение WAL-сообщений, которые не были среплицированы на резервный кластер (сценарий долгой недоступности резервного кластера).

Если сообщения на основном кластере ротировались и не были скопированы на резервный кластер, то в логе текущего лидера DOS кластера появится следующее сообщение:

```
3:17:27.1737   error   nats/monitoring.go:202  check replication detected issue: crossdc replication inconsistent state, please remove crossdc replication and setup it again  {"service_identity": "dos-3", "service_endpoint": "127.0.0.1:20300", "cluster": "source", "datacenter": "moon", "rack": "", "node_id": 3, "trace-request-id": ["0037176e-b663-47e7-b9b9-d4b4cbd796e3"], "span-request-id": ["0820f386-aeb9-47f4-83ab-2aab758684c0"], "repeater": "check_replication", "RemoteCluster": "target", "StreamFirstSeq": 54, "RemoteStreamLastSeq": 29, "PrevRemoteStreamLastSeq": 0}
```

17.1.2 Репликация базы данных MongoDB

Для обеспечения непрерывности работы в Mailion реализована возможность хранения всех данных почтовых серверов в двух ЦОДах. В случае глобального сбоя и выхода из строя одного из ЦОД почтовая система продолжает функционировать с минимальным простоем и минимальной потерей данных в соответствии с установленным SLA.

После восстановления работоспособности пользователям должны быть доступны все функции каталога и почтовой системы, данные почтовых ящиков, функционал календаря на момент последней синхронизации данных между ЦОДами в соответствии с категорией данных.

Репликация MongoDB позволяет включить режим репликации между двумя датацентрами (см. Рисунок 104).

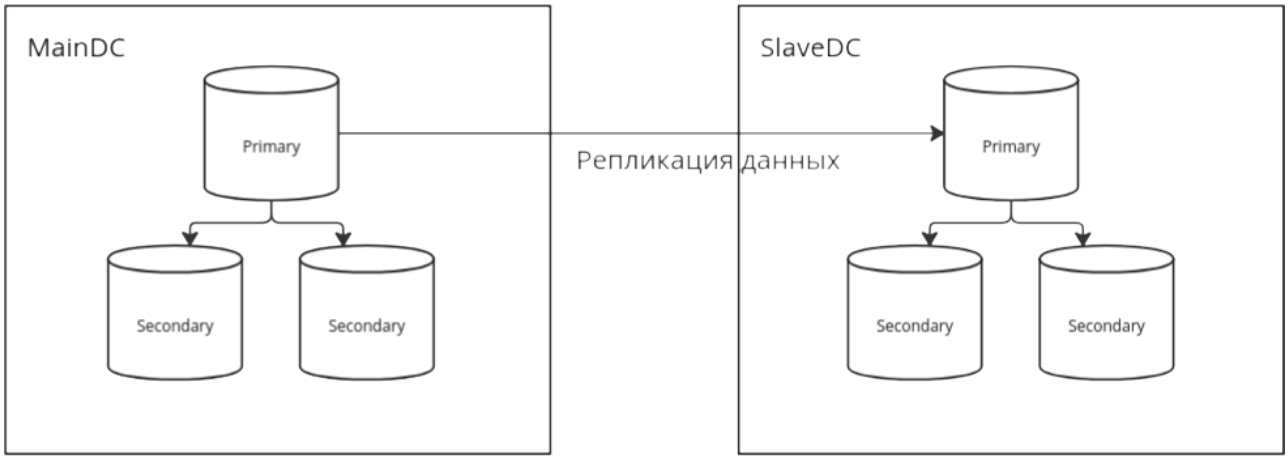


Рисунок 104 – Репликация базы данных между датацентрами

В результате репликации базы данных в случае временной недоступности или полном уничтожении одного из датацентров сохраняются нижеследующие возможности.

Доступ к каталогу:

– пользователи, группы, права;
– глобальная адресная книга;
– личные адресные книги;
– переговорные комнаты и принтеры.

Доступ к почте:

– входящие и исходящие письма;
– возможность отправки и получения писем;

– внутри компании;
– за пределами компании.

Доступ к календарю:

– личный календарь с событиями;
– календари пользователей внутри компании;
– доступ к бронированию переговорных;
– возможность воспользоваться принтером;
– сохраняется список задач.

17.1.2.1 Общий сценарий для репликации

– Подготовка стендов.
– Проверка работоспособности каждого кластера – минимум проверка отправки писем и создания календарных событий.
– Остановка всех сервисов, кроме `mongodb` и `redis`, на кластере, куда реплицируются данные.
– Создание резервных данных `mongodb` на обоих кластерах перед запуском процесса репликации.
– Удаление всех баз сервисов в `mongodb` на кластере, куда реплицируются данные.
– Настройка инструмента репликации.
– Запуск процесса репликации.
– *(Опционально)* Создание тестовой базы и коллекции с тестовыми данными на исходном кластере и проверка их создания и удаления на целевом кластере.
– Проверка статуса репликации.
– Остановка процесса репликации.
– Запуск сервисов на кластере, куда производилась репликация.
– *(Опционально)* Удаление данных `redis` и перевыкатка `redis` при необходимости.
– Проверка работоспособности кластера, на который реплицировались данные.

17.1.2.2 Подробный порядок действий по репликации

1. Предварительно необходимо установить Mailion на двух стендах с использованием одинаковых версий сервисов стендов.
2. Проверить работоспособность каждого кластера:
   2.1 Проверить, какие из сервисов запущены и какие версии используются.
   2.2 Войти под тестовыми тенантами, проверить отправку и получение писем и создание календарных событий.
3. Остановить сервисы на целевом кластере:
   3.1 Использовать **Скрипт остановки и запуска сервисов на стенде** из раздела 17.1.2.3.
   3.2 Проверить, что сервисы остановлены.
4. Создать резервные копии баз данных `mongodb` на обоих кластерах перед запуском процесса репликации:
   4.1 Зайти на машину `ucs-infra-1` на каждом кластере и под пользователем `root` запустить
   скрипт `/srv/docker/mongodb/backup_scripts/mongodb_backup_generic.sh`.
   4.2 Если скрипта нет, то убедиться, что при установке стендов была установлена job `backup`, при необходимости запустить ее.
5. Удалить все базы сервисов в `mongodb` на кластере, куда реплицируются данные, для этого любым удобным способом подключиться к кластеру `mongo` на целевом стенде:
   5.1 Выполнить **Команду для чистки базы данных** из раздела 17.1.2.3.
   5.2 Возможно, понадобится подключиться напрямую к PRIMARY node. Для этого следует выполнить `rs.status()` и найти в выводе, какая нода является PRIMARY.
   5.3 Подключиться напрямую к PRIMARY node.
   5.4 Повторить запуск **Команды для чистки базы данных**.

6. Настроить инструмент репликации.

   Для Mongosync:

   6.1 Скопировать **Dockerfile для Mongosync** из раздела 17.1.2.3 на `ucs-infra-1` на кластере, откуда копируются данные.

   6.2 Собрать образ прямо на `ucs-infra-1` командой:

```
docker build -f Dockerfile . --tag mongosync:latest
```

   6.3 Скопировать все необходимые SSL/TLS-сертификаты на `ucs-infra-1`.

   6.4 Скопировать и запустить **Скрипт для запуска контейнера mongosync** из раздела 17.1.2.3 на `ucs-infra-1`.

   6.5 С помощью `'docker ps -a'` проверить, что контейнер успешно запустился.

7. Запустить процесс репликации.

   Для Mongosync:

   7.1 Зайти внутрь контейнера `mongosync` с помощью команды `docker exec -it mongosync bash` и далее выполнить команду:

```
curl localhost:27182/api/v1/start -XPOST \
--data '
   {
      "source": "cluster0",
      "destination": "cluster1"
   } '
```

   7.2 Получить на выходе `success: true`.

8. *(Опционально)* Создать тестовую базу данных и коллекцию с тестовыми данными на исходном кластере и проверить их создание и удаление на целевом кластере:

   8.1 Подключиться к исходной `mongodb` любым удобным способом.

   8.2 Создать тестовую базу, в ней – тестовую коллекцию и несколько тестовых документов.

   8.3 Проверить, создались ли они на целевом кластере.

   8.4 Удалить один документ в исходной `mongodb`, проверить, удалился ли он на целевой базе данных.

   8.5 Повторить удаление с проверкой последовательно сначала для коллекции, потом для базы данных.

9. Проверить статус репликации.

   Для Mongosync:

   9.1 Зайти внутрь контейнера `mongosync`.

   9.2 Выполнить команду:

```
curl localhost:27182/api/v1/progress
```

   Вывод команды можно подробнее изучить по ссылке https://www.mongodb.com/docs/cluster-to-cluster-sync/current/reference/api/progress/.

10. Остановить процесс репликации.

    Для Mongosync:

    10.1 Если в выводе есть `canCommit: true`, то это означает, что синхронизация по большей части завершилась, и можно делать `commit` изменений.

    В а ж н о – После того как будет сделан `commit`, снова запустить репликацию будет нельзя. Для повторного запуска нужно будет удалить базу с метаинформацией `mongosync`.

    Если прогресс показывает, что можно сделать `commit`, то внутри контейнера нужно выполнить команду:

```
curl localhost:27182/api/v1/commit -XPOST --data '{ }'
```

    10.2 Таким же способом, каким проверяли прогресс, нужно проверять процесс коммита изменений. Когда он закончится, в выводе будет `state: COMMITED`.

11. Запустить сервисы на кластере, куда производилась репликация.

    Использовать **Скрипт остановки и запуска сервисов на стенде** из раздела 17.1.2.3, в конце скрипта не забыть оставить нужный пункт.

12. *(Опционально)* Удалить данные `redis` и обновить роль `redis` при необходимости:

    12.1 Проверить с помощью `mailion_install_info`, все ли сервисы запустились. Если не все, то можно попробовать почистить кэши `redis`.

    12.2 Остановить сервисы с помощью **Скрипта остановки и запуска сервисов на стенде** из раздела 17.1.2.3.

    Для этого в Sparky есть job `mailion_redis_cleanup`.

    12.3 Переинициализировать сервисы `redis` с помощью job `mailion_install_infra`. Необходимо выбрать плейбук `infra` и указать в тегах `redis_cache`.

12.4 Запустить сервисы с помощью **Скрипта остановки и запуска сервисов на стенде** из раздела 17.1.2.3.

12.5 Снова проверить стенд с помощью `mailion_install_info`.

13. Проверить работоспособность кластера, на который реплицировались данные.

    Все выполняется так же, как и в проверке кластера в предыдущих пунктах. Выполнять вход нужно с аккаунтами пользователей исходного стенда, откуда копировались данные.

Обратная миграция выполняется так же, но с дополнительными действиями:

– Необходимо удалить базу с метаинформацией `mongosync` из кластера, который ранее был целевым, но теперь стал исходным.

– Предварительно необходимо выполнить резервное копирование базы данных.

17.1.2.3 Список полезных команд и скриптов

1. Команда для чистки базы данных

```
use admin; \
db.getMongo().getDBNames().filter(n => !
['admin','local','config'].includes(n)).forEach(dname =>
db.getMongo().getDB(dname).dropDatabase());
```

2. Скрипт для запуска контейнера `mongosync`

   В а ж н о – Все необходимые сертификаты лежат в папке **/srv/tls/certs**. При необходимости необходимо поменять местами значения для переменных CLUSTER0 и CLUSTER1.

```
#!/bin/bash -xe
docker run --name mongosync -p 27182:27182 \
    -e 'CLUSTER1=mongodb://<user>:<password>@mongodb.ucs-db-1.disaster-
02.host.ru:27017,mongodb.ucs-db-2.-disaster-02.host.ru:27017,mongodb.ucs-db-3.-
disaster-02.host.ru:27017/?
authSource=admin&replicaSet=ucs&tls=true&tlsCAFile=/etc/pki/tls/certs/ucs-infra-
1.-disaster-02.host.ru-main-
ca.pem&tlsCertificateKeyFile=/etc/pki/tls/certs/merged_mongodb.ucs-db-1.-
disaster-02.host.ru-main-peer.pem' \
    -e 'CLUSTER0=mongodb://<user>:<password>@mongodb.ucs-db-1.-disaster-
01.host.ru:27017,mongodb.ucs-db-2.-disaster-01.host.ru:27017,mongodb.ucs-db-3.-
```

```
disaster-01.host.ru:27017/?
authSource=admin&replicaSet=ucs&tls=true&tlsCAFile=/etc/pki/tls/certs/ucs-infra-
1.-disaster-01.host.ru-main-
ca.pem&tlsCertificateKeyFile=/etc/pki/tls/certs/merged_mongodb.ucs-db-1.-
disaster-01.host.ru-main-peer.pem' \
    -v /srv/tls/certs:/etc/pki/tls/certs \
    -d mongosync:latest \
sh -c "mongosync --cluster0 \$CLUSTER0 --cluster1 \$CLUSTER1 --disableTelemetry"
```

3. Dockerfile для Mongosync

```
FROM hub.host.ru/mongo:4.4.10-17
WORKDIR /mongosync
ENV PACKAGE_NON_ARC="mongosync-ubuntu2004-x86_64-1.7.1"
ENV PACKAGE="${PACKAGE_NON_ARC}.tgz"

RUN apt-get -y install wget curl
RUN wget "https://fastdl.mongodb.org/tools/mongosync/$PACKAGE"

# RUN wget https://fastdl.mongodb.org/tools/mongosync/mongosync-rhel70-x86_64-
1.7.1.tgz
# COPY mongosync-rhel70-x86_64-1.7.1.tgz ./
RUN tar xzvf $PACKAGE && rm ${PACKAGE}
RUN cp ${PACKAGE_NON_ARC}/bin/mongosync ./
RUN cp mongosync /usr/local/bin

CMD ["mongosync"]
```

4. Скрипт остановки и запуска сервисов на стенде

   В а ж н о – Перед запуском необходимо задать **idx** (номер кластера) внутри функций. При этом следует оставить только нужные строки в конце файла.

```
#!/bin/bash -xe

SSH_KEY=<Путь к ssh ключу awx>
SSH_USER='astra'

FRONTEND_CONTAINERS="house cadvisor cox leda imap ararat syslog_ng"
APPS_CONTAINERS="theseus sophokles ares cadvisor phalanx iason razor kongur
viper kex mixer beef clotho themis broteas weaver orpheus atlas marker elysion
othrys mars hog dafnis ektor kronos thoth homeros dowal euripides mosquito
```

```
achill minos daidal odusseus erakles pasifae boreas perseus iolaos talaos
eratosthenis briseis adonis hydra"
OBST_CONTAINERS="cadvisor dispersed_object_store"
MAIL_CONTAINERS="cadvisor lmtp zeus postfix paranoid woof ariadne"
# CONVERTER_CONTAINERS="cadvisor tripoli cvm helpbek jod pregen dirbek
mailbek_search meepo house"
CONVERTER_CONTAINERS="cadvisor tripoli cvm helpbek pregen dirbek mailbek_search
meepo house"

function stop_apps_02 {
    idx="2"
    echo "Stopping frontend"
    for i in {1..2}; do
        stand="ucs-frontend-$i.-disaster-0$idx.host.ru"
        echo "Stopping containers on stand: $stand"
        ssh -i $SSH_KEY astra@$stand "sudo docker stop ${FRONTEND_CONTAINERS}"
    done
    echo "Stopping apps"
    for i in {1..2}; do
        stand="ucs-apps-$i.-disaster-0$idx.host.ru"
        echo "Stopping containers on stand: $stand"
        if (( $i == 2)); then
            APPS_CONTAINERS=$(echo $APPS_CONTAINERS | sed 's/phalanx//g')
        fi
        ssh -i $SSH_KEY astra@$stand "sudo docker stop ${APPS_CONTAINERS}"
    done
    echo "Stopping obst"
    for i in {1..3}; do
        stand="ucs-obst-$i.-disaster-0$idx.host.ru"
        echo "Stopping containers on stand: $stand"
        ssh -i $SSH_KEY astra@$stand "sudo docker stop ${OBST_CONTAINERS}"
    done
    echo "Stopping mail"
    for i in {1..2}; do
        stand="ucs-mail-$i.-disaster-0$idx.host.ru"
        echo "Stopping containers on stand: $stand"
        ssh -i $SSH_KEY astra@$stand "sudo docker stop ${MAIL_CONTAINERS}"
    done
    echo "Stopping converter"
    for i in {1..2}; do
```

```
        stand="ucs-converter-$i.-disaster-0$idx.host.ru"
        echo "Stopping containers on stand: $stand"
        ssh -i $SSH_KEY astra@$stand "sudo docker stop ${CONVERTER_CONTAINERS}"
    done
}

function start_apps_02 {
    idx="2"
    echo "Starting frontend"
    for i in {1..2}; do
        stand="ucs-frontend-$i.-disaster-0$idx.host.ru"
        echo "Starting containers on stand: $stand"
        ssh -i $SSH_KEY astra@$stand "sudo docker start ${FRONTEND_CONTAINERS}"
    done
    echo "Starting apps"
    for i in {1..2}; do
        stand="ucs-apps-$i.-disaster-0$idx.host.ru"
        echo "Starting containers on stand: $stand"
        if (( $i == 2)); then
            APPS_CONTAINERS=$(echo $APPS_CONTAINERS | sed 's/phalanx//g')
        fi
        ssh -i $SSH_KEY astra@$stand "sudo docker start ${APPS_CONTAINERS}"
    done
    echo "Starting obst"
    for i in {1..3}; do
        stand="ucs-obst-$i.-disaster-0$idx.host.ru"
        echo "Starting containers on stand: $stand"
        ssh -i $SSH_KEY astra@$stand "sudo docker start ${OBST_CONTAINERS}"
    done
    echo "Starting mail"
    for i in {1..2}; do
        stand="ucs-mail-$i.-disaster-0$idx.host.ru"
        echo "Starting containers on stand: $stand"
        ssh -i $SSH_KEY astra@$stand "sudo docker start ${MAIL_CONTAINERS}"
    done
    echo "Starting converter"
    for i in {1..2}; do
        stand="ucs-converter-$i.-disaster-0$idx.host.ru"
        echo "Starting containers on stand: $stand"
        ssh -i $SSH_KEY astra@$stand "sudo docker start ${CONVERTER_CONTAINERS}"
```

```
    done
}
 # Оставить необходимые строки
stop_apps_02
#start_apps_02
```

5. Скрипт для запуска восстановления данных из дампа

   В а ж н о – В случае необходимости необходимо отредактировать URL.

```
#!/bin/bash -xe

MONGO_VERSION="6.0.14"

docker run -it --rm -v /srv/backups/manual_backups:/backups -
v /srv/tls/certs:/etc/pki/tls/certs \
        -e 'MONGO_CONN=mongodb://<user>:<password>@mongodb.ucs-db-1.-disaster-
01.host.ru:27017,mongodb.ucs-db-2.-disaster-01.host.ru:27017,mongodb.ucs-db-3.-
disaster-01.host.ru:27017/?
authSource=admin&replicaSet=ucs&tls=true&tlsCAFile=/etc/pki/tls/certs/ucs-infra-
1.-disaster-01.host.ru-main-
ca.pem&tlsCertificateKeyFile=/etc/pki/tls/certs/merged_mongodb.ucs-infra-1.-
disaster-01.host.ru-main-peer.pem' \
        --name mongorestore hub.host.ru/mongo:${MONGO_VERSION} \
        sh -c "mongorestore --drop --gzip \$MONGO_CONN  --
archive=/backups/mongodb_dump_2024_02_28_2102.gz"
restore.sh (END)
```

6. Команда для составления списка сервисов, которые необходимо останавливать/запускать

```
    docker ps -a --format 'table {{.Names}}\t{{.Status}}' | grep 'Up' | grep -
v 'exporter' | grep -v 'syslog_ng' | awk '{print $1}' | tr '\n' ' '
```

7. Команда для паузы процесса реплики в Mongosync (после паузы можно возобновить процесс в отличие от коммита)

```
    curl  localhost:27182/api/v1/pause -XPOST -d '{}'
```

8. Команда для возобновления запуска миграции в Mongosync

```
    curl  localhost:27182/api/v1/resume -XPOST -d '{}'
```

17.1.2.4 Верификация реплицированных данных для Mongosync

Проверка статуса репликации подробно описана в сценарии тестирования и выполняется с помощью эндпоинта: https://www.mongodb.com/docs/cluster-to-cluster-sync/current/reference/api/progress/

Также есть отдельная утилита для проверки верификации Migration Verifier, но она находится в экспериментальном режиме: https://www.mongodb.com/docs/cluster-to-cluster-sync/current/reference/verification/verifier/

17.1.2.5 Принцип работы инструментов Mongosync и MongoShake

Обе утилиты используют `oplog` для репликации данных. MongoShake также позволяет использовать `change-stream`.

Использование `oplog` подразумевает, что на больших объемах данных при запуске репликации не все данные переедут в новый кластер, репликация выполнится только для тех данных, которые покрываются текущим `oplog`. Поэтому при запуске на больших кластерах в начале все равно следует выполнить дамп данных и их восстановление на новый кластер, если достоверно известно, что старый `oplog` уже ротировался. Также на время работы репликации следует либо увеличить, либо отключить ротирование `oplog`.

Оба инструмента способны сохранять свой прогресс и возобновлять работу с чекпоинта `mongosync`. Для сохранения чекпоинтов используется целевой кластер `mongodb`, куда реплицируются данные. Внутри целевых кластеров создаются базы данных с метаинформацией о ходе репликации и чекпоинтах.

Документация по Mongosync API: https://www.mongodb.com/docs/cluster-to-cluster-sync/current/reference/api/

Документация по MongoShake: https://github.com/alibaba/MongoShake/wiki/MongoShake-Detailed-Documentation

17.2 Роли и функции персонала

Роли и функции персонала, задействованного в обслуживании катастрофоустойчивой конфигурации, приведены в таблице 208.

Таблица 208 – Роли и функции персонала

Роль	Функции
дежурный администратор	– получение информации об инциденте (самостоятельно, от ЦОД, от пользователей) – создание инцидента в трекере задач (если есть) – оповещение сотрудника с ролью «Администратор инсталляции»
администратор инсталляции	– переключение нагрузки на резервный ЦОД – работы по восстановлению данных и работоспособности Mailion

Признаки, по которым дежурный администратор может понять, что произошел инцидент, и на основе этих данных сможет принять решение / оповестить ответственное лицо о переключении на резервный ЦОД и начале работ по восстановлению работоспособности Mailion и восстановлению данных:

- информирование от дата-центра (звонок дежурному администратору или иной способ связи);
- нарушения в работе Mailion – каталог, почта, календарь (информация от пользователей);
- нарушения времени ответа сервисов;
- критичные ошибки в логах.

17.3 Ограничения

- При временной недоступности или полном уничтожении основного ЦОД(1) резервный ЦОД(2) становится основным. На данный момент нет обратного переключения с резервного на изначальный основной ЦОД(1) в случае его временной недоступности. После восстановления работоспособности ЦОД(1) становится резервным.
- В случае инцидента при ручном переключении между ЦОД к времени на устранение инцидента добавится время реакции дежурного администратора. В

этом случае должно быть предварительно создано описание уровней инцидентов, а также согласовано время реакции дежурного администратора (SLA).

18 РАБОТА С GARBAGE COLLECTOR

Для управления задачами для сборщика мусора в `ministerium` используются команды:

- `start_gc` – запуск сборщика мусора (см. раздел 18.1);
- `create_gc_task` – создание задачи с отложенным исполнением (см. раздел 18.2);
- `update_gc_task` – обновление задачи по taskID (см. раздел 18.3);
- `delete_gc_task` – удаление задачи по taskID (см. раздел 18.4);
- `get_gc_task` – получение задачи по taskID (см. раздел 18.5);
- `get_all_gc_tasks` – получение всех имеющиеся задач GC (см. раздел 18.6).

18.1 Запуск GC

Для запуска Garbage Collector используется команда `start_gc`.

Пример запроса:

```
nct_ministerium start_gc \
--admin.login <admin> \
--admin.password <password> \
--tenant_id b3e95118-5e5f-4b3f-839e-b62484b6008a \
--cox.balancer_endpoint=hydra.ucs-apps-1.installation.example.net:50053 \
--cox.balancer_endpoint=hydra.ucs-apps-1.installation.example.net:50053 \
--cox.balancer_endpoint=hydra.ucs-apps-1.installation.example.net:50053 \
--cox.compression=none \
--cox.endpoint=grpc-devmail.example.net:3142 \
--cox.load_balanced=False \
--cox.request_timeout=10s \
--cox.service_name=cox \
--cox.use_tls=True \
--cox.use_tls_balancer=False \
--tls_settings.ca_file /home/mo/ministerium_certs/zulu/ca.pem \
--tls_settings.client_cert_file /home/mo/ministerium_certs/zulu/client_crt.pem \
--tls_settings.key_file /home/mo/ministerium_certs/zulu/client_key.pem \
--v
```

18.2 Создание задачи GC

Для создания задачи для сборщика мусора с отложенным исполнением используется команда `create_gc_task`.

Создать задачу может пользователь с правами администратора тенанта. Чистка и удаление объектов будут проведены внутри заданного тенанта.

В результате выполнения команды задача создается, обновляется, читается и удаляется под администратором инсталляции. Основные параметры настройки приведены в таблице 209.

Таблица 209 – Описание основных параметров запросов взаимодействия с GC

Параметр	Описание
recurrence_rule.frequency	Частота выполнения. Допустимые значения: `yearly`, `monthly`, `weekly`, `daily`, `hourly`, `minutely`, `secondly`
recurrence_rule.interval	Интервал повтора отправки
delta	Сдвиг от запланированного времени
retry_policy.count	Количество повторов
retry_policy.delay	Время перед повтором
retry_policy.interval	Интервал

Пример запроса:

```
nct_ministerium create_gc_task \
--admin.login admin \
--admin.password *** \
--tenant_id 1466eab7-967c-411a-a1a7-47a3d1822958 \
--recurrence_rule.frequency=monthly \
--recurrence_rule.interval=2 \
--delta="-3600s" \
--retry_policy.count=5 \
--retry_policy.delay="5m" \
--retry_policy.interval="10m" \
--cox.balancer_endpoint=hydra.ucs-apps-1.installation.example.net:50053 \
--cox.compression=none \
--cox.endpoint=installation.example.net:3142 \
--cox.load_balanced=false \
--cox.request_timeout=10s \
--cox.service_name=cox \
```

```
--cox.use_tls=true \
--cox.use_tls_balancer=false \
--tls_settings.ca_file /home/mo/ministerium_certs/yankee/ca.pem \
--tls_settings.client_cert_file /home/mo/ministerium_certs/yankee/client_crt.pem
\
--tls_settings.key_file /home/mo/ministerium_certs/yankee/client_key.pem \
--v
```

Данная конфигурация описывает правила, при которых созданная задача будет запускаться в рамках указанного тенанта каждый второй (`recurrence_rule.interval=2`) месяц (`recurrence_rule.frequency=monthly`) со сдвигом в 1 час от запланированного времени (`delta=-3600`) и, в случае неуспешного выполнения задачи, будет произведено 5 попыток перезапуска (`retry_policy.count=5`) с интервалом в 10 минут (`retry_policy.interval=10m`).

Пример ответа:

```
{
  "Response": {
    "changed": true,
    "failed": false,
    "msg": "ok"
  },
  "tasks_id": "a4fca8ab-ae0e-5f4d-b808-996d9e9b1d4d"
}
```

18.3 Обновление задачи GC

Для обновления задачи для сборщика мусора используется команда `update_gc_task`.

Пример запроса:

```
nct_ministerium update_gc_task \
--admin.login <login> \
--admin.password *** \
--task_id *** \
--recurrence_rule.frequency=hourly \
--recurrence_rule.interval=1 \
--retry_policy.count=1 \
--retry_policy.delay="1m" \
--cox.balancer_endpoint=hydra.ucs-apps-1.installation.example.net:50053 \
```

```
--cox.compression=none \
--cox.endpoint=grpc-yankee.stageoffice.ru:3142 \
--cox.load_balanced=false \
--cox.request_timeout=10s \
--cox.service_name=cox \
--cox.use_tls=true \
--cox.use_tls_balancer=false \
--tls_settings.ca_file /home/mo/ministerium_certs/yankee/ca.pem \
--tls_settings.client_cert_file /home/mo/ministerium_certs/yankee/client_crt.pem
\
--tls_settings.key_file /home/mo/ministerium_certs/yankee/client_key.pem \
--v
```

Пример ответа:

```
{
  "Response": {
    "changed": true,
    "failed": false,
    "msg": "ok"
  },
  "tasks_id": "a4fca8ab-ae0e-5f4d-b808-996d9e9b1d4d"
}
```

18.4 Удаление задачи GC

Для удаления задачи сборщика мусора используется команда `delete_gc_task`.

Пример запроса:

```
nct_ministerium delete_gc_task \
--admin.login <login> \
--admin.password *** \
--task_id 8f92d229e22c421ba12a442a1dfa0126 \
--cox.balancer_endpoint=hydra.ucs-apps-1.installation.example.net:50053 \
--cox.compression=none \
--cox.endpoint=grpc-installation.example.net:3142 \
--cox.load_balanced=false \
--cox.request_timeout=10s \
--cox.service_name=cox \
--cox.use_tls=true \
--cox.use_tls_balancer=false \
```

```
--tls_settings.ca_file /home/mo/ministerium_certs/yankee/ca.pem \
--tls_settings.client_cert_file /home/mo/ministerium_certs/yankee/client_crt.pem
\
--tls_settings.key_file /home/mo/ministerium_certs/yankee/client_key.pem \
--v
```

Если `task_id` будет принадлежать задаче, не связанной с GC, либо из чужого тенанта, то вернется ошибка.

18.5 Получение задачи GC

Для получения задачи сборщика мусора используется команда `get_gc_task`.

Пример запроса:

```
nct_ministerium get_gc_task \
--admin.login <admin> \
--admin.password <password> \
--task_id *** \
--cox.balancer_endpoint=hydra.ucs-apps-1.installation.example.net:50053 \
--cox.compression=none \
--cox.endpoint=installation.example.net:3142 \
--cox.load_balanced=false \
--cox.request_timeout=10s \
--cox.service_name=cox \
--cox.use_tls=true \
--cox.use_tls_balancer=false \
--tls_settings.ca_file /home/mo/ministerium_certs/yankee/ca.pem \
--tls_settings.client_cert_file /home/mo/ministerium_certs/yankee/client_crt.pem
\
--tls_settings.key_file /home/mo/ministerium_certs/yankee/client_key.pem \
--v
```

Если `task_id` будет принадлежать задаче, не связанной с GC, либо из чужого тенанта, то вернется ошибка.

18.6 Получение всех имеющихся задач GC

Для получения всех задач для сборщика мусора используется команда `get_all_gc_tasks`.

Пример запроса:

```
nct_ministerium get_all_gc_tasks \
--admin.login <admin> \
--admin.password <password> \
--cox.balancer_endpoint=hydra.ucs-apps-1.installation.example.net:50053 \
--cox.compression=none \
--cox.endpoint=grpc-installation.example.net:3142 \
--cox.load_balanced=false \
--cox.request_timeout=10s \
--cox.service_name=cox \
--cox.use_tls=true \
--cox.use_tls_balancer=false \
--tls_settings.ca_file /home/mo/ministerium_certs/yankee/ca.pem \
--tls_settings.client_cert_file /home/mo/ministerium_certs/yankee/client_crt.pem
\
--tls_settings.key_file /home/mo/ministerium_certs/yankee/client_key.pem \
--v
```

Пример ответа:

```
"tasks": [
  {
    "id": "a4fca8ab-ae0e-5f4d-b808-996d9e9b1d4d",
    "operations": [
      {
        "operation_name": 1,
        "Arguments": {
          "GarbageCollectorRegular": {
            "tenant_id": "1466eab7-967c-411a-a1a7-47a3d1822958"
          }
        }
      }
    ],
    "recurrence_rule": {
      "frequency": minutely,
      "interval": 5
    },
    "delta": "0s",
    "retry_policy": {
      "count": 2,
      "delay": "5m"
```

```
    },
    "created_at": {
      "unixmicro": 1674638395636367,
      "zone": 10800
    }
  }
]
```

19 ВОЗМОЖНЫЕ СИТУАЦИИ И СПОСОБЫ РЕШЕНИЯ

Возможные ситуации при эксплуатации **Панели администрирования** ПО «Mailion» и способы решения приведены в таблице 210.

Таблица 210 – Возможные ситуации и способы решения

Описание ситуации	Способ решения
Не получается авторизоваться в ПО «Mailion»	Проверить корректность вводимого логина и пароля
Отображается сообщение: «Не удалось получить данные» в нижнем левом углу экрана	Обновить страницу полностью: – нажать на значок обновления на странице браузера; – нажать клавишу F5. Необходимо обратить внимание, если какие-либо поля ввода были заполнены, то они удалятся. Следует предварительно скопировать или сохранить данные из полей ввода
Бесконечная загрузка страницы	
При переходе в какой-либо раздел Панели управления отсутствуют созданные записи	

20 ТЕХНИЧЕСКАЯ ПОДДЕРЖКА

Контактная информация службы технической поддержки ООО «Новые облачные технологии» в случае возникновения вопросов, не описанных в данном руководстве:

– Адрес электронной почты: support@service.myoffice.ru
– Телефон: 8-800-222-1-888.

ПРИЛОЖЕНИЕ А. ПРИМЕР НАПИСАНИЯ ВНЕШНИХ DNS-ЗАПИСЕЙ

Имя записи	Пример написания записи
api	api-test.example.com IN A <ucs_frontend_vip>
auth	auth-test.example.com IN A <ucs_frontend_vip>
autoconfig	autoconfig-test.example.com IN A <ucs_frontend_vip>
avatars	avatars-test.example.com IN A <ucs_frontend_vip>
caldav	caldav-test.example.com. 900 IN CNAME <ucs_frontend_vip>
carddav	carddav-test.example.com. 878 IN CNAME <ucs_frontend_vip>
db	db-test.example.com IN A <ucs_frontend_vip>
grpc	grpc-test.example.com IN A <ucs_frontend_vip>
imap	imap-test.example.com IN A <ucs_frontend_vip>
mail	mail-test.example.com IN A <ucs_frontend_vip>
mail._domainkey	mail._domainkey.test.example.com. 899 IN TXT "v=DKIM1;" "g=*;" "k=rsa;" "p=<DKIM_KEY>"
mx1	mx-test.example.com. 900 IN A ucs-mail-1.test.example.com
mx2	mx-test.example.com. 900 IN A ucs-mail-2.test.example.com
preview	preview-test.example.com. 900 IN CNAME <ucs_frontend_vip>
relay	relay-test.example.com. 900 IN A <ucs_mail_vip>
resources	resources-test.example.com. 900 IN A <ucs_frontend_vip>
secured	secured-test.example.com. 900 IN A <ucs_frontend_vip>
smtp	smtp-test.example.com IN A <ucs_mail_vip>
_adsp._domainkey	_adsp._domainkey.test.example.com. 900 IN TXT "dkim=all"
_autodiscover._tcp	_autodiscover._tcp.test.example.com. 900 IN SRV 0 0 443 <mailion_external_domain>
_caldavs._tcp	_caldavs._tcp.test.example.com. 900 IN SRV 0 1 6787 caldav-test.example.com.
_carddavs._tcp	_carddavs._tcp.test.example.com. 900 IN SRV 0 1 6787 carddav-test.example.com.
_grpcsec._tcp	_grpcsec._tcp.test.example.com. 900 IN SRV 0 0 3142 grpc-test.example.com.

Имя записи	Пример написания записи
_imap._tcp	_imap._tcp.test.example.com. 900 IN SRV 10 0 143 imap-test.example.com.
_imaps._tcp	_imaps._tcp.test.example.com. 900 IN SRV 0 0 993 imap-test.example.com.
_smtps._tcp	_smtps._tcp.test.example.com. 900 IN SRV 0 0 465 smtp-test.example.com.
_submission._tcp	_submission._tcp.test.example.com. 900 IN SRV 0 0 587 smtp-test.example.com.
_submissions._tcp	_submissions._tcp.test.example.com. 900 IN SRV 0 0 465 smtp-test.example.com.

ПРИЛОЖЕНИЕ Б. КОМАНДЫ, ВЫПОЛНЯЕМЫЕ С ПОМОЩЬЮ ИНТЕРФЕЙСА КОМАНДНОЙ СТРОКИ, И ИХ ОПИСАНИЕ

Доступные команды	Описание
add_email	Добавить E-mail к объекту
add_domain_delegation	Добавить делегацию домена
add_entity_to_group	Связать объект с группой
add_org_structure_link	Добавить связь между двумя объектами элементов оргструктуры
add_users_to_gal_tag	Добавить пользователей к GAL-тегу
change_status	Изменить статус объекта
check_gal_user	Проверить GAL-пользователя в тенанте
check_group_all	Проверить уникальную группу в тенанте
completion	Сгенерировать сценарий автозавершения для указанной командной оболочки
create_domain	Создать новый домен в тенанте
create_gal_user	Создать системного GAL-пользователя
create_group	Создать группу
create_group_all	Создать уникальную группу в тенанте
create_login	Создать логин объекта
create_oauth_client	Создать OAuth клиент
create_password	Создать пароль для логина
create_resource	Создать ресурс
create_tenant	Создать новый тенант
create_tenant_admin	Создать администратора тенанта
create_tenant_gal_tag	Создать GAL-тег для тенанта
create_tenant_quotas_profile	Создать квоты для профиля тенанта
create_user	Создать пользователя
create_user_quotas_profile	Создать квоты для пользователя
create_users_bratch	Создать пользовательскую группу
delete_all_related_messages_by_message_id	Удалить письма у всех получателей в рамках тенанта
delete_domain	Удалить домен

Доступные команды	Описание
delete_entity_audit_levels	Удалить уровни аудита объекта
delete_gal_tag	Удалить GAL-тег
delete_group	Удалить группу
delete_login	Удалить логин
delete_oauth_client	Удалить OAuth клиент
delete_org_structure_element	Удалить элемент оргструктуры
delete_tenant	Удалить тенант
delete_tenant_audit_levels	Удалить уровни аудита тенанта
delete_tenant_quotas_profile	Удалить квоты для профиля тенанта
dynamic_group_filling_status	Проверить статус заполнения динамических групп
export_audit_events_by_app_name_as_file	Экспортировать события аудита по имени приложения в виде файла
export_audit_events_by_methods_codes_as_file	Экспортировать события аудита по коду методов в виде файла
export_audit_events_by_services_names_as_file	Экспортировать события аудита по имени службы в виде файла
find_domain	Найти домен по идентификатору или имени хоста
generate	Сгенерировать bash файл для автозавершения команды
get_audit_events_by_app_name	Получить события аудита по имени приложения
get_audit_events_by_methods_codes	Получить события аудита по коду методов
get_audit_events_by_services_codes	Получить события аудита по коду службы
get_entity_audit_levels	Получить уровни события аудита
get_oauth_client	Получить параметры OAuth клиента
get_orgstructure_element_by_id	Вернуть элемент оргструктуры с получением идентификатора и типа объекта
get_orgstucture_entities_list	Вернуть список объектов оргструктуры
get_org_structure_hierarchy	Вернуть иерархию оргструктуры
get_recount_quotas_processes	Получить все запущенные процессы пересчета квот
get_regions	Вернуть список регионов
get_tenant	Получить информацию о тенанте
get_tenant_audit_levels	Получить аудит текущих настроек безопасности тенанта

Доступные команды	Описание
get_tenant_gals	Получить список GAL-тегов тенанта
get_user_quotas_profile	Получить квоты профиля пользователя
help	Помощь по поводу любой команды
list_domains	Список доменов в тенанте
list_entities	Список объектов по идентификатору региона/тенанта, E-mail или логину. Может быть отфильтрован по типу объекта
list_entity_groups	Список связанных групп с объектом
list_group_members	Список связанных объектов с группой
list_tenants	Список всех тенантов
make_dynamic_group	Создать динамическую группу с участниками по фильтру
recount_quotas	Начать процесс напоминания о пересчете квот для одиночного объекта или всех объектов в тенанте
remove_email	Исключить E-mail из объекта
remove_entity_from_group	Исключить объект из группы
remove_org_structure_link	Удалить связь между двумя элементами оргструктуры
remove_user_quotas_profile	Удалить квоты профиля пользователя
remove_users_from_gal_tag	Удалить пользователей из GAL-тегов
replace_entity_audit_levels	Заменить уровень аудита объекта. Создать, если значения отсутствуют
remove_tenant_audit_levels	Заменить уровень аудита тенанта. Создать, если значения отсутствуют
save_org_structure_element	Создать или обновить элемент оргструктуры
set_domains_to_logins	Выполнить миграцию к установке всех атрибутов доменных логинов, если они не установлены
set_same_domain_delegation	Создание делегации с типом «делегация на одинаковых доменах» (однодоменный режим)
stop_recount_quotas	Остановить процесс пересчета квоты. Некоторые объекты могли иметь непредвиденные упоминания о квотах
unmake_dynamic_group	Изменить динамическую группу. Сделать группу снова статической
update_domain	Обновить домен (не менять имя хоста или идентификатор тенанта, если домен имеет пользователей)
update_domain_delegation	Обновить делегацию домена

Доступные команды	Описание
update_entity_audit_levels	Обновить уровни аудита или объект. Создать, если значения отсутствуют
update_group_profile	Создать или обновить профиль группы
update_oauth_client	Обновить параметры OAuth клиента
update_reserve_email	Обновить резервный E-mail пользователя
update_resource	Обновить ресурс
update_resource_profile	Создать или обновить профиль ресурса
update_roles	Создать или удалить роли объекта
update_tenant	Обновить информацию о тенанте
update_tenant_audit_levels	Обновить уровни аудита тенанта. Создать, если значения отсутствуют
update_tenant_quotas_profile	Обновить квоты профиля тенанта
update_user_profile	Создать или обновить профиль пользователя
update_user_quotas_profile	Обновить квоты профиля пользователя
upload_avatars	Обновить аватары домена

ПРИЛОЖЕНИЕ В. ПРИМЕРЫ JSON-ФАЙЛОВ ДЛЯ КОМАНД, ВЫПОЛНЯЕМЫХ С ПОМОЩЬЮ ИНТЕРФЕЙСА ПРОГРАММНОЙ СТРОКИ

В.1 Файл настроек импорта пользователей

Пример файла настроек **import_config.json** приведен ниже. Описание полей приведено в таблице 211.

```
{
      "token-name": "ucs-access-token",
      "admin": {
            "login": "admin_tenant",
            "password": "****"
      },
      "cox": {
            "endpoint": "127.0.0.1:31415",
            "service_name": "cox",
            "load_balanced": false,
            "request_timeout": "10s",
            "use_tls": false,
            "use_tls_balancer": false,
            "compression": "none"
      },
      "tls_settings": {
            "ca_file": "ncloud_ca_cert.bundle.pem",
            "client_cert_file": "client.pem",
            "key_file": "key.pem"
      },
      "tenant_id": "11068ade-1cce-4125-ab6b-91d977ecf85b",
      "region_id": "2dbacea3-5889-4021-8f38-bc2214dd7423",
      "gal_tags": [
            "1c22be2e-1e2f-5f6d-bec5-842c5d48e9d3"
      ],  "user_data_path": "user_profiles.json",
      "user_data_format": "json",
      "rejected_users_path": "rejected_profiles.json",
      "quotas": {"ALL_MAIL_ATTACHENTS_SIZE": "1MB"},
      "roles": ["14718e3a-6c7b-5c9f-b4de-a897c356cb5e"]
}
```

Таблица 211 – Описание полей файла настроек **import_config.json**

Параметр	Тип	Описание
token-name	Str	Всегда имеет значение "ucs-access-token"
admin	Str	Логин и пароль пользователя, от имени которого будет выполняться импорт, обычно это администратор тенанта или инсталляции
cox	Str	Подключение к **Mailion**
tls_settings	Str	Сертификаты, используемые для подключения к системе
tenant_id	Str	Идентификатор тенанта

Параметр	Тип	Описание
region_id	Str	Идентификатор региона в формате UUID-строки
gal_tags	Str	Список идентификаторов GAL
user_data_path	Str	Путь к файлу с описанием импортируемых пользователей в одном из поддерживаемых форматов
user_data_format	Str	Формат файла импорта, может принимать одно из значений: JSON, CSV
rejected_users_path	Str	Путь к файлу, в который будут записываться пользователи, в процессе импорта которых возникла какая-либо ошибка
quotas	Str	Список квот для создаваемых пользователей: – ONE_MAIL_SIZE (размер письма); – ALL_MAILS_SIZE (размер всех писем); – ALL_MAIL_ATTACHMENTS_SIZE (размер всех вложений в письме)
roles	Str	Список идентификаторов дополнительных ролей пользователя

B.2 Схема записи пользователя

```
{
  "$schema": "http://json-schema.org/draft-07/schema#"
  "type": "object",
  "properties": {
    "correlation_id": {
      "description": "External system correlation ID",
      "type": "string",
      "minLength": 1,
      "maxLength": 256
    },
    "first_name": {
      "description": "First name",
      "type": "string",
      "minLength": 1,
      "maxLength": 255
    },
    "last_name": {
      "description": "Last name",
      "type": "string",
      "minLength": 1,
      "maxLength": 255
    },
    "middle_name": {
      "description": "Middle name",
      "type": "string",
      "minLength": 1,
      "maxLength": 255
    },
    "gender": {
      "description": "Gender",
```

```
      "enum": [
        "UNKNOWN",
        "MALE",
        "FEMALE",
        "NONE",
        "OTHER"
      ]
    },
    "birthday": {
      "description": "Birthday, for example: 2018-11-13",
      "type": "string",
      "format": "date"
    },
    "locale": {
      "description": "Locale tag as described in: https://www.rfc-
editor.org/rfc/bcp/bcp47.txt"
      "type": "string",
      "minLength": 2,
      "maxLength": 16
    },
    "addresses": {
      "description": "User addresses",
      "type": "array",
      "items": {
        "type": "object",
        "properties": {
          "name": {
            "description": "Address name",
            "type": "string",
            "maxLength": 1000
          },
          "country": {
            "description": "Country",
            "type": "string",
            "maxLength": 255
          },
          "region": {
            "description": "Region",
            "type": "string",
            "maxLength": 255
          },
          "city": {
            "description": "City",
            "type": "string",
            "maxLength": 255
          },
          "zip_code": {
            "description": "ZIP code",
            "type": "string",
            "maxLength": 100
          },
          "address": {
            "description": "Address",
            "type": "string",
            "maxLength": 1000
          },
          "floor": {
            "description": "Floor",
            "type": "string",
```

```
          "maxLength": 50
        },
        "room": {
          "description": "Room",
          "type": "string",
          "maxLength": 50
        },
        "workplace": {
          "description": "Workplace",
          "type": "string",
          "maxLength": 100
        },
        "coordinates": {
          "description": "Address coordinates",
          "type": "object",
          "properties": {
            "latitude": {
              "description": "Latitude",
              "type": "number",
              "minimum": -90,
              "maximum": 90
            },
            "longitude": {
              "description": "Longitude",
              "type": "number",
              "minimum": -180,
              "maximum": 180
            }
          },
          "required": [
            "latitude",
            "longitude"
          ]
        },
        "preference": {
          "description": "Level of preference of address",
          "type": "integer"
        },
        "type": {
          "description": "Arbitrary address type",
          "type": "string",
          "maxLength": 255
        }
      }
    }
  },
  "department": {
    "description": "Name of department",
    "type": "string",
    "maxLength": 255
  },
  "title": {
    "description": "Title",
    "type": "string",
    "maxLength": 255
  },
  "phones": {
    "description": "User phones",
    "type": "array",
```

```
    "items": {
      "type": "object",
      "properties": {
        "number": {
          "description": "Phone number",
          "type": "string",
          "pattern": "^(\\+)?[a-zA-Z0-9-.()~*# ]+$",
          "maxLength": 255
        },
        "preferable": {
          "description": "Preferred number marker",
          "type": "boolean"
        },
        "type": {
          "description": "Phone types",
          "type": "array",
          "items": {
            "enum": [
              "HOME",
              "WORK",
              "TEXT",
              "VOICE",
              "FAX",
              "CELL",
              "VIDEO",
              "PAGER",
              "TEXTPHONE"
            ]
          }
        }
      },
      "required": [
        "number"
      ]
    }
  },
  "reserve_email": {
    "description": "Reserve email of the user",
    "type": "string",
    "format": "email",
    "maxLength": 255
  },
  "logins": {
    "description": "User logins",
    "type": "array",
    "items": {
      "type": "object",
      "properties": {
        "login": {
          "description": "Login",
          "type": "string",
          "minLength": 1,
          "maxLength": 255
        },
        "password": {
          "description": "Password",
          "type": "string",
          "minLength": 1,
          "maxLength": 255
```

```
          }
        },
        "required": [
          "login",
          "password"
        ]
      },
      "minItems": 1
    },
    "emails": {
      "description": "User emails",
      "type": "array",
      "items": {
        "type": "object",
        "properties": {
          "email": {
            "description": "Email",
            "type": "string",
            "format": "email",
            "maxLength": 255
          },
          "primary": {
            "description": "Primary email marker",
            "type": "boolean"
          }
        },
        "required": [
          "email"
        ]
      },
      "minItems": 1
    }
  },
  "required": [
    "correlation_id",
    "first_name",
    "emails",
    "logins"
  ]
}
```

B.3 Список глобальных адресных книг

Пример файла **get_tenant_gals.json** приведен ниже. Описание полей файла настроек приведено в таблице 212.

```
{
  "token-name": "ucs-access-token",
  "admin": {
    "login": "admin_tenant",
    "password": "****"
  },
  "cox": {
    "endpoint": "127.0.0.1:31415",
```

```
    "service_name": "cox",
    "load_balanced": false,
    "use_tls": false,
    "use_tls_balancer": false,
    "compression": "none"
  },
  "tls_settings": {
    "ca_file": "ncloud_ca_cert.bundle.pem",
    "client_cert_file": "client.pem",
    "key_file": "key.pem"
  },
  "tenant_id": "01068ade-1cce-4125-ab6b-91d977ecf85b"
}
```

Таблица 212 – Описание полей файла настроек **get_tenant_gals.json**

Параметр	Тип	Описание
token-name	Str	Всегда имеет значение "ucs-access-token"
admin	Str	Логин и пароль пользователя, от имени которого будет выполняться импорт, обычно это администратор тенанта или инсталляции
cox	Str	Подключение к **Mailion**
tls_settings	Str	Сертификаты, используемые для подключения к системе
tenant_id	Str	Идентификатор тенанта
gal_tags	Str	Список идентификаторов GAL
user_data_path	Str	Путь к файлу с описанием импортируемых пользователей в одном из поддерживаемых форматов

B.4 Файл настроек импорта групп

Пример файла настроек **settings.json** приведен ниже. Описание полей приведено в таблице 213.

```
{
  "token-name": "ucs-access-token",
  "admin": {
    "login": "admin_tenant",
    "password": "****"
  },
  "cox": {
    "endpoint": "127.0.0.1:31415",
    "service_name": "cox",
    "load_balanced": false,
    "use_tls": false,
    "use_tls_balancer": false,
    "compression": "none"
  },
  "tls_settings": {
```

```
    "ca_file": "ncloud_ca_cert.bundle.pem",
    "client_cert_file": "client.pem",
    "key_file": "key.pem"
  },
  "tenant_id": "11068ade-1cce-4125-ab6b-91d977ecf85b",
  "region_id": "2dbacea3-5889-4021-8f38-bc2214dd7423",
  "gal_tags": [
    "1c22be2e-1e2f-5f6d-bec5-842c5d48e9d3"
  ],
  "groups_data_path": "groups.json",
  "groups_data_format": "json",
  "rejected_groups_path": "rejected_groups.json",
}
```

Таблица 213 – Описание полей файла настроек **settings.json**

Параметр	Тип	Описание
token-name	Str	Всегда имеет значение "ucs-access-token"
admin	Str	Логин и пароль пользователя, от имени которого будет выполняться импорт, обычно это администратор тенанта или инсталляции
cox	Str	Подключение к **Mailion**
tls_settings	Str	Сертификаты, используемые для подключения к системе
tenant_id	Str	Идентификатор тенанта UUID-строки
region_id	Str	Идентификатор региона в формате UUID-строки
gal_tags	Str	Список идентификаторов GAL
group_data_path	Str	Путь к файлу с описанием импортируемых пользователей в одном из поддерживаемых форматов
group_data_format	Str	Формат файла импорта, может принимать одно из значений: JSON, CSV
rejected_groups_path	Str	Путь к файлу, в который будут записываться пользователи, в процессе импорта которых возникла какая-либо ошибка

B.5 Схема записи группы

```
{
    "$schema": "http://json-schema.org/draft-04/schema#"
    "type": "object",
    "properties": {
      "correlation_id": {
        "type": "string",
        "minLength": 1,
        "maxLength": 255
      },
      "name": {
        "type": "string",
```

```
        "minLength": 1,
        "maxLength": 255
      },
      "description": {
        "type": "string",
        "maxLength": 255
      },
      "email": {
        "type": "string",
        "format": "email",
        "minLength": 1,
        "maxLength": 255
      }
    },
    "required": [
      "correlation_id",
      "name",
      "email"
    ]
  }
```

B.6 Файл настроек для импорта связей групп

Пример файла настроек **settings.json** приведен ниже. Описание полей приведено в таблице 214.

```
{
  "token-name": "ucs-access-token",
  "admin": {
    "login": "admin_tenant",
    "password": "****"
  },
  "cox": {
    "endpoint": "127.0.0.1:31415",
    "service_name": "cox",
    "load_balanced": false,
    "use_tls": false,
    "use_tls_balancer": false,
    "compression": "none"
  },
  "tls_settings": {
    "ca_file": "ncloud_ca_cert.bundle.pem",
    "client_cert_file": "client.pem",
    "key_file": "key.pem"
  },
  "group_links_data_path": "links.json",
  "group_links_data_format": "json",
  "rejected_group_links_path": "rejected_links.json",
}
```

Таблица 214 – Описание полей файла настроек **settings.json**

Параметр	Тип	Обязательный	Описание
token-name	Str	+	Всегда имеет значение "ucs-access-token"
admin	Str	+	Логин и пароль пользователя, от имени которого будет выполняться импорт, обычно это администратор тенанта или инсталляции
cox	Str	+	Подключение к **Mailion**
tls_settings	Str	+	Сертификаты, используемые для подключения к системе
group_links_data_path	Str	+	Путь к файлу с описанием импортируемых ресурсов в одном из поддерживаемых форматов. Если файл имеет расширение .json или .csv, то параметр `group_links_data_format` можно не задавать, формат будет выбран по расширению файла
group_links_data_format	Str	-	Формат файла импорта, может принимать одно из значений: JSON, CSV. Необязательный параметр, если у файла, указанного в параметре `groups_links_data_path`, есть расширение .json или .csv
rejected_groups_links_path	Str	-	Путь к файлу, в который система будет записывать группу, в процессе импорта которой возникла какая-либо ошибка. Если этот параметр не будет задан, то будет использоваться имя файла по умолчанию ("rejected_links.json") и такой файл будет создан в той же директории, что и файл, переданный для импорта

B.7 Схема записи связей групп

```
{
    "$schema": "http://json-schema.org/draft-04/schema#"
    "type": "object",
    "properties": {
      "correlation_id": {
        "type": "string",
        "minLength": 1,
        "maxLength": 255
      },
      "parent": {
        "type": "string",
        "format": "email",
        "minLength": 1,
        "maxLength": 255
      },
      "child": {
        "type": "string",
        "format": "email",
        "minLength": 1,
        "maxLength": 255
      }
    },
    "required": [
      "correlation_id",
      "parent",
      "child"
    ]
  }
```

B.8 Файл настроек импорта ресурсов

Пример файла настроек **settings.json** приведен ниже. Описание полей приведено в таблице 215.

```
{
  "token-name": "ucs-access-token",
  "admin": {
    "login": "admin_tenant",
    "password": "*****"
  },
  "cox": {
    "endpoint": "127.0.0.1:31415",
    "service_name": "cox",
    "load_balanced": false,
    "use_tls": false,
    "use_tls_balancer": false,
    "compression": "none"
  },
  "tls_settings": {
    "ca_file": "ncloud_ca_cert.bundle.pem",
```

```
    "client_cert_file": "client.pem",
    "key_file": "key.pem"
  },
  "tenant_id": "11068ade-1cce-4125-ab6b-91d977ecf85b",
  "region_id": "2dbacea3-5889-4021-8f38-bc2214dd7423",
  "gal_tags": [
    "1c22be2e-1e2f-5f6d-bec5-842c5d48e9d3"
  ],
  "resource_data_path": "resource.json",
  "resource_data_format": "json",
  "rejected_resources_path": "rejected_resource.json",
}
```

Таблица 215 – Описание полей файла настроек **settings.json**

Параметр	Тип	Обязательный	Описание
token-name	Str	+	Всегда имеет значение "ucs-access-token"
admin	Str	+	Логин и пароль пользователя, от имени которого будет выполняться импорт, обычно это администратор тенанта или инсталляции
cox	Str	+	Подключение к **Mailion**
tls_settings	Str	+	Сертификаты, используемые для подключения к системе
tenant_id	Str	+	Идентификатор тенанта UUID-строки
region_id	Str	+	Идентификатор региона в формате UUID-строки
gal_tags	Str	+	Список идентификаторов GAL
resources_data_path	Str	+	Путь к файлу с описанием импортируемых пользователей в одном из поддерживаемых форматов
resources_data_format	Str	-	Формат файла импорта, может принимать одно из значений: JSON, CSV
rejected_resources_path	Str	-	Путь к файлу, в который будут записываться пользователи, в процессе импорта которых возникла какая-либо ошибка

B.9 Схема записи ресурса

```
{
  "$schema": "http://json-schema.org/draft-04/schema#"
```

```
"type": "object",
"properties": {
  "correlation_id": {
    "type": "string",
    "minLength": 1,
    "maxLength": 255
  },
  "name": {
    "type": "string",
    "minLength": 1,
    "maxLength": 255
  },
  "description": {
    "type": "string",
    "maxLength": 255
  },
  "capacity": {
    "type": "integer",
    "minimum": 1
  },
  "email": {
    "type": "string",
    "format": "email",
    "minLength": 1,
    "maxLength": 255
  },
  "location_name": {
    "type": "string",
    "maxLength": 255
  },
  "country": {
    "type": "string"
  },
  "city": {
    "type": "string",
    "maxLength": 255
  },
  "address": {
    "type": "string",
    "maxLength": 255
  },
  "zip_code": {
    "type": "string",
    "maxLength": 255
  },
  "floor": {
    "type": "string",
    "maxLength": 255
  },
  "room": {
    "type": "string",
    "maxLength": 255
  },
  "workplace": {
    "type": "string",
    "maxLength": 255
  },
  "login": {
    "type": "string",
```

```
      "minLength": 1,
      "maxLength": 255
    },
    "password": {
      "type": "string",
      "minLength": 1,
      "maxLength": 255
    },
    "autobook": {
      "type": "boolean"
    },
    "minimal_participation_number": {
      "type": "integer",
      "minimum": 1
    }
  },
  "required": [
    "correlation_id",
    "name",
    "email",
    "password",
    "capacity",
    "minimal_participation_number"
  ]
}
```

B.10 Конфигурационный файл для миграции календаря из Microsoft Exchange в ПО «Mailion»

Пример конфигурационного файла приведен ниже:

```
{
    "daidal": {
        "balancer_endpoints": [
            "hydra.ucs-apps-1.installation.example.net:50053"
        ],
        "compression": "none",
        "keep_alive": false,
        "keep_alive_time": "15s",
        "keep_alive_timeout": "10s",
        "load_balanced": true,
        "request_timeout": "10s",
        "service_name": "daidal",
        "use_tls": true,
        "use_tls_balancer": true
    },
    "dispersed_object_store": {
        "balancer_endpoints": [
            "hydra.ucs-apps-1.installation.example.net:50053"
        ],
        "compression": "none",
        "keep_alive": false,
        "keep_alive_time": "15s",
        "keep_alive_timeout": "10s",
        "load_balanced": true,
        "methods": {
```

```
            "increment_copies": {
                "success_copies_num": "quorum"
            },
            "read": {
                "success_copies_num": "any"
            },
            "write": {
                "success_copies_num": "quorum"
            }
        },
        "namespace": "attach",
        "request_timeout": "10s",
        "service_name": "dispersed-object-store",
        "temporary_ttl": "1h",
        "use_tls": true,
        "use_tls_balancer": true
    },
    "erakles": {
        "balancer_endpoints": [
            "hydra.ucs-apps-1.installation.example.net:50053"
        ],
        "compression": "none",
        "keep_alive": false,
        "keep_alive_time": "15s",
        "keep_alive_timeout": "10s",
        "load_balanced": true,
        "request_timeout": "10s",
        "service_name": "erakles",
        "use_tls": true,
        "use_tls_balancer": true
    },
    "external_sync": {
        "exchanges": {
            "IS7YluhZ318G7Sm89SkkfZbO": {
                "impersonation_password": "vault:ms_exhange_impersonation",
                "impersonation_username": "AD\\ADUSR01",
                "servers": [
                    {
                        "ca_file": "/home/admin-msk/kex/cert/mdcad-dc-
01.ad.example.net.pem",
                        "endpoint": "https://exchange-
ad.ad.example.net/EWS/exchange.asmx"
                        "timeout": "1m",
                        "tls_handshake_timeout": "2s",
                        "tls_min_version": "tls1_2"
                    }
                ],
                "useragent": "ucs-mexa"
            }
        }
    },
    "hog": {
        "balancer_endpoints": [
            "hydra.ucs-apps-1.installation.example.net:50053"
        ],
        "compression": "none",
        "keep_alive": false,
        "keep_alive_time": "15s",
        "keep_alive_timeout": "10s",
```

```
        "load_balanced": true,
        "request_timeout": "10s",
        "service_name": "hog",
        "use_tls": true,
        "use_tls_balancer": true
    },
    "kongur": {
        "balancer_endpoints": [
            "hydra.ucs-apps-1.installation.example.net:50053"
        ],
        "compression": "none",
        "keep_alive": false,
        "keep_alive_time": "15s",
        "keep_alive_timeout": "10s",
        "load_balanced": true,
        "request_timeout": "10s",
        "service_name": "kongur",
        "use_tls": true,
        "use_tls_balancer": true
    },
    "logging": {
        "dump_level": "debug",
        "ultra_human": true
    },
    "marker": {
        "balancer_endpoints": [
            "hydra.ucs-apps-1.installation.example.net:50053"
        ],
        "compression": "none",
        "keep_alive": false,
        "keep_alive_time": "15s",
        "keep_alive_timeout": "10s",
        "load_balanced": true,
        "request_timeout": "10s",
        "service_name": "marker",
        "use_tls": true,
        "use_tls_balancer": true
    },
    "minos": {
        "balancer_endpoints": [
            "hydra.ucs-apps-1.installation.example.net:50053"
        ],
        "compression": "none",
        "keep_alive": false,
        "keep_alive_time": "15s",
        "keep_alive_timeout": "10s",
        "load_balanced": true,
        "request_timeout": "10s",
        "service_name": "minos",
        "use_tls": true,
        "use_tls_balancer": true
    },
    "report_logging": {
        "buffer_capacity": 512,
        "colorize": false,
        "development": true,
        "disable_caller": false,
        "dump_level": "error",
        "elastic_config": null,
```

```
        "enable_dump": false,
        "enable_stacktrace": false,
        "file_config": {
            "path": "report.txt"
        },
        "identity": "m2e",
        "level": "debug",
        "output_format": "text",
        "sampling": null,
        "show_secrets": true,
        "skip_callers": 0,
        "type": "file",
        "ultra_human": false,
        "ultra_human_fields": null
    },
    "server": {
        "balancer_endpoints": [
            "hydra.ucs-apps-1.installation.example.net:50053"
        ],
        "compression": "none",
        "discovery_type": "etcd",
        "keep_alive": false,
        "keep_alive_balancer": false,
        "listen_endpoint": "0.0.0.0:6788",
        "load_balanced": true,
        "max_recv_size": "0B",
        "max_send_size": "0B",
        "service_address": "kex.ucs-apps-1.installation.example.net",
        "service_name": "kex",
        "use_tls": true,
        "use_tls_balancer": true
    },
    "service_auth": {
        "basic": {
            "login": "kex_login",
            "password": "vault:ucs_service_account_kex"
        },
        "type": "basic"
    },
    "sophokles": {
        "balancer_endpoints": [
            "hydra.ucs-apps-1.installation.example.net:50053"
        ],
        "compression": "none",
        "keep_alive": false,
        "keep_alive_time": "15s",
        "keep_alive_timeout": "10s",
        "load_balanced": true,
        "request_timeout": "10s",
        "service_name": "sophokles",
        "use_tls": true,
        "use_tls_balancer": true
    },
    "tls_settings": {
        "ca_file": "/home/admin-msk/kex/certs/ucs-infra-
1.installation.example.net-main-ca.pem",
        "client_auth_type": "require_and_verify_client_cert",
        "client_cert_file": "/home/admin-msk/kex/certs/kex.ucs-apps-
1.installation.example.net-main-client.pem",
```

```
        "key_file": "/home/admin-msk/kex/certs/kex.ucs-apps-
1.installation.example.net-main-key.pem",
        "server_cert_file": "/home/admin-msk/kex/certs/kex.ucs-apps-
1.installation.example.net-main-server.pem",
        "server_name_override": "",
        "tls_min_version": "tls1_2"
    },
    "tracer": {
        "reporter": {
            "buffer_flush_interval": "1s",
            "collector_endpoint": "ucs-infra-1.installation.example.net:6831",
            "log_spans": false,
            "queue_size": 10
        },
        "sampler": {
            "param": 1,
            "type": "const"
        },
        "use_tracer": false
    },
    "ucr_codec": {
        "cipher_key": "vault:codec_secret_key_rcr",
        "doc_preview_url_prefix": "https://api-
installation.example.net/doc_preview"
        "mail_source_url_prefix": "https://api-
installation.example.net/mail_source"
        "rcr_url_prefix": "https://api-installation.example.net/attach/read
    }
}
```

B.11 Конфигурационный файл для миграции календаря из ПО «Mailion» в Microsoft Exchange

Пример конфигурационного файла приведен ниже:

```
{
    "daidal": {
        "balancer_endpoints": [
            "hydra.ucs-apps-1.installation.example.net:50053"
        ],
        "compression": "none",
        "keep_alive": false,
        "keep_alive_time": "15s",
        "keep_alive_timeout": "10s",
        "load_balanced": true,
        "request_timeout": "10s",
        "service_name": "daidal",
        "use_tls": true,
        "use_tls_balancer": true
    },
    "dispersed_object_store": {
        "balancer_endpoints": [
            "hydra.ucs-apps-1.installation.example.net:50053"
        ],
        "compression": "none",
        "keep_alive": false,
```

```
        "keep_alive_time": "15s",
        "keep_alive_timeout": "10s",
        "load_balanced": true,
        "methods": {
            "increment_copies": {
                "success_copies_num": "quorum"
            },
            "read": {
                "success_copies_num": "any"
            },
            "write": {
                "success_copies_num": "quorum"
            }
        },
        "namespace": "attach",
        "request_timeout": "10s",
        "service_name": "dispersed-object-store",
        "temporary_ttl": "1h",
        "use_tls": true,
        "use_tls_balancer": true
    },
    "erakles": {
        "balancer_endpoints": [
            "hydra.ucs-apps-1.installation.example.net:50053"
        ],
        "compression": "none",
        "keep_alive": false,
        "keep_alive_time": "15s",
        "keep_alive_timeout": "10s",
        "load_balanced": true,
        "request_timeout": "10s",
        "service_name": "erakles",
        "use_tls": true,
        "use_tls_balancer": true
    },
    "exponential_backoff": {
        "forever": false,
        "init_interval": "2s",
        "max_elapsed_time": "30s",
        "max_interval": "10s",
        "multiplier": 1.5,
        "randomization_factor": 0.5
    },
    "external_sync": {
        "exchanges": {
            "IS7YluhZ318G7Sm89SkkfZbO": {
                "impersonation_password": "vault:ms_exhange_impersonation",
                "impersonation_username": "AD\\ADUSR01",
                "servers": [
                    {
                        "ca_file": "/home/admin-msk/kex/cert/mdcad-dc-
01.ad.example.net.pem",
                        "endpoint": "https://exchange-
ad.ad.example.net/EWS/exchange.asmx"
                        "timeout": "1m",
                        "tls_handshake_timeout": "2s",
                        "tls_min_version": "tls1_2"
                    }
                ],
```

```
            "useragent": "ucs-mexa"
        }
    }
},
"hog": {
    "balancer_endpoints": [
        "hydra.ucs-apps-1.installation.example.net:50053"
    ],
    "compression": "none",
    "keep_alive": false,
    "keep_alive_time": "15s",
    "keep_alive_timeout": "10s",
    "load_balanced": true,
    "request_timeout": "10s",
    "service_name": "hog",
    "use_tls": true,
    "use_tls_balancer": true
},
"ical": {
    "calscale": "GREGORIAN",
    "prod_id": "Mailion Mailion_1.7",
    "version": "2.0"
},
"kongur": {
    "balancer_endpoints": [
        "hydra.ucs-apps-1.installation.example.net:50053"
    ],
    "compression": "none",
    "keep_alive": false,
    "keep_alive_time": "15s",
    "keep_alive_timeout": "10s",
    "load_balanced": true,
    "request_timeout": "10s",
    "service_name": "kongur",
    "use_tls": true,
    "use_tls_balancer": true
},
"kronos": {
    "balancer_endpoints": [
        "hydra.ucs-apps-1.installation.example.net:50053"
    ],
    "compression": "none",
    "is_external": false,
    "keep_alive": false,
    "keep_alive_time": "15s",
    "keep_alive_timeout": "10s",
    "load_balanced": true,
    "request_timeout": "10s",
    "retry_policy": {
        "count": 3,
        "delay": "5m"
    },
    "service_name": "kronos",
    "use_tls": true,
    "use_tls_balancer": true
},
"logging": {
    "dump_level": "debug",
    "ultra_human": true
```

```
    },
    "marker": {
        "balancer_endpoints": [
            "hydra.ucs-apps-1.installation.example.net:50053"
        ],
        "compression": "none",
        "keep_alive": false,
        "keep_alive_time": "15s",
        "keep_alive_timeout": "10s",
        "load_balanced": true,
        "request_timeout": "10s",
        "service_name": "marker",
        "use_tls": true,
        "use_tls_balancer": true
    },
    "minos": {
        "balancer_endpoints": [
            "hydra.ucs-apps-1.installation.example.net:50053"
        ],
        "compression": "none",
        "keep_alive": false,
        "keep_alive_time": "15s",
        "keep_alive_timeout": "10s",
        "load_balanced": true,
        "request_timeout": "10s",
        "service_name": "minos",
        "use_tls": true,
        "use_tls_balancer": true
    },
    "mixer": {
        "balancer_endpoints": [
            "hydra.ucs-apps-1.installation.example.net:50053"
        ],
        "compression": "none",
        "keep_alive": false,
        "keep_alive_time": "15s",
        "keep_alive_timeout": "10s",
        "load_balanced": true,
        "request_timeout": "10s",
        "service_name": "mixer",
        "use_tls": true,
        "use_tls_balancer": true
    },
    "report_logging": {
        "buffer_capacity": 512,
        "colorize": false,
        "development": true,
        "disable_caller": false,
        "dump_level": "error",
        "elastic_config": null,
        "enable_dump": false,
        "enable_stacktrace": false,
        "file_config": {
            "path": "report.txt"
        },
        "identity": "m2e",
        "level": "debug",
        "output_format": "text",
        "sampling": null,
```

```
        "show_secrets": true,
        "skip_callers": 0,
        "type": "file",
        "ultra_human": false,
        "ultra_human_fields": null
    },
    "server": {
        "balancer_endpoints": [
            "hydra.ucs-apps-1.installation.example.net:50053"
        ],
        "compression": "none",
        "discovery_type": "etcd",
        "keep_alive": false,
        "keep_alive_balancer": false,
        "listen_endpoint": "0.0.0.0:6788",
        "load_balanced": true,
        "max_recv_size": "0B",
        "max_send_size": "0B",
        "service_address": "kex.ucs-apps-1.installation.example.net",
        "service_name": "kex",
        "use_tls": true,
        "use_tls_balancer": true
    },
    "service_auth": {
        "basic": {
            "login": "kex_login",
            "password": "vault:ucs_service_account_kex"
        },
        "type": "basic"
    },
    "sophokles": {
        "balancer_endpoints": [
            "hydra.ucs-apps-1.installation.example.net:50053"
        ],
        "compression": "none",
        "keep_alive": false,
        "keep_alive_time": "15s",
        "keep_alive_timeout": "10s",
        "load_balanced": true,
        "request_timeout": "10s",
        "service_name": "sophokles",
        "use_tls": true,
        "use_tls_balancer": true
    },
    "tls_settings": {
        "ca_file": "/home/admin-msk/kex/certs/ucs-infra-
1.installation.example.net-main-ca.pem",
        "client_auth_type": "require_and_verify_client_cert",
        "client_cert_file": "/home/admin-msk/kex/certs/kex.ucs-apps-
1.installation.example.net-main-client.pem",
        "key_file": "/home/admin-msk/kex/certs/kex.ucs-apps-
1.installation.example.net-main-key.pem",
        "server_cert_file": "/home/admin-msk/kex/certs/kex.ucs-apps-
1.installation.example.net-main-server.pem",
        "server_name_override": "",
        "tls_min_version": "tls1_2"
    },
    "tracer": {
        "reporter": {
```

```
            "buffer_flush_interval": "1s",
            "collector_endpoint": "ucs-infra-1.installation.example.net:6831",
            "log_spans": false,
            "queue_size": 10
        },
        "sampler": {
            "param": 1,
            "type": "const"
        },
        "use_tracer": false
    },
    "ucr_codec": {
        "cipher_key": "vault:codec_secret_key_rcr",
        "doc_preview_url_prefix": "https://api-
installation.example.net/doc_preview"
        "mail_source_url_prefix": "https://api-
installation.example.net/mail_source"
        "rcr_url_prefix": "https://api-installation.example.net/attach/read
    },
    "ultar": {
        "max_cal_size": -1,
        "max_desc_size": 1024,
        "max_sum_size": 255
    }
}
```

B.12 Конфигурационный файл для миграции почты из Microsoft Exchange в ПО «Mailion», из ПО «Mailion» в Microsoft Exchange

Пример конфигурационного файла приведен ниже:

```
{
    "atlas": {
        "balancer_endpoints": [
            "hydra.ucs-apps-1.installation.example.net:50053",
            "hydra.ucs-apps-2.installation.example.net:50053"
        ],
        "compression": "none",
        "load_balanced": true,
        "max_recv_size": "0B",
        "max_send_size": "0B",
        "request_timeout": "10s",
        "service_name": "atlas",
        "use_tls": true,
        "use_tls_balancer": true
    },
    "beef": {
        "balancer_endpoints": [
            "hydra.ucs-apps-1.installation.example.net:50053",
            "hydra.ucs-apps-2.installation.example.net:50053"
        ],
        "compression": "none",
        "load_balanced": true,
        "request_timeout": "10s",
        "service_name": "beef",
        "use_tls": true,
```

```
        "use_tls_balancer": true
    },
    "daidal": {
        "balancer_endpoints": [
            "hydra.ucs-apps-1.installation.example.net:50053",
            "hydra.ucs-apps-2.installation.example.net:50053"
        ],
        "compression": "none",
        "load_balanced": true,
        "request_timeout": "10s",
        "service_name": "daidal",
        "use_tls": true,
        "use_tls_balancer": true
    },
    "erakles": {
        "balancer_endpoints": [
            "hydra.ucs-apps-1.installation.example.net:50053",
            "hydra.ucs-apps-2.installation.example.net:50053"
        ],
        "compression": "none",
        "load_balanced": true,
        "request_timeout": "10s",
        "service_name": "erakles",
        "use_tls": true,
        "use_tls_balancer": true
    },
    "xync": {
        "enabled": false,
        "sync_chunk_length": 100,
        "message_size_limit": "30Mb",
        "save_message_timeout":"1m0s"
    },
    "external_sync": {
        "exchanges": {
            "IS7YluhZ318G7Sm89SkkfZbO": {
                "impersonation_password": "RhtgjcnmLe[f",
                "impersonation_username": "AD\\ADUSR01",
                "servers": [
                    {
                        "ca_file": "/etc/pki/tls/certs/mdcad-dc-
01.ad.example.net.pem",
                        "endpoint": "https://exchange-
ad.ad.example.net/EWS/exchange.asmx"
                        "timeout": "1m",
                        "tls_handshake_timeout": "2s",
                        "tls_min_version": "tls1_2"
                    }
                ],
            }
        }
    },
    "hog": {
        "balancer_endpoints": [
            "hydra.ucs-apps-1.installation.example.net:50053",
            "hydra.ucs-apps-2.installation.example.net:50053"
        ],
        "compression": "none",
        "load_balanced": true,
        "request_timeout": "10s",
```

```
        "service_name": "hog",
        "use_tls": true,
        "use_tls_balancer": true
    },
    "logging": {
        "buffer_capacity": 512,
        "development": true,
        "dump_level": "error",
        "enable_dump": false,
        "identity": "viper",
        "level": "debug",
        "meta_fields_param_prefix": "nctlog_",
        "output_format": "text",
        "show_secrets": true,
        "syslog_config": {
            "address": "172.17.0.1:514",
            "network": "udp"
        },
        "type": "syslog"
    },
    "marker": {
        "balancer_endpoints": [
            "hydra.ucs-apps-1.installation.example.net:50053",
            "hydra.ucs-apps-2.installation.example.net:50053"
        ],
        "compression": "none",
        "load_balanced": true,
        "request_timeout": "10s",
        "service_name": "marker",
        "use_tls": true,
        "use_tls_balancer": true
    },
    "minos": {
        "balancer_endpoints": [
            "hydra.ucs-apps-1.installation.example.net:50053",
            "hydra.ucs-apps-2.installation.example.net:50053"
        ],
        "compression": "none",
        "load_balanced": true,
        "request_timeout": "10s",
        "service_name": "minos",
        "use_tls": true,
        "use_tls_balancer": true
    },
    "server": {
    "compression": "none",
    "discovery_type": "native",
    "listen_endpoint": ":8181",
    "load_balanced": false,
    "max_recv_size": "0B",
    "max_send_size": "0B",
    "service_name": "viper",
    "use_tls": false,
    "use_tls_balancer": false
},
    "service_auth": {
        "basic": {
            "login": "viper_login",
            "password": "ieg9ShohngaevoiXohZo"
```

```
        },
        "type": "basic"
    },
    "sophokles": {
        "balancer_endpoints": [
            "hydra.ucs-apps-1.installation.example.net:50053",
            "hydra.ucs-apps-2.installation.example.net:50053"
        ],
        "compression": "none",
        "load_balanced": true,
        "request_timeout": "10s",
        "service_name": "sophokles",
        "use_tls": true,
        "use_tls_balancer": true
    },
    "tls_settings": {
        "ca_file": "/etc/pki/tls/certs/ucs-infra-1.installation.example.net-
main-ca.pem",
        "client_auth_type": "require_and_verify_client_cert",
        "client_cert_file": "/etc/pki/tls/certs/viper.ucs-apps-
1.installation.example.net-main-client.pem",
        "key_file": "/etc/pki/tls/private/viper.ucs-apps-
1.installation.example.net-main-key.pem",
        "server_cert_file": "/etc/pki/tls/certs/viper.ucs-apps-
1.installation.example.net-main-server.pem",
        "server_name_override": "",
        "tls_min_version": "tls1_2"
    },
    "tracer": {
        "reporter": {
            "buffer_flush_interval": "1s",
            "collector_endpoint": "jaeger.example.net:6831",
            "log_spans": false,
            "queue_size": 10
        },
        "sampler": {
            "param": 1,
            "type": "const"
        },
        "use_tracer": true
    },
    "ucr_codec": {
        "cipher_key": "Ivu6Z0hD3C52fMKvIHK2WEerNyL71EMcIDhnGSQy95U=",
        "doc_preview_url_prefix": "https://api-
installation.example.net/doc_preview"
        "mail_source_url_prefix": "https://api-
installation.example.net/mail_source"
        "rcr_url_prefix": "https://api-installation.example.net/attach/read
    },
    "viper": {
        "balancer_endpoints": [
            "hydra.ucs-apps-1.installation.example.net:50053",
            "hydra.ucs-apps-2.installation.example.net:50053"
        ],
        "compression": "none",
        "load_balanced": true,
        "request_timeout": "10s",
        "service_name": "viper",
        "use_tls": true,
```

```
        "use_tls_balancer": true
    },
    "weaver": {
        "balancer_endpoints": [
            "hydra.ucs-apps-1.installation.example.net:50053",
            "hydra.ucs-apps-2.installation.example.net:50053"
        ],
        "compression": "none",
        "load_balanced": true,
        "request_timeout": "10s",
        "service_name": "weaver",
        "use_tls": true,
        "use_tls_balancer": true
    }
}
```