

ООО «НОВЫЕ ОБЛАЧНЫЕ ТЕХНОЛОГИИ»

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

MAILION

2.1

РУКОВОДСТВО ПО АДМИНИСТРИРОВАНИЮ

Версия 2

На 456 листах

Дата публикации: 05.02.2025

**Москва
2025**

Все упомянутые в этом документе названия продуктов, логотипы, торговые марки и товарные знаки принадлежат их владельцам.

Товарные знаки «МойОфис», «MyOffice», «Squadus», «Mailion» принадлежат ООО «НОВЫЕ ОБЛАЧНЫЕ ТЕХНОЛОГИИ».

Ни при каких обстоятельствах нельзя истолковывать любое содержимое настоящего документа как прямое или косвенное предоставление лицензии или права на использование товарных знаков, логотипов или знаков обслуживания, приведенных в нем. Любое несанкционированное использование этих товарных знаков, логотипов или знаков обслуживания без письменного разрешения их правообладателя строго запрещено.

СОДЕРЖАНИЕ

1 Общие сведения	12
1.1 Назначение	12
1.2 Уровень подготовки пользователя	12
1.3 Системные требования	13
1.4 Уровень доступности ПО «Mailion»	13
1.5 Ограничения	13
1.5.1 Поддерживаемые языки интерфейса	13
1.5.2 Парольная политика	13
2 Подготовка к работе	15
2.1 Доступ к ПО «Mailion»	15
2.2 Запуск системы	15
2.3 Проверка работоспособности системы	15
3 Ролевая модель администрирования	17
3.1 Права администраторов ролевой модели	18
3.2 Создание администраторов	18
3.2.1 Уровень инсталляции	18
3.2.2 Уровень тенанта	18
3.3 Команды управления ролевой моделью	19
3.3.1 Команды управления ролями	19
3.3.2 Команды управления правами	23
3.3.3 Команды создания администраторов	24
3.3.4 Команды управления администраторами тенанта	27
4 Работа в Панели администрирования	30
4.1 Интерфейс приложения Панель администрирования	30
4.2 Управление пользователями	32
4.2.1 Просмотр списка пользователей	32
4.2.2 Просмотр записи о пользователе	33
4.2.3 Создание пользователя	34
4.2.4 Поиск пользователя	38
4.2.5 Блокировка пользователя	39
4.2.6 Разблокировка пользователя	40

4.2.7	Удаление пользователя	42
4.2.8	Сброс пароля пользователя	43
4.2.9	Завершение всех сеансов пользователя	44
4.2.10	Добавление пользователей в группы рассылки	44
4.2.11	Исключение пользователей из группы рассылки	47
4.2.12	Редактирование данных пользователя	48
4.3	Управление группами рассылки	50
4.3.1	Просмотр групп рассылок	50
4.3.2	Просмотр записи о группе	52
4.3.3	Создание группы рассылки	52
4.3.4	Поиск группы рассылки	55
4.3.5	Добавление группы рассылки в другую группу	56
4.3.6	Удаление групп рассылки	57
4.3.7	Редактирование группы рассылки	57
4.3.8	Настройка динамических групп рассылки	59
4.4	Управление ресурсами	61
4.4.1	Создание ресурса	61
4.4.2	Просмотр данных о пространстве для встречи	62
4.4.3	Поиск ресурса	63
4.4.4	Редактировать запись о пространстве для встречи	63
4.4.5	Фильтрация ресурсов	63
4.4.6	Удаление ресурса	63
4.5	Управление доменами	64
4.5.1	Создание домена	64
4.5.2	Поиск домена	65
4.5.3	Просмотр данных о домене	65
4.5.4	Редактировать запись о домене	65
4.5.5	Фильтрация доменов	66
4.5.6	Удаление домена	66
4.6	Управление единицами организационной структуры	66
4.6.1	Создание организационной единицы	67
4.6.2	Просмотр данных	68
4.6.3	Редактирование организационной единицы	68
4.6.4	Поиск единицы организационной структуры	69
4.6.5	Создание дочерней единицы	69

4.6.6	Удаление дочерней единицы	70
4.6.7	Удаление организационной единицы	70
4.7	Управление сотрудниками	71
4.7.1	Добавление нового сотрудника	71
4.7.2	Редактирование записи о сотруднике	73
4.7.3	Поиск сотрудника	73
4.7.4	Удаление сотрудника	73
4.8	Управление справочниками	73
4.8.1	Создание записи в справочнике	73
4.8.2	Поиск записи в справочнике	74
4.8.3	Редактирование записи в справочнике	74
4.8.4	Удалить запись в справочнике	75
4.9	Управление настройками организации	75
4.9.1	Основные настройки	75
4.9.2	Ограничения почты	76
5	Расширенное администрирование с помощью интерфейса командной строки	78
5.1	Информация для работы с интерфейсом командной строки	78
5.1.1	Установка	78
5.1.2	Просмотр информации о командах	78
5.1.3	Получение сертификатов для работы с ministerium	79
5.2	Установка и получение общей квоты тенанта	79
5.3	Операции над тенантом	81
5.3.1	Создание тенанта	81
5.3.2	Создание администратора тенанта	84
5.3.3	Создание пользователя тенанта	86
5.3.4	Добавление роли администратора тенанта пользователю	93
5.3.5	Создание общего почтового ящика	94
5.3.6	Настройка квот и лимитов для почты в тенанте	96
5.3.7	Удаление тенанта	112
5.3.8	Учетная запись для резервного копирования	113
5.3.9	Удаление письма у всех получателей в рамках тенанта	115
5.3.10	Экспорт и импорт данных пользователя	116
5.4	Создание пользовательских GAL-тегов	128
5.5	Работа с импортированными контактами	130

5.5.1	Импорт контактов	130
5.5.2	Удаление импортированных контактов	132
5.5.3	Поиск импортированных контактов	134
5.6	Настройка двухфакторной аутентификации	136
5.7	Создание домена	139
5.8	Создание первичной организационной структуры	143
5.9	Создание организации	146
5.10	Операции над пользователями, группами и ресурсами	148
5.11	Ограничение бронирования списком пользователей	154
5.12	Делегирование управления группами	156
5.13	Создание динамической группы	159
5.14	Массовое создание пользователей в каталоге	162
5.14.1	Подготовка файла импорта	165
5.14.2	Примеры сообщений системы	168
5.14.3	Возможные ошибки при импорте пользователей	169
5.15	Массовое создание групп в каталоге	173
5.15.1	Импорт групп	174
5.15.2	Импорт связей групп	177
5.15.3	Подготовка файла импорта	179
5.15.4	Примеры сообщений системы	180
5.15.5	Возможные ошибки при импорте групп	181
5.15.6	Автоматизация переноса групп и их связей из LDAP-каталогов в Mailion	185
5.16	Массовое создание ресурсов в каталоге	186
5.16.1	Подготовка файла импорта	190
5.16.2	Примеры сообщений системы	191
5.16.3	Возможные ошибки при импорте объектов ресурсов	193
5.17	Удаление пользователя, группы и ресурса	195
5.18	Управление делегированием учетных записей	195
5.18.1	Предоставление доступа к почте пользователя с правами «Не разрешено»	196
5.18.2	Предоставление доступа к почте пользователя с правами «От имени»	198
5.18.3	Предоставление доступа к почте пользователя с правами «Напрямую»	200
5.18.4	Отзыв доступа к делегированной учетной записи у всех делегатов	201
5.18.5	Отзыв доступа к делегированной учетной записи у определенного делегата	204
5.18.6	Просмотр всех делегатов	208

5.18.7	Просмотр всех делегированных учетных записей	210
5.19	Поиск писем по заданным критериям	213
5.20	Поиск сведений о доставленных письмах	222
5.21	Массовое удаление писем	223
5.22	Восстановление удаленных писем в почтовом ящике пользователя	225
5.23	Просмотр истории комментариев блокировки пользователей	229
5.24	Работа с корпоративными подписями	232
5.25	Работа с черными и белыми списками отправителей	239
5.25.1	Добавление отправителей в список	240
5.25.2	Обновление списка отправителей	242
5.25.3	Удаление отправителей из списка	243
5.26	Управление почтовыми правилами и политиками	244
5.26.1	Просмотр созданных правил	244
5.26.2	Создание правила	245
5.26.3	Обновление правила	248
5.26.4	Удаление правила	249
6	Миграция и синхронизация	251
6.1	Синхронизация данных из внешних каталогов	251
6.1.1	Запуск сервиса phalanx	251
6.1.2	Конфигурация сервиса phalanx	252
6.1.3	Основные команды для работы с интеграциями	253
6.1.4	Файл описания интеграции	255
6.2	Миграция внешних пользователей	257
6.3	Миграция идентификаторов из внешних каталогов	258
7	Сопоставление атрибутов LDAP-каталогов	261
7.1	Настройка сопоставления с помощью файла-шаблона	261
7.2	Добавление сопоставления командами	265
7.2.1	Добавление сопоставления при создании домена	266
7.2.2	Добавление сопоставления при настройке делегации домена	270
7.2.3	Добавление сопоставления при обновлении делегирования домена	274
7.2.4	Создание делегации с типом «делегация на одинаковых доменах»	278
8	Регистрация событий в формате CEF	284
9	Настройка интеграции ADFS средствами SAML	289

9.1	Добавление SAML-сервиса в ADFS	290
9.2	Создание интеграции в домене	293
9.3	Настройка плагина в house	295
9.4	Создание пользователя в AD	297
10	Настройка Kerberos	299
10.1	Поддержка Kerberos для домена	299
10.2	Настройка для веб-клиента	302
10.2.1	Настройка браузера для авторизации через Kerberos	302
10.2.2	Проверка конфигурации Kerberos	302
10.2.3	Настройка ОС Windows	302
10.2.4	Настройка браузеров в ОС Windows	303
11	Интеграция с ПО «МойОфис Частное Облако»	310
11.1	Настройка ПО «МойОфис Частное Облако»	310
11.2	Настройка ПО «Mailion»	311
12	Интеграция с ПО Squadus	313
13	Интеграция с ПО Skype4Business	315
14	Настройка ограничений для поиска по вложениям	316
14.1	Ограничение размера вложений для поиска	316
14.2	Отключение поиска по вложениям	316
14.3	Ограничение скорости парсинга	316
15	Настройка поиска в почте	318
16	Обновление сертификатов на фронтенд-серверах	319
17	Резервное копирование и восстановление отдельных сервисов	320
17.1	Dispersed Object Store	320
17.1.1	Снятие резервных копий	321
17.1.2	Проверка статуса резервного копирования	321
17.1.3	Получение списка резервных копий	322
17.1.4	Восстановление из резервной копии	322
17.2	Redis	325
17.2.1	Резервное копирование	325
17.2.2	Восстановление	326
17.3	MongoDB	326

17.3.1 Резервное копирование	326
17.3.2 Восстановление	327
17.4 Подсистема поиска	328
17.4.1 Ручная синхронизация данных поиска по пользователям (dirbek)	328
17.4.2 Ручная переиндексация почтовых ящиков и календарных событий в поиске	329
17.5 Vault	329
17.5.1 Миграция данных в хранилище типа Raft	330
17.5.2 Установка механизма резервного копирования	331
17.5.3 Ручной запуск резервного копирования	331
17.5.4 Восстановление	331
18 Резервное копирование и восстановление всей инсталляции Mailion	333
18.1 Первоначальная настройка	333
18.2 Создание резервных копий	334
18.3 Восстановление данных	335
19 Автоматическая настройка клиента «МойОфис Почта»	337
19.1 Адресные книги CardDAV	337
19.2 Календари CalDAV	337
19.3 Глобальная адресная книга LDAP	338
19.4 Настройки FCM	339
19.5 Другие ответы сервера	339
20 Информационная безопасность	341
20.1 Сбор и анализ журналов	341
20.1.1 Syslog-ng tier	341
20.1.2 Syslog-ng collector	341
20.1.3 Доставка журналов до сервера журналирования	342
20.1.4 Настройка параметров Syslog-ng	342
20.2 Антиспам	343
20.3 Подключение антивирусного модуля KSE (Kaspersky)	349
20.4 Аудит действий	350
20.4.1 Поиск событий безопасности пользователя	350
20.4.2 Поиск событий безопасности администратора	354
20.5 Перечень регистрируемых методов API	373
21 Катастрофоустойчивость	386

21.1 Принцип действия	386
21.1.1 Катастрофоустойчивое развертывание DOS	387
21.1.2 Репликация базы данных MongoDB	398
21.2 Роли и функции персонала	409
21.3 Ограничения	410
22 Возможные ситуации и способы решения	411
23 Работа с подсистемой сбора мусора	412
23.1 Создание задачи с отложенным исполнением	412
23.2 Обновление задачи по taskID	414
23.3 Удаление задачи по taskID	416
23.3.1 Получение сведений о задаче по taskID	417
23.4 Получение сведений о задаче по tenantID	418
23.5 Запуск сбора мусора вручную	419
Приложение А. Команды интерфейса командной строки	420
Приложение Б. Примеры JSON-файлов для команд утилиты ministerium	426
Б.1 Файл настроек импорта пользователей	426
Б.2 Схема записи пользователя	427
Б.3 Список глобальных адресных книг	431
Б.4 Файл настроек импорта групп	432
Б.5 Схема записи группы	433
Б.6 Файл настроек для импорта связей групп	434
Б.7 Схема записи связей групп	435
Б.8 Файл настроек импорта ресурсов	436
Б.9 Схема записи ресурса	437
Приложение В. Права администраторов ролевой модели	439
Внесенные изменения	456

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

В настоящем документе используются следующие сокращения (табл. 1).

Таблица 1 — Сокращения и расшифровки

Сокращение	Расшифровка
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
CO	Cloud Office, Частное облако
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
GAL	Global Address List, глобальная адресная книга (см. также ГАК)
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 различными реализациям служб каталогов, в том числе и Active Directory
SPN	Service Principal Name, уникальный идентификатор экземпляра сервиса. SPN используется аутентификацией Kerberos для сопоставления экземпляра сервиса с учетной записью сервиса (service logon account)
ГАК	Глобальная адресная книга (см. также GAL)
ИАК	Иерархическая адресная книга
ОС	Операционная система
ПК	Персональный компьютер

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;
- Веб-приложение Mailion для работы с электронной почтой, календарями, контактными книгами, интеллектуального поиска информации и управления задачами в веб-браузерах;
- Настольное приложение Mailion для онлайн и оффлайн работы с электронной почтой, календарями, контактными книгами, интеллектуального поиска информации и управления задачами на операционных системах Windows, Linux, macOS;
- Мобильное приложение Mailion для работы с электронной почтой, календарями, контактами и управления задачами с мобильных устройств на операционных системах Android и iOS.

Подробное описание возможностей продукта приведено в документах «Mailion. Функциональные возможности», «Mailion. Настольное приложение. Функциональные возможности», «Mailion. Мобильное приложение для операционных систем Android и iOS. Функциональные возможности».

1.2 Уровень подготовки пользователя

Пользователь Административной панели «Mailion» должен обладать следующими навыками:

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

1.3 Системные требования

Перечень системных требований к аппаратному и программному обеспечению, а также к веб-интерфейсу приведен в документе «Mailion. Руководство по установке».

1.4 Уровень доступности ПО «Mailion»

ПО «Mailion» имеет уровень доступности 99,9 % или «три девятки» при условии обновления системы четыре раза в год.

1.5 Ограничения

1.5.1 Поддерживаемые языки интерфейса

- Русский;
- Английский.

1.5.2 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 2. Парольная политика, заданная по умолчанию, может быть изменена администратором.

Таблица 2 — 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  
}
```

2 ПОДГОТОВКА К РАБОТЕ

2.1 Доступ к ПО «Mailion»

Пользователи получают доступ к ПО «Mailion» с помощью веб-браузера (см. раздел Поддерживаемые веб-браузеры).

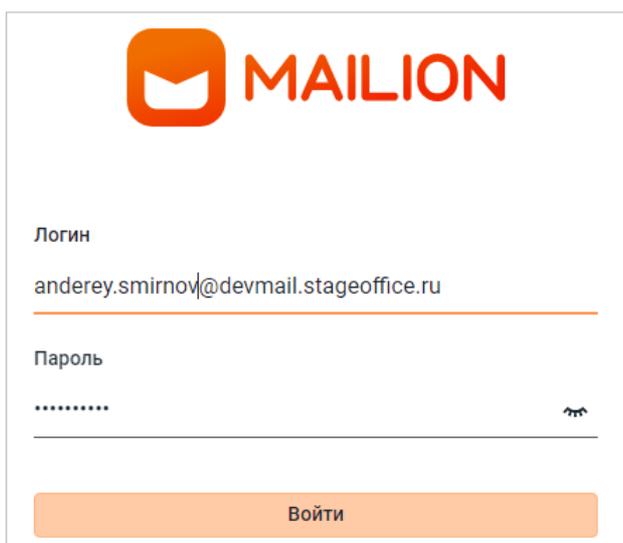
2.2 Запуск системы

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 «Mailion. Руководство пользователя».

2.3 Проверка работоспособности системы

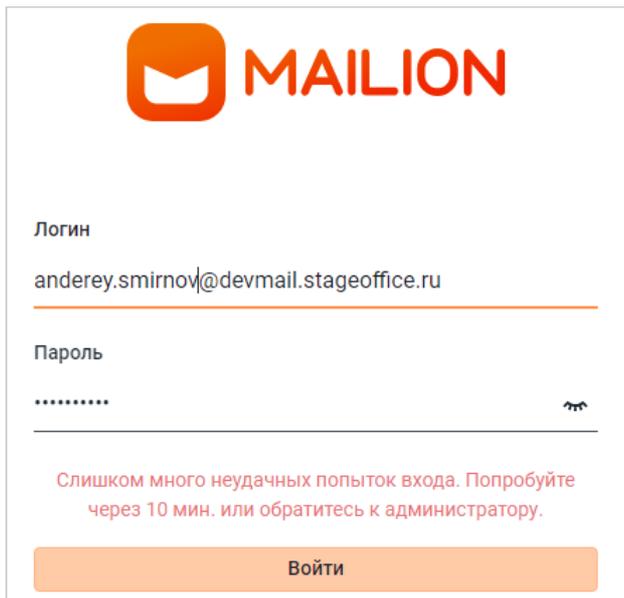
ПО «Mailion» считается работоспособным, если в результате действий пользователя, изложенных в разделах [Доступ к ПО «Mailion»](#) и [Запуск системы](#), на экране монитора отобразилась стартовая страница для входа в ПО «Mailion» без выдачи сообщений о сбое в работе (см. рис. 1).



The screenshot shows the login page for Mailion. At the top, there is the Mailion logo, which consists of an orange envelope icon and the word "MAILION" in orange capital letters. Below the logo, there are two input fields. The first is labeled "Логин" (Login) and contains the text "anderey.smirnov@devmail.stageoffice.ru". The second is labeled "Пароль" (Password) and contains a series of dots, with a small eye icon to its right for toggling visibility. At the bottom of the form, there is an orange button labeled "Войти" (Login).

Рисунок 1 – Стартовая страница для входа в ПО «Mailion»

В случае нескольких неудачных попыток входа возможность ввода логина и пароля будет заблокирована на 10 минут (см. рис. 2).



MAILION

Логин
anderey.smirnov@devmail.stageoffice.ru

Пароль
.....

Слишком много неудачных попыток входа. Попробуйте
через 10 мин. или обратитесь к администратору.

Войти

Рисунок 2 – Неудачная попытка входа

3 РОЛЕВАЯ МОДЕЛЬ АДМИНИСТРИРОВАНИЯ

В прежних версиях Mailion ролевая модель администрирования (РМА) включала в себя две роли: **администратор инсталляции** и **администратор тенанта**. Эти роли не были формализованы, и права обеим ролям назначались по мере необходимости.

В Mailion 2.0 для реализации требований заказчиков крупных систем, нуждающихся в более гибкой структуре администрирования с гранулированным набором прав, ролевая модель администрирования была расширена и теперь включает в себя роли, описанные ниже в табл. 3.

Таблица 3 — Роли администраторов в системе

Роль	Описание
Суперадминистратор	<ul style="list-style-type: none"> – Наделен всеми возможными ролями и контекстами – Отвечает за контроль и управление всеми аспектами администрирования в системе – Имеет полный доступ ко всем функциям и данным, а также право на управление другими администраторами и пользователями
Администратор инсталляции	<ul style="list-style-type: none"> – Отвечает за инсталляцию и создание остальных администраторов – Создает/редактирует/удаляет тенанты всей инсталляции – Создает/наделяет правами администраторов тенантов – Существует в единственном числе
Администратор тенанта	<ul style="list-style-type: none"> – Выполняет все действия, касающиеся пользователей, папок, групп и организационной структуры в пределах тенанта – Отвечает за полный жизненный цикл учетной записи пользователя – Выполняет все доступные функции администратора, кроме установки – Назначается администратором инсталляции
Администратор информационной безопасности	<ul style="list-style-type: none"> – Выполняет действия по управлению политикой безопасности, мониторингу безопасности почтовых ящиков, управлению списками блокирования и разрешения отправителей, доменов и IP-адресов, по настройке системы обнаружения и блокировки вредоносных вложений, управлению антиспам-фильтрами
Администратор аудита инсталляции	<ul style="list-style-type: none"> – Имеет доступ ко всем функциям администратора в режиме чтения, а также к системе журналов аудита в режиме редактирования

Роль	Описание
Администратор аудита тенанта	– Наделен правами, аналогичными правам администратора аудита инсталляции, но с областью действия в пределах конкретного тенанта
Настраиваемый администратор	– Роль администратора с гибким набором прав, которую может создавать только администратор инсталляции

3.1 Права администраторов ролевой модели

Права администраторов ролевой модели описаны в таблице, представленной в [Приложении В](#).

3.2 Создание администраторов

3.2.1 Уровень инсталляции

Суперадминистратор, администраторы инсталляции, информационной безопасности и аудита создаются автоматически при развертывании инсталляции утилитой **dorofej**.

Администраторов информационной безопасности и аудита также можно создать командами **ministerium**: [create admin information security](#) и [create admin audit](#).

Настраиваемый администратор уровня инсталляции создается после развертывания инсталляции следующим способом:

1. Создать пользователя вне тенанта командой [create admin](#).
2. Назначить права командой [grant rights](#).

3.2.2 Уровень тенанта

Процедура создания администратора тенанта описана в разделе [Создание администратора тенанта](#).

Администратор аудита уровня тенанта создается командой [create tenant admin audit](#).

Настраиваемый администратор уровня тенанта создается в два шага:

1. Создать пользователя тенанта командой [create user](#).
2. Назначить права созданному пользователю командой [grant rights](#).

3.3 Команды управления ролевой моделью

3.3.1 Команды управления ролями

Эти команды предусмотрены на случай, если существующие роли по какой-либо причине не устраивают и требуется добавить новые (например, для создания настраиваемого администратора).

3.3.1.1 Создание роли

Для создания роли необходимо выполнить следующий запрос:

```
nct_ministerium create_role \
--config ministerium.json \
--role_data_path <...>
```

Описание параметров запроса приведено в таблице 4.

Таблица 4 — Параметры запроса на создание роли

Параметр	Тип	Обязательный	Описание
config	Str	+	Файл конфигурации ministerium
role_data_path	Str	+	Путь к файлу с данными роли

Пример файла с данными роли:

```
{
  "name": "TestRoleName1",
  "role_ids": ["80de2b0a-e34f-5fae-84cf-b893bd6e9345", "1b0d6b0f-1008-5f65-
b5ad-a6161cf91c41"], // идентификаторы ролей, которые будут включены в эту роль
  "permissions": [
    {
      "effect": "ALLOW",
      "action": "OBJECT_ACTION_READ",
      "objects": [
        {
          "type": "OBJECT_TYPE_ENTITY",
          "id": "", // идентификатор объекта
          "attributes": ["attr1", "attr2"]
        }
      ]
    }
  ],
  "tenant_id": "01068ade-1cce-4125-ab6b-91d977ecf85b" // арендатор роли (может
быть пустым)
}
```

3.3.1.2 Обновление роли

Для обновления роли необходимо выполнить следующий запрос:

```
nct_ministerium update_role \
--config ministerium.json \
--role_data_path <...> \
--role_id <...>
```

Описание параметров запроса приведено в таблице 5.

Таблица 5 — Параметры запроса на обновление роли

Параметр	Тип	Обязательный	Описание
config	Str	+	Файл конфигурации ministerium
role_data_path	Str	+	Путь к файлу с данными роли
role_id	Str	+	Идентификатор роли

Пример файла с данными роли:

```
{
  "name": "NewRoleName",
  "role_ids": ["80de2b0a-e34f-5fae-84cf-b893bd6e9345", "1b0d6b0f-1008-5f65-
b5ad-a6161cf91c41"],
  "permissions": [
    {
      "effect": "ALLOW",
      "action": "OBJECT_ACTION_READ",
      "objects": [
        {
          "type": "OBJECT_TYPE_ENTITY",
          "id": "", // идентификатор объекта
          "attributes": ["attr1", "attr2"]
        }
      ]
    }
  ],
}
```

(например entity_id), пустая строка означает любой идентификатор

Пример файла с удалением разрешений и связей с другими ролями:

```
{
  "role_ids": [], // пустой список означает, что связи будут удалены
  "permissions": [] // пустой список означает, что разрешения будут удалены
}
```

3.3.1.3 Удаление роли

Для удаления роли необходимо выполнить следующий запрос:

```
nct_ministerium delete_role \
--config ministerium.json \
--role_ids <...>
```

Описание параметров запроса приведено в таблице 6.

Таблица 6 — Параметры запроса на удаление роли

Параметр	Тип	Обязательный	Описание
config	Str	+	Файл конфигурации ministerium
role_ids	Str	+	Список идентификаторов ролей

3.3.1.4 Получение ролей

Для получения роли администратора необходимо выполнить следующий запрос:

```
nct_ministerium get_roles \  
--config ministerium.json \  
--role_ids <...>
```

Описание параметров запроса приведено в таблице 7.

Таблица 7 — Параметры запроса на получение ролей

Параметр	Тип	Обязательный	Описание
config	Str	+	Файл конфигурации ministerium
role_ids	Str	+	Список идентификаторов ролей

Пример ответа:

```
{
  "Response": {
    "changed": true,
    "failed": false,
    "msg": "ok"
  },
  "roles": [
    {
      "id": "d9879901-4ba4-5452-9a34-0877eb671a8b",
      "name": "UserRegularTenant",
      "permissions": [
        {
          "effect": 1,
          "action": 11,
          "objects": [
            {
              "type": 37
            }
          ]
        }
      ]
    },
    {
      "action": 1,
      "objects": [
        {
          "type": 14,
          "attributes": [
            "gender"
          ]
        },
        {
          "type": 6,
          "attributes": [
            "profile.user.gender"
          ]
        },
        {
          "type": 1,
          "attributes": [
            "squadus_params"
          ]
        }
      ]
    }
  ],
  {
    "effect": 1,
    "action": 1,
    "objects": [
      {
        "type": 2,
        "attributes": [
          "id",
          "hostname",
          "tenant_id"
        ]
      }
    ]
  }
]
}
```

3.3.1.5 Получение всех ролей

Для получения всех ролей необходимо выполнить следующий запрос:

```
nct_ministerium get_all_roles \  
--config ministerium.json
```

Описание параметров запроса приведено в таблице 8.

Таблица 8 — Параметры запроса на получение ролей

Параметр	Тип	Обязательный	Описание
config	Str	+	Файл конфигурации ministerium

3.3.2 Команды управления правами

3.3.2.1 Назначение прав

Для назначения прав необходимо выполнить следующий запрос:

```
nct_ministerium grant_rights \  
--config ministerium.json \  
--rights_data_path <...>
```

Описание параметров запроса приведено в таблице 9.

Таблица 9 — Параметры запроса на назначение прав

Параметр	Тип	Обязательный	Описание
config	Str	+	Файл конфигурации ministerium
rights_data_path	Str	+	Путь к файлу с данными прав

Пример файла с данными прав:

```
{
  "rights": [
    {
      "context": {
        "type": "TENANT",
        "id": "01068ade-1cce-4125-ab6b-91d977ecf85b", // идентификатор
        контекста (например, тенанта)
        "effect": "ALLOW"
      },
      "subject_id": "1d8a549d-94d9-4f6b-bcd0-27d93a57f85b", // идентификатор
      субъекта, которому назначаются права (например, entity_id сущности)
      "role_ids": ["b7c90fad-2162-5876-8ca4-38563affb35f"], // идентификаторы
      ролей
      "tenant_id": "01068ade-1cce-4125-ab6b-91d977ecf85b" // арендатор назначения
      права (может быть пустым)
    }
  ]
}
```

3.3.2 Отзыв прав

Для отзыва прав необходимо выполнить следующий запрос:

```
nct_ministerium revoke_rights \
--config ministerium.json \
--role_ids <...>
```

Описание параметров запроса приведено в таблице 10.

Таблица 10 — Параметры запроса на назначение прав

Параметр	Тип	Обязательный	Описание
config	Str	+	Файл конфигурации ministerium
role_ids	Str	+	Список идентификаторов прав

3.3.3 Команды создания администраторов

3.3.3.1 Создание администратора аудита инсталляции

Для создания администратора аудита инсталляции необходимо выполнить следующий запрос:

```
nct_ministerium create_admin_audit \
--config ministerium.json \
--login <...> \
--password <...> \
--region_id <...>
```

Описание параметров запроса приведено в таблице 11.

Таблица 11 — Параметры запроса на создание администратора аудита инсталляции

Параметр	Тип	Обязательный	Описание
config	Str	+	Файл конфигурации ministerium
login	Str	+	Логин нового пользователя
password	Str	+	Пароль нового пользователя
region_id	Str	+	Идентификатор региона

3.3.3.2 Создание администратора аудита тенанта

Для создания администратора аудита тенанта необходимо выполнить следующий запрос:

```
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 \
--login <...> \
--password '<...>'
```

Описание параметров запроса приведено в таблице 12.

Таблица 12 — Параметры запроса на создание администратора аудита тенанта

Параметр	Тип	Обязательный	Описание
config	Str	+	Файл конфигурации ministerium
admin.login	Str	+	Логин администратора тенанта
admin.password	Str	+	Пароль администратора тенанта
tenant_id	Str	+	Идентификатор тенанта
region_id	Str	+	Идентификатор региона
login	Str	+	Логин создаваемого администратора тенанта
password	Str	+	Пароль создаваемого администратора тенанта

3.3.3.3 Создание администратора информационной безопасности

Для создания администратора информационной безопасности необходимо выполнить

следующий запрос:

```
nct_ministerium create_admin_information_security \
--config ministerium.json \
--login <...> \
--password <...> \
--region_id <...>
```

Описание параметров запроса приведено в таблице 13.

Таблица 13 — Параметры запроса на создание администратора информационной безопасности

Параметр	Тип	Обязательный	Описание
config	Str	+	Файл конфигурации ministerium
login	Str	+	Логин нового пользователя
password	Str	+	Пароль нового пользователя
region_id	Str	+	Идентификатор региона

3.3.3.4 Создание настраиваемого администратора

Для создания администратора с настраиваемыми правами необходимо выполнить следующий запрос:

```
nct_ministerium create_admin \
--config ministerium.json \
--login <...> \
--password <...> \
--region_id <...>
```

Описание параметров запроса приведено в таблице 14.

Таблица 14 — Параметры запроса на создание настраиваемого администратора

Параметр	Тип	Обязательный	Описание
config	Str	+	Файл конфигурации ministerium
login	Str	+	Логин нового пользователя
password	Str	+	Пароль нового пользователя
region_id	Str	+	Идентификатор региона

3.3.4 Команды управления администраторами тенанта

Для управления администраторами тенанта используются следующие команды:

- **set_tenant_administrator** — добавление роли администратора тенанта пользователю;
- **unset_tenant_administrator** — отзыв роли администратора тенанта у пользователя;
- **list_tenant_administrator** — получение списка администраторов тенанта.

Параметры для всех этих команд одинаковы, их описание приведено в таблице 15.

Таблица 15 — Общие параметры запросов управления администраторами тенанта

Параметр	Тип	Обязательный	Описание
admin.login	string	+	Логин администратора тенанта
admin.password	string	+	Пароль администратора тенанта
cox.balancer_endpoint	string	+	Конечная точка балансировщика нагрузки сервиса
cox.compression	string	-	Метод сжатия данных (варианты: none , gzip), по умолчанию — none
cox.endpoint	string	+	Конечная точка сервиса
cox.load_balanced	boolean	-	Использовать соединение с балансировщиком
cox.request_timeout	duration	-	Время ожидания ответа на запрос 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 команды 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 команды отзыва 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 команды 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.

4 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. рис. 3).

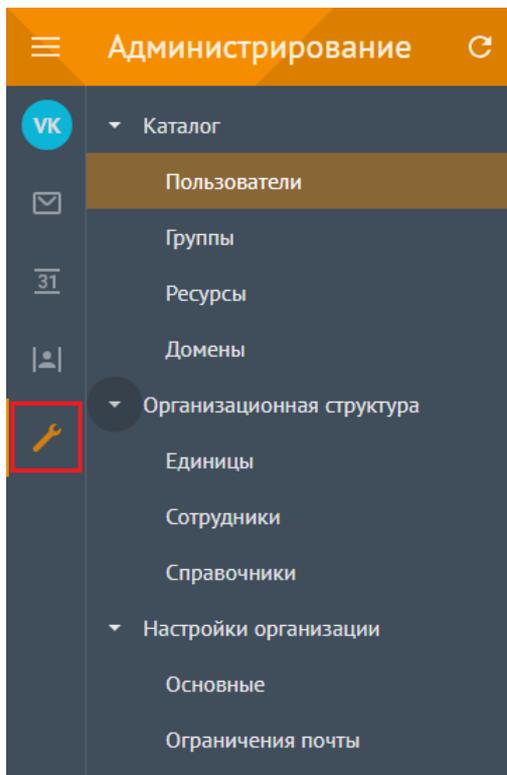


Рисунок 3 – Переход к **Панели администрирования**

4.1 Интерфейс приложения **Панель администрирования**

Интерфейс приложения **Панель администрирования** включает следующие элементы (см. рис. 4):

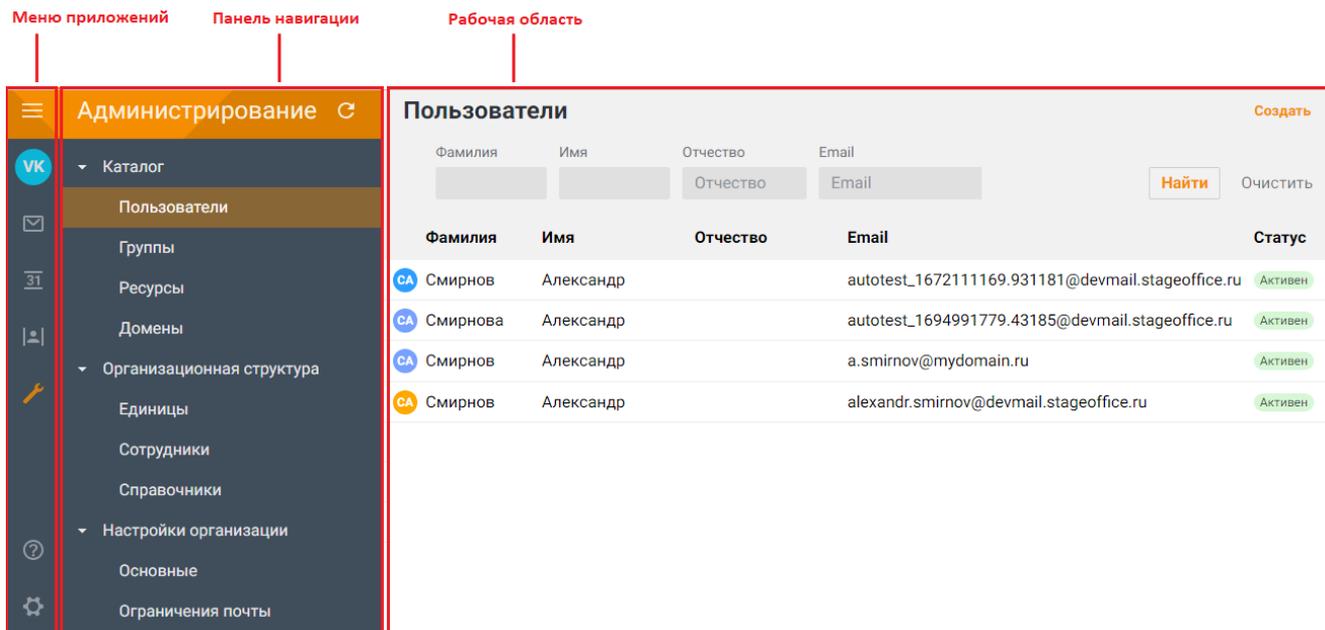


Рисунок 4 – Интерфейс приложения **Панель администрирования**

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 (рис. 5).

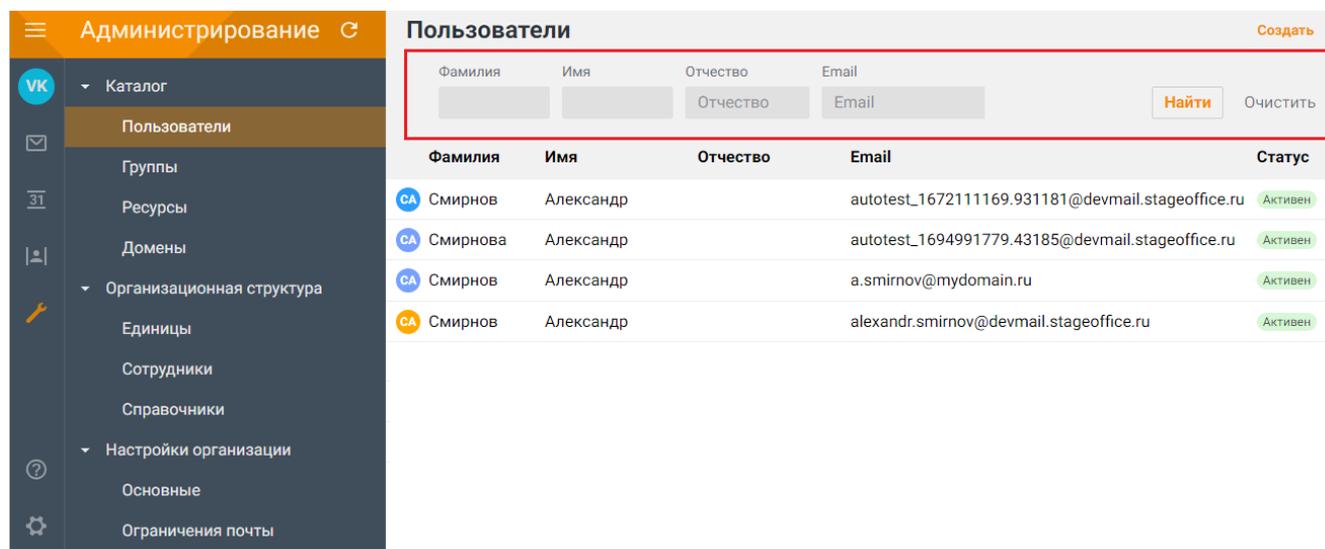


Рисунок 5 – Просмотр полей для поиска

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.

4.2 Управление пользователями

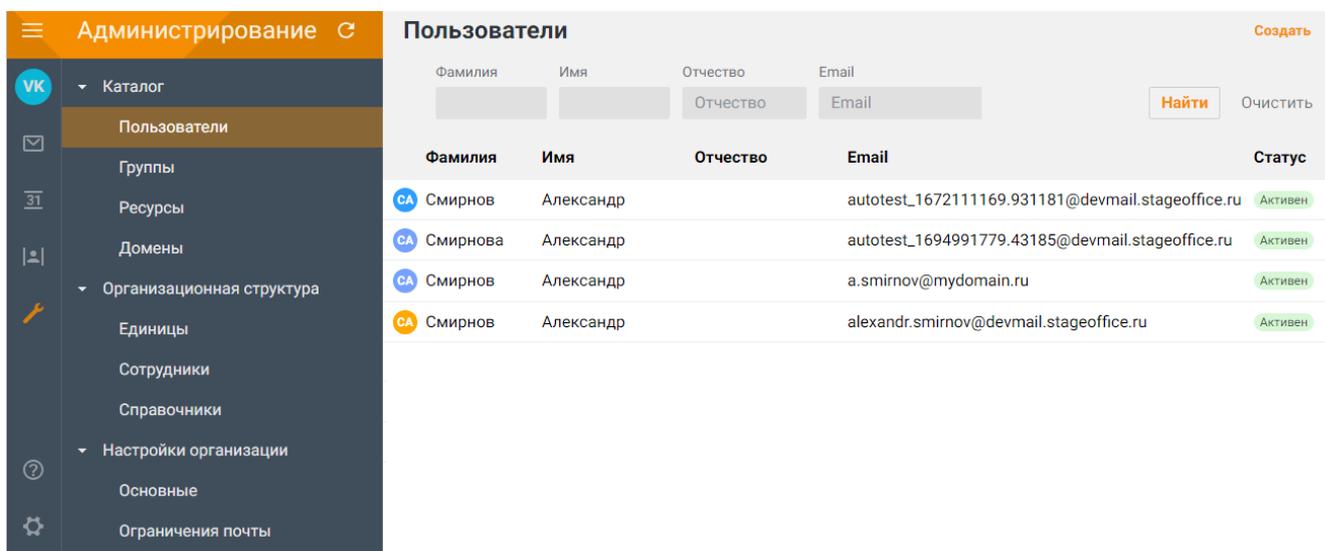
4.2.1 Просмотр списка пользователей

Для просмотра списка пользователей необходимо авторизоваться в ПО «Mailion» и перейти в раздел **Пользователи**. На экране отобразится таблица со списком пользователей (см. рис. 6).

Таблица пользователей содержит следующие столбцы:

- Фамилия;
- Имя;
- Отчество;

- E-mail;
- Статус;
- Должность;
- Отдел;
- Город;
- Логин.



Администрирование ↻

Пользователи Создать

Фамилия: Имя: Отчество: Email:

Фамилия	Имя	Отчество	Email	Статус
Смирнов	Александр		autotest_1672111169.931181@devmail.stageoffice.ru	Активен
Смирнова	Александр		autotest_1694991779.43185@devmail.stageoffice.ru	Активен
Смирнов	Александр		a.smirnov@mydomain.ru	Активен
Смирнов	Александр		alexandr.smirnov@devmail.stageoffice.ru	Активен

Рисунок 6 – Просмотр списка пользователей

По нажатию на строку откроется список групп пользователя.

4.2.2 Просмотр записи о пользователе

Чтобы просмотреть подробную запись о пользователе, необходимо нажать на соответствующую строку и перейти на вкладку **Данные** (рис. 7).

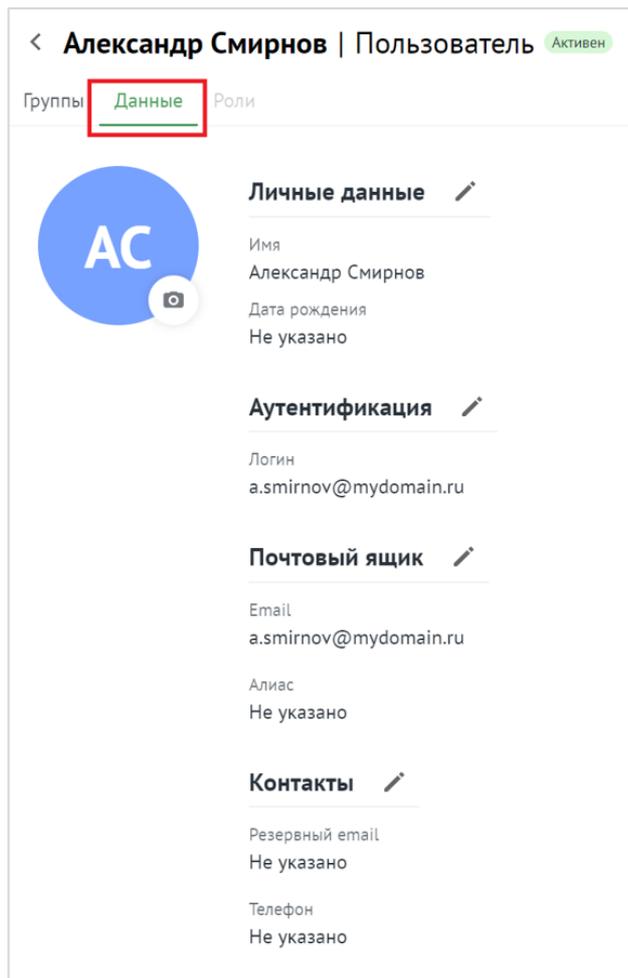


Рисунок 7 – Информация о пользователе на вкладке **Данные**

На этой же вкладке доступно [редактирование](#) записи о пользователе.

4.2.3 Создание пользователя

Для создания нового пользователя в разделе **Пользователи** необходимо нажать на кнопку **Создать** и в открывшейся форме выполнить следующие действия (см. Рисунок 8):

Новый пользователь



Личные данные

Имя (обязательно) Отчество

Фамилия Дата рождения Пол

Аутентификация

Логин (обязательно) Домен

Пароль (обязательно) Сгенерировать автоматически

Почтовый ящик

Основной email (обязательно) Домен

Контакты

Резервный email

Телефон

Адреса

Название адреса

Страна Город

Адрес Индекс

Этаж

Кабинет

Место

Организационная структура

Организация

Подразделение

Проектная группа

Должность

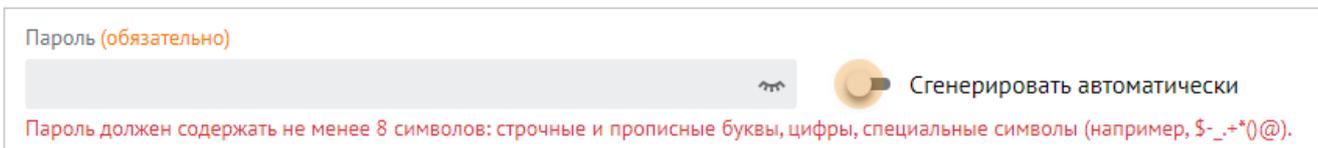
Рисунок 8 – Создание нового пользователя

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. Рисунок 9):



Пароль (обязательно)

Пароль должен содержать не менее 8 символов: строчные и прописные буквы, цифры, специальные символы (например, \$-._+*()@).

Рисунок 9 – Поле ввода пароля с подсказкой



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**.



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).



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:



Для заполнения полей данного блока необходимо предварительно создать объекты организационной структуры (см. раздел [Управление единицами организационной структуры](#)).

- Организация;
- Подразделение;
- Проектная группа;
- Должность.

7. Нажать на кнопку **Сохранить** для создания пользователя с указанными данными или на кнопку **Отмена** для отмены создания пользователя.



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 сохраняются 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 [Расширенное администрирование](#)).

4.2.4 Поиск пользователя

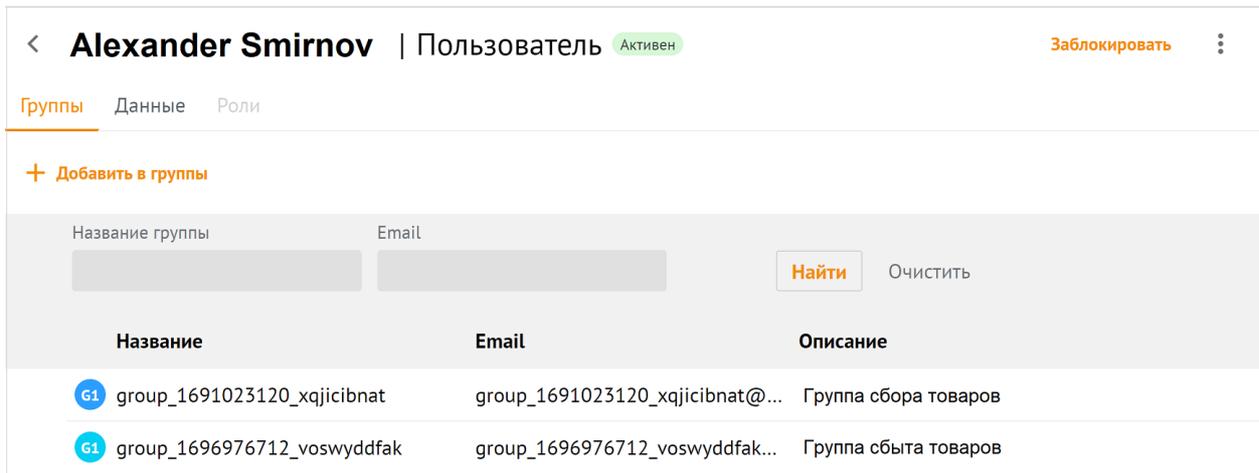
Для поиска пользователя необходимо выполнить следующие действия:

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 10).

Пользователи						Создать
Фамилия	Имя	Отчество	Email	Статус	Должность	
<input type="text" value="Фамилия"/>	<input type="text" value="Имя"/>	<input type="text" value="Отчество"/>	<input type="text" value="Email"/>	<input type="button" value="Найти"/>	<input type="button" value="Очистить"/>	
	Smirnov	Alexander	alexander.smirnov@mydomain.ru	Активен		
	Smirnova	Elena	elena.smirnova@mydomain.ru	Активен		

Рисунок 10 – Поиск пользователя

3. По нажатию на строку откроется список групп рассылок, в которых находится данный пользователь (см. Рисунок 11).



< **Alexander Smirnov** | Пользователь Активен Заблокировать

Группы Данные Роли

+ Добавить в группы

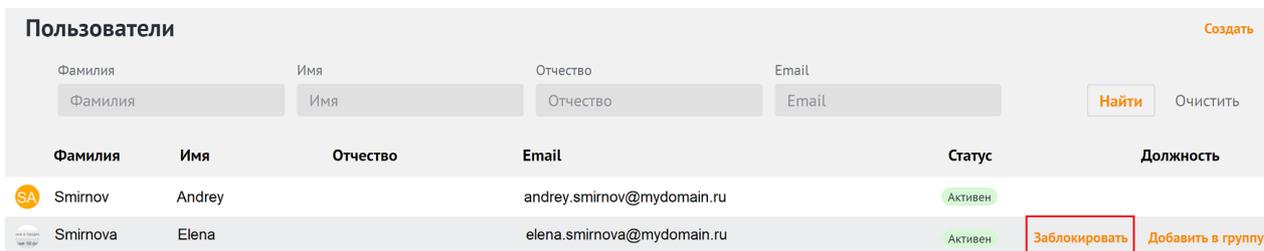
Название группы	Email	
<input type="text"/>	<input type="text"/>	Найти Очистить
Название	Email	Описание
G1 group_1691023120_xqjicibnat	group_1691023120_xqjicibnat@...	Группа сбора товаров
G1 group_1696976712_voswyddfak	group_1696976712_voswyddfak...	Группа сбыта товаров

Рисунок 11 – Список групп рассылок пользователя

4.2.5 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 12).



Пользователи Создать

Фамилия	Имя	Отчество	Email		
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	Найти Очистить	
Фамилия	Имя	Отчество	Email	Статус	Должность
SA Smirnov	Andrey		andrey.smirnov@mydomain.ru	Активен	
SA Smirnova	Elena		elena.smirnova@mydomain.ru	Активен	Заблокировать Добавить в группу

Рисунок 12 – Блокировка пользователя из списка пользователей

2. В списке пользователей нажать на строку пользователя, в открывшейся панели нажать кнопку **Заблокировать** (см. Рисунок 13).

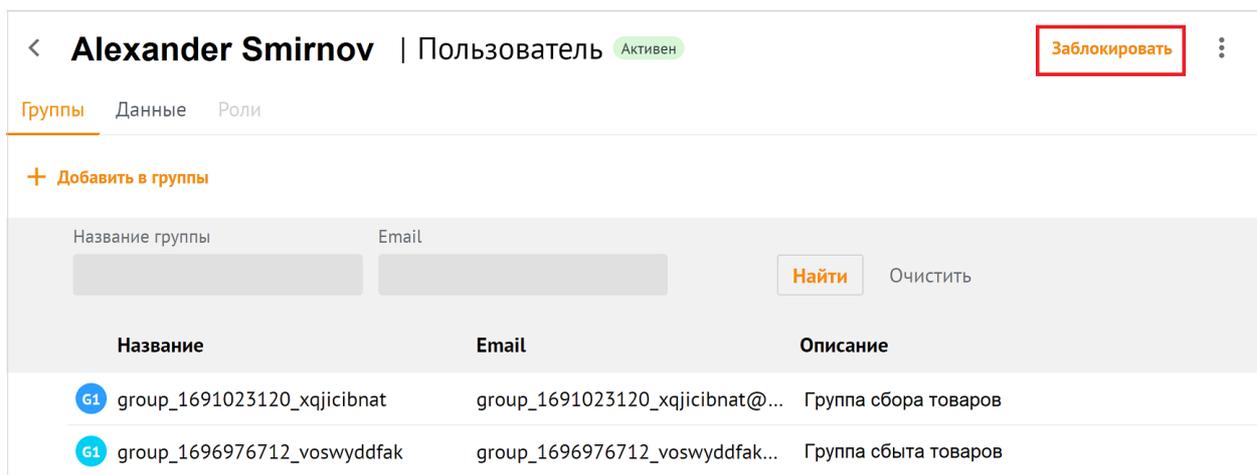


Рисунок 13 – Блокировка пользователя из панели пользователя

После нажатия на кнопку **Заблокировать** на экране возникнет панель для ввода комментария (см. Рисунок 14). После нажатия на кнопку **Заблокировать** пользователь будет заблокирован.

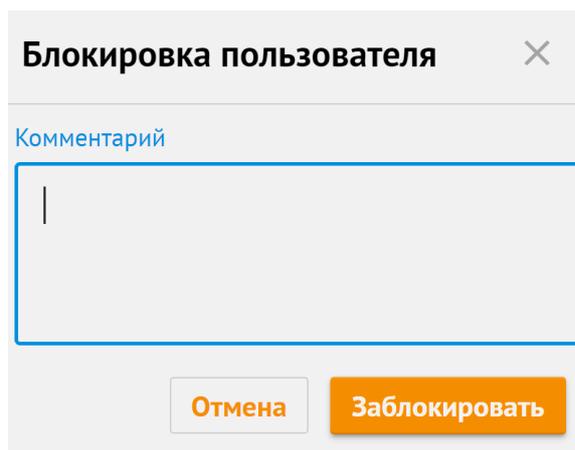


Рисунок 14 – Комментарий к блокировке пользователя

4.2.6 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 15).

Пользователи						Создать
Фамилия	Имя	Отчество	Email			
Фамилия	Имя	Отчество	Email		Найти	Очистить
Фамилия	Имя	Отчество	Email	Статус	Должность	
SA Smirnov	Alexander		alexander.smirnov@devmail.ru	Заблокирован		
SE Smirnova	Elena		elena.smirnova@devmail.ru	Заблокирован	Разблокировать	Добавить в группу

Рисунок 15 – Разблокировка пользователя из списка пользователей

- В списке пользователей нажать на строку заблокированного пользователя, в открывшейся панели нажать кнопку **Разблокировать** (см. Рисунок 16).

< Alexander Smirnov Пользователь			Заблокирован	Разблокировать	⋮
Группы	Данные	Роли			
+ Добавить в группы					
Название группы	Email				
			Найти	Очистить	
Название	Email	Описание			
G1 group_1691023120_xqjicibnat	group_1691023120_xqjicibnat@...	Группа сбора товаров			
G1 group_1696976712_voswyddfak	group_1696976712_voswyddfak...	Группа сбыта товаров			

Рисунок 16 – Разблокировка пользователя из панели пользователя

После нажатия на кнопку **Разблокировать** на экране возникнет панель для подтверждения (см. Рисунок 17). После нажатия на кнопку **Разблокировать** пользователь будет активирован.

Активация пользователя ✕

Пользователь будет разблокирован

Отмена
Разблокировать

Рисунок 17 – Подтверждение разблокировки пользователя

4.2.7 Удаление пользователя

Для удаления пользователя необходимо выполнить следующие действия:

1. Выбрать пользователя из общего списка и нажать на значок \vdots .
2. Нажать на **Удалить** (см. Рисунок 18).

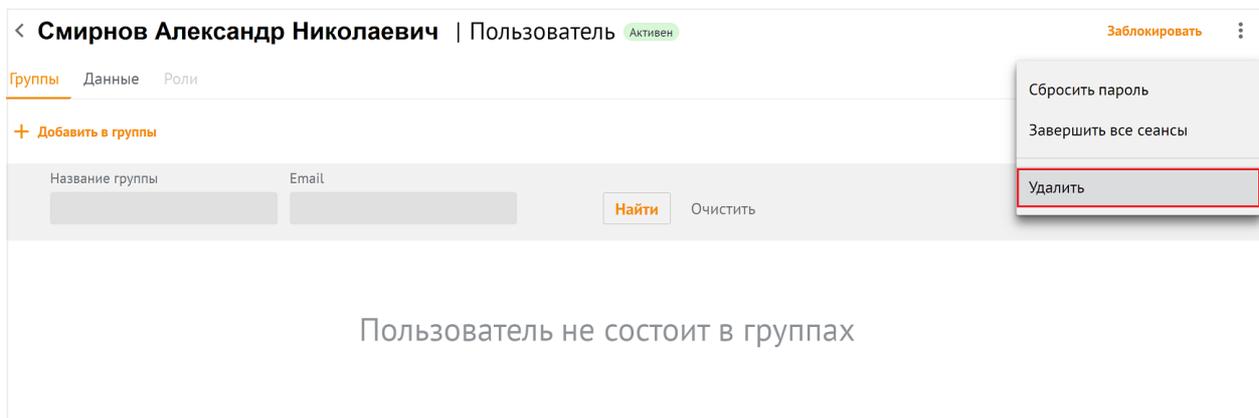


Рисунок 18 – Удаление пользователя

3. В окне подтверждения удаления необходимо нажать на кнопку **Удалить** (Рисунок 19).

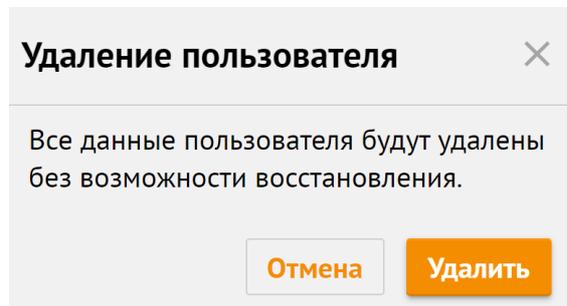


Рисунок 19 – Подтверждение удаления пользователя

4.2.8 Сброс пароля пользователя

Для сброса пароля пользователя необходимо выбрать пользователя из общего списка и нажать на **Сбросить пароль** (см. Рисунок 20).

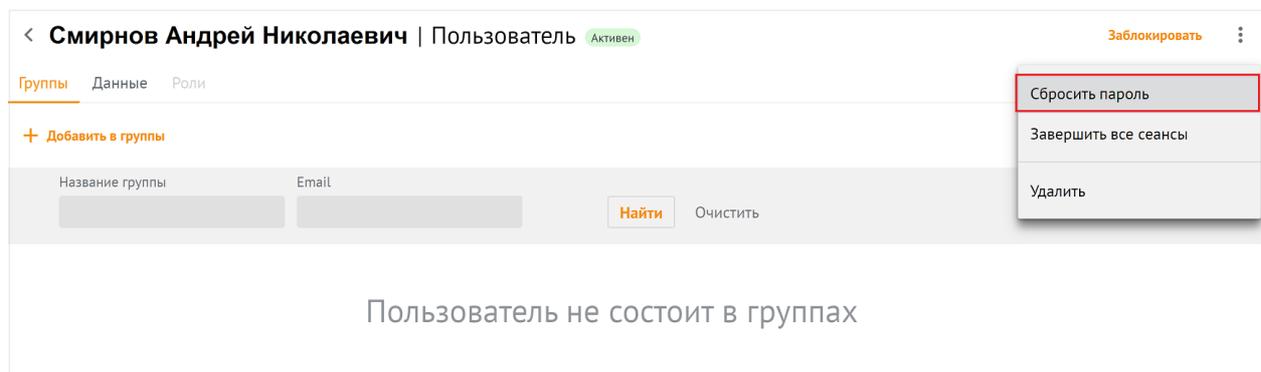


Рисунок 20 – Сброс пароля пользователя

После нажатия на кнопку **Сбросить пароль**, администратор должен ввести новый пароль пользователя и подтвердить его, либо использовать пароль, предложенный автоматическим генератором (Рисунок 21).

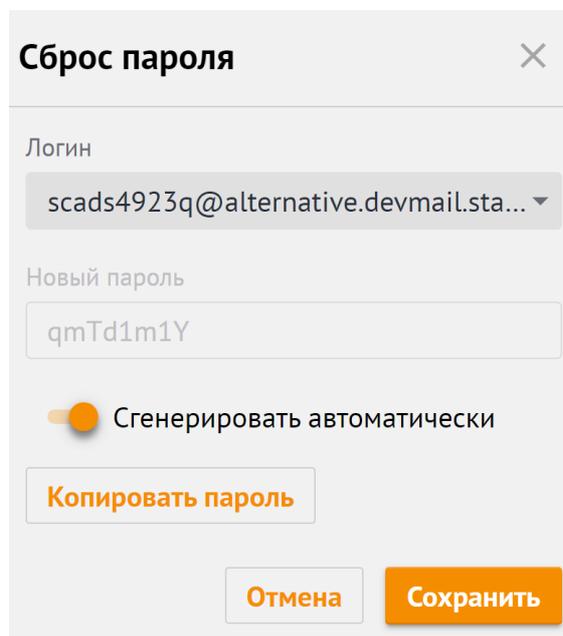


Рисунок 21 – Сгенерировать пароль автоматически

4.2.9 Завершение всех сеансов пользователя

Для завершения всех сеансов пользователя необходимо выбрать пользователя из общего списка и нажать на **Завершить все сеансы** (см. Рисунок 22).

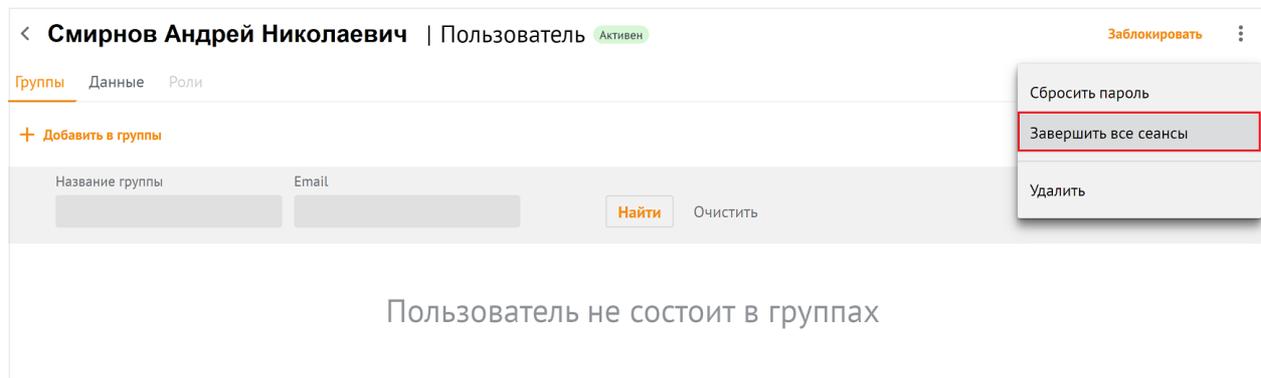


Рисунок 22 – Сброс пароля пользователя

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

4.2.10 Добавление пользователей в группы рассылки

4.2.10.1 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 23).

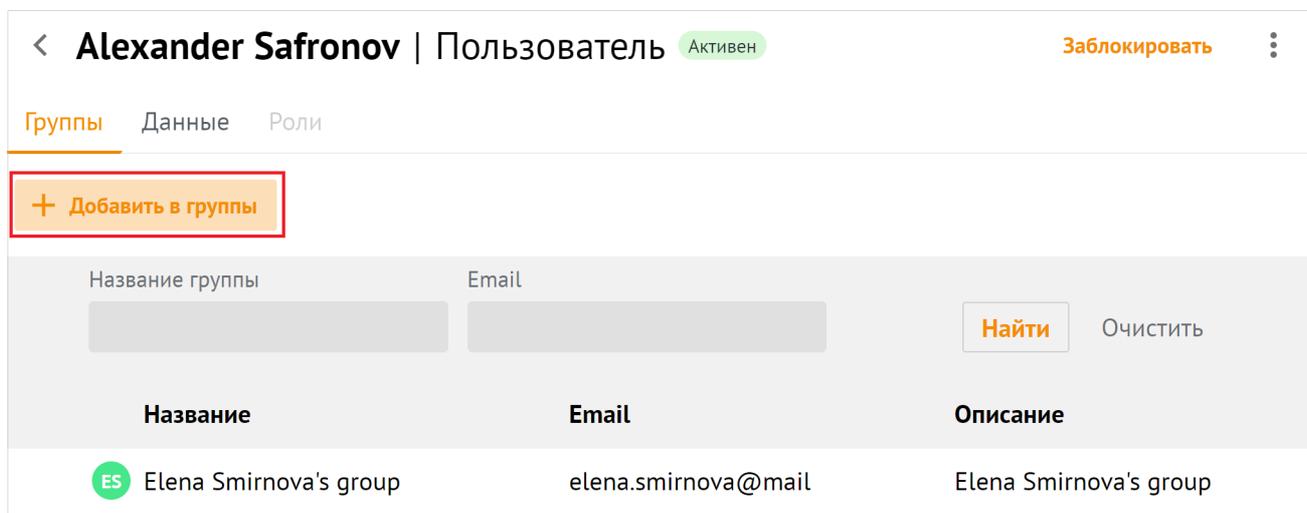
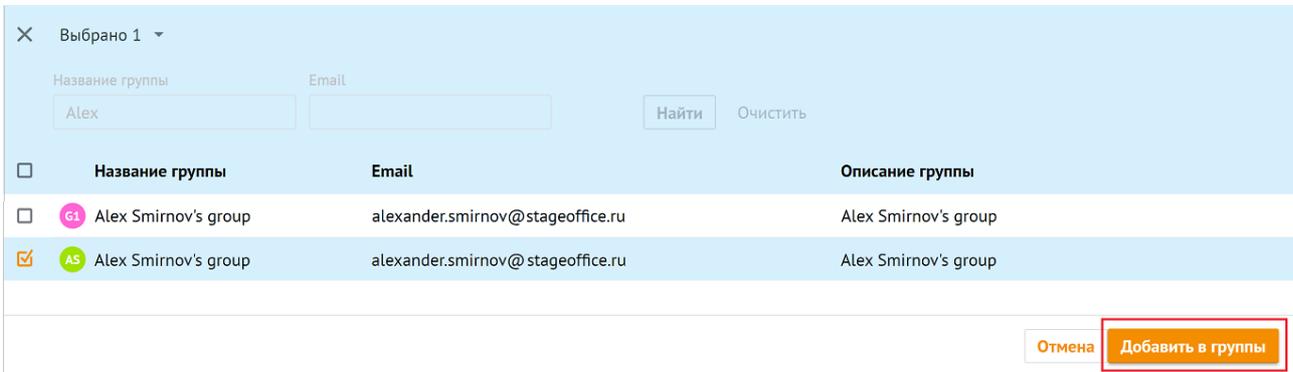


Рисунок 23 – Добавление пользователя в группу рассылки из списка пользователей

- В появившемся списке групп выделить флагами необходимые группы, нажать **Добавить в группы** (см. Рисунок 24).



Выбрано 1

Название группы: Email:

<input type="checkbox"/>	Название группы	Email	Описание группы
<input type="checkbox"/>	Alex Smirnov's group	alexander.smirnov@stageoffice.ru	Alex Smirnov's group
<input checked="" type="checkbox"/>	Alex Smirnov's group	alexander.smirnov@stageoffice.ru	Alex Smirnov's group

Рисунок 24 – Выбор групп рассылки для добавления пользователя



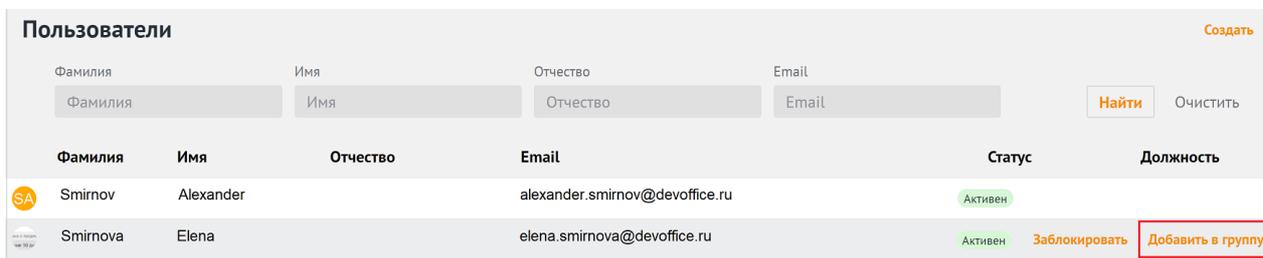
Для добавления пользователя в несколько групп рассылки нужно установить галочку напротив нескольких групп рассылки.

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

4.2.10.2 Добавление пользователя из списка пользователей

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

- В списке пользователей навести курсор на строку пользователя, выбрать **Добавить в группу** (см. Рисунок 25).



Пользователи Создать

Фамилия: Имя: Отчество: Email:

	Фамилия	Имя	Отчество	Email	Статус	Должность
	Smirnov	Alexander		alexander.smirnov@devoffice.ru	Активен	
	Smirnova	Elena		elena.smirnova@devoffice.ru	Активен	<input type="button" value="Заблокировать"/> <input checked="" type="button" value="Добавить в группу"/>

Рисунок 25 – Добавление пользователя в группу рассылки из списка пользователей

- В появившемся списке групп выделить флагами необходимые группы, нажать **Добавить в группы** (см. Рисунок 26).

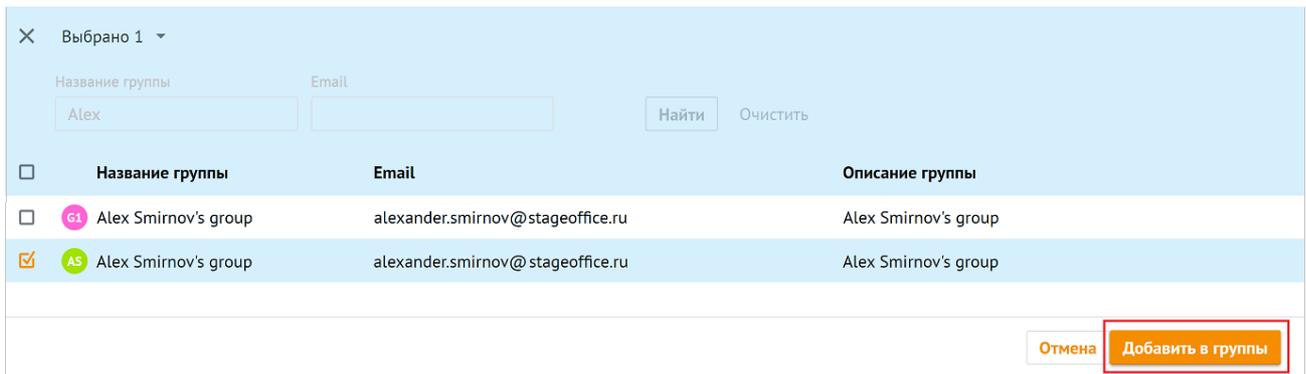


Рисунок 26 – Выбор групп рассылки для добавления пользователя



Для добавления пользователя в несколько групп рассылки нужно установить галочку напротив нескольких групп рассылки.

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

4.2.10.3 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 интересующую группу рассылки, нажать на **Добавить участников** (см. Рисунок 27).

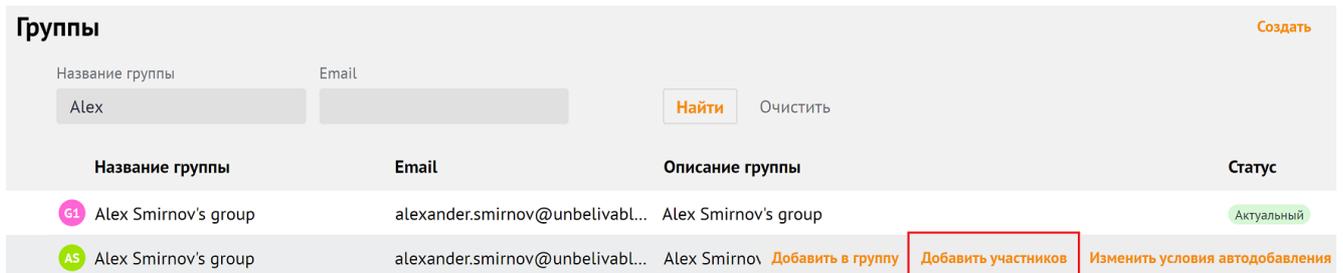


Рисунок 27 – Выбор участника для добавления в группы рассылки

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**.

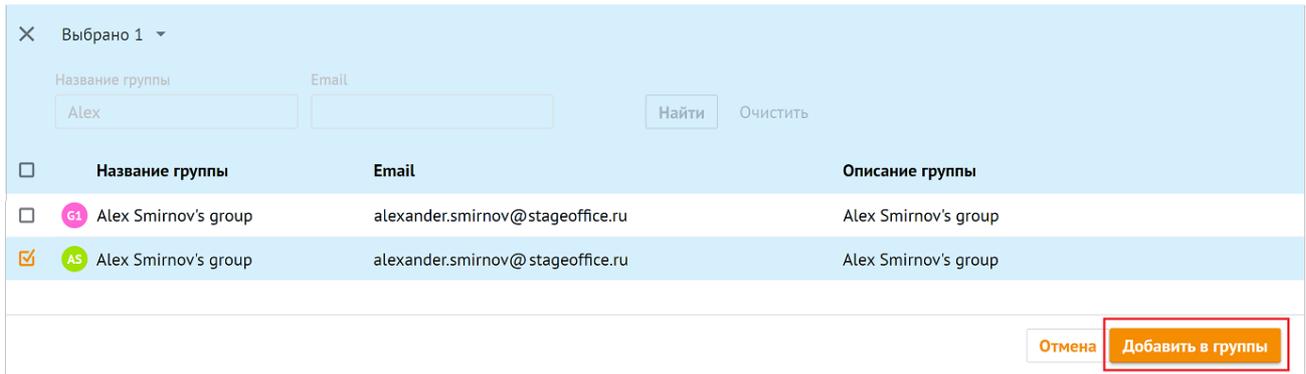


Рисунок 28 – Выбор групп рассылки для добавления пользователя



Для добавления пользователя в несколько групп рассылки нужно установить галочку напротив нескольких групп рассылки.

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

4.2.11 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 29).

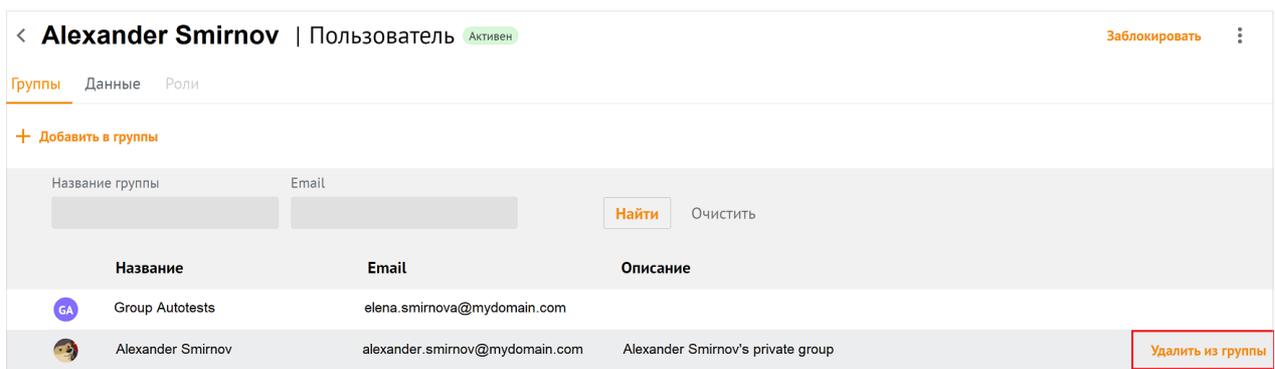


Рисунок 29 – Удаление участника из группы рассылки

2. Открыть группу рассылки, выбрать соответствующего пользователя в группе и нажать на кнопку **Удалить из группы** (см. Рисунок 30).

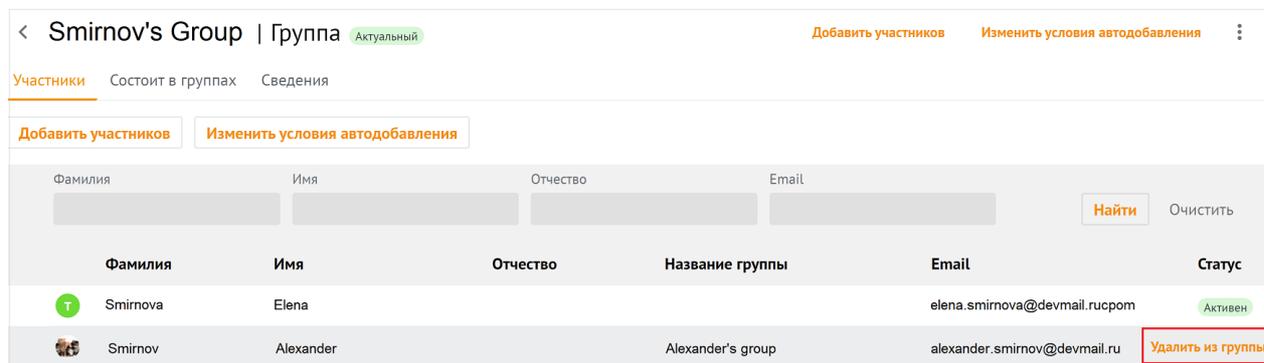


Рисунок 30 – Удаление участника из группы рассылки

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

4.2.12 Редактирование данных пользователя

Для редактирования данных пользователя необходимо в разделе **Пользователи** перейти на вкладку **Данные** (Рисунок 31).

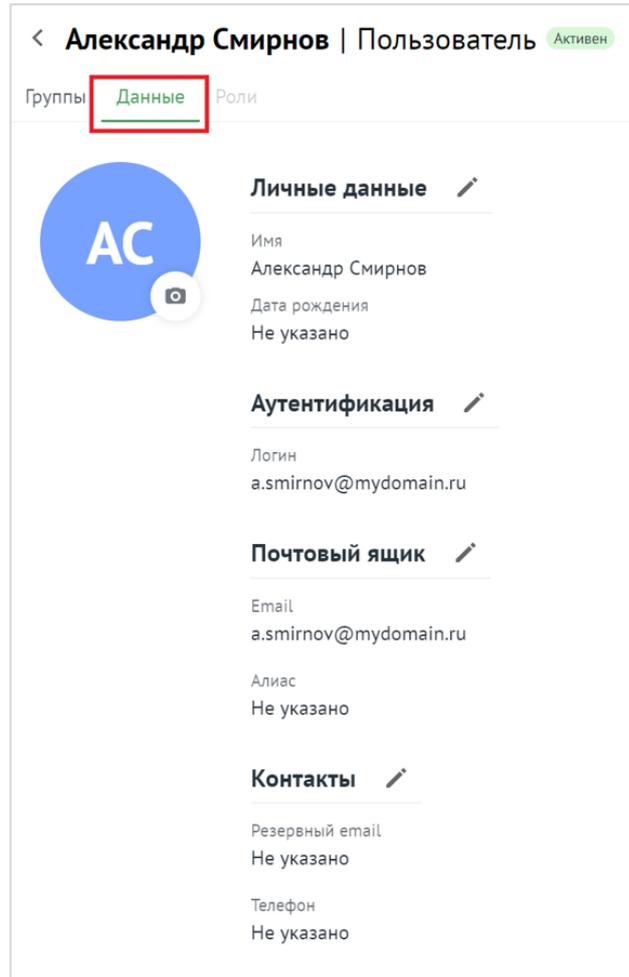
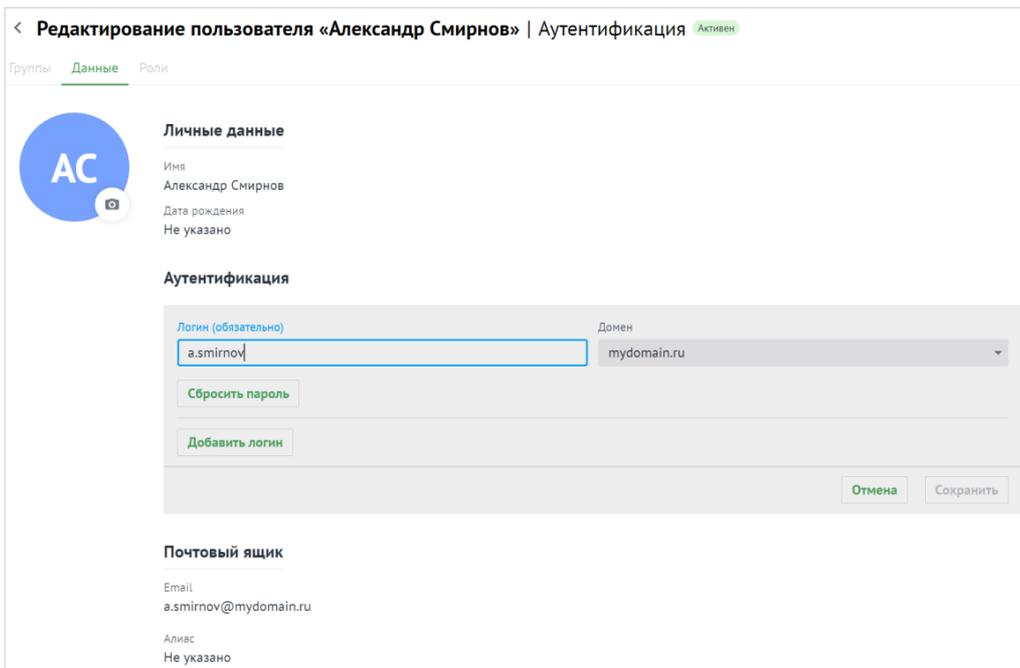


Рисунок 31 – Информация о пользователе на вкладке **Данные**

В результате отобразится информация, заполненная администратором при создании пользователя. При нажатии на иконку  выбранный блок становится редактируемым (Рисунок 32).



The screenshot shows a web interface for editing a user. At the top, there is a breadcrumb: < Редактирование пользователя «Александр Смирнов» | Аутентификация Активен. Below this are tabs: Группы, Данные, Роли. The main content is divided into three sections: 1. **Личные данные**: Includes a profile picture with initials 'AC', name 'Александр Смирнов', and birth date 'Не указано'. 2. **Аутентификация**: Contains a login field with 'a.smirnov', a domain dropdown menu with 'mydomain.ru', and buttons for 'Сбросить пароль', 'Добавить логин', 'Отмена', and 'Сохранить'. 3. **Почтовый ящик**: Shows email 'a.smirnov@mydomain.ru' and alias 'Не указано'.

Рисунок 32 – 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.

4.3 Управление группами рассылки

4.3.1 Просмотр групп рассылок

Для просмотра существующей группы в **Панели администрирования** необходимо выбрать раздел **Группы**. В рабочей области откроется перечень существующих групп (см. Рисунок 33). Об активной группе представлена следующая информация:

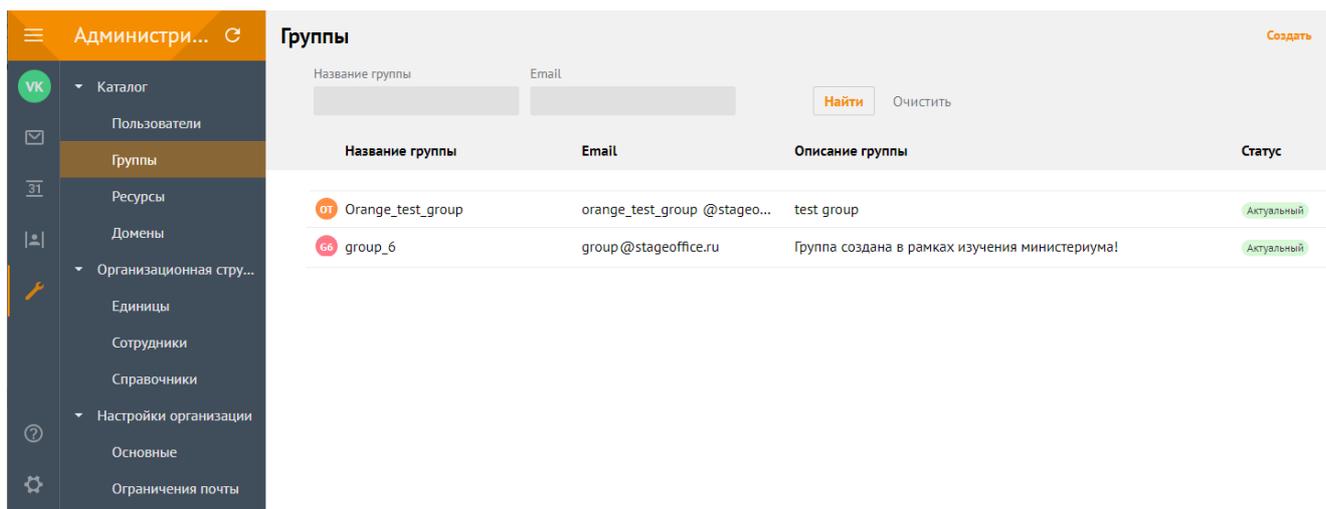


Рисунок 33 – Просмотр списка существующих групп рассылки

- 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 34.

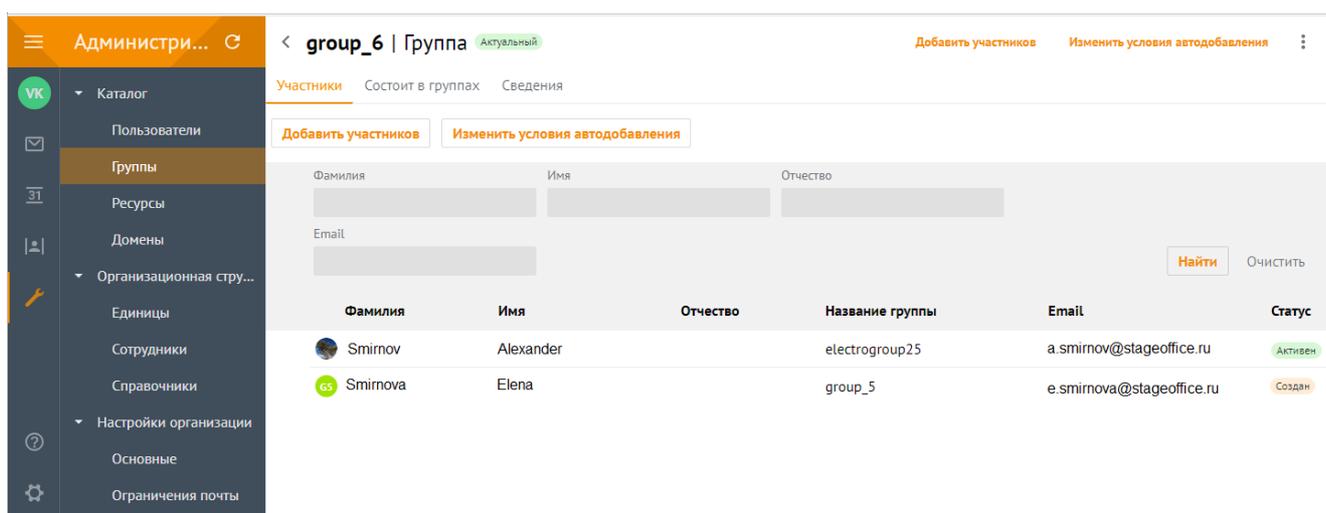


Рисунок 34 – Просмотр содержимого группы рассылки

4.3.2 Просмотр записи о группе

Чтобы просмотреть подробную запись о группе, необходимо открыть список групп, выбрать необходимую группу и перейти на вкладку **Сведения** (см. Рисунок 35).

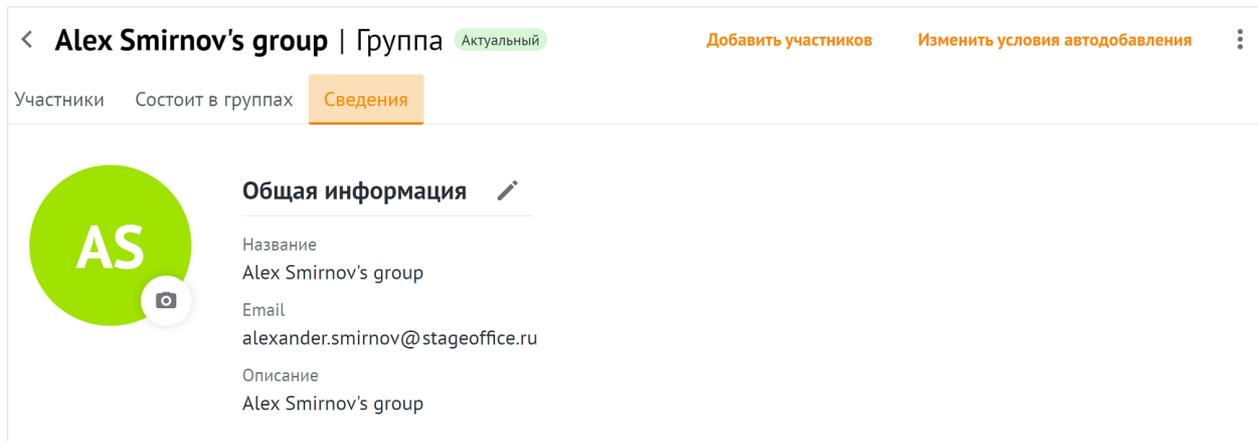


Рисунок 35 – Информация о группе

При нажатии на кнопку  откроется панель [редактирования](#) записи о группе.

4.3.3 Создание группы рассылки

Для создания группы рассылки необходимо выполнить следующие действия:

1. В разделе **Группы** нажать на кнопку **Создать** (см. Рисунок 36).

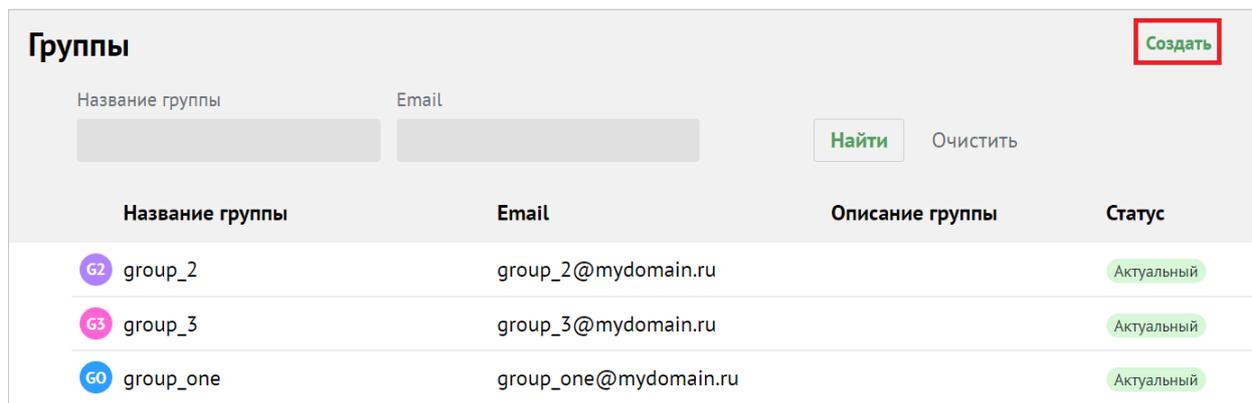


Рисунок 36 – Создание группы рассылки

2. В открывшейся форме создания группы необходимо заполнить следующие поля (см. Рисунок 37):

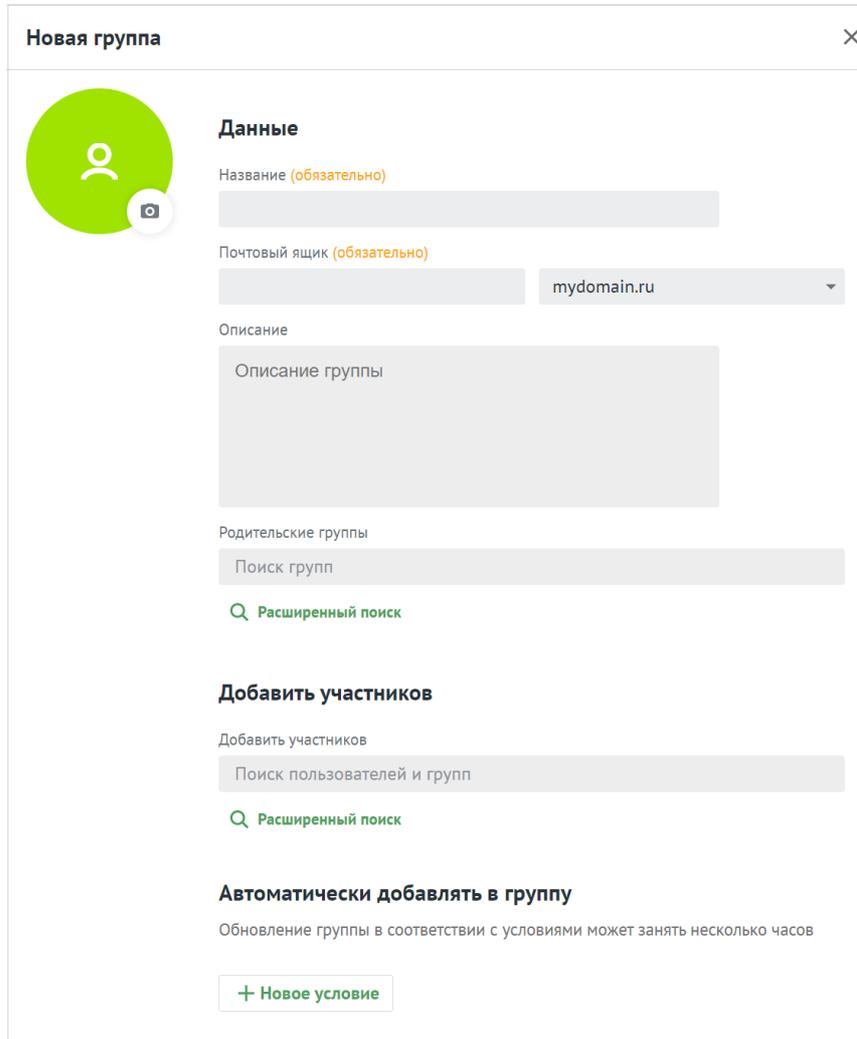


Рисунок 37 – Создание группы рассылки

- 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 (Рисунок 38).

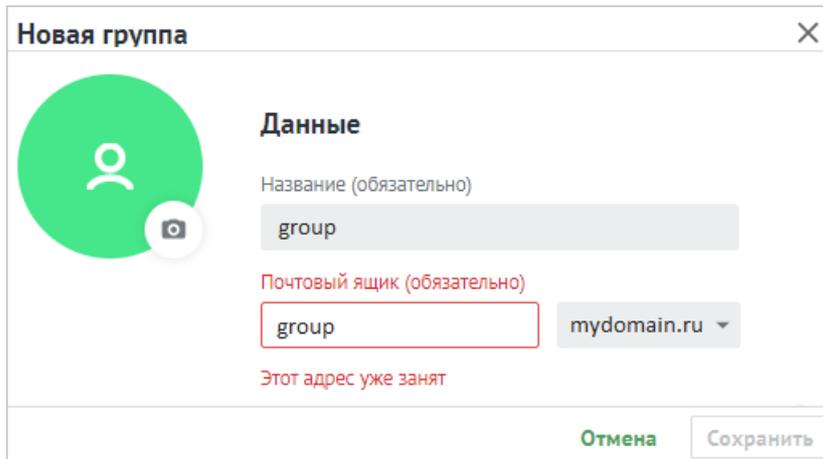
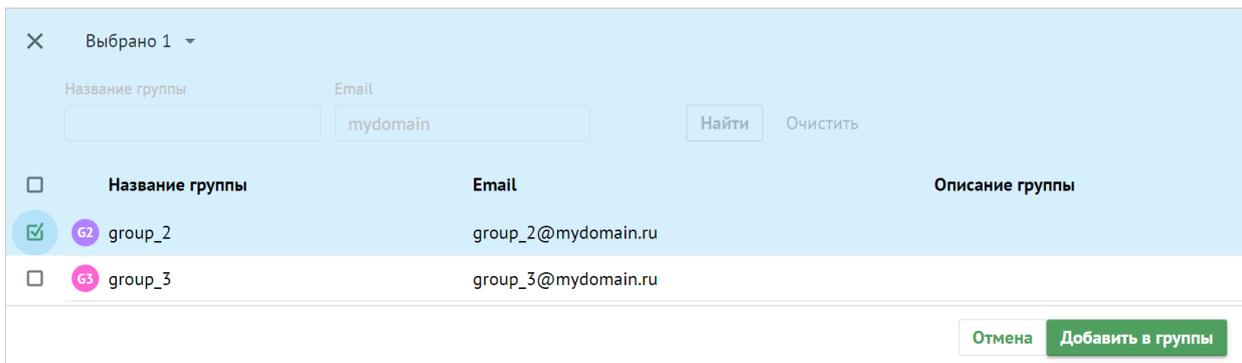


Рисунок 38 – Использование существующего названия почтового ящика

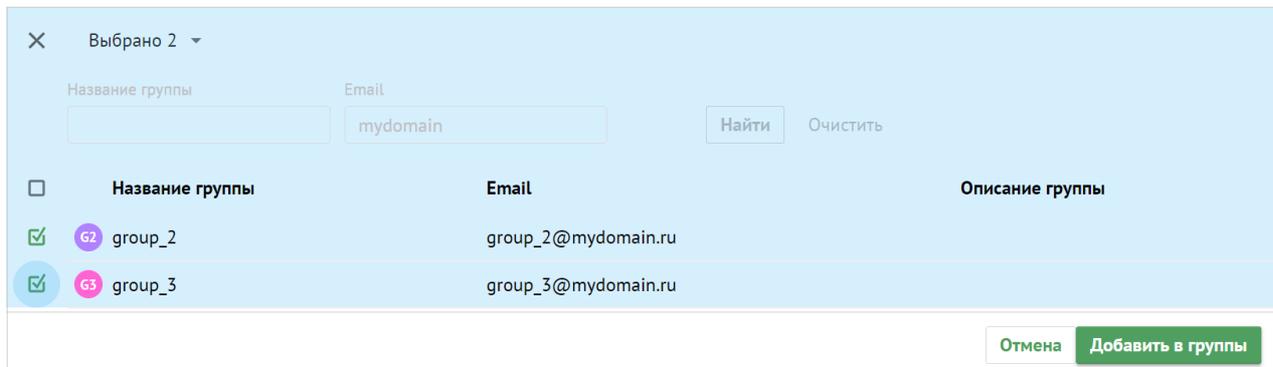
- Описание группы рассылки (опционально).
- Поле **Родительские группы** заполнить вручную или найти с помощью кнопки  (**Расширенный поиск**);
- установить курсор мыши на соответствующую группу и нажать **Добавить в группы** (Рисунок 39);



<input type="checkbox"/>	Название группы	Email	Описание группы
<input checked="" type="checkbox"/>	 group_2	group_2@mydomain.ru	
<input type="checkbox"/>	 group_3	group_3@mydomain.ru	

Рисунок 39 – Добавление в группы

- выбрать группы с помощью отметки из перечня групп и нажать кнопку **Добавить в группы** (Рисунок 40);



Выбрано 2

Название группы: Email:

<input type="checkbox"/>	Название группы	Email	Описание группы
<input checked="" type="checkbox"/>	G2 group_2	group_2@mydomain.ru	
<input checked="" type="checkbox"/>	G3 group_3	group_3@mydomain.ru	

Рисунок 40 – 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 [Настройка динамических групп рассылки](#).

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

Для отмены создания группы нажать на кнопку **Отмена**.

4.3.4 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 41).

Группы Создать

Название группы:
 Email: Найти Очистить

Название группы	Email	Описание группы	Статус
 group_2	group_2@mydomain.ru		Актуальный
 group_3	group_3@mydomain.ru		Актуальный
 group_one	group_one@mydomain.ru		Актуальный

Рисунок 41 – Поиск группы рассылки

4.3.5 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 42).

Группы Создать

Название группы:
 Email: Найти Очистить

Название группы	Email	Описание группы	Статус
 Alex Smirnov's group	alexander.smirnov@unbelivabl...	Alex Smirnov's group	Актуальный
 Alex Smirnov's group	alexander.smirnov@unbelivabl...	Alex Smirnov	Добавить в группу Добавить участников Изменить условия автодобавления

Рисунок 42 – Добавление группы рассылки в другую группу

2. В появившемся списке групп выделить флагами необходимые группы, нажать **Добавить в группы** (см. Рисунок 43).

✕ Выбрано 1 на странице ▾

Название группы:
 Email: Найти Очистить

<input checked="" type="checkbox"/>	Название группы	Email	Описание группы
<input checked="" type="checkbox"/>	 Elena Smirnova's group	elena.smirnova@mail	Elena Smirnova's group

Отмена
Добавить в группы

Рисунок 43 – Выбор групп рассылки для добавления группы

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

4.3.6 Удаление групп рассылки

Для удаления группы рассылки необходимо выбрать группу рассылки из списка и нажать на иконку , а затем на **Удалить** (см. Рисунок 44).

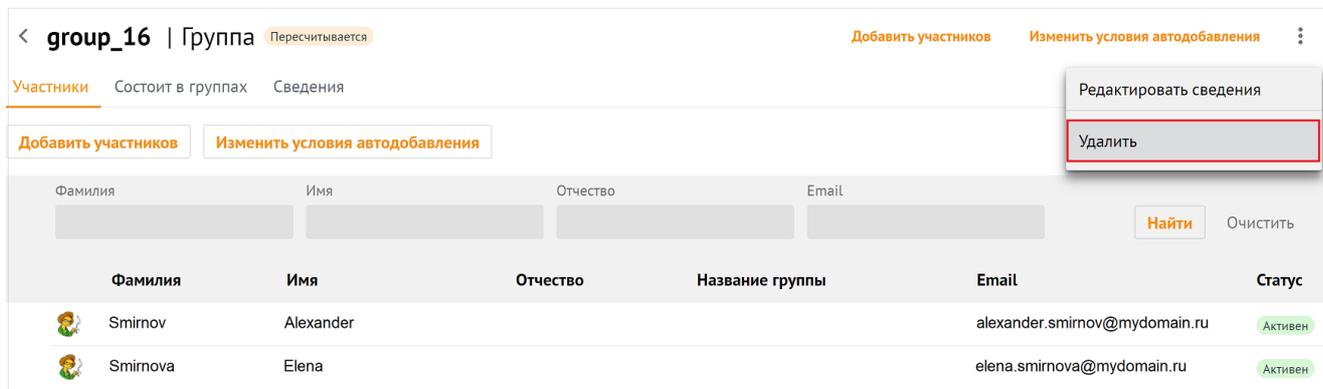


Рисунок 44 – Удаление группы рассылки

Подтвердить удаление группы рассылки, после чего группа будет удалена.

4.3.7 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 45).

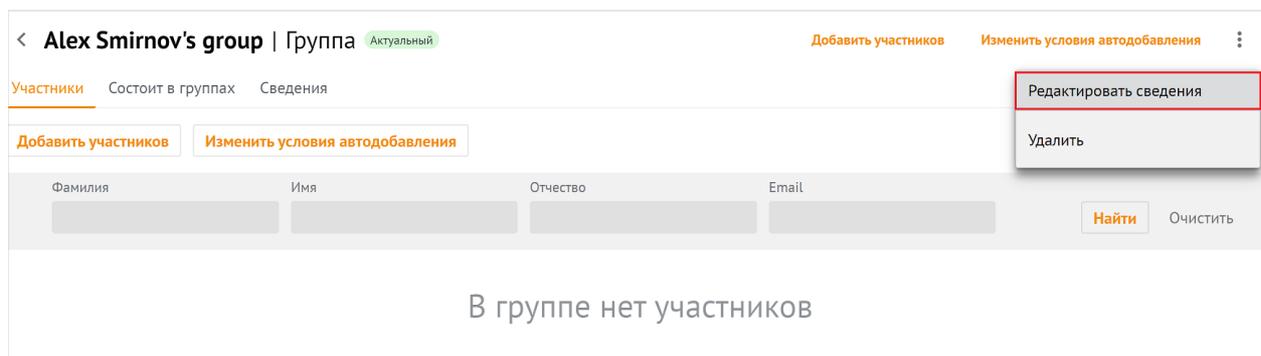


Рисунок 45 – Редактирование группы рассылки

2. Перейти в раздел **Группы**, в списке выбрать необходимую группу, выбрать закладку **Сведения**, в открывшейся форме нажать  (см. Рисунок 46).

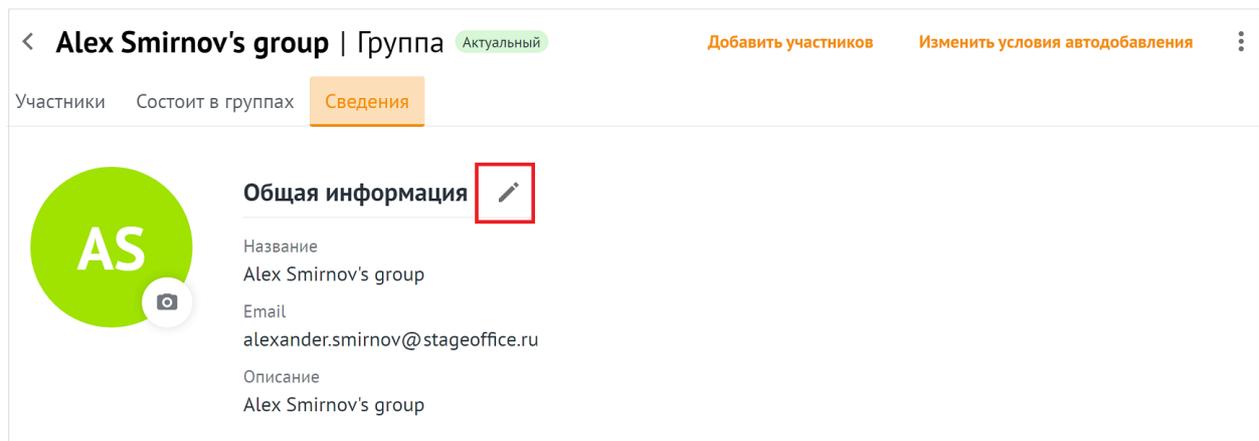


Рисунок 46 – Редактирование группы рассылки

На экране появится панель редактирования группы. Для сохранения изменений следует нажать на кнопку **Сохранить**. Для отмены внесенных изменений использовать кнопку **Отмена** (см. Рисунок 47).

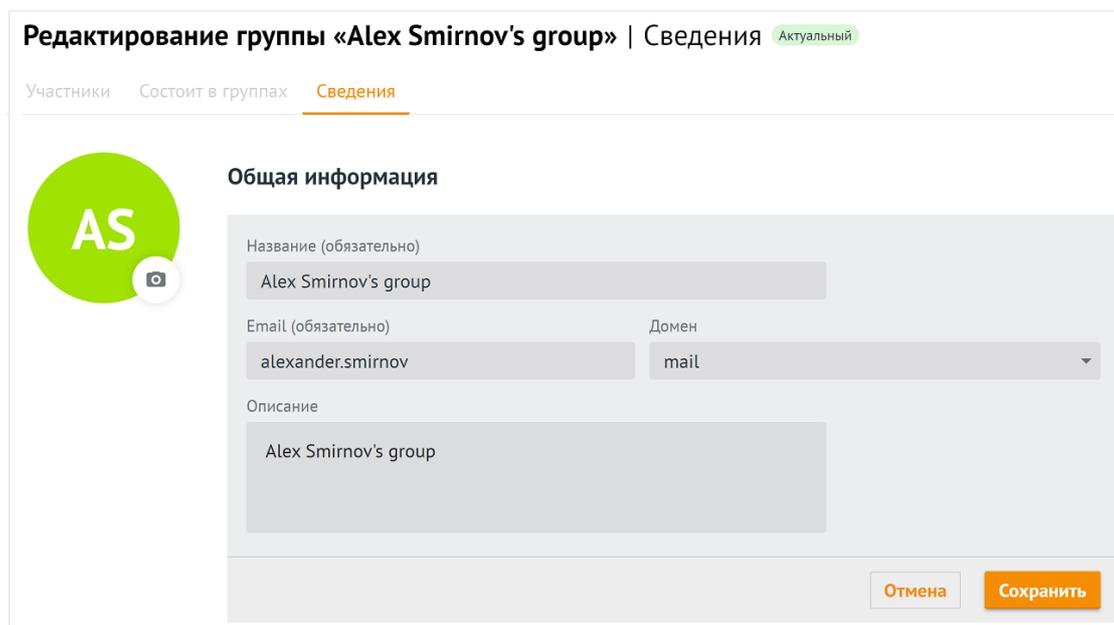


Рисунок 47 – Панель редактирования группы рассылки

4.3.8 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** (Рисунок 48);

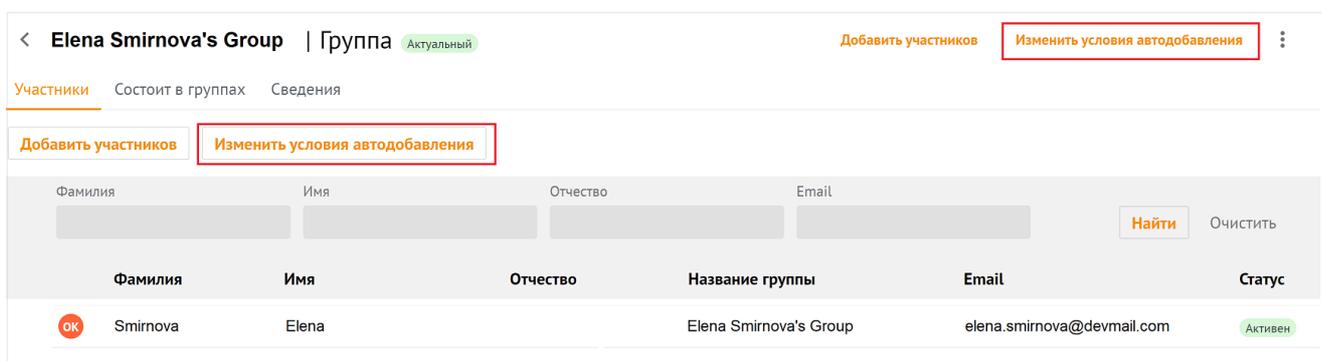


Рисунок 48 – Изменить условия автодобавления

На экране откроется панель настроек правил автоматического добавления (Рисунок 49);

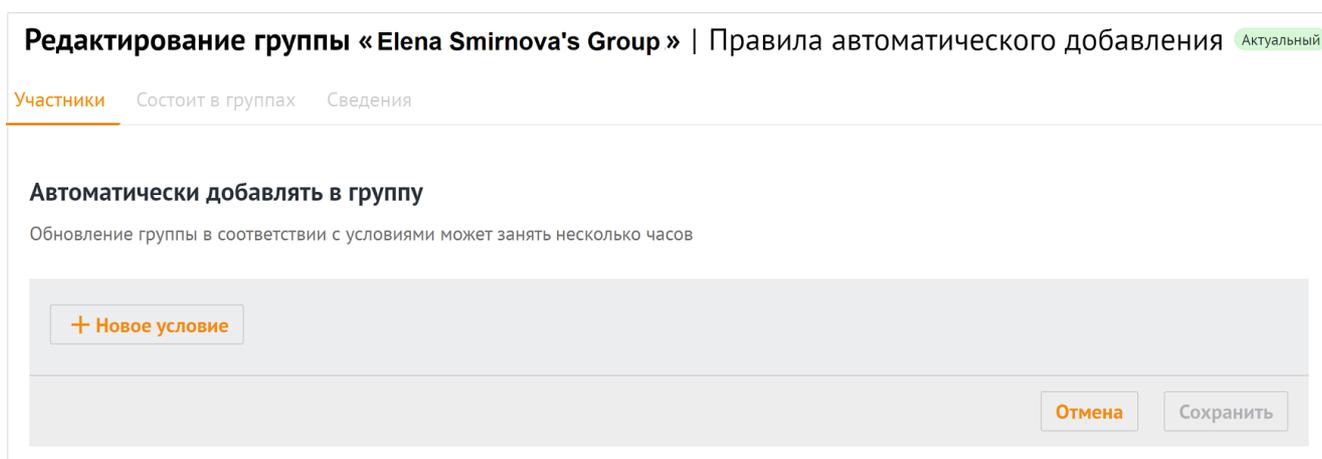


Рисунок 49 – Панель правил автоматического добавления в группу

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:

8. Выбрать соответствующее условие и нажать на кнопку  (**Еще**) напротив строки.

9. Выбрать значение:

–  (**Переместить выше**);

–  (**Переместить ниже**).

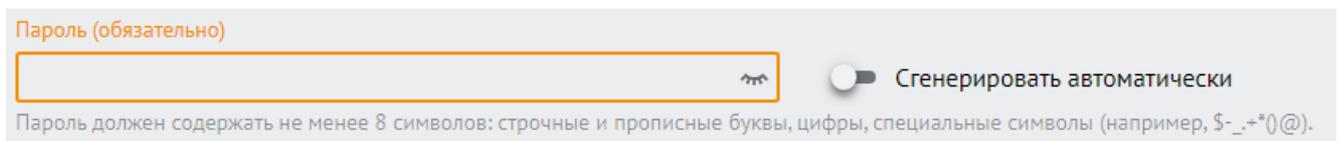
Чтобы удалить правило, необходимо нажать на кнопку  (**Еще**) и на кнопку **Удалить**.

4.4 Управление ресурсами

4.4.1 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. Рисунок 50):



Пароль (обязательно)

Пароль должен содержать не менее 8 символов: строчные и прописные буквы, цифры, специальные символы (например, \$-_*0@).

Рисунок 50 – 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**.



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**

4.4.2 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.

4.4.3 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**.

4.4.4 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**.

4.4.5 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**.

4.4.6 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**.



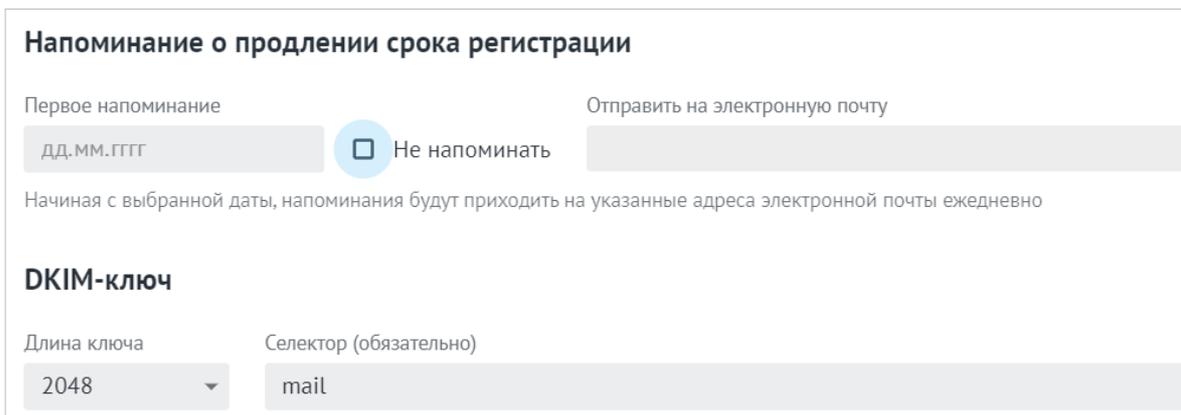
Пространства для встречи удаляются безвозвратно

4.5 Управление доменами

4.5.1 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 51):



Напоминание о продлении срока регистрации

Первое напоминание Не напоминать

Начиная с выбранной даты, напоминания будут приходить на указанные адреса электронной почты ежедневно

DKIM-ключ

Длина ключа Селектор (обязательно)

Рисунок 51 – 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.



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. [Расширенное администрирование](#)).

4.5.2 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**.

4.5.3 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.

4.5.4 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**.

4.5.5 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**.

4.5.6 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.



Домены удаляются безвозвратно

4.6 Управление единицами организационной структуры

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



Создание организации доступно только с помощью интерфейса командной строки. Подробная информация приведена в разделе [Создание организации](#)

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).

4.6.1 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**.

4.6.2 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**.



Поля **Организация** и **Вышестоящее подразделение** для дочерних единиц заполняются автоматически в соответствии с данными родительской единицы

4.6.3 Редактирование организационной единицы

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

1. Нажать на кнопку **Редактировать** в записи о единице.
2. 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**.

4.6.4 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**.

4.6.5 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**.

4.6.6 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**.



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**.

4.6.7 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**.

4.7 Управление сотрудниками

4.7.1 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. Рисунок 52):

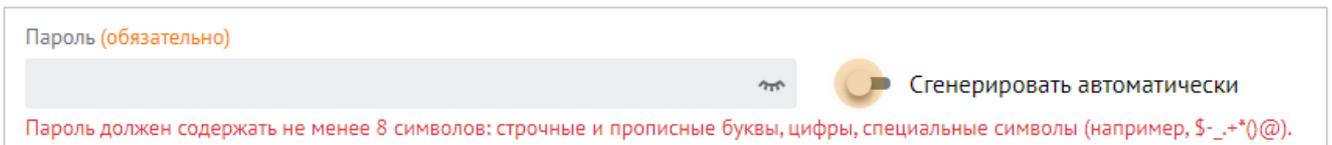


Рисунок 52 – Поле ввода пароля с подсказкой

- 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**.

4.7.2 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**.

4.7.3 Поиск сотрудника

Поиск сотрудника осуществляется в разделе **Сотрудники** аналогично информации, приведенной в разделе [Поиск группы рассылки](#), начиная с пункта 2.

4.7.4 Удаление сотрудника

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

4.8 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 этого справочника.

4.8.1 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:

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

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

4.8.2 Поиск записи в справочнике

Поиск должности или адреса осуществляется в разделе **Справочник** аналогично информации, приведенной в разделе [Поиск группы рассылки](#), начиная с пункта 2.

4.8.3 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**.

4.8.4 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**.

4.9 Управление настройками организации

4.9.1 Основные настройки

Для отображения названия организации и отображения / редактирования региональных настроек следует перейти в раздел **Настройки организации / Основные** (см. Рисунок 53).

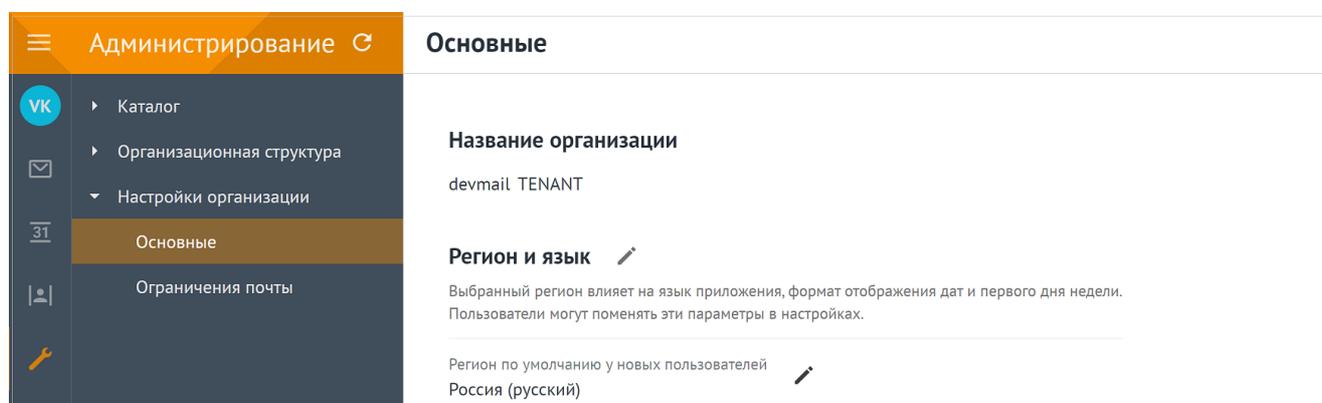
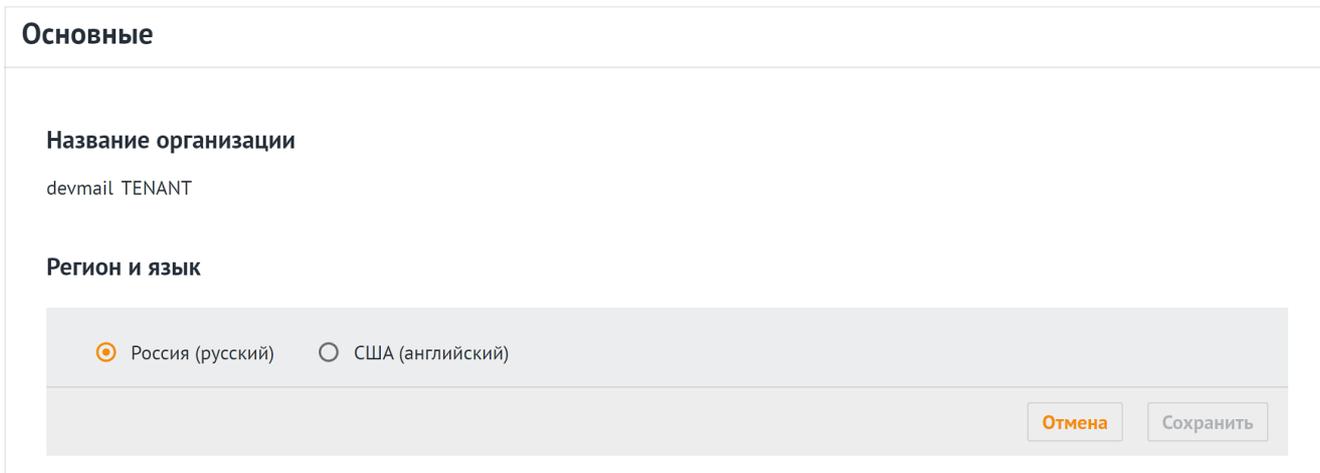


Рисунок 53 – Основные настройки организации (название и регион)

Для изменения региональных настроек необходимо нажать , на экране откроется панель выбора региона и языка (см. Рисунок 54).



Основные

Название организации
devmail TENANT

Регион и язык

Россия (русский) США (английский)

Отмена **Сохранить**

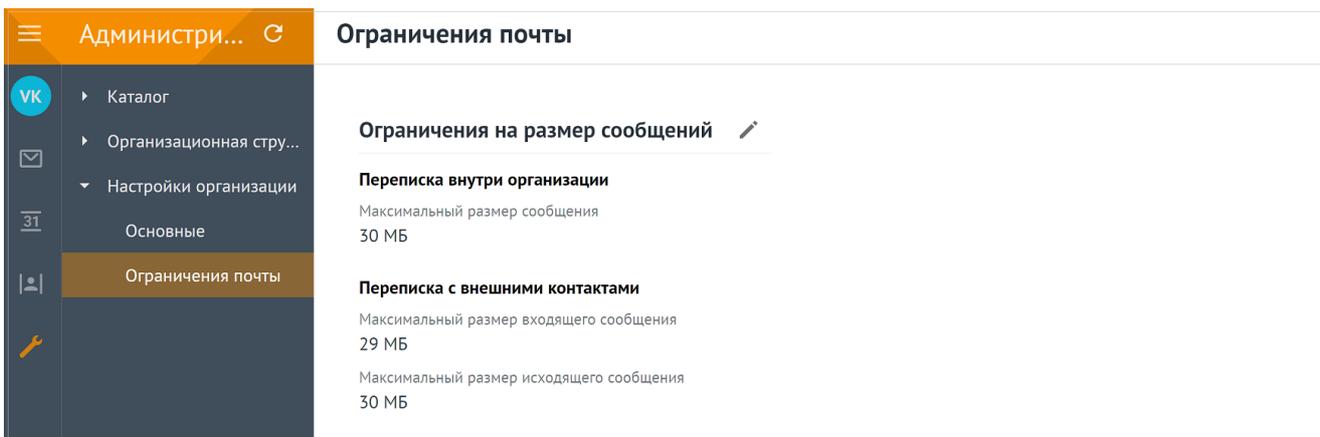
Рисунок 54 – Редактирование региональных настроек

4.9.2 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 55).



Администрирование

Ограничения почты

Ограничения на размер сообщений

Переписка внутри организации
Максимальный размер сообщения
30 МБ

Переписка с внешними контактами
Максимальный размер входящего сообщения
29 МБ
Максимальный размер исходящего сообщения
30 МБ

Рисунок 55 – Отображение ограничений размеров почтовых сообщений

Для изменения ограничений необходимо нажать , на экране откроется форма редактирования максимальных размеров сообщений (см. Рисунок 56).



The screenshot shows a settings form with two main sections:

- Переписка внутри организации**
 - Максимальный размер сообщения: 30 МБ
- Переписка с внешними контактами**
 - Максимальный размер входящего сообщения: 29 МБ
 - Максимальный размер исходящего сообщения: 30 МБ

At the bottom right, there are two buttons: **Отмена** (Cancel) and **Сохранить** (Save).

Рисунок 56 – Редактирование ограничений на размер почтовых сообщений

5 РАСШИРЕННОЕ АДМИНИСТРИРОВАНИЕ С ПОМОЩЬЮ ИНТЕРФЕЙСА КОМАНДНОЙ СТРОКИ



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 оболочку для взаимодействия Mailion с серверной частью.

5.1 Информация для работы с интерфейсом командной строки

5.1.1 Установка

При установке Mailion утилита 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
```

Утилита командной строки **ministerium** совместима со следующими ОС:

- дистрибутивы Linux на основе Debian;
- Fedora;
- ОС, поддерживающие пакеты **rpm** и **deb**.

5.1.2 Просмотр информации о командах



Все команды, вводимые в интерфейсе командной строки вручную, набираются в одну строку. Для более наглядного представления приведенные в данном руководстве команды записаны в виде столбца, с указанием параметров на отдельных строках.

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

```
nct_ministerium --help
```

Для просмотра справки по конкретной команде следует использовать запрос:

```
nct_ministerium <команда> --help
```

Список доступных команд с их описанием приведен в [Приложении А. Команды интерфейса командной строки](#).

5.1.3 Получение сертификатов для работы с ministerium

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

Необходимо наличие доступа с рабочей станции администратора тенанта к серверу, где развернут сервис **cox** (`installation.example.net:3142`).

Пример получения сертификатов:

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

// копирование сертификатов и файла конфигурации
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 файла конфигурации логина и пароля администратора инсталляции
vim /home/user/ministerium/config.json
// 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 ее выполнения с
// рабочей станции
scp user@ucs-infra-1.installation.example.net:/home/user/ministerium.tar.gz .
```

5.2 Установка и получение общей квоты тенанта



Установить общую квоту тенанта может только пользователь с ролью администратора инсталляции.

Квота тенанта — это общий объем дискового пространства, выделяемого для сущностей тенанта. Общую квоту тенанта можно задать с помощью следующего запроса:

```
nct_ministerium update_total_quotas \
--config ministerium.json \
--admin.login <...> \
--admin.password <...> \
--tenant_id 2a3b8043-70ef-4a59-a395-9e28cc5c2685 \
--tenant_total.max_size 40GB
```

Описание параметров запроса приведено в таблице 16.

Таблица 16 — Параметры запроса для задания общей квоты тенанта

Параметр	Тип	Обязательный	Описание
config	Str	+	Конфигурационный файл с параметрами сервиса сох 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
tenant_total.max_size	Str	+	Размер общей квоты тенанта. Допустимые единицы измерения: В, КВ, МВ, GB, ТВ. Пример: 13GB700MB

Пример ответа:

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

Администратор инсталляции также может запросить сведения о размере общей квоты, выделенной на тенант:

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

Описание параметров запроса приведено в таблице 17.

Таблица 17 — Параметры запроса о размере общей квоты тенанта

Параметр	Тип	Обязательный	Описание
config	Str	+	Конфигурационный файл с параметрами сервиса сох и настройками TLS. Формируется

Параметр	Тип	Обязательный	Описание
			автоматически на сервере с ролью ucs_infrastructure и находится по пути <code>/srv/ministerium/config.json</code>
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"
  },
  "mail_total_quota": null,
  "tenant_total_quota": {
    "max_size": 42949672960
  }
}
```



Администратор инсталляции не наделен правами на установку и получение текущего значения почтовой квоты (`mail_total_quota`) тенанта.

5.3 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.

5.3.1 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
```



При выполнении команды `create_tenant` помимо тенанта также создаются:

- системный GAL-пользователь;
- GAL-тег по умолчанию;
- группа ALL.

Описание параметров запроса приведено в таблице 18.

Таблица 18 — Параметры запроса на создание тенанта

Параметр	Тип	Обязательный	Описание
config	Str	+	Конфигурационный файл с параметрами сервиса sox и настройками TLS. Формируется автоматически на сервере с ролью ucs_infrastructure и находится по пути <code>/srv/ministerium/config.js on</code>
display_name	Str	+	Имя тенанта
default_locale	Str	+	Код языка 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

Параметр	Тип	Обязательный	Описание
<code>password.min_lower_case_letters</code>	Int	-	Минимальное количество строчных букв
<code>password.min_digits</code>	Int	-	Минимальное количество цифр
<code>password.min_special_characters</code>	Int	-	Минимальное количество специальных символов

Пример ответа:

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



В случае, если указан хотя бы один параметр парольной политики, в обязательном порядке должны быть указаны остальные. Если параметры парольной политики не были указаны совсем, то 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
      }
    }
  }
}
```

```
}
}
```

5.3.2 Создание администратора тенанта

Для создания администратора 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 ef28480f-0ee4-4f0c-af67-59f100727f31
```

Описание параметров запроса приведено в таблице 19.

Таблица 19 — Параметры запроса на получение GAL-тегов тенанта

Параметр	Тип	Обяз.	Описание
config	Str	+	Конфигурационный файл с параметрами сервиса sox и настройками TLS. Формируется автоматически на сервере с ролью ucs_infrastructure и находится по пути <code>/srv/ministerium/config.json</code>
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 \
--login admin2.tenant2_test \
--password 'BnYs6j*Hw_TT$X)MsD59' \
--profile.first_name Admin2 \
--profile.last_name Test
```

Описание параметров запроса приведено в таблице 20.

Таблица 20 — Параметры запроса на создание администратора тенанта

Параметр	Тип	Обязательный	Описание
config	Str	+	Конфигурационный файл с параметрами сервиса Сох 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
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 [Удаление пользователя, группы, ресурса](#).

5.3.3 Создание пользователя тенанта



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 21.

Таблица 21 — Параметры запроса на получение GAL-тегов тенанта

Параметр	Тип	Обязательный	Описание
config	Str	+	Конфигурационный файл с параметрами сервиса Сох 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 \
```

```
--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 22.

Таблица 22 — Параметры запроса на создание пользователя тенанта

Параметр	Тип	Обязательный	Описание
config	Str	+	Конфигурационный файл с параметрами сервиса Сох 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
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 23.

Таблица 23 — Параметры 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 создании пользователя

Параметр	Тип	Обязательный	Описание
Entities.roles	Str	+	Список ролей должен включать роль user_regular
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 был указан код языка (языковой стандарт), то его значение должно быть равно коду языка, указанному при создании тенанта
Entities.status	Int	+	Значение должно быть равно 2 (ACTIVE)



При сбое создания пользователя
см. раздел [Создание первичной организационной структуры](#)

5.3.3.1 Настройка уведомлений об истечении срока действия пароля

С помощью расширенного администрирования можно настроить отправку уведомлений на почту пользователей о том, что срок 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 24.

Таблица 24 — Параметры запроса на создание уведомления

Параметр	Тип	Обязательный	Описание
admin.login	Str	+	Логин администратора тенанта
admin.password	Str	+	Пароль администратора тенанта
locale	Str	+	Код языка 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 замещает значение 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 25.

Таблица 25 — Параметры 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



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  
  }  
}
```

5.3.4 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:

```
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**.

5.3.5 Создание общего почтового ящика

Общий почтовый ящик позволяет пользователям с соответствующими правами читать поступающую в него почту и отправлять письма от имени его учетной записи без дополнительной авторизации.

Пользователь, которому предоставляется доступ к общему почтовому ящику, получает права **совладельца** на все почтовые папки, календари и адресные книги учетной записи общего почтового ящика и может, в свою очередь, предоставлять доступ к этим объектам другим пользователям, устанавливая требуемые уровни доступа.

Процедура создания общего почтового ящика через ministerium

1. Создать пользователя УЗ общего почтового ящика:

```
nct_ministerium create_user \
--config /srv/ministerium/config.json \
--tenant_id 01068ade-1cce-4125-ab6b-91d977ecf85b \
--type 3 \
--email 'shared_mailbox@example.com' \
--login 'shared_mailbox@example.com'
```

Описание параметров команды приведено в таблице 26.

Таблица 26 — Параметры команды создания общего почтового ящика

Параметр	Тип	Обязательный	Описание
config	Str	+	Путь к файлу с данными авторизации администратора, параметрами сервиса cox и протокола TLS. Формируется автоматически на сервере с ролью ucs_infrastructure и находится по пути /srv/ministerium/config.json
tenant_id	Str	+	Идентификатор тенанта
type	Int	+	Тип пользователя (3 — совместно используемая учетная запись)
email	Str	+	Адрес общего почтового ящика
login	Str	+	Логин общего почтового ящика

Пример ответа:

```
command finished{"client-request-id": "aee26a7c-52bd-4f58-bf07-de287dfcec56",
"command": "create_user", "msg": "ok", "elapsed_time": 2.443276695}
{
  "Response": {
    "changed": true,
    "failed": false,
    "msg": "ok"
  },
  "id": "792c03ce-55e6-4ae8-96c9-042b3f7e6389"
}
```

2. Предоставить другим пользователям доступ к УЗ общего почтового ящика:

```
nct_ministerium set_shared_access \
--config /srv/ministerium/config.json \
--delegate_email shared_mailbox@example.com \
--emails user_1@example.com \
--emails user_2@example.com \
--permissions_by_emails 2
```

Описание параметров команды приведено в таблице 27.

Таблица 26 — Параметры команды предоставления общего доступа к УЗ общего почтового ящика

Параметр	Тип	Обязательный	Описание
config	Str	+	Путь к файлу с данными авторизации администратора, параметрами сервиса cox и протокола TLS. Создается автоматически на сервере с ролью ucs_infrastructure ; путь по у пути /srv/ministerium/config.json
delegate_email	Str	+	Адрес общего почтового ящика
emails	Str	+	Адрес пользователя, которому требуется предоставить доступ к общему почтовому ящику. Для указания нескольких пользователей, --emails добавляется перед каждым из адресов
permissions_by_emails	Int	+	Уровень доступа для отправки писем: 0 — «Не может» (Cannot), пользователь не может отправлять письма от имени делегированной УЗ; 1 — «От имени» (OnBehalf), пользователь может отправлять письма от имени делегированной УЗ, но со своей учетной записи ;

Параметр	Тип	Обязательный	Описание
			2 — «Отправить как» (SendAs), пользователь может отправлять письма с делегированной учетной записи

Пример ответа:

```
{
```

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



Отозвать права доступа у одного или нескольких пользователей можно с помощью команды `unset_shared_access` (см. разделы [Отзыв доступа к делегированной учетной записи у определенного делегата](#), [Отзыв доступа к делегированной учетной записи у всех делегатов](#)).

5.3.6 Настройка квот и лимитов для почты в тенанте

Квота — это общий объем дискового пространства, выделяемого субъекту или группе субъектов. Механизм задания квот используется в Mailion, чтобы установить следующие ограничения:

- общий размер всех писем в почтовом ящике;
- размер отдельного письма;
- суммарный размер вложений для одного письма.

Квоты можно задать как на уровне тенанта, так и на уровне отдельного пользователя.

Квоты, заданные на уровне пользователя, имеют приоритет над квотами на уровне тенанта.

Лимит — это максимальный объем физических или логических ресурсов, которое субъект может использовать за один раз. Механизм задания лимитов используется в Mailion, чтобы установить следующие ограничения:

- размер входящих и исходящих (внутренних и внешних) писем;
- суммарный размер вложений для входящих и исходящих (внутренних и внешних) писем;
- частота отправки писем.



Настройки квот и лимитов в тенанте может выполнять только пользователь с ролью администратора тенанта

Для настройки квот используются команды, приведенные в таблице 27.

Таблица 27 — Команды для настройки квот

Доступные команды	Описание
<code>create_tenant_quotas_profile</code>	Создать квоты профиля тенанта
<code>create_user_quotas_profile</code>	Создать квоты профиля пользователя
<code>delete_tenant_quotas_profile</code>	Удалить квоты профиля тенанта
<code>get_recount_quotas_processes</code>	Получить все запущенные процессы пересчета квот
<code>get_user_quotas_profile</code>	Получить квоты профиля пользователя
<code>recount_quotas</code>	Начать процесс напоминания о пересчете квот для одиночного объекта или всех объектов в тенанте
<code>remove_user_quotas_profile</code>	Удалить квоты профиля пользователя
<code>stop_recount_quotas</code>	Остановить процесс пересчета квоты. Некоторые объекты могли иметь непредвиденные упоминания о квотах
<code>update_tenant_quotas_profile</code>	Обновить квоты профиля тенанта
<code>update_user_quotas_profile</code>	Обновить квоты профиля пользователя
<code>get_total_quotas</code>	Получить размер общей квоты, выделенной на тенант
<code>update_total_quotas</code>	Обновить общую квоту

5.3.6.1 Квоты на уровне тенанта

5.3.6.1.1 Создание квот профиля тенанта

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 28.

Таблица 28 — Параметры 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 тенанта: – ALL_MAILS_SIZE — размер всех писем; – ONE_MAIL_SIZE — размер письма; – ALL_MAIL_ATTACHMENTS_SIZE — размер всех вложений в письме
cox.balancer_endpoint	Str	+	Конечная точка балансировщика нагрузки сервиса
cox.compression	Str	+	Метод сжатия данных (варианты: none, gzip), по умолчанию — none
cox.endpoint	Str	+	Конечная точка сервиса
cox.load_balanced	Bool	+	Балансировщик нагрузки сервиса
cox.request_timeout	Str	+	Таймаут запроса к сервису
cox.service_name	Str	+	Имя сервиса
cox.use_tls	Bool	+	TLS-сертификат

Параметр	Тип	Обязательный	Описание
cox.use_tls_balancer	Bool	+	Защищенная передача данных при подключении к балансировщику
tls_settings.ca_file	Str	+	Путь к СА 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
}
```

5.3.6.1.2 Удаление квот профиля тенанта

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 29.

Таблица 29 — Параметры 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	+	Конечная точка балансировщика нагрузки сервиса

Параметр	Тип	Обязательный	Описание
cox.compression	string	+	Метод сжатия данных (варианты: none, gzip), по умолчанию — none
cox.endpoint	string	+	Конечная точка сервиса
cox.load_balanced	boolean	+	Балансировщик нагрузки сервиса
cox.request_timeout	string	+	Таймаут 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 СА файлу
tls_settings.client_certificate	string	+	Путь к файлу сертификата клиента
tls_settings.key_file	string	+	Путь к файлу с ключом клиента

Пример ответа на данный запрос:

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

5.3.6.1.3 Обновление квот профиля тенанта

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_certificate_file ../certs/client.crt.pem
--tls_settings.key_file ../certs/client_key.pem
```

Описание параметров запроса на обновление квот профиля приведено в таблице 30.

Таблица 30 — Параметры 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	+	Конечная точка балансировщика нагрузки сервиса
cox.compression	Str	+	Метод сжатия данных (варианты: none, gzip), по умолчанию — none
cox.endpoint	Str	+	Конечная точка сервиса
cox.load_balanced	Bool	+	Балансировщик нагрузки сервиса
cox.request_timeout	Str	+	Таймаут 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 СА 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
}
```

5.3.6.2 Квоты на уровне пользователя

5.3.6.2.1 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 31.

Таблица 31 — Параметры 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	+	Конечная точка балансировщика нагрузки сервиса

Параметр	Тип	Обязательный	Описание
cox.compression	Str	+	Метод сжатия данных (варианты: none , gzip), по умолчанию — none
cox.endpoint	Str	+	Конечная точка сервиса
cox.load_balanced	Bool	+	Балансировщик нагрузки сервиса
cox.request_timeout	Str	+	Таймаут 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 СА 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
}
```

5.3.6.2.2 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_cert.pem
--tls_settings.key_file ../certs/client_key.pem
```

Описание параметров запроса на удаление квот профиля приведено в таблице 32.

Таблица 32 — Параметры 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	+	Конечная точка балансировщика нагрузки сервиса
cox.compression	Str	+	Метод сжатия данных (варианты: none , gzip), по умолчанию — none
cox.endpoint	Str	+	Конечная точка сервиса
cox.load_balanced	Bool	+	Балансировщик нагрузки сервиса
cox.request_timeout	Str	+	Таймаут 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
}
```

5.3.6.2.3 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 0ele6928-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
```



В релизе 1.5 имеется ограничение на размер письма — не более 25 МБ.

Описание параметров запроса на обновление квот профиля приведено в таблице 33.

Таблица 33 — Параметры 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);

Параметр	Тип	Обязательный	Описание
			– ALL_MAIL_ATTACHMENTS_SIZE (размер всех вложений в письме)
cox.balancer_endpoint	Str	+	Конечная точка балансировщика нагрузки сервиса
cox.compression	Str	+	Метод сжатия данных (варианты: none , gzip), по умолчанию — none
cox.endpoint	Str	+	Конечная точка сервиса
cox.load_balanced	Bool	+	Балансировщик нагрузки сервиса
cox.request_timeout	Str	+	Таймаут 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
}
```

5.3.6.2.4 Получение квот профиля пользователя

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 34.

Таблица 34 — Параметры 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	+	Конечная точка балансировщика нагрузки сервиса
cox.compression	Str	+	Метод сжатия данных (варианты: none , gzip), по умолчанию — none
cox.endpoint	Str	+	Конечная точка 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 СА 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": {}
}

```

5.3.6.2.5 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 35.

Таблица 35 — Параметры запроса на просмотр пользователей с нулевой квотой

Параметр	Тип	Обязательный	Описание
config	Str	+	Конфигурационный файл с параметрами сервиса Сох 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", ...}
}
```

5.3.6.3 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.

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 36.

Таблица 36 — Параметры 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 Сох 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"
}
```

5.3.6.4 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 37.

Таблица 37 — 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 Сох 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
    ]
  },
  "tenat_total_quota": {
    "max_size": 42949672960
  }
}
```

5.3.6.5 Установка лимитов для 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": "38MB", \
"ONE_MAIL_SIZE_INCOMING": "38MB", \
"ALL_MAIL_ATTACHMENTS_SIZE_INCOMING": "25MB", \
"ALL_MAIL_ATTACHMENTS_SIZE_OUTGOING": "25MB", \
"ONE_MAIL_SIZE_OUTGOING_EXTERNAL": "38MB", \
"ALL_MAIL_ATTACHMENTS_SIZE_OUTGOING_EXTERNAL": "25MB", \
"ONE_MAIL_SIZE_INCOMING_EXTERNAL": "38MB", \
"ALL_MAIL_ATTACHMENTS_SIZE_INCOMING_EXTERNAL": "25MB", \
"MAIL_COUNT_LIMIT": "2", \
"MAIL_COUNT_TIME_LIMIT": "60"}'
```



В примере приведены рекомендованные размеры лимитов по умолчанию. В случае установки собственных лимитов рекомендуется придерживаться правила: лимит на все письмо должен быть в 1,5 раза больше лимита на вложения

Описание параметров запроса приведено в таблице 38.

Таблица 38 — Параметры запроса на установку лимитов почты в тенанте

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 описаны ниже

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 для входящих сообщений;
- `ALL_MAIL_ATTACHMENTS_SIZE_OUTGOING`: максимальный суммарный размер всех вложений для исходящих сообщений;
- `ONE_MAIL_SIZE_OUTGOING_EXTERNAL`: максимальный размер внешнего исходящего сообщения;

- ALL_MAIL_ATTACHMENTS_SIZE_OUTGOING_EXTERNAL: максимальный суммарный размер всех вложений 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 для внешних входящих сообщений;
- MAIL_COUNT_LIMIT — количество писем за указанный период;
- MAIL_COUNT_TIME_LIMIT — минимальный период в секундах.



Последние два параметра ограничивают частоту отправки писем. Например, если MAIL_COUNT_LIMIT=2 и MAIL_COUNT_TIME_LIMIT=60, то пользователь не сможет отправить больше двух писем в минуту

5.3.7 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_cert.pem>
--tls_settings.key_file <.../client_key.pem>
```

Описание параметров запроса приведено в таблице 39.

Таблица 39 — Параметры 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

Параметр	Тип	Обязательный	Описание
<code>cox.balancer_endpoint</code>	Str	+	Конечная точка балансировщика нагрузки сервиса
<code>cox.endpoint</code>	Str	+	Конечная точка сервиса
<code>cox.load_balanced</code>	Bool	+	Балансировщик нагрузки сервиса
<code>cox.request_timeout</code>	Str	+	Таймаут запроса к сервису
<code>cox.service_name</code>	Str	+	Имя сервиса
<code>cox.use_tls</code>	Bool	+	TLS-сертификат
<code>cox.use_tls_balancer</code>	Bool	+	Защищенная передача данных при подключении к балансировщику
<code>tls_settings.ca_file</code>	Str	+	Путь к СА файлу
<code>tls_settings.client_cert_file</code>	Str	+	Путь к файлу сертификата клиента
<code>tls_settings.key_file</code>	Str	+	Путь к файлу с ключом клиента



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.

5.3.8 Учетная запись для резервного копирования

У обычных учетных записей, включая администраторов, нет прав на выполнение операций резервного копирования и восстановления. Для этих операций необходимо использовать специальные учетные записи уровня инсталляции или тенанта.

Уровень инсталляции

При первоначальной установке автоматически создается системная учетная запись с логином **backuper**, наделенная правами на резервное копирование и восстановление данных инсталляции. Пароль для этой учетной записи задается с помощью параметра: `mailion_installation_backuper_password`.

Уровень тенанта

Учетную запись для операций резервного копирования и восстановления на уровне тенанта может создать администратор тенанта с помощью следующей команды:

```
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 <...> \
--password 'BnYs6j*Hw_TT$X)MsD59' \
--profile.first_name <...> \
--profile.last_name <...>
```

Описание параметров запроса приведено в таблице 40.

Таблица 40 — Параметры запроса на создание учетной записи для резервного копирования

Параметр	Тип	Обязательный	Описание
config	Str	+	Конфигурационный файл с параметрами сервиса Сох 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	+	Список идентификаторов ГАК
login	Str	+	Логин создаваемой учетной записи
password	Str	+	Пароль создаваемой учетной записи
profile.first_name	Str	+	Имя пользователя создаваемой учетной записи

Параметр	Тип	Обязательный	Описание
<code>profile.last_name</code>	Str	+	Фамилия пользователя создаваемой учетной записи

5.3.9 Удаление письма у всех получателей в рамках тенанта



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 «Mailion. Руководство пользователя».
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 41.

Таблица 41 — Параметры запроса на удаление письма

Параметр	Тип	Обязательный	Описание
<code>message_id</code>	Str	+	Идентификатор сообщения, которое необходимо удалить
<code>region_id</code>	Str	+	Регион, в котором находится сообщение
<code>tenant_id</code>	Str	+	Идентификатор тенанта, в рамках которого удаляются сообщения

Пример ответа:

```
{
  "Response": {
```

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

После этого выбранное письмо удалится.

5.3.10 Экспорт и импорт данных пользователя

5.3.10.1 Экспорт данных пользователя

С помощью команды экспорта данных пользователя администратор тенанта может выгрузить содержимое почтового ящика выбранного пользователя, события и задачи его календаря, а также контакты из его личной адресной книги в целях архивирования, передачи третьим лицам при юридическом запросе, очистки почтового ящика при превышении квоты, переноса данных из одной инсталляции Mailion в другую и т. п.

Описание команды

Результатом работы команды `export_user_data` является архив формата **tar.gz**, а также каталог с выгруженными данными. Содержимое архива повторяет содержимое каталога с точностью до сжатия. Обе сущности создаются в текущем рабочем каталоге, если с помощью параметра `path` не задано иное.

Пример команды:

```
nct_ministerium export_user_data \
--config ... \
--user 'user@mln.example.net' \
--path /tmp/ \
--start '2024-01-01 00:00:00 +0300' \
--end '2024-08-25 12:00:00 +0300'
```

Описание параметров команды приведено в таблице 42.

Таблица 42 — Параметры команды экспорта данных пользователя

Параметр	Тип	Обязательный	Описание
config	string	+	Путь к файлу конфигурации ministerium
user	string	+	Адрес пользователя, данные которого экспортируются
path	string	+	Путь для сохранения экспортируемых данных

Параметр	Тип	Обязательный	Описание
start	string	+	Дата начала экспорта данных в формате уууу-мм-дд hh:mm:ss +0Z00
end	string	+	Дата конца экспорта данных в формате уууу-мм-дд hh:mm:ss +0Z00

Пример ответа:

```
command finished{"client-request-id": "aee26a7c-52bd-4f58-bf07-de287dfcec56",
"command": "export_user_data", "msg": "ok", "elapsed_time": 2.443276695}
{
  "Response": {
    "changed": true,
    "failed": false,
    "msg": "ok"
  },
  "id": "792c03ce-55e6-4ae8-96c9-042b3f7e6389"
}
```

Терминология

Условимся называть ресурсом наиболее общую категорию экспортируемых данных. В нашем случае это:

- почтовый ящик;
- календарные события;
- календарные задачи;
- личная адресная книга (ЛАК).

Тогда объектом будем называть конечный элемент в этой категории, то есть для перечня выше будет соответственно:

- письмо;
- календарное событие;
- календарная задача;
- контакт ЛАК.

Перечисленные объекты помещены в подкаталоги внутри своих категорий. Один объект может быть ассоциирован с несколькими папками, например, письмо, как копия, существует в нескольких папках почтового ящика.

Письмо описывается двумя текстовыми файлами:

- `message_uuid.json` — описывает метаинформацию письма, включая специфичное для Mailion описание, например, папки хранения и флаги важности.
- `message_uuid.eml` — файл формата EML, можно открыть почтовым клиентом, например, **thunderbird**. Содержит в себе все встроенные/полноценные вложения в представлении BASE64.

Для каждого письма создается папка `attachments`, в которой сохраняются все вложения в оригинальном формате. Если вложений нет, то эта папка будет пустой.



При экспорте цепочек писем есть следующий нюанс: в цепочках каждое письмо выкачивается в виде EML-файла в отдельную папку, то есть признается отдельным объектом со своим UUID. При этом такой EML-файл содержит и предшествующие письма в переписке. Например, цепочка из трех писем $X \rightarrow Y \rightarrow Z$ экспортируется в три отдельные папки со следующими EML-файлами:

1. X
2. $X \rightarrow Y$
3. $X \rightarrow Y \rightarrow Z$

В файлах `messages_names.json` описывается соответствие между UUID писем и их краткой информацией. Такие файлы присутствуют во всех папках почтового ящика пользователя.

```
cat ./user@mln.example.net_53e90215-7d76-412a-9c6d-
b1968e0e10de/mail/Inbox/messages_names.json
// письма в папке Входящие

{
  "0c24cf50-268d-4a02-a182-5898c28ada37": "from:{name:"..." address:"..."}
to_me:true size_group:BIGGER subject_head:"Hello" has_attachments:true to:
{name:"..." address:"..."}",
  "f4c1447b-034d-457d-bdce-7c9ccdf05bf7": "from:{name:"..." address:"..."}
to_me:true size_group:SMALL subject_head:"Задачачи" to:{name:"..." address:"..."}"
}
```

Календарные события

```
└─ calendar
  │   └─ calendar_tags_list.json
  │   └─ Дом
  │       │   └─ 23b1cfc2-d30a-5566-8f6c-afee6cd5fe83
  │       │       │   └─ 23b1cfc2-d30a-5566-8f6c-afee6cd5fe83.json
  │       │       └─ attachments
  │       │           └─ Screenshot.png
  │       └─ events_names.json
  └─ Календарь
      │   └─ a414007b-b792-5e63-ab69-41c6998f3044
      │       │   └─ a414007b-b792-5e63-ab69-41c6998f3044.json
      │       └─ attachments
      └─ events_names.json
... ..
```

В папках `attachments` содержатся встроенные/полноценные вложения событий в оригинальном формате. Если вложений нет, то папка будет пустой.

Суть события описывается в одном текстовом JSON-файле, с UUID объекта в качестве имени.

Календарные задачи

```
... ..
└─ tasks
  │   └─ tasks_tag.json
  │   └─ Задачи
  │       │   └─ 698fa7db-dcb9-531e-92ef-c7b4d94ab261
  │       │       │   └─ 698fa7db-dcb9-531e-92ef-c7b4d94ab261.json
  │       └─ tasks_names.json
```

Суть задачи описывается в одном текстовом JSON-файле, с UUID объекта в качестве имени. Вложенная структура содержит только папку **Задачи**, других быть не может.

Личная адресная книга

```
├─ contacts
│  └─ lal_tags_tree.json
│     └─ Личная адресная книга
│        └─ 1e963cab-d7e5-4c39-bfd3-33b35cc4ab4a
│           └─ 1e963cab-d7e5-4c39-bfd3-33b35cc4ab4a.json
│              └─ avatar.png
│                 └─ contact.vcf
│                    └─ contacts_names.json
│                       └─ home
│                          └─ 8865f8c1-0808-4a5d-a52c-36a3f1c6694c
│                             └─ 8865f8c1-0808-4a5d-a52c-36a3f1c6694c.json
│                                └─ avatar.png
│                                   └─ contact.vcf
│                                      └─ contacts_names.json
│                                         └─ work
│                                            └─ 58ed8737-81c1-463e-87aa-823b2d3edf42
│                                               └─ 58ed8737-81c1-463e-87aa-823b2d3edf42.json
│                                                  └─ contact.vcf
│                                                     └─ contacts_names.json
└─ .....
```

Контакт описывается тремя файлами, последний из которых является необязательным:

- текстовый JSON-файл с внутренним описанием контакта;
- текстовый VCF-файл (VCARD) с описанием контакта; если есть аватар, то добавляется файл в формате BASE64;
- аватар в оригинальном формате.

Потоковая запись на диск

Загрузка содержимого ресурсов осуществляется путем записи на диск в потоковом режиме с фиксацией в файле `sync.state.export` идентификаторов (UUID) обработанных частей объекта. То есть, как только часть объекта получена, например, EML-файл с содержимым письма или файл вложения письма, она попадает на диск. Аналогично в потоковом режиме дополняется содержимое файла `export.log`.

Порядок выгрузки данных:

1. Личная адресная книга.
2. Календарные события.
3. Календарные задачи.
4. Почтовый ящик.

Получение данных не распараллелено, каждый объект ресурса выгружается последовательно.

Формирование архива

Процесс архивации в **tar.gz** запускается в самом конце, когда все ресурсы получены.

Следовательно, если процесс экспорта был по какой-то причине прерван в середине (процесс в терминах операционной системы), то архива с частично полученными ресурсами не будет.

5.3.10.2 Импорт данных пользователя

С помощью команды импорта данных пользователя администратор тенанта может импортировать ранее экспортированные данные для указанного пользователя.

Описание команды

В качестве входных данных для импорта через параметр `path` передается результат работы команды `export_user_data`, а именно — либо каталог с экспортированными данными, либо архив **tar.gz**. Оба варианта равносильны, тип поданной на вход сущности определяется автоматически.

У целевого пользователя воссоздается древо папок, которое было у экспортированного пользователя. Это касается всех ресурсов: почты, календарных событий и задач, личной адресной книги. Иначе говоря, если в экспортированных данных в папке `work` есть письмо, а у целевого пользователя такой папки в ящике нет, то перед импортом письма она будет создана. Если папка уже есть, то импорт будет осуществлен в нее. Даже если в папке нет объектов, она все равно будет создана.

Механизм **sync.state** учитывает уже созданные папки. В случае успеха в предыдущем запуске импорта попытка повторного создания проводиться не будет.

Пример команды:

```
nct_ministerium import_user_data \
--config ... \
--user 'user@mln.example.net' \
--path /tmp/ \
--start '2024-01-01 00:00:00 +0300' \
--end '2024-08-25 12:00:00 +0300'
```

Описание параметров команды приведено в таблице 43.

Таблица 43 — Параметры команды экспорта данных пользователя

Параметр	Тип	Обязательный	Описание
config	string	+	Путь к файлу конфигурации ministerium
user	string	+	Адрес пользователя, для которого импортируются данные

Параметр	Тип	Обязательный	Описание
path	string	+	Путь хранения экспортированных данных
start	string	+	Дата начала импорта данных в формате yyyy-mm-dd hh:mm:ss +0Z00
end	string	+	Дата конца импорта данных в формате yyyy-mm-dd hh:mm:ss +0Z00
state	string	+	Путь к журналам импорта и файлам sync-state-import

Пример ответа:

```
command finished{"client-request-id": "aee26a7c-52bd-4f58-bf07-de287dfcec56",
"command": "import_user_data", "msg": "ok", "elapsed_time": 2.443276695}
{
  "Response": {
    "changed": true,
    "failed": false,
    "msg": "ok"
  },
  "id": "792c03ce-55e6-4ae8-96c9-042b3f7e6389"
}
```

5.3.10.3 Общие детали по экспорту и импорту

Использование файлов sync.state.*

В ходе операций экспорта-импорта на диск записываются текстовые файлы `sync.state.*` в формате JSON, отражающие статус обработанных сущностей. У каждой из команд есть свой такой файл:

- для команды `export_user_data` — `sync.state.export`;
- для команды `import_user_data` — `sync.state.import`.

При повторном запуске той или иной команды выполняется попытка загрузить с диска соответствующий файл `sync.state.*`. Если файл существует, то из него считываются те объекты, которые были успешно обработаны при прошлом запуске. Таким образом, уже скачанные и импортированные объекты (письма, контакты, события и задачи календаря) пропускаются.

Конкретно у файла `sync.state.export` есть дополнительное назначение: для команды `import_user_data` он играет роль спецификатора сущностей-кандидатов к импорту. Именно из содержимого `sync.state.export` команда импорта получает информацию о том, какие данные нужно импортировать и где они находятся в архиве.

Структура файлов `sync.state.export` и `sync.state.import` **ВО МНОГОМ СХОДНА:**

```

{
  "lal_ctx": {
    "tags_tree_path": [ // Путь до файла с описанием древовидной структуры
      "contacts",
      "lal_tags_tree.json"
    ],
    "contacts": { // Перечисление контактов по их UUID с
      "1e963cab-d7e5-4c39-bfd3-33b35cc4ab4a": {
        ... ..
      },
      ... ..
    },
    "processing_resume": { // Резюме по обработанным контактам
      "main_content": {
        "Total": 3,
        "Skipped": 0,
        "Successted": 3,
        "Failed": 0
      }
    }
  },
  "calendar_ctx": { // Состояние по Календарю, то есть по Событиям и
    "tags_list_path": [ // Путь до файла с описанием древовидной структуры
      "calendar",
      "calendar_tags_list.json"
    ],
    "events": { // Перечисление событий по их UUID с результатами их
      "23b1cfc2-d30a-5566-8f6c-afee6cd5fe83": {
        ... ..
      },
      ... ..
    },
    "tasks_tag_path": [ // Путь до файла с описанием папки с Задачами
      "tasks",
      "tasks_tag.json"
    ],
    "tasks": { // Перечисление задач по их UUID с результатами их
      "698fa7db-dcb9-531e-92ef-c7b4d94ab261": {
        ... ..
      },
      ... ..
    },
    "processing_resume": { // Резюме по обработанным событиям и задачам
      "main_content": {
        "Total": 3,
        "Skipped": 0,
        "Successted": 3,
        "Failed": 0
      }
    }
  },
  "mail_ctx": {
    "tags_tree_path": [ // Путь до файла с описанием древовидной структуры
      "mail",
      "mail_tags_tree.json"
    ],
  },
}

```

```
"messages": { // Перечисление писем по их UUID с результатами их
обработки
  "0c24cf50-268d-4a02-a182-5898c28ada37": {
    ... ..
  },
  ... ..
},
"processing_resume": { // Резюме по обработанным письмам
  "main_content": {
    "Total": 5,
    "Skipped": 0,
    "Sucesssed": 5,
    "Failed": 0
  }
}
}
```

Поля для кодирования состояния объекта

Для кодирования состояния обработанной части объекта служит числовое поле `object_uuid.<object_part>.state`. Варианты `<object_part>` зависят от типа объекта, а именно:

У контакта ЛАК три составные части:

- `internal_content`
- `avatar`
- `vcard`

У события календаря две составные части:

- `internal_content`
- `attachments` (описывается массивом, у каждого элемента которого есть свои `uuid` и `state`)

У задачи календаря одна составная часть:

- `internal_content`

У письма три составные части:

- `internal_content`;
- `eml`;
- `attachments` (описывается массивом, у каждого элемента которого есть свой `uuid` и `state`).

Используются следующие коды состояний:

- 0 — состояние неизвестно;
- 1 — данная часть объекта не существует (например, отсутствие аватара у контакта);

- 2 — данная часть объекта обработана успешно;
- 3 — данная часть объекта обработана с ошибкой, подробности — в поле `contact_uuid.<object_part>.err_msg`.

Описание состояния на примерах

Контакт ЛАК:

```
"contacts": {
  "1e963cab-d7e5-4c39-bfd3-33b35cc4ab4a": {
    "internal_content": {
      "path": [ // Описывает путь до файла относительно корня
архива (оно же относительно корня папки с экспортированным контентом)
        "contacts",
        "Личная адресная книга",
        "1e963cab-d7e5-4c39-bfd3-33b35cc4ab4a",
        "1e963cab-d7e5-4c39-bfd3-33b35cc4ab4a.json"
      ],
      "state": {
        "code": 2,
        "code_msg": "Resource processed successfully"
      },
      "err_msg": ""
    },
    "avatar": {
      "path": [], // аналогично internal_content.path
      "state": {...}, // аналогично internal_content.state
      "err_msg": "... " // аналогично internal_content.err_msg
    },
    "vcard": {
      "path": [], // аналогично internal_content.path
      "state": {...}, // аналогично internal_content.state
      "err_msg": "... " // аналогично internal_content.err_msg
    },
    "contact_full_name": "Ivan Ivanov"
  },
  ... ..
}
```

Сообщение почтового ящика:

```

"messages": {
  "0c24cf50-268d-4a02-a182-5898c28ada37": {
    "internal_content": {
      "path": [
        "mail",
        "Inbox",
        "0c24cf50-268d-4a02-a182-5898c28ada37",
        "0c24cf50-268d-4a02-a182-5898c28ada37.json"
      ],
      "state": {
        "code": 2,
        "code_msg": "Resource processed successfully"
      },
      "err_msg": ""
    },
    "eml": {...}, // аналогично internal_content
    "summary": "message_id:\""..." created_at:{...} received_at:{...}
from:{...} to:{...} ...",
    "attachments": {
      "3-1.pdf": {
        "path": [
          "mail",
          "Inbox",
          "0c24cf50-268d-4a02-a182-5898c28ada37",
          "attachments",
          "3-1.pdf"
        ],
        "state": {
          "code": 2,
          "code_msg": "Resource processed successfully"
        },
        "err_msg": ""
      },
      "Screenshot from 2024-06-04 11-29-50.png": {...} // аналогично
примеру выше
    }
  },
  ... ..
},

```

5.3.10.4 Прочие аспекты экспорта/импорта

Журналирование хода операций в консоли и файле

Информация о ходе выполнения выводится в `STDERR`, равно как и в файл журнала в режиме добавления (*appending*). В самом конце небольшое сообщение с результатом выводится в `STDOUT`.

Основную ценность для анализа результатов экспорта/импорта представляют файлы `sync.state.[export|import]` и `[export|import].logs`, а также вывод консоли. Вывод консоли несколько обширней содержимого файлов.

Межинсталляционная работа команд

Реализована работа между инсталляциями Mailion, иначе говоря, возможны:

- экспорт из одной и импорт в ту же инсталляцию;

- между одним и тем же пользователем;
- от одного пользователя к другому;
- экспорт из одной и импорт в другую инсталляцию.

Обработка сигнала SIGINT (CTRL-C) для остановки работы

Утилита **ministerium**, в целом, и команды экспорта/импорта, в частности, игнорируют сигнал SIGINT.



Для прерывания работы можно использовать SIGKILL или сочетание клавиш CTRL-Z. Продолжить работу с точки остановки можно за счет механизма **sync.state**.

5.4 Создание пользовательских GAL-тегов



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 44.

Таблица 44 — Параметры запроса на получение созданного пользователя по его идентификатору

Параметр	Тип	Обязательный	Описание
config	Str	+	Конфигурационный файл с параметрами сервиса Сох 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

Параметр	Тип	Обязательный	Описание
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**.

5.5 Работа с импортированными контактами

5.5.1 Импорт 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 45.

Таблица 45 — Параметры 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	+	Конечная точка балансировщика нагрузки сервиса
cox.compression	Str	+	Метод сжатия данных (варианты: none , gzip), по умолчанию — none
cox.endpoint	Str	+	Конечная точка сервиса
cox.load_balanced	Bool	+	Балансировщик нагрузки сервиса
cox.request_timeout	Str	+	Таймаут 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 СА 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"
}
```

5.5.2 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_cert.pem \
--tls_settings.key_file /***/client_key.pem \
--v
```

Описание параметров запроса на удаление импортированных контактов приведено в таблице 46.

Таблица 46 — Параметры запроса на удаление импортированных контактов

Параметр	Тип	Обязательный	Описание
admin.login	Str	+	Логин администратора тенанта
admin.password	Str	+	Пароль администратора тенанта

Параметр	Тип	Обязательный	Описание
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	+	Конечная точка балансировщика нагрузки сервиса
cox.compression	Str	+	Метод сжатия данных (варианты: none , gzip), по умолчанию — none
cox.endpoint	Str	+	Конечная точка сервиса
cox.load_balanced	Bool	+	Балансировщик нагрузки сервиса
cox.request_timeout	Str	+	Таймаут 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 СА 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"
}
```

5.5.3 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 47.

Таблица 47 — Параметры 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	+	Конечная точка балансировщика нагрузки сервиса
cox.compression	Str	+	Метод сжатия данных (варианты: none , gzip), по умолчанию — none
cox.endpoint	Str	+	Конечная точка сервиса
cox.load_balanced	Bool	+	Балансировщик нагрузки сервиса
cox.request_timeout	Str	+	Таймаут 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 СА 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": "0e3ablef-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"
        }
    ]
}
]
}
}

```

5.6 Настройка двухфакторной аутентификации



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 48.

Таблица 48 — Параметры исключения пользователя

Параметр	Тип	Обязательный	Описание
admin.login	Str	+	Логин администратора тенанта

Параметр	Тип	Обязательный	Описание
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 lddccc69-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 49.

Таблица 49 — Параметры двухфакторной аутентификации тенанта

Параметр	Тип	Обязательный	Описание
config	Str	+	Конфигурационный файл с параметрами сервиса Сох 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
tenant_id	Str	+	Идентификатор тенанта
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)



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 50.

Таблица 50 — Параметры двухфакторной аутентификации тенанта

Параметр	Тип	Обяз.	Описание
config	string	+	Конфигурационный файл с параметрами сервиса Сох и настройками tls. Формируется автоматически на сервере с ролью ucs_infrastructure и находится по пути /srv/ministerium/config.json
admin.login	string	+	Логин администратора тенанта
admin.password	string	+	Пароль администратора тенанта
entity_id	string	+	Идентификатор пользователя, для которого необходимо сбросить второй фактор

Пример ответа:

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

5.7 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 51.

Таблица 51 — Параметры запроса на создание домена без делегирования

Параметр	Тип	Обязательный	Описание
config	Str	+	Конфигурационный файл с параметрами сервиса Сох 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 52.

Таблица 52 — Параметры запроса на получение параметров созданного домена

Параметр	Тип	Обязательный	Описание
config	Str	+	Конфигурационный файл с параметрами сервиса Сох 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
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 53.

Таблица 53 — Параметры 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 54.

Таблица 54 — Параметры запроса на создание домена с делегированием

Параметр	Тип	Обяз.	Описание
config	string	+	Конфигурационный файл с параметрами сервиса Сох и настройками tls. Формируется автоматически на сервере с ролью ucs_infrastructure и находится по пути /srv/ministerium/config.json

Параметр	Тип	Обяз.	Описание
admin.login	string	+	Логин администратора тенанта
admin.password	string	+	Пароль администратора тенанта
tenant_id	string	+	Идентификатор тенанта
hostname	string	-	Имя домена
features.is_authorization	boolean	+	Если значение true, домен можно использовать для авторизации
features.is_mail	boolean	+	Если значение true, домен может принимать почтовые сообщения
features.is_service	boolean	+	Если значение true, домен можно использовать для авторизации по умолчанию
features.is_delegated	boolean	-	Если значение true, домен делегирован внешней системе
external.delegate_id	string	-	Идентификатор делегата, используемый для внешней авторизации
external.domain_alias	string	-	Имя контроллера делегируемого домена
external.default_region_id	string	-	Идентификатор региона по умолчанию для автоматического создания пользователей

Пример ответа:

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

5.8 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 57). Объект Организационной структуры необходимо создать для получения возможности создания объектов **Организаций**.



Рисунок 57 – Примерная схема организационной структуры



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 55.

Таблица 55 — Параметры запроса на создание оргструктуры

Параметр	Тип	Обязательный	Описание
config	Str	+	Конфигурационный файл с параметрами сервиса Сох и настройками TLS. Формируется автоматически на сервере с ролью ucs_infrastructure и находится по пути <code>/srv/ministerium/config.json</code>
admin.login	Str	+	Логин администратора тенанта
admin.password	Str	+	Пароль администратора тенанта
element	Str	+	Элемент организационной структуры для сохранения. Требуемые поля: <ul style="list-style-type: none"> – <code>ORG_STRUCTURE(id, tenant_id, name, description)</code>, – <code>ORGANIZATION(id, tenant_id, name, type, description, logo_identifier, address, phone, countries, leaders, avatar)</code>, – <code>UNIT(id, tenant_id, name, type, description, address, phone, leaders, avatar)</code>, – <code>GROUP(same with unit)</code>, – <code>OCCUPATION(id, tenant_id, name, description, org_group, org_unit, organization)</code>, – <code>COMPETENCE(id, tenant_id, name, description, qualifications)</code>
element_type	Str	+	Тип элемента в организационной структуре 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 56.

Таблица 56 — Параметры запроса на установку связи с тенантом

Параметр	Тип	Обязательный	Описание
config	Str	+	Конфигурационный файл с параметрами сервиса Сох и настройками TLS. Формируется автоматически на сервере с ролью ucs_infrastructure и находится по пути <code>/srv/ministerium/config.json</code>
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.

5.9 Создание организации

Администратор может создать несколько организаций.



В рамках одной оргструктуры нельзя создать организации с одинаковым названием.

Удалить организацию нельзя до тех пор, пока все входящие в нее организационные единицы или группы не будут удалены.



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_cert.pem \
--tls_settings.key_file /builds/0/mail-back-tests/certs/client_key.pem

```

Описание параметров запроса приведено в таблице 57.

Таблица 57 — Параметры 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	+	Конечная точка балансировщика нагрузки сервиса
cox.compression	Str	+	Метод сжатия данных (варианты: none , gzip), по умолчанию — none
cox.endpoint	Str	+	Конечная точка сервиса
cox.load_balanced	Bool	+	Балансировщик нагрузки сервиса
cox.request_timeout	Str	+	Таймаут 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

Параметр	Тип	Обязательный	Описание
<code>tls_settings.ca_file</code>	Bool	+	Путь к СА файлу
<code>tls_settings.client_cert_file</code>	Str	+	Путь к файлу сертификата клиента
<code>tls_settings.key_file</code>	Str	+	Путь к файлу с ключом клиента

Пример ответа:

```
{
  "Response": {
    "msg": "ok",
    "changed": true
  },
  "Id": "e7057610-b04d-4528-9218-db3e7b229fd5"
}
```

5.10 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;
- добавление электронной почты;
- создание логина;
- создание пароля и токена к логину;
- 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
--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 58.

Таблица 58 — Параметры 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
profile.first_name	Str	+	Имя создаваемого пользователя
profile.last_name	Str	+	Фамилия создаваемого пользователя
cox.balancer_endpoint	Str	+	Конечная точка балансировщика нагрузки сервиса
cox.compression	Str	+	Метод сжатия данных (варианты: none , gzip), по умолчанию — none
cox.endpoint	Str	+	Конечная точка сервиса
cox.load_balanced	Bool	+	Балансировщик нагрузки сервиса
cox.request_timeout	Str	+	Таймаут 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
tls_settings.ca_file	Str	+	Путь к СА файлу
tls_settings.client_cert_file	Str	+	Путь к файлу сертификата клиента
tls_settings.key_file	Str	+	Путь к файлу с ключом клиента



На первом шаге создается объект (пользователь). В случае ошибки при выполнении данного шага следующие запросы также не будут выполнены.

2. Добавление электронной почты:

```
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_cert.pem \
--tls_settings.key_file /home/ps/work/first/mail-back-tests/certs/client_key.pem
```

Описание параметров запроса приведено в таблице 59.

Таблица 59 — Параметры запроса на добавление электронной почты

Параметр	Тип	Обязательный	Описание
admin.login	Str	+	Логин администратора тенанта
admin.password	Str	+	Пароль администратора тенанта
entity_id	Str	+	Идентификатор пользователя

Параметр	Тип	Обязательный	Описание
cox.balancer_endpoint	Str	+	Конечная точка 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 СА 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 60.

Таблица 60 — Параметры 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 61.

Таблица 61 — Параметры 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_cr1.pem
--tls_settings.key_file /home/ps/work/first/mail-back-tests/certs/client_key.pem
```

Описание параметров запроса приведено в таблице 62.

Таблица 62 — Параметры 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

Параметр	Тип	Обязательный	Описание
gal_tags	Str	+	Список идентификаторов ГАК
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	+	Код языка 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	+	Конечная точка балансировщика нагрузки сервиса
cox.compression	Str	+	Метод сжатия данных (варианты: none , gzip), по умолчанию — none
cox.endpoint	Str	+	Конечная точка сервиса
cox.load_balanced	Bool	+	Балансировщик нагрузки сервиса

Параметр	Тип	Обязательный	Описание
<code>cox.request_timeout</code>	Str	+	Таймаут запроса к сервису
<code>cox.service_name</code>	Str	+	Имя сервиса
<code>cox.use_tls</code>	Bool	+	TLS-сертификат
<code>cox.use_tls_balancer</code>	Bool	+	Защищенная передача данных при подключении к балансировщику
<code>tls_settings.ca_file</code>	Str	+	Путь к СА файлу
<code>tls_settings.client_cert_file</code>	Str	+	Путь к файлу сертификата клиента
<code>tls_settings.key_file</code>	Str	+	Путь к файлу с ключом клиента

6. Активация:

```
nct_ministerium change_status
--entity_id <entity_id>
--status <status> ...
```

Описание параметров запроса приведено в таблице 63.

Таблица 63 — Параметры запроса на активацию

Параметр	Тип	Обязательный	Описание
<code>entity_id</code>	Str	+	Идентификатор статуса
<code>status</code>	Str	+	Статус



У несозданных объектов необходимо вручную выполнить те запросы, которые остались невыполненными автоматически.

5.11 Ограничение бронирования списком пользователей

Добавление 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 64.

Таблица 64 — Параметры запроса добавления пользователей и групп

Параметр	Тип	Обязательный	Описание
config	Str	+	Конфигурационный файл
entity_ids	Str	+	Список идентификаторов пользователей и групп для добавления
resource_id	Str	+	Идентификатор ресурса

Удаление 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 65.

Таблица 65 — Параметры запроса удаления пользователей и групп

Параметр	Тип	Обязательный	Описание
config	Str	+	Конфигурационный файл
entity_ids	Str	+	Список идентификаторов пользователей и групп для удаления
resource_id	Str	+	Идентификатор ресурса

Получение списка 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 66.

Таблица 66 — Параметры запроса получения списка пользователей и групп

Параметр	Тип	Обязательный	Описание
config	Str	+	Конфигурационный файл

Параметр	Тип	Обязательный	Описание
resource_id	Str	+	Идентификатор ресурса

5.12 Делегирование управления группами

Администратор тенанта может передать произвольному пользователю права на управление составом участников и редактирование данных группы.

Для этого необходимо выполнить запрос на предоставление прав управления 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@inst
allation.exaple.net, autotest_1680079682.528347@installation.exaple.net, autotest_16
80079359.89922@installation.exaple.net, autotest_1680079373.50339@installation.exap
le.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, GR
OUP 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 67.

Таблица 67 — Параметры запроса на предоставление прав управления 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

Параметр	Тип	Обязательный	Описание
			пользователю/пользователям
sharing_roles		+	<p>Выбор из разрешенных к назначению ролей:</p> <ul style="list-style-type: none"> – GROUP_EDITOR (Редактор группы); – GROUP_ADMINISTRATOR (Администратор группы) <p>В релизе 1.7 обе представленные роли позволяют делегировать произвольному пользователю права на управление составом участников и редактирование данных группы</p>
cox.balancer_endpoint	Str	+	Конечная точка балансировщика нагрузки сервиса
cox.compression	Str	+	Метод сжатия данных (варианты: none , gzip), по умолчанию — none
cox.endpoint	Str	+	Конечная точка сервиса
cox.load_balanced	Bool	+	Балансировщик нагрузки сервиса
cox.request_timeout	Str	+	Таймаут 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 СА файлу
tls_settings.client_certificate	Str	+	Путь к файлу сертификата клиента
tls_settings.key_file	Str	+	Путь к файлу с ключом клиента



При делегировании управления группой нескольким пользователям необходимо указать такое же количество ролей в соответствующем порядке.

Пример ответа:

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



Процесс выдачи прав на управление группой может занять до одной минуты. После этого 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 68.

Таблица 68 — Параметры 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



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"
  }
}
```

5.13 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 69.

Таблица 69 — Параметры запроса на создание организационной группы

Параметр	Тип	Обязательный	Описание
config	Str	+	Конфигурационный файл с параметрами сервиса Сох 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	+	Список идентификаторов ГАК
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": "a4fld34a-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 a4fld34a-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 70.

Таблица 70 — Параметры запроса на создание динамической группы

Параметр	Тип	Обязательный	Описание
config	Str	+	Конфигурационный файл с параметрами сервиса Сох 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
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».



Если в массиве есть хотя бы один оператор `or`, то условия объединяются в группы по правилам приоритетности логических операций. При этом список все равно 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  
}
```

5.14 Массовое создание пользователей в каталоге



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 2).
- 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 [Подготовка файла импорта](#).



Перед импортом для каждого отдельного пользователя система выполняет поиск пользователя по почтовым адресам (**emails**) и логинам (**logins**). Если найдено совпадение, то вместо создания нового пользователя выполняется обновление данных. Обновляются все поля пользователя, за исключением 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 71.

Таблица 71 — Параметры запроса на импорт пользователей

Параметр	Тип	Обязательный	Описание
config	Str	+	Конфигурационный файл с параметрами сервиса Сох 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 2).



Процедура импорта будет возможна если все пользователи в файле импорта пройдут проверку по этой схеме.

Описание параметров запроса приведено в таблице 72.

Таблица 72 — Параметры запроса на проверку файла импорта, конфигурации и подключения к ПО «Mailion»

Параметр	Тип	Обязательный	Описание
config	Str	+	Конфигурационный файл с параметрами сервиса Сох 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"
    }
  ]
}
```



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 73.

Таблица 73 — Параметры запроса на получение GAL-тегов тенанта

Параметр	Тип	Обязательный	Описание
config	Str	+	Конфигурационный файл с параметрами сервиса Сох 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 Б (см. раздел [Список глобальных адресных книг](#)).

5.14.1 Подготовка файла импорта



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 74.

Таблица 74 — Параметры 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
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

Параметр	Тип	Обязательный	Описание
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
logins	Str	+	Список логинов пользователя
logins.login	Str	+	Логин
logins.password	Str	+	Пароль



Каждый отдельный пользователь проверяется по JSON схеме записи пользователя, приведенной в приложении (см. раздел [Схема записи пользователя в Приложении 2](#)).

Файл импорта в формате CSV позволяет импортировать пользователей с ограниченным набором данных.

Описание параметров файла импорта **user_profiles.csv** приведено в таблице 75.

Таблица 75 — Параметры 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

5.14.2 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 76.

Таблица 76 — 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 2)
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

5.14.3 Возможные ошибки при импорте пользователей

Описания возможных ошибок при импорте пользователя приведены в таблице 77.

Таблица 77 — Описание возможных ошибок

Название ошибки	Вид в интерфейсе командной строки	Описание
Ошибка декодирования JSON	<pre>{ "msg": "import file validation: decode next user: decode JSON: invalid character '}' looking for beginning of value", "failed": true }</pre>	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	<pre>{ "msg": "import file validation: user correlation ID: : correlation_id: String length must be greater than or equal to 1", "failed": true }</pre>	Сообщение транслирует информацию о том, что обязательное поле "correlation_id" отсутствует или имеет пустое значение
Ошибка в адресе электронной почты	<pre>{ "msg": "import file validation: user correlation ID: f1b97e81-e4a3-4ebd-ba59-e4b864ef4797: emails.0.email: Does not match format 'email'", "failed": true }</pre>	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	<pre>{ "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 }</pre>	Аналогично предыдущему примеру, но отсутствует поле "login" у первой структуры в списке логинов (logins)
Ошибка, дубликат электронного адреса	<pre>{ "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 }</pre>	<p>Еще один пример проверки, выполняемой перед отправкой файла импорта на сервер.</p> <p>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".</p>

Название ошибки	Вид в интерфейсе командной строки	Описание
		Необходимо исправить электронный адрес у одного из пользователей
<p>Ошибка возникшая в процессе импорта пользователя на стороне сервера</p>	<pre>\$ 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"} 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",</pre>	<p>Пример ошибки, возникшей в процессе импорта пользователя на стороне сервера, например по причине отказа сетевого окружения</p>

Название ошибки	Вид в интерфейсе командной строки	Описание
	<pre>"changed": true }] }</pre>	
	<pre>user error</pre>	<p>В этом сообщении говорится о том, что пользователь с идентификатором, указанным в поле "correlation_id" не был импортирован.</p> <p>На это указывает маркер "error" в поле "status" и наличие поля "error", которое содержит сообщение об ошибке со стороны системы.</p> <p>Соответственно этот пользователь будет добавлен в файл, указанный в параметре "rejected_users_path" или в файл с именем по умолчанию</p>
<p>Ошибка проверки кода языка в записи пользователя</p>	<pre>{ "msg": "import file validation: user correlation ID: f1b97e81-e4a3-4ebd-ba59-e4b864ef4797, check user locale: language: tag is not well-formed", "failed": true }</pre>	<p>Пример ошибки, которая выдается если код языка (locale) в записи пользователя не задан или задан некорректно. Пример правильного значения: ru_RU, en_US</p>

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**.



Пользователи не импортированные в систему или частично импортированные 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**.

5.15 Массовое создание групп в каталоге



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 или созданного любым другим способом.

Импорт групп из файла в систему осуществляется в два этапа:

- непосредственно [импорт групп](#);
- [импорт связей](#) данных групп.

5.15.1 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 2).
- Файл импорта, содержащий импортируемые в систему группы, в формате JSON (**groups.json**) или CSV (**groups.csv**). Пример заполняемых полей в файлах приведен в разделе [Подготовка файла импорта](#).



Перед импортом для каждой отдельной группы система выполняет поиск группы по почтовым адресам (emails) и логинам (logins). Если найдено совпадение, то вместо создания новой группы выполняется обновление данных. Обновляются все поля группы, за исключением адресов и логинов — они будут добавлены. В результате импорта основной адрес также может измениться 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 78.

Таблица 78 — Параметры запроса на импорт групп

Параметр	Тип	Обязательный	Описание
config	Str	+	Конфигурационный файл с параметрами сервиса Сох 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 2).



Процедура импорта будет возможна если все группы в файле импорта пройдут проверку по этой схеме.

Описание параметров запроса приведено в таблице 79.

Таблица 79 — Параметры запроса на проверку файла импорта, конфигурации и подключения к ПО «Mailion»

Параметр	Тип	Обязательный	Описание
config	Str	+	Конфигурационный файл с параметрами сервиса Sox 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"
    }
  ]
}
```

```
}
```



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 80.

Таблица 80 — Параметры запроса на получение GAL-тегов тенанта

Параметр	Тип	Обязательный	Описание
config	Str	+	Конфигурационный файл с параметрами сервиса Сох 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 2).

5.15.2 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 2).
 - 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 [Подготовка файла импорта](#).
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 81.

Таблица 81 — Параметры запроса на импорт связей групп

Параметр	Тип	Обязательный	Описание
<code>config</code>	Str	+	Конфигурационный файл с параметрами сервиса Сох и настройками tls. Формируется автоматически на сервере с ролью <code>ucs_infrastructure</code> и находится по пути <code>/srv/ministerium/config.json</code>

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 2).



Процедура импорта будет возможна если все связи групп в файле импорта пройдут проверку по этой схеме.

Описание параметров запроса приведено в таблице 82.

Таблица 82 — Параметры запроса на проверку файла импорта, конфигурации и подключения к ПО «Mailion»

Параметр	Тип	Обязательный	Описание
config	Str	+	Конфигурационный файл с параметрами сервиса Сох 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"
    }
  ]
}

```

5.15.3 Подготовка файла импорта

Формат JSON является основным для системы и позволяет наиболее полно описать группу.

Описание параметров файла импорта **groups.json** приведено в таблице 83.

Таблица 83 — Параметры 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 84.

Таблица 84 — Параметры 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

Параметр	Обязательный	Описание
		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

5.15.4 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 85.

Таблица 85 — 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 2)
import procedure summary	Итог импорта, сообщает количество групп, которые были обработаны системой, количество групп с ошибками и количество успешно импортированных групп

5.15.5 Возможные ошибки при импорте групп

Описания возможных ошибок при импорте групп приведены в таблице 86

Таблица 86 — Описание возможных ошибок

Название ошибки	Вид в интерфейсе командной строки	Описание
Ошибка декодирования JSON	<pre>{ "msg": "import file validation: decode next group: decode JSON: invalid character '}' looking for beginning of value", "failed": true }</pre>	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	<pre>{ "msg": "import file validation: group correlation ID: : correlation_id: String length must be greater than or equal to 1", "failed": true }</pre>	Сообщение транслирует информацию о том, что обязательное поле "correlation_id" отсутствует или имеет пустое значение
Ошибка в адресе электронной почты	<pre>{ "msg": "import file validation: group correlation ID: f1b97e81-e4a3-4ebd-ba59-e4b864ef4797: emails.0.email: Does not match format 'email'", "failed": true }</pre>	Сообщение выводится в случае, если группа с идентификатором (correlation_id) "f1b97e81-e4a3-4ebd-ba59-e4b864ef4797" не прошла проверку по схеме
Ошибка в логине	<pre>{ "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 }</pre>	Аналогично предыдущему примеру, но отсутствует поле "login" у первой структуры в списке логинов (logins)
Ошибка, дубликат электронного адреса	<pre>{ "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 }</pre>	<p>Еще один пример проверки, выполняемой перед отправкой файла импорта на сервер.</p> <p>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".</p> <p>Необходимо исправить электронный адрес у одного из пользователей</p>

Название ошибки	Вид в интерфейсе командной строки	Описание
<p>Ошибка, возникшая в процессе импорта группы на стороне сервера</p>	<pre>\$ 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- 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 }] }</pre>	<p>Пример ошибки возникшей в процессе импорта группы на стороне сервера, например по причине отказа сетевого окружения</p>
	<pre>group error</pre>	<p>В этом сообщении говорится о том, что группа с идентификатором,</p>

Название ошибки	Вид в интерфейсе командной строки	Описание
		<p>указанным в поле "correlation_id" не была импортирована.</p> <p>На это указывает маркер "error" в поле "status" и наличие поля "error", которое содержит сообщение об ошибке со стороны системы.</p> <p>Соответственно эта группа будет добавлена в файл, указанный в параметре "rejected_groups_path" или в файл с именем по умолчанию</p>

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**.



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**.

5.15.6 Автоматизация переноса групп и их связей из LDAP-каталогов в 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
```



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:: WjCo03Tf40GU0w9s8N+ytw==
objectSid:: AQUAAAAAAAAUVAANAUVUO/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](#) и [import_groups_links](#) соответственно.

5.16 Массовое создание ресурсов в каталоге



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 2).

- Файл импорта, содержащий импортируемых в систему пользователей, в формате JSON (**resources.json**) или CSV (**resources.csv**). Пример заполняемых полей в файле приведен в разделе [Подготовка файла импорта](#).



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 87.

Таблица 87 — Параметры запроса на импорт ресурсов

Параметр	Тип	Обязательный	Описание
config	Str	+	Конфигурационный файл с параметрами сервиса Сох 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 2).



Ресурс не будет успешно импортирован, если он не удовлетворяет этой схеме.

Описание параметров запроса приведено в таблице 88.

Таблица 88 — Параметры запроса на проверку файла импорта, конфигурации и подключения к ПО «Mailion»

Параметр	Тип	Обязательный	Описание
config	Str	+	Конфигурационный файл с параметрами сервиса Сох 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"
    }
  ]
}
```



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 89.

Таблица 89 — Параметры запроса на получение GAL-тегов тенанта

Параметр	Тип	Обязательный	Описание
config	Str	+	Конфигурационный файл с параметрами сервиса Сох 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 2).

5.16.1 Подготовка файла импорта



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 90.

Таблица 90 — Параметры 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
zip_code	Str	-	Индекс
floor	Str	-	Этаж

Параметр	Тип	Обязательный	Описание
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



Каждый отдельный объект ресурса проверяется по JSON схеме записи пользователя, приведенной в приложении (см. раздел [Схема записи ресурса](#) в Приложении 2).

Файл импорта в формате CSV позволяет импортировать объекты ресурсов с ограниченным набором данных.

Описание параметров файла импорта **user_profiles.csv** приведено в таблице 91.

Таблица 91 — Параметры 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

5.16.2 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 92.

Таблица 92 — 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 «ок» 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

5.16.3 Возможные ошибки при импорте объектов ресурсов

Описания возможных ошибок при импорте объектов ресурсов приведены в таблице 93

Таблица 93 — Описание возможных ошибок

Название ошибки	Вид в интерфейсе командной строки	Описание
Ошибка декодирования JSON	<pre>{ "msg": "import file validation: decode next user: decode JSON: invalid character '}' looking for beginning of value", "failed": true }</pre>	Сообщение выводится в случае, если утилита не может декодировать файл импорта, в этом случае необходимо проверить корректность синтаксиса JSON или CSV
Повторяющийся correlation ID	<pre>{ "changed": false, "failed": true, "msg": "import file validation: duplicate correlation_id found: 00025fe9-1fb5-4fda-a6ac-c8fb5572b88f" }</pre>	Сообщение выводится в случае, если две записи ресурса в файле имеют одинаково заполненное поле correlation ID
Пустой correlation ID	<pre>{ "changed": false, "failed": true, "msg": "import file validation: resource correlation ID: : resource CorrelationId is empty" }</pre>	Сообщение выводится в случае, если поле correlationID не заполнено
Ошибка создания Email	<pre>{ "Response": { "changed": true, "failed": false, "msg": "ok" }, "responses": [</pre>	Сообщение выводится в случае ошибки создания Email

Название ошибки	Вид в интерфейсе командной строки	Описание
	<pre>{ "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" }] }</pre>	

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**.



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**.

5.17 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 <...> \  
--status <...> ...
```

Описание параметров запроса приведено в таблице 94.

Таблица 94 — Параметры запроса на смену статуса объекта

Параметр	Тип	Обязательный	Описание
entity_id	Str	+	Идентификатор пользователя
status	Str	+	Запрашиваемый статус, в данном случае MARK_DELETED.



Сущность будет помечена на удаление и впоследствии будет удалена в соответствии с политикой хранения для механизма сбора мусора (garbage collector).

5.18 Управление делегированием учетных записей



Управление доступом к почте пользователя выполняется пользователем с ролью администратора тенанта.

Предоставление доступа к почте пользователя может быть выполнено с разными уровнями доступа. При выполнении запроса на доступ к почте задается с помощью параметра **permissions_by_emails**, при этом существует три уровня доступа:

- 0 — уровень доступа с правами «Не может» (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 «Отправить как» (SendAs). Пользователь, которому предоставлены права доступа к почте, получает права совладельца на все почтовые папки, календари и адресные книги, также он может отправлять письма с делегированной учетной записи.

5.18.1 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 95.

Таблица 95 — Параметры запроса на доступ к почте пользователя с правами «Не может» (Cannot)

Параметр	Тип	Обязательный	Описание
admin.login	Str	+	Логин администратора тенанта
admin.password	Str	+	Пароль администратора тенанта
cox.balancer_endpoint	Str	+	Конечная точка балансировщика нагрузки сервиса
cox.compression	Str	+	Метод сжатия данных (варианты: none , gzip), по умолчанию — none
cox.endpoint	Str	+	Конечная точка сервиса
cox.load_balanced	Bool	+	Балансировщик нагрузки сервиса
cox.request_timeout	Str	+	Таймаут 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 может» (Cannot), 1 — разрешение «От имени» (OnBehalf), 2 — разрешение «Отправить как» (SendAs)
tls_settings.ca_file	Str	+	Путь к СА 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"
  }
}
```

5.18.2 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 96.

Таблица 96 — Параметры 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	+	Конечная точка балансировщика нагрузки сервиса

Параметр	Тип	Обязательный	Описание
cox.compression	Str	+	Метод сжатия данных (варианты: none , gzip), по умолчанию — none
cox.endpoint	Str	+	Конечная точка сервиса
cox.load_balanced	Bool	+	Балансировщик нагрузки сервиса
cox.request_timeout	Str	+	Таймаут 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 может» (Cannot), 1 — разрешение «От имени» (OnBehalf), 2 — разрешение «Отправить как» (SendAs).
tls_settings.ca_file	Str	+	Путь к СА 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"
  }
}
```

5.18.3 Предоставление доступа к почте пользователя с правами «Напрямую»

Для предоставления доступа к почте пользователя с правами «Отправить как» (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 97.

Таблица 97 — Параметры запроса на доступ к почте пользователя с правами «Отправить как» (SendAs)

Параметр	Тип	Обязательный	Описание
admin.login	Str	+	Логин администратора тенанта
admin.password	Str	+	Пароль администратора тенанта
cox.balancer_endpoint	Str	+	Конечная точка балансировщика нагрузки сервиса
cox.compression	Str	+	Метод сжатия данных (варианты: none , gzip), по умолчанию — none
cox.endpoint	Str	+	Конечная точка сервиса
cox.load_balanced	Bool	+	Балансировщик нагрузки сервиса
cox.request_timeout	Str	+	Таймаут запроса к сервису
cox.service_name	Str	+	Имя сервиса
cox.use_tls	Bool	+	TLS-сертификат

Параметр	Тип	Обязательный	Описание
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 может» (Cannot), 1 — разрешение «От имени» (OnBehalf), 2 — разрешение «Отправить как» (SendAs)
tls_settings.ca_file	Str	+	Путь к СА 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"
  }
}
```

5.18.4 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 98.

Таблица 98 — Параметры 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	+	Конечная точка балансировщика нагрузки сервиса
cox.compression	Str	+	Метод сжатия данных (варианты: none , gzip), по умолчанию — none
cox.endpoint	Str	+	Конечная точка сервиса
cox.load_balanced	Bool	+	Балансировщик нагрузки сервиса
cox.request_timeout	Str	+	Таймаут 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 СА 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"
  }
}
```

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 99.

Таблица 99 — Параметры 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	+	Конечная точка балансировщика нагрузки сервиса
cox.compression	Str	+	Метод сжатия данных (варианты: none , gzip), по умолчанию — none
cox.endpoint	Str	+	Конечная точка сервиса
cox.load_balanced	Bool	+	Балансировщик нагрузки сервиса

Параметр	Тип	Обязательный	Описание
cox.request_timeout	Str	+	Таймаут 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 СА 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
}
```

5.18.5 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 100.

Таблица 100 — Параметры 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	+	Конечная точка балансировщика нагрузки сервиса
cox.compression	Str	+	Метод сжатия данных (варианты: none , gzip), по умолчанию — none
cox.endpoint	Str	+	Конечная точка сервиса
cox.load_balanced	Bool	+	Балансировщик нагрузки сервиса
cox.request_timeout	Str	+	Таймаут 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 СА 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"
  }
}
```

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 101.

Таблица 101 — Параметры 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	+	Конечная точка балансировщика нагрузки сервиса
cox.compression	Str	+	Метод сжатия данных (варианты: none , gzip), по умолчанию — none
cox.endpoint	Str	+	Конечная точка сервиса

Параметр	Тип	Обязательный	Описание
cox.load_balanced	Bool	+	Балансировщик нагрузки сервиса
cox.request_timeout	Str	+	Таймаут 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 СА 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
}

```

5.18.6 Просмотр всех делегатов

Чтобы увидеть всех пользователей, которым делегирована учетная запись выбранного пользователя необходимо выполнить следующие действия:

1. Выполнить запрос на проверку всех пользователей, которым делегирована учетная запись выбранного пользователя:

```

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 102.

Таблица 102 — Параметры запроса на проверку всех пользователей, которым делегирована учетная запись

Параметр	Тип	Обязательный	Описание
admin.login	Str	+	Логин администратора тенанта

Параметр	Тип	Обязательный	Описание
admin.password	Str	+	Пароль администратора тенанта
cox.balancer_endpoint	Str	+	Конечная точка балансировщика нагрузки сервиса
cox.compression	Str	+	Метод сжатия данных (варианты: none , gzip), по умолчанию — none
cox.endpoint	Str	+	Конечная точка сервиса
cox.load_balanced	Bool	+	Балансировщик нагрузки сервиса
cox.request_timeout	Str	+	Таймаут 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
}
```

5.18.7 Просмотр всех делегированных учетных записей

Чтобы увидеть все делегированные учетные записи необходимо выполнить следующие действия:

1. 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 103.

Таблица 103 — Параметры 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	+	Конечная точка балансировщика нагрузки сервиса
cox.compression	Str	+	Метод сжатия данных (варианты: none , gzip), по умолчанию — none
cox.endpoint	Str	+	Конечная точка сервиса
cox.load_balanced	Bool	+	Балансировщик нагрузки сервиса
cox.request_timeout	Str	+	Таймаут 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 пользователя
tls_settings.ca_file	Str	+	Путь к СА 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
}
```

5.19 Поиск писем по заданным критериям



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_cert
.pem \
--tls_settings.key_file /home/user/ministerium_certs/installation/client_key.pem \
```

Описание параметров поиска приведено в таблице 104.

Таблица 104 — Параметры поиска письма по заданным критериям

Параметр	Тип	Обязательный	Описание
admin.login	Str	+	Логин администратора тенанта
admin.password	Str	+	Пароль администратора тенанта

Параметр	Тип	Обязательный	Описание
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: <ul style="list-style-type: none"> – less (меньше); – greater (больше); – in_range (в диапазоне); – equals (равно); – contains (содержит)
query.text.value	Str	-	Значение поиска
tenant_id	Str	+	Идентификатор тенанта
cox.balancer_endpoint	Str	+	Конечная точка балансировщика нагрузки сервиса
cox.compression	Str	+	Метод сжатия данных (варианты: none, gzip), по умолчанию — none
cox.endpoint	Str	+	Конечная точка сервиса
cox.load_balanced	Bool	+	Балансировщик нагрузки сервиса
cox.request_timeout	Str	+	Таймаут 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 СА 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:

```
[
  {
    "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 105.

Таблица 105 — Описание всех параметров поиска

Параметр	Тип	Обязательный	Описание
admin.login	Str	+	Логин администратора тенанта
admin.password	Str	+	Пароль администратора тенанта
compose_with_or			Объединение полей запроса с помощью ИЛИ. Значение по умолчанию И
cox.balancer_endpoint	Str	+	Конечная точка балансировщика нагрузки сервиса
cox.compression	Str	+	Метод сжатия данных (варианты: none , gzip), по умолчанию — none
cox.endpoint	Str	+	Конечная точка сервиса
cox.load_balanced	Bool	+	Балансировщик нагрузки сервиса
cox.request_timeout	Str	+	Таймаут запроса к сервису
cox.service_name	Str	+	Имя сервиса
cox.use_tls	Bool	+	TLS-сертификат

Параметр	Тип	Обязательный	Описание
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: <ul style="list-style-type: none"> – 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: <ul style="list-style-type: none"> – less (меньше); – greater (больше); – in_range (в диапазоне); – equals (равно); – contains (содержит)
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:

Параметр	Тип	Обязательный	Описание
			<ul style="list-style-type: none"> – 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: <ul style="list-style-type: none"> – 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:

Параметр	Тип	Обязательный	Описание
			<ul style="list-style-type: none"> – less (меньше); – greater (больше); – 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: <ul style="list-style-type: none"> – 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: <ul style="list-style-type: none"> – less (меньше); – greater (больше); – in_range (в диапазоне); – equals (равно); – contains (содержит)

Параметр	Тип	Обязательный	Описание
query.importance.value	Str	-	Фильтр по важности письма. Возможные поисковые значения: <ul style="list-style-type: none"> – 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: <ul style="list-style-type: none"> – less (меньше); – greater (больше); – in_range (в диапазоне); – equals (равно); – contains (содержит)
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: <ul style="list-style-type: none"> – 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

Параметр	Тип	Обязательный	Описание
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: <ul style="list-style-type: none"> – 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: <ul style="list-style-type: none"> – 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: <ul style="list-style-type: none"> – less (меньше); – greater (больше); – in_range (в диапазоне); – equals (равно); – contains (содержит)
query.text.value	Str	-	Поиск в тексте письма

Параметр	Тип	Обязательный	Описание
query.to.operation	Str	-	Оператор для поиска значения в поле письма «Кому». Оператор запроса. Возможные значения: <ul style="list-style-type: none"> – 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 СА 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

5.20 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 106.

Таблица 106 — Параметры 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
    },
    .....
  ]
}
```

5.21 Массовое удаление писем



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 [Поиск писем по заданным критериям](#)).

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_cert.pem \
--tls_settings.key_file /home/user/client_key.pem
```

Описание параметров запроса приведено в таблице 107.

Таблица 107 — Параметры 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	+	Конечная точка балансировщика нагрузки сервиса
cox.compression	Str	+	Метод сжатия данных (варианты: none , gzip), по умолчанию — none
cox.endpoint	Str	+	Конечная точка сервиса
cox.load_balanced	Bool	+	Балансировщик нагрузки сервиса

Параметр	Тип	Обязательный	Описание
<code>cox.request_timeout</code>	Str	+	Таймаут запроса к сервису
<code>cox.service_name</code>	Str	+	Имя сервиса
<code>cox.use_tls</code>	Bool	+	TLS-сертификат
<code>cox.use_tls_balancer</code>	Bool	+	Защищенная передача данных при подключении к балансировщику
<code>tls_settings.ca_file</code>	Str	+	Путь к CA файлу
<code>tls_settings.client_cert_file</code>	Str	+	Путь к файлу сертификата клиента
<code>tls_settings.key_file</code>	Str	+	Путь к файлу с ключом клиента

Пример ответа:

```
{
  "Response": {
    "changed": true,
    "failed": false,
    "msg": "ok"
  },
  "deleted": 1,
  "failed": 0
}
```

5.22 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».



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 108.

Таблица 108 — Параметры запроса на поиск удаленных писем

Параметр	Тип	Обязательный	Описание
config	Str	+	Конфигурационный файл с параметрами сервиса Сох 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": "af1ee084-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 109.

Таблица 109 — Параметры запроса на восстановление письма по идентификатору

Параметр	Тип	Обязательный	Описание
config	Str	+	Конфигурационный файл с параметрами сервиса Сох 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 110.

Таблица 110 — Параметры запроса на восстановление по лимиту на количество писем

Параметр	Тип	Обязательный	Описание
config	Str	+	Конфигурационный файл с параметрами сервиса Сох 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



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 111.

Таблица 111 — Параметры 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



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"
}
```

5.23 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_cert.pem \  
--tls_settings.key_file /home/user/client_key.pem \  

```

Описание параметров запроса приведено в таблице 112.

Таблица 112 — Параметры 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	+	Конечная точка балансировщика нагрузки сервиса
cox.compression	Str	+	Метод сжатия данных (варианты: none , gzip), по умолчанию — none
cox.endpoint	Str	+	Конечная точка сервиса
cox.load_balanced	Bool	+	Балансировщик нагрузки сервиса
cox.request_timeout	Str	+	Таймаут 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 СА 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"
}
]
}
```

5.24 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.



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>

</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.



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_cert.pem
--tls_settings.key_file/home/home/user/client_key.pem
```

Описание параметров запроса приведено в таблице 113.

Таблица 113 — Параметры 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	+	Конечная точка балансировщика нагрузки сервиса
cox.compression	Str	+	Метод сжатия данных (варианты: none , gzip), по умолчанию — none
cox.endpoint	Str	+	Конечная точка сервиса
cox.load_balanced	Bool	+	Балансировщик нагрузки сервиса
cox.request_timeout	Str	+	Таймаут запроса к сервису

Параметр	Тип	Обязательный	Описание
<code>cox.service_name</code>	Str	+	Имя сервиса
<code>cox.use_tls</code>	Bool	+	TLS-сертификат
<code>cox.use_tls_balancer</code>	Bool	+	Защищенная передача данных при подключении к балансировщику
<code>tls_settings.ca_file</code>	Str	+	Путь к CA файлу
<code>tls_settings.client_cert_file</code>	Str	+	Путь к файлу сертификата клиента
<code>tls_settings.key_file</code>	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 114.

Таблица 114 — Параметры 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	+	Конечная точка балансировщика нагрузки сервиса

Параметр	Тип	Обязательный	Описание
cox.compression	Str	+	Метод сжатия данных (варианты: none , gzip), по умолчанию — none
cox.endpoint	Str	+	Конечная точка сервиса
cox.load_balanced	Bool	+	Балансировщик нагрузки сервиса
cox.request_timeout	Str	+	Таймаут 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 СА 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"
  },
  "success_user_count": 1
}
```

5.25 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, будут направляться в папку **Корзина**.



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 115.

Таблица 115 — Параметры запроса на добавление отправителей в список

Параметр	Тип	Обязательный	Описание
config	Str	+	Конфигурационный файл с параметрами сервиса Сох 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"
  },
  "senders": [
    {
      "tenant_id": "...",
      "address": "...",
      "status": 1
    }
  ]
}
```

```

    },
    {
      "tenant_id": "...",
      "address": "...",
      "status": 1
    },
    {
      "tenant_id": "...",
      "address": "...",
      "status": 2
    },
    {
      "tenant_id": "...",
      "address": "...",
      "status": 2
    }
  ]
}

```

5.25.1 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 116.

Таблица 116 — Параметры запроса на добавление отправителей в список

Параметр	Тип	Обязательный	Описание
config	Str	+	Конфигурационный файл с параметрами сервиса Сох 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

Параметр	Тип	Обязательный	Описание
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 117.

Таблица 117 — Параметры запроса на проверку отправителей

Параметр	Тип	Обязательный	Описание
config	Str	+	Конфигурационный файл с параметрами сервиса Сох 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
email	Str	+	Основной электронный адрес

Пример ответа:

```
{
  "Response": {
    "changed": false,
    "failed": false,
    "msg": "ok"
  },
  "email_list": 2
}
```

5.25.2 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 118.

Таблица 118 — Параметры запроса на обновление списка пользователей

Параметр	Тип	Обязательный	Описание
config	Str	+	Конфигурационный файл с параметрами сервиса Сох 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
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 [Добавление отправителей в список](#).

5.25.3 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 119.

Таблица 119 — Параметры запроса на удаление отправителей в списках

Параметр	Тип	Обязательный	Описание
config	Str	+	Конфигурационный файл с параметрами сервиса Сох 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

Параметр	Тип	Обязательный	Описание
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 [Добавление отправителей в список](#).

5.26 Управление почтовыми правилами и политиками



Для управления почтовыми правилами и политиками в тенанте пользователь должен иметь права администратора тенанта.

5.26.1 Просмотр созданных правил

Чтобы посмотреть созданные правила и их идентификаторы, необходимо выполнить команду `list_mail_rules`. Параметры команды вывода правил описаны в таблице 120.

Пример

Вывод списка правил, в которых пользователь с UserID указан в любом из условий:

```
nct_ministerium list_mail_rules \
--config config.json \
--admin.login <...> \
--admin.password <...> \
--search_ids UserID
```

Таблица 120 — Параметры команды просмотра почтовых правил

Параметр	Тип	Обяз.	Описание
config	string	+	Конфигурационный файл с параметрами сервиса сох и настройками TLS. Формируется автоматически на сервере с ролью ucs_infrastructure и находится по пути /srv/ministerium/config.json
admin.login	string	+	Логин администратора тенанта
admin.password	string	+	Пароль администратора тенанта
page_num	int	-	Номер страницы списка правил
page_size	int	-	Количество правил на одной странице
search_ids	string	-	Идентификатор пользователя или группы (необходимо использовать только идентификатор, указание почтового адреса недопустимо)
token-name	string	-	Имя токена



Для указания нескольких пользователей или групп их идентификаторы следует перечислить через запятую.

5.26.2 Создание правила

Чтобы создать правило обработки почты необходимо выполнить команду `create_mail_rule`. Все перечисленные в параметрах команды условия объединяются оператором И, а все исключения — оператором ИЛИ. Параметры команды создания правил описаны в таблице 121.

Примеры

1. Отклонить письма от внешних пользователей, которые пишут на группу GroupID:

```
nct_ministerium create_mail_rule \
--config config.json \
--rule.conditions.recipient.user_ids GroupID \
--rule.conditions.sender.user_type 1 \
--rule.reject
```

2. Отправить скрытую копию пользователю UserID1, если пользователь UserID2 пишет в адрес UserID3:

```
nct_ministerium create_mail_rule \
--config config.json \
--rule.conditions.sender.user_ids UserID2 \
--rule.conditions.recipient.user_ids UserID3 \
--rule.bcc_to UserID1
```

3. Отклонить письма, направленные пользователю UserID1, за исключением отправителя UserID2:

```
nct_ministerium create_mail_rule \
--config config.json \
--rule.conditions.recipient.user_ids UserID1 \
--rule.exceptions.sender.user_ids UserID2 \
--rule.reject
```

4. Отклонить письма, направленные участникам группы GroupID, за исключением пользователей UserID1 и UserID2:

```
nct_ministerium create_mail_rule \
--config config.json \
--rule.conditions.recipient.member_of GroupID \
--rule.exceptions.sender.user_ids UserID1, UserID2 \
--rule.reject
```

Таблица 121 — Параметры команды создания почтовых правил

Параметр	Тип	Обяз.	Описание
config	string	+	Конфигурационный файл с параметрами сервиса сох и настройками TLS. Формируется автоматически на сервере с ролью ucs_infrastructure и находится по пути /srv/ministerium/config.json
admin.login	string	+	Логин администратора тенанта
admin.password	string	+	Пароль администратора тенанта
rule.bcc_to	strings	-	Действие правила: добавление скрытой копии для пользователя UserID или GroupID
rule.conditions.recipient.member_of	strings	-	Условие: выполнить, если получатель является членом группы GroupID
rule.conditions.recipient.user_ids	strings	-	Условие: выполнить, если получатель имеет идентификатор UserID или GroupID
rule.conditions.recipient.user_type	int	-	Условие: выполнить, если получатель является ВНУТРЕННИМ (2) или ВНЕШНИМ (1)

Параметр	Тип	Обяз.	Описание
rule.conditions.sender.member_of	strings	-	Условие: выполнить, если отправитель является членом группы GroupID
rule.conditions.sender.user_ids	strings	-	Условие: выполнить, если отправитель имеет идентификатор UserID или GroupID
rule.conditions.sender.user_type	int	-	Условие: выполнить, если отправитель является ВНУТРЕННИМ (2) или ВНЕШНИМ (1)
rule.enabled_mode	int	-	Состояние правила: включено (1) или отключено (2). По умолчанию: 1
rule.exceptions.recipient.member_of	strings	-	Исключение: исключить, если получатель является членом группы GroupID
rule.exceptions.recipient.user_ids	strings	-	Исключение: исключить, если получателем является UserID или GroupID
rule.exceptions.recipient.user_type	int	-	Исключение: исключить, если получатель является ВНУТРЕННИМ (2) или ВНЕШНИМ (1)
rule.exceptions.sender.member_of	strings	-	Исключение: исключить, если отправитель является членом группы GroupID
rule.exceptions.sender.user_ids	strings	-	Исключение: исключить, если отправителем является UserID или GroupID
rule.exceptions.sender.user_type	strings	-	Исключение: исключить, если отправитель является ВНУТРЕННИМ (2) или ВНЕШНИМ (1)
rule.post_rule_mode	int	-	Флаг остановки обработки правил после данного правила: остановить (1) или продолжить (2). По умолчанию: 2
rule.priority	int	-	Приоритет правила. По умолчанию правило добавляется в конец списка правил
rule.reject		-	Действие правила: отклонить сообщение
token-name	string	-	Имя токена



Для указания нескольких пользователей или групп их идентификаторы следует перечислить через запятую.

5.26.3 Обновление правила

Обновление правил работает по логике замены. Чтобы обновить параметры созданного правила, необходимо выполнить команду `update_mail_rule`, передать идентификатор правила и необходимые критерии (как при создании правила). Параметры команды обновления правил описаны в таблице 122.

Примеры аналогичны примерам для команды `create_mail_rule`, для обновления требуется передать все необходимые критерии правила.

Таблица 122 — Параметры команды создания почтовых правил

Параметр	Тип	Обяз.	Описание
config	string	+	Конфигурационный файл с параметрами сервиса сох и настройками TLS. Формируется автоматически на сервере с ролью <code>ucs_infrastructure</code> и находится по пути <code>/srv/ministerium/config.json</code>
admin.login	string	+	Логин администратора тенанта
admin.password	string	+	Пароль администратора тенанта
rule.bcc_to	strings	-	Действие правила: добавление скрытой копии для пользователя UserID или GroupID
rule.conditions.recipient.member_of	strings	-	Условие: выполнить, если получатель является членом группы GroupID
rule.conditions.recipient.user_ids	strings	-	Условие: выполнить, если получатель имеет идентификатор UserID или GroupID
rule.conditions.recipient.user_type	int	-	Условие: выполнить, если получатель является ВНУТРЕННИМ (2) или ВНЕШНИМ (1)
rule.conditions.sender.member_of	strings	-	Условие: выполнить, если отправитель является членом группы GroupID
rule.conditions.sender.user_ids	strings	-	Условие: выполнить, если отправитель имеет идентификатор UserID или GroupID
rule.conditions.sender.user_type	int	-	Условие: выполнить, если отправитель является ВНУТРЕННИМ (2) или ВНЕШНИМ (1)
rule.enabled_mode	int	-	Состояние правила: включено (1) или отключено (2). По умолчанию: 1
rule.exceptions.recipient.member_of	strings	-	Исключение: исключить, если получатель является членом группы GroupID

Параметр	Тип	Обяз.	Описание
rule.exceptions.recipient.user_ids	strings	-	Исключение: исключить, если получателем является UserID или GroupID
rule.exceptions.recipient.user_type	int	-	Исключение: исключить, если получатель является ВНУТРЕННИМ (2) или ВНЕШНИМ (1)
rule.exceptions.sender.member_of	strings	-	Исключение: исключить, если отправитель является членом группы GroupID
rule.exceptions.sender.user_ids	strings	-	Исключение: исключить, если отправителем является UserID или GroupID
rule.exceptions.sender.user_type	strings	-	Исключение: исключить, если отправитель является ВНУТРЕННИМ (2) или ВНЕШНИМ (1)
rule.post_rule_mode	int	-	Флаг остановки обработки правил после данного правила: остановить (1) или продолжить (2). По умолчанию: 2
rule.priority	int	-	Приоритет правила. По умолчанию правило добавляется в конец списка правил
rule.reject		-	Действие правила: отклонить сообщение
token-name	string	-	Имя токена



Для указания нескольких пользователей или групп их идентификаторы следует перечислить через запятую.

5.26.4 Удаление правила

Чтобы удалить правило необходимо выполнить команду `delete_mail_rule` с передачей идентификатора правила. Параметры команды удаления правила описаны в таблице 123.

Пример

Удалить правило с идентификатором RuleID:

```
nct_ministerium delete_mail_rule \  
--config config.json \  
--admin.login <...> \  
--admin.password <...> \  
--id RuleID
```

Таблица 123 — Параметры команды удаления почтового правила

Параметр	Тип	Обяз.	Описание
config	string	+	Конфигурационный файл с параметрами сервиса сох и настройками TLS. Формируется автоматически на сервере с ролью ucs_infrastructure и находится по пути /srv/ministerium/config.json
admin.login	string	+	Логин администратора тенанта
admin.password	string	+	Пароль администратора тенанта
id	string	-	Идентификатор правила
token-name	string	-	Имя токена

6 МИГРАЦИЯ И СИНХРОНИЗАЦИЯ

6.1 Синхронизация данных из внешних каталогов

Mailion предоставляет возможность синхронизации по LDAP со следующими внешними каталогами: MS Active Directory, FreeIPA, ALD Pro. Этот функционал реализован с помощью сервиса синхронизации данных из внешних каталогов с Mailion — **phalanx**, который поддерживает синхронизацию следующих событий во внешних каталогах:

- создание и редактирование пользователей;
- блокировка пользователей;
- создание и изменение групп рассылки.

Ограничения:

- информация о пользователях обновляется только в одностороннем порядке: из внешнего каталога в Mailion;
- синхронизация контактов и удаления пользователей и пока недоступна.



Принцип работы сервиса **phalanx** с Active Directory отличается от всех других каталогов — другие каталоги позволяют использовать механизм подписки на изменения, которые в них произошли. В Active Directory вместо него используется опрос (*polling*), период которого можно задать отдельно для каждой интеграции с внешним каталогом (описано далее).

6.1.1 Запуск сервиса phalanx

По умолчанию **phalanx** при установке Mailion не запускается. Для его запуска необходимо в файле

```
~/install_mailion/contrib/mailion/<конфигурация_установки>/group_vars/ucs_setup/mailion.yml присвоить параметру phalanx_enabled значение true:
```

```
# Конфигурация PHALANX
# Запустить сервис, отвечающий за контролируемую синхронизацию с внешними каталогами
phalanx_enabled: true
```



При повторном создании группы рассылки для ее корректной работы необходимо выполнить команду `ministerium ldap_sync` с установленным флагом `update_group_members` (см. раздел [Принудительно синхронизировать пользователя или группу](#)).

6.1.2 Конфигурация сервиса phalanx

Интеграции с внешними каталогами для **phalanx** определяются вручную после запуска сервиса — их можно добавлять, менять и удалять во время его работы. Для выполнения этих операций используется командная утилита **ministerium**, которая обновляет данные интеграций в хранилище **etcd**, откуда **phalanx** их извлекает и проводит нужные действия.



В данной версии Mailion действует ограничение, которое будет снято в последующих версиях: любое изменение конфигурации **phalanx** должно быть продолжено перезапуском сервиса. Для этого необходимо выполнить следующие действия:

1. Зайти по **ssh** на машину, где работает сервис **phalanx**.

2. Выполнить команду:

```
$ docker restart phalanx
```

Также сервис можно перезапустить через **ansible** командой:

```
ansible -i inventory/<ваш inventory-файл>.yaml ucs_catalog -m  
ansible.builtin.shell -a "sudo docker restart phalanx")
```

После удаления всех интеграций необходимо вручную остановить работу сервиса **phalanx**:

1. Зайти по **ssh** на машину, где работает сервис **phalanx**.

2. Выполнить команду:

```
$ docker stop phalanx
```

3. Убедиться, что сервис остановлен:

```
$ docker ps -a | grep phalanx
```

Также сервис можно остановить через **ansible** командой:

```
ansible -i inventory/<ваш inventory-файл>.yaml ucs_catalog -m  
ansible.builtin.shell -a "sudo docker stop phalanx"
```

6.1.3 Основные команды для работы с интеграциями

6.1.3.1 Получить сведения обо всех настроенных интеграциях

Пример команды, запрашивающей сведения обо всех настроенных интеграциях:

```
nct_ministerium get_all_ldap_integrations \  
--config /srv/ministerium/config.json
```

Пример ответа:

```
{  
  "Response": {  
    "changed": false,  
    "failed": false,  
    "msg": "ok"  
  },  
  "ldap_integrations": {  
    "my_integration": {  
    },  
    "integration_to_be_removed": {  
    }  
  }  
}
```

Обнаружено две интеграции: `my_integration` и `integration_to_be_removed`.

6.1.3.2 Добавить интеграцию

Пример команды добавления интеграции:

```
nct_ministerium add_ldap_integration \  
--config /srv/ministerium/config.json \  
--file_path new_integration.json \  
--delegate_id ...
```

Параметр	Тип	Обяз.	Описание
config	string	+	Путь к файлу конфигурации
file_path	string	+	Путь к файлу описания интеграции

Пример ответа:

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



Если возникает потребность создать интеграцию заново, необходимо создать ее под новым именем (`delegate_id`), так как в cookie-файлах внешнего каталога сохраняется прежнее имя, что может привести к конфликтам.

6.1.3.3 Удалить интеграцию

Пример команды удаления настроенной интеграции:

```
nct_ministerium remove_ldap_integration \  
--config /srv/ministerium/config.json \  
--delegate_id <имя_удаляемой_интеграции>
```

Параметр	Тип	Обяз.	Описание
config	string	+	Путь к файлу конфигурации
delegate_id	string	+	Имя интеграции

Пример ответа:

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

6.1.3.4 Принудительно синхронизировать пользователя или группу

Для принудительной синхронизации пользователя или группы следует использовать команду `ldap_sync`. Набор параметров зависит от цели выполнения команды — для группы или для пользователя. Для синхронизации пользователя, помимо обязательных параметров, можно указать на выбор `email`, `login` или `user_id`. Для синхронизации группы, помимо обязательных параметров, можно указать на выбор `external_id` или `email`. При синхронизации группы также можно использовать флаг `update_group_members`, указывающий на необходимость синхронизации также и членов группы.

Пример команды для синхронизации пользователя:

```
nct_ministerium ldap_sync \  
--config "/srv/ministerium/config.json" \  
--external_domain AD \  
--external_id "0b2babd2-5bde-2440-86ca-ddd316900278" \  
--login "petr.petrov" \  
--v
```

Пример команды для синхронизации группы:

```
nct_ministerium ldap_sync \
--config "/srv/ministerium/config.json" \
--external_domain AD \
--external_id "0b2babd2-5bde-2440-86ca-ddd316900278" \
--email "group01@ad.example.com" \
--update_group_members=true \
--v
```

Параметр	Тип	Обяз.	Описание
config	string	+	Путь к файлу конфигурации
external_domain	string	+	Имя почтового домена
external_id	string	+	Идентификатор пользователя или группы во внешнем каталоге
email	string	–	Почтовый адрес пользователя или группы
login	string	–	Логин пользователя из внешнего каталога в Mailion
user_id	string	–	Идентификатор пользователя из внешнего каталога в Mailion
update_group_members	boolean	–	Флаг синхронизации членов группы при синхронизации группы: true — синхронизировать (по умолчанию), false — не синхронизировать
v		–	Уровень подробного журналирования

Пример ответа:

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

6.1.4 Файл описания интеграции

В примере добавления интеграции с помощью команды `add_ldap_integration` был использован файл описания интеграции `new_integration.json`.

Пример содержимого файла описания интеграции:

```
{
  "ldap_sync_enabled": true,
  "connection": {
    "servers": [
      {
        "endpoint": "ad.ru:389",
        "tls": {}
      }
    ],
    "base_dn": "dc=DOMAINPART1,dc=DOMAINPART2",
    "bind_user": "mailion_impersonated_user",
    "bind_password": "external_catalog_password",
    "bind_user_template": "DOMAINPART1\\{{.Name}}",
    "pool_length": 10,
    "dial_timeout": {
      "seconds": 10
    },
    "search_page_size": 20,
    "default_attribute_mapping_name": "AD",
    "search_filter_user": "(\u0026(\u0026(objectCategory=person)
(objectClass=user))(|(givenName={{.Name}}*)(sn={{.Name}}*)(middleName={{.Name}}*)
(sAMAccountName={{.Name}}*)(mail={{.Name}}*)))",
    "search_filter_group": "(\u0026(\u0026(objectCategory=group)(|
(groupType=8)(groupType=-2147483646)(groupType=-2147483640)(mail=*)(!
(msExchHideFromAddressLists=TRUE))(|(displayName={{.Name}}*)
(description={{.Name}}*)(mail={{.Name}}*)))",
    "search_filter_resource": "(\u0026(|
(msExchResourceMetaData=ResourceType:Room))(|(givenName={{.Name}}*)(sn={{.Name}}*)
(middleName={{.Name}}*)(sAMAccountName={{.Name}}*)(mail={{.Name}}*)))"
  },
  "connect_retry": {
    "init_interval": {
      "seconds": 7330321442753111419,
      "nanos": 1304113440
    },
    "randomization_factor": 0.34619462,
    "multiplier": 0.91170365,
    "max_interval": {
      "seconds": 7004854706655632745,
      "nanos": 1365864736
    },
    "max_elapsed_time": {
      "seconds": 2667728985810002853,
      "nanos": 207902452
    }
  },
  "is_ad": true,
  "sync_interval": {
    "seconds": 10
  }
}
```

Значения параметров `search_filter_user`, `search_filter_group`, `search_filter_resource` и параметров в секции `connect_retry` рекомендуется оставить без изменения.

Секция	Назначение
<pre>{ "is_ad": true }</pre>	<p>Указывает тип каталога. Если <code>is_ad=true</code>, то эта интеграция с каталогом Active Directory.</p>
<pre>{ "sync_interval" : { "seconds": 10 } }</pre>	<p>Поле <code>seconds</code> определяет период проверки изменений во внешнем каталоге. Рекомендуется использовать значение 10 или меньше. Слишком большой период приведет к большой задержке обновления атрибутов в Mailion.</p>
<pre>{ "ldap_sync_enabled": true }</pre>	<p>Определяет включена ли интеграция. Например, интеграцию можно остановить двумя способами: установить для поля <code>ldap_sync_enabled</code> значение <code>false</code> или полностью удалить интеграцию.</p>
<pre>{ "servers": [{ "endpoint": "ad.ru:389", "tls": { "ca_file": "", "cert_file": "", "key_file": "" } }], "base_dn": "dc=DOMAINPART1,dc=DOMAINPART2", "bind_user": "mailion_impersonated_user", "bind_password": "external_catalog_password", "bind_user_template": "DOMAINPART1\\{{.Name}}", "pool_length": 10, "dial_timeout": { "seconds": 10 }, "search_page_size": 20, "default_attribute_mapping_name": "AD" }</pre>	<p>Данная секция описывает подключение к внешнему каталогу, ее следует заполнять аналогично заполнению таких секций для интеграций, например, orpheus или iason.</p>

6.2 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
```

Описание параметров команды приведено в таблице 124.

Таблица 124 — Параметры команды создания пользователя из внешнего каталога

Параметр	Тип	Обяз.	Описание
config	Str	+	Путь к файлу конфигурации
emails	Str	+	Почтовый адрес пользователя из внешнего каталога
force_remove_outlook_rule_blob	Bool	+	Флаг удаления объекта правил MS Outlook: <ul style="list-style-type: none"> – <code>true</code> — все отключенные правила MS Outlook будут удалены; – <code>false</code> — метод <code>adonis.CreateDelegatedUsers</code> вернет ошибку <code>OUTLOOK_RULE_EXISTS</code>
enable_sync	Bool	+	Флаг включения синхронизации почты и календаря. Значение по умолчанию: <code>false</code>

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": []
}
```

6.3 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 мапингу 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 СОПОСТАВЛЕНИЕ АТТРИБУТОВ LDAP-КАТАЛОГОВ

Для доменов, у которых настроено делегирование от внешнего LDAP-каталога, может быть задано сопоставление атрибутов внешнего каталога с полями (аттрибутами) сущностей в каталоге Mailion. Делегирование осуществляется через одно из подключений к внешнему LDAP-каталогу, которое настраивается в конфигурации сервиса **orpheus**.

В сервисе **orpheus** также предусмотрено сопоставление атрибутов по умолчанию, и каждое подключение к внешнему каталогу в обязательном порядке имеет ссылку на такое сопоставление. Имя сопоставления по умолчанию может иметь произвольное значение, но обычно совпадает с именем каталога, для которого оно предназначено: AD, OpenLDAP, FreeIPA, SambaDC, ALDPRO или REDADM. Сопоставление по умолчанию можно переопределить с помощью описанных далее команд утилиты **ministerium**.

Можно задать другое сопоставление по умолчанию (MAPPING_TYPE_PRESET) или загрузить полностью новое сопоставление из файла для отдельного домена. Сопоставления по умолчанию можно выгрузить в файл, отредактировать и загрузить как уникальное сопоставление (MAPPING_TYPE_CUSTOM). Для каждого делегированного домена может быть настроено отдельное сопоставление.

Сопоставление можно настроить с помощью готового файла-шаблона (см. раздел [Настройка сопоставления с помощью файла-шаблона](#)) или добавить с помощью команд утилиты **ministerium** (см. раздел [Добавление сопоставления командами](#)).

7.1 Настройка сопоставления с помощью файла-шаблона

Для упрощения работы и быстрой настройки сопоставления можно воспользоваться файлом шаблоном, доступным для любого поддерживаемого внешнего каталога. Путь к этому файлу передается в любую из команд (см. [Добавление сопоставления командами](#)), которая поддерживает добавление сопоставления.

Чтобы получить файл-шаблон, 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 125.

Таблица 125 — Параметры запроса на получение файла-шаблона для сопоставления

Параметр	Тип	Обязательный	Описание
output_filepath	Str	+	Путь к файлу-шаблону
preset_name	Str	+	Имя файла-шаблона для требуемого каталога (например, AD)
admin.login	Str	+	Логин администратора
admin.password	Str	+	Пароль администратора
cox.balancer_endpoint	Str	+	Конечная точка балансировщика нагрузки сервиса
cox.compression	Str	+	Метод сжатия данных (варианты: none, gzip), по умолчанию — none
cox.endpoint	Str	+	Конечная точка сервиса
cox.load_balanced	Bool	+	Балансировщик нагрузки сервиса
cox.request_timeout	Str	+	Таймаут 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 СА 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 следует открыть полученный файл (в данном примере, `AD.json`) и внести исправления (при необходимости). Пример файла-шаблона для AD:

```

{
  "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",
    "user_certificate": "userCertificate",
    "user_smime_certificate": "userSMIMECertificate",
    "common_name": "cn"
  },
  "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}}))",
  "search_filter_contact": "(&(&(objectCategory=person)(objectClass=contact))(|
givenName={{.Name}}*)(sn={{.Name}}*)(middleName={{.Name}}*)
(sAMAccountName={{.Name}}*)(mail={{Name}}*))"
}

```

Описание сопоставляемых в секции `attributes_mapping` атрибутов приведено в таблице 126.

Таблица 126 — Карта сопоставления атрибутов в файле-шаблоне

Атрибут Mailion	Атрибут AD	Описание
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

Атрибут Mailion	Атрибут AD	Описание
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	Эл. почта 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 сущности (главное имя пользователя), заведенной в каталоге. Это имя используется как логин, который нельзя изменять. Данный атрибут — особенность AD, но также присутствует во FreeIPA
status	userAccountControl	Статус пользователя
title	title	Должность пользователя
user_certificate	userCertificate	Пользовательский сертификат
user_smime_certificate	userSMIMECertificate	Пользовательский сертификат в формате S/MIME
common_name	cn	Отображаемое имя, используется для отображения названия групп из внешних каталогов

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}} — эл. почта пользователя.

2. **SearchFilterGroup** — шаблон для LDAP-фильтра, с помощью которого будет производиться поиск группы во внешнем каталоге. Доступные переменные шаблона:

- {{.Name}} — имя группы;

- `{{.Email}}` — эл. почта группы.
3. **SearchFilterResource** — шаблон для LDAP-фильтра, с помощью которого будет производиться поиск ресурса во внешнем каталоге. Доступные переменные шаблона:
- `{{.Name}}` — имя ресурса;
 - `{{.Email}}` — эл. почта 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 адресу электронной почты во внешнем каталоге. Доступные переменные шаблона:
- `{{.Email}}` — эл. почта 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.
7. **SearchFilterContact** — шаблон для LDAP-фильтра, с помощью которого производится поиск почтового контакта во внешнем каталоге. С его помощью можно понять, как искать того или иного пользователя. Доступные переменные для шаблона:
- `{{.Name}}` — имя пользователя;
 - `{{.Email}}` — эл. почта пользователя.

7.2 Добавление сопоставления командами

Управление сопоставлением LDAP-атрибутов осуществляется с помощью следующих команд [расширенного администрирования](#):

- [create domain](#) — создание домена. Если в этом запросе добавляется делегирование домена, то можно сразу же задать сопоставление;
- [add domain delegation](#) — добавление делегированного на внешний LDAP-каталог домена;
- [update domain delegation](#) — обновление делегации домена;

- [set_same_domain_delegation](#) — настройка делегации с типом «делегация на одинаковых доменах».



Для команд `add_domain_delegation` и `update_domain_delegation` файл задается с помощью параметра `--delegation.ldap_attributes_mapping.custom_from_file`

7.2.1 Добавление сопоставления при создании домена

Для добавления сопоставления при создании 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 127.

Таблица 127 — Параметры запроса на создание домена

Параметр	Тип	Обяз.	Описание
<code>--admin.login</code>	string	+	Логин администратора
<code>--admin.password</code>	string	+	Пароль администратора
<code>--cox.balancer_endpoint</code>	string	+	Конечная точка балансировщика нагрузки сервиса
<code>--cox.compression</code>	string	+	Использование метода компрессии при соединении с сервисом: попе

Параметр	Тип	Обяз.	Описание
			(по умолчанию), gzip
--cox.endpoint	string	+	Endpoint для непосредственного соединения с сервисом
--cox.load_balanced	boolean	+	Использовать соединение с балансировщиком
--cox.request_timeout	duration	+	Таймаут 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 шаблон 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
--external.is_sync_enabled	boolean	+	Включение/отключение синхронизации с внешним

Параметр	Тип	Обяз.	Описание
			доменом. Если значение false, то выключена. Если значение true, то включена
--external.ldap_attributes_mapping.custom_from_file	string	–	Имя файла для загрузки пользовательского сопоставления атрибутов. Если задано, другие атрибуты игнорируются
--external.ldap_attributes_mapping.mapping	strings	+	Список атрибутов. Формат: key1=value1,key2=value2,... Где keyN — атрибут Mailion, valueN — внешний атрибут
--external.ldap_attributes_mapping.mapping_type	string	+	Тип сопоставления. Доступные значения: MAPPING_TYPE_PRESET (сопоставление по готовому шаблону), MAPPING_TYPE_CUSTOM (пользовательское сопоставление)
--external.ldap_attributes_mapping.search_filter_by_id	string	+	Шаблон LDAP-фильтра для поиска объектов по идентификатору во внешнем каталоге. Пример: (&(ipaUniqueID={{.ID}}))
--external.ldap_attributes_mapping.search_filter_exact_user_by_email	string	+	Шаблон LDAP-фильтра 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	+	Шаблон LDAP-фильтра для точного поиска пользователей по имени во внешнем каталоге. Пример: (&(&(objectCategory=person)(objectClass=user))(sAMAccountName={{.Name}}))
--external.ldap_attributes_mapping.search_filter_group	string	+	Шаблон LDAP-фильтра для поиска групп во внешнем каталоге.

Параметр	Тип	Обяз.	Описание
			<p>Пример: (&(&(objectCategory=group)((groupType=8)(groupType=- 2147483646)(groupType=- 2147483640))(mail=*)(! (msExchHideFromAddressLists=TRU E)))(!(displayName={{.Name}}*) (description={{.Name}}*) (mail={{.Name}}*)))</p>
--external.ldap_attributes_ mapping.search_filter_resource	string	+	<p>Шаблон LDAP-фильтра для поиска ресурсов во внешнем каталоге.</p> <p>Пример: (&((msExchResourceMetaData=Resource Type:Room))((extensionAttribute2={{.Name}}*) (extensionAttribute1={{.Name}}*) (givenName={{.Name}}*) (sn={{.Name}}*) (extensionAttribute3={{.Name}}*) (sAMAccountName={{.Name}}*) (mail={{.Name}}*)))</p>
--external.ldap_attributes_ mapping.search_filter_user	string	+	<p>Шаблон LDAP-фильтра для поиска пользователей во внешнем каталоге.</p> <p>Пример: (&(&(objectCategory=person) (objectClass=user))((extensionAttribute2={{.Name}}*) (extensionAttribute1={{.Name}}*) (givenName={{.Name}}*) (sn={{.Name}}*) (extensionAttribute3={{.Name}}*) (sAMAccountName={{.Name}}*) (mail={{.Name}}*)))</p>
--features.is_authorization	boolean	+	Домен может быть использован при авторизации
--features.is_mail	boolean	+	Если значение true, домен может принимать почтовые сообщения
--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

Параметр	Тип	Обяз.	Описание
			умолчанию
--hostname	string	+	Имя домена
--is_prioritized	boolean	+	Приоритизированный 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 сопоставление добавляется из файла AD.json и сохраняется в домене.

7.2.2 Добавление сопоставления при настройке делегации домена

Для добавления сопоставления 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 128.

Таблица 128 — Параметры запроса на создание домена

Параметр	Тип	Обяз.	Описание
--admin.login	string	+	Логин администратора
--admin.password	string	+	Пароль администратора
--cox.balancer_endpoint	string	+	Конечная точка балансировщика нагрузки сервиса
--cox.compression	string	+	Метод сжатия данных при подключении к сервису: — 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	+	Таймаут 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, 4 — RED_ADM,

Параметр	Тип	Обяз.	Описание
			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 сопоставления 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	+	Фильтры шаблона LDAP для поиска объектов по идентификатору во внешнем каталоге. Пример: (&(ipaUniqueID={{.ID}}))
--delegation.ldap_attributes_mapping.search_filter_exact_user_by_email	string	+	Фильтры 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	+	Фильтры шаблона LDAP для точного поиска пользователей по имени во внешнем каталоге.

Параметр	Тип	Обяз.	Описание
			Пример: (&(&(objectCategory=person)(objectClass=user))(sAMAccountName={{.Name}}))
--delegation.ldap_attributes_mapping.search_filter_group	string	+	Фильтры 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	+	Фильтры 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	+	Фильтры 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 СА
--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

7.2.3 Добавление сопоставления при обновлении делегирования домена

Добавить сопоставление можно с помощью команды обновления делегирования (привязки) домена `update_domain_delegation`. Пример команды:

```
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_changed=whenChanged,last_name=sn,last_name_alt=extensionAttribute1,locale=localeID,login=sAMAccountName,mail=mail,middle_name=extensionAttribute3,middle_name_alt=extensionAttribute3,phone_number_work=telephoneNumber,principal_name=userPrincipalName,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 команды приведено в таблице 129.

Таблица 129 — Параметры команды обновления делегирования домена

Параметр	Тип	Обязательный	Описание
<code>--admin.login</code>	string	+	Логин администратора
<code>--admin.password</code>	string	+	Пароль администратора

Параметр	Тип	Обязательный	Описание
--cox.balancer_endpoint	string	+	Конечная точка 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	+	Таймаут 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, 4 — RED_ADM, 5 — ALD_PRO

Параметр	Тип	Обязательный	Описание
--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	+	Фильтра шаблона LDAP для поиска объектов по идентификатору во внешнем каталоге. Пример: (&(ipaUniqueID={{.ID}}))
--delegation.ldap_attributes_mapping.search_filter_exact_user_by_email	string	+	Фильтра 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	+	Фильтра 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	+	Фильтра 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	+	Фильтра 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	+	Фильтра шаблона LDAP для поиска пользователей во внешнем каталоге. Пример: (&(&(objectCategory=person)(objectClass=user))((extensionAttribute2={{.Name}}*))

Параметр	Тип	Обязательный	Описание
			(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 [Настройка сопоставления с помощью файла-шаблона](#).

7.2.4 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_changed=whenChanged,last_name=sn,last_name_alt=extensionAttribute1,locale=localeID,login=sAMAccountName,mail=mail,middle_name=extensionAttribute3,middle_name_alt=extensionAttribute3,phone_number_work=telephoneNumber,principal_name=userPrincipalName,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 130.

Таблица 130 — Параметры запроса для создания делегации на одинаковых доменах

Параметр	Тип	Обяз.	Описание
--admin.login	string	+	Логин администратора
--admin.password	string	+	Пароль администратора
--cox.balancer_endpoint	string	+	Конечная точка балансировщика нагрузки сервиса
--cox.compression	string	+	Использование метода сжатия при соединении с сервисом: none (по умолчанию), gzip

Параметр	Тип	Обяз.	Описание
--cox.endpoint	string	+	Endpoint для непосредственного соединения с сервисом
--cox.load_balanced	boolean	+	Использовать соединение с балансировщиком
--cox.request_timeout	duration	+	Таймаут 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, 4 — RED_ADM, 5 — ALD_PRO
--delegation.domain_alias	string	+	Имя контроллера внешнего домена
--delegation.domain_auth_name	string	+	Длинная запись домена аутентификации

Параметр	Тип	Обяз.	Описание
--delegation.domain_short_name	string	+	Краткая запись домена аутентификации
--delegation.is_sync_enabled	boolean	+	Включение/отключение синхронизации с внешним доменом: false — выключена; true — включена
--delegation.ldap_attributes_mapping.custom_from_file	string	-	Имя файла для загрузки пользовательского сопоставления 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 сопоставления. Доступные значения: MAPPING_TYPE_PRESET (сопоставление с помощью шаблона), MAPPING_TYPE_CUSTOM (настраиваемое сопоставление)
--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_	string	+	Фильтр шаблона LDAP для точного поиска пользователей

Параметр	Тип	Обяз.	Описание
user_by_name			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}}*)

Параметр	Тип	Обяз.	Описание
			(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 СА
--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 [Настройка сопоставления через файл](#).

8 РЕГИСТРАЦИЯ СОБЫТИЙ В ФОРМАТЕ CEF

Common Event Format (CEF) — это стандартизированный формат, который используется для оптимизации процесса регистрации событий, связанных с безопасностью. Стандартизация упрощает интеграцию журналов из разных источников в единую базу. Это особенно полезно для систем управления информацией и событиями безопасности (SIEM), которые предназначены для сбора и анализа журналов из множества источников для обнаружения и реагирования на угрозы безопасности. CEF реализует структурированный подход к представлению данных для регистрации событий и поддерживает широкий выбор типов и уровней важности событий.

Механизм регистрации событий в формате CEF

1. В процессе взаимодействия пользователя с системой Mailion посредством доступных интерфейсов (web, IMAP, SMTP, ministerium) выполняются gRPC-вызовы к внутренним сервисам.
2. Выполняемые gRPC-вызовы отслеживают перехватчики в шлюзах (**cox, house**).
3. В результате перехвата gRPC-вызова формируется сообщение с данными, необходимыми для формирования CEF-события, которое отправляется в очередь NATS Jetstream для последующей обработки.
4. Сервис **homeros** получает сообщение из NATS Jetstream и формирует из него CEF-событие;
5. Сервис **homeros** отправляют CEF-событие в SIEM систему.

Адаптация формата CEF для Mailion

1. Идентификатор события состоит из шести цифр и классифицирует его:
 - а) Первые две цифры обозначают класс события. Всегда заполняются обе цифры.

Описания идентификаторов классов приведены в таблице 131.

Таблица 131 — Идентификаторы классов событий CEF

Класс	Название	Описание
60xxxx	Administrator	События связанные с действиями администратора
95xxxx	Calendar	Действия в интерфейсе календаря
15xxxx	Contacts	Действия с контактами пользователя
20xxxx	Group	Действия с группами

Класс	Название	Описание
90xxxx	Mail	Действия в интерфейсе почты
30xxxx	Resource	Действия, связанные с управлением ресурсами
80xxxx	System settings	Действия, связанные с системными настройками
10xxxx	User	Все действия связанные с пользователем
85xxxx	User settings	Действия, связанные с настройками пользователя
25xxxx	Орг.структура	Действия, связанные с настройкой орг.структуры

б) Вторые две цифры — подкласс события, описывает совершаемое действие.

в) Последние две цифры — уникальный идентификатор события в подклассе. Описания идентификаторов событий приведены в таблице 132.

Таблица 132 — Идентификаторы событий CEF

Номер события	Результат	Тип события	Пример
xxxx00	success (успех)	Операция выполнена успешно	Пользователь успешно создан
xxxx01	failure (ошибка)	Недостаточно прав	Недостаточно прав для создания пользователя
xxxx02	failure (ошибка)	Дублирование	Пользователь уже существует
xxxx03	failure (ошибка)	Отсутствие	Пользователь не найден
xxxx99	failure (ошибка)	Неизвестная ошибка	Неизвестная ошибка

Пример:

10 (Пользователь) +

10 (Создание пользователя) +

01 (Пользователь успешно создан)

= **101001**

2. Расшифровка обозначений полей журнала в CEF-формате приведена в таблице 133.

Таблица 133 — Поля событий CEF

Поле	Наименование	Тип данных	Длина (макс.)	Описание
cs1	deviceCustomString1	string	4000	Описание события в текстовом формате, которое пользователь видит до внесения изменений в редактируемое поле
cs2	deviceCustomString2	string	4000	Описание события в текстовом формате, которое пользователь видит после внесения изменений в редактируемое поле
cs3	deviceCustomString3	string	4000	
cs4	deviceCustomString4	string	4000	
dpriv	destinationUser Privileges			Роли, назначенные новому пользователю
dst	destinationAddress	ipv4 address		Адрес сервиса, где произошло событие
duid	destinationUserId	string	1023	Идентификатор созданной учетной записи
duser	destinationUserName	string	1023	Имя пользователя созданной учетной записи
dvc	deviceAddress	ipv4 address		IPv4-адрес устройства, где произошло событие
externalId	externalId	string	40	Внешний идентификатор события
fileCreateTime	fileCreateTime	timestamp		Время создания файла
fileId	fileId	string	1023	Идентификатор созданного файла
fileModificationTime	fileModificationTime	timestamp		Время редактирования файла
filePath	filePath	string	1023	Полный путь к созданному файлу
filePermission	filePermission	string	1023	Права доступа к файлу
fileType	fileType	string	1023	Тип созданного файла
fname	fileName	string	1023	Имя созданного файла
ID		string		

Поле	Наименование	Тип данных	Длина (макс.)	Описание
msg	message	string	1023	Сообщение, описывающее событие
Name		string		
oldFileID	oldFileID	string	1023	Идентификатор прежнего файла
oldFilePath	oldFilePath	string	1023	Полный путь к прежнему файлу
outcome	eventOutcome	string	63	Обозначает результат события, обычно 'success' (успех) или 'failure' (ошибка)
Severity	Severity	integer		Числовое значение от 0 до 10
src	sourceAddress	ipv4 address		Описывает IP-адрес источника события. Например: 192.168.0.1
start	startTime	timestamp		Время начала события
suid	sourceUserId	string	1023	Идентификатор пользователя-инициатора
suser	sourceUserName	string	1023	Имя пользователя-инициатора

3. Описание значений поля Severity (Важность события) приведено в таблице 134.

Таблица 134 — Значения поля Severity

Значение	Уровень важности	Описание
0	Critical (Критический)	Критичные события. Являются прямыми индикаторами атаки
1	High (Высокий)	События высокой важности, при множественных повторениях или в совокупности с другими событиями являются индикаторами атаки
2	Medium (Средний)	События средней важности, необходимы для восстановления последовательности действий в случае расследования
3	Low (Низкий)	События низкой важности, напрямую не свидетельствующие об атаке. Являются обогащающими событиями для расследования инцидента
4	Informational (Информация)	Информационные события используемые для обогащения данных
5	Unknown (Неизвестный)	События, возникающие при неизвестной ошибке

Пример записи в журнале

Запись в журнале (необработанное событие) в формате CEF на примере события

«Создание пользователя/Create a User»:

```
<8>2024-10-11T12:24:33+03:00 ca76ee11b91d homeros[1]: CEF:0|MyOffice|MyOffice  
Mailion|2.1|100100|Создание пользователя/Create a User|1|msg=Пользователь  
создан/User created outcome=success start=1728638672681  
suser=admin_tenant@devmail.example.net suid=59ed9c03-0c75-47e2-ac12-eacf6f775431  
duser=Баранов Виктория duid=4dcb233d-9c9a-4d4e-8dd2-f6b565d4e854 src=10.7.96.15  
dst=192.168.4.107 dhost=adonis.ucs-apps-1.zulu.example.net  
externalId=Неизвестно/Unknown dpriv=Обычный пользователь spriv=Администратор  
тенанта sourceServiceName=house
```

9 НАСТРОЙКА ИНТЕГРАЦИИ ADFS СРЕДСТВАМИ SAML

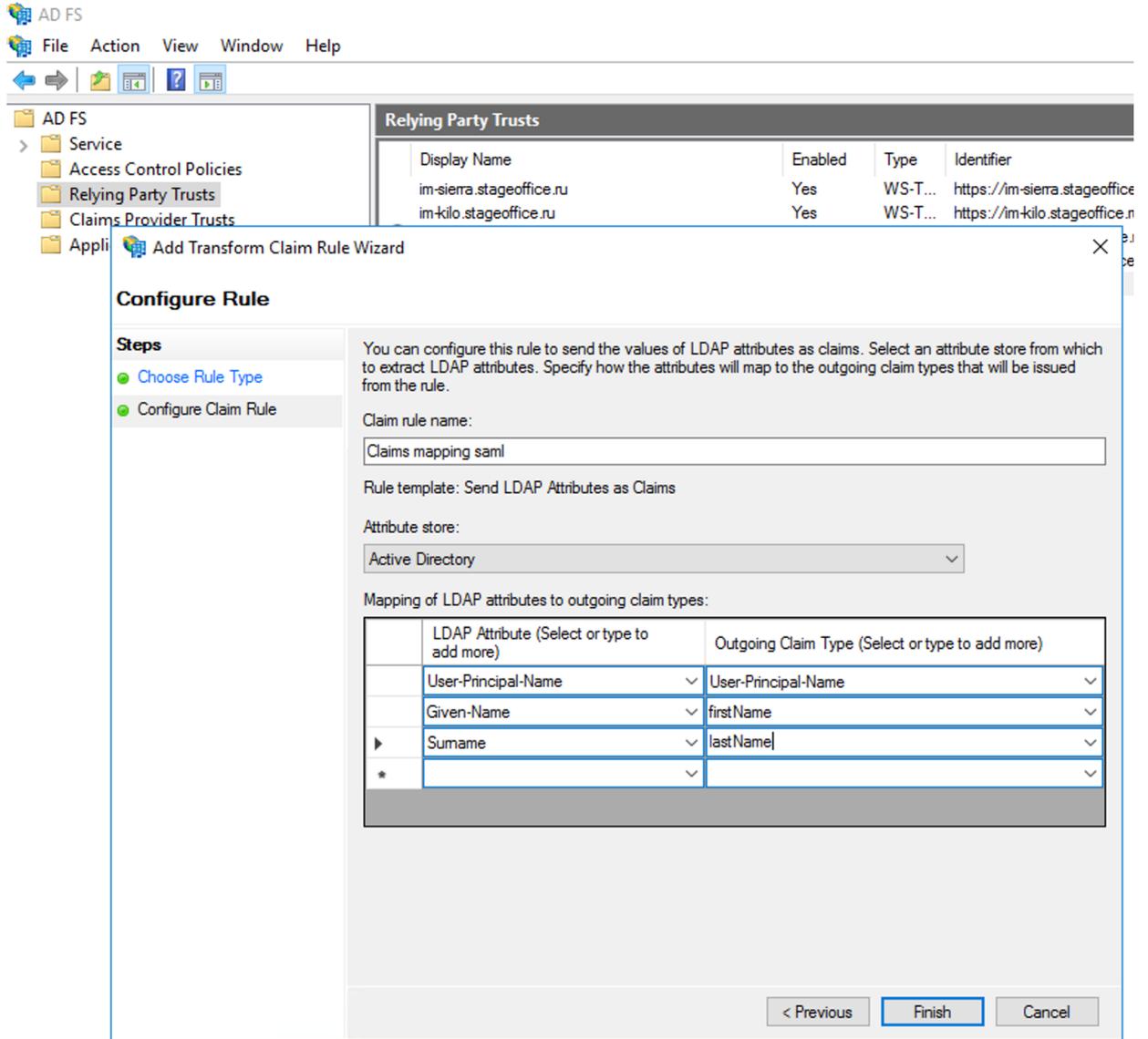
Интеграция с ADFS средствами SAML 2.0 позволяет регистрировать и аутентифицировать пользователей внешнего каталога в Mailion. После настройки интеграции на странице аутентификации появляется дополнительная кнопка авторизации через ADFS. При нажатии на кнопку происходит переадресация на страницу авторизации в AD. При аутентификации через ADFS в Mailion создается новый связанный пользователь. При последующей аутентификации будут использоваться данные ранее созданного пользователя.

9.1 Добавление SAML-сервиса в ADFS

Метаданные сервиса можно получить по ссылке

`https://<mailion_external_domain>/api/saml/metadata`. Можно указать эту ссылку при настройке или скачать файл и указать путь к нему. Настроить сопоставление атрибутов.

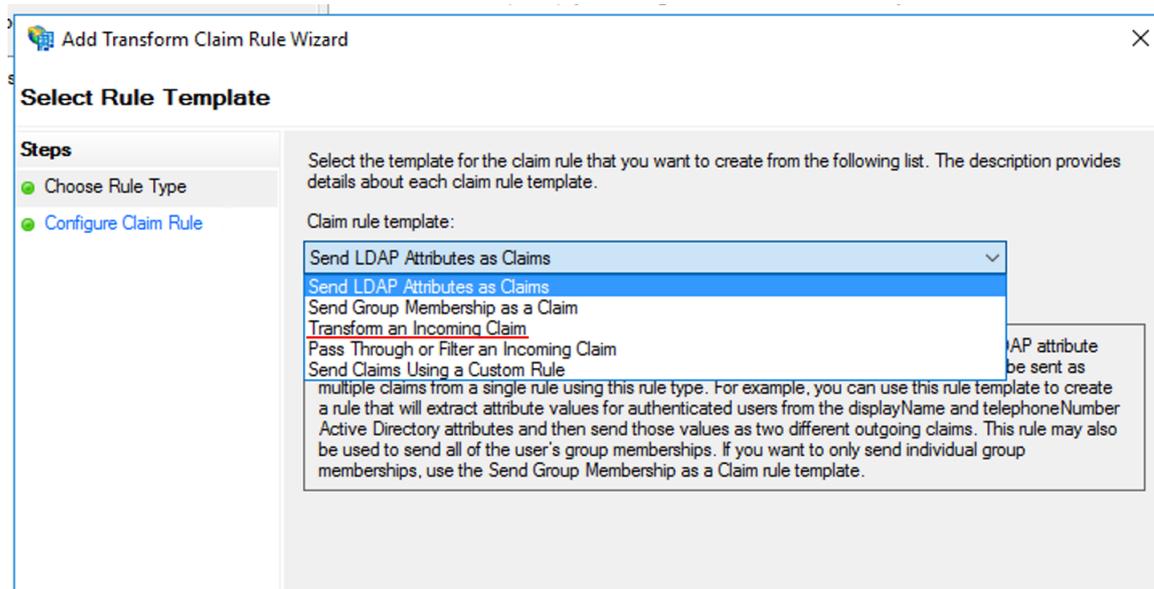
Добавить два правила **Claim mapping** и **Claim transformation rule**.



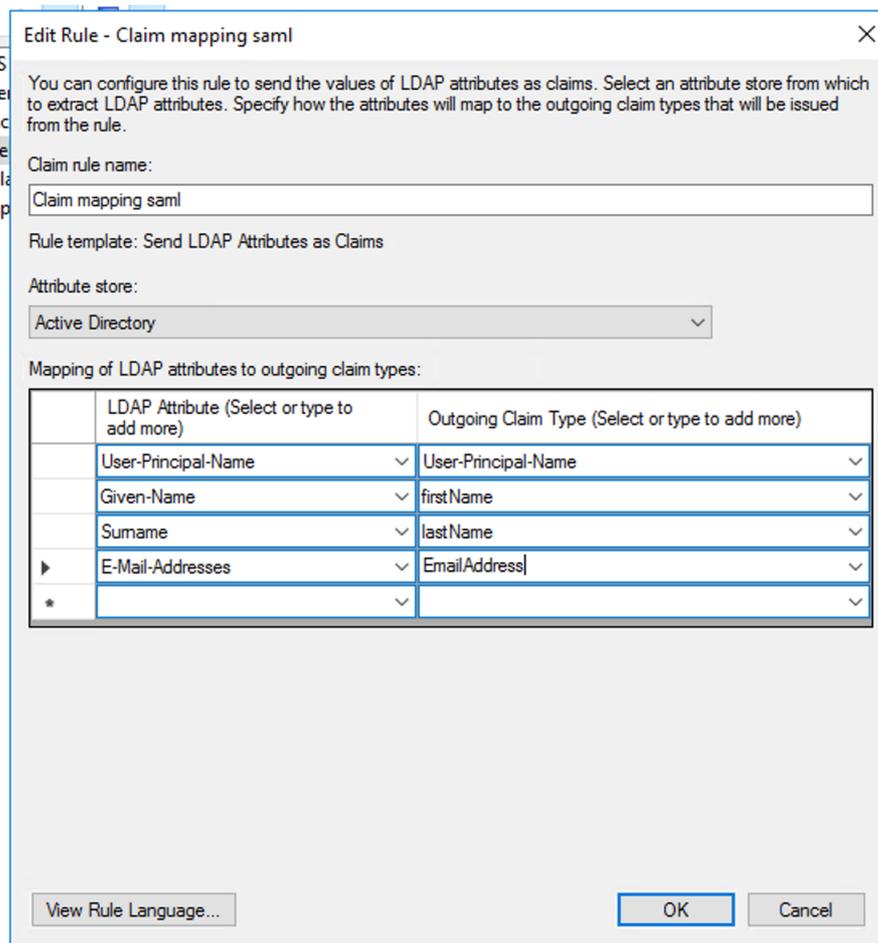
The screenshot shows the AD FS console with the 'Relying Party Trusts' pane selected. A dialog box titled 'Add Transform Claim Rule Wizard' is open, showing the 'Configure Rule' step. The rule name is 'Claims mapping saml', the template is 'Send LDAP Attributes as Claims', and the attribute store is 'Active Directory'. The mapping table is as follows:

	LDAP Attribute (Select or type to add more)	Outgoing Claim Type (Select or type to add more)
	User-Principal-Name	User-Principal-Name
	Given-Name	firstName
	Surname	lastName
*		

Добавить правило **Transform an Incoming Claim**. Для атрибута **Name ID** указать формат **Persistent Identifier**.



Если используется правило формирования почтового ящика EMAIL_GENERATION_RULE_FIRST_LAST_NAME то необходимо добавить атрибут **lastName**, для EMAIL_GENERATION_RULE_EXTERNAL_EMAIL понадобится почтовый ящик **EmailAddress**. Имена соответствующих атрибутов строго фиксированы (**firstName**, **lastName**, **EmailAddress**):



Edit Rule - Claim mapping saml

You can configure this rule to send the values of LDAP attributes as claims. Select an attribute store from which to extract LDAP attributes. Specify how the attributes will map to the outgoing claim types that will be issued from the rule.

Claim rule name:

Rule template: Send LDAP Attributes as Claims

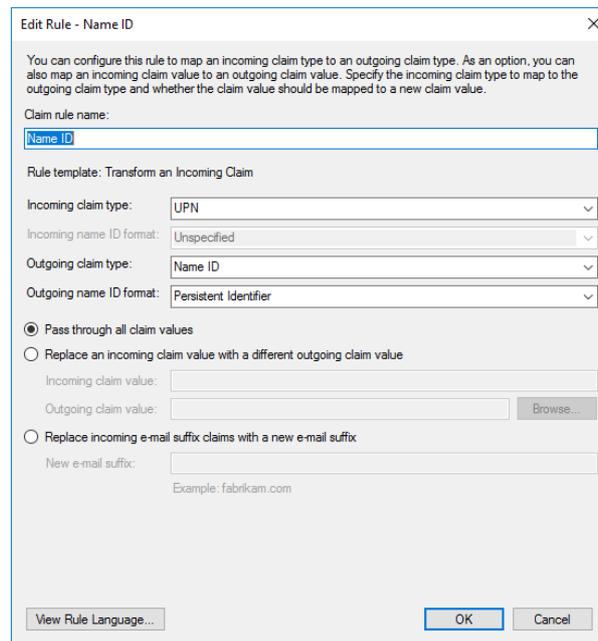
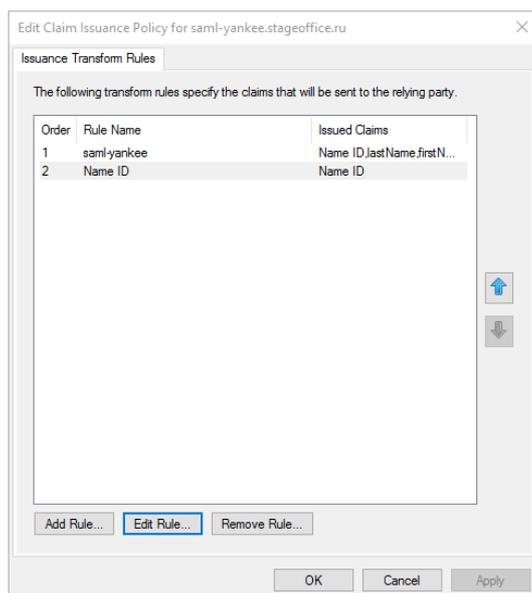
Attribute store:

Mapping of LDAP attributes to outgoing claim types:

	LDAP Attribute (Select or type to add more)	Outgoing Claim Type (Select or type to add more)
	User-Principal-Name	User-Principal-Name
	Given-Name	firstName
	Surname	lastName
▶	E-Mail-Addresses	EmailAddress
*		

View Rule Language...

В правиле **Claim transformation** указать формат **Persistent Identifier** для атрибута типа **Name ID**.



9.2 Создание интеграции в домене

1. Создать или обновить домен в Mailion (который необходимо присваивать пользователям авторизовавшимся через ADFS) и установить флаг --

```
features.is_saml=true:
```

```
nct_ministerium update_domain \
--config ministerium.json \
--admin.login admin_tenant \
--admin.password "****" \
--tenant_id *** \
--id ***domain_id*** \
--features.is_saml true \
--features.is_authorization true \
--features.is_mail true \
--features.is_service true \
--v
```

2. Создать SAML-интеграцию с указанием домена из п. 1:

```
nct_ministerium add_domain_saml_integration \  
--config ministerium.json \  
--admin.login admin_tenant \  
--admin.password "****" \  
--idp_sso_url "https://ad.example.net/adfs/ls" \  
--region_id "71efd978-a2dd-43df-98a0-aae94b3c82b" \  
--sp_entity_id "https://auth.example.net/api/saml" \  
--domain_id "78060a7e-ad7d-41a3-99eb-dc3fb77ealc2" \  
--idp_entity_id "http://ad.example.net/adfs/services/trust" \  
--email_generation_rule=1 \  
--idp_metadata_path federationmetadata.xml \  
--name "Войти с помощью ADFS" \  
--enabled true \  
--v
```

3. Проверить страницу авторизации на наличие кнопки «Войти с помощью ADFS».

Пояснения по параметрам

IDP SSO URL — искать в метаданных по тегу:

```
SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect",
```

атрибут Location. Пример:

```
<SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"  
Location="https://ad.example.net/adfs/ls/">
```

IDP Entity ID — идентификатор внешнего каталога можно получить из атрибута **entityID** в метаданных:

```
<EntityDescriptor ... entityID="http://ad.example.net/adfs/services/trust" ...>
```

IDP Metadata Path — путь к файлу с метаданными внешнего каталога. Ссылка для ADFS по умолчанию: https://<адрес_adfs>/federationmetadata/2007-06/federationmetadata.xml. Пример:

```
https://ad.example.net/federationmetadata/2007-06/federationmetadata.xml
```

9.3 Настройка плагина в house

Пример конфигурации:

```
https://api.example.net/saml {
  grpcmeta
  logging
  tracing
  request-report

  tls /etc/pki/tls/certs/bundle_example.net-
peer.pem /etc/pki/tls/private/example.net-key.pem

  sessions {
    saml_acs /acs
  }

  saml {
    plugin_auth {
      type basic
      basic {
        login saml_plugin_login
        password *****
      }
    }

    service_name saml_plugin

    route {
      acs /acs
      sso /sso
      metadata /metadata
    }

    x509_keypair {
      cert_path /etc/pki/tls/certs/service_cert.cert
      key_path /etc/pki/tls/private/service_key.key
    }

    minos {
      balancer_endpoints {
        hydra.ucs-apps-2.yankee.example.net:50053
        hydra.ucs-apps-1.yankee.example.net:50053
      }
      compression none
      load_balanced true
      request_timeout 10s
      service_name minos
      use_tls true
      use_tls_balancer true
    }

    daidal {
      balancer_endpoints {
        hydra.ucs-apps-2.yankee.example.net:50053
        hydra.ucs-apps-1.yankee.example.net:50053
      }
      load_balanced true
      use_tls true
      use_tls_balancer true
      compression none
      request_timeout 10s
      service_name daidal
    }
  }
}
```

```
    tls_settings {
      ca_file /etc/pki/tls/certs/ucs-infra-1.yankee.example.net-main-ca.pem
      client_auth_type require_and_verify_client_cert
      client_cert_file /etc/pki/tls/certs/house.ucs-frontend-
1.yankee.example.net-main-client.pem
      key_file /etc/pki/tls/private/house.ucs-frontend-1.yankee.example.net-
main-key.pem
      tls_min_version tls1_2
    }

    home_url https://auth-yankee@example.net
  }
  cors / {
    # ...
  }
}
```

Пример генерации ключей в блоке `x509_keypair`:

```
openssl req -x509 -newkey rsa:2048 -keyout saml_service.key -out saml_service.cert
-days 365 -nodes -subj "/CN=auth-yankee.example.net"
```

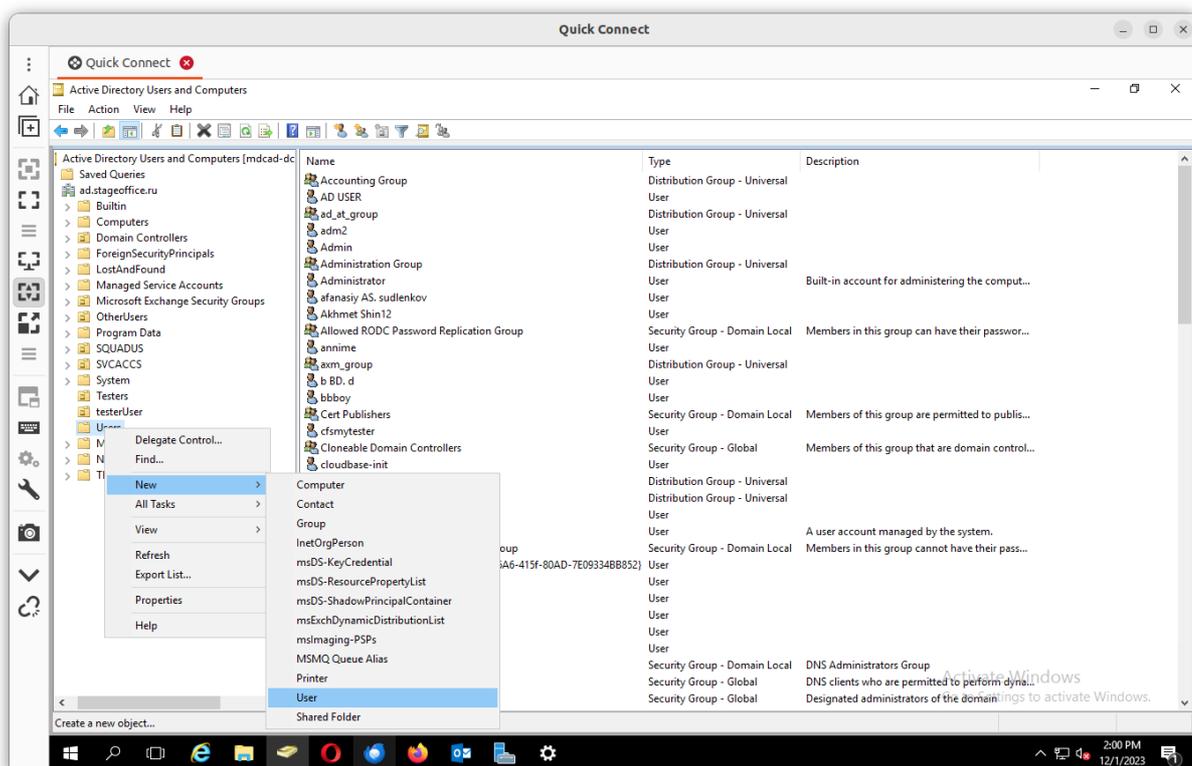
Дополнительно в **house** необходимо задать следующие параметры в папке с конфигурационными файлами Ansible на машине оператора в файле `/root/install_mailion/group_vars/ucs_setup/main.yml`):

```
house_ucs_api_cors_extend:
  origin:
    - "https://{{ ucs_external_adfs_domain }}"
ucs_external_adfs_domain: "adfs.installation.example.net"
```

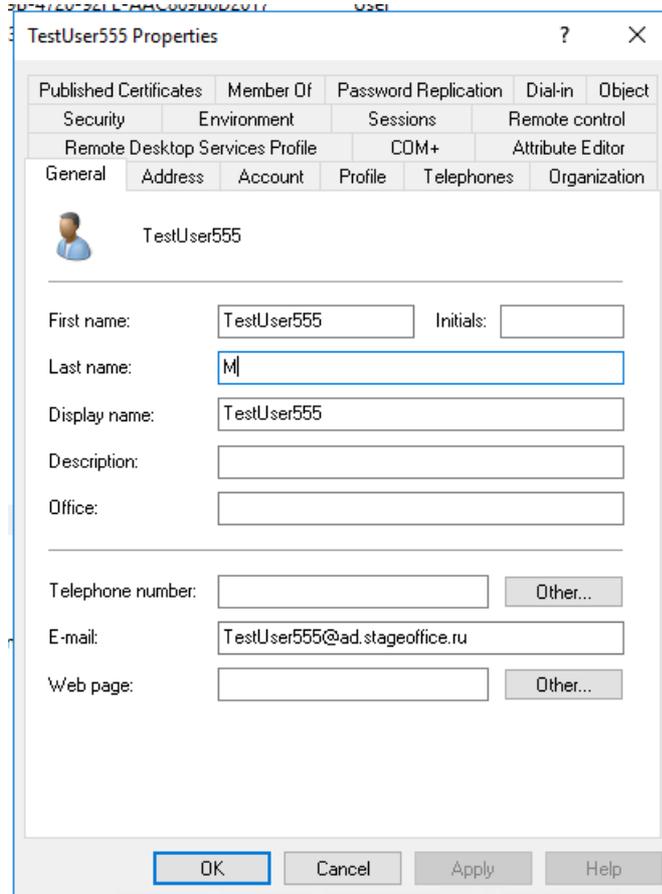
Затем необходимо выполнить развертывание **house**.

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

9.4 Создание пользователя в AD



Заполнить профиль необходимыми атрибутами в зависимости от правила генерации почтового ящика нового пользователя.



The image shows a screenshot of the 'TestUser555 Properties' dialog box in Active Directory. The 'General' tab is selected, and the user's name is 'TestUser555'. The 'Last name' field contains the letter 'M'. The 'E-mail' field contains 'TestUser555@ad.stageoffice.ru'. The 'OK' button is highlighted with a blue border.

Published Certificates	Member Of	Password Replication	Dial-in	Object
Security	Environment	Sessions	Remote control	
Remote Desktop Services Profile	COM+	Attribute Editor		

General | Address | Account | Profile | Telephones | Organization

TestUser555

First name: TestUser555 Initials:

Last name: M

Display name: TestUser555

Description:

Office:

Telephone number: Other...

E-mail: TestUser555@ad.stageoffice.ru

Web page: Other...

OK Cancel Apply Help

10 НАСТРОЙКА KERBEROS

Сетевой протокол Kerberos предназначен для обеспечения безопасной аутентификации. Для корректной работы с Kerberos необходимы следующие условия:

1. В Mailion необходимо добавить домен авторизации, соответствующий домену в AD.
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 А 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`.

10.1 Поддержка Kerberos для домена

Чтобы включить поддержку протокола Kerberos для домена необходимо:

1. На контроллере домена через оснастку AD рабочей станции администратора ОС Windows создать служебных пользователей **stagehttp**, **stageimap**, **stagesmtp**, **stageldap**, **stagegrpc** (рис. 58).

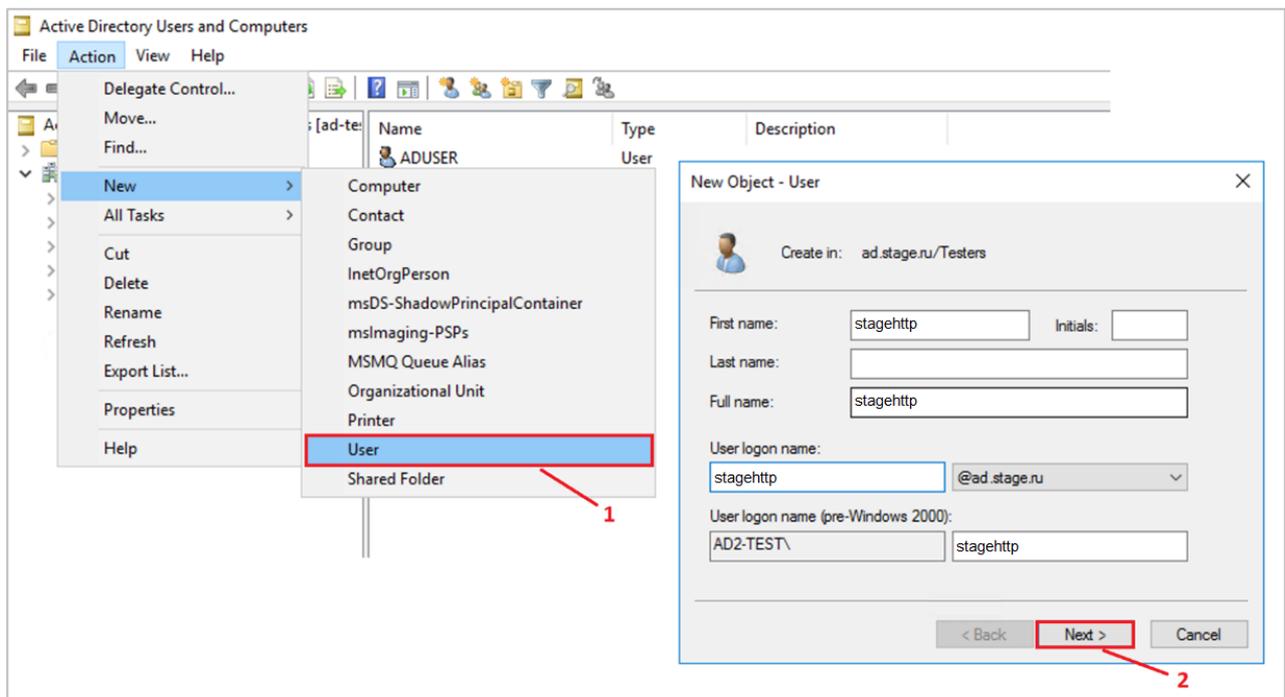


Рисунок 58 — Создание служебных пользователей

2. Запретить изменять пароль и установить пароль бессрочным (рис. 59).

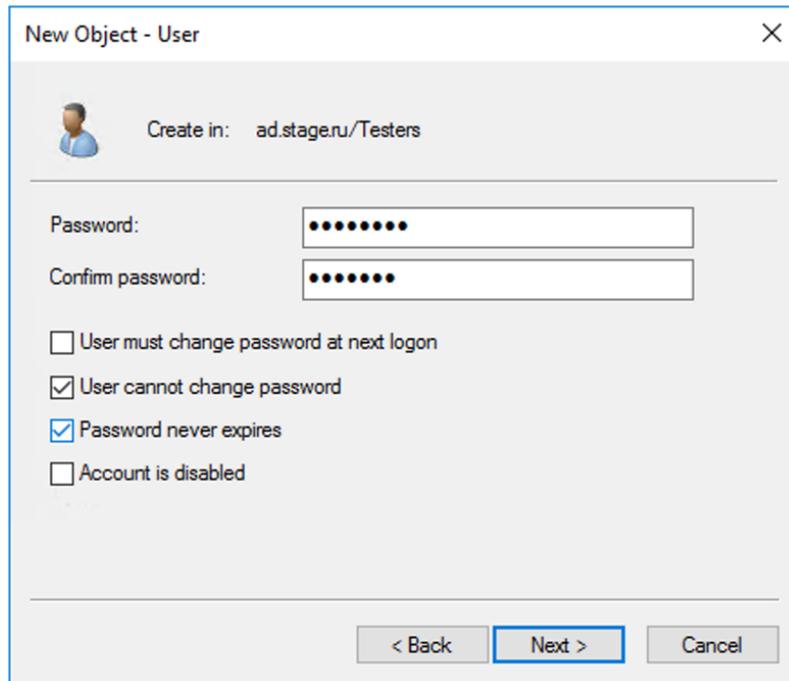


Рисунок 59 — Установка бессрочного пароля

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 135 перечислены SPN, соответствующие системным пользователям.

Таблица 135 — 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 для пользователя **stagehttp**):

1. Открыть командную строку или [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. Для каждого системного пользователя сгенерировать keytab-файл, содержащий пары Kerberos-принципалов и их ключей для зарегистрированного SPN, с помощью следующей команды:



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 установлен утилита для расширенного администрирования [nct-ministerium](#) и выполнить команду:

```
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 этом файле:

```
http://127.0.0.1:8080/session {
    .....
    kerberos
    sessions {
        login /create
        .....
    }
}
```

10.2 Настройка для веб-клиента

10.2.1 Настройка браузера для авторизации через Kerberos

Настройка браузера может выполняться пользователем с одной из следующих ролей:

- 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 на другую учетную запись 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 обратную наклонную черту: AD\ADUSR25).

10.2.2 Проверка конфигурации Kerberos

Перед тем как осуществить настройку необходимо выполнить проверку:

1. Проверить наличие Kerberos в конфигурационном файле:

```
...
kerberos
sessions
  { login /create
...

```

2. Посмотреть в консоль браузера, запрос `session/check` вместе со статусом 401 должен выдавать заголовок: `WWW-Authenticate: Negotiate`.

10.2.3 Настройка ОС Windows



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 60):

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 **Ок**.

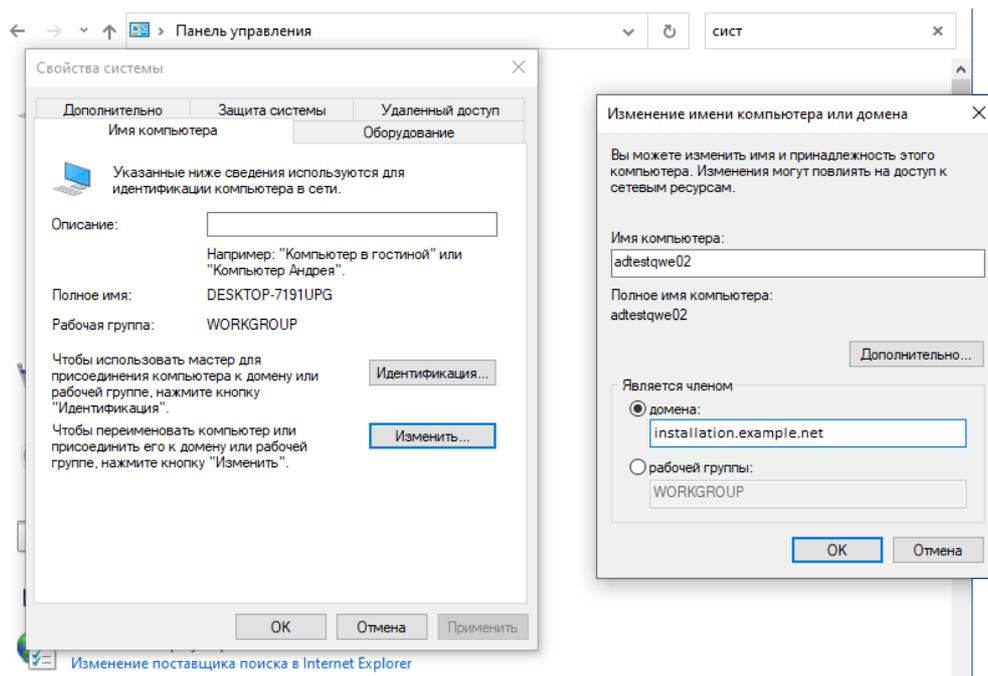


Рисунок 60 — Присоединение ПК к домену

10.2.4 Настройка браузеров в ОС Windows

10.2.4.1 Настройка в Internet Explorer



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 61).

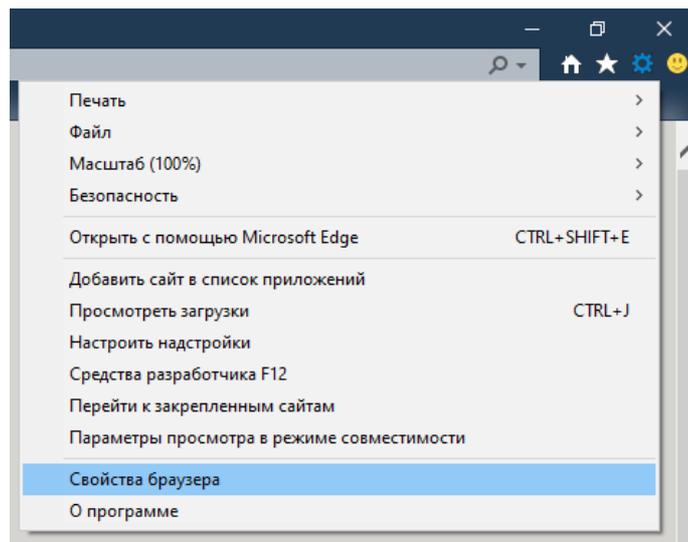


Рисунок 61 — Свойства браузера

2. На вкладке **Безопасность** необходимо выбрать зону **Местная интрасеть** и нажать кнопку **Сайты** (см. Рисунок 62).

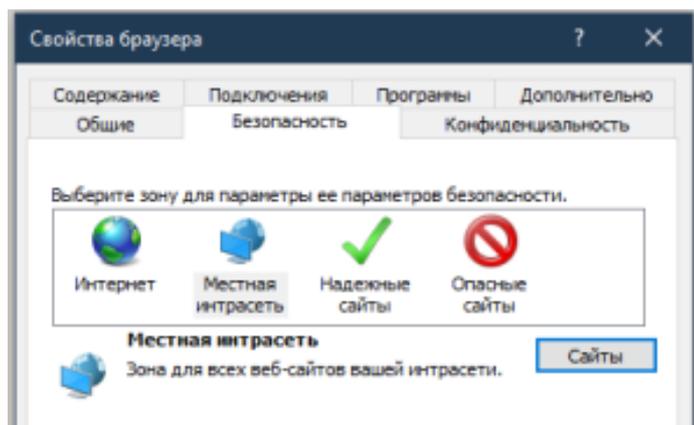


Рисунок 62 — Кнопка **Сайты**

3. Нажать кнопку **Дополнительно** (см. Рисунок 63).

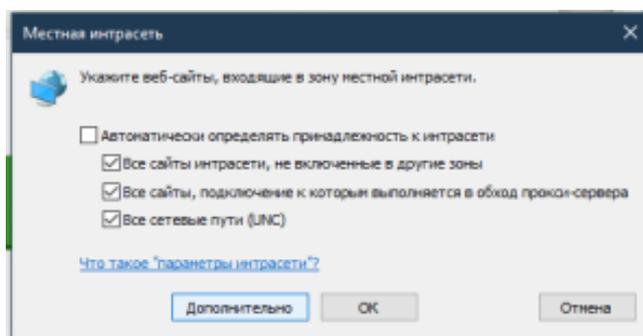


Рисунок 63 — Кнопка **Дополнительно**

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 64).

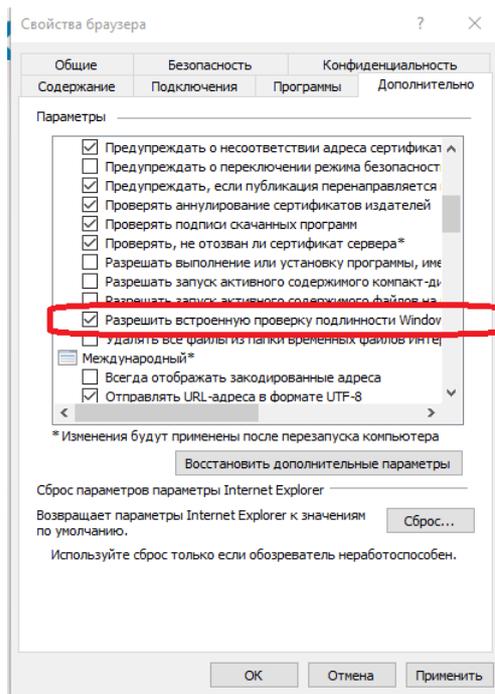


Рисунок 64 — Опция **Разрешить встроенную проверку подлинности Windows**

10.2.4.2 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.

10.2.4.3 Настройка Mozilla Firefox



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.

10.2.4.4 Настройка приложений в ОС Windows

10.2.4.4.1 Thunderbird

Чтобы настроить Kerberos в приложении Thunderbird необходимо выполнить следующие действия:

1. В Thunderbird из меню открыть **Параметры учетной записи** (см. Рисунок 65).

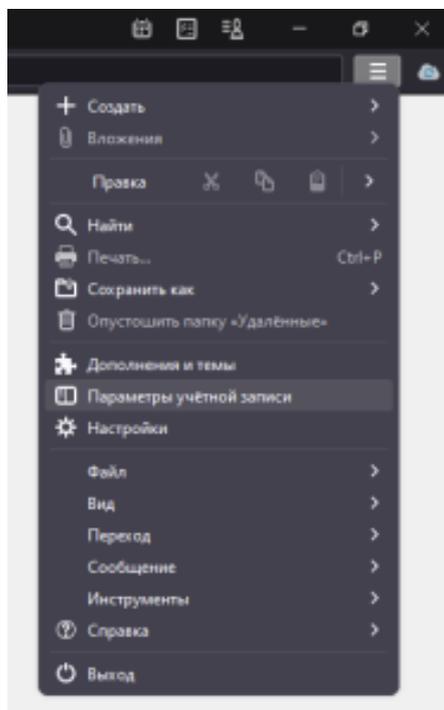


Рисунок 65 — Параметры учетной записи

2. На вкладке **Сервер исходящей почты (SMTP)** нажать кнопку **Добавить/Изменить** (см. Рисунок 66).

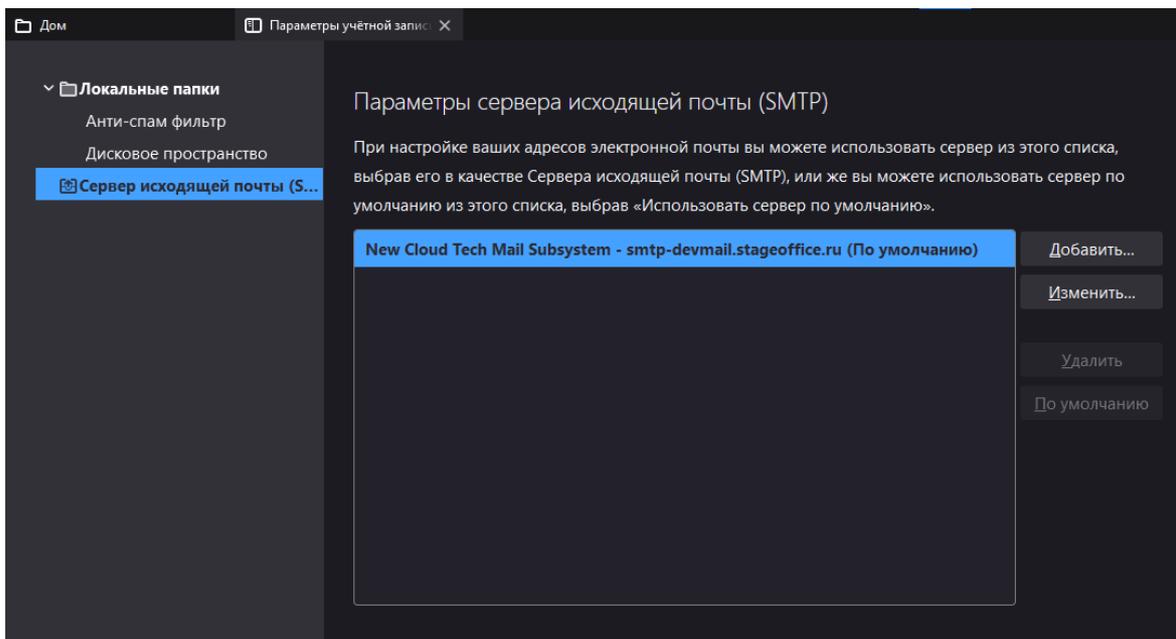


Рисунок 66 — Добавление сервера исходящей почты

3. В **Метод аутентификации** выбрать **Kerberos / GSSAPI**, заполнить оставшиеся необходимые поля и нажать кнопку **ОК** (см. Рисунок 67).

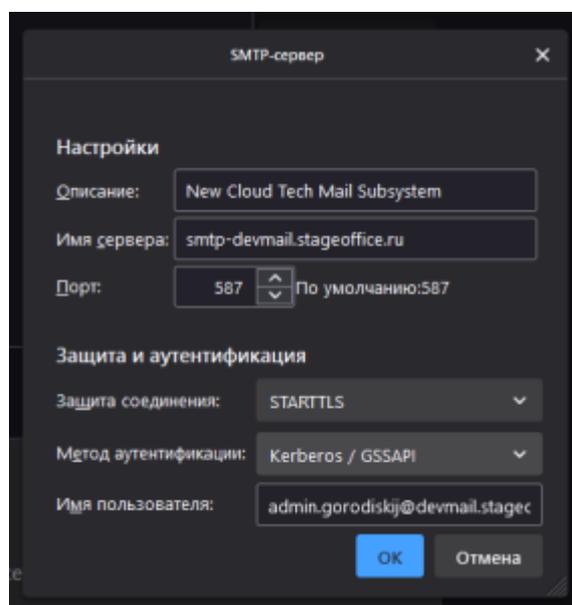


Рисунок 67 — Выбор метода **Kerberos / GSSAPI**

10.2.4.4.2 Microsoft Outlook

Чтобы настроить Kerberos в Microsoft Outlook необходимо выполнить следующие действия:

1. При настройке учетной записи необходимо выбрать **Kerberos** во всплывающем меню **Метод** (см. Рисунок 68).

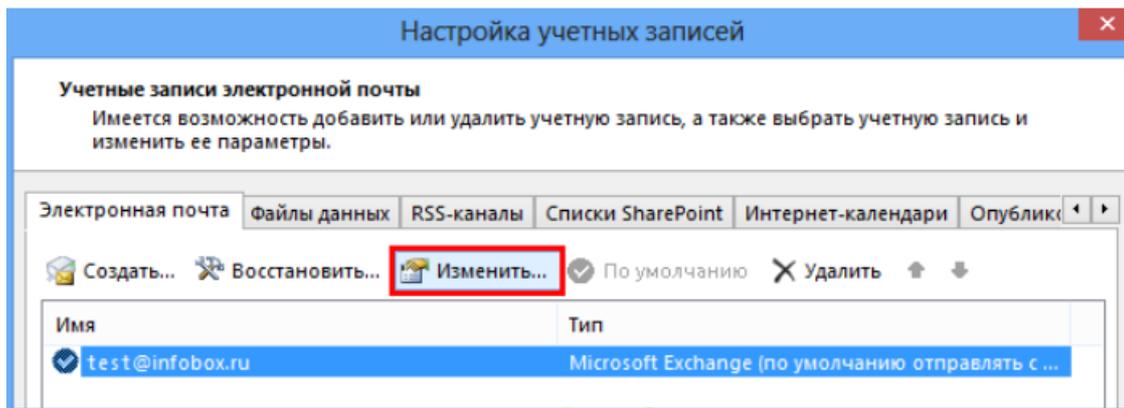


Рисунок 68 — Изменить учетную запись

2. Поля **Имя пользователя** и **Пароль** становятся скрыты, применяется авторизация через Kerberos.

11 ИНТЕГРАЦИЯ С ПО «МОЙОФИС ЧАСТНОЕ ОБЛАКО»

Начиная с версии 1.4 в ПО «Mailion» реализована интеграция с ПО «МойОфис Частное Облако». Данная интеграция дает возможность:

- отправлять пользователям почтовые уведомления о событиях (приветственное письмо, запрос/изменение прав доступа, восстановление пароля и т.п.);
- отправлять вложения, добавляемые из хранилища ПО «МойОфис Частное Облако»;
- возможность быстрого перехода из ПО «МойОфис Частное Облако» в ПО «Mailion».

Для настройки интеграции необходимо по очереди произвести настройку ПО «МойОфис Частное Облако» и ПО «Mailion» соответственно.

11.1 Настройка ПО «МойОфис Частное Облако»

Для настройки интеграции ПО «МойОфис Частное Облако» с ПО «Mailion» необходимо переустановить ПО «МойОфис Частное Облако» с указанием в YAML-файле следующих параметров установки (подробнее об установке см. документ «МойОфис Частное Облако. Система редактирования и совместной работы (СО) МойОфис. Руководство по установке»):

- `mail_integration_mode: none` — режим интеграции «без почты»;
- `common_mail_notification_enabled: true` — включить отправку почтовых уведомлений;
- `csp_allowed_frame_ancestors` — список адресов приложений, куда будет встраиваться виджет:
 - `demo1.example.net`;
 - `demo2.example.net`.

Далее необходимо в режиме **Администрирование** настроить исходящие системные сообщения SMTP-сервера (подробнее см. в документе «МойОфис Частное Облако. Руководство администратора»). После этого в ПО «МойОфис Частное Облако» будет доступна возможность отправки почтовых уведомлений пользователям.

Чтобы добавить ярлык ПО «Mailion» на главную навигационную страницу и в меню приложений ПО «МойОфис Частное Облако» необходимо подготовить специальный бандл и применить его к инсталляции ПО «МойОфис Частное Облако». Подробнее о подготовке бандла см. документ «МойОфис Частное Облако. Система редактирования и совместной работы (СО) МойОфис. Руководство по установке».

Данную операцию необходимо будет повторять после каждого обновления ПО «МойОфис Частное Облако».

Для синхронизации каталогов пользователей, сквозной авторизации и аутентификации пользователей в обеих системах необходимо после переустановки ПО «МойОфис Частное Облако» в ETCD настроить параметры OAuth2-клиента по пути `nct/co/config/wfe/oauth2_clients:`

```
mailion: {
  "client_secret": "mailionpass",
  "redirect_uri": "https://dummyurl.com/callback"
}
```



В системе присутствует ограничение: не реализован автоматический локальный выход (logout) в одной из систем при выходе пользователя из другой системы.

11.2 Настройка ПО «Mailion»

В ПО «Mailion» интеграция настраивается в сервисах **minos** и **house**: в конфигурационных файлах этих сервисов предусмотрены секции, отвечающие за работу сервисов ПО «МойОфис Частное Облако».

Параметры из конфигурационного файла **minos** необходимы для авторизации в сервисе ПО «МойОфис Частное Облако» через протокол авторизации OAuth2-клиента, и эти данные должны соответствовать настройкам в ПО «МойОфис Частное Облако».

Пример секции в конфигурационном файле **minos**:

```
"cloud": {
  "auth_uri": "https://auth-installation.example.ru/oauth2/srv/token"
  "client_id": "mailion",
  "client_secret": "mailionpass",
  "redirect_uri": "https://dummyurl.com/callback"
}
```

Параметры секции описаны в таблице 136.

Таблица 136 — Параметры для интеграции с ЧО в конфигурационном файле **minos**

Параметр	Описание
auth_uri	Конечная точка API для получения токена
client_id	Идентификатор OAuth2-клиента
client_secret	Секрет OAuth2-клиента
redirect_uri	URL-адрес перенаправления домена, участвует в процессе только как дополнительный параметр верификации



Строки **redirect_uri** в секции конфигурационного файла **minos** и в параметрах OAuth2-клиента ПО «МойОфис Частное Облако» должны быть одинаковыми.

Пример секции в конфигурационном файле **house**:

```
ucreader {
  ...
  cloud_attach_url https://coapi-installation.example.ru/api/v1/files
  cloud_attach_reader_path cloud
  cloud_link_attach_reader_path cloud_link
  ...
}
```

Параметры секции описаны в таблице 137.

Таблица 137 — Параметры для интеграции с ЧО в конфигурационном файле **house**

Параметр	Описание
cloud_attach_url	URL-адрес вложения в облаке
cloud_attach_reader_path	Путь к чтению вложения в облаке
cloud_link_attach_reader_path	Ссылка на путь к чтению вложения в облаке

Для загрузки и прикрепления ссылок или файлов к письму в приложении фронтенда необходимо указать ссылку на ПО «МойОфис Частное Облако». Это можно сделать с помощью переменной `external_files_link`, которая указывается в секции `integrations` конфигурационного файла `~/install_mailion/contrib/mailion/<тип инсталляции>/group_vars/ucs_setup/main.yml` на машине оператора:

```
integrations:
  co_auth:
    auth_uri: "https://auth-installation.example.net/oauth2/srv/token"
    client_id: "{{ vault_secrets['cloud_office_client_id'] }}"
    client_secret: "{{ vault_secrets['cloud_office_client_secret'] }}"
    external_api_domain: "coapi-installation.example.net"
    external_files_link: "files-installation.example.net"
    redirect_uri: "https://dummyurl.com/callback"
  ...
mailion_integrations:
  co_auth: true
```

Пример команд включения и отключения интеграций:

```
mailion_integrations:
  co_auth: false
  google_oauth: false
  ...
minos_integrations_co_auth_enabled: "{{ mailion_integrations.co_auth }}"
house_integration_co_enabled: "{{ mailion_integrations.co_auth }}"
```

12 ИНТЕГРАЦИЯ С ПО SQUADUS

Для настройки интеграции необходимо выполнить следующие действия:

1. В файл `/root/install_mailion/group_vars/ucs/main.yml` добавить переменные с адресами сервера Squadus:

```
scc_squadus_endpoint: "im.example.com"
mars_scc_squadus_host: "scc.squadus-vks-apps-1.im.example.com"
```



В переменной `mars_scc_squadus_host` адрес хоста с сервисом **scc** имеет вид:

```
scc.{{ inventory_hostname_apps-1_from_squadus }}.
```

В новых версиях ПО Squadus сервис **scc** переименован в **scandium**, таким образом адрес сервиса будет иметь вид:

```
scandium.{{ inventory_hostname_apps-1_from_squadus }}.
```

2. Добавить переменные с сертификатами для подключения к серверу Squadus.

В переменные необходимо текстом вставить содержимое файлов сертификатов от сервиса **scc** или **scandium** на стенде ПО Squadus. Сервис находится на серверах в Ansible-группе **squadus_meet_apps**. Сами сертификаты находятся в папке `/srv/tls/`.

Пример добавления переменных:

```
# в переменную прописать содержимое из файла:
# squadus-infra-1.im.example.com-main-ca.pem для кластерной установки
# или squadus.im.example.com-main-ca.pem для standalone установки
mars_scc_ca_file:
  -----BEGIN CERTIFICATE-----
  -----END CERTIFICATE-----
# из файла scc.squadus-vks-apps-1.im.example.com-main-client.pem или
scandium.squadus-vks-apps-1.im.example.com-main-client.pem
mars_scc_client_cert_file:
  -----BEGIN CERTIFICATE-----
  -----END CERTIFICATE-----
# из файла scc.im.example.com-main-key.pem или scandium.squadus-vks-apps-
1.im.example.com-main-key.pem
mars_scc_key_file:
  -----BEGIN EC PRIVATE KEY-----
  -----END EC PRIVATE KEY-----
```

3. В этом же файле, в разделе `mailion_integrations` для Squadus выставить флаг `true`.

```
mailion_integrations:
  squadus: true
```

4. После обновления конфигурационного файла применить изменения, запустив плейбук обновления настроек для сервисов **mars**, **perseus**, **kongur**.

```
ansible-playbook playbooks/main.yml [-i hosts_cluster.yml] --diff --limit
ucs_calendar,ucs_catalog --tags mars, perseus, kongur
```

5. Создать в ПО Squadus пользователя с ролью **user**. Затем необходимо авторизоваться под данным пользователем и перейти в настройки профиля. В настройках токена выписать персональный токен. Пример полученного токена:

```
Token: 8ulIBn_VbpH2v5lG67UWfrer4NmWcL3wvxfvOPgAQ8Z  
Your user Id: ZrPewL7roNaezo5Tz
```

6. Добавить данный токен в тенант с помощью [расширенного администрирования](#).

```
[root@ucs-infra-1 ~]# nct_ministerium --config /srv/ministerium/config.json  
update_tenant --tenant_id b16286af-7628-4ce0-a346-69c09302bda8 --  
squadus_params.link https://im-echo.example.com/ --  
squadus_params.squadus_chat_params.api_key  
7TbrjpmZHzHX3cgrRuasG9VfJchLo3ELbGieb3iNBB --  
squadus_params.squadus_chat_params.bot_id EPoitL3byrHWqbSww
```

Пример ответа:

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



Для успешной синхронизации в Mailion и в Squadus должен быть использован один и тот же пользователь.

13 ИНТЕГРАЦИЯ С ПО SKYPE4BUSINESS

Начиная с версии 1.5 в ПО «Mailion» реализована интеграция с ПО Skype4Business. Для включения интеграции необходимо выполнить следующие действия:

1. В файле `/root/install_mailion/group_vars/ucs/main.yml` активировать сервис **ares**. Для этого необходимо установить флаг `true` для параметра `ares_service_enabled`:

```
ares_service_enabled: true
```

2. В этом же файле прописать параметры доступа:

```
vcs:
  type:
    skype_4_business:
      ares_vcs_type: "skype_4_business"
      ares_vcs_endpoint: "vcs_skype_endpoint"
      ares_vcs_login: "vcs_skype_login"
      ares_vcs_password: "Password"
      ares_vcs_skip_insecure_tls: true
```

3. После обновления конфигурационного файла установить сервис **ares** с помощью команды:

```
ansible-playbook playbooks/mailion/calendar.yml [-i hosts_cluster.yml] -diff --
limit ucs_calendar --tags ares
```

14 НАСТРОЙКА ОГРАНИЧЕНИЙ ДЛЯ ПОИСКА ПО ВЛОЖЕНИЯМ

Работа в 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 или ограничение числа потоков одновременного парсинга.

14.1 Ограничение размера вложений для поиска

Данное ограничение гарантирует, что сервис **viper** не будет чрезмерно расходовать ресурсы памяти и сохранит функцию поиска по вложениям для большинства пользователей. Таким образом, поиск будет осуществляться только по вложениям, размер которых не превышает 1 Мбайт.



Настройка лимита сохраняется только в конфигурационных файлах внутри сервиса.

14.2 Отключение поиска по вложениям

Во избежание перегрузки ресурсов оперативной памяти и процессора добавлена возможность отключить поиск по вложениям. Для этого в конфигурационный файл сервиса **viper** для ansible-роли добавлен параметр `viper_disable_attachment_indexing`.

При значении `true` сервис **viper** не будет индексировать вложения при сохранении писем, что приведет к снижению затрат памяти и нагрузки на процессор.

Пример секции в конфигурационном файле:

```
viper_disable_attachment_indexing: true
```

14.3 Ограничение скорости парсинга

Для ограничения числа потоков, которые одновременно выполняют индексацию вложений, в конфигурационный файл сервиса **viper** Mailion добавлен параметр

```
viper_client.tripoli.attach_parsing_thread_limit.
```

Настройка данного параметра влияет на следующие показатели:

- пиковая потребляемая память (чем меньше потоков, тем меньше одновременных вложений будет в памяти сервиса);
- 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 обработки большого количества писем с вложениями за единицу времени замедляет процессы, то для ограничения потребления ресурсов можно уменьшить этот параметр. При этом общая скорость индексации вложений соответственно уменьшится.

По умолчанию значение этого параметра равно количеству доступных виртуальных ядер на виртуальной машине, где запущен сервис **viper**.

Пример секции в конфигурационном файле **inventory.yml**:

```
viper_client:  
  tripoli:  
    attach_parsing_thread_limit: 1
```

15 НАСТРОЙКА ПОИСКА В ПОЧТЕ

Для сервиса поиска по почте и календарю **mailbek** реализованы специальные настройки конвертора запросов, позволяющие управлять расширением последнего слова поискового запроса. Эти настройки задают минимальную длину последнего слова, при которой, в случае отсутствия после него пробелов, это слово будет расширено подстановочным знаком '*' (джокером). Например, запрос `Анна Фил` преобразуется в `Анна Фил*`, если минимальная длина последнего слова установлена равной 3 или меньше, и не будет преобразован, если это значение равно 4. Значение по умолчанию: 3.

Запрос `Анна Фил` расширяться не будет — пробел свидетельствует о том, что запрос введен полностью.

Чтобы включить эту настройку, следует вставить в конфигурационный файл **mailbek_search** следующую секцию:

```
"compatibility": {  
  "mailbek": {  
    "min_auto_jocker_length": 2  
  }  
}
```

Чтобы отключить, необходимо убрать эту секцию из файла.

16 ОБНОВЛЕНИЕ 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}'
```

17 РЕЗЕРВНОЕ КОПИРОВАНИЕ И ВОССТАНОВЛЕНИЕ ОТДЕЛЬНЫХ СЕРВИСОВ

17.1 Dispersed Object Store

В конфигурационном файле Dispersed Object Store (DOS) каждого узла необходимо задать 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 предусмотрены два вида резервного копирования:

1. Локальное — создание резервной копии RocksDB на одном узле, не зависит от конфигурации установки.
2. Кластерное — набор локальных резервных копий всех узлов, которые снимаются для всего кластера в одно время. Кластерные копии можно снять только в кластерной конфигурации.

При работе с обоими видами резервного копирования необходимо учитывать следующие факторы:

- и для автономной (Standalone), и для кластерной инсталляции используется один API; при выполнении операций резервного копирования и восстановления необходимо использовать идентификатор, который вернул DOS;
- идентификаторы локальных и кластерных копий имеют один тип и не зависят от типа инсталляции.

Для восстановления из резервной копии требуется перезапустить узел в режиме восстановления. Для этого необходимо:

1. Остановить узел.
2. В файле конфигурации установить для поля `server.recovery_mode` значение `true`.
3. Запустить узел.

После этого узел готов к восстановлению. После восстановления необходимо вернуть для этого поля значение `false`.



В режиме восстановления узел подключается к кластеру так же, как и в нормальном режиме, но не обрабатывает клиентские запросы.

17.1.1 Снятие резервных копий

Резервное копирование может выполняться вручную или по расписанию.

Для выполнения резервного копирования по расписанию предусмотрен набор переменных Ansible, описанных в таблице 138.

Таблица 138 — Переменные Ansible для резервного копирования

Имя переменной	Тип	Значение по умолчанию	Описание
<code>dispersed_object_store_backup_full_job_cron_enabled</code>	bool	true	Включить создание полной резервной копии по cron-заданию
<code>dispersed_object_store_backup_job_period</code>	str	monthly	Периодичность создания резервной копии

Для создания резервной копии вручную требуется выполнить команду:

```
ucs_dispersed_object_store leader backup run
```

В ответе на успешный запрос резервного копирования поле `backup_time` содержит идентификатор операции. Пример ответа на выполнение команды:

```
{
  "error": {
    "module": 24,
    "code": 200,
    "msg": "succeeded",
    "details": []
  },
  "backup_time": "1693763682", // идентификатор операции резервного копирования
  "rsm_dump_path":
  "/srv/docker/dispersed_object_store/backup/rsm_dump.1693763682.json"
}
```

17.1.2 Проверка статуса резервного копирования

Проверка статуса резервного копирования выполняется с помощью команды:

```
ucs-dispersed-object-store-client leader backup verify \
  --backup_time 1693763682 // идентификатор операции резервного копирования
  --local=<true или false> // тип проверки (локальная/кластерная)
```

Флаг `local` задает тип проверки:

`local = false`: проверка для кластерного резервного копирования (т. е. локальных копий на всех узлах кластера), такую команду можно выполнить только на лидере кластера;

`local = true`: проверка локального резервного копирования, такую команду можно выполнить на любом узле кластера, при этом необходимо использовать внутренний идентификатор операции локального резервного копирования RocksDB.

Данная команда осуществляет проверку:

- возможности восстановления DOS из резервной копии;
- существования и успешности создания резервной копии;
- контрольных резервных копий на всех узлах.

17.1.3 Получение списка резервных копий

Пример команды получения списка резервных копий:

```
ucs-dispersed-object-store-client leader backup list
```

Для кластерной инсталляции команда возвращает список кластерных копий; выполнить ее можно только на лидере кластера. Для инсталляции Standalone команда возвращает список локальных резервных копий.

Возвращаемые коды состояния операций резервного копирования описаны в таблице 139.

Таблица 139 — Расшифровка кодов состояния операций резервного копирования

Код	Описание
1	Резервное копирование успешно завершено
2	Резервное копирование завершилось неудачей
3	Резервное копирование выполняется

17.1.4 Восстановление из резервной копии

При потере или повреждении данных можно восстановить их из резервных копий. Имеются следующие ограничения:

- если данные были повреждены, то для их восстановления из резервных копий необходимо сначала удалить данные в основном хранилище;
- восстанавливаются все данные — например, нельзя восстановить только бэкенд.

17.1.4.1 Восстановление в инсталляции Standalone

Чтобы восстановить данные из резервной копии в инсталляции Standalone, необходимо:

1. В случае потери виртуальной машины запустить на машине оператора установку Standalone DOS на новый узел через Ansible с помощью команды:

```
ansible-playbook -i inventory/ucs_dos_shard.yml -t dispersed_object_store -l <host> -e dispersed_object_store_raft_initialize=false -b playbooks/main.yml
```

2. Остановить узел.

```
docker stop dispersed_object_store
```

3. Смонтировать сетевые диски с резервными копиями DOS в каталог `/srv/docker/dispersed_object_store/backup/` или скопировать данные этого каталога с сервера резервного копирования.

4. На узле DOS в секцию `server` конфигурационного файла `/srv/docker/dispersed_object_store/conf/config.json` добавить параметр `recovery_mode = true`.

5. Запустить DOS с помощью команды:

```
docker start dispersed_object_store
```

6. Запустить команду восстановления из резервной копии:

```
ucs-dispersed-object-store-client leader backup restore \  
--backup_time 1212121212 // идентификатор операции резервного копирования
```

7. Остановить узел:

```
docker stop dispersed_object_store
```

8. На узле DOS в секцию `server` конфигурационного файла `/srv/docker/dispersed_object_store/conf/config.json` добавить параметр `recovery_mode = true`.

9. Запустить DOS помощью команды:

```
docker start dispersed_object_store
```

17.1.4.2 Восстановление в кластерной инсталляции

Чтобы восстановить данные из резервной копии в инсталляции Standalone, необходимо:

1. В случае потери виртуальных машин запустить на машине оператора установку кластерной конфигурации DOS на новый узел через Ansible с помощью команды:

```
ansible-playbook -i inventory/ucs_dos_shard.yml -t dispersed_object_store -l  
<host> -e dispersed_object_store_raft_initialize=false -b playbooks/main.yml
```

2. Остановить все узлы.

```
docker stop dispersed_object_store
```

3. Смонтировать сетевые диски с резервными копиями DOS в каталог `/srv/docker/dispersed_object_store/backup/` или скопировать данные этого каталога с сервера резервного копирования.

4. Скопировать дампы состояний Raft в виде JSON-файла `/srv/docker/dispersed_object_store/backup/rsm_dump.*.json` с узла-лидера в каталоги для резервного копирования остальных узлов.

5. На всех узлах DOS в секцию `server` конфигурационного файла `/srv/docker/dispersed_object_store/conf/config.json` добавить параметр `recovery_mode = true`.

6. Запустить DOS на всех узлах с помощью команды:

```
docker start dispersed_object_store
```

7. Выполнить команду восстановления из резервных копий:

```
ucs-dispersed-object-store-client leader backup restore \  
--backup_time 1693767209 \  
--local=false \  
--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" \  
команда запускается с узла [1]: перечисление конечных точек
```

8. Остановить все узлы:

```
docker stop dispersed_object_store
```

9. На всех узлах DOS в секцию `server` конфигурационного файла `/srv/docker/dispersed_object_store/conf/config.json` добавить параметр `recovery_mode = true`.

10. Запустить DOS на всех узлах с помощью команды:

```
docker start dispersed_object_store
```

17.1.4.3 Восстановление части узлов кластера

Данным методом восстановления можно воспользоваться, если число сохранивших работоспособность узлов в кластере DOS не меньше значения `quorum`. Если выведено из строя больше одного узла, но меньше `quorum`, восстанавливать узлы следует последовательно. Для этого необходимо:

1. В случае потери виртуальной машины запустить на машине оператора установку Standalone DOS на новый узел через Ansible с помощью команды:

```
ansible-playbook -i inventory/ucs_dos_shard.yml -t dispersed_object_store -l <host> -e dispersed_object_store_raft_initialize=false -b playbooks/main.yml
```

2. Остановить узел:

```
docker stop dispersed_object_store
```

3. Смонтировать сетевые диски с резервными копиями DOS в каталог `/srv/docker/dispersed_object_store/backup/` или скопировать данные этого каталога с сервера резервного копирования.

4. На узле DOS в секцию `server` конфигурационного файла `/srv/docker/dispersed_object_store/conf/config.json` добавить параметр `recovery_mode = true`.

5. Запустить DOS с помощью команды:

```
docker start dispersed_object_store
```

6. Если идентификатор операции резервного копирования не известен, его можно найти в списке `backup.ID` локальной резервной копии по пути `.rocksdb_info.timestamp`.

7. Запустить команду восстановления из резервной копии:

```
ucs-dispersed-object-store-client leader backup restore \  
--backup_time 1693767209 // идентификатор операции резервного копирования  
--local=true // восстановление только одного узла
```

8. Остановить узел:

```
docker stop dispersed_object_store
```

9. На узле DOS в секцию `server` конфигурационного файла `/srv/docker/dispersed_object_store/conf/config.json` добавить параметр `recovery_mode = true`.

10. Запустить DOS с помощью команды:

```
docker start dispersed_object_store
```

17.2 Redis

Резервное копирование баз данных Redis не требуется, так как в большей части экземпляров Redis, используемых в ПО «Mailion», хранится кеш. Исключением является Redis для сервиса **dafnis** — в ней хранятся данные о квотах пользователей. Если резервная копия была сделана ранее, при восстановлении хранилища с квотами будут получены некорректные данные фактически используемой квоты и ее расчета в системе. Поэтому, в случае потери данных этого хранилища лучше использовать механизм пересчета квот с помощью команды **recount_quotas** через интерфейс командной строки.

17.2.1 Резервное копирование

Данные Redis находятся в каталоге `/srv/docker/redis/data/dump.rdb`. Для создания резервной копии необходимо:

1. Обновить дампы базы через интерфейс командной строки **redis-cli** с помощью следующей команды, указав порт и пароль:

```
docker exec -ti redis redis-cli -p <порт> -a <пароль> save
```

2. Остановить сервис **redis**, выполнив команду:

```
docker stop redis
```

3. Скопировать дамп **dump.rdb** в резервный каталог.

17.2.2 Восстановление

Для восстановления данных Redis необходимо:

1. Остановить сервис **redis** с помощью команды:

```
# docker stop redis
```

2. Удалить текущие файлы баз из рабочего каталога:

```
# mv dump.rdb dump.rdb.old
# mv appendonly.aof appendonly.aof.old
```

3. Скопировать дампы `dump.rdb` в каталог с данными **redis** `/srv/docker/redis/data/` (необходимо проверить права на файл с базой).

4. Отключить AOF: в конфигурационном файле `/srv/docker/redis/conf/redis.conf` задать для параметра `appendonly` значение `no`.

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 конфигурационном файле `/srv/docker/redis/conf/redis.conf` задать для параметра `appendonly` значение `yes`.

9. Запустить сервис **redis** с помощью команды:

```
# docker start redis13
```

17.3 MongoDB

17.3.1 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/`.



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.



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/#basic-mongodump-operations)

[https://docs.mongodb.com/manual/tutorial/backup-and-restore-tools/#restore-a-database-with-mongorestore.](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>



При развертывании стенда с шардированием MongoDB нужна иная стратегия резервного копирования, не поставляемая на данный момент в продукте.

17.3.2 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'
```



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.--preserveUUID>

17.4 Подсистема поиска

Для резервного копирования данных подсистемы поиска 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 кеша поиска по пользователям, письмам, событиям и пр. можно полностью воссоздать. Подробная информация приведена в разделах [Ручная синхронизация данных поиска по пользователям \(dirbek\)](#) и [Ручная переиндексация почтовых ящиков](#).

17.4.1 Ручная синхронизация данных поиска по пользователям (dirbek)

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
```

17.4.2 Ручная переиндексация почтовых ящиков и календарных событий в поиске

В состав поставки входит вспомогательный скрипт, с помощью которого можно провести переиндексацию ящиков или событий. Установка скрипта производится на машине с ролью **ucs_infrastructure** по пути **/bin/ucs-sreindexer**.

Перед тем, как запустить переиндексацию, в конфигурационный файл необходимо внести логин и пароль администратора тенанта, в котором будет производиться переиндексация. Файл конфигурации находится на машине с ролью **ucs_infrastructure** по пути **/srv/docker/sreindexer/conf/config.yml**. Часть, которую необходимо изменить:

```
---
auth:
  basic:
    login: <...>
    password: <...>
```

При запуске скрипта можно вызвать справку по его использованию 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 переиндексацию всех почтовых ящиков:

```
[root@ucs-infra-1 ~]# /bin/ucs-sreindexer mail <tenant_id>
```

Команда на переиндексацию всех календарных событий:

```
[root@ucs-infra-1 ~]# /bin/ucs-sreindexer cal <tenant_id>
```

17.5 Vault



Механизм резервного копирования в Vault будет работать только при использовании типа хранилища **Raft**. В Mailion до версии 2.1 по умолчанию использовался тип хранилища **File**. Если в системе используется этот тип хранилища, необходимо выполнить миграцию данных в хранилище типа **Raft** (см. раздел [Миграция данных в хранилище типа Raft](#)).

Для работы механизма резервного копирования и восстановления данных необходимо убедиться, что заданы следующие переменные:

```
# Эта настройка включает использование хранилища типа Raft и при развертывании
Vault добавляет в конфигурацию другие узлы из группы ucs_vault
vault_cluster_mode: true
# Эта настройка выключает тип хранилища File (несовместим с резервным копированием
vault)
vault_persistent_storage_enabled: false
```

17.5.1 Миграция данных в хранилище типа Raft

1. Перед миграцией данных необходимо вручную выполнить резервное копирование секретов Vault. Для этого необходимо зайти в веб-интерфейс Vault и сохранить имеющиеся секреты.
2. Зайти по SSH на машину, где установлен Vault.
3. Создать на этой машине файл по пути `/srv/docker/vault/conf/migrate.hcl` со следующим содержимым:

```
storage_source "file" {
  path = "/vault/file"
}
storage_destination "raft" {
  path = "/vault/file"
}

cluster_addr = "https://vault.ucs-db-1.mailion.example.ru:8201"
```

4. Зайти в контейнер Vault:

```
docker exec -it vault bash
```

5. Выполнить внутри контейнера команду:

```
export VAULT_TOKEN='СОХРАНЕННЫЙ НА ЭТАПЕ ИНИЦИАЛИЗАЦИИ Vault ТОКЕН'
vault operator migrate -config /vault/config/migrate.hcl
```

6. Переустановить Vault, задав переменную:

```
vault_cluster_mode: true
```

7. Создать файл по пути `/srv/docker/vault/data/raft/peers.json` со следующим содержимым:

```
[
  {
    "id": "<Идентификатор узла Vault>",
    "address": "<адрес узла Vault>:<кластерный порт узла Vault>",
    "non_voter": false
  }
]
```

Пример:

```
[
  {
    "id": "ucs-db-1.mailion.example.net",
    "address": "ucs-db-1.mailion.example.net:8201",
    "non_voter": false
  }
]
```

8. Перезапустить контейнер Vault:

```
docker restart vault
```

9. Распечатать Vault, используя ключ, сохраненный на этапе инициализации Vault.

17.5.2 Установка механизма резервного копирования

Механизм резервного копирования Vault устанавливается при выполнении плейбука `backup.yml`. Чтобы установка была выполнена, необходимо, чтобы была задана переменная:

```
vault_backup_cron_enabled: true
```

По умолчанию резервное копирование Vault выполняется по расписанию каждый день в 01:00 в каталог `/srv/backups/vault/` на машине из группы `ucs_infra`. Для изменения периодичности резервного копирования можно изменить следующие переменные:

```
vault_backup_cron_time_day: "*"
vault_backup_cron_time_hour: 1
vault_backup_cron_time_minute: 0
vault_backup_cron_time_month: "*"
vault_backup_cron_time_weekday: "*"

```

17.5.3 Ручной запуск резервного копирования

Для ручного запуска резервного копирования данных Vault необходимо:

1. Предварительно выполнить настройку путем запуска плейбука `backup.yml`.
2. Зайти по SSH на машину из группы `ucs_infra`.
3. Запустить скрипт `/srv/docker/vault_backup/backup_scripts/vault_backup.sh`.

17.5.4 Восстановление

Для восстановления данных Vault необходимо:

1. Зайти по SSH на инфраструктурную машину из группы `ucs_infra`.

2. Зайти в контейнер Vault:

```
docker exec -it vault bash
```

3. Выполнить команду:

```
vault operator raft snapshot restore -tls-skip-verify /srv/backups/vault/<snapshot-id>
```

где `snapshot-id` — файл снимка данных

18 РЕЗЕРВНОЕ КОПИРОВАНИЕ И ВОССТАНОВЛЕНИЕ ВСЕЙ ИНСТАЛЛЯЦИИ MAILION

18.1 Первоначальная настройка

1. Необходимо зафиксировать значение `region-id` на машине оператора. Это значение можно получить на машине группы `ucs_infra` следующей командой:

```
root@ucs-infra-1:~# nct_ministerium --config=/srv/ministerium/config.json  
get_regions
```

```
{  
  "Response": {  
    "changed": false,  
    "failed": false,  
    "msg": "ok"  
  },  
  "regions": [  
    {  
      "id": "71efd978-a2dd-43df-98a0-aae94b3c82b",  
      "slug": "ru-1",  
      "display_name": "region ru-1"  
    }  
  ]  
}
```

Затем, используя полученное значение, добавить в файл `group_vars/ucs_<имя_инсталляции>/main.yml` на машине оператора следующую переменную:

```
dorofej_region_id: "71efd978-a2dd-43df-98a0-aae94b3c82b"
```

2. Чтобы обеспечить возможность повторить конфигурацию инсталляции Mailion, необходимо сделать резервную копию каталога с настройками Ansible (`/root/install_mailion` на машине оператора). Копию рекомендуется сохранить на сервер резервного копирования.
3. Если для Mailion выделены виртуальные серверы, необходимо зафиксировать конфигурацию ресурсов виртуальных машин, их названия и количество. Наиболее оптимальным решением для этого является использование инструмента [Terraform](#).
4. Для надежности папку `/srv/backup` на машине группы `ucs_infra` следует подключить к серверу резервного копирования в виде сетевого диска (используя NFS, SMB или другой способ).
5. Если используется Vault, необходимо настроить резервное копирование данного сервиса по инструкции в разделе [Vault](#).
6. Если требуется резервное копирование сертификатов, проверить наличие включенной переменной `certs_backup_cron_enabled`.

7. Сохранить информацию о разметке диска следующей командой:

```
# ansible ucs -m ansible.builtin.shell -b -a "df -h" > filesystem.txt
```

Полученный файл `filesystem.txt` скопировать на сервер резервного копирования.

18.2 Создание резервных копий

Для создания резервных копий следует использовать утилиту `nct_backuper-cli`, которую необходимо установить на сервер резервного копирования. В конфигурацию утилиты необходимо добавить параметры подключения к сервису `sox`.

Пример конфигурационного файла утилиты:

```
{
  "grpc_gateway": "grpc.example.com:3142",
  "login": "backup-user",
  "password": "PassWord@@",
  "tls_settings": {
    "ca_file": "/home/backup/certs/zulu/ca.pem",
    "client_cert_file": "/home/backup/certs/zulu/client.pem",
    "key_file": "/home/backup/certs/zulu/key.pem"
  },
  "storage_path": "/srv/mailion_backup_data/zulu/liliya_1",
  "log_level": "info",
  "max_stored_revisions": 3
}
```

В конфигурации указываются логин и пароль специального пользователя, созданного для выполнения процедур резервного копирования и восстановления. Предусмотрено два вида таких пользователей:

- пользователь уровня инсталляции — может осуществлять работу с любым тенантом инсталляции;
- пользователь уровня отдельного тенанта — может осуществлять работу только в пределах своего тенанта.

Пользователь уровня инсталляции создается в процессе развертывания решения и имеет логин по умолчанию `backup` (может меняться в настройках инсталлятора). Пользователь уровня тенанта создается администратором инсталляции с помощью CLI-утилиты системного администрирования `nct_ministerium`, для этого в утилите предусмотрена команда `create_tenant_backuper`.

На машине группы `ucs_infra` получить значение `tenant-id` командой `nct_ministerium --config=/srv/ministerium/config.json list_tenants`.

Для запуска процедуры создания резервных копий на сервере резервного копирования необходимо перейти в каталог, где сохранены резервные копии и выполнить три команды:

```
# nct_backuper-cli --config backuper-cli.config.json catalog backup -f --tenant-id bafe525a-c5df-490e-ae1d-d31335f7e57c

# nct_backuper-cli --config backuper-cli.config.json calendar backup -f --tenant-id bafe525a-c5df-490e-ae1d-d31335f7e57c

# nct_backuper-cli --config backuper-cli.config.json mail backup -f --tenant-id bafe525a-c5df-490e-ae1d-d31335f7e57c --region-id 71efd978-a2dd-43df-98a0-1ae94b3c82b
```

Эти команды можно добавить в `bash`-скрипт и прописать в `cron` для запуска по расписанию.

18.3 Восстановление данных

Для восстановления данных из резервных копий необходимо:

1. Подготовить новую аппаратную инфраструктуру, аналогичную по числу серверов и ресурсов той, на которой работала прежняя инсталляция Mailion.
2. Выполнить разметку дисков на серверах, аналогичную той, которая использовалась для прежней инсталляции Mailion, и зафиксировать изменения в `/etc/fstab`. Разметка диска была сохранена в файле `filesystem.txt` на сервере резервного копирования.
3. Восстановить на машине оператора каталог `/root/install_mailion`.
4. Если используется Vault, восстановить данные по инструкции описанной в разделе [Vault](#).
5. Восстановить сертификаты Mailion, для этого скопировать с сервера резервного копирования на машину группы **ucs_infra** соответствующий архив и распаковать его командой `tar xf 2025_01_18_0100.tar.gz -C /`.
6. Так как плейбук **ministerium** заново создает тенант, домен и пользователей, это может вызвать ошибку при восстановлении. Установку Mailion необходимо запускать с обязательным пропуском плейбуков **ministerium**. Для этого следует использовать команду:

```
# ansible-playbook playbooks/main.yml --diff --skip-tags=ministerium
```

Более подробно процедура установки описана в разделе «Запуск установки» Руководства по установке Mailion.

7. Перейти в каталог с резервными копиями и выполнить три команды для восстановления данных:

```
# nct_backuper-cli --config backuper-cli.config.json catalog full-restore --
tenant-id bafe525a-c5df-490e-ae1d-d31335f7e57c

# nct_backuper-cli --config backuper-cli.config.json calendar full-restore --
tenant-id bafe525a-c5df-490e-ae1d-d31335f7e57c

# nct_backuper-cli --config backuper-cli.config.json mail full-restore --tenant-id
baf525a-c5df-490e-ae1d-d31335f7e57c --region-id 71efd978-a2dd-43df-98a0-
a1ae94b3c82b
```

19 АВТОМАТИЧЕСКАЯ НАСТРОЙКА КЛИЕНТА «МОЙОФИС ПОЧТА»

Автоматическая настройка конфигурации клиента включает следующие шаги:

1. Проверка наличия А-записи DNS `autoconfig.*`.
2. При отсутствии результата от шага 1 проверяется А-запись `autoconfig-*`.
3. Выполняется POST-запрос на найденный адрес с передачей логина и пароля пользователя, а в ответ приходят параметры конфигурации почтового клиента.

19.1 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 140.

Таблица 140 — Поля секции файла, содержащей адресные книги

Параметр	Тип	Описание
addressbookPasswordUri	string	Специальное поле для настольного клиента — URI домена
login	string	Логин для доступа к CardDAV
addressbookUri	string	URI DAV-коллекции книг

19.2 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 141.

Таблица 141 — Описание полей файла секции файла, содержащей календари

Параметр	Тип	Описание
calendarPasswordUri	string	Специфическое поле для desktop клиента. URI домена.
calendarUri	string	URI DAV-коллекции календарей
login	string	Логин для доступа к CalDAV
eventAttachSizeLimit	string	Максимальный размер вложения в событие в байтах

19.3 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 142.

Таблица 142 — Описание полей секции файла, содержащей календари

Параметр	Тип	Описание
exists	string	Используется ли наш LDAP сервер, как глобальная адресная книга
binddn	string	DN подключения (Bind DN)
description	string	Специфическое поле для desktop клиента. Описание книги.
basedn	string	База поиска
uri	string	Uri LDAP сервера (включает протокол и порт)
searchFilter	string	Фильтр поиска по книге
autocompleteFilter	string	Фильтр для поиска в клиентском автокомплите
fullname	string	Имя и фамилия пользователя из адресной книги, если есть, если нет, то false



Областью действия для LDAP-поиска будет поддерево. Паролем будет являться пароль пользователя

19.4 Настройки FCM

Пример секции файла, содержащей клиентские настройки FCM:

```
"fcm":
{
  "exists": true,
  "ios":
  {
    "api_key": "AIzaSyAFmtvX4xZB3SUSH1Wn9Nsvl02yI4ulKK8",
    "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 143.

Таблица 143 — Описание полей секции файла, содержащей клиентские настройки FCM

Параметр	Тип	Описание
exists	string	Используется ли FCM



Остальные поля используются мобильными клиентами, пояснения по их значениям необходимо уточнять у разработчиков мобильных клиентов

19.5 Другие ответы сервера

Описание примеров сообщений об ошибке приведены в таблице 144.

Таблица 144 — Описание примеров сообщений об ошибке

Пример	Тело сообщения
Неправильный логин или пароль, код ответа 403	<pre>{ "message": "You don't have the permission to access the requested resource. It is either read-protected or not readable by the server." }</pre>
Не передан обязательный параметр, код ответа 400	<pre>{ "message": {"password": "password required"} }</pre>
Ошибка сервера, код ответа 500	<pre>{"message": "Internal Server Error"}</pre>

20 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

20.1 Сбор и анализ журналов

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.

20.1.1 Syslog-ng tier

На каждый сервер в поставке устанавливается экземпляр сервиса **syslog-ng**, именуемый **tier syslog-ng**. Данный экземпляр имеет следующие задачи:

- сбор всех данных, поступающих в него 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 в единый коллектор **syslog-ng**;
- использовать буфер на диске для отправляемых данных (подробнее см. на [официальном сайте разработчика](#));
- настраивать параметры гарантии доставки (по умолчанию гарантия доставки отключена, подробнее см. на [официальном сайте разработчика](#)).

20.1.2 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 от других серверов системы с распределением их по отдельным каталогам.

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);
- фильтры для соединений с других серверов на основе имени сервера (опция).

20.1.3 Доставка журналов до сервера журналирования

Практически каждый сервис в поставке самостоятельно устанавливает соединение с сервером журналирования и отправляет на него свои журналы. Дополнительно на сами контейнеры установлены правила отправки журналов на сервер журналирования через **docker log-driver**.

Такое разделение вызвано следующими доводами:

- **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, которое не может самостоятельно отправлять журналы на серверы журналирования, 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 журналирования.

20.1.4 Настройка параметров Syslog-ng

Описание настройки параметров **Syslog-ng** приведено в таблице 145.

Таблица 145 — 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)

Параметр	Тип	Описание
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
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

20.2 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 МТА 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 МТА (**postfix**) в виде **milter** расширения. Общая схема подключения и работы **milter** и МТА (см. Рисунок 69).

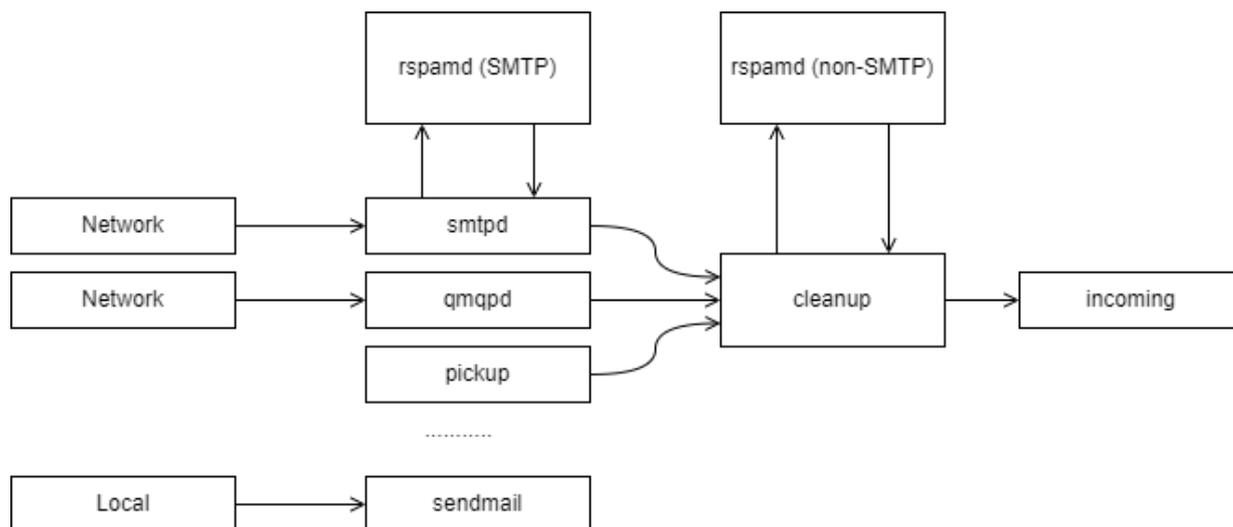


Рисунок 69 — Схема подключения и работы militer и MTA

Типы Militer:

- 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 militer.

Более подробную информацию про **Rspamd** можно найти на [официальном сайте разработчика](#), про [архитектуру postfix](#) и [работу militer в postfix](#) на официальном сайте **postfix**.

Для настройки **Rspamd** в ПО «Mailion» следует использовать переменные роли **Rspamd**. Подробная информация о них описана в таблице 146.

Таблица 146 — 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 <code>docker run --rm -it localhost:5000/nct_rspamd:1.2 rspamadm dkim_keygen -b 2048 -s mail</code>

Параметр	Пример заполнения	Описание
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
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	

Параметр	Пример заполнения	Описание
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 (<u>на пользователя</u>)
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
test_composite_1:		

Параметр	Пример заполнения	Описание
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**.

20.3 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 147.

Таблица 147 — 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 в таблице 148.

Таблица 148 — Настройка переменных ролей Rspamd

Параметр	Пример заполнения	Описание
rspamd_kse_enabled	true	Включение модуля Касперский для rsmamd
rspamd_kse_endpoints	"kaspersky.example.net:8085"	Список серверов управления антивирусной защитой Касперский



Продукт Kaspersky Scan Engine не является частью поставки ПО «Mailion»

20.4 Аудит действий

Чтобы получить события для аудита, необходимо выполнить запрос:

```
nct-ministerium get_audit_events_by_app_name \
--config juliett.json \
--c \
--v \
--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 149.

Таблица 149 — Параметры 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

20.4.1 Поиск событий безопасности пользователя

20.4.1.1 Вход в систему

Для входа в систему и создания сессии 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 150.

Таблица 150 — Параметры запроса на вход в систему и создания сессии

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": "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
}
```

20.4.1.2 Смена пароля пользователя

Для смены пароля пользователя 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 151.

Таблица 151 — Параметры 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
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
}

```

20.4.2 Поиск событий безопасности администратора

20.4.2.1 Операции над пользователем

20.4.2.1.1 Создание пользователя

Для создания пользователя 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 152.

Таблица 152 — Параметры запроса на создание пользователя

Параметр	Тип	Обязательный	Описание
admin.login	Str	+	Логин администратора тенанта
admin.password	Str	+	Пароль администратора тенанта

Параметр	Тип	Обязательный	Описание
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
}

```

20.4.2.1.2 Обновление профиля пользователя

Для обновления профиля пользователя 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 153.

Таблица 153 — Параметры 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
}
```

20.4.2.1.3 Удаление пользователя

Для удаления пользователя 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 154.

Таблица 154 — Параметры 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
}
```

20.4.2.2 Операции над доменом

20.4.2.2.1 Создание домена

Для создания пользователя 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 155.

Таблица 155 — Параметры 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
}

```

20.4.2.2.2 Обновление домена

Для обновления домена 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-1c8e-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 156.

Таблица 156 — Параметры запроса на обновление домена

Параметр	Тип	Обязательный	Описание
admin.login	Str	+	Логин администратора тенанта
admin.password	Str	+	Пароль администратора тенанта
method	Str	+	Метод API

Параметр	Тип	Обязательный	Описание
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
}

```

20.4.2.2.3 Удаление домена

Для удаления домена 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 157.

Таблица 157 — Параметры 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
}
```

20.4.2.3 Операции над ресурсом

20.4.2.3.1 Создание ресурса

Для создания ресурса 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 158.

Таблица 158 — Параметры 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
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": "{\n\"tls_settings\":{\n\"ca_file\":\n\"/builds/0/mail-back-
tests/certs/ca.pem\", \n\"client_cert_file\":\n\"/builds/0/mail-back-
tests/certs/client.crt.pem\", \n\"server_cert_file\":\n\"\", \n\"key_file\":
\n\"/builds/0/mail-back-tests/certs/client_key.pem\", \n\"server_name_override\":\n\"\",
\n\"client_auth_type\":\n\"\", \n\"tls_min_version\":\n\"\",
\n\"prefer_server_cipher_suites\":false, \n\"use_tls_bundle\":false}, \n\"cox\":
{\n\"endpoint\":\n\"grpc-install.example.net:3142\", \n\"balancer_endpoint\":\n\"hydra.ucs-
apps-1.install.example.net:50053\", \n\"balancer_endpoints\":null, \n\"service_name\":
\n\"cox\", \n\"load_balanced\":false, \n\"use_tls\":true, \n\"use_tls_balancer\":false,
\n\"request_timeout\":\n\"10s\", \n\"max_send_size\":\n\"0B\", \n\"max_recv_size\":\n\"0B\",
\n\"compression\":\n\"none\", \n\"is_external\":false}, \n\"token-name\":\n\"ucs-access-
token\", \n\"admin\":{\n\"login\":\n\"admin_tenant@install.example.net\", \n\"password\":
\n\"bKv9jqZ9PSwqKD7s\"}, \n\"tenant_id\":\n\"01068ade-1cce-4125-ab6b-91d977ecf85b\",
\n\"region_id\":\n\"2dbacea3-5889-4021-8f38-bc2214dd7423\", \n\"email\":
\n\"resource_atangkcvo@install.example.net\", \n\"login\":\n\"\", \n\"password\":\n\"\",
\n\"type\":\n\"MEETING_ROOM\", \n\"profile\":{\n\"name\":\n\"autotest_resource_1663294241\",
\n\"description\":\n\"Пропаганда                четко_1663294241\", \n\"location\":\n\"г.
Казань_0.2871,0.4561\", \n\"geolocation\":\n\"0.2471,0.5491\", \n\"company\":
\n\"organization_1663294241\", \n\"department\":\n\"department_1663294241\",
\n\"capacity\":8}, \n\"gal_tags\":[\n\"0c22be2e-1e2f-5f6d-bec5-842c5d48e9d3\"],
\n\"autobook\":true, \n\"work_status\":true, \n\"locale\":\n\"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": "{\n\"Response\":{\n\"changed\":true, \n\"failed\":false, \n\"msg\":
\n\"ok\"}, \n\"id\":\n\"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
}
```

20.4.2.3.2 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 159.

Таблица 159 — Параметры запроса на обновление 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
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_rcv_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
}
```

20.4.2.4 Операции над группами

20.4.2.4.1 Удаление группы

Для удаления группы 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 160.

Таблица 160 — Параметры 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": "{\n\"tls_settings\":{\n\"ca_file\":\n\"/builds/0/mail-back-
tests/certs/ca.pem\", \n\"client_cert_file\":\n\"/builds/0/mail-back-
tests/certs/client.crt.pem\", \n\"server_cert_file\":\n\"\", \n\"key_file\":
\n\"/builds/0/mail-back-tests/certs/client_key.pem\", \n\"server_name_override\":\n\"\",
\n\"client_auth_type\":\n\"\", \n\"tls_min_version\":\n\"\",
\n\"prefer_server_cipher_suites\":false, \n\"use_tls_bundle\":false}, \n\"cox\":
{\n\"endpoint\":\n\"grpc-install.example.net:3142\", \n\"balancer_endpoint\":\n\"hydra.ucs-
apps-1.install.example.net:50053\", \n\"balancer_endpoints\":null, \n\"service_name\":
\n\"cox\", \n\"load_balanced\":false, \n\"use_tls\":true, \n\"use_tls_balancer\":false,
\n\"request_timeout\":\n\"10s\", \n\"max_send_size\":\n\"0B\", \n\"max_rcv_size\":\n\"0B\",
\n\"compression\":\n\"none\", \n\"is_external\":false}, \n\"token-name\":\n\"ucs-access-
token\", \n\"admin\":{\n\"login\":\n\"admin_tenant@install.example.net\", \n\"password\":
\n\"bKv9jqZ9PSwqKD7s\"}, \n\"group_id\":\n\"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": "{\n\"changed\":true, \n\"failed\":false, \n\"msg\":\n\"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
}

```

20.4.2.4.2 Обновление профиля группы

Для обновления профиля группы 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 161.

Таблица 161 — Параметры запроса на обновление профиля 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": "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_jftakfbfov\",\"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
}

```

20.5 Перечень регистрируемых методов API

В таблицах 162 и 163 представлено соответствие реализованных бизнес-функций отправляемым API-запросам в рамках ПО «Mailion».

Таблица 162 — Перечень отслеживаемых запросов при функционировании модуля Nomeros

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 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

Название события	Список запросов
	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 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	v1/erakles/create_entities

Название события	Список запросов
Создание группы/Create a Group	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 Фронтенд-рендеринг: v1/perseus/get_group_entities
Создание подразделения/Create a Subdivision	v1/arachne/organizational_unit/save v1/arachne/link/operate

Название события	Список запросов
	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

Название события	Список запросов
	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 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

Название события	Список запросов
	<p>Изменение логина:</p> <p>v1/erakles/get_entity_by_login</p> <p>v1/erakles/create_logins</p> <p>v1/theseus/create_credentials</p> <p>v1/erakles/delete_login</p> <p>Изменение email:</p> <p>v1/erakles/delete_email</p> <p>v1/erakles/get_entities_by_emails</p> <p>v1/erakles/create_emails</p> <p>Изменения в организационной структуре:</p> <p>v1/arachne/link/operate</p> <p>Изменение аватара:</p> <p>v1/achill/get_all_avatars</p> <p>v1/achill/remove_avatar</p> <p>v1/achill/save_avatar</p> <p>Изменение контактов:</p> <p>v1/erakles/update_entity</p> <p>v1/perseus/update_profile</p>
Блокирование пользователя/Block a User	<p>v1/erakles/change_status</p> <p>v1/erakles/set_blocking_reason</p>
Настройка календаря/Calendar settings changed	<p>v1/hog/update_calendar_schedule</p> <p>Изменение часового пояса:</p> <p>v1/hog/set_timezone</p> <p>Изменение событий приглашения:</p> <p>v1/hog/update_allow_ics_without_me</p> <p>Изменение напоминания о событиях:</p> <p>v1/hog/update_default_calendar_alarm</p>

Название события	Список запросов
	Фронтенд-рендеринг: v1/hog/get_settings
Подсистема «Календарь»	
Создание календаря/Create calendar	v1/marker/create_usertag v1/marker/create_calendar v1/othrys/subscribe
Изменение календаря/Change calendar	v1/marker/rename_tag v1/marker/create_calendar
Удаление календаря/Calendar delete	v1/kongur/delete_calendar
Создание события/Event creation	v1/kongur/save_event
Удаление события/Event delete	v1/kongur/delete_event
Создание задачи/Task creation	v1/kongur/save_todo
Удаление задачи/Task delete	v1/kongur/delete_todo
Подписаться на Календарь	v1/kongur/subscribe_to_internal_calendars
Отписаться от Календаря	v1/marker/delete_usertag
Подключить Календарь	v1/othrys/subscribe
Общий доступ к учетной записи	v1/erakles/set_shared_access
Общий доступ к учетной записи — Предоставить право писать от моего имени	v1/erakles/set_shared_access
Общий доступ к учетной записи — Предоставить право писать с моей учётной записи	v1/erakles/set_shared_access
Общий доступ к учетной записи — Отозвать разрешение на отправку от моего имени	v1/erakles/set_shared_access
Общий доступ к учетной записи — Отозвать разрешение писать с моей учётной записи	v1/erakles/set_shared_access
Общий доступ к учетной записи — Закрывать доступ	v1/erakles/unset_shared_access

Название события	Список запросов
Общий доступ к Календарю	v1/marker/share_tag
Общий доступ к Календарю — Удалить доступ	v1/marker/share_tag
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
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

Название события	Список запросов
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
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

Название события	Список запросов
	Передача двоичного кода вставленного объекта: attach/load_embed Фронтенд-рендеринг вставленного объекта: mixer/get_objects_by_ids

Таблица 163 — 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
SUBSCRIBE	Добавление указанного почтового ящика в список подписок пользователя	
UNSUBSCRIBE	Удаление указанного почтового ящика из списка подписок	

Команда IMAP	Описание события	Название события
	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, включая информацию об IMAP-сервере (вендор, версия и т. д.)	

Команда IMAP	Описание события	Название события
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	

21 КАТАСТРОФОУСТОЙЧИВОСТЬ

Установка почтовой системы Mailion предусматривает вариант, поддерживающий режим катастрофоустойчивости. Клиентам предоставляется возможность выбора требуемого варианта инсталляции.

Катастрофоустойчивый режим подразумевает наличие двух ЦОД для размещения инфраструктуры и хранения данных. При временной недоступности или в случае полного уничтожения основного ЦОД вследствие катастрофы происходит переключение работы почтовой системы и каталога на резервный ЦОД.



Установка и настройка Mailion в режиме катастрофоустойчивости осуществляется силами сотрудников МойОфис

21.1 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 70).

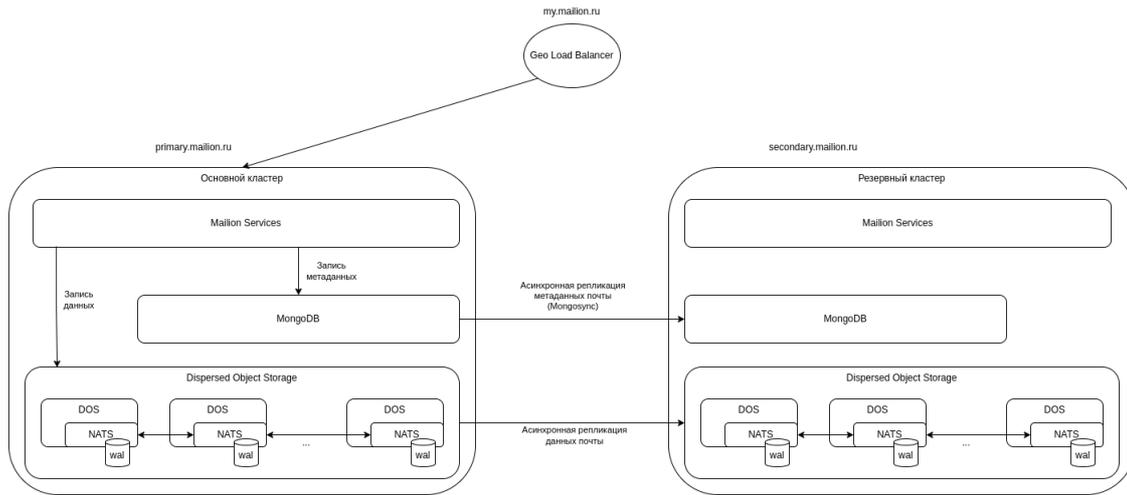


Рисунок 70 – Репликация базы данных между датацентрами

В случае выхода из строя основного кластера администратор переключает нагрузку на резервный кластер (см. Рисунок 71).

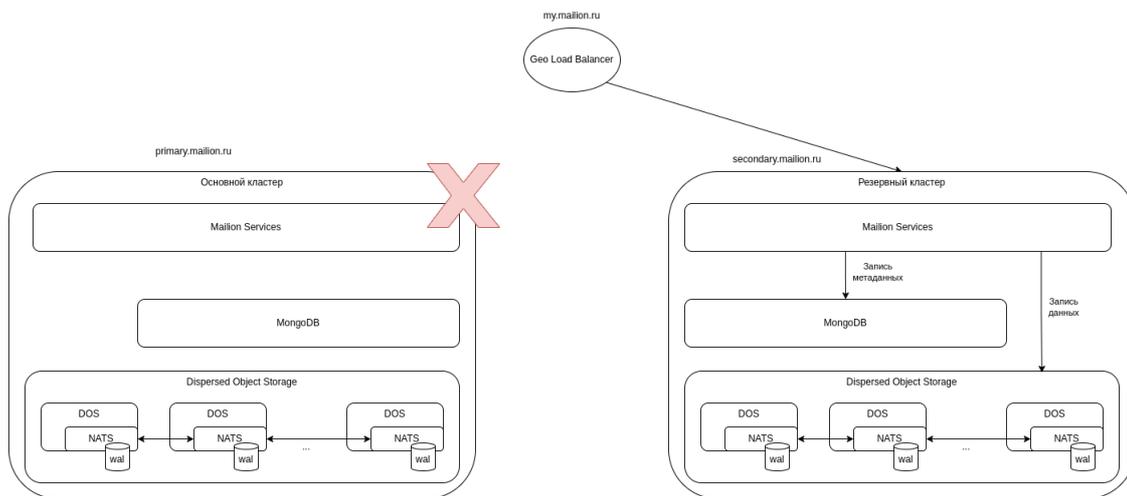


Рисунок 71 – Репликация базы данных между датацентрами

21.1.1 Катастрофоустойчивое развертывание DOS

Для катастрофоустойчивого развертывания DOS используется синхронизация данных DOS в асинхронном режиме на основе копирования записей журнала Write-Ahead Log (WAL) из основного кластера в резервный:

- при записи данных в основном кластере метаданные об этой операции заносятся в WAL;
- WAL хранится в отказоустойчивой очереди NATS [JetStream](#);

- копирование в резервный кластер производится с использованием [NATS Replication Sourcing](#);
- при обработке записей WAL в резервном кластере данные объекта запрашиваются с узла основного кластера, содержащего копию этого объекта, при этом данные объектов между кластерами передаются уже в сжатом виде;
- после получения данных из основного кластера метаданные и данные объекта записываются в резервный кластер.

21.1.1.1 Требования для катастрофоустойчивого развертывания DOS

В таблице 164 приведены требования для катастрофоустойчивого развертывания DOS.

Таблица 164 — Список требований для катастрофоустойчивого развертывания DOS

Требование	Описание
<p>Добавление SSD для WAL DOS (размер зависит от нагрузки на основной кластер и максимального времени, в течение которого система должна выдерживать недоступность резервного кластера без переустановки репликации)</p>	<p>На каждый узел кластера добавить накопитель SSD, размер которого рассчитать по следующей формуле:</p> $\text{размер} = (\text{max_msgx} * 370 / 1000 / 1024 / 1024) * 1,2 \text{ [Гбайт]}$ <p>Формула для расчета max_msgx:</p> $\text{max_msgx} = N * R * 24 * \text{downtime_days}$ <p>Где N — количество пользователей, R — среднее число писем в час на пользователя, downtime_days — максимальное количество дней, в течение которых может быть недоступен резервный кластер.</p> <p>Пример расчета:</p> <p>downtime_days = 3, R = 100,</p> <p>N = 5 000: max_msgx = 36 000 000, размер = 15 Гбайт</p> <p>N = 10 000: max_msgx = 72 000 000, размер = 30 Гбайт</p> <p>N = 100 000: max_msgx = 720 000 000, размер = 300 Гбайт</p>
<p>Достаточная пропускная способность канала между кластерами</p>	<p>Выбор пропускной способности канала зависит от ожидаемой нагрузки и вычисляется по формуле:</p> $N * R * S / (C * 3\,600\,000\,000) \text{ (Гбит/с)}$ <p>Где N — количество пользователей; R — среднее количество писем на пользователя в час; S — средний размер письма (в кбайт); C — коэффициент сжатия (принять равным 2).</p>

Требование	Описание
	Например, для 200 тыс. пользователей, получающих по 100 писем в час при размере письма 500 кбайт получаем необходимую пропускную способность канала 1,4 Гбит/с
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 из основного кластера в резервный и подключений из резервного кластера к основному для копирования данных DOS
Идентичная топология виртуальных машин DOS основного и резервного кластеров	<p>Основной и резервный кластеры должны иметь идентичную топологию виртуальных машин DOS:</p> <ul style="list-style-type: none"> – количество виртуальных машин DOS; – количество дисков на виртуальную машину DOS (и пути монтирования дисков); – размер дисков на виртуальных машинах DOS

21.1.1.2 Настройка катастрофоустойчивости для кластера без данных

Последовательность действий при настройке катастрофоустойчивости для кластера без данных приведена в таблице 165.

Таблица 165 — Настройка катастрофоустойчивости для кластера без данных

Шаг	Команды	Комментарий
Развертывание резервного кластера		
Настройка ntp для основного и резервного кластера		Время на виртуальных машинах DOS на основном и резервном кластере должно быть синхронизировано (с использованием ntp)
Добавление SSD mount point для всех нод на основном и резервном кластере		<p>Размер директории для wal на каждой ноде зависит от сайзинга.</p> <p>При значении по умолчанию для <code>dispersed_object_store_cross_dc_wal_stream_max_msgs</code> — он 11 Гб. Если данный параметр изменяется, то необходимо</p>

Шаг	Команды	Комментарий
		<p>рассчитать необходимый размер директории по формуле:</p> <pre>size = (max_msgx * 370 / 1000 / 1024 / 1024) * 1.2 [Gb]</pre> <p>Формула для расчета max_msgx:</p> <pre>max_msgx = N * 100 * 24 * downtime_days</pre> <p>Где: N — количество пользователей, 100 — среднее число писем в час на пользователя, downtime_days — максимальное количество дней, которое может быть недоступен резервный кластер.</p> <p>downtime_days = 3</p> <p>N=5 000: max_msgx = 36 000 000, size = 15 Гб</p> <p>N=10 000: max_msgx = 72 000 000, size = 30 Гб</p> <p>N=100 000: max_msgx = 720 000 000, size = 300 Гб</p>
<p>Добавление резервного кластера в конфигурацию основного кластера.</p>	<p>Запуск ansible с параметрами для установки кластеров сразу с настроенной конфигурацией для будущей установки репликации.</p> <p>Ansible запускается на каждом кластере. При запуске на основном кластере указываются параметры</p>	<p><code>dispersed_object_store_cross_dc_target_name</code> — имя удаленного кластера</p> <p><code>dispersed_object_store_cross_dc_target_api_urls</code> — список ip удаленного кластера.</p>

Шаг	Команды	Комментарий
<p>Добавление основного кластера в конфигурацию резервного.</p>	<p>резервного кластера в качестве удаленного кластера. При запуске на резервном кластере указываются параметры основного кластера в качестве удаленного кластера.</p> <p>Пример результирующей конфигурации DOS, которая будет сгенерирована с помощью ansible:</p> <pre data-bbox="427 734 941 1971"> "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", </pre>	<p>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 занимают около 370 kb. Значение по умолчанию 25920000 = (3 * 100 * (60 * 60 * 24)) при нагрузке 100 gps 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%).</p> <p>dispersed_object_store_cross_dc_token — token локального кластера</p> <p>dispersed_object_store_cross_dc_target_token — token удаленного кластера</p>

Шаг	Команды	Комментарий
	<pre> "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" } </pre>	
Установка репликации	<p>Для основного кластера следует вызвать команду:</p> <pre>ucs-dispersed-object-store-client dc add --target 'target_name'</pre>	<p>Вместо target_name необходимо использовать значение, которое было добавлено в конфигурацию на шаге Добавление резервного кластера в конфигурацию основного кластера</p>
Переключение режима резервного кластера	<pre>ucs-dispersed-object-store-client leader set_cluster_mode --mode=STANDBY</pre>	<p>Данная команда изменяет режим работы резервного кластера</p>

21.1.1.3 Настройка катастрофоустойчивости для кластера с данными

Последовательность действий при настройке катастрофоустойчивости для кластера с данными приведена в таблице 166.

Таблица 166 — Настройка катастрофоустойчивости для кластера с данными

Шаг	Команды	Комментарий
Развертывание резервного кластера		
Настройка ntp для основного и резервного кластера		<p>Время на виртуальных машинах DOS на основном и резервном кластере должно быть синхронизировано (с использованием ntp)</p>

Шаг	Команды	Комментарий
<p>Добавление SSD mount point для всех нод на основном и резервном кластере</p>		<p>Размер директории для wal на каждой ноде зависит от сайзинга.</p> <p>При значении по умолчанию для <code>dispersed_object_store_cross_dc_wal_stream_max_msgs</code> — он 11 Гб. Если данный параметр изменяется, то необходимо рассчитать необходимый размер директории по формуле:</p> <pre>size = (max_msgx * 370 / 1000 / 1024 / 1024) * 1.2 [Gb]</pre> <p>Формула для расчета <code>max_msgx</code>:</p> <pre>max_msgx = N * 100 * 24 * downtime_days</pre> <p>Где: N — количество пользователей, 100 — среднее число писем в час на пользователя, <code>downtime_days</code> — максимальное количество дней, которое может быть недоступен резервный кластер.</p> <p><code>downtime_days = 3</code></p> <p>N=5 000: <code>max_msgx = 36 000 000</code>, <code>size = 15 Гб</code></p> <p>N=10 000: <code>max_msgx = 72 000 000</code>, <code>size = 30 Гб</code></p> <p>N=100 000: <code>max_msgx = 720 000 000</code>, <code>size = 300 Гб</code></p>

Шаг	Команды	Комментарий
<p>Добавление резервного кластера в конфигурацию основного кластера.</p> <p>Добавление основного кластера в конфигурацию резервного.</p>	<p>Запуск ansible с параметрами для установки кластеров сразу с настроенной конфигурацией для будущей установки репликации.</p> <p>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.</p> <p>Пример результирующей конфигурации DOS, которая будет сгенерирована с помощью ansible:</p> <pre data-bbox="427 1108 941 1982"> "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- </pre>	<p><code>dispersed_object_store_cross_dc_target_name</code> — имя удаленного кластера</p> <p><code>dispersed_object_store_cross_dc_target_api_urls</code> — список ip удаленного кластера.</p> <p><code>dispersed_object_store_cross_dc_wal_stream_max_msgs</code> — 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 занимают около 370 kb. Дефолтное значение $25920000 = (3 * 100 * (60 * 60 * 24))$ при нагрузке 100 gps 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%).</p> <p><code>dispersed_object_store_cross_dc_token</code> — token локального кластера</p> <p><code>dispersed_object_store_cross_dc_target_token</code> — token удаленного кластера</p>

Шаг	Команды	Комментарий
	<pre>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, 1100, 1026, 1007, 1004, 1015, 1010, 1012, 1257] } }, "token": "secret-token" }</pre>	
Рестарт контейнеров DOS основного кластера (для загрузки новой конфигурации)		
Создание репликации между кластерами	<pre>ansible-playbook -i inventory/ucs_dos_crossdc.yml - b -l dispersed_object_store playbooks/crossdc_rep1.yml</pre>	Данный шаг создает репликацию между кластерами и переносит старые документы с помощью backup

21.1.1.4 Переключение с основного кластера на резервный в случае катастрофы

Последовательность действий при переключении с основного кластера на резервный приведена в таблице 167.

Таблица 167 — Переключение с основного кластера на резервный в случае катастрофы

Шаг	Команды	Комментарий
Переключение режима резервного кластера	<code>ucs-dispersed-object-store-client leader set_cluster_mode --mode=NORMAL</code>	Данная команда превращает резервный кластер в основной
Переключение режима основного кластера (опционально)	<code>ucs-dispersed-object-store-client leader set_cluster_mode --mode=STANDBY</code>	Если основной кластер доступен после катастрофы, то данная команда переводит основной кластер в режим follower
Переключение нагрузки на резервный кластер		
Удаление репликации на резервном кластере (опционально)	<code>ucs-dispersed-object-store-client dc delete --force</code>	<ul style="list-style-type: none"> – Если основной кластер временно недоступен и будет вскоре восстановлен, данный шаг можно пропустить. – Удаление репликации необходимо только в том случае, 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 экономит ресурсы, потребляемые в резервном кластере

21.1.1.5 Плановое переключение на резервный кластер без катастрофы

Последовательность действий при переключении с основного кластера на резервный без катастрофы приведена в таблице 168.

Таблица 168 — Переключение с основного кластера на резервный без катастрофы

Шаг	Команды	Комментарий
Переключение режима резервного кластера	<code>ucs-dispersed-object-store-client leader set_cluster_mode --mode=NORMAL</code>	Данная команда превращает резервный кластер в основной

Шаг	Команды	Комментарий
Переключение режима основного кластера (опционально)	<code>ucs-dispersed-object-store-client leader set_cluster_mode --mode=STANDBY</code>	Если основной кластер доступен после катастрофы, то данная команда переводит основной кластер в режим follower
Переключение нагрузки на резервный кластер		Дополнительные шаги не требуются

21.1.1.6 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 выше (см. раздел [Настройка катастрофоустойчивости для кластера с данными](#)), после этого следует произвести переключение нагрузки (см. раздел [Плановое переключение с основного кластера на резервный](#)).

Если основной кластер был недоступен непродолжительное время, произвести плановое переключение нагрузки на основной кластер (см. раздел [Плановое переключение с основного кластера на резервный](#)).

21.1.1.7 Мониторинг репликации

1. Допустимую глубину потери данных в случае инцидента (Recovery Point Objective, RPO) можно отслеживать с помощью набора панелей мониторинга Grafana Dashboards DOS на панели CROSS-DC REPLICATION. В таблице 169 описаны графики мониторинга.

Таблица 169 — Графики мониторинга RPO

Название	Описание	Что необходимо учитывать при трактовке метрики
RPO	Последняя метка времени создания объекта в основном кластере, которая была	Использовать для настройки оповещений

Название	Описание	Что необходимо учитывать при трактовке метрики
	обработана сервером в резервном кластере	
Replication lag	Задержка между временем записи объекта в основном кластере и его обработкой на сервере резервного кластера	Удобно использовать для быстрой оценки репликации на действующих кластерах

2. Переполнение журнала WAL в основном кластере (доступно с версии Mailion 1.9).

Основной кластер раз в 5 минут проверяет переполнение WAL-сообщений, которые не были реплицированы в резервный кластер (сценарий долгой недоступности резервного кластера). Если в основном кластере из-за переполнения произошла ротация сообщений и часть из них не была скопирована в резервный кластер, то в журнале 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}
```

21.1.2 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 72).

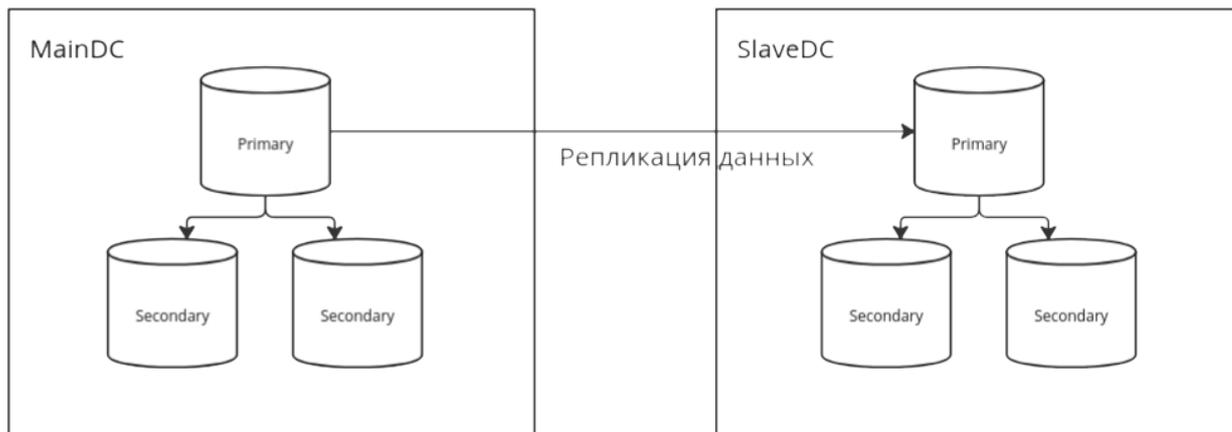


Рисунок 72 – Репликация базы данных между датацентрами

В результате репликации базы данных в случае временной недоступности или полном уничтожении одного из датацентров, сохраняются следующие 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.

21.1.2.1 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 редиса и перевыкатка `redis` при необходимости
- Проверка работоспособности кластера, на который реплицировались данные



Проверка обратной репликации проходит по тому же сценарию, только в отношении другого кластера. Дополнительно перед началом репликации необходимо удалить базу данных с метаданными о ходе репликации.

21.1.2.2 Подробный порядок действий по репликации

1. Предварительно необходимо установить Mailion на двух стендах с использованием одинаковых версий сервисов стендов.
2. Проверить работоспособности каждого кластера:
 - a. Проверить какие из сервисов запущены и какие версии используются;

- b. Войти под тестовыми тенантами, проверить отправку и получение писем и создание календарных событий.
 3. Остановить сервисы на целевом кластере:
 - a. Использовать **Скрипт остановки и запуска сервисов** на стенде из раздела [Список полезных команд и скриптов](#);
 - b. Проверить, что сервисы остановлены.
 4. Создать резервные копии баз данных mongodb на обоих кластерах перед запуском процесса репликации:
 - a. Зайти на машину `ucs-infra-1` на каждом кластере и под пользователем `root` запустить скрипт `/srv/docker/mongodb/backup_scripts/mongodb_backup_generic.sh`;
 - b. 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
 - i. Выполнить **Команду для чистки базы данных** из раздела [Список полезных команд и скриптов](#);
 - ii. Возможно, понадобится подключиться напрямую к PRIMARY node. Для этого следует выполнить `rs.status()` и найти в выводе, какая нода является PRIMARY;
 - iii. Подключиться напрямую к PRIMARY node;
 - iv. Повторить запуск **Команды для чистки базы данных**.
 6. Настроить инструмент репликации:
 - a. Для Mongosync
 - i. Необходимо скопировать Dockerfile для Mongosync из раздела [Список полезных команд и скриптов](#) на `ucs-infra-1` на кластер, откуда копируются данные;
 - ii. Собрать образ прямо на `ucs-infra-1` командой:

```
docker build -f Dockerfile . --tag mongosync:latest
```
 - iii. Скопировать все необходимые SSL/TLS сертификаты на `ucs-infra-1`;
 - iv. Скопировать и запустить **Скрипт для запуска mongosync контейнера** из раздела [Список полезных команд и скриптов](#) на `ucs-infra-1`;
 - v. С помощью `'docker ps -a'` проверить, что контейнер успешно запустился.
 7. Запуск процесса репликации

a. Для Mongosync

- i. Необходимо 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"  
  } '
```

- ii. Получить на выходе `success: true`.

8. (Опционально) создание тестовой базы данных и коллекции с тестовыми данными на исходном кластере и проверка их создания и удаления на целевом кластере

- a. Подключиться к исходной `mongodb` любым удобным способом;
b. Создать тестовую базу, в ней тестовую коллекцию и несколько тестовых документов;
c. Проверить, создались ли они на целевом кластере;
d. Удалить один документ в исходной `mongodb`, проверить, удалился ли он на целевой базе данных;
e. Повторить удаление с проверкой последовательно сначала для коллекции, потом для базы данных.

9. Проверка статуса репликации

a. Для Mongosync

- i. Зайти внутрь контейнера `mongosync`;
ii. Выполнить команду:

```
curl localhost:27182/api/v1/progress
```

- iii. Вывод команды можно подробнее изучить по ссылке <https://www.mongodb.com/docs/cluster-to-cluster-sync/current/reference/api/progress/>.

10. Остановка процесса репликации

a. Для Mongosync

- i. Если в выводе есть `canCommit: true`, то это означает, что синхронизация по большей части завершилась, и можно делать `commit` изменений;

- ii. ВАЖНО!!! После того, как будет сделан `commit`, запустить снова репликацию будет нельзя. Для повторного запуска нужно будет удалить базу с метаданными `mongosync`;
- iii. Если прогресс показывает, что можно сделать `commit`, то внутри контейнера нужно выполнить команду:

```
curl localhost:27182/api/v1/commit -XPOST --data '{ }'
```

- iv. Таким же способом, каким проверяли прогресс, нужно проверять процесс коммита изменений. Когда он закончится в выводе будет `state: COMMITED`.
11. Запуск сервисов на кластере, куда производилась репликация
 - a. Использовать **Скрипт остановки и запуска сервисов** на стенде из раздела [Список полезных команд и скриптов](#), в конце скрипта не забыть оставить нужный пункт
 12. (Опционально) удаление данных `redis` и обновление роли `redis` при необходимости
 - a. Необязательный шаг: проверить с помощью `mailion_install_info` все ли сервисы запустились. Если не все, то можно попробовать почистить кэши `redis`;
 - b. Сначала нужно остановить сервисы с помощью **Скрипта остановки и запуска сервисов** на стенде из раздела [Список полезных команд и скриптов](#);
 - c. Для этого в Sparky есть `job mailion_redis_cleanup`;
 - d. Теперь нужно переинициализировать сервисы `redis` с помощью `job mailion_install_infra`. Необходимо выбрать плейбук `infra` и указать в тегах `redis_cache`;
 - e. Запустить сервисы с помощью **Скрипта остановки и запуска сервисов** на стенде из раздела [Список полезных команд и скриптов](#);
 - f. Снова проверить стенд с помощью `mailion_install_info`.
 13. Проверка работоспособности кластера, на который реплицировались данные
 - a. Все делается так же, как и в проверке кластера в предыдущих пунктах;
 - b. Выполнять вход нужно с аккаунтами пользователей исходного стенда, откуда копировались данные.

Обратная миграция выполняется так же, но с дополнительными действиями:

- Необходимо удалить базу с метаданными `mongosync` из кластера, который ранее был целевым, но теперь стал исходным
- Предварительно необходимо выполнить резервное копирование базы данных

21.1.2.3 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:



1. Все необходимые сертификаты сохранены в каталоге `/srv/tls/certs`.

2. При необходимости можно поменять местами значения 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



Перед запуском необходимо задать внутри функций параметр **idx** (номер кластера) .
При этом в конце файла следует оставить только нужные строки.

```
#!/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 lmtpl 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"
    done
}
```

```
    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



Важно!!!

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 '{}'
```

21.1.2.4 Верификация реплицированных данных для Mongosync

Проверку 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, но она находится в экспериментальном режиме <https://www.mongodb.com/docs/cluster-to-cluster-sync/current/reference/verification/verifier/>.

21.1.2.5 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 вообще отключить ротирование oplog.

Оба инструмента способны сохранять свой прогресс и возобновлять работу с определенного чекпоинта (mongosync с версии 1.7). Для сохранения чекпоинтов используется

целевой кластер mongodb, куда реплицируются данные. Внутри целевых кластеров создаются базы данных с метаданными о ходе репликации и чекпоинтах.

Полезные ссылки:

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>

Документация по Mongo Migration Verfier — <https://www.mongodb.com/docs/cluster-to-cluster-sync/current/reference/verification/verifier/>

21.2 Роли и функции персонала

Роли и функции персонала, задействованного в обслуживании катастрофоустойчивой конфигурации приведены в таблице 170.

Таблица 170 — Роли и функции персонала

Роль	Функции
дежурный администратор	<ul style="list-style-type: none"> – получение информации об инциденте (самостоятельно, от ЦОДа, от пользователей) – создание инцидента в трекере задач (если есть) – оповещение сотрудника с ролью "Администратор инсталляции"
администратор инсталляции	<ul style="list-style-type: none"> – 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.

21.3 Ограничения

- При временной недоступности или полном уничтожении основного ЦОДа(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 ЦОДами 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).

22 ВОЗМОЖНЫЕ СИТУАЦИИ И СПОСОБЫ РЕШЕНИЯ

Возможные ситуации при эксплуатации **Панели администрирования** ПО «Mailion» и способы решения приведены в таблице 171.

Рисунок 73 — 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: <ul style="list-style-type: none"> – нажать на значок обновления на странице браузера; – нажать клавишу F5.
Бесконечная загрузка страницы	
При переходе в какой-либо раздел Панели управления отсутствуют созданные записи	

23 РАБОТА С ПОДСИСТЕМОЙ СБОРА МУСОРА

В Mailion задачи сбора и удаления мусора — неиспользуемых сущностей — реализуют сервисы **kharon** и **styx**. Запуск процедур очистки осуществляет сервис **kronos**.

Для постановки сервису **kronos** задач по отложенному запуску подсистемы сбора мусора (Garbage Collector, GC) предназначены следующие команды утилиты **ministerium**:

- `create_gc_task` — создание задачи с отложенным исполнением;
- `update_gc_task` — обновление задачи по `taskID`;
- `delete_gc_task` — удаление задачи по `taskID`;
- `get_gc_task` — получение сведений о задаче по `taskID`;
- `get_gc_task_by_tenant_id` — получение сведений о задаче по `tenantID`.

После постановки задачи **kronos** самостоятельно запускает GC по заданному расписанию для указанного тенанта. Для каждого тенанта возможна постановка только одной задачи GC.

При запуске GC в тенанте выполняется удаление:

- доменов с истекшим сроком жизни и помеченных к удалению;
- сущностей с истекшим сроком жизни и помеченных к удалению;
- остальных сущностей, которые не попали в группу для удаления.

Также предусмотрена команда ручного запуска сбора мусора в рамках тенанта — `start_gc`.

23.1 Создание задачи с отложенным исполнением

Для создания задачи сбора мусора с отложенным исполнением предназначена команда `create_gc_task`. Создать эту задачу может пользователь с правами администратора тенанта. Поиск и удаление объектов производятся в пределах указанного тенанта.

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" \
--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_cert.pem \
--tls_settings.key_file /home/mo/ministerium_certs/yankee/client_key.pem \
--v
```

В этом примере заданы следующие правила: 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 неудачи при ее выполнении будет произведено 5 попыток ее повторения (`retry_policy.count=5`) с задержкой в 5 минут (`retry_policy.delay=5m`).

Параметры команды описаны в таблице 171.

Таблица 171 — Параметры команды создания задачи GC

Параметр	Описание
<code>recurrence_rule.frequency</code>	Частота выполнения задачи. Допустимые значения: <code>monthly = 1</code> — ежемесячно; <code>weekly = 2</code> — еженедельно; <code>daily = 3</code> — ежедневно; <code>hourly = 4</code> — ежечасно; <code>minutely = 5</code> — ежеминутно; <code>secondly = 6</code> — ежесекундно; <code>yearly = 7</code> — ежегодно
<code>recurrence_rule.interval</code>	Кратность повтора задачи: <code>1</code> = каждый первый период, заданный в <code>recurrence_rule.frequency</code> ; <code>2</code> = каждый второй период, заданный в <code>recurrence_rule.frequency</code> и т. д.
<code>delta</code>	Сдвиг от запланированного времени
<code>retry_policy.count</code>	Количество повторов

Параметр	Описание
retry_policy.delay	Задержка между повторами

Пример ответа при успешном выполнении команды:

```
{
  "Response": {
    "changed": true,
    "failed": false,
    "msg": "ok"
  },
  "tasks_id": "a4fca8ab-ae0e-5f4d-b808-996d9e9b1d4d"
}
```

При попытке создать задачу в другом тенанте возвращается ошибка:

```
{
  "changed": false,
  "failed": true,
  "msg": "send task to kronos: schedule kronos tasks: common.Error(module:KRONOS
code:2001 msg:\"FORBIDDEN\")"
}
```



Если удалить задачу сбора мусора в тенанте и создать ее заново, то ее UUID не изменится — это обусловлено логикой создания задач, имя которых зависит от ID тенанта и имени операции.

23.2 Обновление задачи по taskID

Для обновления задачи сбора мусора по taskID предназначена команда `update_gc_task`. Эта команда использует те же параметры, что и команда создания задачи, с добавлением идентификатора задачи в параметре `--task_id <идентификатор_задачи>`.

Пример запроса:

```
nct_ministerium update_gc_task \  
--admin.login <login> \  
--admin.password *** \  
--task_id <идентификатор_задачи> \  
--recurrence_rule.frequency=hourly \  
--recurrence_rule.interval=1 \  
--delta="-3600s" \  
--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.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:

```
{  
  "Response": {  
    "changed": true,  
    "failed": false,  
    "msg": "ok"  
  },  
  "tasks_id": "a4fca8ab-ae0e-5f4d-b808-996d9e9b1d4d"  
}
```

При попытке обновить задачу в другом тенанте возвращается ошибка:

```
{  
  "changed": false,  
  "failed": true,  
  "msg": "get gc kronos task: get kronos tasks: common.Error(module:KRONOS  
code:2001 msg:\"FORBIDDEN\")"  
}
```

23.3 Удаление задачи по taskID

Для удаления задачи сбора мусора по taskID предназначена команда `delete_gc_task`.

Пример запроса:

```
nct_ministerium delete_gc_task \  
--admin.login <login> \  
--admin.password *** \  
--task_id <идентификатор_задачи> \  
--cox.balancer_endpoint=hydra.ucs-apps-1.installation.example.net:50053 \  
--cox.compression=none \  
--cox.endpoint=grpc-yankee.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:

```
{  
  "Response": {  
    "changed": true,  
    "failed": false,  
    "msg": "ok"  
  },  
  "tasks_id": "b346bb12-5199-5431-9cae-2e5b22852c71"  
}
```

При попытке удалить задачу в другом тенанте возвращается ошибка:

```
{  
  "changed": false,  
  "failed": true,  
  "msg": "get gc kronos task: get kronos tasks: common.Error(module:KRONOS  
code:2001 msg:\\"FORBIDDEN\\")"  
}
```

При попытке удалить несуществующую задачу возвращается ошибка:

```
{  
  "changed": false,  
  "failed": true,  
  "msg": "get gc kronos task: get kronos tasks: common.Error(module:KRONOS  
code:4004 msg:\\"NOT_FOUND\\")"  
}
```

При попытке удалить задачу, не относящуюся к сбору мусора, возвращается ошибка:

```
{  
  "changed": false,  
  "failed": true,  
  "msg": "task with given ID is not a garbage collector task"  
}
```

23.3.1 Получение сведений о задаче по taskID

Для получения сведений о задаче сбора мусора по `taskID` предназначена команда

```
get_gc_task.
```

Пример запроса:

```
nct_ministerium get_gc_task \  
--admin.login <login> \  
--admin.password *** \  
--task_id <идентификатор_задачи> \  
--cox_balancer_endpoint=hydra.ucs-apps-1.installation.example.net:50053 \  
--cox_compression=none \  
--cox_endpoint=grpc-yankee.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_cert.pem \  
--tls_settings.key_file /home/mo/ministerium_certs/yankee/client_key.pem \  
--v
```

Пример ответа:

```
{  
  "Response": {  
    "changed": false,  
    "failed": false,  
    "msg": "ok"  
  },  
  "task": {  
    "id": "d41bc597-79f6-53d3-ad29-ba5735580c6a",  
    "operations": [  
      {  
        "operation_name": 1,  
        "Arguments": {  
          "GarbageCollectorRegular": {  
            "tenant_id": "bafe525a-c5df-490e-ae1d-d31335f7e57c"  
          }  
        }  
      }  
    ]  
  },  
  "recurrence_rule": {  
    "frequency": "MINUTELY",  
    "interval": 5,  
    "by_second": [  
      0  
    ]  
  },  
  "delta": "0s",  
  "retry_policy": {  
    "count": 2,  
    "delay": "5m"  
  },  
  "created_at": {  
    "unixmicro": 1733147312163520,  
    "zone": 10800  
  }  
}
```

23.4 Получение сведений о задаче по tenantID

Для получения сведений о задаче сбора мусора по tenantID предназначена команда

```
get_gc_task_by_tenant_id.
```

Пример запроса:

```
nct_ministerium get_gc_task_by_tenant_id \  
--admin.login <login> \  
--admin.password *** \  
--tenant_id b3e95118-5e5f-4b3f-839e-b62484b6008a \  
--cox.balancer_endpoint=hydra.ucs-apps-1.installation.example.net:50053 \  
--cox.compression=none \  
--cox.endpoint=grpc-yankee.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_cert.pem \  
--tls_settings.key_file /home/mo/ministerium_certs/yankee/client_key.pem \  
--v
```

Пример ответа:

```
{  
  "Response": {  
    "changed": false,  
    "failed": false,  
    "msg": "ok"  
  },  
  "task": {  
    "id": "d41bc597-79f6-53d3-ad29-ba5735580c6a",  
    "operations": [  
      {  
        "operation_name": 1,  
        "Arguments": {  
          "GarbageCollectorRegular": {  
            "tenant_id": "bafe525a-c5df-490e-ae1d-d31335f7e57c"  
          }  
        }  
      }  
    ]  
  },  
  "recurrence_rule": {  
    "frequency": "MINUTELY",  
    "interval": 5,  
    "by_second": [  
      0  
    ]  
  },  
  "delta": "0s",  
  "retry_policy": {  
    "count": 2,  
    "delay": "5m"  
  },  
  "created_at": {  
    "unixmicro": 1733147312163520,  
    "zone": 10800  
  }  
}
```

Если для указанного тенанта нет такой задачи, возвращается ошибка `NOT_FOUND`:

```
{
  "changed": false,
  "failed": true,
  "msg": "get gc kronos task: get kronos tasks: common.Error(module:KRONOS
code:4004 msg:\"NOT_FOUND\")"
}
```

Если задача из другого тенанта, возвращается ошибка `FORBIDDEN`:

```
{
  "changed": false,
  "failed": true,
  "msg": "get gc kronos task: get kronos tasks: common.Error(module:KRONOS
code:2001 msg:\"FORBIDDEN\")"
}
```

23.5 Запуск сбора мусора вручную

Для ручного запуска подсистемы сбора мусора в рамках тенанта предназначена команда `start_gc`. Для выполнения команды требуются права администратора тенанта.

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_cert.pem \
--tls_settings.key_file /home/mo/ministerium_certs/zulu/client_key.pem \
--v
```

ПРИЛОЖЕНИЕ А. КОМАНДЫ ИНТЕРФЕЙСА КОМАНДНОЙ СТРОКИ

1. Команды утилиты ministerium

Доступные команды	Описание
add_email	Добавить объекту адрес электронной почты
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

Доступные команды	Описание
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
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

Доступные команды	Описание
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_orgstructure_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
get_tenant_gals	Получить список GAL-тегов тенанта
get_user_quotas_profile	Получить квоты профиля пользователя
help	Помощь по поводу любой команды

Доступные команды	Описание
list_domains	Список доменов в тенанте
list_entities	Список объектов по идентификатору региона/тенанта, адресу электронной почты 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)

Доступные команды	Описание
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
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 адрес электронной почты пользователя
update_resource	Обновить ресурс
update_resource_profile	Создать или обновить профиль ресурса
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

2. Интерфейс командной строки Dispersed Object Store

В Docker-контейнер Dispersed Object Store встроен интерфейс командной строки **ucs-dispersed-object-store-client** для администрирования DOS-кластера.



Особенности использования утилиты:

- при отсутствии указания `host` и `port` по умолчанию подсоединяется к текущему узлу;
- для команд, которые требуют обращения к лидеру кластера, автоматически находит его и выполняет команду на нем.

Для получения доступа к интерфейсу выполните на узле с экземпляром контейнера DOS следующую команду (обратите внимание на параметр `login` для **bash**).

```
docker exec -it dispersed_object_store bash -l
```

Для получения справки по доступным командам введите:

```
ucs-dispersed-object-store-client --help
```

ПРИЛОЖЕНИЕ Б. ПРИМЕРЫ JSON-ФАЙЛОВ ДЛЯ КОМАНД УТИЛИТЫ MINISTERIUM

Б.1 Файл настроек импорта пользователей

Пример файла настроек **import_config.json** приведен ниже. Описание полей приведено в таблице 172.

```
{
  "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_ATTACHMENTS_SIZE": "1MB"},
  "roles": ["14718e3a-6c7b-5c9f-b4de-a897c356cb5e"]
}
```

Таблица 172 — 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
region_id	Str	Идентификатор региона в формате UUID-строки

Параметр	Тип	Описание
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: <ul style="list-style-type: none"> – 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

Б.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"
]
}
```

Б.3 Список глобальных адресных книг

Пример файла **get_tenant_gals.json** приведен ниже. Описание полей файла настроек приведено в таблице 173.

```
{
  "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 173 — 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

Б.4 Файл настроек импорта групп

Пример файла настроек **settings.json** приведен ниже. Описание полей приведено в таблице 174.

```
{
  "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 174 — 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

Б.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"
]
}

```

Б.6 Файл настроек для импорта связей групп

Пример файла настроек **settings.json** приведен ниже. Описание полей приведено в таблице 175.

```

{
  "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 175 — 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

Параметр	Тип	Обязательный	Описание
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. Не обязательный если у файла, указанного в параметре group_links_data_path есть расширение .json или .csv
rejected_group_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

Б.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"
  ]
}

```

Б.8 Файл настроек импорта ресурсов

Пример файла настроек **settings.json** приведен ниже. Описание полей приведено в таблице 176.

```

{
  "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 176 — 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

Параметр	Тип	Обязательный	Описание
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

Б.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"
]
```

ПРИЛОЖЕНИЕ В. ПРАВА АДМИНИСТРАТОРОВ РОЛЕВОЙ МОДЕЛИ

Права доступа	Администратор инсталляции	Администратор тенанта	Администратор информационной безопасности	Администратор аудита	Супер- администратор
Доступ к инструментам					
Консольная утилита администрирования nct_ministerium	+	+	+	+	+
Панель администратора в веб интерфейсе		+	+	+	+
Журнал аудита системы		+(только чтение)	+(только чтение)	+	+
Группы					
Чтение списка групп		+	+	+	+
Чтение деталей группы		+	+	+	+
Создание		+			+
Редактирование		+			+
Удаление		+			+
Добавление участников		+			+
Исключение участников из группы		+			+
Добавление группы в другую группу или группы		+			+
Исключение группы из другой группы или групп		+			+
Поиск группы рассылки		+	+	+	+
Настройка динамических групп		+			+

Права доступа	Администратор инсталляции	Администратор тенанта	Администратор информационной безопасности	Администратор аудита	Супер- администратор
рассылки					
Массовое создание групп в каталоге		+			+
Пользователи					
Чтение списка		+	+	+	+
Чтение деталей		+	+	+	+
Создание		+			+
Изменение данных		+			+
Блокировка		+	+		+
Удаление		+			+
Добавление в группу или группы		+			+
Удаление из группы или групп		+			+
Сброс пароля		+			+
Сброс активных сессий		+			+
Добавление почтового алиаса		+			+
Удаление почтового алиаса		+			+
Добавление логина		+			+
Изменение логина		+			+
Удаление логина		+			+
Добавление данных организации		+			+
Изменение данных организации		+			+
Удаление данных организации		+			+

Права доступа	Администратор инсталляции	Администратор тенанта	Администратор информационной безопасности	Администратор аудита	Супер- администратор
Поиск пользователя		+	+	+	+
Разблокировка пользователя		+			+
Просмотр списка заблокированных пользователей.		+	+	+	+
Создание пользователя с ролью создателя резервных копий на уровне тенанта		+			+
Массовое создание пользователей в каталоге		+			+
Просмотр истории комментариев блокировки пользователей		+	+	+	+
Установка флага смены пароля		+			+
Создание делегированного пользователя		+			+
Чтение почтового алиаса		+		+	+
Чтение логина		+	+	+	+
Чтение данных организации		+	+	+	+
Организационная структура					
Чтение списка организаций		+	+	+	+
Чтение деталей организации		+	+	+	+
Создание организации		+			+

Права доступа	Администратор инсталляции	Администратор тенанта	Администратор информационной безопасности	Администратор аудита	Супер- администратор
Изменение организации		+			+
Удаление организации		+			+
Чтение списка организационных единиц		+	+	+	+
Чтение деталей организационной единицы		+	+	+	+
Создание организационной единицы		+			+
Изменение организационной единицы		+			+
Удаление организационной единицы		+			+
Чтение списка организационных групп		+	+	+	+
Чтение деталей организационной группы		+	+	+	+
Создание организационной группы		+			+
Изменение организационной группы		+			+
Удаление организационной группы		+			+

Права доступа	Администратор инсталляции	Администратор тенанта	Администратор информационной безопасности	Администратор аудита	Супер- администратор
Чтение списка должностей		+	+	+	+
Чтение деталей должности		+	+	+	+
Создание должности		+			+
Изменение должности		+			+
Удаление должности		+			+
Чтение списка компетенций		+	+	+	+
Чтение деталей компетенции		+	+	+	+
Создание компетенции		+			+
Изменение компетенции		+			+
Удаление компетенции		+			+
Профили					
Создание профиля		+			+
Связь профиля с сущностью		+			+
Чтение данных профиля		+	+	+	+
Изменение профиля		+			+
Удаление профиля		+			+
Адреса					
Создание адреса		+			+
Связь адреса с сущностью		+			+
Чтение адреса		+	+	+	+
Изменение адреса		+			+

Права доступа	Администратор инсталляции	Администратор тенанта	Администратор информационной безопасности	Администратор аудита	Супер- администратор
Удаление адреса		+			+
Домен					
Создание домена		+			+
Изменение домена		+			+
Удаление домена		+			+
Чтение данных домена		+			+
Прикрепление к домену сертификата		+			+
Удаление сертификата из домена		+			+
Поиск домена.		+			+
Фильтрация доменов.		+			+
Получение списка доменов.		+			+
Получить дефолтный маппинг LDAP		+			+
Добавить делегацию доменов		+			+
Обновить делегацию доменов		+			+
Удалить делегацию доменов		+			+
Переключение на однодоменный режим работы		+			+
Переключение на разнодоменный режим работы		+			+
Квоты					
Создание квот профиля тенанта	+				+

Права доступа	Администратор инсталляции	Администратор тенанта	Администратор информационной безопасности	Администратор аудита	Супер- администратор
Создание квоты профиля пользователя		+			+
Удаление квоты профиля тенанта	+				+
Удаление квоты профиля пользователя		+			+
Получение всех запущенных процессов пересчета квот	+	+	+	+	+
Получение квоты профиля пользователя		+	+	+	+
Запуск процесса напоминания о пересчете квот для одиночного объекта или всех объектов в тенанте		+			+
Остановка процесса пересчета квоты.		+			+ (некоторые объекты могли иметь непредвиден ные упоминания о квотах)
Обновление квоты профиля тенанта	+				+
Обновление квоты профиля пользователя					+
Обновление общей квоты	+				+
Получение перечня пользователей,		+	+	+	+

Права доступа	Администратор инсталляции	Администратор тенанта	Администратор информационной безопасности	Администратор аудита	Супер- администратор
получивших нулевую квоту					
Установка лимитов почты в тенанте		+			+
Журналы					
Включение журналов				+	+
Выключение журналов				+	+
Добавление события для регистрации в формате CEF				+	+
Удаления из списка события для регистрации в формате CEF				+	+
Настройка ротации журналов				+	+
Просмотр журналов		+	+	+	+
Поиск событий безопасности пользователя		+	+	+	+
Поиск событий безопасности администратора			+	+	+
Управление администраторами					
Создание администратора тенанта	+				+
Создание настраиваемого администратора	+				+
Создание администратора ИБ	+				+

Права доступа	Администратор инсталляции	Администратор тенанта	Администратор информационной безопасности	Администратор аудита	Супер- администратор
Создание администратора аудита	+				+
Блокировка администратора тенанта	+		+		+
Блокировка администратора ИБ	+		+		+
Блокировка администратора аудита	+		+		+
Блокировка настраиваемого администратора	+		+		+
Удаление администратора тенанта	+				+
Удаление администратора ИБ	+				+
Удаление администратора аудита	+				+
Удаление настраиваемого администратора	+				+
Изменение администратора аудита	+				+
Изменение администратора ИБ	+				+
Изменение настраиваемого администратора	+				+

Права доступа	Администратор инсталляции	Администратор тенанта	Администратор информационной безопасности	Администратор аудита	Супер- администратор
Изменение администратора тенанта	+				+
Получение созданного администратора тенанта по его ID	+	+			+
Получение списка всех администраторов	+	+	+	+	+
Настройки инсталляции					
Изменение настроек инсталляции	+				+
Резервное копирование					
Создание пользователя с ролью создателя резервных копий на уровне инсталляции	+				+
Создание пользователя с ролью создателя резервных копий на уровне тенанта		+			+
Импорт контактов глобальной адресной книги (ГАК)					
Импорт контактов		+	+	+	+
Удаление импортированных контактов		+			+
Поиск импортированных контактов		+			+
Импорт контактов локальной адресной книги (ЛАК)					
Импорт контактов		+			+
Миграция данных					
Запуска мигратора (системный)	+				

Права доступа	Администратор инсталляции	Администратор тенанта	Администратор информационной безопасности	Администратор аудита	Супер- администратор
пользователь)					
Миграция данных календаря		+			+
Миграция почты <ul style="list-style-type: none"> отключение синхронизации для домена отключение синхронизации для конкретного пользователя отключение синхронизации для тенанта 		+			+
Миграция внешних пользователей (из внешних каталогов)		+			+
Миграция идентификаторов из внешних каталогов		+			+
Черные и белые списки отправителей					
Добавление отправителей в список.		+			+
Обновление списка отправителей.		+			+
Удаление отправителей из списка.		+			+
Просмотр получателей по спискам (статус blacklist, whitelist).		+	+	+	+
Ресурсы					

Права доступа	Администратор инсталляции	Администратор тенанта	Администратор информационной безопасности	Администратор аудита	Супер- администратор
Чтение списка ресурсов		+	+	+	+
Создание ресурса (пространство для встреч = название, кол-во участников, логин, пароль, контакты, эл. почта)		+			+
Просмотр данных о ресурсе		+	+	+	+
Поиск ресурса		+	+	+	+
Редактирование записи о ресурсе		+			+
Фильтрация ресурсов		+	+	+	+
Удаление ресурса		+			+
Добавление пользователей и групп, разрешенных для ресурса		+			+
Удаление пользователей и групп, разрешенных для ресурса		+			+
Получение списка пользователей и групп, разрешенных для ресурса		+	+	+	+
Массовое создание ресурсов в каталоге		+			+
Тенант					
Создание тенанта	+	+			+
Проверка успешности создания тенанта	+				+

Права доступа	Администратор инсталляции	Администратор тенанта	Администратор информационной безопасности	Администратор аудита	Супер- администратор
Удаление тенанта	+				+
Обновление атрибутов тенанта	+				+
Получение списка тенантов	+				+
Получение информации о тенанте	+				+
Получение информации о тенанте					+
GAL: пользователи и теги					
Создание GAL- пользователя в тенанте		+			+
Проверка существования GAL- пользователя		+			+
Создание пользовательских GAL-тегов		+			+
Получение GAL-тегов тенанта	+				+
Добавление пользователей к GAL- тегу		+			+
Проверка GAL- пользователя в тенанте		+			+
Создание системного GAL-пользователя	+				+
Создание GAL-тега для тенанта		+			+
Удаление GAL-тега		+			+
Получение списка GAL-тегов тенанта	+				+

Права доступа	Администратор инсталляции	Администратор тенанта	Администратор информационной безопасности	Администратор аудита	Супер- администратор
Удаление пользователей из GAL-тегов		+			+
Группа ALL					
Создание GAL	+				+
Проверка существования группы ALL	+	+			+
Создание группы ALL в тенанте					+
Создание группы ALL	+				
Делегирование групп					
Делегирование управления группами: <ul style="list-style-type: none"> • выдача прав на управление группой пользователю / пользователям; • отзыв прав у пользователя / пользователей 		+			+
Управление делегированием учетных записей		+			+
Двухфакторная аутентификация (2FA)					
Исключение администратора тенанта из перечня пользователей, попадающих под действие команды 2FA		+			+
Установка параметра 2FA тенанта (обновление тенанта)		+			+

Права доступа	Администратор инсталляции	Администратор тенанта	Администратор информационной безопасности	Администратор аудита	Супер- администратор
Сброс пользователю 2-го фактора		+			+
Обновление атрибутов тенанта		+			+
Письма					
Поиск писем по заданным критериям		+	+	+	+
+Поиск сведений о д+оставленных письмах		+	+	+	+
Ма+ссовое удаление писе+m		+			+
Удаление письма у всех получателей в рамках тенанта		+			+
Восстановление удаленных писем в почтовом ящике пользователя		+			+
Интеграции					
CO (Частное облако)	+				+
Squadus	+				+
OAuth2	+				+
Ansible / HashiCorp Vault	+				+
Skype 4 Business	+				+
TrueConf	+				+
eXpress	+				+
IVA	+				+
DLP Infowatch traffic monitor	+				+

Права доступа	Администратор инсталляции	Администратор тенанта	Администратор информационной безопасности	Администратор аудита	Супер- администратор
KLMS 10	+				+
KSMG	+				+
KSE (15.3)	+				+
SIEM KUMA	+				+
Кибер Протега (вопрос)	+				+
Microsoft Active Directory	+				+
FreeIPA	+				+
ALD Pro	+				+
РЕД АДМ	+				+
Samba DC	+				+
Катастрофоустойчивость					
Переключение нагрузки на резервный ЦОД	+				+
Без распределения					
Работа с корпоративными подписями пользователей в тенанте: <ul style="list-style-type: none"> • создание корпоративной подписи; • установка созданной корпоративной подписи как подписи по умолчанию; • удаление подписи 		+			+

Права доступа	Администратор инсталляции	Администратор тенанта	Администратор информационной безопасности	Администратор аудита	Супер- администратор
Управление сотрудниками: <ul style="list-style-type: none"> • добавление нового сотрудника в организационную структуру (создание нового пользователя); • поиск сотрудника; • редактирование записи о сотруднике; • удаление сотрудника 		+			+
Управление настройками: <ul style="list-style-type: none"> • просмотр и редактирование настроек организации/тенанта (регион, язык); • просмотр и редактирование настроек ограничения почты (размеры сообщений) 		+			+

ВНЕСЕННЫЕ ИЗМЕНЕНИЯ

Версия 2, дата публикации: 05.02.2025

1. Добавлен раздел [Управление почтовыми правилами и политиками](#).
2. Добавлен раздел [Регистрация событий в формате CEF](#).
3. Добавлен раздел [Настройка интеграции ADFS средствами SAML](#).
4. Добавлен раздел [Резервное копирование и восстановление всей инсталляции Mailion](#).
5. В раздел [Резервное копирование и восстановление отдельных сервисов](#) добавлен [подраздел для сервиса Vault](#).
6. В разделе [Настройка квот и лимитов для почты в тенанте](#) исправлено описание команды создания квот профиля пользователя `create_user_quotas_profile`.